



NAS 스토리지 관리

ONTAP 9

NetApp
February 14, 2026

목차

NAS 스토리지 관리	1
System Manager로 NAS 프로토콜을 관리합니다	1
ONTAP System Manager를 사용한 NAS 관리에 대해 알아보세요	1
ONTAP System Manager를 사용하여 VMware 데이터 저장소에 NFS 스토리지 프로비저닝	1
ONTAP 시스템 관리자를 사용하여 홈 디렉토리에 대한 NAS 스토리지 제공	2
ONTAP System Manager를 사용하여 NFS를 사용하여 Linux 서버용 NAS 스토리지 프로비저닝	3
ONTAP System Manager를 사용하여 내보내기 정책을 사용하여 액세스 관리	5
ONTAP 시스템 관리자를 사용하여 SMB를 사용하여 Windows 서버용 NAS 스토리지 프로비저닝	5
ONTAP System Manager를 사용하여 NFS와 SMB를 모두 사용하여 Windows와 Linux 모두에 대한 NAS 스토리지를 프로비저닝합니다.	8
ONTAP System Manager를 사용하여 Kerberos로 클라이언트 액세스 보안	10
ONTAP 시스템 관리자를 사용하여 이름 서비스를 통해 클라이언트 액세스를 제공합니다.	12
ONTAP System Manager를 사용하여 디렉토리 및 파일 관리	12
ONTAP System Manager를 사용하여 호스트별 사용자 및 그룹 관리	12
ONTAP 시스템 관리자를 사용하여 NFS 활성 클라이언트 모니터링	16
NAS 스토리지를 설정합니다.	16
NFS 구성	20
ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오	20
ONTAP NFS 구성 워크플로에 대해 알아보세요	21
준비	22
SVM에 대한 NFS 액세스를 구성합니다	34
NFS 지원 SVM에 스토리지 용량 추가	68
추가 ONTAP NFS 정보를 찾을 수 있는 곳	81
ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다르니까	83
NFS 관리	86
NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요	86
NAS 파일 액세스 이해	86
NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다	94
보안 스타일을 구성합니다	99
NFS를 사용하여 파일 액세스를 설정합니다	104
NFS를 사용하여 파일 액세스를 관리합니다	139
지원되는 NFS 버전 및 클라이언트	189
병렬 NFS	194
NFS 및 SMB 파일 및 디렉토리 명명 종속성	217
NFS 트렁킹을 관리합니다	222
ONTAP NFS 트렁킹에 대해 알아보십시오	222
트렁킹을 위해 새 NFS 서버 및 내보내기를 구성합니다	223
트렁킹을 위해 기존 NFS 내보내기 조정	228
RDMA를 통해 NFS를 관리합니다	233

ONTAP에서 RDMA를 통한 NFS에 대해 알아보십시오	233
RDMA를 통해 NFS용 NIC를 구성합니다	235
RDMA를 통해 NFS용 LIF를 구성합니다	237
NFS 구성을 수정합니다	240
CLI를 사용하여 SMB를 구성합니다	240
ONTAP CLI를 사용한 SMB 구성에 대해 알아보십시오	240
ONTAP SMB 구성 워크플로우	241
준비	242
SVM에 대한 SMB 액세스를 구성합니다	252
공유 스토리지에 대한 SMB 클라이언트 액세스를 구성합니다	272
CLI를 사용하여 SMB를 관리합니다	281
ONTAP SMB에 대해 알아보십시오	281
SMB 서버 지원	281
SMB 서버를 관리합니다	288
SMB를 사용하여 파일 액세스를 설정합니다	378
SMB를 사용하여 파일 액세스를 관리합니다	442
SMB 클라이언트 기반 서비스 구축	529
SMB 서버 기반 서비스 구축	542
NFS 및 SMB 파일 및 디렉토리 명명 종속성	608
NAS 데이터에 S3 클라이언트 액세스 제공	614
ONTAP S3 멀티프로토콜 지원에 대해 알아보세요	614
ONTAP S3 클라이언트 액세스를 위한 NAS 데이터 요구 사항에 대해 알아보세요	617
ONTAP SVM에서 NAS 데이터에 대한 S3 프로토콜 액세스 활성화	618
ONTAP S3 NAS 버킷 생성	620
ONTAP S3 클라이언트 사용자 활성화	622
Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성	625
Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 개요	625
SMB 솔루션을 통해 Microsoft Hyper-V 및 SQL Server용 ONTAP를 구성합니다	625
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영	626
원격 VSS와 공유 기반 백업	630
SMB 공유를 통해 Hyper-V 및 SQL Server에서 ODX 복사 오프로드를 사용하는 방법	634
구성 요구 사항 및 고려 사항	635
SMB 구성을 통한 SQL Server 및 Hyper-V 권장 사항	642
SMB를 통한 Hyper-V 또는 SQL Server 구성 계획	642
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 생성	646
SMB 구성을 통해 Hyper-V 및 SQL Server 관리	659
통계를 사용하여 SMB 작업을 통해 Hyper-V 및 SQL Server를 모니터링합니다	664
구성이 무중단 운영이 가능한지 확인합니다	667

NAS 스토리지 관리

System Manager로 NAS 프로토콜을 관리합니다

ONTAP System Manager를 사용한 NAS 관리에 대해 알아보세요

이 섹션에서는 ONTAP 9.7 이상 릴리즈에서 System Manager를 사용하여 NAS 환경을 구성하고 관리하는 방법을 설명합니다.

클래식 시스템 관리자(ONTAP 9.7 이전에서만 사용 가능)를 사용하는 경우 다음 항목을 참조하십시오.

- ["NFS 구성 개요"](#)
- ["SMB 구성 개요"](#)

System Manager는 다음과 같은 워크플로우를 지원합니다.

- NAS 파일 서비스에 사용할 클러스터의 초기 구성입니다.
- 변화하는 스토리지 요구사항에 부합하는 추가 볼륨 프로비저닝
- 업계 표준 인증 및 보안 시설을 위한 구성 및 유지 보수

System Manager를 사용하면 구성 요소 레벨에서 NAS 서비스를 관리할 수 있습니다.

- 프로토콜 - NFS, SMB 또는 둘 다(NAS 멀티 프로토콜)
- 이름 서비스 - DNS, LDAP 및 NIS
- 네임 서비스 스위치
- Kerberos 및 TLS 보안
- 수출 및 공유
- Qtree
- 사용자 및 그룹의 이름 매핑

ONTAP System Manager를 사용하여 VMware 데이터 저장소에 NFS 스토리지 프로비저닝

VMware vSphere(VSC)용 가상 스토리지 콘솔을 사용하여 ESXi 호스트용 ONTAP 기반 스토리지 시스템에서 NFS 볼륨을 프로비저닝하기 전에 ONTAP 9.7 이상용 System Manager를 사용하여 NFS를 사용하도록 설정하십시오.

을 만든 후 ["NFS 지원 스토리지 VM"](#) System Manager에서 NFS 볼륨을 프로비저닝하고 VSC를 사용하여 데이터 저장소를 관리할 수 있습니다.

VSC 7.0부터는 VSC가 의 일부입니다 ["VMware vSphere 가상 어플라이언스인 ONTAP 툴"](#)VSC, VASA(vStorage APIs for Storage Awareness) 공급자, VMware vSphere 기능을 위한 SRA(Storage Replication Adapter) 등이 포함되어 있습니다.

를 확인하십시오 ["NetApp 상호 운용성 매트릭스"](#) 현재 ONTAP 및 VSC 릴리스 간의 호환성을 확인합니다.

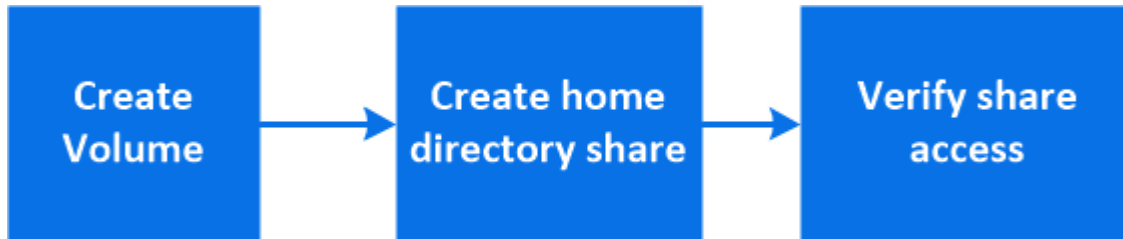
System Manager Classic(ONTAP 9.7 이하 릴리즈용)을 사용하여 ESXi 호스트에 대한 NFS 액세스를 데이터 저장소에 설정하려면 를 참조하십시오 ["VSC 개요를 사용한 ESXi용 NFS 구성"](#)

자세한 내용은 을 참조하십시오 ["TR-4597: ONTAP용 VMware vSphere"](#) VSC 릴리즈에 대한 설명서를 제공합니다.

ONTAP 시스템 관리자를 사용하여 홈 디렉토리에 대한 NAS 스토리지 제공

볼륨을 생성하여 SMB 프로토콜을 사용하여 홈 디렉토리에 대한 스토리지를 제공합니다.

이 절차를 수행하면 의 홈 디렉토리에 대한 새 볼륨이 생성됩니다 ["기존 SMB 지원 스토리지 VM"](#). 볼륨을 구성하거나 사용자 지정 구성을 지정할 때 시스템 기본값을 사용할 수 있습니다.



FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 또한 참조하십시오 ["FlexGroup 볼륨을 생성합니다"](#).

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 ["Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다"](#).

단계

1. SMB 지원 스토리지 VM에 새 볼륨을 추가합니다.

- a. 스토리지 > 볼륨 * 을 선택한 다음 * 추가 * 를 클릭합니다.
- b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

SMB 프로토콜로 구성된 스토리지 VM만 나열됩니다. SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

- 이때 * 저장 * 을 클릭하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.
- 추가 옵션 * 을 클릭하여 권한 부여, 서비스 품질 및 데이터 보호와 같은 서비스를 사용하도록 볼륨 구성을 사용자 지정할 수 있습니다. 을 참조하십시오 [볼륨 구성을 사용자 지정합니다](#) 그런 다음 여기로 돌아와 다음 단계를 완료합니다.

2. [[워크플로의 2단계, 2단계]] * 스토리지 > 공유 * 를 클릭하고 * 추가 * 를 클릭한 다음 * 홈 디렉토리 * 를 선택합니다.

3. Windows 클라이언트에서 다음을 수행하여 공유에 액세스할 수 있는지 확인합니다.

- a. Windows 탐색기에서 드라이브를 다음 형식으로 공유에 매핑합니다.

\\<SMB_Server_Name>\<Share_Name>

공유 이름이 변수(%w, %d 또는 %u)로 생성된 경우, 확인된 이름으로 액세스를 테스트하십시오.

- b. 새로 만든 드라이브에서 테스트 파일을 만든 다음 파일을 삭제합니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

- QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.
- 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.
- ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.



볼륨을 저장한 후 로 돌아갑니다 [\[step2\]](#) 홈 디렉토리에 대한 프로비저닝을 완료합니다.

ONTAP System Manager를 사용하여 NFS를 사용하여 Linux 서버용 NAS 스토리지 프로비저닝

ONTAP System Manager(9.7 이상)에서 NFS 프로토콜을 사용하여 Linux 서버용 스토리지를 제공할 볼륨을 생성합니다.

이 절차를 수행하면 새 볼륨이 생성됩니다 **"기존 NFS 지원 스토리지 VM"**. 볼륨을 구성하거나 사용자 지정 구성을 지정할 때 시스템 기본값을 사용할 수 있습니다.

FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 또한 참조하세요 **"FlexGroup 볼륨을 생성합니다"**.

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 **"Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다"**.

다양한 ONTAP NFS 프로토콜 기능에 대한 자세한 내용은 를 참조하십시오 **"NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요"**.

단계

1. NFS 지원 스토리지 VM에 새 볼륨을 추가합니다.

- 스토리지 > 볼륨 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
- 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

NFS 프로토콜로 구성된 스토리지 VM만 나열됩니다. SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

- 이때 * 저장 * 을 클릭하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.



기본 익스포트 정책은 모든 사용자에게 전체 액세스 권한을 부여합니다.

- 추가 옵션 * 을 클릭하여 권한 부여, 서비스 품질 및 데이터 보호와 같은 서비스를 사용하도록 볼륨 구성을 사용자 지정할 수 있습니다. 을 참조하십시오 [볼륨 구성을 사용자 지정합니다](#) 그런 다음 여기로 돌아와 다음 단계를 완료합니다.

2. Linux 클라이언트에서 다음을 수행하여 액세스를 확인합니다.

- 스토리지 VM의 네트워크 인터페이스를 사용하여 볼륨을 생성하고 마운트합니다.
- 새로 마운트된 볼륨에서 테스트 파일을 생성하고 텍스트를 기록한 다음 파일을 삭제합니다.

액세스를 확인한 후 을(를) 사용할 수 있습니다 ["볼륨의 익스포트 정책으로 클라이언트 액세스 제한"](#) 마운트된 볼륨에 대해 원하는 UNIX 소유권 및 권한을 설정합니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

- QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.
- 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.
- ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.



볼륨을 저장한 후 로 돌아갑니다 [Step 2 in the workflow](#) NFS를 사용하여 Linux 서버의 프로비저닝을 완료하려면 다음을 수행합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

이 작업을 수행하는 방법	자세한 내용은...
System Manager Classic(ONTAP 9.7 이하)	" NFS 구성 개요 "
ONTAP CLI(Command Line Interface)	" ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오 "

ONTAP System Manager를 사용하여 내보내기 정책을 사용하여 액세스 관리

내보내기 정책을 사용하여 NFS 서버에 대한 Linux 클라이언트 액세스를 설정합니다.

이 절차는 에 대한 익스포트 정책을 생성하거나 수정합니다 "[기존 NFS 지원 스토리지 VM](#)".

단계

1. System Manager에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. NFS 지원 볼륨을 클릭하고 * More * 를 클릭합니다.
3. Edit Export Policy * 를 클릭한 다음 * Select an existing policy * 또는 * Add a new policy * 를 클릭합니다.

ONTAP 시스템 관리자를 사용하여 **SMB**를 사용하여 **Windows** 서버용 **NAS** 스토리지 프로비저닝

ONTAP 9.7 이상에서 사용할 수 있는 System Manager를 사용하여 SMB 프로토콜을 사용하여 Windows 서버용 스토리지를 제공할 볼륨을 생성합니다.

이 절차를 수행하면 에 새 볼륨이 생성됩니다 "[기존 SMB 지원 스토리지 VM](#)" 볼륨 루트(/) 디렉토리에 대한 공유를 생성합니다. 볼륨을 구성하거나 사용자 지정 구성을 지정할 때 시스템 기본값을 사용할 수 있습니다. 초기 SMB 구성 후 추가 공유를 생성하고 해당 속성을 수정할 수도 있습니다.

FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 또한 참조하세요 "[FlexGroup 볼륨을 생성합니다](#)".

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 "[Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다](#)".

다양한 ONTAP SMB 프로토콜 기능에 대한 자세한 내용은 를 참조하십시오 "[참고 개요](#)".

시작하기 전에

- ONTAP 9.13.1부터 새로운 볼륨에 대해 용량 분석 및 활동 추적을 기본적으로 사용할 수 있습니다. System Manager에서 클러스터 또는 스토리지 VM 레벨의 기본 설정을 관리할 수 있습니다. 자세한 내용은 을 "[파일 시스템](#)"

분석 설정"참조하십시오.

단계

1. SMB 지원 스토리지 VM에 새 볼륨을 추가합니다.

- 스토리지 > 볼륨 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
- 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

SMB 프로토콜로 구성된 스토리지 VM만 나열됩니다. SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

- 이때 * 저장 * 을 선택하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.
- 추가 옵션 * 을 선택하여 권한 부여, 서비스 품질 및 데이터 보호와 같은 서비스를 사용할 수 있도록 볼륨 구성을 사용자 지정할 수 있습니다. 을 참조하십시오 [볼륨 구성을 사용자 지정합니다](#) 그런 다음 여기로 돌아와 다음 단계를 완료합니다.

2. 공유에 액세스할 수 있는지 확인하기 위해 Windows 클라이언트로 전환합니다.

- Windows 탐색기에서 '_SMB_Server_Name__Share_Name_' 형식으로 드라이브를 공유에 매핑합니다
- 새로 생성된 드라이브에서 테스트 파일을 만들고 텍스트를 기록한 다음 파일을 삭제합니다.

액세스를 확인한 후 공유 ACL을 사용하여 클라이언트 액세스를 제한하고 매핑된 드라이브에서 원하는 보안 속성을 설정할 수 있습니다. 자세한 내용은 ["공유 만들기"](#) 참조하십시오.

공유를 추가하거나 수정합니다

초기 SMB 구성 후 공유를 추가할 수 있습니다. 공유는 사용자가 선택한 기본 값과 속성으로 생성됩니다. 나중에 수정할 수 있습니다.

공유를 구성할 때 다음 공유 속성을 설정할 수 있습니다.

- 액세스 권한
- 공유 속성
 - SMB 데이터를 통해 Hyper-V 및 SQL Server를 포함하는 공유에 대해 지속적인 가용성을 지원합니다(ONTAP 9.10.1부터 시작). 참고 항목:
 - ["SMB를 통한 Hyper-V의 지속적인 가용성 공유 요구사항"](#)
 - ["SMB를 통한 SQL Server의 지속적인 가용성 공유 요구 사항"](#)
 - 이 공유에 액세스하는 동안 SMB 3.0으로 데이터를 암호화합니다.

초기 설정 후 다음 속성을 수정할 수도 있습니다.

- 심볼 링크
 - symlink와 Wipelink를 설정하거나 해제합니다
- 공유 속성
 - 클라이언트가 스냅샷 디렉토리에 액세스할 수 있도록 허용합니다.
 - oplocks를 설정하여 클라이언트가 파일을 잠그고 콘텐츠를 로컬에서 캐시할 수 있도록 합니다(기본값).

- 사용자의 액세스 권한을 기반으로 공유 리소스를 표시하려면 ABE(액세스 기반 열거)를 사용합니다.

단계

1. SMB 지원 볼륨에 새 공유를 추가하려면 스토리지 > 공유 를 클릭하고 추가 를 클릭한 다음 공유 를 선택합니다.
2. 기존 공유를 수정하려면 스토리지 > 공유 를 클릭한 다음  편집 을 선택합니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

- QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.
- 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.
- ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 폴다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.



볼륨을 저장한 후 로 돌아갑니다 [\[step2-compl-prov-win\]](#) SMB를 사용하여 Windows 서버에 대한 프로비저닝을 완료하려면 다음을 수행합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

이 작업을 수행하는 방법	자세한 내용은...
System Manager Classic(ONTAP 9.7 이하)	"SMB 구성 개요"
ONTAP 명령줄 인터페이스입니다	"CLI를 사용한 SMB 구성 개요"

ONTAP System Manager를 사용하여 **NFS**와 **SMB**를 모두 사용하여 **Windows**와 **Linux** 모두에 대한 **NAS** 스토리지를 프로비저닝합니다.

NFS 또는 SMB 프로토콜을 사용하여 클라이언트에 스토리지를 제공할 볼륨을 생성합니다.

이 절차를 수행하면 새 볼륨이 생성됩니다 ["NFS 및 SMB 프로토콜 모두에 대해 설정된 기존 스토리지 VM"](#).



NFS 프로토콜은 일반적으로 Linux 환경에서 사용됩니다. SMB 프로토콜은 일반적으로 Windows 환경에서 사용됩니다. 그러나 NFS와 SMB는 모두 Linux 또는 Windows에서 사용할 수 있습니다.

FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 보다 ["FlexGroup 볼륨을 생성합니다"](#).

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 ["Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다"](#).

단계

1. NFS와 SMB 모두에 대해 설정된 스토리지 VM에 새 볼륨을 추가합니다.

- 스토리지 > 볼륨 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
- 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

NFS 및 SMB 프로토콜을 모두 사용하여 구성된 스토리지 VM만 나열됩니다. NFS 및 SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

c. More Options * 를 클릭하고 * Export via NFS * 를 선택합니다.

기본 설정은 모든 사용자에게 전체 액세스 권한을 부여합니다. 나중에 내보내기 정책에 더 제한적인 규칙을 추가할 수 있습니다.

d. Share via SMB/CIFS * 를 선택합니다.

공유는 * Everyone * 그룹에 대해 "모든 권한"으로 설정된 기본 ACL(액세스 제어 목록)으로 생성됩니다. 나중에 ACL에 제한을 추가할 수 있습니다.

e. 이때 * 저장 * 을 클릭하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.

또는 인증, 서비스 품질 및 데이터 보호와 같은 추가 필수 서비스를 계속 활성화할 수도 있습니다. 을 참조하십시오 [볼륨 구성을 사용자 지정합니다](#) 그런 다음 여기로 돌아와 다음 단계를 완료합니다.

2. Linux 클라이언트에서 내보내기에 액세스할 수 있는지 확인합니다.

- 스토리지 VM의 네트워크 인터페이스를 사용하여 볼륨을 생성하고 마운트합니다.
- 새로 마운트된 볼륨에서 테스트 파일을 생성하고 텍스트를 기록한 다음 파일을 삭제합니다.

3. Windows 클라이언트에서 다음을 수행하여 공유에 액세스할 수 있는지 확인합니다.

a. Windows 탐색기에서 '_SMB_Server_Name__Share_Name_' 형식으로 드라이브를 공유에 매핑합니다

b. 새로 생성된 드라이브에서 테스트 파일을 만들고 텍스트를 기록한 다음 파일을 삭제합니다.

액세스를 확인한 후 "볼륨의 익스포트 정책으로 클라이언트 액세스를 제한하고 공유 ACL로 클라이언트 액세스를 제한합니다"내보낸 볼륨 및 공유 볼륨에 대해 원하는 소유권 및 권한을 설정할 수 있습니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

- QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.
- 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.
- ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.

볼륨을 저장한 후 로 돌아갑니다 [\[step2-compl-prov-nfs-smb\]](#) Windows 및 Linux 서버에 대한 멀티프로토콜 프로비저닝을 완료합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하)	"SMB 및 NFS 멀티 프로토콜 구성 개요"

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
ONTAP 명령줄 인터페이스입니다	• "CLI를 사용한 SMB 구성 개요" • "ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오" • "보안 스타일과 그 효과에 대해 알아보세요" • "다중 프로토콜 환경에서 파일 및 디렉토리 이름의 대/소문자를 구분하십시오"

ONTAP System Manager를 사용하여 Kerberos로 클라이언트 액세스 보안

NAS 클라이언트에 대한 스토리지 액세스를 보호하기 위해 Kerberos를 설정합니다.

이 절차에서는 에 대해 설정된 기존 스토리지 VM에서 Kerberos를 구성합니다 "NFS 를 참조하십시오" 또는 "중소기업".

시작하기 전에 DNS, NTP 및 를 구성해야 합니다 "LDAP를 지원합니다" 스토리지 시스템에서



단계

1. ONTAP 명령줄에서 스토리지 VM 루트 볼륨에 대한 UNIX 권한을 설정합니다.

- 스토리지 VM 루트 볼륨에 대한 관련 권한을 표시합니다 `volume show -volume root_vol_name -fields user,group,unix-permissions`. 에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

스토리지 VM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름...	설정 중...
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	755

- 이러한 값이 표시되지 않으면 `volume modify` 명령을 사용하여 값을 업데이트합니다. 에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스토리지 VM 루트 볼륨에 대한 사용자 권한을 설정합니다.

- 로컬 UNIX 사용자를 표시합니다 `vserver services name-service unix-user show -vserver vserver_name`. 에 대한 자세한 내용은 `vserver services name-service unix-user show` "ONTAP 명령 참조입니다"을 참조하십시오.

스토리지 VM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 ID입니다	기본 그룹 ID입니다
NFS 를 참조하십시오	500입니다	0
루트	0	0

+

- 참고: * NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다. 5단계를 참조하십시오.

- a. 이러한 값이 표시되지 않으면 `vserver services name-service unix-user modify` 명령을 사용하여 값을 업데이트합니다. 에 대한 자세한 내용은 `vserver services name-service unix-user modify` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 스토리지 VM 루트 볼륨에 대한 그룹 권한을 설정합니다.

- a. 로컬 UNIX 그룹을 표시합니다 `vserver services name-service unix-group show -vserver vserver_name`. 에 대한 자세한 내용은 `vserver services name-service unix-group show` "ONTAP 명령 참조입니다"을 참조하십시오.

스토리지 VM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 ID입니다
데몬	1
루트	0

- a. 이러한 값이 표시되지 않으면 `vserver services name-service unix-group modify` 명령을 사용하여 값을 업데이트합니다. 에 대한 자세한 내용은 `vserver services name-service unix-group modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. Kerberos를 구성하려면 System Manager로 전환합니다

5. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택합니다.

6. 설정 * 을 클릭합니다.

7. Kerberos 아래에서 를 → 클릭합니다.

8. Kerberos 영역 아래에서 * 추가 * 를 클릭하고 다음 섹션을 완료합니다.

- Kerberos 영역 추가

KDC 공급업체에 따라 구성 세부 정보를 입력합니다.

- Realm에 네트워크 인터페이스를 추가합니다

추가 * 를 클릭하고 네트워크 인터페이스를 선택합니다.

9. 필요한 경우 Kerberos 사용자 이름에서 로컬 사용자 이름으로 매핑을 추가합니다.

- a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택합니다.
- b. 설정 * 을 클릭한 다음 * 이름 매핑 * 아래에서 를 → 클릭합니다.
- c. UNIX * 에 대한 Kerberos * 에서 정규식을 사용하여 패턴 및 교체를 추가합니다.

ONTAP 시스템 관리자를 사용하여 이름 서비스를 통해 클라이언트 액세스를 제공합니다.

ONTAP에서 LDAP 또는 NIS를 사용하여 호스트, 사용자, 그룹 또는 넷그룹 정보를 조회하여 NAS 클라이언트를 인증합니다.

이 절차는 에 대해 설정된 기존 스토리지 VM에 대한 LDAP 또는 NIS 구성을 생성하거나 수정합니다 ["NFS 를 참조하십시오"](#) 또는 ["중소기업"](#).

LDAP 구성의 경우 환경에 필요한 LDAP 구성 세부 정보가 있어야 하며 기본 ONTAP LDAP 스키마를 사용해야 합니다.

단계

1. 필요한 서비스를 구성합니다. * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 스토리지 VM을 선택하고 * Settings * 를 클릭한 다음 LDAP 또는 NIS를  클릭합니다.
3. 이름 서비스 스위치의 변경 내용 포함: 이름 서비스 스위치 아래에서 를 클릭합니다  .

ONTAP System Manager를 사용하여 디렉토리 및 파일 관리

System Manager 볼륨 표시를 확장하여 디렉토리 및 파일을 보고 삭제합니다.

ONTAP 9.9.1부터 지연 시간이 짧은 비동기 디렉토리 삭제 기능으로 디렉토리가 삭제됩니다.

ONTAP 9.9.1 이상에서 파일 시스템을 보는 방법에 대한 자세한 내용은 을 참조하십시오 ["파일 시스템 분석 개요"](#).

단계

1. 스토리지 > 볼륨 * 을 선택합니다. 볼륨을 확장하여 내용을 봅니다.

ONTAP System Manager를 사용하여 호스트별 사용자 및 그룹 관리

ONTAP 9.10.1부터 System Manager를 사용하여 UNIX 또는 Windows 호스트별 사용자 및 그룹을 관리할 수 있습니다.

다음 절차를 수행할 수 있습니다.

Windows	Unix
• Windows 사용자 및 그룹을 봅니다 • [add-edit-delete-Windows] • [manage-windows-users]	• UNIX 사용자 및 그룹 보기 • [add-edit-delete-UNIX] • [manage-unix-users]

Windows 사용자 및 그룹을 봅니다

System Manager에서 Windows 사용자 및 그룹 목록을 볼 수 있습니다.

단계

1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다.

3. 호스트 사용자 및 그룹 * 영역으로 스크롤합니다.

Windows * 섹션은 선택한 스토리지 VM과 연결된 각 그룹의 사용자 수에 대한 요약 표시합니다.

4. →Windows * 섹션을 클릭합니다.

5. 그룹 * 탭을 클릭한 다음 그룹 이름 옆에 있는 을 ▼ 클릭하여 해당 그룹에 대한 세부 정보를 봅니다.

6. 그룹의 사용자를 보려면 그룹을 선택한 다음 * 사용자 * 탭을 클릭합니다.

Windows 그룹을 추가, 편집 또는 삭제합니다

System Manager에서 Windows 그룹을 추가, 편집 또는 삭제하여 관리할 수 있습니다.

단계

1. System Manager에서 Windows 그룹 목록을 봅니다. 을 참조하십시오 [Windows 사용자 및 그룹을 봅니다](#).
2. 그룹 * 탭에서 다음 작업으로 그룹을 관리할 수 있습니다.

이 작업을 수행하려면...	다음 단계를 수행합니다.
그룹을 추가합니다	1. 을 클릭합니다 + Add . 2. 그룹 정보를 입력합니다. 3. 권한을 지정합니다. 4. 그룹 구성원(로컬 사용자, 도메인 사용자 또는 도메인 그룹 추가)을 지정합니다.
그룹을 편집합니다	1. 그룹 이름 옆에 있는 을 : 클릭한 다음 * 편집 * 을 클릭합니다. 2. 그룹 정보를 수정합니다.
그룹을 삭제합니다	1. 삭제할 그룹 옆에 있는 확인란을 선택합니다. 2. 을 Delete 클릭합니다. ◦ 참고: * 그룹 이름 옆에 있는 을 클릭한 다음 * 삭제 * 를 클릭하여 단일 그룹을 삭제할 수도 있습니다.

Windows 사용자를 관리합니다

System Manager에서 Windows 사용자를 추가, 편집, 삭제, 활성화 또는 비활성화하여 관리할 수 있습니다. Windows 사용자의 암호를 변경할 수도 있습니다.

단계

1. System Manager에서 그룹의 사용자 목록을 봅니다. 을 참조하십시오 [Windows 사용자 및 그룹을 봅니다](#).
2. 사용자 * 탭에서 다음 작업을 통해 사용자를 관리할 수 있습니다.

이 작업을 수행하려면...	다음 단계를 수행합니다.

사용자를 추가합니다	1. 을 클릭합니다 + Add. 2. 사용자 정보를 입력합니다.
사용자를 편집합니다	1. 사용자 이름 옆에 있는 을 :클릭한 다음 * 편집 * 을 클릭합니다. 2. 사용자 정보를 수정합니다.
사용자를 삭제합니다	1. 삭제할 사용자 옆에 있는 확인란을 선택합니다. 2. 을 Delete 클릭합니다. ◦ 참고: * 사용자 이름 옆에 있는 을 클릭한 다음 * 삭제 * 를 클릭하여 단일 사용자를 삭제할 수도 : 있습니다.
사용자 암호를 변경합니다	1. 사용자 이름 옆에 있는 을 :클릭한 다음 * 암호 변경 * 을 클릭합니다. 2. 새 암호를 입력하고 확인합니다.
사용자를 활성화합니다	1. 활성화할 비활성화된 각 사용자 옆에 있는 확인란을 선택합니다. 2. 을 Enable 클릭합니다.
사용자를 비활성화합니다	1. 비활성화할 각 활성화된 사용자 옆에 있는 확인란을 선택합니다. 2. 을 Disable 클릭합니다.

UNIX 사용자 및 그룹 보기

System Manager에서 UNIX 사용자 및 그룹 목록을 볼 수 있습니다.

단계

1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다.
3. 호스트 사용자 및 그룹 * 영역으로 스크롤합니다.

UNIX * 섹션에는 선택한 스토리지 VM과 연결된 각 그룹의 사용자 수가 요약되어 표시됩니다.

4. UNIX * 섹션을 클릭합니다 **→**.
5. 그룹 * 탭을 클릭하여 해당 그룹에 대한 세부 정보를 봅니다.
6. 그룹의 사용자를 보려면 그룹을 선택한 다음 * 사용자 * 탭을 클릭합니다.

UNIX 그룹을 추가, 편집 또는 삭제합니다

System Manager에서는 UNIX 그룹을 추가, 편집 또는 삭제하여 관리할 수 있습니다.

단계

1. System Manager에서 UNIX 그룹 목록을 봅니다. 을 참조하십시오 [UNIX 사용자 및 그룹 보기](#).
2. 그룹 * 탭에서 다음 작업으로 그룹을 관리할 수 있습니다.

이 작업을 수행하려면...	다음 단계를 수행합니다.
그룹을 추가합니다	1. 을 클릭합니다  Add. 2. 그룹 정보를 입력합니다. 3. (선택 사항) 연결된 사용자를 지정합니다.
그룹을 편집합니다	1. 그룹을 선택합니다. 2. 을 클릭합니다  Edit. 3. 그룹 정보를 수정합니다. 4. (선택 사항) 사용자를 추가하거나 제거합니다.
그룹을 삭제합니다	1. 삭제할 그룹을 선택합니다. 2. 을  Delete 클릭합니다.

UNIX 사용자 관리

System Manager에서 Windows 사용자를 추가, 편집 또는 삭제하여 관리할 수 있습니다.

단계

1. System Manager에서 그룹의 사용자 목록을 봅니다. 을 참조하십시오 [UNIX 사용자 및 그룹 보기](#).
2. 사용자 * 탭에서 다음 작업을 통해 사용자를 관리할 수 있습니다.

이 작업을 수행하려면...	다음 단계를 수행합니다.
사용자를 추가합니다	1. 을 클릭합니다  Add. 2. 사용자 정보를 입력합니다.
사용자를 편집합니다	1. 편집할 사용자를 선택합니다. 2. 을 클릭합니다  Edit. 3. 사용자 정보를 수정합니다.
사용자를 삭제합니다	1. 삭제할 사용자를 선택합니다. 2. 을  Delete 클릭합니다.

ONTAP 시스템 관리자를 사용하여 NFS 활성 클라이언트 모니터링

ONTAP 9.8부터 System Manager는 NFS 라이선스가 클러스터에서 라이선스될 때 활성 상태인 NFS 클라이언트 연결을 보여 줍니다.

따라서 연결되어 있지만 유향 상태이며 연결이 끊긴 스토리지 VM에 능동적으로 접속되어 있는 NFS 클라이언트를 빠르게 확인할 수 있습니다.

각 NFS 클라이언트 IP 주소에 대해 * NFS 클라이언트 * 디스플레이에 마지막 액세스 시간 * 네트워크 인터페이스 IP 주소 * NFS 연결 버전 * 스토리지 VM 이름이 표시됩니다

또한 지난 48시간 동안 활성화된 NFS 클라이언트 목록도 * Storage > Volumes * 디스플레이에 표시되고 NFS 클라이언트 수가 * Dashboard * 디스플레이에 포함됩니다.

단계

1. NFS 클라이언트 작업 표시: * 호스트 > NFS 클라이언트 * 를 클릭합니다.

NAS 스토리지를 설정합니다

ONTAP 시스템 관리자를 사용하여 NFS를 사용하여 Linux 서버에 NAS 스토리지 활성화

스토리지 VM을 생성하거나 수정하여 NFS 서버에서 Linux 클라이언트에 데이터를 제공할 수 있도록 합니다.

다음 절차를 사용하여 NFS 프로토콜에 새 스토리지 VM 또는 기존 스토리지 VM을 사용하도록 설정합니다.



시작하기 전에

사용자 환경에 필요한 네트워킹, 인증 또는 보안 서비스에 대한 구성 세부 정보를 기록해 두십시오.

단계

1. 스토리지 VM에서 NFS를 사용하도록 설정합니다.
 - 새 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 * 추가 * 를 클릭하고 스토리지 VM 이름을 입력한 다음 * SMB/CIFS, NFS, S3 * 탭에서 * NFS * 활성화 * 를 선택합니다.
 - i. 기본 언어를 확인합니다.
 - ii. 네트워크 인터페이스를 추가합니다.
 - iii. 스토리지 VM 관리자 계정 정보 업데이트(선택 사항)
 - 기존 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택하고 * 설정 * 을 클릭한 다음  * NFS * 아래를 클릭합니다.
2. 스토리지 VM 루트 볼륨의 익스포트 정책을 엽니다.
 - a. 스토리지 > 볼륨 * 을 클릭하고 스토리지 VM의 루트 볼륨(기본값: _volume-name__root)을 선택한 다음 * 정책

내보내기 * 아래에 표시되는 정책을 클릭합니다.

b. 규칙을 추가하려면 * 추가 * 를 클릭합니다.

- 클라이언트 사양 = 0.0.0.0/0
- 액세스 프로토콜 = NFS
- 액세스 세부 정보 = UNIX 읽기 전용

3. 호스트 이름 확인을 위한 DNS 구성: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 * DNS * 아래에서 * 를 클릭합니다 .

4. 필요에 따라 이름 서비스를 구성합니다.

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 LDAP 또는 NIS를 클릭합니다 .

b.  이름 서비스 스위치 타일을 클릭하여 변경 내용을 포함합니다.

5. 필요한 경우 Kerberos 구성:

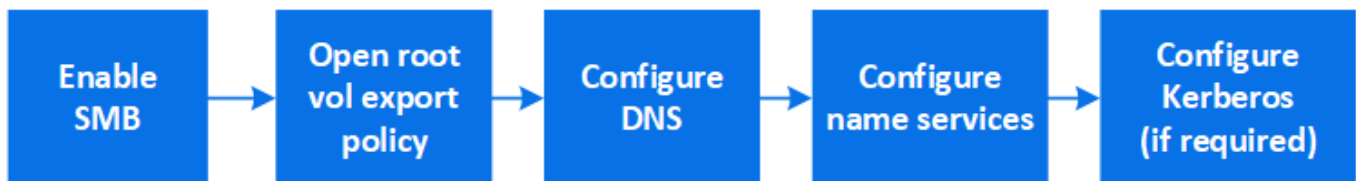
a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

b.  Kerberos 타일을 클릭한 다음 * 추가 * 를 클릭합니다.

ONTAP 시스템 관리자를 사용하여 **SMB**를 사용하여 **Windows** 서버에 **NAS** 스토리지 활성화

스토리지 VM을 생성 또는 수정하여 SMB 서버에서 Windows 클라이언트에 데이터를 제공할 수 있도록 합니다.

이 절차를 사용하면 SMB 프로토콜을 위한 신규 또는 기존 스토리지 VM을 사용할 수 있습니다. 사용자 환경에 필요한 네트워킹, 인증 또는 보안 서비스에 대해 구성 세부 정보를 사용할 수 있다고 가정합니다.



단계

1. 스토리지 VM에서 SMB를 사용하도록 설정합니다.

a. 새 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 * 추가 * 를 클릭한 다음 스토리지 VM 이름을 입력하고 * SMB/CIFS, NFS, S3 * 탭에서 * SMB/CIFS * 활성화 를 선택합니다.

- 다음 정보를 입력합니다.
 - 관리자 이름 및 암호
 - 서버 이름입니다
 - Active Directory 도메인입니다
- 조직 구성 단위를 확인합니다.
- DNS 값을 확인합니다.
- 기본 언어를 확인합니다.
- 네트워크 인터페이스를 추가합니다.

- 스토리지 VM 관리자 계정 정보 업데이트(선택 사항)

b. 기존 스토리지 VM의 경우:: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택하고 * 설정 * 을 클릭한 다음  * SMB * 아래를 클릭합니다.

2. 스토리지 VM 루트 볼륨의 익스포트 정책을 엽니다.

a. 스토리지 > 볼륨 * 을 클릭하고 스토리지 VM의 루트 볼륨(기본값: *volume-name_root*)을 선택한 다음 * 정책 내보내기 * 아래에 표시되는 정책을 클릭합니다.

b. 규칙을 추가하려면 * 추가 * 를 클릭합니다.

- 클라이언트 사양 = 0.0.0.0/0
- 액세스 프로토콜 = SMB
- 액세스 세부 정보 = NTFS 읽기 전용

3. 호스트 이름 확인을 위해 DNS 구성:

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * Settings * 를 클릭하고 * DNS * 아래에서 * 를 클릭합니다 .

b. DNS 서버로 전환하고 SMB 서버를 매핑합니다.

- 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.
- NetBIOS 별칭을 사용하는 경우 별칭 정식 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버의 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.

4. 필요에 따라 이름 서비스를 구성합니다

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 후 * Settings * 를 클릭한 다음 * LDAP * 또는 * NIS * 아래를 클릭합니다 .

b. 이름 서비스 스위치 파일에 변경 내용 포함: * 이름 서비스 스위치 * 를 클릭합니다 .

5. 필요한 경우 Kerberos 구성:

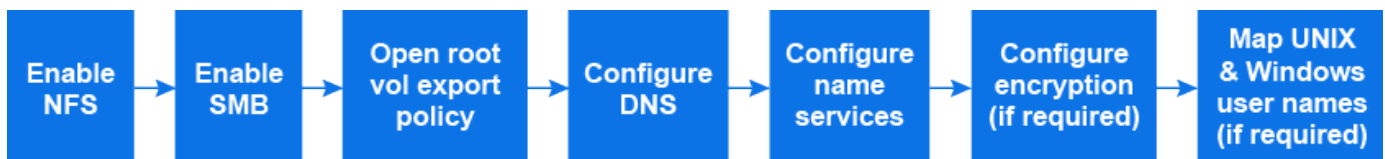
a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

b. →Kerberos * 아래에서 * Add * 를 클릭합니다.

ONTAP 시스템 관리자를 사용하여 **NFS**와 **SMB**를 모두 사용하여 **Windows**와 **Linux** 모두에서 **NAS** 스토리지를 활성화합니다.

NFS 및 SMB 서버가 Linux 및 Windows 클라이언트에 데이터를 제공할 수 있도록 스토리지 VM을 생성하거나 수정합니다.

다음 절차를 사용하여 신규 또는 기존 스토리지 VM이 NFS 및 SMB 프로토콜을 모두 처리하도록 지원할 수 있습니다.



시작하기 전에

사용자 환경에 필요한 네트워킹, 인증 또는 보안 서비스에 대한 구성 세부 정보를 기록해 두십시오.

단계

1. 스토리지 VM에서 NFS 및 SMB를 사용하도록 설정합니다.

- 새 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 * 추가 * 를 클릭한 다음 스토리지 VM 이름을 입력하고 * SMB/CIFS, NFS, S3 * 탭에서 * SMB/CIFS * 활성화 및 * NFS * 활성화 를 선택합니다.
- 다음 정보를 입력합니다.
 - 관리자 이름 및 암호
 - 서버 이름입니다
 - Active Directory 도메인입니다
- 조직 구성 단위를 확인합니다.
- DNS 값을 확인합니다.
- 기본 언어를 확인합니다.
- 네트워크 인터페이스를 추가합니다.
- 스토리지 VM 관리자 계정 정보 업데이트(선택 사항)
- 기존 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다. NFS 또는 SMB가 아직 활성화되지 않은 경우 다음 하위 단계를 완료합니다.
 - NFS * 아래에서  를 클릭합니다.
 - smb * 아래에서 * 를  를 클릭합니다.

2. 스토리지 VM 루트 볼륨의 익스포트 정책을 엽니다.

- 스토리지 > 볼륨 * 을 클릭하고 스토리지 VM의 루트 볼륨(기본값: `volume-name_root`)을 선택한 다음 * 정책 내보내기 * 아래에 표시되는 정책을 클릭합니다.
- 규칙을 추가하려면 * 추가 * 를 클릭합니다.
 - 클라이언트 사양 = 0.0.0.0/0
 - 액세스 프로토콜 = NFS
 - 액세스 세부 정보 = NFS 읽기 전용

3. 호스트 이름 확인을 위해 DNS 구성:

- 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * Settings * 를 클릭하고 * DNS * 아래에서 * 를 클릭합니다  .
- DNS 구성이 완료되면 DNS 서버로 전환하고 SMB 서버를 매핑합니다.
 - 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.
 - NetBIOS 별칭을 사용하는 경우 별칭 정식 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버의 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.

4. 필요에 따라 이름 서비스 구성:

- 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 LDAP 또는 NIS를 클릭합니다  .
- 이름 서비스 스위치 파일에 변경 내용 포함: * 이름 서비스 스위치 * 를 클릭합니다  .

5. 필요한 경우 Kerberos 구성:

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

b. →Kerberos 타일을 클릭한 다음 * 추가 * 를 클릭합니다.

6. 필요한 경우 UNIX 및 Windows 사용자 이름 매핑: * 이름 매핑 * 아래에서 * 추가 * 를 → 클릭합니다.

사이트에 암시적으로 매핑되지 않는 Windows 및 UNIX 사용자 계정이 있는 경우에만 이 작업을 수행해야 합니다. 즉, 각 Windows 사용자 이름의 소문자 버전이 UNIX 사용자 이름과 일치하는 경우에만 이 작업을 수행해야 합니다. LDAP, NIS 또는 로컬 사용자를 사용하여 사용자 이름을 매핑할 수 있습니다. 일치하지 않는 두 사용자 세트가 있는 경우 이름 매핑을 구성해야 합니다.

NFS 구성

ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오

ONTAP 9 CLI 명령을 사용하여 새 SVM(스토리지 가상 머신) 또는 기존 SVM(스토리지 가상 머신)에서 새 볼륨 또는 qtree에 포함된 파일에 대한 NFS 클라이언트 액세스를 구성할 수 있습니다.

다음과 같은 방법으로 볼륨 또는 qtree에 대한 액세스를 구성하려면 다음 절차를 사용하십시오.

- 현재 ONTAP에서 지원하는 모든 버전의 NFS, NFSv3, NFSv4, NFSv4.1, NFSv4.2 또는 pNFS를 사용하는 NFSv4.1을 사용하려고 합니다.

- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

System Manager를 사용하여 NAS 멀티 프로토콜 액세스를 구성하려면 를 참조하십시오"[NFS와 SMB를 모두 사용하여 Windows 및 Linux 모두에 대해 NAS 스토리지를 프로비저닝합니다](#)".

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.

명령 구문에 대한 자세한 내용은 를 "[ONTAP 명령 참조입니다](#)"참조하십시오.

- 새 볼륨의 보안을 위해 UNIX 파일 권한이 사용됩니다.
- SVM 관리자 권한이 아닌 클러스터 관리자 권한이 있습니다.

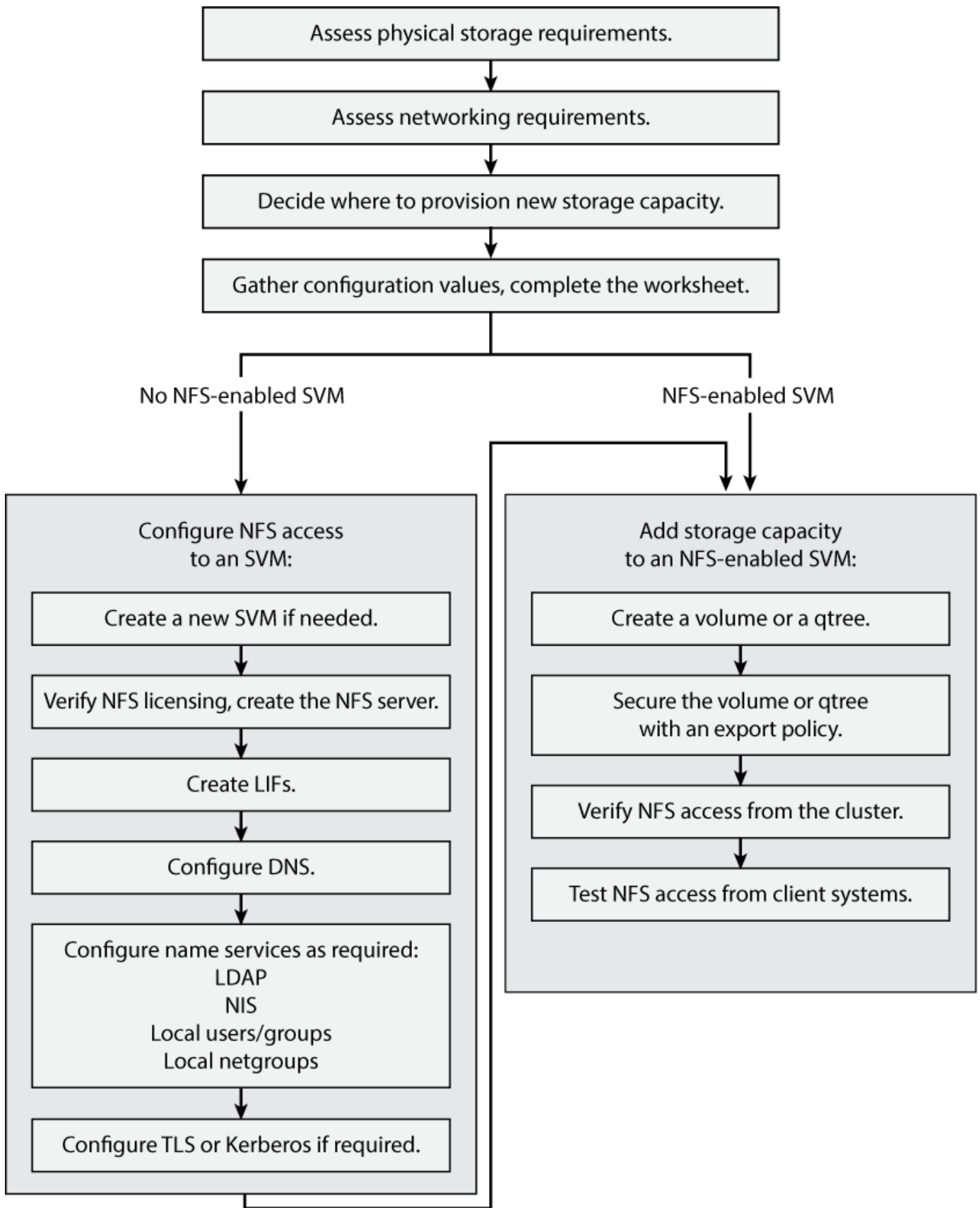
다양한 ONTAP NFS 프로토콜 기능에 대한 자세한 내용은 를 참조하십시오"[NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요](#)".

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	자세한 내용은...
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	" NFS를 사용하여 Linux 서버용 NAS 스토리지 용량 할당 "
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	" NFS 구성 개요 "

ONTAP NFS 구성 워크플로에 대해 알아보세요

NFS를 구성하려면 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음, 목표에 맞는 워크플로우를 선택해야 합니다. 새로운 SVM 또는 기존 SVM에 대한 NFS 액세스를 구성하거나, NFS 액세스를 위해 이미 완벽하게 구성된 기존 SVM에 볼륨 또는 qtree를 추가하십시오.



준비

ONTAP NFS의 물리적 스토리지 요구사항을 평가합니다

클라이언트용 NFS 스토리지를 프로비저닝하기 전에 새 볼륨에 대한 기존 애그리게이트에 충분한 공간이 있는지 확인해야 합니다. 없는 경우 디스크를 기존 Aggregate에 추가하거나 원하는 유형의 새 Aggregate를 생성할 수 있습니다.

단계

1. 기존 애그리게이트에서 사용 가능한 공간 표시:

'스토리지 집계 쇼'

공간이 충분한 집계에 있는 경우 워크시트에 이름을 기록합니다.

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_1         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_2         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_3         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_4         239.0GB   238.9GB   95% online    5 node3  raid_dp, normal
aggr_5         239.0GB   239.0GB   95% online    4 node4  raid_dp, normal
6 entries were displayed.
```

2. 충분한 공간이 있는 애그리게이트가 없는 경우 'Storage aggregate add-disks' 명령을 사용하여 기존 애그리게이트에 디스크를 추가하거나 'Storage aggregate create' 명령을 사용하여 새로운 애그리게이트를 생성합니다.

관련 정보

- ["로컬 계층에 디스크 추가\(애그리게이트\)"](#)
- ["스토리지 집계 추가 디스크"](#)
- ["저장소 집계 생성"](#)

ONTAP NFS 네트워크 구성 요구 사항 평가

NFS 스토리지를 클라이언트에 제공하기 전에 NFS 프로비저닝 요구 사항을 충족하도록 네트워킹이 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

다음과 같은 클러스터 네트워킹 객체를 구성해야 합니다.

- 물리적 및 논리적 포트
- 브로드캐스트 도메인
- 서브넷(필요한 경우)
- IPspace(기본 IPspace 외에 필요 시)
- 페일오버 그룹(필요에 따라 각 브로드캐스트 도메인의 기본 페일오버 그룹 추가)
- 외부 방화벽

단계

1. 사용 가능한 물리적 포트 및 가상 포트를 표시합니다.

네트워크 포트 쇼

- 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.
- 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.
- 에 대한 자세한 내용은 `network port show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. 서브넷 이름을 사용하여 LIF에 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하는지, 사용 가능한 주소가 충분한지 확인합니다. +

네트워크 서브넷 쇼

에 대한 자세한 내용은 `network subnet show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 서브넷은 `network subnet create` 명령을 사용하여 생성된다.

에 대한 자세한 내용은 `network subnet create` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

3. 사용 가능한 IPspace 표시:

네트워크 IPspace 쇼

기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

에 대한 자세한 내용은 `network ipspace show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

4. IPv6 주소를 사용하려면 클러스터에서 IPv6이 활성화되어 있는지 확인합니다.

네트워크 옵션 IPv6 쇼

필요한 경우 'network options ipv6 modify' 명령을 사용하여 IPv6을 사용하도록 설정할 수 있습니다.

및 `network options ipv6 modify` 에 대한 자세한 `network options ipv6 show` 내용은 을 "[ONTAP 명령 참조입니다](#)"참조하십시오.

ONTAP NFS 스토리지 용량 프로비저닝에 대해 알아보십시오

새 NFS 볼륨 또는 qtree를 생성하기 전에 새로운 SVM이나 기존 SVM에 배치할지 여부와

SVM에 필요한 구성의 크기를 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

선택

- 새 SVM에서 볼륨 또는 qtree를 프로비저닝하거나 NFS가 활성화되어 있지만 구성되지 않은 기존 SVM에서 프로비저닝하려면 "SVM에 NFS 액세스 구성" 및 "NFS 스토리지를 NFS 지원 SVM에 추가" 단계를 완료하십시오.

SVM에 대한 NFS 액세스를 구성합니다

NFS 지원 SVM에 NFS 스토리지를 추가합니다

다음 중 하나에 해당하는 경우 새 SVM을 생성할 수 있습니다.

- 클러스터에서 NFS를 처음으로 사용하도록 설정하고 있습니다.
- NFS 지원을 사용하지 않으려는 클러스터에 기존 SVM이 있습니다.
- 하나의 클러스터에 NFS 지원 SVM이 하나 이상 있으며 다른 NFS 서버를 격리된 네임스페이스(멀티 테넌시 시나리오)로 사용하려는 경우를 가정해 보겠습니다. NFS가 활성화되었지만 구성되지 않은 기존 SVM에서 스토리지를 프로비저닝하려면 이 옵션을 선택해야 합니다. 이는 SAN 액세스를 위해 SVM을 생성했거나, SVM 생성 시 프로토콜을 사용하지 않은 경우에 발생할 수 있습니다.

SVM에서 NFS를 사용하도록 설정한 후 볼륨 또는 qtree를 프로비저닝합니다.

- NFS 액세스를 위해 완전히 구성된 기존 SVM에서 볼륨 또는 qtree를 프로비저닝하려면 "NFS 스토리지를 NFS 지원 SVM에 추가"의 단계를 완료하십시오.

NFS 지원 SVM에 NFS 스토리지 추가

ONTAP NFS 구성 워크시트

NFS 구성 워크시트를 사용하면 클라이언트에 대한 NFS 액세스를 설정하는 데 필요한 정보를 수집할 수 있습니다.

스토리지 용량 할당 위치에 대한 결정에 따라 워크시트의 섹션 중 하나 또는 두 섹션을 모두 완료해야 합니다.

SVM에 대한 NFS 액세스를 구성하는 경우 두 섹션을 모두 완료해야 합니다.

- SVM에 대한 NFS 액세스 구성
- NFS 지원 SVM에 스토리지 용량 추가

NFS 지원 SVM에 스토리지 용량을 추가하는 경우 다음 작업만 완료해야 합니다.

- NFS 지원 SVM에 스토리지 용량 추가

SVM에 대한 NFS 액세스를 구성합니다

- SVM 생성을 위한 매개 변수 *

새 SVM을 생성하는 경우 이러한 값을 'vserver create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치

'-vserver'	FQDN(정규화된 도메인 이름)이거나 클러스터 전체에 고유한 SVM 이름을 적용하는 다른 규칙을 따르는 새 SVM에 대해 제공하는 이름입니다.	
'-집계'	새 NFS 스토리지 용량을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-rootvolume'	SVM 루트 볼륨에 제공하는 고유 이름입니다.	
'-rootvolume-security-style'	SVM에 UNIX 보안 스타일을 사용합니다.	유닉스
'-언어'	이 워크플로의 기본 언어 설정을 사용합니다.	1. UTF-8
'IPSpace'	IPspace는 SVM(스토리지 가상 머신)이 상주하는 고유 IP 주소 공간입니다.	

• NFS 서버 생성을 위한 매개 변수 *

새 NFS 서버를 생성하고 지원되는 NFS 버전을 지정할 때 이러한 값을 'vserver NFS create' 명령으로 제공합니다.

NFSv4 이상을 설정하는 경우 보안을 강화하기 위해 LDAP를 사용해야 합니다.

필드에 입력합니다	설명	귀사의 가치
v3 -v4.0 -v4.1 -v4.1 -v4.1 -pNFS	필요에 따라 NFS 버전을 사용하도록 설정합니다.  v4.2는 v4.1이 활성화된 경우 ONTAP 9.8 이상에서도 지원됩니다.	
'-v4-id-domain'	ID 매핑 도메인 이름입니다.	
'-v4-numeric-ids'	숫자 소유자 ID 지원(사용 또는 사용 안 함)	

• LIF 생성을 위한 매개 변수 *

LIF를 생성할 때 이러한 값을 명령과 함께 `network interface create` 제공합니다. 에 대한 자세한 내용은

network interface create "ONTAP 명령 참조입니다"을 참조하십시오.

Kerberos를 사용하는 경우 여러 LIF에서 Kerberos를 사용하도록 설정해야 합니다.

필드에 입력합니다	설명	귀사의 가치
'-lif'	새 LIF에 대해 제공한 이름입니다.	
'-역할'	이 워크플로우에서 데이터 LIF 역할을 사용합니다.	다타
'-데이터-프로토콜'	이 워크플로우에서는 NFS 프로토콜만 사용합니다.	'NFS'입니다
홈 노드	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행할 때 LIF가 반환되는 노드입니다. 에 대한 자세한 내용은 network interface revert "ONTAP 명령 참조입니다"을 참조하십시오.	
``홈 포트``	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 포트 또는 인터페이스 그룹입니다.	
주소	새 LIF가 데이터 액세스에 사용할 클러스터의 IPv4 또는 IPv6 주소입니다.	
넷마스크입니다	LIF의 네트워크 마스크와 게이트웨이입니다.	
'-서브넷'	IP 주소 풀입니다. 주소와 넷마스크를 자동으로 할당하기 위해 -address와 -netmask 대신 사용됩니다.	
방화벽 정책	이 워크플로우에서 기본 데이터 방화벽 정책을 사용합니다.	다타

- DNS 호스트 이름 확인을 위한 매개 변수 *

DNS를 구성할 때 이러한 값을 'vserver services name-service dns create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치
``도메인``	최대 5개의 DNS 도메인 이름	

이름-서버	각 DNS 이름 서버에 대해 최대 3개의 IP 주소를 지정할 수 있습니다.	

네임 서비스 정보

- 로컬 사용자 생성을 위한 매개 변수 *

'vserver services name-service unix-user create' 명령을 사용하여 로컬 사용자를 생성하는 경우 이러한 값을 제공합니다. UNIX 사용자가 포함된 파일을 URI(Uniform Resource Identifier)에서 로드하여 로컬 사용자를 구성하는 경우에는 이러한 값을 수동으로 지정할 필요가 없습니다.

	사용자 이름 '(-user)'입니다	사용자 ID '(-id)'입니다	그룹 ID '(-primary-gid)'입니다	전체 이름(-full-name)
예	합니다	123을 선택합니다	100	존 밀러
1				
2				
3				
...				
해당 없음				

- 로컬 그룹 생성을 위한 매개 변수 *

'vserver services name-service unix-group create' 명령을 사용하여 로컬 그룹을 생성하는 경우 이러한 값을 제공합니다. URI에서 UNIX 그룹이 포함된 파일을 로드하여 로컬 그룹을 구성하는 경우에는 이러한 값을 수동으로 지정할 필요가 없습니다.

	그룹 이름('(-name)')	Group ID('(-id)')
예	엔지니어링	100
1		
2		
3		
...		
해당 없음		

• NIS용 매개 변수 *

이러한 값은 'vserver services name-service NIS-domain create' 명령을 사용하여 입력합니다.



그만큼 `-nis-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-nis-servers` NIS 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

필드에 입력합니다	설명	귀사의 가치
'도메인'	SVM이 이름 조회에 사용할 NIS 도메인입니다.	
'활성'	활성 NIS 도메인 서버입니다.	참 거짓입니다
'NIS-서버'	도메인 구성에 사용되는 NIS 서버의 IP 주소와 호스트 이름을 쉼표로 구분한 목록입니다.	

• LDAP용 매개 변수 *

이러한 값은 'vserver services name-service ldap client create' 명령을 사용하여 입력합니다.

자체 서명된 루트 CA 인증서 '.pem' 파일도 필요합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	LDAP 클라이언트 구성을 생성할 SVM의 이름입니다.	
'-client-config'입니다	새 LDAP 클라이언트 구성에 할당한 이름입니다.	
'LDAP-서버'	LDAP 서버의 IP 주소 및 호스트 이름을 쉼표로 구분하여 나열합니다.	
'-query-timeout'입니다	이 워크플로에 기본 3초를 사용합니다.	3
'-min-bind-level'	최소 바인딩 인증 수준입니다. 기본값은 'anonymous'입니다. 서명 및 봉인을 구성한 경우 'ASL'으로 설정해야 합니다.	
'-preferred-ad-servers'	쉼표로 구분된 목록에서 IP 주소별로 하나 이상의 기본 Active Directory 서버가 있습니다.	
'-ad-domain'입니다	Active Directory 도메인입니다.	

필드에 입력합니다	설명	귀사의 가치
'-스키마'	사용할 스키마 템플릿입니다. 기본 스키마나 사용자 지정 스키마를 사용할 수 있습니다.	
``포트``	이 워크플로우에는 기본 LDAP 서버 포트 '389'를 사용합니다.	389
'-bind-dn'	Bind 사용자 고유 이름입니다.	
'-base-dn'	기본 고유 이름입니다. 기본값은 ""(root)입니다.	
``기본범위``	이 워크플로에 기본 기본 검색 범위 'Subnet'을 사용합니다.	'우방'
'-세션-보안'	LDAP 서명 또는 서명 및 봉인을 활성화합니다. 기본값은 '없음'입니다.	
'-use-start-tls'	TLS를 통해 LDAP를 활성화합니다. 기본값은 false 입니다.	

• Kerberos 인증 매개변수 *

이러한 값은 'vserver NFS Kerberos realm create' 명령을 사용하여 입력합니다. 일부 값은 KDC(Key Distribution Center) 서버로 Microsoft Active Directory를 사용할지, MIT 또는 기타 UNIX KDC 서버를 사용하는지에 따라 달라집니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	KDC와 통신할 SVM.	
``영역``	Kerberos 영역.	
시계 편중	클라이언트와 서버 간에 허용되는 클럭 편중.	
'-KDC-IP'	KDC IP 주소입니다.	
``KDC-포트``	KDC 포트 번호입니다.	
'-adserver-name'입니다	Microsoft KDC 전용: AD 서버 이름입니다.	

'-adserver-ip'입니다	Microsoft KDC 전용: AD 서버 IP 주소입니다.	
'-AdminServer-IP'입니다	UNIX KDC 전용: 관리 서버 IP 주소.	
'-AdminServer-port'입니다	UNIX KDC만 해당: 관리 서버 포트 번호입니다.	
'-passwordserver-IP'입니다	UNIX KDC 전용: 암호 서버 IP 주소입니다.	
'-passwordserver-port'입니다	UNIX KDC 전용: 암호 서버 포트.	
``KDC-벤더'	KDC 공급업체.	{'Microsoft'
'기타}'	``논평'	원하는 코멘트.

이러한 값은 'vserver NFS Kerberos interface enable' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	Kerberos 구성을 생성할 SVM의 이름입니다.	
'-lif'	Kerberos를 사용하도록 설정할 데이터 LIF입니다. 여러 LIF에서 Kerberos를 사용하도록 설정할 수 있습니다.	
'-SPN'	서비스 원칙 이름(SPN)	
``허용된-원력-유형''	클라이언트 기능에 따라 Kerberos over NFS에 대해 허용되는 암호화 유형인 AES-256을 사용하는 것이 좋습니다.	
'-admin-username'입니다	KDC에서 직접 SPN 암호 키를 검색하는 KDC 관리자 자격 증명입니다. 암호가 필요합니다	
'-keytab-Uri'입니다	KDC 관리자 자격 증명이 없는 경우 SPN 키가 포함된 KDC의 keytab 파일입니다.	

'-ou'	Microsoft KDC의 영역을 사용하여 Kerberos를 설정할 때 Microsoft Active Directory 서버 계정이 생성되는 OU(조직 구성 단위)입니다.	

NFS 지원 SVM에 스토리지 용량 추가

- 내보내기 정책 및 규칙 생성을 위한 매개 변수 *

이러한 값은 'vserver export-policy create' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	새 볼륨을 호스팅할 SVM의 이름입니다.	
정책 이름	새 익스포트 정책에 대해 제공한 이름입니다.	

각 규칙에 대해 'vserver export-policy rule create' 명령을 사용하여 이러한 값을 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-clientmatch'	클라이언트 일치 사양.	
룰레인덱스	규칙 목록에서 내보내기 규칙의 위치입니다.	
'-프로토콜'	이 워크플로우에서 NFS를 사용합니다.	'NFS'입니다
'-rorule'	읽기 전용 액세스에 대한 인증 방법입니다.	
'-rwrule'	읽기-쓰기 액세스를 위한 인증 방법입니다.	
'-슈퍼유저'	고급 사용자 액세스를 위한 인증 방법입니다.	
'-anon'	익명 사용자가 매핑되는 사용자 ID입니다.	

각 익스포트 정책에 대해 하나 이상의 규칙을 생성해야 합니다.

'-ruleindex'	'* - clientmatch *'	'* -rorule *'	'*-rwrule *'	'*-슈퍼유저 *'	'*-anon *'

예	0.0.0.0/0, @rootaccess_ne tgroup	모두	krb5	시스템	65534
1					
2					
3					
...					
해당 없음					

- 볼륨 생성을 위한 매개 변수 *

Qtree 대신 볼륨을 생성하는 경우 이 값에 'volume create' 명령을 입력합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	새 볼륨을 호스팅할 새 SVM 또는 기존 SVM의 이름입니다.	
'- 볼륨'	새 볼륨에 제공하는 고유한 설명 이름입니다.	
'-집계'	새 NFS 볼륨을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-size'	새 볼륨의 크기에 대해 제공하는 정수입니다.	
'-user'	볼륨 루트의 소유자로 설정된 사용자의 이름 또는 ID입니다.	
``그룹``	볼륨 루트의 소유자로 설정된 그룹의 이름 또는 ID입니다.	
``보안스타일``	이 워크플로우에는 UNIX 보안 스타일을 사용합니다.	유닉스
``교차점-경로``	새 볼륨을 마운트할 루트(/) 아래의 위치입니다.	

수출정책	기존 익스포트 정책을 사용하려는 경우 볼륨을 생성할 때 해당 이름을 입력할 수 있습니다.	

- qtree 생성을 위한 매개 변수 *

볼륨 대신 qtree를 생성하는 경우 이 값에 'volume qtree create' 명령을 입력합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	qtree가 포함된 볼륨이 있는 SVM의 이름입니다.	
'- 볼륨'	새 qtree를 포함할 볼륨의 이름입니다.	
'-qtree'	새 qtree를 64자 이하로 설명하는 고유한 이름입니다.	
'-qtree-path'	볼륨과 qtree를 별도의 인수로 지정하는 대신 '/vol/volume_name/qtree_name\>' 형식의 qtree 경로 인수를 지정할 수 있습니다.	
'-unix-permissions'	선택 사항: qtree에 대한 UNIX 사용 권한	
수출정책	기존 익스포트 정책을 사용하려는 경우 qtree를 생성할 때 이름을 입력할 수 있습니다.	

관련 정보

- ["ONTAP 명령 참조입니다"](#)

SVM에 대한 NFS 액세스를 구성합니다

NFS 데이터 액세스를 위한 **ONTAP SVM** 생성

NFS 클라이언트에 데이터 액세스를 제공하기 위해 클러스터에 SVM이 하나 이상 없으면 하나 이상의 SVM을 생성해야 합니다.

시작하기 전에

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 [SVM 용량 관리](#) 참조하십시오.

단계

1. SVM 생성:

```
'vserver create -vserver _vserver_name_ -rootvolume _root_volume_name_ -aggregate _aggregate_name_ -rootvolume-security-style UNIX -language C. UTF-8 -IPSpace _IPSpace_name_'
```

- '-rootvolume-security-style' 옵션에 UNIX 설정을 사용합니다.
- 기본 C. UTF-8 '-language' 옵션을 사용합니다.
- IPSpace 설정은 선택 사항입니다.

2. 새로 생성한 SVM의 구성 및 상태 확인:

```
'vserver show -vserver _vserver_name_'
```

허용되는 프로토콜 필드는 NFS를 포함해야 합니다. 나중에 이 목록을 편집할 수 있습니다.

'Vserver 작동 상태' 필드에는 '실행 중' 상태가 표시되어야 합니다. 초기화 중 상태가 표시되는 경우 루트 볼륨 생성 등 일부 중간 작업이 실패한 것으로, SVM을 삭제하고 다시 생성해야 합니다.

예

다음 명령은 IPspace에서 데이터 액세스를 위한 SVM을 생성합니다. spaceba:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

다음 명령을 실행하면 루트 볼륨 1GB 단위로 SVM이 생성되고 자동으로 시작되어 '실행 중' 상태에 있음을 알 수 있습니다. 루트 볼륨에는 규칙을 포함하지 않는 기본 익스포트 정책이 있으므로 생성 시 루트 볼륨을 내보내지 않습니다.

```
cluster1::> vserver show -vserver vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: unix
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 [올 적응형 정책 그룹 템플릿을 설정합니다](#) 참조하십시오.

ONTAP SVM에서 NFS 프로토콜 활성화 확인

SVM에서 NFS를 구성 및 사용하려면 먼저 프로토콜이 활성화되어 있는지 확인해야 합니다.

이 작업에 대해

이는 일반적으로 SVM 설정 중에 수행되지만 설정 중에 프로토콜을 활성화하지 않은 경우 나중에 'vserver add-protocols' 명령을 사용하여 활성화할 수 있습니다.



프로토콜을 생성한 후에는 LIF에서 프로토콜을 추가하거나 제거할 수 없습니다.

"vserver remove-protocols" 명령을 사용하여 SVM에서 프로토콜을 비활성화할 수도 있습니다.

단계

1. 현재 SVM에 대해 활성화 및 비활성화된 프로토콜을 확인합니다.

```
'vserver show -vserver _vserver_name_ -protocols'
```

"vserver show-protocols" 명령을 사용하여 클러스터의 모든 SVM에서 현재 활성화된 프로토콜을 볼 수도 있습니다.

2. 필요한 경우 프로토콜을 활성화 또는 비활성화합니다.

- NFS 프로토콜을 활성화하려면: + 'vserver add-protocols-vserver _vserver_name_ -protocols nfs'
- 프로토콜을 작동 불가능하게 하려면: + "vserver remove-protocols-vserver _name_ -protocols _protocol_name_ [,protocol_name,...]"

3. 활성화된 프로토콜과 비활성화된 프로토콜이 올바르게 업데이트되었는지 확인합니다.

```
'vserver show -vserver _vserver_name_ -protocols'
```

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 현재 설정 및 해제된 프로토콜(허용 및 허용 안 함)이 표시됩니다.

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----
vs1.example.com   nfs                         cifs, fcp, iscsi, ndmp
```

다음 명령을 사용하면 이름이 VS1 인 SVM에서 활성화된 프로토콜 목록에 NFS를 추가하여 NFS를 통해 액세스할 수 있습니다.

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

ONTAP SVM에서 NFS 클라이언트 액세스 열기

SVM 루트 볼륨의 기본 익스포트 정책에는 NFS를 통해 모든 클라이언트가 액세스할 수 있도록 하는 규칙이 포함되어야 합니다. 이 규칙이 없으면 모든 NFS 클라이언트가 SVM 및 해당 볼륨에 대한 액세스가 거부됩니다.

이 작업에 대해

새 SVM이 생성되면 SVM의 루트 볼륨에 대한 기본 익스포트 정책(기본값)이 자동으로 생성됩니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 익스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다.

기본 익스포트 정책에서 모든 NFS 클라이언트에 대한 액세스가 허용되는지 확인하고, 나중에 개별 볼륨 또는 qtree에 대한 사용자 지정 익스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. 기존 SVM을 사용하는 경우 기본 루트 볼륨 익스포트 정책을 확인하십시오.

'vserver export-policy rule show'를 선택합니다

명령 출력은 다음과 같아야 합니다.


```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance
```

```

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

이러한 규칙이 열려 있는 액세스를 허용하는 경우 이 작업은 완료된 것입니다. 그렇지 않은 경우 다음 단계를 진행하십시오.

2. SVM 루트 볼륨에 대한 익스포트 규칙 생성:

```
'vserver export-policy rule create-vserver _vserver_name_ -policyname default-ruleindex 1-protocol nfs-
clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any'
```

SVM이 Kerberos로 보호되는 볼륨만 포함할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5' 또는 'krb5i'로 설정할 수 있습니다. 예를 들면 다음과 같습니다.

```
'-rorule krb5i-rwrule krb5i-superuser krb5i'
```

3. 'vserver export-policy rule show' 명령을 사용하여 규칙 생성을 확인합니다.

결과

이제 모든 NFS 클라이언트가 SVM에서 생성된 모든 볼륨 또는 qtree에 액세스할 수 있습니다.

ONTAP NFS 서버 생성

클러스터에서 NFS 라이선스가 등록되었는지 확인한 후 "vserver NFS create" 명령을 사용하여 SVM에 NFS 서버를 생성하고 해당 명령이 지원하는 NFS 버전을 지정할 수 있습니다.

이 작업에 대해

SVM은 하나 이상의 NFS 버전을 지원하도록 구성할 수 있습니다. NFSv4 이상을 지원하는 경우:

- NFSv4 사용자 ID 매핑 도메인 이름은 NFSv4 서버 및 타겟 클라이언트에서 동일해야 합니다.

NFSv4 서버와 클라이언트가 동일한 이름을 사용하는 한 LDAP 또는 NIS 도메인 이름과 같을 필요는 없습니다.

- 타겟 클라이언트는 NFSv4 숫자 ID 설정을 지원해야 합니다.
- 보안을 위해 NFSv4 구축에서는 이름 서비스에 LDAP를 사용해야 합니다.

시작하기 전에

SVM은 NFS 프로토콜을 허용하도록 구성해야 합니다.

단계

1. NFS 라이선스가 클러스터에서 라이선스되었는지 확인합니다.

```
'system license show-package nfs'
```

그렇지 않은 경우 영업 담당자에게 문의하십시오.

2. NFS 서버 생성:

```
'vserver NFS create -vserver_vserver_name_-v3{enabled | disabled} -v4.0{enabled | disabled} -v4-id-domain_NFSv4_id_domain_-v4-numeric-ids{enabled | disabled} -v4.1{enabled | disabled | pNFS{enabled | disabled}}'
```

를 선택합니다

NFS 버전의 조합을 사용하도록 선택할 수 있습니다. pNFS를 지원하려면 '-v4.1'과 '-v4.1-pNFS' 옵션을 모두 사용해야 합니다.

v4 이상을 사용하는 경우 다음 옵션도 올바르게 설정되어 있어야 합니다.

- '-v4-id-domain'

이 선택적 매개 변수는 NFSv4 프로토콜에서 정의된 사용자 및 그룹 이름의 문자열 형식 도메인 부분을 지정합니다. 기본적으로 ONTAP은 NIS 도메인이 설정되어 있는 경우 NIS 도메인을 사용하고, 설정되어 있지 않으면 DNS 도메인이 사용됩니다. 대상 클라이언트가 사용하는 도메인 이름과 일치하는 값을 입력해야 합니다.

- '-v4-numeric-ids'

이 선택적 매개 변수는 NFSv4 소유자 속성에서 숫자 문자열 식별자를 지원하도록 설정되었는지 여부를 지정합니다. 기본 설정은 활성화되지만 타겟 클라이언트가 이 설정을 지원하는지 확인해야 합니다.

나중에 'vserver nfs modify' 명령을 사용하여 추가 NFS 기능을 활성화할 수 있습니다.

3. NFS가 실행 중인지 확인합니다.

```
'vserver NFS status-vserver_vserver_name_'
```

4. NFS가 원하는 대로 구성되었는지 확인합니다.

```
'vserver nfs show -vserver_vserver_name_'
```

예

다음 명령을 실행하면 NFSv3 및 NFSv4.0이 설정된 VS1 이라는 SVM에 NFS 서버가 생성됩니다.

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id-domain my_domain.com
```

다음 명령을 실행하면 이름이 VS1 인 새 NFS 서버의 상태와 구성 값이 검증됩니다.

```

vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

Vserver: vs1
General NFS Access: true
NFS v3: enabled
NFS v4.0: enabled
UDP Protocol: enabled
TCP Protocol: enabled
Default Windows User: -
NFSv4.0 ACL Support: disabled
NFSv4.0 Read Delegation Support: disabled
NFSv4.0 Write Delegation Support: disabled
NFSv4 ID Mapping Domain: my_domain.com
...

```

ONTAP NFS LIF를 생성합니다

LIF는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트에 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 up 상태로 구성되어야 합니다. 에 대한 자세한 내용은 up ["ONTAP 명령 참조입니다"](#)을 참조하십시오.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 네트워크 서브넷 만들기 명령을 사용하여 만듭니다.

에 대한 자세한 내용은 `network subnet create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

이 작업에 대해

- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- Kerberos 인증을 사용하는 경우 여러 LIF에서 Kerberos를 사용하도록 설정합니다.
- 클러스터에 LIF가 많은 경우 'network interface capacity show' 명령을 사용하여 클러스터에서 지원되는 LIF 용량과 각 노드에서 지원되는 LIF 용량을 확인할 수 있습니다 (고급 권한 수준에서).

및 `network interface capacity details show` 에 대한 자세한 `network interface capacity`

show 내용은 을 ["ONTAP 명령 참조입니다"](#)참조하십시오.

- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

ONTAP 9.4부터는 FC-NVMe가 지원됩니다. FC-NVMe LIF를 생성하는 경우 다음 사항을 알아야 합니다.

- NVMe 프로토콜은 LIF가 생성된 FC 어댑터에서 지원되어야 합니다.
- FC-NVMe는 데이터 LIF에서 유일한 데이터 프로토콜일 수 있습니다.
- SAN을 지원하는 모든 SVM(스토리지 가상 머신)에서 관리 트래픽을 처리하는 하나의 LIF를 구성해야 합니다.
- NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
- SVM당 하나의 NVMe LIF에서 데이터 트래픽을 처리할 수 있습니다

단계

1. LIF 생성:

```
'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol nfs-home-  
node_node_name_-home-port_port_name_{-address_{-address_netmask_ip_address_-subnet-  
name_subnet_name_-}firewall-policy data-auto-revert{true|false}
```

에 대한 자세한 내용은 `network interface create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

옵션을 선택합니다	설명
• ONTAP 9.5 이하 *	<pre>'network interface create-vserver_vserver_name_- lif_lif_name_-role data-protocol nfs-home- node_node_name_-home-port_port_name_{- address_{-address_netmask_ip_address_- -subnet-name_subnet_name_-}firewall-policy data- auto-revert{true</pre>
<pre>false}</pre>	
• ONTAP 9.6 이상 *	<pre>'network interface create-vserver_vserver_name_- lif_lif_name_-role data-protocol nfs-home- node_node_name_-home-port_port_name_{- address_{-address_netmask_ip_address_- -subnet-name_subnet_name_-}firewall-policy data- auto-revert{true</pre>
<pre>false}</pre>	

- 서비스 정책(ONTAP 9.6에서 시작)을 사용하여 LIF를 생성할 때는 '-role' 매개 변수가 필요하지 않습니다.
- LIF를 생성할 때 '-data-protocol' 매개 변수를 지정해야 하며 나중에 데이터 LIF를 삭제 및 다시 생성하지 않고 수정할 수 없습니다.

서비스 정책(ONTAP 9.6부터)을 사용하여 LIF를 생성할 때는 '-data-protocol' 매개 변수가 필요하지 않습니다.

- 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도

있습니다.

에 대한 자세한 내용은 `network interface revert` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

- '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
- IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
- 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.
- 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 `network route create` 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.
- '-firewall-policy' 옵션의 경우 LIF 역할과 동일한 기본 data를 사용합니다.

필요에 따라 나중에 사용자 지정 방화벽 정책을 만들고 추가할 수 있습니다.



ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 ["LIF의 방화벽 정책을 구성합니다"](#)을 참조하십시오.

- '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 false로 설정할 수 있습니다.
 - a. 'network interface show' 명령을 사용하여 LIF가 성공적으로 생성되었는지 확인합니다.
 - b. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면...	사용...
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

- c. Kerberos를 사용하는 경우 1단계부터 3단계까지 반복하여 추가 LIF를 생성합니다.

Kerberos는 이러한 각 LIF에서 별도로 설정해야 합니다.

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 cluster-1의 모든 LIF가 표시됩니다. 데이터 LIF datalif1 및 datalif3은 IPv4 주소로 구성되고 datalif4는 IPv6 주소로 구성됩니다.

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
cluster-1	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1	clus1	up/up	192.0.2.12/24	node-1	e0a
	clus2	up/up	192.0.2.13/24	node-1	e0b
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
node-2	clus1	up/up	192.0.2.14/24	node-2	e0a
	clus2	up/up	192.0.2.15/24	node-2	e0b
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com	datalif3	up/up	192.0.2.146/30	node-2	e0c
	datalif4	up/up	2001::2/64	node-2	e0c

5 entries were displayed.

다음 명령을 실행하면 기본 데이터 파일 서비스 정책에 할당된 NAS 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

관련 정보

- ["네트워크 Ping"](#)
- ["네트워크 인터페이스"](#)

ONTAP NFS SVM 호스트 이름 확인을 위해 DNS 활성화

SVM에서 DNS를 사용하도록 설정하려면 'vserver services name-service dns' 명령을 사용하고, 호스트 이름 확인을 위해 DNS를 사용하도록 구성할 수 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. DNS 서버 이름을 하나만 입력하면 'vserver services name-service dns create' 명령이 경고를 보냅니다.

이 작업에 대해

에 대해 자세히 ["SVM에서 동적 DNS 구성"](#) 알아보십시오.

단계

1. SVM에서 DNS 활성화:

```
'vserver services name-service dns create -vserver _vserver_name_ -domain _domain_name_ -name-
servers _ip_address_ -state enabled'
```

다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



를 클릭합니다 vserver services name-service dns create Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. 'vserver services name-service dns show' 명령을 사용하여 DNS 도메인 구성을 표시합니다.

다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

이름 서비스 구성

ONTAP NFS 이름 서비스에 대해 알아보세요

스토리지 시스템의 구성에 따라 ONTAP는 클라이언트에 대한 적절한 액세스를 제공하기 위해 호스트, 사용자, 그룹 또는 넷그룹 정보를 조회해야 합니다. 이 정보를 얻으려면 ONTAP가 로컬 또는 외부 이름 서비스에 액세스하도록 이름 서비스를 구성해야 합니다.

클라이언트 인증 중에 NIS 또는 LDAP와 같은 이름 서비스를 사용하여 이름 조회를 용이하게 해야 합니다. 특히 NFSv4 이상을 구축할 때 보안을 강화하기 위해 가능하면 LDAP를 사용하는 것이 좋습니다. 또한 외부 이름 서버를 사용할 수 없는 경우 로컬 사용자 및 그룹을 구성해야 합니다.

이름 서비스 정보는 모든 소스에서 동기화되어야 합니다.

ONTAP가 로컬 또는 외부 이름 서비스에 문의하여 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑 정보를 검색할 수 있도록 이름 서비스 스위치 테이블을 올바르게 구성해야 합니다.

시작하기 전에

사용자 환경에 적용할 수 있는 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑에 사용할 이름 서비스를 결정해야 합니다.

넷그룹을 사용할 계획이라면 RFC 5952에 지정된 대로 넷그룹에 지정된 모든 IPv6 주소를 단축하고 압축해야 합니다.

이 작업에 대해

사용하지 않는 정보 소스는 포함하지 마십시오. 예를 들어 NIS가 사용자 환경에서 사용되지 않는 경우 '-Sources NIS' 옵션을 지정하지 마십시오.

단계

1. 이름 서비스 스위치 테이블에 필요한 항목을 추가합니다.

```
'vserver services name-service ns-switch create -vserver _vserver_name_ -database _database_name_ -sources _source_names_'
```

2. 이름 서비스 스위치 테이블에 원하는 순서대로 필요한 항목이 포함되어 있는지 확인합니다.

```
'vserver services name-service ns-switch show -vserver _vserver_name_'
```

수정하려면 'vserver services name-service ns-switch modify' 또는 'vserver services name-service ns-switch delete' 명령을 사용해야 합니다.

예

다음 예에서는 SVM VS1 에서 로컬 넷그룹 파일을 사용할 수 있도록 이름 서비스 스위치 테이블에 새 항목을 생성하고 외부 NIS 서버에서 넷그룹 정보를 순서대로 찾습니다.

```
cluster::> vservice ns-switch create -vserver vs1  
-database netgroup -sources files,nis
```

작업을 마친 후

- 데이터 액세스를 제공하려면 SVM에 지정한 이름 서비스를 구성해야 합니다.
- SVM에 대한 네임 서비스를 삭제할 경우 네임 서비스 스위치 테이블에서 해당 서비스를 제거해야 합니다.

이름 서비스 스위치 테이블에서 이름 서비스를 삭제하지 않으면 스토리지 시스템에 대한 클라이언트 액세스가 예상대로 작동하지 않을 수 있습니다.

로컬 **UNIX** 사용자 및 그룹을 구성합니다

ONTAP NFS SVM에 대한 로컬 **UNIX** 사용자 및 그룹에 대해 알아보세요.

SVM에서 로컬 UNIX 사용자 및 그룹을 사용하여 인증 및 이름 매핑을 수행할 수 있습니다. UNIX 사용자 및 그룹을 수동으로 만들거나 UNIX 사용자 또는 그룹이 포함된 파일을 URI(Uniform

Resource Identifier)에서 로드할 수 있습니다.

클러스터에 결합된 로컬 UNIX 사용자 그룹 및 그룹 구성원의 기본 최대 제한은 32,768입니다. 클러스터 관리자가 이 제한을 수정할 수 있습니다.

ONTAP NFS SVM에서 로컬 UNIX 사용자 생성

'vserver services name-service unix-user create' 명령을 사용하여 로컬 UNIX 사용자를 생성할 수 있습니다. 로컬 UNIX 사용자는 이름 매핑 처리에 사용되는 UNIX 이름 서비스 옵션으로 SVM에서 생성하는 UNIX 사용자입니다.

단계

1. 로컬 UNIX 사용자 생성:

```
'vserver services name-service unix-user create-vserver_vserver_name_-user_user_name_-id_integer_-primary-gid_integer_-full-name_full_name_'
```

'-user_user_name_'은(는) 사용자 이름을 지정합니다. 사용자 이름의 길이는 64자 이하여야 합니다.

'-id_integer_'는 사용자가 지정하는 사용자 ID를 지정합니다.

기본 그룹 ID는 -primary-gid_integer_ 로 지정합니다. 그러면 사용자가 기본 그룹에 추가됩니다. 사용자를 생성한 후 원하는 추가 그룹에 사용자를 수동으로 추가할 수 있습니다.

예

다음 명령을 실행하면 이름이 johnm인 로컬 UNIX 사용자가 이름이 vs1 인 SVM에 생성됩니다. 사용자는 ID 123 및 기본 그룹 ID 100을 가지고 있습니다.

```
node::> vserver services name-service unix-user create -vserver vs1 -user johnm -id 123 -primary-gid 100 -full-name "John Miller"
```

ONTAP NFS SVM에 로컬 UNIX 사용자 목록 로드

SVM에서 개별 로컬 UNIX 사용자를 수동으로 생성하는 대신 로컬 UNIX 사용자 목록을 URI(Uniform Resource Identifier)에서 SVM으로 로드하여 작업을 단순화할 수 있습니다('vserver services name-service unix-user load-from-Uri').

단계

1. 로드할 로컬 UNIX 사용자 목록이 포함된 파일을 생성합니다.

파일은 UNIX '/etc/passwd' 형식의 사용자 정보를 포함해야 합니다.

'user_name:password:user_ID:group_ID:full_name'

명령에서는 'PASSWORD' 필드 값과 'FULL_NAME' 필드 뒤에 있는 필드 값('HOME_DIRECTORY' 및 'shell')이 삭제됩니다.

지원되는 최대 파일 크기는 2.5MB입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

목록에 중복 항목이 포함되어 있으면 목록을 로드하지 못하고 오류 메시지가 표시됩니다.

3. 파일을 서버에 복사합니다.

스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 사용자 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

```
'vserver services name-service unix-user load-from-uri-vserver_vserver_name_-Uri{ftp|http|https|https}://Uri
-overwrite{true|false}'
```

'-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/passwd' 에서 이름이 VS1 인 SVM으로 로컬 UNIX 사용자 목록이 로드됩니다. SVM의 기존 사용자는 URI의 정보로 덮어써지지 않습니다.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

ONTAP NFS SVM에 로컬 UNIX 그룹 생성

"vserver services name-service unix-group create" 명령을 사용하여 SVM에 로컬인 UNIX 그룹을 생성할 수 있습니다. 로컬 UNIX 그룹은 로컬 UNIX 사용자와 함께 사용됩니다.

단계

1. 로컬 UNIX 그룹 생성:

```
'vserver services name-service unix-group create-vserver_vserver_name_-name_group_name_-
id_integer_'
```

'-name_group_name_'은 그룹 이름을 지정합니다. 그룹 이름의 길이는 64자 이하여야 합니다.

'-id_integer_'는 지정하는 그룹 ID를 지정합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 eng인 로컬 그룹이 생성됩니다. 그룹에 ID 101이 있습니다.

```
vs1::> vsserver services name-service unix-group create -vsserver vs1 -name eng -id 101
```

ONTAP NFS SVM의 로컬 UNIX 그룹에 사용자 추가

'vsserver services name-service unix-group adduser' 명령을 사용하여 SVM에 로컬인 보조 UNIX 그룹에 사용자를 추가할 수 있습니다.

단계

1. 로컬 UNIX 그룹에 사용자 추가:

```
'vsserver services name-service unix-group adduser-vsserver_vsserver_name_-name_group_name_-username_user_name_'
```

'-name"group_name'은 사용자의 기본 그룹 외에도 사용자를 추가할 UNIX 그룹의 이름을 지정합니다.

예

다음 명령을 실행하면 이름이 max인 사용자가 이름이 eng인 로컬 UNIX 그룹에 이름이 vs1 인 SVM에 추가됩니다.

```
vs1::> vsserver services name-service unix-group adduser -vsserver vs1 -name eng -username max
```

ONTAP NFS SVM의 URI에서 로컬 UNIX 그룹 로드

개별 로컬 UNIX 그룹을 수동으로 생성하는 대신 'vsserver services name-service unix-group load-from-uri' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 로컬 UNIX 그룹 목록을 로드할 수 있습니다.

단계

1. 로드할 로컬 UNIX 그룹 목록이 포함된 파일을 생성합니다.

파일은 UNIX '/etc/group' 형식의 그룹 정보를 포함해야 합니다.

```
'group_name:password:group_ID:comma_separated_list_of_users'
```

이 명령어는 'PASSWORD' 필드의 값을 삭제한다.

지원되는 최대 파일 크기는 1MB입니다.

그룹 파일에서 각 줄의 최대 길이는 32,768자입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

목록에 중복 항목이 없어야 합니다. 그렇지 않으면 목록을 로드하지 못합니다. SVM에 이미 있는 항목이 있으면 "-overwrite" 매개 변수를 "true"로 설정하여 모든 기존 항목을 새 파일로 덮어쓰거나 새 파일에 기존 항목을 복제하는 항목이 없는지 확인해야 합니다.

3. 파일을 서버에 복사합니다.

스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 그룹 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

```
'vserver services name-service unix-group load-from-uri-vserver_vserver_name_-  
Uri{ftp|http|FTPS|https}://{Uri-overwrite{true|false}}'
```

'-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다. 이 매개 변수를 "true"로 지정하면 ONTAP은 지정된 SVM의 기존 로컬 UNIX 그룹 데이터베이스 전체를 로드하는 파일의 항목으로 바꿉니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/group' 에서 VS1 이라는 SVM으로 로컬 UNIX 그룹 목록이 로드됩니다. SVM의 기존 그룹은 URI의 정보로 덮어써지지 않습니다.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/group -overwrite false
```

넷그룹으로 작업합니다

ONTAP NFS SVM의 넷그룹에 대해 알아보세요

사용자 인증 및 내보내기 정책 규칙의 클라이언트와 일치시키기 위해 넷그룹을 사용할 수 있습니다. 외부 이름 서버(LDAP 또는 NIS)에서 넷그룹에 대한 액세스를 제공하거나, 'vserver services name-service netgroup load' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다.

시작하기 전에

넷그룹을 사용하기 전에 다음 조건이 충족되는지 확인해야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹의 모든 호스트는 순방향 및 역방향 DNS 조회를 일관되게 제공하기 위해 정방향(A) 및 역방향(PTR) DNS 레코드를 모두 포함해야 합니다.

또한 클라이언트의 IP 주소에 PTR 레코드가 여러 개 있는 경우 이러한 모든 호스트 이름은 넷그룹의 구성원이어야 하며 해당 레코드가 있어야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹에 있는 모든 호스트의 이름은 철자가 올바르고 올바른 대소문자를 사용해야 합니다. 넷그룹에서 사용되는 호스트 이름의 대/소문자 불일치로 인해 내보내기 검사 실패와 같은 예기치 않은 동작이 발생할 수 있습니다.
- 넷그룹에 지정된 모든 IPv6 주소는 RFC 5952에 지정된 대로 단축되고 압축되어야 합니다.

예를 들어 2011:hu9:0:0:0:0:3:1은 2011:hu9:3:1로 단축되어야 합니다.

이 작업에 대해

넷그룹으로 작업하는 경우 다음 작업을 수행할 수 있습니다.

- 'vserver export-policy netgroup check-membership' 명령을 사용하여 클라이언트 IP가 특정 넷그룹의 구성원인지 여부를 확인할 수 있습니다.
- 'vserver services name-service getxxbyy netgrp' 명령을 사용하여 클라이언트가 넷그룹에 속하는지 확인할 수 있습니다.

조회를 수행하는 기본 서비스는 구성된 이름 서비스 스위치 순서에 따라 선택됩니다.

ONTAP NFS SVM의 URI에서 넷그룹 로드

내보내기 정책 규칙에서 클라이언트를 일치시키는 데 사용할 수 있는 방법 중 하나는 netgroup에 나열된 호스트를 사용하는 것입니다. 외부 이름 서버에 저장된 넷그룹을 사용하는 대신 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다('vserver services name-service netgroup load').

시작하기 전에

넷그룹 파일은 SVM에 로드되기 전에 다음 요구 사항을 충족해야 합니다.

- 파일은 NIS를 채우는 데 사용되는 것과 동일한 적절한 넷그룹 텍스트 파일 형식을 사용해야 합니다.

ONTAP는 넷그룹 텍스트 파일 형식을 로드하기 전에 검사합니다. 파일에 오류가 있으면 로드되지 않고 파일에서 수행해야 하는 수정 사항을 나타내는 메시지가 표시됩니다. 오류를 해결한 후 Netgroup 파일을 지정된 SVM에 다시 로드할 수 있습니다.

- 넷그룹 파일의 호스트 이름에 있는 모든 영문자는 소문자여야 합니다.
- 지원되는 최대 파일 크기는 5MB입니다.
- 네스팅 넷그룹에 대해 지원되는 최대 수준은 1000입니다.
- 넷그룹 파일에 호스트 이름을 정의할 때는 운영 DNS 호스트 이름만 사용할 수 있습니다.

내보내기 액세스 문제를 방지하려면 DNS CNAME 또는 라운드 로빈 레코드를 사용하여 호스트 이름을 정의하면 안 됩니다.

- 넷그룹 파일에서 3중 그룹의 사용자 및 도메인 부분은 ONTAP에서 지원하지 않으므로 비워 두어야 합니다.

호스트/IP 부분만 지원됩니다.

이 작업에 대해

ONTAP는 로컬 넷그룹 파일에 대한 호스트 별 검색을 지원합니다. 넷그룹 파일을 로드하면 ONTAP에서 자동으로 netgroup.byhost 맵을 생성하여 넷그룹 기준 호스트 검색을 설정합니다. 이렇게 하면 내보내기 정책 규칙을 처리하여 클라이언트 액세스를 평가할 때 로컬 넷그룹 검색 속도를 크게 높일 수 있습니다.

단계

1. URI를 통해 넷그룹을 SVM에 로드:

```
'vserver services name-service netgroup load-vserver_vserver_name_-source{ftp|http|FTPS|https}://Uri'
```

넷그룹 파일을 로드하고 넷그룹을 생성합니다. byhost 맵은 몇 분 정도 걸릴 수 있습니다.

넷그룹을 업데이트하려면 파일을 편집하고 업데이트된 넷그룹 파일을 SVM에 로드할 수 있습니다.

예

다음 명령을 실행하면 HTTP URL 'http://intranet/downloads/corp-netgroup': 에서 이름이 VS1 인 SVM에 넷그룹 정의가 로드됩니다

```
vs1::> vsserver services name-service netgroup load -vsserver vs1  
-source http://intranet/downloads/corp-netgroup
```

ONTAP NFS SVM 넷그룹 정의 확인

SVM에 넷그룹을 로드한 후 'vsserver services name-service netgroup status' 명령을 사용하여 넷그룹 정의의 상태를 확인할 수 있습니다. 이렇게 하면 SVM을 백업하는 모든 노드에서 넷그룹 정의가 일관되는지 확인할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 넷그룹 정의의 상태를 확인합니다.

'vsserver services name-service netgroup status'

자세한 보기에 추가 정보를 표시할 수 있습니다.

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

예

권한 수준을 설정한 후 다음 명령을 실행하면 모든 SVM에 대한 넷그룹 상태가 표시됩니다.

```
vs1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by technical support.

Do you wish to continue? (y or n): y

```
vs1::*> vserver services name-service netgroup status
```

Virtual

Server	Node	Load Time	Hash Value

-----	-----	-----	-----
-----	-----	-----	-----

vs1

	node1	9/20/2006 16:04:53	

e6cb38ec1396a280c0d2b77e3a84eda2

	node2	9/20/2006 16:06:26	

e6cb38ec1396a280c0d2b77e3a84eda2

	node3	9/20/2006 16:08:08	

e6cb38ec1396a280c0d2b77e3a84eda2

	node4	9/20/2006 16:11:33	

e6cb38ec1396a280c0d2b77e3a84eda2

ONTAP NFS SVM에 대한 NIS 도메인 구성 생성

사용자 환경에서 NIS(Network Information Service)를 사용하여 이름 서비스를 제공하는 경우 'vserver services name-service NIS-domain create' 명령을 사용하여 SVM에 대한 NIS 도메인 구성을 생성해야 합니다.

시작하기 전에

SVM에서 NIS 도메인을 구성하기 전에 구성된 모든 NIS 서버를 사용할 수 있고 연결할 수 있어야 합니다.

NIS를 사용하여 디렉터리 검색을 수행할 경우 NIS 서버의 맵에는 각 항목에 대해 1,024자를 초과할 수 없습니다. 이 제한을 준수하지 않는 NIS 서버를 지정하지 마십시오. 그렇지 않으면 NIS 항목에 종속된 클라이언트 액세스가 실패할 수 있습니다.

이 작업에 대해

NIS 데이터베이스에 netgroup.byhost 맵이 포함되어 있으면 ONTAP에서 이를 사용하여 더 빨리 검색할 수 있습니다. 클라이언트 액세스 문제를 방지하려면 디렉토리의 netgroup.byhost 및 netgroup 맵을 항상 동기화해야 합니다. ONTAP 9.7부터 NIS 넷그룹.byhost 항목은 vserver services name-service NIS-domain netgroup-database 명령을 사용하여 캐싱될 수 있습니다.

호스트 이름 확인에 NIS를 사용하는 것은 지원되지 않습니다.

단계

1. NIS 도메인 구성 생성:

```
vserver services name-service nis-domain create -vserver vs1 -domain
```


<domain_name> -nis-servers <IP_addresses>

NIS 서버는 최대 10개까지 지정할 수 있습니다.



그만큼 -nis-servers 필드는 다음을 대체합니다. -servers 필드입니다. 다음을 사용할 수 있습니다. -nis-servers NIS 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

2. 도메인이 생성되었는지 확인합니다.

'vserver services name-service NIS-domain show'를 참조하십시오

예

다음 명령을 실행하면 NIS 도메인용 NIS 도메인 구성이 생성됩니다. SVM은 IP 주소의 NIS nisdomain 서버로 이름이 vs1 지정됩니다. 192.0.2.180

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

LDAP를 사용합니다

ONTAP NFS SVM에서 LDAP 이름 서비스 사용에 대해 알아보세요

환경에서 LDAP를 네임 서비스로 사용하는 경우 LDAP 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 LDAP 클라이언트로 설정해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 Active Directory 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. 이름 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 활성화하려면 LDAP 클라이언트 modify 명령에 '-try-channel-binding' 매개 변수를 사용합니다.

자세한 내용은 을 참조하십시오 ["Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항"](#).

- ONTAP용 LDAP를 구성하기 전에 사이트 배포가 LDAP 서버 및 클라이언트 구성에 대한 모범 사례를 충족하는지 확인해야 합니다. 특히 다음 조건을 충족해야 합니다.
 - LDAP 서버의 도메인 이름이 LDAP 클라이언트의 항목과 일치해야 합니다.
 - LDAP 서버에서 지원하는 LDAP 사용자 암호 해시 유형에는 ONTAP에서 지원하는 해시 유형이 포함되어야 합니다.
 - 암호화(모든 유형) 및 SHA-1(SHA, SSHA).
 - ONTAP 9.8부터 SHA-2 해시(SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, SSHA-512)도 지원됩니다.
 - LDAP 서버에 세션 보안 조치가 필요한 경우 LDAP 클라이언트에서 이를 구성해야 합니다.

다음 세션 보안 옵션을 사용할 수 있습니다.

- LDAP 서명(데이터 무결성 검사 제공) 및 LDAP 서명 및 봉인(데이터 무결성 검사 및 암호화 제공)

- TLS를 시작합니다
- LDAPS(TLS 또는 SSL을 통한 LDAP)
- 서명되고 봉인된 LDAP 쿼리를 사용하려면 다음 서비스를 구성해야 합니다.
 - LDAP 서버는 GSSAPI(Kerberos) SASL 메커니즘을 지원해야 합니다.
 - LDAP 서버에는 DNS 서버에 설정된 PTR 레코드와 DNS A/AAAA 레코드가 있어야 합니다.
 - Kerberos 서버는 DNS 서버에 SRV 레코드가 있어야 합니다.
- 시작 TLS 또는 LDAPS를 활성화하려면 다음 사항을 고려해야 합니다.
 - LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.
 - LDAPS를 사용하는 경우 ONTAP 9.5 이상에서 TLS 또는 SSL에 대해 LDAP 서버를 활성화해야 합니다. SSL은 ONTAP 9.0-9.4에서 지원되지 않습니다.
 - 도메인에 인증서 서버가 이미 구성되어 있어야 합니다.
- ONTAP 9.5 이상에서 LDAP 조회 추적을 활성화하려면 다음 조건을 충족해야 합니다.
 - 두 도메인은 다음 신뢰 관계 중 하나로 구성해야 합니다.
 - 양방향
 - 원웨이 - 프라이머리(primary)가 추천 도메인을 신뢰하는 곳입니다
 - 부모-자식
 - DNS는 참조된 모든 서버 이름을 확인하도록 구성되어야 합니다.
 - 도메인 암호는 -bind-as-cifs-server가 true로 설정된 경우 인증하기 위해 동일해야 합니다.

LDAP 조회 추적에는 다음 구성이 지원되지 않습니다.



- 모든 ONTAP 버전:
 - 관리 SVM의 LDAP 클라이언트
- ONTAP 9.8 및 이전 버전(9.9.1 이상에서 지원됨):
 - LDAP 서명 및 봉인('-session-security' 옵션)
 - 암호화된 TLS 연결('-use-start-tls' 옵션)
 - LDAPS 포트 636을 통한 통신('-use-ldaps-for-ad-ldap' 옵션)

- SVM에서 LDAP 클라이언트를 구성할 때 LDAP 스키마를 입력해야 합니다.

대부분의 경우 기본 ONTAP 스키마 중 하나가 적합합니다. 그러나 사용자 환경의 LDAP 스키마가 이러한 스키마와 다른 경우 LDAP 클라이언트를 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다. 사용자 환경의 요구 사항에 대해서는 LDAP 관리자에게 문의하십시오.

- 호스트 이름 확인에 LDAP를 사용하는 것은 지원되지 않습니다.

를 참조하십시오

- ["NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"](#)
- ["ONTAP SMB SVM에 자체 서명된 루트 CA 인증서를 설치합니다"](#)

ONTAP NFS SVM에 대한 새 LDAP 클라이언트 스키마 생성

사용자 환경의 LDAP 스키마가 ONTAP 기본값과 다른 경우 LDAP 클라이언트 구성을 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2012 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

기본값이 아닌 LDAP 스키마를 사용해야 하는 경우 LDAP 클라이언트 구성을 생성하기 전에 만들어야 합니다. 새 스키마를 만들기 전에 LDAP 관리자에게 문의하십시오.

ONTAP에서 제공하는 기본 LDAP 스키마는 수정할 수 없습니다. 새 스키마를 만들려면 복사본을 만든 다음 복사본을 적절하게 수정합니다.

단계

1. 기존 LDAP 클라이언트 스키마 템플릿을 표시하여 복사할 템플릿을 식별합니다.

'vserver services name-service ldap client schema show'를 참조하십시오

2. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

3. 기존 LDAP 클라이언트 스키마의 복사본을 만듭니다.

'vserver services name-service LDAP 클라이언트 스키마 복사 - vservice_vservice_name_-
schema_existing_schema_name_-new-schema-name_new_schema_name_'

4. 새 스키마를 수정하고 사용자 환경에 맞게 사용자 지정합니다.

'vserver services name-service LDAP 클라이언트 스키마 수정

5. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

ONTAP NFS 액세스를 위한 LDAP 클라이언트 구성 생성

ONTAP가 사용자 환경의 외부 LDAP 또는 Active Directory 서비스에 액세스하도록 하려면 먼저 스토리지 시스템에서 LDAP 클라이언트를 설정해야 합니다.

시작하기 전에

Active Directory 도메인 확인된 목록의 처음 세 개 서버 중 하나가 작동 중이고 데이터를 제공하고 있어야 합니다. 그렇지 않으면 이 작업이 실패합니다.



여러 대의 서버가 있으며 그 중 어느 시점에서든 3대 이상의 서버가 다운됩니다.

단계

1. "vserver services name-service ldap client create" 명령에 대한 적절한 구성 값을 확인하려면 LDAP 관리자에게 문의하십시오.

- a. LDAP 서버에 대한 도메인 기반 또는 주소 기반 연결을 지정합니다.

AD-DOMAIN과 -SERS 옵션은 상호 배타적입니다.

- Active Directory 도메인에서 LDAP 서버 검색을 설정하려면 '-ad-domain' 옵션을 사용합니다.
 - 를 사용할 수 있습니다 -restrict-discovery-to-site LDAP 서버 검색을 지정된 도메인의 CIFS 기본 사이트로 제한하는 옵션입니다. 이 옵션을 사용하는 경우 에서 CIFS 기본 사이트도 지정해야 합니다 -default-site.
- '-preferred-ad-servers' 옵션을 사용하여 쉼표로 구분된 목록에서 IP 주소로 하나 이상의 기본 Active Directory 서버를 지정할 수 있습니다. 클라이언트를 생성한 후 'vserver services name-service ldap client modify' 명령을 사용하여 이 목록을 수정할 수 있습니다.
- 를 사용합니다 -servers 쉼표로 구분된 목록의 IP 주소로 하나 이상의 LDAP 서버(Active Directory 또는 UNIX)를 지정하는 옵션입니다.



은 더 이상 사용되지 않습니다. -ldap-servers 필드는 다음을 대체합니다. -servers 필드. 이 필드에는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

- b. 기본 또는 사용자 지정 LDAP 스키마를 지정합니다.

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 읽기 전용 스키마를 사용할 수 있습니다. 그렇지 않으면 기본 스키마를 사용하는 것이 좋습니다. 이 경우 기본 스키마(읽기 전용)를 복사한 다음 복사본을 수정하여 고유한 스키마를 만들 수 있습니다.

기본 스키마:

- MS-AD-BIS

RFC-2307bis를 기반으로 하는 이 방식은 대부분의 표준 Windows 2012 이상 LDAP 구축에 선호되는 LDAP 스키마입니다.

- AD-IDMU

UNIX용 Active Directory ID 관리를 기반으로 하는 이 스키마는 대부분의 Windows 2008, Windows 2012 이상 AD 서버에 적합합니다.

- AD-SFU

UNIX용 Active Directory 서비스를 기반으로 하는 이 스키마는 대부분의 Windows 2003 및 이전 AD 서버에 적합합니다.

- RFC-2307

RFC-2307(LDAP를 네트워크 정보 서비스로 사용하는 접근 방식)에 따라 이 스키마는 대부분의 UNIX AD 서버에 적합합니다.

c. 바인딩 값을 선택합니다.

- '-min-bind-level{anonymous|simple|sasl}'은 최소 bind authentication level을 지정한다.

기본값은 ' * anonymous * '입니다.

- '-bind-dn_ldap_DN_'은 바인딩 사용자를 지정합니다.

Active Directory 서버의 경우 계정(domain\user) 또는 보안 주체(user@domain.com) 양식에서 사용자를 지정해야 합니다. 그렇지 않으면 고유 이름(CN=user, DC=domain, DC=com) 형식으로 사용자를 지정해야 합니다.

- '-BIND-PASSWORD_PASSWORD_'는 바인딩 암호를 지정합니다.

d. 필요한 경우 세션 보안 옵션을 선택합니다.

LDAP 서버에서 필요한 경우 LDAP 서명 및 봉인 또는 TLS를 통한 LDAP를 활성화할 수 있습니다.

- '--세션-보안{none|sign|seal}'

서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

또한 서명과 봉인 바인딩이 실패할 경우 바인딩 인증을 ' * anonymous * ' 또는 ' * simple * '로 되돌리지 않으려면 '-min-bind-level' {'s ASL'}을 설정해야 합니다.

- '-use-start-tls{'true'|'false'}

' * true*'로 설정되어 있고 LDAP 서버가 이를 지원하는 경우 LDAP 클라이언트는 서버에 암호화된 TLS 연결을 사용합니다. 기본값은 ' * FALSE * '입니다. 이 옵션을 사용하려면 LDAP 서버의 자체 서명된 루트 CA 인증서를 설치해야 합니다.



스토리지 VM에 도메인에 추가된 SMB 서버가 있고 LDAP 서버가 SMB 서버의 홈 도메인의 도메인 컨트롤러 중 하나인 경우 을 수정할 수 있습니다 -session-security-for-ad -ldap 옵션을 선택합니다 vserver cifs security modify 명령.

e. 포트, 쿼리 및 기준 값을 선택합니다.

기본값을 사용하는 것이 좋지만 LDAP 관리자에게 해당 값이 사용자 환경에 적합한지 확인해야 합니다.

- '-port_port_'는 LDAP 서버 포트를 지정합니다.

기본값은 389입니다.

Start TLS를 사용하여 LDAP 연결을 보호하려면 기본 포트 389를 사용해야 합니다. 시작 TLS는 LDAP 기본 포트 389를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다. 포트를 변경하면 Start TLS가 실패합니다.

- '-query-timeout_integer_'는 쿼리 시간 제한(초)을 지정합니다.

허용 범위는 1 ~ 10초입니다. 기본값은 3초입니다.

- '-base-dn_ldap_dn_'은 기본 DN을 지정합니다.

필요한 경우 여러 값을 입력할 수 있습니다(예: LDAP 조회 추적을 사용하는 경우). 기본값은 ""(root)입니다.

- '-base-scope'{'base'|'onelevel'|'subtree'}는 기본 검색 범위를 지정합니다.

기본값은 'Subtree'입니다.

- '-referral-enabled'{'true'|'false'}는 LDAP 조회 추적 활성화 여부를 지정합니다.

ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에 반환되어 원하는 레코드가 참조된 LDAP 서버에 있음을 나타내는 경우 ONTAP LDAP 클라이언트가 다른 LDAP 서버에 조회 요청을 참조할 수 있습니다. 기본값은 '* FALSE *'입니다.

참조된 LDAP 서버에 있는 레코드를 검색하려면 LDAP 클라이언트 구성의 일부로 참조된 레코드의 기본 dn을 기본 dn에 추가해야 합니다.

2. 스토리지 VM에서 LDAP 클라이언트 구성을 생성합니다.

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



LDAP 클라이언트 구성을 생성할 때 스토리지 VM 이름을 제공해야 합니다.

3. LDAP 클라이언트 구성이 성공적으로 생성되었는지 확인합니다.

```
'vserver services name-service ldap client show-client-config client_config_name'
```

예

다음 명령을 실행하면 스토리지 VM VS1이 LDAP용 Active Directory 서버와 함께 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

다음 명령을 실행하면 스토리지 VM VS1이 Active Directory 서버와 작동하여 서명과 봉인이 필요한 LDAP에 대해 ldap1이라는 새 LDAP 클라이언트 구성이 생성되고 LDAP 서버 검색이 지정된 도메인의 특정 사이트로 제한됩니다.

```
cluster1::> vservice services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

다음 명령을 실행하면 스토리지 VM VS1이 LDAP 조회 추적이 필요한 LDAP용 Active Directory 서버와 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vservice services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

다음 명령을 실행하면 기본 DN을 지정하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vservice services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

다음 명령을 실행하면 조회 추적을 활성화하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vservice services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

ONTAP NFS SVM과 LDAP 클라이언트 구성 연결

SVM에서 LDAP를 활성화하려면 "vservice services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결해야 합니다.

시작하기 전에

- LDAP 도메인은 네트워크 내에 이미 존재해야 하며 SVM이 있는 클러스터에서 액세스할 수 있어야 합니다.
- SVM에 LDAP 클라이언트 구성이 있어야 합니다.

단계

1. SVM에서 LDAP 지원:

'vserver services name-service LDAP create-vserver_vserver_name_-client-config_client_config_name_'



그만큼 vserver services name-service ldap create 명령은 자동 구성 검증을 수행하고 ONTAP 이름 서버에 접속할 수 없는 경우 오류 메시지를 보고합니다.

다음 명령을 실행하면 "VS1" SVM에서 LDAP를 활성화하고 "ldap1" LDAP 클라이언트 구성을 사용하도록 구성합니다.

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. vserver services name-service ldap check 명령을 사용하여 이름 서버의 상태를 확인합니다.

다음 명령은 SVM VS1 에서 LDAP 서버의 유효성을 검사합니다.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

ONTAP NFS SVM에 대한 LDAP 소스 확인

SVM을 위한 네임 서비스 스위치 테이블에 네임 서비스에 대한 LDAP 소스가 올바르게 나열되어 있는지 확인해야 합니다.

단계

1. 현재 이름 서비스 스위치 테이블 내용을 표시합니다.

'vserver services name-service ns-switch show -vserver_svm_name_'

다음 명령을 실행하면 SVM My_SVM의 결과가 표시됩니다.


```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
```

Vserver	Database	Source
-----	-----	-----
My_SVM	hosts	files, dns
My_SVM	group	files,ldap
My_SVM	passwd	files,ldap
My_SVM	netgroup	files
My_SVM	namemap	files

5 entries were displayed.

이름 매핑 정보를 검색할 소스 및 순서를 지정합니다. UNIX 전용 환경에서는 이 항목이 필요하지 않습니다. 이름 매핑은 UNIX와 Windows를 모두 사용하는 혼합 환경에서만 필요합니다.

2. 필요에 따라 ns-switch 항목을 업데이트합니다.

ns-switch 항목을 업데이트하려면...	명령 입력...
사용자 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database passwd -sources ldap, files'
그룹 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database group-sources ldap, files'
넷그룹 정보입니다	'vserver services name-service ns-switch modify -vserver_vserver_name_-database 넷그룹 - 소스 LDAP, 파일'

강력한 보안을 위해 **NFS**와 **Kerberos** 사용

보안 인증을 위해 **ONTAP NFS**와 함께 **Kerberos**를 사용하는 방법에 대해 알아보세요.

Kerberos가 강력한 인증을 위해 사용자 환경에서 사용되는 경우 Kerberos 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 Kerberos 클라이언트로 사용하도록 설정해야 합니다.

환경은 다음 지침을 충족해야 합니다.

- ONTAP용 Kerberos를 구성하기 전에 Kerberos 서버 및 클라이언트 구성에 대한 모범 사례를 따라야 합니다.
- 가능하면 Kerberos 인증이 필요한 경우 NFSv4 이상을 사용합니다.

NFSv3은 Kerberos와 함께 사용할 수 있습니다. 하지만 Kerberos의 모든 보안 이점은 NFSv4 이상의 ONTAP 구축에서만 실현됩니다.

- 중복 서버 액세스를 프로모션하려면 Kerberos가 동일한 SPN을 사용하여 클러스터의 여러 노드에 있는 여러 데이터 LIF에서 활성화되어야 합니다.
- SVM에서 Kerberos를 사용하도록 설정할 경우 NFS 클라이언트 구성에 따라 볼륨 또는 qtree의 내보내기 규칙에 다음 보안 방법 중 하나를 지정해야 합니다.
 - "krb5"(Kerberos v5 프로토콜)
 - "krb5i"(체크섬을 사용한 무결성 검사를 포함한 Kerberos v5 프로토콜)
 - "krb5p"(개인정보 보호 서비스가 있는 Kerberos v5 프로토콜)

Kerberos 서버 및 클라이언트 외에도 ONTAP가 Kerberos를 지원하도록 다음과 같은 외부 서비스를 구성해야 합니다.

- 디렉터리 서비스

SSL/TLS를 통해 LDAP를 사용하도록 구성된 Active Directory 또는 OpenLDAP와 같은 환경에서 보안 디렉터리 서비스를 사용해야 합니다. 요청이 일반 텍스트로 전송되므로 안전하지 않은 NIS를 사용하지 마십시오.

- NTP

NTP를 실행하는 작업 시간 서버가 있어야 합니다. 시간 편중이 발생하여 Kerberos 인증 실패를 방지하려면 이 작업이 필요합니다.

- 도메인 이름 확인(DNS)

각 UNIX 클라이언트와 각 SVM LIF에는 정방향 및 역방향 조회 영역에서 KDC에 등록된 적절한 서비스 레코드(SRV)가 있어야 합니다. 모든 참가자는 DNS를 통해 제대로 확인할 수 있어야 합니다.

ONTAP SVM에서 NFS Kerberos 구성에 대한 UNIX 권한 확인

Kerberos를 사용하려면 SVM 루트 볼륨 및 로컬 사용자 및 그룹에 대해 특정 UNIX 사용 권한을 설정해야 합니다.

단계

1. SVM 루트 볼륨에 대한 관련 권한을 표시합니다.

```
'volume show-volume_root_vol_name_-fields user, group, unix-permissions
```

SVM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름...	설정 중...
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	755

이 값이 표시되지 않으면 볼륨 수정 명령을 사용하여 값을 업데이트합니다.

2. 로컬 UNIX 사용자를 표시합니다.

'vserver services name-service unix-user show -vserver_vserver_name_'

SVM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 ID입니다	기본 그룹 ID입니다	설명
NFS 를 참조하십시오	500입니다	0	GSS INIT 단계에 필요함. NFS 클라이언트 사용자 SPN의 첫 번째 구성 요소가 사용자로 사용됩니다. NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다.
루트	0	0	마운팅에 필요합니다.

이러한 값이 표시되지 않으면 'vserver services name-service unix-user modify' 명령을 사용하여 해당 값을 업데이트할 수 있습니다.

3. 로컬 UNIX 그룹을 표시합니다.

'vserver services name-service unix-group show -vserver_vserver__name'

SVM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 ID입니다
데몬	1
루트	0

이러한 값이 표시되지 않으면 'vserver services name-service unix-group modify' 명령을 사용하여 해당 값을 업데이트할 수 있습니다.

ONTAP SVM에서 NFS Kerberos 영역 구성 만들기

ONTAP가 사용자 환경에서 외부 Kerberos 서버에 액세스하도록 하려면 먼저 기존 Kerberos 영역을 사용하도록 SVM을 구성해야 합니다. 이렇게 하려면 Kerberos KDC 서버에 대한 구성 값을 수집한 다음 "vserver NFS Kerberos realm create" 명령을 사용하여 SVM에서 Kerberos 영역 구성을 생성해야 합니다.

시작하기 전에

클러스터 관리자는 인증 문제를 방지하기 위해 스토리지 시스템, 클라이언트 및 KDC 서버에서 NTP를 구성해야 합니다. 클라이언트와 서버 간의 시간 차이(클럭 편중)는 인증 실패의 일반적인 원인입니다.

단계

1. Kerberos 관리자에게 문의하여 "vserver NFS Kerberos realm create" 명령을 제공하는 적절한 구성 값을 확인하십시오.
2. SVM에서 Kerberos 영역 구성 생성:

```
"vserver NFS Kerberos 영역 create -vserver _vserver_name_  
-realm _realm_name_{AD_KDC_server_values|AD_KDC_server_values}_-comment "text"
```

3. Kerberos 영역 구성이 성공적으로 생성되었는지 확인합니다.

가상 NFS Kerberos 영역 표시

예

다음 명령을 실행하면 Microsoft Active Directory 서버를 KDC 서버로 사용하는 SVM VS1 용 NFS Kerberos 영역 구성이 생성됩니다. Kerberos 영역은 AUTH.EXAMPLE.COM 입니다. Active Directory 서버의 이름은 ad-1이고 IP 주소는 10.10.8.14입니다. 허용되는 시간 편차는 300초(기본값)입니다. KDC 서버의 IP 주소는 10.10.8.14이고 포트 번호는 88(기본값)입니다. "Microsoft Kerberos 구성"이 주석입니다.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
AUTH.EXAMPLE.COM -adserver-name ad-1  
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88  
-kdc-vendor Microsoft  
-comment "Microsoft Kerberos config"
```

다음 명령을 실행하면 MIT KDC를 사용하는 SVM VS1 용 NFS Kerberos 영역 구성이 생성됩니다. Kerberos 영역은 SECURITY.EXAMPLE.COM 입니다. 허용되는 시간 편차는 300초입니다. KDC 서버의 IP 주소는 10.10.9.1이고 포트 번호는 88입니다. KDC 공급업체는 UNIX 공급업체를 나타내는 기타 벤더입니다. 관리 서버의 IP 주소는 10.10.9.1이고 포트 번호는 749(기본값)입니다. 암호 서버의 IP 주소는 10.10.9.1이고 포트 번호는 464(기본값)입니다. "UNIX Kerberos 구성"이 주석입니다.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
SECURITY.EXAMPLE.COM. -clock-skew 300  
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1  
-adminserver-port 749  
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX  
Kerberos config"
```

ONTAP SVM에 대해 NFS Kerberos 허용 암호화 유형 구성

기본적으로 ONTAP는 NFS Kerberos인 DES, 3DES, AES-128, AES-256에 대해 다음 암호화 유형을 지원합니다. "vserver nfs modify" 명령을 '-enc-types' 매개 변수와 함께 사용하면 각 SVM에 대해 허용된 암호화 유형을 특정 환경의 보안 요구사항에 맞게 구성할 수 있습니다.

이 작업에 대해

클라이언트 호환성을 극대화하기 위해 ONTAP는 기본적으로 약한 DES와 강력한 AES 암호화를 모두 지원합니다. 예를 들어, 보안을 강화하려는 경우 사용자 환경에서 이 절차를 사용하여 DES 및 3DES를 비활성화하고 클라이언트가 AES

암호화만 사용하도록 할 수 있습니다.

사용 가능한 가장 강력한 암호화를 사용해야 합니다. ONTAP의 경우, AES-256입니다. 해당 환경에서 이 암호화 수준이 지원되는지 KDC 관리자에게 확인해야 합니다.

- SVM에서 AES를 완전히 활성화 또는 비활성화(AES-128 및 AES-256 모두)하면 원래의 DES 기본/키텍 파일이 삭제되므로 SVM을 위한 모든 LIF에서 Kerberos 구성을 비활성화해야 합니다.

이를 변경하기 전에 NFS 클라이언트가 SVM에서 AES 암호화를 사용하지 않는지 확인해야 합니다.

- DES 또는 3DES를 활성화 또는 비활성화할 경우 LIF에서 Kerberos 구성을 변경할 필요가 없습니다.

단계

1. 허용되는 암호화 유형을 사용하거나 사용하지 않도록 설정합니다.

활성화 또는 비활성화하려는 경우...	다음 단계를 따르십시오...
DES 또는 3DES입니다	a. SVM의 NFS Kerberos 허용 암호화 유형을 구성합니다. + 'vserver NFS modify -vserver_vserver_name_-enc -types_encryption_types_' 여러 암호화 유형을 쉼표로 구분합니다. b. 성공적으로 변경되었는지 확인합니다. + 'vserver nfs show -vserver_vserver_name_-fields fitted-enc-types'

활성화 또는 비활성화하려는 경우...	다음 단계를 따르십시오...
AES-128 또는 AES-256	a. SVM 및 LIF Kerberos 사용 설정 식별: + 'vserver NFS Kerberos interface show' b. NFS Kerberos에서 허용할 암호화 유형을 수정하려는 SVM의 모든 LIF에서 Kerberos를 해제합니다. + 'vserver NFS Kerberos interface disable-lif_lif_name_' c. SVM의 NFS Kerberos 허용 암호화 유형을 구성합니다. + 'vserver NFS modify -vserver_vserver_name_-enc -types_encryption_types_' 여러 암호화 유형을 쉼표로 구분합니다. d. 성공적으로 변경되었는지 확인합니다. + 'vserver nfs show -vserver_vserver_name_-fields fitted-enc-types' e. SVM의 모든 LIF에서 Kerberos를 사용하도록 다시 설정합니다. + 'vserver NFS Kerberos interface enable-lif_lif_name_-spN_service_principal_name_' f. 모든 LIF에서 Kerberos가 설정되어 있는지 확인합니다. + 'vserver NFS Kerberos interface show'

ONTAP LIF에서 NFS Kerberos 활성화

데이터 LIF에서 Kerberos를 사용하도록 설정하려면 'vserver NFS Kerberos interface enable' 명령을 사용하십시오. 그러면 SVM에서 NFS에 Kerberos 보안 서비스를 사용할 수 있습니다.

이 작업에 대해

Active Directory KDC를 사용하는 경우 사용되는 SPN의 처음 15자는 영역 또는 도메인 내의 SVM에서 고유해야 합니다.

단계

1. NFS Kerberos 구성 생성:

```
'vserver NFS Kerberos interface enable-vserver_vserver_name_-lif_logical_interface_-spN_service_principal_name_'
```

ONTAP에서 Kerberos 인터페이스를 활성화하려면 KDC의 SPN에 대한 암호 키가 필요합니다.

Microsoft KDC의 경우 KDC에 문의하고 CLI에서 사용자 이름 및 암호 프롬프트가 발급되어 비밀 키를 얻습니다. Kerberos 영역의 다른 OU에 SPN을 만들어야 하는 경우 선택적 '-ou' 매개 변수를 지정할 수 있습니다.

비 Microsoft KDC의 경우 다음 두 가지 방법 중 하나를 사용하여 비밀 키를 얻을 수 있습니다.

만약...	다음 매개 변수도 명령에 포함해야 합니다.
KDC에서 직접 키를 검색하려면 KDC 관리자 자격 증명을 사용합니다	'-admin-username" kdc_admin_username'
KDC 관리자 자격 증명이 없지만 키가 포함된 KDC의 keytab 파일이 있습니다	'-keytab-uri '{ftp

2. Kerberos가 LIF에서 설정되었는지 확인합니다.

```
'vserver nfs Kerberos-config show'
```

3. 1단계와 2단계를 반복하여 여러 LIF에서 Kerberos를 사용하도록 설정합니다.

예

다음 명령을 실행하면 OU lab2ou 에서 SPN NFS /ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM 와 함께 논리 인터페이스 ves03-d1에서 이름이 VS1 인 SVM에 대한 NFS Kerberos 구성이 생성되고 확인됩니다.

```
vs1::> vsserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vsserver nfs kerberos-config show
      Logical
Vserver Interface Address      Kerberos  SPN
-----
vs0      ves01-a1
          10.10.10.30 disabled -
vs2      ves01-d1
          10.10.10.40 enabled  nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

NFS 지원 SVM에 스토리지 용량 추가

ONTAP NFS 지원 SVM에 스토리지 용량을 추가하는 방법에 대해 알아보세요.

NFS 지원 SVM에 스토리지 용량을 추가하려면 스토리지 컨테이너를 제공할 볼륨 또는 qtree를 생성하고 해당 컨테이너의 익스포트 정책을 생성하거나 수정해야 합니다. 그런 다음 클러스터에서 NFS 클라이언트 액세스를 확인하고 클라이언트 시스템에서 액세스를 테스트할 수 있습니다.

시작하기 전에

- SVM에서 NFS를 완전히 설정해야 합니다.
- SVM 루트 볼륨의 기본 익스포트 정책에는 모든 클라이언트에 액세스할 수 있는 규칙이 포함되어 있어야 합니다.
- 이름 서비스 구성에 대한 모든 업데이트를 완료해야 합니다.

- Kerberos 구성에 대한 추가 또는 수정을 완료해야 합니다.

ONTAP NFS 내보내기 정책 만들기

내보내기 규칙을 만들기 전에 해당 규칙을 보유할 내보내기 정책을 만들어야 합니다. 'vserver export-policy create' 명령을 사용하여 익스포트 정책을 생성할 수 있습니다.

단계

1. 익스포트 정책 생성:

```
'vserver export-policy create -vserver _vserver_name_ -policyname _policy_name_'
```

정책 이름은 최대 256자까지 지정할 수 있습니다.

2. 익스포트 정책이 생성되었는지 확인:

```
'vserver export-policy show -policyname _policy_name_'
```

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 exp1 이라는 익스포트 정책이 생성되는지 검증 및 됩니다.

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
-----
vs1              exp1
```

ONTAP NFS 내보내기 정책에 규칙 추가

규칙이 없으면 내보내기 정책은 클라이언트에 데이터에 대한 액세스를 제공할 수 없습니다. 새 내보내기 규칙을 만들려면 클라이언트를 식별하고 클라이언트 일치 형식을 선택하고, 액세스 및 보안 유형을 선택하고, 익명 사용자 ID 매핑을 지정하고, 규칙 인덱스 번호를 선택하고, 액세스 프로토콜을 선택해야 합니다. 그런 다음 'vserver export-policy rule create' 명령을 사용하여 내보내기 정책에 새 규칙을 추가할 수 있습니다.

시작하기 전에

- 내보내기 규칙을 추가할 익스포트 정책이 이미 있어야 합니다.
- 데이터 SVM에서 DNS를 올바르게 구성해야 하며, DNS 서버는 NFS 클라이언트를 위한 올바른 항목을 가지고 있어야 합니다.

이는 ONTAP가 특정 클라이언트 일치 형식에 대해 데이터 SVM의 DNS 구성을 사용하여 DNS 조회를 수행하고, 익스포트 정책 규칙 일치의 실패로 인해 클라이언트 데이터 액세스가 차단되기 때문입니다.

- Kerberos를 사용하여 인증하는 경우 NFS 클라이언트에서 사용되는 다음 보안 방법 중 하나를 결정해야 합니다.
 - "krb5"(Kerberos V5 프로토콜)

- "krb5i"(체크섬을 사용한 무결성 검사가 가능한 Kerberos V5 프로토콜)
- 'krb5p'(개인정보 보호 서비스가 있는 Kerberos V5 프로토콜)

이 작업에 대해

내보내기 정책의 기존 규칙이 클라이언트 일치 및 액세스 요구 사항을 포함하는 경우에는 새 규칙을 생성할 필요가 없습니다.

Kerberos를 사용하여 인증하는 경우 Kerberos를 통해 SVM의 모든 볼륨에 액세스할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5, krb5i 또는 krb5p로 설정할 수 있습니다.

단계

1. 새 규칙의 클라이언트 및 클라이언트 일치 형식을 식별합니다.

'-clientmatch' 옵션은 규칙이 적용되는 클라이언트를 지정합니다. 하나 또는 여러 개의 클라이언트 일치 값을 지정할 수 있습니다. 여러 값의 사양은 쉼표로 구분해야 합니다. 다음 형식 중 하나로 일치 항목을 지정할 수 있습니다.

클라이언트 일치 형식입니다	예
도메인 이름 앞에 "." 문자가 옵니다	
호스트 이름입니다	'host1' 또는 'host1, host2,...'
IPv4 주소입니다	10.1.12.24 또는 + 10.1.12.24,10.1.12.25,...+
서브넷 마스크가 있는 IPv4 주소는 비트 수로 표시됩니다	10.1.12.10/4, 또는 + 10.1.12.10/4,10.1.12.11/4,...+
네트워크 마스크가 있는 IPv4 주소입니다	10.1.16.0/255.255.255.0 또는 + 10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0,...+
점선 형식의 IPv6 주소입니다	'::1.2.3.4' 또는 '::1.2.3.4,::1.2.3.5,...'
서브넷 마스크가 있는 IPv6 주소는 비트 수로 표시됩니다	"ff::00/32" 또는 "ff::00/32, ff: 01/32,..."
넷그룹 이름 앞에 @ 문자가 오는 단일 넷그룹	'@netgroup1' 또는 '@netgroup1,@netgroup2,...'

클라이언트 정의 형식(예: '.example.com,@netgroup1')을 결합할 수도 있습니다.

IP 주소를 지정할 때 다음 사항에 유의하십시오.

- 10.1.12.10-10.1.12.70 등의 IP 주소 범위를 입력할 수 없습니다.

이 형식의 항목은 텍스트 문자열로 해석되며 호스트 이름으로 처리됩니다.

- 클라이언트 액세스의 세부 관리에 대한 내보내기 규칙에서 개별 IP 주소를 지정할 때 동적으로 할당되는 IP 주소(예: DHCP) 또는 임시로 할당된 IP 주소(예: IPv6)를 지정하지 마십시오.

그렇지 않으면 IP 주소가 변경되면 클라이언트가 액세스 권한을 잃게 됩니다.

- 네트워크 마스크로 IPv6 주소(예: ff::12/ff::00)를 입력할 수 없습니다.

2. 클라이언트 일치에 대한 액세스 및 보안 유형을 선택합니다.

지정된 보안 유형으로 인증하는 클라이언트에 대해 다음 액세스 모드 중 하나 이상을 지정할 수 있습니다.

- '-rorule'(읽기 전용 액세스)
- '-rwrule'(읽기-쓰기 액세스)
- '-superuser'(루트 액세스)



내보내기 규칙에서 해당 보안 유형에 대한 읽기 전용 액세스도 허용하는 경우 클라이언트는 특정 보안 유형에 대한 읽기-쓰기 액세스만 얻을 수 있습니다. 읽기 전용 매개 변수가 읽기-쓰기 매개 변수보다 보안 형식에 대해 더 제한적인 경우 클라이언트는 읽기-쓰기 액세스를 얻지 못할 수 있습니다. 슈퍼유저 액세스도 마찬가지입니다.

규칙에 대해 여러 보안 유형의 심표로 구분된 목록을 지정할 수 있습니다. 보안 유형을 "모두" 또는 "사용 안 함"으로 지정하는 경우 다른 보안 유형을 지정하지 마십시오. 다음 유효한 보안 유형 중에서 선택하십시오.

보안 유형을 다음으로 설정한 경우...	일치하는 클라이언트가 내보낸 데이터에 액세스할 수 있습니다...
모두	항상, 들어오는 보안 유형에 관계없이.
"없음"	보안 유형을 가진 클라이언트만 나열되면 익명 액세스 권한이 부여됩니다. 다른 보안 유형과 함께 나열되는 경우 지정된 보안 유형의 클라이언트는 액세스 권한이 부여되고 다른 보안 유형의 클라이언트는 익명 액세스 권한이 부여됩니다.
"안 돼.	수신 보안 유형에 관계없이 사용 안 함.
krb5	Kerberos 5에 의해 인증되는 경우 인증 전용: 각 요청 및 응답의 헤더가 서명됩니다.
krb5i	Kerberos 5i에 의해 인증되는 경우. 인증 및 무결성: 각 요청 및 응답의 헤더와 본문이 서명됩니다.
크르b5p	Kerberos 5p에 의해 인증되는 경우 인증, 무결성 및 개인 정보 보호: 각 요청 및 응답의 헤더와 본문이 서명되고 NFS 데이터 페이로드가 암호화됩니다.
NTLM	CIFS NTLM에 의해 인증되는 경우
'스'입니다	NFS AUTH_SYS에 의해 인증되는 경우

권장 보안 유형은 '시스', 또는 Kerberos를 사용하는 경우 krb5, krb5i, krb5p입니다.

NFSv3에서 Kerberos를 사용하는 경우, 내보내기 정책 규칙은 krb5 이외에 '-rorule' 및 '-rwrule' 액세스를 허용해야 합니다. 이는 내보내기에 대한 NLM(Network Lock Manager) 액세스를 허용해야 하기 때문입니다.

3. 익명 사용자 ID 매핑을 지정합니다.

'anon' 옵션은 사용자 ID가 0인 클라이언트 요청에 매핑된 UNIX 사용자 ID 또는 사용자 이름을 지정합니다. 이 사용자 이름은 일반적으로 사용자 이름 루트와 연결됩니다. 기본값은 65534입니다. NFS 클라이언트는 일반적으로 사용자 ID 65534를 사용자 이름 nobody(또는 *root squooting*)와 연결합니다. ONTAP에서 이 사용자 ID는 사용자 pcuser와 연결됩니다. 사용자 ID가 0인 클라이언트에서 액세스를 비활성화하려면 값을 65535로 지정합니다.

4. 규칙 인덱스 순서를 선택합니다.

ruleindex 옵션은 규칙의 인덱스 번호를 지정합니다. 규칙은 인덱스 번호 목록의 순서에 따라 평가되며, 인덱스 번호가 낮은 규칙은 먼저 평가됩니다. 예를 들어 인덱스 번호가 1인 규칙은 인덱스 번호가 2인 규칙 전에 평가됩니다.

추가하는 경우...	그러면...
엑스포트 정책에 대한 첫 번째 규칙	1을 입력합니다.
엑스포트 정책에 대한 추가 규칙	a. 정책에 기존 규칙을 표시합니다. + 'vserver export-policy rule show-instance-policyname_your_policy_' b. 평가해야 하는 순서에 따라 새 규칙의 인덱스 번호를 선택합니다.

5. 해당 NFS 액세스 값 {'NFS'|'NFS3'|'nfs4'}을 선택합니다.

NFS는 어떤 버전이든 일치하며 NFS3, nfs4는 특정 버전만을 일치시킵니다.

6. 내보내기 규칙을 만들어 기존 엑스포트 정책에 추가합니다.

```
'vserver export-policy rule create-vserver_vserver_name_-policyname_policy_name_-ruleindex_integer_-protocol{nNFS|NFS3|nfs4}-clientmatch {text|"text,text,..."}-rorule_security_type_-superuser_security_type_ananID
```

7. 내보내기 정책의 규칙을 표시하여 새 규칙이 있는지 확인합니다.

```
'vserver export-policy rule show-policyname_policy_name_'
```

명령은 해당 정책에 적용되는 규칙 목록을 포함하여 해당 엑스포트 정책에 대한 요약을 표시합니다. ONTAP는 각 규칙에 규칙 인덱스 번호를 할당합니다. 규칙 인덱스 번호를 알고 나면 이 번호를 사용하여 지정된 엑스포트 규칙에 대한 자세한 정보를 표시할 수 있습니다.

8. 내보내기 정책에 적용된 규칙이 올바르게 구성되었는지 확인합니다.

```
'vserver export-policy rule show -policyname_policy_name_-vserver_vserver_name_-ruleindex_integer_'
```

예

다음 명령은 RS1이라는 엑스포트 정책에서 VS1이라는 SVM에 엑스포트 규칙이 생성되었는지 확인합니다. 규칙에 인덱스 번호가 1입니다. 이 규칙은 eng.company.com 도메인에 있는 모든 클라이언트와 netgroup@netgroup1과

일치합니다. 이 규칙은 모든 NFS 액세스를 설정합니다. AUTH_SYS로 인증된 사용자에게 대한 읽기 전용 및 읽기-쓰기 액세스를 활성화합니다. UNIX 사용자 ID가 0인 클라이언트는 Kerberos로 인증되지 않는 한 익명화됩니다.

```
vs1::> vsserver export-policy rule create -vsserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgroup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5
```

```
vs1::> vsserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs1	exp1	1	nfs	eng.company.com, @netgroup1	sys

```
vs1::> vsserver export-policy rule show -policyname exp1 -vsserver vs1
-ruleindex 1
```

```

Vserver: vs1
Policy Name: exp1
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

다음 명령은 expol2라는 익스포트 정책에서 VS2라는 SVM에 익스포트 규칙이 생성되었는지 확인합니다. 규칙의 인덱스 번호는 21입니다. 이 규칙은 클라이언트를 netgroup dev_netgroup_main의 구성원과 일치시킵니다. 이 규칙은 모든 NFS 액세스를 설정합니다. AUTH_SYS로 인증되고 읽기-쓰기 및 루트 액세스에 Kerberos 인증이 필요한 사용자에게 대해 읽기 전용 액세스를 활성화합니다. UNIX 사용자 ID가 0인 클라이언트는 Kerberos로 인증되지 않는 한 루트 액세스가 거부됩니다.

```
vs2::> vsserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5
```

```
vs2::> vsserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs2	expol2	21	nfs	@dev_netgroup_main	sys

```
vs2::> vsserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21
```

```

Vserver: vs2
Policy Name: expol2
Rule Index: 21
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
@dev_netgroup_main
RO Access Rule: sys
RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true

```

볼륨 또는 **qtree** 스토리지 컨테이너를 생성합니다

ONTAP NFS 볼륨 생성

볼륨을 생성하고 "volume create" 명령을 사용하여 해당 접합 지점 및 기타 속성을 지정할 수 있습니다.

이 작업에 대해

클라이언트에서 데이터를 사용할 수 있도록 하려면 볼륨에 `_junction path_`가 포함되어야 합니다. 새 볼륨을 생성할 때 접합 경로를 지정할 수 있습니다. 접합 경로를 지정하지 않고 볼륨을 생성하는 경우, "volume mount" 명령을 사용하여 SVM 네임스페이스에서 볼륨을 `_mount_`해야 합니다.

시작하기 전에

- NFS를 설정하고 실행해야 합니다.
- SVM 보안 유형은 UNIX여야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 **"파일 시스템 분석 설정"**. 에 대한 자세한 내용은 volume create **"ONTAP 명령 참조입니다"**을 참조하십시오.

단계

1. 교차점으로 볼륨을 생성합니다.

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path [-policy
export_policy_name]
```

'-junction-path'의 선택 항목은 다음과 같습니다.

- 루트 바로 아래, 예: `'/new_vol'`

새 볼륨을 생성하고 SVM 루트 볼륨에 직접 마운트하도록 지정할 수 있습니다.

- 기존 디렉토리 아래에, 예: `"/existing_dir/new_vol"`

새 볼륨을 생성하고 기존 계층 구조에서 기존 볼륨에 마운트하도록 지정할 수 있습니다. 이 볼륨은 디렉토리로 표시됩니다.

새 볼륨 아래의 새 계층 구조에서 `"/new_dir/new_vol"`와 같은 새 디렉토리에 볼륨을 생성하려면 먼저 SVM 루트 볼륨에 대한 분기인 새 상위 볼륨을 생성해야 합니다. 그런 다음 새 상위 볼륨(새 디렉토리)의 접합 경로에 새 하위 볼륨을 생성합니다.

+ 기존 익스포트 정책을 사용하려는 경우 볼륨을 생성할 때 지정할 수 있습니다. 나중에 볼륨 수정 명령을 사용하여 내보내기 정책을 추가할 수도 있습니다.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

```
volume show -vserver svm_name -volume volume_name -junction
```

예

다음 명령을 실행하면 SVM vs1.example.com 및 애그리게이트 aggr1에 user1이라는 새 볼륨이 생성됩니다. 새 볼륨은 'users'에서 사용할 수 있습니다. 볼륨의 크기는 750GB이고 볼륨 유형은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

다음 명령을 실행하면 SVM "vs1.example.com" 및 애그리게이트 "aggr1"에 "home4"라는 새 볼륨이 생성됩니다. VS1

SVM은 이름 공간에 /ENG/ 디렉토리가 이미 있으며, '/ENG/' 네임스페이스의 홈 디렉토리가 되는 '/ENG/HOME'에서 새 볼륨을 사용할 수 있습니다. 볼륨 크기는 750GB이고 볼륨 보장은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

ONTAP NFS qtree 생성

'volume qtree create' 명령을 사용하여 데이터를 포함하는 qtree를 생성하고 해당 속성을 지정할 수 있습니다.

시작하기 전에

- SVM과 새 qtree가 포함될 볼륨이 이미 존재해야 합니다.
- SVM 보안 스타일은 UNIX여야 하며 NFS를 설정하고 실행해야 합니다.

단계

1. qtree 생성:

```
'볼륨 qtree create-vserver_vserver_name_{-volume_volume_name_-qtree_qtree_name_-qtree-path_qtree
path_} - 보안 스타일 UNIX [-policy_export_policy_name_]'
```

볼륨과 qtree를 별도의 인수로 지정하거나 qtree 경로 인수를 '/vol/volume_name/_qtree_name' 형식으로 지정할 수 있습니다.

기본적으로 Qtree는 상위 볼륨의 익스포트 정책을 상속하지만, 자체 정책을 사용하도록 구성할 수 있습니다. 기존 익스포트 정책을 사용하려는 경우 qtree를 생성할 때 지정할 수 있습니다. 나중에 'volume qtree modify' 명령을 사용하여 익스포트 정책을 추가할 수도 있습니다.

2. qtree가 원하는 접합 경로로 생성되었는지 확인합니다.

```
'volume qtree show-vserver_vserver_name_{-volume_volume_name_-qtree_qtree_name_-qtree-
path_qtree path_}'
```

예

다음 예에서는 junction path '/vol/data1'이 있는 SVM vs1.example.com 에 qt01이라는 이름의 qtree를 생성합니다.

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style unix  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: unix  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

내보내기 정책을 사용하여 **NFS** 액세스를 보호합니다

내보내기 정책을 사용하여 **ONTAP NFS** 액세스 보안에 대해 알아보세요.

엑스포트 정책을 사용하여 볼륨 또는 qtree에 대한 NFS 액세스를 특정 매개 변수와 일치하는 클라이언트로 제한할 수 있습니다. 새 스토리지를 프로비저닝할 때 기존 정책 및 규칙을 사용하거나, 기존 정책에 규칙을 추가하거나, 새 정책 및 규칙을 생성할 수 있습니다. 내보내기 정책의 구성을 확인할 수도 있습니다



ONTAP 9.3부터 오류 규칙 목록에 규칙 위반을 기록하는 백그라운드 작업으로 내보내기 정책 구성 검사를 활성화할 수 있습니다. 'vserver export-policy config-checker' 명령은 checker를 호출하여 결과를 표시합니다. 이 명령을 사용하면 구성을 확인하고 정책에서 잘못된 규칙을 삭제할 수 있습니다. 명령은 호스트 이름, 넷그룹 및 익명 사용자에 대한 내보내기 구성만 검증합니다.

ONTAP NFS 내보내기 규칙의 처리 순서를 관리합니다.

'vserver export-policy rule setindex' 명령을 사용하여 기존 엑스포트 규칙의 인덱스 번호를 수동으로 설정할 수 있습니다. 이렇게 하면 ONTAP가 클라이언트 요청에 내보내기 규칙을 적용하는 우선 순위를 지정할 수 있습니다.

이 작업에 대해

새 인덱스 번호가 이미 사용 중인 경우 명령은 지정된 위치에 규칙을 삽입하고 이에 따라 목록의 순서를 다시 지정합니다.

단계

1. 지정된 엑스포트 규칙의 인덱스 번호 수정:


```
'vserver export-policy rule setindex-vserver_virtual_server_name_-policyname_policy_name_-ruleindex_integer_-newruleindex_integer_'
```

예

다음 명령을 실행하면 VS1 이라는 SVM의 RS1 익스포트 정책에서 인덱스 번호 3에 있는 익스포트 규칙의 인덱스 번호가 인덱스 번호 2로 변경됩니다.

```
vs1::> vserver export-policy rule setindex -vserver vs1  
-policyname rs1 -ruleindex 3 -newruleindex 2
```

볼륨에 **ONTAP NFS** 내보내기 정책 할당

SVM에 포함된 각 볼륨은 클라이언트의 볼륨 데이터 액세스 익스포트 규칙이 포함된 익스포트 정책과 연결되어야 합니다.

이 작업에 대해

볼륨을 생성할 때 또는 볼륨을 생성한 후 언제든지 익스포트 정책을 볼륨에 연결할 수 있습니다. 하나의 정책을 여러 볼륨에 연결할 수 있지만 하나의 익스포트 정책을 볼륨에 연결할 수 있습니다.

단계

1. 볼륨을 생성할 때 익스포트 정책을 지정하지 않은 경우 볼륨에 익스포트 정책을 할당합니다.

```
'volume modify -vserver_vserver_name_-volume_volume_name_-policy_export_policy_name_'
```

2. 정책이 볼륨에 할당되었는지 확인합니다.

```
'volume show-volume_volume_name_-fields policy'입니다
```

예

다음 명령은 SVM VS1 볼륨 vol1에 익스포트 정책 NFS_policy를 할당하고 할당을 확인합니다.

```
cluster::> volume modify -vserver vs1 -volume vol1 -policy nfs_policy  
  
cluster::>volume show -volume vol -fields policy  
vserver volume      policy  
-----  
vs1      vol1      nfs_policy
```

ONTAP NFS 내보내기 정책을 **qtree**에 할당합니다.

전체 볼륨을 내보내는 대신, 볼륨에 있는 특정 qtree를 익스포트하여 클라이언트에서 직접 액세스할 수도 있습니다. 익스포트 정책을 qtree에 할당하여 qtree를 내보낼 수 있습니다. 새 qtree를 생성하거나 기존 qtree를 수정하여 익스포트 정책을 할당할 수 있습니다.

시작하기 전에

엑스포트 정책이 있어야 합니다.

이 작업에 대해

기본적으로 Qtree는 생성 시 별도로 지정하지 않을 경우 포함하는 볼륨의 상위 엑스포트 정책을 상속합니다.

qtree를 생성하거나 qtree를 생성한 후 언제든지 엑스포트 정책을 qtree에 연결할 수 있습니다. 하나의 정책을 여러 qtree와 연결할 수 있지만 하나의 엑스포트 정책을 qtree에 연결할 수 있습니다.

단계

1. Qtree 생성 시 엑스포트 정책을 지정하지 않은 경우 qtree에 엑스포트 정책을 할당하십시오.

```
'볼륨 qtree modify -vserver_vserver_name_-qtree -path /vol/volume_name /qtree_name-export  
-policy_export_policy_name_'
```

2. 정책이 qtree에 할당되었는지 확인합니다.

```
'volume qtree show-qtree_qtree_name_-fields export-policy'
```

예

다음 명령은 SVM VS1의 qtree q1에 엑스포트 정책 NFS_policy를 할당하고 할당을 확인합니다.

```
cluster::> volume modify -vserver vs1 -qtree-path /vol/vol1/qt1 -policy  
nfs_policy  
  
cluster::>volume qtree show -volume vol1 -fields export-policy  
vserver volume qtree export-policy  
-----  
vs1      data1  qt01  nfs_policy
```

클러스터에서 **ONTAP NFS** 클라이언트 액세스를 확인하세요.

UNIX 관리 호스트에서 UNIX 파일 권한을 설정하여 선택한 클라이언트에 공유에 대한 액세스 권한을 부여할 수 있습니다. 'vserver export-policy check-access' 명령을 사용하여 필요에 따라 내보내기 규칙을 조정하여 클라이언트 액세스를 확인할 수 있습니다.

단계

1. 클러스터에서 'vserver export-policy check-access' 명령을 사용하여 내보내기에 대한 클라이언트 액세스를 확인합니다.

다음 명령은 IP 주소 1.2.4를 사용하여 볼륨 home2에 대한 NFSv3 클라이언트의 읽기/쓰기 액세스를 확인합니다. 명령 출력에서는 볼륨이 내보내기 정책 'exp-home-dir'을 사용하고 액세스가 거부됨을 보여 줍니다.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
```

Path	Policy	Policy Owner	Policy Owner Type	Rule Index	Access
/	default	vs1_root	volume	1	read
/eng	default	vs1_root	volume	1	read
/eng/home2	exp-home-dir	home2	volume	1	denied

3 entries were displayed.

- 출력을 검사하여 내보내기 정책이 의도한 대로 작동하고 클라이언트 액세스가 예상대로 작동하는지 확인합니다.

특히, 볼륨 또는 qtree에서 사용하는 익스포트 정책과 이로 인해 클라이언트가 사용하는 액세스 유형을 확인해야 합니다.

- 필요한 경우 익스포트 정책 규칙을 다시 구성하십시오.

클라이언트 시스템에서 **ONTAP NFS** 액세스 테스트

새 스토리지 개체에 대한 NFS 액세스를 검증한 후 NFS 관리 호스트에 로그인하고 SVM에서 데이터를 읽고 쓰는 방법으로 구성을 테스트해야 합니다. 그런 다음 클라이언트 시스템에서 루트 이외의 사용자로 프로세스를 반복해야 합니다.

시작하기 전에

- 클라이언트 시스템에는 이전에 지정한 내보내기 규칙에서 허용하는 IP 주소가 있어야 합니다.
- 루트 사용자에 대한 로그인 정보가 있어야 합니다.

단계

- 클러스터에서 새 볼륨을 호스팅하는 LIF의 IP 주소를 확인합니다.

```
'network interface show -vserver_svm_name_'
```

에 대한 자세한 내용은 `network interface show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

- 관리 호스트 클라이언트 시스템에 루트 사용자로 로그인합니다.
- 디렉토리를 마운트 폴더로 변경합니다.

```
"cd /mnt/"
```

- SVM의 IP 주소를 사용하여 새 폴더를 생성하고 마운트합니다.

a. 새 폴더: + `mkdir /mnt/folder`를 만듭니다

b. 이 새 디렉토리에 새 볼륨을 마운트합니다. + `mount -t nfs -o hard_IPAddress_:/volume_name/mnt/folder`

- c. 디렉터리를 새 폴더 + 'cd_folder_'로 변경합니다

다음 명령을 실행하면 test1이라는 폴더가 생성됩니다. test1 마운트 폴더의 192.0.2.130 IP 주소에 vol1 볼륨을 마운트하고 새 test1 디렉토리로 변경합니다.

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 새 파일을 만들고 파일이 있는지 확인한 후 다음 파일에 텍스트를 씁니다.

- a. 테스트 파일을 만듭니다. + "touch_filename_"
- b. 파일이 있는지 확인합니다.: + "ls -l_filename_"
- c. cat>_filename_'을 입력합니다

텍스트를 입력하고 Ctrl+D를 눌러 테스트 파일에 텍스트를 씁니다.

- d. 테스트 파일의 내용을 표시합니다. "cat_filename_"
- e. 테스트 파일: + "rm_filename_"을 제거합니다
- f. 상위 디렉토리로 돌아가기: + "cd..."

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. 루트로 마운트된 볼륨에 대해 원하는 UNIX 소유권 및 권한을 설정합니다.
7. 내보내기 규칙에서 식별된 UNIX 클라이언트 시스템에서 이제 새 볼륨에 액세스할 수 있는 권한이 있는 사용자 중 하나로 로그인하고 3-5단계의 절차를 반복하여 볼륨을 마운트하고 파일을 생성할 수 있는지 확인합니다.

추가 **ONTAP NFS** 정보를 찾을 수 있는 곳

NFS 클라이언트 액세스를 성공적으로 테스트한 후 추가 NFS 구성을 수행하거나 SAN 액세스를 추가할 수 있습니다. 프로토콜 액세스가 완료되면 SVM(스토리지 가상 머신)의 루트 볼륨을 보호해야 합니다.

NFS 구성

다음 정보 및 기술 보고서를 사용하여 NFS 액세스를 추가로 구성할 수 있습니다.

- ["NFS 관리"](#)

NFS를 사용하여 파일 액세스를 구성 및 관리하는 방법에 대한 설명은 [여기](#)에 나와 있습니다.

- ["NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"](#)

NFSv3 및 NFSv4 운영 가이드 역할을 하며 NFSv4를 중심으로 ONTAP 운영 체제에 대한 개요를 제공합니다.

- ["NetApp 기술 보고서 4073: 안전한 통합 인증"](#)

NFS 스토리지 인증을 위한 UNIX 기반 Kerberos 버전 5(krb5) 서버 및 Windows Server Active Directory(AD)를 KDC 및 LDAP(Lightweight Directory Access Protocol) ID 공급자로 사용하도록 ONTAP를 구성하는 방법은 [여기](#)에 나와 있습니다.

- ["NetApp 기술 보고서 3580: NFSv4 향상 및 모범 사례 가이드 Data ONTAP 구축"](#)

여기서는 ONTAP를 실행하는 시스템에 접속된 AIX, Linux 또는 Solaris 클라이언트에서 NFSv4 구성 요소를 구축하는 동안 따라야 하는 Best Practice를 설명합니다.

네트워킹 구성

다음 정보 및 기술 보고서를 사용하여 네트워킹 기능 및 이름 서비스를 추가로 구성할 수 있습니다.

- ["NFS 관리"](#)

여기서는 ONTAP 네트워킹을 구성하고 관리하는 방법에 대해 설명합니다.

- ["NetApp 기술 보고서 4182: 이더넷 스토리지 설계 고려사항 및 clustered Data ONTAP 구성에 대한 모범 사례"](#)

ONTAP 네트워크 구성의 구현을 설명하고 일반적인 네트워크 배포 시나리오 및 모범 사례 권장 사항을 제공합니다.

- ["NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"](#)

인증 위해 LDAP, NIS, DNS 및 로컬 파일 구성을 구성하는 방법은 [여기](#)에 나와 있습니다.

SAN 프로토콜 구성

새 SVM에 대한 SAN 액세스를 제공하거나 수정하려는 경우 여러 호스트 운영 체제에서 사용할 수 있는 FC 또는 iSCSI 구성 정보를 사용할 수 있습니다.

루트 볼륨 보호

SVM에서 프로토콜을 구성한 후에는 루트 볼륨이 보호되는지 확인해야 합니다.

- ["데이터 보호"](#)

NAS 지원 SVM에 대한 NetApp의 모범 사례인 SVM 루트 볼륨을 보호하기 위해 로드 공유 미러를 생성하는 방법에 대해 설명합니다. 또한, 로드 공유 미러에서 SVM 루트 볼륨을 프로모션하여 볼륨 장애 또는 손실로부터 빠르게 복구하는 방법을 설명합니다.

ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다른지

ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다른지

ONTAP에서 NFS 익스포트 구성하는 방법에 대한 생소한 사용자는 7-Mode와 ONTAP 익스포트 구성 툴을 비교할 수 있을 뿐만 아니라 7-Mode '/etc/exports' 파일을 클러스터 정책 및 규칙과 비교할 수 있습니다.

ONTAP에는 '/etc/exports' 파일과 'exportfs' 명령이 없습니다. 대신 익스포트 정책을 정의해야 합니다. 익스포트 정책을 사용하면 7-Mode와 동일한 방식으로 클라이언트 액세스를 제어할 수 있으며, 여러 볼륨에 동일한 익스포트 정책을 다시 사용할 수 있는 등 기능도 추가로 제공됩니다.

관련 정보

["NFS 관리"](#)

["NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"](#)

7-Mode 및 ONTAP NFS 내보내기 비교에 대해 알아보세요

ONTAP의 내보내기는 7-Mode 환경에 있는 내보내기와 다르게 정의 및 사용됩니다.

차이 영역	향상됩니다	ONTAP
내보내기 정의 방법	내보내기는 '/etc/exports' 파일에 정의되어 있습니다.	내보내기는 SVM 내에서 익스포트 정책을 생성하여 정의합니다. SVM에는 둘 이상의 익스포트 정책이 포함될 수 있습니다.
수출 범위	• 내보내기는 지정된 파일 경로 또는 qtree에 적용됩니다. • 각 파일 경로 또는 qtree에 대해 '/etc/exports'에 별도의 항목을 생성해야 합니다. • 내보내기는 '/etc/exports' 파일에 정의되어 있는 경우에만 지속적입니다.	• 익스포트 정책은 볼륨에 포함된 모든 파일 경로 및 qtree를 포함하여 전체 볼륨에 적용됩니다. • 원하는 경우 둘 이상의 볼륨에 내보내기 정책을 적용할 수 있습니다. • 모든 내보내기 정책은 시스템을 다시 시작할 때마다 유지됩니다.
펜싱(동일한 리소스에 대한 특정 클라이언트에 대해 다른 액세스 지정)	내보낸 단일 리소스에 대해 특정 클라이언트에 서로 다른 액세스 권한을 제공하려면 각 클라이언트와 허용된 액세스 권한을 '/etc/exports' 파일에 나열해야 합니다.	익스포트 정책은 다양한 개별 익스포트 규칙으로 구성됩니다. 각 내보내기 규칙은 리소스에 대한 특정 액세스 권한을 정의하고 해당 권한이 있는 클라이언트를 나열합니다. 특정 클라이언트에 대해 다른 액세스를 지정하려면 각 특정 액세스 권한 집합에 대한 내보내기 규칙을 만들고 해당 권한이 있는 클라이언트를 나열한 다음 익스포트 정책에 규칙을 추가해야 합니다.

이름 앨리어싱	내보내기를 정의할 때 파일 경로 이름과 내보내기 이름을 다르게 지정할 수 있습니다. '/etc/exports' 파일에서 해당 내보내기를 정의할 때 '-actual' 매개변수를 사용해야 합니다.	내보낸 볼륨의 이름을 실제 볼륨 이름과 다르게 설정할 수 있습니다. 이렇게 하려면 SVM 네임스페이스 내에서 사용자 지정 접합 경로 이름을 사용하여 볼륨을 마운트해야 합니다.  기본적으로 볼륨은 해당 볼륨 이름으로 마운트됩니다. 볼륨의 접합 경로 이름을 사용자 지정하려면 마운트를 해제하고 이름을 바꾼 다음 다시 마운트해야 합니다.

ONTAP NFS 내보내기 정책 예제에 대해 알아보세요

내보내기 정책의 예를 검토하여 ONTAP에서 내보내기 정책의 작동 방식을 보다 잘 이해할 수 있습니다.

7-Mode 내보내기의 ONTAP 구현 예

다음 예에서는 '/etc/export' 파일에 나타나는 7-Mode 내보내기를 보여 줍니다.

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

이 내보내기를 클러스터된 내보내기 정책으로 복제하려면 세 개의 익스포트 규칙을 사용하여 익스포트 정책을 생성한 다음 볼륨 vol1에 익스포트 정책을 할당해야 합니다.

규칙	요소	값
규칙 1	'-clientmatch'(클라이언트 사양)	'@readonly_netgroup'
'-ruleindex'(규칙 목록에 있는 내보내기 규칙의 위치)	"1"	'-프로토콜'
'NFS'입니다	'-rorule'(읽기 전용 액세스 허용)	Sys(AUTH_SYS로 인증받은 클라이언트)
'-rwrule'(읽기-쓰기 액세스 허용)	"안 돼.	'-superuser'(슈퍼유저 액세스 허용)
'없음'(root_squashed_to anon)	규칙 2	'-clientmatch'
'@rootaccess_netgroup'	룰레인덱스	2

규칙	요소	값
'-프로토콜'	'NFS'입니다	'-rorule'
'스'입니다	'-rwrule'	'스'입니다
'-슈퍼유저'	'스'입니다	규칙 3
'-clientmatch'	'@readwrite_netgroup1, @readwrite_netgroup2'	룰레인덱스
3	'-프로토콜'	'NFS'입니다
'-rorule'	'스'입니다	'-rwrule'
'스'입니다	'-슈퍼유저'	"없음"

1. exp_vol1이라는 익스포트 정책을 생성합니다.

```
'vserver export-policy create-vserver NewSVM-policyname exp_vol1'
```

2. 기본 명령에 다음 매개 변수를 사용하여 세 개의 규칙을 생성합니다.

- 기본 명령: + 'vserver export-policy rule create-vserver NewSVM-policyname exp_vol1'
- 규칙 매개 변수: + ``clientmatch@readonly_netgroup-ruleindex 1-protocol nfs-rorule sys-rwrule never-superuser none'+ '-clientmatch@rootaccess_netgroup-rindex 2-protocol nfs-rorule_rule_rule_rule -clientmatch@readwrite_wrule_wrule -rrulule_nfs -rrrrrule_none

3. 볼륨 vol1에 정책을 할당합니다.

```
'volume modify -vserver NewSVM-volume vol1-policy exp_vol1'
```

7-Mode 익스포트 통합의 예

다음 예에서는 10개의 qtree당 한 줄이 포함된 7-Mode '/etc/export' 파일을 보여 줍니다.

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```


ONTAP에서는 각 qtree에 대해 -clientmatch host1519s 등의 규칙이 있는 정책 또는 -clientmatch host2057s 등의 규칙이 있는 정책 중 하나가 필요합니다.

1. exp_vol1q1 및 exp_vol1q2라는 두 개의 익스포트 정책을 생성합니다.
 - 'vserver export-policy create-vserver NewSVM-policyname exp_vol1q1'
 - 'vserver export-policy create-vserver NewSVM-policyname exp_vol1q2'
2. 각 정책에 대한 규칙 생성:
 - 'vserver export-policy rule create-vserver newSVM-policyname exp_vol1q1-clientmatch host1519s-rwrule sys-superuser sys'
 - 'vserver export-policy rule create-vserver newSVM-policyname exp_vol1q2-clientmatch host1519s-rwrule sys-superuser sys'
3. qtree에 정책을 적용합니다.
 - '볼륨 qtree modify -vserver NewSVM-qtree-path /vol/vol1/q_1472-export-policy exp_vol1q1'
 - [다음 4 qtree...]
 - '볼륨 qtree modify -vserver NewSVM-qtree-path /vol/vol1/q_2237 -export-policy exp_vol1q2'
 - [다음 4 qtree...]

나중에 이러한 호스트에 대해 추가 qtree를 추가해야 하는 경우 동일한 익스포트 정책을 사용합니다.

NFS 관리

NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요

ONTAP에는 NFS 프로토콜에 사용할 수 있는 파일 액세스 기능이 포함되어 있습니다. NFS 서버를 사용하도록 설정하고 볼륨 또는 qtree를 내보낼 수 있습니다.

다음과 같은 상황에서 이러한 절차를 수행합니다.

- ONTAP NFS 프로토콜의 기능 범위를 이해하고자 합니다.
- 기본 NFS 구성이 아닌, 덜 일반적인 구성 및 유지보수 작업을 수행하려는 경우
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

NAS 파일 액세스 이해

네임스페이스 및 교차점

ONTAP NAS 네임스페이스 및 연결 지점에 대해 알아보세요

nas_namespace_는 단일 파일 시스템 계층을 생성하기 위해 _junction points_에 함께 결합된 볼륨의 논리적 그룹입니다. 권한이 충분한 클라이언트는 저장소에 있는 파일의 위치를 지정하지 않고 네임스페이스의 파일에 액세스할 수 있습니다. Junced 볼륨은 클러스터의 모든 위치에 상주할 수 있습니다.

관심 파일이 포함된 모든 볼륨을 마운트하는 대신 NAS 클라이언트는 nfs_export_를 마운트하거나 smb_share에

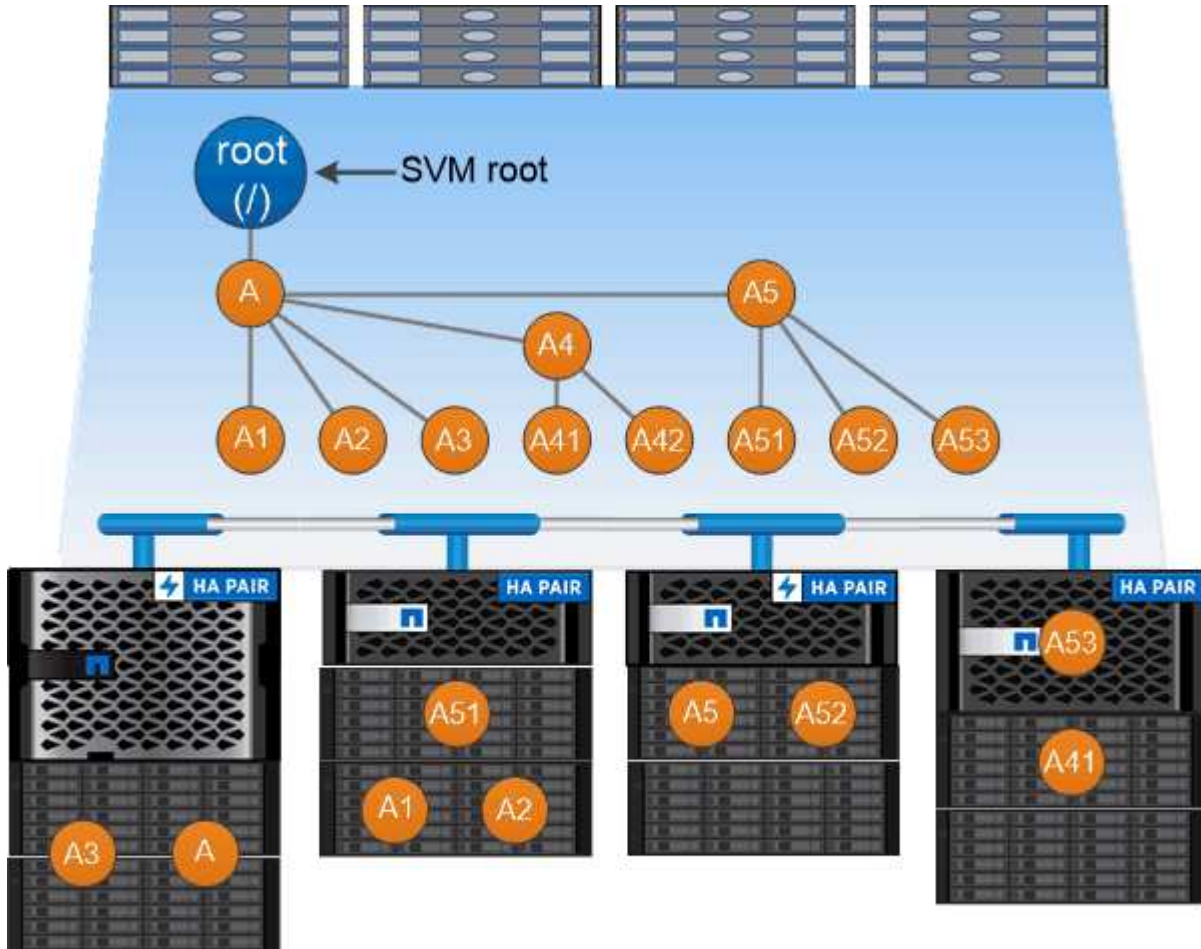
액세스합니다. _ 내보내기 또는 공유는 전체 네임스페이스 또는 네임스페이스 내의 중간 위치를 나타냅니다. 클라이언트는 해당 액세스 지점 아래에 마운트된 볼륨만 액세스합니다.

필요에 따라 네임스페이스에 볼륨을 추가할 수 있습니다. 상위 볼륨 접합 바로 아래 또는 볼륨 내의 디렉토리에 접합 지점을 생성할 수 있습니다. "vol3"이라는 이름의 볼륨에 대한 볼륨 접합부의 경로는 "/vol1/vol2/vol3" 또는 "/vol1/dir2/vol3" 또는 "/dir1/dir2/vol3"일 수 있습니다. 이 경로를 _junction path _라고 합니다

모든 SVM에는 고유한 네임스페이스가 있습니다. SVM 루트 볼륨은 네임스페이스 계층 구조의 진입점입니다.



노드 운영 중단 또는 파일오버 발생 시에도 데이터가 계속 사용 가능하도록 하려면 SVM 루트 볼륨에 대해 _load-sharing mirror_copy를 생성해야 합니다.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

예

다음 예에서는 junction path "/eng/home"이 있는 SVM VS1 상에 ""home4""라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

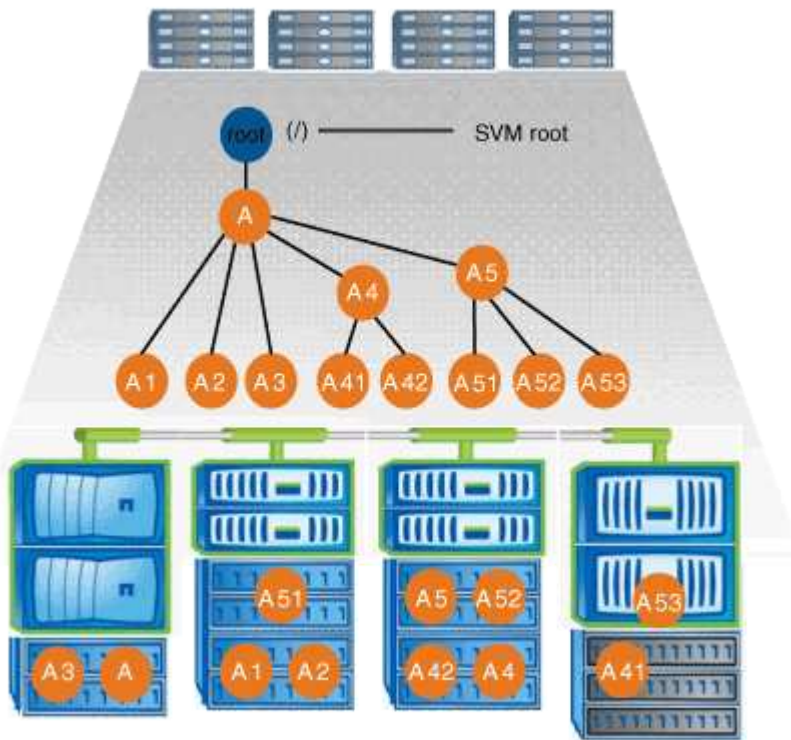
SVM 이름 공간을 생성할 때 사용할 수 있는 몇 가지 일반적인 NAS 네임스페이스 아키텍처가 있습니다. 비즈니스 및 워크플로우 요구사항에 맞는 네임스페이스 아키텍처를 선택할 수 있습니다.

네임스페이스 맨 위에는 항상 루트 볼륨이 있으며, 이 볼륨은 슬래시(/)로 표시됩니다. 루트 아래의 네임스페이스 아키텍처는 세 가지 기본 범주로 분류됩니다.

- 네임스페이스 루트에 대한 단일 분기만 있는 단일 분기 트리
- 여러 개의 분기된 나무는 여러 교차점이 네임스페이스의 루트를 가리킵니다
- 각각 별도의 연결 지점이 있는 여러 독립형 볼륨이 이름 공간의 루트를 가리킵니다

단일 분기 트리가 있는 네임스페이스입니다

단일 분기 트리가 있는 아키텍처는 SVM 네임스페이스의 루트에 대한 단일 삽입 지점을 갖습니다. 단일 삽입 지점은 접합된 볼륨이거나 루트 아래의 디렉토리일 수 있습니다. 다른 모든 볼륨은 단일 삽입 지점(볼륨 또는 디렉토리 가능) 아래의 접합 지점에 마운트됩니다.

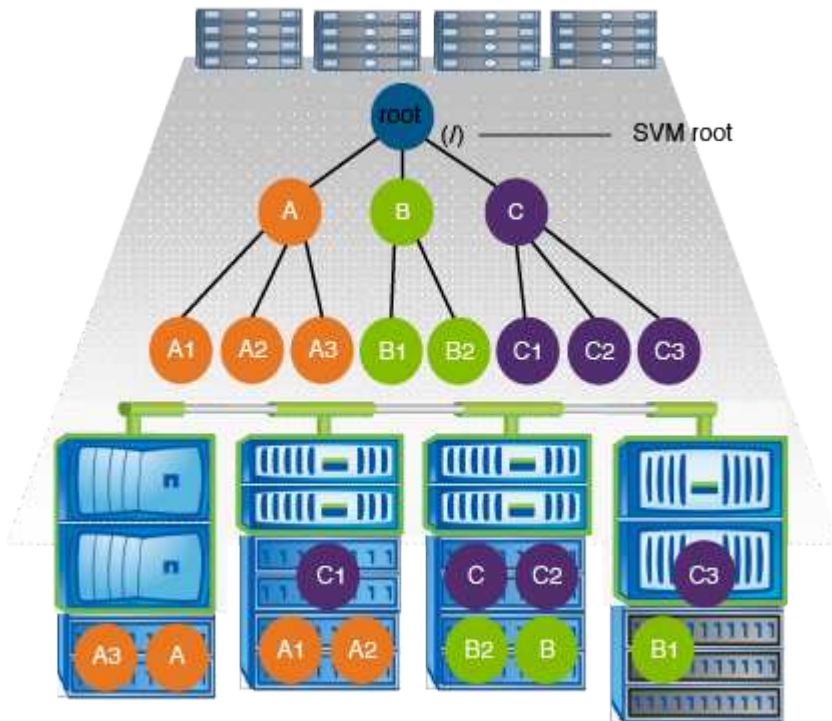


예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 연결 구성은 "데이터"라는 디렉토리인 단일 삽입 지점 아래에 모든 볼륨이 접합되는 다음과 같은 구성으로 보일 수 있습니다.

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	corp1	true	/data/dir1/corp1	RW_volume
vs1	corp2	true	/data/dir1/corp2	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	eng1	true	/data/data1/eng1	RW_volume
vs1	eng2	true	/data/data1/eng2	RW_volume
vs1	sales	true	/data/data1/sales	RW_volume
vs1	vol1	true	/data/vol1	RW_volume
vs1	vol2	true	/data/vol2	RW_volume
vs1	vol3	true	/data/vol3	RW_volume
vs1	vs1_root	-	/	-

여러 개의 분기 트리가 있는 네임스페이스입니다

여러 개의 분기 트리가 있는 아키텍처에는 SVM 네임스페이스의 루트에 대한 여러 삽입 지점이 있습니다. 삽입 지점은 루트 아래의 분기된 볼륨 또는 디렉토리일 수 있습니다. 다른 모든 볼륨은 삽입 지점(볼륨 또는 디렉토리일 수 있음) 아래의 접합 지점에 마운트됩니다.

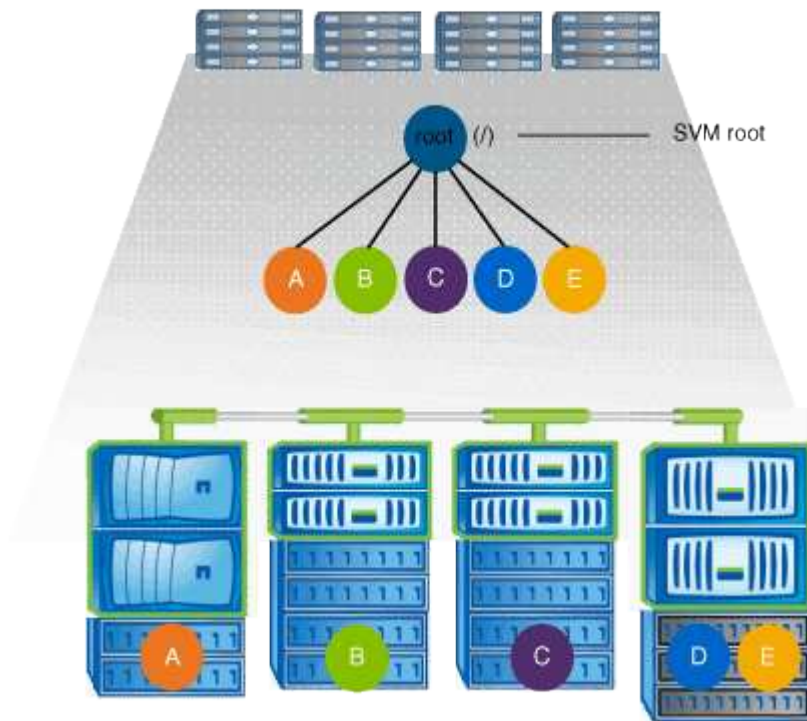


예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 접합 구성은 SVM의 루트 볼륨에 세 개의 삽입 지점이 있는 다음과 같은 구성을 예로 들 수 있습니다. 두 개의 삽입 지점은 "데이터"와 "프로젝트"라는 디렉토리입니다. 한 삽입 지점은 "audit"이라는 이름의 접합부입니다.

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	audit	true	/audit	RW_volume
vs1	audit_logs1	true	/audit/logs1	RW_volume
vs1	audit_logs2	true	/audit/logs2	RW_volume
vs1	audit_logs3	true	/audit/logs3	RW_volume
vs1	eng	true	/data/eng	RW_volume
vs1	mktg1	true	/data/mktg1	RW_volume
vs1	mktg2	true	/data/mktg2	RW_volume
vs1	project1	true	/projects/project1	RW_volume
vs1	project2	true	/projects/project2	RW_volume
vs1	vs1_root	-	/	-

여러 개의 독립 실행형 볼륨이 있는 네임스페이스

독립 실행형 볼륨이 있는 아키텍처에서 모든 볼륨은 SVM 네임스페이스의 루트에 대한 삽입 지점을 갖습니다. 하지만 볼륨이 다른 볼륨 아래에 접합되지 않습니다. 각 볼륨은 고유한 경로를 가지고 있으며, 루트 바로 아래에 접합되거나 루트 아래의 디렉토리 아래에 접합됩니다.



예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 접합 구성은 다음 구성과 비슷합니다. 여기서 SVM의 루트 볼륨에 5개의 삽입 지점을 두고 각 삽입 지점을 단일 볼륨의 경로를 나타냅니다.

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Active			
vs1	eng	true	/eng		RW_volume
vs1	mktg	true	/vol/mktg		RW_volume
vs1	project1	true	/project1		RW_volume
vs1	project2	true	/project2		RW_volume
vs1	sales	true	/sales		RW_volume
vs1	vs1_root	-	/		-

ONTAP에서 파일 액세스를 제어하는 방법

ONTAP NAS 파일 액세스 제어에 대해 알아보세요

ONTAP는 사용자가 지정하는 인증 기반 및 파일 기반 제한 사항에 따라 파일에 대한 액세스를 제어합니다.

클라이언트가 스토리지 시스템에 접속하여 파일을 액세스하는 경우 ONTAP는 다음 두 가지 작업을 수행해야 합니다.

- 인증

ONTAP는 신뢰할 수 있는 소스로 ID를 확인하여 클라이언트를 인증해야 합니다. 또한 클라이언트의 인증 유형은 클라이언트가 내보내기 정책을 구성할 때 데이터에 액세스할 수 있는지 여부를 결정하는 데 사용할 수 있는 방법 중 하나입니다(CIFS의 경우 선택 사항).

- 권한 부여

ONTAP는 사용자의 자격 증명을 파일 또는 디렉터리에 구성된 권한과 비교하고 제공할 액세스 유형(있는 경우)을 확인하여 사용자를 승인해야 합니다.

파일 액세스 제어를 제대로 관리하려면 ONTAP가 NIS, LDAP 및 Active Directory 서버와 같은 외부 서비스와 통신해야 합니다. CIFS 또는 NFS를 사용하여 파일 액세스를 위한 스토리지 시스템을 구성하려면 ONTAP의 환경에 따라 적절한 서비스를 설정해야 합니다.

ONTAP NAS SVM에 대한 인증 기반 제한 사항에 대해 알아보세요.

인증 기반 제한 사항을 사용하여 SVM(스토리지 가상 머신)에 연결할 수 있는 클라이언트 시스템과 사용자를 지정할 수 있습니다.

ONTAP는 UNIX 서버와 Windows 서버 모두에서 Kerberos 인증을 지원합니다.

ONTAP NAS SVM에 대한 파일 기반 제한 사항에 대해 알아보세요.

ONTAP은 세 가지 보안 수준을 평가하여 엔티티가 SVM에 있는 파일 및 디렉토리에 대해 요청된 작업을 수행할 수 있는 권한이 있는지 확인합니다. 액세스는 세 가지 보안 수준을 평가한 후 유효한 권한에 의해 결정됩니다.

모든 스토리지 객체에는 최대 3가지 유형의 보안 계층이 포함될 수 있습니다.

- 내보내기(NFS) 및 공유(SMB) 보안

내보내기 및 공유 보안은 지정된 NFS 내보내기 또는 SMB 공유에 대한 클라이언트 액세스에 적용됩니다. 관리 권한이 있는 사용자는 SMB 및 NFS 클라이언트의 내보내기 및 공유 수준 보안을 관리할 수 있습니다.

- 스토리지 레벨 Access Guard 파일 및 디렉토리 보안

스토리지 레벨 액세스 가드 보안은 SMB 및 NFS 클라이언트가 SVM 볼륨에 액세스하는 데 적용됩니다. NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에게 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.



NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다. 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 액세스 가드 보안을 취소할 수 없습니다.

- NTFS, UNIX 및 NFSv4 네이티브 파일 레벨 보안

네이티브 파일 레벨 보안은 스토리지 객체를 나타내는 파일 또는 디렉토리에 존재합니다. 클라이언트에서 파일 수준 보안을 설정할 수 있습니다. 파일 권한은 SMB 또는 NFS를 사용하여 데이터를 액세스하든 관계없이 유효합니다.

ONTAP가 NFS 클라이언트 인증을 처리하는 방식

NAS 클라이언트에 대한 **ONTAP** 인증에 대해 알아보세요

NFS 클라이언트가 SVM에서 데이터에 액세스하려면 먼저 제대로 인증되어야 합니다. ONTAP는 UNIX 자격 증명을 구성하는 이름 서비스와 비교하여 클라이언트를 인증합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP는 SVM의 이름 서비스 구성에 따라 다른 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. ONTAP는 로컬 UNIX 계정, NIS 도메인 및 LDAP 도메인에 대한 자격 증명을 확인할 수 있습니다. ONTAP가 사용자를 성공적으로 인증할 수 있도록 하나 이상의 사용자를 구성해야 합니다. 여러 개의 이름 서비스와 ONTAP가 서비스를 검색하는 순서를 지정할 수 있습니다.

UNIX 볼륨 보안 스타일을 사용하는 순수 NFS 환경에서는 이 구성으로 NFS 클라이언트에서 접속하는 사용자에게 대해 적절한 파일 액세스를 인증하고 제공할 수 있습니다.

혼합, NTFS 또는 통합 볼륨 보안 스타일을 사용하는 경우 ONTAP는 Windows 도메인 컨트롤러에서 인증을 위해 UNIX 사용자의 SMB 사용자 이름을 얻어야 합니다. 이 문제는 로컬 UNIX 계정이나 LDAP 도메인을 사용하여 개별 사용자를 매핑하거나 기본 SMB 사용자를 대신 사용하여 발생할 수 있습니다. ONTAP에서 검색할 이름 서비스를 순서대로 지정하거나 기본 SMB 사용자를 지정할 수 있습니다.

ONTAP이 이름 서비스를 사용하는 방법을 알아보세요

ONTAP는 이름 서비스를 사용하여 사용자 및 클라이언트에 대한 정보를 얻습니다. ONTAP는 이 정보를 사용하여 스토리지 시스템의 데이터에 액세스하거나 데이터를 관리하는 사용자를 인증하고 혼합 환경에서 사용자 자격 증명을 매핑합니다.

스토리지 시스템을 구성할 때 ONTAP에서 인증에 사용할 사용자 자격 증명을 얻기 위해 사용할 이름 서비스를 지정해야 합니다. ONTAP는 다음과 같은 이름 서비스를 지원합니다.

- 로컬 사용자(파일)

- 외부 NIS 도메인(NIS)
- 외부 LDAP 도메인(LDAP)

'vserver services name-service ns-switch' 명령 제품군을 사용하여 소스로 SVM을 구성하여 네트워크 정보 및 검색 순서를 검색할 수 있습니다. 이러한 명령은 UNIX 시스템에서 '/etc/nsswitch.conf' 파일과 동일한 기능을 제공합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP은 지정된 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. 이름 서비스가 올바르게 구성되어 있고 ONTAP에서 UNIX 자격 증명을 얻을 수 있는 경우 ONTAP는 사용자를 성공적으로 인증합니다.

보안 스타일이 혼합된 환경에서는 ONTAP가 사용자 자격 증명을 매핑해야 할 수 있습니다. ONTAP가 사용자 자격 증명을 적절하게 매핑할 수 있도록 사용자 환경에 맞게 이름 서비스를 구성해야 합니다.

ONTAP에서는 SVM 관리자 계정을 인증하는 데에도 이름 서비스를 사용합니다. 이름 서비스 스위치를 구성하거나 수정할 때 실수로 SVM 관리자 계정에 대한 인증을 비활성화하지 않도록 주의해야 합니다. SVM 관리 사용자에 대한 자세한 내용은 [참조하십시오 "관리자 인증 및 RBAC"](#).

NFS 클라이언트에서 ONTAP SMB 파일 액세스 권한 부여

ONTAP는 Windows NT 파일 시스템(NTFS) 보안 의미를 사용하여 NFS 클라이언트의 UNIX 사용자가 NTFS 권한이 있는 파일에 액세스할 수 있는지 여부를 결정합니다.

ONTAP는 사용자의 UNIX UID(사용자 ID)를 SMB 자격 증명으로 변환한 다음 SMB 자격 증명을 사용하여 사용자에게 파일에 대한 액세스 권한이 있는지 확인합니다. SMB 자격 증명은 일반적으로 사용자의 Windows 사용자 이름인 기본 SID(보안 식별자)와 사용자가 구성원인 Windows 그룹에 해당하는 하나 이상의 그룹 SID로 구성됩니다.

프로세스가 도메인 컨트롤러에 접속하기 때문에 ONTAP가 UNIX UID를 SMB 자격 증명으로 변환하는 데 걸리는 시간은 수십 밀리초에서 수백 밀리초로 지정할 수 있습니다. ONTAP는 UID를 SMB 자격 증명에 매핑하고 자격 증명 캐시에 매핑을 입력하여 변환으로 인한 검증 시간을 줄입니다.

ONTAP NFS 자격 증명 캐시 작동 방식

NFS 사용자가 스토리지 시스템의 NFS 내보내기에 대한 액세스를 요청할 경우 ONTAP는 외부 이름 서버 또는 로컬 파일에서 사용자 자격 증명을 검색하여 사용자를 인증해야 합니다. 그런 다음 ONTAP는 나중에 참조할 수 있도록 이러한 자격 증명을 내부 자격 증명 캐시에 저장합니다. NFS 자격 증명 캐시의 작동 방식을 이해하면 잠재적인 성능 및 액세스 문제를 처리할 수 있습니다.

자격 증명 캐시가 없으면 ONTAP는 NFS 사용자가 액세스를 요청할 때마다 이름 서비스를 쿼리해야 합니다. 사용량이 많은 스토리지 시스템에서 많은 사용자가 액세스하는 경우 심각한 성능 문제가 신속하게 발생하여 원치 않는 지연이 발생하거나 NFS 클라이언트 액세스가 거부 될 수 있습니다.

ONTAP는 자격 증명 캐시를 사용하여 사용자 자격 증명을 검색한 다음 NFS 클라이언트가 다른 요청을 보낼 때 빠르고 쉽게 액세스할 수 있도록 미리 결정된 시간 동안 저장합니다. 이 방법은 다음과 같은 이점을 제공합니다.

- NIS 또는 LDAP와 같은 외부 이름 서버에 대한 요청 수를 줄여 스토리지 시스템의 로드를 간소화합니다.
- 외부 네임 서버에 대한 요청 수를 줄여 부하를 덜어줍니다.
- 외부 소스에서 자격 증명을 얻기 위한 대기 시간을 없애 사용자 액세스 속도를 높입니다.

ONTAP는 자격 증명 캐시에 양의 자격 증명과 음의 자격 증명을 모두 저장합니다. 양의 자격 증명은 사용자가 인증되고

액세스 권한이 부여되었음을 의미합니다. 음수 자격 증명은 사용자가 인증되지 않고 액세스가 거부되었음을 의미합니다.

기본적으로 ONTAP은 24시간 동안 양의 자격 증명을 저장합니다. 즉, 처음에 사용자를 인증한 후 ONTAP는 해당 사용자의 액세스 요청에 대해 24시간 동안 캐시된 자격 증명을 사용합니다. 사용자가 24시간 후에 액세스를 요청하면 주기가 다시 시작됩니다. ONTAP는 캐시된 자격 증명을 삭제하고 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 24시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 24시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

기본적으로 ONTAP는 2시간 동안 부정 자격 증명을 저장합니다. 즉, 처음에 사용자에 대한 액세스를 거부하면 ONTAP는 해당 사용자의 액세스 요청을 2시간 동안 계속 거부합니다. 사용자가 2시간 후에 액세스를 요청하는 경우 주기가 다시 시작됩니다. ONTAP는 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 2시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 2시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다

지정된 연결 지점으로 **ONTAP NAS** 볼륨 생성

데이터 볼륨을 생성할 때 교차점을 지정할 수 있습니다. 결과 볼륨은 교차점에 자동으로 마운트되며 NAS 액세스를 위해 즉시 구성할 수 있습니다.

시작하기 전에

- 볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "[파일 시스템 분석 설정](#)". 에 대한 자세한 내용은 `volume create` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.



다음 문자는 접합 경로에서 사용할 수 없습니다. * # " > < | ? \

또한 접합 경로 길이는 255자를 초과할 수 없습니다.

단계

1. 교차점으로 볼륨을 생성합니다.

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

접합 경로는 루트(/)로 시작해야 하며 디렉터리와 접합된 볼륨을 모두 포함할 수 있습니다. 접합 경로에는 볼륨의 이름을 포함할 필요가 없습니다. 접합 경로는 볼륨 이름과 무관합니다.

볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 만드는 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

교차경로는 대/소문자를 구분하지 않고 /eng은 /eng과 같습니다. CIFS 공유를 생성하는 경우 Windows는 연결 경로를 대/소문자를 구분하는 것처럼 처리합니다. 예를 들어, 교차점이 /eng인 경우 SMB 공유의 경로는 /eng가 아니라 /eng로 시작해야 합니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

예

다음 예에서는 접합 경로가 있는 SVM VS1에 /eng/home 이라는 이름의 볼륨을 home4 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

		Junction		Junction	
Vserver	Volume	Active	Junction Path	Path	Source
vs1	home4	true	/eng/home	RW_volume	

특정 연결 지점 없이 ONTAP NAS 볼륨 생성

교차점을 지정하지 않고 데이터 볼륨을 생성할 수 있습니다. 결과 볼륨은 자동으로 마운트되지 않으며 NAS 액세스에 대해 구성할 수 없습니다. 해당 볼륨에 대해 SMB 공유 또는 NFS 내보내기를 구성하려면 먼저 볼륨을 마운트해야 합니다.

시작하기 전에

- 볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 on 명령을 `-analytics-state` 실행합니다.

용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 다음 명령을 사용하여 교차점 없이 볼륨을 생성합니다.

```
'volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size{integer[KB|MB|GB|TB|PB]} - security-style{NTFS|UNIX|MIXED}'입니다
```

볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 [volume create "ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 볼륨이 교차점 없이 생성되었는지 확인합니다.

```
'volume show -vserver vs1 -volume volume_name -junction'
```

예

다음 예에서는 교차점에 마운트되지 않은 SVM VS1 상에 "sales"라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

NAS 네임스페이스에서 **ONTAP NFS** 볼륨을 마운트하거나 마운트 해제합니다.

SVM(스토리지 가상 시스템) 볼륨에 포함된 데이터에 대한 NAS 클라이언트 액세스를 구성하려면 먼저 NAS 네임스페이스에 볼륨을 마운트해야 합니다. 볼륨이 현재 마운트되지 않은 경우 볼륨을 연결 지점에 마운트할 수 있습니다. 볼륨을 마운트 해제할 수도 있습니다.

이 작업에 대해

볼륨을 마운트 해제하고 오프라인으로 전환하면 마운트 해제된 볼륨의 네임스페이스 내에 포함된 접합 지점의 볼륨 데이터를 비롯하여 연결 지점 내의 모든 데이터를 NAS 클라이언트에서 액세스할 수 없습니다.



볼륨에 대한 NAS 클라이언트 액세스를 중단하려면 볼륨을 마운트 해제하는 것만으로는 충분하지 않습니다. 볼륨을 오프라인으로 전환하거나 클라이언트 측 파일 핸들 캐시가 무효화되도록 다른 단계를 수행해야 합니다. 자세한 내용은 다음 기술 자료 문서를 참조하십시오.

["ONTAP의 네임스페이스에서 제거후에도 NFSv3 클라이언트가 볼륨에 계속 액세스할 수 있습니다"](#)

볼륨을 마운트 해제하고 오프라인으로 전환하면 볼륨 내의 데이터가 손실되지 않습니다. 또한 마운트 해제된 볼륨 내의 볼륨이나 디렉토리 및 연결 지점에 생성된 기존 볼륨 내보내기 정책 및 SMB 공유가 보존됩니다. 마운트 해제된 볼륨을 다시 마운트하면 NAS 클라이언트가 기존 익스포트 정책과 SMB 공유를 사용하여 볼륨 내에 포함된 데이터에 액세스할

수 있습니다.

단계

1. 원하는 작업을 수행합니다.

원하는 작업	명령 입력...
볼륨을 마운트합니다	'volume mount -vserver <i>svm_name</i> - volume <i>volume_name</i> -junction- path <i>junction_path</i> '
볼륨을 마운트 해제합니다	volume unmount -vserver <i>svm_name</i> -volume <i>volume_name</i> volume offline -vserver <i>svm_name</i> -volume <i>volume_name</i>

2. 볼륨이 원하는 마운트 상태에 있는지 확인합니다.

```
volume show -vserver svm_name -volume volume_name -fields state,junction-  
path,junction-active
```

예

다음 예에서는 SVM "VS1"에 있는 "판매"라는 볼륨을 접합 지점 ""/판매"에 마운트합니다.

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales  
  
cluster1::> volume show -vserver vs1 state,junction-path,junction-active  
  
vserver    volume    state    junction-path    junction-active  
-----  
vs1        data      online   /data            true  
vs1        home4     online   /eng/home        true  
vs1        sales     online   /sales           true
```

다음 예에서는 SVM "VS1"에 있는 "데이터"라는 이름의 볼륨을 마운트 해제하고 오프라인으로 전환합니다.

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

ONTAP NAS 볼륨 마운트 및 접합 지점 정보를 표시합니다

스토리지 가상 시스템(SVM)에 대해 마운트된 볼륨 및 볼륨이 마운트된 접합 지점에 대한 정보를 표시할 수 있습니다. 또한 어느 볼륨이 분기점에 마운트되지 않는지 확인할 수 있습니다. 이 정보를 사용하여 SVM 네임스페이스를 이해하고 관리할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

를 표시하려면...	명령 입력...
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 요약 정보	'volume show -vserver_vserver_name_-junction'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 자세한 정보	'volume show -vserver_vserver_name_-volume_volume_name_-instance'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 특정 정보	a. 필요한 경우 볼륨 표시 필드? 명령을 사용하여 '-fields' 매개 변수에 대한 유효한 필드를 표시할 수 있습니다 b. '-fields' 매개 변수 'volume show-vserver_vserver_name_-fields_fieldname_,...'를 사용하여 원하는 정보를 표시합니다

예

다음 예는 SVM VS1 에서 마운트 및 마운트 해제된 볼륨에 대한 요약을 표시합니다.

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

다음 예는 SVM VS2 에 있는 볼륨의 지정된 필드에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
```

vserver	volume	aggregate	size	state	type	security-style	junction-path	junction-parent	node
vs2	data1	aggr3	2GB	online	RW	unix	-	-	node3
vs2	data2	aggr3	1GB	online	RW	ntfs	/data2		
vs2	data2_1	aggr3	8GB	online	RW	ntfs	/data2/d2_1		
vs2	data2_2	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	pubs	aggr1	1GB	online	RW	unix	/publications		
vs2	images	aggr3	2TB	online	RW	ntfs	/images		
vs2	logs	aggr1	1GB	online	RW	unix	/logs		
vs2	vs2_root	aggr3	1GB	online	RW	ntfs	/	-	node3

보안 스타일을 구성합니다

보안 스타일이 데이터 액세스에 미치는 영향

ONTAP NAS 보안 스타일 알아보기

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 NFSv4.x ACL	Unix	NFS 및 SMB
NTFS입니다	중소기업	NTFS ACL	NTFS입니다	
혼합	NFS 또는 SMB	NFSv3 모드 비트 NFSv4.ACL	Unix	
		NTFS ACL	NTFS입니다	
통합(ONTAP 9.4 및 이전 릴리즈에서 무한 확장 볼륨에만 해당)	NFS 또는 SMB	NFSv3 모드 비트 NFSv4.1 ACL	Unix	
		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](#).

그만큼 `show-effective-permissions` 매개변수를 사용하여 `vserver security file-directory` 명령을 사용하면 지정된 파일이나 폴더 경로에 대해 Windows 또는 UNIX 사용자에게 부여된 유효 권한을 표시할 수 있습니다. 또한 선택적 매개 변수를 `-share-name` 사용하면 효과적인 공유 권한을 표시할 수 있습니다. 에 대한 자세한 내용은 `vserver security file-directory show-effective-permissions` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.



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.

관련 정보

- ["ONTAP 명령 참조입니다"](#)

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.

ONTAP NAS SVM에서 사용할 보안 스타일을 결정하세요.

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. - 대부분의 사용자는 NFS 클라이언트입니다. - 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다.
NTFS입니다	- 파일 시스템은 Windows 관리자가 관리합니다. - 대부분의 사용자는 SMB 클라이언트입니다. - 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다.
혼합	파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다.

ONTAP NFS 보안 스타일 상속에 대해 알아보십시오

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.

ONTAP NFS UNIX 권한 보존에 대해 알아보세요

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 **ONTAP NFS SVM**에서 **UNIX** 권한 관리

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.

ONTAP NFS SVM 루트 볼륨에서 보안 스타일 구성

SVM(Storage Virtual Machine) 루트 볼륨 보안 스타일을 구성하여 SVM의 루트 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 보안 스타일을 정의하려면 '-rootvolume-security-style' 매개 변수와 함께 'vserver create' 명령을 사용하십시오.

루트 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합입니다.

2. 생성한 SVM의 루트 볼륨 보안 유형을 포함하여 구성을 표시하고 확인합니다.

```
'vserver show -vserver_vserver_name_'
```

ONTAP NFS FlexVol 볼륨에서 보안 스타일 구성

FlexVol 볼륨 보안 스타일을 구성하여 SVM(스토리지 가상 머신)의 FlexVol 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

FlexVol 볼륨이	명령 사용...
아직 없습니다	보안 스타일을 지정하기 위해 볼륨 생성 및 '-security-style' 매개 변수를 포함합니다.
이미 있습니다	볼륨 수정, -security-style 매개 변수를 포함해서 보안 스타일을 지정합니다.

FlexVol 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합입니다.

FlexVol 볼륨을 만들 때 보안 스타일을 지정하지 않으면 볼륨은 루트 볼륨의 보안 스타일을 상속합니다.

볼륨 생성 또는 볼륨 수정 명령에 대한 자세한 내용은 을 참조하십시오 ["논리적 스토리지 관리"](#).

2. 생성한 FlexVol 볼륨의 보안 스타일을 포함하여 구성을 표시하려면 다음 명령을 입력합니다.

```
'volume show-volume volume_name-instance'
```

ONTAP NFS qtree에서 보안 스타일 구성

Qtree 볼륨 보안 스타일을 구성하여 Qtree에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

qtree가...	명령 사용...
아직 없습니다	볼륨 qtree create를 수행하고 보안 스타일을 지정하는 -security-style 매개 변수를 포함합니다.
이미 있습니다	볼륨 qtree 수정과 보안 유형을 지정하는 -security-style 매개 변수를 포함합니다.

qtree 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS, 혼합입니다.

Qtree를 만들 때 보안 스타일을 지정하지 않으면 기본 보안 스타일이 '혼합'으로 설정됩니다.

'볼륨 qtree 생성' 또는 '볼륨 qtree 수정' 명령에 대한 자세한 내용은 을 참조하십시오 ["논리적 스토리지 관리"](#).

2. 생성한 qtree의 보안 스타일을 포함하여 구성을 표시하려면 'volume qtree show-qtree_qtree_name_-instance'

명령을 입력합니다

NFS를 사용하여 파일 액세스를 설정합니다

ONTAP SVM에서 **NFS** 파일 액세스 설정에 대해 알아보세요

고객이 NFS를 사용하여 SVM(스토리지 가상 시스템)의 파일에 액세스할 수 있도록 하려면 여러 단계를 완료해야 합니다. 환경의 현재 구성에 따라 몇 가지 추가 단계가 선택적으로 제공됩니다.

클라이언트가 NFS를 사용하여 SVM의 파일에 액세스할 수 있으려면 다음 작업을 완료해야 합니다.

1. SVM에서 NFS 프로토콜을 활성화합니다.

NFS를 통해 클라이언트에서 데이터에 액세스할 수 있도록 SVM을 구성해야 합니다.

2. SVM에서 NFS 서버를 생성합니다.

NFS 서버는 SVM에서 NFS를 통해 파일을 처리할 수 있는 논리적 엔티티입니다. NFS 서버를 생성하고 허용할 NFS 프로토콜 버전을 지정해야 합니다.

3. SVM에 익스포트 정책을 구성합니다.

클라이언트에서 볼륨 및 qtree를 사용할 수 있도록 익스포트 정책을 구성해야 합니다.

4. 네트워크 및 스토리지 환경에 따라 적절한 보안 및 기타 설정으로 NFS 서버를 구성합니다.

이 단계에는 Kerberos, LDAP, NIS, 이름 매핑 및 로컬 사용자 구성이 포함될 수 있습니다.

내보내기 정책을 사용하여 **NFS** 액세스를 보호합니다

내보내기 정책이 **ONTAP NFS** 볼륨 또는 **Qtree**에 대한 클라이언트 액세스를 제어하는 방법

익스포트 정책에는 각 클라이언트 액세스 요청을 처리하는 `_export rules_`이 하나 이상 포함되어 있습니다. 프로세스 결과에 따라 클라이언트가 거부되었는지, 액세스 권한이 부여되었는지, 액세스 수준이 결정됩니다. 클라이언트가 데이터에 액세스할 수 있도록 SVM(스토리지 가상 시스템)에 익스포트 규칙과 함께 익스포트 정책이 있어야 합니다.

볼륨 또는 qtree에 대한 클라이언트 액세스를 구성하기 위해 각 볼륨 또는 qtree에 정확히 하나의 익스포트 정책을 연결합니다. SVM에는 여러 익스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨 또는 qtree를 사용하는 SVM에 대해 다음을 수행할 수 있습니다.

- 개별 클라이언트 액세스 제어를 SVM의 각 볼륨 또는 qtree에 서로 다른 익스포트 정책을 지정하여 각 볼륨 또는 qtree에 대한 볼륨 또는 qtree를 관리할 수 있습니다.
- 각 볼륨 또는 qtree에 대해 새로운 익스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨 또는 qtree에 동일한 익스포트 정책을 할당합니다.

클라이언트가 해당 익스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우 권한 거부 메시지와 함께 요청이 실패합니다. 클라이언트가 익스포트 정책의 규칙과 일치하지 않으면 액세스가 거부됩니다. 내보내기 정책이 비어 있으면 모든 액세스가 암시적으로 거부됩니다.

ONTAP를 실행하는 시스템에서 익스포트 정책을 동적으로 수정할 수 있습니다.

ONTAP NFS SVM에 대한 기본 내보내기 정책

각 SVM에는 규칙이 없는 기본 익스포트 정책이 있습니다. 클라이언트가 SVM에서 데이터에 액세스하려면 먼저 규칙과 함께 익스포트 정책이 있어야 합니다. SVM에 포함된 각 FlexVol 볼륨은 익스포트 정책과 연결되어야 합니다.

SVM을 생성할 때 스토리지 시스템은 SVM의 루트 볼륨에 대한 기본 익스포트 정책인 'Default'를 자동으로 생성합니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 익스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다. 또는 규칙을 사용하여 사용자 지정 익스포트 정책을 생성할 수도 있습니다. 기본 익스포트 정책을 수정 및 변경할 수 있지만, 기본 익스포트 정책은 삭제할 수 없습니다.

SVM이 포함된 FlexVol 볼륨에서 스토리지 시스템은 볼륨을 생성한 후 SVM의 루트 볼륨에 대한 기본 익스포트 정책과 연결합니다. 기본적으로 SVM에서 생성된 각 볼륨은 루트 볼륨의 기본 익스포트 정책과 연결됩니다. SVM에 포함된 모든 볼륨에 기본 익스포트 정책을 사용하거나, 각 볼륨에 대해 고유한 익스포트 정책을 생성할 수 있습니다. 여러 볼륨을 동일한 익스포트 정책에 연결할 수 있습니다.

ONTAP NFS 내보내기 규칙 작동 방식

내보내기 규칙은 익스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을 처리하는 방법을 결정하기 위해 구성된 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청을 일치시킵니다.

클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 익스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 익스포트 정책에 표시되는 순서대로 처리됩니다. 규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 권한이 사용되며 추가 규칙은 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

다음 조건을 사용하여 내보내기 규칙을 구성하여 클라이언트 액세스 권한을 결정할 수 있습니다.

- NFSv4 또는 SMB와 같이 요청을 보내는 클라이언트에서 사용하는 파일 액세스 프로토콜입니다.
 - 호스트 이름 또는 IP 주소와 같은 클라이언트 식별자입니다.
- '-clientmatch' 필드의 최대 크기는 4096자입니다.
- Kerberos v5, NTLM 또는 AUTH_SYS와 같이 클라이언트에서 인증하는 데 사용되는 보안 유형입니다.

규칙이 여러 조건을 지정하는 경우 클라이언트는 규칙을 적용하기 위해 모든 조건을 충족해야 합니다.



ONTAP 9.3부터 오류 규칙 목록에 규칙 위반을 기록하는 백그라운드 작업으로 내보내기 정책 구성 검사를 활성화할 수 있습니다. 'vserver export-policy config-checker' 명령은 checker를 호출하고 결과를 표시하며, 이 명령을 사용하여 구성을 확인하고 정책에서 잘못된 규칙을 삭제할 수 있습니다.

명령은 호스트 이름, 넷그룹 및 익명 사용자에 대한 내보내기 구성만 검증합니다.

예

익스포트 정책에는 다음 매개 변수가 있는 익스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3

- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv3 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.17.37입니다.

클라이언트 액세스 프로토콜이 일치하더라도 클라이언트의 IP 주소는 내보내기 규칙에 지정된 IP 주소와 다른 서브넷에 있습니다. 따라서 클라이언트 일치가 실패하고 이 규칙은 이 클라이언트에 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv4 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.16.54입니다.

클라이언트 액세스 프로토콜이 일치하고 클라이언트의 IP 주소가 지정된 서브넷에 있습니다. 따라서 클라이언트 일치가 성공하고 이 규칙이 이 클라이언트에 적용됩니다. 클라이언트는 보안 유형에 관계없이 읽기-쓰기 액세스를 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 따라서 두 클라이언트 모두 읽기 전용 액세스 권한이 부여됩니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

나열되지 않은 보안 유형을 사용하는 **NFS** 클라이언트에 대한 **ONTAP SVM** 액세스 관리

클라이언트가 엑스포트 규칙의 액세스 매개 변수에 나열되지 않은 보안 유형을 자체적으로 표시할 경우, 액세스 매개 변수에서 "없음" 옵션을 사용하는 대신 클라이언트에 대한 액세스를 거부하거나 익명 사용자 ID에 매핑할 수 있습니다.

클라이언트는 다른 보안 유형으로 인증되었거나 전혀 인증되지 않았기 때문에 액세스 매개 변수에 나열되지 않은 보안

형식(security type AUTH_none)으로 자신을 나타낼 수 있습니다. 기본적으로 클라이언트는 해당 수준에 대한 액세스가 자동으로 거부됩니다. 그러나, 액세스 파라미터에 'none' 옵션을 추가할 수 있습니다. 따라서 목록에 없는 보안 스타일이 있는 클라이언트는 대신 익명 사용자 ID에 매핑됩니다. '-anon' 매개 변수는 해당 클라이언트에 할당되는 사용자 ID를 결정합니다. '-anon' 매개 변수에 지정된 사용자 ID는 익명 사용자에게 적합한 권한으로 구성된 유효한 사용자여야 합니다.

'-anon' 파라미터의 유효 값은 0부터 65535까지입니다.

'-anon'에 할당된 사용자 ID입니다	이로 인해 클라이언트 액세스 요청이 처리되었습니다
0-65533	클라이언트 액세스 요청은 익명 사용자 ID에 매핑되며 이 사용자에게 대해 구성된 권한에 따라 액세스를 가져옵니다.
65534	클라이언트 액세스 요청이 nobody 사용자에게 매핑되고 이 사용자에게 대해 구성된 권한에 따라 액세스 권한이 부여됩니다. 이것이 기본값입니다.
65,535입니다	이 ID에 매핑되면 클라이언트의 액세스 요청이 거부되고 클라이언트는 보안 유형 AUTH_NONE으로 표시됩니다. 사용자 ID가 0인 클라이언트의 액세스 요청은 이 ID에 매핑될 때 거부되며 클라이언트는 다른 보안 유형을 제공합니다.

none 옵션을 사용할 때는 읽기 전용 매개변수가 먼저 처리된다는 점을 기억해야 합니다. 목록에 없는 보안 유형의 클라이언트에 대한 내보내기 규칙을 구성할 때 다음 지침을 고려하십시오.

읽기 전용에는 없음 이 포함됩니다	읽기-쓰기에는 없음도 있습니다	목록에 없는 보안 유형의 클라이언트에 대한 액세스
아니요	아니요	거부됨
아니요	예	읽기 전용이 먼저 처리되므로 거부됩니다
예	아니요	익명 읽기 전용
예	예	익명으로서 읽기-쓰기

예

다음 예에서는 다음을 포함하는 내보내기 정책을 보여줍니다. -rwrule any 매개변수:

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0"
- "어이, 없습니다.
- '어다나'

- -아노온 70세

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, NFSv3 프로토콜을 사용하여 액세스 요청을 전송하며, 인증되지 않았습니다(보안 유형 AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수는 AUTH_SYS로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기 전용 매개 변수는 다른 보안 유형을 사용하여 인증된 클라이언트에 사용자 ID 70을 가진 익명 사용자로 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 모든 보안 유형에 대해 읽기-쓰기 액세스를 허용하지만 이 경우에는 읽기 전용 규칙에 의해 이미 필터링된 클라이언트에만 적용됩니다.

따라서 클라이언트 #1과 #3은 사용자 ID가 70인 익명 사용자로만 읽기-쓰기 권한을 받습니다. 클라이언트 #2는 고유한 사용자 ID를 사용하여 읽기-쓰기 권한을 받습니다.

다음 예에서는 다음을 포함하는 내보내기 정책을 보여줍니다. -rwrule none 매개변수:

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- "어이, 없습니다.
- '-rwrule' none
- -아노온 70세

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, NFSv3 프로토콜을 사용하여 액세스 요청을 전송하며, 인증되지 않았습니다(보안 유형 AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수는 AUTH_SYS로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기 전용 매개 변수는 다른 보안 유형을 사용하여 인증된 클라이언트에 사용자 ID 70을 가진 익명 사용자로 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 익명 사용자로만 읽기-쓰기 액세스를 허용합니다.

따라서 클라이언트 #1과 클라이언트 #3은 사용자 ID가 70인 익명 사용자로만 읽기-쓰기 권한을 받습니다. 클라이언트 #2는 자체 사용자 ID를 사용하여 읽기 전용 액세스를 얻지만 읽기-쓰기 액세스는 거부됩니다.

ONTAP 보안 유형이 **NFS** 클라이언트 액세스 수준을 결정하는 방식

클라이언트가 에서 인증한 보안 유형은 내보내기 규칙에서 특별한 역할을 합니다. 보안 유형에 따라 클라이언트가 볼륨 또는 qtree에 액세스하는 액세스 수준이 어떻게 결정되는지 이해해야

합니다.

세 가지 액세스 수준은 다음과 같습니다.

1. 읽기 전용
2. 읽기-쓰기
3. 슈퍼유저(사용자 ID가 0인 클라이언트의 경우)

보안 유형별 액세스 수준은 이 순서대로 평가되므로 내보내기 규칙에서 액세스 수준 매개 변수를 구성할 때 다음 규칙을 준수해야 합니다.

클라이언트가 액세스 레벨을 얻는 경우...	이러한 액세스 매개 변수는 클라이언트의 보안 유형과 일치해야 합니다.
일반 사용자 읽기 전용	읽기 전용('rorule')
일반 사용자 읽기-쓰기	읽기 전용('rorule') 및 읽기/쓰기('rwrule')
고급 사용자 읽기 전용	읽기 전용('rorule') 및 '-superuser'
고급 사용자 읽기-쓰기	읽기 전용('rorule') 및 읽기/쓰기('rwrule') 및 '-superuser'

다음은 이러한 세 가지 액세스 매개 변수 각각에 대해 유효한 보안 유형입니다.

- 모두
- "없음"
- "안 돼."

이 보안 유형은 '-superuser' 매개변수와 함께 사용할 수 없습니다.

- krb5
- krb5i
- 크르b5p
- NTLM
- '스'입니다

클라이언트의 보안 유형을 세 가지 액세스 매개 변수 각각에 일치시킬 경우 다음과 같은 세 가지 결과가 발생할 수 있습니다.

클라이언트의 보안 유형인 경우...	그러면 고객은...
access 매개 변수에 지정된 것과 일치합니다.	해당 사용자 ID를 사용하여 해당 수준에 대한 액세스를 가져옵니다.

클라이언트의 보안 유형인 경우...	그러면 고객은...
지정된 옵션과 일치하지 않지만 액세스 매개 변수에는 '없음' 옵션이 포함됩니다.	'-anon' 매개 변수로 지정한 사용자 ID를 가진 익명 사용자로 해당 수준에 대한 액세스를 가져옵니다.
지정된 옵션과 일치하지 않으며 액세스 매개 변수에 '없음' 옵션이 포함되어 있지 않습니다.	이 수준은 지정되지 않은 경우에도 항상 '없음'을 포함하므로 '-superuser' 매개 변수에는 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0"
- 모든 것
- '-rwrule"s, krb5'
- 슈퍼유저 krb5

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID가 0이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, Kerberos v5로 인증되었습니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, 사용자 ID 0이 있으며, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, 인증하지 않았습니다(AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두와 일치합니다. 읽기 전용 매개 변수는 보안 유형에 관계없이 모든 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 AUTH_SYS 또는 Kerberos v5로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기-쓰기 액세스를 허용합니다. 슈퍼유저 매개 변수를 사용하면 Kerberos v5로 인증된 사용자 ID 0을 가진 클라이언트에 슈퍼유저 액세스가 가능합니다.

따라서 클라이언트 #1은 세 가지 액세스 매개 변수와 모두 일치하기 때문에 슈퍼유저 읽기-쓰기 액세스 권한을 얻습니다. 클라이언트 #2에 읽기-쓰기 액세스 권한이 있지만 고급 사용자 액세스 권한이 없습니다. 클라이언트 #3은 읽기 전용 액세스 권한을 얻지만 고급 사용자 액세스는 받지 않습니다.

ONTAP NFS 슈퍼유저 액세스 요청 관리에 대해 알아보세요

엑스포트 정책을 구성할 때는 스토리지 시스템이 사용자 ID 0의 클라이언트 액세스 요청을 받으면 수행할 작업을 고려해야 합니다. 즉, 고급 사용자로서 엑스포트 규칙을 설정해야 합니다.

UNIX 환경에서 사용자 ID 0을 가진 사용자는 일반적으로 시스템에 대한 무제한 액세스 권한이 있는 슈퍼유저라고 합니다. 고급 사용자 권한을 사용하는 것은 시스템 위반 및 데이터 보안을 비롯한 여러 가지 이유로 위험할 수 있습니다.

기본적으로 ONTAP는 사용자 ID 0을 사용하는 클라이언트를 익명 사용자에게 매핑합니다. 그러나 내보내기 규칙에서 '-superuser' 매개 변수를 지정하여 보안 유형에 따라 사용자 ID 0으로 나타나는 클라이언트를 처리하는 방법을 결정할 수 있습니다. 다음은 '-superuser' 파라미터에 대한 유효한 옵션입니다.

- 모두

- "없음"

이 설정은 '-superuser' 파라미터를 지정하지 않을 경우 기본 설정입니다.

- krb5
- NTLM
- '스'입니다

'-superuser' 매개 변수 구성에 따라 사용자 ID 0으로 표시하는 클라이언트가 처리되는 방법에는 두 가지가 있습니다.

'-superuser' 매개변수와 클라이언트의 보안 유형이...	그러면 고객은...
일치	사용자 ID 0을 사용하여 슈퍼유저 액세스 권한을 가져옵니다.
일치하지 않습니다	'-anon' 매개 변수에 지정된 사용자 ID와 할당된 사용 권한을 가진 익명 사용자로 액세스를 가져옵니다. 이는 읽기 전용 또는 읽기/쓰기 매개 변수가 '없음' 옵션을 지정하는지 여부에 관계없이 적용됩니다.

클라이언트가 NTFS 보안 스타일로 볼륨에 액세스하기 위해 사용자 ID 0을 제공하고 '-superuser' 매개 변수가 'none'으로 설정된 경우 ONTAP는 익명 사용자의 이름 매핑을 사용하여 적절한 자격 증명을 얻습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0"
- 모든 것
- '-rwrule' krb5, NTLM
- '-anon"127

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID 746을 가지고 있으며, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5를 사용하여 인증합니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다.

클라이언트 #2에서 슈퍼유저 액세스 권한을 얻을 수 없습니다. 대신 '-superuser' 매개 변수가 지정되지 않아 익명으로 매핑됩니다. 즉, 기본적으로 '없음'으로 설정되어 있으며 사용자 ID 0을 익명으로 자동 매핑합니다. 또한 보안 형식이 읽기-쓰기 매개 변수와 일치하지 않기 때문에 클라이언트 #2는 읽기 전용 액세스만 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM
- 슈퍼유저 krb5
- 0

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID가 0이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, Kerberos v5로 인증되었습니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

내보내기 규칙은 사용자 ID가 0인 클라이언트에 대한 슈퍼유저 액세스를 허용합니다. 클라이언트 #1은 읽기 전용 및 '-superuser' 매개 변수의 사용자 ID와 보안 유형과 일치하기 때문에 슈퍼유저 액세스 권한을 얻습니다. 보안 유형이 읽기-쓰기 매개 변수나 '-superuser' 매개 변수와 일치하지 않기 때문에 클라이언트 #2에서 읽기-쓰기 또는 슈퍼유저 액세스 권한을 얻지 못합니다. 대신 클라이언트 #2가 익명 사용자에게 매핑되며 이 경우 사용자 ID 0이 있습니다.

ONTAP NFS 내보내기 정책 캐시에 대해 알아보세요

시스템 성능을 개선하기 위해 ONTAP는 로컬 캐시를 사용하여 호스트 이름 및 넷그룹과 같은 정보를 저장합니다. 이렇게 하면 ONTAP에서 외부 소스에서 정보를 검색하는 것보다 내보내기 정책 규칙을 더 빠르게 처리할 수 있습니다. 캐시의 정의 및 작업을 이해하면 클라이언트 액세스 문제를 해결하는 데 도움이 됩니다.

NFS 내보내기에 대한 클라이언트 액세스를 제어하기 위해 익스포트 정책을 구성합니다. 각 익스포트 정책에는 규칙이 포함되어 있으며, 각 규칙에는 액세스를 요청하는 클라이언트와 규칙을 일치시키는 매개 변수가 포함되어 있습니다. 이러한 매개 변수 중 일부는 도메인 이름, 호스트 이름 또는 넷그룹과 같은 개체를 확인하기 위해 ONTAP에서 DNS 또는 NIS 서버와 같은 외부 소스에 연결해야 합니다.

외부 소스와의 이러한 통신에는 약간의 시간이 소요됩니다. 성능을 높이기 위해 ONTAP는 여러 캐시의 각 노드에 정보를 로컬로 저장하여 익스포트 정책 규칙 개체를 해결하는 데 걸리는 시간을 단축합니다.

캐시 이름입니다	저장된 정보의 유형입니다
액세스	해당 익스포트 정책에 대한 클라이언트 매핑
이름	UNIX 사용자 이름을 해당 UNIX 사용자 ID에 매핑
ID입니다	UNIX 사용자 ID와 해당 UNIX 사용자 ID 및 확장 UNIX 그룹 ID의 매핑
호스트	호스트 이름을 해당 IP 주소에 매핑

캐시 이름입니다	저장된 정보의 유형입니다
넷그룹	구성원의 해당 IP 주소에 대한 넷그룹 매핑
쇼마운트	SVM 네임스페이스에서 내보낸 디렉토리 목록입니다

ONTAP에서 검색 및 로컬에 저장한 후 환경에 있는 외부 이름 서버의 정보를 변경하면 캐시에 오래된 정보가 포함될 수 있습니다. ONTAP를 새로 고치면 특정 기간이 지나면 자동으로 캐시가 새로 고쳐지지만 다른 캐시에 만료 및 새로 고침 시간과 알고리즘이 다릅니다.

캐시에 오래된 정보가 포함되는 또 다른 가능한 이유는 ONTAP가 캐시된 정보를 새로 고치려고 하지만 이름 서버와 통신하려고 할 때 오류가 발생하는 것입니다. 이 경우 ONTAP는 클라이언트 중단을 방지하기 위해 로컬 캐시에 현재 저장되어 있는 정보를 계속 사용합니다.

따라서 성공해야 하는 클라이언트 액세스 요청이 실패하고 실패해야 하는 클라이언트 액세스 요청이 성공할 수 있습니다. 이러한 클라이언트 액세스 문제를 해결할 때 일부 익스포트 정책 캐시를 보고 수동으로 플러시할 수 있습니다.

ONTAP NFS 액세스 캐시에 대해 알아보세요

ONTAP은 액세스 캐시를 사용하여 클라이언트 액세스 작업에 대한 익스포트 정책 규칙 평가 결과를 볼륨 또는 qtree에 저장합니다. 따라서 클라이언트가 입출력 요청을 보낼 때마다 내보내기 정책 규칙 평가 프로세스를 거치는 것보다 액세스 캐시에서 정보를 훨씬 빠르게 검색할 수 있기 때문에 성능이 향상됩니다.

NFS 클라이언트가 볼륨 또는 qtree의 데이터에 액세스하기 위해 I/O 요청을 보낼 때마다 ONTAP는 각 I/O 요청을 평가하여 I/O 요청을 허용하거나 거부할 것인지 결정해야 합니다. 이 평가에서는 볼륨 또는 qtree와 관련된 익스포트 정책의 모든 익스포트 정책 규칙을 검사합니다. 볼륨 또는 qtree에 대한 경로에 하나 이상의 접합 지점이 포함되는 경우, 경로를 따라 여러 익스포트 정책을 위해 이 점검을 수행해야 할 수 있습니다.

이 평가는 초기 마운트 요청뿐만 아니라 읽기, 쓰기, 목록, 복사 및 기타 작업과 같이 NFS 클라이언트에서 전송된 모든 입출력 요청에 대해 수행됩니다.

ONTAP가 해당 익스포트 정책 규칙을 식별하고 요청을 허용 또는 거부할지 결정한 후에는 ONTAP가 액세스 캐시에 이 정보를 저장하기 위한 항목을 생성합니다.

NFS 클라이언트가 I/O 요청을 보낼 때 ONTAP는 클라이언트의 IP 주소, SVM의 ID, 타겟 볼륨 또는 qtree와 관련된 익스포트 정책을 기록한 다음, 액세스 캐시에서 일치하는 항목을 확인합니다. 액세스 캐시에 일치하는 항목이 있는 경우 ONTAP는 저장된 정보를 사용하여 I/O 요청을 허용하거나 거부합니다. 일치하는 항목이 없는 경우 ONTAP는 위에서 설명한 모든 해당 정책 규칙을 평가하는 일반적인 프로세스를 수행합니다.

활성 상태로 사용되지 않는 액세스 캐시 항목은 새로 고쳐지지 않습니다. 이렇게 하면 외부 이름 서비스와의 불필요한 소모적인 통신이 줄어듭니다.

액세스 캐시에서 정보를 검색하는 것이 모든 입출력 요청에 대해 전체 익스포트 정책 규칙 평가 프로세스를 수행하는 것보다 훨씬 빠릅니다. 따라서 액세스 캐시를 사용하면 클라이언트 액세스 검사의 오버헤드를 줄여 성능을 크게 향상시킬 수 있습니다.

ONTAP NFS 액세스 캐시 매개변수에 대해 알아보세요

여러 매개 변수는 액세스 캐시의 항목에 대한 새로 고침 기간을 제어합니다. 이러한 매개 변수의 작동 방식을 이해하면 액세스 캐시를 조정하고 저장된 정보의 최근 성능과 균형을 유지하도록

매개 변수를 수정할 수 있습니다.

액세스 캐시는 볼륨 또는 qtree에 액세스하려는 클라이언트에 적용되는 하나 이상의 익스포트 규칙으로 구성된 항목을 저장합니다. 이러한 항목은 새로 고쳐지기 전에 일정 시간 동안 저장됩니다. 새로 고침 시간은 액세스 캐시 매개 변수에 의해 결정되며 액세스 캐시 항목의 유형에 따라 달라집니다.

개별 SVM에 대한 액세스 캐시 매개 변수를 지정할 수 있습니다. 따라서 SVM 액세스 요구사항에 따라 매개 변수가 달라질 수 있습니다. 활성 상태로 사용되지 않는 액세스 캐시 항목은 새로 고쳐지지 않으므로 외부 이름 서비스와의 불필요한 소모적인 통신이 줄어듭니다.

액세스 캐시 항목 유형입니다	설명	새로 고침 기간(초)
양의 입력	액세스 캐시 항목으로 인해 클라이언트에 대한 액세스 거부가 발생되지 않았습니다.	최소: 300 최대: 86,400 기본값: 3,600
음수 항목	액세스 캐시 항목으로 인해 클라이언트에 대한 액세스 거부가 발생했습니다.	최소: 60 최대: 86,400 기본값: 3,600

예

NFS 클라이언트가 클러스터의 볼륨에 액세스하려고 합니다. ONTAP은 클라이언트를 익스포트 정책 규칙과 일치시키고 클라이언트가 익스포트 정책 규칙 구성에 따라 액세스할 수 있는지 확인합니다. ONTAP은 액세스 캐시에 있는 내보내기 정책 규칙을 양의 항목으로 저장합니다. 기본적으로 ONTAP은 액세스 캐시의 양의 항목을 1시간 (3,600초) 동안 유지한 다음 해당 항목을 자동으로 새로 고쳐 정보를 최신 상태로 유지합니다.

액세스 캐시가 불필요하게 가득 차는 것을 방지하기 위해 특정 기간 동안 사용하지 않은 기존 액세스 캐시 항목을 지우기 위한 추가 매개 변수가 있습니다. 이 '-하비스트-timeout' 매개 변수는 허용되는 범위는 60초에서 2,592,000초이며 기본 설정은 86,400초입니다.

ONTAP NFS qtree에서 내보내기 정책 제거

특정 익스포트 정책을 qtree에 더 이상 할당하지 않으려는 경우, qtree를 수정하여 포함하는 볼륨의 익스포트 정책을 상속하도록 익스포트 정책을 제거할 수 있습니다. 이렇게 하려면 '-export-policy' 매개 변수와 빈 이름 문자열("")을 사용하여 볼륨 qtree modify 명령을 사용할 수 있습니다.

단계

1. qtree에서 익스포트 정책을 제거하려면 다음 명령을 입력합니다.

```
"볼륨 qtree modify -vserver vservice_name -qtree -path /vol/volume_name /qtree_name -export-policy""
```

2. qtree가 적절히 수정되었는지 확인합니다.

```
'볼륨 qtree show-qtree qtree_name-fields export-policy'
```

ONTAP에서는 qtree ID에 대한 선택적 추가 검증을 수행할 수 있습니다. 이 검증에서는 클라이언트 파일 작업 요청이 유효한 qtree ID를 사용하고 클라이언트가 동일한 qtree 내의 파일만 이동할 수 있는지 확인합니다. '-validate-qtree-export' 매개 변수를 수정하여 이 유효성 검사를 활성화 또는 비활성화할 수 있습니다. 이 매개 변수는 기본적으로 사용하도록 설정됩니다.

이 작업에 대해

이 매개 변수는 SVM(스토리지 가상 머신)에서 하나 이상의 qtree에 익스포트 정책을 직접 할당한 경우에만 효과적입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

Qtree ID 검증을 원하는 경우...	다음 명령을 입력합니다...
활성화됨	'vserver nfs modify -vserver vservers_name -validate -qtree -export enabled'
사용 안 함	'vserver nfs modify -vserver vservers_name -validate -qtree -export disabled'

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

ONTAP NFS FlexVol 볼륨에 대한 정책 제한 및 중첩된 연결 내보내기

중첩 교차점에 덜 제한적인 정책을 설정하지만 상위 수준 교차점에 더 제한적인 정책을 설정하도록 내보내기 정책을 구성한 경우 하위 수준 교차점에 액세스하지 못할 수 있습니다.

상위 레벨의 교차로에서 낮은 레벨의 교차로보다 제한적인 익스포트 정책이 있는지 확인해야 합니다.

강력한 보안을 위해 **NFS**와 **Kerberos** 사용

Kerberos에 대한 ONTAP NFS 지원

Kerberos는 클라이언트/서버 응용 프로그램에 대해 강력한 보안 인증을 제공합니다. 인증을 통해 사용자 및 프로세스 ID를 서버에 확인할 수 있습니다. ONTAP 환경에서 Kerberos는 SVM(스토리지 가상 머신)과 NFS 클라이언트 간에 인증을 제공합니다.

ONTAP 9에서는 다음과 같은 Kerberos 기능이 지원됩니다.

- 무결성 검사를 통한 Kerberos 5 인증(krb5i)

Krb5i는 체크섬을 사용하여 클라이언트와 서버 간에 전송되는 각 NFS 메시지의 무결성을 확인합니다. 이는 보안상의 이유(예: 데이터가 무단 변경되지 않도록 보장) 및 데이터 무결성을 위해(예: 불안정한 네트워크에서 NFS를 사용할 때 데이터 손상을 방지) 모두에 유용합니다.

- Kerberos 5 개인 정보 확인 인증(krb5p)

Krb5p는 체크섬을 사용하여 클라이언트와 서버 사이의 모든 트래픽을 암호화합니다. 이는 보다 안전하며 부하가 더 많이 발생합니다.

- 128비트 및 256비트 AES 암호화

AES(Advanced Encryption Standard)는 전자 데이터의 보안을 위한 암호화 알고리즘입니다. ONTAP은 128비트 키(AES-128)로 AES와 256비트 키(AES-256) 암호화를 사용하여 Kerberos를 더욱 강력하게 지원합니다.

- SVM 레벨 Kerberos 영역 구성

이제 SVM 관리자가 SVM 레벨에서 Kerberos 영역 구성을 생성할 수 있습니다. 즉, SVM 관리자는 더 이상 Kerberos 영역 구성을 위해 클러스터 관리자에 의존하지 않고 다중 테넌시 환경에서 개별 Kerberos 영역 구성을 생성할 수 있습니다.

ONTAP NFS를 사용하여 Kerberos를 구성하기 위한 요구 사항

시스템에서 NFS로 Kerberos를 구성하기 전에 네트워크 및 스토리지 환경의 특정 항목이 올바르게 구성되었는지 확인해야 합니다.



환경을 구성하는 단계는 사용 중인 클라이언트 운영 체제, 도메인 컨트롤러, Kerberos, DNS 등의 버전과 유형에 따라 다릅니다. 이러한 모든 변수를 문서화하는 것은 이 문서의 범위를 벗어납니다. 자세한 내용은 각 구성 요소에 대한 각 설명서를 참조하십시오.

Windows Server 2008 R2 Active Directory 및 Linux 호스트를 사용하는 환경에서 NFSv3 및 NFSv4를 사용하여 ONTAP 및 Kerberos 5를 설정하는 방법에 대한 자세한 내용은 기술 보고서 4073을 참조하십시오.

다음 항목을 먼저 구성해야 합니다.

네트워크 환경 요구 사항

- Kerberos

Windows Active Directory 기반 Kerberos 또는 MIT Kerberos와 같은 KDC(키 배포 센터)를 사용하여 작동하는 Kerberos 설정이 있어야 합니다.

NFS 서버는 시스템 보안 주체의 주요 구성 요소로 NFS를 사용해야 합니다.

- 디렉터리 서비스

SSL/TLS를 통해 LDAP를 사용하도록 구성된 Active Directory 또는 OpenLDAP와 같은 환경에서 보안 디렉터리 서비스를 사용해야 합니다.

- NTP

NTP를 실행하는 작업 시간 서버가 있어야 합니다. 시간 편중이 발생하여 Kerberos 인증 실패를 방지하려면 이

작업이 필요합니다.

- 도메인 이름 확인(DNS)

각 UNIX 클라이언트와 각 SVM LIF에는 정방향 및 역방향 조회 영역에서 KDC에 등록된 적절한 서비스 레코드(SRV)가 있어야 합니다. 모든 참가자는 DNS를 통해 제대로 확인할 수 있어야 합니다.

- 사용자 계정

각 클라이언트에는 Kerberos 영역에 사용자 계정이 있어야 합니다. NFS 서버는 시스템 보안 주체의 기본 구성 요소로 "NFS"를 사용해야 합니다.

NFS 클라이언트 요구 사항

- NFS 를 참조하십시오

NFSv3 또는 NFSv4를 사용하여 네트워크를 통해 통신하도록 각 클라이언트를 올바르게 구성해야 합니다.

고객은 RFC1964 및 RFC2203을 지원해야 합니다.

- Kerberos

각 클라이언트는 Kerberos 인증을 사용하도록 적절히 구성되어야 하며, 다음과 같은 세부 정보가 포함되어야 합니다.

- TGS 통신에 대한 암호화가 활성화되었습니다.

강력한 보안을 위한 AES-256.

- TGT 통신을 위한 가장 안전한 암호화 유형이 활성화됩니다.
- Kerberos 영역과 도메인이 올바르게 구성되었습니다.
- GSS가 활성화되었습니다.

시스템 자격 증명을 사용하는 경우:

- gssd를 -n 매개변수로 실행하지 마십시오.
- 루트 사용자로 "kinit"를 실행하지 마십시오.

- 각 클라이언트는 최신 및 업데이트된 운영 체제 버전을 사용해야 합니다.

Kerberos와 AES 암호화를 위한 최고의 호환성과 안정성을 제공합니다.

- DNS

올바른 이름 확인을 위해 DNS를 사용하도록 각 클라이언트를 올바르게 구성해야 합니다.

- NTP

각 클라이언트는 NTP 서버와 동기화되어야 합니다.

- 호스트 및 도메인 정보

각 클라이언트의 '/etc/hosts' 및 '/etc/resolv.conf' 파일은 각각 올바른 호스트 이름과 DNS 정보를 포함해야 합니다.

- keytab 파일

각 클라이언트에는 KDC의 keytab 파일이 있어야 합니다. 영역은 대문자여야 합니다. 가장 강력한 보안을 위해서는 암호화 유형이 AES-256이어야 합니다.

- 선택 사항: 최상의 성능을 위해 클라이언트는 최소한 두 개의 네트워크 인터페이스를 가질 수 있습니다. 하나는 로컬 영역 네트워크와 통신하며 다른 하나는 스토리지 네트워크와 통신하기 위한 것입니다.

수행할 수 있습니다

- NFS 라이선스

스토리지 시스템에 유효한 NFS 라이선스가 설치되어 있어야 합니다.

- CIFS 라이선스

CIFS 라이선스는 선택 사항입니다. 멀티프로토콜 이름 매핑을 사용할 때는 Windows 자격 증명을 확인하는 데만 필요합니다. 엄격한 UNIX 전용 환경에서는 필요하지 않습니다.

- SVM

시스템에 SVM이 하나 이상 구성되어 있어야 합니다.

- SVM의 DNS

각 SVM에서 DNS를 구성해야 합니다.

- NFS 서버

SVM에서 NFS를 구성해야 합니다.

- AES 암호화

가장 강력한 보안을 위해서는 Kerberos에 AES-256 암호화만 허용하도록 NFS 서버를 구성해야 합니다.

- SMB 서버

멀티프로토콜 환경을 실행 중인 경우 SVM에서 SMB를 구성해야 합니다. 멀티 프로토콜 이름 매핑에 SMB 서버가 필요합니다.

- 볼륨

루트 볼륨과 SVM에서 사용하도록 구성된 데이터 볼륨이 하나 이상 있어야 합니다.

- 루트 볼륨

SVM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름	설정
보안 스타일	Unix
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	777

루트 볼륨과 달리 데이터 볼륨은 보안 스타일을 가질 수 있습니다.

- Unix 그룹

SVM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 ID입니다
데몬	1
루트	0
pcuser	65534(SVM 생성 시 ONTAP에서 자동으로 생성)

- Unix 사용자

SVM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 ID입니다	기본 그룹 ID입니다	설명
NFS 를 참조하십시오	500입니다	0	GSS INIT 단계에 필요함 NFS 클라이언트 사용자 SPN의 첫 번째 구성 요소가 사용자로 사용됩니다.
pcuser	65534	65534	NFS 및 CIFS를 멀티프로토콜 용도로 필요합니다 SVM을 생성할 때 ONTAP이 pcuser 그룹을 자동으로 생성하여 추가했습니다.
루트	0	0	마운팅에 필요합니다

NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다.

- 익스포트 정책 및 규칙

루트 및 데이터 볼륨 및 qtree에 필요한 익스포트 규칙을 사용하여 익스포트 정책을 구성해야 합니다. Kerberos를 통해 SVM의 모든 볼륨에 액세스할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5', krb5i 또는 krb5p로 설정할 수 있습니다.

- Kerberos - UNIX 이름 매핑

NFS 클라이언트 사용자 SPN에 의해 식별된 사용자에게 루트 권한을 부여하려면 루트에 대한 이름 매핑을 생성해야 합니다.

관련 정보

["NetApp 기술 보고서 4073: 안전한 통합 인증"](#)

["NetApp 상호 운용성 매트릭스 툴"](#)

["시스템 관리"](#)

["논리적 스토리지 관리"](#)

NFSv4에 대한 ONTAP 사용자 ID 도메인을 지정합니다.

사용자 ID 도메인을 지정하려면 '-v4-id-domain' 옵션을 설정합니다.

이 작업에 대해

기본적으로 ONTAP에서는 NFSv4 사용자 ID 매핑이 설정된 경우 NIS 도메인을 사용합니다. NIS 도메인이 설정되어 있지 않으면 DNS 도메인이 사용됩니다. 예를 들어 여러 사용자 ID 도메인이 있는 경우 사용자 ID 도메인을 설정해야 할 수 있습니다. 도메인 이름은 도메인 컨트롤러의 도메인 구성과 일치해야 합니다. NFSv3에는 필요하지 않습니다.

단계

1. 다음 명령을 입력합니다.

```
'vserver nfs modify -vserver vservice_name -v4-id-domain NIS_domain_name'
```

이름 서비스 구성

ONTAP NFS 이름 서비스 스위치 구성에 대해 자세히 알아보십시오

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다. 환경에 맞게 적절하게 구성할 수 있도록 표의 기능과 ONTAP에서 표의 사용 방법을 이해해야 합니다.

ONTAP 이름 서비스 스위치 테이블은 ONTAP가 특정 유형의 이름 서비스 정보에 대한 정보를 검색하기 위해 어떤 이름 서비스 소스를 참조합니다. ONTAP는 SVM별로 개별 네임 서비스 스위치 테이블을 유지 관리합니다.

데이터베이스 유형

이 테이블에는 다음과 같은 각 데이터베이스 유형에 대해 별도의 이름 서비스 목록이 저장됩니다.

데이터베이스 유형입니다	다음에 대한 이름 서비스 소스를 정의합니다.	유효한 소스는...
호스트	호스트 이름을 IP 주소로 변환	파일, DNS
그룹	사용자 그룹 정보를 찾는 중입니다	파일, NIS, LDAP
암호	사용자 정보를 찾는 중입니다	파일, NIS, LDAP
넷그룹	넷그룹 정보를 찾는 중입니다	파일, NIS, LDAP
이름맵	사용자 이름 매핑 중	파일, LDAP

소스 유형

소스는 해당 정보를 검색하는 데 사용할 이름 서비스 소스를 지정합니다.

원본 유형 지정...	에서 정보를 조회하려면...	관리 대상 명령 제품군...
파일	로컬 소스 파일	SVM 서비스 이름 서비스 유닉스 사용자 SVM 서비스 이름 서비스 유닉스 그룹 SVM 서비스 이름 서비스 넷그룹 SVM 서비스 이름-서비스 DNS 호스트
NIS를 선택합니다	SVM의 NIS 도메인 구성에 지정된 외부 NIS 서버	'vserver services name-service nis- domain'을 선택합니다
LDAP를 지원합니다	SVM의 LDAP 클라이언트 구성에 지정된 외부 LDAP 서버	'vserver services name-service ldap'
DNS	SVM의 DNS 구성에 지정된 외부 DNS 서버	SVM 서비스 이름-서비스 DNS

데이터 액세스와 SVM 관리 인증 모두에 NIS 또는 LDAP를 사용하려는 경우에도 NIS 또는 LDAP 인증이 실패할 경우 "파일"을 포함하고 로컬 사용자를 대체 수단으로 구성해야 합니다.

외부 소스에 액세스하는 데 사용되는 프로토콜입니다

외부 소스의 서버에 액세스하기 위해 ONTAP는 다음 프로토콜을 사용합니다.

외부 이름 서비스 소스입니다	액세스에 사용되는 프로토콜입니다
NIS를 선택합니다	UDP입니다

외부 이름 서비스 소스입니다	액세스에 사용되는 프로토콜입니다
DNS	UDP입니다
LDAP를 지원합니다	TCP

예

다음 예는 SVM svm_1의 이름 서비스 스위치 구성을 표시합니다.

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source	Order
svm_1	hosts	files,	
		dns	
svm_1	group	files	
svm_1	passwd	files	
svm_1	netgroup	nis,	
		files	

호스트의 IP 주소를 조회하기 위해 ONTAP는 먼저 로컬 소스 파일을 참조합니다. 쿼리가 결과를 반환하지 않으면 다음으로 DNS 서버가 선택됩니다.

사용자 또는 그룹 정보를 조회하기 위해 ONTAP는 로컬 소스 파일만 참조합니다. 쿼리가 결과를 반환하지 않으면 조회가 실패합니다.

넷그룹 정보를 조회하기 위해 ONTAP는 먼저 외부 NIS 서버를 참조합니다. 쿼리가 결과를 반환하지 않으면 로컬 넷그룹 파일이 다음에 선택됩니다.

SVM svm_1의 테이블에는 이름 매핑에 대한 이름 서비스 항목이 없습니다. 따라서 ONTAP는 기본적으로 로컬 소스 파일만 참조합니다.

관련 정보

["NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"](#)

LDAP를 사용합니다

ONTAP NFS SVM용 LDAP에 대해 알아보세요

LDAP(Lightweight Directory Access Protocol) 서버를 사용하면 사용자 정보를 중앙에서 관리할 수 있습니다. 사용자 환경의 LDAP 서버에 사용자 데이터베이스를 저장하는 경우 기존 LDAP 데이터베이스에서 사용자 정보를 조회하도록 스토리지 시스템을 구성할 수 있습니다.

- ONTAP용 LDAP를 구성하기 전에 사이트 배포가 LDAP 서버 및 클라이언트 구성에 대한 모범 사례를 충족하는지 확인해야 합니다. 특히 다음 조건을 충족해야 합니다.
 - LDAP 서버의 도메인 이름이 LDAP 클라이언트의 항목과 일치해야 합니다.

- LDAP 서버에서 지원하는 LDAP 사용자 암호 해시 유형에는 ONTAP에서 지원하는 해시 유형이 포함되어야 합니다.
 - 암호화(모든 유형) 및 SHA-1(SHA, SSHA).
 - ONTAP 9.8부터 SHA-2 해시(SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, SSHA-512)도 지원됩니다.
- LDAP 서버에 세션 보안 조치가 필요한 경우 LDAP 클라이언트에서 이를 구성해야 합니다.

다음 세션 보안 옵션을 사용할 수 있습니다.

- LDAP 서명(데이터 무결성 검사 제공) 및 LDAP 서명 및 봉인(데이터 무결성 검사 및 암호화 제공)
- TLS를 시작합니다
- LDAPS(TLS 또는 SSL을 통한 LDAP)
- 서명되고 봉인된 LDAP 쿼리를 사용하려면 다음 서비스를 구성해야 합니다.
 - LDAP 서버는 GSSAPI(Kerberos) SASL 메커니즘을 지원해야 합니다.
 - LDAP 서버에는 DNS 서버에 설정된 PTR 레코드와 DNS A/AAAA 레코드가 있어야 합니다.
 - Kerberos 서버는 DNS 서버에 SRV 레코드가 있어야 합니다.
- 시작 TLS 또는 LDAPS를 활성화하려면 다음 사항을 고려해야 합니다.
 - LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.
 - LDAPS를 사용하는 경우 ONTAP 9.5 이상에서는 LDAP 서버에서 TLS 또는 SSL을 활성화해야 합니다. ONTAP 9.4~9.0에서는 SSL이 지원되지 않습니다.
 - 도메인에 인증서 서버가 이미 구성되어 있어야 합니다.
- ONTAP 9.5 이상에서 LDAP 조회 추적을 활성화하려면 다음 조건을 충족해야 합니다.
 - 두 도메인은 다음 신뢰 관계 중 하나로 구성해야 합니다.
 - 양방향
 - 원웨이 - 프라이머리(primary)가 추천 도메인을 신뢰하는 곳입니다
 - 부모-자식
 - DNS는 참조된 모든 서버 이름을 확인하도록 구성되어야 합니다.
 - '--bind-as-cifs-server'가 true로 설정된 경우 도메인 암호가 인증을 위해 동일해야 합니다.

LDAP 조회 추적에는 다음 구성이 지원되지 않습니다.



- 모든 ONTAP 버전:
- 관리 SVM의 LDAP 클라이언트
- ONTAP 9.8 및 이전 버전(9.9.1 이상에서 지원됨):
- LDAP 서명 및 봉인('-session-security' 옵션)
- 암호화된 TLS 연결('-use-start-tls' 옵션)
- LDAPS 포트 636을 통한 통신('-use-ldaps-for-ad-ldap' 옵션)

- ONTAP 9.11.1부터 를 사용할 수 있습니다 ["ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른](#)

바인딩을 사용합니다."

- SVM에서 LDAP 클라이언트를 구성할 때 LDAP 스키마를 입력해야 합니다.

대부분의 경우 기본 ONTAP 스키마 중 하나가 적합합니다. 그러나 사용자 환경의 LDAP 스키마가 이러한 스키마와 다른 경우 LDAP 클라이언트를 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다. 사용자 환경의 요구 사항에 대해서는 LDAP 관리자에게 문의하십시오.

- 호스트 이름 확인에 LDAP를 사용하는 것은 지원되지 않습니다.

자세한 내용은 을 참조하십시오 "[NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법](#)".

ONTAP NFS SVM에 대한 LDAP 서명 및 봉인에 대해 알아보세요.

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록 서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 NFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다. 테스트

SVM에서 '-session-security-for-ad-ldap' 옵션을 사용하여 SVM에서 SMB 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

ONTAP NFS SVM용 LDAPS에 대해 알아보세요

ONTAP가 LDAP 통신을 보호하는 방법에 대한 특정 용어와 개념을 이해해야 합니다. ONTAP는 Active Directory 통합 LDAP 서버 또는 UNIX 기반 LDAP 서버 간에 인증된 세션을 설정하기 위해 시작 TLS 또는 LDAPS를 사용할 수 있습니다.

용어

ONTAP에서 LDAPS를 사용하여 LDAP 통신을 보호하는 방법에 대해 이해해야 하는 특정 용어가 있습니다.

- * LDAP *

(Lightweight Directory Access Protocol) 정보 디렉터리에 액세스하고 관리하는 프로토콜입니다. LDAP는 사용자, 그룹 및 넷그룹과 같은 객체를 저장하기 위한 정보 디렉터리로 사용됩니다. 또한 LDAP는 이러한 객체를 관리하고 LDAP 클라이언트의 LDAP 요청을 처리하는 디렉토리 서비스를 제공합니다.

- SSL *

(Secure Sockets Layer) 인터넷을 통해 정보를 안전하게 전송하기 위해 개발된 프로토콜입니다. SSL은 ONTAP 9 이상에서 지원되지만 TLS 사용을 위해 더 이상 사용되지 않습니다.

- * TLS *

(전송 계층 보안) IETF 표준 트랙 프로토콜로서 이전 SSL 사양에 기초합니다. SSL의 후속 제품입니다. TLS는 ONTAP 9.5 이상에서 지원됩니다.

- * LDAPS(SSL 또는 TLS를 통한 LDAP) *

LDAP 클라이언트와 LDAP 서버 간의 보안 통신을 위해 TLS 또는 SSL을 사용하는 프로토콜입니다. SSL을 통한 LDAP와 TLS를 통한 LDAP라는 용어는 서로 바꿔 사용되기도 합니다. LDAPS는 ONTAP 9.5 이상에서 지원됩니다.

- ONTAP 9.8-9.5에서는 LDAPS를 포트 636에서만 활성화할 수 있습니다. 그렇게 하려면 다음을 사용하세요.
-use-ldaps-for-ad-ldap 매개변수를 사용하여 `vserver cifs security modify` 명령.
- ONTAP 9.9.1부터 포트 636이 기본값으로 유지되지만 LDAPS는 모든 포트에서 활성화할 수 있습니다. 이렇게 하려면 `-ldaps-enabled` 매개 변수를 `true` 설정하고 원하는 `-port` 매개 변수를 지정합니다. 에 대한 자세한 내용은 `vserver services name-service ldap client create` "ONTAP 명령 참조입니다"를 참조하십시오.



LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.

- * TLS * 를 시작합니다

(`start_tls`, `STARTTLS` 및 `StartTLS` 라고도 함) TLS 프로토콜을 사용하여 보안 통신을 제공하는 메커니즘입니다.

ONTAP는 LDAP 통신 보안을 위해 STARTTLS를 사용하며 기본 LDAP 포트(389)를 사용하여 LDAP 서버와 통신합니다. LDAP 서버는 LDAP 포트 389를 통한 연결을 허용하도록 구성해야 합니다. 그렇지 않으면 SVM에서 LDAP 서버로의 LDAP TLS 연결이 실패합니다.

ONTAP에서 LDAPS를 사용하는 방법

ONTAP는 TLS 서버 인증을 지원하므로 SVM LDAP 클라이언트가 바인딩 작업 중에 LDAP 서버의 ID를 확인할 수 있습니다. TLS를 사용하는 LDAP 클라이언트는 공용 키 암호화의 표준 기술을 사용하여 서버의 인증서와 공용 ID가 유효하며 클라이언트의 신뢰할 수 있는 CA 목록에 나열된 CA(인증 기관)에서 발급되었는지 확인할 수 있습니다.

LDAP는 TLS를 사용하여 통신을 암호화하는 STARTTLS를 지원합니다. STARTTLS는 표준 LDAP 포트(389)를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다.

ONTAP는 다음을 지원합니다.

- Active Directory 통합 LDAP 서버와 SVM 간의 SMB 관련 트래픽을 위한 LDAPS
- 이름 매핑 및 기타 UNIX 정보를 위한 LDAP 트래픽용 LDAPS

Active Directory 통합 LDAP 서버 또는 UNIX 기반 LDAP 서버를 사용하여 LDAP 이름 매핑과 사용자, 그룹 및 네트그룹과 같은 기타 UNIX 정보에 대한 정보를 저장할 수 있습니다.

- 자체 서명된 루트 CA 인증서

Active-Directory 통합 LDAP를 사용하는 경우 도메인에 Windows Server 인증서 서비스가 설치될 때 자체 서명된 루트 인증서가 생성됩니다. LDAP 이름 매핑에 UNIX 기반 LDAP 서버를 사용하는 경우 자체 서명된 루트 인증서는 해당 LDAP 애플리케이션에 적합한 방법을 사용하여 생성 및 저장됩니다.

기본적으로 LDAPS는 비활성화되어 있습니다.

ONTAP NFS SVM에 대한 LDAP RFC2307bis 지원 활성화

LDAP를 사용하고 중첩된 그룹 구성원을 사용하는 추가 기능이 필요한 경우 ONTAP를 구성하여 LDAP RFC2307bis 지원을 활성화할 수 있습니다.

시작하기 전에

사용할 기본 LDAP 클라이언트 스키마 중 하나의 복사본을 만들어야 합니다.

이 작업에 대해

LDAP 클라이언트 스키마에서 그룹 객체는 memberUid 특성을 사용합니다. 이 속성은 여러 값을 포함할 수 있으며 해당 그룹에 속한 사용자의 이름을 나열합니다. RFC2307bis가 활성화된 LDAP 클라이언트 스키마에서 그룹 객체는 uniqueMember 속성을 사용합니다. 이 속성은 LDAP 디렉토리에 있는 다른 객체의 전체 DN(고유 이름)을 포함할 수 있습니다. 이렇게 하면 그룹이 다른 그룹을 구성원으로 포함할 수 있으므로 중첩된 그룹을 사용할 수 있습니다.

사용자는 중첩된 그룹을 포함하여 256개 이상의 그룹의 구성원이 아니어야 합니다. ONTAP은 256 그룹 제한을 초과하는 모든 그룹을 무시합니다.

기본적으로 RFC2307bis 지원은 비활성화되어 있습니다.



RFC2307bis 지원은 MS-AD-BIS 스키마를 사용하여 LDAP 클라이언트를 생성할 때 ONTAP에서 자동으로 활성화됩니다.

자세한 내용은 을 참조하십시오 ["NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"](#).

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. RFC2307 LDAP 클라이언트 스키마를 수정하여 RFC2307bis 지원을 활성화합니다.

```
'vserver services name-service ldap client schema modify -vserver vserver_name -schema schema -name -enable -rfc2307bis true'
```

3. LDAP 서버에서 지원되는 객체 클래스와 일치하도록 스키마를 수정합니다.

```
'vserver services name-service ldap client schema modify -vserver vserver -name -schema schema_name -group-of-unique-names-object-class object_class'
```

4. LDAP 서버에서 지원되는 속성 이름과 일치하도록 스키마를 수정합니다.

```
'vserver services name-service ldap client schema modify -vserver vserver -name -schema schema_name -unique-member-attribute attribute_name'
```

5. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

LDAP 디렉토리 검색을 위한 ONTAP NFS 구성 옵션

사용자, 그룹 및 넷그룹 정보를 포함한 LDAP 디렉토리 검색을 최적화하려면 ONTAP LDAP 클라이언트가 사용자 환경에 가장 적합한 방식으로 LDAP 서버에 접속하도록 구성해야 합니다. 기본 LDAP 기본 및 범위 검색 값이 충분하면 사용자 지정 값이 더 적합한 시기를 지정하는 매개 변수가 무엇인지 이해해야 합니다.

사용자, 그룹 및 넷그룹 정보에 대한 LDAP 클라이언트 검색 옵션을 사용하면 LDAP 쿼리가 실패하여 스토리지 시스템에 대한 클라이언트 액세스가 실패하는 것을 방지할 수 있습니다. 또한 클라이언트 성능 문제를 방지하기 위해 가능한 한 효율적으로 검색을 수행할 수 있습니다.

기본 및 범위 검색 값입니다

LDAP 베이스는 LDAP 클라이언트가 LDAP 쿼리를 수행하는 데 사용하는 기본 DN입니다. 사용자, 그룹 및 넷그룹 검색을 포함한 모든 검색은 기본 DN을 사용하여 수행됩니다. 이 옵션은 LDAP 디렉토리가 상대적으로 작고 모든 관련 항목이 동일한 DN에 있을 때 적합합니다.

사용자 지정 기본 DN을 지정하지 않으면 기본값은 "root"입니다. 즉, 각 쿼리는 전체 디렉터리를 검색합니다. 이렇게 하면 LDAP 쿼리의 성공 가능성이 최대화되지만 비효율적이며 대규모 LDAP 디렉토리의 성능이 크게 저하될 수 있습니다.

LDAP 기본 범위는 LDAP 클라이언트가 LDAP 쿼리를 수행하는 데 사용하는 기본 검색 범위입니다. 사용자, 그룹 및 넷그룹 검색을 포함한 모든 검색은 기본 범위를 사용하여 수행됩니다. LDAP 쿼리가 명명된 항목만 검색할지, DN 아래의 항목 하나 또는 DN 아래의 전체 하위 트리를 검색할지 여부를 결정합니다.

사용자 지정 기본 범위를 지정하지 않으면 기본값은 'Subtree'입니다. 즉, 각 쿼리는 DN 아래의 전체 하위 트리를 검색합니다. 이렇게 하면 LDAP 쿼리의 성공 가능성이 최대화되지만 비효율적이며 대규모 LDAP 디렉토리의 성능이 크게 저하될 수 있습니다.

사용자 지정 기준 및 범위 검색 값

필요에 따라 사용자, 그룹 및 넷그룹 검색에 대해 별도의 기본 값과 범위 값을 지정할 수 있습니다. 이러한 방식으로 검색 기준 및 쿼리 범위를 제한하면 LDAP 디렉토리의 하위 섹션으로 검색이 제한되므로 성능이 크게 향상됩니다.

사용자 지정 기준 및 범위 값을 지정하면 사용자, 그룹 및 넷그룹 검색에 대한 일반 기본 검색 기준 및 범위가 재정의됩니다. 사용자 지정 기준 및 범위 값을 지정하는 매개 변수는 고급 권한 수준에서 사용할 수 있습니다.

LDAP 클라이언트 매개 변수...	사용자 지정...
'-base-dn'	모든 LDAP 검색에 대한 기본 DN입니다. 필요한 경우 여러 값을 입력할 수 있습니다(예: ONTAP 9.5 이상 릴리스에서 LDAP 참조 추적이 활성화된 경우).
``기본범위``	모든 LDAP 검색에 대한 기본 범위입니다.
'-user-dn'	모든 LDAP 사용자 검색에 대한 기본 DN입니다. 이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
'- 사용자 범위'	모든 LDAP 사용자 검색의 기본 범위입니다. 이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
``그룹-dn``	모든 LDAP 그룹 검색에 대한 기본 DN입니다.
그룹-범위	모든 LDAP 그룹 검색에 대한 기본 범위입니다.
'-넷그룹-dn'	모든 LDAP 넷그룹 검색에 대한 기본 DN입니다.

넷그룹 범위	모든 LDAP 넷그룹 검색에 대한 기본 범위입니다.

여러 사용자 정의 기본 DN 값

LDAP 디렉토리 구조가 더 복잡한 경우 여러 기본 DNS를 지정하여 LDAP 디렉토리의 여러 부분을 검색하여 특정 정보를 검색해야 할 수 있습니다. 사용자, 그룹 및 넷그룹 DN 매개 변수에 대해 여러 DNS를 지정할 수 있습니다. 이를 세미콜론(;)으로 분리하고 전체 DN 검색 목록을 큰따옴표(")로 둘러싸서 지정할 수 있습니다. DN에 세미콜론이 포함된 경우 DN의 세미콜론 바로 앞에 이스케이프 문자(\)를 추가해야 합니다.

범위는 해당 매개 변수에 지정된 DNS의 전체 목록에 적용됩니다. 예를 들어 사용자 범위에 대해 서로 다른 세 개의 사용자 DNS 및 하위 트리의 목록을 지정하면 LDAP 사용자는 지정된 세 DNS에 대해 전체 하위 트리를 검색합니다.

ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에서 반환되지 않는 경우 ONTAP LDAP 클라이언트가 다른 LDAP 서버에 조회 요청을 참조할 수 있도록 LDAP_READIAL DIADIGING_을 지정할 수도 있습니다. 클라이언트는 추천 데이터를 사용하여 추천 데이터에 설명된 서버에서 대상 객체를 검색합니다. 참조된 LDAP 서버에 있는 객체를 검색하려면, LDAP 클라이언트 구성의 일부로 참조된 객체의 base-dn을 base-dn에 추가할 수 있습니다. 그러나 LDAP 클라이언트 생성 또는 수정 중에 참조 추적이 활성화('referral-enabled true' 옵션 사용)된 경우에만 참조 객체가 조회됩니다.

사용자 지정 LDAP 검색 필터

LDAP 구성 옵션 매개 변수를 사용하여 사용자 지정 검색 필터를 생성할 수 있습니다. '-group-membership-filter' 매개 변수는 LDAP 서버에서 그룹 구성원 자격을 조회할 때 사용할 검색 필터를 지정합니다.

유효한 필터의 예는 다음과 같습니다.

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

에 대해 자세히 ["ONTAP에서 LDAP를 구성하는 방법"](#)을 알아보십시오.

ONTAP NFS SVM에 대한 LDAP 디렉토리 netgroup-by-host 검색 성능 향상

LDAP 환경이 호스트별 넷그룹 검색을 허용하도록 구성된 경우 ONTAP를 구성하여 이를 활용하고 호스트별 넷그룹 검색을 수행할 수 있습니다. 따라서 넷그룹 검색 속도를 크게 높이고 넷그룹 검색 중 대기 시간으로 인해 발생할 수 있는 NFS 클라이언트 액세스 문제를 줄일 수 있습니다.

시작하기 전에

LDAP 디렉토리에는 netgroup.byhost 맵이 포함되어야 합니다.

DNS 서버에는 NFS 클라이언트에 대한 정방향(A) 및 역방향(PTR) 조회 레코드가 모두 포함되어야 합니다.

넷그룹에 IPv6 주소를 지정할 때는 RFC 5952에 지정된 대로 항상 각 주소를 줄이고 압축해야 합니다.

이 작업에 대해

NIS 서버는 넷그룹, 넷그룹, byuser, netgroup.byhost라는 세 개의 개별 맵에 넷그룹 정보를 저장합니다. 넷그룹 byuser와 netgroup.byhost 맵의 목적은 넷그룹 검색 속도를 높이는 것입니다. ONTAP는 NIS 서버에서 호스트 별로 넷그룹 검색을 수행하여 마운트 응답 시간을 향상시킬 수 있습니다.

기본적으로 LDAP 디렉토리에는 NIS 서버와 같은 netgroup.byhost 맵이 없습니다. 하지만 타사 툴을 사용하여 NIS 넷그룹을 LDAP 디렉토리에 가져올 수도 있습니다. byhost 맵을 LDAP 디렉토리에 가져와서 빠르게 넷그룹을 통한 호스트 간 검색을 수행할 수 있습니다. 호스트 별로 넷그룹을 검색할 수 있도록 LDAP 환경을 구성한 경우 netgroup.byhost의 맵 이름, DN 및 검색 범위를 사용하여 ONTAP LDAP 클라이언트를 구성하여 더 빠른 호스트 기준 넷그룹을 검색할 수 있습니다.

Netgroup-by-host 검색에 대한 결과를 더 빨리 수신하면 NFS 클라이언트가 내보내기에 대한 액세스를 요청할 때 ONTAP에서 익스포트 규칙을 더 빠르게 처리할 수 있습니다. 따라서 넷그룹 검색 지연 문제로 인해 액세스가 지연될 가능성이 줄어듭니다.

단계

1. LDAP 디렉토리로 가져온 NIS 넷그룹 byhost 맵의 정확한 전체 고유 이름을 가져옵니다.

지도 DN은 가져오기에 사용한 타사 도구에 따라 다를 수 있습니다. 최상의 성능을 얻으려면 정확한 맵 DN을 지정해야 합니다.

2. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

3. 스토리지 가상 시스템(SVM)의 LDAP 클라이언트 구성에서 Netgroup-by-host 검색을 설정합니다. 'vserver services name-service ldap client modify -vserver vserver_name -client -config config config_name -is-netgroup-byhost-enabled true-netgroup-byhost-dn netgroup-by-host_map_ninggroup-byhost-scope netgroup-by-host_search_scope

'-is-netgroup-byhost-enabled {'true'|'false'}LDAP 디렉토리에 대한 호스트 별 넷그룹 검색을 설정하거나 해제합니다. 기본값은 false 입니다.

dnetgroup-byhost-dn dnetgroup-by-host_map_ninged_name은 LDAP 디렉토리에 있는 netgroup.byhost 맵의 고유 이름을 지정합니다. 넷그룹별 검색에 대한 기본 DN을 재정의합니다. 이 매개 변수를 지정하지 않으면 ONTAP에서는 기본 DN을 대신 사용합니다.

'-netgroup-byhost-scope {'base'|'onelevel'|'ubtree'}는 넷그룹-호스트 검색 범위를 지정합니다. 이 매개변수를 지정하지 않으면 기본값은 'Subtree'입니다.

LDAP 클라이언트 구성이 아직 없는 경우 'vserver services name-service ldap client create' 명령을 사용하여 새 LDAP 클라이언트 구성을 생성할 때 이러한 매개 변수를 지정하여 Netgroup-by-host 검색을 설정할 수 있습니다.



그만큼 -ldap-servers 필드는 다음을 대체합니다. -servers 필드입니다. 다음을 사용할 수 있습니다. -ldap-servers LDAP 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 명령을 실행하면 이름이 netgroup.byhost 맵 ""nisMapName="netgroup.byhost", dc=corp, dc=example, dc=com" 및 기본 검색 범위 'subtree'를 사용하여 넷그룹을 호스트별로 검색할 수 있도록 이름이 ""ldap_corp""인 기존 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

작업을 마친 후

클라이언트 액세스 문제를 방지하려면 디렉토리의 netgroup.byhost 및 netgroup 맵을 항상 동기화해야 합니다.

관련 정보

["IETF RFC 5952: IPv6 주소 텍스트 표현에 대한 권장 사항입니다"](#)

ONTAP NFS SVM에 대한 **nsswitch** 인증을 위해 **LDAP** 빠른 바인딩을 사용합니다.

ONTAP 9.11.1부터는 LDAP_Fast BIND_FUNCION(CONNEC동시 바인드)을 활용하여 클라이언트 인증 요청을 더 빠르고 간편하게 수행할 수 있습니다. 이 기능을 사용하려면 LDAP 서버가 빠른 바인딩 기능을 지원해야 합니다.

이 작업에 대해

빠른 바인딩이 없으면 ONTAP는 LDAP 단순 바인드를 사용하여 LDAP 서버에서 관리자 사용자를 인증합니다. 이 인증 방법을 사용하면 ONTAP에서 사용자 또는 그룹 이름을 LDAP 서버로 보내고, 저장된 해시 암호를 받고, 서버 해시 코드를 사용자 암호에서 로컬로 생성된 해시 암호와 비교합니다. 동일한 경우 ONTAP는 로그인 권한을 부여합니다.

빠른 바인딩 기능을 사용하면 ONTAP는 보안 연결을 통해 사용자 자격 증명(사용자 이름 및 암호)만 LDAP 서버로 전송합니다. 그런 다음 LDAP 서버가 이러한 자격 증명을 검증하고 ONTAP에 로그인 권한을 부여하도록 지시합니다.

빠른 바인딩의 한 가지 장점은 LDAP 서버에서 암호 해싱이 수행되기 때문에 ONTAP가 LDAP 서버에서 지원하는 모든 새로운 해싱 알고리즘을 지원할 필요가 없다는 것입니다.

["빠른 바인딩 사용에 대해 알아보십시오."](#)

시작하기 전에

LDAP 고속 바인딩에 기존 LDAP 클라이언트 구성을 사용할 수 있습니다. 그러나 LDAP 클라이언트를 TLS 또는 LDAPS용으로 구성하는 것이 좋습니다. 그렇지 않으면 암호를 일반 텍스트로 유선으로 보냅니다.

ONTAP 환경에서 LDAP 고속 바인딩을 사용하려면 다음 요구 사항을 충족해야 합니다.

- ONTAP admin 사용자는 빠른 바인딩을 지원하는 LDAP 서버에 구성해야 합니다.
- ONTAP SVM은 이름 서비스 스위치(nsswitch) 데이터베이스에서 LDAP에 대해 구성해야 합니다.
- ONTAP admin 사용자 및 그룹 계정은 빠른 바인딩을 사용하여 nsswitch 인증에 맞게 구성해야 합니다.
- 빠른 바인딩이 성공하려면 관리자의 UID 번호와 GID 번호가 입력되어 있고 조회 가능해야 합니다.

단계

1. LDAP 관리자에게 LDAP 서버에서 LDAP 고속 바인딩이 지원되는지 확인하십시오.
2. ONTAP 관리자 사용자 자격 증명에 LDAP 서버에 구성되어 있는지 확인합니다.
3. LDAP 고속 바인딩에 대해 admin 또는 data SVM이 올바르게 구성되었는지 확인합니다.
 - a. LDAP 빠른 바인딩 서버가 LDAP 클라이언트 구성에 나열되는지 확인하려면 다음을 입력합니다.

```
'vserver services name-service ldap client show'
```

["LDAP 클라이언트 구성에 대해 자세히 알아보십시오."](#)
 - b. LDAP가 nsswitch 'passwd' 데이터베이스에 대해 구성된 소스 중 하나인지 확인하려면 다음을 입력합니다.

```
'vserver services name-service ns-switch show'
```

"nsswitch 구성에 대해 알아봅니다."

4. admin 사용자가 nsswitch를 사용하여 인증하는지, 그리고 계정에서 LDAP 빠른 바인딩 인증이 활성화되어 있는지 확인합니다.

- 기존 사용자의 경우 '보안 로그인 수정'을 입력하고 다음 파라미터 설정을 확인합니다.

```
'-authentication-method nsswitch'
```

```
'-is-ldap-fastbind true'
```

에 대한 자세한 내용은 `security login modify` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

- 새 관리자는 를 참조하십시오 ["LDAP 또는 NIS ONTAP 계정 액세스를 설정합니다"](#).

ONTAP NFS SVM에 대한 LDAP 통계 표시

스토리지 시스템의 스토리지 가상 머신(SVM)에 대한 LDAP 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

시작하기 전에

- SVM에서 LDAP 클라이언트를 구성해야 합니다.
- 데이터를 볼 수 있는 LDAP 객체를 식별해야 합니다.

단계

1. 카운터 객체에 대한 성능 데이터 보기:

```
'스타티틱스 쇼'
```

예

다음 예제에서는 카운터에 대해 * `smpl_1` * 이라는 샘플의 통계를 표시합니다. `avg_processor_busy` 및 `cpu_busy`

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
```

Counter	Value
-----	-----
avg_processor_busy	6%
cpu_busy	

관련 정보

- ["통계에 따르면"](#)
- ["통계 시작"](#)
- ["통계 중지"](#)

이름 매핑을 구성합니다

ONTAP NAS SVM에 대한 이름 매핑 구성에 대해 알아보세요.

ONTAP는 이름 매핑을 사용하여 SMB ID를 UNIX ID에 매핑하고, Kerberos ID를 UNIX ID에 매핑하며, UNIX ID를 SMB ID에 매핑합니다. 사용자 자격 증명을 얻고 NFS 클라이언트나 SMB 클라이언트에서 연결 중인지 여부와 관계없이 적절한 파일 액세스를 제공하려면 이 정보가 필요합니다.

이름 매핑을 사용할 필요가 없는 두 가지 예외가 있습니다.

- 순수 UNIX 환경을 구성하고 볼륨에 SMB 액세스 또는 NTFS 보안 스타일을 사용하지 않을 계획입니다.
- 대신 사용할 기본 사용자를 구성합니다.

이 시나리오에서는 모든 개별 클라이언트 자격 증명을 매핑하지 않고 모든 클라이언트 자격 증명에 동일한 기본 사용자에게 매핑되기 때문에 이름 매핑이 필요하지 않습니다.

사용자 이름 매핑만 사용할 수 있으며 그룹에서는 사용할 수 없습니다.

그러나 개별 사용자 그룹을 특정 사용자에게 매핑할 수 있습니다. 예를 들어, 영업이라는 단어가 있는 모든 AD 사용자를 특정 UNIX 사용자 및 사용자의 UID에 매핑할 수 있습니다.

ONTAP에서 사용자에게 대한 자격 증명을 매핑해야 하는 경우 먼저 로컬 이름 매핑 데이터베이스와 LDAP 서버에서 기존 매핑을 확인합니다. SVM의 네임 서비스 구성에 따라 1개 또는 2개 모두를 검사할지 여부를 결정합니다.

- Windows에서 UNIX로의 매핑의 경우

매핑을 찾을 수 없는 경우 ONTAP는 소문자 Windows 사용자 이름이 UNIX 도메인의 유효한 사용자 이름인지 확인합니다. 이렇게 해도 문제가 해결되지 않으면 기본 UNIX 사용자를 사용합니다(구성된 경우). 기본 UNIX 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

- UNIX에서 Windows로의 매핑의 경우

매핑을 찾을 수 없는 경우 ONTAP는 SMB 도메인의 UNIX 이름과 일치하는 Windows 계정을 찾으려고 시도합니다. 이 기능이 작동하지 않으면 기본 SMB 사용자를 사용합니다(구성된 경우). 기본 SMB 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

컴퓨터 계정은 기본적으로 지정된 기본 UNIX 사용자에게 매핑됩니다. 기본 UNIX 사용자를 지정하지 않으면 컴퓨터 계정 매핑이 실패합니다.

- ONTAP 9.5부터 기본 UNIX 사용자가 아닌 다른 사용자에게 시스템 계정을 매핑할 수 있습니다.
- ONTAP 9.4 이하 버전에서는 시스템 계정을 다른 사용자에게 매핑할 수 없습니다.

컴퓨터 계정에 대한 이름 매핑이 정의되어 있더라도 매핑은 무시됩니다.

ONTAP NAS SVM에서 UNIX-Windows 사용자 이름 매핑을 위한 다중 도메인 검색

ONTAP는 UNIX 사용자를 Windows 사용자에게 매핑할 때 다중 도메인 검색을 지원합니다. 일치하는 결과가 반환될 때까지 검색된 모든 신뢰할 수 있는 도메인이 대체 패턴과 일치하는 항목을 검색합니다. 또는 검색된 신뢰할 수 있는 도메인 목록 대신 사용되는 기본 신뢰할 수 있는 도메인 목록을 구성할 수 있으며 일치하는 결과가 반환될 때까지 순서대로 검색됩니다.

도메인 트러스트가 **UNIX** 사용자에게 **Windows** 사용자 이름 매핑 검색에 미치는 영향

다중 도메인 사용자 이름 매핑의 작동 방식을 이해하려면 ONTAP에서 도메인 트러스트가 작동하는 방식을 이해해야 합니다. SMB 서버의 홈 도메인과의 Active Directory 트러스트 관계는 양방향 신뢰일 수도 있고 인바운드 신뢰나 아웃바운드 트러스트를 포함한 두 가지 단방향 트러스트 유형 중 하나일 수도 있습니다. 홈 도메인은 SVM의 SMB 서버가 속하는 도메인입니다.

- 양방향 트러스트

양방향 트러스트를 사용하면 두 도메인이 서로 신뢰합니다. SMB 서버의 홈 도메인에 다른 도메인과의 양방향 트러스트가 있는 경우 홈 도메인이 신뢰할 수 있는 도메인에 속한 사용자를 인증하고 권한을 부여할 수 있으며 그 반대의 경우도 마찬가지입니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색은 홈 도메인과 다른 도메인 간의 양방향 트러스트가 있는 도메인에서만 수행할 수 있습니다.

• _아웃바운드 트러스트 _

아웃바운드 트러스트를 사용하면 홈 도메인이 다른 도메인을 신뢰합니다. 이 경우 홈 도메인이 아웃바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하고 권한을 부여할 수 있습니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 아웃바운드 트러스트가 `_not_sunfre` 검색되었습니다.

• _인바운드 신뢰 _

인바운드 트러스트를 사용하면 다른 도메인이 SMB 서버의 홈 도메인을 신뢰합니다. 이 경우 홈 도메인은 인바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하거나 승인할 수 없습니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 인바운드 트러스트가 `_not_sound`입니다.

이름 매핑에 대한 다중 도메인 검색을 구성하는 데 와일드카드(*)를 사용하는 방법

다중 도메인 이름 매핑 검색은 Windows 사용자 이름의 도메인 섹션에서 와일드카드를 사용하여 쉽게 수행할 수 있습니다. 다음 표에서는 이름 매핑 항목의 도메인 부분에서 와일드카드를 사용하여 다중 도메인 검색을 사용하는 방법을 보여 줍니다.

패턴	교체	결과
루트	* {백슬래시} {백슬래시} 관리자	UNIX 사용자 "root"는 "administrator"라는 사용자에게 매핑됩니다. "administrator"라는 이름의 첫 번째 일치하는 사용자를 찾을 때까지 모든 신뢰할 수 있는 도메인을 순서대로 검색합니다.
*	* {백슬래시} {백슬래시} *	유효한 UNIX 사용자는 해당 Windows 사용자에게 매핑됩니다. 모든 신뢰할 수 있는 도메인은 해당 이름을 가진 첫 번째 일치하는 사용자를 찾을 때까지 순서대로 검색됩니다.  * {백슬래시} {백슬래시} * 패턴은 UNIX에서 Windows로의 이름 매핑에만 유효하며 다른 방법으로는 사용할 수 없습니다.

다중 도메인 이름 검색 수행 방법

다음 두 가지 방법 중 하나를 선택하여 다중 도메인 이름 검색에 사용되는 신뢰할 수 있는 도메인 목록을 확인할 수 있습니다.

- ONTAP에서 컴파일한 자동으로 검색된 양방향 트러스트 목록을 사용합니다
- 컴파일하는 신뢰할 수 있는 기본 도메인 목록을 사용합니다

UNIX 사용자가 사용자 이름의 도메인 섹션에 와일드카드를 사용하여 Windows 사용자에게 매핑된 경우 Windows 사용자는 다음과 같이 모든 신뢰할 수 있는 도메인에서 찾을 수 있습니다.

- 선호하는 트러스트된 도메인 목록이 구성되어 있으면 매핑된 Windows 사용자는 이 검색 목록에서만 순서대로 검색됩니다.
- 신뢰할 수 있는 도메인의 기본 설정 목록이 구성되어 있지 않으면 홈 도메인의 모든 양방향 신뢰할 수 있는 도메인에서 Windows 사용자가 표시됩니다.
- 홈 도메인에 대해 양방향으로 신뢰할 수 있는 도메인이 없는 경우 사용자는 홈 도메인에서 표시됩니다.

UNIX 사용자가 사용자 이름의 도메인 섹션이 없는 Windows 사용자에게 매핑된 경우 Windows 사용자는 홈 도메인에서 찾을 수 있습니다.

ONTAP NAS SVM에 대한 이름 매핑 변환 규칙

ONTAP 시스템은 각 SVM에 대해 일련의 변환 규칙을 유지합니다. 각 규칙은 A_pattern_과 A_replacement_의 두 부분으로 구성됩니다. 변환은 적절한 목록의 시작 부분에서 시작하여 첫 번째 일치 규칙을 기반으로 대체를 수행합니다. 이 패턴은 UNIX 형식의 정규식입니다. 대체는 UNIX 'ed' 프로그램과 마찬가지로 패턴에서 부분식을 나타내는 이스케이프 시퀀스를 포함하는 문자열입니다.

ONTAP NAS SVM에 대한 이름 매핑 만들기

'vserver name-mapping create' 명령을 사용하여 이름 매핑을 생성할 수 있습니다. 이름 매핑을 사용하여 Windows 사용자가 UNIX 보안 스타일 볼륨에 액세스하고 그 반대로 액세스할 수 있습니다.

이 작업에 대해

각 SVM에서 ONTAP은 각 방향에 대해 최대 12,500개의 이름 매핑을 지원합니다.

단계

1. 이름 매핑 생성:

```
vserver name-mapping create-vserver vserver_name-direction{KRB-unix|win-unix|unix-win} - position integer-pattern text-replacement text'
```



`-pattern` 및 `-replacement` 문은 정규식으로 공식화할 수 있습니다. 또한 이 문을 사용하여 null 대체 문자열 (공백 문자) 을 사용하여 사용자에게 대한 매핑을 명시적으로 거부할 `` 수도 `-replacement` 있습니다. 에 대한 자세한 내용은 `vserver name-mapping create`
link:<https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html> ["ONTAP 명령 참조입니다"] 을 참조하십시오.

Windows와 UNIX 간 매핑이 생성될 때 새 매핑이 생성될 때 ONTAP 시스템에 대한 열린 연결이 있는 모든 SMB

클라이언트는 로그아웃했다가 다시 로그인하여 새 매핑을 확인해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 UNIX에서 Windows로의 매핑입니다. 매핑은 UNIX 사용자 johnd를 Windows 사용자 ENG\JohnDoe에 매핑합니다.

```
vs1::> vsriver name-mapping create -vsriver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 Windows에서 UNIX로의 매핑입니다. 여기에는 정규식이 포함됩니다. 매핑은 SVM과 연결된 LDAP 도메인의 사용자에게 도메인 ENG의 모든 CIFS 사용자를 매핑합니다.

```
vs1::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 이 패턴에는 이스케이프해야 하는 Windows 사용자 이름의 요소로 "\$"가 포함됩니다. 매핑은 Windows 사용자 ENG\John\$ops를 UNIX 사용자 John_ops에 매핑합니다.

```
vs1::> vsriver name-mapping create -direction win-unix -position 1
-pattern ENG\\john$ops
-replacement john_ops
```

ONTAP NAS SVM의 기본 사용자 구성

사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우 사용할 기본 사용자를 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 사용자를 구성하지 않아야 합니다.

이 작업에 대해

CIFS 인증의 경우 각 Windows 사용자를 개별 UNIX 사용자에게 매핑하지 않으려면 대신 기본 UNIX 사용자를 지정할 수 있습니다.

NFS 인증의 경우 각 UNIX 사용자를 개별 Windows 사용자에게 매핑하지 않으려면 대신 기본 Windows 사용자를 지정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...

기본 UNIX 사용자를 구성합니다	'vserver cifs options modify-default-unix-user user_name'을 선택합니다
기본 Windows 사용자를 구성합니다	'vserver nfs modify-default-win-user user_name'을 선택합니다

NFS 이름 매핑을 관리하기 위한 **ONTAP** 명령

이름 매핑을 관리하기 위한 특정 **ONTAP** 명령이 있습니다.

원하는 작업	이 명령 사용...
이름 매핑을 생성합니다	<code>vserver name-mapping create</code>
특정 위치에 이름 매핑을 삽입합니다	<code>vserver name-mapping insert</code>
이름 매핑을 표시합니다	<code>vserver name-mapping show</code>
두 이름 매핑의 위치를 교환합니다. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	<code>vserver name-mapping swap</code>
이름 매핑을 수정합니다	<code>vserver name-mapping modify</code>
이름 매핑을 삭제합니다	<code>vserver name-mapping delete</code>
올바른 이름 매핑을 확인합니다	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

에 대한 자세한 내용은 `vserver name-mapping` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

ONTAP SVM에 대한 Windows NFS 클라이언트의 액세스 활성화

ONTAP는 Windows NFSv3 클라이언트에서 파일 액세스를 지원합니다. 즉, NFSv3을 지원하는 Windows 운영 체제를 실행하는 클라이언트가 클러스터의 NFSv3 내보내기에 있는 파일에 액세스할 수 있습니다. 이 기능을 성공적으로 사용하려면 SVM(스토리지 가상 시스템)을 올바르게 구성하고 특정 요구사항과 제한사항을 숙지해야 합니다.

이 작업에 대해

기본적으로 Windows NFSv3 클라이언트 지원은 비활성화되어 있습니다.

시작하기 전에

SVM에서 NFSv3을 활성화해야 합니다.

단계

1. Windows NFSv3 클라이언트 지원 설정:

```
vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
```

2. Windows NFSv3 클라이언트를 지원하는 모든 SVM에서 를 사용하지 않도록 설정합니다 -enable-ejukebox 및 -v3-connection-drop 매개 변수:

```
vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
```

이제 Windows NFSv3 클라이언트가 스토리지 시스템에 내보내기를 마운트할 수 있습니다.

3. 각 Windows NFSv3 클라이언트가 '-o mtype=hard' 옵션을 지정하여 하드 마운트를 사용하는지 확인합니다.

이 작업은 안정적인 마운트를 보장하기 위해 필요합니다.

```
mount-o mtype=hard\\10.53.33.10\vol\vol1 z:\"
```

ONTAP SVM에 대한 NFS 클라이언트에서 내보내기 표시 활성화

NFS 클라이언트는 'howmount -e' 명령을 사용하여 ONTAP NFS 서버에서 사용할 수 있는 내보내기 목록을 볼 수 있습니다. 이렇게 하면 마운트할 파일 시스템을 식별하는 데 도움이 됩니다.

ONTAP 사용하면 기본적으로 NFS 클라이언트가 내보내기 목록을 볼 수 있습니다. 이전 릴리즈에서는 showmount 명령의 옵션을 vserver nfs modify 명시적으로 설정해야 합니다. 익스포트 목록을 보려면 SVM에서 NFSv3을 설정해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM의 showmount 기능이 표시됩니다.

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
-----
vs1      enabled
```

NFS 클라이언트에서 실행된 다음 명령은 IP 주소가 10.63.21.9인 NFS 서버의 내보내기 목록을 표시합니다.

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix      (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

NFS를 사용하여 파일 액세스를 관리합니다

ONTAP SVM에 대해 NFSv3 활성화 또는 비활성화

'-v3' 옵션을 수정하여 NFSv3을 설정하거나 해제할 수 있습니다. 이렇게 하면 NFSv3 프로토콜을 사용하는 클라이언트에 대한 파일 액세스가 허용됩니다. 기본적으로 NFSv3은 설정되어 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
NFSv3을 사용하도록 설정합니다	'vserver NFS modify -vserver vserver_name -v3 enabled'
NFSv3을 사용하지 않도록 설정합니다	'vserver NFS modify -vserver vserver_name -v3 disabled'

ONTAP SVM에 대해 NFSv4.0 활성화 또는 비활성화

'-v4.0' 옵션을 수정하여 NFSv4.0을 설정하거나 해제할 수 있습니다. 이렇게 하면 NFSv4.0 프로토콜을 사용하는 클라이언트에 대한 파일 액세스가 허용됩니다. ONTAP 9.9.1에서는 NFSv4.0이 기본적으로 설정되어 있으며 이전 릴리즈에서는 기본적으로 사용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
NFSv4.0을 사용하도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4.0 enabled'
NFSv4.0을 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 disabled'

ONTAP SVM에 대해 NFSv4.1 활성화 또는 비활성화

'-v4.1' 옵션을 수정하여 NFSv4.1을 설정 또는 해제할 수 있습니다. 따라서 NFSv4.1 프로토콜을 사용하여 클라이언트에 파일을 액세스할 수 있습니다. ONTAP 9.9.1에서는 NFSv4.1이 기본적으로 활성화되어 있지만 이전 릴리즈에서는 기본적으로 사용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
NFSv4.1을 활성화하십시오	'vserver nfs modify -vserver vserver_name -v4.1 enabled'
NFSv4.1을 비활성화하십시오	'vserver nfs modify -vserver vserver_name -v4.1 disabled'

ONTAP NFSv4 스토어풀 한도 관리

ONTAP 9.13부터 관리자는 NFSv4 서버가 클라이언트 저장소 풀 리소스 제한당 한도에 도달하면 NFSv4 클라이언트에 대한 리소스를 거부하도록 설정할 수 있습니다. 클라이언트가 NFSv4 저장소 풀 리소스를 너무 많이 사용하면 NFSv4 저장소 풀 리소스를 사용할 수 없어 다른 NFSv4 클라이언트가 차단될 수 있습니다.

또한 이 기능을 사용하면 각 클라이언트에서 사용하는 활성 저장소 리소스를 볼 수 있습니다. 이렇게 하면 시스템 리소스가 소진되는 클라이언트를 쉽게 식별할 수 있으며 클라이언트 리소스 제한에 따라 적용할 수 있습니다.

사용된 저장소 풀 리소스를 봅니다

를 클릭합니다 `vserver nfs storepool show` 명령 사용된 저장소 리소스 수를 표시합니다. 저장소 풀은 NFSv4 클라이언트가 사용하는 리소스 풀입니다.

단계

1. 관리자 권한으로 를 실행합니다 `vserver nfs storepool show` NFSv4 클라이언트의 저장소 풀 정보를 표시하는 명령입니다.

예

이 예에서는 NFSv4 클라이언트의 저장소 풀 정보를 표시합니다.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-IP: 10.0.1.1

Client-IP Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount
-----
-----

10.0.2.1      nfs4.1      true      2 1 0 4
10.0.2.2      nfs4.2      true      2 1 0 4

2 entries were displayed.
```

저장소 풀 제한 컨트롤을 사용하거나 사용하지 않도록 설정합니다

관리자는 다음 명령을 사용하여 저장소 풀 제한 컨트롤을 사용하거나 사용하지 않도록 설정할 수 있습니다.

단계

1. 관리자는 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
저장소 풀 제한 컨트롤을 활성화합니다	<code>vserver nfs storepool config modify -limit-enforce enabled</code>
저장소 풀 제한 컨트롤을 비활성화합니다	<code>vserver nfs storepool config modify -limit-enforce disabled</code>

차단된 클라이언트 목록을 봅니다

저장소 풀 제한이 설정된 경우 관리자는 클라이언트별 리소스 임계값에 도달하면 차단된 클라이언트를 확인할 수 있습니다. 관리자는 다음 명령을 사용하여 차단된 클라이언트로 표시된 클라이언트를 확인할 수 있습니다.

단계

1. 를 사용합니다 `vserver nfs storepool blocked-client show` NFSv4 차단된 클라이언트 목록을 표시하는 명령입니다.

차단된 클라이언트 목록에서 클라이언트를 제거합니다

클라이언트별 임계값에 도달한 클라이언트는 연결이 끊어지고 블록 클라이언트 캐시에 추가됩니다. 관리자는 다음

명령을 사용하여 클라이언트를 블록 클라이언트 캐시에서 제거할 수 있습니다. 이렇게 하면 클라이언트가 ONTAP NFSv4 서버에 접속할 수 있습니다.

단계

1. 를 사용합니다 `vserver nfs storepool blocked-client flush -client-ip <ip address>` 차단된 클라이언트 캐시를 플러시하는 명령입니다.
2. 를 사용합니다 `vserver nfs storepool blocked-client show` 클라이언트가 블록 클라이언트 캐시에서 제거되었는지 확인하는 명령입니다.

예

이 예에서는 모든 노드에서 IP 주소 "10.2.1.1"이 플러시되는 차단된 클라이언트를 표시합니다.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
-----
10.1.1.1

1 entries were displayed.
```

ONTAP SVM에 대한 pNFS 활성화 또는 비활성화

pNFS는 NFS 클라이언트가 스토리지 장치에서 직접 및 병렬로 읽기/쓰기 작업을 수행할 수 있도록 지원하여 잠재적 병목 현상으로 NFS 서버를 우회함으로써 성능을 개선합니다. pNFS(parallel NFS)를 활성화 또는 비활성화하려면 '-v4.1-pNFS' 옵션을 수정합니다.

ONTAP 릴리즈가...	pNFS 기본값은...
9.8 이상	사용 안 함
9.7 이하	활성화됨

시작하기 전에

pNFS를 사용하려면 NFSv4.1 지원이 필요합니다.

pNFS를 활성화하려면 먼저 NFS 조회를 비활성화해야 합니다. 둘 다 동시에 활성화할 수는 없습니다.

SVM에서 Kerberos와 pNFS를 사용하는 경우 SVM의 모든 LIF에서 Kerberos를 사용하도록 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
pNFS를 활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -pNFS enabled'
pNFS를 비활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -pNFS disabled'

관련 정보

- [NFS 트렁킹 개요](#)

ONTAP SVM에 대한 TCP 및 UDP를 통한 NFS 액세스 제어

TCP와 UDP를 통해 각각 '-TCP' 및 '-UDP' 매개 변수를 수정하여 SVM(스토리지 가상 시스템)에 대한 NFS 액세스를 설정하거나 해제할 수 있습니다. 따라서 NFS 클라이언트가 사용자 환경에서 TCP 또는 UDP를 통해 데이터에 액세스할 수 있는지 여부를 제어할 수 있습니다.

이 작업에 대해

이러한 매개 변수는 NFS에만 적용됩니다. 보조 프로토콜에는 영향을 미치지 않습니다. 예를 들어, TCP를 통한 NFS가 해제되어 있는 경우 TCP를 통한 마운트 작업은 계속 성공합니다. TCP 또는 UDP 트래픽을 완전히 차단하려면 내보내기 정책 규칙을 사용할 수 있습니다.



명령 실패 오류를 방지하려면 NFS용 TCP를 해제하기 전에 SnapDiff RPC Server를 꺼야 합니다. 'vserver snapdiff -rpc -server off -vserver vserver name' 명령을 사용하여 TCP를 비활성화할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

NFS 액세스를 원하는 경우...	명령 입력...
TCP를 통해 활성화되었습니다	'vserver nfs modify -vserver vserver_name -tcp enabled'
TCP를 통해 비활성화되었습니다	'vserver nfs modify -vserver vserver_name -tcp disabled'
UDP를 통해 활성화됩니다	'vserver nfs modify -vserver vserver_name -udp enabled'
UDP를 통해 비활성화되었습니다	'vserver nfs modify -vserver vserver_name -udp disabled'

ONTAP SVM에 대한 예약되지 않은 포트에서 NFS 요청 제어

'-mount-rotonly' 옵션을 설정하여 예약되지 않은 포트에서 NFS 마운트 요청을 거부할 수 있습니다. 예약되지 않은 포트의 모든 NFS 요청을 거부하려면 '-nfs-rotonly' 옵션을 설정합니다.

이 작업에 대해

기본적으로 '-mount-rootonly' 옵션은 'enabled'입니다.

기본적으로 '-nfs-rootonly' 옵션은 '사용 안 함'입니다.

이러한 옵션은 NULL 프로시저에는 적용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
예약되지 않은 포트에서 NFS 마운트 요청을 허용합니다	'vserver nfs modify -vserver vservice_name -mount -rootonly disabled'
예약되지 않은 포트에서 NFS 마운트 요청을 거부합니다	'vserver nfs modify -vserver vservice_name -mount -rootonly enabled'
예약되지 않은 포트에서 모든 NFS 요청을 허용합니다	'vserver nfs modify -vserver vservice_name -nfs-rootonly disabled'
예약되지 않은 포트의 모든 NFS 요청을 거부합니다	'vserver nfs modify -vserver vservice_name -nfs-rootonly enabled'

알 수 없는 **UNIX** 사용자의 **ONTAP NTFS** 볼륨 또는 **qtree**에 대한 **NFS** 액세스를 처리합니다.

ONTAP가 NTFS 보안 스타일로 볼륨이나 qtree에 연결하려고 시도하는 UNIX 사용자를 식별할 수 없는 경우 사용자를 Windows 사용자에게 명시적으로 매핑할 수 없습니다. 보다 엄격한 보안을 위해 이러한 사용자에 대한 액세스를 거부하거나 모든 사용자에 대한 최소 액세스 수준을 보장하도록 ONTAP를 기본 Windows 사용자에게 매핑하도록 구성할 수 있습니다.

시작하기 전에

이 옵션을 활성화하려면 기본 Windows 사용자를 구성해야 합니다.

이 작업에 대해

UNIX 사용자가 NTFS 보안 스타일로 볼륨이나 qtree에 액세스하려고 할 경우 ONTAP에서 NTFS 권한을 올바르게 평가할 수 있도록 UNIX 사용자를 Windows 사용자에게 먼저 매핑해야 합니다. 그러나 ONTAP가 구성된 사용자 정보 이름 서비스 소스에서 UNIX 사용자의 이름을 찾을 수 없는 경우 UNIX 사용자를 특정 Windows 사용자에게 명시적으로 매핑할 수 없습니다. 다음과 같은 방법으로 이러한 알 수 없는 UNIX 사용자를 처리하는 방법을 결정할 수 있습니다.

- 알 수 없는 UNIX 사용자에 대한 액세스를 거부합니다.

이렇게 하면 모든 UNIX 사용자가 NTFS 볼륨이나 qtree에 액세스할 수 있도록 명시적 매핑이 요구되므로 보안이 더욱 강화됩니다.

- 알 수 없는 UNIX 사용자를 기본 Windows 사용자로 매핑합니다.

따라서 모든 사용자가 기본 Windows 사용자를 통해 NTFS 볼륨 또는 qtree에 대한 최소 액세스 수준을 얻을 수

있으므로 보안이 낮지만 편의성이 높아집니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

알 수 없는 UNIX 사용자에게 기본 Windows 사용자를 사용하려는 경우...	명령 입력...
활성화됨	'vserver nfs modify -vserver vserver_name -map -unknown -uid -to -default-windows-user enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -map -unknown -uid -to -default-windows-user disabled'

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

예약되지 않은 포트에서 **ONTAP NFS** 내보내기를 마운트하는 클라이언트에 대한 고려 사항

'-mount-rootonly' 옵션은 사용자가 루트로 로그인한 경우에도 예약되지 않은 포트를 사용하여 NFS 내보내기를 마운트하는 클라이언트를 지원해야 하는 스토리지 시스템에서 해제되어야 합니다. 이러한 클라이언트에는 Hummingbird 클라이언트와 Solaris NFS/IPv6 클라이언트가 포함됩니다.

'-mount-rootonly' 옵션이 설정된 경우 ONTAP는 예약되지 않은 포트를 사용하는 NFS 클라이언트가 허용되지 않습니다. 즉, 번호가 1,023보다 큰 포트를 사용하여 NFS 내보내기를 마운트할 수 있습니다.

ONTAP NFS SVM에 대한 도메인을 확인하여 넷그룹에 대한 보다 엄격한 액세스 검사를 수행합니다.

기본적으로 ONTAP는 넷그룹에 대한 클라이언트 액세스를 평가할 때 추가 검증을 수행합니다. 추가 검사를 통해 클라이언트 도메인이 SVM(스토리지 가상 머신)의 도메인 구성과 일치하는지 확인합니다. 그렇지 않으면 ONTAP는 클라이언트 액세스를 거부합니다.

이 작업에 대해

ONTAP에서 클라이언트 액세스에 대한 익스포트 정책 규칙을 평가하고 익스포트 정책 규칙에 넷그룹이 포함되어 있는 경우, ONTAP는 클라이언트의 IP 주소가 넷그룹에 속하는지 여부를 결정해야 합니다. 이를 위해 ONTAP는 DNS를 사용하여 클라이언트의 IP 주소를 호스트 이름으로 변환하고 FQDN(정규화된 도메인 이름)을 얻습니다.

넷그룹 파일에 호스트에 대한 짧은 이름만 나열되고 호스트에 대한 짧은 이름이 여러 도메인에 있는 경우 다른 도메인의 클라이언트가 이 검사 없이 액세스할 수 있습니다.

이를 방지하기 위해 ONTAP는 호스트의 DNS에서 반환된 도메인을 SVM용으로 구성된 DNS 도메인 이름 목록과 비교합니다. 일치하는 경우 액세스가 허용됩니다. 일치하지 않으면 액세스가 거부됩니다.

이 검증은 기본적으로 활성화되어 있습니다. 고급 권한 수준에서 사용할 수 있는 '-netgroup-dns-domain-search' 매개 변수를 수정하여 이 매개 변수를 관리할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

넷그룹에 대한 도메인 확인을 원할 경우...	입력...
활성화됨	'vserver nfs modify -vserver vserver_name -netgroup -dns -domain -search enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -netgroup -dns -domain -search disabled'

3. 권한 수준을 admin으로 설정합니다.

'Set-Privilege admin'입니다

ONTAP SVM의 NFSv3 서비스에 사용되는 포트 수정

스토리지 시스템의 NFS 서버에서는 마운트 데몬, Network Lock Manager 등의 서비스를 사용하여 특정 기본 네트워크 포트를 통해 NFS 클라이언트와 통신합니다. 대부분의 NFS 환경에서 기본 포트는 올바르게 작동하고 수정할 필요가 없지만, NFSv3 환경에서 다른 NFS 네트워크 포트를 사용하려는 경우에는 변경할 수 있습니다.

시작하기 전에

스토리지 시스템에서 NFS 포트를 변경하려면 모든 NFS 클라이언트가 시스템에 다시 연결해야 하므로 먼저 이 정보를 사용자에게 전달해야 합니다.

이 작업에 대해

각 SVM(스토리지 가상 머신)에 대해 NFS 마운트 데몬, Network Lock Manager, Network Status Monitor, NFS 할당량 데몬 서비스에서 사용하는 포트를 설정할 수 있습니다. 포트 번호 변경은 TCP 및 UDP를 통해 데이터에 액세스하는 NFS 클라이언트에 영향을 줍니다.

NFSv4 및 NFSv4.1의 포트는 변경할 수 없습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. NFS에 대한 액세스 해제:

'vserver nfs modify -vserver vserver_name -access false'

3. 특정 NFS 서비스의 NFS 포트를 설정합니다.

'vserver nfs modify -vserver vs1 vs1_namenfs_port_parameterport_number'

NFS 포트 매개 변수입니다	설명	기본 포트입니다
'- mountd-port'입니다	NFS 마운트 데몬입니다	635
'`NLM-PORT'	네트워크 잠금 관리자	4045
'-NSM-port'입니다	네트워크 상태 모니터	4046
'`rquotad-port`'	NFS 할당량 데몬입니다	4049

기본 포트 이외에 허용되는 포트 번호 범위는 1024 ~ 65535입니다. 각 NFS 서비스는 고유한 포트를 사용해야 합니다.

4. NFS에 대한 액세스 설정:

'vserver nfs modify -vserver vs1 -access TRUE'

5. 'network connections listening show' 명령어를 이용하여 포트 번호 변화를 확인한다.

에 대한 자세한 내용은 network connections listening show ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

6. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 NFS 마운트 데몬 포트가 1113으로 설정됩니다.

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster           cluster1-01_clus_1:7700        TCP/ctlopccp
vs1               data1:4046                   TCP/sm
vs1               data1:4046                   UDP/sm
vs1               data1:4045                   TCP/nlm-v4
vs1               data1:4045                   UDP/nlm-v4
vs1               data1:1113                   TCP/mount
vs1               data1:1113                   UDP/mount
...
vs1::*> set -privilege admin

```

NFS 서버를 관리하기 위한 **ONTAP** 명령입니다

NFS 서버를 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
NFS 서버를 생성합니다	'vserver nfs create'
NFS 서버를 표시합니다	'vserver nfs show'
NFS 서버를 수정합니다	'vserver nfs modify(가상 NFS 수정)'
NFS 서버를 삭제합니다	'vserver nfs delete'

NFSv3 마운트 지점 아래에 있는 '.snapshot' 디렉토리를 숨깁니다	'-v3-hide-snapshot' 옵션이 활성화된 'vserver nfs' 명령입니다
 이 옵션을 사용하는 경우에도 '.snapshot' 디렉토리에 대한 명시적 액세스는 계속 허용됩니다.	

에 대한 자세한 내용은 `vserver nfs` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

ONTAP NAS SVM의 이름 서비스 문제 해결

클라이언트가 이름 서비스 문제로 인해 액세스 오류가 발생하는 경우, 'vserver services name-service getxxbyy' 명령 제품군을 사용하여 다양한 이름 서비스 조회를 수동으로 수행하고 조회에 대한 세부 정보와 결과를 확인하여 문제 해결에 도움이 될 수 있습니다.

이 작업에 대해

- 각 명령에 대해 다음을 지정할 수 있습니다.

- 조회를 수행할 노드 또는 SVM(스토리지 가상 머신)의 이름입니다.

이를 통해 특정 노드 또는 SVM에 대한 네임 서비스 조회를 테스트하여 잠재적 네임 서비스 구성 문제에 대한 검색 범위를 좁힐 수 있습니다.

- 조회에 사용된 소스를 표시할지 여부를 나타냅니다.

이를 통해 올바른 소스가 사용되었는지 확인할 수 있습니다.

- ONTAP는 구성된 이름 서비스 스위치 순서에 따라 조회를 수행하기 위한 서비스를 선택합니다.
- 이러한 명령은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

를 검색하려면...	명령 사용...
호스트 이름의 IP 주소입니다	'vserver services name-service getxxyy getaddrinfo'"vserver services name-service getxxyy gethostbyname'(IPv4 주소만 해당)
그룹 ID별 그룹 구성원	'vserver services name-service getxxyy getgrbygid'
그룹 이름으로 그룹의 구성원	'vserver services name-service getxxyy getgrbyname'
사용자가 속한 그룹 목록입니다	'vserver services name-service getxxyy getgrlist'

IP 주소의 호스트 이름입니다	'vserver services name-service getxxbyyy GetNameInfo"vserver services name-service getxxyy gethostbyaddr'(IPv4 주소만)
사용자 이름별 사용자 정보	'vserver services name-service getxxbyyy getpwbyname' '-use-RBAC' 매개변수를 TRUE로 지정하여 RBAC 사용자의 이름 확인을 테스트할 수 있습니다.
사용자 ID별 사용자 정보	'vserver services name-service getxxbyyy getpwbyuid' '-use-RBAC' 매개 변수를 true로 지정하여 RBAC 사용자의 이름 확인을 테스트할 수 있습니다.
클라이언트의 넷그룹 구성원 자격	'vserver services name-service getxxbyyy netgrp'
Netgroup-by-host 검색을 사용하는 클라이언트의 넷그룹 구성원 자격	'vserver services name-service getxxbyyy netgrpbyhost'

다음 예에서는 acast1.eng.example.com 호스트의 IP 주소를 획득하여 SVM VS1 에 대한 DNS 조회 테스트를 보여 줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

다음 예에서는 UID 501768을 가진 사용자의 사용자 정보를 검색함으로써 SVM VS1 에 대한 NIS 조회 테스트를 보여 줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

다음 예제는 이름이 ldap1인 사용자의 사용자 정보를 검색함으로써 SVM VS1 에 대한 LDAP 조회 테스트를 보여줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

다음 예에서는 클라이언트 dnshost0이 넷그룹 lnetgroup136의 구성원인지 여부를 확인함으로써 SVM V1에 대한 넷그룹 조회 테스트를 보여 줍니다.

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 수행한 테스트의 결과를 분석하고 필요한 조치를 취합니다.

만약...	다음을 확인하십시오.
호스트 이름 또는 IP 주소 조회에 실패했거나 잘못된 결과가 발생했습니다	DNS 구성
조회가 잘못된 소스를 쿼리했습니다	네임 서비스 스위치 구성
사용자 또는 그룹 조회에 실패했거나 잘못된 결과가 발생했습니다	• 네임 서비스 스위치 구성 • 소스 구성(로컬 파일, NIS 도메인, LDAP 클라이언트) • 네트워크 구성(예: LIF 및 라우트)
호스트 이름 조회가 실패했거나 시간이 초과되었으며 DNS 서버가 DNS 짧은 이름(예: host1)을 확인하지 않습니다.	최상위 도메인(TLD) 쿼리에 대한 DNS 구성 vserver services name-service dns modify 명령에 대한 '-is-tld-query-enabled false' 옵션을 사용하여 TLD 쿼리를 비활성화할 수 있습니다.

관련 정보

"NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

ONTAP NAS SVM에 대한 이름 서비스 연결 확인

DNS 및 LDAP(Lightweight Directory Access Protocol) 이름 서버를 확인하여 ONTAP 에 연결되어 있는지 확인할 수 있습니다. 이러한 명령은 admin 권한 수준에서 사용할 수 있습니다.

이 작업에 대해

이름 서비스 구성 검사기를 사용하여 필요에 따라 유효한 DNS 또는 LDAP 네임 서비스 구성을 확인할 수 있습니다. 이러한 검증 검사는 명령줄 또는 System Manager에서 시작할 수 있습니다.

DNS 구성의 경우 모든 서버가 테스트되고 유효한 구성으로 간주되려면 해당 구성이 제대로 작동되어야 합니다. LDAP 구성의 경우 서버가 가동되는 한 구성이 유효합니다. 'ip-config-validation' 필드가 true(기본값 false)가 아닌 경우 이름 서비스 명령은 구성 검사기를 적용합니다.

단계

1. 적절한 명령을 사용하여 네임 서비스 구성을 확인합니다. UI는 구성된 서버의 상태를 표시합니다.

확인하려면...	이 명령 사용...
DNS 구성 상태입니다	'vserver services name-service dns check'
LDAP 구성 상태입니다	'vserver services name-service ldap check'

```
cluster1::> vserver services name-service dns check -vserver vs0
```

Vserver	Name Server	Status	Status Details
vs0	10.11.12.13	up	Response time (msec): 55
vs0	10.11.12.14	up	Response time (msec): 70
vs0	10.11.12.15	down	Connection refused.

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```
| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13". |
```

구성된 서버 중 하나(name-servers/ldap-servers)에 연결할 수 있고 서비스를 제공하는 경우 구성 검증이 성공적으로 수행됩니다. 일부 서버에 연결할 수 없는 경우 경고가 표시됩니다.

NAS 이름 서비스 스위치 항목을 관리하기 위한 ONTAP 명령

이름 서비스 스위치 항목은 생성, 표시, 수정 및 삭제하여 관리할 수 있습니다.

원하는 작업	이 명령 사용...
이름 서비스 스위치 항목을 생성합니다	'vserver services name-service ns-switch create'
이름 서비스 스위치 항목을 표시합니다	'vserver services name-service ns-switch show'
이름 서비스 스위치 항목을 수정합니다	'vserver services name-service ns-switch modify'를 참조하십시오
이름 서비스 스위치 항목을 삭제합니다	'vserver services name-service ns-switch delete'

에 대한 자세한 내용은 `vserver services name-service ns-switch` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

관련 정보

["NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"](#)

NAS 이름 서비스 캐시를 관리하기 위한 ONTAP 명령

TTL(Time To Live) 값을 수정하여 이름 서비스 캐시를 관리할 수 있습니다. TTL 값은 이름 서비스 정보가 캐시에 지속되는 기간을 결정합니다.

TTL 값을 수정하려는 경우...	이 명령 사용...
Unix 사용자	'vserver services name-service cache unix-user settings'
Unix 그룹	'vserver services name-service cache unix-group settings'
Unix 넷그룹	'vserver services name-service cache netgroups settings'(SVM 서비스 이름 서비스 캐시 넷그룹 설정)
호스트	'vserver services name-service cache hosts settings'(SVM 서비스 이름 서비스 캐시 호스트 설정)
그룹 구성원 자격	'vserver services name-service cache group-membership settings'

관련 정보

["ONTAP 명령 참조입니다"](#)

NFS 이름 매핑을 관리하기 위한 ONTAP 명령

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
이름 매핑을 생성합니다	<code>vserver name-mapping create</code>
특정 위치에 이름 매핑을 삽입합니다	<code>vserver name-mapping insert</code>
이름 매핑을 표시합니다	<code>vserver name-mapping show</code>
두 이름 매핑의 위치를 교환합니다. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	<code>vserver name-mapping swap</code>
이름 매핑을 수정합니다	<code>vserver name-mapping modify</code>
이름 매핑을 삭제합니다	<code>vserver name-mapping delete</code>
올바른 이름 매핑을 확인합니다	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

에 대한 자세한 내용은 `vserver name-mapping` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NAS 로컬 UNIX 사용자를 관리하기 위한 ONTAP 명령

로컬 UNIX 사용자를 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
로컬 UNIX 사용자를 생성합니다	' <code>vserver services name-service unix-user create</code> '를 참조하십시오
URI에서 로컬 UNIX 사용자를 로드합니다	' <code>vserver services name-service unix-user load-from-uri</code> '
로컬 UNIX 사용자를 표시합니다	' <code>vserver services name-service unix-user show</code> '를 참조하십시오
로컬 UNIX 사용자를 수정합니다	' <code>vserver services name-service unix-user modify</code> '를 참조하십시오
로컬 UNIX 사용자를 삭제합니다	' <code>vserver services name-service unix-user delete</code> '

에 대한 자세한 내용은 `vserver services name-service unix-user` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NAS 로컬 UNIX 그룹을 관리하기 위한 ONTAP 명령

로컬 UNIX 그룹을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
로컬 UNIX 그룹을 생성합니다	'vserver services name-service unix-group create'를 참조하십시오
로컬 UNIX 그룹에 사용자를 추가합니다	'vserver services name-service unix-group adduser'
URI에서 로컬 UNIX 그룹을 로드합니다	가상 서버 서비스 이름 서비스 unix-group load-from-uri
로컬 UNIX 그룹을 표시합니다	'vserver services name-service unix-group show'를 참조하십시오
로컬 UNIX 그룹을 수정합니다	'vserver services name-service unix-group modify'를 참조하십시오
로컬 UNIX 그룹에서 사용자를 삭제합니다	'vserver services name-service unix-group deluser'
로컬 UNIX 그룹을 삭제합니다	'vserver services name-service unix-group delete'

에 대한 자세한 내용은 `vserver services name-service unix-group` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

ONTAP NFS SVM의 로컬 UNIX 사용자, 그룹 및 그룹 멤버에 대한 제한

ONTAP는 클러스터의 최대 UNIX 사용자 및 그룹 수와 이러한 제한을 관리하는 명령에 대한 제한을 도입했습니다. 이러한 제한을 사용하면 관리자가 클러스터에 너무 많은 로컬 UNIX 사용자 및 그룹을 생성하지 못하도록 하여 성능 문제를 방지할 수 있습니다.

로컬 UNIX 사용자 그룹 및 그룹 구성원의 총 수에 대한 제한이 있습니다. 로컬 UNIX 사용자에게는 별도의 제한이 있습니다. 제한은 클러스터 전반에 적용됩니다. 이러한 각 새 제한은 미리 할당된 하드 제한까지 수정할 수 있는 기본값으로 설정됩니다.

데이터베이스	기본 제한	엄격한 제한
로컬 UNIX 사용자	32,768입니다	65,536
로컬 UNIX 그룹 및 그룹 구성원	32,768입니다	65,536

ONTAP NFS SVM에 대한 로컬 UNIX 사용자 및 그룹에 대한 제한 관리

로컬 UNIX 사용자 및 그룹에 대한 제한을 관리하기 위한 특정 ONTAP 명령이 있습니다. 클러스터 관리자는 이러한 명령을 사용하여 과도한 수의 로컬 UNIX 사용자 및 그룹과 관련된 것으로 여겨지는 클러스터의 성능 문제를 해결할 수 있습니다.

이 작업에 대해

이러한 명령은 클러스터 관리자가 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 사용...
로컬 UNIX 사용자 제한에 대한 정보를 표시합니다	'vserver services unix-user max-limit show'를 선택합니다
로컬 UNIX 그룹 제한에 대한 정보를 표시합니다	'vserver services unix-group max-limit show'를 선택합니다
로컬 UNIX 사용자 제한을 수정합니다	'vserver services unix-user max-limit modify'를 참조하십시오
로컬 UNIX 그룹 제한을 수정합니다	'vserver services unix-group max-limit modify'를 참조하십시오

에 대한 자세한 내용은 `vserver services unix` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NFS 로컬 넷그룹을 관리하기 위한 ONTAP 명령

로컬 넷그룹을 URI에서 로드하고, 노드 간에 상태를 확인하고, 표시하고, 삭제하여 관리할 수 있습니다.

원하는 작업	명령 사용...
URI에서 넷그룹을 로드합니다	'vserver services name-service netgroup load'
전체 노드에서 넷그룹의 상태를 확인합니다	'vserver services name-service netgroup status' 고급 권한 수준에서 사용할 수 있습니다.
로컬 넷그룹을 표시합니다	'vserver services name-service netgroup file show'를 참조하십시오
로컬 넷그룹을 삭제합니다	'vserver services name-service 넷그룹 파일 삭제'

에 대한 자세한 내용은 `vserver services name-service netgroup file` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NFS NIS 도메인 구성을 관리하기 위한 ONTAP 명령

NIS 도메인 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
NIS 도메인 구성을 생성합니다	'vserver services name-service nis-domain create'를 참조하십시오

NIS 도메인 구성을 표시합니다	'vserver services name-service NIS-domain show'를 참조하십시오
NIS 도메인 구성의 바인딩 상태를 표시합니다	'vserver services name-service nis-domain show-bound'
NIS 통계를 표시합니다	고급 권한 수준 이상에서 사용할 수 있는 SVM 서비스 이름 서비스 NIS-도메인 표시-통계.
NIS 통계를 지웁니다	고급 권한 수준 이상에서 사용할 수 있는 SVM 서비스 이름 서비스 NIS-도메인 지우기-통계.
NIS 도메인 구성을 수정합니다	'vserver services name-service NIS-domain modify'를 참조하십시오
NIS 도메인 구성을 삭제합니다	'vserver services name-service nis-domain delete'
호스트 별 넷그룹 검색에 대한 캐싱을 설정합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service NIS-domain netgroup-database config modify'입니다.

에 대한 자세한 내용은 `vserver services name-service nis-domain` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NFS LDAP 클라이언트 구성을 관리하기 위한 ONTAP 명령

LDAP 클라이언트 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.



SVM 관리자는 클러스터 관리자가 생성한 LDAP 클라이언트 구성을 수정하거나 삭제할 수 없습니다.

원하는 작업	이 명령 사용...
LDAP 클라이언트 구성을 생성합니다	'vserver services name-service ldap client create'
LDAP 클라이언트 구성을 표시합니다	'vserver services name-service ldap client show'
LDAP 클라이언트 구성을 수정합니다	'vserver services name-service ldap client modify'를 참조하십시오
LDAP 클라이언트 바인딩 암호를 변경합니다	'vserver services name-service ldap client modify-bind-password'
LDAP 클라이언트 구성을 삭제합니다	'vserver services name-service ldap client delete'

에 대한 자세한 내용은 `vserver services name-service ldap client` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NFS LDAP 구성을 관리하기 위한 ONTAP 명령

LDAP 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
LDAP 구성을 생성합니다	'vserver services name-service ldap create'
LDAP 구성을 표시합니다	'vserver services name-service ldap show'
LDAP 구성을 수정합니다	'vserver services name-service ldap modify'를 참조하십시오
LDAP 구성을 삭제합니다	'vserver services name-service ldap delete'

에 대한 자세한 내용은 `vserver services name-service ldap` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NFS LDAP 클라이언트 스키마 템플릿을 관리하기 위한 ONTAP 명령

LDAP 클라이언트 스키마 템플릿을 관리하기 위한 특정 ONTAP 명령이 있습니다.



SVM 관리자는 클러스터 관리자가 생성한 LDAP 클라이언트 스키마를 수정하거나 삭제할 수 없습니다.

원하는 작업	이 명령 사용...
기존 LDAP 스키마 템플릿을 복사합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 복사'입니다.
LDAP 스키마 템플릿을 표시합니다	'vserver services name-service ldap client schema show'를 참조하십시오
LDAP 스키마 템플릿을 수정합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 수정'입니다.
LDAP 스키마 템플릿을 삭제합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 삭제'입니다.

에 대한 자세한 내용은 `vserver services name-service ldap client schema` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NFS Kerberos 인터페이스 구성을 관리하기 위한 ONTAP 명령

NFS Kerberos 인터페이스 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...

LIF에서 NFS Kerberos를 사용하도록 설정합니다	'vserver NFS Kerberos interface enable'
NFS Kerberos 인터페이스 구성을 표시합니다	vserver nfs Kerberos interface show를 선택합니다
NFS Kerberos 인터페이스 구성을 수정합니다	가상 NFS Kerberos 인터페이스 수정
LIF에서 NFS Kerberos를 사용하지 않도록 설정합니다	'vserver NFS Kerberos interface disable'

에 대한 자세한 내용은 vserver nfs kerberos interface ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

NFS Kerberos 영역 구성을 관리하기 위한 ONTAP 명령

NFS Kerberos 영역 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
NFS Kerberos 영역 구성을 생성합니다	'vserver NFS Kerberos 영역 생성'
NFS Kerberos 영역 구성을 표시합니다	가상 NFS Kerberos 영역 표시
NFS Kerberos 영역 구성을 수정합니다	가상 NFS Kerberos 영역 수정
NFS Kerberos 영역 구성을 삭제합니다	'vserver NFS Kerberos 영역 삭제'

에 대한 자세한 내용은 vserver nfs kerberos realm ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

수출 정책 관리를 위한 ONTAP 명령

내보내기 정책을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
엑스포트 정책에 대한 정보를 표시합니다	vserver export-policy show를 참조하십시오
엑스포트 정책의 이름을 바꿉니다	'vserver export-policy rename'
엑스포트 정책을 복사합니다	'vserver export-policy copy'
엑스포트 정책을 삭제합니다	'vserver export-policy delete'

에 대한 자세한 내용은 `vserver export-policy` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

내보내기 규칙 관리를 위한 **ONTAP** 명령

내보내기 규칙을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
엑스포트 규칙을 생성합니다	'vserver export-policy rule create'
내보내기 규칙에 대한 정보를 표시합니다	'vserver export-policy rule show'를 선택합니다
엑스포트 규칙을 수정합니다	'vserver export-policy rule modify'입니다
엑스포트 규칙을 삭제합니다	'vserver export-policy rule delete'



서로 다른 클라이언트와 일치하는 동일한 내보내기 규칙을 여러 개 구성한 경우 내보내기 규칙을 관리할 때 해당 규칙을 동기화 상태로 유지해야 합니다.

에 대한 자세한 내용은 `vserver export-policy` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NFS 자격 증명 캐시를 구성합니다

ONTAP SVM의 **NFS** 자격 증명 캐시 **TTL**(수명)을 수정하는 이유

ONTAP는 보다 빠른 액세스를 제공하고 성능을 향상시키기 위해 자격 증명 캐시를 사용하여 NFS 내보내기 액세스에 대한 사용자 인증에 필요한 정보를 저장합니다. 자격 증명 캐시에 정보가 저장되는 기간을 구성하여 사용자 환경에 맞게 정보를 사용자 지정할 수 있습니다.

NFS 자격 증명 캐시 TTL(Time-to-Live)을 수정하면 문제를 해결하는 데 도움이 되는 몇 가지 시나리오가 있습니다. 이러한 시나리오가 무엇인지, 그리고 이러한 수정 결과로 초래되는 결과를 이해해야 합니다.

이유

다음과 같은 경우 기본 TTL을 변경하십시오.

문제	구제 조치
사용자 환경의 네임 서버에서 ONTAP의 요청 로드가 높기 때문에 성능이 저하됩니다.	캐시된 양의 자격 증명과 음의 자격 증명에 대한 TTL을 늘려 ONTAP에서 이름 서버로 보내는 요청 수를 줄입니다.
이름 서버 관리자가 이전에 거부된 NFS 사용자에게 대한 액세스를 허용하도록 변경되었습니다.	캐시된 음수 자격 증명에 대한 TTL을 줄여 NFS 사용자가 외부 이름 서버에서 새 자격 증명을 요청할 때까지 ONTAP를 기다려야 하는 시간을 줄임으로써 액세스 권한을 얻을 수 있습니다.

문제	구제 조치
이름 서버 관리자가 이전에 허용된 NFS 사용자에게 대한 액세스를 거부하도록 변경되었습니다.	캐시된 양의 자격 증명에 대한 TTL을 줄여 ONTAP가 외부 이름 서버에서 새 자격 증명을 요청하는 시간을 줄임으로써 NFS 사용자가 액세스를 거부하도록 합니다.

결과

양의 자격 증명과 음수 자격 증명을 캐시하기 위해 시간을 개별적으로 수정할 수 있습니다. 그러나 그렇게 할 때의 장단점을 모두 알아야 합니다.

만약...	장점은...	단점은...
양의 자격 증명 캐시 시간을 늘립니다	ONTAP는 이름 서버에 자격 증명 요청을 덜 자주 전송하여 이름 서버의 부하를 줄입니다.	이전에는 액세스가 허용되었지만 더 이상 허용되지 않았던 NFS 사용자에게 대한 액세스를 거부하는 데 시간이 더 오래 걸립니다.
양의 자격 증명 캐시 시간을 줄입니다	이전에는 액세스가 허용되었지만 이제는 그렇지 않은 NFS 사용자에게 대한 액세스를 거부하는 데 걸리는 시간이 더 적게 걸립니다.	ONTAP는 이름 서버에 자격 증명 요청을 더 자주 전송하여 이름 서버의 로드를 증가시킵니다.
부정적인 자격 증명 캐시 시간을 늘립니다	ONTAP는 이름 서버에 자격 증명 요청을 덜 자주 전송하여 이름 서버의 부하를 줄입니다.	이전에는 액세스가 허용되지 않았지만 지금은 NFS 사용자에게 액세스 권한을 부여하는 데 시간이 더 오래 걸립니다.
부정적인 자격 증명 캐시 시간을 줄입니다	이전에는 액세스가 허용되지 않았지만 지금은 NFS 사용자에게 액세스 권한을 부여하는 데 시간이 더 적게 걸립니다.	ONTAP는 이름 서버에 자격 증명 요청을 더 자주 전송하여 이름 서버의 로드를 증가시킵니다.

ONTAP SVM에 대한 캐시된 NFS 사용자 자격 증명의 수명 구성

SVM(스토리지 가상 시스템)의 NFS 서버를 수정하여 ONTAP에서 NFS 사용자에게 대한 자격 증명을 내부 캐시(TTL(Time-to-Live)에 저장하는 시간을 구성할 수 있습니다. 따라서 네임 서버의 높은 부하나 NFS 사용자 액세스에 영향을 미치는 자격 증명의 변경과 관련된 특정 문제를 완화할 수 있습니다.

이 작업에 대해

이러한 매개 변수는 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

캐싱된 TTL을 수정하려는 경우...	명령 사용...
양의 자격 증명	<pre>'vserver nfs modify -vserver vservice_name -cached -cred -positive -ttl time_to_live'</pre> TTL은 밀리초 단위로 측정됩니다. ONTAP 9.10.1 이상부터 기본값은 1시간(3,600,000밀리초)입니다. ONTAP 9.9.1 이하 버전의 경우 기본값은 24시간(86,400,000밀리초)입니다. 이 값에 허용되는 범위는 1분(60000밀리초)~7일(604,800,000밀리초)입니다.
음수 자격 증명	<pre>'vserver nfs modify -vserver vservice_name -cached -cred -negative -tl time_to_live'</pre> TTL은 밀리초 단위로 측정됩니다. 기본값은 2시간(7,200,000밀리초)입니다. 이 값에 허용되는 범위는 1분(60000밀리초)~7일(604,800,000밀리초)입니다.

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

엑스포트 정책 캐시 관리

ONTAP NAS SVM에 대한 내보내기 정책 캐시 플러시

ONTAP는 빠른 액세스를 위해 여러 엑스포트 정책 캐시를 사용하여 엑스포트 정책과 관련된 정보를 저장합니다. 내보내기 정책 캐시를 수동으로 플러싱하면('vserver export-policy cache flush') 오래된 정보가 제거되고 ONTAP가 적절한 외부 리소스에서 현재 정보를 검색하도록 합니다. 이렇게 하면 NFS 내보내기에 대한 클라이언트 액세스와 관련된 다양한 문제를 해결할 수 있습니다.

이 작업에 대해

다음과 같은 이유로 인해 엑스포트 정책 캐시 정보가 오래된 것일 수 있습니다.

- 정책 규칙을 내보내기 위한 최근 변경 사항
- 이름 서버의 호스트 이름 레코드에 대한 최근 변경 사항
- 이름 서버의 넷그룹 항목에 대한 최근 변경 사항
- 네트워크 중단 상태에서 복구되어 넷그룹이 완전히 로드되지 않았습니다

단계

1. 이름 서비스 캐시를 사용하지 않는 경우 다음 작업 중 하나를 고급 권한 모드에서 수행합니다.

플러시를 원하는 경우...	명령 입력...
모든 익스포트 정책 캐시(Showmount 제외)	'vserver export-policy cache flush-vserver vserver_name'
익스포트 정책 규칙 액세스 캐시	'vserver export-policy cache flush-vserver vserver_name-cache access'는 선택 사항인 '-node' 매개변수를 포함하여 액세스 캐시를 플러시할 노드를 지정할 수 있습니다.
호스트 이름 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache host'
넷그룹 캐시입니다	넷그룹의 처리는 리소스를 많이 소모하는 작업입니다. 오래된 넷그룹으로 인해 발생하는 클라이언트 액세스 문제를 해결하려는 경우에만 넷그룹 캐시를 플러시해야 합니다.
showmount 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache showmount'

2. 이름 서비스 캐시가 활성화된 경우 다음 작업 중 하나를 수행합니다.

플러시를 원하는 경우...	명령 입력...
익스포트 정책 규칙 액세스 캐시	'vserver export-policy cache flush-vserver vserver_name-cache access'는 선택 사항인 '-node' 매개변수를 포함하여 액세스 캐시를 플러시할 노드를 지정할 수 있습니다.
호스트 이름 캐시입니다	'vserver services name-service cache hosts forward-lookup delete-all'
넷그룹 캐시입니다	SVM 서비스 이름-서비스 캐시 넷그룹 IP-넷그룹 삭제-모두 SVM 서비스 이름-서비스 캐시 넷그룹 구성원 삭제-모두(All) 넷그룹 처리는 리소스를 많이 소모합니다. 오래된 넷그룹으로 인해 발생하는 클라이언트 액세스 문제를 해결하려는 경우에만 넷그룹 캐시를 플러시해야 합니다.
showmount 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache showmount'

ONTAP NFS SVM에 대한 내보내기 정책 **netgroup** 대기열 및 캐시 표시

ONTAP는 넷그룹 큐를 가져와 확인할 때 넷그룹 큐를 사용하고 넷그룹 캐시를 사용하여 결과 정보를 저장합니다. 익스포트 정책 넷그룹 관련 문제를 해결할 때 'vserver export-policy netgroup queue show' 및 'vserver export-policy netgroup cache show' 명령을 사용하여

넷그룹 큐의 상태와 넷그룹 캐시의 내용을 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

엑스포트 정책 넷그룹을 표시하려면...	명령 입력...
대기열	'vserver export-policy netgroup queue show'를 선택합니다
캐시	'vserver export-policy netgroup cache show -vserver vservice_name'을 선택합니다

에 대한 자세한 내용은 `vserver export-policy netgroup` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

클라이언트 IP 주소가 **ONTAP NFS** 넷그룹의 멤버인지 확인하세요.

넷그룹과 관련된 NFS 클라이언트 액세스 문제를 해결할 때 'vserver export-policy netgroup check-membership' 명령을 사용하여 클라이언트 IP가 특정 넷그룹의 구성원인지 여부를 확인할 수 있습니다.

이 작업에 대해

넷그룹 구성원 자격을 확인하면 ONTAP가 클라이언트가 넷그룹의 구성원인지 여부를 확인할 수 있습니다. 또한 넷그룹 정보를 새로 고치는 동안 ONTAP 넷그룹 캐시가 임시 상태인지 여부를 알 수 있습니다. 이 정보는 클라이언트가 예기치 않게 액세스 권한을 부여받거나 거부되는 이유를 이해하는 데 도움이 될 수 있습니다.

단계

1. 클라이언트 IP 주소의 넷그룹 멤버십을 확인합니다. 'vserver export-policy netgroup check-membership-vserver vservice_name-netgroup netgroup_name-client-ip client_ip'

명령을 실행하면 다음 결과가 반환될 수 있습니다.

- 클라이언트가 넷그룹의 구성원입니다.

역방향 조회 검사 또는 호스트 별 넷그룹 검색을 통해 확인되었습니다.

- 클라이언트가 넷그룹의 구성원입니다.

ONTAP 넷그룹 캐시에서 발견되었습니다.

- 클라이언트가 넷그룹의 구성원이 아닙니다.
- ONTAP가 현재 넷그룹 캐시를 새로 고치고 있기 때문에 클라이언트의 구성원을 확인할 수 없습니다.

이 작업이 수행되지 않을 때까지 멤버 자격은 명시적으로 배제될 수 없습니다. 'vserver export-policy netgroup queue show' 명령을 사용하여 넷그룹의 로드를 모니터링하고 작업이 완료된 후 검사를 다시 시도하십시오.

예

다음 예에서는 IP 주소가 172.17.16.72인 클라이언트가 SVM VS1 에 있는 넷그룹 수은의 구성원인지 여부를

확인합니다.

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup mercury -client-ip 172.17.16.72
```

ONTAP NFS SVM에 대한 액세스 캐시 성능 최적화

여러 매개 변수를 구성하여 액세스 캐시를 최적화하고 성능과 액세스 캐시에 저장된 정보의 현재 상태 간에 적절한 균형을 찾을 수 있습니다.

이 작업에 대해

액세스 캐시 새로 고침 기간을 구성할 때는 다음 사항을 염두에 두십시오.

- 값이 높을수록 액세스 캐시에서 항목이 더 오래 유지됩니다.

ONTAP는 액세스 캐시 항목을 새로 고치는 데 리소스를 적게 사용하기 때문에 성능이 향상됩니다. 단점은 익스포트 정책 규칙이 변경되고 액세스 캐시 항목이 오래되면 업데이트하는 데 시간이 오래 걸린다는 것입니다. 따라서 액세스를 받아야 하는 클라이언트가 거부되고 거부되어야 하는 클라이언트가 액세스할 수 있습니다.

- 값이 낮을수록 ONTAP에서 액세스 캐시 항목을 더 자주 새로 고칩니다.

장점은 항목이 더 최신 항목이고 클라이언트가 올바르게 액세스 권한을 부여하거나 거부될 가능성이 더 높다는 점입니다. 단점은 ONTAP에서 액세스 캐시 항목을 새로 고치는 데 더 많은 리소스를 사용하기 때문에 성능이 저하된다는 것입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

수정 방법	입력...
양의 항목에 대한 새로 고침 기간	'vserver export-policy access-cache config modify -all-vservers-refresh-period-positive timeout_value'
음수 항목의 새로 고침 기간	'vserver export-policy access-cache config modify -all-vservers-refresh-period-negative timeout_value'
이전 항목의 제한 시간	'vserver export-policy access-cache config modify -all-vservers-ab하비스트-timeout_value'

3. 새 매개 변수 설정을 확인합니다.

'vserver export-policy access-cache config show-all-vservers'

4. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

파일 잠금 관리

ONTAP NFS SVM의 프로토콜 간 파일 잠금에 대해 알아보세요.

파일 잠금은 사용자가 이전에 다른 사용자가 연 파일에 액세스하지 못하도록 클라이언트 응용 프로그램에서 사용하는 방법입니다. ONTAP가 파일을 잠그는 방법은 클라이언트의 프로토콜에 따라 다릅니다.

클라이언트가 NFS 클라이언트인 경우 잠금이 권고사항이고, 클라이언트가 SMB 클라이언트인 경우 잠금이 필수입니다.

NFS와 SMB 파일 잠금의 차이로 인해 NFS 클라이언트가 SMB 애플리케이션에서 이전에 연 파일에 액세스하지 못할 수 있습니다.

NFS 클라이언트가 SMB 애플리케이션에 의해 잠긴 파일에 액세스하려고 할 때 다음이 발생합니다.

- 혼합 볼륨 또는 NTFS 볼륨에서 rm, rmdir, mv 등의 파일 조작 작업으로 인해 NFS 응용 프로그램이 실패할 수 있습니다.
- NFS 읽기 및 쓰기 작업은 SMB 거부-읽기 및 거부-쓰기 열기 모드에 의해 각각 거부됩니다.
- 배타적 SMB bytelock로 파일의 쓰기 범위가 잠기면 NFS 쓰기 작업이 실패합니다.

UNIX 보안 스타일 볼륨에서 NFS 링크 해제 및 이름 바꾸기 작업은 SMB 잠금 상태를 무시하고 파일에 대한 액세스를 허용합니다. UNIX 보안 스타일 볼륨에서 다른 모든 NFS 작업은 SMB 잠금 상태를 존중합니다.

ONTAP NFS SVM의 읽기 전용 비트에 대해 알아보세요.

읽기 전용 비트는 파일을 쓰기 가능(사용 안 함)인지 읽기 전용(사용 가능)인지를 나타내기 위해 파일별로 설정됩니다.

Windows를 사용하는 SMB 클라이언트는 파일당 읽기 전용 비트를 설정할 수 있습니다. NFS 클라이언트는 파일당 읽기 전용 비트를 사용하는 프로토콜 작업이 없으므로 파일당 읽기 전용 비트를 설정하지 않습니다.

ONTAP는 Windows를 사용하는 SMB 클라이언트가 해당 파일을 생성할 때 파일에 읽기 전용 비트를 설정할 수 있습니다. 또한 ONTAP는 NFS 클라이언트와 SMB 클라이언트 간에 파일이 공유될 때 읽기 전용 비트를 설정할 수 있습니다. 일부 소프트웨어는 NFS 클라이언트 및 SMB 클라이언트에서 사용할 때 읽기 전용 비트를 사용하도록 설정해야 합니다.

ONTAP가 NFS 클라이언트와 SMB 클라이언트 간에 공유되는 파일에 대해 적절한 읽기 및 쓰기 권한을 유지하려면 다음 규칙에 따라 읽기 전용 비트를 처리합니다.

- NFS는 읽기 전용 비트가 설정된 파일을 쓰기 권한 비트가 설정되지 않은 것처럼 처리합니다.
- NFS 클라이언트가 모든 쓰기 권한 비트를 사용하지 않도록 설정하고 이전에 해당 비트 중 하나 이상이 활성화된 경우 ONTAP는 해당 파일에 대해 읽기 전용 비트를 설정합니다.
- NFS 클라이언트가 쓰기 권한 비트를 설정하면 ONTAP는 해당 파일에 대해 읽기 전용 비트를 해제합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 NFS 클라이언트가 해당 파일에 대한 권한을 검색하려고 하면 파일에 대한 권한 비트가 NFS 클라이언트로 전송되지 않고 ONTAP는 쓰기 권한 비트가 마스킹된 상태로 NFS 클라이언트에 사용 권한 비트를 전송합니다.

- 파일에 대한 읽기 전용 비트가 설정되어 있고 SMB 클라이언트가 읽기 전용 비트를 사용하지 않도록 설정한 경우 ONTAP는 해당 파일에 대한 소유자의 쓰기 권한 비트를 설정합니다.
- 읽기 전용 비트가 설정된 파일은 루트에서만 쓸 수 있습니다.

읽기 전용 비트는 다음과 같은 방식으로 ACL 및 Unix 모드 비트와 상호 작용합니다.

파일에 읽기 전용 비트가 설정된 경우:

- 해당 파일의 ACL에는 변경 사항이 없습니다. NFS 클라이언트는 읽기 전용 비트가 설정되기 전과 동일한 ACL을 보게 됩니다.
- 파일에 대한 쓰기 접근을 허용하는 모든 Unix 모드 비트는 무시됩니다.
- NFS와 SMB 클라이언트는 모두 파일을 읽을 수 있지만, 수정할 수는 없습니다.
- ACL 및 UNIX 모드 비트는 읽기 전용 비트 때문에 무시됩니다. 즉, ACL이 쓰기 액세스를 허용하더라도 읽기 전용 비트는 수정을 방지합니다.

파일에 읽기 전용 비트가 설정되지 않은 경우:

- ONTAP ACL 및 UNIX 모드 비트를 기반으로 액세스를 결정합니다.
 - ACL 또는 UNIX 모드 비트가 쓰기 액세스를 거부하는 경우 NFS 및 SMB 클라이언트는 파일을 수정할 수 없습니다.
 - ACL이나 UNIX 모드 비트가 쓰기 액세스를 거부하지 않으면 NFS 및 SMB 클라이언트가 파일을 수정할 수 있습니다.



파일 권한 변경은 SMB 클라이언트에 즉시 적용되지만 NFS 클라이언트가 특성 캐싱을 사용하는 경우 NFS 클라이언트에 즉시 적용되지 않을 수 있습니다.

ONTAP NFS와 Windows가 공유 경로 구성 요소의 잠금을 처리하는 방식이 어떻게 다른지 알아보세요.

Windows와 달리 ONTAP는 파일이 열려 있는 동안 열려 있는 파일에 대한 경로의 각 구성 요소를 잠그지 않습니다. 이 동작은 SMB 공유 경로에도 영향을 줍니다.

ONTAP는 경로의 각 구성 요소를 잠그지 않으므로 열려 있는 파일 또는 공유 위에 있는 경로 구성 요소의 이름을 바꿀 수 있습니다. 이렇게 하면 특정 응용 프로그램에 문제가 발생하거나 SMB 구성의 공유 경로가 잘못될 수 있습니다. 이로 인해 공유에 액세스할 수 없게 될 수 있습니다.

경로 구성 요소의 이름을 변경하여 발생하는 문제를 방지하기 위해 사용자 또는 응용 프로그램이 중요한 디렉터리의 이름을 바꾸지 못하도록 하는 Windows ACL(액세스 제어 목록) 보안 설정을 적용할 수 있습니다.

에 대해 자세히 알아보십시오 ["클라이언트가 액세스하는 동안 디렉토리의 이름을 변경하지 못하도록 하는 방법"](#).

ONTAP NFS SVM에 대한 잠금 정보 표시

현재 파일 잠금에 대한 정보를 표시할 수 있습니다. 여기에는 보유한 잠금의 유형 및 잠금 상태, 바이트 범위 잠금에 대한 세부 정보, 공유 잠금 모드, 위임 잠금 및 편의적 잠금, 잠금이 내구성 또는 지속 핸들로 열렸는지 여부 등이 포함됩니다.

이 작업에 대해

NFSv4 또는 NFSv4.1을 통해 설정된 잠금에 대해 클라이언트 IP 주소를 표시할 수 없습니다.

기본적으로 명령은 모든 잠금에 대한 정보를 표시합니다. 명령 매개 변수를 사용하여 특정 SVM(스토리지 가상 머신)의 잠금에 대한 정보를 표시하거나 명령의 출력을 다른 기준으로 필터링할 수 있습니다.

'vserver lock show' 명령은 네 가지 유형의 잠금에 대한 정보를 표시합니다.

- 바이트 범위 잠금 - 파일의 일부만 잠급니다.
- 공유 잠금 - 열린 파일을 잠급니다.
- SMB를 통한 클라이언트 측 캐싱을 제어하는 편의적 잠금 기능
- 위임 - NFSv4.x에서 클라이언트 측 캐싱을 제어합니다

선택적 매개 변수를 지정하면 각 잠금 유형에 대한 중요한 정보를 확인할 수 있습니다. 에 대한 자세한 내용은 `vserver locks show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 잠금에 대한 정보를 표시합니다.

예

다음 예에서는 '/vol1/file1' 경로가 있는 파일의 NFSv4 잠금에 대한 요약 정보를 표시합니다. sharelock 액세스 모드는 write-deny_none 이며, 잠금이 쓰기 위임과 함께 부여되었습니다.

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1                  lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation -
                                     Delegation Type: write
```

다음 예에서는 경로 '/data2/data2_2/intro.pptx'를 사용하여 파일의 SMB 잠금에 대한 자세한 oplock 및 sharelock 정보를 표시합니다. IP 주소가 10.3.1.3인 클라이언트에 write-deny_none의 공유 잠금 액세스 모드를 가진 파일에 내구성 있는 핸들이 부여됩니다. 배치 oplock 레벨이 있는 리스 oplock이 부여됩니다.

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
```

```
        Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: -
Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: durable
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

        Vserver: vs1
            Volume: data2_2
Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
        Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
    Lock Protocol: cifs
        Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: -
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

파일 잠금으로 인해 클라이언트가 파일에 액세스하지 못하는 경우 현재 보류된 잠금에 대한 정보를 표시한 다음 특정 잠금을 중단할 수 있습니다. 잠금을 해제해야 하는 시나리오의 예로는 응용 프로그램 디버깅이 있습니다.

이 작업에 대해

``vserver locks break`` 명령은 advanced 권한 수준 이상에서만 사용할 수 있습니다. [에 대한 자세한 내용은 `vserver locks break` link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html](https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html) ["ONTAP 명령 참조입니다"]을 참조하십시오.

단계

1. 잠금을 해제해야 하는 정보를 찾으려면 'vserver lock show' 명령을 사용합니다.

에 대한 자세한 내용은 `vserver locks show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

3. 다음 작업 중 하나를 수행합니다.

다음을 지정하여 잠금을 해제하려면...	명령 입력...
SVM 이름, 볼륨 이름, LIF 이름 및 파일 경로	<code>'vserver lock break - vserver vserver_name - volume volume_name - path path path -lif lif'</code>
잠금 ID입니다	<code>'vserver lock break-lockid UUID'</code>

4. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

ONTAP FPolicy의 첫 번째 읽기 및 첫 번째 쓰기 필터가 **NFS**에서 작동하는 방식을 알아보세요.

FPolicy가 읽기/쓰기 작업이 있는 외부 FPolicy 서버를 사용하여 모니터링되는 이벤트로 사용되는 경우 NFS 클라이언트에서 읽기/쓰기 요청의 트래픽이 많을 때 응답 시간이 오래 됩니다. NFS 클라이언트의 경우 FPolicy에서 첫 번째 읽기 및 첫 번째 쓰기 필터를 사용하므로 FPolicy 알림의 수가 줄어들고 성능이 향상됩니다.

NFS에서 클라이언트는 해당 핸들을 폐치하여 파일에서 I/O를 수행합니다. 이 핸들은 서버와 클라이언트의 재부팅 후에도 유효합니다. 따라서 클라이언트는 핸들을 캐시하고 핸들을 다시 검색하지 않고 요청을 보낼 수 있습니다. 일반 세션에서 많은 읽기/쓰기 요청이 파일 서버로 전송됩니다. 이러한 모든 요청에 대해 알림이 생성되는 경우 다음과 같은 문제가 발생할 수 있습니다.

- 추가 알림 처리 및 응답 시간 증가로 인한 로드 증가

- 서버가 모든 알림의 영향을 받지 않더라도 FPolicy 서버에 많은 수의 알림이 전송됩니다.

클라이언트에서 특정 파일에 대한 첫 번째 읽기/쓰기 요청을 받으면 캐시 항목이 생성되고 읽기/쓰기 횟수가 증가합니다. 이 요청은 첫 번째 읽기/쓰기 작업으로 표시되며 FPolicy 이벤트가 생성됩니다. NFS 클라이언트에 대한 FPolicy 필터를 계획하고 생성하기 전에 FPolicy 필터 작동 방식에 대한 기본 사항을 이해해야 합니다.

- First-read: 첫 번째 읽기에 대한 클라이언트 읽기 요청을 필터링합니다.

NFS 이벤트에 이 필터를 사용하면 '-file-session-io-grouping-count' 및 '-file-session-io-grouping-duration' 설정에 따라 FPolicy가 처리되는 첫 번째 읽기 요청이 결정됩니다.

- First-write: 첫 번째 쓰기에 대한 클라이언트 쓰기 요청을 필터링합니다.

NFS 이벤트에 이 필터를 사용하면 '-file-session-io-grouping-count' 및 '-file-session-io-grouping-duration' 설정에 따라 FPolicy가 처리하는 첫 번째 쓰기 요청이 결정됩니다.

다음 옵션은 NFS 서버 데이터베이스에 추가됩니다.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

ONTAP SVM에 대한 NFSv4.1 서버 구현 ID 수정

NFSv4.1 프로토콜에는 서버 도메인, 이름 및 날짜를 문서화하는 서버 구현 ID가 포함됩니다. 서버 구현 ID 기본값을 수정할 수 있습니다. 예를 들어, 사용 통계를 수집하거나 상호 운용성 문제를 해결하는 경우 기본값을 변경하면 유용합니다. 자세한 내용은 RFC 5661을 참조하십시오.

이 작업에 대해

세 옵션의 기본값은 다음과 같습니다.

옵션을 선택합니다	옵션 이름입니다	기본값
NFSv4.1 구현 ID 도메인	'-v4.1-구현도메인'	NetApp.com
NFSv4.1 구현 ID 이름	'-v4.1-구현명'	클러스터 버전 이름입니다
NFSv4.1 구현 ID 날짜	'-v4.1-구현일'	클러스터 버전 날짜입니다

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

NFSv4.1 구현 ID를 수정하려는 경우...	명령 입력...
도메인	'vserver nfs modify-v4.1-imImplementation-domain domain'
이름	'vserver nfs modify-v4.1-im구현-name 이름'
날짜	'vserver nfs modify-v4.1-dimImplementation-date date'

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

NFSv4 ACL 관리

ONTAP SVM에 대한 NFSv4 ACL 활성화의 이점에 대해 알아보세요.

NFSv4 ACL을 설정하면 많은 이점이 있습니다.

NFSv4 ACL을 설정하면 다음과 같은 이점이 있습니다.

- 파일 및 디렉토리에 대한 사용자 액세스를 세밀하게 제어합니다
- NFS 보안 강화
- CIFS와의 상호 운용성 향상
- 사용자당 16개 그룹의 NFS 제한을 제거합니다

ONTAP SVM에 대한 NFSv4 ACL에 대해 알아보세요

NFSv4 ACL을 사용하는 클라이언트는 시스템의 파일 및 디렉토리에 대한 ACL을 설정하고 볼 수 있습니다. 새 파일 또는 하위 디렉토리가 ACL이 있는 디렉토리에 생성되면 새 파일 또는 하위 디렉토리는 적절한 상속 플래그로 태그가 지정된 ACL의 모든 ACE(액세스 제어 항목)를 상속합니다.

NFSv4 요청의 결과로 파일이나 디렉토리가 생성되면 결과 파일 또는 디렉토리의 ACL은 파일 생성 요청에 ACL이 포함되는지, 표준 UNIX 파일 액세스 권한만 포함되는지, 상위 디렉토리에 ACL이 있는지 여부에 따라 달라집니다.

- 요청에 ACL이 포함된 경우 해당 ACL이 사용됩니다.
- 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.



상위 ACL은 '-v4.0-acl'이 'off'로 설정되어 있어도 상속된다.

- 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 새 객체는 모드 비트로만 생성됩니다.



매개 변수가 또는 `vserver export-policy rule` 패밀리의 명령을 사용하여 `vserver nfs` 로 `restricted` 설정된 경우 `-chown-mode` NFSv4 ACL을 사용하여 설정된 온디스크 사용 권한이 루트 사용자가 파일 소유권을 변경할 수 있는 경우에도 슈퍼 사용자만 파일 소유권을 변경할 수 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#) 참조하십시오.

ONTAP SVM에 대한 NFSv4 ACL 수정을 활성화하거나 비활성화합니다.

ONTAP가 ACL이 있는 파일 또는 디렉토리에 대해 'chmod' 명령을 수신하면 기본적으로 ACL이 유지되고 모드 비트 변경을 반영하도록 수정됩니다. 대신 ACL을 삭제하고자 하는 경우 동작을 변경하기 위해 '-v4-acl-preserve' 파라미터를 비활성화할 수 있습니다.

이 작업에 대해

통합 보안 스타일을 사용할 때 이 매개 변수는 클라이언트가 파일 또는 디렉토리에 대해 chmod, chgroup 또는 chown 명령을 보낼 때 NTFS 파일 권한을 보존할지 또는 삭제할지 여부도 지정합니다.

이 매개 변수의 기본값은 활성화되어 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
기본 NFSv4 ACL 보존 및 수정 설정 (기본값)	'vserver nfs modify -vserver vserver_name -v4-acl-preserve enabled'
모드 비트를 변경할 때 NFSv4 ACL을 보존하고 삭제합니다	'vserver nfs modify -vserver vserver_name -v4-acl-preserve disabled'

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

ONTAP이 NFSv4 ACL을 사용하여 파일을 삭제할 수 있는지 여부를 확인하는 방법을 알아보세요.

파일을 삭제할 수 있는지 여부를 확인하기 위해 ONTAP에서는 파일의 삭제 비트와 포함하는 디렉토리의 `delete_child` 비트를 함께 사용합니다. 자세한 내용은 NFS 4.1 RFC 5661을 참조하십시오.

ONTAP SVM에 대한 NFSv4 ACL 활성화 또는 비활성화

NFSv4 ACL을 설정하거나 해제하려면 '-v4.0-acl' 및 '-v4.1-acl' 옵션을 수정할 수 있습니다. 이러한 옵션은 기본적으로 비활성화되어 있습니다.

이 작업에 대해

'-v4.0-acl' 또는 '-v4.1-acl' 옵션은 NFSv4 ACL의 설정 및 보기를 제어하지만 액세스 검사를 위해 이러한 ACL의 적용을 제어하지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면...
NFSv4.0 ACL을 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -acl enabled'
NFSv4.0 ACL을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -acl disabled'
NFSv4.1 ACL을 활성화합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -acl enabled'
NFSv4.1 ACL을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -acl disabled'

ONTAP SVM에 대한 NFSv4 ACL의 최대 ACE 제한 수정

매개 변수 '-v4-acl-max-aces'를 수정하여 각 NFSv4 ACL에 대해 허용되는 최대 ACE 수를 수정할 수 있습니다. 기본적으로 이 제한은 각 ACL에 대해 400개의 ACE로 설정됩니다. 이 제한을 늘리면 400개 이상의 ACE가 포함된 ACL을 사용하여 ONTAP를 실행하는 스토리지 시스템으로 데이터를 성공적으로 마이그레이션할 수 있습니다.

이 작업에 대해

이 제한을 늘리면 NFSv4 ACL을 사용하여 파일을 액세스하는 클라이언트의 성능에 영향을 줄 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. NFSv4 ACL의 최대 ACE 제한 수정:

'vserver nfs modify -v4-acl-max-aces max_ace_limit'

의 유효한 범위

최대 에이스 한계는 192에서 1024로

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

NFSv4 파일 위임을 관리합니다

ONTAP SVM에 대한 NFSv4 읽기 파일 위임을 활성화하거나 비활성화합니다.

NFSv4 읽기 파일 위임을 설정하거나 해제하려면 '-v4.0-read-delegation' 또는 '-v4.1-read-delegation' 옵션을 수정할 수 있습니다. 읽기 파일 위임을 사용하면 파일 열기 및 닫기와 관련된 메시지 오버헤드를 상당 정도 제거할 수 있습니다.

이 작업에 대해

기본적으로 읽기 파일 위임은 사용되지 않습니다.

읽기 파일 위임을 설정할 경우 서버 재부팅 또는 재시작, 클라이언트 재부팅 또는 재시작, 네트워크 파티션 발생 후 서버와 클라이언트에서 위임을 복구해야 한다는 단점이 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면...
NFSv4 읽기 파일 위임을 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled'
NFSv4.1 읽기 파일 위임을 사용하도록 설정합니다	다음 명령을 입력합니다. + 'vserver NFS modify -vserver vserver_name -v4.1 -read-delegation enabled'
NFSv4 읽기 파일 위임을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled'
NFSv4.1 읽기 파일 위임을 사용하지 않도록 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled'

결과

파일 위임 옵션은 변경되자마자 적용됩니다. NFS를 재부팅하거나 다시 시작할 필요가 없습니다.

ONTAP SVM에 대한 **NFSv4** 쓰기 파일 위임을 활성화하거나 비활성화합니다.

쓰기 파일 위임을 설정하거나 해제하려면 '-v4.0-write-delegation' 또는 '-v4.1-write-delegation' 옵션을 수정할 수 있습니다. 쓰기 파일 위임을 사용하면 파일 열기 및 닫기 외에도 파일 및 레코드 잠금과 관련된 메시지 오버헤드를 상당 정도 제거할 수 있습니다.

이 작업에 대해

기본적으로 쓰기 파일 위임은 사용되지 않습니다.

쓰기 파일 위임을 설정할 경우 서버 재부팅 또는 재시작, 클라이언트 재부팅 또는 재시작, 네트워크 파티션 발생 후 위임을 복구하려면 서버와 해당 클라이언트가 추가 작업을 수행해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면...
NFSv4 쓰기 파일 위임을 설정합니다	'vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled' 명령을 입력합니다
NFSv4.1 쓰기 파일 위임을 사용하도록 설정합니다	'vserver NFS modify -vserver vserver_name -v4.1 -write-delegation enabled' 명령을 입력합니다
NFSv4 쓰기 파일 위임을 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled' 명령을 입력합니다
NFSv4.1 쓰기 파일 위임을 사용하지 않도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled' 명령을 입력합니다

결과

파일 위임 옵션은 변경되자마자 적용됩니다. NFS를 재부팅하거나 다시 시작할 필요가 없습니다.

NFSv4 파일을 구성하고 잠금을 기록합니다

ONTAP SVM에 대한 **NFSv4** 파일 및 레코드 잠금에 대해 알아보세요.

NFSv4 클라이언트의 경우 ONTAP는 NFSv4 파일 잠금 메커니즘을 지원하여 임대 기반 모델에서 모든 파일 잠금의 상태를 유지합니다.

["NetApp 기술 보고서 3580: NFSv4 향상 및 모범 사례 가이드 Data ONTAP 구축"](#)

ONTAP SVM에 대한 **NFSv4** 잠금 임대 기간 지정

NFSv4 잠금 임대 기간(즉, ONTAP가 클라이언트에 잠금을 부여하는 기간)을 지정하려면 '-v4-lease-seconds' 옵션을 수정할 수 있습니다. 리스 기간이 짧을수록 서버 복구 속도가 빨라지며 리스 기간이 길면 매우 많은 양의 클라이언트를 처리하는 서버에 유용합니다.

이 작업에 대해

기본적으로 이 옵션은 30으로 설정되어 있습니다. 이 옵션의 최소값은 10입니다. 이 옵션의 최대값은 'locking.lease_seconds' 옵션으로 설정할 수 있는 locking grace 기간입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

```
'vserver nfs modify -vserver vservice_name -v4-lease-seconds number_of_seconds'
```

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

ONTAP SVM에 대한 NFSv4 잠금 유예 기간 지정

NFSv4 잠금 유예 기간(즉, 서버 복구 중에 클라이언트가 ONTAP에서 잠금 상태를 복구하려는 기간)을 지정하려면 "-v4-grace-seconds" 옵션을 수정할 수 있습니다.

이 작업에 대해

기본적으로 이 옵션은 45로 설정되어 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

```
'vserver nfs modify -vserver vservice_name -v4-grace-seconds number_of_seconds _'
```

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

ONTAP SVM에 대한 NFSv4 참조에 대해 알아보세요

NFSv4 조회를 설정하면 ONTAP는 NFSv4 클라이언트에 ""intra-SVM" 조회를 제공합니다. SVM 내 의뢰는 NFSv4 요청을 수신하는 클러스터 노드가 SVM(스토리지 가상 머신)의 다른 논리 인터페이스(LIF)에 NFSv4 클라이언트를 참조하는 경우를 말합니다.

NFSv4 클라이언트는 해당 시점부터 타겟 LIF에서 조회 대상이 된 경로를 액세스해야 합니다. 원래 클러스터 노드는 SVM에 데이터 볼륨이 상주하는 클러스터 노드에 상주하는 LIF가 존재한다고 판단하여 클라이언트가 데이터에 더 빠르게 액세스하고 추가 클러스터 통신을 피할 수 있게 해줍니다.

ONTAP SVM에 대한 NFSv4 참조 활성화 또는 비활성화

'-v4-fsid-change' 및 '-v4.0-referral' 또는 '-v4.1-referral' 옵션을 활성화하여 스토리지 가상 시스템(SVM)에서 NFSv4 조회를 설정할 수 있습니다. NFSv4 조회를 설정하면 이 기능을 지원하는 NFSv4 클라이언트에 대한 데이터 액세스 속도가 빨라집니다.

시작하기 전에

NFS 조회를 설정하려면 먼저 parallel NFS를 해제해야 합니다. 동시에 둘 다 활성화할 수 없습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
NFSv4 조회를 설정합니다	'vserver nfs modify -vserver vserver_name -v4 -fsid -change enabled'"vserver nfs modify -vserver vserver vserver_name -v4.0 -referral enabled'
NFSv4 조회를 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 -referral disabled'
NFSv4.1 조회를 사용하도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4 -fsid -change enabled'"vserver nfs modify -vserver vserver vserver_name -v4.1 -referral enabled'
NFSv4.1 조회를 비활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -referral disabled'

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

ONTAP NFS SVM에 대한 통계 표시

스토리지 시스템에서 SVM(스토리지 가상 머신)에 대한 NFS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tistics catalog object show' 명령을 사용하여 데이터를 볼 수 있는 NFS 객체를 식별합니다.

'스타티틱스 카탈로그 객체 표시 - 객체 NFS *'

2. 자폐 시작 및 선택적 '자폐 중지' 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.
3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

예: **NFSv3** 성능 모니터링

다음 예제에는 NFSv3 프로토콜의 성능 데이터가 나와 있습니다.

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

다음 명령을 실행하면 성공한 읽기 및 쓰기 요청 수와 총 읽기 및 쓰기 요청 수를 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1
```

Counter	Value
read_success	40042
read_total	40042
write_success	1492052
write_total	1492052

관련 정보

- ["성능 모니터링 설정"](#)
- ["통계 카탈로그 객체 표시"](#)
- ["통계에 따르면"](#)
- ["통계 시작"](#)
- ["통계 중지"](#)

ONTAP NFS SVM에 대한 DNS 통계 표시

스토리지 시스템에서 SVM(스토리지 가상 머신)에 대한 DNS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tortisics catalog object show' 명령어를 사용하여 데이터를 볼 수 있는 DNS 객체를 확인할 수 있다.

'통계 카탈로그 객체 표시 - 객체 EXTERNAL_SERVICE_op **'

2. 자폐 시작, 자폐 중지 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.

3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

DNS 통계 모니터링

다음 예에서는 DNS 쿼리에 대한 성능 데이터를 보여 줍니다. 다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

다음 명령을 실행하면 전송된 DNS 쿼리 수와 수신, 실패 또는 제한 시간이 초과된 DNS 쿼리 수를 비교하여 표시하는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	0
num_requests_sent	1
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

다음 명령을 실행하면 특정 서버의 DNS 쿼리에 대해 특정 오류가 수신된 횟수를 표시하는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id dns_sample2 -counter  
server_ip_address|error_string|count
```

Object: external_service_op_error

Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109

Start-time: 3/8/2016 11:23:21

End-time: 3/8/2016 11:24:25

Elapsed-time: 64s

Scope: vs1

Counter	Value
count	1
error_string	NXDOMAIN
server_ip_address	10.72.219.109

3 entries were displayed.

관련 정보

- ["성능 모니터링 설정"](#)
- ["통계 카탈로그 객체 표시"](#)
- ["통계에 따르면"](#)
- ["통계 시작"](#)
- ["통계 중지"](#)

ONTAP NFS SVM에 대한 NIS 통계 표시

스토리지 시스템에 SVM(스토리지 가상 머신)에 대한 NIS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tortisics catalog object show' 명령을 사용하여 데이터를 볼 수 있는 NIS 객체를 식별합니다.

'통계 카탈로그 객체 표시 - 객체 EXTERNAL_SERVICE_op *'

2. 자폐 시작, 자폐 중지 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.
3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

NIS 통계 모니터링

다음 예에서는 NIS 쿼리에 대한 성능 데이터를 보여 줍니다. 다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.


```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

다음 명령을 실행하면 전송된 NIS 쿼리 수와 수신, 실패 또는 시간 초과 NIS 쿼리 수를 비교하여 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	1
num_requests_sent	2
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

다음 명령을 실행하면 특정 서버의 NIS 쿼리에 대해 특정 오류가 수신된 횟수를 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id nis_sample2 -counter  
server_ip_address|error_string|count
```

Object: external_service_op_error

Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221

Start-time: 3/8/2016 11:33:05

End-time: 3/8/2016 11:33:10

Elapsed-time: 5s

Scope: vs1

Counter	Value
count	1
error_string	YP_NOTFOUND
server_ip_address	10.227.13.221

3 entries were displayed.

관련 정보

- ["성능 모니터링 설정"](#)
- ["통계 카탈로그 객체 표시"](#)
- ["통계에 따르면"](#)
- ["통계 시작"](#)
- ["통계 중지"](#)

ONTAP NFS를 통한 VMware vStorage 지원에 대해 알아보세요

ONTAP는 NFS 환경에서 특정 VMware VAAI(vStorage APIs for Array Integration) 기능을 지원합니다.

지원되는 기능

지원되는 기능은 다음과 같습니다.

- 복사본 오프로드

ESXi 호스트에서 호스트를 사용하지 않고 소스 및 대상 데이터 저장소 위치 간에 직접 VMDK(가상 머신 또는 가상 머신 디스크)를 복제할 수 있습니다. 이렇게 하면 ESXi 호스트 CPU 주기와 네트워크 대역폭이 절약됩니다. 복제 오프로드는 소스 볼륨이 스파스 상태인 경우 공간 효율성을 유지합니다.

- 공간 예약

VMDK 파일용 공간을 예약하여 스토리지 공간을 보장합니다.

제한 사항

VMware vStorage over NFS에는 다음과 같은 제한 사항이 있습니다.

- 다음과 같은 경우 복사 오프로드 작업이 실패할 수 있습니다.
 - 소스 또는 타겟 볼륨에서 웨이브다리를 실행하는 동안 일시적으로 볼륨이 오프라인 상태가 되기 때문입니다
 - 소스 또는 타겟 볼륨을 이동하는 동안
 - 소스 또는 타겟 LIF를 이동하는 동안
 - Takeover 또는 Giveback 작업을 수행하는 동안
 - 스위치오버 또는 스위치백 작업을 수행하는 동안
- 다음 시나리오에서 파일 핸들 형식의 차이로 인해 서버 측 복제가 실패할 수 있습니다.

Qtree를 내보낸 적이 없는 SVM으로 현재 또는 이전에 qtree를 내보낸 SVM에서 데이터를 복사하려고 합니다. 이러한 제한 사항을 해결하려면 대상 SVM에서 qtree를 하나 이상 내보낼 수 있습니다.

관련 정보

["Data ONTAP에서 지원하는 VAAI 오프로드 작업은 무엇입니까?"](#)

ONTAP NFS를 통한 VMware vStorage 활성화 또는 비활성화

"vserver NFS modify" 명령을 사용하여 SVM(스토리지 가상 머신)에서 VMware vStorage over NFS에 대한 지원을 설정하거나 해제할 수 있습니다.

이 작업에 대해

기본적으로 VMware vStorage over NFS에 대한 지원은 비활성화되어 있습니다.

단계

1. SVM에 대한 현재 vStorage 지원 상태 표시:

```
'vserver nfs show -vserver vserver_name -instance'
```

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
VMware vStorage 지원을 설정합니다	'vserver nfs modify -vserver vserver_name -vStorage enabled'
VMware vStorage 지원을 사용하지 않도록 설정합니다	'vserver nfs modify -vserver vserver_name -vStorage disabled'

작업을 마친 후

이 기능을 사용하려면 먼저 VMware VAAI용 NFS 플러그인을 설치해야 합니다. 자세한 내용은 [_VMware VAAI_용 NetApp NFS 플러그인 설치](#) 를 참조하십시오.

관련 정보

ONTAP NFS SVM에서 rquota 지원 활성화 또는 비활성화

원격 할당량 프로토콜(rquota)을 사용하면 NFS 클라이언트가 원격 시스템에서 사용자에게 대한 할당량 정보를 얻을 수 있습니다. rquota 버전에 대한 지원은 ONTAP 버전에 따라 다릅니다.

- rquota v1은 ONTAP 9 이상에서 지원됩니다.
- rquota v2는 ONTAP 9.12.1 이상에서 지원됩니다.

rquota v1에서 rquota v2로 업그레이드하면 사용자 할당량 한도에 예상치 못한 변경 사항이 나타날 수 있습니다. 이러한 변경 사항은 rquota v1과 rquota v2의 할당량 계산 방식의 차이로 인해 발생합니다. 자세한 내용은 다음을 참조하세요. "[NetApp 기술 자료: 사용자 할당량 제한이 예기치 않게 변경된 이유는 무엇입니까?](#)".

이 작업에 대해

기본적으로 rquota는 비활성화되어 있습니다.

단계

1. rquota 설정 또는 해제:

원하는 작업	다음 명령을 입력합니다...
SVM에 대해 rquota 지원을 설정합니다	<pre>vserver nfs modify -vserver vserver_name -rquota enable</pre>
SVM에 대한 rquota 지원을 비활성화합니다	<pre>vserver nfs modify -vserver vserver_name -rquota disable</pre>

할당량에 대한 자세한 내용은 을 참조하십시오 "[논리적 스토리지 관리](#)".

ONTAP SVM의 NFSv3 및 NFSv4 성능 개선 사항과 TCP 전송 크기에 대해 알아보세요.

TCP 최대 전송 크기를 수정하여 지연 시간이 긴 네트워크를 통해 스토리지 시스템에 접속하는 NFSv3 및 NFSv4 클라이언트의 성능을 향상시킬 수 있습니다.

클라이언트가 지연 시간이 10밀리초 이상 인 WAN(Wide Area Network) 또는 MAN(Metro Area Network)과 같이 지연 시간이 긴 네트워크를 통해 스토리지 시스템에 액세스하는 경우 TCP 최대 전송 크기를 수정하여 연결 성능을 향상시킬 수 있습니다. LAN(Local Area Network)과 같이 지연 시간이 짧은 네트워크에서 스토리지 시스템에 액세스하는 클라이언트는 이러한 매개 변수를 수정해도 거의 이점을 얻을 수 없습니다. 처리량 향상이 지연 시간에 미치는 영향을 상쇄하지 않는다면 이러한 매개 변수를 사용해서는 안 됩니다.

스토리지 환경에서 이러한 매개 변수를 수정하여 이점을 얻을 수 있는지 확인하려면 먼저 성능이 떨어지는 NFS 클라이언트에 대한 포괄적인 성능 평가를 수행해야 합니다. 낮은 성능이 클라이언트에 대한 과도한 라운드 트립 지연 및 작은 요청 때문인지 검토합니다. 이러한 조건에서는 클라이언트와 서버가 사용 가능한 대역폭을 완전히 사용할 수 없습니다. 왜냐하면 대부분의 듀티 사이클이 연결을 통해 전송되는 작은 요청과 응답을 대기하는 데 소비하기

때문입니다.

NFSv3 및 NFSv4 요청 크기를 늘리면 클라이언트 및 서버에서 사용 가능한 대역폭을 보다 효율적으로 사용하여 단위 시간당 더 많은 데이터를 이동할 수 있으므로 연결의 전반적인 효율성이 향상됩니다.

스토리지 시스템과 클라이언트 간의 구성은 달라질 수 있습니다. 스토리지 시스템과 클라이언트는 전송 작업에 대해 최대 1MB의 크기를 지원합니다. 그러나 스토리지 시스템이 1MB의 최대 전송 크기를 지원하도록 구성했지만 클라이언트가 64KB만 지원하는 경우 마운트 전송 크기는 64KB 이하로 제한됩니다.

이러한 매개변수를 수정하기 전에 대용량 응답을 조립하고 전송하는 데 필요한 기간 동안 스토리지 시스템에 메모리가 추가로 소비된다는 점을 염두에 두어야 합니다. 스토리지 시스템에 대한 대기 시간이 많을수록 추가 메모리 소비량이 증가합니다. 메모리 용량이 큰 스토리지 시스템은 이 변경으로 인해 거의 영향을 주지 않을 수 있습니다. 메모리 용량이 낮은 스토리지 시스템에서 눈에 띄는 성능 저하가 발생할 수 있습니다.

이 매개 변수를 사용하는 것은 클러스터의 여러 노드에서 데이터를 검색하는 기능에 달려 있습니다. 클러스터 네트워크의 지연으로 인해 전반적인 응답 시간이 길어질 수 있습니다. 이러한 매개 변수를 사용하면 전반적인 지연 시간이 증가하는 경향이 있습니다. 따라서 지연 시간에 민감한 워크로드에 부정적인 영향이 나타날 수 있습니다.

ONTAP SVM에 대한 NFSv3 및 NFSv4 TCP 최대 전송 크기 수정

NFSv3 및 NFSv4.x 프로토콜을 사용하여 모든 TCP 연결에 대해 최대 전송 크기를 구성하려면 '-tcp-max-xfer-size' 옵션을 수정할 수 있습니다.

이 작업에 대해

각 SVM(스토리지 가상 머신)별로 이러한 옵션을 개별적으로 수정할 수 있습니다.

ONTAP 9부터 v3-tcp-max-read-size와 v3-tcp-max-write-size 옵션은 더 이상 사용되지 않습니다. 대신 '-tcp-max-xfer-size' 옵션을 사용해야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
NFSv3 또는 NFSv4 TCP 최대 전송 크기를 수정합니다	<code>'vserver nfs modify -vserver vserver_name -tcp -max -xfer-size integer_max_xfer_size'</code>

옵션을 선택합니다	범위	기본값
'-tcp-max-xfer-size'를 선택합니다	8192 ~ 1048576바이트	65536바이트



입력하는 최대 전송 크기는 4KB(4096바이트)의 배수여야 합니다. 제대로 정렬되지 않은 요청은 성능에 부정적인 영향을 줍니다.

3. 'vserver nfs show-fields tcp-max-xfer-size' 명령을 사용하여 변경 사항을 확인합니다.

4. 클라이언트가 정적 마운트를 사용하는 경우 새 매개 변수 크기를 마운트 해제하고 다시 마운트하여 적용합니다.

예

다음 명령을 실행하면 이름이 VS1인 SVM에서 NFSv3 및 NFSv4.x TCP 최대 전송 크기가 1048576바이트로 설정됩니다.

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

ONTAP SVM에 대해 NFS 사용자에게 허용되는 그룹 ID 수를 구성합니다.

기본적으로 ONTAP는 Kerberos(RPCSEC_GSS) 인증을 사용하여 NFS 사용자 자격 증명을 처리할 때 최대 32개의 그룹 ID를 지원합니다. AUTH_SYS 인증을 사용하는 경우 RFC 5531에 정의된 대로 기본 최대 그룹 ID 수는 16입니다. 기본 그룹 수보다 많은 그룹의 구성원인 사용자가 있는 경우 최대 1,024개까지 늘릴 수 있습니다.

이 작업에 대해

사용자의 자격 증명에 기본 그룹 ID 수보다 많은 수의 그룹 ID가 있는 경우 나머지 그룹 ID가 잘리고 스토리지 시스템에서 파일을 액세스하려고 할 때 오류가 발생할 수 있습니다. SVM당 최대 그룹 수를 환경의 최대 그룹을 나타내는 숫자로 설정해야 합니다.



확장 그룹을 활성화하기 위한 AUTH_SYS 인증 전제 조건을 이해하려면(-auth-sys-extended-groups) 기본 최대값인 16을 초과하는 그룹 ID를 사용하는 경우 다음을 참조하십시오. "[NetApp 지식 기반: auth-sys-extended-groups를 활성화하기 위한 전제 조건은 무엇입니까?](#)"

다음 표는 세 가지 샘플 구성에서 최대 그룹 ID 수를 결정하는 "vserver NFS modify" 명령의 두 가지 매개 변수를 보여 줍니다.

매개 변수	설정	결과 그룹 ID 제한
'확장-그룹-제한'	32인치	RPCSEC_GSS:32
``auth-sys-extended-groups``	'비활성화'입니다 기본 설정입니다.	AUTH_SYS:16
'확장-그룹-제한'	256입니다	RPCSEC_GSS:256
``auth-sys-extended-groups``	'비활성화'입니다	AUTH_SYS:16
'확장-그룹-제한'	512	RPCSEC_GSS:512
``auth-sys-extended-groups``	"활성화됨"	AUTH_SYS:512

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

허용된 보조 그룹의 최대 수를 설정하려면...	명령 입력...
RPCSEC_GSS에만 해당하고 AUTH_SYS는 기본값 16으로 설정된 상태로 둡니다	'vserver nfs modify -vserver vs1 -auth-sys-extended-groups disabled'
RPCSEC_GSS 및 AUTH_SYS의 경우	'vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled'

3. '-extended-groups-limit' 값을 확인하고 AUTH_SYS가 확장된 그룹('vserver nfs show -vserver vs1 -fields auth-sys-extended-groups, extended-groups-limit')을 사용하고 있는지 확인합니다
4. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

예

다음 예에서는 AUTH_SYS 인증에 대해 확장된 그룹을 활성화하고, AUTH_SYS 및 RPCSEC_GSS 인증에 대해 확장 그룹의 최대 수를 512로 설정합니다. 이러한 변경은 VS1 이라는 SVM에 액세스하는 클라이언트에만 적용됩니다.

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                  512

vs1::*> set -privilege admin
```

관련 정보

- ["NetApp 기술 자료: ONTAP 9에 대한 NFS 인증을 위한 AUTH_SYS 확장 그룹 변경 사항"](#)

ONTAP SVM에 대한 NTFS 보안 스타일 데이터에 대한 루트 사용자 액세스를 제어합니다.

NFS 클라이언트가 NTFS 보안 스타일 데이터에 액세스하고 NTFS 클라이언트가 NFS 보안 스타일 데이터에 액세스할 수 있도록 ONTAP를 구성할 수 있습니다. NFS 데이터 저장소에서 NTFS 보안 스타일을 사용하는 경우 루트 사용자가 액세스를 처리하는 방법을 결정하고 이에

따라 SVM(스토리지 가상 머신)을 구성해야 합니다.

이 작업에 대해

루트 사용자가 NTFS 보안 스타일 데이터에 액세스할 때 다음 두 가지 옵션이 있습니다.

- 다른 NFS 사용자와 마찬가지로 루트 사용자를 Windows 사용자에게 매핑하고 NTFS ACL에 따라 액세스를 관리합니다.
- NTFS ACL을 무시하고 루트에 대한 전체 액세스를 제공합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

루트 사용자가 다음을 수행할 수 있도록 하려면...	명령 입력...
Windows 사용자에게 매핑되어야 합니다	'vserver nfs modify -vserver vservers_name -ignore -nt-acl-for-root disabled'
NT ACL 검사를 생략합니다	'vserver nfs modify -vserver vservers_name -ignore -nt-acl-for-root enabled'

기본적으로 이 매개 변수는 사용되지 않습니다.

이 매개 변수가 설정되어 있지만 루트 사용자에게 대한 이름 매핑이 없는 경우 ONTAP에서는 감사를 위해 기본 SMB 관리자 자격 증명을 사용합니다.

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

지원되는 NFS 버전 및 클라이언트

지원되는 ONTAP NFS 버전 및 클라이언트에 대해 알아보세요

네트워크에서 NFS를 사용하려면 먼저 ONTAP가 지원하는 NFS 버전과 클라이언트를 알아야 합니다.

이 표에서는 ONTAP에서 주 및 부 NFS 프로토콜 버전이 기본적으로 지원되는 경우 설명합니다. 기본적으로 지원에서는 이 버전이 NFS 프로토콜을 지원하는 ONTAP의 최초 버전임을 표시하지 않습니다.

버전	지원	도입됨
NFSv3	예	모든 ONTAP 릴리스

버전	지원	도입됨
NFSv4.0	예	ONTAP 8 를 참조하십시오
NFSv4.1	예	ONTAP 8.1 를 참조하십시오
NFSv4.2	예	ONTAP 9.8
pNFS를 사용합니다	예	ONTAP 8.1 를 참조하십시오

ONTAP가 지원하는 NFS 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

["NetApp 상호 운용성 매트릭스 툴"](#)

NFSv4.0 기능에 대한 **ONTAP** 지원에 대해 알아보세요

ONTAP는 SPKM3 및 LIPKEY 보안 메커니즘을 제외한 NFSv4.0의 모든 필수 기능을 지원합니다.

지원되는 NFSv4 기능은 다음과 같습니다.

- * 복합 *

클라이언트가 단일 RPC(원격 프로시저 호출) 요청에서 여러 파일 작업을 요청할 수 있습니다.

- * 파일 위임 *

서버가 읽기 및 쓰기 액세스를 위해 일부 유형의 클라이언트에 파일 제어를 위임할 수 있도록 합니다.

- * 의사 fs *

NFSv4 서버에서 스토리지 시스템의 마운트 지점을 결정하는 데 사용됩니다. NFSv4에는 마운트 프로토콜이 없습니다.

- * 잠금 *

임대 기반. NFSv4에는 별도의 NLM(Network Lock Manager) 또는 NSM(Network Status Monitor) 프로토콜이 없습니다.

NFSv4.0 프로토콜에 대한 자세한 내용은 RFC 3530을 참조하십시오.

NFSv4에 대한 **ONTAP** 지원 제한 사항에 대해 알아보세요.

NFSv4에 대한 ONTAP 지원의 몇 가지 제한 사항에 대해 알고 있어야 합니다.

- 위임 기능은 모든 클라이언트 유형에서 지원되지 않습니다.
- ONTAP 9.4 및 이전 릴리즈에서는 UTF8 볼륨 이외의 볼륨에 ASCII가 아닌 문자가 있는 이름이 스토리지 시스템에서 거부됩니다.

ONTAP 9.5 이상 릴리즈에서는 utf8mb4 언어 설정으로 생성하고 NFS v4를 사용하여 마운트된 볼륨이 더 이상 이 제한을 받지 않습니다.

- 모든 파일 핸들은 영구적이며, 서버는 휘발성 파일 핸들을 제공하지 않습니다.
- 마이그레이션 및 복제는 지원되지 않습니다.
- NFSv4 클라이언트는 읽기 전용 로드 공유 미러에서 지원되지 않습니다.

ONTAP는 직접 읽기 및 쓰기 액세스를 위해 NFSv4 클라이언트를 로드 공유 미러 소스로 라우팅합니다.

- 명명된 특성은 지원되지 않습니다.
- 다음을 제외한 모든 권장 속성이 지원됩니다.
 - '보관'
 - '숨겨짐'
 - 동질성
 - 'mimetype'입니다
 - 쿼터쿼터_AVAIL_HARD를 선택합니다
 - 쿼터가용성 소프트웨어
 - quota_used
 - '시스템'
 - Time_backup을 선택합니다



"quota *" 특성은 지원하지 않지만 ONTAP는 RQUOTA Side Band 프로토콜을 통해 사용자 및 그룹 할당량을 지원합니다.

NFSv4.1에 대한 ONTAP 지원에 대해 알아보세요

ONTAP 9.8부터는 NFSv4.1이 활성화된 경우 기본적으로 nconnect 기능을 사용할 수 있습니다.

이전 버전의 NFS 클라이언트 구축에서는 마운트와 단일 TCP 연결만 사용합니다. ONTAP에서 단일 TCP 연결은 IOPS 증가에 따라 병목 현상을 일으킬 수 있습니다.

nconnect는 단일 마운트에 대해 여러 TCP 연결(최대 16개)을 허용하여 NFS 클라이언트 성능을 개선하고, IOPS가 증가함에 따라 단일 TCP 연결에서 발생할 수 있는 성능 병목 현상을 극복하는 데 도움이 됩니다.

NFSv4.1은 ONTAP 9.9.1 이상에서 기본적으로 활성화되어 있습니다. 이전 릴리즈에서는 SVM(스토리지 가상 머신)에서 NFS 서버를 생성할 때 '-v4.1' 옵션을 지정하고 이를 '사용'으로 설정하여 사용할 수 있습니다.

ONTAP는 NFSv4.1 디렉토리 및 파일 레벨 위임을 지원하지 않습니다.

관련 정보

["NFS 성능을 위한 nconnect에 대해 알아보세요".](#)

NFSv4.2에 대한 ONTAP 지원에 대해 알아보세요

ONTAP 9.8부터 ONTAP는 NFSv4.2 사용 클라이언트에 대한 액세스를 허용하는 NFSv4.2 프로토콜을 지원합니다.

ONTAP 9.9.1 이상에서는 NFSv4.2가 기본적으로 활성화되어 있습니다. ONTAP 9.8에서는 다음을 지정하여 v4.2를 수동으로 활성화해야 합니다. `-v4.2` 옵션 및 설정 `enabled` 스토리지 가상 머신(SVM)에 NFS 서버를 생성할 때. NFSv4.1을 활성화하면 클라이언트가 v4.2로 마운트된 동안에도 NFSv4.1 기능을 사용할 수 있습니다.

연속적인 ONTAP 릴리즈는 NFSv4.2 옵션 기능에 대한 지원을 확장합니다.

다음으로 시작...	NFSv4.2의 옵션 기능은 다음과 같습니다.
ONTAP 9.12.1	• NFS 확장 속성입니다 • Sparse 파일 • 공간 예약
ONTAP 9.9.1	MAC(Mandatory Access Control) 레이블 NFS

NFS v4.2 보안 레이블

ONTAP 9.9.1부터 NFS 보안 레이블을 활성화할 수 있습니다. 기본적으로 비활성화되어 있습니다.

NFS v4.2 보안 레이블에서 ONTAP NFS 서버는 MAC(Mandatory Access Control)를 인식하여 클라이언트가 전송한 `sec_label` 특성을 저장 및 검색합니다.

자세한 내용은 을 참조하십시오 "[RFC 7240](#)".

ONTAP 9.12.1부터는 NDMP 덤프 작업에 NFS v4.2 보안 레이블이 지원됩니다. 이전 릴리즈의 파일 또는 디렉터리에서 보안 레이블이 발견되면 덤프가 실패합니다.

단계

1. 권한 설정을 고급으로 변경합니다.

```
set -privilege advanced
```

2. 보안 레이블 활성화:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS 확장 속성입니다

ONTAP 9.12.1부터 NFS 확장 특성(xattrs)이 기본적으로 사용하도록 설정됩니다.

확장 특성은 에 의해 정의된 표준 NFS 속성입니다 "[RFC 8276](#)" 최신 NFS 클라이언트에서 사용하도록 설정됩니다. 사용자 정의 메타데이터를 파일 시스템 객체에 연결하는 데 사용할 수 있으며 고급 보안 구축에 관심이 있습니다.

NFS 확장 속성은 현재 NDMP 덤프 작업에 지원되지 않습니다. 파일 또는 디렉토리에서 확장 속성이 발견되면 덤프는 진행되지만 해당 파일 또는 디렉토리의 확장 속성은 백업하지 않습니다.

확장 속성을 비활성화해야 하는 경우 `vserver nfs modify -v4.2-xattrs disabled` 명령.

NFS 성능을 위한 **nconnect**에 대해 알아보세요

ONTAP 9.8부터 NFSv4.1이 활성화된 경우 **nconnect** 기능을 기본적으로 사용할 수 있습니다. **nconnect**는 단일 마운트에 대해 여러 TCP 연결을 허용하여 NFS 클라이언트 성능을 향상시킵니다.

nconnect 작동 방식

이전 버전의 NFS 클라이언트 구축에서는 마운트와 단일 TCP 연결만 사용합니다. ONTAP에서 단일 TCP 연결은 IOPS 증가에 따라 병목 현상을 일으킬 수 있습니다.

nconnect가 활성화된 클라이언트는 단일 NFS 마운트와 연관된 여러 TCP 연결(최대 16개)을 가질 수 있습니다. **nconnect**는 단 하나의 IP 주소만 사용하고 해당 단일 IP를 통해 여러 TCP 연결을 설정하여 NFS 내보내기를 마운트합니다. NFS 클라이언트는 파일 작업을 라운드 로빈 방식으로 여러 TCP 연결에 분산하여 사용 가능한 네트워크 대역폭에서 더 높은 처리량을 얻습니다.

지원되는 **NFS** 버전

- **nconnect**는 NFSv3, NFSv4.2 및 NFSv4.1 마운트에 권장됩니다.
- **nconnect**는 NFSv4.0 마운트에 권장되지 않습니다.



최적의 성능을 위해 NetApp NFSv4.0 대신 **nconnect**와 함께 NFSv4.1을 사용할 것을 권장합니다. NFSv4.0은 여러 연결을 지원하는 반면, **nconnect**를 탑재한 NFSv4.1은 더 나은 부하 분산과 향상된 처리량을 제공합니다.

고객 지원

nconnect가 클라이언트 버전에서 지원되는지 확인하려면 NFS 클라이언트 설명서를 참조하십시오.

관련 정보

- ["NFSv4.1에 대한 ONTAP 지원에 대해 알아보세요"](#)
- ["NFSv4.2에 대한 ONTAP 지원에 대해 알아보세요"](#)

병렬 **NFS**에 대한 **ONTAP** 지원에 대해 알아보세요

ONTAP는 pNFS(parallel NFS)를 지원합니다. pNFS 프로토콜은 클라이언트가 클러스터의 여러 노드에 분산된 파일 세트에 직접 액세스할 수 있도록 함으로써 성능을 개선합니다. 클라이언트가 볼륨에 대한 최적의 경로를 찾는 데 도움이 됩니다.

ONTAP NFS 하드 마운트에 대해 알아보세요

장착 문제를 해결할 때 올바른 장착 유형을 사용하고 있는지 확인해야 합니다. NFS는 소프트웨어 마운트와 하드 마운트의 두 가지 마운트 유형을 지원합니다. 안정성을 위해 하드 마운트만

사용해야 합니다.

소프트 마운트를 사용하면 안 됩니다. 특히, NFS 시간 제한이 자주 발생할 가능성이 있습니다. 이러한 시간 초과로 인해 경합 상태가 발생하여 데이터가 손상될 수 있습니다.

병렬 NFS

소개

ONTAP 의 병렬 NFS(pNFS)에 대해 알아보세요

병렬 NFS는 2010년 1월 RFC-5661에 따라 RFC 표준으로 도입되었으며, 이를 통해 클라이언트가 메타데이터와 데이터 경로를 분리하여 NFSv4.1 서버의 파일 데이터에 직접 액세스할 수 있게 되었습니다. 이러한 직접 접근 방식은 데이터 현지화, CPU 효율성, 작업 병렬화를 통해 성능상의 이점을 제공합니다. 이후 2018년에는 pNFS 레이아웃 유형(RFC-8434)을 다루는 RFC가 작성되었으며, 이는 파일, 블록 및 객체 레이아웃에 대한 표준을 정의합니다. ONTAP pNFS 작업에 파일 레이아웃 유형을 활용합니다.



2024년 7월부터 이전에 PDF로 게시되었던 기술 보고서의 콘텐츠가 ONTAP 제품 문서에 통합되었습니다. ONTAP NFS 스토리지 관리 설명서에는 이제 _TR-4063: NetApp ONTAP의 병렬 네트워크 파일 시스템(pNFS)_의 내용이 포함되어 있습니다.

수년 동안 NFSv3는 거의 모든 사용 사례에 사용되는 NFS 프로토콜의 표준 버전이었습니다. 그러나 이 프로토콜에는 상태 저장 기능 부족, 기본적인 권한 모델, 기본 잠금 기능 등의 한계가 있었습니다. NFSv4.0(RFC 7530)은 NFSv3에 비해 여러 가지 개선 사항을 도입했으며, 병렬 NFS(pNFS)와 같은 기능이 추가된 후속 NFSv4.1(RFC 5661)과 NFSv4.2(RFC 7862) 버전에서 더욱 개선되었습니다.

NFSv4.x의 이점

NFSv4.x는 NFSv3에 비해 다음과 같은 이점을 제공합니다.

- NFSv4는 운영에 단일 포트(2049)만 사용하므로 방화벽에 친화적입니다.
- NFSv4.x의 위임과 같은 고급적이고 공격적인 캐시 관리
- 암호화를 사용하는 강력한 RPC 보안 선택
- 문자의 국제화
- 복합 연산
- TCP에서만 작동합니다
- 상태 저장 프로토콜(NFSv3과 같은 상태 비저장 프로토콜 아님)
- 효율적인 인증 메커니즘을 위한 전체 Kerberos 통합
- NFS 추천
- UNIX 및 Windows와 호환되는 액세스 제어 지원
- 문자열 기반 사용자 및 그룹 식별자
- pNFS(NFSv4.1)
- 확장된 속성(NFSv4.2)

- 보안 레이블(NFSv4.2)
- 스파스 파일 작업(FALLOCATE)(NFSv4.2)

모범 사례 및 기능에 대한 세부 정보를 포함하여 일반 NFSv4.x에 대한 자세한 내용은 다음을 참조하세요. "[NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드](#)".

관련 정보

- "[NFS 구성 개요](#)"
- "[NFS 관리 개요](#)"
- "[FlexGroup 볼륨 관리](#)"
- "[NFS 트렁킹 개요](#)"
- <https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf>
- "[NetApp 기술 보고서 4616: ONTAP에서 Microsoft Active Directory와 NFS Kerberos](#)"

ONTAP의 pNFS 아키텍처에 대해 알아보세요

pNFS 아키텍처는 세 가지 주요 구성 요소로 구성됩니다. pNFS를 지원하는 NFS 클라이언트, 메타데이터 작업을 위한 전용 경로를 제공하는 메타데이터 서버, 파일에 대한 로컬 경로를 제공하는 데이터 서버입니다.

pNFS에 대한 클라이언트 액세스에는 NFS 서버에서 사용 가능한 데이터 및 메타데이터 경로에 대한 네트워크 연결이 필요합니다. NFS 서버에 클라이언트가 접근할 수 없는 네트워크 인터페이스가 포함되어 있는 경우, 서버는 접근할 수 없는 클라이언트에 대한 데이터 경로를 광고할 수 있으며, 이로 인해 중단이 발생할 수 있습니다.

메타데이터 서버

pNFS의 메타데이터 서버는 NFS 서버에서 pNFS가 활성화된 경우 클라이언트가 NFSv4.1 이상을 사용하여 마운트를 시작하면 설정됩니다. 이 작업이 완료되면 모든 메타데이터 트래픽이 이 연결을 통해 전송되고 인터페이스가 다른 노드로 마이그레이션되더라도 마운트 기간 동안 이 연결에 남아 있게 됩니다.

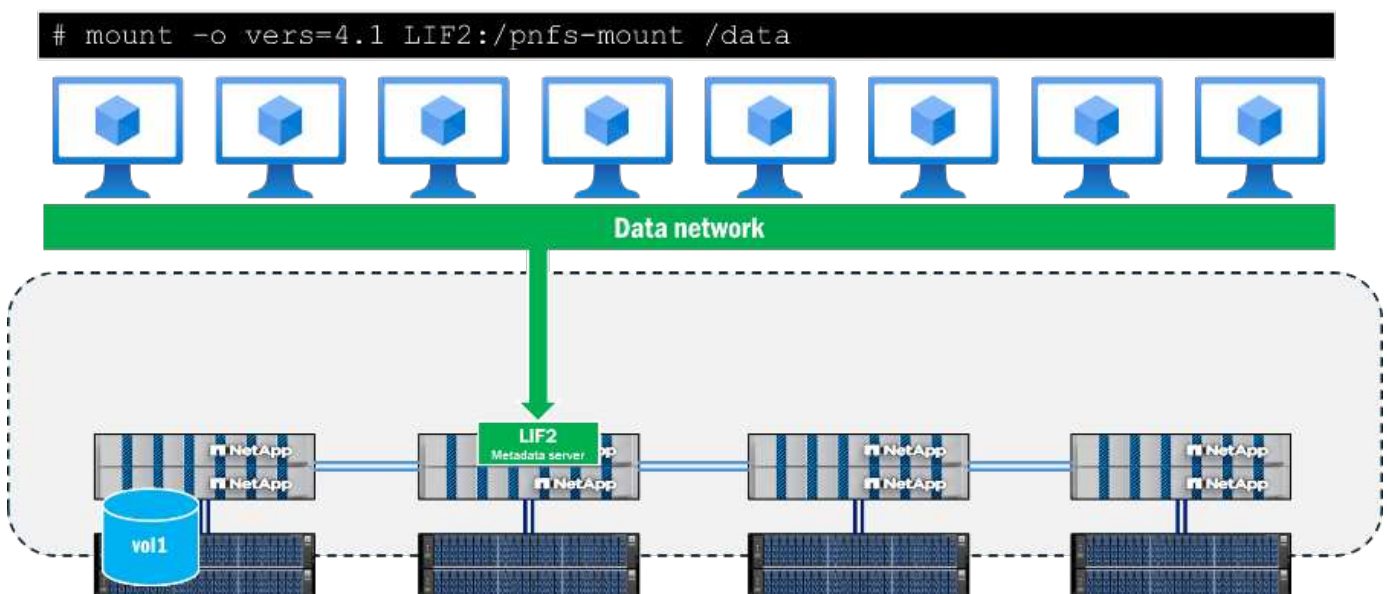


그림 1. ONTAP에서 pNFS에 메타데이터 서버를 구축합니다.

pNFS 지원은 마운트 호출 중, 특히 EXCHANGE_ID 호출에서 결정됩니다. 이는 NFS 작업 아래의 패킷 캡처에서 플래그로 볼 수 있습니다. pNFS 플래그가 있는 경우 EXCHGID4_FLAG_USE_PNFS_DS 그리고 EXCHGID4_FLAG_USE_PNFS_MDS 1로 설정된 경우 해당 인터페이스는 pNFS에서 데이터 작업과 메타데이터 작업 모두에 적합합니다.

```

  Operations (count: 1)
    Opcode: EXCHANGE_ID (42)
      Status: NFS4_OK (0)
      clientid: 0x004050a97100001c
      seqid: 0x00000001
      flags: 0x00060100, EXCHGID4_FLAG_USE_PNFS_DS, EXCHGID4_FLAG_USE_PNFS_MDS, EXCHGID4_FLAG_BIND_PRINC
        0... .. = EXCHGID4_FLAG_CONFIRMED_R: Not set
        .0... .. = EXCHGID4_FLAG_UPD_CONFIRMED_REC_A: Not set
        ....1... .. = EXCHGID4_FLAG_USE_PNFS_DS: Set
        ....1... .. = EXCHGID4_FLAG_USE_PNFS_MDS: Set
        ....0... .. = EXCHGID4_FLAG_USE_NON_PNFS: Not set
        ....1... .. = EXCHGID4_FLAG_BIND_PRINC_STATEID: Set
        ....0... .. = EXCHGID4_FLAG_SUPP_MOVED_MIGR: Not set
        ....0... .. = EXCHGID4_FLAG_SUPP_MOVED_REFER: Not set

```

그림 2. pNFS 마운트를 위한 패킷 캡처

NFS의 메타데이터는 일반적으로 파일 핸들, 권한, 액세스 및 수정 시간, 소유권 정보와 같은 파일 및 폴더 속성으로 구성됩니다. 메타데이터에는 통화 생성 및 삭제, 통화 연결 및 연결 해제, 이름 변경 등이 포함될 수 있습니다.

pNFS에는 pNFS 기능에 특정한 메타데이터 호출 하위 집합도 있으며 이에 대해서는 다음에서 자세히 설명합니다. "RFC 5661". 이러한 호출은 pNFS 적격 장치, 데이터 세트에 대한 장치 매핑 및 기타 필요한 정보를 결정하는 데 사용됩니다. 다음 표는 이러한 pNFS 관련 메타데이터 작업 목록을 보여줍니다.

작동	설명
레이아웃	메타데이터 서버에서 데이터 서버 맵을 가져옵니다.
레이아웃커밋	서버는 레이아웃을 커밋하고 메타데이터 맵을 업데이트합니다.
레이아웃 반환	데이터가 수정된 경우 레이아웃이나 새 레이아웃을 반환합니다.
장치 정보 가져오기	클라이언트는 스토리지 클러스터의 데이터 서버에서 업데이트된 정보를 받습니다.
장치 목록 가져오기	클라이언트는 스토리지 클러스터에 참여하는 모든 데이터 서버 목록을 요청합니다.
CB_레이아웃리콜	충돌이 감지되면 서버는 클라이언트에서 데이터 레이아웃을 다시 호출합니다.
CB_리콜_ANY	모든 레이아웃을 메타데이터 서버로 반환합니다.
CB_알림_장치ID	장치 ID 변경 사항을 알립니다.

데이터 경로 정보

메타데이터 서버가 설정되고 데이터 작업이 시작되면 ONTAP pNFS 읽기 및 쓰기 작업에 적합한 장치 ID와 클러스터의 볼륨을 로컬 네트워크 인터페이스와 연결하는 장치 매핑을 추적하기 시작합니다. 이 프로세스는 마운트에서 읽기 또는 쓰기 작업이 수행될 때 발생합니다. 메타데이터 호출(예: GETATTR. 이러한 장치 매핑은 실행되지 않습니다. 따라서 실행 1s 마운트 지점 내부의 명령을 사용해도 매핑이 업데이트되지 않습니다.

아래와 같이 고급 권한으로 ONTAP CLI를 사용하여 장치와 매핑을 볼 수 있습니다.


```

::*> pnfs devices show -vserver DEMO
(vserver nfs pnfs devices show)
Vserver Name      Mapping ID      Volume MSID      Mapping Status
Generation
-----
DEMO              16             2157024470      available        1

::*> pnfs devices mappings show -vserver SVM
(vserver nfs pnfs devices mappings show)
Vserver Name      Mapping ID      Dsid             LIF IP
-----
DEMO              16             2488             10.193.67.211

```



이 명령에는 볼륨 이름이 없습니다. 대신 해당 볼륨과 연관된 숫자 ID, 즉 마스터 세트 ID(MSID)와 데이터 세트 ID(DSID)가 사용됩니다. 매핑과 관련된 볼륨을 찾으려면 다음을 사용할 수 있습니다.
`volume show -dsid [dsid_numeric]` 또는 `volume show -msid [msid_numeric]`
 ONTAP CLI의 고급 권한으로.

클라이언트가 메타데이터 서버 연결과 원격인 노드에 있는 파일을 읽거나 쓰려고 시도하면 pNFS는 해당 작업에 대한 데이터 로컬리티를 보장하기 위해 적절한 액세스 경로를 협상하고 클라이언트는 파일에 액세스하기 위해 클러스터 네트워크를 탐색하는 대신 광고된 pNFS 장치로 리디렉션합니다. 이렇게 하면 CPU 오버헤드와 네트워크 지연 시간을 줄이는 데 도움이 됩니다.

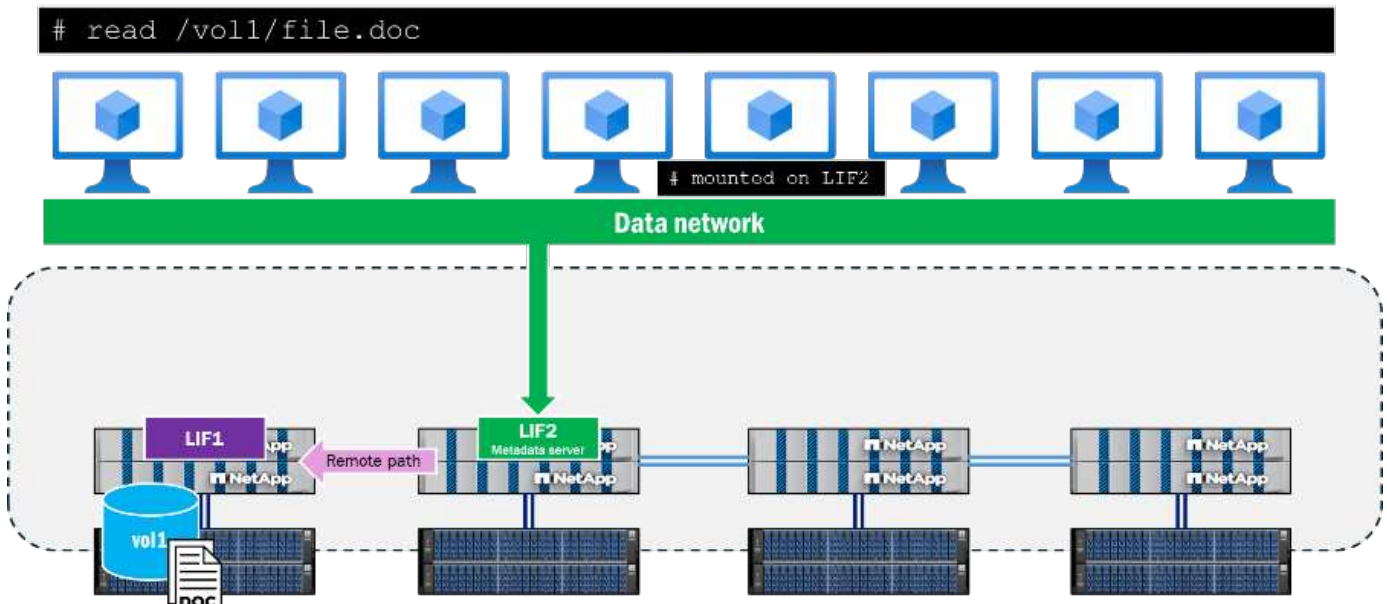


그림 3. pNFS 없이 NFSv4.1을 사용한 원격 읽기 경로

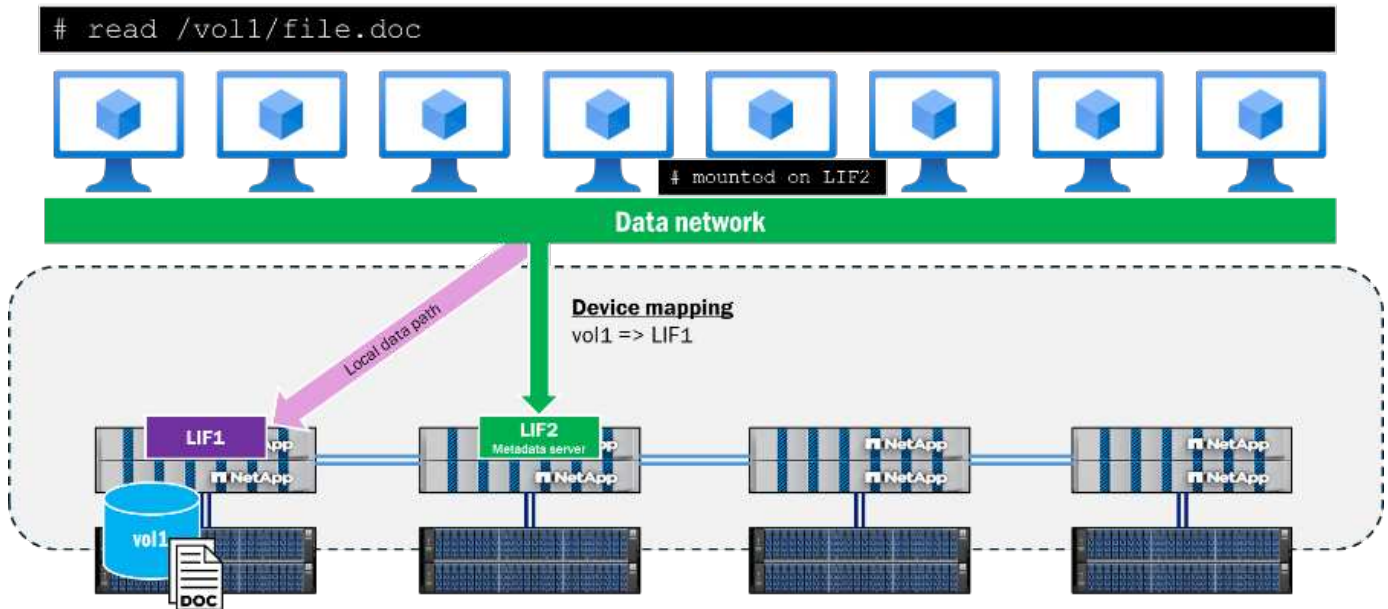


그림 4. pNFS를 사용한 로컬화된 읽기 경로

pNFS 제어 경로

pNFS의 메타데이터와 데이터 부분 외에도 pNFS 제어 경로도 있습니다. 제어 경로는 NFS 서버에서 파일 시스템 정보를 동기화하는 데 사용됩니다. ONTAP 클러스터에서 백엔드 클러스터 네트워크는 주기적으로 복제되어 모든 pNFS 장치와 장치 매핑이 동기화되도록 합니다.

pNFS 장치 채우기 워크플로

다음은 클라이언트가 볼륨의 파일을 읽거나 쓰라는 요청을 한 후 ONTAP 에서 pNFS 장치가 채워지는 방식을 설명합니다.

1. 클라이언트가 읽기 또는 쓰기를 요청하면 OPEN이 수행되고 파일 핸들이 검색됩니다.
2. OPEN이 수행되면 클라이언트는 메타데이터 서버 연결을 통해 LAYOUTGET 호출을 통해 파일 핸들을 저장소로 전송합니다.
3. LAYOUTGET은 상태 ID, 스트라이프 크기, 파일 세그먼트, 장치 ID 등 파일 레이아웃에 대한 정보를 클라이언트에 반환합니다.
4. 그런 다음 클라이언트는 장치 ID를 가져와 서버에 GETDEVINFO 호출을 보내 장치와 연결된 IP 주소를 검색합니다.
5. 저장소는 로컬에서 장치에 접속할 수 있는 관련 IP 주소 목록이 포함된 응답을 보냅니다.
6. 클라이언트는 저장소에서 다시 전송된 로컬 IP 주소를 통해 NFS 대화를 계속합니다.

pNFS와 FlexGroup 볼륨의 상호 작용

ONTAP 의 FlexGroup 볼륨은 클러스터의 여러 노드에 걸쳐 있는 FlexVol volume 구성 요소로 스토리지를 제공하므로 워크로드가 단일 마운트 지점을 유지하면서 여러 하드웨어 리소스를 활용할 수 있습니다. 여러 네트워크 인터페이스를 갖춘 여러 노드가 작업 부하와 상호 작용하므로 ONTAP 에서 원격 트래픽이 백엔드 클러스터 네트워크를 통과하는 것은 자연스러운 결과입니다.

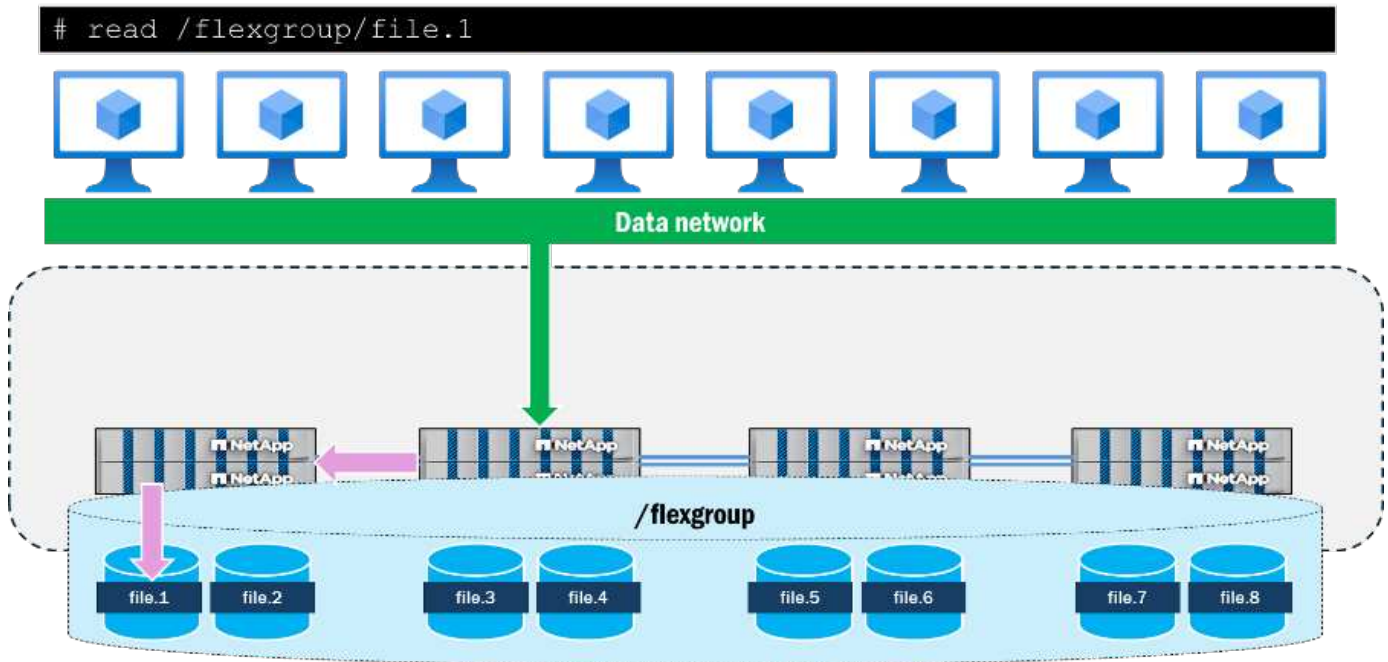


그림 5. pNFS 없이 FlexGroup 볼륨에서 단일 파일 액세스

pNFS를 활용할 때 ONTAP FlexGroup 볼륨의 파일 및 볼륨 레이아웃을 추적하고 이를 클러스터의 로컬 데이터 인터페이스에 매핑합니다. 예를 들어, 액세스 중인 파일이 포함된 구성 볼륨이 노드 1에 있는 경우 ONTAP 클라이언트에게 데이터 트래픽을 노드 1의 데이터 인터페이스로 리디렉션하도록 알립니다.

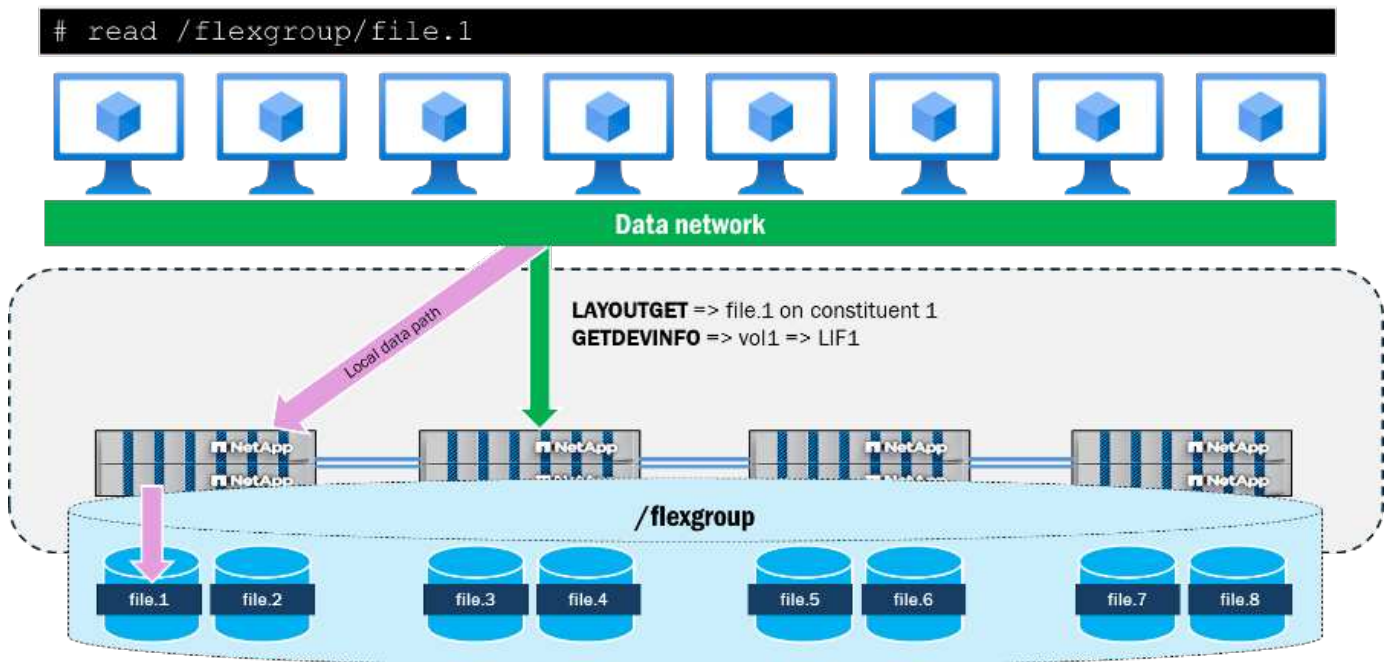


그림 6. pNFS를 사용한 FlexGroup 볼륨의 단일 파일 액세스

pNFS는 또한 pNFS가 없는 NFSv4.1에서는 제공하지 않는 단일 클라이언트의 파일에 대한 병렬 네트워크 경로를 제공합니다. 예를 들어, 클라이언트가 pNFS 없이 NFSv4.1을 사용하여 동일한 마운트에서 동시에 4개의 파일에 액세스하려는 경우 모든 파일에 동일한 네트워크 경로가 사용되고 ONTAP 클러스터는 대신 해당 파일에 원격 요청을 보냅니다. 모든 작업이 단일 경로를 따라 단일 노드에 도착하고 데이터 작업과 함께 메타데이터 작업도 처리하기 때문에 마운트 경로가 작업의 병목 현상이 될 수 있습니다.

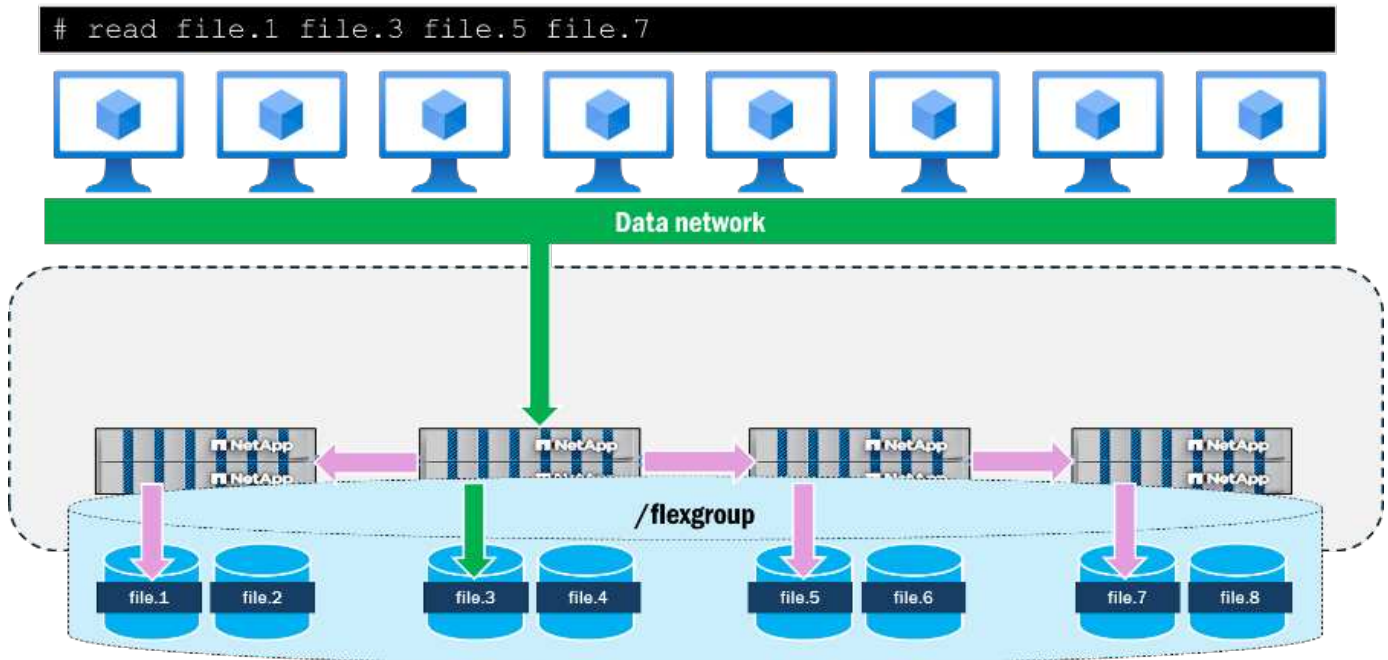


그림 7. pNFS 없이 FlexGroup 볼륨에서 여러 개의 동시 파일 액세스

pNFS를 사용하여 단일 클라이언트에서 동일한 4개 파일에 동시에 액세스하는 경우, 클라이언트와 서버는 파일을 사용하여 각 노드에 대한 로컬 경로를 협상하고 데이터 작업에 여러 TCP 연결을 사용하는 반면, 마운트 경로는 모든 메타데이터 작업의 위치 역할을 합니다. 이렇게 하면 파일에 대한 로컬 경로를 사용하여 지연 시간을 줄일 수 있을 뿐만 아니라, 클라이언트가 네트워크를 포화시킬 만큼 충분한 데이터를 전송할 수 있다면 여러 네트워크 인터페이스를 사용하여 처리량 이점을 추가할 수도 있습니다.

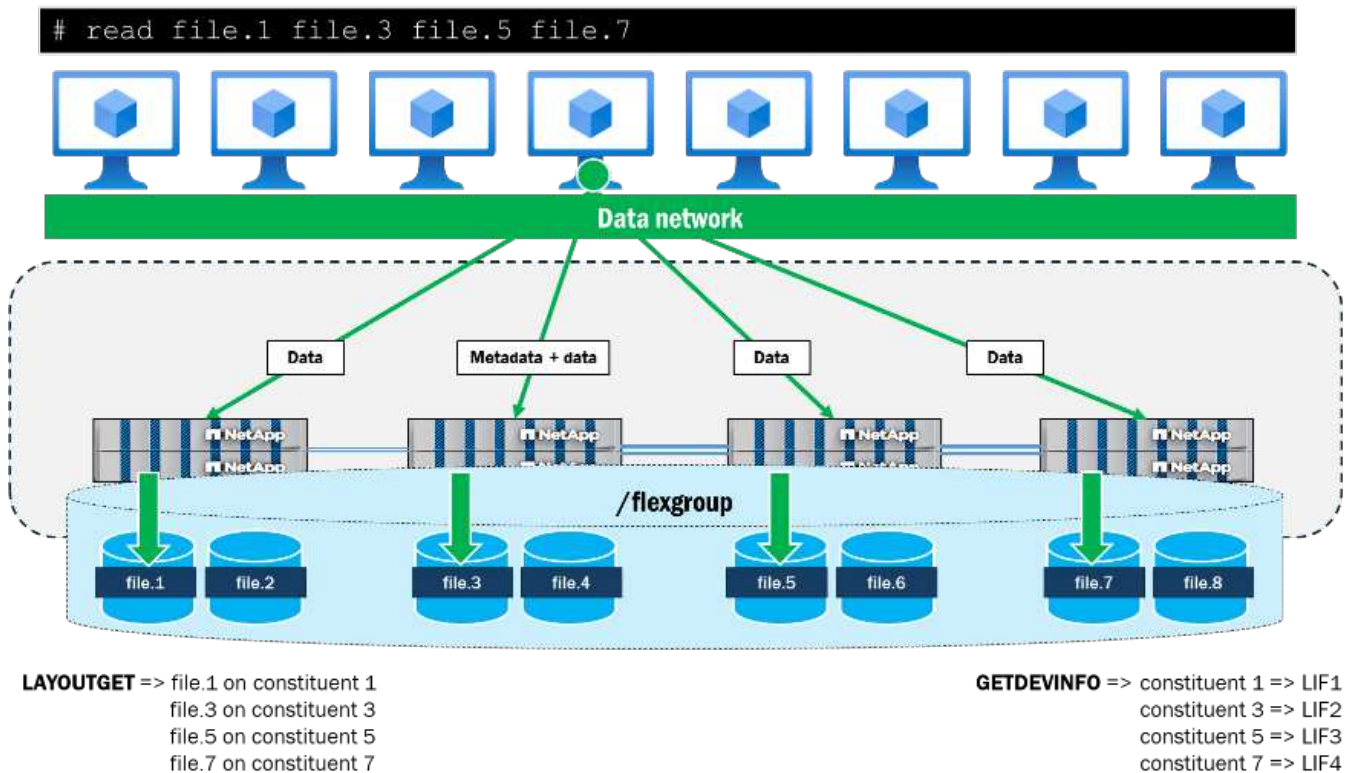


그림 8. pNFS를 사용한 FlexGroup 볼륨에서 여러 개의 동시 파일 액세스

다음은 4개의 10GB 파일(모두 2개의 ONTAP 클러스터 노드에 걸쳐 있는 다른 구성 볼륨에 있음)을 dd를 사용하여 병렬로 읽는 단일 RHEL 9.5 클라이언트에서 실행한 간단한 테스트 결과를 보여줍니다. 각 파일의 경우, pNFS를

사용하면 전체 처리량과 완료 시간이 향상되었습니다. pNFS 없이 NFSv4.1을 사용하는 경우, 마운트 지점에 로컬인 파일과 원격인 파일 간의 성능 차이가 pNFS를 사용하는 경우보다 컸습니다.

시험	파일당 처리량(MB/s)	파일당 완료 시간
NFSv4.1: pNFS 없음	• 파일.1-228(로컬) • 파일.2-227(로컬) • 파일.3-192(원격) • 파일.4-192(원격)	• 파일.1-46(로컬) • 파일.2-46.1(로컬) • 파일.3-54.5(원격) • 파일.4-54.5(원격)
NFSv4.1: pNFS 포함	• 파일.1-248(로컬) • 파일.2-246(로컬) • 파일.3-244(pNFS를 통한 로컬) • 파일.4-244(pNFS를 통한 로컬)	• 파일.1-42.3(로컬) • 파일.2-42.6(로컬) • 파일.3-43(pNFS를 통한 로컬) • 파일.4-43(pNFS를 통한 로컬)

관련 정보

- ["FlexGroup 볼륨 관리"](#)
- ["NetApp 기술 보고서 4571: FlexGroup 모범 사례"](#)

ONTAP 에서의 pNFS 사용 사례

pNFS는 다양한 ONTAP 기능과 함께 사용하여 성능을 개선하고 NFS 워크로드에 대한 유연성을 높일 수 있습니다.

nconnect를 사용한 pNFS

NFS는 최근의 일부 클라이언트와 서버에 새로운 마운트 옵션을 도입했는데, 이를 통해 단일 IP 주소를 마운트하는 동안 여러 TCP 연결을 제공할 수 있는 방법이 제공됩니다. 이를 통해 작업을 더 효율적으로 병렬화하고, NFS 서버와 클라이언트의 제한을 해결하고, 특정 작업 부하에 대한 전반적인 성능을 향상시킬 수 있는 메커니즘이 제공됩니다. 클라이언트가 nconnect를 지원하는 경우 ONTAP 9.8 이상에서 nconnect가 지원됩니다.

pNFS와 함께 nconnect를 사용하는 경우, NFS 서버에서 광고한 각 pNFS 장치에 대해 nconnect 옵션을 사용하여 연결이 병렬화됩니다. 예를 들어, nconnect가 4로 설정되어 있고 pNFS에 적합한 인터페이스가 4개 있는 경우, 생성되는 연결의 총 수는 마운트 지점당 최대 16개(nconnect 4개 x IP 주소 4개)가 됩니다.

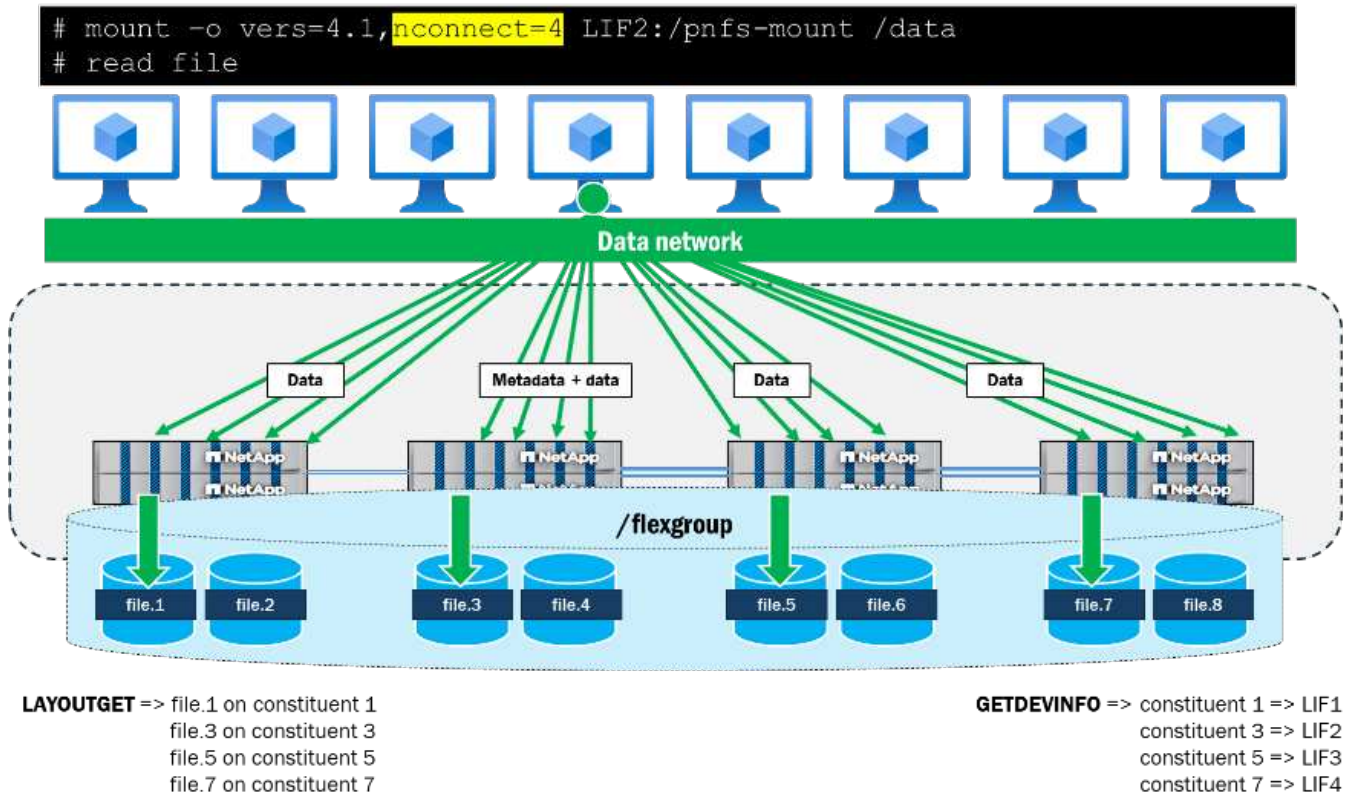


그림 9. nconnect가 4로 설정된 pNFS

"NFSv4.1에 대한 ONTAP 지원에 대해 자세히 알아보세요"

NFSv4.1 세션 트렁킹을 사용한 pNFS

NFSv4.1 세션 트렁킹 ("RFC 5661, 섹션 2.10.5")은 클라이언트와 서버 간에 여러 개의 TCP 연결을 사용하여 데이터 전송 속도를 높이는 것입니다. ONTAP 9.14.1에는 NFSv4.1 세션 트렁킹에 대한 지원이 추가되었으며 세션 트렁킹을 지원하는 클라이언트와 함께 사용해야 합니다.

ONTAP에서는 세션 트렁킹을 클러스터의 여러 노드에 걸쳐 사용하여 연결 전반에 걸쳐 추가 처리량과 중복성을 제공할 수 있습니다.

세션 트렁킹은 여러 가지 방법으로 설정할 수 있습니다.

- 마운트 옵션을 통해 자동으로 검색: 대부분의 최신 NFS 클라이언트에서 세션 트렁킹은 마운트 옵션을 통해 설정할 수 있습니다(OS 공급업체의 설명서 확인). 이 옵션은 NFS 서버에 신호를 보내 세션 트렁크에 대한 정보를 클라이언트로 다시 전송합니다. 이 정보는 NFS 패킷을 통해 나타납니다. fs_location4 부르다.

사용되는 마운트 옵션은 클라이언트의 OS 버전에 따라 달라집니다. 예를 들어, Ubuntu Linux 플레이어는 일반적으로 다음을 사용합니다. max_connect=n 세션 트렁크를 사용해야 한다는 신호를 보냅니다. RHEL Linux 배포판에서는 trunkdiscovery mount 옵션이 사용됩니다.

우분투 예제

```
mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
```

RHEL 예제

```
mount -o vers=4.1,truksdiscovery 10.10.10.10:/pNFS /mnt/pNFS
```



사용하려고 시도하는 경우 `max_connect` RHEL 배포판에서는 `nconnect`로 처리되며 세션 트렁킹이 예상대로 작동하지 않습니다.

- 수동으로 설정: 각 개별 IP 주소를 동일한 내보내기 경로와 마운트 지점에 마운트하여 세션 트렁킹을 수동으로 설정할 수 있습니다. 예를 들어, 동일한 노드에 두 개의 IP 주소(10.10.10.10 및 10.10.10.11)가 있는 경우 내보내기 경로 `/pNFS`, `mount` 명령을 두 번 실행합니다.

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

트렁크에 참여하려는 모든 인터페이스에서 이 과정을 반복합니다.



각 노드는 자체 세션 트렁크를 갖습니다. 줄기는 노드를 가로지르지 않습니다.



pNFS를 사용할 때는 세션 트렁킹 또는 `nconnect`만 사용하세요. 둘 다 사용하면 바람직하지 않은 동작이 발생할 수 있습니다. 예를 들어, 메타데이터 서버 연결만 `nconnect`의 이점을 얻고 데이터 서버는 단일 연결을 사용합니다.

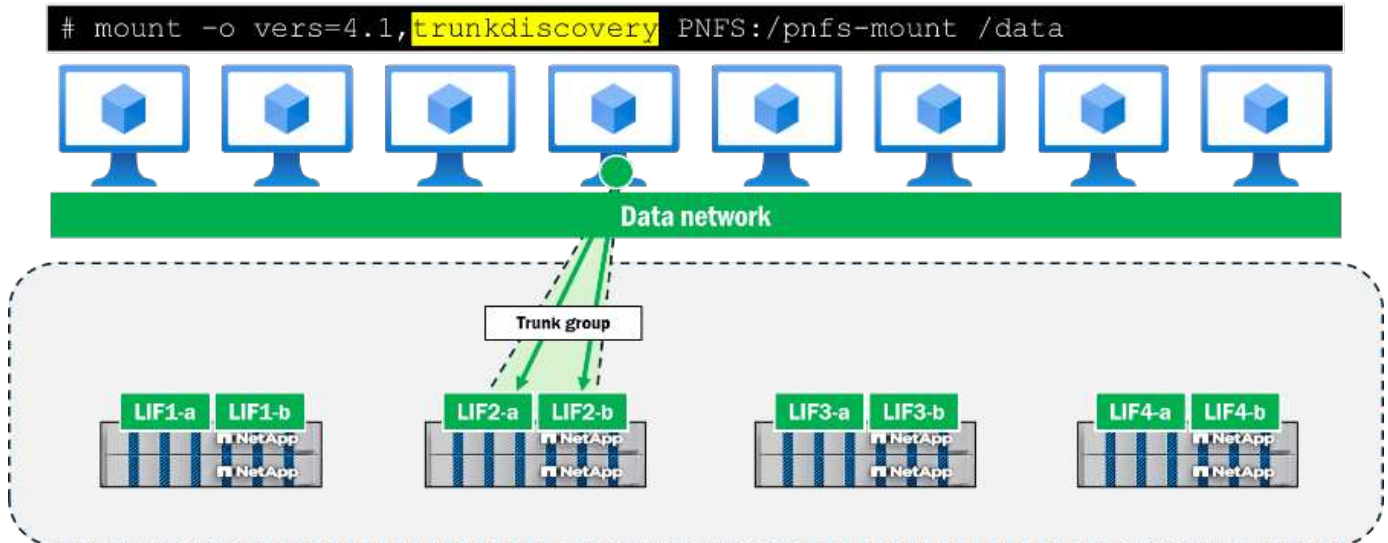
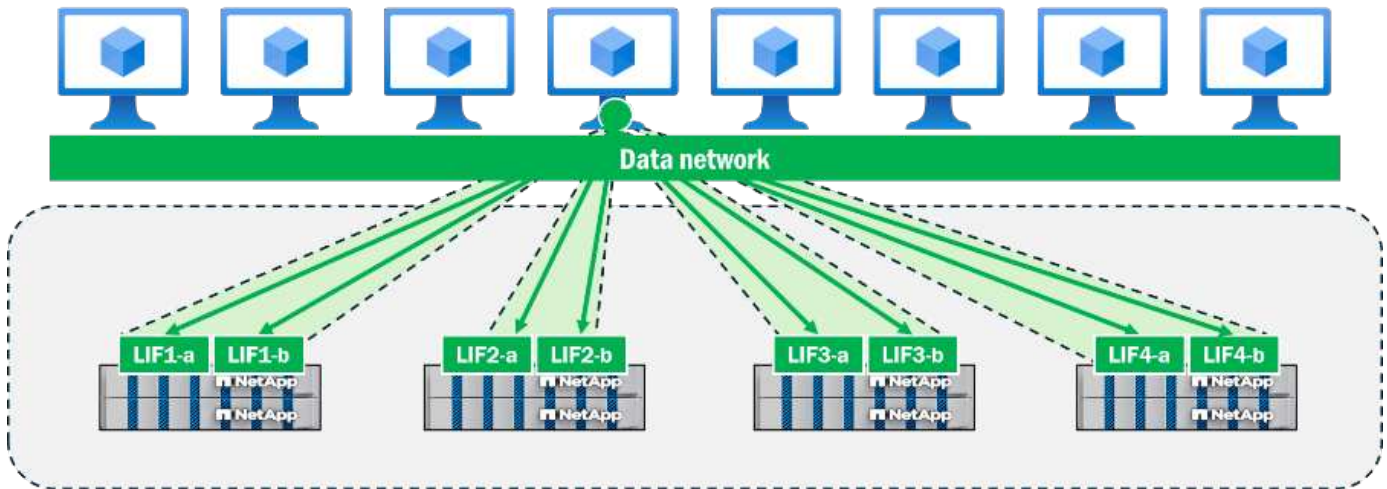


그림 10. ONTAP의 NFSv4.1 세션 트렁킹

pNFS는 클러스터에 참여하는 각 노드에 대한 로컬 경로를 제공할 수 있으며, 세션 트렁킹과 함께 사용하면 pNFS는 노드당 세션 트렁크를 활용하여 전체 클러스터의 처리량을 극대화할 수 있습니다.

```
# mount -o vers=4.1, trunkdiscovery PNFS:/pnfs-mount /data
```



언제 **trunkdiscovery** 이 사용되는 경우, 마운트 인터페이스가 위치한 NFS 서버 노드의 나열된 세션 트렁크 인터페이스에 대해 추가된 GETATTR 호출(FS_Locations)이 활용됩니다. 해당 주소가 반환되면 반환된 주소로 후속 마운트가 수행됩니다. 이는 마운트 중 패킷 캡처에서 확인할 수 있습니다.

198	1.219372			NFS	246	V4	Call (Reply In 199)	GETATTR FH: 0x787f5cf1
199	1.219579			NFS	238	V4	Reply (Call In 198)	GETATTR


```

  ▾ Opcode: SEQUENCE (53)
    Status: NFS4_OK (0)
    sessionid: 7100001e004090a90000000000000409
    seqid: 0x00000000
    slot id: 0
    high slot id: 63
    target high slot id: 63
    > status flags: 0x00000000
  ▾ Opcode: PUTFH (22)
    Status: NFS4_OK (0)
  ▾ Opcode: GETATTR (9)
    Status: NFS4_OK (0)
  ▾ Attr mask: 0x01000100 (FSID, FS_Locations)
    ▾ reqd_attr: FSID (8)
      > fattr4_fsid
    ▾ reco_attr: FS_Locations (24)
      ▾ fattr4_fs_locations
        pathname components: 0
        ▾ fs_location4
          num: 1
        ▾ fs_location4
          ▾ servers
            num: 1
            ▾ server: 
              length: 14
              contents: 
              fill bytes: opaque data
            pathname components: 0
  
```

그림 11. 마운트 중 NFS 세션 트렁크 검색: 패킷 캡처

"NFS 트렁킹에 대해 자세히 알아보세요"

pNFS 대 NFSv4.1 참조

NFSv4.1 참조는 마운트 요청 시 클라이언트를 볼륨 위치로 안내하는 초기 마운트 경로 리디렉션 모드를 제공합니다.

NFSv4.1 참조는 단일 SVM 내에서 작동합니다. 이 기능은 NFS 마운트를 데이터 볼륨과 동일한 노드에 있는 네트워크 인터페이스로 로컬화하려고 시도합니다. 클라이언트에 마운트된 동안 해당 인터페이스나 볼륨이 다른 노드로 이동하면 새로운 마운트가 설정될 때까지 데이터 경로는 더 이상 지역화되지 않습니다.

pNFS는 마운트 경로를 지역화하려고 시도하지 않습니다. 대신 마운트 경로를 사용하여 메타데이터 서버를 구축한 다음 필요에 따라 데이터 경로를 동적으로 로컬화합니다.

NFSv4.1 참조는 pNFS와 함께 사용할 수 있지만 해당 기능은 필요하지 않습니다. pNFS로 추천을 활성화해도 눈에 띄는 결과는 나타나지 않습니다.

"NFSv4 참조 활성화 또는 비활성화"

pNFS와 고급 용량 균형 조정의 상호 작용

"고급 용량 밸런싱" ONTAP에서는 FlexGroup 볼륨의 구성 볼륨에 파일 데이터의 일부를 기록합니다(단일 FlexVol 볼륨에서는 지원되지 않음). 파일이 커짐에 따라 ONTAP 같은 노드나 다른 노드에 있을 수 있는 다른 구성 볼륨의 새로운 멀티파트 inode에 데이터를 쓰기 시작하기로 결정합니다. 이러한 다중 inode 파일에 대한 쓰기, 읽기 및 메타데이터 작업은 클라이언트에 투명하고 중단 없이 수행됩니다. 고급 용량 밸런싱은 FlexGroup 구성 볼륨 간의 공간 관리를 개선하여 보다 일관된 성능을 제공합니다.

pNFS는 NFS 서버에 저장된 파일 레이아웃 정보에 따라 데이터 IO를 로컬 네트워크 경로로 리디렉션할 수 있습니다. 여러 구성 볼륨에 걸쳐 여러 부분으로 구성된 단일 대용량 파일이 생성되고 잠재적으로 클러스터의 여러 노드에 걸쳐 있을 때 ONTAP의 pNFS는 각 파일 부분에 로컬 트래픽을 제공할 수 있습니다. ONTAP 모든 파일 부분에 대한 파일 레이아웃 정보도 유지 관리하기 때문입니다. 파일을 읽을 때, 데이터 경로 지역성은 필요에 따라 변경됩니다.

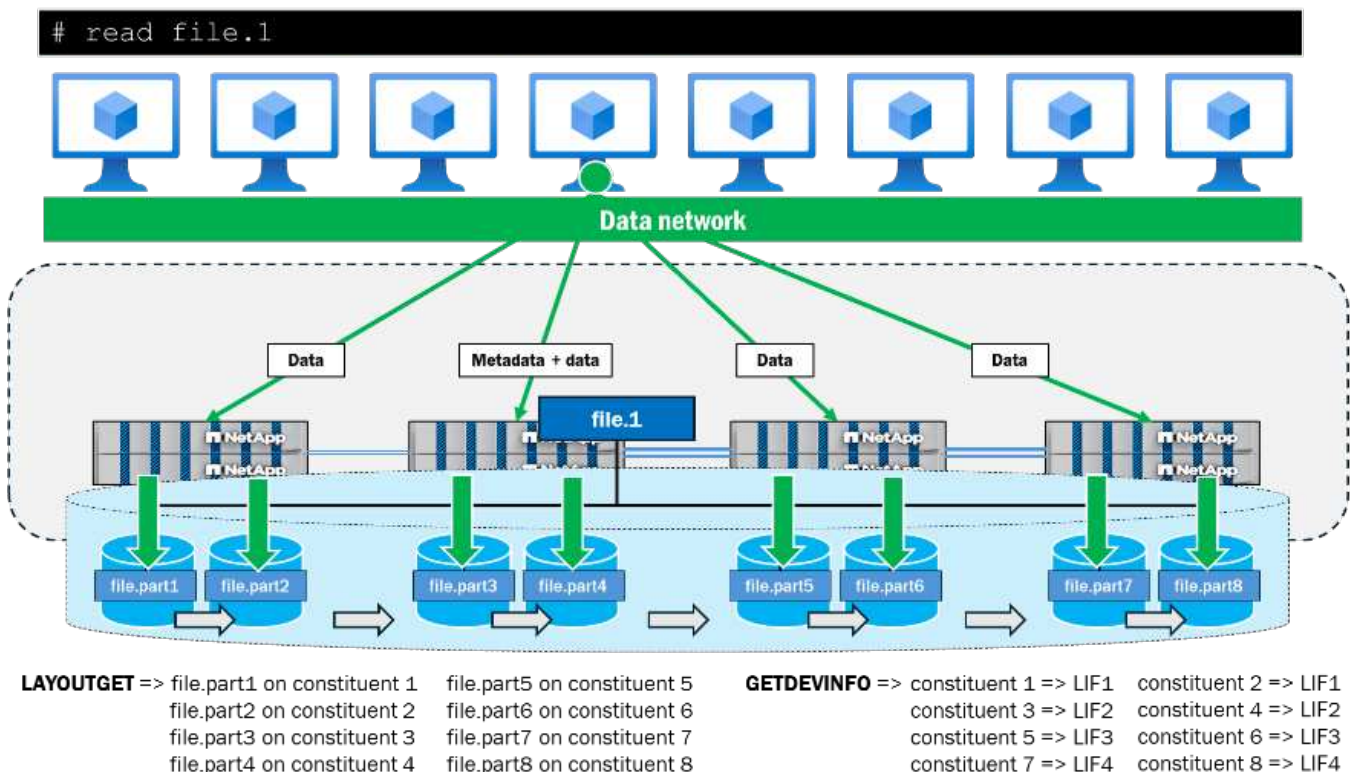


그림 12. pNFS를 통한 고급 용량 균형 조정

관련 정보

- "FlexGroup 볼륨 구성"

pNFS는 메타데이터와 데이터 경로를 분리하고, 데이터 지역화를 제공하며, 병렬 작업을 가능하게 하여 기존 NFS를 개선하기 위해 도입되었습니다.

기존 NFS의 과제와 pNFS의 이점

다음 표는 기존 NFS의 문제점을 보여주고 ONTAP 의 pNFS가 이를 어떻게 해결하는지 설명합니다.

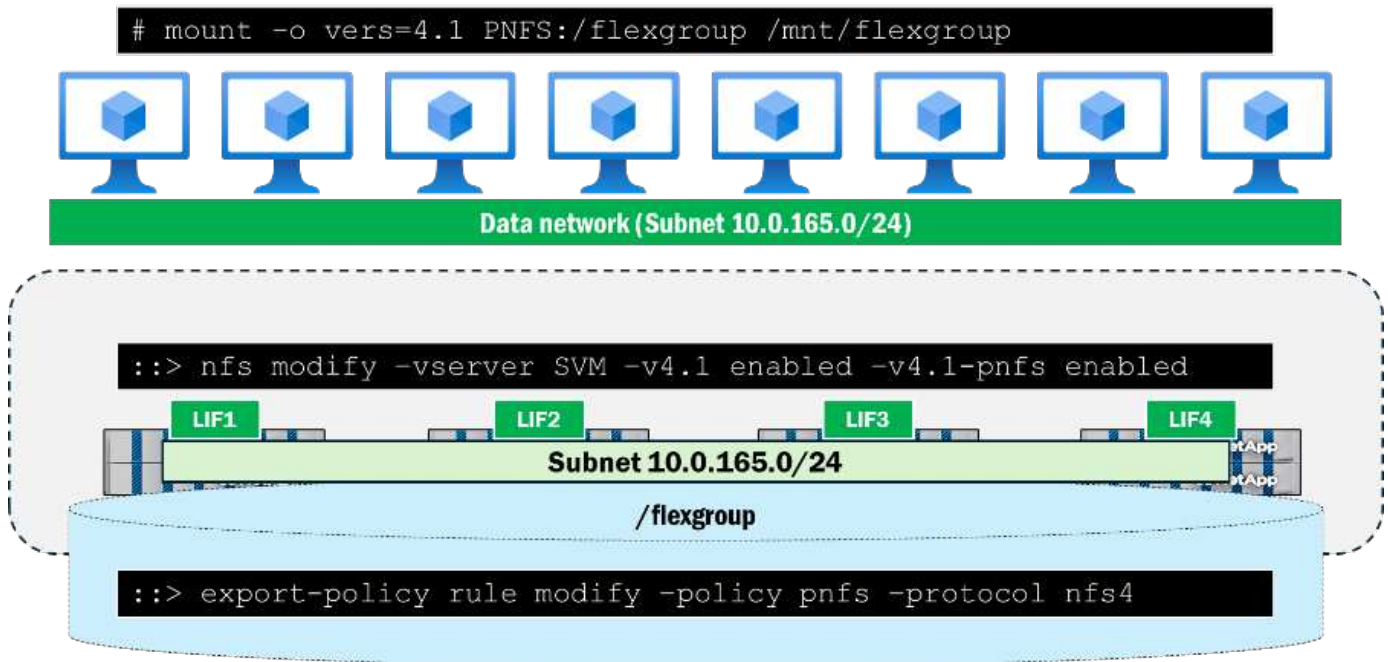
도전	pNFS의 이점
메타데이터와 데이터의 동일한 경로 기존 NFS에서는 메타데이터와 데이터가 동일한 경로를 통과하므로 네트워크와 CPU가 모두 포화 상태가 될 수 있습니다. 단일 경로가 클러스터의 단일 하드웨어 노드에 연결되기 때문입니다. 많은 사용자가 동일한 NFS 내보내기에 액세스하려고 시도하는 경우 이러한 문제는 더욱 악화됩니다.	메타데이터와 데이터 경로가 분리되어 있으며, 데이터 경로가 병렬화되어 있습니다 NFS 트래픽에 대한 메타데이터와 데이터 경로를 분리하고 데이터 경로에 대해 여러 네트워크 경로를 제공함으로써 ONTAP 클러스터에서 CPU 및 네트워크 리소스가 극대화되어 워크로드에 대한 확장성이 향상됩니다.
작업 부하 분산 과제 ONTAP NAS 클러스터에서는 최대 24개의 노드를 가질 수 있으며, 각 노드는 고유한 데이터 볼륨과 네트워크 인터페이스 세트를 가질 수 있습니다. 각 볼륨은 자체 워크로드 또는 워크로드의 하위 집합을 호스팅할 수 있으며 FlexGroup 볼륨을 사용하면 간소화를 위해 해당 워크로드가 단일 네임스페이스에 액세스하는 여러 노드에 존재할 수 있습니다. 클라이언트가 NFS 내보내기를 마운트하면 네트워크 트래픽이 단일 노드에 설정됩니다. 액세스하는 데이터가 클러스터 내의 별도 노드에 있는 경우 원격 트래픽이 발생하여 작업 부하에 지연이 발생하고 관리가 복잡해질 수 있습니다.	데이터 구조에 대한 로컬 병렬 경로 pNFS는 메타데이터에서 데이터 경로를 분리하고 클러스터 내 볼륨의 로컬성에 따라 여러 병렬 데이터 경로를 제공하므로 클러스터 내 네트워크 트래픽의 거리를 줄이고 클러스터 내 여러 하드웨어 리소스를 활용하여 대기 시간을 줄일 수 있습니다. 또한 ONTAP 의 pNFS는 데이터 트래픽을 자동으로 리디렉션하므로 관리자가 여러 개의 내보내기 경로와 위치를 관리할 필요성이 줄어듭니다.
NFS 마운트 지점의 재배치 마운트 지점이 설정된 후에는 볼륨을 마운트 해제하고 다시 마운트하는 것이 방해가 될 수 있습니다. ONTAP 노드 간에 네트워크 인터페이스를 마이그레이션하는 기능을 제공하지만, 이로 인해 관리 오버헤드가 발생하고 NFSv4.x를 사용하는 상태 저장 NFS 연결에 방해가 됩니다. 마운트 지점을 이전하는 이유 중 일부는 데이터 지역성 문제와 관련이 있습니다.	자동 경로 재배치 pNFS를 사용하면 NFS 서버는 네트워크 인터페이스와 볼륨의 위치 테이블을 유지 관리합니다. pNFS의 메타데이터 경로를 통해 클라이언트로부터 데이터 구조가 요청되면 서버는 클라이언트에 최적화된 네트워크 경로를 전달하고, 클라이언트는 해당 경로를 데이터 작업에 사용합니다. 이를 통해 작업 부하에 대한 관리 오버헤드가 크게 줄어들고 어떤 경우에는 성능이 향상될 수 있습니다.

구성 요구 사항

NetApp ONTAP 에서 pNFS를 구성하려면 다음이 필요합니다.

- pNFS를 지원하고 NFSv4.1 이상으로 마운트된 NFS 클라이언트
- ONTAP 의 NFS 서버에서 NFSv4.1이 활성화됨 (`nfs modify -v4.1 enabled`; 기본적으로 꺼짐)
- ONTAP 의 NFS 서버에서 pNFS가 활성화됨 (`nfs modify -v4.1-pnfs enabled`; 기본적으로 비활성화됨)

- 노드당 최소 하나의 네트워크 인터페이스가 NFS 클라이언트로 라우팅 가능
- NFSv4를 허용하는 내보내기 정책 및 규칙이 있는 SVM의 데이터 볼륨



위의 구성 요구 사항을 충족하면 pNFS는 그 자체로 작동합니다.

관련 정보

- ["NFS 구성"](#)
- ["NFSv4.1에 대한 ONTAP 지원"](#)
- ["pNFS용 네트워크 인터페이스 연결"](#)

계획

pNFS 배포 계획

사용자 환경에 pNFS를 배포하기 전에 전제 조건을 충족하는지 확인하고 상호 운용성 요구 사항과 구성 제한 사항을 이해해야 합니다.

필수 구성 요소

ONTAP 에서 pNFS를 활성화하고 사용하기 전에 다음 요구 사항이 충족되는지 확인하세요.

- NFS 서버에서 NFSv4.1 이상이 활성화되어 있습니다.
- 적어도 하나 **"데이터 LIF는 노드당 존재합니다."** NFS 서버를 호스팅하는 SVM의 클러스터에서
- 모두 **"SVM의 데이터 LIF는 라우팅 가능합니다."** NFS 클라이언트에
- NFS 클라이언트는 pNFS를 지원합니다(2014년 이후의 대부분의 최신 Linux 배포판).
- SVM의 클라이언트와 모든 데이터 LIF 간의 네트워크 연결이 작동합니다.
- 모든 데이터 LIF에 대해 DNS 확인(호스트 이름 사용 시)이 올바르게 구성되었습니다.

- "FlexGroup 볼륨" 구성됨(최상의 결과를 위해 권장됨)
- "NFSv4.x ID 도메인이 일치합니다." 클라이언트와 ONTAP 간
- "NFS 케르베로스" (사용되는 경우) SVM의 모든 데이터 LIF에서 활성화됩니다.

모범 사례 요약

사용자 환경에서 pNFS를 구현할 때 다음 모범 사례를 따르세요.

- 사용 "FlexGroup 볼륨" 최상의 성능과 용량 확장을 위해
- 모든 것을 확인하십시오 "SVM의 네트워크 인터페이스는 라우팅 가능합니다." 고객에게
- "NFSv4.0을 해제합니다" 클라이언트가 NFSv4.1 이상을 사용하도록 하려면
- 여러 네트워크 인터페이스와 노드에 걸쳐 마운트 포인트를 분산합니다.
- 라운드 로빈 DNS를 사용하세요 "부하 분산 메타데이터 서버"
- 확인하다 "NFSv4.x ID 도메인이 일치합니다." 클라이언트와 서버에서
- 지휘하다 "네트워크 인터페이스 마이그레이션" 그리고 "스토리지 장애 조치" 유지 관리 기간 동안
- 할 수 있게 하다 "NFS 케르베로스" Kerberos 보안을 사용하는 경우 모든 데이터 LIF에 대해
- 사용을 피하세요 "NFSv4.1 참조" pNFS를 사용할 때
- 시험 "nconnect 설정" TCP 연결 제한이 너무 커지지 않도록 주의하세요.
- 고려하다 "세션 트렁킹" 대안으로 "nConnect(연결)" (둘을 함께 사용하지 마세요)
- 확인하다 "클라이언트 OS 공급업체 지원" 배포 전 pNFS용

상호 운용성

ONTAP 의 pNFS는 RFC 호환 NFS 클라이언트와 함께 작동하도록 설계되었습니다. 다음 고려 사항이 적용됩니다.

- 가장 현대적인 "2014년 이후의 Linux 배포판" pNFS 지원(RHEL 6.4, Fedora 17 이상)
- pNFS가 지원되는지 클라이언트 OS 공급업체에 확인하세요.
- pNFS는 FlexVol 과 함께 작동합니다. "FlexGroup 볼륨"
- pNFS는 NFSv4.1에서 지원됩니다. "NFSv4.2"
- pNFS는 다음과 함께 사용할 수 있습니다. "NFS 케르베로스" (krb5, krb5i, krb5p) 하지만 성능에 영향을 미칠 수 있습니다.
- pNFS는 다음과 함께 사용할 수 있습니다. "nConnect(연결)" 또는 "세션 트렁킹" (하지만 동시에 두 가지를 할 수는 없음)
- pNFS는 작동하지 않습니다 "NFSv4.0"

제한

ONTAP 의 pNFS에는 다음 제한이 적용됩니다.

- "TCP 연결 제한" 노드당 플랫폼에 따라 다릅니다(특정 제한 사항은 NetApp Hardware Universe 확인하세요)
- 최대 파일 크기: 볼륨 유형 및 ONTAP 버전에 따라 다름

- 최대 파일 수: 최대 2000억 개의 파일 ["FlexGroup 볼륨"](#)
- 최대 용량: 최대 60PB ["FlexGroup 볼륨"](#)
- ["네트워크 인터페이스 수"](#): 노드당 최소 하나의 데이터 LIF가 필요합니다. 부하 분산을 위해 더 필요할 수 있습니다.

사용시 ["pNFS와 연결"](#)TCP 연결 수가 빠르게 증가한다는 점을 알아두세요.

- nconnect를 사용한 각 클라이언트 마운트는 데이터 LIF당 여러 개의 TCP 연결을 생성합니다.
- 많은 클라이언트가 높은 nconnect 값을 사용하므로 ["TCP 연결 제한"](#) 초과될 수 있습니다
- TCP 연결 제한을 초과하면 기존 연결이 해제될 때까지 새 연결이 차단됩니다.

관련 정보

- ["pNFS용 네트워크 인터페이스 연결"](#)
- ["NFSv4.1 활성화 또는 비활성화"](#)
- ["NFSv4.1에 대한 ONTAP 지원"](#)
- ["NFSv4.2에 대한 ONTAP 지원"](#)
- ["NetApp Hardware Universe를 참조하십시오"](#)

pNFS 튜닝 및 성능 모범 사례

ONTAP 에서 pNFS를 사용할 때 최상의 결과를 얻으려면 다음 고려 사항과 모범 사례를 활용하세요.

볼륨 유형 권장 사항

ONTAP 의 pNFS는 FlexVol 볼륨과 FlexGroup 볼륨 모두에서 작동하지만, 가장 좋은 전반적인 결과를 얻으려면 FlexGroup 볼륨을 사용하세요.

FlexGroup 볼륨은 다음을 제공합니다.

- pNFS가 데이터 트래픽을 로컬화할 수 있도록 하면서 클러스터의 여러 하드웨어 리소스를 포괄할 수 있는 단일 마운트 지점
- 대용량 가능성(최대 60PB) 및 많은 파일 수(최대 2000억 개의 파일)
- 용량 균형 조정 및 잠재적 성능 이점을 위한 다중 파트 파일 지원
- 단일 작업 부하를 지원하는 볼륨 및 하드웨어에 대한 병렬 액세스

["FlexGroup 볼륨 관리에 대해 알아보세요"](#)

고객 추천

모든 NFS 클라이언트가 pNFS를 지원하는 것은 아니지만, 대부분의 최신 클라이언트는 pNFS를 지원합니다. RHEL 6.4와 Fedora 17이 최초로 pNFS를 지원한 클라이언트(대략 2014년)였으므로, 지난 몇 년 동안 출시된 클라이언트 버전은 이 기능을 완벽하게 지원한다고 추정하는 것이 타당합니다. ONTAP의 NFS 지원 입장은 "클라이언트가 해당 기능을 지원하고 RFC를 준수하며, 당사가 해당 기능을 지원하는 경우 해당 조합은 지원됩니다."입니다. 하지만 클라이언트 OS 공급업체가 pNFS를 지원하는지 확인하는 것이 가장 좋습니다.

볼륨 이동

ONTAP 동일한 클러스터 내의 노드나 집계 간에 볼륨을 중단 없이 이동할 수 있는 기능을 제공하여 용량과 성능 균형을 유연하게 조절할 수 있습니다. ONTAP 에서 볼륨 이동이 발생하면 pNFS 장치 매핑이 자동으로 업데이트되어 필요한 경우 클라이언트에게 새로운 볼륨-인터페이스 관계를 사용하도록 알립니다.

"볼륨 이동에 대해 알아보세요"

네트워크 인터페이스 마이그레이션

ONTAP 동일한 클러스터 내의 노드 간에 네트워크 인터페이스를 이동하여 성능 균형과 유지 관리 유연성을 제공하는 기능을 제공합니다. 볼륨 이동과 마찬가지로 ONTAP 에서 네트워크 인터페이스 마이그레이션이 발생하면 pNFS 장치 매핑이 자동으로 업데이트되어 필요한 경우 클라이언트에게 새로운 볼륨-인터페이스 관계를 사용하도록 알립니다.

그러나 NFSv4.1은 상태 저장 프로토콜이므로 네트워크 인터페이스 마이그레이션은 NFS 마운트를 적극적으로 사용하는 클라이언트에 방해가 될 수 있습니다. 유지 관리 창에서 네트워크 인터페이스 마이그레이션을 수행하고 잠재적인 네트워크 중단에 대해 클라이언트에게 알리는 것이 가장 좋습니다.

스토리지 장애 조치/환불

pNFS는 NFSv4.1과 동일한 저장소 장애 조치 고려 사항을 따릅니다. 이것들은 다음에서 자세히 다루어집니다.

["NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"](#)일반적으로 pNFS와 관련된 모든 저장소 장애 조치/환불은 프로토콜의 상태성으로 인해 잠재적인 저장소 중단이 예상되므로 유지 관리 창에서 수행해야 합니다.

메타데이터 워크로드

메타데이터 작업은 크기가 작지만 작업 부하에 따라 숫자가 많아질 수 있습니다(대량의 파일을 만들고 있습니까? "찾기" 명령을 실행하고 있습니까? 그리고 총 파일 개수. 결과적으로 메타데이터 호출이 많은 작업 부하는 NFS 서버의 CPU에 부담을 주고 단일 연결에서 병목 현상이 발생할 가능성이 있습니다. pNFS(및 일반적으로 NFSv4.x)는 프로토콜 버전의 상태 저장, 잠금 메커니즘 및 일부 보안 기능이 CPU 사용률과 지연 시간에 부정적인 영향을 미칠 수 있으므로 성능에 따라 달라지는 높은 메타데이터 작업 부하는 적합하지 않습니다. 이러한 작업 유형(높은 GETATTR 또는 SETATTR 등)은 일반적으로 NFSv3에서 더 나은 성능을 보입니다.

메타데이터 서버

pNFS의 메타데이터 서버는 NFS 내보내기의 초기 마운트 시 설정됩니다. 마운트 지점이 설정되면 다시 마운트되거나 데이터 인터페이스가 이동될 때까지 그 자리에 유지됩니다. 이러한 이유로 동일한 볼륨에 액세스하는 여러 클라이언트가 SVM 전반에서 서로 다른 노드와 데이터 인터페이스에 마운트되도록 하는 것이 가장 좋습니다. 이 접근 방식은 클러스터의 네트워크 인터페이스를 극대화하는 동시에 노드와 CPU 리소스 전반에 걸쳐 메타데이터 서버의 부하를 분산합니다. 이를 달성하는 한 가지 방법은 라운드 로빈 DNS 설정을 설정하는 것입니다. ["NetApp 기술 보고서 4523: ONTAP의 DNS 부하 분산"](#).

NFSv4.x ID 도메인

NFSv4.x는 여러 가지 방법으로 보안 기능을 제공합니다(자세한 내용은 다음에서 다룹니다. ["NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"](#)). NFSv4.x ID 도메인은 NFS 내보내기에서 사용자와 그룹을 인증하려고 할 때 클라이언트와 서버가 ID 도메인에 동의해야 하는 방법 중 하나입니다. ID 도메인 불일치의 부작용 중 하나는 원치 않는 액세스를 방지하기 위해 사용자 또는 그룹이 익명화된 사용자(기본적으로 압축됨)로 표시되는 것입니다. NFSv4.x(및 pNFS)를 사용하는 경우 클라이언트와 서버에서 NFSv4.x ID 도메인이 일치하는지 확인하는 것이 가장 좋습니다.

nConnect(연결)

앞서 언급했듯이 ONTAP의 nconnect는 일부 작업 부하에서 성능을 개선하는 데 도움이 될 수 있습니다. pNFS를 사용하는 경우 nconnect가 스토리지 시스템에 대한 총 TCP 연결 수를 크게 늘려 성능을 향상시킬 수 있지만, 많은 클라이언트가 마운트 옵션을 활용할 경우 스토리지의 TCP 연결에 과부하가 걸려 문제가 발생할 수도 있다는 점을 이해하는 것이 중요합니다. NetApp Hardware Universe 노드당 TCP 연결 제한을 다룹니다.

노드의 TCP 연결 제한을 초과하면 기존 연결이 해제될 때까지 새로운 TCP 연결이 허용되지 않습니다. 이는 폭풍우가 잦은 환경에서는 복잡한 문제를 야기할 수 있습니다.

다음 표는 nconnect를 사용한 pNFS가 TCP 연결 제한을 초과할 수 있는 방식을 보여줍니다.

클라이언트 수	nconnect 값	마운트당, 노드당 총 잠재적 TCP 연결 수
1	4	4
100	4	400
1000입니다	8	8000
10000	8	80000
10000	16	160000 ¹

¹ 대부분의 ONTAP 단일 노드 TCP 연결 제한을 초과합니다.

NFSv4.1 세션 트렁킹

ONTAP의 세션 트렁킹을 사용하면 NFSv4.x 마운트에 대한 처리량과 경로 복원력을 높일 수 있습니다. pNFS와 함께 사용하면 클러스터의 각 노드가 세션 트렁크를 설정할 수 있습니다. 그러나 세션 트렁크는 노드당 최소 두 개의 인터페이스가 필요하고, pNFS는 의도한 대로 작동하려면 노드당 최소 하나의 인터페이스가 필요합니다. 또한 SVM의 모든 인터페이스는 NFS 클라이언트로 라우팅될 수 있어야 합니다. nconnect를 활용할 경우 세션 트렁킹과 pNFS가 제대로 작동하지 않습니다. nconnect와 세션 트렁킹은 상호 배타적인 기능으로 간주하세요.

"NFS 트렁킹에 대해 알아보세요"

네트워크 인터페이스 연결

pNFS가 제대로 작동하려면 클러스터의 각 노드에 라우팅 가능한 네트워크 인터페이스가 필요합니다. pNFS를 호스팅하는 NFS 서버와 동일한 SVM에 NFS 클라이언트로 라우팅할 수 없는 다른 네트워크 인터페이스가 있는 경우 ONTAP 여전히 클라이언트에 대한 장치 매핑에서 해당 인터페이스를 광고합니다. NFS 클라이언트가 다른 서브넷의 인터페이스를 통해 데이터에 액세스하려고 하면 연결할 수 없게 되어 서비스 중단이 발생합니다. pNFS를 사용할 때 클라이언트가 액세스할 수 있는 SVM의 네트워크 인터페이스만 허용하는 것이 가장 좋습니다.



기본적으로 pNFS는 SVM에 있는 모든 데이터 LIF가 NFS 클라이언트의 인터페이스로 라우팅 가능해야 합니다. 왜냐하면 pNFS 장치 목록에는 SVM에 있는 모든 데이터 LIF가 포함되기 때문입니다. 결과적으로 라우팅 불가능한 데이터 LIF가 선택될 수 있으며, 이는 서비스 중단 상황을 초래할 수 있습니다. 모범 사례로, pNFS를 사용할 때만 라우팅 가능한 데이터 LIF를 구성하십시오.

ONTAP 9.18.1 RC1 이상 버전부터는 서브넷별로 pNFS 트래픽에 사용할 수 있는 인터페이스를 지정할 수 있으므로 라우팅 가능한 인터페이스와 라우팅 불가능한 인터페이스를 혼합하여 사용할 수 있습니다. 해당 명령어에 대한 자세한 내용은 NetApp 지원팀에 문의하십시오.

NFSv4.0

NFSv4.0은 NFSv4.1과 함께 ONTAP NFS 서버에서 활성화할 수 있는 옵션입니다. 하지만 pNFS는 NFSv4.0에서는 작동하지 않습니다. NFS 서버에서 NFSv4.0이 활성화된 경우 클라이언트가 자신도 모르게 해당 프로토콜 버전을 마운트할 가능성이 있으며 pNFS를 활용할 수 없습니다. 따라서 pNFS를 사용할 때 NFSv4.0을 명시적으로 비활성화하는 것이 가장 좋습니다. NFSv4.1은 여전히 활성화되어 있어야 하며 NFSv4.0과 독립적으로 작동할 수 있습니다.

NFSv4.1 참조

NFSv4.1 참조는 볼륨을 소유한 노드의 네트워크 인터페이스로의 클라이언트에서 마운트 경로를 지역화합니다. pNFS는 데이터 경로를 지역화하고, 마운트 경로는 메타데이터 서버가 됩니다.

두 기능을 함께 사용할 수는 있지만, pNFS와 함께 NFSv4.1 참조를 사용하면 동일한 노드에 여러 메타데이터 서버를 쌓아 여러 클러스터 노드에 메타데이터 서버를 분산하는 기능이 저하되는 바람직하지 않은 효과가 발생할 수 있습니다. pNFS를 사용할 때 메타데이터 서버가 클러스터 전체에 고르게 분산되지 않으면 단일 노드의 CPU가 메타데이터 요청으로 과부하가 걸려 성능 병목 현상이 발생할 수 있습니다.

따라서 pNFS를 사용할 때 NFSv4.1 참조를 사용하지 않는 것이 가장 좋습니다. 대신, 클러스터의 여러 네트워크 인터페이스와 노드에 마운트 포인트를 분산하세요.

["NFSv4 참조 활성화 또는 비활성화에 대해 알아보세요."](#)

NFS 케르베로스

NFS Kerberos를 사용하면 krb5를 사용하여 인증을 암호화하고 krb5i 및 krb5p를 사용하여 데이터 패킷을 추가로 암호화할 수 있습니다. 이는 SVM에서 네트워크 인터페이스별로 활성화되며 자세한 내용은 다음에서 다룹니다.

["NetApp 기술 보고서 4616: ONTAP에서 Microsoft Active Directory와 NFS Kerberos"](#).

pNFS는 SVM의 노드와 네트워크 인터페이스 전반에 걸쳐 데이터 트래픽을 리디렉션할 수 있으므로 SVM의 각 네트워크 인터페이스에서 NFS Kerberos를 활성화하고 작동시켜야 합니다. SVM의 네트워크 인터페이스 중 Kerberos가 활성화되어 있지 않으면 pNFS가 해당 인터페이스의 데이터 볼륨에 액세스하려고 할 때 제대로 작동하지 않습니다.

예를 들어, 두 개의 네트워크 인터페이스(Kerberos에 대해 하나만 활성화됨)가 있는 pNFS 지원 SVM에서 병렬 dd를 사용하여 읽기 테스트를 실행할 때, Kerberos 지원 인터페이스에 있는 파일은 잘 수행되었지만, Kerberos가 활성화되지 않은 인터페이스가 있는 노드의 파일은 읽기를 완료하지 못했습니다. 두 인터페이스 모두에서 Kerberos가 활성화되었을 때 모든 파일이 예상대로 작동했습니다.

SVM의 모든 네트워크 인터페이스에서 NFS Kerberos가 활성화된 경우 pNFS와 함께 NFS Kerberos를 사용할 수 있습니다. NFS Kerberos는 패킷 암호화/복호화로 인해 성능 저하가 발생할 수 있으므로 워크로드에 NFS Kerberos를 적용하여 pNFS를 철저히 테스트하여 성능 저하가 워크로드에 지나치게 큰 영향을 미치지 않는지 확인하는 것이 가장 좋습니다.

아래는 RHEL 9.5 클라이언트에서 pNFS와 함께 krb5(인증) 및 krb5p(종단 간 암호화)를 사용할 때의 병렬 읽기 성능에 대한 예입니다. 이 테스트에서 Krb5p는 70%의 성능 저하를 보였습니다.

케르베로스 맛	MB/초	완료 시간
krb5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43.1 • File3-44 • File4-44.1
krb5p	• File1-72.9 • File2-72.8 • File3-71.4 • File4-71.2	• File1-143.9 • File2-144.1 • File3-146.9 • File4-147.3

"강력한 보안을 위해 NFS를 사용한 Kerberos에 대해 알아보세요"

NFSv4.2

NFSv4.2는 ONTAP 9.8에 추가되었으며 사용 가능한 최신 NFSv4.x 버전입니다(RFC-7862). NFSv4.2에는 이를 활성화/비활성화하는 명시적인 옵션이 없습니다. 대신 NFSv4.1과 함께 활성화/비활성화됩니다. (-4.1 enabled). 클라이언트가 NFSv4.2를 지원하는 경우 별도로 지정하지 않으면 mount 명령 중에 지원되는 가장 높은 NFS 버전을 협상합니다. minorversion=2 마운트 옵션.

ONTAP 의 NFSv4.2는 다음 기능을 지원합니다.

- 보안 라벨(MAC 라벨)
- 확장 속성
- 스파스 파일 작업(FALLOCATE)

pNFS는 NFSv4.1에서 처음 도입되었지만 NFSv4.2에서도 지원되며 관련 기능도 제공됩니다.

"NFSv4.2에 대한 ONTAP 지원에 대해 알아보세요"

pNFS 명령, 통계 및 이벤트 로그

이러한 ONTAP CLI 명령은 특히 pNFS와 관련이 있습니다. 이를 사용하여 구성, 문제 해결 및 통계 수집이 가능합니다.

NFSv4.1을 활성화하십시오

```
nfs modify -vserver SVM -v4.1 enabled
```

pNFS를 활성화합니다

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```


pNFS 장치 표시(고급 권한)

```
pnfs devices show -vserver SVM
```

Vserver Name Generation	Mapping ID	Volume MSID	Mapping Status	
-----	-----	-----	-----	
SVM	17	2157024470	notavailable	2
SVM	18	2157024463	notavailable	2
SVM	19	2157024469	available	3
SVM	20	2157024465	available	4
SVM	21	2157024467	available	3
SVM	22	2157024462	available	1

pNFS 장치 매핑 표시(고급 권한)

```
pnfs devices mappings show -vserver SVM
```

Vserver Name	Mapping ID	Dsid	LIF IP
-----	-----	-----	-----
SVM	19	2449	10.x.x.x
SVM	20	2512	10.x.x.y
SVM	21	2447	10.x.x.x
SVM	22	2442	10.x.x.y

pNFS 특정 성능 카운터 캡처(고급 권한)

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

pNFS 특정 성능 카운터 보기(고급 권한)

```
statistics show -object nfsv4_1 -vserver SVM
```

pNFS 특정 카운터 목록 보기(고급 권한)

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

Object: nfsv4_1

Counter	Description
-----	-----
getdeviceinfo_avg_latency	Average latency of NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_error	The number of failed NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_percent	Percentage of NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_success	The number of successful NFSv4.1 GETDEVICEINFO operations.
getdeviceinfo_total	Total number of NFSv4.1 GETDEVICEINFO operations.
getdevicelist_avg_latency	Average latency of NFSv4.1 GETDEVICELIST operations.
getdevicelist_error	The number of failed NFSv4.1 GETDEVICELIST operations.
getdevicelist_percent	Percentage of NFSv4.1 GETDEVICELIST operations.
getdevicelist_success	The number of successful NFSv4.1 GETDEVICELIST operations.
getdevicelist_total	Total number of NFSv4.1 GETDEVICELIST operations.
layoutcommit_avg_latency	Average latency of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_error	The number of failed NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_percent	Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success	The number of successful NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_total	Total number of NFSv4.1 LAYOUTCOMMIT operations.
layoutget_avg_latency	Average latency of NFSv4.1 LAYOUTGET operations.
layoutget_error	The number of failed NFSv4.1 LAYOUTGET operations.
layoutget_percent	Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success	The number of successful NFSv4.1 LAYOUTGET operations.
layoutget_total	Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency	Average latency of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_error	The number of failed NFSv4.1 LAYOUTRETURN operations.
layoutreturn_percent	Percentage of NFSv4.1 LAYOUTRETURN operations.

layoutreturn_success	The number of successful NFSv4.1 LAYOUTRETURN operations.
layoutreturn_total	Total number of NFSv4.1 LAYOUTRETURN operations.

NFS에 대한 활성 네트워크 연결 보기

SVM에 여러 TCP 연결이 이루어지고 있는지 확인하려면 다음을 수행하십시오. `network connections active show` 명령.

예를 들어, NFS 세션 트렁크를 보고 싶다면 노드당 서로 다른 인터페이스에서 동일한 클라이언트의 연결을 찾으세요.

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
```

	Vserver	Interface	Remote	
CID Ctx Name	Name:Local	Port	Host:Port	
Protocol/Service				

Node: node-01				
2304333128 14 PNFS	data1:2049		ubuntu22-224:740	TCP/nfs
2304333144 10 PNFS	data3:2049		ubuntu22-224:864	TCP/nfs
2304333151 5 PNFS	data1:2049		ubuntu22-226:848	TCP/nfs
2304333167 15 PNFS	data3:2049		ubuntu22-226:684	TCP/nfs
Node: node-02				
2497668321 12 PNFS	data2:2049		ubuntu22-224:963	TCP/nfs
2497668337 18 PNFS	data4:2049		ubuntu22-224:859	TCP/nfs
2497668344 14 PNFS	data2:2049		ubuntu22-226:675	TCP/nfs
2497668360 7 PNFS	data4:2049		ubuntu22-226:903	TCP/nfs

연결된 클라이언트의 NFS 버전 정보 보기

NFS 연결도 볼 수 있습니다. `nfs connected-clients show` 명령. 표시된 클라이언트 목록은 지난 48시간 동안 활성 NFS 트래픽이 있었던 클라이언트라는 점을 명심하세요. 유효 NFS 클라이언트(아직 마운트되어 있더라도)는 마운트에 액세스할 때까지 표시되지 않을 수 있습니다. 최근에 액세스한 클라이언트만 표시하도록 필터링하려면 다음을 지정하세요. `-idle-time` 특징.

예를 들어, pNFS SVM에서 지난 10분 동안 활동이 있었던 클라이언트를 보려면 다음을 수행합니다.

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

Node: node-01

Vserver: PNFS Data-IP: 10.x.x.x Local Remote Client-IP Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

관련 정보

- ["ONTAP의 병렬 NFS\(pNFS\)에 대해 알아보세요"](#)

NFS 및 SMB 파일 및 디렉토리 명명 종속성

ONTAP NFS 및 **SMB** 파일 및 디렉토리 명명 종속성에 대해 알아보세요.

파일 및 디렉토리 명명 규칙은 ONTAP 클러스터 및 클라이언트의 언어 설정과 함께 네트워크 클라이언트의 운영 체제 및 파일 공유 프로토콜에 따라 다릅니다.

운영 체제 및 파일 공유 프로토콜에는 다음이 결정됩니다.

- 문자 파일 이름에 사용할 수 있습니다
- 파일 이름의 대/소문자 구분

ONTAP는 ONTAP 릴리즈별 파일, 디렉토리 및 qtree 이름에서 멀티바이트 문자를 지원합니다.

ONTAP NFS SVM에 대한 다양한 운영 체제의 유효한 문자에 대해 알아보세요.

다른 운영 체제를 사용하는 클라이언트에서 파일 또는 디렉토리에 액세스하는 경우 두 운영 체제 모두에서 유효한 문자를 사용해야 합니다.

예를 들어 UNIX를 사용하여 파일 또는 디렉토리를 생성하는 경우 MS-DOS 파일 또는 디렉토리 이름에 콜론이 허용되지 않으므로 이름에 콜론(:)을 사용하지 마십시오. 유효한 문자의 제한 사항은 운영 체제마다 다르므로 금지된 문자에 대한 자세한 내용은 클라이언트 운영 체제 설명서를 참조하십시오.

ONTAP NFS 다중 프로토콜 환경에서 파일 및 디렉토리 이름의 대소문자 구분에 대해 알아보세요.

파일 및 디렉토리 이름은 NFS 클라이언트의 경우 대/소문자를 구분하며, SMB 클라이언트의 경우 대/소문자를 구분하지 않지만 대/소문자를 구분합니다. SMB 공유를 생성하는 동안 그리고 공유 내의 데이터에 액세스할 때 경로를 지정할 때 취해야 할 조치와 멀티 프로토콜 환경에 미치는 영향을 이해해야 합니다.

SMB 클라이언트가 testdir라는 디렉토리를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 testdir로 표시합니다. 그러나 SMB 사용자가 나중에 디렉터리 이름 testdir을 만들려고 하면 해당 이름이 SMB 클라이언트에 현재

있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 "testdir"이라는 디렉토리를 생성할 경우 NFS 및 SMB 클라이언트는 다음과 같이 디렉토리 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 디렉토리 이름이 대/소문자를 구분하기 때문에 디렉토리 이름이 생성될 때 testdir와 testDIR 같은 두 디렉토리 이름을 모두 볼 수 있습니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 디렉토리를 구분합니다. 한 디렉토리에 기본 파일 이름이 있습니다. 추가 디렉토리에는 8.3 파일 이름이 할당됩니다.
 - SMB 클라이언트에서는 testdir과 testDIR~1이 표시됩니다.
 - ONTAP는 두 디렉토리를 구분하기 위해 'TESTDIR~1' 디렉토리 이름을 생성한다.

이 경우 SVM(스토리지 가상 머신)에서 공유를 생성하거나 수정하는 동안 공유 경로를 지정할 때 8.3 이름을 사용해야 합니다.

마찬가지로 SMB 클라이언트가 test.txt를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 test.txt로 표시합니다. 그러나 SMB 사용자가 나중에 Test.txt를 생성하려고 하면 SMB 클라이언트에 해당 이름이 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 Test.txt라는 파일을 만들면 NFS 및 SMB 클라이언트는 다음과 같이 파일 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 파일 이름이 대/소문자를 구분하기 때문에 이름이 test.txt와 Test.txt로 만들어지면 두 파일 이름이 모두 표시됩니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 파일을 구분합니다. 한 파일에 기본 파일 이름이 있습니다. 8.3 파일 이름이 추가로 할당됩니다.
 - SMB 클라이언트의 경우 test.txt와 test~1.TXT가 표시됩니다.
 - ONTAP는 두 파일을 구별하기 위해 'test~1.TXT' 파일 이름을 만듭니다.



Vserver CIFS 문자 매핑 명령을 사용하여 문자 매핑을 생성한 경우 일반적으로 대/소문자를 구분하지 않는 Windows 조치가 발생할 수 있습니다. 즉, 파일 이름 조치는 문자 매핑이 작성되었고 파일 이름이 해당 문자 매핑을 사용하는 경우에만 대/소문자를 구분합니다.

ONTAP NFS 파일 및 디렉토리 이름 생성에 대해 알아보세요

ONTAP는 SMB 클라이언트에서 액세스할 수 있는 디렉토리인 원래 긴 이름과 8.3 형식의 이름을 사용하여 파일 또는 디렉토리의 이름을 두 개 생성하고 유지합니다.

파일 또는 디렉토리 이름이 8자 이름 또는 3자 확장자 제한(파일의 경우)을 초과하는 경우, ONTAP는 다음과 같이 8.3 형식 이름을 생성합니다.

- 이름이 6자를 초과하면 원본 파일 또는 디렉터리 이름이 6자로 잘립니다.
- 잘려서 더 이상 고유하지 않은 파일 또는 디렉토리 이름에 물결표(~)와 숫자(1 - 5)를 추가합니다.

비슷한 이름이 5개 이상 있어 숫자가 부족하면 원래 이름과 아무런 관계가 없는 고유한 이름이 만들어집니다.

- 파일의 경우 파일 확장명이 3자로 잘립니다.

예를 들어, NFS 클라이언트가 'specifications.html'이라는 파일을 생성할 경우 ONTAP에서 생성한 8.3 형식 파일 이름은 'specif~1.htm'입니다. 이 이름이 이미 있는 경우 ONTAP에서는 파일 이름 끝에 다른 번호를 사용합니다. 예를 들어, NFS 클라이언트가 'specifications_new.html'이라는 다른 파일을 만들 경우 'specifications_new.html'의 8.3 형식은 'specif~2.htm'입니다.

다중 바이트 파일, 디렉토리 및 **qtree** 이름에 대한 **ONTAP NFS** 처리에 대해 알아보세요.

ONTAP 9.5부터 4바이트 UTF-8 인코딩 이름을 지원하므로 BMP(기본 다국어 플레인) 외부의 유니코드 보조 문자를 포함하는 파일, 디렉터리 및 트리 이름을 만들고 표시할 수 있습니다. 이전 릴리스에서는 이러한 보조 문자가 멀티 프로토콜 환경에서 올바르게 표시되지 않았습니다.

4바이트 UTF-8 인코딩된 이름을 지원하기 위해 새 `_utf8mb4_language` 코드를 "vserver" 및 "volume" 명령 제품군에 사용할 수 있습니다.

- 다음 방법 중 하나로 새 볼륨을 만들어야 합니다.
- 볼륨 '-language' 옵션을 명시적으로 설정하기:

'볼륨 생성 - 언어 utf8mb4{...}'

- 옵션으로 생성되거나 수정된 SVM에서 볼륨 '-language' 옵션 상속:

```vserver[create|modify] -language utf8mb4{...}"volume create{...}'`

- ONTAP 9.6 이하 버전을 사용하는 경우 utf8mb4 지원을 위해 기존 볼륨을 수정할 수 없으며 새로운 utf8mb4 지원 볼륨을 생성한 다음 클라이언트 기반 복사 툴을 사용하여 데이터를 마이그레이션해야 합니다.

ONTAP 9.7P1 이상을 사용 중인 경우 지원 요청을 통해 utf8mb4에 대한 기존 볼륨을 수정할 수 있습니다. 자세한 내용은 [참조하십시오 "ONTAP에서 생성한 후 볼륨 언어를 변경할 수 있습니까?"](#).

를 누릅니다

utf8mb4 지원을 위해 SVM을 업데이트할 수 있지만 기존 볼륨에 원래 언어 코드가 유지됩니다.

를 누릅니다



4바이트 UTF-8 문자를 사용하는 LUN 이름은 현재 지원되지 않습니다.

- 유니코드 문자 데이터는 일반적으로 16비트 UTF-16(Unicode Transformation Format)을 사용하는 Windows 파일 시스템 응용 프로그램과 8비트 UTF-8(Unicode Transformation Format)을 사용하는 NFS 파일 시스템에 표시됩니다.

ONTAP 9.5 이전 버전에서는 Windows 클라이언트에서 생성한 UTF-16 보조 문자를 포함한 이름이 다른 Windows 클라이언트에 올바르게 표시되었지만 NFS 클라이언트용 UTF-8로 올바르게 변환되지 않았습니다. 마찬가지로, 생성된 NFS 클라이언트에서 UTF-8 보완 문자를 사용하는 이름은 Windows 클라이언트의 UTF-16으로 올바르게 변환되지 않았습니다.

- ONTAP 9.4 이하를 실행하는 시스템에서 유효하거나 잘못된 보조 문자가 포함된 파일 이름을 만들면 ONTAP가 파일 이름을 거부하고 잘못된 파일 이름 오류를 반환합니다.

이 문제를 방지하려면 파일 이름에 BMP 문자만 사용하고 보조 문자는 사용하지 마십시오. 또는 ONTAP 9.5 이상으로 업그레이드하십시오.

유니코드 문자는 qtree 이름에 사용할 수 있습니다.

- 'volume qtree' 명령군 또는 System Manager를 사용하여 qtree 이름을 설정하거나 수정할 수 있습니다.
- Qtree 이름에는 일본어 및 중국어 문자와 같은 유니코드 형식의 멀티바이트 문자가 포함될 수 있습니다.

- ONTAP 9.5 이전 버전에서는 BMP 문자(즉, 3바이트로 표현될 수 있는 문자)만 지원되었습니다.



ONTAP 9.5 이전의 릴리즈에서는 qtree 상위 볼륨의 연결 경로에 유니코드 문자가 있는 qtree 및 디렉토리 이름이 포함될 수 있습니다. 볼륨 표시 명령은 상위 볼륨에 UTF-8 언어 설정이 있는 경우 이러한 이름을 올바르게 표시합니다. 그러나 상위 볼륨 언어가 UTF-8 언어 설정 중 하나가 아닌 경우 junction-path의 일부 부분은 숫자 NFS 대체 이름을 사용하여 표시됩니다.

- 9.5 이상 릴리즈에서는 qtree 이름이 qtree 이름으로 지원되지만 qtree가 utf8mb4에 대해 활성화된 볼륨에 있습니다.

## ONTAP NFS 볼륨에서 SMB 파일 이름 변환을 위한 문자 매핑 구성

NFS 클라이언트는 SMB 클라이언트 및 특정 Windows 애플리케이션에 유효하지 않은 문자를 포함하는 파일 이름을 생성할 수 있습니다. SMB 클라이언트가 유효하지 않은 NFS 이름의 파일에 액세스할 수 있도록 볼륨의 파일 이름 변환에 대한 문자 매핑을 구성할 수 있습니다.

이 작업에 대해

NFS 클라이언트가 생성한 파일을 SMB 클라이언트가 액세스할 때 ONTAP는 파일 이름을 찾습니다. 이름이 유효한 SMB 파일 이름이 아닌 경우(예: 포함된 콜론 ":" 문자가 있는 경우) ONTAP는 각 파일에 대해 유지되는 8.3 파일 이름을 반환합니다. 그러나 이로 인해 중요한 정보를 긴 파일 이름으로 인코딩하는 응용 프로그램에 문제가 발생합니다.

따라서 다른 운영 체제의 클라이언트 간에 파일을 공유하는 경우 두 운영 체제 모두에서 유효한 파일 이름에 문자를 사용해야 합니다.

그러나 SMB 클라이언트에 대해 유효한 파일 이름이 아닌 문자를 포함하는 파일 이름을 생성하는 NFS 클라이언트가 있는 경우, 잘못된 NFS 문자를 SMB 및 특정 Windows 애플리케이션이 허용하는 유니코드 문자로 변환하는 맵을 정의할 수 있습니다. 예를 들어, 이 기능은 CATIA MCAD 및 Mathematica 응용 프로그램과 이 요구 사항이 있는 다른 응용 프로그램을 지원합니다.

볼륨별로 문자 매핑을 구성할 수 있습니다.

볼륨에 문자 매핑을 구성할 때 다음 사항을 염두에 두어야 합니다.

- 문자 매핑이 교차점에 적용되지 않습니다.

각 접합 볼륨에 대해 문자 매핑을 명시적으로 구성해야 합니다.

- 올바르게 않거나 잘못된 문자를 나타내는 데 사용되는 유니코드 문자가 파일 이름에 일반적으로 나타나지 않는 문자인지 확인해야 합니다. 그렇지 않으면 원치 않는 매핑이 발생합니다.

예를 들어 콜론(:)을 하이픈(-)에 매핑하려고 하지만 파일 이름에 하이픈(-)이 올바르게 사용된 경우 "'a-b'"라는 파일에 액세스하려는 Windows 클라이언트의 요청이 "'a:b'"(원하는 결과가 아님)의 NFS 이름에 매핑됩니다.

- 문자 매핑을 적용한 후에도 매핑에 여전히 잘못된 Windows 문자가 포함되어 있으면 ONTAP는 Windows 8.3 파일 이름으로 다시 돌아갑니다.
- FPolicy 알림, NAS 감사 로그, 보안 추적 메시지에 매핑된 파일 이름이 표시됩니다.
- DP 유형의 SnapMirror 관계가 생성될 때 소스 볼륨의 문자 매핑이 대상 DP 볼륨에 복제되지 않습니다.
- 대소문자 구분: 매핑된 Windows 이름이 NFS 이름으로 전환되기 때문에 이름 조회는 NFS 의미를 따릅니다. 여기에는 NFS 조회가 대/소문자를 구분한다는 사실도 포함됩니다. 즉, 매핑된 공유에 액세스하는 응용 프로그램이 대/소문자를 구분하지 않는 Windows 동작에 의존해서는 안 됩니다. 그러나 8.3 이름은 사용할 수 있으며 대

/소문자를 구분하지 않습니다.

- 부분 매핑 또는 잘못된 매핑: 이름을 매핑하여 디렉터리 열거("dir")를 수행하는 클라이언트로 반환하면 결과 유니코드 이름이 Windows 유효성을 검사합니다. 이름에 여전히 잘못된 문자가 있거나 Windows에 유효하지 않은 경우(예: "." 또는 공백으로 끝나는 경우) 잘못된 이름 대신 8.3 이름이 반환됩니다.

## 단계

### 1. 문자 매핑 구성:

```
'vserver cifs character-mapping create-vserver vservice_name-volume volume_name-mapping mapping_text,...'
```

매핑은 ""로 구분된 소스-타겟 문자 쌍 목록으로 구성됩니다. 문자는 16진수를 사용하여 입력한 유니코드 문자입니다. 예: 3C:E03C.

콜론으로 구분된 각 mapping\_text 쌍의 첫 번째 값은 번역할 NFS 문자의 16진수 값이고 두 번째 값은 SMB가 사용하는 유니코드 값입니다. 매핑 쌍은 고유해야 합니다(일대일 매핑이 있어야 함).

#### ◦ 소스 매핑

다음 표에서는 소스 매핑에 사용할 수 있는 유니코드 문자 집합을 보여 줍니다.

| 유니코드 문자입니다 | 인쇄된 문자 | 설명                |
|------------|--------|-------------------|
| 0x01-0x19  | 해당 없음  | 인쇄할 수 없는 제어 문자입니다 |
| 0x5C       | \      | 백슬래시              |
| 0x3A       | :      | 결장                |
| 0x2A       | *      | 별표                |
| 0x3F       | ?      | 물음표               |
| 0x22       | "      | 인용 부호가 있습니다       |
| 0x3C       | 를 누릅니다 | 보다 작음             |
| 0x3E       | 를 누릅니다 | 보다 큼              |
| 0x7C       |        |                   |
| 세로선        | 0xB1   | ±                 |

#### ◦ 타겟 매핑

U+E0000...U+F8FF 범위의 유니코드 "전용 용도 영역"에서 대상 문자를 지정할 수 있습니다.



예

다음 명령을 실행하면 SVM(스토리지 가상 시스템) VS1 에서 "data"라는 이름의 볼륨에 대한 문자 매핑이 생성됩니다.

```
cluster1::> vservers cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vservers cifs character-mapping show
```

| Vserver | Volume Name | Character Mapping         |
|---------|-------------|---------------------------|
| vs1     | data        | 3c:e17c, 3e:f17d, 2a:f745 |

**SMB** 파일 이름 변환을 위한 문자 매핑을 관리하기 위한 **ONTAP NFS** 명령

FlexVol 볼륨에서 SMB 파일 이름 변환에 사용되는 파일 문자 매핑을 생성, 수정, 정보 표시 또는 삭제하여 문자 매핑을 관리할 수 있습니다.

| 원하는 작업                 | 이 명령 사용...                                       |
|------------------------|--------------------------------------------------|
| 새 파일 문자 매핑을 만듭니다       | 'vservers cifs character-mapping create'         |
| 파일 문자 매핑에 대한 정보를 표시합니다 | 'vservers cifs character-mapping show'           |
| 기존 파일 문자 매핑을 수정합니다     | 'vservers cifs character-mapping modify'를 참조하십시오 |
| 파일 문자 매핑을 삭제합니다        | 'vservers cifs character-mapping delete'         |

에 대한 자세한 내용은 vservers cifs character-mapping ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

## NFS 트렁킹을 관리합니다

### ONTAP NFS 트렁킹에 대해 알아보십시오

ONTAP 9.14.1부터 NFSv4.1 클라이언트는 세션 트렁킹을 활용하여 NFS 서버의 서로 다른 LIF에 대한 여러 연결을 열 수 있으므로 데이터 전송 속도가 향상되고 다중 경로를 통한 복원력을 제공할 수 있습니다.

트렁킹은 FlexVol 볼륨을 트렁킹 가능 클라이언트, 특히 VMware 및 Linux 클라이언트 또는 RDMA, TCP 또는 pNFS를 통한 NFS에 내보내는 데 유리합니다.

ONTAP 9.14.1에서는 트렁킹이 단일 노드의 LIF로 제한되며, 트렁킹이 여러 노드에 대한 LIF를 확장할 수 없습니다.

FlexGroup 볼륨은 트렁킹이 지원됩니다. 이는 성능 향상을 제공할 수 있지만, FlexGroup 볼륨에 대한 다중 경로 액세스는 단일 노드에서만 구성할 수 있습니다.

이 릴리즈에서는 세션 트렁킹만 경로 다중화에 지원됩니다.

## 트렁킹 사용 방법

트렁킹이 제공하는 다중 경로 이점을 활용하려면 트렁킹 사용 NFS 서버가 포함된 SVM에 연결된 LIF 세트(\_트렁킹 그룹 \_이라고도 함)가 필요합니다. 트렁킹 그룹의 LIF는 클러스터의 동일한 노드에 홈 포트가 있어야 하고 이러한 홈 포트에 상주해야 합니다. 트렁킹 그룹의 모든 LIF가 동일한 페일오버 그룹의 구성원이라는 것이 모범 사례입니다.

ONTAP은 지정된 클라이언트에서 노드당 최대 16개의 트렁킹 연결을 지원합니다.

클라이언트가 트렁킹 사용 서버에서 내보내기를 마운트할 때 트렁킹 그룹의 LIF에 대한 IP 주소 수를 지정합니다. 클라이언트가 첫 번째 LIF에 연결되면 추가 LIF가 NFSv4.1 세션에만 추가되고 트렁킹 그룹 요구사항을 준수하는 경우 트렁킹에 사용됩니다. 그런 다음 클라이언트는 자체 알고리즘(예: 라운드 로빈)에 따라 여러 연결을 통해 NFS 작업을 분산합니다.

최상의 성능을 얻으려면 단일 경로 내보내기가 아닌 다중 경로 내보내기 전용 SVM에 트렁킹을 구성해야 합니다. 즉, 트렁킹이 활성화된 클라이언트에만 내보내기가 제공되는 SVM에서 NFS 서버에서만 트렁킹을 활성화해야 합니다.

## 지원되는 클라이언트

ONTAP NFSv4.1 서버는 NFSv4.1 세션 트렁킹을 지원하는 모든 클라이언트의 트렁킹을 지원합니다.

다음 클라이언트는 ONTAP 9.14.1에서 테스트되었습니다.

- VMware - ESXi 7.0U3F 이상
- Linux - RHEL(Red Hat Enterprise Linux) 8.8 및 9.3



컨트롤러 장애 조치(failover)에서 트렁킹된 LIF가 다른 노드로 마이그레이션되는 경우 RHEL NFS 클라이언트는 트렁킹을 다시 설정하지 않습니다. LIF가 다른 노드로 마이그레이션되면 트렁킹 그룹에서 제거됩니다. 트렁킹 그룹의 모든 LIF가 마이그레이션되면 NFS 클라이언트는 첫 번째 LIF만 사용하여 I/O를 계속합니다.



NFS 서버에서 트렁킹이 설정된 경우 트렁킹을 지원하지 않는 NFS 클라이언트에서 내보낸 공유에 액세스하는 사용자가 성능 저하를 겪을 수 있습니다. SVM 데이터 LIF에 대한 여러 마운트에 단일 TCP 연결만 사용되기 때문입니다.

## NFS 트렁킹과 nconnect 간의 차이

ONTAP 9.8부터는 NFSv4.1이 활성화된 경우 기본적으로 nconnect 기능을 사용할 수 있습니다. nconnect 지원 클라이언트에서는 단일 NFS 마운트로 단일 LIF를 통해 여러 TCP 연결(최대 16개)을 가질 수 있습니다.

반면, 트렁킹은 여러 LIF에 여러 개의 TCP 연결을 제공하는 \_multipathing\_functionality입니다. 사용자 환경에 추가 NIC를 사용할 수 있는 경우 트렁킹은 nconnect의 기능을 뛰어넘는 병렬 처리 및 성능을 제공합니다.

에 대해 자세히 "[nConnect\(연결\)](#)"알아보십시오.

## 트렁킹을 위해 새 NFS 서버 및 내보내기를 구성합니다

ONTAP SVM에 트렁킹 지원 NFS 서버를 생성합니다

ONTAP 9.14.1부터 NFS 서버에서 트렁킹을 활성화할 수 있습니다. NFSv4.1은 NFS 서버가 생성될 때 기본적으로 사용하도록 설정됩니다.

시작하기 전에

트렁킹 지원 NFS 서버를 생성하려면 SVM이 필요합니다. SVM은 다음과 같아야 합니다.

- 클라이언트 데이터 요구 사항을 충족할 수 있는 충분한 저장소 지원.
- NFS에 대해 설정되었습니다.

기존 SVM을 사용할 수 있지만 트렁킹을 활성화하려면 모든 NFSv4.x 클라이언트를 다시 마운트해야 하므로 시스템이 중단될 수 있습니다. 다시 마운트할 수 없는 경우, NFS 서버에 대한 새 SVM을 생성하십시오.

단계

1. 적합한 SVM이 없는 경우 다음을 생성합니다.

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8
```

2. 새로 생성한 SVM의 구성 및 상태 확인:

```
'vserver show -vserver_svm_name_'
```

에 대해 자세히 알아보십시오 ["SVM 생성"](#).

3. NFS 서버 생성:

```
vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
-v4.1-trunking enabled -v4-id-domain my_domain.com
```

4. NFS가 실행 중인지 확인합니다.

```
vserver nfs status -vserver svm_name
```

5. NFS가 원하는 대로 구성되었는지 확인합니다.

```
vserver nfs show -vserver svm_name
```

에 대해 자세히 알아보십시오 ["NFS 서버 구성"](#)

작업을 마친 후

필요에 따라 다음 서비스를 구성합니다.

- ["DNS"](#)
- ["LDAP를 지원합니다"](#)
- ["Kerberos"](#)

**ONTAP NFS** 트렁킹을 위한 네트워크를 준비합니다

NFSv4.1 트렁킹을 활용하려면 트렁킹 그룹의 LIF가 동일한 노드에 있어야 하고 동일한 노드에 홈 포트가 있어야 합니다. LIF는 같은 노드의 페일오버 그룹에서 구성되어야 합니다.

이 작업에 대해

LIF 및 NIC의 일대일 매핑은 최고의 성능 향상을 생성하지만 트렁킹은 활성화하지 않아도 됩니다. NIC가 2개 이상 설치되어 있으면 성능상의 이점을 얻을 수 있지만 반드시 필요한 것은 아닙니다.

트렁킹 그룹의 모든 LIF는 동일한 페일오버 그룹에 속해야 합니다. LIF가 같은 노드의 페일오버 그룹에 구성되어 있으면 해당 노드의 컨트롤러 페일오버로 인해 LIF가 오프라인 상태가 될 수 있습니다. 같은 노드의 페일오버 그룹에 LIF가 구성되어 있지 않고 다른 노드로 페일오버하면 트렁킹이 더 이상 작동하지 않습니다.

페일오버 그룹에서 접속(및 기본 NIC)을 추가하거나 제거할 때마다 트렁킹 페일오버 그룹을 조정해야 합니다.

시작하기 전에

- 페일오버 그룹을 생성하려면 NIC와 연결된 포트 이름을 알아야 합니다.
- 포트는 모두 같은 노드에 있어야 합니다.

단계

1. 사용할 네트워크 포트의 이름 및 상태를 확인합니다.

```
network port show
```

2. 페일오버 그룹을 생성합니다.

```
network interface failover-groups create -vserver <svm_name> -failover-group <failover_group_name> -targets <ports_list>
```



페일오버 그룹이 반드시 있어야 하는 것은 아니지만 이 그룹이 반드시 권장됩니다.

- <svm\_name> 은 NFS 서버가 포함된 SVM의 이름입니다.
- <ports\_list> 은 페일오버 그룹에 추가될 포트의 목록입니다.

포트는 다음과 같이 node1:e0c 형식으로 추가됩니다 <node\_name>:<port\_number>.

다음 명령을 실행하면 SVM VS1에 대한 페일오버 그룹 fg3이 생성되고 포트 3개가 추가됩니다.

```
network interface failover-groups create -vserver vs1 -failover-group fg3 -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

에 대해 자세히 알아보십시오 ["페일오버 그룹:"](#)

에 대한 자세한 내용은 `network interface failover-groups create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. 필요한 경우 트렁킹 그룹 구성원에 대한 LIF를 생성합니다.

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address> [-service-policy <policy>] [-auto-revert <true|false>]
```

- -home-node - LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 노드입니다.

또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트에 자동으로 되돌아가는지 여부를 지정할 수도

있습니다.

- -home-port LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 물리적 포트 또는 논리 포트입니다.
- 를 사용하여 IP 주소를 지정할 수 있습니다 -address 및 -netmask 옵션이 아닌 옵션 -subnet 옵션을 선택합니다.
- IP 주소를 할당할 때 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 경로를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 network route create 내용은 을 ["ONTAP 명령 참조입니다"](#)참조하십시오.
- -service-policy - LIF에 대한 서비스 정책. 정책을 지정하지 않으면 기본 정책이 자동으로 할당됩니다. 를 사용합니다 network interface service-policy show 명령을 사용하여 사용 가능한 서비스 정책을 검토합니다.
- -auto-revert - 시작, 관리 데이터베이스 상태 변경 또는 네트워크 연결이 이루어질 때 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정합니다. 기본 설정은 false 이지만 환경의 네트워크 관리 정책에 따라 true로 설정할 수 있습니다.

트렁킹 그룹의 모든 LIF에 대해 이 단계를 반복합니다.

다음 명령을 실행하면 이 생성됩니다 lif-A SVM을 위해 vs1, 포트에 있습니다 e0c 노드 cluster1\_01:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

에 대해 자세히 알아보십시오 ["LIF 생성:"](#)

#### 4. LIF가 생성되었는지 확인:

```
network interface show
```

#### 5. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

| 다음을 확인하려면... | 사용...   |
|--------------|---------|
| IPv4 주소입니다   | 네트워크 핑  |
| IPv6 주소입니다   | 네트워크 핑6 |

#### 관련 정보

- ["네트워크 Ping"](#)
- ["네트워크 인터페이스"](#)
- ["네트워크 포트가 표시됩니다"](#)

#### ONTAP 볼륨 익스포트 정책을 생성합니다

데이터 공유에 대한 클라이언트 액세스를 제공하려면 하나 이상의 볼륨을 생성해야 하며 볼륨에 하나 이상의 규칙이 포함된 익스포트 정책이 있어야 합니다.

클라이언트 내보내기 요구 사항:

- Linux 클라이언트는 트렁킹 연결(즉, 각 LIF)에 대해 별도의 마운트 및 마운트 지점을 가져야 합니다.
- VMware 클라이언트에는 여러 LIF가 지정된, 내보낸 볼륨에 대해 단일 마운트 지점만 필요합니다.

VMware 클라이언트는 익스포트 정책에서 루트 액세스 권한이 필요합니다.

단계

1. 익스포트 정책 생성:

```
vserver export-policy create -vserver svm_name -policyname policy_name
```

정책 이름은 최대 256자까지 지정할 수 있습니다.

2. 익스포트 정책이 생성되었는지 확인:

```
'vserver export-policy show-policyname_policy_name_'
```

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 exp1 이라는 익스포트 정책이 생성되는지 검증 및 됩니다.

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. 익스포트 규칙을 생성하여 기존 익스포트 정책에 추가:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

를 클릭합니다 -clientmatch 매개 변수는 내보내기를 마운트할 트렁킹 가능 Linux 또는 VMware 클라이언트를 식별해야 합니다.

에 대해 자세히 알아보십시오 ["내보내기 규칙을 만드는 중입니다."](#)

4. 교차점으로 볼륨을 생성합니다.

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

에 대해 자세히 알아보십시오 ["볼륨 생성"](#)

5. 볼륨이 원하는 집합 지점으로 생성되었는지 확인합니다.

```
volume show -vserver svm_name -volume volume_name -junction-path
```

**ONTAP** 볼륨 또는 **NFS** 트렁킹용 데이터 공유를 마운트합니다

트렁킹을 지원하는 Linux 및 VMware 클라이언트는 트렁킹이 활성화된 ONTAP NFSv4.1 서버에서 볼륨 또는 데이터 공유를 마운트할 수 있습니다.

에 대해 자세히 알아보십시오 ["지원되는 클라이언트"](#).

#### Linux 클라이언트 요구 사항

ONTAP 9.16.1 이상 및 Red Hat Enterprise Linux 버전 8.7 이상(RHEL 8의 경우) 또는 9.2 이상(RHEL 9의 경우)을 Linux 클라이언트로 사용하는 경우 트렁킹 그룹에 하나의 마운트 지점만 필요합니다. 다음 옵션을 사용하여 내보낸 볼륨을 이 명령으로 마운트합니다. `trunkdiscovery`

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

그렇지 않으면 트렁킹 그룹의 각 연결에 대해 별도의 마운트 지점이 필요합니다. 옵션을 사용하여 다음과 유사한 명령을 사용하여 내보낸 볼륨을 마운트합니다 `max_connect`.

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

버전 (`vers`) 값은 이어야 합니다 4.1 이상.

를 클릭합니다 `max_connect` 값은 트렁킹 그룹의 연결 수에 해당합니다.

#### VMware 클라이언트 요구 사항

트렁킹 그룹의 각 연결에 대한 IP 주소를 포함하는 마운트 문이 필요합니다.

다음과 유사한 명령을 사용하여 내보낸 데이터 저장소를 마운트합니다.

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

를 클릭합니다 `-H` 값은 트렁킹 그룹의 연결에 해당합니다.

## 트렁킹을 위해 기존 **NFS** 내보내기 조정

### ONTAP NFS 트렁킹을 위한 단일 경로 내보내기 조정

트렁킹을 사용하도록 기존 단일 경로(비트렁킹) NFSv4.1 내보내기를 조정할 수 있습니다. 서버 및 클라이언트 사전 요구 사항이 충족되면 트렁킹을 사용할 수 있는 클라이언트는 서버에서 트렁킹이 활성화되는 즉시 향상된 성능을 활용할 수 있습니다.

트렁킹을 위해 단일 경로 내보내기를 조정함으로써 기존 볼륨 및 SVM에서 내보낸 데이터 세트를 유지할 수 있습니다.

이렇게 하려면 NFS 서버에서 트렁킹을 활성화하고, 네트워킹 및 내보내기 구성을 업데이트하고, 내보낸 공유를 클라이언트에 다시 마운트해야 합니다.

트렁킹을 활성화하면 서버를 다시 시작할 수 있습니다. 그런 다음 VMware 클라이언트는 내보낸 데이터 저장소를 다시 마운트해야 합니다. Linux 클라이언트는 `mount` 를 사용하여 내보낸 볼륨을 다시 마운트해야 합니다 `max_connect` 옵션을 선택합니다.

**ONTAP NFS** 서버에서 트렁킹을 활성화합니다

NFS 서버에서 트렁킹을 명시적으로 설정해야 합니다. NFSv4.1은 NFS 서버가 생성될 때 기본적으로 사용하도록 설정됩니다.

트렁킹을 활성화한 후 다음 서비스가 필요에 따라 구성되었는지 확인합니다.

- ["DNS"](#)
- ["LDAP를 지원합니다"](#)
- ["Kerberos"](#)

단계

1. 트렁킹을 활성화하고 다음과 같이 NFSv4.1이 설정되어 있는지 확인합니다.

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. NFS가 실행 중인지 확인합니다.

```
vserver nfs status -vserver svm_name
```

3. NFS가 원하는 대로 구성되었는지 확인합니다.

```
vserver nfs show -vserver svm_name
```

에 대해 자세히 알아보십시오 ["NFS 서버 구성"](#)

... 이 SVM에서 Windows 클라이언트를 지원하는 경우 공유를 이동한 다음 서버를 삭제합니다.

```
vserver cifs show -vserver svm_name
```

를 누릅니다

```
vserver cifs delete -vserver svm_name
```

**ONTAP NFS** 트렁킹용 네트워크를 업데이트합니다

NFSv4.1 트렁킹을 활용하려면 트렁킹 그룹의 LIF가 동일한 노드에 있어야 하고 동일한 노드에 홈 포트가 있어야 합니다. LIF는 같은 노드의 페일오버 그룹에서 구성되어야 합니다.

이 작업에 대해

LIF 및 NIC의 일대일 매핑은 최고의 성능 향상을 생성하지만 트렁킹은 활성화하지 않아도 됩니다. NIC가 2개 이상 설치되어 있으면 성능상의 이점을 얻을 수 있지만 반드시 필요한 것은 아닙니다.

트렁킹 그룹의 모든 LIF는 동일한 페일오버 그룹에 속해야 합니다. LIF가 같은 노드의 페일오버 그룹에 구성되어 있으면 해당 노드의 컨트롤러 페일오버로 인해 LIF가 오프라인 상태가 될 수 있습니다. 같은 노드의 페일오버 그룹에 LIF가 구성되어 있지 않고 다른 노드로 페일오버하면 트렁킹이 더 이상 작동하지 않습니다.



페일오버 그룹에서 접속(및 기본 NIC)을 추가하거나 제거할 때마다 트렁킹 페일오버 그룹을 조정해야 합니다.

시작하기 전에

- 페일오버 그룹을 생성하려면 NIC와 연결된 포트 이름을 알아야 합니다.
- 포트는 모두 같은 노드에 있어야 합니다.

단계

1. 사용할 네트워크 포트의 이름 및 상태를 확인합니다.

네트워크 포트 쇼

에 대한 자세한 내용은 `network port show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. 트렁킹 페일오버 그룹을 생성하거나 트렁킹을 위해 기존 그룹을 수정합니다.

```
network interface failover-groups create -vserver <svm_name> -failover-group
<failover_group_name> -targets <ports_list>
```

```
network interface failover-groups modify -vserver <svm_name> -failover-group
<failover_group_name> -targets <ports_list>
```



페일오버 그룹이 반드시 있어야 하는 것은 아니지만 이 그룹이 반드시 권장됩니다.

- <svm\_name> 은 NFS 서버가 포함된 SVM의 이름입니다.
- <ports\_list> 은 페일오버 그룹에 추가될 포트의 목록입니다.

예를 들어, node1:e0c 포트는 형식으로 <node\_name>:<port\_number> 추가됩니다.

다음 명령을 실행하면 페일오버 그룹이 생성됩니다 fg3 SVM VS1의 경우 다음 3개의 포트 추가:

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

에 대해 자세히 알아보십시오 "[페일오버 그룹](#):"

3. 필요에 따라 트렁킹 그룹 구성원에 대한 추가 LIF를 생성합니다.

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node
<node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
[-service-policy <policy>] [-auto-revert <true|false>]
```

- -home-node - LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 노드입니다.

LIF가 를 사용하여 홈 노드 및 홈 포트에 자동으로 되돌리는지 여부를 지정할 수 있습니다 -auto-revert 옵션을 선택합니다.

- -home-port LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 물리적 포트 또는 논리 포트입니다.
- 를 사용하여 IP 주소를 지정할 수 있습니다 -address 및 -netmask 옵션.

- 서브넷을 사용하지 않고 IP 주소를 수동으로 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 경로를 구성해야 할 수 있습니다. `network route create`` 명령 페이지에는 SVM 내에서 정적 라우트를 생성하는 방법에 대한 정보가 포함되어 있습니다. 에 대한 자세한 내용은 ``network route create`` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.
- `-service-policy` - LIF에 대한 서비스 정책. 정책을 지정하지 않으면 기본 정책이 자동으로 할당됩니다. 를 사용합니다 `network interface service-policy show`` 명령을 사용하여 사용 가능한 서비스 정책을 검토합니다.

에 대한 자세한 내용은 `network interface service-policy show`` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

- `-auto-revert` - 시작, 관리 데이터베이스 상태 변경 또는 네트워크 연결이 이루어질 때 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정합니다. \*기본 설정은 `false``이지만 사용자 환경의 네트워크 관리 정책에 따라 `true``로 설정할 수 있습니다.

트렁킹 그룹에 필요한 각각의 추가 LIF에 대해 이 단계를 반복합니다.

다음 명령을 실행하면 이 생성됩니다 `lif-A`` SVM을 위해 `vs1``, 포트에 있습니다 `e0c`` 노드 `cluster1_01``:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

에 대해 자세히 알아보십시오 ["LIF 생성:"](#)

#### 4. LIF가 생성되었는지 확인:

```
network interface show
```

#### 5. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

| 다음을 확인하려면... | 사용...   |
|--------------|---------|
| IPv4 주소입니다   | 네트워크 핑  |
| IPv6 주소입니다   | 네트워크 핑6 |

#### 관련 정보

- ["네트워크 Ping"](#)
- ["네트워크 인터페이스"](#)

#### ONTAP 볼륨 익스포트 정책을 수정합니다

클라이언트가 기존 데이터 공유에 대해 트렁킹을 활용할 수 있도록 하려면 익스포트 정책과 규칙 및 규칙이 연결되는 볼륨을 수정해야 할 수 있습니다. Linux 클라이언트 및 VMware 데이터 저장소에는 서로 다른 내보내기 요구 사항이 있습니다.

클라이언트 내보내기 요구 사항:

- Linux 클라이언트는 트렁킹 연결(즉, 각 LIF)에 대해 별도의 마운트 및 마운트 지점을 가져야 합니다.

ONTAP 9.14.1로 업그레이드할 때 이미 볼륨을 내보낸 경우에는 트렁킹 그룹에서 해당 볼륨을 계속 사용할 수 있습니다.

- VMware 클라이언트에는 여러 LIF가 지정된, 내보낸 볼륨에 대해 단일 마운트 지점만 필요합니다.

VMware 클라이언트는 익스포트 정책에서 루트 액세스 권한이 필요합니다.

## 단계

1. 기존 익스포트 정책이 있는지 확인:

`vserver export-policy show`를 참조하십시오

2. 기존 내보내기 정책 규칙이 트렁킹 구성에 적합한지 확인합니다.

'`vserver export-policy rule show-policyname_policy_name_`'

특히 를 확인합니다 `-clientmatch` 매개 변수는 내보내기를 마운트할 트렁킹 가능 Linux 또는 VMware 클라이언트를 올바르게 식별합니다.

조정이 필요한 경우 를 사용하여 규칙을 수정합니다 `vserver export-policy rule modify` 명령을 실행하거나 새 규칙을 만듭니다.

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

에 대해 자세히 알아보십시오 ["내보내기 규칙을 만드는 중입니다."](#)

3. 내보낸 기존의 볼륨이 온라인 상태인지 확인합니다.

`volume show -vserver svm_name`

## ONTAP 볼륨 또는 데이터 공유를 NFS 트렁킹에 다시 마운트합니다

트렁킹되지 않은 클라이언트 연결을 트렁킹 연결로 변환하려면 Linux 및 VMware 클라이언트의 기존 마운트를 분리하고 LIF에 대한 정보를 사용하여 다시 마운트해야 합니다.

에 대해 자세히 알아보십시오 ["지원되는 클라이언트"](#).



VMware 클라이언트의 마운트를 해제하면 데이터 저장소의 모든 VM에 대해 중단이 발생합니다. 또는 트렁킹을 사용할 수 있는 새 데이터 저장소를 생성하고 \* storage vMotion \* 을 사용하여 VM을 이전 데이터 저장소에서 새 데이터 저장소로 이동하는 방법도 있습니다. 자세한 내용은 VMware 설명서를 참조하십시오.

### Linux 클라이언트 요구 사항

ONTAP 9.16.1 이상 및 Red Hat Enterprise Linux 버전 8.7 이상(RHEL 8의 경우) 또는 9.2 이상(RHEL 9의 경우)을 Linux 클라이언트로 사용하는 경우 트렁킹 그룹에 하나의 마운트 지점만 필요합니다. 다음 옵션을 사용하여 내보낸 볼륨을 이 명령으로 마운트합니다. `trunkdiscovery`

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

그렇지 않으면 트렁킹 그룹의 각 연결에 대해 별도의 마운트 지점이 필요합니다. 옵션을 사용하여 다음과 유사한 명령을 사용하여 내보낸 볼륨을 마운트합니다 `max_connect`.

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

버전 (`vers`) 값은 이어야 합니다 4.1 이상.

를 클릭합니다 `max_connect` 값은 트렁킹 그룹의 연결 수에 해당합니다.

### VMware 클라이언트 요구 사항

트렁킹 그룹의 각 연결에 대한 IP 주소를 포함하는 마운트 문이 필요합니다.

다음과 유사한 명령을 사용하여 내보낸 데이터 저장소를 마운트합니다.

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

를 클릭합니다 `-H` 값은 트렁킹 그룹의 연결과 일치해야 합니다.

## RDMA를 통해 NFS를 관리합니다

### ONTAP에서 RDMA를 통한 NFS에 대해 알아보십시오

RDMA 기반 NFS는 RDMA 지원 네트워크 어댑터를 사용하여 스토리지 시스템 메모리와 호스트 시스템 메모리 간에 데이터를 직접 복사할 수 있으므로 CPU 중단과 오버헤드를 피할 수 있습니다.

RDMA 상 NFS 구성은 머신 러닝 및 분석과 같은 지연 시간에 민감하거나 대역폭이 높은 워크로드를 사용하는 고객을 위해 설계되었습니다. RDMA 기반 ONTAP NFS는 모든 NFS 기반 워크로드에 사용할 수 있습니다. 또한 NVIDIA는 GDS(GPU Direct Storage)를 지원하기 위해 RDMA를 통해 NFS를 확장했습니다. GDS는 RDMA를 사용하여 스토리지 시스템과 GPU 메모리 간에 데이터를 직접 전송함으로써 CPU와 메인 메모리를 모두 우회함으로써 GPU 지원 워크로드를 더욱 가속화합니다.

ONTAP 9.10.1부터 NFSv4.0 프로토콜에 대해 NFS over RDMA 구성이 지원됩니다. 이후 ONTAP 릴리스에서는 추가 NFS 버전을 위한 지원이 도입되었습니다.

## 요구 사항

- 사용할 NFS 버전에 대해 올바른 ONTAP 버전을 실행하고 있는지 확인합니다.

| NFS 버전  | ONTAP 지원        |
|---------|-----------------|
| NFSv4.0 | ONTAP 9.10.1 이상 |
| NFSv4.1 | ONTAP 9.14.1 이상 |
| NFSv3   | ONTAP 9.15.1 이상 |

- ONTAP 9.12.1로 시작하는 System Manager를 사용하여 RDMA를 통해 NFS를 구성할 수 있습니다. ONTAP 9.10.1 및 9.11.1에서는 CLI를 사용하여 RDMA를 통해 NFS를 구성해야 합니다.
- 고가용성(HA) 쌍의 두 노드는 동일한 버전이어야 합니다.
- 스토리지 시스템 컨트롤러가 RDMA를 지원해야 함:

| ONTAP로 시작하는 중... | 다음 컨트롤러는 <b>RDMA</b> 를 지원합니다.                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------|
| 9.10.1 이상        | <ul style="list-style-type: none"> <li>• AFF A400</li> <li>• AFF A700</li> <li>• AFF A800</li> </ul>                         |
| ONTAP 9.14.1 이상  | <ul style="list-style-type: none"> <li>• AFF C-Series로 문의하십시오</li> <li>• AFF A900 탑재</li> </ul>                              |
| ONTAP 9.15.1 이상  | <ul style="list-style-type: none"> <li>• AFF A1K 를 참조하십시오</li> <li>• AFF A90 를 참조하십시오</li> <li>• AFF A70 를 참조하십시오</li> </ul> |
| ONTAP 9.16.1 이상  | <ul style="list-style-type: none"> <li>• AFF A50 를 참조하십시오</li> <li>• AFF A30 를 참조하십시오</li> <li>• AFF A20 를 참조하십시오</li> </ul> |

- 데이터 LIF는 RDMA를 지원하도록 구성해야 합니다.
- 대상 RNIC 지원에 대한 자세한 내용은 ["NetApp Hardware Universe를 참조하십시오"](#)참조하십시오.
- RDMA 기반 NFS에 대해 지원되는 클라이언트 운영 체제에 대한 자세한 내용은 ["NetApp 상호 운용성 매트릭스\(IMT\)"](#)참조하십시오. RoCE v2 지원 RNIC에 대해서는 해당 RNIC 공급업체 설명서를 참조하십시오.



RDMA 상의 NFS에서는 인터페이스 그룹이 지원되지 않습니다.

## 다음 단계

- [RDMA를 통해 NFS용 NIC를 구성합니다](#)
- [RDMA를 통해 NFS용 LIF를 구성합니다](#)

- [RDMA를 통한 NFS 설정에 대해 설명합니다](#)

#### 관련 정보

- ["RDMA 를 참조하십시오"](#)
- [NFS 트렁킹 개요](#)
- ["RFC 7530: NFS 버전 4 프로토콜"](#)
- ["RFC 8166: 원격 프로시저 호출 버전 1을 위한 원격 직접 메모리 액세스 전송"](#)
- ["RFC 8167: RPC-over-RDMA 전송에 대한 양방향 원격 프로시저 호출"](#)
- ["RFC 8267: RPC-over-RDMA 버전 1에 NFS 상위 계층의 바인딩"](#)

## RDMA를 통해 NFS용 NIC를 구성합니다

RDMA를 통한 NFS를 사용하려면 클라이언트 시스템과 스토리지 플랫폼 모두에 NIC 구성이 필요합니다.

#### 스토리지 플랫폼 구성

대상 RNIC 지원에 대한 자세한 내용은 ["NetApp Hardware Universe를 참조하십시오"](#)을 참조하십시오.

고가용성(HA) 구성을 사용하는 경우 두 노드 모두 동일한 RNIC를 사용하여 RDMA 페일오버를 지원해야 합니다. NIC는 RoCE를 지원해야 합니다.

- ONTAP 9.10.1부터 다음 명령을 사용하여 RDMA 오프로드 프로토콜 목록을 볼 수 있습니다.

```
network port show -rdma-protocols roce
```

에 대한 자세한 내용은 `network port show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

- ONTAP 9.16.1부터 우선 순위 흐름 제어(PFC)를 사용하는 것이 좋습니다. 다음 명령을 사용하여 PFC를 구성합니다 `network port modify`.

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
pfc -pfc-queues-admin 3
```

- ONTAP 9.16.1 이전에는 기본 전역 흐름 제어(GFC)를 사용하는 것이 좋습니다. 흐름 제어 설정이 변경된 경우 다음 명령을 사용하여 GFC를 `network port modify` 구성합니다.

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
full
```

에 대한 자세한 내용은 `network port modify` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

## 클라이언트 시스템 구성

RDMA 기반 NFS에 대해 지원되는 클라이언트 운영 체제에 대한 자세한 내용은 ["NetApp 상호 운용성 매트릭스\(IMT\)"](#)참조하십시오. RoCE v2 지원 RNIC에 대해서는 해당 RNIC 공급업체 설명서를 참조하십시오.

클라이언트와 서버를 직접 연결할 수 있지만 페일오버 성능을 향상시키려면 스위치를 사용하는 것이 좋습니다.

클라이언트, 서버, 모든 스위치 및 스위치의 모든 포트는 점보 프레임을 사용하여 구성해야 합니다. 클라이언트 및 스위치의 흐름 제어 구성은 ONTAP의 흐름 제어 구성과 일치해야 합니다. ONTAP 9.16.1부터 ONTAP, 스위치 및 클라이언트에서 우선 순위 흐름 제어를 활성화하고 구성하는 것이 가장 좋습니다. ONTAP 9.16.1 이전에는 전역 흐름 제어를 사용하는 것이 좋습니다.

이 구성이 확인되면 RDMA를 사용하여 NFS 내보내기를 마운트할 수 있습니다.

## 시스템 관리자

ONTAP 9.12.1 이상을 사용하여 System Manager를 사용하여 RDMA를 통해 NFS와 네트워크 인터페이스를 구성해야 합니다.

### 단계

1. RDMA가 지원되는지 확인합니다. Network > Ethernet Ports \* 로 이동하여 그룹 보기에서 해당 노드를 선택합니다. 노드를 확장할 때 지정된 포트에 대한 \* RDMA 프로토콜 \* 필드를 확인합니다. 값 \* RoCE \* 는 RDMA가 지원됨을 나타내고 대시(\*-\*)는 지원되지 않음을 나타냅니다.
2. VLAN을 추가하려면 \* + VLAN \* 을 선택합니다. 적절한 노드를 선택합니다. 포트 \* 드롭다운 메뉴에서 사용 가능한 포트가 RDMA를 지원하는 경우 \* RoCE Enabled \* 라는 텍스트가 표시됩니다. RDMA를 지원하지 않으면 텍스트가 표시되지 않습니다.
3. 의 워크플로를 따릅니다 [NFS를 사용하여 Linux 서버용 NAS 스토리지를 설정합니다](#) 새 NFS 서버를 구성합니다.

네트워크 인터페이스를 추가할 때 \* RoCE 포트 사용 \* 을 선택할 수 있습니다. RDMA 상에서 NFS를 사용하려는 네트워크 인터페이스에 대해 이 옵션을 선택합니다.

### CLI를 참조하십시오

1. 다음 명령을 사용하여 NFS 서버에서 RDMA 액세스가 활성화되어 있는지 확인합니다.

```
vserver nfs show-vserver <SVM_name>
```

기본적으로 -RDMA가 활성화되어 있어야 합니다. 그렇지 않은 경우 NFS 서버에서 RDMA 액세스를 설정합니다.

```
vserver nfs modify -vserver <SVM_name> -rdma enabled
```

2. RDMA를 통해 NFSv4.0을 통해 클라이언트를 마운트합니다.
  - a. proto 매개 변수의 입력은 서버 IP 프로토콜 버전에 따라 다릅니다. IPv4인 경우 를 사용합니다 proto=rdma. IPv6인 경우 를 사용합니다 proto=rdma6.
  - b. NFS 타겟 포트를 로 지정합니다 port=20049 표준 포트 2049 대신:

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049
<Server_IP_address>:/<volume_path> <mount_point>
```

3. \* 선택 사항 \*: 클라이언트를 마운트 해제해야 하는 경우 명령을 실행합니다 unmount <mount\_path>

### 추가 정보

- [ONTAP NFS 서버 생성](#)
- [NFS를 사용하여 Linux 서버용 NAS 스토리지를 설정합니다](#)

## RDMA를 통해 NFS용 LIF를 구성합니다

RDMA에서 NFS를 사용하려면 LIF(네트워크 인터페이스)가 RDMA와 호환되도록 구성해야 합니다. LIF와 페일오버 쌍 모두 RDMA를 지원할 수 있어야 합니다.



## 새 LIF를 생성합니다

### 시스템 관리자

System Manager를 사용하여 RDMA 상의 NFS용 네트워크 인터페이스를 생성하려면 ONTAP 9.12.1 이상을 실행해야 합니다.

#### 단계

1. Network > Overview > Network Interfaces \* 를 선택합니다.
2. 를 선택합니다 **+ Add**.
3. NFS, SMB/CIFS, S3 \* 를 선택하면 \* RoCE 포트 사용 \* 옵션이 제공됩니다. RoCE 포트 사용 \* 의 확인란을 선택합니다.
4. 스토리지 VM 및 홈 노드를 선택합니다. 이름, IP 주소 및 서브넷 마스크 를 할당합니다.
5. IP 주소와 서브넷 마스크를 입력하면 System Manager에서는 브로드캐스트 도메인 목록을 RoCE 지원 포트가 있는 목록으로 필터링합니다. 브로드캐스트 도메인을 선택합니다. 선택적으로 게이트웨이를 추가할 수 있습니다.
6. 저장 \* 을 선택합니다.

### CLI를 참조하십시오

#### 단계

1. LIF 생성:

```
'network interface create-vserver_SVM_name_-lif_lif_name_-service-policy_service_policy_name_-home-node_node_name_-home-port_port_name_{-address_netmask_netmask_value_-subnet_subnet_name_} -firewall-policy_mdma_policy_name_auto-tridc-midc-midc_name_
```

- 서비스 정책은 default-data-files 또는 data-nfs 네트워크 인터페이스 서비스를 포함하는 사용자 지정 정책이어야 합니다.
- '-RDMA-protocols' 매개변수는 기본적으로 비어 있는 목록을 허용합니다. RoCE를 가치로 추가하면 LIF는 RoCE 오프로드를 지원하는 포트에서만 구성할 수 있으며, 봇 LIF 마이그레이션 및 페일오버에 영향을 줍니다.

## LIF를 수정합니다

## 시스템 관리자

System Manager를 사용하여 RDMA 상의 NFS용 네트워크 인터페이스를 생성하려면 ONTAP 9.12.1 이상을 실행해야 합니다.

### 단계

1. Network > Overview > Network Interfaces \* 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆의 \* > 편집 \* 을 선택합니다 .
3. RoCE 포트 사용 \* 을 선택하여 RDMA 상 NFS를 활성화하거나 이 상자의 선택을 취소하여 비활성화합니다. 네트워크 인터페이스가 RoCE 가능 포트에 있는 경우 \* RoCE 포트 사용 \* 옆에 확인란이 표시됩니다.
4. 필요에 따라 다른 설정을 수정합니다.
5. 변경 사항을 확인하려면 \* 저장 \* 을 선택합니다.

### CLI를 참조하십시오

1. 'network interface show' 명령을 사용하여 LIF의 상태를 확인할 수 있습니다. 서비스 정책은 data-nfs 네트워크 인터페이스 서비스를 포함해야 합니다. RDMA-protocols 목록에는 RoCE가 포함되어야 합니다. 이러한 조건 중 하나가 참이 아니면 LIF를 수정하십시오.

에 대한 자세한 내용은 `network interface show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. LIF를 수정하려면 다음을 실행합니다.

```
'network interface modify vserver_SVM_name_-lif_lif_name_-service-policy_service_policy_name_-
home-node_name_-home-port_port_name_{-address_-netmask_netmask_value_-}[-subnet_name_]_
-firewall-policy_policy_name_mdma-auto-tridf-protocol
```

에 대한 자세한 내용은 `network interface modify` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.



LIF가 현재 해당 프로토콜을 지원하는 포트에 할당되지 않은 경우 LIF에서 특정 오프로드 프로토콜을 요구하도록 수정하면 오류가 발생합니다.

## LIF 마이그레이션

ONTAP을 사용하면 네트워크 인터페이스(LIF)를 마이그레이션하여 RDMA를 통해 NFS를 사용할 수도 있습니다. 이 마이그레이션을 수행할 때는 대상 포트가 RoCE를 지원하는지 확인해야 합니다. ONTAP 9.12.1부터 이 절차를 시스템 관리자에서 완료할 수 있습니다. 네트워크 인터페이스의 대상 포트를 선택할 때 System Manager에서 포트가 RoCE를 지원하는지 여부를 지정합니다.

다음과 같은 경우에만 LIF를 RDMA를 통한 NFS 구성으로 마이그레이션할 수 있습니다.

- RoCE 가능 포트에서 호스팅되는 NFS RDMA 네트워크 인터페이스(LIF)입니다.
- RoCE 가능 포트에서 호스팅되는 NFS TCP 네트워크 인터페이스(LIF)입니다.
- RoCE가 아닌 지원 포트에서 호스팅되는 NFS TCP 네트워크 인터페이스(LIF)입니다.

네트워크 인터페이스 마이그레이션에 대한 자세한 내용은 [LIF 마이그레이션](#)을 참조하십시오.

## 관련 정보

- LIF를 생성합니다
- LIF를 생성합니다
- LIF를 수정합니다
- LIF 마이그레이션

## NFS 구성을 수정합니다

대부분의 경우 RDMA를 통한 NFS용 NFS 지원 스토리지 VM의 구성을 수정할 필요가 없습니다.

그러나 Mellanox 칩 및 LIF 마이그레이션과 관련된 문제를 처리하는 경우 NFSv4 잠금 유예 기간을 늘려야 합니다. 기본적으로 유예 기간은 45초로 설정됩니다. ONTAP 9.10.1부터 유예 기간의 최대값은 180입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

```
vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
```

이 작업에 대한 자세한 내용은 [ONTAP SVM에 대한 NFSv4 잠금 유예 기간 지정](#) 참조하십시오.

## CLI를 사용하여 SMB를 구성합니다

### ONTAP CLI를 사용한 SMB 구성에 대해 알아보십시오

ONTAP 9 CLI 명령을 사용하여 새 SVM이나 기존 SVM에서 새 볼륨 또는 qtree에 포함된 파일에 대한 SMB 클라이언트 액세스를 구성할 수 있습니다.



*smb*(서버 메시지 블록)는 CIFS(Common Internet File System) 프로토콜의 최신 방언을 의미합니다. ONTAP CLI(Command-Line Interface) 및 OnCommand 관리 툴에서도 *\_cifs\_*가 계속 표시됩니다.

다음과 같은 방법으로 볼륨 또는 qtree에 대한 SMB 액세스를 구성하려면 다음 절차를 사용하십시오.

- SMB 버전 2 이상을 사용하려고 합니다.
- NFS 클라이언트(멀티 프로토콜 구성 아님)가 아니라 SMB 클라이언트만 지원합니다.
- NTFS 파일 권한은 새 볼륨을 보호하는 데 사용됩니다.
- SVM 관리자 권한이 아닌 클러스터 관리자 권한이 있습니다.

SVM 및 LIF를 생성하려면 클러스터 관리자 권한이 필요합니다. SVM 관리자 권한으로 다른 SMB 구성 작업을 수행할 수 있습니다.

- System Manager나 자동화된 스크립팅 도구가 아니라 CLI를 사용하려고 합니다.

System Manager를 사용하여 NAS 멀티 프로토콜 액세스를 구성하려면 [참조하십시오](#) "NFS와 SMB를 모두

사용하여 Windows 및 Linux 모두에 대해 NAS 스토리지를 프로비저닝합니다".

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

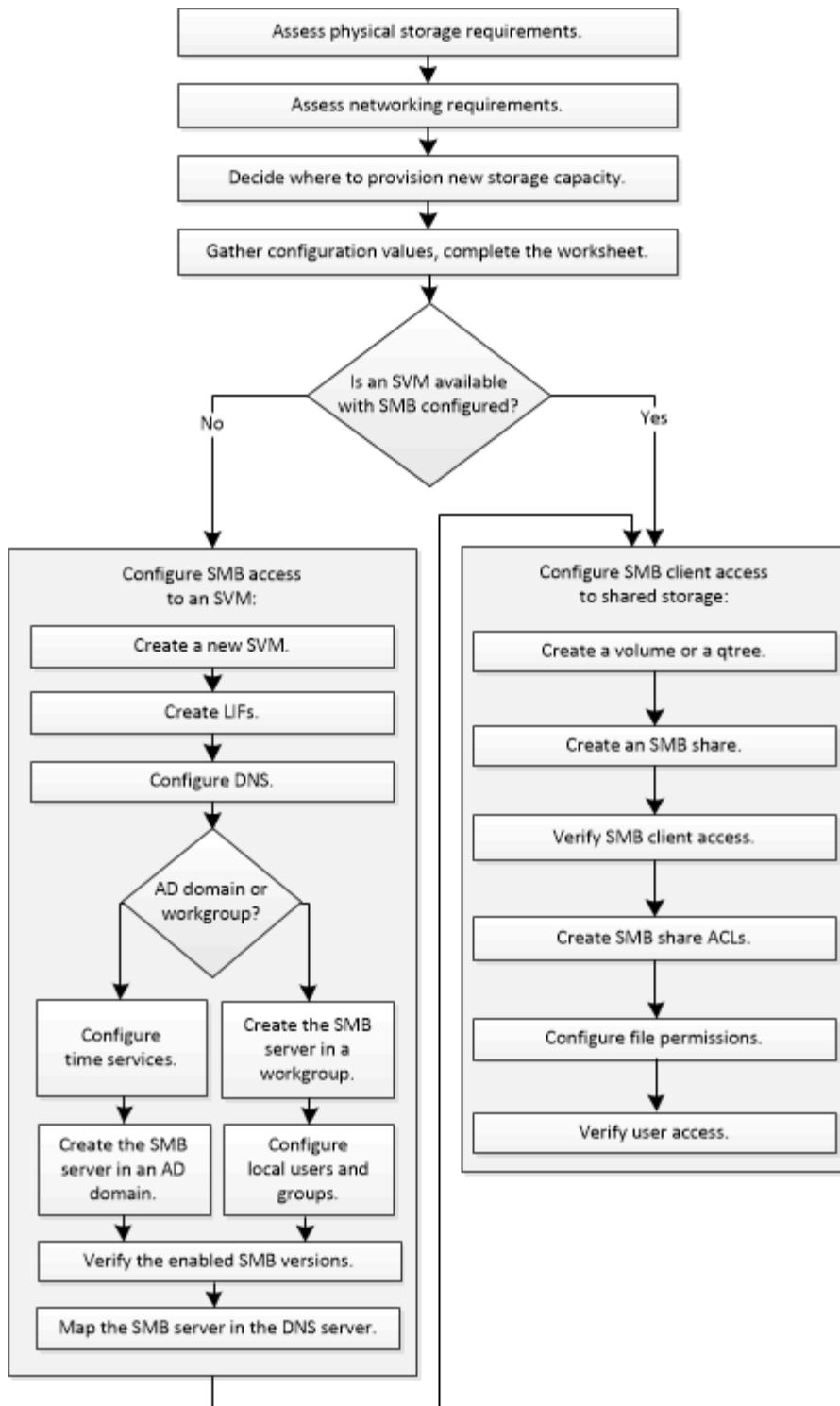
ONTAP SMB 프로토콜 기능 범위에 대한 자세한 내용은 ["SMB 참조 개요"](#)을 참조하십시오.

#### ONTAP에서 이 작업을 수행하는 다른 방법

| 에서 이러한 작업을 수행하려면...                          | 자세한 내용은...                                             |
|----------------------------------------------|--------------------------------------------------------|
| 재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)    | <a href="#">"SMB를 사용하여 Windows 서버용 NAS 스토리지 용량 할당"</a> |
| System Manager Classic(ONTAP 9.7 이하에서 사용 가능) | <a href="#">"SMB 구성 개요"</a>                            |

#### ONTAP SMB 구성 워크플로우

SMB를 구성하려면 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음 목표에 맞는 워크플로우를 선택하고, 새 SVM 또는 기존 SVM에 SMB 액세스를 구성하거나, SMB 액세스에 대해 이미 완벽하게 구성된 기존 SVM에 볼륨 또는 qtree를 추가해야 합니다.



## 준비

**ONTAP SMB**의 물리적 스토리지 요구사항을 평가합니다

클라이언트용 SMB 스토리지를 프로비저닝하기 전에 새 볼륨에 대한 기존 애그리게이트에 충분한 공간이 있는지 확인해야 합니다. 없는 경우 디스크를 기존 Aggregate에 추가하거나 원하는 유형의 새 Aggregate를 생성할 수 있습니다.

## 단계

## 1. 기존 집계에서 사용 가능한 공간 표시: '스토리지 집계 표시'

공간이 충분한 집계가 있는 경우 워크시트에 이름을 기록합니다.

```
cluster::> storage aggregate show
Aggregate Size Available Used% State #Vols Nodes RAID Status

aggr_0 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_1 239.0GB 11.13GB 95% online 1 node1 raid_dp, normal
aggr_2 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_3 239.0GB 11.13GB 95% online 1 node2 raid_dp, normal
aggr_4 239.0GB 238.9GB 95% online 5 node3 raid_dp, normal
aggr_5 239.0GB 239.0GB 95% online 4 node4 raid_dp, normal
6 entries were displayed.
```

2. 충분한 공간이 있는 애그리게이트가 없는 경우 'Storage aggregate add-disks' 명령을 사용하여 기존 애그리게이트에 디스크를 추가하거나 'Storage aggregate create' 명령을 사용하여 새로운 애그리게이트를 생성합니다.

### 관련 정보

- ["스토리지 집계 추가 디스크"](#)
- ["저장소 집계 생성"](#)

## ONTAP SMB 네트워킹 요구사항을 평가합니다

SMB 스토리지를 클라이언트에 제공하기 전에 네트워킹이 SMB 프로비저닝 요구 사항을 충족하도록 올바르게 구성되었는지 확인해야 합니다.

### 시작하기 전에

다음과 같은 클러스터 네트워킹 객체를 구성해야 합니다.

- 물리적 및 논리적 포트
- 브로드캐스트 도메인
- 서브넷(필요한 경우)
- IPspace(기본 IPspace 외에 필요 시)
- 파일오버 그룹(필요에 따라 각 브로드캐스트 도메인의 기본 파일오버 그룹 추가)
- 외부 방화벽

## 단계

### 1. 사용 가능한 물리적 포트와 가상 포트를 네트워크 포트 쇼로 표시합니다

- 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.
- 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.

에 대한 자세한 내용은 `network port show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

### 2. 서브넷 이름을 사용하여 LIF에 대한 IP 주소와 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하는지, 사용 가능한 충분한 주소가 있는지 확인하십시오. 'network subnet show

에 대한 자세한 내용은 `network subnet show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 서브넷은 `network subnet create` 명령을 사용하여 생성된다.

에 대한 자세한 내용은 `network subnet create` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

### 3. 사용 가능한 IPspace 표시: '네트워크 IPspace 쇼'

기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

에 대한 자세한 내용은 `network ipspace show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

### 4. IPv6 주소를 사용하려면 클러스터에서 IPv6가 활성화되어 있는지 확인합니다. 'network options ipv6 show'

필요한 경우 'network options ipv6 modify' 명령을 사용하여 IPv6를 사용하도록 설정할 수 있습니다.

및 `network options ipv6 modify`에 대한 자세한 `network options ipv6 show` 내용은 "[ONTAP 명령 참조입니다](#)" 참조하십시오.

## ONTAP SMB 스토리지 용량 프로비저닝에 대해 알아보십시오

새 SMB 볼륨 또는 qtree를 생성하기 전에 새로운 SVM이나 기존 SVM에 배치할 것인지, SVM에 필요한 구성의 양을 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

## 선택

- 새 SVM에서 볼륨 또는 qtree를 프로비저닝하거나 SMB가 활성화되었지만 구성되지 않은 기존 SVM에서 프로비저닝하려는 경우 "'SVM에 SMB 액세스 구성' 및 "'SMB 지원 SVM에 스토리지 용량 추가" 단계를 완료하십시오.

### SVM에 대한 SMB 액세스 구성

### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

다음 중 하나에 해당하는 경우 새 SVM을 생성할 수 있습니다.

- 클러스터에서 SMB를 처음으로 활성화하는 경우
- SMB 지원을 사용하지 않으려는 클러스터에 기존 SVM이 있습니다.
- 클러스터에 하나 이상의 SMB 지원 SVM이 있으며 다음 연결 중 하나를 원합니다.

- 다른 Active Directory 포리스트 또는 워크그룹에.
- SMB 서버(멀티 테넌시 시나리오) 또한 이 옵션을 선택하여 SMB를 활성화했지만 구성되지 않은 기존 SVM에서 스토리지를 프로비저닝해야 합니다. 이는 SAN 액세스를 위해 SVM을 생성했거나, SVM 생성 시 프로토콜을 사용하지 않은 경우에 발생할 수 있습니다.

SVM에서 SMB를 활성화한 후 볼륨 또는 qtree를 계속해서 프로비저닝합니다.

- SMB 액세스를 위해 완벽하게 구성된 기존 SVM에서 볼륨 또는 qtree를 프로비저닝하려면 "'SMB 지원 SVM에 스토리지 용량 추가' 단계를 완료하십시오.

#### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

### ONTAP SMB 구성 워크시트

SMB 구성 워크시트를 사용하면 클라이언트에 대한 SMB 액세스를 설정하는 데 필요한 정보를 수집할 수 있습니다.

스토리지 용량 할당 위치에 대한 결정에 따라 워크시트의 섹션 중 하나 또는 두 섹션을 모두 완료해야 합니다.

- SVM에 대한 SMB 액세스를 구성하는 경우 두 섹션을 모두 완료해야 합니다.

#### SVM에 대한 SMB 액세스 구성

#### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

- SMB 지원 SVM에 스토리지 용량을 추가하려면 두 번째 섹션만 완료해야 합니다.

#### 공유 스토리지에 대한 SMB 클라이언트 액세스 구성

매개 변수에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

### SVM에 대한 SMB 액세스 구성

- SVM 생성을 위한 매개 변수 \*

새로운 SVM을 생성하는 경우 명령을 통해 이러한 값을 `vserver create` 제공합니다. 에 대한 자세한 내용은 `vserver create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다  | 설명                                                                              | 귀사의 가치 |
|------------|---------------------------------------------------------------------------------|--------|
| '-vserver' | FQDN(정규화된 도메인 이름)이거나 클러스터 전체에 고유한 SVM 이름을 적용하는 다른 규칙을 따르는 새 SVM에 대해 제공하는 이름입니다. |        |
| '-집계'      | 새 SMB 스토리지 용량을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.                                |        |



| 필드에 입력합니다                    | 설명                                         | 귀사의 가치   |
|------------------------------|--------------------------------------------|----------|
| '-rootvolume'                | SVM 루트 볼륨에 제공하는 고유 이름입니다.                  |          |
| '-rootvolume-security-style' | SVM에 NTFS 보안 스타일을 사용하십시오.                  | NTFS     |
| '-언어'                        | 이 워크플로의 기본 언어 설정을 사용합니다.                   | 1. UTF-8 |
| 'IPSpace'                    | 선택 사항: IPspace는 SVM이 상주하는 별개의 IP 주소 공간입니다. |          |

• LIF 생성을 위한 매개 변수 \*

LIF를 생성할 때 이러한 값을 명령과 함께 `network interface create` 제공합니다. 에 대한 자세한 내용은 `network interface create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다   | 설명                                                                                                                                                      | 귀사의 가치    |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| '-lif'      | 새 LIF에 대해 제공한 이름입니다.                                                                                                                                    |           |
| '-역할'       | 이 워크플로우에서 데이터 LIF 역할을 사용합니다.                                                                                                                            | 다타        |
| '-데이터-프로토콜' | 이 워크플로우에서는 SMB 프로토콜만 사용합니다.                                                                                                                             | 'CIFS'입니다 |
| 홈 노드        | LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행할 때 LIF가 반환되는 노드입니다.<br><br>에 대한 자세한 내용은 <code>network interface revert</code> <a href="#">"ONTAP 명령 참조입니다"</a> 을 참조하십시오. |           |
| ``홈 포트``    | LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 포트 또는 인터페이스 그룹입니다.                                                                                           |           |
| 주소          | 새 LIF가 데이터 액세스에 사용할 클러스터의 IPv4 또는 IPv6 주소입니다.                                                                                                           |           |

| 필드에 입력합니다 | 설명                                                                         | 귀사의 가치 |
|-----------|----------------------------------------------------------------------------|--------|
| 넷마스크입니다   | LIF의 네트워크 마스크와 게이트웨이입니다.                                                   |        |
| '-서브넷'    | IP 주소 풀입니다. 주소와 넷마스크를 자동으로 할당하기 위해 -address와 -netmask 대신 사용됩니다.            |        |
| 방화벽 정책    | 이 워크플로우에서 기본 데이터 방화벽 정책을 사용합니다.                                            | 다타     |
| 자동 되돌리기   | 선택 사항: 데이터 LIF가 시작 시 또는 다른 상황에서 홈 노드로 자동 전환되는지 여부를 지정합니다. 기본 설정은 false입니다. |        |

- DNS 호스트 이름 확인을 위한 매개 변수 \*

DNS를 구성할 때 명령과 함께 이러한 값을 `vserver services name-service dns create` 제공합니다. 에 대한 자세한 내용은 `vserver services name-service dns create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다 | 설명                                        | 귀사의 가치 |
|-----------|-------------------------------------------|--------|
| ``도메인'    | 최대 5개의 DNS 도메인 이름                         |        |
| 이름-서버     | 각 DNS 이름 서버에 대해 최대 3개의 IP 주소를 지정할 수 있습니다. |        |

#### Active Directory 도메인에서 SMB 서버 설정

시간 서비스 구성에 대한 매개 변수 \*

시간 서비스를 구성할 때 이러한 값을 명령과 함께 `cluster time-service ntp server create` 제공합니다. 에 대한 자세한 내용은 `cluster time-service ntp server create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다 | 설명                                                   | 귀사의 가치 |
|-----------|------------------------------------------------------|--------|
| '-서버'     | Active Directory 도메인에 대한 NTP 서버의 호스트 이름 또는 IP 주소입니다. |        |

- Active Directory 도메인에서 SMB 서버를 생성하기 위한 매개 변수 \*

새 SMB 서버를 생성하고 도메인 정보를 지정할 때 이러한 값을 명령과 함께 `vserver cifs create` 제공합니다. 에 대한 자세한 내용은 `vserver cifs create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다      | 설명                                                                                       | 귀사의 가치 |
|----------------|------------------------------------------------------------------------------------------|--------|
| '-vserver'     | SMB 서버를 생성할 SVM의 이름입니다.                                                                  |        |
| '-cifs-server' | SMB 서버의 이름(최대 15자).                                                                      |        |
| ``도메인'         | SMB 서버와 연결할 Active Directory 도메인의 FQDN(정규화된 도메인 이름)입니다.                                  |        |
| '-ou'          | 선택 사항: SMB 서버와 연결할 Active Directory 도메인 내의 조직 단위입니다. 기본적으로 이 매개 변수는 CN=Computers로 설정됩니다. |        |
| '-NetBIOS-별칭'  | 선택 사항: NetBIOS 별칭 목록으로, SMB 서버 이름에 대한 대체 이름입니다.                                          |        |
| ``논평'          | 선택 사항: 서버에 대한 텍스트 설명입니다. Windows 클라이언트는 네트워크에서 서버를 검색할 때 이 SMB 서버 설명을 볼 수 있습니다.          |        |

#### 작업 그룹에서 **SMB** 서버 설정

- 작업 그룹에서 SMB 서버를 생성하기 위한 매개 변수 \*

새 SMB 서버를 생성하고 지원되는 SMB 버전을 지정할 때 이러한 값에 명령을 입력합니다 `vserver cifs create`.  
에 대한 자세한 내용은 `vserver cifs create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다      | 설명                                                                              | 귀사의 가치 |
|----------------|---------------------------------------------------------------------------------|--------|
| '-vserver'     | SMB 서버를 생성할 SVM의 이름입니다.                                                         |        |
| '-cifs-server' | SMB 서버의 이름(최대 15자).                                                             |        |
| ``워크그룹"        | 작업 그룹의 이름(최대 15자).                                                              |        |
| ``논평'          | 선택 사항: 서버에 대한 텍스트 설명입니다. Windows 클라이언트는 네트워크에서 서버를 검색할 때 이 SMB 서버 설명을 볼 수 있습니다. |        |

- 로컬 사용자 생성을 위한 매개 변수 \*

명령을 사용하여 로컬 사용자를 만들 때 이러한 값을 `vserver cifs users-and-groups local-user create` 제공합니다. 이러한 서버는 작업 그룹의 SMB 서버에 필요하며 AD 도메인의 선택적 서버에 필요합니다. 에 대한 자세한 내용은 `vserver cifs users-and-groups local-user create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다              | 설명                                                                      | 귀사의 가치 |
|------------------------|-------------------------------------------------------------------------|--------|
| '-vserver'             | 로컬 사용자를 생성할 SVM의 이름입니다.                                                 |        |
| '-user-name'입니다        | 로컬 사용자의 이름(최대 20자).                                                     |        |
| 이름                     | 선택 사항: 사용자의 전체 이름입니다. 전체 이름에 공백이 포함된 경우 전체 이름을 큰따옴표로 묶습니다.              |        |
| ``설명``                 | 선택 사항: 로컬 사용자에 대한 설명입니다. 설명에 공백이 있으면 매개 변수를 따옴표로 묶어야 합니다.               |        |
| '-is-account-disabled' | 선택 사항: 사용자 계정의 사용 여부를 지정합니다. 이 매개 변수를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다. |        |

- 로컬 그룹 생성을 위한 매개 변수 \*

명령을 사용하여 로컬 그룹을 만들 때 이러한 값을 `vserver cifs users-and-groups local-group create` 제공합니다. AD 도메인 및 워크그룹의 SMB 서버에 대해서는 선택 사항입니다. 에 대한 자세한 내용은 `vserver cifs users-and-groups local-group create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다  | 설명                                                       | 귀사의 가치 |
|------------|----------------------------------------------------------|--------|
| '-vserver' | 로컬 그룹을 생성할 SVM의 이름입니다.                                   |        |
| ``그룹 이름``  | 로컬 그룹의 이름입니다(최대 256자).                                   |        |
| ``설명``     | 선택 사항: 로컬 그룹에 대한 설명입니다. 설명에 공백이 있으면 매개 변수를 따옴표로 묶어야 합니다. |        |

#### SMB 지원 SVM에 스토리지 용량 추가

- 볼륨 생성을 위한 매개 변수 \*

qtree가 아닌 볼륨을 생성하는 경우 명령과 함께 이러한 값을 `volume create` 제공합니다. 에 대한 자세한 내용은 `volume create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다  | 설명                                          | 귀사의 가치 |
|------------|---------------------------------------------|--------|
| '-vserver' | 새 볼륨을 호스팅할 새 SVM 또는 기존 SVM의 이름입니다.          |        |
| '- 볼륨'     | 새 볼륨에 제공하는 고유한 설명 이름입니다.                    |        |
| '-집계'      | 새 SMB 볼륨을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다. |        |
| '-size'    | 새 볼륨의 크기에 대해 제공하는 정수입니다.                    |        |
| '-보안-스타일'  | 이 워크플로에 NTFS 보안 스타일을 사용합니다.                 | NTFS   |
| '`교차점-경로`' | 새 볼륨을 마운트할 루트(/) 아래의 위치입니다.                 |        |

- qtree 생성을 위한 매개 변수 \*

볼륨 대신 qtree를 생성하는 경우 명령과 함께 이러한 값을 `volume qtree create` 제공합니다. 에 대한 자세한 내용은 `volume qtree create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다     | 설명                                                                                        | 귀사의 가치 |
|---------------|-------------------------------------------------------------------------------------------|--------|
| '-vserver'    | qtree가 포함된 볼륨이 있는 SVM의 이름입니다.                                                             |        |
| '- 볼륨'        | 새 qtree를 포함할 볼륨의 이름입니다.                                                                   |        |
| '-qtree'      | 새 qtree를 64자 이하로 설명하는 고유한 이름입니다.                                                          |        |
| '-qtree-path' | 볼륨과 qtree를 별도의 인수로 지정하는 대신<br>'/vol/volume_name/qtree_name>' 형식의 qtree 경로 인수를 지정할 수 있습니다. |        |

- SMB 공유 생성을 위한 매개 변수 \*

명령을 사용하여 이러한 값을 `vserver cifs share create` 입력합니다. 에 대한 자세한 내용은 `vserver cifs share create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다  | 설명                                                                                   | 귀사의 가치 |
|------------|--------------------------------------------------------------------------------------|--------|
| '-vserver' | SMB 공유를 생성할 SVM의 이름입니다.                                                              |        |
| '-공유-이름'   | 생성할 SMB 공유의 이름입니다(최대 256자).                                                          |        |
| '-경로'      | SMB 공유의 경로 이름(최대 256자). 공유를 생성하기 전에 이 경로가 볼륨에 있어야 합니다.                               |        |
| '-공유-속성'   | 선택 사항: 공유 속성 목록입니다. 기본 설정은 oplocks, 탐색 가능, changentify, swing-previous-versions입니다.  |        |
| '`논평`'     | 선택 사항: 서버에 대한 텍스트 설명입니다(최대 256자). Windows 클라이언트는 네트워크에서 탐색할 때 이 SMB 공유 설명을 볼 수 있습니다. |        |

- SMB ACL(공유 액세스 제어 목록) 생성을 위한 매개 변수 \*

명령을 사용하여 이러한 값을 `vserver cifs share access-control create` 입력합니다. 에 대한 자세한 내용은 `vserver cifs share access-control create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

| 필드에 입력합니다             | 설명                                                                                        | 귀사의 가치         |
|-----------------------|-------------------------------------------------------------------------------------------|----------------|
| '-vserver'            | SMB ACL을 생성할 SVM의 이름입니다.                                                                  |                |
| '-share'              | 생성할 SMB 공유의 이름입니다.                                                                        |                |
| '-user-group-type'입니다 | 공유의 ACL에 추가할 사용자 또는 그룹의 유형입니다. 기본 유형은 Windows입니다                                          | "창"            |
| '- 사용자 또는 그룹'         | 공유의 ACL에 추가할 사용자 또는 그룹입니다. 사용자 이름을 지정하는 경우 "domain\username" 형식을 사용하여 사용자의 도메인을 포함해야 합니다. |                |
| 허락                    | 사용자 또는 그룹에 대한 권한을 지정합니다.                                                                  | '[No_access    |
| Read                  | Change                                                                                    | Full_Control]' |

## SVM에 대한 SMB 액세스를 구성합니다

### ONTAP SVM에 대한 SMB 액세스를 구성합니다

SMB 클라이언트 액세스를 위해 SVM이 아직 구성되지 않은 경우 새 SVM을 생성 및 구성하거나 기존 SVM을 구성해야 합니다. SMB를 구성하려면 SVM 루트 볼륨 액세스를 열고, SMB 서버를 생성하고, LIF를 생성하고, 호스트 이름 확인을 지원하고, 이름 서비스를 구성하고, 필요한 경우 Kerberos 보안 활성화.

### ONTAP SVM을 생성하여 SMB 데이터 액세스를 제공합니다

SMB 클라이언트에 데이터 액세스를 제공하기 위해 클러스터에 SVM을 하나 이상 가지고 있지 않은 경우 하나 생성해야 합니다.

#### 시작하기 전에

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 [SVM 용량 관리](#) 참조하십시오.

#### 단계

1. SVM 생성: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
  - '-rootvolume-security-style' 옵션에 NTFS 설정을 사용합니다.
  - 기본 C. UTF-8 '-language' 옵션을 사용합니다.
  - IPSpace 설정은 선택 사항입니다.
2. 새로 생성한 SVM의 구성 및 상태 확인: `vserver show -vserver vserver_name`

허용되는 프로토콜 필드에는 CIFS가 포함되어야 합니다. 나중에 이 목록을 편집할 수 있습니다.

'Vserver 작동 상태' 필드에는 '실행 중' 상태가 표시되어야 합니다. 초기화 중 상태가 표시되는 경우 루트 볼륨 생성 등 일부 중간 작업이 실패한 것으로, SVM을 삭제하고 다시 생성해야 합니다.

#### 예

다음 명령은 IPspace에서 데이터 액세스를 위한 SVM을 생성합니다 ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

다음 명령을 실행하면 루트 볼륨 1GB 단위로 SVM이 생성되고 자동으로 시작되어 '실행 중' 상태에 있음을 알 수 있습니다. 루트 볼륨에는 규칙을 포함하지 않는 기본 익스포트 정책이 있으므로 생성 시 루트 볼륨을 내보내지 않습니다.

```
cluster1::> vserver show -vserver vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 [올 적응형 정책 그룹 템플릿을 설정합니다](#) 참조하십시오.

**ONTAP SVM에서 SMB 프로토콜이 활성화되었는지 확인합니다**

SVM에서 SMB를 구성 및 사용하려면 먼저 프로토콜이 활성화되어 있는지 확인해야 합니다.

이 작업에 대해

이는 일반적으로 SVM 설정 중에 수행되지만 설정 중에 프로토콜을 활성화하지 않은 경우 나중에 'vserver add-protocols' 명령을 사용하여 활성화할 수 있습니다.



프로토콜을 생성한 후에는 LIF에서 프로토콜을 추가하거나 제거할 수 없습니다.

"vserver remove-protocols" 명령을 사용하여 SVM에서 프로토콜을 비활성화할 수도 있습니다.

단계

1. SVM에 대해 현재 활성화 및 비활성화된 프로토콜은 'vserver show -vserver vserver\_name -protocols'(vserver show -vserver vserver vserver\_name -protocol)를 확인하십시오



"vserver show-protocols" 명령을 사용하여 클러스터의 모든 SVM에서 현재 활성화된 프로토콜을 볼 수도 있습니다.

2. 필요한 경우 프로토콜을 활성화 또는 비활성화합니다.

- SMB 프로토콜을 활성화하려면: 'vserver add-protocols-vserver vserver\_name-protocols cifs'
- 프로토콜을 작동 불가능하게 하려면: "vserver remove-protocols-vserver vserver\_name-protocols protocol\_name[,protocol\_name,...]"

3. 활성화된 프로토콜과 비활성화된 프로토콜이 'vserver show -vserver vserver\_name -protocols'(vserver show -vserver vserver\_name -protocol)로 올바르게 업데이트되었는지 확인합니다

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 현재 설정 및 해제된 프로토콜(허용 및 허용 안 함)이 표시됩니다.

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver Allowed Protocols Disallowed Protocols

vs1.example.com cifs nfs, fcp, iscsi, ndmp
```

다음 명령을 실행하면 VS1 이라는 SVM의 활성화된 프로토콜 목록에 "CIFS"를 추가하여 SMB를 통해 액세스할 수 있습니다.

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

## ONTAP SVM 루트 볼륨의 SMB 익스포트 정책을 엽니다

SVM 루트 볼륨의 기본 익스포트 정책에는 SMB를 통한 모든 클라이언트의 개방형 액세스를 지원하는 규칙이 포함되어야 합니다. 이러한 규칙이 없으면 모든 SMB 클라이언트가 SVM 및 해당 볼륨에 대한 액세스가 거부됩니다.

이 작업에 대해

새 SVM이 생성되면 SVM의 루트 볼륨에 대한 기본 익스포트 정책(기본값)이 자동으로 생성됩니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 익스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다.

모든 SMB 액세스가 기본 익스포트 정책에서 열려 있는지 확인하고, 나중에 개별 볼륨 또는 qtree에 대한 사용자 지정 익스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. 기존 SVM을 사용하는 경우 기본 루트 볼륨 익스포트 정책('vserver export-policy rule show')을 확인하십시오

명령 출력은 다음과 같아야 합니다.

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance
```

```

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

이러한 규칙이 열려 있는 액세스를 허용하는 경우 이 작업은 완료된 것입니다. 그렇지 않은 경우 다음 단계를 진행하십시오.

2. SVM 루트 볼륨에 대한 익스포트 규칙을 생성합니다. 'vserver export-policy rule create-vserver vserver\_name-policyname default-ruleindex 1-protocol cifs-clientmatch 0.0.0.0/0 -rorule any-rwrule any-superuser any'입니다
3. 'vserver export-policy rule show' 명령을 사용하여 규칙 생성을 확인합니다.

결과

이제 모든 SMB 클라이언트가 SVM에서 생성된 모든 볼륨 또는 qtree에 액세스할 수 있습니다.

## ONTAP SMB LIF를 생성합니다

LIF는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트에 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 up 상태로 구성되어야 합니다. 에 대한 자세한 내용은 up ["ONTAP 명령 참조입니다"](#)을 참조하십시오.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 네트워크 서브넷 만들기 명령을 사용하여 만듭니다.

에 대한 자세한 내용은 `network subnet create` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

이 작업에 대해

- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- 클러스터에 LIF가 많은 경우 'network interface capacity show' 명령을 사용하여 클러스터에서 지원되는 LIF 용량과 각 노드에서 지원되는 LIF 용량을 확인할 수 있습니다 (고급 권한 수준에서).

에 대한 자세한 내용은 network interface "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

단계

#### 1. LIF 생성:

```
'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-
node_node_name_-home-port_port_name_{-address_ip_address_-netmask ip_address_-subnet-
name_subnet_name_-}firewall-policy data-auto-revert{true|false}'
```

\* ONTAP 9.5 이하 \*

```
'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-
node_node_name_-home-port_port_name_{-address_name_- netmask_ip_address_-
- subnet-name_subnet_name_-}firewall-policy data-auto-revert{true
false}
```

\* ONTAP 9.6 이상 \*

```
'network interface create-vserver_vserver_name_-lif_lif_name_-service-policy_service_policy_name_-
home-node_node_name_-home-port_port_name_{-address_netmask_ip_address_-
-subnet_name_subnet_name_-}firewall-policy data-auto-revert_revert_false
```

- 서비스 정책(ONTAP 9.6부터)을 사용하여 LIF를 생성할 때는 '-role' 매개 변수가 필요하지 않습니다.
- 를 클릭합니다 -data-protocol ONTAP 9.6부터 서비스 정책을 사용하여 LIF를 생성할 때 매개 변수가 필요하지 않습니다. ONTAP 9.5 이하 버전을 사용하는 경우 -data-protocol LIF를 생성할 때 매개 변수를 지정해야 하며 나중에 데이터 LIF를 폐기 및 재생성하지 않고 수정할 수 없습니다.
- 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도 있습니다.

- '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
- IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet\_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
- 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.

- 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 network route create 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.
- '-firewall-policy' 옵션의 경우 LIF 역할과 동일한 기본 data를 사용합니다.

필요에 따라 나중에 사용자 지정 방화벽 정책을 만들고 추가할 수 있습니다.



ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 ["LIF의 방화벽 정책을 구성합니다"](#)를 참조하십시오.

- '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 false로 설정할 수 있습니다.

## 2. LIF가 성공적으로 생성되었는지 확인합니다.

네트워크 인터페이스 쇼

## 3. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

| 다음을 확인하려면... | 사용...   |
|--------------|---------|
| IPv4 주소입니다   | 네트워크 핑  |
| IPv6 주소입니다   | 네트워크 핑6 |

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1\_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 cluster-1의 모든 LIF가 표시됩니다. 데이터 LIF datalif1 및 datalif3은 IPv4 주소로 구성되고 datalif4는 IPv6 주소로 구성됩니다.

```
network interface show
```

| Vserver                   | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is    |
|---------------------------|-------------------|-------------------|----------------------|--------------|--------------|-------|
| Home                      |                   |                   |                      |              |              |       |
| -----                     | -----             | -----             | -----                | -----        | -----        | ----- |
| cluster-1                 |                   |                   |                      |              |              |       |
| true                      | cluster_mgmt      | up/up             | 192.0.2.3/24         | node-1       | e1a          |       |
| node-1                    |                   |                   |                      |              |              |       |
| true                      | clus1             | up/up             | 192.0.2.12/24        | node-1       | e0a          |       |
| true                      | clus2             | up/up             | 192.0.2.13/24        | node-1       | e0b          |       |
| true                      | mgmt1             | up/up             | 192.0.2.68/24        | node-1       | e1a          |       |
| node-2                    |                   |                   |                      |              |              |       |
| true                      | clus1             | up/up             | 192.0.2.14/24        | node-2       | e0a          |       |
| true                      | clus2             | up/up             | 192.0.2.15/24        | node-2       | e0b          |       |
| true                      | mgmt1             | up/up             | 192.0.2.69/24        | node-2       | e1a          |       |
| vs1.example.com           |                   |                   |                      |              |              |       |
| true                      | datalif1          | up/down           | 192.0.2.145/30       | node-1       | e1c          |       |
| vs3.example.com           |                   |                   |                      |              |              |       |
| true                      | datalif3          | up/up             | 192.0.2.146/30       | node-2       | e0c          |       |
| true                      | datalif4          | up/up             | 2001::2/64           | node-2       | e0c          |       |
| 5 entries were displayed. |                   |                   |                      |              |              |       |

다음 명령을 실행하면 기본 데이터 파일 서비스 정책에 할당된 NAS 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

#### 관련 정보

- ["네트워크 Ping"](#)
- ["네트워크 인터페이스 복원"](#)

## ONTAP SMB 호스트 이름 확인을 위해 DNS를 활성화합니다

명령을 사용하여 SVM에서 DNS를 사용하도록 설정하고, 호스트 이름 확인에 DNS를 사용하도록 구성할 수 `vserver services name-service dns` 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다. 에 대한 자세한 내용은 `vserver services name-service dns` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. `vserver services name-service dns create`` DNS 서버 이름을 하나만 입력하면 명령이 경고를 표시합니다. 에 대한 자세한 내용은 ``vserver services name-service dns create` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

이 작업에 대해

에 대해 자세히 "[SVM에서 동적 DNS 구성](#)"알아보십시오.

단계

1. SVM에서 DNS를 활성화합니다. `'vserver services name-service dns create-vserver vserver_name-domain domain_name-name-servers ip_address-state enabled'`

다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



를 클릭합니다 `vserver services name-service dns create` Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. `'vserver services name-service dns show'` 명령을 사용하여 DNS 도메인 구성을 표시합니다.

다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

```
vserver services name-service dns show
```

|                 |         |             | Name                        |
|-----------------|---------|-------------|-----------------------------|
| Vserver         | State   | Domains     | Servers                     |
| cluster1        | enabled | example.com | 192.0.2.201,<br>192.0.2.202 |
| vs1.example.com | enabled | example.com | 192.0.2.201,<br>192.0.2.202 |

다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com
```

| Vserver         | Name Server | Status | Status Details          |
|-----------------|-------------|--------|-------------------------|
| vs1.example.com | 10.0.0.50   | up     | Response time (msec): 2 |
| vs1.example.com | 10.0.0.51   | up     | Response time (msec): 2 |

**Active Directory** 도메인에서 **SMB** 서버를 설정합니다

**SMB** 서버에 대한 **ONTAP** 시간 서비스를 구성합니다

Active Domain 컨트롤러에서 SMB 서버를 생성하기 전에 SMB 서버가 속할 도메인의 도메인 컨트롤러에 대한 클러스터 시간 및 시간이 5분 이내에 일치하는지 확인해야 합니다.

이 작업에 대해

Active Directory 도메인에서 사용하는 것과 동일한 NTP 서버를 동기화에 사용하도록 클러스터 NTP 서비스를 구성해야 합니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 설정할 수 있습니다.

단계

1. cluster time-service NTP server create 명령을 사용하여 시간 서비스를 구성합니다.
  - 대칭 인증 없이 시간 서비스를 구성하려면 'cluster time-service ntp server create-server\_ip\_address' 명령을 입력합니다
  - 대칭적 인증으로 시간 서비스를 구성하려면 'cluster time-service ntp server create-server\_ip\_address-key-id key-id key\_id"cluster time-service ntp server create-server 10.10.10.1"cluster time-service ntp server create-server 10.10.10.10.10.2' 명령을 입력한다
2. cluster time-service ntp server show 명령을 사용하여 시간 서비스가 올바르게 설정되었는지 확인합니다.

클러스터 시간 서비스 NTP 서버가 표시됩니다

| Server     | Version |
|------------|---------|
| -----      | -----   |
| 10.10.10.1 | auto    |
| 10.10.10.2 | auto    |

## 관련 정보

- ["클러스터 시간 - 서비스 NTP"](#)

**NTP** 서버에서 대칭 인증을 관리하기 위한 **ONTAP** 명령

ONTAP 9.5부터 NTP(네트워크 시간 프로토콜) 버전 3이 지원됩니다. NTPv3에는 SHA-1 키를 사용한 대칭 인증이 포함되어 있어 네트워크 보안을 강화합니다.

| 수행할 작업...                                                          | 이 명령 사용...                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 대칭 인증 없이 NTP 서버를 구성합니다                                             | 클러스터 시간 서비스 NTP 서버는 서버 서버 서버 서버 이름(server_name)을 만듭니다                                                                                                                                                                                                              |
| 대칭 인증을 사용하여 NTP 서버를 구성합니다                                          | 클러스터 시간 서비스 NTP 서버는 '-server"server_ip_address"-key-id"key_id"'를 생성합니다                                                                                                                                                                                             |
| 기존 NTP 서버에 대칭 인증 사용 기존 NTP 서버는 필요한 키 ID를 추가하여 인증을 사용하도록 수정할 수 있습니다 | 클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 이름 키 ID 키 ID                                                                                                                                                                                                              |
| 공유 NTP 키를 구성합니다                                                    | <div> 클러스터 시간 서비스 NTP 키는 ``id"sshared_key_id"-type'sshared_key_type' -value'sshared_key_value'를 만듭니다 </div> <div>  공유 키는 ID로 참조됩니다. ID, 유형 및 값은 노드와 NTP 서버 모두에서 동일해야 합니다 </div> |
| 알 수 없는 키 ID로 NTP 서버를 구성합니다                                         | 클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다                                                                                                                                                                                                                    |
| NTP 서버에 키 ID가 구성되지 않은 서버를 구성합니다.                                   | <div> 클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다 </div> <div>  키 ID, 유형 및 값은 NTP 서버에 구성된 키 ID, 유형 및 값과 동일해야 합니다. </div>                                                    |
| 대칭 인증을 사용하지 않도록 설정합니다                                              | 클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 이름 인증 비활성화                                                                                                                                                                                                                |



## 관련 정보

- ["클러스터 시간 - 서비스 NTP"](#)

ONTAP Active Directory 도메인에 SMB 서버를 생성합니다

"vserver cifs create" 명령을 사용하여 SVM에 SMB 서버를 생성하고 해당 서버가 속한 AD(Active Directory) 도메인을 지정할 수 있습니다.

### 시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 SMB 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버와 SMB 서버에 연결할 도메인의 AD 도메인 컨트롤러에 연결할 수 있어야 합니다.

SMB 서버에 연결할 AD 도메인에서 시스템 계정을 만들 수 있는 권한이 있는 모든 사용자는 SVM에 SMB 서버를 생성할 수 있습니다. 여기에는 다른 도메인의 사용자가 포함될 수 있습니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-Uri' 매개 변수에 vserver cifs' 명령을 포함하여 포함시키십시오.

### 이 작업에 대해

Activity Directory 도메인에서 SMB 서버를 생성하는 경우:

- 도메인을 지정할 때는 FQDN(정규화된 도메인 이름)을 사용해야 합니다.
- 기본 설정은 Active Directory CN=Computer 개체에 SMB 서버 컴퓨터 계정을 추가하는 것입니다.
- '-ou' 옵션을 사용하여 SMB 서버를 다른 OU(조직 구성 단위)에 추가하도록 선택할 수 있습니다.
- SMB 서버에 대해 심표로 구분된 하나 이상의 NetBIOS 별칭 목록(최대 200)을 추가하도록 선택할 수도 있습니다.

SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 서버의 이름에 응답하도록 할 때 유용합니다.

및 선택적 매개 변수 및 명령 요구 사항에 대한 자세한 vserver cifs 내용은 ["ONTAP 명령 참조입니다"](#) 참조하십시오.

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다. ONTAP는 '-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러 통신을 암호화해야 하며 기본값은 false입니다. SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다. .

["SMB 관리"](#) SMB 서버 구성 옵션에 대한 자세한 내용은 에 나와 있습니다.

### 단계

1. smb 라이선스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

SMB 라이선스는 에 포함되어 ["ONTAP 1 을 참조하십시오"](#) 있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이선스가 필요하지 않습니다.

2. AD 도메인에서 SMB 서버를 생성합니다.(+ vserver cifs create -vserver vserver\_name -cifs -server smb\_server\_name -domain FQDN [-ou 조직\_unit] [-NetBIOS-별칭 netbios\_name,...] [-keytab -Uri {(ftp | http)://hostname | ip\_address}] [-comment text] +'

도메인에 참가할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

다음 명령을 실행하면 도메인 "example.com"에 SMB 서버 "smb\_server01"이 생성됩니다

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

다음 명령을 실행하면 도메인 "mydomain.com"에 SMB 서버 "smb\_server02"가 생성되고 keytab 파일을 사용하여 ONTAP 관리자를 인증합니다.

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

이 예제에서 명령 출력은 "smb\_server01"이라는 SMB 서버가 SVM vs1.example.com에서 생성되어 "example.com" 도메인에 가입된 것을 보여 줍니다.

```
cluster1::> vserver cifs show -vserver vs1

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. 필요한 경우 도메인 컨트롤러(ONTAP 9.8 이상)와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver svm\_name -encryption -required-for-dc-connection true'

예

다음 명령을 실행하면 "example.com" 도메인의 SVM vs2.example.com에 "smb\_server02" 이름의 SMB 서버가 생성됩니다. 컴퓨터 계정은 "OU=ENG,OU=Corp,DC=example,DC=com" 컨테이너에 생성됩니다. SMB 서버에는 NetBIOS 별칭이 할당됩니다.

```
cluster1::> vsserver cifs create -vsserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01
```

```
cluster1::> vsserver cifs show -vsserver vs1
```

```

 Vserver: vs2.example.com
 CIFS Server NetBIOS Name: SMB_SERVER02
 NetBIOS Domain/Workgroup Name: EXAMPLE
 Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
 Authentication Style: domain
 CIFS Server Administrative Status: up
 CIFS Server Description: -
 List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

다음 명령을 사용하면 다른 도메인의 사용자(이 경우 신뢰할 수 있는 도메인 관리자)가 SVM vs3.example.com 에 "smb\_server03" 이름의 SMB 서버를 생성할 수 있습니다. '-domain' 옵션은 SMB 서버를 생성하려는 홈 도메인(DNS 구성에 지정됨)의 이름을 지정합니다. 사용자 이름 옵션은 신뢰할 수 있는 도메인의 관리자를 지정합니다.

- 홈 도메인: example.com
- 신뢰할 수 있는 도메인: trust.lab.com
- 신뢰할 수 있는 도메인의 사용자 이름: Administrator1

```
cluster1::> vsserver cifs create -vsserver vs3.example.com -cifs-server
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com
Password: . . .
```

**ONTAP SMB** 인증을 위한 **keytab** 파일을 생성합니다

ONTAP 9.7부터 ONTAP는 keytab 파일을 사용하여 AD(Active Directory) 서버에서 SVM 인증을 지원합니다. AD 관리자는 keytab 파일을 생성하여 ONTAP 관리자가 이를 URI(Uniform Resource Identifier)로 사용할 수 있도록 합니다. 이 URI는 'vsserver cifs' 명령에 AD 도메인과의 Kerberos 인증이 필요한 경우에 제공됩니다.

AD 관리자는 표준 Windows Server "ktpass" 명령을 사용하여 keytab 파일을 만들 수 있습니다. 이 명령은 인증이 필요한 기본 도메인에서 실행해야 합니다. "ktpass" 명령은 기본 도메인 사용자에게 대해서만 keytab 파일을 생성하는 데 사용할 수 있으며, trusted-domain 사용자를 사용하여 생성된 키는 지원되지 않습니다.

Keytab 파일은 특정 ONTAP 관리자 사용자를 위해 생성됩니다. admin 사용자의 암호가 변경되지 않는 한, 특정 암호화 유형 및 도메인에 대해 생성된 키는 변경되지 않습니다. 따라서 admin 사용자의 암호를 변경할 때마다 새 keytab 파일이 필요합니다.

지원되는 암호화 유형은 다음과 같습니다.

- AES256-SHA1
- DES-CBC-MD5



ONTAP는 DES-CBC-CRC 암호화 유형을 지원하지 않습니다.

- RC4-HMAC

AES256은 가장 높은 암호화 유형으로, ONTAP 시스템에서 활성화된 경우 사용해야 합니다.

keytab 파일은 admin 암호를 지정하거나 임의로 생성된 암호를 사용하여 생성할 수 있습니다. 그러나 언제든지 한 개의 암호 옵션만 사용할 수 있습니다. AD 서버에서는 키 탭 파일 내의 키를 해독하기 위해 관리자 사용자 고유의 개인 키가 필요하기 때문입니다. 특정 관리자에 대한 개인 키를 변경하면 keytab 파일이 무효화됩니다.

워크그룹에서 **SMB** 서버를 설정합니다

**ONTAP** 워크그룹의 **SMB** 서버 구성에 대해 알아보십시오

작업 그룹에서 **SMB** 서버를 구성원으로 설정하는 작업은 **SMB** 서버를 생성한 다음 로컬 사용자 및 그룹을 만드는 작업으로 구성됩니다.

Microsoft Active Directory 도메인 인프라를 사용할 수 없는 경우 작업 그룹에서 **SMB** 서버를 구성할 수 있습니다.

작업 그룹 모드의 **SMB** 서버는 NTLM 인증만 지원하며 Kerberos 인증을 지원하지 않습니다.

지정된 작업 그룹을 사용하여 **ONTAP SVM**에 **SMB** 서버를 생성합니다

"vserver cifs create" 명령을 사용하여 SVM에 **SMB** 서버를 생성하고 해당 서버가 속한 작업 그룹을 지정할 수 있습니다.

시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 **SMB** 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버에 연결할 수 있어야 합니다.

이 작업에 대해

워크그룹 모드의 **SMB** 서버는 다음 **SMB** 기능을 지원하지 않습니다.

- **SMB3** Witness 프로토콜
- **SMB3** CA 공유
- **SMB**를 통한 SQL
- 폴더 리디렉션
- 로밍 프로필
- GPO(그룹 정책 개체)
- VSS(볼륨 스냅샷 서비스)

및 선택적 구성 매개 변수 및 명령 요구 사항에 대한 자세한 vserver cifs 내용은 을 ["ONTAP 명령 참조입니다"](#) 참조하십시오.

## 단계

1. smb 라이선스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

SMB 라이선스는 에 포함되어 ["ONTAP 1 을 참조하십시오"](#) 있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이선스가 필요하지 않습니다.

2. 워크그룹에서 SMB 서버를 생성합니다. 'vserver cifs create -vserver vserver\_name-cifs-server cifs\_server\_name-workgroup workgroup\_name[-comment text]'

다음 명령을 실행하면 워크그룹 workgroup01에 SMB 서버 "smb\_server01"이 생성됩니다.

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

다음 예제에서 명령 출력은 "workgroup01" 워크그룹의 SVM vs1.example.com 에서 "smb\_server01" 이름의 SMB 서버가 생성되었음을 보여 줍니다.

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

## 작업을 마친 후

작업 그룹의 CIFS 서버의 경우 SVM에서 로컬 사용자와 로컬 그룹을 생성해야 합니다(선택 사항).

## 관련 정보

### ["SMB 관리"](#)

로컬 **ONTAP SMB** 사용자 계정을 생성합니다

SMB 연결을 통해 SVM에 포함된 데이터에 대한 액세스를 승인하는 데 사용할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. SMB 세션을 생성할 때 인증에 로컬 사용자 계정을 사용할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 사용자 기능이 기본적으로 활성화됩니다.

로컬 사용자 계정을 생성할 때 사용자 이름을 지정해야 하며 계정을 연결할 SVM을 지정해야 합니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs users-and-groups local-user` 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

단계

1. 로컬 사용자: `vserver cifs users-and-groups local-user create-vserver_vserver_name_-user-name_user_name__optional_parameters_`를 생성합니다

다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

- 이름

사용자의 전체 이름입니다.

- ``설명``

로컬 사용자에 대한 설명입니다.

- `'-is-account-disabled{true|false}'`

사용자 계정의 사용 여부를 지정합니다. 이 매개 변수를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다.

명령을 실행하면 로컬 사용자 암호를 묻는 메시지가 표시됩니다.

2. 로컬 사용자의 암호를 입력한 다음 암호를 확인합니다.
3. 사용자가 성공적으로 생성되었는지 확인합니다. `vserver cifs users-and-groups local-user show -vserver_vserver_name_`

예

다음 예에서는 SVM `vs1.example.com` 과 관련된 "sUE Chang"이라는 전체 이름으로 로컬 사용자 "sMB\_SERVER01\sue"를 생성합니다.

```
cluster1::> vsriver cifs users-and-groups local-user create -vsriver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vsriver cifs users-and-groups local-user show
Vserver User Name Full Name Description

vs1 SMB_SERVER01\Administrator Built-in administrator
account
vs1 SMB_SERVER01\sue Sue Chang
```

로컬 **ONTAP SMB** 그룹을 생성합니다

SMB 연결을 통해 SVM과 관련된 데이터에 대한 액세스 권한을 부여하는 데 사용할 수 있는 로컬 그룹을 생성할 수 있습니다. 그룹의 구성원이 보유한 사용자 권한 또는 기능을 정의하는 권한을 할당할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 그룹 기능이 기본적으로 활성화됩니다.

로컬 그룹을 생성할 때 그룹 이름을 지정해야 하며 그룹을 연결할 SVM을 지정해야 합니다. 로컬 도메인 이름을 사용하거나 사용하지 않고 그룹 이름을 지정할 수 있으며, 선택적으로 로컬 그룹에 대한 설명을 지정할 수 있습니다. 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 vsriver cifs users-and-groups local-group 내용은 을 ["ONTAP 명령 참조입니다"](#)참조하십시오.

단계

1. 로컬 그룹 'vsriver cifs users-and-groups local-group create-vsvriver vsriver\_name-group-name group\_name'을 생성합니다

다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

◦ ``설명``

로컬 그룹에 대한 설명입니다.

2. 그룹이 성공적으로 생성되었는지 확인합니다. 'vsriver cifs users-and-groups local-group show-vsvriver vsriver\_name'

예

다음 예에서는 SVM VS1 관련 로컬 그룹 "sMB\_SERVER01\engineering"을 생성합니다.

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

| Vserver         | Group Name               | Description                          |
|-----------------|--------------------------|--------------------------------------|
| vs1.example.com | BUILTIN\Administrators   | Built-in Administrators group        |
| vs1.example.com | BUILTIN\Backup Operators | Backup Operators group               |
| vs1.example.com | BUILTIN\Power Users      | Restricted administrative privileges |
| vs1.example.com | BUILTIN\Users            | All users                            |
| vs1.example.com | SMB_SERVER01\engineering |                                      |
| vs1.example.com | SMB_SERVER01\sales       |                                      |

작업을 마친 후

새 그룹에 구성원을 추가해야 합니다.

로컬 **ONTAP SMB** 그룹 구성원 자격을 관리합니다

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 구성원 자격을 관리할 수 있습니다. 이 기능은 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하려는 경우 또는 사용자가 해당 그룹에 연결된 권한을 가지도록 하려는 경우에 유용합니다.

이 작업에 대해

더 이상 로컬 사용자, 도메인 사용자 또는 도메인 그룹이 그룹의 구성원 자격에 따라 액세스 권한이나 권한을 가지도록 하지 않으려면 그룹에서 해당 구성원을 제거할 수 있습니다.

로컬 그룹에 구성원을 추가할 때는 다음 사항을 염두에 두어야 합니다.

- special\_everyone\_group에 사용자를 추가할 수 없습니다.
- 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.
- 도메인 사용자 또는 그룹을 로컬 그룹에 추가하려면 ONTAP에서 SID에 대한 이름을 확인할 수 있어야 합니다.

로컬 그룹에서 구성원을 제거할 때는 다음 사항을 염두에 두어야 합니다.

- special\_everyone\_group에서 구성원을 제거할 수 없습니다.
- 로컬 그룹에서 구성원을 제거하려면 ONTAP에서 해당 이름을 SID로 확인할 수 있어야 합니다.

단계

1. 그룹에 구성원을 추가하거나 그룹에서 구성원을 제거합니다.

- 멤버(+ vserver cifs users-and-groups local-group add-member -vserver\_name -group-name group\_name -member-name name[...]+)를 추가합니다



로컬 사용자, 도메인 사용자 또는 도메인 그룹의 심표로 구분된 목록을 지정하여 지정된 로컬 그룹에 추가할 수 있습니다.

- 멤버(+ vserver cifs users-and-groups local-group remove-member-vserver vserver\_name -group-name group\_name -member-name[,...]+'')를 제거합니다

로컬 사용자, 도메인 사용자 또는 도메인 그룹의 심표로 구분된 목록을 지정하여 지정된 로컬 그룹에서 제거할 수 있습니다.

예

다음 예에서는 SVM vs1.example.com 에서 로컬 사용자 "sMB\_SERVER01\SUB"를 로컬 그룹 "sMB\_SERVER01\engineering"에 추가합니다.

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

다음 예에서는 SVM vs1.example.com 에서 로컬 그룹 "sMB\_SERVER01\engineering"에서 로컬 사용자 "sMB\_SERVER01\SUB" 및 "sMB\_SERVER01\James"를 제거합니다.

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

활성화된 **ONTAP SMB** 버전을 확인합니다

ONTAP 9 릴리즈에서는 클라이언트 및 도메인 컨트롤러와의 연결에 대해 기본적으로 설정되는 SMB 버전을 결정합니다. SMB 서버가 사용자 환경에 필요한 클라이언트 및 기능을 지원하는지 확인해야 합니다.

이 작업에 대해

클라이언트 및 도메인 컨트롤러 모두에 연결하는 경우 가능하면 SMB 2.0 이상을 활성화해야 합니다. 보안상의 이유로 SMB 1.0은 사용하지 않는 것이 좋습니다. 사용자 환경에서 필요하지 않은 것으로 확인된 경우에는 사용하지 않도록 설정해야 합니다.

ONTAP 9.3부터는 새 SVM에서 기본적으로 비활성화되어 있습니다.



SMB1-enabled-for-dc-connections가 false로 설정되어 있고 -SMB1-enabled가 true로 설정되어 있으면 ONTAP는 SMB 1.0 연결을 클라이언트로 거부하지만 인바운드 SMB 1.0 연결을 서버로 계속 허용합니다.

"**SMB 관리**" 지원되는 SMB 버전 및 기능에 대한 자세한 내용은 [여기](#) 나와 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

## 2. 활성화된 SMB 버전을 확인합니다.

```
vserver cifs options show
```

목록을 아래로 스크롤하여 클라이언트 연결에 대해 설정된 SMB 버전을 볼 수 있으며 AD 도메인 연결에 대해 AD 도메인에서 SMB 서버를 구성하는 경우

## 3. 필요에 따라 클라이언트 연결에 대해 SMB 프로토콜을 설정하거나 해제합니다.

### ◦ SMB 버전 활성화하기:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

에 사용할 수 있는 값 smb\_version:

- '-SMB1-활성화됨'
- '-SMB2-ENABLED'입니다
- '-SMB3-enabled'입니다
- -smb31-enabled

다음 명령을 실행하면 SVM vs1.example.com 에서 SMB 3.1이 활성화됩니다.

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
-enabled true
```

### ◦ SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

## 4. SMB 서버가 Active Directory 도메인에 있는 경우 필요에 따라 DC 연결에 대한 SMB 프로토콜을 설정하거나 해제합니다.

### ◦ SMB 버전 활성화하기:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

### ◦ SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

## ONTAP SMB 서버를 DNS 서버에 매핑합니다

Windows 사용자가 SMB 서버 이름에 드라이브를 매핑할 수 있도록 사이트의 DNS 서버에는 SMB 서버 이름 및 모든 NetBIOS 별칭을 가리키는 항목이 데이터 LIF의 IP 주소에 있어야 합니다.

시작하기 전에

사이트의 DNS 서버에 대한 관리 액세스 권한이 있어야 합니다. 관리 액세스 권한이 없는 경우 DNS 관리자에게 이 작업을 수행하도록 요청해야 합니다.

이 작업에 대해

SMB 서버 이름에 NetBIOS 별칭을 사용하는 경우 각 별칭에 대해 DNS 서버 진입점을 만드는 것이 좋습니다.

단계

1. DNS 서버에 로그인합니다.
2. 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 LIF의 IP 주소에 매핑합니다.
3. NetBIOS 별칭을 사용하는 경우 별칭 정규 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버 데이터 LIF의 IP 주소에 매핑합니다.

결과

매핑이 네트워크를 통해 전파되면 Windows 사용자는 드라이브를 SMB 서버 이름 또는 NetBIOS 별칭에 매핑할 수 있습니다.

## 공유 스토리지에 대한 SMB 클라이언트 액세스를 구성합니다

공유 **ONTAP** 스토리지에 대한 **SMB** 클라이언트 액세스를 구성합니다

SVM에서 공유 스토리지에 SMB 클라이언트가 액세스할 수 있도록 하려면 스토리지 컨테이너를 제공할 볼륨 또는 qtree를 생성한 다음 해당 컨테이너에 대한 공유를 생성하거나 수정해야 합니다. 그런 다음 공유 및 파일 권한을 구성하고 클라이언트 시스템에서 액세스를 테스트할 수 있습니다.

시작하기 전에

- SVM에서 SMB를 완전히 설정해야 합니다.
- 이름 서비스 구성에 대한 모든 업데이트를 완료해야 합니다.

- Active Directory 도메인 또는 작업 그룹 구성에 대한 추가 또는 수정 작업을 완료해야 합니다.

볼륨 또는 **qtree** 스토리지 컨테이너를 생성합니다

**ONTAP SMB** 볼륨을 생성합니다

볼륨을 생성하고 "volume create" 명령을 사용하여 해당 접합 지점 및 기타 속성을 지정할 수 있습니다.

이 작업에 대해

클라이언트에서 데이터를 사용할 수 있도록 하려면 볼륨에 `_junction path_`가 포함되어야 합니다. 새 볼륨을 생성할 때 접합 경로를 지정할 수 있습니다. 접합 경로를 지정하지 않고 볼륨을 생성하는 경우, "volume mount" 명령을 사용하여 SVM 네임스페이스에서 볼륨을 `_mount_`해야 합니다.

시작하기 전에

- SMB를 설정하고 실행해야 합니다.
- SVM 보안 스타일은 NTFS여야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "[파일 시스템 분석 설정](#)". 에 대한 자세한 내용은 `volume create` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

단계

1. 교차점으로 볼륨을 생성합니다. `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path`

'-junction-path'의 선택 항목은 다음과 같습니다.

- 루트 바로 아래, 예: `'/new_vol'`

새 볼륨을 생성하고 SVM 루트 볼륨에 직접 마운트하도록 지정할 수 있습니다.

- 기존 디렉토리 아래에 `'/existing_dir/new_vol'` 등이 있습니다

새 볼륨을 생성하고 기존 계층 구조에서 기존 볼륨에 마운트하도록 지정할 수 있습니다. 이 볼륨은 디렉토리로 표시됩니다.

새 볼륨 아래의 새 계층 구조에서 `"/new_dir/new_vol"`과 같은 새 디렉토리에 볼륨을 생성하려면 먼저 SVM 루트 볼륨에 대한 분기인 새 상위 볼륨을 생성해야 합니다. 그런 다음 새 상위 볼륨(새 디렉토리)의 접합 경로에 새 하위 볼륨을 생성합니다.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다. `volume show -vserver svm_name -volume volume_name -junction`

예

다음 명령을 실행하면 SVM `vs1.example.com` 및 애그리게이트 `aggr1`에 `user1`이라는 새 볼륨이 생성됩니다. 새

볼륨은 '/users'에서 사용할 수 있습니다. 볼륨의 크기는 750GB이고 볼륨 유형은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction

```

| Vserver         | Volume | Active | Junction Path | Junction Path Source |
|-----------------|--------|--------|---------------|----------------------|
| vs1.example.com | users1 | true   | /users        | RW_volume            |

다음 명령을 실행하면 SVM의 "'home4' vs1.example.com'"와 애그리게이트 "'aggr1'"에 새 볼륨이 생성됩니다. VS1 SVM은 이름 공간에 /ENG/ 디렉토리가 이미 있으며, '/ENG/' 네임스페이스의 홈 디렉토리가 되는 '/ENG/HOME'에서 새 볼륨을 사용할 수 있습니다. 볼륨 크기는 750GB이고 볼륨 보장은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

| Vserver         | Volume | Active | Junction Path | Junction Path Source |
|-----------------|--------|--------|---------------|----------------------|
| vs1.example.com | home4  | true   | /eng/home     | RW_volume            |

## ONTAP SMB qtree를 생성합니다

'volume qtree create' 명령을 사용하여 데이터를 포함하는 qtree를 생성하고 해당 속성을 지정할 수 있습니다.

시작하기 전에

- SVM과 새 qtree가 포함될 볼륨이 이미 존재해야 합니다.
- SVM 보안 스타일은 NTFS여야 하며 SMB를 설정하고 실행해야 합니다.

단계

1. qtree:'volume qtree create-vserver vserver\_name{-volume volume\_name-qtree qtree\_name|-qtree-path qtree path qtree path}-security-style NTFS'를 생성합니다

볼륨과 qtree를 별도의 인수로 지정하거나 qtree 경로 인수를 '/vol/volume\_name/\_qtree\_name' 형식으로 지정할 수 있습니다.

2. qtree가 'volume qtree show-vserver vserver\_name{-volume volume\_name-qtree qtree qtree\_name|-qtree-path qtree path}' 접합 경로로 생성되었는지 확인합니다

예

다음 예에서는 junction path '/vol/data1'이 있는 SVM vs1.example.com 에 qt01이라는 이름의 qtree를 생성합니다.

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

Vserver Name: vs1.example.com
Volume Name: data1
Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
Security Style: ntfs
Oplock Mode: enable
Unix Permissions: ---rwxr-xr-x
Qtree Id: 2
Qtree Status: normal
Export Policy: default
Is Export Policy Inherited: true
```

## ONTAP SMB 공유를 생성할 때의 요구 사항 및 고려 사항

SMB 공유를 생성하기 전에 공유 경로 및 공유 속성, 특히 홈 디렉토리에 대한 요구 사항을 이해해야 합니다.

SMB 공유를 생성하려면 클라이언트가 액세스할 디렉토리 경로 구조('vserver cifs share create' 명령의 '-path' 옵션 사용)를 지정해야 합니다. 디렉토리 경로는 SVM 네임스페이스에서 생성한 볼륨 또는 qtree의 접합 경로에 해당합니다. 공유를 생성하기 전에 디렉토리 경로 및 해당 접속 경로가 있어야 합니다.

공유 경로에는 다음과 같은 요구 사항이 있습니다.

- 디렉토리 경로 이름은 최대 255자까지 지정할 수 있습니다.
- 경로 이름에 공백이 있으면 전체 문자열을 따옴표로 묶어야 합니다(예: "/new volume/mount here").
- 공유의 UNC 경로("\\servername\sharename\filepath")에 256자 이상(UNC 경로의 초기 "\\\" 제외)이 포함되어 있으면 Windows 속성 상자의 \* Security \* 탭을 사용할 수 없습니다.

이것은 ONTAP 문제가 아니라 Windows 클라이언트 문제입니다. 이 문제를 방지하려면 256자를 초과하는 UNC 경로를 사용하여 공유를 생성하지 마십시오.

공유 속성 기본값은 다음과 같이 변경할 수 있습니다.

- 모든 주식의 기본 초기 속성은 oplocks, 탐색 가능, 변경 및 이전 버전 사용입니다.
- 공유를 생성할 때 공유 속성을 지정하는 것은 선택 사항입니다.

그러나 공유를 생성할 때 공유 속성을 지정하면 기본값이 사용되지 않습니다. 공유를 만들 때 '-share-properties'

매개 변수를 사용하는 경우 심표로 구분된 목록을 사용하여 공유에 적용할 모든 공유 속성을 지정해야 합니다.

- 홈 디렉토리 공유를 지정하려면 홈 디렉토리 속성을 사용합니다.

이 기능을 사용하면 연결된 사용자와 변수 집합을 기반으로 서로 다른 디렉토리에 매핑되는 공유를 구성할 수 있습니다. 사용자별로 별도의 공유를 생성할 필요 없이 몇 가지 홈 디렉토리 매개 변수를 사용하여 단일 공유를 구성하여 엔트리 포인트(공유)와 해당 홈 디렉토리(SVM의 디렉토리) 간의 사용자 관계를 정의할 수 있습니다.



공유를 생성한 후에는 이 속성을 추가하거나 제거할 수 없습니다.

홈 디렉토리 공유에는 다음과 같은 요구 사항이 있습니다.

- SMB 홈 디렉토리를 생성하기 전에 'vserver cifs home-directory search-path add' 명령을 사용하여 적어도 하나의 홈 디렉토리 검색 경로를 추가해야 합니다.
- '-share-properties' 파라미터의 homed디렉토리 값으로 지정된 홈 디렉토리 공유에는 공유 이름에 '%w'(Windows 사용자 이름) 동적 변수가 포함되어야 합니다.

공유 이름에는 "%d"(도메인 이름) 동적 변수(예: "%d/%w") 또는 공유 이름의 정적 부분(예: "home1\_%w")이 추가로 포함될 수 있습니다.

- 관리자 또는 사용자가 공유를 사용하여 다른 사용자의 홈 디렉토리에 연결하는 경우('vserver cifs home-directory modify' 명령 옵션 사용) 동적 공유 이름 패턴 앞에는 물결표('~')가 와야 합니다.

에 대한 자세한 내용은 `vserver cifs share` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

관련 정보

- ["SMB 관리"](#)

## ONTAP SMB 공유를 생성합니다

SMB 클라이언트와 SMB 서버의 데이터를 공유하려면 먼저 SMB 공유를 생성해야 합니다. 공유를 생성할 때 공유를 홈 디렉토리로 지정하는 등의 공유 속성을 설정할 수 있습니다. 선택적 설정을 구성하여 공유를 사용자 지정할 수도 있습니다.

시작하기 전에

공유를 생성하기 전에 SVM 네임스페이스에 볼륨 또는 qtree의 디렉토리 경로가 있어야 합니다.

이 작업에 대해

공유를 생성할 때 기본 공유 ACL(기본 공유 권한)은 '모든 사용자/모든 권한'입니다. 공유에 대한 액세스를 테스트한 후에는 기본 공유 ACL을 제거하고 보다 안전한 대체 공유 ACL로 대체해야 합니다.

단계

1. 필요한 경우 공유에 대한 디렉토리 경로 구조를 생성합니다.

'vserver cifs share create' 명령은 공유 생성 중에 '-path' 옵션에 지정된 경로를 확인합니다. 지정한 경로가 없으면 명령이 실패합니다.

2. 지정된 SVM과 연결된 SMB 공유 생성: "+ vserver cifs share create -vserver vserver\_name -share-name share\_name -path path [-share-properties share\_properties,...] [Other\_attributes] [-comment text]+"

3. 공유가 생성되었는지 확인합니다. "vserver cifs share show-share-name share\_name"

예

다음 명령을 실행하면 SVM vs1.example.com "sHARE1"이라는 SMB 공유가 생성됩니다. 디렉터리 경로는 '/users'이며 기본 속성으로 만들어집니다.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1
```

| Vserver         | Share  | Path   | Properties             | Comment | ACL             |
|-----------------|--------|--------|------------------------|---------|-----------------|
| vs1.example.com | SHARE1 | /users | oplocks                | -       | Everyone / Full |
| Control         |        |        | browsable              |         |                 |
|                 |        |        | changenotify           |         |                 |
|                 |        |        | show-previous-versions |         |                 |

#### ONTAP SMB 클라이언트 액세스를 확인합니다

공유에 데이터를 액세스 및 기록하여 SMB를 올바르게 구성했는지 확인해야 합니다. SMB 서버 이름 및 NetBIOS 별칭을 사용하여 액세스를 테스트해야 합니다.

단계

1. Windows 클라이언트에 로그인합니다.
2. SMB 서버 이름을 사용하여 액세스 테스트:
  - a. Windows 탐색기에서 드라이브를 공유 위치에 's.\smb\_Server\_Name\Share\_Name' 형식으로 매핑합니다  
  
매핑에 성공하지 못한 경우 DNS 매핑이 아직 네트워크 전체에 전파되지 않았을 수 있습니다. 나중에 SMB 서버 이름을 사용하여 액세스를 테스트해야 합니다.  
  
SMB 서버의 이름이 vs1.example.com 이고 공유 이름이 share1 인 경우 'n.\vs0.example.com\SHARE1' 을 입력해야 합니다
  - b. 새로 만든 드라이브에서 테스트 파일을 만든 다음 파일을 삭제합니다.  
  
SMB 서버 이름을 사용하여 공유에 대한 쓰기 액세스를 확인했습니다.
3. NetBIOS 별칭에 대해 2단계를 반복합니다.

#### ONTAP SMB 공유 액세스 제어 목록을 생성합니다

SMB 공유에 대한 ACL(액세스 제어 목록)을 생성하여 공유 권한을 구성하면 사용자 및 그룹의 공유에 대한 액세스 수준을 제어할 수 있습니다.

시작하기 전에



공유에 대한 액세스 권한을 부여할 사용자 또는 그룹을 결정해야 합니다.

이 작업에 대해

로컬 또는 도메인 Windows 사용자 또는 그룹 이름을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

새 ACL을 생성하기 전에 보안 위험을 야기시키는 기본 공유 ACL 'Everyone/Full Control'을 삭제해야 합니다.

워크그룹 모드에서 로컬 도메인 이름은 SMB 서버 이름입니다.

단계

1. 기본 공유 ACL: ``vserver cifs share access-control delete-vserver\_vserver\_name\_-share\_share\_name\_-user-or-group everyone"을 삭제합니다
2. 새 ACL 구성:

| 을 사용하여 <b>ACL</b> 을 구성하려면... | 명령 입력...                                                                                                                                                                 |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 사용자                  | 'vserver cifs share access-control create-vserver_name_-share_share_name_-user-group-type windows-user-or-group_windows_domain_name\\user_name_-permission access_right' |
| Windows 그룹                   | 'vserver cifs share access-control create-vserver_name_-share_share_name_-user-group-type windows-user-or-group_windows_group_name_-permission access_right'             |

3. 'vserver cifs share access-control show' 명령을 사용하여 공유에 적용된 ACL이 올바른지 확인하십시오.

예

다음 명령을 실행하면 vs1.example.com`"SVM: "Sales" 공유에 대한 "Sales Team" Windows 그룹에 대한 "Change" 권한이 부여됩니다

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
```

| Vserver         | Share Name | User/Group Name        | User/Group Type | Access Permission |
|-----------------|------------|------------------------|-----------------|-------------------|
| vs1.example.com | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs1.example.com | sales      | DOMAIN\"Sales Team"    | windows         | Change            |

다음 명령은 로컬 윈도우 그룹인 '타이거 팀'과 'Full\_Control'에 대한 'SUE Chang'이라는 이름의 변경 권한을 VS1 SVM의 'datavol5' 공유에 부여합니다.

```
cluster1::> vservers cifs share access-control create -vservers vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vservers cifs share access-control create -vservers vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vservers cifs share access-control show -vservers vs1
```

| Vserver      | Share    | User/Group             | User/Group | Access |
|--------------|----------|------------------------|------------|--------|
| Permission   | Name     | Name                   | Type       |        |
| vs1          | c\$      | BUILTIN\Administrators | windows    |        |
| Full_Control |          |                        |            |        |
| vs1          | datavol5 | DOMAIN\"Tiger Team"    | windows    | Change |
| vs1          | datavol5 | DOMAIN\"Sue Chang"     | windows    |        |
| Full_Control |          |                        |            |        |

## ONTAP SMB 공유에서 NTFS 파일 사용 권한을 구성합니다

공유에 대한 액세스 권한이 있는 사용자 또는 그룹에 대한 파일 액세스를 설정하려면 Windows 클라이언트에서 공유하는 파일 및 디렉토리에 대한 NTFS 파일 권한을 구성해야 합니다.

시작하기 전에

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

이 작업에 대해

["SMB 관리"](#) 및 Windows 설명서에는 표준 및 고급 NTFS 권한을 설정하는 방법에 대한 정보가 포함되어 있습니다.

단계

1. Windows 클라이언트에 관리자로 로그인합니다.
2. Windows 탐색기의 \* Tools \* 메뉴에서 \* Map network drive \* 를 선택합니다.
3. 네트워크 드라이브 매핑 \* 상자를 완료합니다.
  - a. 드라이브 \* 문자를 선택합니다.
  - b. 폴더 \* 상자에 사용 권한을 적용할 데이터와 공유 이름을 포함하는 공유가 포함된 SMB 서버 이름을 입력합니다.

SMB 서버 이름이 smb\_SERVER01이고 공유 이름이 "smb\_SERVER01"이면  
"\\smb\_SERVER01\share1"을 입력합니다.



SMB 서버 이름 대신 SMB 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.

4. NTFS 파일 권한을 설정할 파일 또는 디렉터리를 선택합니다.

5. 파일 또는 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 \* 속성 \* 을 선택합니다.

6. 보안 \* 탭을 선택합니다.

보안 탭에는 NTFS 권한이 설정된 사용자 및 그룹 목록이 표시됩니다. Object>에 대한 권한 상자에는 선택한 사용자 또는 그룹에 적용되는 허용 및 거부 권한 목록이 표시됩니다.

7. 편집 \* 을 클릭합니다.

Object> 사용 권한 상자가 열립니다.

8. 원하는 작업을 수행합니다.

| 원하는 경우                              | 다음을 수행합니다.                                                                                                                                                |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 새 사용자 또는 그룹에 대한 표준 NTFS 권한을 설정합니다   | <p>a. 추가 * 를 클릭합니다.</p> <p>사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 창이 열립니다.</p> <p>b. 선택할 개체 이름 입력 * 상자에 NTFS 권한을 추가할 사용자 또는 그룹의 이름을 입력합니다.</p> <p>c. 확인 * 을 클릭합니다.</p> |
| 사용자 또는 그룹에서 표준 NTFS 권한을 변경하거나 제거합니다 | 그룹 또는 사용자 이름 * 상자에서 변경하거나 제거할 사용자 또는 그룹을 선택합니다.                                                                                                           |

9. 원하는 작업을 수행합니다.

| 원하는 작업                                      | 다음을 수행합니다                                                                                   |
|---------------------------------------------|---------------------------------------------------------------------------------------------|
| 새 사용자 또는 기존 사용자 또는 그룹에 대해 표준 NTFS 권한을 설정합니다 | Object>*에 대한 권한 상자에서 선택한 사용자 또는 그룹에 대해 허용하거나 허용하지 않을 액세스 유형에 대해 * 허용 * 또는 * 거부 * 상자를 선택합니다. |
| 사용자 또는 그룹을 제거합니다                            | 제거 * 를 클릭합니다.                                                                               |



일부 또는 모든 표준 권한 상자를 선택할 수 없는 경우 상위 개체에서 사용 권한이 상속되기 때문입니다. 특수 권한 \* 상자는 선택할 수 없습니다. 이 옵션을 선택하면 선택한 사용자 또는 그룹에 대해 하나 이상의 세분화된 고급 권한이 설정되었음을 의미합니다.

10. 해당 개체에 대한 NTFS 권한을 추가, 제거 또는 편집한 후 \* 확인 \* 을 클릭합니다.

## ONTAP SMB 사용자 공유 액세스를 확인합니다

구성한 사용자가 SMB 공유 및 해당 공유에 포함된 파일에 액세스할 수 있는지 테스트해야 합니다.

단계

1. Windows 클라이언트에서 공유에 대한 액세스 권한이 있는 사용자 중 하나로 로그인합니다.
2. Windows 탐색기의 \* Tools \* 메뉴에서 \* Map network drive \* 를 선택합니다.
3. 네트워크 드라이브 매핑 \* 상자를 완료합니다.
  - a. 드라이브 \* 문자를 선택합니다.
  - b. 폴더 \* 상자에 사용자에게 제공할 공유 이름을 입력합니다.

SMB 서버 이름이 smb\_SERVER01이고 공유 이름이 "smb\_SERVER01"이면  
"\\smb\_SERVER01\share1"을 입력합니다.

- c. 마침 \* 을 클릭합니다.

선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

4. 테스트 파일을 만들고, 파일이 있는지 확인하고, 텍스트를 작성한 다음 테스트 파일을 제거합니다.

## CLI를 사용하여 SMB를 관리합니다

### ONTAP SMB에 대해 알아보십시오

SMB 프로토콜에서 ONTAP 파일 액세스 기능을 사용할 수 있습니다. CIFS 서버를 설정하고, 공유를 생성하고, Microsoft 서비스를 설정할 수 있습니다.



*smb*(서버 메시지 블록)는 CIFS(Common Internet File System) 프로토콜의 최신 방언을 의미합니다. ONTAP CLI(Command-Line Interface) 및 OnCommand 관리 툴에서도 *\_cifs\_*가 계속 표시됩니다.

### SMB 서버 지원

#### ONTAP SMB 서버 지원에 대해 알아보십시오

SMB 클라이언트가 클러스터의 파일에 액세스할 수 있도록 SVM(스토리지 가상 머신)에서 SMB 서버를 설정 및 구성할 수 있습니다.

- 클러스터의 각 데이터 SVM은 하나의 Active Directory 도메인에 정확히 바인딩할 수 있습니다.
- Data SVM을 동일한 도메인에 연결할 필요가 없습니다.
- 여러 SVM을 동일한 도메인에 바인딩할 수 있습니다.

SMB 서버를 생성하기 전에 데이터 제공을 위해 사용 중인 SVM 및 LIF를 구성해야 합니다. 데이터 네트워크가 편평하지 않은 경우 IPspace, 브로드캐스트 도메인 및 서브넷을 구성해야 할 수도 있습니다.

관련 정보

## "네트워크 관리"

### 서버 수정

## "시스템 관리"

지원되는 **ONTAP SMB** 버전 및 기능

SMB(Server Message Block)는 Microsoft Windows 클라이언트 및 서버에서 사용하는 원격 파일 공유 프로토콜입니다. 모든 SMB 버전이 지원됩니다. ONTAP SMB 서버가 사용자 환경에 필요한 클라이언트 및 기능을 지원하는지 확인해야 합니다.

ONTAP가 지원하는 SMB 클라이언트 및 도메인 컨트롤러에 대한 최신 정보는 [\\_Interoperability Matrix Tool\\_](#)에서 확인할 수 있습니다.

SMB 2.0 이상 버전은 ONTAP SMB 서버에 대해 기본적으로 활성화되어 있으며 필요에 따라 활성화하거나 비활성화할 수 있습니다. SMB 1.0은 필요에 따라 활성화 또는 비활성화할 수 있습니다.



도메인 컨트롤러에 대한 SMB 1.0 및 2.0 연결의 기본 설정은 ONTAP 버전에도 따라 다릅니다. 에 대한 자세한 내용은 `vserver cifs security modify` ["ONTAP 명령 참조입니다"](#)을 참조하십시오. SMB 1.0을 실행하는 기존 CIFS 서버가 있는 환경의 경우 보안 및 규정 준수 향상을 준비하기 위해 가능한 한 빨리 최신 SMB 버전으로 마이그레이션해야 합니다. 자세한 내용은 NetApp 담당자에게 문의하십시오.

다음 표에서는 각 SMB 버전에서 지원되는 SMB 기능을 보여 줍니다. 일부 SMB 기능은 기본적으로 활성화되어 있으며 일부는 추가 구성이 필요합니다.

| * 이 기능은 * 입니다          | * 지원 필요: * | * 는 다음 <b>SMB</b> 버전에 대해 <b>ONTAP 9</b> 에서 지원됩니다. * |       |
|------------------------|------------|-----------------------------------------------------|-------|
|                        |            | 3.0                                                 | 3.1.1 |
| 레거시 SMB 1.0 기능         |            | X                                                   | X     |
| 내구성이 뛰어난 핸들            |            | X                                                   | X     |
| 결합 작업                  |            | X                                                   | X     |
| 비동기 작업                 |            | X                                                   | X     |
| 읽기 및 쓰기 버퍼 크기가 증가되었습니다 |            | X                                                   | X     |
| 확장성 향상                 |            | X                                                   | X     |
| SMB 서명                 | X          | X                                                   | X     |

| * 이 기능은 * 입니다                           | * 지원 필요: * | * 는 다음 <b>SMB</b> 버전에 대해 <b>ONTAP 9</b> 에서 지원됩니다. * |   |
|-----------------------------------------|------------|-----------------------------------------------------|---|
| ADS(대체 데이터 스트림)<br>파일 형식입니다             | X          | X                                                   | X |
| Large MTU(ONTAP<br>9.7부터 기본적으로<br>활성화됨) | X          | X                                                   | X |
| oplocks 리스                              |            | X                                                   | X |
| 지속적으로 사용 가능한<br>공유                      | X          | X                                                   | X |
| 영구 핸들                                   |            | X                                                   | X |
| 증인                                      |            | X                                                   | X |
| SMB 암호화: AES-128-<br>CCM                | X          | X                                                   | X |
| 스케일아웃(CA 공유에<br>필요)                     |            | X                                                   | X |
| 투명한 페일오버                                |            | X                                                   | X |
| SMB 멀티 채널(ONTAP<br>9.4로 시작)             | X          | X                                                   | X |
| 사전 인증 무결성                               |            |                                                     | X |
| 클러스터 클라이언트<br>페일오버 v.2(CCFv2)           |            |                                                     | X |
| SMB 암호화: AES-128-<br>GCM                | X          |                                                     | X |

#### 관련 정보

[ONTAP 서명을 사용하여 네트워크 보안을 강화하는 방법에 대해 알아보세요.](#)

[서버 최소 인증 보안 수준 설정](#)

[SMB를 통한 데이터 전송을 위해 SMB 서버에서 필요한 SMB 암호화 구성](#)

["NetApp 상호 운용성"](#)

## ONTAP SMB에서 지원되지 않는 Windows 기능

네트워크에서 CIFS를 사용하기 전에 ONTAP에서 지원하지 않는 특정 Windows 기능을 알고 있어야 합니다.

ONTAP는 다음 Windows 기능을 지원하지 않습니다.

- 암호화된 파일 시스템(EFS)
- 변경 저널에서 NTFS(NT File System) 이벤트 로깅
- Microsoft FRS(파일 복제 서비스)
- Microsoft Windows 인덱싱 서비스
- HSM(Hierarchical Storage Management)을 통한 원격 스토리지
- Windows 클라이언트의 할당량 관리
- Windows 할당량 의미 체계입니다
- LMHOSTS 파일입니다
- NTFS 네이티브 압축

ONTAP SMB SVM에서 NIS 또는 LDAP 이름 서비스를 구성합니다

SMB 액세스를 사용하면 NTFS 보안 스타일 볼륨에서 데이터에 액세스할 때도 UNIX 사용자에게 대한 사용자 매핑이 항상 수행됩니다. 정보가 NIS 또는 LDAP 디렉토리 저장소에 저장되어 있는 해당 UNIX 사용자에게 Windows 사용자를 매핑하거나 이름 매핑에 LDAP를 사용하는 경우 SMB 설정 중에 이러한 이름 서비스를 구성해야 합니다.

시작하기 전에

네임 서비스 데이터베이스 구성을 네임 서비스 인프라에 맞게 사용자 지정해야 합니다.

이 작업에 대해

SVM은 이름 서비스 ns-switch 데이터베이스를 사용하여 지정된 이름 서비스 데이터베이스의 소스를 조회하는 순서를 결정합니다. ns 스위치 소스는, nis 또는 ldap 의 조합이 될 수 있습니다 files. 그룹 데이터베이스의 경우 ONTAP는 구성된 모든 소스에서 그룹 구성원 자격을 얻은 다음 통합된 그룹 구성원 정보를 사용하여 액세스 검사를 수행합니다. UNIX 그룹 정보를 가져올 때 이러한 소스 중 하나를 사용할 수 없는 경우 ONTAP에서 전체 UNIX 자격 증명을 가져올 수 없으며 이후의 액세스 검사에 실패할 수 있습니다. 따라서 항상 ns-switch 설정에서 그룹 데이터베이스에 대해 모든 ns-switch 소스가 구성되어 있는지 확인해야 합니다.

기본값은 SMB 서버가 모든 Windows 사용자를 로컬 'passwd' 데이터베이스에 저장된 기본 UNIX 사용자에게 매핑하도록 하는 것입니다. 기본 구성을 사용하려면 NIS 또는 LDAP UNIX 사용자 및 그룹 이름 서비스 구성 또는 LDAP 사용자 매핑은 SMB 액세스에 대해 선택 사항입니다.

단계

1. UNIX 사용자, 그룹 및 넷그룹 정보가 NIS 이름 서비스를 통해 관리되는 경우 NIS 이름 서비스를 구성합니다.
  - a. 'vserver services name-service ns-switch show' 명령을 사용하여 이름 서비스의 현재 순서를 확인합니다.

이 예에서는 NIS를 이름 서비스 소스로 사용할 수 있는 세 개의 데이터베이스(group, passwd, netgroup)가 파일(file)만 소스로 사용하고 있습니다.

'vserver services name-service ns-switch show-vserver vs1'

| Vserver | Database | Enabled | Source<br>Order |
|---------|----------|---------|-----------------|
| vs1     | hosts    | true    | dns,<br>files   |
| vs1     | group    | true    | files           |
| vs1     | passwd   | true    | files           |
| vs1     | netgroup | true    | files           |
| vs1     | namemap  | true    | files           |

그룹 및 암호 데이터베이스에 NIS 소스를 추가하고 선택적으로 넷그룹 데이터베이스에 추가해야 합니다.

- b. 'vserver services name-service ns-switch modify' 명령을 사용하여 이름 서비스 ns-switch 데이터베이스 순서를 원하는 대로 조정합니다.

최상의 성능을 위해 SVM에서 네임 서비스를 구성하려는 경우를 제외하고 네임 서비스 데이터베이스에 네임 서비스를 추가할 수 없습니다.

둘 이상의 이름 서비스 데이터베이스에 대한 구성을 수정하는 경우 수정할 각 이름 서비스 데이터베이스에 대해 명령을 별도로 실행해야 합니다.

이 예에서 NIS와 파일은 그룹 데이터베이스와 암호 데이터베이스의 소스로 구성됩니다. 나머지 이름 서비스 데이터베이스는 변경되지 않습니다.

```
'vserver services name-service ns-switch modify -vserver vs1 -database group -sources nis, files'
'vserver services name-service ns-switch modify -vserver vs1 -database passwd -sources nis, files'
```

- c. 'vserver services name-service ns-switch show' 명령을 사용하여 이름 서비스의 순서가 올바른지 확인합니다.

'vserver services name-service ns-switch show-vserver vs1'

| Vserver | Database | Enabled | Source<br>Order |
|---------|----------|---------|-----------------|
| vs1     | hosts    | true    | dns,<br>files   |
| vs1     | group    | true    | nis,<br>files   |
| vs1     | passwd   | true    | nis,<br>files   |
| vs1     | netgroup | true    | files           |
| vs1     | namemap  | true    | files           |

- d. NIS 이름 서비스 구성을 만듭니다



```
vserver services name-service nis-domain create -vserver <vserver_name>
-domain <NIS_domain_name> -servers <NIS_server_IPaddress>, ...

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```



1. 이 필드는 NIS 서버의 호스트 이름이나 IP 주소를 사용할 수 있습니다

e. NIS 이름 서비스가 올바르게 구성되어 있는지 확인합니다. `vserver services name-service nis-domain show vserver <vserver_name>`

'vserver services name-service nis-domain show vserver vs1'

| Vserver | Domain      | Server    |
|---------|-------------|-----------|
| vs1     | example.com | 10.0.0.60 |

2. UNIX 사용자, 그룹 및 넷그룹 정보 또는 이름 매핑이 LDAP 이름 서비스에 의해 관리되는 경우 찾은 정보를 사용하여 LDAP 이름 서비스를 구성합니다 ["NFS 관리"](#).

**ONTAP SMB** 이름 서비스 스위치 구성에 대해 자세히 알아보십시오

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다. 환경에 맞게 적절하게 구성할 수 있도록 표의 기능과 ONTAP에서 표의 사용 방법을 이해해야 합니다.

ONTAP 이름 서비스 스위치 테이블은 ONTAP가 특정 유형의 이름 서비스 정보에 대한 정보를 검색하기 위해 어떤 이름 서비스 소스를 참조합니다. ONTAP는 SVM별로 개별 네임 서비스 스위치 테이블을 유지 관리합니다.

데이터베이스 유형

이 테이블에는 다음과 같은 각 데이터베이스 유형에 대해 별도의 이름 서비스 목록이 저장됩니다.

| 데이터베이스 유형입니다 | 다음에 대한 이름 서비스 소스를 정의합니다. | 유효한 소스는...    |
|--------------|--------------------------|---------------|
| 호스트          | 호스트 이름을 IP 주소로 변환        | 파일, DNS       |
| 그룹           | 사용자 그룹 정보를 찾는 중입니다       | 파일, NIS, LDAP |
| 암호           | 사용자 정보를 찾는 중입니다          | 파일, NIS, LDAP |
| 넷그룹          | 넷그룹 정보를 찾는 중입니다          | 파일, NIS, LDAP |
| 이름맵          | 사용자 이름 매핑 중              | 파일, LDAP      |

## 소스 유형

소스는 해당 정보를 검색하는 데 사용할 이름 서비스 소스를 지정합니다.

| 원본 유형 지정... | 에서 정보를 조회하려면...                    | 관리 대상 명령 제품군...                                                                                      |
|-------------|------------------------------------|------------------------------------------------------------------------------------------------------|
| 파일          | 로컬 소스 파일                           | SVM 서비스 이름 서비스 유닉스 사용자 SVM 서비스 이름 서비스 유닉스 그룹<br><br>SVM 서비스 이름 서비스 넷그룹<br><br>SVM 서비스 이름-서비스 DNS 호스트 |
| NIS를 선택합니다  | SVM의 NIS 도메인 구성에 지정된 외부 NIS 서버     | 'vserver services name-service nis-domain'을 선택합니다                                                    |
| LDAP를 지원합니다 | SVM의 LDAP 클라이언트 구성에 지정된 외부 LDAP 서버 | 'vserver services name-service ldap'                                                                 |
| DNS         | SVM의 DNS 구성에 지정된 외부 DNS 서버         | SVM 서비스 이름-서비스 DNS                                                                                   |

데이터 액세스와 SVM 관리 인증 모두에 NIS 또는 LDAP를 사용하려는 경우에도 NIS 또는 LDAP 인증이 실패할 경우 "파일"을 포함하고 로컬 사용자를 대체 수단으로 구성해야 합니다.

외부 소스에 액세스하는 데 사용되는 프로토콜입니다

외부 소스의 서버에 액세스하기 위해 ONTAP는 다음 프로토콜을 사용합니다.

|                 |                   |
|-----------------|-------------------|
| 외부 이름 서비스 소스입니다 | 액세스에 사용되는 프로토콜입니다 |
| NIS를 선택합니다      | UDP입니다            |
| DNS             | UDP입니다            |
| LDAP를 지원합니다     | TCP               |

예

다음 예는 SVM의 VM\_1'에 대한 이름 서비스 스위치 구성을 표시합니다.

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

| Vserver | Database | Source        |
|---------|----------|---------------|
| -----   | -----    | -----         |
| svm_1   | hosts    | files,<br>dns |
| svm_1   | group    | files         |
| svm_1   | passwd   | files         |
| svm_1   | netgroup | nis,<br>files |

사용자 또는 그룹 정보를 조회하기 위해 ONTAP은 로컬 소스 파일만 참조합니다. 쿼리가 결과를 반환하지 않으면 조회가 실패합니다.

넷그룹 정보를 조회하기 위해 ONTAP은 먼저 외부 NIS 서버를 참조합니다. 쿼리가 결과를 반환하지 않으면 로컬 넷그룹 파일이 다음에 선택됩니다.

SVM svm\_1의 테이블에는 이름 매핑에 대한 이름 서비스 항목이 없습니다. 따라서 ONTAP은 기본적으로 로컬 소스 파일만 참조합니다.

## SMB 서버를 관리합니다

### ONTAP SMB 서버를 수정합니다

"vserver cifs modify" 명령을 사용하여 작업 그룹에서 Active Directory 도메인으로, 작업 그룹에서 다른 작업 그룹으로 또는 Active Directory 도메인에서 작업 그룹으로 SMB 서버를 이동할 수 있습니다.

이 작업에 대해

SMB 서버 이름 및 관리 상태와 같은 SMB 서버의 다른 속성을 수정할 수도 있습니다. 에 대한 자세한 내용은 vserver cifs modify ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

선택

- 작업 그룹에서 Active Directory 도메인으로 SMB 서버 이동:

- SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- 작업 그룹에서 Active Directory 도메인으로 SMB 서버를 이동합니다: 'vserver cifs modify -vserver\_vserver\_name\_-domain\_domain\_name\_'

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 'example'.com 도메인 내의 'ou=\_example\_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-uri' 매개 변수에 vserver cifs 명령을 포함하여 포함시키십시오.

- 작업 그룹에서 다른 작업 그룹으로 SMB 서버 이동:

- a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMB 서버의 워크그룹을 수정합니다. 'vserver cifs modify -vserver\_vserver\_name\_-workgroup\_new\_workgroup\_name\_'

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory 도메인에서 작업 그룹으로 SMB 서버 이동:

- a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMB 서버를 Active Directory 도메인에서 작업 그룹('vserver cifs modify -vserver\_vserver\_name\_-workgroup\_workgroup\_name\_')으로 이동합니다

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



워크그룹 모드로 전환하려면 모든 도메인 기반 기능을 사용하지 않도록 설정하고 지속적으로 사용 가능한 공유, 새도우 복제본 및 AES를 포함하여 시스템에서 해당 구성을 자동으로 제거해야 합니다. 그러나 "EXAMPLE.COM\UserName" 같은 도메인 구성 공유 ACL은 제대로 작동하지 않지만 ONTAP에서는 제거할 수 없습니다. 명령이 완료된 후 외부 툴을 사용하여 가능한 한 빨리 이러한 공유 ACL을 제거합니다. AES가 활성화된 경우 "example.com" 도메인에서 Windows 계정을 비활성화할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 입력하라는 메시지가 표시될 수 있습니다.

- 'vserver cifs modify' 명령의 적절한 매개 변수를 사용하여 다른 속성을 수정합니다.

옵션을 사용하여 **SMB** 서버를 사용자 지정합니다

사용 가능한 **ONTAP 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. ONTAP은 `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 `false`입니다.

- \* 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 새도우 복제본 기능 활성화 또는 비활성화 \*

ONTAP는 새도우 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

- \* 새도 복사본 디렉토리 수준 구성 \*

이 옵션을 구성하면 새도우 복제본 기능을 사용할 때 새도우 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 사용자에게 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 ONTAP은 UNIX 보안 기능이 있는 볼륨의 파일 및 폴더를 NTFS ACL을 사용한 NTFS 파일 보안으로 SMB 클라이언트에 제공합니다. 사용하지 않도록 설정하면 ONTAP은 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. ONTAP은 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.

#### ONTAP SMB 서버 옵션을 구성합니다

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<br>b. 'vserver cifs options modify -vserver_vserver_name options_'<br>c. 'Set-Privilege admin'입니다 |

SMB 서버 옵션에 대한 자세한 vserver cifs options modify 내용은 ["ONTAP 명령 참조입니다"](#) 참조하십시오.

#### ONTAP 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 사용자에게 대한 **ONTAP SMB** 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 사용자에게 대한 액세스를 제어할 수 있습니다.

| 값        | 설명                             |
|----------|--------------------------------|
| 무제한(기본값) | 익명 사용자에게 대한 액세스 제한을 지정하지 않습니다. |
| 번호 매기기   | 익명 사용자에게 대해서만 열거를 제한하도록 지정합니다. |
| "접근 불가"  | 익명 사용자에게 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 서버 옵션](#)

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

**UNIX** 보안 스타일 데이터를 위해 **SMB** 클라이언트에 **ONTAP** 파일 보안을 제공하는 방법에 대해 알아보십시오

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 스타일을 구성합니다](#)
- [Qtree에서 보안 스타일 구성](#)

**UNIX** 보안 스타일 데이터의 경우 **ONTAP SMB** 클라이언트에 **NTFS ACL** 표시를 구성합니다

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

**ONTAP SMB FlexVol** 볼륨에 대한 **UNIX** 사용 권한을 유지하는 방법에 대해 알아봅니다

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.

**ONTAP SMB 서버의 Windows 보안 탭을 사용하여 UNIX 권한을 관리하는 방법에 대해 알아봅니다**

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.

**SMB 서버 보안 설정을 관리합니다**

**ONTAP SMB 클라이언트 인증 처리에 대해 알아봅니다**

사용자가 SVM에 포함된 데이터에 액세스하기 위해 SMB 연결을 생성하려면 먼저 SMB 서버가 속해 있는 도메인에서 인증을 받아야 합니다. SMB 서버는 Kerberos와 NTLM(NTLMv1 또는 NTLMv2)의 두 가지 인증 방법을 지원합니다. Kerberos는 도메인 사용자를 인증하는 데 사용되는 기본 방법입니다.

**Kerberos 인증**

ONTAP는 인증된 SMB 세션을 생성할 때 Kerberos 인증을 지원합니다.

Kerberos는 Active Directory의 기본 인증 서비스입니다. Kerberos 서버 또는 Kerberos KDC(Key Distribution Center) 서비스는 Active Directory에 보안 원칙에 대한 정보를 저장하고 검색합니다. NTLM 모델과 달리 SMB 서버와

같은 다른 컴퓨터와 세션을 설정하려는 Active Directory 클라이언트는 KDC에 직접 문의하여 세션 자격 증명을 얻습니다.

**NTLM 인증**

NTLM 클라이언트 인증은 암호를 기반으로 사용자별 비밀번호에 대한 공유 지식을 기반으로 하는 본인 확인 응답 프로토콜을 사용하여 수행됩니다.

사용자가 로컬 Windows 사용자 계정을 사용하여 SMB 연결을 만들면 NTLMv2를 사용하여 SMB 서버에서 로컬로 인증이 수행됩니다.

**ONTAP SVM** 재해 복구 구성을 위한 **SMB** 서버 보안 설정에 대해 알아보십시오

ID가 보존되지 않는 재해 복구 대상으로 구성된 SVM(SnapMirror 구성에서 'identity-preserve' 옵션이 'false'로 설정됨)을 생성하기 전에 SVM 대상에서 SMB 서버 보안 설정이 관리되는 방식을 알아야 합니다.

- 기본이 아닌 SMB 서버 보안 설정은 대상에 복제되지 않습니다.

대상 SVM에서 SMB 서버를 생성할 때 모든 SMB 서버 보안 설정이 기본값으로 설정됩니다. SVM 재해 복구 대상이 초기화, 업데이트 또는 재동기화되면 소스의 SMB 서버 보안 설정이 타겟으로 복제되지 않습니다.

- 기본이 아닌 SMB 서버 보안 설정을 수동으로 구성해야 합니다.

소스 SVM에 기본값이 아닌 SMB 서버 보안 설정이 구성되어 있는 경우 SnapMirror 관계가 깨진 후, 대상이 읽기-쓰기 상태가 되면 대상 SVM에서 동일한 설정을 수동으로 구성해야 합니다.

**ONTAP SMB** 서버 보안 설정에 대한 정보를 표시합니다

SMB 서버 보안 설정에 대한 정보를 SVM(스토리지 가상 머신)에 표시할 수 있습니다. 이 정보를 사용하여 보안 설정이 올바른지 확인할 수 있습니다.

이 작업에 대해

표시된 보안 설정은 해당 개체의 기본값이거나 ONTAP CLI를 사용하거나 Active Directory 그룹 정책 개체(GPO)를 사용하여 구성된 기본값이 아닌 값일 수 있습니다.

일부 옵션이 유효하지 않으므로 워크그룹 모드에서 SMB 서버에 대해 "vserver cifs security show" 명령을 사용하지 마십시오.

단계

1. 다음 작업 중 하나를 수행합니다.

| 에 대한 정보를 표시하려면...   | 명령 입력...                                                                                                                 |
|---------------------|--------------------------------------------------------------------------------------------------------------------------|
| 지정된 SVM의 모든 보안 설정   | 'vserver cifs security show -vserver_vserver_name_'                                                                      |
| SVM의 특정 보안 설정 또는 설정 | 'vserver cifs security show -vserver_vserver_name_- 필드 [fieldname,...]'를 입력하면 '-fields?'를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다. |

예

다음 예는 SVM VS1 보안 설정을 모두 보여줍니다.

```
cluster1::> vservers cifs security show -vservers vs1

Vserver: vs1

Kerberos Clock Skew: 5 minutes
Kerberos Ticket Age: 10 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
Client Session Security: none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

표시되는 설정은 실행 중인 ONTAP 버전에 따라 다릅니다.

다음 예에서는 SVM VS1 Kerberos 클럭 편차를 보여 줍니다.

```
cluster1::> vservers cifs security show -vservers vs1 -fields kerberos-
clock-skew

vserver kerberos-clock-skew

vs1 5
```

## 관련 정보

[GPO 구성에 대한 정보를 표시합니다](#)

로컬 **SMB** 사용자에게 대한 **ONTAP** 암호 복잡성을 구성합니다

필수 비밀번호 복잡성은 스토리지 가상 시스템(SVM)의 로컬 SMB 사용자를 위해 향상된 보안을 제공합니다. 필요한 암호 복잡성 기능은 기본적으로 활성화되어 있습니다. 이 기능을 사용하지

않도록 설정하고 언제든지 다시 사용하도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버에서 로컬 사용자, 로컬 그룹 및 로컬 사용자 인증을 설정해야 합니다.



이 작업에 대해

일부 옵션이 유효하지 않으므로 작업 그룹 모드에서 CIFS 서버에 대한 명령을 사용하지 마십시오  
`vserver cifs security modify`.

단계

1. 다음 작업 중 하나를 수행합니다.

| 로컬 <b>SMB</b> 사용자에게 대한 암호 복잡성에 필요한 경우... | 명령 입력...                                                                                                          |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 활성화됨                                     | <code>'vserver cifs security modify<br/>-vserver_vserver_name_-is-password-Complexity<br/>-required true'</code>  |
| 사용 안 함                                   | <code>'vserver cifs security modify<br/>-vserver_vserver_name_-is-password-Complexity<br/>-required false'</code> |

2. 필요한 암호 복잡성에 대한 보안 설정을 확인합니다. `'vserver cifs security show -vserver_vserver_name_'`

예

다음 예에서는 SVM VS1 용 로컬 SMB 사용자에게 대해 필요한 암호 복잡성이 활성화된 것을 보여 줍니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required

vs1 true
```

관련 정보

- [서버 보안 설정에 대한 정보 표시](#)
- [로컬 사용자 및 그룹에 대해 알아보세요](#)
- [로컬 사용자 암호 요구 사항](#)
- [로컬 사용자 계정 암호를 변경합니다](#)

ONTAP SMB 서버 Kerberos 보안 설정을 수정합니다

허용되는 최대 Kerberos 클록 비뿔어짐 시간, Kerberos 티켓 수명 및 티켓 갱신 최대 일 수를

비롯한 특정 CIFS 서버 Kerberos 보안 설정을 수정할 수 있습니다.

이 작업에 대해

'vserver cifs security modify' 명령을 사용하여 CIFS 서버 Kerberos 설정을 수정하면 '-vserver' 매개 변수로 지정한 단일 SVM(스토리지 가상 머신)에서만 설정이 수정됩니다. Active Directory 그룹 정책 개체(GPO)를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM에 대한 Kerberos 보안 설정을 중앙에서 관리할 수 있습니다.

단계

1. 다음 작업 중 하나 이상을 수행합니다.

| 원하는 작업                                                          | 입력...                                                                                                                              |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 허용되는 최대 Kerberos 클럭 편중 시간을 분(9.13.1 이상) 또는 초(9.12.1 이하)로 지정합니다. | <code>'vserver cifs security modify -vserver_vserver_name_-Kerberos-clock -suts_integer_in_minutes_'</code><br><br>기본 설정은 5분입니다.   |
| Kerberos 티켓 수명(시간)을 지정합니다.                                      | <code>'vserver cifs security modify -vserver_vserver_name_-Kerberos-티켓-age integer_in_hours'</code> 를 선택합니다<br><br>기본 설정은 10시간입니다. |
| 티켓 갱신 최대 일 수를 지정하십시오.                                           | <code>'vserver cifs security modify -vserver_vserver_name_- Kerberos - renew - age_integer_in_days _'</code><br><br>기본 설정은 7일입니다.  |
| 모든 KDC가 도달할 수 없음으로 표시되는 KDC의 소켓에 대한 시간 제한을 지정합니다.               | <code>'vserver cifs security modify -vserver_vserver_name_-Kerberos-KDC -timeout_integer_in_seconds _'</code><br><br>기본 설정은 3초입니다. |

2. Kerberos 보안 설정을 확인합니다.

```
'vserver cifs security show -vserver_vserver_name_'
```

예

다음 예에서는 Kerberos 보안을 다음과 같이 변경합니다. ""Kerberos Clock Skew""는 3분으로 설정되고 ""Kerberos Ticket Age""는 SVM VS1 v1의 경우 8시간으로 설정됩니다.



```
cluster1::> vservice cifs security modify -vservice vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vservice cifs security show -vservice vs1

Vservice: vs1

 Kerberos Clock Skew: 3 minutes
 Kerberos Ticket Age: 8 hours
 Kerberos Renewal Age: 7 days
 Kerberos KDC Timeout: 3 seconds
 Is Signing Required: false
 Is Password Complexity Required: true
 Use start_tls For AD LDAP connection: false
 Is AES Encryption Enabled: false
 LM Compatibility Level: lm-ntlm-ntlmv2-krb
 Is SMB Encryption Required: false
```

#### 관련 정보

"서버 보안 설정에 대한 정보 표시"

"지원되는 GPO"

"CIFS 서버에 그룹 정책 객체 적용"

**ONTAP SMB** 서버 최소 인증 보안 수준을 설정합니다

SMB 클라이언트 액세스에 대한 비즈니스 보안 요구 사항을 충족하도록 SMB 서버에서 `_LMCompatibilityLevel_` 이라고도 하는 SMB 서버 최소 보안 수준을 설정할 수 있습니다. 최소 보안 수준은 SMB 서버가 SMB 클라이언트에서 허용하는 최소 보안 토큰입니다.



이 작업에 대해

- 워크그룹 모드의 SMB 서버는 NTLM 인증만 지원합니다. Kerberos 인증은 지원되지 않습니다.
- `LMCompatibilityLevel` 관리자 인증이 아닌 SMB 클라이언트 인증에만 적용됩니다.

최소 인증 보안 수준을 지원하는 네 가지 보안 수준 중 하나로 설정할 수 있습니다.

| 값                       | 설명                                                            |
|-------------------------|---------------------------------------------------------------|
| lm-NTLM-NTLMv2-KRB(기본값) | SVM(스토리지 가상 시스템)은 LM, NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다.   |
| NTLM-NTLMv2-KRB         | SVM은 NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 인증을 거부합니다. |

| 값          | 설명                                                             |
|------------|----------------------------------------------------------------|
| NTLMv2-KRB | SVM은 NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 및 NTLM 인증을 거부합니다. |
| KRB        | SVM은 Kerberos 인증 보안만 수락합니다. SVM은 LM, NTLM 및 NTLMv2 인증을 거부합니다.  |

#### 단계

1. 최소 인증 보안 수준을 설정합니다. 'vserver cifs security modify -vserver\_vserver\_name\_-lm -compatibility -level{lm-NTLM-NTLMv2-KRB | NTLM-NTLMv2-KRB | NTLMv2-KRB | KRB | KRB}'
2. 인증 보안 수준이 원하는 수준('vserver cifs security show -vserver\_vserver\_name\_')으로 설정되어 있는지 확인합니다

#### 관련 정보

#### Kerberos 기반 통신을 위한 AES 암호화 구성

AES 암호화를 사용하여 **Kerberos** 기반 통신을 위한 강력한 **ONTAP SMB** 보안을 구성합니다

Kerberos 기반 통신을 사용하여 보안을 강화하기 위해 SMB 서버에서 AES-256 및 AES-128 암호화를 활성화할 수 있습니다. 기본적으로 SVM에서 SMB 서버를 생성할 때 AES(고급 암호화 표준) 암호화가 사용되지 않습니다. AES 암호화로 제공되는 강력한 보안을 활용하려면 이 기능을 활성화해야 합니다.

SMB를 위한 Kerberos 관련 통신은 SVM에서 SMB 서버를 생성하는 동안이나 SMB 세션 설정 단계에서 사용됩니다. SMB 서버는 Kerberos 통신을 위해 다음과 같은 암호화 유형을 지원합니다.

- AES 256
- AES 128
- DES
- RC4-HMAC

Kerberos 통신에 가장 높은 보안 암호화 유형을 사용하려면 SVM에서 Kerberos 통신에 AES 암호화를 사용하도록 설정해야 합니다.

SMB 서버가 생성되면 도메인 컨트롤러는 Active Directory에 컴퓨터 시스템 계정을 만듭니다. 이때 KDC는 특정 컴퓨터 계정의 암호화 기능을 인식합니다. 그런 다음 인증 중에 클라이언트가 서버에 제공하는 서비스 티켓을 암호화하기 위해 특정 암호화 유형을 선택합니다.

ONTAP 9.12.1부터 Active Directory(AD) KDC에 알릴 암호화 유형을 지정할 수 있습니다. 이 옵션을 사용하여 권장 암호화 유형을 활성화할 수 -advertised-enc-types 있으며 이 옵션을 사용하여 약한 암호화 유형을 비활성화할 수 있습니다. 이 방법을 "[Kerberos 기반 통신을 위한 AES 암호화 구성](#)"알아보십시오.



인텔 AES 새 명령어(인텔 AES NI)는 SMB 3.0에서 사용할 수 있으며, AES 알고리즘을 개선하고 지원되는 프로세서 제품군에서 데이터 암호화를 가속화합니다. SMB 3.1.1부터 AES-128-GCM은 SMB 암호화에 사용되는 해시 알고리즘으로 AES-128-CCM을 대체합니다.

#### 관련 정보

**ONTAP SMB Kerberos** 기반 통신에 대해 **AES** 암호화를 구성합니다

Kerberos 기반 통신에서 가장 강력한 보안을 활용하려면 SMB 서버에서 AES-256 및 AES-128 암호화를 사용해야 합니다. ONTAP 9.13.1부터 AES 암호화는 기본적으로 사용하도록 설정됩니다. SMB 서버가 AD(Active Directory) KDC와 Kerberos 기반 통신을 위해 AES 암호화 유형을 선택하지 않도록 하려면 AES 암호화를 사용하지 않도록 설정할 수 있습니다.

AES 암호화가 기본적으로 사용되는지 여부와 암호화 유형을 지정하는 옵션이 있는지 여부는 ONTAP 버전에 따라 다릅니다.

| ONTAP 버전입니다 | AES 암호화 사용... | 암호화 유형을 지정할 수 있습니까? |
|-------------|---------------|---------------------|
| 9.13.1 이상   | 기본적으로 사용됩니다   | 예                   |
| 9.12.1      | 수동            | 예                   |
| 9.11.1 이하   | 수동            | 아니요                 |

ONTAP 9.12.1부터 AES 암호화는 `el` 사용하여 활성화 및 비활성화됩니다 `-advertised-enc-types` 옵션: AD KDC에 보급된 암호화 유형을 지정할 수 있습니다. 기본 설정은 `rc4` 및 `des` 그러나 AES 유형이 지정되면 AES 암호화가 활성화됩니다. 이 옵션을 사용하여 약한 RC4 및 DES 암호화 유형을 명시적으로 비활성화할 수도 있습니다. ONTAP 9.11.1 이하 버전에서는 `el` 사용해야 합니다 `-is-aes-encryption-enabled` AES 암호화를 활성화 및 비활성화하는 옵션과 암호화 유형을 지정할 수 없습니다.

보안을 강화하기 위해 SVM(Storage Virtual Machine)은 AES 보안 옵션을 수정할 때마다 AD에서 시스템 계정 암호를 변경합니다. 암호를 변경하려면 컴퓨터 계정이 포함된 OU(조직 구성 단위)에 대한 관리 AD 자격 증명이 필요할 수 있습니다.

SVM이 ID가 보존되지 않는 재해 복구 대상으로 구성된 경우( `-identity-preserve` 옵션이 `ro` 설정되어 있습니다 `false` SnapMirror 구성에서 기본 SMB 서버가 아닌 보안 설정은 대상에 복제되지 않습니다. 소스 SVM에서 AES 암호화를 사용하도록 설정한 경우 수동으로 활성화해야 합니다.

## 예 1. 단계

### ONTAP 9.12.1 이상

1. 다음 작업 중 하나를 수행합니다.

| Kerberos 통신을 위한 AES 암호화 유형을 원하는 경우... | 명령 입력...                                                                                             |
|---------------------------------------|------------------------------------------------------------------------------------------------------|
| 활성화됨                                  | <pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre> |
| 사용 안 함                                | <pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>         |

◦ 참고: \* -is-aes-encryption-enabled 옵션은 ONTAP 9.12.1에서 사용되지 않으며 이후 릴리스에서 제거될 수 있습니다.

2. AES 암호화가 필요에 따라 활성화 또는 비활성화되었는지 확인합니다. `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

### 예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver advertised-enc-types

vs1 aes-128,aes-256
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vsserver cifs security modify -vsserver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsserver cifs security show -vsserver vs2 -fields advertised-
enc-types
```

```
vsserver advertised-enc-types
----- -
vs2 aes-128,aes-256
```

#### ONTAP 9.11.1 이전 버전

1. 다음 작업 중 하나를 수행합니다.

| Kerberos 통신을 위한 AES 암호화 유형을 원하는 경우... | 명령 입력...                                                                                 |
|---------------------------------------|------------------------------------------------------------------------------------------|
| 활성화됨                                  | 'vsserver cifs security modify -vsserver vsserver_name -is-aes-encryption-enabled true'  |
| 사용 안 함                                | 'vsserver cifs security modify -vsserver vsserver_name -is-aes-encryption-enabled false' |

2. AES 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vsserver cifs security show -vsserver vsserver\_name -fields is -aes-encryption-enabled'

AES 암호화가 활성화된 경우 is-aes-encryption-enabled 필드가 true로 표시되고, 비활성화된 경우 false로 표시됩니다.

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vsriver cifs security modify -vsriver vs1 -is-aes
-encryption-enabled true

cluster1::> vsriver cifs security show -vsriver vs1 -fields is-aes-
encryption-enabled

vsriver is-aes-encryption-enabled

vs1 true
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vsriver cifs security modify -vsriver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vsriver cifs security show -vsriver vs2 -fields is-aes-
encryption-enabled

vsriver is-aes-encryption-enabled

vs2 true
```

#### 관련 정보

"도메인 사용자가 Domain-Tunnel을 사용하여 클러스터에 로그인하지 못했습니다"

**SMB** 서명을 사용하여 네트워크 보안을 강화합니다

**ONTAP SMB** 서명을 사용하여 네트워크 보안을 향상시키는 방법에 대해 알아보십시오

SMB 서명을 사용하면 SMB 서버와 클라이언트 사이의 네트워크 트래픽이 손상되지 않도록 할 수 있으며, 재생 공격을 차단하여 이 작업을 수행합니다. 기본적으로 ONTAP는 클라이언트가 요청할 때 SMB 서명을 지원합니다. 필요에 따라 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버를 구성할 수 있습니다.

서명 정책이 **ONTAP SMB** 서버와의 통신에 어떤 영향을 미치는지 알아봅니다

CIFS 서버 SMB 서명 보안 설정 외에도 Windows 클라이언트의 두 SMB 서명 정책은 클라이언트와 CIFS 서버 간의 디지털 통신 서명을 제어합니다. 비즈니스 요구 사항에 맞게 설정을 구성할 수 있습니다.

클라이언트 SMB 정책은 MMC(Microsoft Management Console) 또는 Active Directory GPO를 사용하여 구성되는 Windows 로컬 보안 정책 설정을 통해 제어됩니다. 클라이언트 SMB 서명 및 보안 문제에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

다음은 Microsoft 클라이언트에 대한 두 가지 SMB 서명 정책에 대한 설명입니다.

- 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)'

이 설정은 클라이언트의 SMB 서명 기능이 설정되었는지 여부를 제어합니다. 기본적으로 활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 CIFS 서버와의 클라이언트 통신은 CIFS 서버의 SMB 서명 설정에 따라 달라집니다.

- 마이크로네트워크 클라이언트: 디지털 서명 통신(항상)

이 설정은 클라이언트가 서버와 통신하기 위해 SMB 서명을 필요로 하는지 제어합니다. 기본적으로 비활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 SMB 서명 동작은 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)' 및 CIFS 서버의 설정에 대한 정책 설정을 기반으로 합니다.



환경에 SMB 서명이 필요하도록 구성된 Windows 클라이언트가 포함된 경우 CIFS 서버에서 SMB 서명을 설정해야 합니다. 그렇지 않으면 CIFS 서버가 이러한 시스템에 데이터를 제공할 수 없습니다.

클라이언트 및 CIFS 서버 SMB 서명 설정의 효과적인 결과는 SMB 세션이 SMB 1.0 또는 SMB 2.x 이상을 사용하는지 여부에 따라 달라집니다.

다음 표에는 세션이 SMB 1.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.

| 클라이언트                  | ONTAP — 서명이 필요하지 않습니다 | ONTAP — 서명이 필요합니다 |
|------------------------|-----------------------|-------------------|
| 서명이 비활성화되었으며 필요하지 않습니다 | 서명되지 않았습니다            | 서명됨               |
| 서명이 활성화되었으며 필요하지 않습니다  | 서명되지 않았습니다            | 서명됨               |
| 서명이 비활성화되었으며 필수입니다     | 서명됨                   | 서명됨               |
| 서명이 설정되어 있어야 합니다       | 서명됨                   | 서명됨               |



클라이언트에서 서명이 비활성화되었지만 CIFS 서버에서 필요한 경우 이전 Windows SMB 1 클라이언트와 일부 비 Windows SMB 1 클라이언트가 연결되지 않을 수 있습니다.

다음 표에는 세션에서 SMB 2.x 또는 SMB 3.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.



SMB 2.x 및 SMB 3.0 클라이언트의 경우 SMB 서명이 항상 사용하도록 설정됩니다. 비활성화할 수 없습니다.

| 클라이언트         | ONTAP — 서명이 필요하지 않습니다 | ONTAP — 서명이 필요합니다 |
|---------------|-----------------------|-------------------|
| 서명이 필요하지 않습니다 | 서명되지 않았습니다            | 서명됨               |
| 서명이 필요합니다     | 서명됨                   | 서명됨               |

다음 표에는 기본 Microsoft 클라이언트 및 서버 SMB 서명 동작이 요약되어 있습니다.

| 프로토콜    | 해시 알고리즘입니다   | 활성화/비활성화할 수 있습니다 | 필요/필요하지 않습니다 | 클라이언트 기본값입니다  | 서버 기본값        | DC 기본값   |
|---------|--------------|------------------|--------------|---------------|---------------|----------|
| SMB 1.0 | MD5          | 예                | 예            | 활성화됨(필요하지 않음) | 사용 안 함(필수 아님) | 필수 요소입니다 |
| SMB 2.x | HMAC SHA-256 | 아니요              | 예            | 필요하지 않습니다     | 필요하지 않습니다     | 필수 요소입니다 |
| SMB 3.0 | AES-CMAC     | 아니요              | 예            | 필요하지 않습니다     | 필요하지 않습니다     | 필수 요소입니다 |



Microsoft는 더 이상 '고유 서명 통신(클라이언트에서 동의한 경우)' 또는 '고유 서명 통신(서버에서 동의한 경우)' 그룹 정책 설정을 사용할 것을 권장하지 않습니다. Microsoft는 또한 "EnableSecuritySignature" 레지스트리 설정을 더 이상 사용하지 않을 것을 권장합니다. 이러한 옵션은 SMB 1 동작에만 영향을 미치며 Digitally sign communications (Always)(항상 서명 통신) 그룹 정책 설정 또는 RequireSecuritySignature(요구 보안 서명) 레지스트리 설정으로 대체할 수 있습니다. 또한 Microsoft 블로그에서 자세한 정보를 얻을 수 있습니다. [The SMB 서명의 기본 사항\(SMB1 및 SMB2 모두 포함\)](#)

## ONTAP SMB 서명의 성능 영향에 대해 알아보십시오

SMB 세션에서 SMB 서명을 사용하면 Windows 클라이언트와 주고 받는 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드) 모두에 영향을 미칩니다.

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 서명된 SMB 트래픽의 성능을 향상시킬 수 있습니다. SMB 서명 오프로드는 SMB 서명이 설정된 경우 기본적으로 설정됩니다.

향상된 SMB 서명 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.



훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 서명의 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경에서 테스트를 통해서만 확인할 수 있습니다.

대부분의 Windows 클라이언트는 서버에서 SMB 서명을 사용하는 경우 기본적으로 협상합니다. 일부 Windows 클라이언트에 대해 SMB 보호가 필요하고 SMB 서명으로 인해 성능 문제가 발생하는 경우 재생 공격에 대한 보호가 필요하지 않은 Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정할 수 있습니다. Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

## ONTAP SMB 서명 구성 권장 사항

SMB 클라이언트와 CIFS 서버 간에 SMB 서명 동작을 구성하여 보안 요구 사항을 충족할 수 있습니다. CIFS 서버에서 SMB 서명을 구성할 때 선택하는 설정은 보안 요구 사항에 따라 다릅니다.

클라이언트 또는 CIFS 서버에서 SMB 서명을 구성할 수 있습니다. SMB 서명을 구성할 때 다음 권장 사항을 고려하십시오.

| 만약...                                      | 권장 사항...                                                                      |
|--------------------------------------------|-------------------------------------------------------------------------------|
| 클라이언트와 서버 간의 통신 보안을 강화하려는 경우               | 클라이언트에서 'Require Option(Sign Always)' 보안 설정을 활성화하여 클라이언트에서 SMB 서명이 필요하도록 합니다. |
| 모든 SMB 트래픽이 특정 SVM(스토리지 가상 머신)에 서명하기를 원합니다 | SMB 서명이 필요하도록 보안 설정을 구성하여 CIFS 서버에 SMB 서명이 필요합니다.                             |

Windows 클라이언트 보안 설정 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

여러 데이터 LIF에 대한 ONTAP SMB 서명 구성에 대해 자세히 알아보십시오

SMB 서버에서 필요한 SMB 서명을 설정하거나 해제하는 경우 SVM에 대한 여러 데이터 LIF 구성에 대한 지침을 숙지해야 합니다.

SMB 서버를 구성할 때 여러 데이터 LIF가 구성되어 있을 수 있습니다. 이 경우 DNS 서버에 동일한 SMB 서버 호스트 이름을 사용하는 CIFS 서버에 대한 여러 개의 "A" 레코드 항목이 포함되어 있고 각 항목은 고유한 IP 주소를 사용합니다. 예를 들어, 두 개의 데이터 LIF가 구성된 SMB 서버의 DNS 'A' 레코드 항목은 다음과 같습니다.

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

일반적으로 필요한 SMB 서명 설정을 변경하면 클라이언트의 새 연결만 SMB 서명 설정의 변경 사항에 영향을 받습니다. 그러나 이 동작에 대한 예외는 있습니다. 클라이언트가 공유에 대한 기존 연결을 가지고 있고, 원래 연결을 유지하면서 설정을 변경한 후 클라이언트가 동일한 공유에 대한 새 연결을 생성하는 경우가 있습니다. 이 경우 새로운 SMB 연결과 기존 SMB 연결이 모두 새로운 SMB 서명 요구 사항을 적용합니다.

다음 예제를 고려해 보십시오.

1. CLIENT1은 'O:\' 경로를 사용하여 SMB 서명이 필요 없이 공유에 연결합니다.
2. 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버 구성을 수정합니다.
3. CLIENT1은 '\:' 경로를 사용하여('O:\' 경로를 사용하여 연결을 유지하면서) 필요한 SMB 서명과 동일한 공유에 연결합니다.
4. 그 결과, "O:\"와 "s:\" 드라이브 모두에서 데이터에 액세스할 때 SMB 서명이 사용됩니다.

수신 **SMB** 트래픽에 대한 **ONTAP** 서명을 구성합니다

필요한 SMB 서명을 설정하여 클라이언트가 SMB 메시지에 서명하도록 요구 사항을 적용할 수 있습니다. 활성화된 경우 ONTAP는 유효한 서명이 있는 경우에만 SMB 메시지를 수락합니다. SMB 서명을 허용하되 SMB 서명이 필요하지 않은 경우 필요한 SMB 서명을 사용하지 않도록 설정할 수 있습니다.

이 작업에 대해

기본적으로 필요한 SMB 서명은 사용되지 않습니다. 필요한 SMB 서명을 언제든지 설정하거나 해제할 수 있습니다.

다음과 같은 상황에서는 SMB 서명이 기본적으로 비활성화되어 있지 않습니다.



1. 필요한 SMB 서명이 설정되어 있고 클러스터가 SMB 서명을 지원하지 않는 ONTAP 버전으로 되돌려집니다.
2. 이후 클러스터는 SMB 서명을 지원하는 ONTAP 버전으로 업그레이드됩니다.

이러한 경우 지원되는 ONTAP 버전에 원래 구성된 SMB 서명 구성은 재버전과 후속 업그레이드를 통해 유지됩니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napMirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 필요한 SMB 서명을 사용하도록 설정한 경우, 대상 SVM에서 필요한 SMB 서명을 수동으로 활성화해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

| SMB 서명이 필요한 경우 | 명령 입력...                                                                           |
|----------------|------------------------------------------------------------------------------------|
| 활성화됨           | 'vserver cifs security modify<br>-vserver_vserver_name_-is-signing-required true'  |
| 사용 안 함         | 'vserver cifs security modify<br>-vserver_vserver_name_-is-signing-required false' |

2. 다음 명령의 출력에서 "is signing required" 필드의 값이 원하는 값으로 설정되어 있는지 확인하여 필요한 SMB 서명이 활성화되어 있는지 또는 비활성화되어 있는지 확인합니다. 'vserver cifs security show

-vserver\_vserver\_name\_-fields is-signing-required'

예

다음 예에서는 SVM VS1 에 필요한 SMB 서명을 활성화합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver is-signing-required
----- -
vs1 true
```



암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

관련 정보

- ["SnapMirror 생성"](#)

**ONTAP SMB** 세션이 서명되어 있는지 확인합니다

CIFS 서버에서 연결된 SMB 세션에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 SMB 세션이 서명되었는지 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

| 에 대한 정보를 표시하려면...                | 명령 입력...                                                                       |
|----------------------------------|--------------------------------------------------------------------------------|
| 지정된 스토리지 가상 시스템(SVM)에서 서명된 모든 세션 | 'vserver cifs session show -vserver_vserver_name_-is-session-signed true'      |
| SVM에서 특정 세션 ID와 서명된 세션의 세부 정보    | 'vserver cifs session show -vserver_vserver_name_-session-id integer-instance' |

예

다음 명령을 실행하면 SVM VS1 에서 서명된 세션에 대한 세션 정보가 표시됩니다. 기본 요약 출력에는 ""세션 서명됨" 출력 필드가 표시되지 않습니다.

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node: node1
Vserver: vs1
Connection Session
ID ID Workstation Windows User Open Idle

3151272279 1 10.1.1.1 DOMAIN\joe 2 23s
```

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 세션의 서명 여부를 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## 관련 정보

### SMB 서명 세션 통계 모니터링

#### ONTAP SMB 서명 세션 통계를 모니터링합니다

SMB 세션 통계를 모니터링하고 서명된 설정된 세션과 그렇지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 서명된 SMB 세션 수를 모니터링하는 데 사용할 수 있는 'signed\_sessions' 카운터를 제공합니다. 'Signed\_sessions' 카운터는 다음과 같은 통계 객체와 함께 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 세션에 대해 SMB 서명을 모니터링할 수 있습니다.

- 'MB1'을 사용하면 SMB 1.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.
- 'MB2'를 사용하면 SMB 2.x 및 SMB 3.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.

SMB 3.0 통계는 'MB2' 객체의 출력에 포함됩니다.

서명된 세션의 수를 총 세션 수와 비교하려면 'signed\_sessions' 카운터의 출력을 '설정된\_sessions' 카운터의 출력과 비교할 수 있습니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:'et-Privilege advanced로 설정합니다

2. 데이터 수집 시작:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id
sample_ID [-node node_name]
```

'-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

에 대한 자세한 내용은 `statistics start` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

자세히 알아보세요 `statistics stop` 에서 ["ONTAP 명령 참조입니다"](#) .

4. SMB 서명 통계 보기:

| 에 대한 정보를 보려면...                                       | 입력...                                                |
|-------------------------------------------------------|------------------------------------------------------|
| 서명된 세션                                                | shope-sample-id sample_ID-counter<br>signed_sessions |
| <i>node_name</i> [-node_node_name_]                   | 서명된 세션 및 설정된 세션                                      |
| shope-sample-id_sample_ID_-counter<br>signed_sessions | ESTANCE_SECURIONS                                    |

단일 노드에 대한 정보만 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

에 대한 자세한 내용은 `statistics show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 2.x 및 SMB 3.0 서명 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 서명된 SMB 세션과 샘플의 노드별 설정된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

| Counter              | Value |
|----------------------|-------|
| -----                | ----- |
| established_sessions | 0     |
| node_name            | node1 |
| signed_sessions      | 0     |
| established_sessions | 1     |
| node_name            | node2 |
| signed_sessions      | 1     |
| established_sessions | 0     |
| node_name            | node3 |
| signed_sessions      | 0     |
| established_sessions | 0     |
| node_name            | node4 |
| signed_sessions      | 0     |

다음 명령을 실행하면 샘플에서 노드 2에 대해 서명된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

| Counter         | Value |
|-----------------|-------|
| -----           | ----- |
| node_name       | node2 |
| signed_sessions | 1     |

다음 명령을 실행하면 admin 권한 레벨로 다시 이동됩니다.

```
cluster1::*> set -privilege admin
```

## 관련 정보

- [SMB 세션이 서명되었는지 확인합니다](#)
- ["성능 모니터링 및 관리 개요"](#)

**SMB**를 통한 데이터 전송을 위해 **SMB** 서버에서 필요한 **SMB** 암호화를 구성합니다

## ONTAP SMB 암호화에 대해 알아보십시오

SMB를 통한 데이터 전송을 위한 SMB 암호화는 SMB 서버에서 활성화 또는 비활성화할 수 있는 향상된 보안 기능입니다. 공유 속성 설정을 통해 공유별로 원하는 SMB 암호화 설정을 구성할 수도 있습니다.

기본적으로 SVM(스토리지 가상 머신)에 SMB 서버를 생성할 때 SMB 암호화는 사용하지 않도록 설정됩니다. SMB 암호화를 통해 제공되는 향상된 보안을 활용하려면 이 기능을 활성화해야 합니다.

암호화된 SMB 세션을 생성하려면 SMB 클라이언트가 SMB 암호화를 지원해야 합니다. Windows Server 2012 및 Windows 8부터 시작되는 Windows 클라이언트는 SMB 암호화를 지원합니다.

SVM의 SMB 암호화는 두 가지 설정을 통해 제어됩니다.

- SVM에서 기능을 활성화하는 SMB 서버 보안 옵션
- 공유 단위로 SMB 암호화 설정을 구성하는 SMB 공유 속성입니다

SVM의 모든 데이터에 액세스하려면 암호화를 사용할지, 선택한 공유에서만 데이터에 액세스하려면 SMB 암호화가 필요한지 여부를 결정할 수 있습니다. SVM 레벨 설정이 공유 레벨 설정보다 우선합니다.

효과적인 SMB 암호화 구성은 두 가지 설정의 조합에 따라 달라지며 다음 표에 설명되어 있습니다.

| SMB 서버 SMB 암호화가 활성화되었습니다 | 공유 암호화 데이터 설정이 활성화되었습니다 | 서버측 암호화 동작                                                                             |
|--------------------------|-------------------------|----------------------------------------------------------------------------------------|
| 참                        | 거짓                      | SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.                 |
| 참                        | 참                       | 공유 레벨 암호화와 관계없이 SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다. |
| 거짓                       | 참                       | 특정 공유에 대해 공유 수준 암호화가 설정됩니다. 이 구성을 사용하면 트리 연결로부터 암호화가 수행됩니다.                            |
| 거짓                       | 거짓                      | 암호화가 활성화되지 않았습니다.                                                                      |

암호화를 지원하지 않는 SMB 클라이언트는 암호화가 필요한 SMB 서버 또는 공유에 연결할 수 없습니다.



암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

## ONTAP SMB 암호화가 성능에 미치는 영향에 대해 알아보십시오

SMB 세션에서 SMB 암호화를 사용하면 Windows 클라이언트와 서버 간의 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버 모두에 영향을 미칩니다(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드).

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 암호화된 SMB 트래픽에서 성능을 향상시킬 수 있습니다. SMB 암호화 오프로드는 SMB 암호화가 활성화된 경우 기본적으로 활성화됩니다.

향상된 SMB 암호화 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 암호화가 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경의 테스트를 통해서만 확인할 수 있습니다.

SMB 서버에서 SMB 암호화는 기본적으로 비활성화되어 있습니다. 암호화가 필요한 SMB 공유 또는 SMB 서버에서만 SMB 암호화를 활성화해야 합니다. SMB 암호화를 통해 ONTAP는 요청을 암호 해독하고 모든 요청에 대한 응답을 암호화하는 추가 처리를 수행합니다. 따라서 필요한 경우에만 SMB 암호화를 활성화해야 합니다.

들어오는 트래픽에 대해 **ONTAP SMB** 암호화를 사용하거나 사용하지 않도록 설정합니다

수신 SMB 트래픽에 SMB 암호화가 필요한 경우 CIFS 서버 또는 공유 레벨에서 설정할 수 있습니다. 기본적으로 SMB 암호화는 필요하지 않습니다.

이 작업에 대해

CIFS 서버에서 SMB 암호화를 설정하면 CIFS 서버의 모든 공유에 적용됩니다. CIFS 서버의 모든 공유에 대해 SMB 암호화가 필요하지 않거나 공유 단위로 수신 SMB 트래픽에 대해 필요한 SMB 암호화를 설정하려는 경우 CIFS 서버에서 필요한 SMB 암호화를 해제할 수 있습니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napmirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 SMB 암호화를 사용하도록 설정한 경우 대상에서 CIFS 서버 SMB 암호화를 수동으로 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

|                                                                 |                                                                                               |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>CIFS</b> 서버에서 들어오는 <b>SMB</b> 트래픽에 대해 <b>SMB</b> 암호화가 필요한 경우 | 명령 입력...                                                                                      |
| 활성화됨                                                            | 'vserver cifs security modify<br>-vserver_vserver_name_-is-smb-encryption<br>-required true'  |
| 사용 안 함                                                          | 'vserver cifs security modify<br>-vserver_vserver_name_-is-smb-encryption<br>-required false' |

2. CIFS 서버에서 필요한 SMB 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vserver cifs security show -vserver\_vserver\_name\_-fields is-smb-encryption-required'

CIFS 서버에 필요한 SMB 암호화가 설정되어 있으면 is-smb-encryption-required 필드에 true가 표시되고, 비활성화된 경우에는 false가 표시됩니다.

예

다음 예에서는 SVM VS1에서 CIFS 서버에 대해 수신 SMB 트래픽에 필요한 SMB 암호화를 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver is-smb-encryption-required

vs1 true
```

관련 정보

- ["SnapMirror 생성"](#)

클라이언트가 암호화된 **ONTAP SMB** 세션을 사용하여 연결되어 있는지 확인합니다

연결된 SMB 세션에 대한 정보를 표시하여 클라이언트가 암호화된 SMB 연결을 사용하는지 여부를 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

SMB 클라이언트 세션은 다음 세 가지 암호화 수준 중 하나를 가질 수 있습니다.

- "암호화되지 않음"

SMB 세션이 암호화되지 않았습니다. SVM(스토리지 가상 시스템) 레벨 또는 공유 레벨 암호화가 구성되지 않았습니다.

- 부분적으로 암호화되었습니다

트리 연결이 발생하면 암호화가 시작됩니다. 공유 수준 암호화가 구성됩니다. SVM 레벨 암호화가 활성화되지 않았습니다.

- '암호화됨'

SMB 세션이 완전히 암호화됩니다. SVM 레벨 암호화가 활성화됩니다. 공유 수준 암호화가 활성화되어 있거나 활성화되어 있지 않을 수 있습니다. SVM 레벨 암호화 설정이 공유 레벨 암호화 설정보다 우선합니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

| 에 대한 정보를 표시하려면...                 | 명령 입력...                                                                        |
|-----------------------------------|---------------------------------------------------------------------------------|
| 지정된 SVM의 세션에 대해 지정된 암호화 설정을 갖는 세션 | 'vserver cifs session show -vserver_vserver_name_{encrypted                     |
| sPartially-encrypted              | encrypted}-instance'                                                            |
| 지정된 SVM에서 특정 세션 ID의 암호화 설정입니다     | 'vserver cifs session show -vserver_vserver_name_-session-id_integer_-instance' |

## 예

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 암호화 설정을 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## ONTAP SMB 암호화 통계를 모니터링합니다

SMB 암호화 통계를 모니터링하고 설정된 세션 및 공유 연결이 암호화되고 암호화되지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 다음 카운터를 제공하며, 이 카운터를 사용하여 암호화된 SMB 세션 수를 모니터링하고 연결을 공유할 수 있습니다.

| 카운터 이름                 | 설명                                        |
|------------------------|-------------------------------------------|
| '암호화 세션'               | 암호화된 SMB 3.0 세션의 수를 제공합니다                 |
| '암호화_공유_연결'            | 트리 연결이 발생한 암호화된 공유 수를 제공합니다               |
| "암호화되지 않은 세션"이 끼어들었습니다 | 에서는 클라이언트 암호화 기능이 부족하여 거부된 세션 설정 수를 제공합니다 |
| "암호화되지 않은_공유"가 있습니다    | 에서는 클라이언트 암호화 기능이 없어 거부된 공유 매핑 수를 제공합니다   |

이러한 카운터는 다음 통계 개체에서 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 3.0 세션에 대해 SMB 암호화를 모니터링할 수 있습니다.

SMB 3.0 통계는 'CIFS' 객체의 출력에 포함됩니다. 암호화된 세션의 수를 총 세션 수와 비교하려면 "encrypted\_sessions" 카운터의 출력과 "encrypted\_sessions" 카운터의 출력을 비교할 수 있습니다.

암호화된 공유 연결 수와 총 공유 연결 수를 비교하려면 에 대한 출력을 비교할 수 있습니다 encrypted\_share\_connections 에 대한 출력이 있는 카운터 connected\_shares 카운터.

- reped\_cencrypted\_sessions는 SMB 암호화를 지원하지 않는 클라이언트로부터 암호화를 요구하는 SMB 세션을 설정하려고 시도한 횟수를 제공합니다.
- refened\_cencrypted\_share는 SMB 암호화를 지원하지 않는 클라이언트의 암호화가 필요한 SMB 공유에 연결하려고 시도한 횟수를 제공합니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:+et-Privilege advanced로 설정합니다

2. 데이터 수집 시작:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

'-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

에 대한 자세한 내용은 `statistics start` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

자세히 알아보세요 `statistics stop` 에서 "[ONTAP 명령 참조입니다](#)".

4. SMB 암호화 통계 보기:

| 에 대한 정보를 보려면...                                                    | 입력...                                                              |
|--------------------------------------------------------------------|--------------------------------------------------------------------|
| 암호화된 세션                                                            | 'shope-sample-id_sample_ID_-counter<br>encrypted_sessions          |
| <i>node_name</i> [-node_node_name_]                                | 암호화된 세션 및 설정된 세션                                                   |
| shope-sample-id_sample_ID_-counter<br>encrypted_sessions           | encrypted_sessions                                                 |
| <i>node_name</i> [-node_node_name_]                                | 암호화된 공유 연결                                                         |
| 'shope-sample-id_sample_ID_-counter<br>encrypted_share_connections | <i>node_name</i> [-node_node_name_]                                |
| 암호화된 공유 연결 및 연결된 공유                                                | 'sHow-sample-id_sample_ID_-counter<br>encrypted_share_connections  |
| Connected_share                                                    | <i>node_name</i> [-node_node_name_]                                |
| 암호화되지 않은 세션이 거부되었습니다                                               | shope-sample-id_sample_ID_-counter<br>rejected_sencrypted_sessions |
| <i>node_name</i> [-node_node_name_]                                | 암호화되지 않은 공유 연결이 거부되었습니다                                            |
| 'shd-sample-id_sample_ID_-counter<br>rejected_sencrypted_share     | <i>node_name</i> [-node_node_name_]                                |

단일 노드에 대해서만 정보를 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

에 대한 자세한 내용은 `statistics show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 3.0 암호화 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 해당 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 암호화된 SMB 세션 및 샘플의 노드에 의해 설정된 SMB 세션이 표시됩니다.

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2
```

| Counter              | Value |
|----------------------|-------|
| established_sessions | 1     |
| encrypted_sessions   | 1     |

2 entries were displayed

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 세션이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2
```

| Counter                       | Value |
|-------------------------------|-------|
| rejected_unencrypted_sessions | 1     |

1 entry was displayed.

다음 명령을 실행하면 샘플의 노드에 의해 연결된 SMB 공유 및 암호화된 SMB 공유의 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:41:43  
Scope: vsim2

| Counter                     | Value |
|-----------------------------|-------|
| connected_shares            | 2     |
| encrypted_share_connections | 1     |

2 entries were displayed.

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 공유 연결이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:42:06  
Scope: vsim2

| Counter                     | Value |
|-----------------------------|-------|
| rejected_unencrypted_shares | 1     |

1 entry was displayed.

#### 관련 정보

- 서버에서 사용 가능한 통계, 개체 및 카운터를 확인합니다.
- "성능 모니터링 및 관리 개요"

#### 보안 LDAP 세션 통신

**ONTAP SMB LDAP** 서명 및 봉인에 대해 자세히 알아보십시오

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록



서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 CIFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준\_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다.

SVM에서 SVM CIFS 보안 수정 명령에 대한 '-session-security-for-ad-ldap' 옵션을 사용하여 CIFS 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

## ONTAP SMB 서버에서 LDAP 서명 및 봉인을 활성화합니다

CIFS 서버가 Active Directory LDAP 서버와의 보안 통신을 위해 서명 및 봉인을 사용하려면 먼저 CIFS 서버 보안 설정을 수정하여 LDAP 서명 및 봉인을 설정해야 합니다.

시작하기 전에

적절한 보안 구성 값을 확인하려면 AD 서버 관리자에게 문의해야 합니다.

단계

1. Active Directory LDAP 서버에서 서명되고 봉인된 트래픽을 사용할 수 있도록 CIFS 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver\_vserver\_name\_-session-security-for-ad-ldap{none|sign|seal}'

서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)를 사용할 수 있습니다. 기본값은 '없음'입니다.

2. LDAP 서명 및 봉인 보안 설정이 올바르게 설정되었는지 확인합니다. 'vserver cifs security show -vserver\_vserver\_name\_'



SVM이 이름 매핑 또는 사용자, 그룹, 넷그룹과 같은 기타 UNIX 정보를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령의 '-session-security' 옵션을 사용하여 해당 설정을 활성화해야 합니다.

## TLS를 통해 LDAP를 구성합니다

### ONTAP SMB SVM에 대한 자체 서명 루트 CA 인증서를 내보냅니다

Active Directory 통신을 보호하기 위해 SSL/TLS를 통한 LDAP를 사용하려면 먼저 Active Directory 인증서 서비스의 자체 서명 루트 CA 인증서 복사본을 인증서 파일로 내보내고 ASCII 텍스트 파일로 변환해야 합니다. 이 텍스트 파일은 ONTAP에서 SVM(스토리지 가상 머신)에 인증서를 설치하는 데 사용됩니다.

시작하기 전에

CIFS 서버가 속한 도메인에 대해 Active Directory 인증서 서비스가 이미 설치 및 구성되어 있어야 합니다. Active Director 인증서 서비스 설치 및 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

"Microsoft TechNet 라이브러리: [technet.microsoft.com](http://technet.microsoft.com)"

단계

1. '.pem' 텍스트 형식인 도메인 컨트롤러의 루트 CA 인증서를 얻습니다.

"[Microsoft TechNet 라이브러리: technet.microsoft.com](https://technet.microsoft.com)"

작업을 마친 후

SVM에 인증서를 설치합니다.

관련 정보

"[Microsoft TechNet 라이브러리](https://technet.microsoft.com)"

**ONTAP SMB SVM**에 자체 서명된 루트 **CA** 인증서를 설치합니다

LDAP 서버에 바인딩할 때 TLS를 사용한 LDAP 인증이 필요한 경우 먼저 SVM에 자체 서명된 루트 CA 인증서를 설치해야 합니다.

이 작업에 대해

TLS 통신을 사용하는 ONTAP 내의 모든 응용 프로그램은 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 디지털 인증서 상태를 확인할 수 있습니다. OCSP가 TLS를 통해 LDAP에 대해 활성화된 경우 해지된 인증서가 거부되고 연결이 실패합니다.

단계

1. 자체 서명된 루트 CA 인증서 설치:

- a. 인증서 설치를 시작합니다. 'Security certificate install - vserver vserver\_name -type server -ca'

콘솔 출력에는 'Please enter Certificate: press <Enter> when done(인증서를 입력하십시오. 완료되면 <Enter> 키를 누르십시오)' 메시지가 표시됩니다

- b. 텍스트 편집기로 인증서 '.pem' 파일을 열고 '-----'로 시작하는 줄을 포함하여 인증서를 복사합니다. 인증서 시작 ---- '-----'로 끝나는 종료 인증서 ---- 그런 다음 명령 프롬프트 뒤에 인증서를 붙여 넣습니다.
- c. 인증서가 올바르게 표시되는지 확인합니다.
- d. Enter 키를 눌러 설치를 완료합니다.

2. 인증서가 설치되어 있는지 확인합니다. 'Security certificate show -vserver\_vserver\_name\_'

관련 정보

- "[보안 인증서 설치](#)"
- "[보안 인증서가 표시됩니다](#)"

**ONTAP SMB** 서버에서 **TLS**를 통한 **LDAP**를 활성화합니다

SMB 서버가 Active Directory LDAP 서버와의 보안 통신에 TLS를 사용하려면 먼저 SMB 서버 보안 설정을 수정하여 TLS를 통한 LDAP를 활성화해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 AD(Active Directory) 및 이를 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. AD 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 설정하려면 'vserver cifs security modify' 명령을 사용하여 '-try-channel-binding-for-ad-ldap' 매개 변수를 사용합니다.

자세한 내용은 다음을 참조하십시오.

- ["ONTAP NFS SVM용 LDAP에 대해 알아보세요"](#)
- ["Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항"](#).

단계

1. Active Directory LDAP 서버와 보안 LDAP 통신을 허용하는 SMB 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver \_vserver\_name\_ -use-start-tls-for-ad-ldap true'
2. TLS를 통한 LDAP 보안 설정이 "true"로 설정되어 있는지 확인합니다. vserver cifs security show -vserver \_vserver\_name\_



SVM이 이름 매핑 또는 기타 UNIX 정보(예: 사용자, 그룹 및 넷그룹)를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령을 사용하여 '-use-start-tls' 옵션도 수정해야 합니다.

성능 및 이중화를 위해 **ONTAP SMB** 다중 채널을 구성합니다

ONTAP 9.4부터 SMB 다중 채널을 구성하여 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 연결을 제공할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다.

시작하기 전에

SMB 3.0 이상 버전에서 클라이언트가 협상하는 경우에만 SMB 멀티 채널 기능을 사용할 수 있습니다. SMB 3.0 이상은 기본적으로 ONTAP SMB 서버에서 사용하도록 설정됩니다.

이 작업에 대해

ONTAP 클러스터에서 적절한 구성이 식별되는 경우 SMB 클라이언트가 자동으로 여러 네트워크 연결을 감지하고 사용합니다.

SMB 세션의 동시 연결 수는 구축한 NIC에 따라 달라집니다.

- \* 클라이언트와 ONTAP 클러스터의 1G NIC \*

클라이언트는 NIC당 하나의 연결을 설정하고 모든 연결에 세션을 바인딩합니다.

- \* 클라이언트 및 ONTAP 클러스터에 10G 이상의 대용량 NIC \*

클라이언트는 NIC당 최대 4개의 연결을 설정하고 모든 연결에 세션을 바인딩합니다. 클라이언트는 여러 개의 10G 및 대용량 NIC에 연결을 설정할 수 있습니다.

다음 매개 변수(고급 권한)도 수정할 수 있습니다.

- -max-connections-per-session

다중 채널 세션당 허용되는 최대 연결 수입니다. 기본값은 32개 연결입니다.

기본값보다 더 많은 연결을 설정하려면 기본값인 32개의 연결을 사용하는 클라이언트 구성을 동일하게 조정해야 합니다.

- -max-lifs-per-session

Multichannel 세션당 광고되는 최대 네트워크 인터페이스 수입니다. 기본값은 256개의 네트워크 인터페이스입니다.

#### 단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. SMB 서버에서 SMB 멀티 채널 활성화:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAP가 SMB 멀티 채널 세션을 보고하는지 확인합니다.

```
vserver cifs session show
```

4. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

#### 예

다음 예에서는 모든 SMB 세션에 대한 정보를 표시하며 단일 세션에 대해 여러 개의 연결을 표시합니다.

```
cluster1::> vserver cifs session show
Node: node1
Vserver: vs1
Connection Session Open
Idle
IDs ID Workstation Windows User Files
Time

138683,
138684,
138685 1 10.1.1.1 DOMAIN\
4s
Administrator
```

다음 예에서는 세션 ID 1이 있는 SMB 세션에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

**SMB** 서버에서 기본 **Windows** 사용자를 **UNIX** 사용자 매핑으로 구성합니다

기본 **ONTAP SMB UNIX** 사용자를 구성합니다

기본 **UNIX** 사용자는 사용자의 다른 모든 매핑 시도가 실패하거나 **UNIX**와 **Windows** 간에 개별 사용자를 매핑하지 않으려는 경우에 사용하도록 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 **UNIX** 사용자를 구성하지 않아야 합니다.

이 작업에 대해

기본적으로 기본 **UNIX** 사용자의 이름은 ""pcuser""입니다. 즉, 기본적으로 기본 **UNIX** 사용자에 대한 사용자 매핑이 설정됩니다. 기본 **UNIX** 사용자로 사용할 다른 이름을 지정할 수 있습니다. 지정하는 이름은 **SVM**(스토리지 가상 머신)용으로 구성된 네임 서비스 데이터베이스에 있어야 합니다. 이 옵션이 null 문자열로 설정된 경우 **CIFS** 서버를 **UNIX** 기본 사용자로 액세스할 수 없습니다. 즉, 각 사용자는 **CIFS** 서버를 액세스하기 전에 암호 데이터베이스에 계정이 있어야 합니다.

사용자가 기본 **UNIX** 사용자 계정을 사용하여 **CIFS** 서버에 접속하려면 다음과 같은 사전 요구 사항을 충족해야 합니다.

- 사용자가 인증됩니다.
- 사용자가 **CIFS** 서버의 로컬 **Windows** 사용자 데이터베이스, **CIFS** 서버의 홈 도메인 또는 신뢰할 수 있는 도메인에 있습니다(**CIFS** 서버에서 다중 도메인 이름 매핑 검색이 설정된 경우).
- 사용자 이름이 null 문자열에 명시적으로 매핑되어 있지 않습니다.

단계

## 1. 기본 UNIX 사용자 구성:

| 원하는 작업                        | 입력...                                                        |
|-------------------------------|--------------------------------------------------------------|
| 기본 UNIX 사용자 ""pcuser"" 사용     | 'vserver cifs options modify-default-unix-user pcuser'       |
| 다른 UNIX 사용자 계정을 기본 사용자로 사용합니다 | 'vserver cifs options modify-default-unix-user _user_name_ ' |
| 기본 UNIX 사용자를 비활성화합니다          | 'vserver cifs options modify-default-unix-user''             |

'vserver cifs options modify-default-unix-user pcuser'

## 2. 기본 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver \_vserver\_name\_ '

다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group : -
Default Unix User : pcuser
Guest Unix User : pcuser
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -
```

게스트 **ONTAP SMB UNIX** 사용자를 구성합니다

게스트 UNIX 사용자 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 게스트 UNIX 사용자에게 매핑되고 CIFS 서버에 연결할 수 있습니다. 또는 신뢰할 수 없는 도메인의 사용자 인증에 실패하도록 하려면 게스트 UNIX 사용자를 구성하지 않아야 합니다. 기본값은 신뢰할 수 없는 도메인의 사용자가 CIFS 서버에 접속할 수 없도록 하는 것입니다(게스트 UNIX 계정이 구성되지 않음).

이 작업에 대해

게스트 UNIX 계정을 구성할 때 다음 사항을 염두에 두어야 합니다.

- CIFS 서버가 홈 도메인 또는 신뢰할 수 있는 도메인 또는 로컬 데이터베이스에 대한 도메인 컨트롤러에 대해 사용자를 인증할 수 없고 이 옵션이 설정된 경우 CIFS 서버는 사용자를 게스트 사용자로 간주하고 지정된 UNIX 사용자에게 매핑합니다.
- 이 옵션을 null 문자열로 설정하면 게스트 UNIX 사용자가 비활성화됩니다.

- SVM(Storage Virtual Machine) 이름 서비스 데이터베이스 중 하나에서 게스트 UNIX 사용자로 사용할 UNIX 사용자를 생성해야 합니다.
- 게스트 사용자로 로그인한 사용자는 자동으로 CIFS 서버에 있는 BUILTIN\guests 그룹의 구성원입니다.
- 'homedirs-public' 옵션은 인증된 사용자에게만 적용됩니다. 게스트 사용자로 로그인한 사용자는 홈 디렉토리가 없으며 다른 사용자의 홈 디렉토리에 액세스할 수 없습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

| 원하는 작업                | 입력...                                                     |
|-----------------------|-----------------------------------------------------------|
| 게스트 UNIX 사용자를 구성합니다   | 'vserver cifs options modify-guest-unix-user _unix_name_' |
| 게스트 UNIX 사용자를 비활성화합니다 | 'vserver cifs options modify-guest-unix-user''            |

'vserver cifs options modify-guest-unix-user pcuser'

2. 게스트 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver \_vserver\_name\_'

다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group : -
Default Unix User : pcuser
Guest Unix User : pcuser
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -
```

관리자 그룹을 **ONTAP SMB** 루트에 매핑합니다

사용자 환경에 CIFS 클라이언트만 있고 SVM(스토리지 가상 시스템)을 멀티프로토콜 스토리지 시스템으로 설정한 경우, SVM에서 파일에 액세스할 수 있는 루트 권한이 있는 Windows 계정이 하나 이상 있어야 합니다. 그렇지 않으면 충분한 사용자 권한이 없기 때문에 SVM을 관리할 수 없습니다.

이 작업에 대해

스토리지 시스템이 NTFS 전용으로 설정된 경우 이 /etc 디렉토리에는 administrators 그룹이 ONTAP 구성 파일에 액세스할 수 있는 파일 수준 ACL이 있습니다.

## 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 관리자 그룹을 루트에 적절하게 매핑하는 CIFS 서버 옵션을 구성합니다.

| 원하는 작업                      | 그러면...                                                                                                                                                                                                                                                            |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 관리자 그룹 구성원을 루트에 매핑합니다       | 'vserver cifs options modify -vserver_vserver_name_-is-admin-users-mapped-to-root-enabled true' 계정을 루트로 매핑하는 '/etc/usermap.cfg' 항목이 없는 경우에도 administrators 그룹의 모든 계정은 루트로 간주됩니다. administrators 그룹에 속하는 계정을 사용하여 파일을 생성하는 경우 UNIX 클라이언트에서 파일을 볼 때 파일은 루트에서 소유합니다. |
| 관리자 그룹 구성원을 루트에 매핑하도록 해제합니다 | "vserver cifs options modify -vserver_vserver_name_-is-admin-users-mapped-to-root-enabled false" administrators 그룹의 계정은 더 이상 루트에 매핑되지 않습니다. 단일 사용자만 루트에 명시적으로 매핑할 수 있습니다.                                                                                         |

3. 옵션이 원하는 값('vserver cifs options show -vserver\_vserver\_name\_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

**ONTAP SMB** 세션을 통해 연결된 사용자 유형에 대한 정보를 표시합니다

SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시할 수 있습니다. 따라서 적절한 유형의 사용자만 SVM(스토리지 가상 머신)의 SMB 세션을 통해 연결할 수 있습니다.

이 작업에 대해

다음 유형의 사용자는 SMB 세션을 통해 연결할 수 있습니다.

- '로컬 사용자'

로컬 CIFS 사용자로 인증되었습니다

- '다민 사용자'입니다

도메인 사용자로 인증됨(CIFS 서버의 홈 도메인 또는 신뢰할 수 있는 도메인)

- 'guest-user'입니다

게스트 사용자로 인증되었습니다

- 익명의 사용자

익명 또는 null 사용자로 인증되었습니다

## 단계



1. SMB 세션을 통해 연결된 사용자 유형을 확인합니다. 'vserver cifs session show -vserver\_vserver\_name\_-windows-user\_windows\_user\_name\_-fields windows-user, address, lif-address, user-type'

|                                |                                                                        |
|--------------------------------|------------------------------------------------------------------------|
| 설정된 세션에 대한 사용자 유형 정보를 표시하려면... | 다음 명령을 입력합니다...                                                        |
| 사용자 유형이 지정된 모든 세션에 대해          | 'vserver cifs session show -vserver_vserver_name_-user-type{local-user |
| domain-user                    | guest-user                                                             |
| anonymous-user}'입니다            | 특정 사용자의 경우                                                             |

예

다음 명령을 실행하면 ""iepubs\user1" 사용자가 설정한 SVM VS1 세션의 사용자 유형에 대한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node vserver session-id connection-id lif-address address
windows-user user-type

pub1node1 pub1 1 3439441860 10.0.0.1 10.1.1.1
IEPUBS\user1 domain-user
```

과도한 **Windows** 클라이언트 리소스 사용을 제한하는 **ONTAP** 명령 옵션입니다

'vserver cifs options modify' 명령 옵션을 사용하면 Windows 클라이언트의 리소스 사용을 제어할 수 있습니다. 이 기능은 클라이언트가 리소스 사용의 정상적인 범위를 벗어난 경우(예: 열려 있는 파일의 수가 비정상적으로 많거나 세션이 열려 있거나 변경 알림 요청이 있는 경우) 유용합니다.

Windows 클라이언트 리소스 사용을 제어하기 위해 'vserver cifs options modify' 명령에 대한 다음 옵션이 추가되었습니다. 이 옵션 중 최대값이 초과되면 요청이 거부되고 EMS 메시지가 전송됩니다. 이 옵션에 대해 구성된 제한값의 80%에 도달하면 EMS 경고 메시지도 전송됩니다.

- '-max-오픈-파일-트리 단위'

CIFS 트리당 동일한 파일에 대한 최대 열기 수입니다

- '-max-same-user-sessions-per-connection'

동일한 사용자가 접속당 연 최대 세션 수입니다

- '-max-same-tree-connect-per-session'

세션당 동일한 공유에 대한 최대 트리 연결 수입니다

- '-max-s위치-세트당-트리'

트리당 설정된 최대 시계 수(\_CHANGE ALBERS\_라고도 함)입니다

에 대한 자세한 내용은 `vserver cifs options modify` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

ONTAP 9.4부터 SMB 버전 2 이상을 실행하는 서버는 클라이언트가 SMB 연결을 통해 서버로 전송할 수 있는 미해결 요청(*smb* 크레딧) 수를 제한할 수 있습니다. SMB 크레딧의 관리는 클라이언트가 시작하고 서버에 의해 제어됩니다.

SMB 연결에서 허용할 수 있는 최대 요청 수는 '-max-credits' 옵션으로 제어됩니다. 이 옵션의 기본값은 128입니다.

#### 기존 **oplocks** 및 리스 **oplocks**로 클라이언트 성능 향상

기존 및 임대 확대를 통해 **ONTAP SMB** 클라이언트 성능을 개선하는 방법에 대해 알아보십시오

기존 **oplocks**(기회 잠금) 및 리스 **oplocks**는 특정 파일 공유 시나리오에서 SMB 클라이언트가 미리 읽기, 쓰기 후 및 잠금 정보의 클라이언트측 캐싱을 수행할 수 있도록 합니다. 그러면 클라이언트는 해당 파일에 액세스해야 한다는 사실을 서버에 정기적으로 알려주지 않고 파일을 읽거나 파일에 쓸 수 있습니다. 이렇게 하면 네트워크 트래픽이 줄어들어 성능이 향상됩니다.

리스 **oplocks**는 SMB 2.1 프로토콜 이상에서 사용할 수 있는 향상된 형태의 **oplocks**입니다. 리스 **oplocks**를 사용하면 클라이언트가 자체적으로 시작된 여러 SMB에서 클라이언트 캐싱 상태를 확보하고 유지할 수 있습니다.

**oplocks**는 다음 두 가지 방법으로 제어할 수 있습니다.

- 공유를 생성할 때 공유 속성에 의해 'vserver cifs share create' 명령을 사용하거나 생성 후 'vserver share properties' 명령을 사용합니다.
- qtree가 생성될 때 'volume qtree create' 명령을 사용하거나 생성 후 'volume qtree oplock' 명령을 사용하여 qtree 속성에 의해 생성됩니다.

**oplocks**를 사용할 때 **ONTAP SMB** 캐시 데이터 손실 고려 사항을 작성하는 방법에 대해 알아보십시오

경우에 따라 프로세스에 파일에 배타적 **oplock**이 있고 두 번째 프로세스에서 파일을 열려고 시도할 경우 첫 번째 프로세스에서는 캐시된 데이터를 무효화하고 쓰기 및 잠금을 플러시해야 합니다. 그런 다음 클라이언트는 **oplock** 및 파일에 대한 액세스를 양도해야 합니다. 이 플러시 중에 네트워크 장애가 발생하면 캐시된 쓰기 데이터가 손실될 수 있습니다.

- 데이터 손실 가능성

다음과 같은 상황에서는 쓰기 캐시된 데이터가 있는 모든 애플리케이션에서 해당 데이터가 손실될 수 있습니다.

- 연결은 SMB 1.0을 사용하여 이루어집니다.
- 파일에 배타적 **oplock**이 있습니다.
- 해당 **oplock**을 깨거나 파일을 닫도록 합니다.
- 쓰기 캐시를 플러시하는 프로세스 중에 네트워크 또는 타겟 시스템에서 오류가 발생합니다.

- 오류 처리 및 쓰기 완료

캐시 자체는 오류 처리를 하지 않습니다. 애플리케이션에서 캐시에 쓰기를 수행할 때는 항상 쓰기가 완료됩니다. 캐시가 네트워크를 통해 타겟 시스템에 쓰기를 수행하는 경우 쓰기가 완료된 것으로 가정해야 합니다. 그렇지 않으면 데이터가 손실되기 때문입니다.

oplocks를 사용하면 클라이언트가 파일을 잠그고 콘텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. oplocks는 스토리지 가상 시스템(SVM)에 상주하는 SMB 공유에 설정됩니다. 경우에 따라 oplocks를 해제할 수 있습니다. 공유별로 oplocks를 설정하거나 해제할 수 있습니다.

#### 이 작업에 대해

공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 해제됩니다. 공유에서 oplocks를 비활성화하면 볼륨 oplock 설정보다 우선적으로 적용됩니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다.

심표로 구분된 목록을 사용하여 oplock 공유 속성을 지정하는 것 외에도 다른 공유 속성을 지정할 수 있습니다. 다른 공유 매개 변수를 지정할 수도 있습니다.

#### 단계

1. 해당 작업을 수행합니다.

| 원하는 작업                                  | 그러면...                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 공유를 생성하는 동안 공유에 oplocks를 설정합니다          | <p>'vserver cifs share create -vserver_vserver_name_-share-name share_name -path path_to_share-share-properties [oplocks,...]' 명령을 입력합니다</p> <div>  <p>공유에서 oplocks, browsable, changentify의 기본 공유 속성만 사용하려면 SMB 공유를 생성할 때 '-share-properties' 매개 변수를 지정하지 않아도 됩니다. 기본값 이외의 공유 속성을 조합하려면 해당 공유에 사용할 공유 속성 목록과 함께 '-share-properties' 매개 변수를 지정해야 합니다.</p> </div> |
| 공유를 생성하는 동안 공유에 oplocks를 사용하지 않도록 설정합니다 | <p>'vserver cifs share create-vserver_vserver_name_-share-name_share_name_-path_to_share_-share-properties[other_share_property,...]' 명령을 입력합니다</p> <div>  <p>oplocks를 해제할 때는 공유를 생성할 때 공유 속성 목록을 지정해야 하지만 "oplocks" 속성을 지정해서는 안 됩니다.</p> </div>                                                                                                                 |

#### 관련 정보

[기존 SMB 공유에서 oplocks를 설정하거나 해제합니다](#)

[oplock 상태를 모니터링합니다](#)

SMB 볼륨 및 qtree에서 **oplocks**를 사용하거나 사용하지 않도록 설정하는 **ONTAP** 명령입니다

oplocks를 사용하면 클라이언트가 파일을 잠그고 콘텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. 볼륨 또는 qtree에서 oplocks를 설정하거나 해제하는 명령을 알아야 합니다. 또한 볼륨 및 qtree에서 oplocks를 설정하거나 해제할 수 있는 시기를 알아야 합니다.

- oplocks는 기본적으로 볼륨에 설정됩니다.
- 볼륨을 생성할 때는 oplocks를 해제할 수 없습니다.
- 언제든지 기존 볼륨에서 SVM에 대한 oplocks를 설정하거나 해제할 수 있습니다.
- SVM에 대해 qtree에서 oplocks를 설정할 수 있습니다.

oplock 모드 설정은 qtree ID 0의 속성으로, 모든 볼륨에 있는 기본 qtree입니다. qtree를 생성할 때 oplock 설정을 지정하지 않으면 qtree가 기본적으로 사용되는 상위 볼륨의 oplock 설정을 상속합니다. 그러나 새 qtree에 oplock 설정을 지정하면 볼륨의 oplock 설정보다 우선합니다.

| 원하는 작업                       | 이 명령 사용...                                                 |
|------------------------------|------------------------------------------------------------|
| 볼륨 또는 qtree에 oplocks를 설정합니다  | '-oplock-mode' 매개 변수가 'enable'로 설정된 볼륨 qtree oplocks       |
| 볼륨 또는 qtree에서 oplocks를 해제합니다 | '-oplock-mode' 매개 변수가 '사용할 수 있음'으로 설정된 볼륨 qtree oplocks입니다 |

## 관련 정보

[oplock 상태를 모니터링합니다](#)

기존 **ONTAP SMB** 공유에서 **oplocks**를 사용하거나 사용하지 않도록 설정합니다

oplocks는 기본적으로 스토리지 가상 시스템(SVM)의 SMB 공유에 설정됩니다. 경우에 따라 oplocks를 해제할 수도 있습니다. 이전에 공유에서 oplocks를 해제한 경우에는 oplocks를 다시 설정할 수도 있습니다.

## 이 작업에 대해

공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 비활성화됩니다. 공유에 oplocks를 사용하지 않도록 설정하면 볼륨에서 oplocks를 설정하는 것이 우선합니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다. 언제든지 기존 공유에 oplocks를 설정하거나 해제할 수 있습니다.

## 단계

1. 해당 작업을 수행합니다.

| 원하는 작업                                  | 그러면...                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 기존 공유를 수정하여 공유에 oplocks를 설정합니다          | <p>'vserver cifs share properties add -vserver _vserver_name _share-name share_name-share-properties oplocks' 명령을 입력합니다</p> <div>  <p>쉼표로 구분된 목록을 사용하여 추가할 추가 공유 속성을 지정할 수 있습니다.</p> </div> <p>새로 추가된 속성은 기존 공유 속성 목록에 추가됩니다. 이전에 지정한 공유 속성은 그대로 유지됩니다.</p>     |
| 기존 공유를 수정하여 공유에 oplocks를 사용하지 않도록 설정합니다 | <p>'vserver cifs share properties remove-vserver _vserver_name _share-name _share_name _share-properties oplocks' 명령을 입력합니다</p> <div>  <p>쉼표로 구분된 목록을 사용하여 제거할 추가 공유 속성을 지정할 수 있습니다.</p> </div> <p>제거한 공유 속성은 기존 공유 속성 목록에서 삭제되지만 이전에 구성한 공유 속성은 제거하지 않습니다.</p> |

## 예

다음 명령을 실행하면 스토리지 가상 시스템(SVM, 이전 명칭 Vserver) VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 설정됩니다.

```
cluster1::> vsriver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vsriver cifs share properties show
Vserver Share Properties

vs1 Engineering oplocks
 browsable
 changenotify
 showsnapshot
```

다음 명령을 실행하면 SVM VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 해제됩니다.

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
```

| Vserver | Share       | Properties                                |
|---------|-------------|-------------------------------------------|
| vs1     | Engineering | browsable<br>changenotify<br>showsnapshot |

#### 관련 정보

- [SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다](#)
- [oplock 상태를 모니터링합니다](#)
- [기존 주식에 주식 속성 추가 또는 제거](#)

#### ONTAP SMB oplock 상태를 모니터링합니다

oplock 상태에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보를 사용하여 oplocks가 있는 파일, oplock 레벨 및 oplock 상태 수준이 무엇인지, oplock 리스가 사용되는지 여부를 확인할 수 있습니다. 수동으로 해제해야 하는 잠금에 대한 정보를 확인할 수도 있습니다.

#### 이 작업에 대해

모든 oplocks에 대한 정보를 요약 양식 또는 세부 목록 양식에 표시할 수 있습니다. 선택적 매개 변수를 사용하여 기존 잠금의 하위 집합에 대한 정보를 표시할 수도 있습니다. 예를 들어, 지정된 클라이언트 IP 주소 또는 지정된 경로를 사용하여 출력 반환만 잠그도록 지정할 수 있습니다.

기존 및 리스 oplocks에 대한 다음 정보를 표시할 수 있습니다.

- oplock이 설정된 SVM, 노드, 볼륨 및 LIF입니다
- UUID를 잠급니다
- oplock을 사용하는 클라이언트의 IP 주소입니다
- oplock이 설정된 경로입니다
- 잠금 프로토콜(SMB) 및 유형(oplock)
- 잠금 상태
- oplock 레벨
- 연결 상태 및 SMB 만료 시간입니다
- 임대 oplock이 부여된 경우 그룹 ID를 엽니다

에 대한 자세한 내용은 `vservers oplocks show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

#### 단계

1. 'vservers lock show' 명령을 사용하여 oplock 상태를 표시합니다.

예

다음 명령을 실행하면 모든 잠금에 대한 기본 정보가 표시됩니다. 표시된 파일의 oplock은 "임시 배치" oplock 레벨로 허가됩니다.

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

| Volume | Object Path                            | LIF         | Protocol | Lock Type   | Client      |
|--------|----------------------------------------|-------------|----------|-------------|-------------|
| vol1   | /vol1/notes.txt                        | node1_data1 |          |             |             |
|        |                                        |             | cifs     | share-level | 192.168.1.5 |
|        | Sharelock Mode: read_write-deny_delete |             |          |             |             |
|        |                                        |             |          | op-lock     | 192.168.1.5 |
|        | Oplock Level: read-batch               |             |          |             |             |

다음 예제는 경로 '/data2/data2\_2/intro.pptx'를 사용하여 파일의 잠금에 대한 자세한 정보를 표시합니다. IP 주소가 10.3.1.3 인 클라이언트에 배치 oplock 레벨이 있는 파일에 리스 oplock이 부여됩니다.



자세한 정보를 표시할 때 이 명령은 oplock 및 sharelock 정보에 대한 별도의 출력을 제공합니다. 이 예제는 oplock 섹션의 출력만 보여 줍니다.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

```

 Vserver: vs1
 Volume: data2_2
 Logical Interface: lif2
 Object Path: /data2/data2_2/intro.pptx
 Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
 Lock Protocol: cifs
 Lock Type: op-lock
 Node Holding Lock State: node3
 Lock State: granted
 Bytelock Starting Offset: -
 Number of Bytes Locked: -
 Bytelock is Mandatory: -
 Bytelock is Exclusive: -
 Bytelock is Superlock: -
 Bytelock is Soft: -
 Oplock Level: batch
 Shared Lock Access Mode: -
 Shared Lock is Soft: -
 Delegation Type: -
 Client Address: 10.3.1.3
 SMB Open Type: -
 SMB Connect State: connected
 SMB Expiration Time (Secs): -
 SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## 관련 정보

[SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다](#)

[기존 SMB 공유에서 oplocks를 설정하거나 해제합니다](#)

[SMB 볼륨 및 Qtree에서 Oplock을 활성화하거나 비활성화하기 위한 명령](#)

**SMB** 서버에 그룹 정책 개체를 적용합니다

그룹 정책 개체를 **ONTAP SMB** 서버에 적용하는 방법에 대해 알아봅니다

SMB 서버는 Active Directory 환경의 컴퓨터에 적용되는 \_group 정책 특성\_이라는 규칙 집합인 GPO(그룹 정책 개체)를 지원합니다. GPO를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM(스토리지 가상 머신)에 대한 설정을 중앙에서 관리할 수 있습니다.

SMB 서버에서 GPO를 사용하도록 설정하면 ONTAP가 GPO 정보를 요청하는 Active Directory 서버에 LDAP 쿼리를 보냅니다. SMB 서버에 적용할 수 있는 GPO 정의가 있는 경우 Active Directory 서버는 다음 GPO 정보를 반환합니다.



- GPO 이름입니다
- 현재 GPO 버전입니다
- GPO 정의의 위치입니다
- GPO 정책 집합에 대한 UUID(Universally Unique Identifier) 목록입니다

#### 관련 정보

- [서버의 파일 액세스 보안에 대해 알아보세요](#)
- ["SMB 및 NFS 감사 및 보안 추적"](#)

지원되는 **ONTAP SMB GPO**에 대해 알아보니다

모든 GPO(그룹 정책 개체)가 CIFS 지원 SVM(스토리지 가상 머신)에 적용되는 것은 아니지만 SVM은 관련 GPO 세트를 인식하고 처리할 수 있습니다.

현재 SVM에서 지원되는 GPO는 다음과 같습니다.

- 고급 감사 정책 구성 설정:

객체 액세스: 중앙 액세스 정책 스테이징

다음 설정을 포함하여 중앙 액세스 정책(CAP) 스테이징에 대해 감사할 이벤트 유형을 지정합니다.

- 감사 금지
- 성공 이벤트만 감사합니다
- 오류 이벤트만 감사합니다
- 성공 및 실패 이벤트를 모두 감사합니다



세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

Advanced Audit Policy Configuration/Audit Policies/Object Access GPO에서 Audit Central Access Policy Staging 설정을 이용하여 설정한다.



고급 감사 정책 구성 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 대해 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 레지스트리 설정:
  - CIFS 지원 SVM에 대한 그룹 정책 업데이트 간격

레지스트리 GPO를 사용하여 설정합니다.

- 그룹 정책 무작위 오프셋을 새로 고칩니다

레지스트리 GPO를 사용하여 설정합니다.

- BranchCache에 대한 해시 게시

BranchCache GPO의 해시 게시는 BranchCache 운영 모드에 해당합니다. 지원되는 세 가지 작동 모드가 지원됩니다.

- 공유당
- 전체 공유
- '레지스트리' GPO를 사용하여 설정을 비활성화했습니다.

◦ BranchCache에 대한 해시 버전 지원

다음 세 가지 해시 버전 설정이 지원됩니다.

- BranchCache 버전 1
- BranchCache 버전 2
- BranchCache 버전 1 및 2는 레지스트리 GPO를 사용하여 설정합니다.



BranchCache GPO 설정을 사용하려면 이러한 설정을 적용할 CIFS 지원 SVM에 BranchCache를 구성해야 합니다. SVM에 BranchCache가 구성되어 있지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

• 보안 설정

◦ 감사 정책 및 이벤트 로그

- 로그온 이벤트를 감사합니다

다음 설정을 포함하여 감사할 로그온 이벤트의 유형을 지정합니다.

- 감사 금지
- 성공 이벤트만 감사합니다
- 장애 이벤트 감사
- Local Policies/Audit Policy GPO에서 Audit logon events 설정을 이용하여 성공 및 실패 이벤트를 모두 Audit한다.



세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

- 개체 액세스를 감사합니다

다음 설정을 포함하여 감사할 개체 액세스 유형을 지정합니다.

- 감사 금지
- 성공 이벤트만 감사합니다
- 장애 이벤트 감사
- Local Policies/Audit Policy GPO의 Audit object access 설정을 이용하여 성공 이벤트와 실패 이벤트를 모두 Audit한다.



세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

- 로그 보존 방법입니다

다음 설정을 포함하여 감사 로그 보존 방법을 지정합니다.

- 로그 파일의 크기가 최대 로그 크기를 초과할 경우 이벤트 로그를 덮어씁니다
- 이벤트 로그 GPO의 보안 로그 보관 방법 설정을 사용하여 이벤트 로그(수동으로 로그 지우기) 집합을 덮어쓰지 마십시오.

- 최대 로그 크기입니다

감사 로그의 최대 크기를 지정합니다.

이벤트 로그 GPO에서 최대 보안 로그 크기 설정을 사용하여 설정합니다.



감사 정책 및 이벤트 로그 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 파일 시스템 보안

GPO를 통해 파일 보안을 적용할 파일 또는 디렉터리 목록을 지정합니다.

파일 시스템 GPO를 사용하여 설정합니다.



파일 시스템 보안 GPO를 구성하는 볼륨 경로가 SVM 내에 있어야 합니다.

- Kerberos 정책

- 최대 클럭 불균형

컴퓨터 시계 동기화에 대한 최대 허용 시간(분)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 컴퓨터 시계 동기화에 대한 최대 허용 한도를 사용하여 설정합니다.

- 최대 항공권 사용 기간

사용자 티켓의 최대 수명(시간)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 사용자 티켓의 최대 수명 설정을 사용하여 설정합니다.

- 최대 티켓 갱신 기간

사용자 티켓 갱신에 대한 최대 수명(일)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 사용자 티켓 갱신을 위한 최대 수명 설정을 사용하여 설정합니다.

- 사용자 권한 할당(권한 권한)

- 소유권 가져오기

보안 개체의 소유권을 가져올 권한이 있는 사용자 및 그룹 목록을 지정합니다.

Local Policies/User Rights Assignment GPO에서 파일 또는 기타 개체의 소유권 가져오기 설정을

사용하여 설정합니다.

- 보안 권한

파일, 폴더 및 Active Directory 개체와 같은 개별 리소스의 개체 액세스에 대한 감사 옵션을 지정할 수 있는 사용자 및 그룹 목록을 지정합니다.

Local Policies/User Rights Assignment GPO에서 MManage auditing and security log 설정을 이용하여 설정한다.

- 알림 권한 변경(통과 확인 무시)

사용자 및 그룹에 통과 디렉터리에 대한 권한이 없더라도 디렉터리 트리를 통과할 수 있는 사용자 및 그룹 목록을 지정합니다.

사용자가 파일 및 디렉토리의 변경 알림을 수신하는 경우에도 동일한 권한이 필요합니다. Local Policies/User Rights Assignment GPO에서 통과 확인 무시 설정을 사용하여 설정합니다.

- 레지스트리 값

- 서명 필요 설정

필요한 SMB 서명을 설정 또는 해제할지 여부를 지정합니다.

보안 옵션 GPO의 'Microsoft 네트워크 서버: 디지털 서명 통신(항상)' 설정을 사용하여 설정합니다.

- 익명 제한

익명 사용자의 제한 사항을 지정하고 다음 세 가지 GPO 설정을 포함합니다.

- SAM(보안 계정 관리자) 계정의 열거 없음:

이 보안 설정은 컴퓨터에 대한 익명 연결에 대해 부여되는 추가 권한을 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 설정을 사용하여 설정합니다.

- SAM 계정 및 공유의 열거 없음

이 보안 설정은 SAM 계정과 공유의 익명 열거가 허용되는지 여부를 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts and 공유 설정을 이용하여 설정한다.

- 공유 및 명명된 파이프에 대한 익명 액세스를 제한합니다

이 보안 설정은 공유 및 파이프에 대한 익명 액세스를 제한합니다. 이 옵션이 활성화된 경우 ONTAP에서 이 옵션이 "no-access"로 표시됩니다.

Local Policies/Security Options GPO에서 Network access: restrict anonymous access to named pipes and Shares 설정을 이용하여 설정한다.

정의된 그룹 정책과 적용된 그룹 정책에 대한 정보를 표시할 때 "익명 사용자에게 대한 결과 제한" 출력 필드는 세 가지 익명 GPO 제한 설정의 결과 제한에 대한 정보를 제공합니다. 가능한 결과 제한은 다음과 같습니다.

- "접근 불가"

익명 사용자는 지정된 공유 및 명명된 파이프에 대한 액세스가 거부되며 SAM 계정과 공유의 열거를 사용할 수 없습니다. 네트워크 액세스: 명명된 파이프 및 공유에 대한 익명 액세스 제한 GPO가 설정된 경우 이러한 제한이 나타납니다.

- 번호 매기기

익명 사용자는 지정된 공유 및 명명된 파이프에 액세스할 수 있지만 SAM 계정과 공유의 열거를 사용할 수는 없습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

- 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
- Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 또는 Network access: do not allow anonymous enumeration of SAM accounts and 공유 GPO(SAM 계정과 공유의 익명 열거 허용 안 함) 중 하나가 활성화됩니다.

- 무제한입니다

익명 사용자는 모든 액세스 권한이 있으며 열거형을 사용할 수 있습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

- 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
- Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 및 Network access: do not allow anonymous enumeration of SAM accounts and ses(SAM 계정과 공유의 익명 열거 허용 안 함) GPO가 모두 비활성화됩니다.
- 제한된 그룹

제한된 그룹을 구성하여 기본 제공 그룹 또는 사용자 정의 그룹의 구성원을 중앙에서 관리할 수 있습니다. 그룹 정책을 통해 제한된 그룹을 적용하면 CIFS 서버 로컬 그룹의 구성원은 적용된 그룹 정책에 정의된 멤버 자격 목록 설정과 일치하도록 자동으로 설정됩니다.

제한 그룹 GPO를 사용하여 설정합니다.

- 중앙 액세스 정책 설정

중앙 액세스 정책 목록을 지정합니다. 중앙 액세스 정책과 관련 중앙 액세스 정책 규칙에 따라 SVM의 여러 파일에 대한 액세스 권한이 결정됩니다.

#### 관련 정보

- [서버에서 GPO 지원 활성화 또는 비활성화](#)
- [서버의 파일 액세스 보안에 대해 알아보세요](#)
- ["SMB 및 NFS 감사 및 보안 추적"](#)
- [서버 보안 설정 수정](#)
- [지점 사무실에서 공유 콘텐츠를 캐시하기 위해 BranchCache를 사용하는 방법에 대해 알아보세요.](#)
- [ONTAP 서명을 사용하여 네트워크 보안을 강화하는 방법에 대해 알아보세요.](#)

- [바이패스 트래버스 검사 구성에 대해 알아보세요](#)
- [익명 사용자의 액세스 제한을 구성합니다](#)

#### GPO에 대한 ONTAP SMB 서버 요구 사항

SMB 서버에서 GPO(그룹 정책 개체)를 사용하려면 시스템이 여러 요구 사항을 충족해야 합니다.

- SMB는 클러스터에서 라이선스가 있어야 합니다. SMB 라이선스는 에 포함되어 ["ONTAP 1 을 참조하십시오"](#) 있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.
- SMB 서버는 Windows Active Directory 도메인에 구성 및 가입해야 합니다.
- SMB 서버 관리자 상태는 켜져야 합니다.
- GPO를 구성하고 SMB 서버 컴퓨터 개체가 포함된 Windows Active Directory OU(조직 단위)에 적용해야 합니다.
- SMB 서버에서 GPO 지원을 활성화해야 합니다.

#### ONTAP SMB 서버에서 GPO 지원을 설정하거나 해제합니다

CIFS 서버에서 GPO(그룹 정책 개체) 지원을 설정하거나 해제할 수 있습니다. CIFS 서버에서 GPO 지원을 설정하면 CIFS 서버 컴퓨터 개체가 포함된 OU(조직 구성 단위)에 적용되는 그룹 정책에 정의된 적용 가능한 GPO가 CIFS 서버에 적용됩니다.



이 작업에 대해

워크그룹 모드에서는 CIFS 서버에서 GPO를 설정할 수 없습니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

| 원하는 작업       | 명령 입력...                                                                     |
|--------------|------------------------------------------------------------------------------|
| GPO를 활성화합니다  | 'vserver cifs group-policy modify<br>-vserver_vserver_name_-status enabled'  |
| GPO를 비활성화합니다 | 'vserver cifs group-policy modify<br>-vserver_vserver_name_-status disabled' |

2. GPO 지원이 'vserver cifs group-policy show-vserver+vserver\_name\_'(SVM CIFS 그룹 정책 표시) 상태로 설정되어 있는지 확인합니다

워크그룹 모드의 CIFS 서버에 대한 그룹 정책 상태는 "사용 안 함"으로 표시됩니다.

#### 예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에 대한 GPO 지원을 설정합니다.

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

Vserver: vs1
Group Policy Status: enabled
```

## 관련 정보

[지원되는 GPO에 대해 알아보세요](#)

[GPO에 대한 서버 요구 사항](#)

[SMB 서버에서 GPO 업데이트에 대해 알아보세요](#)

[SMB 서버에서 GPO 설정을 수동으로 업데이트합니다.](#)

[GPO 구성에 대한 정보를 표시합니다](#)

**SMB** 서버에서 **GPO**를 업데이트하는 방법

**ONTAP SMB** 서버에서 **GPO**를 업데이트하는 방법에 대해 알아봅니다

기본적으로 ONTAP는 90분마다 GPO(그룹 정책 개체) 변경 내용을 검색하고 적용합니다. 보안 설정은 16시간마다 새로 고쳐집니다. ONTAP에서 GPO를 자동으로 업데이트하기 전에 GPO를 업데이트하여 새 GPO 정책 설정을 적용하려면 ONTAP 명령을 사용하여 CIFS 서버에서 수동 업데이트를 트리거하면 됩니다.

- 기본적으로 모든 GPO는 90분마다 확인 및 업데이트됩니다.

이 간격은 구성 가능하며 '새로 고침 간격' 및 '임의 오프셋' GPO 설정을 사용하여 설정할 수 있습니다.

ONTAP는 Active Directory에 GPO 변경 사항을 쿼리합니다. Active Directory에 기록된 GPO 버전 번호가 CIFS 서버의 GPO 버전 번호보다 높을 경우 ONTAP는 새 GPO를 검색하고 적용합니다. 버전 번호가 같으면 CIFS 서버의 GPO가 업데이트되지 않습니다.

- 보안 설정 GPO는 16시간마다 새로 고쳐집니다.

ONTAP는 이러한 GPO의 변경 여부에 관계없이 보안 설정 GPO를 16시간마다 검색하고 적용합니다.



현재 ONTAP 버전에서는 16시간 기본값을 변경할 수 없습니다. Windows 클라이언트 기본 설정입니다.

- 모든 GPO는 ONTAP 명령을 사용하여 수동으로 업데이트할 수 있습니다.

이 명령은 Windows 'gpupdate.exe' /force' 명령을 시뮬레이션합니다.

## 관련 정보

[SMB 서버에서 GPO 설정을 수동으로 업데이트합니다.](#)

CIFS 서버에서 GPO(그룹 정책 개체) 설정을 즉시 업데이트하려면 설정을 수동으로 업데이트할 수 있습니다. 변경된 설정만 업데이트하거나 이전에 적용되었지만 변경되지 않은 설정을 포함하여 모든 설정에 대해 업데이트를 적용할 수 있습니다.

#### 단계

1. 적절한 작업을 수행합니다.

| 업데이트하려면...      | 명령 입력...                                                                                  |
|-----------------|-------------------------------------------------------------------------------------------|
| GPO 설정이 변경되었습니다 | 'vserver cifs group-policy update-vserver_vserver_name_'                                  |
| 모든 GPO 설정       | 'vserver cifs group-policy update-vserver_vserver_name_-force-re애플리케이션-all-settings true' |

#### 관련 정보

[SMB 서버에서 GPO 업데이트에 대해 알아보세요](#)

ONTAP SMB GPO 구성에 대한 정보를 표시합니다

Active Directory에 정의된 GPO(그룹 정책 개체) 구성과 CIFS 서버에 적용된 GPO 구성에 대한 정보를 표시할 수 있습니다.

#### 이 작업에 대해

CIFS 서버가 속한 도메인의 Active Directory에 정의된 모든 GPO 구성에 대한 정보를 표시하거나 CIFS 서버에 적용된 GPO 구성에 대한 정보만 표시할 수 있습니다.

#### 단계

1. 다음 작업 중 하나를 수행하여 GPO 구성에 대한 정보를 표시합니다.

| 모든 그룹 정책 구성에 대한 정보를 표시하려면... | 명령 입력...                                                       |
|------------------------------|----------------------------------------------------------------|
| Active Directory에 정의되어 있습니다  | 'vserver cifs group-policy show-defined-vserver_vserver_name_' |
| CIFS 지원 스토리지 가상 시스템(SVM)에 적용 | 'vserver cifs group-policy show-applied-vserver_vserver_name_' |

#### 예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory에 정의된 GPO 구성을 보여 줍니다.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```



Vserver: vs1

-----

GPO Name: Default Domain Policy

Level: Domain

Status: enabled

Advanced Audit Settings:

Object Access:

Central Access Policy Staging: failure

Registry Settings:

Refresh Time Interval: 22

Refresh Random Offset: 8

Hash Publication Mode for BranchCache: per-share

Hash Version Support for BranchCache : version1

Security Settings:

Event Audit and Event Log:

Audit Logon Events: none

Audit Object Access: success

Log Retention Method: overwrite-as-needed

Max Log Size: 16384

File Security:

/vol1/home

/vol1/dirl

Kerberos:

Max Clock Skew: 5

Max Ticket Age: 10

Max Renew Age: 7

Privilege Rights:

Take Ownership: usr1, usr2

Security Privilege: usr1, usr2

Change Notify: usr1, usr2

Registry Values:

Signing Required: false

Restrict Anonymous:

No enumeration of SAM accounts: true

No enumeration of SAM accounts and shares: false

Restrict anonymous access to shares and named pipes: true

Combined restriction for anonymous user: no-access

Restricted Groups:

gpr1

gpr2

Central Access Policy Settings:

Policies: cap1

cap2

GPO Name: Resultant Set of Policy

Status: enabled

Advanced Audit Settings:

Object Access:

Central Access Policy Staging: failure

Registry Settings:

Refresh Time Interval: 22

Refresh Random Offset: 8

Hash Publication for Mode BranchCache: per-share

Hash Version Support for BranchCache: version1

Security Settings:

Event Audit and Event Log:

Audit Logon Events: none

Audit Object Access: success

Log Retention Method: overwrite-as-needed

Max Log Size: 16384

File Security:

/vol1/home

/vol1/dir1

Kerberos:

Max Clock Skew: 5

Max Ticket Age: 10

Max Renew Age: 7

Privilege Rights:

Take Ownership: usr1, usr2

Security Privilege: usr1, usr2

Change Notify: usr1, usr2

Registry Values:

Signing Required: false

Restrict Anonymous:

No enumeration of SAM accounts: true

No enumeration of SAM accounts and shares: false

Restrict anonymous access to shares and named pipes: true

Combined restriction for anonymous user: no-access

Restricted Groups:

gpr1

gpr2

Central Access Policy Settings:

Policies: cap1

cap2

다음 예에서는 CIFS 지원 SVM VS1 V1에 적용된 GPO 구성을 보여 줍니다.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

```
Vserver: vs1
```

```

```

```
GPO Name: Default Domain Policy
 Level: Domain
 Status: enabled
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
 File Security:
 /vol1/home
 /vol1/dir1
 Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
 Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
 Registry Values:
 Signing Required: false
 Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
 Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

GPO Name: Resultant Set of Policy
 Level: RSOP
Advanced Audit Settings:
 Object Access:
```

```
Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
 File Security:
 /vol1/home
 /vol1/dir1
 Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
 Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
 Registry Values:
 Signing Required: false
 Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
 Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2
```

## 관련 정보

서버에서 [GPO 지원 활성화 또는 비활성화](#)

**ONTAP SMB**의 제한된 그룹 **GPO**에 대한 정보를 표시합니다

Active Directory에서 GPO(그룹 정책 개체)로 정의되고 CIFS 서버에 적용되는 제한된 그룹에 대한 자세한 정보를 표시할 수 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- 그룹 정책 이름입니다
- 그룹 정책 버전입니다
- 링크

그룹 정책이 구성되는 수준을 지정합니다. 가능한 출력 값은 다음과 같습니다.

- ONTAP에서 그룹 정책이 구성되면 Local이 됩니다
- 도메인 컨트롤러의 사이트 수준에서 그룹 정책이 구성되면 '사이트'입니다
- 도메인 컨트롤러의 도메인 수준에서 그룹 정책이 구성되면 "domain"입니다
- 조직 단위(OrganizationalUnit) - 도메인 컨트롤러의 조직 단위(OU) 수준에서 그룹 정책이 구성된 경우
- 다양한 수준에서 정의된 모든 그룹 정책에서 파생된 정책의 결과 집합에 대한 RSoP
- 제한된 그룹 이름입니다
- 제한된 그룹에 속하고 속하지 않는 사용자 및 그룹
- 제한된 그룹이 추가되는 그룹의 목록입니다

그룹은 여기에 나열된 그룹 이외의 그룹의 구성원이 될 수 있습니다.

#### 단계

1. 다음 작업 중 하나를 수행하여 모든 제한된 그룹 GPO에 대한 정보를 표시합니다.

| 모든 제한된 그룹 <b>GPO</b> 에 대한 정보를 표시하려면... | 명령 입력...                                                                       |
|----------------------------------------|--------------------------------------------------------------------------------|
| Active Directory에 정의되어 있습니다            | 'vserver cifs group-policy restricted-group show-defined-vserver vserver_name' |
| CIFS 서버에 적용됩니다                         | 'vserver cifs group-policy restricted-group show-applied-vserver vserver_name' |

#### 예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory 도메인에 정의된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy restricted-group show-defined
-vsriver vs1
```

```
Vsriver: vs1
```

```

```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

다음 예에서는 CIFS 지원 SVM VS1 에 적용된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy restricted-group show-applied
-vsriver vs1
```

```
Vsriver: vs1
```

```

```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

관련 정보

[GPO 구성에 대한 정보를 표시합니다](#)

Active Directory에 정의된 중앙 액세스 정책에 대한 자세한 정보를 표시할 수 있습니다. GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 정책의 이름입니다
- SID
- 설명
- 생성 시간
- 수정 시간
- 구성원 규칙



CIFS 서버는 GPO를 지원하지 않으므로 워크그룹 모드의 CIFS 서버는 표시되지 않습니다.

단계

1. 다음 작업 중 하나를 수행하여 중앙 액세스 정책에 대한 정보를 표시합니다.

| 모든 중앙 액세스 정책에 대한 정보를 표시하려면... | 명령 입력...                                                                             |
|-------------------------------|--------------------------------------------------------------------------------------|
| Active Directory에 정의되어 있습니다   | 'vserver cifs group-policy central-access-policy show-defined-vserver_vserver_name_' |
| CIFS 서버에 적용됩니다                | 'vserver cifs group-policy central-access-policy show-applied-vserver_vserver_name_' |

예

다음 예에서는 Active Directory에 정의된 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy central-access-policy show-defined
```

```
Vserver Name SID

vs1 p1 S-1-17-3386172923-1132988875-3044489393-
3993546205
 Description: policy #1
 Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
 Member Rules: r1

vs1 p2 S-1-17-1885229282-1100162114-134354072-
822349040
 Description: policy #2
 Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
 Member Rules: r1
 r2
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs group-policy central-access-policy show-applied
```

```
Vserver Name SID

vs1 p1 S-1-17-3386172923-1132988875-3044489393-
3993546205
 Description: policy #1
 Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
 Member Rules: r1

vs1 p2 S-1-17-1885229282-1100162114-134354072-
822349040
 Description: policy #2
 Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
 Member Rules: r1
 r2
```

#### 관련 정보

- [서버의 파일 액세스 보안에 대해 알아보세요](#)



- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

**ONTAP SMB** 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

Active Directory에 정의된 중앙 액세스 정책과 연결된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 중앙 액세스 정책 GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책 규칙에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

정의되고 적용된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 규칙의 이름입니다
- 설명
- 생성 시간
- 수정 시간
- 현재 권한
- 제안된 권한
- 타겟 리소스

|                                                 |                                                                                   |
|-------------------------------------------------|-----------------------------------------------------------------------------------|
| 중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시하려면... | 명령 입력...                                                                          |
| Active Directory에 정의되어 있습니다                     | 'vserver cifs group-policy central-access-rule show-defined-vserver vserver_name' |
| CIFS 서버에 적용됩니다                                  | 'vserver cifs group-policy central-access-rule show-applied-vserver vserver_name' |

예

다음 예에서는 Active Directory에 정의된 중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
cluster1::> vservers cifs group-policy central-access-rule show-defined
```

```
Vserver Name

vs1 r1
 Description: rule #1
 Creation Time: Tue Oct 22 09:33:48 2013
 Modification Time: Tue Oct 22 09:33:48 2013
 Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
 Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1 r2
 Description: rule #2
 Creation Time: Tue Oct 22 10:27:57 2013
 Modification Time: Tue Oct 22 10:27:57 2013
 Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
 Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 중앙 액세스 정책과 연결된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
cluster1::> vservers cifs group-policy central-access-rule show-applied
```

```
Vserver Name

vs1 r1
 Description: rule #1
 Creation Time: Tue Oct 22 09:33:48 2013
 Modification Time: Tue Oct 22 09:33:48 2013
 Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
 Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1 r2
 Description: rule #2
 Creation Time: Tue Oct 22 10:27:57 2013
 Modification Time: Tue Oct 22 10:27:57 2013
 Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
 Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

#### 관련 정보

- [서버의 파일 액세스 보안에 대해 알아보세요](#)
- [GPO 구성에 대한 정보를 표시합니다](#)
- [중앙 액세스 정책에 대한 정보를 표시합니다](#)

**SMB** 서버 컴퓨터 계정 암호를 관리하기 위한 **ONTAP** 명령입니다

암호를 변경, 재설정 및 비활성화하고 자동 업데이트 일정을 구성하기 위한 명령을 알아야 합니다. SMB 서버에서 자동으로 업데이트되도록 스케줄을 구성할 수도 있습니다.

| 원하는 작업                                         | 이 명령 사용...                                                                                |
|------------------------------------------------|-------------------------------------------------------------------------------------------|
| ONTAP가 AD 서비스와 동기화될 때 도메인 계정 암호를 변경합니다         | 'vserver cifs domain password change'를 선택합니다                                              |
| ONTAP가 AD 서비스와 동기화되지 않은 경우 도메인 계정 암호를 다시 설정합니다 | 'vserver cifs domain password reset'                                                      |
| 자동 컴퓨터 계정 암호 변경을 위해 SMB 서버를 구성합니다              | 'vserver cifs domain password schedule modify<br>-vserver vs1-is-schedule -enabled true'  |
| SMB 서버에서 자동 컴퓨터 계정 암호 변경을 비활성화합니다              | 'vserver cifs domain password schedule modify<br>-vserver vs1-is-schedule -enabled false' |

예 대한 자세한 내용은 `vserver cifs domain password` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

도메인 컨트롤러 연결을 관리합니다

**ONTAP SMB**에서 검색된 서버에 대한 정보를 표시합니다

CIFS 서버에서 검색된 LDAP 서버 및 도메인 컨트롤러와 관련된 정보를 표시할 수 있습니다.

단계

1. 검색된 서버와 관련된 정보를 표시하려면 'vserver cifs domain discovered-servers show' 명령을 입력합니다

예

다음 예에서는 SVM VS1 에서 검색된 서버를 보여 줍니다.

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
```

```
Vserver: vs1
```

| Domain Name | Type    | Preference | DC-Name | DC-Address | Status |
|-------------|---------|------------|---------|------------|--------|
| example.com | MS-LDAP | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-LDAP | adequate   | DC-2    | 1.1.3.5    | OK     |
| example.com | MS-DC   | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-DC   | adequate   | DC-2    | 1.1.3.5    | OK     |

관련 정보

- 서버를 재설정하고 재검색합니다
- 서버 중지 또는 시작

**ONTAP SMB** 서버를 재설정하고 재검색합니다

CIFS 서버에서 서버를 재설정하고 재검색하면 CIFS 서버가 LDAP 서버 및 도메인 컨트롤러에 대한 저장된 정보를 삭제할 수 있습니다. 서버 정보를 폐기한 후 CIFS 서버는 이러한 외부 서버에 대한 현재 정보를 다시 가져옵니다. 이 기능은 연결된 서버가 적절하게 응답하지 않는 경우에 유용할 수 있습니다.

단계

1. 'vserver cifs domain discovered - servers reset -servers -vserver\_vserver\_name\_' 명령을 입력합니다
2. 새로 재검색된 서버에 대한 정보를 표시합니다. 'vserver cifs domain discovered-servers show -vserver\_vserver\_name\_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 VS1 용 서버를 재설정하고 다시 검색합니다.

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
```

```
Vserver: vs1
```

| Domain Name | Type    | Preference | DC-Name | DC-Address | Status |
|-------------|---------|------------|---------|------------|--------|
| example.com | MS-LDAP | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-LDAP | adequate   | DC-2    | 1.1.3.5    | OK     |
| example.com | MS-DC   | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-DC   | adequate   | DC-2    | 1.1.3.5    | OK     |

관련 정보

- 검색된 서버에 대한 정보를 표시합니다
- 서버 중지 또는 시작

**ONTAP SMB** 도메인 컨트롤러 검색을 관리합니다

ONTAP 9.3부터는 DC(도메인 컨트롤러)가 검색되는 기본 프로세스를 수정할 수 있습니다. 이렇게 하면 사이트 또는 기본 DC 풀로 검색을 제한할 수 있으며, 이는 환경에 따라 성능 개선을 초래할 수 있습니다.

이 작업에 대해

기본적으로 동적 검색 프로세스는 기본 DC, 로컬 사이트의 모든 DC 및 모든 원격 DC를 포함하여 사용 가능한 모든

DC를 검색합니다. 이 구성을 사용하면 특정 환경에서 인증 및 공유 액세스에 지연 시간이 발생할 수 있습니다. 사용하려는 DC 풀을 이미 결정했거나 원격 DC가 부적절하거나 액세스할 수 없는 경우 검색 방법을 변경할 수 있습니다.

ONTAP 9.3 이상 릴리즈에서는 "cifs domain discovered-servers" 명령의 discovery-mode 매개 변수를 사용하여 다음 검색 옵션 중 하나를 선택할 수 있습니다.

- 도메인의 모든 DC가 검색됩니다.
- 로컬 사이트의 DC만 검색됩니다.

를 클릭합니다 default-site 사이트 및 서비스의 사이트에 할당되지 않은 LIF와 함께 이 모드를 사용하도록 SMB 서버에 대한 매개 변수를 정의할 수 있습니다.

- 서버 검색은 수행되지 않으며, SMB 서버 구성은 기본 DC에만 의존합니다.

이 모드를 사용하려면 먼저 SMB 서버의 기본 DC를 정의해야 합니다.

시작하기 전에

advanced 권한 수준이어야 합니다.

단계

1. 원하는 검색 옵션을 지정합니다. 'vserver cifs domain discovered-servers discovery-mode modify -vserver\_vserver\_name\_-mode{all|site|none}'

'모드' 파라미터 옵션:

- 모두

사용 가능한 모든 DC를 검색합니다(기본값).

- '사이트'입니다

사이트에 대한 DC 검색을 제한합니다.

- "없음"

검색을 수행하지 않고 기본 DC만 사용하십시오.

기본 **ONTAP SMB** 도메인 컨트롤러를 추가합니다

ONTAP는 DNS를 통해 도메인 컨트롤러를 자동으로 검색합니다. 필요에 따라 특정 도메인의 기본 도메인 컨트롤러 목록에 하나 이상의 도메인 컨트롤러를 추가할 수 있습니다.

이 작업에 대해

지정된 도메인에 대한 기본 도메인 컨트롤러 목록이 이미 있는 경우 새 목록이 기존 목록과 병합됩니다.

단계

1. 기본 도메인 컨트롤러 목록에 추가하려면 + "vserver cifs domain preferred-dc add-vserver\_vserver\_name\_-domain\_domain\_name\_-preferred-dc ip\_address,...+" 명령을 입력합니다

'-vserver\_vserver\_name\_'은 SVM(Storage Virtual Machine) 이름을 지정합니다.

'-domain\_domain\_name\_'은 지정된 도메인 컨트롤러가 속한 도메인의 정규화된 Active Directory 이름을 지정합니다.

'-preferred-dc\_ip\_address\_',... 기본 설정 도메인 컨트롤러의 IP 주소를 쉼표로 구분된 목록으로 지정합니다.

예

다음 명령을 실행하면 cifs.lab.example.com 도메인에 대한 외부 액세스를 관리하기 위해 SVM VS1의 SMB 서버가 사용하는 기본 도메인 컨트롤러 목록에 도메인 컨트롤러 172.17.102.25 및 172.17.102.24가 추가됩니다.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

관련 정보

[기본 도메인 컨트롤러를 관리하는 명령입니다](#)

기본 **SMB** 도메인 컨트롤러를 관리하기 위한 **ONTAP** 명령입니다

기본 도메인 컨트롤러를 추가, 표시 및 제거하는 명령을 알아야 합니다.

| 원하는 작업             | 이 명령 사용...                                |
|--------------------|-------------------------------------------|
| 기본 도메인 컨트롤러를 추가합니다 | 'vserver cifs domain preferred-dc add'    |
| 기본 도메인 컨트롤러를 표시합니다 | 'vserver cifs domain preferred-dc show'   |
| 기본 도메인 컨트롤러를 제거합니다 | 'vserver cifs domain preferred-dc remove' |

에 대한 자세한 내용은 vserver cifs domain preferred-dc "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

관련 정보

[기본 도메인 컨트롤러를 추가합니다](#)

**ONTAP SMB** 도메인 컨트롤러에 대한 암호화된 연결을 활성화합니다

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다.

이 작업에 대해

ONTAP는 '-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러(DC) 통신을 암호화해야 하며 기본값은 false입니다. SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다.

암호화된 DC 통신이 필요한 경우 ONTAP는 SMB3 연결만 협상하므로 '-SMB2-enabled-for-DC-connections' 옵션이 무시됩니다. DC가 SMB3 및 암호화를 지원하지 않는 경우 ONTAP가 이를 통해 연결되지 않습니다.

단계

1. DC와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver\_svm\_name\_-encryption -required-for-dc-connection true'

null 세션을 사용하여 **Kerberos**가 아닌 환경의 스토리지에 액세스합니다

**ONTAP SMB** null 세션을 사용하여 **Kerberos**가 아닌 환경의 스토리지에 액세스합니다

null 세션 액세스는 스토리지 시스템 데이터와 같은 네트워크 리소스 및 로컬 시스템에서 실행되는 클라이언트 기반 서비스에 대한 권한을 제공합니다. 클라이언트 프로세스가 "시스템" 계정을 사용하여 네트워크 리소스에 액세스할 때 Null 세션이 발생합니다. Null 세션 구성은 비 Kerberos 인증에만 적용됩니다.

**ONTAP SMB** 스토리지 시스템이 null 세션 액세스를 제공하는 방법에 대해 알아보십시오

null 세션 공유는 인증이 필요하지 않으므로 null 세션 액세스가 필요한 클라이언트의 IP 주소가 스토리지 시스템에 매핑되어야 합니다.

기본적으로 매핑되지 않은 null 세션 클라이언트는 공유 열거형과 같은 특정 ONTAP 시스템 서비스에 액세스할 수 있지만 스토리지 시스템 데이터에 액세스하지 못하도록 제한됩니다.



ONTAP에서는 옵션을 사용하여 Windows RestrictAnonymous 레지스트리 설정 값을 `-restrict-anonymous` 지원합니다. 이렇게 하면 매핑되지 않은 null 사용자가 시스템 리소스를 보거나 액세스할 수 있는 범위를 제어할 수 있습니다. 예를 들어 공유 열거를 사용하지 않도록 설정하고 IPC\$ 공유(숨겨진 명령된 파이프 공유)에 액세스할 수 있습니다. 및 `vserver cifs options show -restrict-anonymous`의 옵션에 대해 자세히 `vserver cifs options modify` "[ONTAP 명령 참조입니다](#)" 알아봅니다.

달리 구성하지 않는 한 null 세션을 통해 스토리지 시스템 액세스를 요청하는 로컬 프로세스를 실행하는 클라이언트는 ""Everyone""과 같은 제한적이지 않은 그룹의 구성원입니다. 선택한 스토리지 시스템 리소스에 대해 null 세션 액세스를 제한하려면 모든 null 세션 클라이언트가 속한 그룹을 생성해야 합니다. 이 그룹을 생성하면 스토리지 시스템 액세스를 제한하고 null 세션 클라이언트에 적용되는 스토리지 시스템 리소스 권한을 설정할 수 있습니다.

ONTAP는 'vserver name-mapping' 명령 세트에서 null 사용자 세션을 사용하여 스토리지 시스템 리소스에 액세스할 수 있는 클라이언트의 IP 주소를 지정하는 매핑 구문을 제공합니다. Null 사용자에게 대한 그룹을 생성한 후에는 null 세션에만 적용되는 스토리지 시스템 리소스 및 리소스 권한에 대한 액세스 제한을 지정할 수 있습니다. Null 사용자는 익명 로그인으로 식별됩니다. Null 사용자는 홈 디렉토리에 액세스할 수 없습니다.

매핑된 IP 주소에서 스토리지 시스템을 액세스하는 모든 null 사용자에게 매핑된 사용자 권한이 부여됩니다. null 사용자로 매핑된 스토리지 시스템에 대한 무단 액세스를 방지하려면 적절한 예방 조치를 고려하십시오. 최대한의 보호를 위해, IP 주소 "스포크"의 가능성을 제거하기 위해, 별도의 네트워크에 null 사용자 스토리지 시스템 액세스를 필요로 하는 모든 클라이언트와 스토리지 시스템을 배치하십시오.

관련 정보

[익명 사용자의 액세스 제한을 구성합니다](#)

**ONTAP SMB** 파일 시스템 공유에 null 사용자에게 액세스 권한을 부여합니다

null 세션 클라이언트가 사용할 그룹을 할당하고 null 세션 클라이언트의 IP 주소를 기록하여 null 세션을 사용하여 데이터를 액세스할 수 있는 스토리지 시스템의 클라이언트 목록에 추가하는 방식으로 null 세션 클라이언트를 통해 스토리지 시스템 리소스에 대한 액세스를 허용할 수 있습니다.

단계

1. "vserver name-mapping create" 명령을 사용하여 Null 사용자를 IP 한정자를 사용하여 유효한 Windows 사용자에게 매핑합니다.

다음 명령을 실행하면 유효한 호스트 이름이 google.com 인 user1에 null 사용자가 매핑됩니다.

```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

다음 명령을 실행하면 유효한 IP 주소가 10.238.2.54/32인 user1에 null 사용자가 매핑됩니다.

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. 이름 매핑을 확인하려면 'vserver name-mapping show' 명령을 사용하십시오.

```
vserver name-mapping show

Vserver: vs1
Direction: win-unix
Position Hostname IP Address/Mask

1 - 10.72.40.83/32 Pattern: anonymous logon
 Replacement: user1
```

3. "vserver cifs options modify -win-name -for-null-user" 명령을 사용하여 null 사용자에게 Windows 구성원을 할당합니다.

이 옵션은 Null 사용자에게 유효한 이름 매핑이 있는 경우에만 적용할 수 있습니다.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. "vserver cifs options show" 명령을 사용하여 null 사용자가 Windows 사용자 또는 그룹에 매핑되었는지 확인합니다.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```



## SMB 서버의 NetBIOS 별칭을 관리합니다

ONTAP SMB 서버의 NetBIOS 별칭 관리에 대해 자세히 알아보십시오

NetBIOS 별칭은 SMB 클라이언트가 SMB 서버에 연결할 때 사용할 수 있는 SMB 서버의 대체 이름입니다. SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 파일 서버의 이름에 응답하도록 할 때 유용할 수 있습니다.

SMB 서버를 생성할 때 또는 SMB 서버를 생성한 후 언제든지 NetBIOS 별칭 목록을 지정할 수 있습니다. 목록에서 NetBIOS 별칭을 언제든지 추가하거나 제거할 수 있습니다. NetBIOS 별칭 목록에 있는 이름을 사용하여 SMB 서버에 연결할 수 있습니다.

관련 정보

[NetBIOS over TCP 연결에 대한 정보를 표시합니다](#)

ONTAP SMB 서버에 NetBIOS 별칭 목록을 추가합니다

SMB 클라이언트가 별칭을 사용하여 SMB 서버에 접속하도록 하려면 NetBIOS 별칭 목록을 만들거나 NetBIOS 별칭의 기존 목록에 NetBIOS 별칭을 추가할 수 있습니다.

이 작업에 대해

- NetBIOS 별칭 이름은 최대 15자까지 지정할 수 있습니다.
- SMB 서버에서 최대 200개의 NetBIOS 별칭을 구성할 수 있습니다.
- 다음 문자는 허용되지 않습니다.

@# \* ()+=+[];:","<>V?

단계

1. NetBIOS 별칭: + 'vserver cifs add-netbios-alias-vserver\_vserver\_name\_-NetBIOS-alias\_netbios\_alias,...'를 추가합니다

```
'vserver cifs add-netbios-alias-vserver vs1-netbios-alias alias_1, alias_2, alias_3'
```

- 심표로 구분된 목록을 사용하여 하나 이상의 NetBIOS 별칭을 지정할 수 있습니다.
- 지정된 NetBIOS 별칭이 기존 목록에 추가됩니다.
- 목록이 현재 비어 있는 경우 새 NetBIOS 별칭 목록이 생성됩니다.

2. NetBIOS 별칭이 올바르게 추가되었는지 확인합니다. 'vserver cifs show -vserver vserver\_name -display -netbios -aliases'

```
'vserver cifs show-vserver vs1-display-netbios-aliases'
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

## 관련 정보

- [SMB 서버 목록에서 NetBIOS 별칭 제거](#)
- [SMB 서버에 대한 NetBIOS 별칭 목록 표시](#)

ONTAP SMB 서버 목록에서 **NetBIOS** 별칭을 제거합니다

CIFS 서버에 대한 특정 NetBIOS 별칭이 필요하지 않은 경우 목록에서 해당 NetBIOS 별칭을 제거할 수 있습니다. 목록에서 모든 NetBIOS 별칭을 제거할 수도 있습니다.

## 이 작업에 대해

심표로 구분된 목록을 사용하여 둘 이상의 NetBIOS 별칭을 제거할 수 있습니다. '-NetBIOS-aliases' 매개 변수의 값으로 ':'를 지정하여 CIFS 서버에서 모든 NetBIOS 별칭을 제거할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

| 을(를) 제거하려면...      | 입력...                                                                             |
|--------------------|-----------------------------------------------------------------------------------|
| 목록에서 특정 NetBIOS 별칭 | 'vserver cifs remove-netbios-alias-vserver_name_-netbios-alias_netbios_alias_...' |
| 목록에서 모든 NetBIOS 별칭 | 'vserver cifs remove-netbios-aliases-vserver_vserver_name_-netbios-aliases-'      |

```
'vserver cifs remove-netbios-alias-vserver vs1-netbios-alias_1'
```

2. 지정된 NetBIOS 별칭이 제거되었는지 확인합니다. 'vserver cifs show -vserver\_vserver\_name\_-display-netbios-aliases'

```
'vserver cifs show-vserver vs1-display-netbios-aliases'
```

```
Vserver: vs1

Server Name: CIFS_SERVER
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

ONTAP SMB 서버에 대한 **NetBIOS** 별칭 목록을 표시합니다

NetBIOS 별칭 목록을 표시할 수 있습니다. 이 기능은 SMB 클라이언트가 CIFS 서버에 접속할 수 있는 이름 목록을 확인하려는 경우에 유용할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

|                                      |                                             |
|--------------------------------------|---------------------------------------------|
| 다음에 대한 정보를 표시하려면...                  | 입력...                                       |
| CIFS 서버의 NetBIOS 별칭입니다               | 'vserver cifs show-display-netbios-aliases' |
| 자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록입니다 | 'vserver cifs show-instance'                |

다음 예에서는 CIFS 서버의 NetBIOS 별칭에 대한 정보를 표시합니다.

'vserver cifs show-display-netbios-aliases'

```
Vserver: vs1

 Server Name: CIFS_SERVER
 NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

다음 예에서는 자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록을 표시합니다.

'vserver cifs show-instance'

```

 Vserver: vs1
 CIFS Server NetBIOS Name: CIFS_SERVER
 NetBIOS Domain/Workgroup Name: EXAMPLE
 Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
 Authentication Style: domain
 CIFS Server Administrative Status: up
 CIFS Server Description:
 List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

에 대한 자세한 내용은 `vserver cifs show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

#### 관련 정보

- [서버에 NetBIOS 별칭 목록 추가](#)
- [서버 관리를 위한 명령어](#)

**ONTAP SMB** 클라이언트가 **NetBIOS** 별칭을 사용하여 연결되어 있는지 확인합니다

SMB 클라이언트가 NetBIOS 별칭을 사용하여 연결되어 있는지 여부와 연결된 경우 연결에 사용되는 NetBIOS 별칭을 확인할 수 있습니다. 이 기능은 연결 문제를 해결할 때 유용할 수 있습니다.

이 작업에 대해

SMB 연결에 연결된 NetBIOS 별칭(있는 경우)을 표시하려면 '-instance' 매개 변수를 사용해야 합니다. CIFS 서버 이름 또는 IP 주소를 사용하여 SMB 연결을 수행하는 경우 NetBIOS 이름 필드의 출력은 "-"(하이픈)입니다.

단계

1. 원하는 작업을 수행합니다.

| 다음에 대한 <b>NetBIOS</b> 정보를 표시하려면... | 입력...                                                           |
|------------------------------------|-----------------------------------------------------------------|
| SMB 연결                             | 'vserver cifs session show-instance'                            |
| 지정된 NetBIOS 별칭을 사용하는 연결:           | 'vserver cifs session show-instance-netbios-name_netbios_name_' |

다음 예에서는 세션 ID 1과 SMB 연결을 설정하는 데 사용되는 NetBIOS 별칭에 대한 정보를 표시합니다.

'vserver cifs session show-session-id 1-instance'

```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted

```

기타 **SMB** 서버 작업을 관리합니다

**ONTAP SMB** 서버를 중지 또는 시작합니다

사용자가 SMB 공유를 통해 데이터에 액세스하지 않는 상태에서 작업을 수행할 때 유용할 수 있는 SVM에서 CIFS 서버를 중지할 수 있습니다. CIFS 서버를 시작하여 SMB 액세스를 재시작할 수 있습니다. CIFS 서버를 중지하면 스토리지 가상 시스템(SVM)에서 허용되는 프로토콜도 수정할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

| 원하는 작업                                                      | 명령 입력...                                                  |
|-------------------------------------------------------------|-----------------------------------------------------------|
| CIFS 서버를 중지합니다                                              | 'vserver cifs stop-vserver_vserver_name_[-foreground{true |
| false}]]'                                                   | CIFS 서버를 시작합니다                                            |
| 'vserver cifs start -vserver_vserver_name_[-foreground{true | false}]]'                                                 |

'-foreground'는 포그라운드와 배경에서 명령을 실행할지 여부를 지정합니다. 이 매개 변수를 입력하지 않으면 true로 설정되고 포그라운드에서 명령이 실행됩니다.

2. 'vserver cifs show' 명령을 사용하여 CIFS 서버 관리 상태가 올바른지 확인합니다.

## 예

다음 명령은 SVM VS1 에서 CIFS 서버를 시작합니다.

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

Vserver: vs1
CIFS Server NetBIOS Name: VS1
NetBIOS Domain/Workgroup Name: DOMAIN
Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
```

## 관련 정보

- [검색된 서버에 대한 정보를 표시합니다](#)
- [서버를 재설정하고 재검색합니다](#)

## ONTAP SMB 서버를 다른 OU로 이동합니다

CIFS 서버 생성 프로세스는 다른 OU를 지정하지 않는 한 설정 중에 기본 OU(조직 구성 단위) CN=컴퓨터를 사용합니다. 설정 후 CIFS 서버를 다른 OU로 이동할 수 있습니다.

## 단계

1. Windows 서버에서 \* Active Directory 사용자 및 컴퓨터 \* 트리를 엽니다.
2. SVM(스토리지 가상 머신)에 대한 Active Directory 개체를 찾습니다.

3. 개체를 마우스 오른쪽 단추로 클릭하고 \* 이동 \* 을 선택합니다.

4. SVM과 연결할 OU를 선택합니다

#### 결과

SVM 객체가 선택한 OU에 배치됩니다.

**ONTAP SMB** 서버를 이동하기 전에 동적 **DNS** 도메인을 수정하십시오

SMB 서버를 다른 도메인으로 이동할 때 Active Directory 통합 DNS 서버가 DNS에 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SMB 서버를 이동하기 전에 SVM(스토리지 가상 시스템)에서 DDNS(동적 DNS)를 수정해야 합니다.

#### 시작하기 전에

SMB 서버 컴퓨터 계정이 포함될 새 도메인의 서비스 위치 레코드가 포함된 DNS 도메인을 사용하려면 SVM에서 DNS 이름 서비스를 수정해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서비스를 사용해야 합니다.

#### 이 작업에 대해

DDNS(SVM에서 구성된 경우)는 데이터 LIF의 DNS 레코드를 자동으로 새 도메인에 추가하지만 원래 도메인의 DNS 레코드는 원래 DNS 서버에서 자동으로 삭제되지 않습니다. 수동으로 삭제해야 합니다.

SMB 서버를 이동하기 전에 DDNS 수정을 완료하려면 다음 항목을 참조하십시오.

#### "동적 DNS 서비스를 구성합니다"

**ONTAP SMB SVM**을 **Active Directory** 도메인에 가입합니다

"vserver cifs modify" 명령을 사용하여 도메인을 수정하여 기존 SMB 서버를 삭제하지 않고 SVM(스토리지 가상 시스템)을 Active Directory 도메인에 연결할 수 있습니다. 현재 도메인에 다시 참가하거나 새 도메인에 가입할 수 있습니다.

#### 시작하기 전에

- SVM에는 이미 DNS 구성이 있어야 합니다.
- SVM을 위한 DNS 구성은 타겟 도메인을 지원할 수 있어야 합니다.

DNS 서버에는 도메인 LDAP 및 도메인 컨트롤러 서버에 대한 SRV(서비스 위치 레코드)가 포함되어 있어야 합니다.

#### 이 작업에 대해

- Active Directory 도메인 수정을 계속하려면 CIFS 서버의 관리 상태를 로 설정해야 down 합니다.
- 명령이 성공적으로 완료되면 관리 상태가 자동으로 로 up`설정됩니다. 에 대한 자세한 내용은 `up "[ONTAP 명령 참조입니다](#)"을 참조하십시오.
- 도메인에 가입할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

#### 단계

1. SVM을 CIFS 서버 도메인에 가입합니다. 'vserver cifs modify -vserver\_vserver\_name\_ -domain\_domain\_name\_-status -admin down'

에 대한 자세한 내용은 `vserver cifs modify` "[ONTAP 명령 참조입니다](#)"을 참조하십시오. 새 도메인에 대해 DNS를 다시 구성해야 하는 경우 에 대한 자세한 `vserver dns modify` 내용은 를 "[ONTAP 명령 참조입니다](#)"참조하십시오.

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 'example'.com 도메인 내의 'ou=\_example\_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-uri' 매개 변수에 `vserver cifs` 명령을 포함하여 포함시키십시오.

## 2. CIFS 서버가 원하는 Active Directory 도메인에 있는지 확인합니다. 'vserver cifs show'

예

다음 예에서는 SVM VS1 의 SMB 서버 ""CIFSSERVER1""이 keytab 인증을 사용하여 example.com 도메인에 연결됩니다.

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

|         | Server      | Status | Domain/Workgroup | Authentication |
|---------|-------------|--------|------------------|----------------|
| Vserver | Name        | Admin  | Name             | Style          |
| -----   | -----       | -----  | -----            | -----          |
| vs1     | CIFSSERVER1 | up     | EXAMPLE          | domain         |

**TCP** 연결을 통한 **ONTAP SMB NetBIOS**에 대한 정보를 표시합니다

NBT(NetBIOS over TCP) 연결에 대한 정보를 표시할 수 있습니다. 이는 NetBIOS 관련 문제를 해결할 때 유용할 수 있습니다.

단계

1. 'vserver cifs nbtstat' 명령을 사용하여 NetBIOS over TCP 연결에 대한 정보를 표시합니다.



IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

예

다음 예제에서는 ""cluster1""에 대해 표시되는 NetBIOS 이름 서비스 정보를 보여 줍니다.

```
cluster1::> vserver cifs nbtstat
```

```
Vserver: vs1
Node: cluster1-01
Interfaces:
 10.10.10.32
 10.10.10.33
Servers:
 17.17.1.2 (active)
NBT Scope:
 []
NBT Mode:
 [h]
NBT Name NetBIOS Suffix State Time Left Type

CLUSTER_1 00 wins 57
CLUSTER_1 20 wins 57

Vserver: vs1
Node: cluster1-02
Interfaces:
 10.10.10.35
Servers:
 17.17.1.2 (active)
CLUSTER_1 00 wins 58
CLUSTER_1 20 wins 58
4 entries were displayed.
```

**SMB** 서버를 관리하기 위한 **ONTAP** 명령입니다

생성, 표시, 수정, 중지, 시작 명령을 알아야 합니다. 및 SMB 서버 삭제. 또한 서버를 재설정 및 재검색, 컴퓨터 계정 암호 변경 또는 재설정, 컴퓨터 계정 암호 변경 예약, NetBIOS 별칭 추가 또는 제거 등의 명령도 있습니다.

| 원하는 작업                 | 이 명령 사용...                        |
|------------------------|-----------------------------------|
| SMB 서버를 생성합니다          | 'vserver cifs create'             |
| SMB 서버에 대한 정보를 표시합니다   | 'vserver cifs show'               |
| SMB 서버를 수정합니다          | 'vserver cifs modify(가상 CIFS 수정)' |
| SMB 서버를 다른 도메인으로 이동합니다 | 'vserver cifs modify(가상 CIFS 수정)' |



|                                    |                                                          |
|------------------------------------|----------------------------------------------------------|
| SMB 서버를 중지합니다                      | 'vserver cifs stop'                                      |
| SMB 서버를 시작합니다                      | 'vserver cifs start'를 선택합니다                              |
| SMB 서버를 삭제합니다                      | 'vserver cifs delete'                                    |
| SMB 서버의 서버를 재설정하고 다시 검색합니다         | 'vserver cifs domain discovered - servers reset-servers' |
| SMB 서버의 컴퓨터 계정 암호를 변경합니다           | 'vserver cifs domain password change'를 선택합니다             |
| SMB 서버의 컴퓨터 계정을 재설정합니다             | 'vserver cifs domain password change'를 선택합니다             |
| SMB 서버의 컴퓨터 계정에 대한 자동 암호 변경을 예약합니다 | 'vserver cifs domain password schedule modify'를 참조하십시오   |
| SMB 서버에 대한 NetBIOS 별칭을 추가합니다       | 'vserver cifs add-netbios-aliases'                       |
| SMB 서버의 NetBIOS 별칭을 제거합니다          | 'vserver cifs remove-netbios-aliases'                    |

에 대한 자세한 내용은 `vserver cifs` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

#### 관련 정보

["SMB 서버를 삭제할 때 로컬 사용자 및 그룹이 어떻게 됩니까"](#)

**ONTAP SMB NetBIOS** 이름 서비스를 활성화합니다

ONTAP 9부터는 NetBIOS 이름 서비스(NBNS, Windows 인터넷 이름 서비스 또는 WINS라고도 함)가 기본적으로 사용되지 않습니다. 이전에는 CIFS 지원 SVM(스토리지 가상 머신)이 네트워크에서 WINS가 활성화되었는지 여부에 관계없이 이름 등록 브로드캐스트를 전송했습니다. NBNS가 필요한 구성으로 이러한 브로드캐스트를 제한하려면 새 CIFS 서버에 대해 NBNS를 명시적으로 설정해야 합니다.

#### 시작하기 전에

- 이미 NBNS를 사용하고 있으며 ONTAP 9로 업그레이드하는 경우 이 작업을 완료할 필요가 없습니다. NBNS는 이전과 마찬가지로 계속 작동합니다.
- NBNS는 UDP(포트 137)를 통해 활성화됩니다.
- IPv6을 통한 NBNS는 지원되지 않습니다.

#### 단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

## 2. CIFS 서버에서 NBNS를 설정합니다.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled true
```

## 3. 관리자 권한 수준으로 돌아갑니다.

```
set -privilege admin
```

## SMB 액세스 및 SMB 서비스에 IPv6를 사용합니다

IPv6에 대한 **ONTAP SMB** 요구 사항에 대해 알아보십시오

SMB 서버에서 IPv6를 사용하려면 먼저 IPv6를 지원하는 ONTAP 및 SMB 버전과 라이선스 요구 사항이 무엇인지 알아야 합니다.

### ONTAP 라이선스 요구 사항

SMB 라이선스가 있는 경우 IPv6에 대한 특수 라이선스가 필요하지 않습니다. SMB 라이선스는 에 포함되어 ["ONTAP 1을 참조하십시오"](#) 있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

### SMB 프로토콜 버전 요구 사항

- SVM의 경우 ONTAP는 모든 버전의 SMB 프로토콜에서 IPv6를 지원합니다.



IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

**ONTAP SMB 액세스 및 CIFS 서비스를 통한 IPv6 지원에 대해 자세히 알아보십시오**

CIFS 서버에서 IPv6를 사용하려면 ONTAP가 CIFS 서비스에 대한 SMB 액세스 및 네트워크 통신을 위해 IPv6를 지원하는 방법을 알고 있어야 합니다.

### Windows 클라이언트 및 서버 지원

ONTAP는 IPv6를 지원하는 Windows 서버 및 클라이언트를 지원합니다. 다음은 Microsoft Windows 클라이언트 및 서버 IPv6 지원에 대한 설명입니다.

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 이상에서는 DNS, LDAP, CLDAP 및 Kerberos 서비스를 포함한 SMB 파일 공유 및 Active Directory 서비스에 대해 IPv6를 지원합니다.

IPv6 주소가 구성된 경우 Windows 7 및 Windows Server 2008 이상 릴리즈에서는 Active Directory 서비스에 대해 기본적으로 IPv6을 사용합니다. IPv6 연결을 통한 NTLM 및 Kerberos 인증이 모두 지원됩니다.

ONTAP에서 지원하는 모든 Windows 클라이언트는 IPv6 주소를 사용하여 SMB 공유에 연결할 수 있습니다.

ONTAP가 지원하는 Windows 클라이언트에 대한 최신 정보는 를 참조하십시오 ["상호 운용성 매트릭스"](#).



NT 도메인은 IPv6에서 지원되지 않습니다.

## 추가 CIFS 서비스 지원

ONTAP는 SMB 파일 공유 및 Active Directory 서비스에 대한 IPv6 지원 외에도 다음에 대한 IPv6 지원을 제공합니다.

- 오프라인 폴더, 로밍 프로필, 폴더 리디렉션 및 이전 버전을 포함한 클라이언트측 서비스입니다
- 동적 홈 디렉토리(홈 디렉토리 기능), symlink 및 Widelink, BranchCache, ODX 복사 오프로드, 자동 노드 추천 등의 서버 측 서비스 및 이전 버전
- Windows 로컬 사용자 및 그룹을 사용하여 액세스 제어 및 권한 관리, CLI를 사용한 파일 권한 및 감사 정책 설정, 보안 추적, 파일 잠금 관리, SMB 작업 모니터링 등의 파일 액세스 관리 서비스입니다
- NAS 멀티 프로토콜 감사
- FPolicy를 참조하십시오
- 지속적으로 사용 가능한 공유, Witness 프로토콜 및 원격 VSS(SMB 구성 기반 Hyper-V에 사용)

## 네임 서비스 및 인증 서비스 지원

IPv6에서는 다음 이름 서비스와의 통신이 지원됩니다.

- 도메인 컨트롤러
- DNS 서버
- LDAP 서버
- KDC 서버
- NIS 서버

**ONTAP SMB** 서버가 **IPv6**를 사용하여 외부 서버에 연결하는 방법에 대해 알아봅니다

요구 사항을 충족하는 구성을 생성하려면 CIFS 서버가 외부 서버에 연결할 때 IPv6을 사용하는 방법을 알고 있어야 합니다.

- 원본 주소 선택

외부 서버에 연결하려고 시도하면 선택한 소스 주소는 대상 주소와 같은 유형이어야 합니다. 예를 들어, IPv6 주소에 연결하는 경우 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)에는 소스 주소로 사용할 IPv6 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다. 마찬가지로, SVM을 IPv4 주소에 연결할 경우 소스 주소로 사용할 IPv4 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다.

- DNS를 사용하여 동적으로 검색된 서버의 경우 서버 검색은 다음과 같이 수행됩니다.
  - 클러스터에서 IPv6이 비활성화되어 있으면 IPv4 서버 주소만 검색됩니다.
  - 클러스터에서 IPv6이 활성화되어 있으면 IPv4 및 IPv6 서버 주소가 모두 검색됩니다. 주소가 속한 서버의 적합성과 IPv6 또는 IPv4 데이터 또는 관리 LIF의 가용성에 따라 두 유형 중 하나를 사용할 수 있습니다. 동적 서버 검색은 도메인 컨트롤러 및 LSA, NETLOGON, Kerberos 및 LDAP와 같은 관련 서비스를 검색하는 데 사용됩니다.
- DNS 서버 연결

DNS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 DNS 이름 서비스 구성에 따라 달라집니다. DNS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 DNS 이름 서비스 구성에서 IPv4 주소를 사용하여 DNS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. DNS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.

- LDAP 서버 접속 구성

LDAP 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 LDAP 클라이언트 구성에 따라 달라집니다. LDAP 클라이언트가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결됩니다. 필요한 경우 LDAP 클라이언트 구성에서 IPv4 주소를 사용하여 LDAP 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. LDAP 클라이언트 구성을 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.



LDAP 클라이언트 구성은 UNIX 사용자, 그룹 및 넷그룹 이름 서비스에 대해 LDAP를 구성할 때 사용됩니다.

- NIS 서버 접속

NIS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 NIS 이름 서비스 구성에 따라 달라집니다. NIS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 NIS 이름 서비스 구성에서 IPv4 주소를 사용하여 NIS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. NIS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.



NIS 이름 서비스는 UNIX 사용자, 그룹, 넷그룹 및 호스트 이름 객체를 저장하고 관리하는 데 사용됩니다.

#### 관련 정보

- [서버에 IPv6 활성화](#)
- [IPv6 세션에 대한 정보를 모니터링하고 표시합니다.](#)

**ONTAP SMB** 서버에 **IPv6**를 사용하도록 설정합니다

클러스터 설정 중에 IPv6 네트워크가 활성화되지 않습니다. SMB용 IPv6를 사용하려면 클러스터 설정이 완료된 후 클러스터 관리자가 IPv6을 사용하도록 설정해야 합니다. 클러스터 관리자가 IPv6을 사용하도록 설정하면 전체 클러스터에 대해 설정됩니다.

#### 단계

1. IPv6 사용:'네트워크 옵션 IPv6 수정 사용 참'을 선택합니다

IPv6이 활성화되었습니다. SMB 액세스를 위한 IPv6 데이터 LIF를 구성할 수 있습니다.

#### 관련 정보

- [IPv6 세션에 대한 정보를 모니터링하고 표시합니다.](#)
- ["System Manager를 사용하여 네트워크를 시각화합니다"](#)
- ["클러스터에서 IPv6 활성화"](#)
- ["네트워크 옵션 IPv6 수정"](#)

ONTAP SMB 서버에 대해 IPv6를 사용하지 않도록 설정하는 방법에 대해 자세히 알아보십시오

네트워크 옵션을 사용하여 클러스터에 IPv6이 설정되어 있어도 동일한 명령을 사용하여 SMB용 IPv6를 해제할 수 없습니다. 대신 ONTAP는 클러스터 관리자가 클러스터에서 마지막 IPv6 사용 인터페이스를 비활성화할 때 IPv6를 비활성화합니다. IPv6 지원 인터페이스 관리에 대해서는 클러스터 관리자와 통신해야 합니다.

관련 정보

- ["System Manager를 사용하여 ONTAP 네트워크를 시각화합니다"](#)

IPv6 ONTAP SMB 세션에 대한 정보를 모니터링하고 표시합니다

IPv6 네트워크를 사용하여 연결된 SMB 세션에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보는 IPv6 SMB 세션에 대한 기타 유용한 정보와 함께 IPv6를 사용하여 연결 중인 클라이언트를 확인하는 데 유용합니다.

단계

1. 원하는 작업을 수행합니다.

| 다음 사항을 확인할 수 있습니다.                            | 명령 입력...                                                                                                                              |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| SVM(스토리지 가상 시스템)에 대한 SMB 세션은 IPv6를 사용하여 연결됩니다 | 'vserver cifs session show -vserver_vserver_name_-instance'                                                                           |
| IPv6은 지정된 LIF 주소를 통해 SMB 세션에 사용됩니다            | 'vserver cifs session show -vserver_vserver_name_-lif-address_LIF_ip_address_-instance'<br><br>'LIF_IP_address'는 데이터 LIF의 IPv6 주소입니다. |

## SMB를 사용하여 파일 액세스를 설정합니다

보안 스타일을 구성합니다

보안 스타일이 데이터 액세스에 미치는 영향

ONTAP SMB 보안 스타일과 그 영향에 대해 알아보십시오

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 톨을 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<br>NFSv4.x ACL | Unix                     | NFS 및 SMB              |
| 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 [참조하십시오 FlexGroup 볼륨 관리 개요](#).

그만큼 `show-effective-permissions` 매개변수를 사용하여 `vserver security file-directory` 명령을 사용하면 지정된 파일이나 폴더 경로에 대해 Windows 또는 UNIX 사용자에게 부여된 유효 권한을 표시할 수 있습니다. 또한 선택적 매개 변수를 `-share-name` 사용하면 효과적인 공유 권한을 표시할 수 있습니다. 에 대한 자세한 내용은 `vserver security file-directory show-effective-permissions` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.



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.

#### 관련 정보

- ["ONTAP 명령 참조입니다"](#)

#### ONTAP SMB 보안 스타일을 설정할 위치 및 시기에 대해 알아보십시오

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

#### ONTAP SVM에서 사용할 SMB 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    | <ul style="list-style-type: none"><li>• 파일 시스템은 UNIX 관리자가 관리합니다.</li><li>• 대부분의 사용자는 NFS 클라이언트입니다.</li><li>• 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다.</li></ul>        |
| NTFS입니다 | <ul style="list-style-type: none"><li>• 파일 시스템은 Windows 관리자가 관리합니다.</li><li>• 대부분의 사용자는 SMB 클라이언트입니다.</li><li>• 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다.</li></ul> |
| 혼합      | 파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다.                                                                                                  |

**ONTAP SMB** 보안 스타일 상속에 대해 알아보십시오

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.

**ONTAP SMB FlexVol** 볼륨에 대한 **UNIX** 사용 권한을 유지하는 방법에 대해 알아보십시오

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.

**ONTAP SMB 서버의 Windows 보안 탭을 사용하여 UNIX 권한을 관리하는 방법에 대해 알아봅니다**

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.

**ONTAP SVM 루트 볼륨에 SMB 보안 형식을 구성합니다**

SVM(Storage Virtual Machine) 루트 볼륨 보안 스타일을 구성하여 SVM의 루트 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 보안 스타일을 정의하려면 '-rootvolume-security-style' 매개 변수와 함께 'vserver create' 명령을 사용하십시오.

루트 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합입니다.

2. 생성한 SVM의 루트 볼륨 보안 스타일('vserver show -vserver\_vserver\_name\_')을 포함하여 구성을 표시하고 확인합니다

**ONTAP FlexVol 볼륨에 SMB 보안 스타일을 구성합니다**

FlexVol 볼륨 보안 스타일을 구성하여 SVM(스토리지 가상 머신)의 FlexVol 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.



|             |                                                         |
|-------------|---------------------------------------------------------|
| FlexVol 볼륨이 | 명령 사용...                                                |
| 아직 없습니다     | 보안 스타일을 지정하기 위해 볼륨 생성 및 '-security-style' 매개 변수를 포함합니다. |
| 이미 있습니다     | 볼륨 수정, -security-style 매개 변수를 포함해서 보안 스타일을 지정합니다.       |

FlexVol 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합입니다.

FlexVol 볼륨을 만들 때 보안 스타일을 지정하지 않으면 볼륨은 루트 볼륨의 보안 스타일을 상속합니다.

볼륨 생성 또는 볼륨 수정 명령에 대한 자세한 내용은 을 참조하십시오 ["논리적 스토리지 관리"](#).

2. 생성한 FlexVol 볼륨의 보안 스타일을 포함하여 구성을 표시하려면 다음 명령을 입력합니다.

```
'volume show-volume volume_name-instance'
```

**ONTAP qtree**에서 **SMB** 보안 스타일을 구성합니다

Qtree 볼륨 보안 스타일을 구성하여 Qtree에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

|                  |                                                                  |
|------------------|------------------------------------------------------------------|
| <b>qtree가...</b> | 명령 사용...                                                         |
| 아직 없습니다          | 볼륨 qtree create를 수행하고 보안 스타일을 지정하는 -security-style 매개 변수를 포함합니다. |
| 이미 있습니다          | 볼륨 qtree 수정과 보안 유형을 지정하는 -security-style 매개 변수를 포함합니다.           |

qtree 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS, 혼합입니다.

Qtree를 만들 때 보안 스타일을 지정하지 않으면 기본 보안 스타일이 '혼합'으로 설정됩니다.

'볼륨 qtree 생성' 또는 '볼륨 qtree 수정' 명령에 대한 자세한 내용은 을 참조하십시오 ["논리적 스토리지 관리"](#).

2. 생성한 qtree의 보안 스타일을 포함하여 구성을 표시하려면 ' volume qtree show-qtree qtree qtree\_name-instance ' 명령을 입력합니다

**NAS** 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다

**NAS** 네임스페이스에서 **ONTAP SMB** 데이터 볼륨을 생성하고 관리하는 방법에 대해 알아보십시오

NAS 환경에서 파일 액세스를 관리하려면 SVM(스토리지 가상 머신)에서 데이터 볼륨과 접합

지점을 관리해야 합니다. 여기에는 네임스페이스 아키텍처 계획, 접합 지점을 사용하거나 사용하지 않는 볼륨 생성, 볼륨 마운트 또는 마운트 해제, 데이터 볼륨 및 NFS 서버 또는 CIFS 서버 네임스페이스에 대한 정보 표시 등이 포함됩니다.

지정된 접합 지점으로 **ONTAP SMB** 데이터 볼륨을 생성합니다

데이터 볼륨을 생성할 때 교차점을 지정할 수 있습니다. 결과 볼륨은 교차점에 자동으로 마운트되며 NAS 액세스를 위해 즉시 구성할 수 있습니다.

시작하기 전에

볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.



다음 문자는 접합 경로에 사용할 수 없습니다. `*#"><|? \`

또한 접합 경로 길이는 255자를 초과할 수 없습니다.

단계

1. "volume create-vserver\_name\_-volume\_volume\_name\_-aggregate\_aggregate\_name\_-size{integer[KB|MB|GB|TB|PB]}-security-style{NTFS|UNIX|MIXED}-junction-path\_junction\_path\_"를 사용하여 볼륨을 생성합니다

접합 경로는 루트(/)로 시작해야 하며 디렉터리와 접합된 볼륨을 모두 포함할 수 있습니다. 접합 경로에는 볼륨의 이름을 포함할 필요가 없습니다. 접합 경로는 볼륨 이름과 무관합니다.

볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 만드는 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

교차경로는 대/소문자를 구분하지 않고 /eng은 /eng과 같습니다. CIFS 공유를 생성하는 경우 Windows는 연결 경로를 대/소문자를 구분하는 것처럼 처리합니다. 예를 들어, junction이 /eng인 경우 CIFS 공유의 경로는 /eng가 아니라 /eng로 시작해야 합니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 volume create "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. 볼륨이 원하는 접합 지점 'volume show-vserver\_vserver\_name\_-volume\_volume\_name\_-junction'을 사용하여 생성되었는지 확인합니다

예

다음 예에서는 junction path "/eng/home"이 있는 SVM VS1 상에 ""home4""라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

| Vserver | Volume | Active | Junction Path | Junction Path Source |
|---------|--------|--------|---------------|----------------------|
| vs1     | home4  | true   | /eng/home     | RW_volume            |

접합 지점을 지정하지 않고 **ONTAP SMB** 데이터 볼륨을 생성합니다

교차점을 지정하지 않고 데이터 볼륨을 생성할 수 있습니다. 결과 볼륨은 자동으로 마운트되지 않으며 NAS 액세스에 대해 구성할 수 없습니다. 해당 볼륨에 대해 SMB 공유 또는 NFS 내보내기를 구성하려면 먼저 볼륨을 마운트해야 합니다.

시작하기 전에

볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.

단계

1. 다음 명령을 사용하여 접합 지점 없이 볼륨을 생성합니다. 'volume create-vserver\_name\_-volume\_volume\_name\_-aggregate\_aggregate\_name\_-size{integer[KB|MB|GB|TB|PB]} - security-style{NTFS|UNIX|MIXED}'

볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 volume create "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. 볼륨이 "volume show-vserver\_name\_-volume\_volume\_name\_-junction" 접합 지점 없이 생성되었는지 확인합니다

예

다음 예에서는 교차점에 마운트되지 않은 SVM VS1 상에 "sales"라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Active | Junction Path | Junction Path Source |
|---------|----------|--------|---------------|----------------------|
| vs1     | data     | true   | /data         | RW_volume            |
| vs1     | home4    | true   | /eng/home     | RW_volume            |
| vs1     | vs1_root | -      | /             | -                    |
| vs1     | sales    | -      | -             | -                    |

**NAS** 네임스페이스에서 기존 **ONTAP SMB** 볼륨을 마운트하거나 마운트 해제합니다

SVM(스토리지 가상 시스템) 볼륨에 포함된 데이터에 대한 NAS 클라이언트 액세스를 구성하려면 먼저 NAS 네임스페이스에 볼륨을 마운트해야 합니다. 볼륨이 현재 마운트되지 않은 경우 볼륨을 연결 지점에 마운트할 수 있습니다. 볼륨을 마운트 해제할 수도 있습니다.

이 작업에 대해

볼륨을 마운트 해제하고 오프라인으로 전환하면 마운트 해제된 볼륨의 네임스페이스 내에 포함된 접합 지점의 볼륨 데이터를 비롯하여 연결 지점 내의 모든 데이터를 NAS 클라이언트에서 액세스할 수 없습니다.



볼륨에 대한 NAS 클라이언트 액세스를 중단하려면 볼륨을 마운트 해제하는 것만으로는 충분하지 않습니다. 볼륨을 오프라인으로 전환하거나 클라이언트 측 파일 핸들 캐시가 무효화되도록 다른 단계를 수행해야 합니다. 자세한 내용은 다음 기술 자료 문서를 참조하십시오. ["ONTAP의 네임스페이스에서 제거후에도 NFSv3 클라이언트가 볼륨에 계속 액세스할 수 있습니다"](#)

볼륨을 마운트 해제하고 오프라인으로 전환하면 볼륨 내의 데이터가 손실되지 않습니다. 또한 마운트 해제된 볼륨 내의 볼륨이나 디렉토리 및 연결 지점에 생성된 기존 볼륨 내보내기 정책 및 SMB 공유가 보존됩니다. 마운트 해제된 볼륨을 다시 마운트하면 NAS 클라이언트가 기존 익스포트 정책과 SMB 공유를 사용하여 볼륨 내에 포함된 데이터에 액세스할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

| 원하는 작업     | 명령 입력...                                                                                  |
|------------|-------------------------------------------------------------------------------------------|
| 볼륨을 마운트합니다 | 'volume mount-vserver_svm_name_-<br>volume_volume_name_-junction-<br>path_junction_path_' |

| 원하는 작업        | 명령 입력...                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|
| 볼륨을 마운트 해제합니다 | <pre>volume unmount -vserver svm_name -volume volume_name</pre> <pre>volume offline -vserver svm_name -volume volume_name</pre> |

## 2. 볼륨이 원하는 마운트 상태에 있는지 확인합니다.

```
volume show -vserver svm_name -volume volume_name -fields state,junction-
path,junction-active
```

예

다음 예에서는 SVM "VS1"에 있는 "판매"라는 볼륨을 접합 지점 "/판매"에 마운트합니다.

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

| vserver | volume | state  | junction-path | junction-active |
|---------|--------|--------|---------------|-----------------|
| vs1     | data   | online | /data         | true            |
| vs1     | home4  | online | /eng/home     | true            |
| vs1     | sales  | online | /sales        | true            |

다음 예에서는 SVM "VS1"에 있는 "데이터"라는 이름의 볼륨을 마운트 해제하고 오프라인으로 전환합니다.

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

| vserver | volume | state   | junction-path | junction-active |
|---------|--------|---------|---------------|-----------------|
| vs1     | data   | offline | -             | -               |
| vs1     | home4  | online  | /eng/home     | true            |
| vs1     | sales  | online  | /sales        | true            |

**ONTAP SMB** 볼륨 마운트 및 접합 지점 정보를 표시합니다

스토리지 가상 시스템(SVM)에 대해 마운트된 볼륨 및 볼륨이 마운트된 접합 지점에 대한 정보를 표시할 수 있습니다. 또한 어느 볼륨이 분기점에 마운트되지 않는지 확인할 수 있습니다. 이

정보를 사용하여 SVM 네임스페이스를 이해하고 관리할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

| 를 표시하려면...                        | 명령 입력...                                                                                                                                                                          |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SVM에서 마운트 및 마운트 해제된 볼륨에 대한 요약 정보  | 'volume show -vserver vserver_name-junction'                                                                                                                                      |
| SVM에서 마운트 및 마운트 해제된 볼륨에 대한 자세한 정보 | 'volume show -vserver vserver_name -volume volume_name -instance'                                                                                                                 |
| SVM에서 마운트 및 마운트 해제된 볼륨에 대한 특정 정보  | <p>a. 필요한 경우 볼륨 표시 필드? 명령을 사용하여 '-fields' 매개 변수에 대한 유효한 필드를 표시할 수 있습니다</p> <p>b. '-fields' 매개 변수를 사용하여 원하는 정보를 표시합니다. volume show -vserver vserver_name -fields fieldname,...</p> |

예

다음 예는 SVM VS1 에서 마운트 및 마운트 해제된 볼륨에 대한 요약을 표시합니다.

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Active | Junction Path | Junction Path Source |
|---------|----------|--------|---------------|----------------------|
| vs1     | data     | true   | /data         | RW_volume            |
| vs1     | home4    | true   | /eng/home     | RW_volume            |
| vs1     | vs1_root | -      | /             | -                    |
| vs1     | sales    | true   | /sales        | RW_volume            |

다음 예는 SVM VS2 에 있는 볼륨의 지정된 필드에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume aggregate size state type security-style junction-path
junction-parent node

vs2 data1 aggr3 2GB online RW unix - -
node3
vs2 data2 aggr3 1GB online RW ntfs /data2
vs2_root node3
vs2 data2_1 aggr3 8GB online RW ntfs /data2/d2_1
data2 node3
vs2 data2_2 aggr3 8GB online RW ntfs /data2/d2_2
data2 node3
vs2 pubs aggr1 1GB online RW unix /publications
vs2_root node1
vs2 images aggr3 2TB online RW ntfs /images
vs2_root node3
vs2 logs aggr1 1GB online RW unix /logs
vs2_root node1
vs2 vs2_root aggr3 1GB online RW ntfs / -
node3
```

이름 매핑을 구성합니다

**ONTAP SMB** 이름 매핑 구성에 대해 자세히 알아보십시오

ONTAP는 이름 매핑을 사용하여 CIFS ID를 UNIX ID에 매핑하고, Kerberos ID를 UNIX ID에 매핑하며, UNIX ID를 CIFS ID에 매핑합니다. 사용자 자격 증명을 얻고 NFS 클라이언트나 CIFS 클라이언트에서 연결 중인지에 관계없이 적절한 파일 액세스를 제공하려면 이 정보가 필요합니다.

이름 매핑을 사용할 필요가 없는 두 가지 예외가 있습니다.

- 순수 UNIX 환경을 구성하고 볼륨에 CIFS 액세스 또는 NTFS 보안 스타일을 사용하지 않을 계획입니다.
- 대신 사용할 기본 사용자를 구성합니다.

이 시나리오에서는 모든 개별 클라이언트 자격 증명을 매핑하지 않고 모든 클라이언트 자격 증명에 동일한 기본 사용자에게 매핑되기 때문에 이름 매핑이 필요하지 않습니다.

사용자 이름 매핑만 사용할 수 있으며 그룹에서는 사용할 수 없습니다.

그러나 개별 사용자 그룹을 특정 사용자에게 매핑할 수 있습니다. 예를 들어, 영업이라는 단어가 있는 모든 AD 사용자를 특정 UNIX 사용자 및 사용자의 UID에 매핑할 수 있습니다.

ONTAP에서 사용자에게 대한 자격 증명을 매핑해야 하는 경우 먼저 로컬 이름 매핑 데이터베이스와 LDAP 서버에서 기존 매핑을 확인합니다. SVM의 네임 서비스 구성에 따라 1개 또는 2개 모두를 검사할지 여부를 결정합니다.

- Windows에서 UNIX로의 매핑의 경우

매핑을 찾을 수 없는 경우 ONTAP는 소문자 Windows 사용자 이름이 UNIX 도메인의 유효한 사용자 이름인지 확인합니다. 이렇게 해도 문제가 해결되지 않으면 기본 UNIX 사용자를 사용합니다(구성된 경우). 기본 UNIX 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

- UNIX에서 Windows로의 매핑의 경우

매핑을 찾을 수 없는 경우 ONTAP는 SMB 도메인의 UNIX 이름과 일치하는 Windows 계정을 찾으려고 시도합니다. 이 기능이 작동하지 않으면 기본 SMB 사용자를 사용합니다(구성된 경우). 기본 CIFS 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 가져올 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

컴퓨터 계정은 기본적으로 지정된 기본 UNIX 사용자에게 매핑됩니다. 기본 UNIX 사용자를 지정하지 않으면 컴퓨터 계정 매핑이 실패합니다.

- ONTAP 9.5부터 기본 UNIX 사용자가 아닌 다른 사용자에게 시스템 계정을 매핑할 수 있습니다.
- ONTAP 9.4 이하 버전에서는 시스템 계정을 다른 사용자에게 매핑할 수 없습니다.

컴퓨터 계정에 대한 이름 매핑이 정의되어 있더라도 매핑은 무시됩니다.

UNIX 사용자와 Windows 사용자 이름 간 매핑에 대한 ONTAP SMB 다중 도메인 검색에 대해 알아보십시오

ONTAP는 UNIX 사용자를 Windows 사용자에게 매핑할 때 다중 도메인 검색을 지원합니다. 일치하는 결과가 반환될 때까지 검색된 모든 신뢰할 수 있는 도메인이 대체 패턴과 일치하는 항목을 검색합니다. 또는 검색된 신뢰할 수 있는 도메인 목록 대신 사용되는 기본 신뢰할 수 있는 도메인 목록을 구성할 수 있으며 일치하는 결과가 반환될 때까지 순서대로 검색됩니다.

도메인 트러스트가 UNIX 사용자에게 Windows 사용자 이름 매핑 검색에 미치는 영향

다중 도메인 사용자 이름 매핑의 작동 방식을 이해하려면 ONTAP에서 도메인 트러스트가 작동하는 방식을 이해해야 합니다. CIFS 서버의 홈 도메인과의 Active Directory 트러스트 관계는 양방향 신뢰일 수도 있고 인바운드 트러스트 또는 아웃바운드 트러스트를 포함한 두 가지 단방향 트러스트 유형 중 하나일 수도 있습니다. 홈 도메인은 SVM의 CIFS 서버가 속하는 도메인입니다.

- \_양방향 트러스트 \_

양방향 트러스트를 사용하면 두 도메인이 서로 신뢰합니다. CIFS 서버의 홈 도메인에 다른 도메인과의 양방향 트러스트가 있는 경우 홈 도메인이 신뢰할 수 있는 도메인에 속한 사용자를 인증하고 권한을 부여할 수 있으며 그 반대의 경우도 마찬가지입니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색은 홈 도메인과 다른 도메인 간의 양방향 트러스트가 있는 도메인에서만 수행할 수 있습니다.



• \_아웃바운드 트러스트 \_

아웃바운드 트러스트를 사용하면 홈 도메인이 다른 도메인을 신뢰합니다. 이 경우 홈 도메인이 아웃바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하고 권한을 부여할 수 있습니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 아웃바운드 트러스트가 `_not_sunfre` 검색되었습니다.

• \_인바운드 신뢰 \_

인바운드 트러스트를 사용하면 다른 도메인이 CIFS 서버의 홈 도메인을 신뢰합니다. 이 경우 홈 도메인은 인바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하거나 승인할 수 없습니다.

UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 인바운드 트러스트가 `_not_sound`입니다.

이름 매핑에 대한 다중 도메인 검색을 구성하는 데 와일드카드(\*)를 사용하는 방법

다중 도메인 이름 매핑 검색은 Windows 사용자 이름의 도메인 섹션에서 와일드카드를 사용하여 쉽게 수행할 수 있습니다. 다음 표에서는 이름 매핑 항목의 도메인 부분에서 와일드카드를 사용하여 다중 도메인 검색을 사용하는 방법을 보여 줍니다.

| 패턴 | 교체        | 결과                                                                                                                                                                                                                                                                                  |
|----|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 루트 | • \\ 관리자  | UNIX 사용자 "root"는 "administrator"라는 사용자에게 매핑됩니다. "administrator"라는 이름의 첫 번째 일치하는 사용자를 찾을 때까지 모든 신뢰할 수 있는 도메인을 순서대로 검색합니다.                                                                                                                                                            |
| *  | \\ * \\ * | <p>유효한 UNIX 사용자는 해당 Windows 사용자에게 매핑됩니다. 모든 신뢰할 수 있는 도메인은 해당 이름을 가진 첫 번째 일치하는 사용자를 찾을 때까지 순서대로 검색됩니다.</p> <div>  <p>패턴 \\ * \\ * 은 UNIX에서 Windows로의 이름 매핑에만 유효하며 다른 방법은 사용할 수 없습니다.</p> </div> |

다중 도메인 이름 검색 수행 방법

다음 두 가지 방법 중 하나를 선택하여 다중 도메인 이름 검색에 사용되는 신뢰할 수 있는 도메인 목록을 확인할 수 있습니다.

- ONTAP에서 컴파일한 자동으로 검색된 양방향 트러스트 목록을 사용합니다

- 컴파일하는 신뢰할 수 있는 기본 도메인 목록을 사용합니다

UNIX 사용자가 사용자 이름의 도메인 섹션에 와일드카드를 사용하여 Windows 사용자에게 매핑된 경우 Windows 사용자는 다음과 같이 모든 신뢰할 수 있는 도메인에서 찾을 수 있습니다.

- 선호하는 트러스트된 도메인 목록이 구성되어 있으면 매핑된 Windows 사용자는 이 검색 목록에서만 순서대로 검색됩니다.
- 신뢰할 수 있는 도메인의 기본 설정 목록이 구성되어 있지 않으면 홈 도메인의 모든 양방향 신뢰할 수 있는 도메인에서 Windows 사용자가 표시됩니다.
- 홈 도메인에 대해 양방향으로 신뢰할 수 있는 도메인이 없는 경우 사용자는 홈 도메인에서 표시됩니다.

UNIX 사용자가 사용자 이름의 도메인 섹션이 없는 Windows 사용자에게 매핑된 경우 Windows 사용자는 홈 도메인에서 찾을 수 있습니다.

**ONTAP SMB** 이름 매핑 변환 규칙에 대해 알아보십시오

ONTAP 시스템은 각 SVM에 대해 일련의 변환 규칙을 유지합니다. 각 규칙은 `A_pattern_` 과 `A_replacement_` 의 두 부분으로 구성됩니다. 변환은 적절한 목록의 시작 부분에서 시작하여 첫 번째 일치 규칙을 기반으로 대체를 수행합니다. 이 패턴은 UNIX 형식의 정규식입니다. 대체는 UNIX 'ed' 프로그램과 마찬가지로 패턴에서 부분식을 나타내는 이스케이프 시퀀스를 포함하는 문자열입니다.

**ONTAP SMB** 이름 매핑을 생성합니다

'vserver name-mapping create' 명령을 사용하여 이름 매핑을 생성할 수 있습니다. 이름 매핑을 사용하여 Windows 사용자가 UNIX 보안 스타일 볼륨에 액세스하고 그 반대로 액세스할 수 있습니다.

이 작업에 대해

각 SVM에서 ONTAP은 각 방향에 대해 최대 12,500개의 이름 매핑을 지원합니다.

단계

1. 이름 매핑을 작성하십시오. 'vserver name-mapping create-vserver\_vserver\_name\_-direction{KRB-UNIX|win-unix|unix-win}-position\_integer\_-pattern text-replacement\_text\_'



``-pattern`` 및 ``-replacement`` 문은 정규식으로 공식화할 수 있습니다. 또한 이 문을 사용하여 null 대체 문자열 (공백 문자) 을 사용하여 사용자에 대한 매핑을 명시적으로 거부할 ``" "`` 수도 ``-replacement`` 있습니다. 에 대한 자세한 내용은 ``vserver name-mapping create`` link:<https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html> ["ONTAP 명령 참조입니다"^] 을 참조하십시오.

Windows와 UNIX 간 매핑이 생성될 때 새 매핑이 생성될 때 ONTAP 시스템에 대한 열린 연결이 있는 모든 SMB 클라이언트는 로그아웃했다가 다시 로그인하여 새 매핑을 확인해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 UNIX에서 Windows로의 매핑입니다. 매핑은 UNIX 사용자 johnd를 Windows 사용자 ENG\JohnDoe에 매핑합니다.

```
vs1::> vsriver name-mapping create -vsriver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 Windows에서 UNIX로의 매핑입니다. 여기에는 정규식이 포함됩니다. 매핑은 SVM과 연결된 LDAP 도메인의 사용자에게 도메인 ENG의 모든 CIFS 사용자를 매핑합니다.

```
vs1::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 이 패턴에는 이스케이프해야 하는 Windows 사용자 이름의 요소로 ""\$가 포함됩니다. 매핑은 Windows 사용자 ENG\John\$ops를 UNIX 사용자 John\_ops에 매핑합니다.

```
vs1::> vsriver name-mapping create -direction win-unix -position 1
-pattern ENG\\john$ops
-replacement john_ops
```

기본 **ONTAP SMB** 사용자를 구성합니다

사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우 사용할 기본 사용자를 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 사용자를 구성하지 않아야 합니다.

이 작업에 대해

CIFS 인증의 경우 각 Windows 사용자를 개별 UNIX 사용자에게 매핑하지 않으려면 대신 기본 UNIX 사용자를 지정할 수 있습니다.

NFS 인증의 경우 각 UNIX 사용자를 개별 Windows 사용자에게 매핑하지 않으려면 대신 기본 Windows 사용자를 지정할 수 있습니다.

단계

- 1. 다음 작업 중 하나를 수행합니다.

| 원하는 작업                | 다음 명령을 입력합니다...                                            |
|-----------------------|------------------------------------------------------------|
| 기본 UNIX 사용자를 구성합니다    | 'vsriver cifs options modify-default-unix-user_user_name_' |
| 기본 Windows 사용자를 구성합니다 | 'vsriver nfs modify -default-win-user_user_name_'          |

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

| 원하는 작업                                                                | 이 명령 사용...                                                                                                                        |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 이름 매핑을 생성합니다                                                          | <code>vserver name-mapping create</code>                                                                                          |
| 특정 위치에 이름 매핑을 삽입합니다                                                   | <code>vserver name-mapping insert</code>                                                                                          |
| 이름 매핑을 표시합니다                                                          | <code>vserver name-mapping show</code>                                                                                            |
| 두 이름 매핑의 위치를 교환합니다.<br>참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다. | <code>vserver name-mapping swap</code>                                                                                            |
| 이름 매핑을 수정합니다                                                          | <code>vserver name-mapping modify</code>                                                                                          |
| 이름 매핑을 삭제합니다                                                          | <code>vserver name-mapping delete</code>                                                                                          |
| 올바른 이름 매핑을 확인합니다                                                      | <code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code> |

에 대한 자세한 내용은 `vserver name-mapping` "[ONTAP 명령 참조입니다](#)"를 참조하십시오.

다중 도메인 이름 매핑 검색을 구성합니다

**ONTAP SMB** 다중 도메인 이름 매핑 검색을 사용하거나 사용하지 않도록 설정합니다

다중 도메인 이름 매핑 검색을 사용하면 UNIX 사용자를 Windows 사용자 이름 매핑에 구성할 때 Windows 이름의 도메인 부분에서 와일드 카드(\)를 사용할 수 있습니다. 이름의 도메인 부분에서 와일드카드()를 사용하면 ONTAP에서 CIFS 서버의 컴퓨터 계정이 포함된 도메인과 양방향 트러스트가 있는 모든 도메인을 검색할 수 있습니다.

이 작업에 대해

양방향으로 신뢰할 수 있는 모든 도메인을 검색하는 대신 선호하는 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다. 선호하는 신뢰할 수 있는 도메인 목록이 구성되면 ONTAP는 검색된 양방향으로 신뢰할 수 있는 도메인 대신 선호하는 신뢰할 수 있는 도메인 목록을 사용하여 다중 도메인 이름 매핑 검색을 수행합니다.

- 다중 도메인 이름 매핑 검색은 기본적으로 사용하도록 설정됩니다.
- 이 옵션은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

2. 다음 작업 중 하나를 수행합니다.

| 다중 도메인 이름 매핑 검색을 사용하려는 경우... | 명령 입력...                                                                                                |
|------------------------------|---------------------------------------------------------------------------------------------------------|
| 활성화됨                         | 'vserver cifs options modify<br>-vserver_vserver_name_-is-trusted-domain-enum<br>-search-enabled true'  |
| 사용 안 함                       | 'vserver cifs options modify<br>-vserver_vserver_name_-is-trusted-domain-enum<br>-search-enabled false' |

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

[사용 가능한 서버 옵션](#)

신뢰할 수 있는 **ONTAP SMB** 도메인을 재설정하고 재검색합니다

신뢰할 수 있는 모든 도메인을 강제로 다시 검색할 수 있습니다. 이 기능은 신뢰할 수 있는 도메인 서버가 제대로 응답하지 않거나 트러스트 관계가 변경된 경우에 유용할 수 있습니다. CIFS 서버의 컴퓨터 계정이 포함된 도메인인 홈 도메인과의 양방향 트러스트가 있는 도메인만 검색됩니다.

단계

1. 'vserver cifs domain trusts retrover' 명령을 사용하여 신뢰할 수 있는 도메인을 재설정하고 다시 검색합니다.

```
'vserver cifs domain r트러스트 reDiscover - vserver vs1'
```

관련 정보

[검색된 신뢰할 수 있는 도메인에 대한 정보를 표시합니다](#)

검색된 신뢰할 수 있는 **ONTAP SMB** 도메인에 대한 정보를 표시합니다

CIFS 서버의 컴퓨터 계정이 포함된 도메인인 CIFS 서버의 홈 도메인에 대해 검색된 신뢰할 수 있는 도메인에 대한 정보를 표시할 수 있습니다. 이 기능은 검색된 신뢰할 수 있는 도메인과 검색된 신뢰할 수 있는 도메인 목록 내에서 해당 도메인의 순서가 어떻게 정렬되는지 알고 싶을 때 유용합니다.

이 작업에 대해

홈 도메인과 양방향 트러스트가 있는 도메인만 검색됩니다. 홈 도메인의 DC(도메인 컨트롤러)가 DC에서 결정한 순서대로 신뢰할 수 있는 도메인 목록을 반환하므로 목록 내의 도메인 순서를 예측할 수 없습니다. 신뢰할 수 있는 도메인 목록을 표시하여 다중 도메인 이름 매핑 검색에 대한 검색 순서를 결정할 수 있습니다.

표시된 신뢰할 수 있는 도메인 정보는 노드 및 SVM(스토리지 가상 머신)별로 그룹화됩니다.

단계

1. 'vserver cifs domain trusts show' 명령을 사용하여 검색된 신뢰할 수 있는 도메인에 대한 정보를 표시합니다.

'vserver cifs domain ships ships vs1'이 표시됩니다

```
Node: node1
Vserver: vs1

Home Domain Trusted Domain

EXAMPLE.COM CIFS1.EXAMPLE.COM,
 CIFS2.EXAMPLE.COM
 EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain Trusted Domain

EXAMPLE.COM CIFS1.EXAMPLE.COM,
 CIFS2.EXAMPLE.COM
 EXAMPLE.COM
```

#### 관련 정보

[신뢰할 수 있는 도메인을 다시 설정하고 다시 검색합니다](#)

기본 설정 목록에서 신뢰할 수 있는 **ONTAP SMB** 도메인을 추가, 제거 또는 교체합니다

SMB 서버의 기본 설정 신뢰할 수 있는 도메인 목록에서 신뢰할 수 있는 도메인을 추가하거나 제거하거나 현재 목록을 수정할 수 있습니다. 기본 설정 신뢰할 수 있는 도메인 목록을 구성하는 경우 다중 도메인 이름 매핑 검색을 수행할 때 검색된 양방향 신뢰할 수 있는 도메인 대신 이 목록이 사용됩니다.

#### 이 작업에 대해

- 기존 목록에 신뢰할 수 있는 도메인을 추가하는 경우 새 목록이 기존 목록과 병합되고 끝에 새 항목이 추가됩니다. 신뢰할 수 있는 도메인은 신뢰할 수 있는 도메인 목록에 나타나는 순서대로 검색됩니다.
- 기존 목록에서 신뢰할 수 있는 도메인을 제거하고 목록을 지정하지 않는 경우 지정된 SVM(스토리지 가상 머신)에 대한 신뢰할 수 있는 전체 도메인 목록이 제거됩니다.
- 신뢰할 수 있는 도메인의 기존 목록을 수정하면 새 목록이 기존 목록을 덮어씁니다.



선호하는 트러스트된 도메인 목록에 양방향 트러스트된 도메인만 입력해야 합니다. 기본 도메인 목록에 아웃바운드 또는 인바운드 트러스트 도메인을 입력할 수 있지만 다중 도메인 이름 매핑 검색을 수행할 때는 사용되지 않습니다. ONTAP는 단방향 도메인의 항목을 건너뛰고 목록에서 다음 양방향 신뢰할 수 있는 도메인으로 이동합니다.

#### 단계

1. 다음 작업 중 하나를 수행합니다.

|                                          |                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------|
| 기본 설정 신뢰할 수 있는 도메인 목록을 사용하여 다음을 수행하려면... | 명령 사용...                                                                                         |
| 신뢰할 수 있는 도메인을 목록에 추가합니다                  | 'vserver cifs domain name-mapping-search add-vserver_vserver_name_-trusted-domain FQDN,...'      |
| 목록에서 신뢰할 수 있는 도메인을 제거합니다                 | 'vserver cifs domain name-mapping-search remove-vserver_vserver_name_-trusted-domain FQDN,...']' |
| 기존 목록을 수정합니다                             | 'vserver cifs domain name-mapping-search modify -vserver_vserver_name_-trusted-domain FQDN,...'  |

예

다음 명령을 실행하면 SVM VS1 에서 사용하는 신뢰할 수 있는 도메인 2개(cifs1.example.com 및 cifs2.example.com 추가할 수 있습니다.

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

다음 명령을 실행하면 SVM VS1 에서 사용되는 목록에서 신뢰할 수 있는 도메인 2개가 제거됩니다.

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

다음 명령을 실행하면 SVM VS1 에서 사용하는 신뢰할 수 있는 도메인 목록이 수정됩니다. 새 목록이 원본 목록을 대체합니다.

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

관련 정보

[기본 설정 신뢰할 수 있는 도메인 목록에 대한 정보를 표시합니다](#)

기본 설정 신뢰할 수 있는 **ONTAP SMB** 도메인 목록에 대한 정보를 표시합니다

신뢰할 수 있는 도메인이 기본 설정된 신뢰할 수 있는 도메인 목록에 있는지, 다중 도메인 이름 매핑 검색이 설정된 경우 검색 순서에 대한 정보를 표시할 수 있습니다. 자동으로 검색된 신뢰할 수 있는 도메인 목록을 사용하는 대신 기본 설정 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

| 다음에 대한 정보를 표시하려면...                             | 명령 사용...                                                              |
|-------------------------------------------------|-----------------------------------------------------------------------|
| SVM(스토리지 가상 머신)별로 그룹화된 클러스터의 모든 기본 신뢰할 수 있는 도메인 | 'vserver cifs domain name-mapping-search show'                        |
| 지정된 SVM에서 선호 트러스트된 도메인 모두                       | 'vserver cifs domain name-mapping-search show -vserver_vserver_name_' |

다음 명령을 실행하면 클러스터의 모든 기본 설정 신뢰할 수 있는 도메인에 대한 정보가 표시됩니다.

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver Trusted Domains

vs1 CIFS1.EXAMPLE.COM
```

#### 관련 정보

[선호하는 목록에서 신뢰할 수 있는 도메인을 추가, 제거 또는 교체합니다.](#)

#### SMB 공유를 생성하고 구성합니다

**ONTAP SMB** 공유 생성 및 구성에 대해 자세히 알아보십시오

사용자와 애플리케이션이 SMB를 통해 CIFS 서버의 데이터를 액세스하려면 먼저 볼륨의 명명된 액세스 지점인 SMB 공유를 생성하고 구성해야 합니다. 공유 매개 변수를 지정하고 속성을 공유하여 공유를 사용자 지정할 수 있습니다. 언제든지 기존 공유를 수정할 수 있습니다.

SMB 공유를 생성할 때 ONTAP는 모든 사용자에게 대한 모든 권한 권한이 있는 공유에 대한 기본 ACL을 생성합니다.

SMB 공유는 스토리지 가상 머신(SVM)의 CIFS 서버에 연결됩니다. SVM이 삭제되거나 SMB 공유가 연결된 CIFS 서버가 SVM에서 삭제된 경우 SMB 공유가 삭제됩니다. SVM에서 CIFS 서버를 다시 생성하는 경우 SMB 공유를 다시 생성해야 합니다.

#### 관련 정보

- [로컬 사용자 및 그룹에 대해 알아보세요](#)
- ["Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"](#)
- [볼륨에서 파일 이름 번역을 위한 문자 매핑 구성](#)

기본 관리 **ONTAP SMB** 공유에 대해 알아보십시오

SVM(스토리지 가상 시스템)에서 CIFS 서버를 생성하면 기본 관리 공유가 자동으로 생성됩니다. 이러한 기본 공유가 무엇이고 어떻게 사용되는지 이해해야 합니다.

ONTAP는 CIFS 서버를 생성할 때 다음과 같은 기본 관리 공유를 생성합니다.



ONTAP 9.8부터 관리자\$ 공유는 기본적으로 더 이상 생성되지 않습니다.



- IPC\$
- 관리 비용(ONTAP 9.7 이하 버전에만 해당)
- c\$

\$ 문자로 끝나는 공유는 숨겨진 공유이므로 기본 관리 공유는 내 컴퓨터에서 표시되지 않지만 공유 폴더를 사용하여 볼 수 있습니다.

#### IPC\$ 및 admin\$ 기본 공유가 사용되는 방법입니다

IPC\$ 및 admin\$ 공유는 ONTAP에서 사용되며 Windows 관리자가 SVM에 상주하는 데이터에 액세스하는 데 사용할 수 없습니다.

- IPC\$ 공유입니다

IPC\$ 공유는 프로그램 간 통신에 필수적인 명명된 파이프를 공유하는 리소스입니다. IPC\$ 공유는 컴퓨터의 원격 관리 및 컴퓨터의 공유 리소스를 볼 때 사용됩니다. IPC\$ 공유의 공유 설정, 공유 속성 또는 ACL은 변경할 수 없습니다. IPC\$ 공유의 이름을 바꾸거나 삭제할 수도 없습니다.

- 관리 비용 공유(ONTAP 9.7 이하만 해당)



ONTAP 9.8부터 관리자\$ 공유는 기본적으로 더 이상 생성되지 않습니다.

SVM의 원격 관리 중에 admin\$ 공유가 사용됩니다. 이 리소스의 경로는 항상 SVM 루트로 연결되는 경로입니다. admin\$ 공유에 대한 공유 설정, 공유 속성 또는 ACL은 변경할 수 없습니다. admin\$ 공유의 이름을 바꾸거나 삭제할 수도 없습니다.

#### c\$ 기본 공유가 사용되는 방식

c\$ 공유는 클러스터 또는 SVM 관리자가 SVM 루트 볼륨에 액세스하고 관리하는 데 사용할 수 있는 관리 공유입니다.

c\$ 공유의 특징은 다음과 같습니다.

- 이 공유의 경로는 항상 SVM 루트 볼륨의 경로이며 수정할 수 없습니다.
- c\$ 공유의 기본 ACL은 Administrator/Full Control입니다.

이 사용자는 BUILTIN\administrator입니다. 기본적으로 BUILTIN\관리자는 공유에 매핑하고 매핑된 루트 디렉토리에서 파일 및 폴더를 보거나, 만들거나, 수정하거나, 삭제할 수 있습니다. 이 디렉터리의 파일과 폴더를 관리할 때는 주의해야 합니다.

- c\$ 공유의 ACL을 변경할 수 있습니다.
- c\$ 공유 설정을 변경하고 속성을 공유할 수 있습니다.
- c\$ 공유를 삭제할 수 없습니다.
- SVM 관리자는 네임스페이스 접합을 교차하여 매핑된 c\$ 공유에서 나머지 SVM 네임스페이스에 액세스할 수 있습니다.
- c\$ 공유는 Microsoft 관리 콘솔을 사용하여 액세스할 수 있습니다.

#### 관련 정보

[Windows 보안 탭을 사용하여 고급 파일 권한 구성](#)

SMB 서버에서 SMB 공유를 생성할 때는 ONTAP 공유 이름 지정 요구 사항을 염두에 두어야 합니다.

ONTAP의 공유 명명 규칙은 Windows의 명명 규칙과 동일하며 다음과 같은 요구 사항을 포함합니다.

- 각 공유의 이름은 SMB 서버에 대해 고유해야 합니다.
- 공유 이름은 대/소문자를 구분하지 않습니다.
- 최대 공유 이름 길이는 80자입니다.
- 유니코드 공유 이름이 지원됩니다.
- \$ 문자로 끝나는 공유 이름은 숨겨진 공유입니다.
- ONTAP 9.7 이전 버전의 경우 admin\$, ipc\$ 및 c\$ 관리 공유가 모든 CIFS 서버에서 자동으로 생성되며 예약된 공유 이름이 됩니다. ONTAP 9.8부터는 관리자\$ 공유가 더 이상 자동으로 생성되지 않습니다.
- 공유를 생성할 때 공유 이름 ONTAP\_admin\$(를) 사용할 수 없습니다.
- 공백이 포함된 공유 이름이 지원됩니다.
  - 공유 이름의 첫 문자 또는 마지막 문자로 공백을 사용할 수 없습니다.
  - 공백이 포함된 공유 이름은 따옴표로 묶어야 합니다.



작은따옴표는 공유 이름의 일부로 간주되며 따옴표 대신 사용할 수 없습니다.

- SMB 공유의 이름을 지정할 경우 다음과 같은 특수 문자가 지원됩니다.

! @ # \$ % & ' \_ - . ~ ( ) { }

- SMB 공유의 이름을 지정할 때 다음 특수 문자는 지원되지 않습니다.

\*\* [ ] " / \ : ; | < > , ? \* =

멀티 프로토콜 환경에서 공유를 생성할 때의 **ONTAP SMB** 디렉토리 대소문자 구분 요구사항에 대해 알아보십시오

8.3 명명 체계가 사용되는 SVM에서 공유를 생성하여 이름 간 사례만 차이가 나는 디렉토리 이름을 구별할 경우, 클라이언트가 원하는 디렉토리 경로에 연결되도록 공유 경로에 8.3 이름을 사용해야 합니다.

다음 예에서는 Linux 클라이언트에 ""testdir"" 및 ""testdir""이라는 이름의 디렉토리 두 개가 생성되었습니다. 디렉토리가 포함된 볼륨의 연결 경로는 '/home'입니다. 첫 번째 출력은 Linux 클라이언트에서 출력되고 두 번째 출력은 SMB 클라이언트에서 출력됩니다.

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir
```

```
Directory of Z:\
```

```
04/17/2015 11:23 AM <DIR> testdir
04/17/2015 11:24 AM <DIR> TESTDI~1
```

두 번째 디렉토리에 공유를 생성할 때 공유 경로에 8.3 이름을 사용해야 합니다. 이 예에서 첫 번째 디렉토리의 공유 경로는 "/home/testdir"이고 두 번째 디렉토리의 공유 경로는 "/home/TESTDI~1"입니다.

**SMB** 공유 속성을 사용합니다

**ONTAP SMB** 공유 속성 사용에 대해 자세히 알아보십시오

SMB 공유의 속성을 사용자 지정할 수 있습니다.

사용 가능한 공유 속성은 다음과 같습니다.

| 공유 속성            | 설명                                                                                                                                                                                                    |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oplocks          | 이 속성은 공유에서 클라이언트 측 캐시라고도 하는 편의적 잠금을 사용하도록 지정합니다.                                                                                                                                                      |
| "탐색 가능"          | 이 속성을 사용하면 Windows 클라이언트가 공유를 탐색할 수 있습니다.                                                                                                                                                             |
| '하울스냅샷'          | 이 속성은 클라이언트가 스냅샷을 보고 탐색할 수 있도록 지정합니다.                                                                                                                                                                 |
| '변상강화하는'         | 이 속성은 공유에서 변경 통지 요청을 지원하도록 지정합니다. SVM에서 공유하면 기본 초기 속성이 됩니다.                                                                                                                                           |
| 'attributecache' | 이 속성을 사용하면 SMB 공유의 파일 속성 캐싱을 통해 속성에 더 빠르게 액세스할 수 있습니다. 기본값은 특성 캐싱을 사용하지 않는 것입니다. 이 속성은 SMB 1.0을 통해 공유에 연결하는 클라이언트가 있는 경우에만 사용해야 합니다. 클라이언트가 SMB 2.x 또는 SMB 3.0을 통해 공유에 연결하는 경우에는 이 공유 속성을 사용할 수 없습니다. |

| 공유 속성           | 설명                                                                                                                                                                                                                            |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "계속 사용할 수 있습니다. | 이 속성을 사용하면 SMB 클라이언트가 지속적으로 파일을 열 수 있습니다. 이렇게 열린 파일은 페일오버 및 반환과 같은 운영 중단 이벤트로부터 보호됩니다.                                                                                                                                        |
| 브랜치캐시           | 이 속성은 클라이언트가 이 공유 내의 파일에 대해 BranchCache 해시를 요청할 수 있도록 공유를 지정합니다. 이 옵션은 CIFS BranchCache 구성에서 ""공유당""을 운영 모드로 지정한 경우에만 유용합니다.                                                                                                  |
| '액세스 기반 열거'     | 이 속성은 이 공유에서 Access 기반 열거(ABE)를 사용하도록 지정합니다. 개별 사용자의 액세스 권한에 따라 사용자가 ABE로 필터링된 공유 폴더를 볼 수 있으므로 사용자에게 액세스 권한이 없는 폴더 또는 기타 공유 리소스를 표시할 수 없습니다.                                                                                  |
| 네임스페이스-캐싱       | 이 속성은 이 공유에 연결하는 SMB 클라이언트가 CIFS 서버가 반환하는 디렉터리 열거 결과를 캐시할 수 있도록 지정함으로써 성능을 향상시킬 수 있습니다. 기본적으로 SMB 1 클라이언트는 디렉터리 열거 결과를 캐시하지 않습니다. SMB 2 및 SMB 3 클라이언트는 기본적으로 캐시 디렉터리 열거 결과를 제공하므로 이 공유 속성을 지정하면 SMB 1 클라이언트 연결에만 성능 이점이 있습니다. |
| '암호화-데이터'       | 이 속성은 이 공유에 액세스할 때 SMB 암호화를 사용하도록 지정합니다. SMB 데이터에 액세스할 때 암호화를 지원하지 않는 SMB 클라이언트는 이 공유에 액세스할 수 없습니다.                                                                                                                           |

기존 **ONTAP SMB** 공유에서 공유 속성을 추가하거나 제거합니다

공유 속성을 추가하거나 제거하여 기존 SMB 공유를 사용자 지정할 수 있습니다. 이 기능은 환경의 변화하는 요구 사항에 맞게 공유 구성을 변경하려는 경우에 유용합니다.

시작하기 전에

수정할 속성이 있는 공유가 있어야 합니다.

이 작업에 대해

공유 속성 추가 지침:

- 침표로 구분된 목록을 사용하여 하나 이상의 공유 속성을 추가할 수 있습니다.
- 이전에 지정한 공유 속성은 그대로 유지됩니다.

새로 추가된 속성은 기존 공유 속성 목록에 추가됩니다.

- 공유에 이미 적용된 공유 속성에 새 값을 지정하면 새로 지정한 값이 원래 값을 대체합니다.

- 'vserver cifs share properties add' 명령을 사용하여 공유 속성을 제거할 수 없습니다.

'vserver cifs share properties remove' 명령을 사용하여 공유 속성을 제거할 수 있습니다.

공유 속성 제거 지침:

- 심표로 구분된 목록을 사용하여 하나 이상의 공유 속성을 제거할 수 있습니다.
- 이전에 지정했지만 제거하지 않은 공유 속성은 그대로 유지됩니다.

단계

1. 적절한 명령을 입력합니다.

| 원하는 작업       | 명령 입력...                                                                                                  |
|--------------|-----------------------------------------------------------------------------------------------------------|
| 공유 속성 추가     | 'vserver cifs 공유 속성 add-vserver_vserver_name_-share-name_share_name_-share-properties_,...'               |
| 공유 속성을 제거합니다 | 'vserver CIFS 공유 속성 remove-vserver_vserver_name_-share-name_share_name_-share-properties_properties_,...' |

2. 공유 속성 설정을 확인합니다. 'vserver cifs share show -vserver vserver\_name -share-name share\_name'

예

다음 명령을 실행하면 SVM VS1 에서 "shhowsnapshot" 공유 속성이 "share1"이라는 공유에 추가됩니다.

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver Share Path Properties Comment ACL

vs1 share1 /share1 oplocks - Everyone / Full
Control
 browsable
 changenotify
 showsnapshot
```

다음 명령을 실행하면 SVM VS1 의 "shay2"라는 공유에서 탐색 가능한 공유 속성이 제거됩니다.

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name
share2 -share-properties browsable

cluster1::> vsriver cifs share show -vsriver vs1
```

| Vsriver | Share  | Path    | Properties   | Comment | ACL             |
|---------|--------|---------|--------------|---------|-----------------|
| vs1     | share2 | /share2 | oplocks      | -       | Everyone / Full |
| Control |        |         | changenotify |         |                 |

관련 정보

[공유 관리를 위한 명령](#)

**force-group** 공유 설정을 사용하여 **ONTAP SMB** 사용자 액세스를 최적화합니다

ONTAP 명령줄에서 UNIX 효과적인 보안이 설정된 데이터에 대한 공유를 생성할 때 해당 공유의 SMB 사용자가 생성한 모든 파일이 UNIX 그룹 데이터베이스에서 미리 정의된 그룹이어야 하는 **\_force-group\_**이라는 동일한 그룹에 속하도록 지정할 수 있습니다. **force-group**을 사용하면 다양한 그룹에 속한 SMB 사용자가 파일에 쉽게 액세스할 수 있습니다.

강제 그룹 지정은 공유가 UNIX 또는 혼합 qtree에 있는 경우에만 의미가 있습니다. 이러한 공유의 파일에 대한 액세스는 UNIX GID가 아닌 Windows 권한에 의해 결정되므로 NTFS 볼륨이나 qtree의 공유에 대해 강제 그룹을 설정할 필요가 없습니다.

공유에 대해 **force-group**이 지정된 경우 공유의 다음 내용이 적용됩니다.

- 이 공유에 액세스하는 **force-group**의 SMB 사용자는 **force-group**의 GID로 일시적으로 변경됩니다.
- 이 GID를 사용하면 주 GID 또는 UID로 정상적으로 액세스할 수 없는 이 공유의 파일에 액세스할 수 있습니다.
- SMB 사용자가 생성한 이 공유의 모든 파일은 파일 소유자의 기본 GID에 관계없이 동일한 강제 그룹에 속합니다.

SMB 사용자가 NFS에서 생성된 파일에 액세스하려고 하면 SMB 사용자의 기본 GID가 액세스 권한을 결정합니다.

**force-group**은 NFS 사용자가 이 공유의 파일에 액세스하는 방법에 영향을 주지 않습니다. NFS에서 생성된 파일은 파일 소유자로부터 GID를 가져옵니다. 액세스 권한 결정은 파일에 액세스하려는 NFS 사용자의 UID 및 기본 GID를 기반으로 합니다.

**force-group**을 사용하면 다양한 그룹에 속한 SMB 사용자가 파일에 쉽게 액세스할 수 있습니다. 예를 들어 회사 웹 페이지를 저장하고 엔지니어링 및 마케팅 부서의 사용자에게 쓰기 권한을 부여하기 위해 공유를 만들고 **"webgroup1"** 그룹에 쓰기 권한을 부여할 수 있습니다. 강제 그룹 때문에 이 공유에 있는 SMB 사용자가 만든 모든 파일은 **"webgroup1"** 그룹의 소유입니다. 또한 공유에 액세스할 때 **"webgroup1"** 그룹의 GID가 자동으로 할당됩니다. 따라서 엔지니어링 및 마케팅 부서에서 사용자의 액세스 권한을 관리할 필요 없이 모든 사용자가 이 공유에 쓸 수 있습니다.

관련 정보

[강제 그룹 공유 설정으로 공유 만들기](#)

강제 그룹 공유 설정을 사용하여 **ONTAP SMB** 공유를 생성합니다

UNIX 파일 보안이 설정된 볼륨 또는 Qtree에서 데이터에 액세스하는 SMB 사용자가 ONTAP 동일한 UNIX 그룹에 속한 것으로 간주하도록 하려면 force-group 공유 설정을 사용하여 SMB 공유를 생성할 수 있습니다.

#### 단계

1. SMB 공유: 'vserver cifs share create-vserver\_name\_-share-name\_share\_name\_-path path path -force -group-for-create\_unix\_group\_name\_'을 생성합니다

공유의 UNC 경로('\\\\servername\\sharename\\filepath')에 256자 이상(UNC 경로의 초기 "\" 제외)이 포함되어 있으면 Windows 속성 상자의 \* 보안 \* 탭을 사용할 수 없습니다. 이것은 ONTAP 문제가 아니라 Windows 클라이언트 문제입니다. 이 문제를 방지하려면 256자를 초과하는 UNC 경로를 사용하여 공유를 생성하지 마십시오.

공유가 생성된 후 force 그룹을 제거하려면 언제든지 공유를 수정하고 빈 문자열("")을 "-force-group-for-create" 매개 변수의 값으로 지정할 수 있습니다. 공유를 수정하여 강제 그룹을 제거하는 경우 이 공유에 대한 모든 기존 연결은 이전에 설정된 강제 그룹을 기본 GID로 계속 설정합니다.

#### 예

다음 명령을 실행하면 "/Corp/CompanyInfo" 디렉토리에 웹에서 액세스할 수 있는 ""웹 페이지" 공유가 생성되며, 이 디렉토리에서 SMB 사용자가 생성한 모든 파일이 webgroup1 그룹에 할당됩니다.

```
'vserver cifs share create-vserver vs1-share-name povp-path/corp/CompanyInfo-force-group-for-create webgroup1'
```

#### 관련 정보

[강제 그룹 공유 설정을 사용하여 사용자 액세스 최적화](#)

**MMC**를 사용하여 **ONTAP SMB** 공유에 대한 정보를 봅니다

SVM에서 SMB 공유에 대한 정보를 확인하고 MMC(Microsoft Management Console)를 사용하여 일부 관리 작업을 수행할 수 있습니다. 공유를 보려면 먼저 MMC를 SVM에 연결해야 합니다.

#### 이 작업에 대해

MMC를 사용하여 SVM에 포함된 공유에 대해 다음 작업을 수행할 수 있습니다.

- 공유 보기
- 활성 세션을 봅니다
- 열린 파일을 봅니다
- 시스템의 세션, 파일 및 트리 연결 목록을 열거합니다
- 시스템에서 열려 있는 파일을 닫습니다
- 열려 있는 세션을 닫습니다
- 공유 생성/관리



이전 기능에 의해 표시되는 뷰는 특정 노드에 한정되며 클러스터에는 해당되지 않습니다. 따라서 MMC를 사용하여 SMB 서버 호스트 이름(즉, cifs01.domain.local)에 연결하면 클러스터 내의 단일 LIF로 DNS를 설정한 방법에 따라 라우팅됩니다.

ONTAP용 MMC에서는 다음 기능이 지원되지 않습니다.

- 새 로컬 사용자/그룹을 생성합니다
- 기존 로컬 사용자/그룹 관리/보기
- 이벤트 또는 성능 로그 보기
- 스토리지
- 서비스 및 애플리케이션

작업이 지원되지 않는 경우, remote procedure call failed' 오류가 발생할 수 있습니다.

### "FAQ: ONTAP에서 Windows MMC 사용"

단계

1. Windows 서버에서 컴퓨터 관리 MMC를 열려면 \* 제어판 \* 에서 \* 관리 도구 \* > \* 컴퓨터 관리 \* 를 선택합니다.
2. 작업 \* > \* 다른 컴퓨터에 연결 \* 을 선택합니다.

컴퓨터 선택 대화 상자가 나타납니다.

3. 스토리지 시스템의 이름을 입력하거나 \* Browse \* 를 클릭하여 스토리지 시스템을 찾습니다.
4. 확인 \* 을 클릭합니다.

MMC를 SVM에 연결합니다.

5. 탐색 창에서 \* 공유 폴더 \* > \* 공유 \* 를 클릭합니다.

SVM의 공유 목록이 오른쪽 표시 창에 표시됩니다.

6. 공유의 공유 속성을 표시하려면 공유를 두 번 클릭하여 \* 속성 \* 대화 상자를 엽니다.
7. MMC를 사용하여 스토리지 시스템에 접속할 수 없는 경우 스토리지 시스템에서 다음 명령 중 하나를 사용하여 BUILTIN\Administrators 그룹 또는 BUILTIN\Power Users 그룹에 사용자를 추가할 수 있습니다.

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

### SMB 공유를 관리하기 위한 ONTAP 명령

'vserver cifs share' 및 'vserver cifs share properties' 명령을 사용하여 SMB 공유를 관리할 수 있습니다.



| 원하는 작업               | 이 명령 사용...                                              |
|----------------------|---------------------------------------------------------|
| SMB 공유를 생성합니다        | 'vserver cifs share create'                             |
| SMB 공유를 표시합니다        | 'vserver cifs share show'를 선택합니다                        |
| SMB 공유를 수정합니다        | 'vserver cifs share modify'를 선택합니다                      |
| SMB 공유를 삭제합니다        | 'vserver cifs share delete'                             |
| 기존 공유에 공유 속성을 추가합니다  | 'vserver cifs share properties add'를 선택합니다              |
| 기존 공유에서 공유 속성을 제거합니다 | 'vserver cifs share properties remove(가상 CIFS 공유 속성 제거) |
| 공유 속성에 대한 정보를 표시합니다  | 'vserver cifs share properties show'를 선택합니다             |

에 대한 자세한 내용은 `vserver cifs` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

## SMB 공유 ACL을 사용하여 파일 액세스 보호

ONTAP SMB 공유 레벨 ACL 관리에 대해 자세히 알아보십시오

공유 수준 ACL을 변경하여 사용자에게 공유에 대한 액세스 권한을 더 많이 또는 덜 부여할 수 있습니다. Windows 사용자 및 그룹 또는 UNIX 사용자 및 그룹을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

기본적으로 공유 수준 ACL은 Everyone이라는 표준 그룹에 모든 권한을 부여합니다. ACL에 대한 모든 제어 기능은 도메인 및 모든 신뢰할 수 있는 도메인의 모든 사용자가 공유에 대한 모든 액세스 권한을 갖는다는 것을 의미합니다. Windows 클라이언트의 Microsoft Management Console(MMC)이나 ONTAP 명령줄을 사용하여 공유 수준 ACL에 대한 액세스 수준을 제어할 수 있습니다. ["공유 액세스 제어 목록 만들기"](#)..

MMC를 사용할 때 다음 지침이 적용됩니다.

- 지정된 사용자 및 그룹 이름은 Windows 이름이어야 합니다.
- Windows 권한만 지정할 수 있습니다.

ONTAP 명령줄을 사용할 때 다음 지침이 적용됩니다.

- 지정된 사용자 및 그룹 이름은 Windows 이름 또는 UNIX 이름일 수 있습니다.

ACL을 생성하거나 수정할 때 사용자 및 그룹 유형을 지정하지 않으면 기본 유형은 Windows 사용자 및 그룹입니다.

- Windows 권한만 지정할 수 있습니다.

ONTAP SMB 공유 액세스 제어 목록을 생성합니다

SMB 공유에 대한 ACL(액세스 제어 목록)을 생성하여 공유 권한을 구성하면 사용자 및 그룹의

공유에 대한 액세스 수준을 제어할 수 있습니다.

이 작업에 대해

로컬 또는 도메인 Windows 사용자 또는 그룹 이름 또는 UNIX 사용자 또는 그룹 이름을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

새 ACL을 생성하기 전에 보안 위험을 야기시키는 기본 공유 ACL 'Everyone/Full Control'을 삭제해야 합니다.

워크그룹 모드에서 로컬 도메인 이름은 SMB 서버 이름입니다.

단계

1. 기본 공유 ACL인 'vserver cifs share access-control delete-vserver <vserver\_name>-share <share\_name>-user-or-group everyone'을 삭제하십시오
2. 새 ACL 구성:

| 을 사용하여 <b>ACL</b> 을 구성하려면... | 명령 입력...                                                                                                                                                                                                                                        |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 사용자                  | <pre>vserver cifs share access-control<br/>create -vserver &lt;vserver_name&gt; -share<br/>&lt;share_name&gt; -user-group-type windows<br/>-user-or-group<br/>&lt;Windows_domain_name\user_name&gt;<br/>-permission &lt;access_right&gt;</pre>  |
| Windows 그룹                   | <pre>vserver cifs share access-control<br/>create -vserver &lt;vserver_name&gt; -share<br/>&lt;share_name&gt; -user-group-type windows<br/>-user-or-group<br/>&lt;Windows_domain_name\group_name&gt;<br/>-permission &lt;access_right&gt;</pre> |
| Unix 사용자입니다                  | <pre>vserver cifs share access-control<br/>create -vserver &lt;vserver_name&gt; -share<br/>&lt;share_name&gt; -user-group-type &lt;unix-<br/>user&gt; -user-or-group &lt;UNIX_user_name&gt;<br/>-permission &lt;access_right&gt;</pre>          |
| Unix 그룹                      | <pre>vserver cifs share access-control<br/>create -vserver &lt;vserver_name&gt; -share<br/>&lt;share_name&gt; -user-group-type &lt;unix-<br/>group&gt; -user-or-group<br/>&lt;UNIX_group_name&gt; -permission<br/>&lt;access_right&gt;</pre>    |

3. 'vserver cifs share access-control show' 명령을 사용하여 공유에 적용된 ACL이 올바른지 확인하십시오.

예

다음 명령을 실행하면 이 표시됩니다 Change "vs1.example.com" SVM에서 "Sales" 공유를 위한 "Sales Team" Windows 그룹에 대한 권한:

```
cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vsserver cifs share access-control show -vsserver
vs1.example.com
```

| Vserver         | Share Name | User/Group Name        | User/Group Type | Access Permission |
|-----------------|------------|------------------------|-----------------|-------------------|
| vs1.example.com | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs1.example.com | sales      | DOMAIN\Sales Team      | windows         | Change            |

다음 명령을 실행하면 Read "vs2.example.com" SVM의 "eng" 공유에 대한 "engineering" UNIX 그룹에 대한 권한이 부여됩니다.

```
cluster1::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

| Vserver         | Share Name | User/Group Name        | User/Group Type | Access Permission |
|-----------------|------------|------------------------|-----------------|-------------------|
| vs2.example.com | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs2.example.com | eng        | engineering            | unix-group      | Read              |

다음 명령은 Change "Tiger Team"이라는 로컬 Windows 그룹에 Full\_Control 대한 권한을 부여하고 "VS1" SVM에서 "datavol5" 공유에 대해 "Sue Chang"이라는 로컬 Windows 사용자에게 권한을 부여합니다.

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

| Vsriver | Share Name | User/Group Name        | User/Group Type | Access Permission |
|---------|------------|------------------------|-----------------|-------------------|
| vs1     | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs1     | datavol5   | Tiger Team             | windows         | Change            |
| vs1     | datavol5   | Sue Chang              | windows         | Full_Control      |

**SMB** 공유 액세스 제어 목록을 관리하기 위한 **ONTAP** 명령

**SMB ACL**(액세스 제어 목록)을 관리하기 위한 명령을 알아야 합니다. 여기에는 **ACL** 생성, 표시, 수정 및 삭제가 포함됩니다.

| 원하는 작업       | 이 명령 사용...                                         |
|--------------|----------------------------------------------------|
| 새 ACL을 생성합니다 | 'vsriver cifs share access-control create'         |
| ACL을 표시합니다   | 'vsriver cifs share access-control show'를 참조하십시오   |
| ACL을 수정합니다   | 'vsriver cifs share access-control modify'를 참조하십시오 |
| ACL을 삭제한다    | 'vsriver cifs share access-control delete'         |

파일 권한을 사용하여 파일 액세스를 보호합니다

**ONTAP SMB SVM**에 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 | <p>a. 추가 * 를 클릭합니다.</p> <p>b. 선택할 개체 이름 입력 * 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다.</p> <p>c. 확인 * 을 클릭합니다.</p> |

|                                 |                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------|
| 원하는 작업                          | 다음을 수행합니다.                                                                       |
| 사용자 또는 그룹의 고급 NTFS 권한을 변경합니다    | a. 사용 권한 항목: * 상자에서 고급 사용 권한을 변경할 사용자 또는 그룹을 선택합니다.<br>b. 편집 * 을 클릭합니다.          |
| 사용자 또는 그룹에 대한 고급 NTFS 권한을 제거합니다 | a. 사용 권한 항목: * 상자에서 제거할 사용자 또는 그룹을 선택합니다.<br>b. 제거 * 를 클릭합니다.<br>c. 13단계로 건너뛵니다. |

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.



## DAC(Dynamic Access Control)를 사용하여 파일 액세스 보안

ONTAP SMB 서버에 대한 DAC 파일 액세스 보안에 대해 알아보세요

동적 액세스 제어를 사용하고 Active Directory에서 중앙 액세스 정책을 생성한 후 적용된 GPO(그룹 정책 개체)를 통해 SVM의 파일 및 폴더에 적용하여 액세스를 보호할 수 있습니다. 중앙 액세스 정책 스테이징 이벤트를 사용하여 변경 내용을 적용하기 전에 중앙 액세스 정책에 대한 영향을 확인할 수 있도록 감사를 구성할 수 있습니다.

### CIFS 자격 증명에 추가

동적 액세스 제어 전에 CIFS 자격 증명에는 보안 주체(사용자의) ID와 Windows 그룹 구성원이 포함되어 있습니다. 동적 액세스 제어를 사용하면 디바이스 ID, 디바이스 클레임 및 사용자 클레임을 비롯한 세 가지 유형의 정보가 자격 증명에 추가됩니다.

- 장치 ID

사용자가 로그인하는 장치의 ID 및 그룹 멤버십은 제외하고 사용자의 ID 정보의 아날로그.

- 장치 요청

장치 보안 주체에 대한 어설션. 예를 들어 장치 클레임은 특정 OU의 구성원일 수 있습니다.

- 사용자 클레임

사용자 보안 주체에 대한 어설션. 예를 들어 사용자 클레임은 AD 계정이 특정 OU의 구성원일 수 있습니다.

### 중앙 액세스 정책

파일에 대한 중앙 액세스 정책을 사용하면 조직에서 사용자 그룹, 사용자 클레임, 장치 클레임 및 리소스 속성을 사용하는 조건부 식을 포함하는 인증 정책을 중앙에서 배포하고 관리할 수 있습니다.

예를 들어, 비즈니스에 큰 영향을 미치는 데이터에 액세스하려면 정규직 직원이어야 하며 관리되는 장치의 데이터만 액세스할 수 있어야 합니다. 중앙 액세스 정책은 Active Directory에서 정의되고 GPO 메커니즘을 통해 파일 서버로 배포됩니다.

### 고급 감사를 통한 중앙 액세스 정책 스테이징

중앙 액세스 정책은 '성질'일 수 있으며, 이 경우 파일 액세스 검사 중에 "what-if" 방식으로 평가됩니다. 정책이 적용된 경우 어떤 결과가 발생했는지, 현재 구성된 것과 어떻게 다른 결과가 감사 이벤트로 기록됩니다. 이렇게 하면 관리자가 감사 이벤트 로그를 사용하여 실제로 정책을 적용하기 전에 액세스 정책 변경의 영향을 확인할 수 있습니다. 액세스 정책 변경의 영향을 평가한 후 GPO를 통해 원하는 SVM에 정책을 배포할 수 있습니다.

### 관련 정보

- [지원되는 GPO에 대해 알아보세요](#)
- [SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.](#)
- [서버에서 GPO 지원 활성화 또는 비활성화](#)
- [GPO 구성에 대한 정보를 표시합니다](#)
- [중앙 액세스 정책에 대한 정보를 표시합니다](#)

- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다
- 서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다.
- 서버 보안에 대한 정보 표시
- "SMB 및 NFS 감사 및 보안 추적"

ONTAP SMB 서버에 지원되는 DAC 기능

CIFS 서버에서 DAC(동적 액세스 제어)를 사용하려면 ONTAP가 Active Directory 환경에서 동적 액세스 제어 기능을 지원하는 방법을 이해해야 합니다.

동적 액세스 제어에 지원됩니다

ONTAP는 CIFS 서버에서 동적 액세스 제어가 설정된 경우 다음 기능을 지원합니다.

| 기능                                        | 설명                                                                                                                                                                                                               |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 파일 시스템에 대한 클레임입니다                         | 청구는 사용자에게 대한 일부 진실을 나타내는 간단한 이름 및 값 쌍입니다. 사용자 자격 증명에는 클레임 정보가 포함되며 파일의 보안 설명자는 클레임 검사에 포함된 액세스 검사를 수행할 수 있습니다. 따라서 관리자는 파일에 액세스할 수 있는 사용자를 보다 세밀하게 제어할 수 있습니다.                                                   |
| 파일 액세스 검사에 대한 조건식입니다                      | 파일의 보안 매개 변수를 수정할 때 사용자는 임의로 복잡한 조건식을 파일의 보안 설명자에 추가할 수 있습니다. 조건부 표현식에는 클레임 확인이 포함될 수 있습니다.                                                                                                                      |
| 중앙 액세스 정책을 통해 파일 액세스를 중앙 집중식으로 제어         | 중앙 액세스 정책은 파일에 태그를 지정할 수 있는 Active Directory에 저장된 일종의 ACL입니다. 디스크에 있는 보안 설명자와 태그가 지정된 중앙 액세스 정책 모두의 액세스 검사가 액세스를 허용하는 경우에만 파일에 대한 액세스가 부여됩니다. 따라서 관리자는 디스크의 보안 설명자를 수정하지 않고도 중앙 위치(AD)에서 파일에 대한 액세스를 제어할 수 있습니다. |
| 중앙 액세스 정책 스테이징                            | 중앙 액세스 정책의 "변경"을 통해 실제 파일 액세스에 영향을 주지 않고 보안 변경 사항을 시도하는 기능을 추가하고 감사 보고서에서 변경 효과를 확인할 수 있습니다.                                                                                                                     |
| ONTAP CLI를 사용하여 중앙 액세스 정책 보안에 대한 정보 표시 지원 | 'vserver security file-directory show' 명령을 확장하여 적용된 중앙 액세스 정책에 대한 정보를 표시합니다.                                                                                                                                     |
| 중앙 액세스 정책을 포함하는 보안 추적                     | 적용된 중앙 액세스 정책에 대한 정보가 포함된 결과를 표시하도록 'vserver security trace' 명령 제품군을 확장합니다.                                                                                                                                      |

동적 액세스 제어에 지원되지 않습니다

CIFS 서버에서 동적 액세스 제어가 설정된 경우 ONTAP은 다음 기능을 지원하지 않습니다.

| 기능                       | 설명                                                   |
|--------------------------|------------------------------------------------------|
| NTFS 파일 시스템 객체의 자동 분류    | 이 확장명은 ONTAP에서 지원되지 않는 Windows 파일 분류 인프라스트럭처의 확장입니다. |
| 중앙 액세스 정책 스테이징 이외의 고급 감사 | 고급 감사를 위해 중앙 액세스 정책 스테이징만 지원됩니다.                     |

ONTAP SMB 서버에서 DAC 및 중앙 액세스 정책을 사용하는 방법에 대해 알아보세요.

DAC(Dynamic Access Control) 및 중앙 액세스 정책을 사용하여 CIFS 서버의 파일과 폴더를 보호할 때 고려해야 할 몇 가지 사항이 있습니다.

정책 규칙이 **DOMAIN\administrator** 사용자에게 적용되는 경우 **NFS** 액세스가 루트에 대해 거부될 수 있습니다

특정 상황에서는 루트 사용자가 액세스하려는 데이터에 중앙 액세스 정책 보안이 적용될 때 루트에 대한 NFS 액세스가 거부될 수 있습니다. 이 문제는 중앙 액세스 정책에 도메인\관리자에게 적용되는 규칙이 포함되어 있고 루트 계정이 도메인관리자 계정에 매핑된 경우에 발생합니다.

도메인관리자 사용자에게 규칙을 적용하는 대신 도메인관리자 그룹과 같은 관리 권한이 있는 그룹에 규칙을 적용해야 합니다. 이렇게 하면 이 문제의 근본 영향을 받지 않고 root를 domain\administrator 계정에 매핑할 수 있습니다.

**Active Directory**에서 적용된 중앙 액세스 정책을 찾을 수 없는 경우 **CIFS** 서버의 **BUILTIN\Administrators** 그룹에 리소스에 대한 액세스 권한이 있습니다

CIFS 서버에 포함된 리소스에 중앙 액세스 정책이 적용될 수 있지만 CIFS 서버가 중앙 액세스 정책의 SID를 사용하여 Active Directory에서 정보를 검색하려고 하면 SID가 Active Directory의 기존 중앙 액세스 정책 SID와 일치하지 않습니다. 이러한 경우 CIFS 서버는 해당 리소스에 대한 로컬 기본 복구 정책을 적용합니다.

로컬 기본 복구 정책을 사용하면 CIFS 서버의 BUILTIN\Administrators 그룹이 해당 리소스에 액세스할 수 있습니다.

ONTAP SMB 서버에 대한 DAC 활성화 또는 비활성화

DAC(Dynamic Access Control)를 사용하여 CIFS 서버의 객체를 보호할 수 있는 옵션은 기본적으로 해제되어 있습니다. CIFS 서버에서 동적 액세스 제어를 사용하려면 이 옵션을 설정해야 합니다. 나중에 동적 액세스 제어를 사용하여 CIFS 서버에 저장된 객체를 보호하지 않으려는 경우 이 옵션을 해제할 수 있습니다.

Active Directory에서 동적 액세스 제어를 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

["Microsoft TechNet: 동적 액세스 제어 시나리오 개요"](#)

이 작업에 대해

동적 액세스 제어가 설정되면 파일 시스템에 동적 액세스 제어 관련 항목이 있는 ACL이 포함될 수 있습니다. 동적 액세스 제어를 사용하지 않으면 현재 동적 액세스 제어 항목은 무시되고 새 항목은 허용되지 않습니다.

이 옵션은 고급 권한 수준에서만 사용할 수 있습니다.

#### 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

| 동적 액세스 제어를 원하는 경우... | 명령 입력...                                                                     |
|----------------------|------------------------------------------------------------------------------|
| 활성화됨                 | 'vserver cifs options modify<br>-vserver_vserver_name_-is-dac-enabled true'  |
| 사용 안 함               | 'vserver cifs options modify<br>-vserver_vserver_name_-is-dac-enabled false' |

3. 관리자 권한 수준으로 복귀: 'Set-Privilege admin

#### 관련 정보

서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다.

**ONTAP SMB** 서버에서 **DAC**가 비활성화된 경우 **DAC ACE**가 포함된 **ACL** 관리

동적 액세스 제어 ACE로 ACL이 적용된 리소스가 있고 SVM(스토리지 가상 시스템)에서 동적 액세스 제어를 사용하지 않도록 설정한 경우 해당 리소스에서 비 동적 액세스 제어 ACE를 관리하기 전에 동적 액세스 제어 ACE를 제거해야 합니다.

#### 이 작업에 대해

동적 액세스 제어를 사용하지 않도록 설정한 후에는 기존 동적 액세스 제어 ACE를 제거하거나 기존 동적 액세스 제어 ACE를 제거해야 새로운 비 동적 액세스 제어 ACE를 추가할 수 있습니다.

일반적으로 ACL을 관리하는 데 사용하는 툴을 사용하여 이러한 단계를 수행할 수 있습니다.

#### 단계

1. 리소스에 적용되는 동적 액세스 제어 ACE를 결정합니다.
2. 리소스에서 동적 액세스 제어 ACE를 제거합니다.
3. 리소스에서 원하는 대로 비 동적 액세스 제어 ACE를 추가하거나 제거합니다.

**ONTAP SMB** 서버의 데이터를 보호하기 위한 중앙 액세스 정책 구성

CIFS 서버에서 DAC(Dynamic Access Control) 활성화, Active Directory에서 중앙 액세스 정책 구성, GPO를 사용하여 Active Directory 컨테이너에 중앙 액세스 정책 적용 등 중앙 액세스 정책을 사용하여 CIFS 서버의 데이터에 안전하게 액세스하기 위해 수행해야 하는 몇 가지 단계가 있습니다. 그리고 CIFS 서버에서 GPO를 사용하도록 설정합니다.

#### 시작하기 전에

- 중앙 액세스 정책을 사용하도록 Active Directory를 구성해야 합니다.
- 중앙 액세스 정책을 만들고 CIFS 서버가 포함된 컨테이너에 GPO를 만들고 적용하려면 Active Directory 도메인

컨트롤러에 대한 충분한 액세스 권한이 있어야 합니다.

- 필요한 명령을 실행하려면 SVM(스토리지 가상 머신)에 대한 충분한 관리 액세스 권한이 있어야 합니다.

이 작업에 대해

중앙 액세스 정책은 Active Directory의 GPO(그룹 정책 개체)에 정의되고 적용됩니다. Active Directory의 중앙 액세스 정책을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

#### "Microsoft TechNet: 중앙 액세스 정책 시나리오"

단계

1. "vserver cifs options modify" 명령을 사용하여 아직 활성화되지 않은 SVM에서 동적 액세스 제어를 활성화하십시오.

```
'vserver cifs options modify -vserver vs1-is-dac-enabled true'
```

2. "vserver cifs group-policy modify" 명령을 사용하여 CIFS 서버가 아직 설정되지 않은 경우 CIFS 서버에서 GPO(그룹 정책 개체)를 사용하도록 설정합니다.

```
'vserver cifs group-policy modify - vserver vs1-status enabled'
```

3. Active Directory에 중앙 액세스 규칙 및 중앙 액세스 정책을 생성합니다.
4. GPO(그룹 정책 개체)를 만들어 Active Directory에 중앙 액세스 정책을 배포합니다.
5. CIFS 서버 컴퓨터 계정이 있는 컨테이너에 GPO를 적용합니다.
6. 'vserver cifs group-policy update' 명령을 사용하여 CIFS 서버에 적용된 GPO를 수동으로 업데이트합니다.

```
'vserver cifs group-policy update-vserver vs1'을 선택합니다
```

7. "vserver cifs group-policy show-applied" 명령을 사용하여 GPO 중앙 액세스 정책이 CIFS 서버의 리소스에 적용되는지 확인합니다.

다음 예에서는 기본 도메인 정책에 CIFS 서버에 적용되는 두 가지 중앙 액세스 정책이 있음을 보여 줍니다.

```
'vserver cifs group-policy show-applied'
```

```
Vserver: vs1

GPO Name: Default Domain Policy
Level: Domain
Status: enabled
Advanced Audit Settings:
Object Access:
Central Access Policy Staging: failure
Registry Settings:
Refresh Time Interval: 22
Refresh Random Offset: 8
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache: all-versions
Security Settings:
```

```
Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
File Security:
 /vol1/home
 /vol1/dir1
Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
```

```

File Security:
 /vol1/home
 /vol1/dir1
Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2
2 entries were displayed.

```

#### 관련 정보

- [SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.](#)
- [GPO 구성에 대한 정보를 표시합니다](#)
- [중앙 액세스 정책에 대한 정보를 표시합니다](#)
- [중앙 액세스 정책 규칙에 대한 정보를 표시합니다](#)
- [서버에 대한 DAC 활성화 또는 비활성화](#)

#### ONTAP SMB 서버의 DAC 보안에 대한 정보 표시

DAC(Dynamic Access Control) 보안에 대한 정보를 NTFS 볼륨과 NTFS 유효 보안 데이터가 혼합된 보안 스타일 볼륨에서 표시할 수 있습니다. 여기에는 조건부 ACE, 리소스 ACE 및 중앙 액세스 정책 ACE에 대한 정보가 포함됩니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

#### 이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

## 단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

| 정보를 표시하려면...                                                | 다음 명령을 입력합니다...                                                                                |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| 요약 양식                                                       | 'vserver security file-directory show -vserver vserver_name -path path path'                   |
| 세부 정보가 확장됩니다                                                | 'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true' |
| 여기서 출력은 그룹 및 사용자 SID와 함께 표시됩니다                              | 'vserver security file-directory show -vserver vserver_name -path path -lookup-names false'    |
| 16진수 비트 마스크가 텍스트 형식으로 변환되는 파일과 디렉터리의 파일 및 디렉터리 보안에 대해 설명합니다 | 'vserver security file-directory show -vserver vserver_name -path path path -텍스트 마스크 true'     |

## 예

다음 예제는 SVM VS1 경로의 동적 액세스 제어 보안 정보 /vol1 을 보여줍니다.



```

cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
 Vserver: vs1
 File Path: /vol1
 File Inode Number: 112
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attribute: -
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0xbf14
 Owner:CIFS1\Administrator
 Group:CIFS1\Domain Admins
 SACL - ACEs
 ALL-Everyone-0xf01ff-OI|CI|SA|FA
 RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
 POLICY ID-All resources - No Write-
0x0-OI|CI

 DACL - ACEs
 ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI

 ALLOW-Everyone-0x1f01ff-OI|CI
 ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)

```

#### 관련 정보

- [GPO 구성에 대한 정보를 표시합니다](#)
- [중앙 액세스 정책에 대한 정보를 표시합니다](#)
- [중앙 액세스 정책 규칙에 대한 정보를 표시합니다](#)

#### ONTAP SMB 서버의 DAC에 대한 고려 사항 되돌리기

DAC(동적 액세스 제어)를 지원하지 않는 ONTAP 버전으로 되돌릴 경우 어떤 일이 발생할지, 되돌리기 전과 후에 무엇을 해야 하는지 알고 있어야 합니다.

하나 이상의 SVM(스토리지 가상 머신)에서 동적 액세스 제어와 동적 액세스 제어를 지원하지 않는 ONTAP 버전으로

클러스터를 되돌리려면 되돌리기 전에 다음을 수행해야 합니다.

- 클러스터에서 활성화된 모든 SVM에서 동적 액세스 제어를 해제해야 합니다.
- "file-op" 이벤트 유형만 사용하려면 "cap-staging" 이벤트 유형이 포함된 클러스터의 감사 구성을 수정해야 합니다.

동적 액세스 제어 ACE가 있는 파일 및 폴더에 대한 몇 가지 중요한 복원 고려 사항을 이해하고 이에 대한 조치를 취해야 합니다.

- 클러스터를 되돌린 경우 기존 동적 액세스 제어 ACE는 제거되지 않지만 파일 액세스 검사에서는 무시됩니다.
- 동적 액세스 제어 ACE는 재버전 후에 무시되므로 동적 액세스 제어 ACE가 있는 파일에서 파일에 대한 액세스가 변경됩니다.

이렇게 하면 사용자가 이전에는 액세스할 수 없었던 파일에 액세스하거나 이전에 액세스할 수 없었던 파일에 액세스할 수 있습니다.

- 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용하여 이전 보안 수준을 복원해야 합니다.

되돌리기 전에 또는 다시 버전이 완료된 직후 작업을 수행할 수 있습니다.



동적 액세스 제어 ACE는 다시 버전 변경 후 무시되므로 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용할 때 제거할 필요가 없습니다. 그러나 필요한 경우 수동으로 제거할 수 있습니다.

내보내기 정책을 사용하여 **SMB** 액세스를 보호합니다

**ONTAP SMB** 액세스를 통한 내보내기 정책 사용에 대해 알아보세요

SMB 서버에서 SMB 액세스에 대한 익스포트 정책을 사용하는 경우, SMB 클라이언트에서 SVM 볼륨에 대한 액세스를 제어할 때 익스포트 정책이 사용됩니다. 데이터에 액세스하려면 SMB 액세스를 허용하는 익스포트 정책을 생성한 다음, SMB 공유를 포함하는 볼륨과 정책을 연결할 수 있습니다.

내보내기 정책에는 데이터에 대한 액세스가 허용되는 클라이언트와 읽기 전용 및 읽기-쓰기 액세스에 지원되는 인증 프로토콜을 지정하는 하나 이상의 규칙이 적용됩니다. 모든 클라이언트, 클라이언트 서브넷 또는 특정 클라이언트에 대한 SMB 액세스를 허용하고 Kerberos 인증, NTLM 인증 또는 데이터에 대한 읽기 전용 및 읽기-쓰기 액세스를 결정할 때 Kerberos 및 NTLM 인증을 사용하여 인증을 허용하도록 내보내기 정책을 구성할 수 있습니다.

내보내기 정책에 적용된 모든 내보내기 규칙을 처리한 후 ONTAP는 클라이언트에 액세스 권한이 부여되었는지 여부와 허용되는 액세스 수준을 결정할 수 있습니다. 내보내기 규칙은 Windows 사용자 및 그룹이 아니라 클라이언트 컴퓨터에 적용됩니다. 내보내기 규칙은 Windows 사용자 및 그룹 기반 인증 및 권한 부여를 대체하지 않습니다. 내보내기 규칙은 공유 및 파일 액세스 권한 외에도 액세스 보안의 또 다른 계층을 제공합니다.

볼륨에 대한 클라이언트 액세스를 구성하기 위해 각 볼륨에 정확히 하나의 익스포트 정책을 연결합니다. 각 SVM에는 여러 익스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨이 있는 SVM에 대해 다음을 수행할 수 있습니다.

- SVM의 각 볼륨에 서로 다른 익스포트 정책을 지정하여 개별 클라이언트 액세스 제어를 SVM의 각 볼륨에 할당
- 각 볼륨에 대해 새로운 익스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨에 동일한 익스포트 정책을 할당합니다.

각 SVM에는 규칙이 없는 "기본값"이라는 익스포트 정책이 하나 이상 있습니다. 이 익스포트 정책을 삭제할 수는 없지만 이름을 바꾸거나 수정할 수는 있습니다. 기본적으로 SVM의 각 볼륨은 기본 익스포트 정책과 연결됩니다. SVM에서

SMB 액세스에 대한 익스포트 정책을 사용하지 않도록 설정한 경우, "기본값" 익스포트 정책은 SMB 액세스에 영향을 미치지 않습니다.

NFS 및 SMB 호스트 모두에 대한 액세스를 제공하는 규칙을 구성하고 이 규칙을 익스포트 정책에 연결할 수 있습니다. 그런 다음, NFS 및 SMB 호스트 모두에 액세스해야 하는 데이터가 포함된 볼륨에 연결할 수 있습니다. 또는 SMB 클라이언트만 액세스해야 하는 일부 볼륨이 있는 경우, SMB 프로토콜을 사용해서만 액세스를 허용하고 읽기 전용 및 쓰기 액세스에 Kerberos 또는 NTLM(또는 둘 다)만 사용하는 규칙을 사용하여 익스포트 정책을 구성할 수 있습니다. 그러면 익스포트 정책이 SMB 액세스만 원하는 볼륨에 연결됩니다.

SMB에 대한 익스포트 정책이 설정되어 있고 클라이언트가 해당 익스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우, 요청이 실패하고 권한 거부 메시지가 표시됩니다. 클라이언트가 볼륨의 익스포트 정책에 있는 규칙과 일치하지 않으면 액세스가 거부됩니다. 내보내기 정책이 비어 있으면 모든 액세스가 암시적으로 거부됩니다. 공유 및 파일 권한이 액세스를 허용하는 경우에도 마찬가지입니다. 즉, SMB 공유가 포함된 볼륨에서 다음을 최소한으로 허용하도록 익스포트 정책을 구성해야 합니다.

- 모든 클라이언트 또는 적절한 클라이언트 하위 집합에 대한 액세스를 허용합니다
- SMB를 통한 액세스를 허용합니다
- Kerberos 또는 NTLM 인증(또는 둘 다)을 사용하여 적절한 읽기 전용 및 쓰기 액세스 허용

에 대해 자세히 알아보십시오 ["익스포트 정책 구성 및 관리"](#).

**ONTAP SMB** 수출 규칙에 대해 알아보세요

내보내기 규칙은 익스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을 처리하는 방법을 결정하기 위해 구성된 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청을 일치시킵니다.

클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 익스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 익스포트 정책에 표시되는 순서대로 처리됩니다. 규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 권한이 사용되며 추가 규칙은 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

다음 조건을 사용하여 내보내기 규칙을 구성하여 클라이언트 액세스 권한을 결정할 수 있습니다.

- NFSv4 또는 SMB와 같이 요청을 보내는 클라이언트에서 사용하는 파일 액세스 프로토콜입니다.
  - 호스트 이름 또는 IP 주소와 같은 클라이언트 식별자입니다.
- '-clientmatch' 필드의 최대 크기는 4096자입니다.
- Kerberos v5, NTLM 또는 AUTH\_SYS와 같이 클라이언트에서 인증하는 데 사용되는 보안 유형입니다.

규칙이 여러 조건을 지정하는 경우 클라이언트는 규칙을 적용하기 위해 모든 조건을 충족해야 합니다.

예

익스포트 정책에는 다음 매개 변수가 있는 익스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0"
- 모든 것

- '어다나'

클라이언트 액세스 요청은 NFSv3 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.17.37입니다.

클라이언트 액세스 프로토콜이 일치하더라도 클라이언트의 IP 주소는 내보내기 규칙에 지정된 IP 주소와 다른 서브넷에 있습니다. 따라서 클라이언트 일치가 실패하고 이 규칙은 이 클라이언트에 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv4 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.16.54입니다.

클라이언트 액세스 프로토콜이 일치하고 클라이언트의 IP 주소가 지정된 서브넷에 있습니다. 따라서 클라이언트 일치가 성공하고 이 규칙이 이 클라이언트에 적용됩니다. 클라이언트는 보안 유형에 관계없이 읽기-쓰기 액세스를 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH\_SYS로 인증됩니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 따라서 두 클라이언트 모두 읽기 전용 액세스 권한이 부여됩니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

**SMB**를 통한 액세스를 제한하거나 허용하는 **ONTAP** 내보내기 정책 규칙의 예

이 예에서는 **SMB** 액세스에 대한 엑스포트 정책이 설정된 **SVM**에서 **SMB**를 통한 액세스를 제한 또는 허용하는 엑스포트 정책 규칙을 생성하는 방법을 보여줍니다.

**SMB** 액세스에 대한 엑스포트 정책은 기본적으로 비활성화되어 있습니다. **SMB** 액세스에 대한 엑스포트 정책을 설정한 경우에만 **SMB** 액세스를 제한하거나 허용하는 엑스포트 정책 규칙을 구성해야 합니다.

## SMB 액세스에 대한 익스포트 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 익스포트 규칙이 생성됩니다.

- 정책 이름: cifs1
- 색인 번호: 1
- 클라이언트 일치: 192.168.1.0/24 네트워크의 클라이언트만 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다
- 읽기 전용 액세스: NTLM 또는 Kerberos 인증을 사용하는 클라이언트에 대한 액세스
- 읽기-쓰기 액세스: Kerberos 인증을 사용하는 클라이언트에 대한 액세스

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

## SMB 및 NFS 액세스에 대한 익스포트 규칙

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 익스포트 규칙이 생성됩니다.

- 정책 이름: cifs nfs1
- 색인 번호: 2
- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 및 NFS 액세스
- 읽기 전용 액세스: 모든 클라이언트에 대해
- 읽기-쓰기 액세스: Kerberos(NFS 및 SMB) 또는 NTLM 인증(SMB)을 사용하는 클라이언트에 대한 액세스
- UNIX 사용자 ID 0(영)에 대한 매핑: 사용자 ID 65534에 매핑됨(일반적으로 사용자 이름에 매핑되지 않음)
- SUID 및 SGID 액세스: 허용

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs nfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

## NTLM을 사용한 SMB 액세스에 대한 내보내기 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 익스포트 규칙이 생성됩니다.

- 정책 이름: ntlm1
- 색인 번호: 1
- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다

- 읽기 전용 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다
- 읽기-쓰기 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다



NTLM 전용 액세스에 대해 읽기 전용 옵션 또는 읽기/쓰기 옵션을 구성하는 경우 클라이언트 일치 옵션에서 IP 주소 기반 항목을 사용해야 합니다. 그렇지 않으면 "액세스 거부" 오류가 발생합니다. 이는 ONTAP가 호스트 이름을 사용하여 클라이언트의 액세스 권한을 확인할 때 Kerberos SPN(서비스 사용자 이름)을 사용하기 때문입니다. NTLM 인증은 SPN 이름을 지원하지 않습니다.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

**SMB** 액세스를 위한 **ONTAP** 내보내기 정책 활성화 또는 비활성화

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 익스포트 정책을 설정하거나 해제할 수 있습니다. 내보내기 정책을 사용하여 리소스에 대한 SMB 액세스를 제어하는 것은 선택 사항입니다.

시작하기 전에

다음은 SMB에 대한 익스포트 정책을 설정하기 위한 요구 사항입니다.

- 클라이언트에 대한 내보내기 규칙을 만들기 전에 DNS에 "PTR" 레코드가 있어야 합니다.
- SVM에서 NFS 클라이언트에 대한 액세스를 제공하고 NFS 액세스에 사용할 호스트 이름이 CIFS 서버 이름과 다른 경우 호스트 이름에 대한 추가 "A" 및 "PTR" 레코드 세트가 필요합니다.

이 작업에 대해

SVM에서 새 CIFS 서버를 설정할 때 SMB 액세스에 대한 익스포트 정책을 사용하는 것은 기본적으로 해제되어 있습니다. 인증 프로토콜 또는 클라이언트 IP 주소 또는 호스트 이름을 기반으로 액세스를 제어하려는 경우 SMB 액세스에 대한 익스포트 정책을 설정할 수 있습니다. 언제든지 SMB 액세스에 대한 익스포트 정책을 설정하거나 해제할 수 있습니다.



NFS 지원 SVM에서 CIFS/SMB에 대한 익스포트 정책을 활성화하면 Linux 클라이언트가 SVM에서 명령을 사용하여 연결된 익스포트 정책 규칙을 통해 모든 SMB 볼륨의 접합 경로를 볼 수 있습니다  
showmount -e.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 익스포트 정책 활성화 또는 비활성화:
  - 내보내기 정책 활성화: 'vserver cifs options modify -vserver\_vserver\_name\_-is-exportpolicy -enabled true'
  - 익스포트 정책 비활성화: 'vserver cifs options modify -vserver\_vserver\_name\_-is-exportpolicy -enabled false'
3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 익스포트 정책을 사용하여 SVM VS1 기반 리소스에 대한 SMB 클라이언트 액세스를 제어할 수 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

**Storage-Level Access Guard**를 사용하여 파일 액세스를 보호합니다

**Storage-Level Access Guard**를 사용하여 안전한 **ONTAP SMB** 파일 액세스에 대해 알아보세요.

기본 파일 수준 및 내보내기/공유 보안을 사용하여 액세스를 보호하는 것 외에도 ONTAP가 볼륨 수준에서 적용한 세 번째 보안 계층인 스토리지 수준 액세스 가드를 구성할 수 있습니다.

Storage-Level Access Guard는 모든 NAS 프로토콜에서 해당 프로토콜이 적용된 스토리지 객체에 액세스하는 데 적용됩니다.

NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에게 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.

### Storage-Level Access Guard 동작

- Storage-Level Access Guard는 스토리지 개체의 모든 파일 또는 모든 디렉토리에 적용됩니다.

볼륨의 모든 파일 또는 디렉토리에는 Storage-Level Access Guard 설정이 적용되기 때문에 전파를 통한 상속은 필요하지 않습니다.

- 저장소 수준 액세스 가드를 구성하여 파일에만 적용하거나 디렉터리에만 적용하거나 볼륨 내의 파일과 디렉터리에 모두 적용할 수 있습니다.

- 파일 및 디렉터리 보안

스토리지 객체 내의 모든 디렉터리 및 파일에 적용됩니다. 기본 설정입니다.

- 파일 보안

스토리지 객체 내의 모든 파일에 적용됩니다. 이 보안을 적용해도 디렉터리에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

- 디렉터리 보안

스토리지 객체 내의 모든 디렉토리에 적용됩니다. 이 보안을 적용해도 파일에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

추가 액세스 권한은 제공하지 않습니다.

- NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다.

스토리지 객체 레벨에서 적용되고 유효 사용 권한을 결정하는 데 사용되는 메타데이터에 저장됩니다.

- 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 보안을 취소할 수 없습니다.

스토리지 관리자만 수정할 수 있습니다.

- NTFS 또는 혼합 보안 스타일을 사용하는 볼륨에 스토리지 수준 액세스 가드를 적용할 수 있습니다.
- 볼륨이 포함된 SVM에 CIFS 서버가 구성되어 있는 경우 UNIX 보안 스타일을 사용하는 볼륨에 Storage-Level Access Guard를 적용할 수 있습니다.
- 볼륨이 볼륨 집합 경로 아래에 마운트되고 해당 경로에 Storage-Level Access Guard가 있는 경우 그 아래에 마운트된 볼륨으로 전파되지 않습니다.
- Storage-Level Access Guard 보안 설명자는 SnapMirror 데이터 복제 및 SVM 복제를 통해 복제됩니다.
- 바이러스 스캐너용 특별한 디스펜션이 있습니다.

저장소 수준 액세스 가드가 개체에 대한 액세스를 거부하더라도 이러한 서버에서 파일과 디렉토리를 선별하기 위해 예외적인 액세스가 허용됩니다.

- 스토리지 레벨 액세스 가드로 인해 액세스가 거부되면 FPolicy 알림이 전송되지 않습니다.

## 액세스 확인 순서

파일 또는 디렉토리에 대한 액세스는 내보내기 또는 공유 권한, 볼륨에 설정된 Storage-Level Access Guard 권한, 파일 및/또는 디렉토리에 적용되는 기본 파일 권한의 합집합에 의해 결정됩니다. 모든 보안 수준을 평가하여 파일 또는 디렉토리에 있는 유효한 권한을 결정합니다. 보안 액세스 검사는 다음 순서로 수행됩니다.

1. SMB 공유 또는 NFS 익스포트 레벨 사용 권한
2. 스토리지 레벨 액세스 가드
3. NTFS 파일/폴더 ACL(액세스 제어 목록), NFSv4 ACL 또는 UNIX 모드 비트

## Storage-Level Access Guard 사용 사례

Storage-Level Access Guard는 클라이언트 측에서 볼 수 없는 스토리지 수준에서 추가 보안을 제공하므로 사용자 또는 관리자가 데스크톱에서 해당 보안을 취소할 수 없습니다. 스토리지 레벨에서 액세스를 제어하는 기능이 유용하다고 볼 수 있는 특정 사용 사례가 있습니다.

이 기능의 일반적인 사용 사례는 다음과 같습니다.

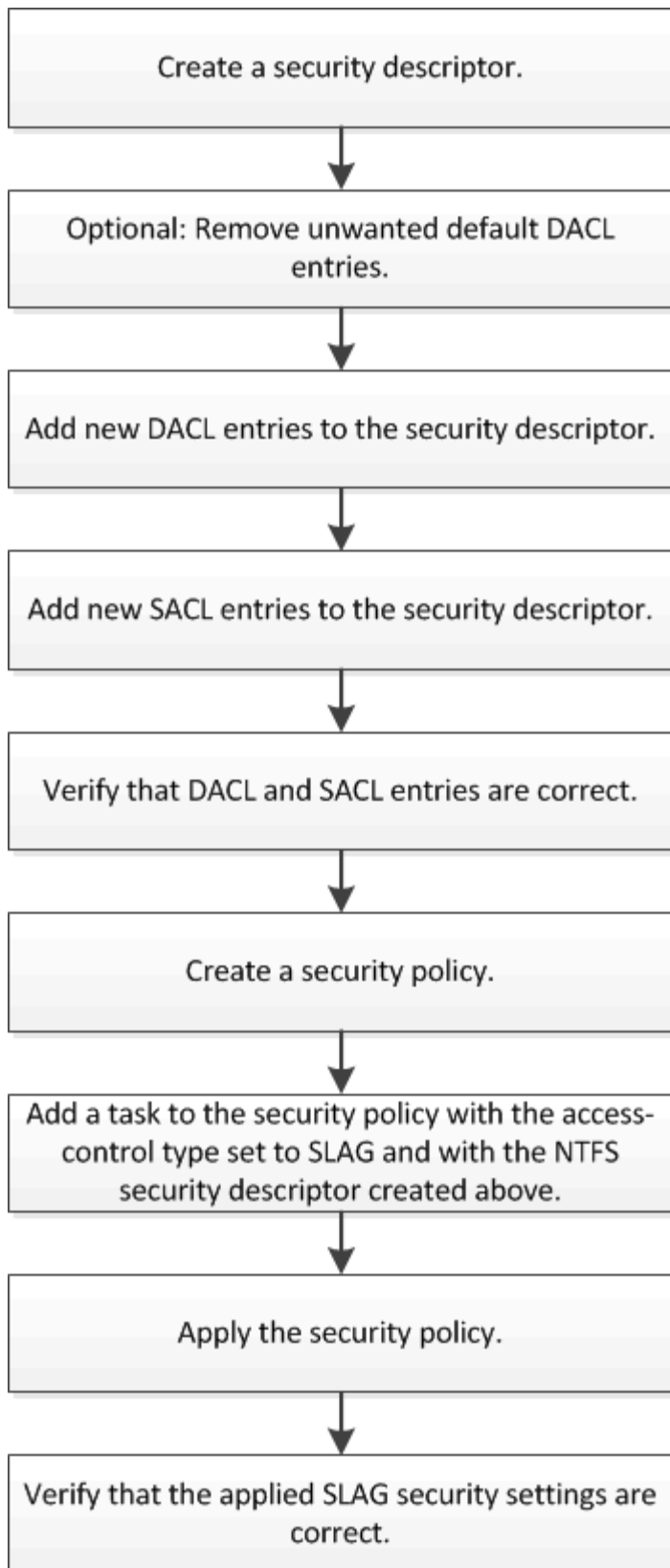
- 스토리지 수준에서 모든 사용자의 액세스를 감사 및 제어하여 지적 재산을 보호합니다
- 은행 및 거래 그룹을 비롯한 금융 서비스 기업을 위한 스토리지
- 정부 서비스 및 개별 부서용 개별 파일 스토리지



- 모든 학생 파일을 보호하는 대학

**ONTAP SMB** 서버에서 **Storage-Level Access Guard**에 대한 구성 워크플로

스토리지 레벨 액세스 가드(slag)를 구성하는 워크플로에서는 NTFS 파일 권한 및 감사 정책을 구성하는 데 사용하는 것과 동일한 ONTAP CLI 명령을 사용합니다. 지정된 대상에서 파일 및 디렉토리 액세스를 구성하는 대신 지정된 SVM(스토리지 가상 머신) 볼륨의 슬래그를 구성합니다.



관련 정보

[서버에서 스토리지 수준 액세스 보호 구성](#)

볼륨 또는 qtree에 스토리지 레벨 액세스 가드를 구성하려면 여러 단계를 수행해야 합니다. Storage-Level Access Guard는 스토리지 레벨에서 설정된 액세스 보안 수준을 제공합니다. 모든 NAS 프로토콜에서 적용된 스토리지 객체에 대한 모든 액세스에 적용되는 보안을 제공합니다.

#### 단계

1. 'vserver security file-directory NTFS create' 명령을 사용하여 보안 설명자를 생성합니다.

```
'vserver security file-directory NTFS create-vserver vs1-ntfs-sd sd1'vserver security file-directory NTFS show-vserver vs1'
```

```
Vserver: vs1
```

| NTFS Security<br>Descriptor Name | Owner Name |
|----------------------------------|------------|
| -----                            | -----      |
| sd1                              | -          |

보안 설명자는 다음 네 가지 기본 ACE(DACL 액세스 제어 항목)를 사용하여 만들어집니다.

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

| Account Name           | Access<br>Type | Access<br>Rights | Apply To                           |
|------------------------|----------------|------------------|------------------------------------|
| -----                  | -----          | -----            | -----                              |
| BUILTIN\Administrators | allow          | full-control     | this-folder, sub-folders,<br>files |
| BUILTIN\Users          | allow          | full-control     | this-folder, sub-folders,<br>files |
| CREATOR OWNER          | allow          | full-control     | this-folder, sub-folders,<br>files |
| NT AUTHORITY\SYSTEM    | allow          | full-control     | this-folder, sub-folders,<br>files |

Storage-Level Access Guard를 구성할 때 기본 항목을 사용하지 않으려면 보안 설명자에 고유한 ACE를 만들고 추가하기 전에 해당 항목을 제거할 수 있습니다.

2. Storage-Level Access Guard 보안으로 구성하지 않으려는 보안 설명자에서 기본 DACL ACE 중 하나를 제거합니다.

- a. 'vserver security file-directory NTFS DACL remove' 명령을 사용하여 불필요한 DACL ACE를 제거합니다.

이 예제에서는 세 개의 기본 DACL ACE가 보안 설명자인 BUILTIN\Administrators, BUILTIN\Users 및 Creator Owner에서 제거됩니다.

```
'vserver security file-directory NTFS DACL remove-vserver vs1-ntfs-sd SD1-access-type allow-account builtin\users"vserver security file-directory NTFS DACL remove-vserver vs1-directory vs1-access-directs builtl-creator' vserver security file-directs -directs -ntfs -directs -ntfs -directs -directs -creator
```

- b. 'vserver security file-directory NTFS DACL show' 명령을 사용하여 스토리지 수준 액세스 가드 보안에 사용하지 않을 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

이 예제에서 명령의 출력은 NT AUTHORITY\SYSTEM DEFAULT DACL ACE 항목만 남겨 두고 세 개의 기본 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

```
'vserver security file-directory NTFS DACL show -vserver vs1'
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name Access Access Apply To
 Type Rights

NT AUTHORITY\SYSTEM
 allow full-control this-folder, sub-folders,
files
```

3. 'vserver security file-directory NTFS DACL add' 명령을 사용하여 하나 이상의 DACL 항목을 보안 설명자에 추가합니다.

이 예제에서는 보안 설명자에 두 개의 DACL ACE가 추가됩니다.

```
'vserver security file-directory NTFS DACL add-vserver vs1-ntfs-sd SD1-access-type allow-account example\engineering-rights full-control-apply-to this-folder, sub-folders, files"vserver security file-directory ntfs DACL add-vserver vs1-ntfs-access-type allow-account" example\Domain Users"-read-folders 폴더에 대한 읽기 권한
```

4. 'vserver security file-directory NTFS SACL add' 명령을 사용하여 하나 이상의 SACL 항목을 보안 설명자에 추가합니다.

이 예제에서는 두 개의 SACL ACE가 보안 설명자에 추가됩니다.

```
'vserver security file-directory NTFS SACL add-vserver vs1-ntfs-sd SD1-access-type failure-account' example\Domain Users"-rights read-apply-to this-folder, sub-folders, files"vserver security file-directory NTFS SACL add-vserver vs1-ntfs-sd-access-type success-account example\engineering-folders full-control-folders
```

5. 'vserver security file-directory NTFS DACL show' 및 'vserver security file-directory NTFS SACL show' 명령을 각각 사용하여 DACL 및 SACL ACE가 올바르게 구성되었는지 확인합니다.

이 예제에서 다음 명령은 보안 설명자 "Sd1"의 DACL 항목에 대한 정보를 표시합니다.

```
'vserver security file-directory NTFS DACL show -vserver vs1-NTFS-SD SD1'
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

| Account Name         | Access Type | Access Rights | Apply To                        |
|----------------------|-------------|---------------|---------------------------------|
| -----                | -----       | -----         | -----                           |
| EXAMPLE\Domain Users | allow       | read          | this-folder, sub-folders, files |
| EXAMPLE\engineering  | allow       | full-control  | this-folder, sub-folders, files |
| NT AUTHORITY\SYSTEM  | allow       | full-control  | this-folder, sub-folders, files |

이 예제에서 다음 명령은 보안 설명자 "sd1"에 대한 SACL 항목에 대한 정보를 표시합니다.

'vserver security file-directory NTFS SACL show -vserver vs1-NTFS-SD SD1'

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

| Account Name         | Access Type | Access Rights | Apply To                        |
|----------------------|-------------|---------------|---------------------------------|
| -----                | -----       | -----         | -----                           |
| EXAMPLE\Domain Users | failure     | read          | this-folder, sub-folders, files |
| EXAMPLE\engineering  | success     | full-control  | this-folder, sub-folders, files |

6. 'vserver security file-directory policy create' 명령을 사용하여 보안 정책을 생성합니다.

다음 예제에서는 ""정책1""이라는 정책을 만듭니다.

'vserver security file-directory policy create-vserver vs1-policy-name policy1'

7. 'vserver security file-directory policy show' 명령을 사용하여 정책이 올바르게 구성되었는지 확인합니다.

'vserver security file-directory policy show'를 선택합니다

|         |             |
|---------|-------------|
| Vserver | Policy Name |
| -----   | -----       |
| vs1     | policy1     |

8. 을 사용하여 연결된 보안 설명자가 있는 작업을 보안 정책에 추가합니다 `vserver security file-directory policy task add` 명령과 함께 `-access-control` 매개 변수를 로 설정합니다 `slag`.

정책에 둘 이상의 Storage-Level Access Guard 작업이 포함될 수 있지만 파일 디렉터리 및 Storage-Level Access Guard 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉터리 작업이 포함되어야 합니다.

이 예제에서는 보안 설명자 'Sd1'에 할당된 "정책1"이라는 정책에 작업이 추가됩니다. 액세스 제어 유형이 '슬래그'로 설정된 '/datavol1' 경로에 할당됩니다.

'vserver security file-directory policy task add-vserver vs1-policy-name policy1-path/datavol1-access-control slag-security-type ntfs-ntfs-mode propagate-ntfs-sd SD1'

9. 'vserver security file-directory policy task show' 명령을 사용하여 작업이 올바르게 구성되었는지 확인합니다.

'vserver security file-directory policy task show -vserver vs1-policy-name policy1'

```
Vserver: vs1
Policy: policy1
```

| Index    | File/Folder | Access  | Security | NTFS      | NTFS       |
|----------|-------------|---------|----------|-----------|------------|
| Security | Path        | Control | Type     | Mode      | Descriptor |
| Name     |             |         |          |           |            |
| -----    | -----       | -----   | -----    | -----     | -----      |
| 1        | /datavol1   | slag    | ntfs     | propagate | sd1        |

10. 'vserver security file-directory apply' 명령을 사용하여 Storage-Level Access Guard 보안 정책을 적용합니다.

'vserver security file-directory apply-vserver vs1-policy-name policy1'

보안 정책을 적용할 작업이 예약됩니다.

11. 'vserver security file-directory show' 명령을 사용하여 적용된 Storage-Level Access Guard 보안 설정이 올바른지 확인합니다.

이 예제에서 명령의 출력은 스토리지 레벨 액세스 가드 보안이 NTFS 볼륨 '/datavol1'에 적용되었음을 보여 줍니다. 모든 사용자에게 모든 권한을 허용하는 기본 DACL이 그대로 유지되더라도 Storage-Level Access Guard 보안은 Storage-Level Access Guard 설정에 정의된 그룹에 대한 액세스를 제한(및 감사)합니다.

'vserver security file-directory show -vserver vs1-path/datavol1'

```

 Vserver: vs1
 File Path: /datavol1
File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

#### 관련 정보

- [NTFS 파일 보안, NTFS 감사 정책 및 스토리지 수준 액세스 보호 관리를 위한 명령](#)
- [서버의 Storage-Level Access Guard에 대한 구성 워크플로](#)
- [서버의 Storage-Level Access Guard에 대한 정보 표시](#)
- [서버에서 스토리지 수준 액세스 보호 제거](#)

볼륨 또는 qtree 또는 둘 다에서 슬래그를 구성할 수 있습니다. 슬래그 매트릭스는 표에 나열된 다양한 시나리오에서 적용 가능한 슬래그 구성인 볼륨 또는 qtree를 정의합니다.

|                                        | AFS에서 볼륨 슬래그 | 스냅샷의 볼륨 슬래그 | AFS에서 qtree 슬래그 | 스냅샷에서 Qtree 슬래그 |
|----------------------------------------|--------------|-------------|-----------------|-----------------|
| AFS(Access File System)에서 볼륨 액세스       | 예            | 아니요         | 해당 없음           | 해당 없음           |
| 스냅샷의 볼륨 액세스                            | 예            | 아니요         | 해당 없음           | 해당 없음           |
| AFS에서 qtree 액세스(qtree에 슬래그가 있는 경우)     | 아니요          | 아니요         | 예               | 아니요             |
| AFS에서 qtree 액세스(qtree에 슬래그가 없는 경우)     | 예            | 아니요         | 아니요             | 아니요             |
| 스냅샷에서 qtree 액세스(qtree AFS에 슬래그가 있는 경우) | 아니요          | 아니요         | 예               | 아니요             |
| 스냅샷에서 qtree 액세스(qtree AFS에 슬래그가 없는 경우) | 예            | 아니요         | 아니요             | 아니요             |

#### ONTAP SMB 서버에서 Storage-Level Access Guard에 대한 정보 표시

Storage-Level Access Guard는 볼륨 또는 qtree에 적용되는 세 번째 보안 계층입니다. Windows 속성 창을 사용하면 저장소 수준 액세스 가드 설정을 볼 수 없습니다. ONTAP CLI를 사용하여 스토리지 레벨 액세스 가드 보안에 대한 정보를 확인해야 합니다. 이 정보는 구성을 확인하거나 파일 액세스 문제를 해결하는 데 사용할 수 있습니다.

이 작업에 대해

SVM(Storage Virtual Machine)의 이름과 스토리지 레벨 액세스 가드 보안 정보를 표시할 볼륨 또는 qtree의 경로를 입력해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

단계

1. Storage-Level Access Guard 보안 설정을 원하는 수준으로 표시합니다.

| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                          |
|--------------|--------------------------------------------------------------------------|
| 요약 양식        | 'vserver security file-directory show -vserver_vserver_name_-path_path_' |



|              |                                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------|
| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                                                 |
| 세부 정보가 확장됩니다 | 'vserver security file-directory show<br>-vserver_vserver_name_-path_path_-expand-mask<br>true' |

예

다음 예에서는 SVM VS1 에서 경로 '/datavol1'을 사용하여 NTFS 보안 스타일 볼륨에 대한 Storage-Level Access Guard 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

 Vserver: vs1
 File Path: /datavol1
 File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-OI|CI|IO

 Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에서 혼합 보안 형식 볼륨에 대한 Storage-Level Access Guard 정보를 표시합니다. 이 볼륨의 최상위 수준에는 UNIX의 효과적인 보안이 있습니다. 이 볼륨에는 Storage-Level Access Guard 보안이 있습니다.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

 Vserver: vs1
 File Path: /datavol5
 File Inode Number: 3374
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
 ACLs: Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

#### ONTAP SMB 서버에서 스토리지 수준 액세스 보호 제거

저장소 수준에서 액세스 보안을 더 이상 설정하지 않으려면 볼륨 또는 qtree에서 저장소 수준 액세스 가드를 제거할 수 있습니다. Storage-Level Access Guard를 제거해도 일반 NTFS 파일 및 디렉터리 보안은 수정하거나 제거되지 않습니다.

#### 단계

1. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에 Storage-Level Access Guard가 구성되어 있는지 확인합니다.

```
'vserver security file-directory show -vserver vs1-path/datavol2'
```

```

 Vserver: vs1
 File Path: /datavol2
 File Inode Number: 99
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0xbf14
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 SACL - ACEs
 AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
 DACL - ACEs
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
 ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

 Storage-Level Access Guard security
 DACL (Applies to Directories):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 DACL (Applies to Files):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. 'vserver security file-directory remove-slag' 명령을 사용하여 Storage-Level Access Guard를 제거합니다.

```
'vserver security file-directory remove-slag-vserver vs1-path/datavol2'
```

3. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에서 Storage-Level Access Guard가 제거되었는지 확인합니다.

```
'vserver security file-directory show -vserver vs1-path/datavol2'
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

```

## SMB를 사용하여 파일 액세스를 관리합니다

로컬 사용자 및 그룹을 인증 및 인증에 사용합니다

**ONTAP**에서 로컬 사용자 및 그룹을 사용하는 방법

로컬 **ONTAP SMB** 사용자 및 그룹에 대해 알아보세요

사용자 환경에서 로컬 사용자 및 그룹을 구성하고 사용할지 여부를 결정하기 전에 로컬 사용자 및 그룹의 정의 및 이에 대한 몇 가지 기본 정보를 알아야 합니다.

### • \* 로컬 사용자 \*

생성된 SVM(스토리지 가상 머신)만 볼 수 있는 고유한 SID(보안 식별자)를 가진 사용자 계정 로컬 사용자 계정에는 사용자 이름 및 SID를 비롯한 일련의 속성이 있습니다. 로컬 사용자 계정은 NTLM 인증을 사용하여 CIFS 서버에서 로컬로 인증됩니다.

사용자 계정에는 여러 가지 용도가 있습니다.

- 사용자에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
- SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.

### • \* 로컬 그룹 \*

고유한 SID가 있는 그룹은 해당 SID가 생성된 SVM에서만 볼 수 있습니다. 그룹에는 구성원 집합이 포함됩니다. 구성원은 로컬 사용자, 도메인 사용자, 도메인 그룹 및 도메인 컴퓨터 계정일 수 있습니다. 그룹을 생성, 수정 또는 삭제할 수 있습니다.

그룹은 여러 가지 용도로 사용됩니다.

- 해당 구성원에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
- SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.

- \* 로컬 도메인 \*

SVM에서 범위가 지정된 로컬 영역 로컬 도메인의 이름은 CIFS 서버 이름입니다. 로컬 사용자 및 그룹은 로컬 도메인 내에 포함됩니다.

- \* SID(보안 식별자) \*

SID는 Windows 스타일의 보안 주체를 식별하는 가변 길이 숫자 값입니다. 예를 들어 일반적인 SID는 S-1-5-21-3139654847-1303905135-2517279418-123456의 형태를 사용합니다.

- \* NTLM 인증 \*

CIFS 서버에서 사용자를 인증하는 데 사용되는 Microsoft Windows 보안 방법입니다.

- \* 클러스터 복제 데이터베이스(RDB) \*

클러스터의 각 노드에 인스턴스가 있는 복제된 데이터베이스입니다. 로컬 사용자 및 그룹 객체가 RDB에 저장됩니다.

## 로컬 **ONTAP SMB** 사용자 및 로컬 그룹을 생성하는 이유

SVM(스토리지 가상 시스템)에서 로컬 사용자 및 로컬 그룹을 생성하는 데는 여러 가지 이유가 있습니다. 예를 들어 DC(도메인 컨트롤러)를 사용할 수 없거나, 로컬 그룹을 사용하여 권한을 할당하거나, SMB 서버가 작업 그룹에 있는 경우 로컬 사용자 계정을 사용하여 SMB 서버에 액세스할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 사용자 계정을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 사용자를 사용할 수 없습니다.

로컬 사용자는 작업 그룹 구성에 필요합니다.

- 도메인 컨트롤러를 사용할 수 없는 경우 SMB 서버를 인증하고 로그인할 수 있어야 합니다.

로컬 사용자는 도메인 컨트롤러가 다운되었을 때 NTLM 인증을 사용하여 SMB 서버를 인증할 수 있으며, 네트워크 문제로 인해 SMB 서버가 도메인 컨트롤러에 접속할 수 없게 되는 경우

- 로컬 사용자에게 사용자 권한 관리 권한을 할당하려고 합니다.

*User Rights Management* 는 SMB 서버 관리자가 SVM에 대한 사용자 및 그룹의 권한을 제어할 수 있는 기능입니다. 사용자 계정에 권한을 할당하거나 해당 권한이 있는 로컬 그룹의 구성원으로 만들어 사용자에게 권한을 할당할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 그룹을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 그룹을 사용할 수 없습니다.

로컬 그룹은 작업 그룹 구성에 필요하지 않지만 로컬 작업 그룹 사용자에게 대한 액세스 권한을 관리하는 데 유용할 수 있습니다.

- 공유 및 파일 액세스 제어를 위해 로컬 그룹을 사용하여 파일 및 폴더 리소스에 대한 액세스를 제어하려는 경우
- Customized\_User Rights Management\_Privileges를 사용하여 로컬 그룹을 생성하려고 합니다.

일부 기본 제공 사용자 그룹에는 사전 정의된 권한이 있습니다. 사용자 지정된 권한 집합을 할당하려면 로컬 그룹을 생성하고 해당 그룹에 필요한 권한을 할당할 수 있습니다. 그런 다음 로컬 사용자, 도메인 사용자 및 도메인 그룹을 로컬 그룹에 추가할 수 있습니다.

#### 관련 정보

- [로컬 사용자 인증에 대해 알아보세요](#)
- [지원되는 권한 목록입니다](#)

#### 로컬 ONTAP SMB 사용자 인증에 대해 알아보세요

로컬 사용자가 CIFS 서버의 데이터를 액세스하려면 먼저 인증된 세션을 생성해야 합니다.

SMB는 세션 기반이므로 세션이 처음 설정될 때 사용자 ID를 한 번만 결정할 수 있습니다. CIFS 서버는 로컬 사용자를 인증할 때 NTLM 기반 인증을 사용합니다. NTLMv1과 NTLMv2가 모두 지원됩니다.

ONTAP는 세 가지 사용 사례에서 로컬 인증을 사용합니다. 각 활용 사례는 사용자 이름의 도메인 부분(domain\user 형식)이 CIFS 서버의 로컬 도메인 이름(CIFS 서버 이름)과 일치하는지 여부에 따라 달라집니다.

- 도메인 부분이 일치합니다

데이터에 대한 액세스를 요청할 때 로컬 사용자 자격 증명을 제공하는 사용자는 CIFS 서버에서 로컬로 인증됩니다.

- 도메인 부분이 일치하지 않습니다

ONTAP는 CIFS 서버가 속한 도메인의 도메인 컨트롤러에서 NTLM 인증을 사용하려고 합니다. 인증에 성공하면 로그인이 완료된 것입니다. 성공하지 못하면 다음 단계는 인증이 성공하지 못한 이유에 따라 달라집니다.

예를 들어 사용자가 Active Directory에 있지만 암호가 잘못되었거나 만료된 경우 ONTAP는 CIFS 서버에서 해당 로컬 사용자 계정을 사용하지 않습니다. 대신 인증에 실패합니다. ONTAP가 CIFS 서버에 있는 경우 NetBIOS 도메인 이름이 일치하지 않아도 인증을 위해 해당 로컬 계정을 사용하는 경우도 있습니다. 예를 들어 일치하는 도메인 계정이 있지만 비활성화된 경우 ONTAP는 CIFS 서버에서 해당 로컬 계정을 사용하여 인증합니다.

- 도메인 부분이 지정되지 않았습니다

ONTAP는 먼저 로컬 사용자로 인증을 시도합니다. 로컬 사용자로 인증에 실패하면 ONTAP는 CIFS 서버가 속한 도메인의 도메인 컨트롤러를 사용하여 사용자를 인증합니다.

로컬 또는 도메인 사용자 인증이 성공적으로 완료되면 ONTAP는 로컬 그룹 구성원 자격 및 권한을 고려하여 전체 사용자 액세스 토큰을 생성합니다.

로컬 사용자의 NTLM 인증에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

관련 정보

[서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다.](#)

**ONTAP SMB** 사용자 액세스 토큰에 대해 알아보세요

사용자가 공유를 매핑하면 인증된 SMB 세션이 설정되고 사용자, 사용자의 그룹 구성원 자격 및 누적 권한, 매핑된 UNIX 사용자에 대한 정보가 포함된 사용자 액세스 토큰이 생성됩니다.

이 기능을 사용하지 않는 한 로컬 사용자 및 그룹 정보도 사용자 액세스 토큰에 추가됩니다. 액세스 토큰이 구성되는 방식은 로컬 사용자에 대한 로그인인지 Active Directory 도메인 사용자에 대한 로그인인지에 따라 달라집니다.

- 로컬 사용자 로그인입니다

로컬 사용자는 다른 로컬 그룹의 구성원이 될 수 있지만 로컬 그룹은 다른 로컬 그룹의 구성원이 될 수 없습니다. 로컬 사용자 액세스 토큰은 특정 로컬 사용자가 구성원인 그룹에 할당된 모든 권한의 합집합으로 구성됩니다.

- 도메인 사용자 로그인

도메인 사용자가 로그인하면 ONTAP는 사용자가 구성원인 모든 도메인 그룹의 사용자 SID 및 SID가 포함된 사용자 액세스 토큰을 얻습니다. ONTAP는 도메인 사용자 액세스 토큰의 조합과 사용자의 도메인 그룹(있는 경우)의 로컬 멤버십에서 제공하는 액세스 토큰, 도메인 사용자 또는 해당 도메인 그룹 구성원에 할당된 모든 직접 권한을 사용합니다.

로컬 및 도메인 사용자 로그인의 경우 사용자 액세스 토큰에 대해 기본 그룹 제거도 설정됩니다. 기본 RID는 Domain Users(RID 513)입니다. 기본값을 변경할 수 없습니다.

Windows-to-UNIX 및 UNIX-to-Windows 이름 매핑 프로세스는 로컬 및 도메인 계정에 대해 동일한 규칙을 따릅니다.



UNIX 사용자에서 로컬 계정으로 자동 매핑은 암시적으로 수행되지 않습니다. 이 작업이 필요한 경우 기존 이름 매핑 명령을 사용하여 명시적 매핑 규칙을 지정해야 합니다.

로컬 그룹이 포함된 **ONTAP SMB SVM**에서 **SnapMirror**를 사용하는 방법에 대해 알아보세요.

로컬 그룹이 포함된 SVM이 소유한 볼륨에 SnapMirror를 구성할 때는 지침을 숙지해야 합니다.

SnapMirror에서 다른 SVM으로 복제된 파일, 디렉토리 또는 공유에 적용된 ACE의 로컬 그룹은 사용할 수 없습니다. SnapMirror 기능을 사용하여 다른 SVM의 볼륨에 DR 미러를 생성하고 볼륨에 로컬 그룹에 ACE가 있는 경우 ACE는 미러에서 유효하지 않습니다. 데이터를 다른 SVM으로 복제하면 데이터가 다른 로컬 도메인에 효과적으로 교차합니다. 로컬 사용자 및 그룹에 부여되는 사용 권한은 원래 생성된 SVM의 범위 내에서만 유효합니다.

**ONTAP SMB** 서버를 삭제하면 사용자와 그룹에 어떤 영향이 있는지 알아보세요.

CIFS 서버가 생성될 때 로컬 사용자 및 그룹의 기본 세트가 생성되고 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)과 연결됩니다. SVM 관리자는 언제든지 로컬 사용자 및 그룹을 생성할 수 있습니다. CIFS 서버를 삭제할 때 로컬 사용자 및 그룹에 어떤 일이 발생하는지 알고 있어야 합니다.

로컬 사용자 및 그룹은 SVM에 연결되어 있으므로 보안 고려 사항으로 인해 CIFS 서버를 삭제할 때 삭제되지 않습니다.



CIFS 서버가 삭제되어도 로컬 사용자 및 그룹은 삭제되지 않지만 숨겨집니다. SVM에서 CIFS 서버를 다시 생성할 때까지 로컬 사용자 및 그룹을 보거나 관리할 수 없습니다.



CIFS 서버 관리 상태는 로컬 사용자 또는 그룹의 표시에는 영향을 주지 않습니다.

로컬 **ONTAP SMB** 사용자 및 그룹과 함께 **Microsoft Management Console**을 사용하는 방법을 알아보세요.

Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 정보를 볼 수 있습니다. 이 ONTAP 릴리스에서는 Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 다른 관리 작업을 수행할 수 없습니다.

**ONTAP SMB** 클러스터 되돌리기에 대해 알아보세요

로컬 사용자 및 그룹을 지원하지 않는 ONTAP 릴리즈로 클러스터를 되돌리려는 경우 로컬 사용자 및 그룹을 사용하여 파일 액세스 또는 사용자 권한을 관리하려면 특정 고려 사항을 알고 있어야 합니다.

- 보안상의 이유로 ONTAP가 로컬 사용자 및 그룹 기능을 지원하지 않는 버전으로 되돌려지면 구성된 로컬 사용자, 그룹 및 권한에 대한 정보가 삭제되지 않습니다.
- ONTAP의 이전 주요 버전으로 되돌릴 때 ONTAP는 인증 및 자격 증명 생성 중에 로컬 사용자 및 그룹을 사용하지 않습니다.
- 로컬 사용자 및 그룹은 파일 및 폴더 ACL에서 제거되지 않습니다.
- 로컬 사용자 또는 그룹에 부여된 권한으로 인해 부여되는 액세스에 의존하는 파일 액세스 요청이 거부됩니다.

액세스를 허용하려면 로컬 사용자 및 그룹 개체 대신 도메인 개체를 기반으로 액세스를 허용하도록 파일 권한을 다시 구성해야 합니다.

어떤 로컬 권한이 있는지 확인합니다

지원되는 **ONTAP SMB** 권한 목록

ONTAP에는 지원되는 권한이 미리 정의되어 있습니다. 미리 정의된 특정 로컬 그룹에는 이러한 권한 중 일부가 기본적으로 추가됩니다. 또한 미리 정의된 그룹에서 권한을 추가하거나 제거하거나 새 로컬 사용자 또는 그룹을 만들고 만든 그룹 또는 기존 도메인 사용자 및 그룹에 권한을 추가할 수도 있습니다.

다음 표에는 SVM(스토리지 가상 시스템)에서 지원되는 권한이 나열되어 있으며 할당된 권한이 있는 BUILTIN 그룹 목록이 제공됩니다.

| 권한 이름입니다             | 기본 보안 설정입니다                                             | 설명                             |
|----------------------|---------------------------------------------------------|--------------------------------|
| '세TcbPrivilege'입니다   | 없음                                                      | 운영 체제의 일부로 작동합니다               |
| 'BackupPrivilege'입니다 | 'BUILTIN\Administrators',<br>'BUILTIN\Backup Operators' | 파일 및 디렉토리를 백업하고 모든 ACL을 재정의합니다 |

| 권한 이름입니다                | 기본 보안 설정입니다                                                                                                       | 설명                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 스저장창고특권                 | 'BUILTIN\Administrators',<br>'BUILTIN\Backup Operators'                                                           | 파일 및 디렉토리를 복원하고 모든 ACL을 재정의하면 유효한 사용자 또는 그룹 SID가 파일 소유자로 설정됩니다         |
| '새테이크오너선프리빌리지'          | 'BUILTIN\Administrators'                                                                                          | 파일 또는 기타 개체의 소유권을 가져옵니다                                                |
| '보안 권한'                 | 'BUILTIN\Administrators'                                                                                          | 감사 관리<br><br>여기에는 보안 로그 보기, 덤프 및 지우기가 포함됩니다.                           |
| '스변경NotifyPrivilege'입니다 | 'BUILTIN\Administrators',<br>'BUILTIN\Backup Operators',<br>'BUILTIN\Power Users',<br>'BUILTIN\Users', 'Everyone' | 횡단 검사를 무시합니다<br><br>이 권한이 있는 사용자는 폴더, 교집합 또는 교차로를 횡단(x) 권한이 필요하지 않습니다. |

#### 관련 정보

- [권한 할당에 대해 알아보세요](#)
- [바이패스 트래버스 검사 구성에 대해 알아보세요](#)

#### ONTAP SMB 권한 할당에 대해 알아보세요

로컬 사용자 또는 도메인 사용자에게 직접 권한을 할당할 수 있습니다. 또는 할당된 권한이 해당 사용자에게 부여할 기능과 일치하는 로컬 그룹에 사용자를 할당할 수 있습니다.

- 생성한 그룹에 권한 집합을 할당할 수 있습니다.

그런 다음 해당 사용자에게 부여할 권한이 있는 사용자를 그룹에 추가합니다.

- 기본 권한이 해당 사용자에게 부여할 권한과 일치하는 미리 정의된 그룹에 로컬 사용자 및 도메인 사용자를 할당할 수도 있습니다.

#### 관련 정보

- [로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다](#)
- [로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거합니다](#)
- [로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정합니다](#)
- [바이패스 트래버스 검사 구성에 대해 알아보세요](#)

ONTAP SMB 서버의 **BUILTIN** 그룹 및 로컬 관리자 계정에 대해 알아보세요.

BUILTIN 그룹 및 로컬 관리자 계정을 사용할 때 유의해야 할 몇 가지 지침이 있습니다. 예를 들어 로컬 관리자 계정의 이름을 바꿀 수는 있지만 이 계정은 삭제할 수 없습니다.

- Administrator 계정의 이름을 바꿀 수는 있지만 삭제할 수는 없습니다.
- 관리자 계정은 BUILTIN\Administrators 그룹에서 제거할 수 없습니다.
- BUILTIN 그룹은 이름을 바꿀 수 있지만 삭제할 수 없습니다.

BUILTIN 그룹의 이름을 바꾼 후 잘 알려진 이름으로 다른 로컬 개체를 만들 수 있지만 개체에 새 RID가 할당됩니다.

- 로컬 게스트 계정이 없습니다.

#### 관련 정보

#### 사전 정의된 BUILTIN 그룹 및 기본 권한

로컬 **ONTAP SMB** 사용자 암호에 대한 요구 사항

기본적으로 로컬 사용자 암호는 복잡성 요구 사항을 충족해야 합니다. 암호 복잡성 요구 사항은 Microsoft Windows\_Local 보안 정책 \_에 정의된 요구 사항과 비슷합니다.

암호는 다음 기준을 충족해야 합니다.

- 6자 이상이어야 합니다
- 사용자 계정 이름을 포함해서는 안 됩니다
- 다음 4개 범주 중 3개 이상의 문자를 포함해야 합니다.
  - 영어 대문자(A ~ Z)
  - 영어 소문자(a ~ z)
  - 기본 10자리(0 ~ 9)
  - 특수 문자:

~ ! @ # \$ % {caret} & \* \_ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /

#### 관련 정보

- [로컬 사용자에게 대한 암호 복잡성 구성](#)
- [서버 보안 설정에 대한 정보 표시](#)
- [로컬 사용자 계정 암호를 변경합니다](#)

미리 정의된 **BUILTIN** 그룹 및 기본 **ONTAP SMB** 권한

ONTAP에서 제공하는 미리 정의된 BUILTIN 그룹 집합에 로컬 사용자 또는 도메인 사용자의 구성원을 할당할 수 있습니다. 사전 정의된 그룹에는 사전 정의된 권한이 할당됩니다.

다음 표에는 미리 정의된 그룹이 설명되어 있습니다.

| 미리 정의된 <b>BUILTIN</b> 그룹                                                                                                                                                                                                                            | 기본 권한                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>"BUILTIN\Administrators" RID 544</p> <p>처음 만들어지면 500여 개 계정을 없앤다고 하면 자동으로 이 그룹의 회원이 됩니다. SVM(Storage Virtual Machine)이 도메인에 가입되면 domain\Domain Admins 그룹이 그룹에 추가됩니다. SVM이 도메인을 벗어나면 domain\Domain Admins 그룹이 그룹에서 제거됩니다.</p>                      | <ul style="list-style-type: none"> <li>• 'BackupPrivilege'입니다</li> <li>• 스토리지창고특권</li> <li>• '보안 권한'</li> <li>• '새테이크오너선프리빌리지'</li> <li>• '스변경NotifyPrivilege'입니다</li> </ul> |
| <p>"BUILTIN\Power Users" RID 547</p> <p>이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 다음과 같은 특성을 갖습니다.</p> <ul style="list-style-type: none"> <li>• 로컬 사용자 및 그룹을 생성하고 관리할 수 있습니다.</li> <li>• 자체 또는 다른 개체를 'BUILTIN\Administrators' 그룹에 추가할 수 없습니다.</li> </ul> | <p>'스변경NotifyPrivilege'입니다</p>                                                                                                                                               |
| <p>"BUILTIN\Backup Operators" RID 551</p> <p>이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 백업 의도로 열린 파일 또는 폴더에 대한 읽기 및 쓰기 권한을 재정의할 수 있습니다.</p>                                                                                                                | <ul style="list-style-type: none"> <li>• 'BackupPrivilege'입니다</li> <li>• 스토리지창고특권</li> <li>• '스변경NotifyPrivilege'입니다</li> </ul>                                              |
| <p>"BUILTIN\Users" RID 545</p> <p>처음 만들어도 이 그룹에는 인증된 사용자 특별 그룹 외에 구성원이 없습니다. SVM이 도메인에 가입되면 이 그룹에 domain\Domain Users" 그룹이 추가됩니다. SVM이 도메인을 벗어나면 이 그룹에서 "도메인 사용자" 그룹이 제거됩니다.</p>                                                                    | <p>'스변경NotifyPrivilege'입니다</p>                                                                                                                                               |
| <p>모든 사람의 ID S-1-0입니다</p> <p>이 그룹에는 게스트(익명 사용자 제외)를 포함한 모든 사용자가 포함됩니다. 이 그룹은 묵시적 멤버십을 가진 암시적 그룹입니다.</p>                                                                                                                                             | <p>'스변경NotifyPrivilege'입니다</p>                                                                                                                                               |

#### 관련 정보

- [서버의 BUILTIN 그룹 및 로컬 관리자 계정에 대해 알아보세요.](#)
- [지원되는 권한 목록입니다](#)
- [바이패스 트래버스 검사 구성에 대해 알아보세요](#)

로컬 사용자 및 그룹 기능을 설정하거나 해제합니다

로컬 **ONTAP SMB** 사용자 및 그룹 기능에 대해 알아보세요

NTFS 보안 스타일 데이터의 액세스 제어에 로컬 사용자 및 그룹을 사용하려면 먼저 로컬 사용자 및 그룹 기능을 활성화해야 합니다. 또한 SMB 인증에 로컬 사용자를 사용하려면 로컬 사용자 인증 기능을 활성화해야 합니다.

로컬 사용자 및 그룹 기능 및 로컬 사용자 인증은 기본적으로 사용됩니다. 이 옵션이 설정되어 있지 않으면 로컬 사용자 및 그룹을 구성하고 사용할 수 있도록 설정하기 전에 설정해야 합니다. 언제든지 로컬 사용자 및 그룹 기능을 사용하지 않도록 설정할 수 있습니다.

로컬 사용자 및 그룹 기능을 명시적으로 해제하는 것 외에도, 클러스터의 노드가 해당 기능을 지원하지 않는 ONTAP 릴리즈로 되돌려지는 경우 ONTAP는 로컬 사용자 및 그룹 기능을 비활성화합니다. 클러스터의 모든 노드에서 지원하는 ONTAP 버전이 실행될 때까지 로컬 사용자 및 그룹 기능이 활성화되지 않습니다.

#### 관련 정보

- [로컬 사용자 계정을 수정합니다](#)
- [로컬 그룹을 수정합니다](#)
- [로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다](#)

#### ONTAP SMB 서버에서 로컬 사용자 및 그룹 활성화 또는 비활성화

SVM(스토리지 가상 머신)에서 SMB 액세스를 위해 로컬 사용자 및 그룹을 설정하거나 해제할 수 있습니다. 로컬 사용자 및 그룹 기능은 기본적으로 활성화되어 있습니다.

#### 이 작업에 대해

SMB 공유 및 NTFS 파일 권한을 구성할 때 로컬 사용자 및 그룹을 사용할 수 있으며 SMB 연결을 생성할 때 로컬 사용자를 인증에 사용할 수도 있습니다. 로컬 사용자를 인증에 사용하려면 로컬 사용자 및 그룹 인증 옵션도 활성화해야 합니다.

#### 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

| 로컬 사용자 및 그룹을 사용하려는 경우... | 명령 입력...                                                                                            |
|--------------------------|-----------------------------------------------------------------------------------------------------|
| 활성화됨                     | 'vserver cifs options modify<br>-vserver_vserver_name_-is-local-users-and-groups<br>-enabled true'  |
| 사용 안 함                   | 'vserver cifs options modify<br>-vserver_vserver_name_-is-local-users-and-groups<br>-enabled false' |

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

#### 예

다음 예에서는 SVM VS1 에서 로컬 사용자 및 그룹 기능을 사용하도록 설정합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

#### 관련 정보

- [서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다.](#)
- [로컬 사용자 계정을 설정하거나 해제합니다](#)

**ONTAP SMB** 서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다.

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 로컬 사용자 인증을 설정하거나 해제할 수 있습니다. 기본값은 로컬 사용자 인증을 허용하는 것입니다. 이는 SVM이 도메인 컨트롤러에 연결할 수 없거나 도메인 레벨 액세스 제어를 사용하지 않도록 선택하는 경우에 유용합니다.

#### 시작하기 전에

CIFS 서버에서 로컬 사용자 및 그룹 기능을 설정해야 합니다.

#### 이 작업에 대해

언제든지 로컬 사용자 인증을 활성화 또는 비활성화할 수 있습니다. SMB 연결을 생성할 때 인증에 로컬 사용자를 사용하려면 CIFS 서버의 로컬 사용자 및 그룹 옵션도 설정해야 합니다.

#### 단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

| 로컬 인증을 사용하려는 경우... | 명령 입력...                                                                               |
|--------------------|----------------------------------------------------------------------------------------|
| 활성화됨               | 'vserver cifs options modify<br>-vserver_vserver_name_-is-local-auth-enabled true'     |
| 사용 안 함             | 'vserver cifs options modify<br>-vserver_vserver_name_-is-local-auth-enabled<br>false' |

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

#### 예

다음 예에서는 SVM VS1 에서 로컬 사용자 인증을 사용합니다.

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vservers cifs options modify -vservers vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

## 관련 정보

- [로컬 사용자 인증에 대해 알아보세요](#)
- [서버에서 로컬 사용자 및 그룹 활성화 또는 비활성화](#)

로컬 사용자 계정을 관리합니다

## 로컬 ONTAP SMB 사용자 계정 수정

기존 사용자의 전체 이름 또는 설명을 변경하고 사용자 계정을 활성화하거나 비활성화하려면 로컬 사용자 계정을 수정할 수 있습니다. 사용자 이름이 손상되었거나 관리를 위해 이름 변경이 필요한 경우 로컬 사용자 계정의 이름을 바꿀 수도 있습니다.

| 원하는 작업                    | 명령 입력...                                                                                                                                          |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 로컬 사용자의 전체 이름을 수정합니다      | 'vservers cifs users-and-groups local-user modify -vservers_vserver_name _user-name_user_name_-full-name text' 전체 이름에 공백이 포함되어 있으면 큰따옴표로 묶어야 합니다. |
| 로컬 사용자의 설명을 수정합니다         | 'vservers cifs users-and-groups local-user modify -vservers_vserver_name _user-name_user_name_-description text' 설명에 공백이 포함된 경우 큰따옴표로 묶어야 합니다.    |
| 로컬 사용자 계정을 활성화하거나 비활성화합니다 | 'vservers cifs users-and-groups local-user modify -vservers_vserver_name _user-name_user_name_-is-account-disabled{true                           |
| false}'                   | 로컬 사용자 계정의 이름을 바꿉니다                                                                                                                               |

## 예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 로컬 사용자 "cifs\_server\sue"를 "cifs\_server\sue\_new"로 바꿉니다.1

```
cluster1::> vsserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vsserver vs1
```

## 로컬 **ONTAP SMB** 사용자 계정 활성화 또는 비활성화

사용자가 SMB 연결을 통해 SVM(스토리지 가상 머신)에 포함된 데이터에 액세스할 수 있도록 하려면 로컬 사용자 계정을 활성화합니다. 사용자가 SMB를 통해 SVM 데이터에 액세스하지 못하도록 하려면 로컬 사용자 계정을 사용하지 않도록 설정할 수도 있습니다.

이 작업에 대해

사용자 계정을 수정하여 로컬 사용자를 활성화할 수 있습니다.

단계

1. 적절한 작업을 수행합니다.

| 원하는 작업          | 명령 입력...                                                                                                                  |
|-----------------|---------------------------------------------------------------------------------------------------------------------------|
| 사용자 계정을 활성화합니다  | 'vsserver cifs users-and-groups local-user modify -vsserver_vserver_name_-user-name_user_name_-is-account-disabled false' |
| 사용자 계정을 비활성화합니다 | 'vsserver cifs users-and-groups local-user modify -vsserver_vserver_name_-user-name_user_name_-is-account-disabled true'  |

## 로컬 **ONTAP SMB** 사용자 계정 비밀번호 변경

로컬 사용자의 계정 암호를 변경할 수 있습니다. 이 방법은 사용자의 암호가 손상되었거나 사용자가 암호를 잊어버린 경우에 유용합니다.

단계

1. 'vsserver cifs users-and-groups local-user set-password-vsserver\_vserver\_name\_-user-name\_user\_name\_' 작업을 수행하여 암호를 변경하십시오

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 과 연관된 로컬 사용자 ""cifs\_server\sue""의 암호를 설정합니다.

```
cluster1::> vsserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vsserver vs1

Enter the new password:
Confirm the new password:
```

관련 정보



**ONTAP SMB** 로컬 사용자에게 대한 정보 표시

모든 로컬 사용자의 목록을 요약 양식에 표시할 수 있습니다. 특정 사용자에게 대해 구성된 계정 설정을 확인하려면 해당 사용자에게 대한 자세한 계정 정보와 여러 사용자에게 대한 계정 정보를 표시할 수 있습니다. 이 정보를 통해 사용자 설정을 수정해야 하는지 여부를 확인하고 인증 또는 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

사용자 암호에 대한 정보는 표시되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

| 원하는 작업                              | 명령 입력...                                                                                            |
|-------------------------------------|-----------------------------------------------------------------------------------------------------|
| SVM(스토리지 가상 시스템)의 모든 사용자에게 대한 정보 표시 | 'vserver cifs users-and-groups local-user show -vserver_vserver_name_'                              |
| 사용자에게 대한 자세한 계정 정보를 표시합니다           | 'vserver cifs users-and-groups local-user show-instance-vserver_vserver_name_-user-name_user_name_' |

명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

예

다음 예제는 SVM VS1 의 모든 로컬 사용자에게 대한 정보를 표시합니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver User Name Full Name Description
----- -
vs1 CIFS_SERVER\Administrator James Smith Built-in administrator
account
vs1 CIFS_SERVER\sue Sue Jones
```

로컬 사용자의 **ONTAP SMB** 그룹 멤버십에 대한 정보를 표시합니다.

로컬 사용자가 속한 로컬 그룹에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 파일 및 폴더에 대한 사용자의 액세스 권한을 결정할 수 있습니다. 이 정보는 사용자가 파일 및 폴더에 대해 가질 액세스 권한을 결정하거나 파일 액세스 문제를 해결할 때 유용할 수 있습니다.

이 작업에 대해

명령을 사용자 지정하여 표시할 정보만 표시할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

| 원하는 작업                                              | 명령 입력...                                                                                  |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------|
| 지정된 로컬 사용자의 로컬 사용자 구성원 정보를 표시합니다                    | 'vserver cifs users-and-groups local-user show-membership-user-name_user_name_'           |
| 이 로컬 사용자가 구성원인 로컬 그룹의 로컬 사용자 구성원 정보를 표시합니다          | 'vserver cifs users-and-groups local-user show-membership_group_name_'                    |
| 지정된 SVM(스토리지 가상 머신)과 연결된 로컬 사용자의 사용자 구성원 정보를 표시합니다. | 'vserver cifs users-and-groups local-user show-membership-vserver_vserver_name_'          |
| 지정된 SVM의 모든 로컬 사용자에 대한 세부 정보를 표시합니다                 | 'vserver cifs users-and-groups local-user show-membership-instance-vserver_vserver_name_' |

## 예

다음 예에서는 SVM VS1 상의 모든 로컬 사용자에 대한 구성원 정보를 표시합니다. 사용자 "cifs\_server\Administrator"는 "BUILTIN\Administrators" 그룹의 구성원이고 "cifs\_server\sue"는 "cifs\_server\G1" 그룹의 구성원입니다.

```
cluster1::> vservers cifs users-and-groups local-user show-membership
-vserver vs1
```

| Vserver | User Name                 | Membership             |
|---------|---------------------------|------------------------|
| vs1     | CIFS_SERVER\Administrator | BUILTIN\Administrators |
|         | CIFS_SERVER\sue           | CIFS_SERVER\g1         |

## 로컬 ONTAP SMB 사용자 계정 삭제

CIFS 서버에 대한 로컬 SMB 인증이 더 이상 필요하지 않거나 SVM에 포함된 데이터에 대한 액세스 권한을 결정하기 위해 SVM(스토리지 가상 시스템)에서 로컬 사용자 계정을 삭제할 수 있습니다.

이 작업에 대해

로컬 사용자를 삭제할 때 다음 사항에 유의하십시오.

- 파일 시스템이 변경되지 않았습니다.
- 이 사용자를 참조하는 파일 및 디렉토리의 Windows 보안 설명자는 조정되지 않습니다.
- 로컬 사용자에 대한 모든 참조는 멤버 자격 및 권한 데이터베이스에서 제거됩니다.
- Administrator와 같이 잘 알려진 표준 사용자는 삭제할 수 없습니다.

## 단계

1. 삭제할 로컬 사용자 계정의 이름을 확인합니다. 'vserver cifs users-and-groups local-user show -vserver\_vserver\_name\_'
2. 로컬 사용자 'vserver cifs users-and-groups local-user delete -vserver\_vserver\_name\_-user-name\_username\_name\_'을 삭제합니다
3. 사용자 계정이 삭제되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver\_vserver\_name\_'

## 예

다음 예에서는 SVM VS1 관련 로컬 사용자 ""cifs\_server\sue""를 삭제합니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver User Name Full Name Description
----- -
vs1 CIFS_SERVER\Administrator James Smith Built-in administrator
account
vs1 CIFS_SERVER\sue Sue Jones

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver User Name Full Name Description
----- -
vs1 CIFS_SERVER\Administrator James Smith Built-in administrator
account
```

로컬 그룹을 관리합니다

## 로컬 ONTAP SMB 그룹 수정

기존 로컬 그룹에 대한 설명을 변경하거나 그룹의 이름을 변경하여 기존 로컬 그룹을 수정할 수 있습니다.

| 원하는 작업          | 명령 사용...                                                                                                                                          |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 로컬 그룹 설명을 수정합니다 | 'vserver cifs users-and-groups local-group modify -vserver_vserver_name_-group-name_group_name_-description text' 설명에 공백이 포함되어 있으면 큰따옴표로 묶어야 합니다. |
| 로컬 그룹의 이름을 바꿉니다 | 'vserver cifs users-and-groups local-group rename -vserver_vserver_name_-group-name_group_name_-new-group-name_new_group_name_'                   |

예

다음 예에서는 로컬 그룹 `"cifs_server\engineering"`의 이름을 `"cifs_server\engineering_new"`로 바꿉니다.

```
cluster1::> vsriver cifs users-and-groups local-group rename -vsriver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

다음 예에서는 로컬 그룹 `"cifs_server\engineering"`의 설명을 수정합니다.

```
cluster1::> vsriver cifs users-and-groups local-group modify -vsriver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

### ONTAP SMB 로컬 그룹에 대한 정보 표시

클러스터 또는 지정된 SVM(스토리지 가상 머신)에 구성된 모든 로컬 그룹 목록을 표시할 수 있습니다. 이 정보는 SVM에 포함된 데이터에 대한 파일 액세스 문제 또는 SVM의 사용자 권한(권한) 문제를 해결할 때 유용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

| 에 대한 정보를 원할 경우... | 명령 입력...                                                                |
|-------------------|-------------------------------------------------------------------------|
| 클러스터의 모든 로컬 그룹입니다 | 'vsriver cifs users-and-groups local-group show'를 참조하십시오                |
| SVM의 모든 로컬 그룹     | 'vsriver cifs users-and-groups local-group show -vsriver_vserver_name_' |

이 명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vsriver cifs` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

예

다음 예제는 SVM VS1 의 모든 로컬 그룹에 대한 정보를 표시합니다.

```
cluster1::> vservers cifs users-and-groups local-group show -vservers vs1
```

| Vserver | Group Name               | Description                          |
|---------|--------------------------|--------------------------------------|
| vs1     | BUILTIN\Administrators   | Built-in Administrators group        |
| vs1     | BUILTIN\Backup Operators | Backup Operators group               |
| vs1     | BUILTIN\Power Users      | Restricted administrative privileges |
| vs1     | BUILTIN\Users            | All users                            |
| vs1     | CIFS_SERVER\engineering  |                                      |
| vs1     | CIFS_SERVER\sales        |                                      |

## 로컬 **ONTAP SMB** 그룹 구성원 자격을 관리합니다

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 구성원 자격을 관리할 수 있습니다. 이 기능은 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하려는 경우 또는 사용자에게 해당 그룹에 연결된 권한을 부여하려는 경우에 유용합니다.

이 작업에 대해

로컬 그룹에 구성원을 추가하기 위한 지침:

- special\_everyone\_group에 사용자를 추가할 수 없습니다.
- 사용자를 추가하려면 로컬 그룹이 있어야 합니다.
- 사용자를 로컬 그룹에 추가하려면 사용자가 있어야 합니다.
- 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.
- 도메인 사용자 또는 그룹을 로컬 그룹에 추가하려면 Data ONTAP에서 SID에 대한 이름을 확인할 수 있어야 합니다.

로컬 그룹에서 구성원을 제거하는 지침:

- special\_everyone\_group에서 구성원을 제거할 수 없습니다.
- 구성원을 제거할 그룹이 있어야 합니다.
- ONTAP는 그룹에서 제거하려는 구성원 이름을 해당 SID로 확인할 수 있어야 합니다.

단계

1. 그룹에서 구성원을 추가 또는 제거합니다.

| 원하는 작업         | 그런 다음 명령을 사용합니다...                                                                                                                                                                    |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 그룹에 구성원을 추가합니다 | 'vservers cifs users-and-groups local-group add-member-vserver_name_-group-name_group_name_-member-names name[,...]'지정된 로컬 그룹에 추가할 심표로 구분된 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 목록을 지정할 수 있습니다. |

|                 |                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 원하는 작업          | 그런 다음 명령을 사용합니다...                                                                                                                                                                        |
| 그룹에서 구성원을 제거합니다 | 'vserver cifs users-and-groups local-group remove-members-vserver_name_-group-name_group_name_-member-names name[,...]'지정된 로컬 그룹에서 제거할 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 심표로 구분된 목록을 지정할 수 있습니다. |

다음 예에서는 SVM VS1 상의 로컬 그룹 "sMB\_server\sue"와 도메인 그룹 "AD\_DOM\DOM\_ENG"를 로컬 그룹 "sMB\_server\engineering"에 추가합니다.

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

다음 예에서는 SVM VS1 로컬 그룹 "sMB\_server\sue"와 "sMB\_server\james"를 SVM VS1 로컬 그룹 "sMB\_server\engineering"에서 제거합니다.

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

## 관련 정보

[로컬 그룹 구성원에 대한 정보를 표시합니다](#)

로컬 그룹 구성원에 대한 **ONTAP SMB** 정보 표시

클러스터 또는 지정된 SVM(스토리지 가상 머신)에 구성된 로컬 그룹의 모든 구성원 목록을 표시할 수 있습니다. 이 정보는 파일 액세스 문제 또는 사용자 권한(권한) 문제를 해결할 때 유용할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

|                        |                                                                             |
|------------------------|-----------------------------------------------------------------------------|
| 다음에 대한 정보를 표시하려면...    | 명령 입력...                                                                    |
| 클러스터의 모든 로컬 그룹의 구성원입니다 | 'vserver cifs users-and-groups local-group show-ups'                        |
| SVM에 있는 모든 로컬 그룹의 구성원  | 'vserver cifs users-and-groups local-group show-ners-vserver_vserver_name_' |

예

다음 예는 SVM VS1 로컬 그룹의 모든 구성원에 대한 정보를 표시합니다.

```
cluster1::> vsriver cifs users-and-groups local-group show-members
-vserver vs1
```

| Vserver | Group Name              | Members                                                                    |
|---------|-------------------------|----------------------------------------------------------------------------|
| vs1     | BUILTIN\Administrators  | CIFS_SERVER\Administrator<br>AD_DOMAIN\Domain Admins<br>AD_DOMAIN\dom_grp1 |
|         | BUILTIN\Users           | AD_DOMAIN\Domain Users<br>AD_DOMAIN\dom_usr1                               |
|         | CIFS_SERVER\engineering | CIFS_SERVER\james                                                          |

### 로컬 **ONTAP SMB** 그룹 삭제

SVM(스토리지 가상 시스템)에서 로컬 그룹을 삭제하여 해당 SVM과 관련된 데이터에 대한 액세스 권한을 결정하거나 SVM 사용자 권한(권한)을 그룹 멤버에 할당할 필요가 없는 경우 해당 로컬 그룹을 삭제할 수 있습니다.

이 작업에 대해

로컬 그룹을 삭제할 때 다음 사항에 유의하십시오.

- 파일 시스템이 변경되지 않았습니다.
- 이 그룹을 참조하는 파일 및 디렉토리의 Windows 보안 설명자는 조정되지 않습니다.
- 그룹이 없으면 오류가 반환됩니다.
- special\_everyone\_group은 삭제할 수 없습니다.
- BUILTIN\Administrators\_\_BUILTIN\Users\_와 같은 기본 제공 그룹은 삭제할 수 없습니다.

단계

1. SVM에 로컬 그룹 목록을 표시하여 삭제할 로컬 그룹의 이름을 확인합니다. 'vsriver cifs users-and-groups local-group show -vserver vsriver\_name'
2. 로컬 그룹 'vsriver cifs users-and-groups local-group delete -vserver\_vserver\_name\_-group-name\_group\_name\_'을 삭제합니다
3. 그룹이 삭제되었는지 확인합니다. 'vsriver cifs users-and-groups local-user show -vserver\_vserver\_name\_'

예

다음 예에서는 SVM VS1 관련 로컬 그룹 ""cifs\_server\sales""를 삭제합니다.

```
cluster1::> vservers cifs users-and-groups local-group show -vservers vs1
```

| Vserver | Group Name               | Description                          |
|---------|--------------------------|--------------------------------------|
| vs1     | BUILTIN\Administrators   | Built-in Administrators group        |
| vs1     | BUILTIN\Backup Operators | Backup Operators group               |
| vs1     | BUILTIN\Power Users      | Restricted administrative privileges |
| vs1     | BUILTIN\Users            | All users                            |
| vs1     | CIFS_SERVER\engineering  |                                      |
| vs1     | CIFS_SERVER\sales        |                                      |

```
cluster1::> vservers cifs users-and-groups local-group delete -vservers vs1
-group-name CIFS_SERVER\sales
```

```
cluster1::> vservers cifs users-and-groups local-group show -vservers vs1
```

| Vserver | Group Name               | Description                          |
|---------|--------------------------|--------------------------------------|
| vs1     | BUILTIN\Administrators   | Built-in Administrators group        |
| vs1     | BUILTIN\Backup Operators | Backup Operators group               |
| vs1     | BUILTIN\Power Users      | Restricted administrative privileges |
| vs1     | BUILTIN\Users            | All users                            |
| vs1     | CIFS_SERVER\engineering  |                                      |

로컬 데이터베이스에서 **ONTAP SMB** 도메인 사용자 및 그룹 이름 업데이트

CIFS 서버의 로컬 그룹에 도메인 사용자 및 그룹을 추가할 수 있습니다. 이러한 도메인 개체는 클러스터의 로컬 데이터베이스에 등록됩니다. 도메인 개체의 이름이 변경된 경우 로컬 데이터베이스를 수동으로 업데이트해야 합니다.

이 작업에 대해

도메인 이름을 업데이트할 SVM(스토리지 가상 시스템)의 이름을 지정해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 적절한 작업을 수행합니다.

|                                              |                                                                                               |
|----------------------------------------------|-----------------------------------------------------------------------------------------------|
| 도메인 사용자 및 그룹을 업데이트하려면 다음을 수행합니다.             | 이 명령 사용...                                                                                    |
| 성공적으로 업데이트되었지만 업데이트에 실패한 도메인 사용자 및 그룹을 표시합니다 | 'vservers cifs users-and-groups update-names-vserver_vserver_name_'                           |
| 성공적으로 업데이트된 도메인 사용자 및 그룹을 표시합니다              | 'vservers cifs users-and-groups update-names-vserver_vserver_name_-display-failed-only false' |



|                                  |                                                                                             |
|----------------------------------|---------------------------------------------------------------------------------------------|
| 도메인 사용자 및 그룹을 업데이트하려면 다음을 수행합니다. | 이 명령 사용...                                                                                  |
| 업데이트에 실패한 도메인 사용자 및 그룹만 표시합니다    | 'vserver cifs users-and-groups update-names-vserver_vserver_name_-display-failed-only true' |
| 업데이트에 대한 모든 상태 정보를 표시하지 않습니다     | 'vserver cifs users-and-groups update-names-vserver_vserver_name_-suppress-all-output TRUE' |

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 스토리지 가상 머신(SVM, 이전의 Vserver) VS1 과 관련된 도메인 사용자 및 그룹의 이름을 업데이트합니다. 마지막 업데이트 시 업데이트해야 할 종속 이름 체인이 있습니다.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver: vs1
SID: S-1-5-21-123456789-234565432-987654321-12345
Domain: EXAMPLE1
Out-of-date Name: dom_user1
Updated Name: dom_user2
Status: Successfully updated

Vserver: vs1
SID: S-1-5-21-123456789-234565432-987654322-23456
Domain: EXAMPLE2
Out-of-date Name: dom_user1
Updated Name: dom_user2
Status: Successfully updated

Vserver: vs1
SID: S-1-5-21-123456789-234565432-987654321-123456
Domain: EXAMPLE1
Out-of-date Name: dom_user3
Updated Name: dom_user4
Status: Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
 to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
 to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
 to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
 to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

로컬 권한을 관리합니다

## ONTAP SMB 로컬 또는 도메인 사용자나 그룹에 권한 추가

권한을 추가하여 로컬 또는 도메인 사용자 또는 그룹의 사용자 권한을 관리할 수 있습니다. 추가된 권한은 이러한 개체에 할당된 기본 권한을 재정의합니다. 사용자 또는 그룹에 있는 권한을 사용자 지정할 수 있으므로 보안이 강화됩니다.

시작하기 전에

권한을 추가할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

객체에 권한을 추가하면 해당 사용자 또는 그룹에 대한 기본 권한이 재정의됩니다. 권한을 추가해도 이전에 추가한 권한은 제거되지 않습니다.

로컬 또는 도메인 사용자 또는 그룹에 권한을 추가할 때는 다음 사항을 염두에 두어야 합니다.

- 하나 이상의 권한을 추가할 수 있습니다.
- 도메인 사용자 또는 그룹에 권한을 추가할 때 ONTAP는 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다.

ONTAP가 도메인 컨트롤러에 연결할 수 없는 경우 명령이 실패할 수 있습니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에 하나 이상의 권한을 추가합니다. 'vserver cifs users-and-groups privilege add-privilege-vserver\_name\_-user-or-group-name name name-Privileges\_Privilege\_[,...]'
2. 원하는 권한이 객체에 적용되었는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 사용자 " cifs\_server\sue ""에 "seTcbPrivilege" 및 "setTakeOwnershipPrivilege" 권한을 추가합니다1.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege
```

## ONTAP SMB 로컬 또는 도메인 사용자나 그룹의 권한 제거

권한을 제거하여 로컬 또는 도메인 사용자 또는 그룹에 대한 사용자 권한을 관리할 수 있습니다. 이렇게 하면 사용자와 그룹이 보유한 최대 권한을 사용자 지정할 수 있으므로 보안이 강화됩니다.

시작하기 전에

권한을 제거할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거할 때는 다음 사항을 염두에 두어야 합니다.

- 하나 이상의 권한을 제거할 수 있습니다.
- 도메인 사용자 또는 그룹에서 권한을 제거할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다.

ONTAP가 도메인 컨트롤러에 연결할 수 없는 경우 명령이 실패할 수 있습니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에서 하나 이상의 권한을 제거합니다. 'vserver cifs users-and-groups privilege remove-privilege-vserver\_name\_-user-or-group-name\_name\_-Privileges\_Privilege\_[,...]'
2. 원하는 권한이 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_' 객체에서 제거되었는지 확인합니다

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 사용자 " cifs\_server\sue "(cifs\_server\sue ")에서 "seTcbPrivilege' 및 "setegenershipPrivilege" 권한을 제거합니다1.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue -
```

## ONTAP SMB 로컬 또는 도메인 사용자 및 그룹에 대한 권한 재설정

로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정할 수 있습니다. 이 기능은 로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 수정한 후 해당 수정 사항이 더 이상 필요 또는 필요하지 않을 때 유용합니다.

이 작업에 대해

로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 재설정하면 해당 개체에 대한 권한 항목이 제거됩니다.

## 단계

1. 로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 재설정합니다. 'vserver cifs users-and-groups privilege reset-privilege-vserver\_name\_-user-or-group-name\_name\_'
2. 객체에 대한 권한이 재설정되었는지 확인합니다. 'vserver cifs users-and-groups privilege show -vserver\_vserver\_name\_-user-or-group-name\_name\_'

## 예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 에서 사용자 "cifs\_server\sue"에 대한 권한을 재설정합니다. 기본적으로 일반 사용자는 자신의 계정과 연결된 권한이 없습니다.

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

다음 예제에서는 "BUILTIN\Administrators" 그룹에 대한 권한을 다시 설정하여 권한 항목을 효과적으로 제거합니다.

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver User or Group Name Privileges

vs1 BUILTIN\Administrators SeRestorePrivilege
 SeSecurityPrivilege
 SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

## ONTAP SMB 권한 재정의에 대한 정보 표시

도메인 또는 로컬 사용자 계정 또는 그룹에 할당된 사용자 지정 권한에 대한 정보를 표시할 수 있습니다. 이 정보를 통해 원하는 사용자 권한이 적용되는지 여부를 확인할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

|                                                      |                                                                                       |
|------------------------------------------------------|---------------------------------------------------------------------------------------|
| 다음에 대한 정보를 표시하려면...                                  | 이 명령을 입력하십시오...                                                                       |
| SVM(스토리지 가상 시스템)의 모든 도메인 및 로컬 사용자 및 그룹에 대한 사용자 지정 권한 | 'vserver cifs users-and-groups privilege show -vserver_vserver_name_'                 |
| SVM에서 특정 도메인 또는 로컬 사용자 및 그룹에 대한 사용자 지정 권한            | 'vserver cifs users-and-groups 권한 표시 -vserver_vserver_name_-user-or-group-name_name_' |

이 명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs users-and-groups privilege show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

예

다음 명령을 실행하면 SVM VS1 에 대한 로컬 또는 도메인 사용자 및 그룹과 명시적으로 연결된 모든 권한이 표시됩니다.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 BUILTIN\Administrators SeTakeOwnershipPrivilege
 SeRestorePrivilege
vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege
```

우회 통과 검사를 구성합니다

**ONTAP SMB** 바이패스 트래버스 검사 구성에 대해 알아보세요.

통과 확인 무시 사용자 권한(`_privilege_`라고도 함)은 사용자가 이동 중인 디렉터리에 대한 권한이 없더라도 경로 내의 모든 디렉터리를 파일로 이동할 수 있는지 여부를 결정합니다. 통과 확인을 허용 또는 허용하지 않을 경우 어떤 일이 발생하는지, 그리고 SVM(스토리지 가상 시스템)에서 사용자에게 대한 통과 확인을 건너뛰도록 구성하는 방법을 이해해야 합니다.

우회 통과 확인을 허용 또는 허용하지 않을 때 발생하는 현상

- 허용되는 경우 사용자가 파일에 액세스하려고 할 때 ONTAP는 파일에 대한 액세스 허용 또는 거부 여부를 결정할 때 중간 디렉터리에 대한 통과 권한을 확인하지 않습니다.
- 허용되지 않는 경우 ONTAP는 파일 경로에 있는 모든 디렉터리에 대해 트래버스(실행) 권한을 확인합니다.

중간 디렉터리에 ""X""(통과 권한)이 없으면 ONTAP는 해당 파일에 대한 액세스를 거부합니다.

우회 통과 검사를 구성합니다

ONTAP CLI를 사용하거나 이 사용자 권한으로 Active Directory 그룹 정책을 구성하여 통과 통과 확인 바이패스를 구성할 수 있습니다.

'eChangeNotifyPrivilege' 권한은 사용자가 횡단 확인을 우회할 수 있는지 여부를 제어합니다.

- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에 추가하면 통과 확인을 건너뛸 수 있습니다.
- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에서 제거하면 통과 확인을 건너뛸 수 없습니다.

기본적으로 SVM의 다음 BUILTIN 그룹에는 횡단 확인을 건너뛸 수 있는 권한이 있습니다.

- 'BUILTIN\Administrators'
- 'BUILTIN\Power Users'
- 'BUILTIN\Backup Operators'
- 'BUILTIN\Users'
- '모든 사람'

이러한 그룹 중 하나의 구성원이 통과 확인을 건너뛰도록 허용하지 않으려면 그룹에서 이 권한을 제거해야 합니다.

CLI를 사용하여 SVM에서 로컬 SMB 사용자 및 그룹에 대한 통과 검사를 구성할 때 다음 사항을 염두에 두어야 합니다.

- 사용자 지정 로컬 또는 도메인 그룹의 구성원이 통과 확인을 건너뛰도록 하려면 해당 그룹에 'eChangeNotifyPrivilege' 권한을 추가해야 합니다.
- 개별 로컬 또는 도메인 사용자가 횡단 검사를 무시하도록 허용하고 해당 권한이 있는 그룹의 구성원이 아닌 경우 해당 사용자 계정에 'eChangeNotifyPrivilege' 권한을 추가할 수 있습니다.
- 언제든지 'ChangeNotifyPrivilege' 권한을 제거하여 로컬 또는 도메인 사용자 또는 그룹에 대한 통과 확인을 사용하지 않도록 설정할 수 있습니다.



지정된 로컬 또는 도메인 사용자 또는 그룹에 대한 우회 트래버스 검사를 비활성화하려면 "Everyone" 그룹에서 'ChangeNotifyPrivilege' 권한도 제거해야 합니다.

#### 관련 정보

- [사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다](#)
- [디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다](#)
- [볼륨에서 파일 이름 번역을 위한 문자 매핑 구성](#)
- [공유 액세스 제어 목록 만들기](#)
- [Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다](#)
- [지원되는 권한 목록입니다](#)
- [로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다](#)

사용자 또는 그룹이 **ONTAP SMB** 디렉터리 트래버스 검사를 우회하도록 허용

사용자가 이동 중인 디렉토리에 대한 사용 권한이 없더라도 경로 내의 모든 디렉토리를 통과할 수 있도록 하려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하면 됩니다. 기본적으로 사용자는 디렉터리 통과 확인을 건너뛸 수 있습니다.

시작하기 전에

- SVM에 SMB 서버가 있어야 합니다.
- 로컬 사용자 및 그룹 SMB 서버 옵션을 활성화해야 합니다.
- 'eChangeNotifyPrivilege' 권한을 추가할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

#### 이 작업에 대해

도메인 사용자 또는 그룹에 권한을 추가할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

#### 단계

1. 로컬 또는 도메인 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하여 통과 확인을 사용하지 않도록 설정합니다. 'vserver cifs users-and-groups privilege add-privilege \_vserver\_name\_-user-or-group-name\_name\_-Privileges SeChangeNotifyPrivilege'

'-user-or-group-name' 매개 변수의 값은 로컬 사용자 또는 그룹 또는 도메인 사용자 또는 그룹입니다.

2. 지정된 사용자 또는 그룹이 통과 확인 생략 기능을 사용하도록 설정했는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_'

#### 예

다음 명령을 사용하면 "Example\eng" 그룹에 속한 사용자가 'seChangeNotifyPrivilege' 권한을 그룹에 추가하여 디렉터리 통과 확인을 건너뛸 수 있습니다.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 EXAMPLE\eng SeChangeNotifyPrivilege
```

#### 관련 정보

[디렉터리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다](#)

사용자 또는 그룹이 **ONTAP SMB** 디렉터리 트래버스 검사를 우회하는 것을 허용하지 않음

사용자가 이동 중인 디렉토리에 대한 권한이 없기 때문에 경로 내의 모든 디렉토리를 이동하지 않으려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에서 'seChangeNotifyPrivilege' 권한을 제거할 수 있습니다.

#### 시작하기 전에

권한을 제거할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

#### 이 작업에 대해

도메인 사용자 또는 그룹에서 권한을 제거할 때 ONTAP은 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

#### 단계



1. 통과 확인 무시 허용 안 함: 'vserver cifs users-and-groups privilege remove-privilege-vserver\_vserver\_name\_-user-or-group-name\_name\_-Privileges SeChangeNotifyPrivilege'

이 명령은 '-user-or-group-name\_name\_' 매개 변수 값으로 지정한 로컬 또는 도메인 사용자 또는 그룹에서 'seChangeNotifyPrivilege' 권한을 제거합니다.

2. 지정된 사용자 또는 그룹이 통과 확인을 사용하지 않도록 설정했는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver\_name\_-user-or-group-name\_name\_'

예

다음 명령을 실행하면 디렉토리 트래버스 검사를 거치지 않고 "example\eng" 그룹에 속한 사용자가 사용할 수 없습니다.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 EXAMPLE\eng SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 EXAMPLE\eng -
```

관련 정보

[사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다](#)

파일 보안 및 감사 정책에 대한 정보를 표시합니다

**ONTAP SMB** 파일 보안 및 감사 정책 보기에 대해 알아보세요

SVM(스토리지 가상 머신)의 볼륨 내에 포함된 파일 및 디렉토리의 파일 보안에 대한 정보를 표시할 수 있습니다. FlexVol 볼륨의 감사 정책에 대한 정보를 표시할 수 있습니다. 구성된 경우 FlexVol 볼륨의 저장소 수준 액세스 가드 및 동적 액세스 제어 보안 설정에 대한 정보를 표시할 수 있습니다.

파일 보안에 대한 정보 표시

다음 보안 스타일을 사용하여 볼륨 및 Qtree(FlexVol 볼륨의 경우) 내에 포함된 데이터에 적용되는 파일 보안에 대한 정보를 표시할 수 있습니다.

- NTFS입니다
- Unix
- 혼합

## 감사 정책에 대한 정보 표시

다음 NAS 프로토콜을 통해 FlexVol 볼륨의 액세스 이벤트를 감사하기 위한 감사 정책에 대한 정보를 표시할 수 있습니다.

- SMB(모든 버전)
- NFSv4.x

## 스토리지 레벨 액세스 가드(슬래그) 보안에 대한 정보 표시

스토리지 레벨 액세스 가드 보안은 FlexVol 볼륨 및 qtree 개체에 다음 보안 스타일로 적용할 수 있습니다.

- NTFS입니다
- 혼합
- UNIX(볼륨을 포함하는 SVM에서 CIFS 서버가 구성된 경우)

## DAC(Dynamic Access Control) 보안에 대한 정보 표시

동적 액세스 제어 보안은 다음 보안 스타일을 사용하여 FlexVol 볼륨 내의 개체에 적용할 수 있습니다.

- NTFS입니다
- 혼합(오브젝트에 NTFS 유효 보안이 있는 경우)

## 관련 정보

- [Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요](#)
- [서버의 Storage-Level Access Guard에 대한 정보 표시](#)

## NTFS 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시

NTFS 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안 스타일, 적용되는 권한, DOS 속성 정보 등)를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

## 이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용하므로 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.
- ACL 출력은 NTFS 보안이 설정된 파일 및 폴더에 대해 표시됩니다.
- 볼륨 루트 또는 qtree에서 Storage-Level Access Guard 보안을 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 ACL과 Storage-Level Access Guard ACL이 모두 표시될 수 있습니다.
- 또한 동적 액세스 제어가 지정된 파일 또는 디렉터리 경로에 대해 구성된 경우 이 출력에는 동적 액세스 제어 ACE에 대한 정보도 표시됩니다.

## 단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------|
| 요약 양식        | 'vserver security file-directory show<br>-vserver_vserver_name_-path_path_'                     |
| 세부 정보가 확장됩니다 | 'vserver security file-directory show<br>-vserver_vserver_name_-path_path_-expand-mask<br>true' |

예

다음 예제는 SVM VS1 경로의 /vol4" 보안 정보를 보여줍니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

Vserver: vs1
File Path: /vol4
File Inode Number: 64
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
ALLOW-Everyone-0x10000000-
```

OI|CI|IO

다음 예에서는 SVM VS1 경로의 /data/engineering에 대한 확장된 마스크와 함께 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

Vserver: vs1
File Path: /data/engineering
File Inode Number: 5544
```

```

Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
 ...0 = Offline
 0. = Sparse
 0... = Normal
 0. = Archive
 1 = Directory
 0.. = System
 0. = Hidden
 0 = Read Only
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004

 1... = Self Relative
 .0.. = RM Control Valid
 ..0. = SACL Protected
 ...0 = DACL Protected
 0... = SACL Inherited
 0.. = DACL Inherited
 0. = SACL Inherit Required
 0 = DACL Inherit Required
 0. = SACL Defaulted
 0 = SACL Present
 0... = DACL Defaulted
 1.. = DACL Present
 0. = Group Defaulted
 0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 0... =
Generic Read
 .0.. =
Generic Write
 ..0. =
Generic Execute
 ...0 =

```

|                                    |             |   |
|------------------------------------|-------------|---|
| Generic All                        | .....0..... | = |
| System Security                    | .....1..... | = |
| Synchronize                        | .....1..... | = |
| Write Owner                        | .....1..... | = |
| Write DAC                          | .....1..... | = |
| Read Control                       | .....1..... | = |
| Delete                             | .....1..... | = |
| Write Attributes                   | .....1..... | = |
| Read Attributes                    | .....1..... | = |
| Delete Child                       | .....1..... | = |
| Execute                            | .....1..... | = |
| Write EA                           | .....1..... | = |
| Read EA                            | .....1..... | = |
| Append                             | .....1..... | = |
| Write                              | .....1..... | = |
| Read                               | .....1..... | = |
| ALLOW-Everyone-0x10000000-OI CI IO |             |   |
| Generic Read                       | 0.....      | = |
| Generic Write                      | .0.....     | = |
| Generic Execute                    | ..0.....    | = |
| Generic All                        | ...1.....   | = |
| System Security                    | .....0..... | = |
| Synchronize                        | .....0..... | = |

|                  |               |
|------------------|---------------|
| Write Owner      | .....0..... = |
| Write DAC        | .....0..... = |
| Read Control     | .....0..... = |
| Delete           | .....0..... = |
| Write Attributes | .....0..... = |
| Read Attributes  | .....0..... = |
| Delete Child     | .....0..... = |
| Execute          | .....0..... = |
| Write EA         | .....0..... = |
| Read EA          | .....0..... = |
| Append           | .....0..... = |
| Write            | .....0..... = |
| Read             | .....0..... = |

다음 예에서는 SVM VS1 에서 경로 '/datavol1'이 있는 볼륨에 대한 Storage-Level Access Guard 보안 정보를 비롯한 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
```

```

 Vserver: vs1
 File Path: /datavol1
 File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-OI|CI|IO

 Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

#### 관련 정보

- [혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다](#)
- [UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다](#)

보안 스타일 및 효과적인 보안 스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등 혼합 보안 스타일 볼륨에 대한 파일 및 디렉터리 보안에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- 혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉터리 등 UNIX 파일 권한을 사용하는 일부 파일 및 폴더가 포함될 수 있습니다.
- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 있을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉터리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 UNIX 파일 사용 권한과 Storage-Level Access Guard ACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉터리 경로에 동적 액세스 제어기가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------|
| 요약 양식        | 'vserver security file-directory show -vserver vservice_name -path path path'                   |
| 세부 정보가 확장됩니다 | 'vserver security file-directory show -vserver vservice_name -path path path -expand-mask true' |

예

다음 예에서는 SVM VS1 경로 '/projects'에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다. 이 혼합 보안 방식 경로에는 UNIX의 효과적인 보안이 있습니다.



```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```
 Vserver: vs1
 File Path: /projects
File Inode Number: 78
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
 ...0 = Offline
 0. = Sparse
 0... = Normal
 0. = Archive
 1 = Directory
 0.. = System
 0. = Hidden
 0 = Read Only
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 700
Unix Mode Bits in Text: rwx-----
 ACLs: -
```

다음 예제는 SVM VS1 경로 '/data'에 대한 보안 정보를 보여줍니다. 이 혼합 보안 방식 경로에는 NTFS의 효과적인 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

 Vserver: vs1
 File Path: /data
 File Inode Number: 544
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-
```

OI|CI|IO

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에 있는 볼륨에 대한 보안 정보를 표시합니다. 이러한 혼합 보안 유형의 최상위 수준에는 UNIX의 효과적인 보안이 있습니다. 이 볼륨에는 Storage-Level Access Guard 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
 Vserver: vs1
 File Path: /datavol5
 File Inode Number: 3374
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
 ACLs: Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 AUDIT-EXAMPLE\market-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-EXAMPLE\market-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 AUDIT-EXAMPLE\market-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-EXAMPLE\market-0x1f01ff
```

#### 관련 정보

- [NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다](#)
- [UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다](#)

**UNIX** 보안 스타일 볼륨에서 **ONTAP SMB** 파일 보안에 대한 정보 표시

UNIX 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안 스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등)를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 디렉토리 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 모드 비트 또는 NFSv4 ACL 중 하나의 UNIX 파일 권한만 사용합니다.
- NFSv4 보안이 설정된 파일 및 폴더에 대해서만 ACL 출력이 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉토리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- NFSv4 보안 설명자의 경우 ACL 출력의 소유자 및 그룹 출력 필드는 적용되지 않습니다.

NTFS 보안 설명자에만 의미가 있습니다.

- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------|
| 요약 양식        | 'vserver security file-directory show<br>-vserver_vserver_name_-path_path_'                     |
| 세부 정보가 확장됩니다 | 'vserver security file-directory show<br>-vserver_vserver_name_-path_path_-expand-mask<br>true' |

예

다음 예제는 SVM VS1 경로의 / home 경로에 대한 보안 정보를 표시합니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

 Vserver: vs1
 File Path: /home
 File Inode Number: 9590
 Security Style: unix
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx-----
 ACLs: -
```

다음 예에서는 SVM VS1 경로의 /home 경로에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

 Vserver: vs1
 File Path: /home
 File Inode Number: 9590
 Security Style: unix
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: 0x10
 ...0 = Offline
 0. = Sparse
 0... = Normal
 0. = Archive
 1 = Directory
 0.. = System
 0. = Hidden
 0 = Read Only
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx-----
 ACLs: -
```

- 보안 스타일 볼륨의 파일 보안에 대한 정보 표시
- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다

**SMB FlexVol** 볼륨의 **NTFS** 감사 정책에 대한 정보를 표시하는 **ONTAP** 명령

FlexVol 볼륨에서 보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 시스템 액세스 제어 목록에 대한 정보를 포함하여 NTFS 감사 정책에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 폴더의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 감사 정책에 NTFS SACL(시스템 액세스 제어 목록)만 사용합니다.
- NTFS 효과적인 보안이 적용된 혼합 보안 스타일 볼륨의 파일과 폴더에 NTFS 감사 정책이 적용될 수 있습니다.

혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 포함될 수 있으며 NTFS SACL이 포함될 수도 있고 포함되지 않을 수도 있습니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 및 폴더 NFSv4 SACL 및 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.
- NTFS 유효 보안이 있는 파일 및 폴더에 대한 보안 정보를 표시할 때 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.

NTFS 보안 스타일 파일 및 폴더는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용합니다.

- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.

단계

1. 파일 및 디렉터리 감사 정책 설정을 원하는 수준으로 표시합니다.

| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                              |
|--------------|------------------------------------------------------------------------------|
| 요약 양식        | 'vserver security file-directory show -vserver vserver_name -path path path' |

|              |                                                                                                |
|--------------|------------------------------------------------------------------------------------------------|
| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                                                |
| 를 참조하십시오     | 'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true' |

예

다음 예에서는 SVM VS1 경로의 /Corp 경로에 대한 감사 정책 정보를 표시합니다. 경로에 NTFS 유효 보안이 있습니다. NTFS 보안 설명자는 성공 및 성공/실패 SACL 항목을 모두 포함합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
 Vserver: vs1
 File Path: /corp
 File Inode Number: 357
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8014
 Owner:DOMAIN\Administrator
 Group:BUILTIN\Administrators
 SACL - ACEs
 ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
 SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
 DACL - ACEs
 ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
 ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
 ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

다음 예제는 SVM VS1 경로의 /datavol1 경로에 대한 감사 정책 정보를 표시합니다. 이 경로에는 일반 파일 및 폴더 SACL과 Storage-Level Access Guard SACL이 모두 포함됩니다.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

 Vserver: vs1
 File Path: /datavol1
 File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0xaa14
 Owner: BUILTIN\Administrators
 Group: BUILTIN\Administrators
 SACL - ACEs
 AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
 DACL - ACEs
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
 ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

 Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

**SMB FlexVol** 볼륨의 **NFSv4** 감사 정책에 대한 정보를 표시하는 **ONTAP** 명령

보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 SACL(시스템 액세스 제어 목록)에 대한 정보를 포함하여 ONTAP CLI를 사용하여 FlexVol 볼륨에서 NFSv4 감사 정책에 대한



정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 디렉토리의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 감사 정책에 NFSv4 SACL만 사용합니다.
- UNIX 보안 스타일의 혼합 보안 스타일 볼륨에 있는 파일과 디렉토리에는 NFSv4 감사 정책이 적용될 수 있습니다.

혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준은 UNIX 또는 NTFS의 유효 보안을 가질 수 있으며 NFSv4 SACL을 포함하거나 포함하지 않을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 NFSv4 파일 및 디렉터리 SACL과 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

| 정보를 표시하려면... | 다음 명령을 입력합니다...                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------|
| 요약 양식        | 'vserver security file-directory show -vserver vservice_name -path path path'                   |
| 세부 정보가 확장됩니다 | 'vserver security file-directory show -vserver vservice_name -path path path -expand-mask true' |

예

다음 예제는 SVM VS1 경로 /lab에 대한 보안 정보를 보여 줍니다. 이 UNIX 보안 스타일 경로에는 NFSv4 SACL이 있습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab
```

```

 Vserver: vs1
 File Path: /lab
 File Inode Number: 288
 Security Style: unix
 Effective Style: unix
 DOS Attributes: 11
 DOS Attributes in Text: ----D--R
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 0
 Unix Mode Bits in Text: -----
 ACLs: NFSV4 Security Descriptor
 Control:0x8014
 SACL - ACEs
 SUCCESSFUL-S-1-520-0-0xf01ff-SA
 FAILED-S-1-520-0-0xf01ff-FA
 DACL - ACEs
 ALLOW-S-1-520-1-0xf01ff
```

**ONTAP SMB** 파일 보안 및 감사 정책 정보를 표시하는 방법을 알아보세요.

와일드카드 문자(\*)를 사용하여 지정된 경로 또는 루트 볼륨 아래에 있는 모든 파일 및 디렉토리의 파일 보안 및 감사 정책에 대한 정보를 표시할 수 있습니다.

와일드카드 문자(\*)는 모든 파일 및 디렉토리의 정보를 표시할 아래의 지정된 디렉터리 경로의 마지막 하위 구성 요소로 사용할 수 있습니다. "" \* ""로 명명된 특정 파일이나 디렉토리의 정보를 표시하려면 큰따옴표("") 안에 전체 경로를 제공해야 합니다.

예

와일드카드 문자를 사용하여 다음 명령을 실행하면 SVM VS1 경로의 '/1/' 아래에 있는 모든 파일 및 디렉토리에 대한 정보가 표시됩니다.

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

 Vserver: vs1
 File Path: /1/1
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8514
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

 Vserver: vs1
 File Path: /1/1/abc
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8404
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

다음 명령을 실행하면 SVM VS1 의 path '/vol1/a' 아래에 " \*"로 명명된 파일의 정보가 표시됩니다. 경로는 큰따옴표(")로 묶습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"
```

```
 Vserver: vs1
 File Path: "/vol1/a/*"
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 1002
 Unix Group Id: 65533
 Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
 ACLs: NFSV4 Security Descriptor
 Control:0x8014
 SACL - ACEs
 AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
 DACL - ACEs
 ALLOW-EVERYONE@-0x1f00a9-FI|DI
 ALLOW-OWNER@-0x1f01ff-FI|DI
 ALLOW-GROUP@-0x1200a9-IG
```

**CLI를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다**

**SMB NTFS 파일 보안, NTFS 감사 정책 및 스토리지 수준 액세스 보호 관리를 위한 ONTAP 명령**

CLI를 사용하여 스토리지 가상 시스템(SVM)에서 NTFS 파일 보안, NTFS 감사 정책 및 스토리지 레벨 액세스 가드를 관리할 수 있습니다.

SMB 클라이언트 또는 CLI를 사용하여 NTFS 파일 보안 및 감사 정책을 관리할 수 있습니다. 그러나 CLI를 사용하여 파일 보안 및 감사 정책을 구성하면 원격 클라이언트를 사용하여 파일 보안을 관리할 필요가 없습니다. CLI를 사용하면 단일 명령을 사용하여 여러 파일과 폴더에 보안을 적용하는 데 걸리는 시간을 크게 줄일 수 있습니다.

ONTAP에서 SVM 볼륨에 적용한 또 다른 보안 계층인 스토리지 레벨 액세스 가드를 구성할 수 있습니다. Storage-Level Access Guard는 모든 NAS 프로토콜에서 Storage-Level Access Guard가 적용되는 스토리지 객체에 대한 액세스에 적용됩니다.

스토리지 레벨 액세스 가드는 ONTAP CLI에서만 구성 및 관리할 수 있습니다. SMB 클라이언트에서 스토리지 수준 액세스 가드 설정을 관리할 수 없습니다. 또한 NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다. 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 액세스 가드 보안을 취소할 수 없습니다. 따라서 Storage-Level Access Guard는 스토리지 관리자가 독립적으로 설정하고 관리하는 데이터 액세스를 위한 추가 보안 계층을 제공합니다.



스토리지 레벨 액세스 가드에 대해 NTFS 액세스 권한만 지원되지만, ONTAP는 UNIX 사용자가 볼륨을 소유하는 SVM에서 Windows 사용자에게 매핑될 경우 스토리지 레벨 액세스 가드가 적용되는 볼륨의 데이터에 대해 NFS에 대한 액세스를 위한 보안 검사를 수행할 수 있습니다.

## NTFS 보안 스타일 볼륨

NTFS 보안 스타일 볼륨 및 Qtree에 포함된 모든 파일 및 폴더는 NTFS의 효율적인 보안을 사용합니다. "vserver security file-directory" 명령 제품군을 사용하여 NTFS 보안 스타일 볼륨에 다음 유형의 보안을 구현할 수 있습니다.

- 볼륨에 포함된 파일 및 폴더에 대한 파일 권한 및 감사 정책
- 볼륨에 대한 스토리지 레벨 액세스 가드 보안

## 혼합 보안 형식 볼륨

혼합 보안 스타일 볼륨 및 qtree에는 UNIX의 효과적인 보안이 있는 일부 파일과 폴더가 포함될 수 있으며, 모드 비트 또는 NFSv4.x ACL 및 NFSv4.x 감사 정책, NTFS 효과적인 보안이 설정된 일부 파일 및 폴더, NTFS 파일 권한 및 감사 정책을 사용하는 일부 파일 및 폴더가 포함될 수 있습니다. 'vserver security file-directory' 명령 제품군을 사용하여 혼합 보안 스타일 데이터에 다음 유형의 보안을 적용할 수 있습니다.

- 혼합 볼륨 또는 qtree에서 NTFS 유효 보안 유형을 사용하는 파일 및 폴더에 대한 파일 권한 및 감사 정책
- 스토리지 레벨 액세스 NTFS 및 UNIX의 효율적인 보안 방식으로 볼륨에 대한 보호

## Unix 보안 스타일 볼륨

UNIX 보안 스타일 볼륨 및 qtree에는 UNIX 유효 보안(모드 비트 또는 NFSv4.x ACL)이 있는 파일 및 폴더가 포함되어 있습니다. UNIX 보안 스타일 볼륨에 보안을 구현하기 위해 'vserver security file-directory' 명령 제품군을 사용하려면 다음 사항을 염두에 두어야 합니다.

- "vserver security file-directory" 명령 제품군은 UNIX 보안 스타일 볼륨 및 qtree에서 UNIX 파일 보안 및 감사 정책을 관리하는 데 사용할 수 없습니다.
- SVM과 타겟 볼륨에 CIFS 서버가 포함된 경우 "vserver security file-directory" 명령 제품군을 사용하여 UNIX 보안 스타일 볼륨에서 Storage-Level Access Guard를 구성할 수 있습니다.

## 관련 정보

- [파일 보안 및 감사 정책 보기에 대해 알아보세요](#)
- [서버에 NTFS 보안 설명자 만들기](#)
- [파일 및 폴더에 감사 정책을 구성하고 적용하는 명령](#)
- [Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요](#)

## SMB 파일 및 폴더 보안을 설정하기 위한 ONTAP 명령

원격 클라이언트의 개입 없이 로컬로 파일 및 폴더 보안을 적용 및 관리할 수 있으므로 많은 수의 파일 또는 폴더에 대해 대량 보안을 설정하는 데 걸리는 시간을 크게 줄일 수 있습니다.

CLI를 사용하여 다음과 같은 사용 사례에서 파일 및 폴더 보안을 설정할 수 있습니다.

- 홈 디렉토리의 파일 스토리지와 같은 대규모 엔터프라이즈 환경에 있는 파일의 스토리지
- 데이터 마이그레이션
- Windows 도메인 변경
- NTFS 파일 시스템 전반에 걸쳐 파일 보안 및 감사 정책 표준화

ONTAP 명령을 사용하여 **SMB** 파일 및 폴더 보안을 설정할 때의 제한 사항에 대해 알아보세요.

CLI를 사용하여 파일 및 폴더 보안을 설정할 때 특정 제한 사항을 알고 있어야 합니다.

- 'vserver security file-directory' 명령 제품군은 NFSv4 ACL 설정을 지원하지 않습니다.

NTFS 보안 설명자는 NTFS 파일 및 폴더에만 적용할 수 있습니다.

보안 설명자를 사용하여 **ONTAP SMB** 파일 및 폴더 보안을 적용합니다.

보안 설명자는 사용자가 파일 및 폴더에 대해 수행할 수 있는 작업과 사용자가 파일 및 폴더에 액세스할 때 감사할 작업을 결정하는 액세스 제어 목록을 포함합니다.

- \* 권한 \*

권한은 개체의 소유자가 허용하거나 거부하고 개체(사용자, 그룹 또는 컴퓨터 개체)가 지정된 파일이나 폴더에서 수행할 수 있는 작업을 결정합니다.

- \* 보안 설명자 \*

보안 설명자는 파일 또는 폴더와 관련된 권한을 정의하는 보안 정보가 포함된 데이터 구조입니다.

- \* ACL(액세스 제어 목록) \*

액세스 제어 목록은 보안 설명자가 적용된 파일 또는 폴더에서 사용자, 그룹 또는 컴퓨터 개체가 수행할 수 있는 작업에 대한 정보를 포함하는 보안 설명자에 포함된 목록입니다. 보안 설명자는 다음 두 가지 유형의 ACL을 포함할 수 있습니다.

- DACL(임의 액세스 제어 목록)
- 시스템 액세스 제어 목록(SACL)

- \* DACL(임의 액세스 제어 목록) \*

DACL에는 파일 또는 폴더에 대한 작업을 수행할 수 있는 액세스가 허용 또는 거부된 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. DACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- \* 시스템 액세스 제어 목록(SACL) \*

SACL에는 성공 또는 실패 감사 이벤트가 기록되는 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. SACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- \* ACE(액세스 제어 항목) \*

ACE는 DACL 또는 SACL의 개별 항목입니다.

- DACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에 대해 허용 또는 거부된 액세스 권한을 지정합니다.
- SACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에서 수행하는 지정된 작업을 감사할 때 기록할 성공 또는 실패 이벤트를 지정합니다.

- \* 사용 권한 상속 \*

권한 상속에서는 보안 설명자에 정의된 권한이 부모 개체에서 개체로 전파되는 방법을 설명합니다. 상속 가능한 권한만 자식 개체에서 상속합니다. 상위 객체에 대한 권한을 설정할 때 폴더, 하위 폴더, 파일이 이 폴더에 적용, 하위 폴더, 파일 등을 통해 해당 항목을 상속할 수 있는지 여부를 결정할 수 있습니다.

#### 관련 정보

- ["SMB 및 NFS 감사 및 보안 추적"](#)
- [파일 및 폴더에 감사 정책을 구성하고 적용하는 명령](#)

**ONTAP SVM** 재해 복구 대상에서 로컬 **SMB** 사용자 또는 그룹을 사용하는 파일 디렉토리 정책을 적용하는 방법에 대해 알아보세요.

파일 디렉토리 정책 구성에서 보안 설명자나 DACL 또는 SACL 항목의 로컬 사용자 또는 그룹을 사용하는 경우 ID 폐기 구성의 SVM(Storage Virtual Machine) 재해 복구 대상에 파일 디렉토리 정책을 적용하기 전에 염두에 두어야 할 몇 가지 지침이 있습니다.

소스 클러스터의 소스 SVM이 소스 SVM에서 데이터 및 구성을 소스 SVM에서 타겟 클러스터의 대상 SVM으로 복제하는 SVM을 위한 재해 복구 구성을 구성할 수 있습니다.

SVM 재해 복구의 두 가지 유형 중 하나를 설정할 수 있습니다.

- ID가 보존됩니다

이 구성에서는 SVM과 CIFS 서버의 ID가 보존됩니다.

- ID가 삭제되었습니다

이 구성에서는 SVM과 CIFS 서버의 ID가 유지되지 않습니다. 이 시나리오에서는 대상 SVM의 SVM 및 CIFS 서버의 이름이 소스 SVM의 SVM 및 CIFS 서버 이름과 다릅니다.

#### ID 폐기 구성에 대한 지침

로컬 사용자, 그룹 및 권한 구성이 포함된 SVM 소스의 경우 ID가 폐기된 구성에서 SVM 대상의 CIFS 서버 이름과 일치하도록 로컬 도메인(로컬 CIFS 서버 이름)의 이름을 변경해야 합니다. 예를 들어, 소스 SVM 이름이 `""VS1""`이고 CIFS 서버 이름이 `""CIFS1""`이고 대상 SVM 이름이 `""VS1_DST""`이고 CIFS 서버 이름이 `""CIFS1_DST""`인 경우 로컬 사용자 `""CIFS1\user1""`의 로컬 도메인 이름이 `""FS1""`로 자동 변경됩니다.

```
cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1_dst
```

| Vsriver               | User Name           | Full Name | Description |
|-----------------------|---------------------|-----------|-------------|
| vs1                   | CIFS1\Administrator |           | Built-in    |
| administrator account |                     |           |             |
| vs1                   | CIFS1\user1         | -         | -           |

```
cluster1dst::> vsriver cifs users-and-groups local-user show -vsriver vs1_dst
```

| Vsriver               | User Name               | Full Name | Description |
|-----------------------|-------------------------|-----------|-------------|
| vs1_dst               | CIFS1_DST\Administrator |           | Built-in    |
| administrator account |                         |           |             |
| vs1_dst               | CIFS1_DST\user1         | -         | -           |

로컬 사용자 및 그룹 데이터베이스에서 로컬 사용자 및 그룹 이름이 자동으로 변경되더라도 파일 디렉토리 정책 구성('vsriver security file-directory' 명령 제품군을 사용하여 CLI에 구성된 정책)에서 로컬 사용자 또는 그룹 이름이 자동으로 변경되지 않습니다.

예를 들어, "vs1"의 경우 "-account" 매개 변수가 "CIFS1\user1"로 설정된 DACL 항목을 구성한 경우 대상의 CIFS 서버 이름을 반영하도록 대상 SVM에서 설정이 자동으로 변경되지 않습니다.

```
cluster1::> vsriver security file-directory ntfs dacl show -vsriver vs1
```

```
Vsriver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

| Account Name | Access Type | Access Rights | Apply To    |
|--------------|-------------|---------------|-------------|
| CIFS1\user1  | allow       | full-control  | this-folder |

```
cluster1::> vsriver security file-directory ntfs dacl show -vsriver vs1_dst
```

```
Vsriver: vs1_dst
```

```
NTFS Security Descriptor Name: sd1
```

| Account Name    | Access Type | Access Rights | Apply To    |
|-----------------|-------------|---------------|-------------|
| **CIFS1**\user1 | allow       | full-control  | this-folder |



CIFS 서버 이름을 대상 CIFS 서버 이름으로 수동으로 변경하려면 'vserver security file-directory modify' 명령을 사용해야 합니다.

계정 매개 변수가 포함된 파일 디렉토리 정책 구성 구성 요소입니다

로컬 사용자 또는 그룹을 포함할 수 있는 매개 변수 설정을 사용할 수 있는 세 가지 파일 디렉토리 정책 구성 구성 요소가 있습니다.

- 보안 설명자

필요에 따라 보안 설명자의 소유자와 보안 설명자의 소유자의 기본 그룹을 지정할 수 있습니다. 보안 설명자가 소유자 및 기본 그룹 항목에 대해 로컬 사용자 또는 그룹을 사용하는 경우, 계정 이름에 대상 SVM을 사용하도록 보안 설명자를 수정해야 합니다. 'vserver security file-directory NTFS modify' 명령을 사용하여 계정 이름을 필요에 따라 변경할 수 있습니다.

- DACL 항목

각 DACL 항목은 계정과 연결되어 있어야 합니다. 대상 SVM 이름을 사용하려면 로컬 사용자 또는 그룹 계정을 사용하는 모든 DACL을 수정해야 합니다. 기존 DACL 항목에 대한 계정 이름을 수정할 수 없으므로 보안 설명자에서 로컬 사용자 또는 그룹의 DACL 항목을 제거하고 수정된 대상 계정 이름으로 새 DACL 항목을 만든 다음 이러한 새 DACL 항목을 적절한 보안 설명자와 연결해야 합니다.

- SACL 항목

각 SACL 항목은 계정과 연결되어 있어야 합니다. 대상 SVM 이름을 사용하려면 로컬 사용자 또는 그룹 계정을 사용하는 SACL을 수정해야 합니다. 기존 SACL 항목에 대한 계정 이름을 수정할 수 없으므로 보안 설명자에서 로컬 사용자 또는 그룹을 가진 SACL 항목을 제거하고 수정된 대상 계정 이름으로 새 SACL 항목을 만든 다음 이러한 새 SACL 항목을 적절한 보안 설명자와 연결해야 합니다.

정책을 적용하기 전에 파일 디렉토리 정책 구성에 사용되는 로컬 사용자 또는 그룹을 변경해야 합니다. 그렇지 않으면 적용 작업이 실패합니다.

**CLI**를 사용하여 **NTFS** 파일 및 폴더에 파일 보안을 구성하고 적용합니다

## **ONTAP SMB 서버에서 NTFS 보안 설명자 생성**

NTFS 보안 설명자(파일 보안 정책)를 생성하는 것은 NTFS ACL(액세스 제어 목록)을 구성하여 SVM(스토리지 가상 머신) 내에 있는 파일 및 폴더에 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결할 수 있습니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

| 오브젝트                      | 액세스 유형입니다 | 액세스 권한 | 사용 권한을 적용할 위치입니다 |
|---------------------------|-----------|--------|------------------|
| BUILTIN\Administrators입니다 | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |
| BUILTIN\사용자               | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |
| 작성자 소유자                   | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |
| NT AUTHORITY\SYSTEM       | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다
- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 ["ONTAP 명령 참조입니다"](#) 참조하십시오.

#### ONTAP SMB 서버의 NTFS 보안 설명자에 NTFS DACL 액세스 제어 항목 추가

NTFS 보안 설명자에 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)를 추가하는 것은 파일이나 폴더에 NTFS ACL을 구성하고 적용하는 두 번째 단계입니다. 각 항목은 액세스가 허용되거나 거부된 개체를 식별하고 ACE에 정의된 파일 또는 폴더에 대해 개체가 수행할 수 있거나 수행할 수 없는 작업을 정의합니다.

이 작업에 대해

보안 설명자의 DACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 DACL이 포함된 경우 명령은 새 ACE를 DACL에 추가합니다. 보안 설명자에 DACL이 포함되어 있지 않으면 명령에서 DACL을 생성하고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정에 대해 허용 또는 거부할 권한을 지정하여 DACL 항목을 선택적으로 사용자 지정할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)



DACL 항목에 대한 권한을 지정하지 않으면 기본값은 "모든 권한"으로 설정됩니다.

선택적으로 상속 적용 방법을 지정하여 DACL 항목을 사용자 지정할 수 있습니다.

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 이 절차에서 설명하는 명령에 대한 자세한

내용은 를 ["ONTAP 명령 참조입니다"](#)참조하십시오.

#### 단계

1. 보안 설명자에 DACL 항목을 추가합니다. 'vserver security file -directory NTFS DACL add -vserver vs1 -ntfs -sd sd1 -access-type {allow | deny} -account name\_or\_SID optional\_parameters'

```
'vserver security file-directory NTFS DACL add-NTFS-SD SD1-access-type deny-account domain\joe-
rights full-control-apply-to this-folder-vserver-vs1'
```

2. DACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS DACL show -vserver vs1 -ntfs -sd sd1 -access-type {allow|deny} -account name\_or\_SID'

```
'vserver security file-directory NTFS DACL show -vserver vs1-ntfs-sd SD1-access-type deny-account
domain\joe'
```

```
Vserver: vs1
Security Descriptor Name: sd1
 Allow or Deny: deny
 Account Name or SID: DOMAIN\joe
 Access Rights: full-control
Advanced Access Rights: -
 Apply To: this-folder
 Access Rights: full-control
```

에 대한 자세한 내용은 `vserver security file-directory ntfs dacl` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

### ONTAP SMB 보안 정책 생성

SVM에 대한 파일 보안 정책을 생성하는 것은 파일이나 폴더에 ACL을 구성 및 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각 작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

#### 단계

1. 'vserver security file-directory policy create-vserver vs1-policy-name policy\_name' 보안 정책을 생성합니다

```
'vserver security file-directory policy create-policy-name policy1-vserver vs1'
```

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
Vserver Policy Name

vs1 policy1
```

## ONTAP SMB 보안 정책에 작업 추가

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 디렉터리 작업을 통해 적용된 ACL은 SMB 클라이언트 또는 ONTAP CLI를 통해 관리할 수 있습니다.

- 스토리지 레벨 액세스 가드 작업

지정된 볼륨에 Storage-Level Access Guard 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 스토리지 레벨 액세스 가드 작업을 통해 적용된 ACL은 ONTAP CLI를 통해서만 관리할 수 있습니다.

작업에는 파일(또는 폴더) 또는 파일 집합(또는 폴더)의 보안 구성에 대한 정의가 포함됩니다. 정책의 모든 작업은 경로로 고유하게 식별됩니다. 단일 정책 내에서 경로당 하나의 작업만 있을 수 있습니다. 정책에 중복된 작업 항목이 있을 수 없습니다.

정책에 작업 추가 지침:

- 정책당 최대 10,000개의 작업 항목이 있을 수 있습니다.
- 정책에는 하나 이상의 작업이 포함될 수 있습니다.

정책에 둘 이상의 작업이 포함될 수 있지만 파일 디렉터리 및 저장소 수준 액세스 가드 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉터리 작업이 포함되어야 합니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

추가 액세스 권한은 제공하지 않습니다.

보안 정책에 작업을 추가할 때 다음 네 가지 필수 매개 변수를 지정해야 합니다.

- SVM 이름



적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.



감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

단계

1. 보안 정책('vserver security file-directory apply-vserver vs1-policy-name policy1')을 적용합니다

```
'vserver security file-directory apply-vserver vs1-policy-name policy1'
```

정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

## ONTAP SMB 보안 정책 작업 모니터링

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용해야 합니다.

단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vs1'을 모니터링합니다

```
'vserver security file-directory job show -vserver vs1'
```

| Job ID                                         | Name            | Vserver | Node  | State   |
|------------------------------------------------|-----------------|---------|-------|---------|
| 53322                                          | Fsecurity Apply | vs1     | node1 | Success |
| Description: File Directory Security Apply Job |                 |         |       |         |

## ONTAP SMB 파일 보안 확인

파일 보안 설정을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 머신)의 파일 또는 폴더에 원하는 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

보안 설정을 확인할 파일과 폴더의 경로와 데이터가 포함된 SVM의 이름을 제공해야 합니다. 옵션 '-Expand-mask' 매개 변수를 사용하여 보안 설정에 대한 자세한 정보를 표시할 수 있습니다.

단계

1. 파일 및 폴더 보안 설정 표시: 'vserver security file-directory show -vserver vs1-path/data/engineering-expand-mask true']

'vserver security file-directory show -vserver vs1-path/data/engineering-expand-mask true'

```
Vserver: vs1
 File Path: /data/engineering
File Inode Number: 5544
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
 ...0 = Offline
 0. = Sparse
 0... = Normal
 0. = Archive
 1 = Directory
 0.. = System
 0. = Hidden
 0 = Read Only
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004

 1... = Self Relative
 .0.. = RM Control Valid
 ..0. = SACL Protected
 ...0 = DACL Protected
 0... = SACL Inherited
 0.. = DACL Inherited
 0. = SACL Inherit Required
 0 = DACL Inherit Required
 0. = SACL Defaulted
 0 = SACL Present
 0... = DACL Defaulted
 1.. = DACL Present
 0. = Group Defaulted
```

```

.....0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
0... .. =
Generic Read
.0.. .. =
Generic Write
..0. .. =
Generic Execute
...0 .. =
Generic All
....0 .. =
System Security
.....1 .. =
Synchronize
.....1... .. =
Write Owner
.....1.. .. =
Write DAC
.....1. .. =
Read Control
.....1 .. =
Delete
.....1 .. =
Write Attributes
.....1... .. =
Read Attributes
.....1.. .. =
Delete Child
.....1. .. =
Execute
.....1 .. =
Write EA
.....1... .. =
Read EA
.....1.. .. =
Append
.....1. .. =
Write
.....1 .. =
Read
.....1 =

ALLOW-Everyone-0x10000000-OI|CI|IO

```



|                  |                                                 |
|------------------|-------------------------------------------------|
| Generic Read     | 0 . . . . . =                                   |
| Generic Write    | . 0 . . . . . =                                 |
| Generic Execute  | . . 0 . . . . . =                               |
| Generic All      | . . . 1 . . . . . =                             |
| System Security  | . . . . . 0 . . . . . =                         |
| Synchronize      | . . . . . 0 . . . . . =                         |
| Write Owner      | . . . . . 0 . . . . . =                         |
| Write DAC        | . . . . . . 0 . . . . . =                       |
| Read Control     | . . . . . . . 0 . . . . . =                     |
| Delete           | . . . . . . . . 0 . . . . . =                   |
| Write Attributes | . . . . . . . . . 0 . . . . . =                 |
| Read Attributes  | . . . . . . . . . . 0 . . . . . =               |
| Delete Child     | . . . . . . . . . . . 0 . . . . . =             |
| Execute          | . . . . . . . . . . . . 0 . . . . . =           |
| Write EA         | . . . . . . . . . . . . . 0 . . . . . =         |
| Read EA          | . . . . . . . . . . . . . . 0 . . . . . =       |
| Append           | . . . . . . . . . . . . . . . 0 . . . . . =     |
| Write            | . . . . . . . . . . . . . . . . 0 . . . . . =   |
| Read             | . . . . . . . . . . . . . . . . . 0 . . . . . = |

CLI를 사용하여 NTFS 파일 및 폴더에 감사 정책을 구성하고 적용합니다

NTFS 파일 및 폴더에 SMB 감사 정책을 구성하고 적용하기 위한 ONTAP 명령

ONTAP CLI를 사용할 때 NTFS 파일 및 폴더에 감사 정책을 적용하려면 몇 가지 단계를 수행해야 합니다. 먼저 NTFS 보안 설명자를 만들고 보안 설명자에 SACL을 추가합니다. 그런

다음 보안 정책을 만들고 정책 작업을 추가합니다. 그런 다음 SVM(스토리지 가상 시스템)에 보안 정책을 적용합니다.

이 작업에 대해

보안 정책을 적용한 후 보안 정책 작업을 모니터링하고 적용된 감사 정책의 설정을 확인할 수 있습니다.



감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

관련 정보

- [Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요](#)
- [SMB 파일 및 폴더 보안을 설정하기 위해 명령을 사용할 때의 제한 사항에 대해 알아보세요.](#)
- [보안 설명자를 사용하여 파일 및 폴더 보안을 적용합니다.](#)
- ["SMB 및 NFS 감사 및 보안 추적"](#)
- [서버에 NTFS 보안 설명자 만들기](#)

## ONTAP SMB 서버에서 NTFS 보안 설명자 생성

NTFS 보안 설명자 감사 정책을 생성하는 것은 SVM에 상주하는 파일 및 폴더에 NTFS ACL(액세스 제어 목록)을 구성 및 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결합니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

| 오브젝트                      | 액세스 유형입니다 | 액세스 권한 | 사용 권한을 적용할 위치입니다 |
|---------------------------|-----------|--------|------------------|
| BUILTIN\Administrators입니다 | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |
| BUILTIN\사용자               | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |
| 작성자 소유자                   | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |
| NT AUTHORITY\SYSTEM       | 허용        | 모든 권한  | 폴더, 하위 폴더, 파일    |

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다

- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

단계

1. 고급 매개 변수를 사용하려면 권한 수준을 고급:'Set-Privilege Advanced'로 설정합니다
2. 보안 설명자:'vserver security file-directory NTFS create-vserver vserver\_name-NTFS-SD sd\_nameoptional\_parameters'를 생성합니다  
  
'vserver security file-directory NTFS create-NTFS-SD SD1-vserver vs1-owner domain\joe'
3. 보안 설명자 구성이 올바른지 확인합니다. 'vserver security file-directory NTFS show -vserver vserver\_name -NTFS-SD sd\_name'

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. 고급 권한 수준인 경우 'Set-Privilege admin'으로 돌아갑니다

#### ONTAP SMB 서버의 NTFS 보안 설명자에 NTFS SACL 액세스 제어 항목 추가

SACL(시스템 액세스 제어 목록) ACE(액세스 제어 항목)를 NTFS 보안 설명자에 추가하는 것은 SVM의 파일 또는 폴더에 대한 NTFS 감사 정책을 생성하는 두 번째 단계입니다. 각 항목은 감사하려는 사용자 또는 그룹을 식별합니다. SACL 항목은 성공한 액세스 시도 또는 실패한 액세스 시도를 감사할지 여부를 정의합니다.

이 작업에 대해

보안 설명자의 SACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 SACL이 포함된 경우 이 명령은 새 ACE를 SACL에 추가합니다. 보안 설명자에 SACL이 포함되어 있지 않으면 명령에서 SACL을 만들고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정의 성공 또는 실패 이벤트에 대해 감사할 권한을 지정하여 SACL 항목을 구성할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)



SACL 항목에 대한 권한을 지정하지 않으면 기본 설정은 "모든 권한"입니다.

"apply to" 매개 변수를 사용하여 상속을 적용하는 방법을 지정하여 SACL 항목을 선택적으로 사용자 지정할 수 있습니다. 이 매개 변수를 지정하지 않으면 기본적으로 이 SACL 항목을 이 폴더, 하위 폴더 및 파일에 적용합니다.

단계

1. 보안 설명자에 SACL 항목을 추가합니다. 'vserver security file-directory NTFS SACL add -vserver vs1 -ntfs -sd sd\_name -access -type {failure | success} -account name\_or\_SID optional\_parameters'

```
'vserver security file-directory NTFS SACL add-NTFS-SD SD1-access-type failure-account domain\joe-rights full-control-apply-to this-folder-vs1'
```

2. SACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS SACL show -vserver vs1 -ntfs -sd sd\_name -access -type {failure | success} -account name\_or\_SID'

```
'vserver security file-directory NTFS SACL show -vserver vs1-NTFS-SD SD1-access-type deny-account domain\joe'
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

## ONTAP SMB 보안 정책 생성

SVM(스토리지 가상 머신)에 대한 감사 정책을 생성하는 것은 ACL을 구성하여 파일 또는 폴더에 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각 작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(스토리지 가상 머신)(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

단계

1. 'vserver security file-directory policy create-vserver vs1 -policy-name policy\_name' 보안 정책을 생성합니다

```
'vserver security file-directory policy create-policy-name policy1-vserver vs1'
```

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
Vserver Policy Name

vs1 policy1
```

## ONTAP SMB 보안 정책에 작업 추가

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 디렉터리 작업을 통해 적용된 ACL은 SMB 클라이언트 또는 ONTAP CLI를 통해 관리할 수 있습니다.

- 스토리지 레벨 액세스 가드 작업

지정된 볼륨에 Storage-Level Access Guard 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 스토리지 레벨 액세스 가드 작업을 통해 적용된 ACL은 ONTAP CLI를 통해서만 관리할 수 있습니다.

작업에는 파일(또는 폴더) 또는 파일 집합(또는 폴더)의 보안 구성에 대한 정의가 포함됩니다. 정책의 모든 작업은 경로로 고유하게 식별됩니다. 단일 정책 내에서 경로당 하나의 작업만 있을 수 있습니다. 정책에 중복된 작업 항목이 있을 수 없습니다.

정책에 작업 추가 지침:

- 정책당 최대 10,000개의 작업 항목이 있을 수 있습니다.
- 정책에는 하나 이상의 작업이 포함될 수 있습니다.

정책에 둘 이상의 작업이 포함될 수 있지만 파일 디렉터리 및 저장소 수준 액세스 가드 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉터리 작업이 포함되어야 합니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

추가 액세스 권한은 제공하지 않습니다.

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 유형입니다

- 전파 모드
- 인덱스 위치
- 액세스 제어 유형입니다

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉토리 정책 작업 추가 - vserver vserver\_name -policy -name policy\_name -path path -NTFS-SD\_nameoptional\_parameters'

파일 디렉토리는 '-access-control' 파라미터의 기본값입니다. 파일 및 디렉터리 액세스 작업을 구성할 때 액세스 제어 유형을 지정하는 것은 선택 사항입니다.

'vserver security file-directory policy task add-vserver vs1-policy-name policy1-path/home/dir1-security-type NTFS-NTFS-MODE propagate-NTFS-SD SD2-index-num 1-access-control file-directory'를 선택합니다

2. 정책 작업 구성을 확인합니다. 'vserver security file-directory policy task show -vserver vserver\_name -policy -name policy\_name -path path path'

'vserver security file-directory policy task show'를 선택합니다

```
Vserver: vs1
Policy: policy1
```

| Index           | File/Folder | Access         | Security | NTFS      | NTFS |
|-----------------|-------------|----------------|----------|-----------|------|
| Security        | Path        | Control        | Type     | Mode      |      |
| Descriptor Name |             |                |          |           |      |
| -----           | -----       | -----          | -----    | -----     |      |
| 1               | /home/dir1  | file-directory | ntfs     | propagate | sd2  |

에 대한 자세한 내용은 vserver security file-directory policy task ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

## ONTAP SMB 보안 정책 적용

파일 또는 폴더에 NTFS ACL을 생성하고 적용하는 마지막 단계는 SVM에 감사 정책을 적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.



감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

#### 단계

1. 'vserver security file-directory apply-vserver vs1-policy-name policy1' 보안 정책을 적용합니다

```
'vserver security file-directory apply-vserver vs1-policy-name policy1'
```

정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

### ONTAP SMB 보안 정책 작업 모니터링

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용해야 합니다.

#### 단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vs1'을 모니터링합니다

```
'vserver security file-directory job show -vserver vs1'
```

| Job ID                                         | Name            | Vserver | Node  | State   |
|------------------------------------------------|-----------------|---------|-------|---------|
| 53322                                          | Fsecurity Apply | vs1     | node1 | Success |
| Description: File Directory Security Apply Job |                 |         |       |         |

### ONTAP SMB 감사 정책 확인

감사 정책을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 시스템)의 파일 또는 폴더에 원하는 감사 보안 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

'vserver security file-directory show' 명령을 사용하여 감사 정책 정보를 표시합니다. 표시할 파일 또는 폴더 감사 정책 정보를 가진 데이터의 경로와 데이터가 들어 있는 SVM의 이름을 제공해야 합니다.

#### 단계

1. 감사 정책 설정 표시: 'vserver security file-directory show -vserver\_vserver\_name\_-path\_path\_'

예

다음 명령을 실행하면 SVM VS1 경로의 ""/Corp" 경로에 적용된 감사 정책 정보가 표시됩니다. 경로에 성공 및 성공/실패 SACL 항목이 모두 적용됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

Vserver: vs1
File Path: /corp
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8014
 Owner:DOMAIN\Administrator
 Group:BUILTIN\Administrators
 SACL - ACEs
 ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
 SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
 DACL - ACEs
 ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
 ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
 ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

**ONTAP SMB** 보안 정책 작업 관리에 대해 알아보세요

특정 상황에서 보안 정책 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을 수정할 수 없습니다. 정책을 수정할 수 있는 조건이나 수정할 수 없는 조건을 이해해야 정책을 수정할 수 있습니다. 정책 수정에는 정책에 할당된 작업을 추가, 제거 또는 수정하고 정책을 삭제 또는 수정하는 작업이 포함됩니다.

해당 정책에 대한 작업이 있고 해당 작업이 다음 상태인 경우 해당 정책에 할당된 보안 정책 또는 작업을 수정할 수 없습니다.

- 작업이 실행 중이거나 진행 중입니다.
- 작업이 일시 중지되었습니다.
- 작업이 재개되고 실행 중 상태입니다.



- 작업이 다른 노드로 장애 조치를 기다리는 경우

다음 상황에서 보안 정책에 대한 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을 성공적으로 수정할 수 있습니다.

- 정책 작업이 중지되었습니다.
- 정책 작업이 성공적으로 완료되었습니다.

#### SMB 서버에서 NTFS 보안 설명자를 관리하기 위한 ONTAP 명령

보안 설명자를 관리하기 위한 특정 ONTAP 명령이 있습니다. 보안 설명자에 대한 정보를 생성, 수정, 삭제 및 표시할 수 있습니다.

| 원하는 작업                       | 이 명령 사용...                                            |
|------------------------------|-------------------------------------------------------|
| NTFS 보안 설명자를 만듭니다            | 'vserver security file-directory NTFS create'         |
| 기존 NTFS 보안 설명자를 수정합니다        | 'vserver security file-directory NTFS modify'를 참조하십시오 |
| 기존 NTFS 보안 설명자에 대한 정보를 표시합니다 | 'vserver security file-directory NTFS show'           |
| NTFS 보안 설명자를 삭제합니다           | 'vserver security file-directory NTFS delete'         |

에 대한 자세한 내용은 `vserver security file-directory ntfs` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

#### SMB 서버에서 NTFS DACL 액세스 제어 항목을 관리하기 위한 ONTAP 명령

DACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS DACL에 추가할 수 있습니다. DACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS DACL을 관리할 수도 있습니다.

| 원하는 작업                          | 이 명령 사용...                                                |
|---------------------------------|-----------------------------------------------------------|
| ACE를 만들어 NTFS DACL에 추가합니다       | 'vserver security file-directory NTFS DACL add'           |
| NTFS DACL에서 기존 ACE를 수정합니다       | 'vserver security file-directory NTFS DACL modify'를 선택합니다 |
| NTFS DACL의 기존 ACE에 대한 정보를 표시합니다 | 'vserver security file-directory NTFS DACL show'          |
| NTFS DACL에서 기존 ACE를 제거합니다       | 'vserver security file-directory NTFS DACL remove'        |

에 대한 자세한 내용은 `vserver security file-directory ntfs dacl` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

SACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS SACL에 추가할 수 있습니다. SACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS SACL을 관리할 수도 있습니다.

| 원하는 작업                          | 이 명령 사용...                                                 |
|---------------------------------|------------------------------------------------------------|
| ACE를 만들어 NTFS SACL에 추가합니다       | 'vserver security file-directory NTFS SACL add'            |
| NTFS SACL에서 기존 ACE를 수정합니다       | 'vserver security file-directory NTFS SACL modify'를 참조하십시오 |
| NTFS SACL의 기존 ACE에 대한 정보를 표시합니다 | 'vserver security file-directory NTFS SACL show'           |
| NTFS SACL에서 기존 ACE를 제거합니다       | 'vserver security file-directory NTFS SACL remove'         |

에 대한 자세한 내용은 `vserver security file-directory ntfs sacl` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

#### SMB 보안 정책을 관리하기 위한 ONTAP 명령

보안 정책을 관리하기 위한 특정 ONTAP 명령이 있습니다. 정책에 대한 정보를 표시하고 정책을 삭제할 수 있습니다. 보안 정책을 수정할 수 없습니다.

| 원하는 작업              | 이 명령 사용...                                              |
|---------------------|---------------------------------------------------------|
| 보안 정책을 생성합니다        | 'vserver security file-directory policy create'를 참조하십시오 |
| 보안 정책에 대한 정보를 표시합니다 | 'vserver security file-directory policy show'를 선택합니다    |
| 보안 정책을 삭제합니다        | 'vserver security file-directory policy delete'         |

에 대한 자세한 내용은 `vserver security file-directory policy` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

#### SMB 보안 정책 작업을 관리하기 위한 ONTAP 명령

보안 정책 작업에 대한 정보를 추가, 수정, 제거 및 표시하는 ONTAP 명령이 있습니다.

| 원하는 작업          | 이 명령 사용...                                        |
|-----------------|---------------------------------------------------|
| 보안 정책 작업을 추가합니다 | 'vserver security file-directory policy task add' |

| 원하는 작업                 | 이 명령 사용...                                                  |
|------------------------|-------------------------------------------------------------|
| 보안 정책 작업을 수정합니다        | 'vserver security file-directory policy task modify'를 선택합니다 |
| 보안 정책 작업에 대한 정보를 표시합니다 | 'vserver security file-directory policy task show'를 선택합니다   |
| 보안 정책 작업을 제거합니다        | 'vserver security file-directory policy task remove'        |

에 대한 자세한 내용은 `vserver security file-directory policy task` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

#### **SMB** 보안 정책 작업을 관리하기 위한 **ONTAP** 명령

보안 정책 작업에 대한 정보를 일시 중지, 다시 시작, 중지 및 표시하는 ONTAP 명령이 있습니다.

| 원하는 작업                 | 이 명령 사용...                                                                                 |
|------------------------|--------------------------------------------------------------------------------------------|
| 보안 정책 작업을 일시 중지합니다     | 'vserver security file-directory job pause -vserver vserver_name -id integer'              |
| 보안 정책 작업을 다시 시작합니다     | 'vserver security file-directory job resume - vserver vserver_name -id integer'            |
| 보안 정책 작업에 대한 정보를 표시합니다 | 'vserver security file-directory job show -vserver_name' 이 명령을 사용하여 작업의 작업 ID를 확인할 수 있습니다. |
| 보안 정책 작업을 중지합니다        | 'vserver security file-directory job stop -vserver vserver_name -id integer'               |

에 대한 자세한 내용은 `vserver security file-directory job` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

#### **SMB** 공유에 대한 메타데이터 캐시를 구성합니다

##### **ONTAP SMB** 메타데이터 캐싱에 대해 알아보세요

메타데이터 캐싱을 사용하면 SMB 1.0 클라이언트에서 파일 속성 캐싱을 통해 파일 및 폴더 특성에 더 빠르게 액세스할 수 있습니다. 공유별로 특성 캐싱을 설정하거나 해제할 수 있습니다. 메타데이터 캐시가 설정된 경우 캐시된 항목에 대한 라이브 시간을 구성할 수도 있습니다. 클라이언트가 SMB 2.x 또는 SMB 3.0을 통해 공유에 접속하는 경우에는 메타데이터 캐싱을 구성할 필요가 없습니다.

SMB 메타데이터 캐시가 설정되면 제한된 시간 동안 경로 및 파일 속성 데이터를 저장합니다. 따라서 공통 워크로드를 사용하는 SMB 1.0 클라이언트의 SMB 성능이 향상될 수 있습니다.

특정 작업의 경우 SMB는 경로 및 파일 메타데이터에 대한 여러 개의 동일한 쿼리를 포함할 수 있는 상당한 양의

트래픽을 생성합니다. SMB 메타데이터 캐싱을 사용하여 캐시에서 정보를 가져오는 방식으로 SMB 1.0 클라이언트의 중복 쿼리 수를 줄이고 성능을 향상할 수 있습니다.



가능성은 낮지만 메타데이터 캐시가 오래된 정보를 SMB 1.0 클라이언트에 제공할 수도 있습니다. 귀사의 환경에서 이러한 위험을 감당할 수 없는 경우 이 기능을 활성화하지 마십시오.

#### ONTAP SMB 메타데이터 캐시 활성화

SMB 메타데이터 캐시를 설정하여 SMB 1.0 클라이언트의 SMB 성능을 향상할 수 있습니다. 기본적으로 SMB 메타데이터 캐싱은 해제되어 있습니다.

##### 단계

- 원하는 작업을 수행합니다.

| 원하는 작업                        | 명령 입력...                                                                                                             |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------|
| 공유를 생성할 때 SMB 메타데이터 캐싱을 설정합니다 | 'vserver cifs share create -vserver_vserver_name_-share-name_share_name_-path_path_-share-properties attributecache' |
| 기존 공유에서 SMB 메타데이터 캐싱을 설정합니다   | "vserver cifs 공유 속성 add -vserver_vserver_name_-share-name_share_name_-share-properties attributecache"               |

##### 관련 정보

- [메타데이터 캐시 항목의 수명 구성](#)
- [기존 주식에 주식 속성 추가 또는 제거](#)

#### ONTAP SMB 메타데이터 캐시 항목의 수명 구성

SMB 메타데이터 캐시 항목의 수명을 구성하여 사용자 환경에서 SMB 메타데이터 캐시 성능을 최적화할 수 있습니다. 기본값은 10초입니다.

##### 시작하기 전에

SMB 메타데이터 캐시 기능을 활성화해야 합니다. SMB 메타데이터 캐싱이 설정되어 있지 않으면 SMB 캐시 TTL 설정이 사용되지 않습니다.

##### 단계

- 원하는 작업을 수행합니다.

|                                                |                                                                                                                           |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 다음과 같은 경우 <b>SMB</b> 메타데이터 캐시 항목의 수명을 구성하려는 경우 | 명령 입력...                                                                                                                  |
| 공유를 생성합니다                                      | 'vserver cifs share-create-vserver_vserver_name_-share-name_share_name_-path_path_-attribute-cache-tl[integer][integerm]' |

|                                                |                                                                                                                          |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 다음과 같은 경우 <b>SMB</b> 메타데이터 캐시 항목의 수명을 구성하려는 경우 | 명령 입력...                                                                                                                 |
| 기존 공유를 수정합니다                                   | 'vserver cifs share-modify-vserver_vserver_name_-share-name_share_name_-attribute-cache-tl[integerh][integerm][integer]' |

공유를 생성하거나 수정할 때 추가 공유 구성 옵션과 속성을 지정할 수 있습니다. 에 대한 자세한 내용은 `vserver cifs share` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

## 파일 잠금 관리

프로토콜 간 **ONTAP SMB** 파일 잠금에 대해 알아보세요

파일 잠금은 사용자가 이전에 다른 사용자가 연 파일에 액세스하지 못하도록 클라이언트 응용 프로그램에서 사용하는 방법입니다. ONTAP가 파일을 잠그는 방법은 클라이언트의 프로토콜에 따라 다릅니다.

클라이언트가 NFS 클라이언트인 경우 잠금이 권고사항이고, 클라이언트가 SMB 클라이언트인 경우 잠금이 필수입니다.

NFS와 SMB 파일 잠금의 차이로 인해 NFS 클라이언트가 SMB 애플리케이션에서 이전에 연 파일에 액세스하지 못할 수 있습니다.

NFS 클라이언트가 SMB 애플리케이션에 의해 잠긴 파일에 액세스하려고 할 때 다음이 발생합니다.

- 혼합 볼륨 또는 NTFS 볼륨에서 `rm`, `rmdir`, `mv` 등의 파일 조작 작업으로 인해 NFS 응용 프로그램이 실패할 수 있습니다.
- NFS 읽기 및 쓰기 작업은 SMB 거부-읽기 및 거부-쓰기 열기 모드에 의해 각각 거부됩니다.
- 배타적 SMB bytelock로 파일의 쓰기 범위가 잠기면 NFS 쓰기 작업이 실패합니다.
- 연결을 끊습니다
  - NTFS 파일 시스템의 경우 SMB 및 CIFS 삭제 작업이 지원됩니다.

마지막으로 닫은 후에 파일이 제거됩니다.

- NFS 연결 해제 작업은 지원되지 않습니다.

NTFS 및 SMB 의미가 필요하고 NFS에 대해 마지막 Delete-On-Close 작업이 지원되지 않기 때문에 지원되지 않습니다.

- UNIX 파일 시스템의 경우 연결 해제 작업이 지원됩니다.

NFS 및 UNIX 시맨틱이 필요하기 때문에 지원됩니다.

- 이름 바꾸기
  - NTFS 파일 시스템의 경우 SMB 또는 CIFS에서 대상 파일을 열면 대상 파일의 이름을 바꿀 수 있습니다.
  - NFS 이름 변경은 지원되지 않습니다.

NTFS 및 SMB 의미가 필요하므로 지원되지 않습니다.

UNIX 보안 스타일 볼륨에서 NFS 링크 해제 및 이름 바꾸기 작업은 SMB 잠금 상태를 무시하고 파일에 대한 액세스를 허용합니다. UNIX 보안 스타일 볼륨에서 다른 모든 NFS 작업은 SMB 잠금 상태를 존중합니다.

**ONTAP SMB** 읽기 전용 비트에 대해 알아보세요

읽기 전용 비트는 파일을 쓰기 가능(사용 안 함)인지 읽기 전용(사용 가능)인지를 나타내기 위해 파일별로 설정됩니다.

Windows를 사용하는 SMB 클라이언트는 파일당 읽기 전용 비트를 설정할 수 있습니다. NFS 클라이언트는 파일당 읽기 전용 비트를 사용하는 프로토콜 작업이 없으므로 파일당 읽기 전용 비트를 설정하지 않습니다.

ONTAP는 Windows를 사용하는 SMB 클라이언트가 해당 파일을 생성할 때 파일에 읽기 전용 비트를 설정할 수 있습니다. 또한 ONTAP는 NFS 클라이언트와 SMB 클라이언트 간에 파일이 공유될 때 읽기 전용 비트를 설정할 수 있습니다. 일부 소프트웨어는 NFS 클라이언트 및 SMB 클라이언트에서 사용할 때 읽기 전용 비트를 사용하도록 설정해야 합니다.

ONTAP가 NFS 클라이언트와 SMB 클라이언트 간에 공유되는 파일에 대해 적절한 읽기 및 쓰기 권한을 유지하려면 다음 규칙에 따라 읽기 전용 비트를 처리합니다.

- NFS는 읽기 전용 비트가 설정된 파일을 쓰기 권한 비트가 설정되지 않은 것처럼 처리합니다.
- NFS 클라이언트가 모든 쓰기 권한 비트를 사용하지 않도록 설정하고 이전에 해당 비트 중 하나 이상이 활성화된 경우 ONTAP는 해당 파일에 대해 읽기 전용 비트를 설정합니다.
- NFS 클라이언트가 쓰기 권한 비트를 설정하면 ONTAP는 해당 파일에 대해 읽기 전용 비트를 해제합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 NFS 클라이언트가 해당 파일에 대한 권한을 검색하려고 하면 파일에 대한 권한 비트가 NFS 클라이언트로 전송되지 않고 ONTAP는 쓰기 권한 비트가 마스킹된 상태로 NFS 클라이언트에 사용 권한 비트를 전송합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 SMB 클라이언트가 읽기 전용 비트를 사용하지 않도록 설정한 경우 ONTAP는 해당 파일에 대한 소유자의 쓰기 권한 비트를 설정합니다.
- 읽기 전용 비트가 설정된 파일은 루트에서만 쓸 수 있습니다.

읽기 전용 비트는 다음과 같은 방식으로 ACL 및 Unix 모드 비트와 상호 작용합니다.

파일에 읽기 전용 비트가 설정된 경우:

- 해당 파일의 ACL에는 변경 사항이 없습니다. NFS 클라이언트는 읽기 전용 비트가 설정되기 전과 동일한 ACL을 보게 됩니다.
- 파일에 대한 쓰기 접근을 허용하는 모든 Unix 모드 비트는 무시됩니다.
- NFS와 SMB 클라이언트는 모두 파일을 읽을 수 있지만, 수정할 수는 없습니다.
- ACL 및 UNIX 모드 비트는 읽기 전용 비트 때문에 무시됩니다. 즉, ACL이 쓰기 액세스를 허용하더라도 읽기 전용 비트는 수정을 방지합니다.

파일에 읽기 전용 비트가 설정되지 않은 경우:

- ONTAP ACL 및 UNIX 모드 비트를 기반으로 액세스를 결정합니다.
  - ACL 또는 UNIX 모드 비트가 쓰기 액세스를 거부하는 경우 NFS 및 SMB 클라이언트는 파일을 수정할 수 없습니다.

- ACL이나 UNIX 모드 비트가 쓰기 액세스를 거부하지 않으면 NFS 및 SMB 클라이언트가 파일을 수정할 수 있습니다.



파일 권한 변경은 SMB 클라이언트에 즉시 적용되지만 NFS 클라이언트가 특성 캐싱을 사용하는 경우 NFS 클라이언트에 즉시 적용되지 않을 수 있습니다.

공유 경로 구성 요소에 대한 잠금 처리에서 **ONTAP**가 **Windows**와 어떻게 다른지 설명합니다

**Windows**와 달리 **ONTAP**는 파일이 열려 있는 동안 열려 있는 파일에 대한 경로의 각 구성 요소를 잠그지 않습니다. 이 동작은 SMB 공유 경로에도 영향을 줍니다.

**ONTAP**는 경로의 각 구성 요소를 잠그지 않으므로 열려 있는 파일 또는 공유 위에 있는 경로 구성 요소의 이름을 바꿀 수 있습니다. 이렇게 하면 특정 응용 프로그램에 문제가 발생하거나 SMB 구성의 공유 경로가 잘못될 수 있습니다. 이로 인해 공유에 액세스할 수 없게 될 수 있습니다.

경로 구성 요소의 이름을 변경하여 발생하는 문제를 방지하려면 사용자나 응용 프로그램이 중요한 디렉터리의 이름을 바꾸지 못하도록 보안 설정을 적용할 수 있습니다.

#### **ONTAP SMB** 잠금에 대한 정보 표시

현재 파일 잠금에 대한 정보를 표시할 수 있습니다. 여기에는 보유한 잠금의 유형 및 잠금 상태, 바이트 범위 잠금에 대한 세부 정보, 공유 잠금 모드, 위임 잠금 및 편의적 잠금, 잠금이 내구성 또는 지속 핸들로 열렸는지 여부 등이 포함됩니다.

이 작업에 대해

NFSv4 또는 NFSv4.1을 통해 설정된 잠금에 대해 클라이언트 IP 주소를 표시할 수 없습니다.

기본적으로 명령은 모든 잠금에 대한 정보를 표시합니다. 명령 매개 변수를 사용하여 특정 SVM(스토리지 가상 머신)의 잠금에 대한 정보를 표시하거나 명령의 출력을 다른 기준으로 필터링할 수 있습니다.

'vserver lock show' 명령은 네 가지 유형의 잠금에 대한 정보를 표시합니다.

- 바이트 범위 잠금 - 파일의 일부만 잠급니다.
- 공유 잠금 - 열린 파일을 잠급니다.
- SMB를 통한 클라이언트 측 캐싱을 제어하는 편의적 잠금 기능
- 위임 - NFSv4.x에서 클라이언트 측 캐싱을 제어합니다

선택적 매개 변수를 지정하면 각 잠금 유형에 대한 중요한 정보를 확인할 수 있습니다. 에 대한 자세한 내용은 `vserver locks show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 잠금에 대한 정보를 표시합니다.

예

다음 예에서는 '/vol1/file1' 경로가 있는 파일의 NFSv4 잠금에 대한 요약 정보를 표시합니다. sharelock 액세스 모드는 write-deny\_none 이며, 잠금이 쓰기 위임과 함께 부여되었습니다.

```
cluster1::> vsriver locks show
```

```
Vserver: vs0
```

| Volume | Object Path                     | LIF   | Protocol | Lock Type   | Client |
|--------|---------------------------------|-------|----------|-------------|--------|
| -----  | -----                           | ----- | -----    | -----       |        |
| ----   |                                 |       |          |             |        |
| vol1   | /vol1/file1                     | lif1  | nfsv4    | share-level | -      |
|        | Sharelock Mode: write-deny_none |       |          |             |        |
|        |                                 |       |          | delegation  | -      |
|        | Delegation Type: write          |       |          |             |        |

다음 예에서는 경로 '/data2/data2\_2/intro.pptx'를 사용하여 파일의 SMB 잠금에 대한 자세한 oplock 및 sharelock 정보를 표시합니다. IP 주소가 10.3.1.3인 클라이언트에 write-deny\_none의 공유 잠금 액세스 모드를 가진 파일에 내구성 있는 핸들이 부여됩니다. 배치 oplock 레벨이 있는 리스 oplock이 부여됩니다.

```
cluster1::> vsriver locks show -instance -path /data2/data2_2/intro.pptx
```

```
Vserver: vs1
```

```
Volume: data2_2
```

```
Logical Interface: lif2
```

```
Object Path: /data2/data2_2/intro.pptx
```

```
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
```

```
Lock Protocol: cifs
```

```
Lock Type: share-level
```

```
Node Holding Lock State: node3
```

```
Lock State: granted
```

```
Bytelock Starting Offset: -
```

```
Number of Bytes Locked: -
```

```
Bytelock is Mandatory: -
```

```
Bytelock is Exclusive: -
```

```
Bytelock is Superlock: -
```

```
Bytelock is Soft: -
```

```
Oplock Level: -
```

```
Shared Lock Access Mode: write-deny_none
```

```
Shared Lock is Soft: false
```

```
Delegation Type: -
```

```
Client Address: 10.3.1.3
```

```
SMB Open Type: durable
```

```
SMB Connect State: connected
```

```
SMB Expiration Time (Secs): -
```

```
SMB Open Group ID:
```

```
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

```
Vserver: vs1
```

```
Volume: data2_2
```



```

Logical Interface: lif2
 Object Path: /data2/data2_2/test.pptx
 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
 Lock Protocol: cifs
 Lock Type: op-lock
Node Holding Lock State: node3
 Lock State: granted
Bytelock Starting Offset: -
 Number of Bytes Locked: -
 Bytelock is Mandatory: -
 Bytelock is Exclusive: -
 Bytelock is Superlock: -
 Bytelock is Soft: -
 Oplock Level: batch
Shared Lock Access Mode: -
 Shared Lock is Soft: -
 Delegation Type: -
 Client Address: 10.3.1.3
 SMB Open Type: -
 SMB Connect State: connected
SMB Expiration Time (Secs): -
 SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

#### ONTAP SMB 잠금 해제

파일 잠금으로 인해 클라이언트가 파일에 액세스하지 못하는 경우 현재 보류된 잠금에 대한 정보를 표시한 다음 특정 잠금을 중단할 수 있습니다. 잠금을 해제해야 하는 시나리오의 예로는 응용 프로그램 디버깅이 있습니다.

이 작업에 대해

``vserver locks break`` 명령은 advanced 권한 수준 이상에서만 사용할 수 있습니다. 에 대한 자세한 내용은 ``vserver locks break`` [link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html](https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html) ["ONTAP 명령 참조입니다"^]을 참조하십시오.

단계

1. 잠금을 해제해야 하는 정보를 찾으려면 'vserver lock show' 명령을 사용합니다.

에 대한 자세한 내용은 `vserver locks show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
3. 다음 작업 중 하나를 수행합니다.

|                               |                                                                                            |
|-------------------------------|--------------------------------------------------------------------------------------------|
| 다음을 지정하여 잠금을 해제하려면...         | 명령 입력...                                                                                   |
| SVM 이름, 볼륨 이름, LIF 이름 및 파일 경로 | 'vserver lock break - vserver vserver_name - volume volume_name - path path path -lif lif' |
| 잠금 ID입니다                      | 'vserver lock break-lockid UUID'                                                           |

#### 4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

### SMB 작업을 모니터링합니다

#### ONTAP SMB 세션 정보 표시

SMB 연결 및 세션 ID와 세션을 사용하는 워크스테이션의 IP 주소를 포함하여 설정된 SMB 세션에 대한 정보를 표시할 수 있습니다. 세션의 SMB 프로토콜 버전 및 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시하여 세션이 무중단 운영을 지원하는지 여부를 확인할 수 있습니다.

이 작업에 대해

SVM의 모든 세션에 대한 정보를 요약 형식으로 표시할 수 있습니다. 그러나 대부분의 경우 반환되는 출력량이 큼니다. 옵션 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 대한 출력을 표시할 수 있습니다.

필드를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

- '-instance' 매개 변수를 사용하면 설정된 SMB 세션에 대한 자세한 정보를 표시할 수 있습니다.
- '-fields' 매개 변수 또는 '-instance' 매개 변수를 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

#### 1. 다음 작업 중 하나를 수행합니다.

|                             |                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------|
| <b>SMB 세션 정보를 표시하려면...</b>  | <b>다음 명령을 입력합니다...</b>                                                            |
| SVM의 모든 세션에 대해 요약 양식을 작성합니다 | 'vserver cifs session show -vserver vserver_name'을 선택합니다                          |
| 지정된 연결 ID에 있습니다             | 'vserver cifs session show -vserver vserver_name -connection -id integer'를 선택합니다  |
| 지정된 워크스테이션 IP 주소에서          | 'vserver cifs session show -vserver vserver_name -address workstation_ip_address' |
| 지정된 LIF IP 주소입니다            | 'vserver cifs session show -vserver vserver_name -lif-address LIF_ip_address'     |

|                                                                                           |                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SMB 세션 정보를 표시하려면...</b>                                                                | 다음 명령을 입력합니다...                                                                                                                                                                                                                                                                   |
| 지정된 노드에서                                                                                  | 'vserver cifs session show -vserver vserver_name<br>-node{node_name                                                                                                                                                                                                               |
| local}'                                                                                   | 지정된 Windows 사용자로부터                                                                                                                                                                                                                                                                |
| 'vserver cifs session show -vserver vserver_name<br>-windows-user domain_name\\user_name' | 지정된 인증 메커니즘을 사용합니다                                                                                                                                                                                                                                                                |
| 'vserver cifs session show -vserver vserver_name<br>-auth-mechanism{NTLMv1                | NTLMv2                                                                                                                                                                                                                                                                            |
| Kerberos                                                                                  | Anonymous}'                                                                                                                                                                                                                                                                       |
| 지정된 프로토콜 버전을 사용하여                                                                         | 'vserver cifs session show -vserver vserver_name<br>-protocol -version{SMB1                                                                                                                                                                                                       |
| SMB2                                                                                      | SMB2_1                                                                                                                                                                                                                                                                            |
| SMB3                                                                                      | SMB3_1}'을 선택합니다<br><br>[NOTE]<br>====<br>지속적으로 사용 가능한 보호 기능과 SMB 멀티 채널은<br>SMB 3.0 이상 세션에서만 사용할 수 있습니다. 모든<br>적격 세션에서 해당 상태를 보려면 이 매개 변수를 'MB3'<br>이상으로 설정한 값으로 지정해야 합니다.<br><br>=====                                                                                            |
| 지속적으로 사용 가능한 보호 수준을 지정합니다                                                                 | 'vserver cifs session show -vserver vserver_name<br>-Continuously-available{No                                                                                                                                                                                                    |
| Yes                                                                                       | Partial}'<br><br>[NOTE]<br>====<br>계속 사용 가능한 상태가 "부분"인 경우 세션에 하나<br>이상의 열려 있는 연속 사용 가능한 파일이 포함되어<br>있지만 세션에 계속 사용 가능한 보호 기능이 있는 일부<br>파일이 열려 있지 않은 것입니다. 'vserver cifs sessions<br>file show' 명령을 사용하여 설정된 세션에서 계속 사용<br>가능한 보호 기능을 사용하여 열려 있지 않은 파일을<br>확인할 수 있습니다.<br><br>===== |
| 지정된 SMB 서명 세션 상태                                                                          | 'vserver cifs session show -vserver vserver_name<br>-is-session -signed{true                                                                                                                                                                                                      |

다음 명령을 실행하면 IP 주소가 10.1.1.1인 워크스테이션에서 설정된 SVM VS1 세션의 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node: node1
Vserver: vs1
Connection Session
ID ID Workstation Windows User Open Idle

3151272279,
3151272280,
3151272281 1 10.1.1.1 DOMAIN\joe 2 23s
```

다음 명령을 실행하면 SVM VS1 에서 지속적으로 사용 가능한 보호 기능을 지원하는 세션에 대한 자세한 세션 정보가 표시됩니다. 도메인 계정을 사용하여 연결을 만들었습니다.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

다음 명령을 실행하면 SVM VS1 기반 SMB 3.0 및 SMB 멀티 채널을 사용하는 세션에 대한 세션 정보가 표시됩니다. 이 예에서 사용자는 LIF IP 주소를 사용하여 SMB 3.0 지원 클라이언트에서 이 공유에 연결했습니다. 따라서 인증 메커니즘은 NTLMv2로 기본값입니다. 지속적으로 사용 가능한 보호 기능을 사용하여 연결하려면 Kerberos 인증을 사용하여 연결해야 합니다.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```
Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

## 관련 정보

### 열려 있는 SMB 파일에 대한 정보 표시

#### 열려 있는 **ONTAP SMB** 파일에 대한 정보 표시

SMB 연결 및 세션 ID, 호스팅 볼륨, 공유 이름 및 공유 경로를 포함하여 열려 있는 SMB 파일에 대한 정보를 표시할 수 있습니다. 파일의 지속적인 사용 가능한 보호 수준에 대한 정보를 표시할 수 있습니다. 이 정보는 열려 있는 파일이 무중단 작업을 지원하는 상태에 있는지 여부를 확인하는 데 유용합니다.

#### 이 작업에 대해

설정된 SMB 세션에서 열린 파일에 대한 정보를 표시할 수 있습니다. 표시된 정보는 SMB 세션 내의 특정 파일에 대한 SMB 세션 정보를 확인해야 할 때 유용합니다.

예를 들어, 열린 파일 중 일부가 지속적으로 사용 가능한 보호 기능을 통해 열려 있고 일부는 지속적으로 사용 가능한 보호 기능을 통해 열려 있지 않은 SMB 세션이 있는 경우(vserver cifs session show 명령의 출력 값이 부분(Partial)인 경우), 이 명령을 사용하여 계속 사용할 수 없는 파일을 확인할 수 있습니다.

선택적 매개 변수 없이 'vserver cifs session file show' 명령을 사용하면 SVM(스토리지 가상 시스템)에서 설정된 SMB 세션의 모든 열려 있는 파일에 대한 정보를 요약 형식으로 표시할 수 있습니다.

그러나 대부분의 경우 반환되는 출력량이 큼니다. 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할

수 있습니다. 이 기능은 열려 있는 파일의 작은 하위 집합에 대한 정보만 보려는 경우에 유용합니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 출력을 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

- '-instance' 매개 변수를 사용하여 열려 있는 SMB 파일에 대한 자세한 정보를 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

| 열려 있는 <b>SMB</b> 파일을 표시하려면...                                                              | 다음 명령을 입력합니다...                                                       |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| SVM에 대해 요약 형식으로 표시됩니다                                                                      | 'vserver cifs session file show -vserver vserver_name'을 선택합니다         |
| 지정된 노드에서                                                                                   | 'vserver cifs session file show -vserver vserver_name -node{node_name |
| local}'를 선택합니다                                                                             | 지정된 파일 ID에 있습니다                                                       |
| 'vserver cifs session file show -vserver vserver_name -file-id integer'를 선택합니다             | 지정된 SMB 연결 ID에서                                                       |
| 'vserver cifs session file show -vserver vserver_name -connection -id integer'를 선택합니다      | 지정된 SMB 세션 ID에서                                                       |
| 'vserver cifs session file show -vserver vserver_name -session-id integer'를 선택합니다          | 지정된 호스팅 집계에서                                                          |
| 'vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name'  | 지정된 볼륨에서                                                              |
| 'vserver cifs session file show -vserver vserver_name -hosting -volume volume volume_name' | 지정된 SMB 공유에서                                                          |
| 'vserver cifs session file show -vserver vserver_name -share share_name'                   | 지정된 SMB 경로에 있어야 합니다                                                   |
| 'vserver cifs session file show -vserver vserver_name -path path path'                     | 지속적으로 사용 가능한 보호 수준을 지정합니다                                             |

|                                                                                     |                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 열려 있는 <b>SMB</b> 파일을 표시하려면...                                                       | 다음 명령을 입력합니다...                                                                                                                                                                 |
| 'vserver cifs session file show -vserver<br>vserver_name -Continuously-available{No | Yes}'<br><br>[NOTE]<br>====<br>계속 사용 가능한 상태가 '아니요'인 경우 열려 있는<br>파일은 Takeover와 Giveback에서 중단 없이 복구할 수<br>없습니다. 또한, 고가용성 관계에 있는 파트너 간의 일반<br>애그리게이트 재배치에서 복구할 수 없습니다.<br><br>==== |
| 지정된 다시 연결된 상태에서                                                                     | 'vserver cifs session file show -vserver<br>vserver_name -re연결됨{No                                                                                                              |

출력 결과를 구체화하는 데 사용할 수 있는 추가 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs session file show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

예

다음 예에서는 SVM VS1 에서 열린 파일에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1
Node: node1
Vserver: vs1
Connection: 3151274158
Session: 1
File File Open Hosting Continuously
ID Type Mode Volume Share Available

41 Regular r data data Yes
Path: \mytest.rtf
```

다음 예에서는 SVM VS1에서 파일 ID 82가 있는 개방형 SMB 파일에 대한 자세한 정보를 표시합니다.

```
cluster1::> vsriver cifs session file show -vsriver vs1 -file-id 82
-instance
```

```

Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

관련 정보

[세션 정보 표시](#)

**ONTAP SMB** 서버에서 사용 가능한 통계, 개체 및 카운터를 확인합니다.

CIFS, SMB, 감사 및 BranchCache 해시 통계에 대한 정보를 얻고 성능을 모니터링하려면 데이터를 가져올 수 있는 개체와 카운터를 알고 있어야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

| 다음 사항을 확인하고자 하는 경우: | 입력...                                               |
|---------------------|-----------------------------------------------------|
| 사용할 수 있는 개체         | '통계 카탈로그 개체 쇼'                                      |
| 사용할 수 있는 특정 개체입니다   | statistics catalog object show -object object_name  |
| 사용할 수 있는 카운터        | statistics catalog counter show -object object_name |

사용 가능한 개체 및 카운터를 비롯한 에 대한 자세한 statistics catalog object show 내용은 에서 ["ONTAP 명령 참조입니다"](#)알아보십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다



예

다음 명령을 실행하면 고급 권한 수준에 표시된 대로 클러스터에서 CIFS 및 SMB 액세스와 관련된 선택한 통계 개체에 대한 설명이 표시됩니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
 audit_ng CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
 cifs The CIFS object reports activity of the
 Common Internet File System protocol
 ...

cluster1::*> statistics catalog object show -object nblade_cifs
 nblade_cifs The Common Internet File System (CIFS)
 protocol is an implementation of the
Server
 ...

cluster1::*> statistics catalog object show -object smb1
 smb1 These counters report activity from the
SMB revision of the protocol. For information
 ...

cluster1::*> statistics catalog object show -object smb2
 smb2 These counters report activity from the
 SMB2/SMB3 revision of the protocol. For
 ...

cluster1::*> statistics catalog object show -object hashd
 hashd The hashd object provides counters to
measure the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

다음 명령을 실행하면 고급 권한 수준에서 표시되는 "CIFS" 개체의 일부 카운터에 대한 정보가 표시됩니다.



이 예제에서는 "CIFS" 객체에 대해 사용 가능한 카운터를 모두 표시하지 않고 출력이 잘립니다.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

| Counter              | Description                                                                  |
|----------------------|------------------------------------------------------------------------------|
| -----                | -----                                                                        |
| active_searches      | Number of active searches over SMB and SMB2                                  |
| auth_reject_too_many | Authentication refused after too many requests were made in rapid succession |
| avg_directory_depth  | Average number of directories crossed by SMB                                 |
| ...                  | and SMB2 path-based commands                                                 |
| ...                  | ...                                                                          |

```
cluster2::> statistics start -object client -sample-id
```

Object: client

| Counter              | Value                   |
|----------------------|-------------------------|
| -----                | -----                   |
| cifs_ops             | 0                       |
| cifs_read_ops        | 0                       |
| cifs_read_recv_ops   | 0                       |
| cifs_read_recv_size  | 0B                      |
| cifs_read_size       | 0B                      |
| cifs_write_ops       | 0                       |
| cifs_write_recv_ops  | 0                       |
| cifs_write_recv_size | 0B                      |
| cifs_write_size      | 0B                      |
| instance_name        | vserver_1:10.72.205.179 |
| instance_uuid        | 2:10.72.205.179         |
| local_ops            | 0                       |
| mount_ops            | 0                       |

[...]

- 통계를 표시합니다
- "통계 카탈로그 카운터 개체 표시"
- "통계 시작"

## ONTAP SMB 통계 표시

CIFS 및 SMB, 감사 및 BranchCache 해시에 대한 통계를 비롯한 다양한 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

시작하기 전에

객체에 대한 정보를 표시하려면 먼저 '통계 시작' 및 '통계 중지' 명령을 사용하여 데이터 샘플을 수집해야 합니다.

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 ["ONTAP 명령 참조입니다"](#).

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

| 에 대한 통계를 표시하려면...     | 입력...                      |
|-----------------------|----------------------------|
| 모든 SMB 버전             | '통계 표시 - 객체 CIFS'          |
| SMB 1.0               | '스타티틱스 쇼-객체 SMB1'          |
| SMB 2.x 및 SMB 3.0     | '스타티틱스 쇼 오브젝트 SMB2'        |
| 노드의 CIFS 하위 시스템입니다    | '스타티틱스 쇼-객체 nblade_cifs'   |
| 멀티프로토콜 감사             | '스타티틱스 쇼-객체 감사_ng'         |
| BranchCache 해시 서비스입니다 | '스타티틱스 쇼-객체 해시드'           |
| 다이나믹 DNS              | '통계 표시 - 오브젝트 DDNS_UPDATE' |

에 대한 자세한 내용은 `statistics show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

- 서버에서 사용 가능한 통계, 개체 및 카운터를 확인합니다.
- SMB 서명 세션 통계 모니터링
- BranchCache 통계를 표시합니다
- 통계를 사용하여 자동 노드 조회 활동을 모니터링합니다
- "Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"

- "성능 모니터링 설정"

## SMB 클라이언트 기반 서비스 구축

오프라인 파일을 사용하여 오프라인 사용을 위해 파일 캐싱을 허용합니다

오프라인 파일을 사용하여 **ONTAP SMB** 파일을 오프라인에서 사용할 수 있도록 캐싱하는 방법에 대해 알아보세요.

ONTAP는 오프라인 사용을 위해 파일을 로컬 호스트에 캐시할 수 있는 Microsoft 오프라인 파일 기능 또는 클라이언트측 캐싱을 지원합니다. 사용자는 오프라인 파일 기능을 사용하여 네트워크에서 연결이 끊어진 경우에도 파일 작업을 계속할 수 있습니다.

Windows 사용자 문서 및 프로그램이 자동으로 공유에서 캐시되는지 아니면 파일을 수동으로 캐시하도록 선택해야 하는지 여부를 지정할 수 있습니다. 수동 캐싱은 새 공유에 대해 기본적으로 설정됩니다. 오프라인으로 사용할 수 있는 파일은 Windows 클라이언트의 로컬 디스크와 동기화됩니다. 동기화는 특정 스토리지 시스템 공유에 대한 네트워크 접속이 복구되는 경우에 발생합니다.

오프라인 파일 및 폴더는 CIFS 서버에 저장된 파일 및 폴더의 버전과 동일한 액세스 권한을 유지하므로 오프라인 파일 및 폴더에 대한 작업을 수행하려면 CIFS 서버에 저장된 파일 및 폴더에 대한 충분한 권한이 있어야 합니다.

사용자 및 네트워크의 다른 사용자가 동일한 파일을 변경한 경우 사용자는 파일의 로컬 버전을 네트워크에 저장하거나 다른 버전을 유지하거나 둘 다 저장할 수 있습니다. 사용자가 두 버전을 모두 유지할 경우 로컬 사용자의 변경 내용이 있는 새 파일이 로컬에 저장되고 캐시된 파일은 CIFS 서버에 저장된 파일 버전의 변경 내용으로 덮어쓰입니다.

공유 구성 설정을 사용하여 공유 단위로 오프라인 파일을 구성할 수 있습니다. 공유를 만들거나 수정할 때 네 개의 오프라인 폴더 구성 중 하나를 선택할 수 있습니다.

- 캐싱이 없습니다

공유에 대한 클라이언트 측 캐시를 해제합니다. 파일과 폴더는 클라이언트에 로컬로 자동으로 캐시되지 않으며 사용자는 파일 또는 폴더를 로컬로 캐시하도록 선택할 수 없습니다.

- 수동 캐싱

공유에 캐시할 파일을 수동으로 선택할 수 있습니다. 기본 설정입니다. 기본적으로 파일 또는 폴더는 로컬 클라이언트에 캐시되지 않습니다. 사용자는 오프라인 사용을 위해 로컬로 캐시할 파일과 폴더를 선택할 수 있습니다.

- 자동 문서 캐싱

사용자 문서를 공유에 자동으로 캐시할 수 있습니다. 액세스한 파일 및 폴더만 로컬로 캐시됩니다.

- 자동 프로그램 캐싱

프로그램 및 사용자 문서를 자동으로 공유에 캐시할 수 있습니다. 액세스한 파일, 폴더 및 프로그램만 로컬로 캐시됩니다. 또한 이 설정을 사용하면 클라이언트가 네트워크에 연결되어 있는 경우에도 로컬로 캐시된 실행 파일을 실행할 수 있습니다.

Windows 서버 및 클라이언트에서 오프라인 파일을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

- 로밍 프로필을 사용하여 SVM과 연결된 CIFS 서버에 사용자 프로필을 중앙에서 저장합니다
- 폴더 리디렉션을 사용하여 서버에 데이터를 저장하는 방법에 대해 알아보세요.
- 지점 사무실에서 공유 콘텐츠를 캐시하기 위해 BranchCache를 사용하는 방법에 대해 알아보세요.
- "Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

오프라인 **ONTAP SMB** 파일 사용에 대한 요구 사항에 대해 알아보세요.

CIFS 서버에서 Microsoft 오프라인 파일 기능을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

### ONTAP 버전 요구 사항

ONTAP 릴리스는 오프라인 파일을 지원합니다.

### SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 오프라인 파일을 지원합니다.

### Windows 클라이언트 요구 사항

Windows 클라이언트는 오프라인 파일을 지원해야 합니다.

오프라인 파일 기능을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

["mysupport.netapp.com/matrix"](http://mysupport.netapp.com/matrix)

오프라인 **ONTAP SMB** 파일 배포를 위한 지침

홈 디렉토리에 'showsnapshot' 공유 속성이 설정된 홈 디렉토리 공유에 오프라인 파일을 배포할 때 이해해야 하는 몇 가지 중요한 지침이 있습니다.

공유 속성이 오프라인 파일이 구성된 홈 디렉토리 공유에 설정된 경우 showsnapshot Windows 클라이언트는 사용자의 홈 디렉토리에 있는 폴더 아래에 모든 스냅샷을 캐싱합니다. ~snapshot

다음 중 하나에 해당하면 Windows 클라이언트가 홈 디렉토리 아래에 있는 모든 스냅샷을 캐시합니다.

- 사용자가 클라이언트에서 홈 디렉토리를 오프라인으로 사용할 수 있도록 합니다.

홈 디렉토리에 있는 '~snapshot' 폴더의 내용이 포함되어 오프라인으로 사용할 수 있습니다.

- 사용자는 '내 문서'와 같은 폴더를 CIFS 서버 공유에 있는 홈 디렉토리의 루트로 리디렉션하도록 폴더 리디렉션을 구성합니다.

일부 Windows 클라이언트는 리디렉션된 폴더를 자동으로 오프라인으로 사용할 수 있도록 만들 수 있습니다. 폴더가 홈 디렉토리의 루트로 리디렉션되면 "~snapshot" 폴더가 캐시된 오프라인 콘텐츠에 포함됩니다.



오프라인 파일에 폴더가 포함된 오프라인 파일 배포는 ~snapshot 피해야 합니다. 폴더의 스냅샷에는 ~snapshot ONTAP가 스냅샷을 생성한 시점의 볼륨에 있는 모든 데이터가 포함됩니다. 따라서 폴더의 오프라인 복사본을 만들면 ~snapshot 클라이언트에서 많은 로컬 스토리지가 사용되고, 오프라인 파일 동기화 중에 네트워크 대역폭이 소모되며, 오프라인 파일을 동기화하는 데 걸리는 시간이 늘어납니다.

오프라인 **SMB** 파일 지원을 구성하기 위한 **ONTAP** 명령

SMB 공유를 생성할 때 또는 언제든지 기존 SMB 공유를 수정하여 오프라인 파일 4개 설정 중 하나를 지정하여 ONTAP CLI를 사용하여 오프라인 파일 지원을 구성할 수 있습니다. 수동 오프라인 파일 지원은 기본 설정입니다.

이 작업에 대해

오프라인 파일 지원을 구성할 때 다음 네 가지 오프라인 파일 설정 중 하나를 선택할 수 있습니다.

| 설정   | 설명                                                                                                                       |
|------|--------------------------------------------------------------------------------------------------------------------------|
| "없음" | Windows 클라이언트가 이 공유의 모든 파일을 캐싱하지 않습니다.                                                                                   |
| 수동   | Windows 클라이언트의 사용자가 캐시할 파일을 수동으로 선택할 수 있습니다.                                                                             |
| 문서   | Windows 클라이언트가 오프라인 액세스를 위해 사용자가 사용하는 사용자 문서를 캐시할 수 있도록 합니다.                                                             |
| 프로그램 | Windows 클라이언트가 오프라인 액세스를 위해 사용자가 사용하는 프로그램을 캐시에 저장하도록 허용합니다. 클라이언트는 공유를 사용할 수 있는 경우에도 오프라인 모드에서 캐시된 프로그램 파일을 사용할 수 있습니다. |

오프라인 파일 설정은 하나만 선택할 수 있습니다. 기존 SMB 공유에서 오프라인 파일 설정을 수정하면 새 오프라인 파일 설정이 원래 설정으로 대체됩니다. 기존의 다른 SMB 공유 구성 설정 및 공유 속성은 제거 또는 교체되지 않습니다. 이러한 구성 작업은 명시적으로 제거 또는 변경될 때까지 유효합니다.

단계

1. 적절한 작업을 수행합니다.

| 에서 오프라인 파일을 구성하려면... | 명령 입력...                                                                                                       |
|----------------------|----------------------------------------------------------------------------------------------------------------|
| 새로운 SMB 공유           | 'vserver cifs share create - vserver vserver_name<br>-share-name share_name -path path -offline<br>-files{none |
| manual               | documents                                                                                                      |
| programs}'           | 기존 SMB 공유입니다                                                                                                   |

|                                                                                                |            |
|------------------------------------------------------------------------------------------------|------------|
| 에서 오프라인 파일을 구성하려면...                                                                           | 명령 입력...   |
| 'vserver cifs share modify -vserver vserver_name<br>-share-name share_name -offline-files{none | manual     |
| documents                                                                                      | programs}' |

2. SMB 공유 구성이 올바른지 확인합니다. 'vserver cifs share show -vserver vserver\_name -share-name share\_name -instance'

예

다음 명령을 실행하면 오프라인 파일이 "문서"로 설정된 "data1"이라는 SMB 공유가 생성됩니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: Offline files
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: documents
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

다음 명령을 실행하면 오프라인 파일 설정을 '수동'으로 변경하고 파일 및 디렉토리 모드 생성 마스크에 대한 값을 추가하여 "data1"이라는 기존 SMB 공유가 수정됩니다.

```
cluster1::> vsriver cifs share modify -vsriver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vsriver cifs share show -vsriver vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: 644
Directory Mode Creation Mask: 777
Share Comment: Offline files
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

## 관련 정보

### 기존 주식에 주식 속성 추가 또는 제거

컴퓨터 관리 MMC를 사용하여 **ONTAP SMB** 공유에서 오프라인 파일 지원 구성

사용자가 오프라인에서 사용할 수 있도록 로컬로 파일을 캐시하도록 허용하려면 컴퓨터 관리 MMC(Microsoft Management Console)를 사용하여 오프라인 파일 지원을 구성할 수 있습니다.

## 단계

1. Windows 서버에서 MMC를 열려면 Windows 탐색기에서 로컬 컴퓨터 아이콘을 마우스 오른쪽 단추로 클릭한 다음 \* 관리 \* 를 선택합니다.
2. 왼쪽 패널에서 \* 컴퓨터 관리 \* 를 선택합니다.
3. 작업 \* > \* 다른 컴퓨터에 연결 \* 을 선택합니다.

컴퓨터 선택 대화 상자가 나타납니다.

4. CIFS 서버의 이름을 입력하거나 \* Browse \* 를 클릭하여 CIFS 서버를 찾습니다.

CIFS 서버의 이름이 SVM(Storage Virtual Machine) 호스트 이름과 같으면 SVM 이름을 입력합니다. CIFS 서버 이름이 SVM 호스트 이름과 다른 경우 CIFS 서버의 이름을 입력합니다.



5. 확인 \* 을 클릭합니다.
6. 콘솔 트리에서 \* 시스템 도구 \* > \* 공유 폴더 \* 를 클릭합니다.
7. 공유 \* 를 클릭합니다.
8. 결과 창에서 공유를 마우스 오른쪽 버튼으로 클릭합니다.
9. 속성 \* 을 클릭합니다.

선택한 공유의 속성이 표시됩니다.

10. 일반 \* 탭에서 \* 오프라인 설정 \* 을 클릭합니다.

오프라인 설정 대화 상자가 나타납니다.

11. 필요에 따라 오프라인 사용 가능성 옵션을 구성합니다.
12. 확인 \* 을 클릭합니다.

로밍 프로필을 사용하여 **SVM**과 연결된 **SMB** 서버에 사용자 프로필을 중앙에서 저장합니다

로밍 프로필을 사용하여 **ONTAP SMB** 사용자 프로필을 중앙에서 저장하는 방법에 대해 알아보세요.

ONTAP는 SVM(스토리지 가상 머신)과 연결된 CIFS 서버에 Windows 로밍 프로필을 저장할 수 있도록 지원합니다. 사용자 로밍 프로파일을 구성하면 사용자가 로그인하는 위치에 관계없이 자동 리소스 사용 가능 여부 등의 이점이 제공됩니다. 또한 로밍 프로필은 사용자 프로필의 관리 및 관리를 간소화합니다.

로밍 사용자 프로필에는 다음과 같은 이점이 있습니다.

- 자동 리소스 가용성

사용자가 Windows 8, Windows 7, Windows 2000 또는 Windows XP를 실행하는 네트워크의 컴퓨터에 로그인하면 사용자의 고유한 프로필을 자동으로 사용할 수 있습니다. 사용자는 네트워크에서 사용하는 각 컴퓨터에 프로파일을 만들 필요가 없습니다.

- 간편한 컴퓨터 교체

사용자 프로파일 정보는 모두 네트워크에서 별도로 유지되므로 사용자의 프로파일을 새 대체 컴퓨터에 쉽게 다운로드할 수 있습니다. 사용자가 새 컴퓨터에 처음 로그인하면 사용자 프로필의 서버 복사본이 새 컴퓨터에 복사됩니다.

#### 관련 정보

- [오프라인 사용을 위해 파일을 캐싱하는 오프라인 파일 사용에 대해 알아보세요.](#)
- [폴더 리디렉션을 사용하여 서버에 데이터를 저장하는 방법에 대해 알아보세요.](#)

로밍 **ONTAP SMB** 프로필 사용에 대한 요구 사항에 대해 알아보세요.

CIFS 서버에서 Microsoft의 로밍 프로필을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

## ONTAP 버전 요구 사항

ONTAP는 로밍 프로필을 지원합니다.

## SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 로밍 프로필을 지원합니다.

## Windows 클라이언트 요구 사항

사용자가 로밍 프로필을 사용하려면 Windows 클라이언트가 이 기능을 지원해야 합니다.

로밍 프로필을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

["NetApp 상호 운용성 매트릭스 툴"](#)

## Active Directory 사용자 및 컴퓨터 MMC를 통해 로밍 ONTAP SMB 프로필 구성

사용자가 네트워크의 컴퓨터에 로그인할 때 자동으로 사용자 프로필을 사용할 수 있도록 하려면 Active Directory 사용자 및 컴퓨터 MMC 스냅인을 통해 로밍 프로필을 구성할 수 있습니다. Windows Server에서 로밍 프로필을 구성하는 경우 Active Directory 관리 센터를 사용할 수 있습니다.

단계

1. Windows 서버에서 Active Directory 사용자 및 컴퓨터 MMC(또는 Windows 서버의 Active Directory 관리 센터)를 엽니다.
2. 로밍 프로필을 구성할 사용자를 찾습니다.
3. 사용자를 마우스 오른쪽 단추로 클릭하고 \* 속성 \* 을 클릭합니다.
4. 프로필 \* 탭에서 사용자의 로밍 프로필을 저장할 공유의 프로파일 경로를 입력한 다음 '%username%'을(를) 입력합니다.

예를 들어, 프로파일 경로는 다음과 같습니다: '\\vs1.example.com\profiles\%username%'. 사용자가 처음 로그인하면 '%username%'이(가) 사용자 이름으로 대체됩니다.



'\\vs1.example.com\profiles\%username%' 경로에서 'profiles'는 SVM(Storage Virtual Machine) VS1 공유에 대한 공유 이름이며 모든 사람에게 모든 권한이 부여됩니다.

5. 확인 \* 을 클릭합니다.

## SMB 서버에 데이터를 저장하려면 폴더 리디렉션을 사용합니다

ONTAP SMB 서버에 데이터를 저장하기 위해 폴더 리디렉션을 사용하는 방법에 대해 알아보세요.

ONTAP는 사용자 또는 관리자가 로컬 폴더의 경로를 CIFS 서버의 위치로 리디렉션할 수 있도록 Microsoft 폴더 리디렉션을 지원합니다. SMB 공유에 데이터가 저장되어 있더라도 리디렉션된 폴더가 로컬 Windows 클라이언트에 저장된 것처럼 나타납니다.

폴더 리디렉션은 주로 홈 디렉터리를 이미 배포했으며 기존 홈 디렉터리 환경과의 호환성을 유지하고자 하는 조직을 위한 것입니다.

- 문서, 바탕 화면, 시작 메뉴 등을 리디렉션할 수 있는 폴더의 예로 들 수 있습니다.
- 사용자는 Windows 클라이언트에서 폴더를 리디렉션할 수 있습니다.
- 관리자는 Active Directory에서 GPO를 구성하여 폴더 리디렉션을 중앙 집중식으로 구성 및 관리할 수 있습니다.
- 관리자가 로밍 프로필을 구성한 경우 폴더 리디렉션을 통해 관리자가 사용자 데이터를 프로필 데이터에서 나눌 수 있습니다.
- 관리자는 폴더 리디렉션 및 오프라인 파일을 함께 사용하여 로컬 폴더의 데이터 스토리지를 CIFS 서버로 리디렉션하는 동시에 사용자가 콘텐츠를 로컬로 캐시할 수 있습니다.

#### 관련 정보

- [오프라인 사용을 위해 파일을 캐싱하는 오프라인 파일 사용에 대해 알아보세요.](#)
- [로밍 프로필을 사용하여 SVM과 연결된 CIFS 서버에 사용자 프로필을 중앙에서 저장합니다](#)

**ONTAP SMB** 폴더 리디렉션 사용에 대한 요구 사항에 대해 알아보세요.

CIFS 서버에서 Microsoft의 폴더 리디렉션을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

#### ONTAP 버전 요구 사항

ONTAP는 Microsoft 폴더 리디렉션을 지원합니다.

#### SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP는 모든 버전의 SMB에서 Microsoft의 폴더 리디렉션을 지원합니다.

#### Windows 클라이언트 요구 사항

사용자가 Microsoft의 폴더 리디렉션을 사용하려면 Windows 클라이언트가 이 기능을 지원해야 합니다.

폴더 리디렉션을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

#### Windows 속성을 사용하여 ONTAP SMB 폴더 리디렉션 구성

Windows 속성 창을 사용하여 폴더 리디렉션을 구성할 수 있습니다. 이 방법을 사용하면 Windows 사용자가 SVM 관리자의 도움 없이 폴더 리디렉션을 구성할 수 있다는 이점이 있습니다.

#### 단계

1. Windows 탐색기에서 네트워크 공유로 리디렉션할 폴더를 마우스 오른쪽 단추로 클릭합니다.
2. 속성 \* 을 클릭합니다.  
  
선택한 공유의 속성이 표시됩니다.
3. 바로 가기 \* 탭에서 \* 대상 \* 을 클릭하고 선택한 폴더를 리디렉션할 네트워크 위치의 경로를 지정합니다.

예를 들어, 폴더를 "Q:\\"에 매핑된 홈 디렉토리의 "ata" 폴더로 리디렉션하려면 "Q:\data"를 대상으로 지정합니다.

#### 4. 확인 \* 을 클릭합니다.

오프라인 폴더 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

#### 관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

**SMB 2.x**를 사용하여 **Windows** 클라이언트에서 **ONTAP ~snapshot** 디렉토리에 액세스하는 방법에 대해 알아보세요.

SMB 2.x를 사용하여 Windows 클라이언트에서 디렉토리에 액세스하는 방법은 ~snapshot SMB 1.0에 사용되는 방법과 다릅니다. SMB 2.x 연결을 사용하여 스냅샷에 저장된 데이터에 성공적으로 액세스할 때 디렉토리에 액세스하는 방법을 이해해야 ~snapshot 합니다.

SVM 관리자는 가상 서버 CIFS 공유 속성 제품군의 명령을 사용하여 'showsnapshot' 공유 속성을 활성화하거나 비활성화하여 Windows 클라이언트의 사용자가 공유의 '~snapshot' 디렉토리를 보고 액세스할 수 있는지 여부를 제어합니다.

`showsnapshot` 공유 속성을 비활성화하면 SMB 2.x를 사용하는 Windows 클라이언트의 사용자는 디렉토리를 볼 수 `~snapshot` 없으며 디렉토리 내의 특정 스냅샷이나 디렉토리에 대한 경로를 수동으로 입력하는 경우에도 디렉토리 `~snapshot` 내의 스냅샷에 액세스할 수 `~snapshot` 없습니다.

'showsnapshot' 공유 속성이 활성화되면 SMB 2.x를 사용하는 Windows 클라이언트의 사용자는 공유 루트 또는 공유 루트 아래의 연결 지점 또는 디렉토리 내에서 '~snapshot' 디렉토리를 볼 수 없습니다. 그러나 공유에 접속한 후에는 공유 경로의 끝에 수동으로 \~snapshot을 추가하여 숨겨진 '~snapshot' 디렉토리에 액세스할 수 있습니다. 숨겨진 '~snapshot' 디렉토리는 두 개의 진입점에서 액세스할 수 있습니다.

- 공유 루트에 있습니다
- 공유 공간의 모든 접합 지점에서

공유 내의 비접속 하위 디렉토리에서는 숨겨진 '~snapshot' 디렉토리에 액세스할 수 없습니다.

#### 예

다음 예제에서 보여 주는 구성을 사용하면 "eng" 공유에 SMB 2.x가 연결되어 있는 Windows 클라이언트의 사용자가 공유 경로 및 경로의 모든 연결 지점에서 공유 경로에 "\~snapshot"을 수동으로 추가하여 '~snapshot' 디렉토리에 액세스할 수 있습니다. 숨겨진 '~snapshot' 디렉토리는 다음 세 가지 경로에서 액세스할 수 있습니다.

- '\\VS1\ENG\~스냅샷'
- '\\VS1\ENG\projects1\~스냅샷'
- '\\VS1\ENG\projects2\~스냅샷'

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume junction-path

vs1 vs1_root /
vs1 vs1_vol1 /eng
vs1 vs1_vol2 /eng/projects1
vs1 vs1_vol3 /eng/projects2

cluster1::> vsserver cifs share show
Vserver Share Path Properties Comment ACL

vs1 eng /eng oplocks - Everyone / Full Control
 chngenotify
 browsable
 showsnapshot
```

이전 버전을 사용하여 파일 및 폴더를 복구합니다

이전 버전을 사용하여 **ONTAP SMB** 파일 및 폴더 복구에 대해 알아보세요

Microsoft 이전 버전을 사용하는 기능은 특정 형태의 스냅샷을 지원하고 이를 사용하도록 설정한 파일 시스템에 적용할 수 있습니다. 스냅샷 기술은 ONTAP의 핵심 요소입니다. 사용자는 Microsoft 이전 버전 기능을 사용하여 Windows 클라이언트에서 스냅샷의 파일과 폴더를 복구할 수 있습니다.

이전 버전 기능을 사용하면 스토리지 관리자의 개입 없이 스냅샷을 탐색하거나 스냅샷에서 데이터를 복구할 수 있습니다. 이전 버전은 구성할 수 없습니다. 항상 활성화되어 있습니다. 스토리지 관리자가 공유에서 스냅샷을 사용할 수 있도록 설정한 경우 사용자는 이전 버전을 사용하여 다음 작업을 수행할 수 있습니다.

- 실수로 삭제된 파일을 복구합니다.
- 실수로 파일을 덮어쓴 경우 복구
- 작업 중 파일 버전을 비교합니다.

스냅샷에 저장된 데이터는 읽기 전용입니다. 파일을 변경하려면 파일 복사본을 다른 위치에 저장해야 합니다. 스냅샷은 주기적으로 삭제되므로 이전 버전의 파일을 영구적으로 보존하려면 이전 버전에 포함된 파일의 복사본을 만들어야 합니다.

**Microsoft** 이전 버전을 사용하기 위한 **ONTAP SMB** 요구 사항

CIFS 서버에서 이전 버전을 사용하려면 먼저 ONTAP 및 SMB의 버전과 지원 대상 Windows 클라이언트를 알아야 합니다. 또한 스냅샷 설정 요구 사항에 대해서도 알아야 합니다.

**ONTAP** 버전 요구 사항

이전 버전을 지원합니다.

## SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 이전 버전을 지원합니다.

## Windows 클라이언트 요구 사항

사용자가 이전 버전을 사용하여 스냅샷의 데이터에 액세스하려면 Windows 클라이언트가 해당 기능을 지원해야 합니다.

이전 버전을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

## "NetApp 상호 운용성 매트릭스 툴"

### 스냅샷 설정에 대한 요구 사항

이전 버전을 사용하여 스냅샷의 데이터에 액세스하려면 활성화된 스냅샷 정책이 데이터를 포함하는 볼륨에 연결되어 있어야 하고, 클라이언트가 스냅샷 데이터에 액세스할 수 있어야 하며, 스냅샷이 있어야 합니다.

**Windows** 이전 버전 탭을 사용하여 **ONTAP SMB** 스냅샷 데이터를 보고 관리합니다.

Windows 클라이언트 시스템의 사용자는 Windows 속성 창의 이전 버전 탭을 사용하여 SVM(스토리지 가상 시스템) 관리자의 개입 없이 스냅샷에 저장된 데이터를 복원할 수 있습니다.

### 이 작업에 대해

관리자가 공유를 포함하는 볼륨에 스냅샷을 설정하고 관리자가 스냅샷을 표시하도록 공유를 구성한 경우에는 이전 버전 탭을 사용하여 SVM에 저장된 데이터의 스냅샷에서 데이터를 보고 관리할 수 있습니다.

### 단계

1. Windows 탐색기에서 CIFS 서버에 저장된 데이터의 매핑된 드라이브 콘텐츠를 표시합니다.
2. 스냅샷을 보거나 관리할 매핑된 네트워크 드라이브에서 파일 또는 폴더를 마우스 오른쪽 단추로 클릭합니다.
3. 속성 \* 을 클릭합니다.

선택한 파일 또는 폴더의 속성이 표시됩니다.

4. 이전 버전 \* 탭을 클릭합니다.

선택한 파일 또는 폴더의 사용 가능한 스냅샷 목록이 폴더 버전: 상자에 표시됩니다. 나열된 스냅샷은 스냅샷 이름 접두사 및 생성 타임스탬프로 식별됩니다.

5. 폴더 버전: \* 상자에서 관리할 파일 또는 폴더의 복사본을 마우스 오른쪽 단추로 클릭합니다.
6. 적절한 작업을 수행합니다.

|                         |               |
|-------------------------|---------------|
| 원하는 작업                  | 다음을 수행합니다.    |
| 해당 스냅샷의 데이터를 봅니다        | 열기 * 를 클릭합니다. |
| 해당 스냅샷에서 데이터 복제본을 생성합니다 | 복사 * 를 클릭합니다. |

스냅샷의 데이터는 읽기 전용입니다. 이전 버전 탭에 나열된 파일과 폴더를 수정하려면 쓰기 가능한 위치에 수정할 파일 및 폴더의 복사본을 저장하고 복사본을 수정해야 합니다.

7. 스냅샷 데이터 관리를 마친 후 \* 확인 \* 을 클릭하여 \* 속성 \* 대화 상자를 닫습니다.

이전 버전 탭을 사용하여 스냅샷 데이터를 보고 관리하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

#### 관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

**ONTAP SMB** 스냅샷을 이전 버전에서 사용할 수 있는지 확인하세요.

활성화된 스냅샷 정책이 공유를 포함하는 볼륨에 적용되고 볼륨 구성에서 스냅샷에 대한 액세스를 허용하는 경우에만 이전 버전 탭에서 스냅샷을 볼 수 있습니다. 스냅샷 가용성을 확인하는 것은 이전 버전 액세스 권한을 가진 사용자를 지원할 때 유용합니다.

#### 단계

1. 공유 데이터가 있는 볼륨에 자동 스냅샷이 설정되어 있는지 여부와 클라이언트가 스냅샷 디렉토리에 액세스할 수 있는지 여부를 확인합니다. `volume show -vserver vservers -volume volume-name -fields vservers,volume,snapdir-access,snapshot-policy,snapshot-count`

이 출력에는 볼륨과 연결된 스냅샷 정책, 클라이언트 스냅샷 디렉토리 액세스 사용 여부 및 사용 가능한 스냅샷 수가 표시됩니다.

2. 연결된 스냅샷 정책이 설정되었는지 확인합니다. `volume snapshot policy show -policy policy-name`
3. 사용 가능한 스냅샷 나열: `volume snapshot show -volume volume_name`

스냅샷 정책 및 스냅샷 스케줄을 구성하고 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. "[데이터 보호](#)"

#### 예

다음 예에서는 "data1"의 공유 데이터 및 사용 가능한 스냅샷을 포함하는 "data1" 볼륨과 연관된 스냅샷 정책에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver volume snapdir-access snapshot-policy snapshot-count

vs1 data1 true default 10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

Number of Is
Policy Name Schedules Enabled Comment

default 3 true Default policy with hourly, daily &
weekly schedules.

Schedule Count Prefix SnapMirror Label

hourly 6 hourly -
daily 2 daily daily
weekly 2 weekly weekly

cluster1::> volume snapshot show -volume data1

Vserver Volume Snapshot State Size Total% Used%

vs1 data1

weekly.2012-12-16_0015 valid 408KB 0% 1%
daily.2012-12-22_0010 valid 420KB 0% 1%
daily.2012-12-23_0010 valid 192KB 0% 0%
weekly.2012-12-23_0015 valid 360KB 0% 1%
hourly.2012-12-23_1405 valid 196KB 0% 0%
hourly.2012-12-23_1505 valid 196KB 0% 0%
hourly.2012-12-23_1605 valid 212KB 0% 0%
hourly.2012-12-23_1705 valid 136KB 0% 0%
hourly.2012-12-23_1805 valid 200KB 0% 0%
hourly.2012-12-23_1905 valid 184KB 0% 0%
```

#### 관련 정보

- [이전 버전 액세스를 활성화하기 위한 스냅샷 구성 생성](#)
- ["데이터 보호"](#)

이전 버전 액세스를 활성화하기 위해 **ONTAP SMB** 스냅샷 구성을 만듭니다.

스냅샷에 대한 클라이언트 액세스가 설정되어 있고 스냅샷이 있는 경우 이전 버전 기능을 항상 사용할 수 있습니다. 스냅샷 구성이 이러한 요구 사항을 충족하지 않는 경우 를 충족하는 스냅샷 구성을 생성할 수 있습니다.



## 단계

1. 이전 버전 액세스를 허용하려는 공유가 포함된 볼륨에 연결된 스냅샷 정책이 없는 경우 스냅샷 정책을 볼륨에 연결하고 명령을 사용하여 활성화합니다. `volume modify`

에 대한 자세한 내용은 `volume modify` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 명령을 사용하여 옵션을 `true` 설정하여 `-snap-dir` 스냅샷에 대한 액세스를 `volume modify` 설정합니다.

에 대한 자세한 내용은 `volume modify` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. `volume snapshot policy show` 명령을 사용하여 스냅샷 정책이 설정되어 있고 스냅샷 디렉토리에 대한 액세스가 설정되어 있는지 `volume show` 확인합니다.

`volume snapshot policy show`에 대한 자세한 `volume show` 내용은 ["ONTAP 명령 참조입니다"](#) 참조하십시오.

스냅샷 정책 및 스냅샷 스케줄을 구성하고 관리하는 방법에 대한 자세한 내용은 ["데이터 보호"](#)을 참조하십시오.

## 관련 정보

["데이터 보호"](#)

**ONTAP SMB** 접합을 포함하는 이전 버전 디렉토리 복원에 대해 알아보세요.

이전 버전을 사용하여 교차점이 포함된 폴더를 복원할 때 유의해야 할 몇 가지 지침이 있습니다.

이전 버전을 사용하여 정션 포인트인 하위 폴더가 있는 폴더를 복원할 때 "액세스 거부" 오류로 인해 복구가 실패할 수 있습니다.

복원하려는 폴더에 '-parent' 옵션과 함께 'vol show' 명령을 사용하여 교차점이 있는지 여부를 확인할 수 있습니다. 또한 'vserver security trace' 명령을 사용하여 파일 및 폴더 액세스 문제에 대한 자세한 로그를 생성할 수 있습니다.

## 관련 정보

[NAS 네임스페이스에서 데이터 볼륨 생성 및 관리](#)

## SMB 서버 기반 서비스 구축

홈 디렉토리를 관리합니다

**ONTAP SMB** 서버에서 동적 홈 디렉토리를 활성화하는 방법에 대해 알아보세요.

ONTAP 홈 디렉토리를 사용하면 연결된 사용자와 변수 집합을 기반으로 서로 다른 디렉토리에 매핑되는 SMB 공유를 구성할 수 있습니다. 각 사용자에게 대해 별도의 공유를 생성하는 대신 몇 가지 홈 디렉토리 매개 변수를 사용하여 하나의 공유를 구성하여 진입점(공유)과 홈 디렉토리(SVM의 디렉토리) 간의 사용자 관계를 정의할 수 있습니다.

게스트 사용자로 로그인한 사용자는 홈 디렉토리가 없으며 다른 사용자의 홈 디렉토리에 액세스할 수 없습니다. 사용자가 디렉토리에 매핑되는 방식을 결정하는 변수는 네 가지입니다.

- \* 공유 이름 \*

사용자가 연결하는 공유의 이름입니다. 이 공유에 대한 홈 디렉토리 속성을 설정해야 합니다.

공유 이름에는 다음 동적 이름을 사용할 수 있습니다.

- '%w'(사용자의 Windows 사용자 이름)
- '%d'(사용자의 Windows 도메인 이름)
- '%u'(사용자가 매핑한 UNIX 사용자 이름)공유 이름을 모든 홈 디렉토리에 고유하도록 하려면 공유 이름에 '%w' 또는 '%u' 변수가 포함되어야 합니다. 공유 이름에는 "%d"와 "%w" 변수(예: "%d"/"%w")가 모두 포함될 수 있으며, 공유 이름에는 정적 부분과 변수 부분(예: home\_""%w")이 포함될 수 있습니다.

#### • \* 공유 경로 \*

이 경로는 공유에 의해 정의되고 공유 이름 중 하나와 연관되며, SVM의 루트에서 사용자의 전체 홈 디렉토리 경로를 생성하기 위해 각 검색 경로에 추가됩니다. 정적(예: "home"), 동적(예: "%w") 또는 두 가지 조합(예: "eng/%w")일 수 있습니다.

#### • \* 검색 경로 \*

ONTAP에서 홈 디렉토리를 검색하도록 지정하는 SVM 루트의 절대 경로 세트입니다. 명령을 사용하여 검색 경로를 하나 이상 지정할 수 `vserver cifs home-directory search-path add` 있습니다. 여러 개의 검색 경로를 지정하면 ONTAP는 유효한 경로를 찾을 때까지 지정된 순서대로 경로를 시도합니다. 에 대한 자세한 내용은 `vserver cifs home-directory search-path add` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

#### • \* 디렉토리 \*

사용자를 위해 생성한 사용자의 홈 디렉토리입니다. 디렉터리 이름은 일반적으로 사용자의 이름입니다. 검색 경로로 정의된 디렉토리 중 하나에 홈 디렉토리를 생성해야 합니다.

예를 들어, 다음 설정을 고려합니다.

- 사용자: John Smith
- 사용자 도메인: Acme
- 사용자 이름: jsmith
- SVM 이름: vs1
- 홈 디렉토리 공유 이름 #1: home\_"%w" - 공유 경로: "%w"
- 홈 디렉토리 공유 이름 #2:"%w" - 공유 경로: "%d/%w"
- 검색 경로 #1:'/vol0home/home'
- 검색 경로 #2:'/vol1home/home'
- 검색 경로 #3:'/vol2home/home'
- 홈 디렉토리: '/vol1home/home/jsmith'

시나리오 1: 사용자가 '\\VS1\home\_jsmith'에 연결합니다. 첫 번째 홈 디렉토리 공유 이름과 일치하고 상대 경로 jsmith를 생성합니다. ONTAP는 이제 각 검색 경로를 순서대로 확인하여 jsmith라는 디렉토리를 검색합니다.

- '/vol0home/home/jsmith'가 존재하지 않아 2번 검색경로로 이동함.
- '/vol1home/home/jsmith'가 존재하므로 검색 경로 #3이 확인되지 않고 사용자가 홈 디렉토리에 연결되어 있습니다.

시나리오 2: 사용자가 '\\VS1\jsmith'에 연결합니다. 두 번째 홈 디렉토리 공유 이름과 일치하고 상대 경로 Acme/jsmith를 생성합니다. ONTAP은 이제 각 검색 경로를 순서대로 확인하여 "Acme/jsmith"라는 디렉토리를 검색합니다.

- '/vol0home/home/acme/jsmith'가 존재하지 않고 검색 경로 #2로 이동합니다.
- '/vol1home/home/acme/jsmith'가 존재하지 않고 검색 경로 #3으로 이동합니다.
- '/vol2home/home/acme/jsmith'가 존재하지 않아 홈 디렉토리가 존재하지 않아 연결이 실패합니다.

홈 디렉토리 공유

## ONTAP SMB 홈 디렉토리 공유 추가

SMB 홈 디렉토리 기능을 사용하려면 공유 속성에 포함된 홈 디렉토리 속성에 공유를 하나 이상 추가해야 합니다.

이 작업에 대해

'vserver cifs share create' 명령을 사용하여 공유를 생성할 때 홈 디렉토리 공유를 생성하거나 'vserver cifs share modify' 명령을 사용하여 언제든지 기존 공유를 홈 디렉토리 공유로 변경할 수 있습니다.

홈 디렉토리 공유를 생성하려면 공유를 생성하거나 수정할 때 '-share-properties' 옵션에 homedirectory 값을 포함해야 합니다. 사용자가 홈 디렉토리에 연결할 때 동적으로 확장되는 변수를 사용하여 공유 이름을 지정하고 경로를 공유할 수 있습니다. 경로에서 사용할 수 있는 변수는 각각 Windows 사용자 이름, 도메인 및 매핑된 UNIX 사용자 이름에 해당하는 "%w", "%d" 및 "%u"입니다.

단계

1. 홈 디렉토리 공유 추가: + 'vserver cifs share create -vserver\_vserver\_name\_-share-name\_share\_name\_-path\_path\_-share-properties homedirectory [...]'

'-vserver'vserver'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

'-share-name\_share-name\_'은 홈 디렉토리 공유 이름을 지정합니다.

공유 이름에 리터럴 문자열 '%w', '%u' 또는 '%d' 중 하나가 포함된 경우 필수 변수 중 하나가 포함된 것 외에도 ONTAP가 리터럴 문자열을 변수(예: "%w")로 취급하지 않도록 리터럴 문자열 앞에 %(percent) 문자를 입력해야 합니다.

- 공유 이름에는 '%w' 또는 '%u' 변수가 포함되어야 합니다.
- 공유 이름에는 "%d" 변수(예: "%d"/"%w") 또는 공유 이름의 정적 부분(예: home1\_""%w")이 추가로 포함될 수 있습니다.
- 관리자가 공유를 사용하여 다른 사용자의 홈 디렉토리에 연결하거나 사용자가 다른 사용자의 홈 디렉토리에 연결할 수 있도록 허용하는 경우 동적 공유 이름 패턴 앞에는 물결표(~)가 와야 합니다.

vserver cifs home-directory modify는 '-is-home-dirs-access-for-admin-enabled' 옵션을 true로 설정하거나 고급 옵션 '-is-home-dirs-access-for-public-enabled'를 true로 설정하여 이 액세스를 활성화하는 데 사용됩니다.

path는 홈 디렉토리의 상대 경로를 지정합니다.

'-share-properties homedirectory[,...]'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다.

심표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

1. 'vserver cifs share show' 명령을 사용하여 홈 디렉토리 공유를 성공적으로 추가했는지 확인하십시오.

예

다음 명령을 실행하면 "%w"라는 홈 디렉토리 공유가 생성됩니다. oplocks, browsable, changenotify 공유 속성은 homedir 공유 속성을 설정하는 것 외에도 설정됩니다.



이 예에서는 SVM의 모든 공유에 대한 출력을 표시하지 않습니다. 출력이 잘립니다.

```
cluster1::> vs1 cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vs1 cifs share show -vserver vs1
Vserver Share Path Properties Comment ACL

vs1 %w %w oplocks - Everyone / Full
Control
 browsable
 changenotify
 homedirectory
```

관련 정보

- [홈 디렉토리 검색 경로 추가](#)
- [서버에서 자동 노드 참조를 사용하기 위한 요구 사항 및 지침](#)
- [사용자 홈 디렉토리에 대한 접근성 관리](#)

홈 디렉토리 공유에 대한 고유한 **ONTAP SMB** 사용자 이름 요구 사항에 대해 알아보세요.

공유를 동적으로 생성하려면 "%w"(Windows 사용자 이름) 또는 "%u"(UNIX 사용자 이름) 변수를 사용하여 홈 디렉토리 공유를 생성할 때 고유한 사용자 이름을 지정해야 합니다. 공유 이름이 사용자 이름에 매핑됩니다.

정적 공유 이름과 사용자 이름이 같을 때 다음 두 가지 문제가 발생할 수 있습니다.

- 사용자가 net view 명령을 사용하여 클러스터의 공유를 나열하면 동일한 사용자 이름의 공유 두 개가 표시됩니다.
- 사용자가 해당 공유 이름에 연결하면 사용자는 항상 정적 공유에 연결되어 있으며 동일한 이름으로 홈 디렉토리 공유에 액세스할 수 없습니다.

예를 들어 "administrator"라는 이름의 공유가 있고 "administrator" Windows 사용자 이름이 있습니다. 홈 디렉토리 공유를 만들고 해당 공유에 연결하면 ""administrator"" 홈 디렉토리 공유가 아니라 ""administrator"" 정적 공유에 연결됩니다.

다음 단계를 수행하여 중복된 공유 이름으로 문제를 해결할 수 있습니다.

- 사용자의 홈 디렉토리 공유와 더 이상 충돌하지 않도록 정적 공유의 이름을 바꿉니다.

- 사용자에게 더 이상 정적 공유 이름과 충돌하지 않도록 새 사용자 이름을 제공합니다.
- '%w' 매개 변수를 사용하는 대신 "'home'"과 같은 정적 이름으로 CIFS 홈 디렉토리 공유를 생성하여 공유 이름과 충돌하지 않도록 합니다.

업그레이드 후 정적 **ONTAP SMB** 홈 디렉토리 공유 이름에 어떤 일이 발생하는지 알아보세요.

홈 디렉토리 공유 이름에는 "%w" 또는 "%u" 동적 변수가 포함되어야 합니다. 새로운 요구 사항으로 ONTAP 버전으로 업그레이드한 후 기존 정적 홈 디렉토리 공유 이름에 어떤 일이 발생할지 알고 있어야 합니다.

홈 디렉토리 구성에 정적 공유 이름이 포함되어 있고 ONTAP로 업그레이드하면 정적 홈 디렉토리 공유 이름이 변경되지 않으며 여전히 유효합니다. 그러나 "%w" 또는 "%u" 변수를 포함하지 않는 새 홈 디렉토리 공유는 생성할 수 없습니다.

이러한 변수 중 하나를 사용자의 홈 디렉토리 공유 이름에 포함하도록 요구하면 모든 공유 이름이 홈 디렉토리 구성에서 고유하도록 할 수 있습니다. 필요한 경우 정적 홈 디렉토리 공유 이름을 "%w" 또는 "%u" 변수가 포함된 이름으로 변경할 수 있습니다.

#### ONTAP SMB 홈 디렉토리 검색 경로 추가

ONTAP SMB 홈 디렉토리를 사용하려면 하나 이상의 홈 디렉토리 검색 경로를 추가해야 합니다.

이 작업에 대해

'vserver cifs home-directory search-path add' 명령을 사용하여 홈 디렉토리 검색 경로를 추가할 수 있습니다.

'vserver cifs home-directory search-path add' 명령은 명령 실행 중에 '-path' 옵션에 지정된 경로를 확인합니다. 지정된 경로가 없으면 명령을 실행하면 계속할 것인지 여부를 묻는 메시지가 생성됩니다. 당신은 'y'나 'n'을 선택합니다. 계속하려면 y를 선택하면 ONTAP가 검색 경로를 생성합니다. 그러나 홈 디렉토리 구성에서 검색 경로를 사용하려면 먼저 디렉토리 구조를 만들어야 합니다. 계속하지 않도록 선택하면 명령이 실패하고 검색 경로가 생성되지 않습니다. 그런 다음 경로 디렉토리 구조를 생성하고 'vserver cifs home-directory search-path add' 명령을 다시 실행할 수 있습니다.

단계

1. 홈 디렉토리 검색 경로 'vserver cifs home-directory search-path add-vserver vserver-path path path' 추가
2. 'vserver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.

예

다음 예에서는 SVM VS1 홈 디렉토리 구성에 경로 '/home1'을 추가합니다.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver Position Path

vs1 1 /home1
```

다음 예에서는 SVM VS1 홈 디렉토리 구성에 경로 '/home2'를 추가하려고 합니다. 경로가 존재하지 않습니다. 계속하지 않도록 선택할 수 있습니다.

```
cluster::> vservers cifs home-directory search-path add -vservers vs1 -path /home2
Warning: The specified path "/home2" does not exist in the namespace
 belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

## 관련 정보

### 홈 디렉토리 공유 추가

%w 및 %d 변수를 사용하여 **ONTAP SMB** 홈 디렉토리 구성을 만듭니다.

"%w" 및 "%d" 변수를 사용하여 홈 디렉토리 설정을 작성할 수 있습니다. 사용자는 동적으로 생성된 공유를 사용하여 홈 공유에 연결할 수 있습니다.

## 단계

1. 사용자의 홈 디렉토리를 포함할 qtree를 생성합니다: 'volume qtree create-vservers vservers\_name-qtree-path qtree\_path'
2. qtree가 올바른 보안 유형인 'volume qtree show'를 사용하는지 확인합니다
3. Qtree에서 원하는 보안 스타일을 사용하지 않는 경우 'volume qtree security' 명령을 사용하여 보안 스타일을 변경하십시오.
4. 홈 디렉토리 공유 추가: "vservers cifs share create-vservers vservers-share-name %w-path %d/%w-share-properties homedir디렉토리[,...]"

'-vservers"vservers'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

'-share-name '%w'는 홈 디렉토리 공유 이름을 지정합니다. ONTAP는 각 사용자가 홈 디렉토리에 접속할 때 동적으로 공유 이름을 생성합니다. 공유 이름은 *WINDOWS\_USER\_NAME* 형식입니다.

'-path '%d/%w'는 홈 디렉토리의 상대 경로를 지정합니다. 상대 경로는 각 사용자가 자신의 홈 디렉토리에 접속할 때 동적으로 생성되며 *domain/windows\_user\_name* 형식이 됩니다.

'-share-properties homedir디렉토리 [,...]+'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다. 심표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

5. 'vservers cifs share show' 명령을 사용하여 공유에 원하는 구성이 있는지 확인합니다.
6. 홈 디렉토리 검색 경로 'vservers cifs home-directory search-path add-vservers vservers-path path path' 추가

'-vservers\_vservers-name\_'은 검색 경로를 추가할 CIFS 지원 SVM을 지정합니다.

'-path\_path\_'는 검색 경로에 대한 절대 디렉토리 경로를 지정합니다.

7. 'vservers cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.
8. 홈 디렉토리가 있는 사용자의 경우 홈 디렉토리를 포함하도록 지정된 qtree 또는 볼륨에 해당 디렉토리를

생성합니다.

예를 들어, '/vol/vol1/users' 경로와 생성할 디렉토리가 mydomain\user1인 사용자 이름으로 qtree를 생성한 경우 '/vol/vol1/users/mydomain/user1' 경로를 사용하여 디렉토리를 생성합니다.

/home1 에 마운트된 ""home1" 볼륨을 생성한 경우 "/home1/mydomain/user1" 경로를 사용하여 디렉토리를 생성합니다.

9. 드라이브를 매핑하거나 UNC 경로를 사용하여 연결하여 사용자가 홈 공유에 성공적으로 연결할 수 있는지 확인합니다.

예를 들어, mydomain\user1 사용자가 SVM VS1 에 있는 8단계에서 생성한 디렉토리에 연결하려는 경우 user1은 UNC 경로 "\\VS1\user1"을 사용하여 연결됩니다.

예

다음 예제의 명령은 다음과 같은 설정으로 홈 디렉토리 구성을 만듭니다.

- 공유 이름은 %W입니다
- 상대 홈 디렉토리 경로는 %d/%W입니다
- 홈 디렉토리 /home1 을 포함하는 데 사용되는 검색 경로는 NTFS 보안 스타일로 구성된 볼륨입니다.
- SVM VS1 에서 구성이 생성됩니다.

사용자가 Windows 호스트에서 홈 디렉토리에 액세스할 때 이 유형의 홈 디렉토리 구성을 사용할 수 있습니다. 또한 사용자가 Windows 및 UNIX 호스트에서 홈 디렉토리를 액세스할 때 이 유형의 구성을 사용할 수 있으며 파일 시스템 관리자는 Windows 기반 사용자 및 그룹을 사용하여 파일 시스템에 대한 액세스를 제어할 수 있습니다.

```

cluster::> vservers cifs share create -vservers vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vservers cifs share show -vservers vs1 -share-name %w

 Vserver: vs1
 Share: %w
CIFS Server NetBIOS Name: VS1
 Path: %d/%w
 Share Properties: oplocks
 browsable
 changenotify
 homedirectory
 Symlink Properties: enable
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
 Volume Name: -
 Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vservers cifs home-directory search-path add -vservers vs1 -path
/home1

cluster::> vservers cifs home-directory search-path show
Vserver Position Path

vs1 1 /home1

```

#### 관련 정보

- [%u 변수를 사용하여 홈 디렉토리를 구성하십시오](#)
- [추가 홈 디렉토리 구성에 대해 알아보세요](#)
- [사용자 홈 디렉토리 경로에 대한 정보 표시](#)

#### %u 변수를 사용하여 ONTAP SMB 홈 디렉토리 구성

'%w' 변수를 사용하여 공유 이름을 지정하는 홈 디렉토리 구성을 만들 수 있지만 '%u' 변수를 사용하여 홈 디렉토리 공유의 상대 경로를 지정할 수 있습니다. 그런 다음 사용자는 홈 디렉토리의 실제 이름 또는 경로를 인식하지 않고 Windows 사용자 이름을 사용하여 생성된 동적 공유를 사용하여 홈 공유에 연결할 수 있습니다.

#### 단계



1. 사용자의 홈 디렉토리를 포함할 qtree를 생성합니다: 'volume qtree create-vserver vserver\_name-qtree-path qtree\_path'
2. qtree가 올바른 보안 유형인 'volume qtree show'를 사용하는지 확인합니다
3. Qtree에서 원하는 보안 스타일을 사용하지 않는 경우 'volume qtree security' 명령을 사용하여 보안 스타일을 변경하십시오.
4. 홈 디렉토리 공유 추가: "vserver cifs share create-vserver vserver-share-name%w-path%u-share-properties homed디렉토리,...]"

'-vserver'vserver'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

'-share-name '%w'는 홈 디렉토리 공유 이름을 지정합니다. 공유 이름은 각 사용자가 홈 디렉토리에 접속하고 *windows\_user\_name* 형식으로 작성될 때 동적으로 생성됩니다.



'-share-name' 옵션에도 '%u' 변수를 사용할 수 있습니다. 이렇게 하면 매핑된 UNIX 사용자 이름을 사용하는 상대 공유 경로가 생성됩니다.

'-path '%u'는 홈 디렉토리의 상대 경로를 지정합니다. 상대 경로는 각 사용자가 홈 디렉토리에 접속하고 *Mapped\_UNIX\_USER\_NAME* 형식으로 작성될 때 동적으로 생성됩니다.



이 옵션의 값에는 정적 요소도 포함될 수 있습니다. 예: 'ENG/%u'.

'-share-properties' + homed디렉토리 \[,...\]+'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다. 쉼표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

5. 'vserver cifs share show' 명령을 사용하여 공유에 원하는 구성이 있는지 확인합니다.
6. 홈 디렉토리 검색 경로 'vserver cifs home-directory search-path add-vserver vserver-path path path' 추가

'-vserver'vserver'는 검색 경로를 추가할 CIFS 지원 SVM을 지정합니다.

path는 검색경로에 대한 절대 디렉토리 경로를 지정합니다.

7. 'vserver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.
8. UNIX 사용자가 없으면 'vserver services UNIX -user create' 명령을 사용하여 UNIX 사용자를 생성합니다.



사용자를 매핑하기 전에 Windows 사용자 이름을 매핑할 UNIX 사용자 이름이 있어야 합니다.

9. "vserver name-mapping create -vserver vserver\_name -direction win -unix -priority integer -pattern windows\_user\_name -replacement unix\_user\_name" 명령을 사용하여 UNIX 사용자에 대한 Windows 사용자의 이름 매핑을 생성합니다



Windows 사용자를 UNIX 사용자에게 매핑하는 이름 매핑이 이미 있는 경우 매핑 단계를 수행할 필요가 없습니다.

Windows 사용자 이름이 해당 UNIX 사용자 이름으로 매핑됩니다. Windows 사용자가 홈 디렉토리 공유에 접속하면 디렉토리 이름이 UNIX 사용자 이름과 일치한다는 것을 인식하지 않고 동적으로 생성된 홈 디렉토리에 Windows 사용자 이름에 해당하는 공유 이름을 연결합니다.

10. 홈 디렉토리가 있는 사용자의 경우 홈 디렉토리를 포함하도록 지정된 qtree 또는 볼륨에 해당 디렉토리를 생성합니다.

예를 들어, 생성하려는 디렉토리가 "unixuser1"인 사용자의 매핑된 UNIX 사용자 이름과 함께 "/vol/vol1/users" 경로를 사용하여 qtree를 생성한 경우 "/vol/vol1/users/unixuser1" 경로를 사용하여 디렉토리를 생성할 수 있습니다.

/home1 에 마운트된 "home1" 볼륨을 생성한 경우 "/home1/unixuser1" 경로를 사용하여 디렉토리를 생성합니다.

11. 드라이브를 매핑하거나 UNC 경로를 사용하여 연결하여 사용자가 홈 공유에 성공적으로 연결할 수 있는지 확인합니다.

예를 들어, 사용자 mydomain\user1이 UNIX 사용자 unixuser1에 매핑되고 SVM VS1에 있는 10단계에서 생성한 디렉토리에 연결하려는 경우 user1은 UNC 경로 "\\VS1\user1"을 사용하여 연결됩니다.

예

다음 예제의 명령은 다음과 같은 설정으로 홈 디렉토리 구성을 만듭니다.

- 공유 이름은 %W입니다
- 상대 홈 디렉토리 경로는 %u입니다
- 홈 디렉토리 /home1 을 포함하는 데 사용되는 검색 경로는 UNIX 보안 스타일로 구성된 볼륨입니다.
- SVM VS1 에서 구성이 생성됩니다.

사용자가 Windows 호스트 또는 Windows 및 UNIX 호스트 모두에서 홈 디렉토리에 액세스할 때 이 유형의 홈 디렉토리 구성을 사용할 수 있으며 파일 시스템 관리자는 UNIX 기반 사용자 및 그룹을 사용하여 파일 시스템에 대한 액세스를 제어할 수 있습니다.

```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vsriver cifs share show -vsriver vs1 -share-name %u
```

```

 Vserver: vs1
 Share: %w
CIFS Server NetBIOS Name: VS1
 Path: %u
 Share Properties: oplocks
 browsable
 changenotify
 homedirectory
 Symlink Properties: enable
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
 Volume Name: -
 Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1
```

```
cluster::> vsriver cifs home-directory search-path show -vsriver vs1
```

| Vserver | Position | Path   |
|---------|----------|--------|
| -----   |          |        |
| vs1     | 1        | /home1 |

```
cluster::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vsriver name-mapping show -pattern user1
```

| Vserver | Direction | Position               |
|---------|-----------|------------------------|
| -----   |           |                        |
| vs1     | win-unix  | 5                      |
|         |           | Pattern: user1         |
|         |           | Replacement: unixuser1 |

#### 관련 정보

- [%w 및 %d 변수를 사용하여 홈 디렉토리 구성을 만듭니다.](#)
- [추가 홈 디렉토리 구성에 대해 알아보세요](#)
- [사용자 홈 디렉토리 경로에 대한 정보 표시](#)

추가 **ONTAP SMB** 홈 디렉토리 구성에 대해 알아보세요

"%w", "%d", "%u" 변수를 사용하여 홈 디렉토리 설정을 추가로 생성할 수 있습니다. 이 변수를 사용하여 필요에 맞게 홈 디렉토리 구성을 사용자 정의할 수 있습니다.

공유 이름과 검색 경로에서 변수와 정적 문자열을 조합하여 여러 홈 디렉토리 구성을 만들 수 있습니다. 다음 표에는 여러 가지 홈 디렉토리 구성을 만드는 방법을 보여 주는 몇 가지 예가 나와 있습니다.

| '/vol1/user'가 홈 디렉토리를 포함할 때 생성되는 경로...                                       | 공유 명령...                                                                                                        |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 사용자를 '/vol1/user/win_username'으로 안내하는 공유 경로 '\\vs1~win_username'을 만듭니다       | 'vserver cifs share create-share-name~%w-path%w-share-properties oplocks, browsable, changenotify, homedir'     |
| 사용자를 '/vol1/user/domain/win_username'으로 안내하는 공유 경로 '\\vs1win_username'을 만듭니다 | 'vserver cifs share create-share-name %w-path %d/%w-share-properties oplocks, browsable, changenotify, homedir' |
| 사용자를 '/vol1/user/unix_username'으로 안내하는 공유 경로 '\\vs1win_username'을 만듭니다       | 'vserver cifs share create-share-name %w-path %u-share-properties oplocks, browsable, changenotify, homedir'    |
| 사용자를 '/vol1/user/unix_username'으로 안내하는 공유 경로 '\\vs1unix_username'을 생성합니다     | 'vserver cifs share create-share-name %u-path %u-share-properties oplocks, browsable, changenotify, homedir'    |

#### SMB 검색 경로를 관리하기 위한 **ONTAP** 명령

SMB 홈 디렉토리 구성을 위한 검색 경로를 관리하기 위한 특정 **ONTAP** 명령이 있습니다. 예를 들어, 검색 경로에 대한 정보를 추가, 제거 및 표시하는 명령이 있습니다. 검색 경로 순서를 변경하는 명령도 있습니다.

| 원하는 작업          | 이 명령 사용...                                        |
|-----------------|---------------------------------------------------|
| 검색 경로를 추가합니다    | 'vserver cifs home-directory search-path add'     |
| 검색 경로를 표시합니다    | 'vserver cifs home-directory search-path show'    |
| 검색 경로 순서를 변경합니다 | 'vserver cifs home-directory search-path reorder' |
| 검색 경로를 제거합니다    | 'vserver cifs home-directory search-path remove'  |

에 대한 자세한 내용은 `vserver cifs home-directory search-path` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

#### **ONTAP SMB** 사용자 홈 디렉토리 경로에 대한 정보 표시

스토리지 가상 시스템(SVM)에 SMB 사용자의 홈 디렉토리 경로를 표시할 수 있습니다. SVM은

CIFS 홈 디렉토리 경로가 여러 개 구성되어 있고 사용자의 홈 디렉토리가 있는 경로를 확인하려는 경우에 사용할 수 있습니다.

#### 단계

1. 'vserver cifs home-directory show-user' 명령을 사용하여 홈 디렉토리 경로를 표시합니다.

'vserver cifs home-directory show-user-vserver vs1-username user1'

| Vserver | User  | Home Dir Path |
|---------|-------|---------------|
| -----   | ----- | -----         |
| vs1     | user1 | /home/user1   |

#### 관련 정보

[사용자 홈 디렉토리에 대한 접근성 관리](#)

#### ONTAP SMB 사용자 홈 디렉토리에 대한 접근성 관리

기본적으로 사용자의 홈 디렉토리는 해당 사용자만 액세스할 수 있습니다. 공유의 동적 이름 앞에 물결표(~)가 있는 공유의 경우 Windows 관리자 또는 다른 사용자(공용 액세스)가 사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제할 수 있습니다.

#### 시작하기 전에

SVM(스토리지 가상 머신)의 홈 디렉토리 공유는 앞에 물결표(~)가 오는 동적 공유 이름으로 구성해야 합니다. 다음 사례는 공유 명명 요구 사항을 보여 줍니다.

| 홈 디렉토리 공유 이름입니다 | 공유에 연결하는 명령의 예                                                              |
|-----------------|-----------------------------------------------------------------------------|
| ~ %d~ %w        | 'net use * {백슬래시} {백슬래시}IPaddress{백슬래시} ~domain~user/u:credentials'을 사용하십시오 |
| ~ %w            | 'net use * {백슬래시} {백슬래시}IPaddress{백슬래시} ~user/u:credentials'를 사용하십시오        |
| ~abc~ %w        | 'net use * {백슬래시} {백슬래시}IPaddress{백슬래시}abc~user/u:credentials'를 사용하십시오      |

#### 단계

1. 적절한 작업을 수행합니다.

|                                     |                                                                                                                               |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제하려면... | 다음을 입력하십시오.                                                                                                                   |
| Windows 관리자                         | 'vserver cifs home-directory modify -vserver_vserver_name_-is-home-dirs-access-for-admin-enabled{true false}' 기본값은 'true'입니다. |

|                                     |                                                                                                                                                                             |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제하려면... | 다음을 입력하십시오.                                                                                                                                                                 |
| 모든 사용자(공용 액세스)                      | a. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다<br>b. 액세스 설정 또는 해제:'vserver cifs home-directory modify -vserver_vserver_name_-is-home-dirs-access-for-public-enabled{true |

다음 예에서는 사용자의 홈 디렉토리에 대한 공용 액세스를 활성화합니다. + 'Set-Privilege advanced' + 'vserver cifs home-directory modify -vserver vs1-is-home-dirs-access-for-public-enabled true' + 'Set-Privilege admin'

관련 정보

[사용자 홈 디렉토리 경로에 대한 정보 표시](#)

**UNIX** 심볼 링크에 대한 **SMB** 클라이언트 액세스를 구성합니다

**ONTAP SMB** 클라이언트가 **UNIX** 심볼릭 링크에 액세스할 수 있도록 하는 방법에 대해 알아보세요.

심볼 링크는 다른 파일 또는 디렉토리에 대한 참조가 포함된 UNIX 환경에서 생성되는 파일입니다. 클라이언트가 심볼 링크에 액세스하는 경우 클라이언트는 심볼 링크가 참조하는 타겟 파일 또는 디렉토리로 리디렉션됩니다. ONTAP는 Wwidelink(로컬 파일 시스템 외부의 타겟을 포함한 절대 링크)를 포함하여 상대 및 절대 심볼 링크를 지원합니다.

ONTAP는 SMB 클라이언트가 SVM에 구성된 UNIX 심볼 링크를 따라갈 수 있도록 지원합니다. 이 기능은 선택 사항이며 다음 설정 중 하나로 'vserver cifs share create' 명령의 '-symlink-properties' 옵션을 사용하여 공유별로 구성할 수 있습니다.

- 읽기/쓰기 권한으로 설정됩니다
- 읽기 전용 액세스를 사용하도록 설정되었습니다
- SMB 클라이언트에서 심볼 링크를 숨겨 사용할 수 없습니다
- SMB 클라이언트의 심볼 링크에 대한 액세스 없이 비활성화됩니다

공유에 대한 심볼 링크를 설정하면 추가 구성 없이 상대 심볼 링크가 작동합니다.

공유에 대한 심볼 링크를 설정하면 절대 심볼 링크가 즉시 작동하지 않습니다. 먼저 대상 SMB 경로에 대한 심볼 링크의 UNIX 경로 간에 매핑을 생성해야 합니다. 절대 심볼 링크 매핑을 생성할 때 로컬 링크인지 또는 \_wwidelink\_ 인지를 지정할 수 있습니다. widelink는 다른 스토리지 디바이스의 파일 시스템에 대한 링크이거나 동일한 ONTAP 시스템에서 별도의 SVM에 호스팅된 파일 시스템에 대한 링크일 수 있습니다. widelink를 만들 때는 클라이언트가 따라야 하는 정보를 포함해야 합니다. 즉, 클라이언트가 디렉터리 연결 지점을 검색할 재분석 지점을 만들어야 합니다. 로컬 공유 외부에 있는 파일 또는 디렉토리에 대한 절대 심볼 링크를 생성하지만 인접성을 로컬로 설정하면 ONTAP는 타겟에 대한 액세스를 허용하지 않습니다.



클라이언트가 로컬 심볼 링크(절대 또는 상대 링크)를 삭제하려고 하면 타겟 파일이나 디렉토리가 아닌 심볼 링크만 삭제됩니다. 그러나 클라이언트가 widelink를 삭제하려고 하면 wwidelink가 참조하는 실제 타겟 파일이나 디렉토리가 삭제될 수 있습니다. 클라이언트가 SVM 외부에서 타겟 파일 또는 디렉토리를 명시적으로 열고 삭제할 수 있기 때문에 ONTAP에서는 이 기능을 제어할 수 없습니다.

• \* 재분석 지점 및 ONTAP 파일 시스템 서비스 \*

reparse point\_는 파일과 함께 볼륨에 선택적으로 저장할 수 있는 NTFS 파일 시스템 객체입니다. 재분석 지점은 SMB 클라이언트가 NTFS 스타일 볼륨으로 작업할 때 향상된 파일 시스템 서비스 또는 확장된 파일 시스템 서비스를 받을 수 있는 기능을 제공합니다. 재분석 지점은 재분석 지점의 유형을 식별하는 표준 태그 및 클라이언트가 추가 처리를 위해 SMB 클라이언트에서 검색할 수 있는 재분석 지점의 콘텐츠로 구성됩니다. 확장된 파일 시스템 기능에 사용할 수 있는 개체 유형 중 ONTAP는 재분석 포인트 태그를 사용하여 NTFS 심볼 링크 및 디렉터리 연결 지점에 대한 지원을 구현합니다. 재분석 지점의 내용을 이해할 수 없는 SMB 클라이언트는 단순히 무시하며 재분석 지점에서 활성화할 수 있는 확장 파일 시스템 서비스를 제공하지 않습니다.

• \* 심볼 링크에 대한 디렉터리 교차점 및 ONTAP 지원 \*

디렉터리 교차점은 파일이 저장된 대체 위치를 다른 경로(심볼 링크) 또는 별도의 스토리지 디바이스(widelinks)에 참조할 수 있는 파일 시스템 디렉터리 구조 내의 위치입니다. ONTAP SMB 서버는 디렉터리 연결 지점을 재분석 지점으로 Windows 클라이언트에 노출하므로, 디렉터리 연결 지점을 이동할 때 사용 가능한 클라이언트가 ONTAP에서 재분석 지점 내용을 가져올 수 있습니다. 따라서 동일한 파일 시스템에 포함된 것처럼 다른 경로 또는 스토리지 디바이스를 탐색하고 연결할 수 있습니다.

• \* 재분석 포인트 옵션을 사용하여 widelink 지원 활성화 \*

이 `-is-use-junctions-as-reparse-points-enabled` 옵션은 ONTAP 9에서 기본적으로 활성화되어 있습니다. 모든 SMB 클라이언트가 와이드링크를 지원하지는 않으므로, 정보 활성화 옵션은 프로토콜 버전별로 구성 가능합니다. 이를 통해 관리자는 지원되는 SMB 클라이언트와 지원되지 않는 SMB 클라이언트를 모두 지원할 수 있습니다. 이 옵션을 활성화해야 합니다. `-widelink-as-reparse-point-versions` 와이드링크를 사용하여 공유에 액세스하는 각 클라이언트 프로토콜의 경우 기본값은 SMB1입니다.

관련 정보

- ["Windows 백업 애플리케이션 및 Unix 스타일 symlink"](#)
- ["Microsoft 설명서: 지점 재분석"](#)

ONTAP SMB 액세스를 위한 UNIX 심볼릭 링크 구성 시 제한 사항

SMB 액세스를 위해 UNIX 심볼 링크를 구성할 때 특정 제한 사항을 알고 있어야 합니다.

| 제한 | 설명                                                                                                                                                                                                                              |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 45 | <p>CIFS 서버 이름에 FQDN을 사용할 때 지정할 수 있는 CIFS 서버 이름의 최대 길이입니다.</p> <div>  <p>또는 CIFS 서버 이름을 NetBIOS 이름으로 지정할 수 있습니다. 이 이름은 15자로 제한됩니다.</p> </div> |
| 80 | 공유 이름의 최대 길이입니다.                                                                                                                                                                                                                |

| 제한  | 설명                                                                                                                                            |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 256 | 심볼 링크를 생성할 때 또는 기존 심볼 링크의 UNIX 경로를 수정할 때 지정할 수 있는 UNIX 경로의 최대 길이입니다. UNIX 경로는 "/"(슬래시)로 시작하고 "/"로 끝나야 합니다. 시작 및 끝 슬래시는 모두 256자 제한의 일부로 계산됩니다. |
| 256 | 심볼 링크를 생성하거나 기존 심볼 링크의 CIFS 경로를 수정할 때 지정할 수 있는 CIFS 경로의 최대 길이입니다. CIFS 경로는 "/"(슬래시)로 시작하고 "/"로 끝나야 합니다. 시작 및 끝 슬래시는 모두 256자 제한의 일부로 계산됩니다.    |

## 관련 정보

### 공유에 대한 심볼릭 링크 매핑 만들기

#### ONTAP SMB 서버에서 자동 DFS 광고 제어

CIFS 서버 옵션은 공유에 연결할 때 SMB 클라이언트에 DFS 기능을 알리는 방법을 제어합니다. ONTAP는 클라이언트가 SMB를 통해 심볼 링크에 액세스할 때 DFS 조회를 사용하므로 이 옵션을 비활성화하거나 활성화할 때 어떤 영향이 있는지 알고 있어야 합니다.

CIFS 서버 옵션은 CIFS 서버가 SMB 클라이언트에 DFS를 사용할 수 있음을 자동으로 알리는지 여부를 결정합니다. 기본적으로 이 옵션은 설정되어 있으며 CIFS 서버는 심볼 링크에 대한 액세스가 비활성화된 공유에 연결할 때도 SMB 클라이언트에 DFS를 사용할 수 있다고 항상 알립니다. CIFS 서버가 심볼 링크에 대한 액세스가 설정된 공유에 연결할 때만 DFS를 클라이언트에 제공할 수 있음을 알려려면 이 옵션을 사용하지 않도록 설정할 수 있습니다.

이 옵션을 비활성화하면 어떻게 되는지 알고 있어야 합니다.

- 심볼 링크에 대한 공유 구성은 변경되지 않습니다.
- 공유 매개 변수가 심볼 링크 액세스를 허용하도록 설정된 경우(읽기-쓰기 액세스 또는 읽기 전용 액세스) CIFS 서버는 해당 공유에 접속하는 클라이언트에 DFS 기능을 알립니다.

클라이언트 연결 및 심볼 링크에 대한 액세스는 중단 없이 계속됩니다.

- 공유 매개 변수가 액세스를 비활성화하거나 공유 매개 변수의 값이 null인 경우 심볼 링크 액세스를 허용하지 않도록 설정된 경우 CIFS 서버는 해당 공유에 접속하는 클라이언트에 DFS 기능을 알리지 않습니다.

클라이언트는 CIFS 서버가 DFS를 사용할 수 있고 더 이상 DFS를 광고하지 않기 때문에 심볼 링크 액세스가 비활성화된 공유에 접속된 클라이언트는 CIFS 서버 옵션을 비활성화한 후 이러한 공유에 액세스하지 못할 수 있습니다. 이 옵션을 사용하지 않도록 설정한 후 이러한 공유에 연결된 클라이언트를 재부팅해야 캐시된 정보가 지워질 수 있습니다.

이러한 변경 사항은 SMB 1.0 연결에는 적용되지 않습니다.

#### ONTAP SMB 공유에서 UNIX 심볼릭 링크 지원 구성

SMB 공유를 생성할 때 또는 언제든지 기존 SMB 공유를 수정하여 심볼 링크 공유 속성 설정을



지정하여 SMB 공유에 대한 UNIX 심볼 링크 지원을 구성할 수 있습니다. UNIX 심볼 링크 지원은 기본적으로 활성화되어 있습니다. 공유에서 UNIX 심볼 링크 지원을 해제할 수도 있습니다.

이 작업에 대해

SMB 공유에 대한 UNIX 심볼 링크 지원을 구성할 때 다음 설정 중 하나를 선택할 수 있습니다.

| 설정                    | 설명                                                                                                                                          |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 'enable'(사용되지 않음 *)   | 심볼 링크가 읽기-쓰기 액세스를 사용하도록 설정되도록 지정합니다.                                                                                                        |
| READ_ONLY'(사용되지 않음 *) | 읽기 전용 액세스를 위해 symlink를 사용하도록 지정합니다. 이 설정은 Wodelink에는 적용되지 않습니다. Widelink 액세스는 항상 읽기-쓰기입니다.                                                  |
| 'hide'(사용되지 않음 *)     | SMB 클라이언트가 symlink를 볼 수 없도록 지정합니다.                                                                                                          |
| 엄정한 보안 없음             | 클라이언트가 공유 경계 외부의 symlink를 따르도록 지정합니다.                                                                                                       |
| '체조'입니다               | symlink가 읽기-쓰기 액세스를 위해 로컬로 설정되도록 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 true로 설정되어 있어도 DFS 광고는 생성되지 않습니다. 기본 설정입니다.                       |
| '체임링크', '와이델링크'       | 읽기-쓰기 액세스를 위해 로컬 symlink와 wizenlink를 모두 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 false로 설정되어 있어도 로컬 symlink와 Wipelink 모두에 대해 DFS 광고가 생성됩니다. |
| "할 수 없습니다             | symlinks 및 wizenlinks를 사용하지 않도록 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 true로 설정되어 있어도 DFS 광고는 생성되지 않습니다.                                  |
| ""(null, 설정되지 않음)     | 공유의 심볼 링크를 해제합니다.                                                                                                                           |
| '-'(설정되지 않음)          | 공유의 심볼 링크를 해제합니다.                                                                                                                           |



• enable\_, hide 및 \_read-only\_parameters는 더 이상 사용되지 않으며 ONTAP의 향후 릴리스에서 제거될 수 있습니다.

단계

1. 심볼 링크 지원을 구성하거나 사용하지 않도록 설정:

| 만약...                                                                                                | 입력...                                                                                                 |
|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 새로운 SMB 공유                                                                                           | '+vserver cifs share create-vserver vserver_name-share-name share-path-path-symlink-properties{enable |
| hide                                                                                                 | read-only                                                                                             |
| ""                                                                                                   | -                                                                                                     |
| symlinks                                                                                             | symlinks-and-wdelink                                                                                  |
| disable},...]+'                                                                                      | 기존 SMB 공유입니다                                                                                          |
| '+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink -properties{enable | hide                                                                                                  |
| read-only                                                                                            | "                                                                                                     |
| -                                                                                                    | symlinks                                                                                              |
| symlinks-and-wifelink                                                                                | disable},...]+'                                                                                       |

2. SMB 공유 구성이 올바른지 확인합니다. 'vserver cifs share show -vserver vserver\_name -share-name share\_name -instance'

예

다음 명령을 실행하면 UNIX 심볼 링크 구성이 "enable"로 설정된 "data1"이라는 SMB 공유가 생성됩니다.

```
cluster1::> vservers cifs share create -vservers vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vservers cifs share show -vservers vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

## 관련 정보

### 공유에 대한 심볼릭 링크 매핑 만들기

#### ONTAP SMB 공유에 대한 심볼릭 링크 매핑 만들기

SMB 공유에 대한 UNIX 심볼 링크 매핑을 생성할 수 있습니다. 상위 폴더에 상대적인 파일이나 폴더를 참조하는 상대 심볼 링크를 만들거나 절대 경로를 사용하여 파일 또는 폴더를 참조하는 절대 심볼 링크를 만들 수 있습니다.

#### 이 작업에 대해

SMB 2.x를 사용하는 경우 Mac OS X 클라이언트에서 Widelink에 액세스할 수 없습니다. 사용자가 Mac OS X 클라이언트의 widelink를 사용하여 공유에 연결하려고 하면 시도가 실패합니다. 그러나 SMB 1을 사용하는 경우 Mac OS X 클라이언트에서 Wistelink를 사용할 수 있습니다.

#### 단계

1. SMB 공유에 대한 심볼 링크 매핑을 생성하려면 다음을 수행합니다. "vservers cifs symlink create -vservers virtual\_server\_name -unix-path path path path -share-name share\_name -cifs-path path path path[-cifs-server server\_name][-locality{local|free|widelink}][-home-directory{true|false}]"

'-vservers'virtual\_server\_name'은 SVM(Storage Virtual Machine) 이름을 지정합니다.

'-unix-path' path는 UNIX 경로를 지정합니다. UNIX 경로는 슬래시("/")로 시작해야 하며 슬래시("/")로 끝나야 합니다.

'-share-name' share\_name'은 매핑할 SMB 공유의 이름을 지정합니다.

'-cifs-path' path는 CIFS 경로를 지정합니다. CIFS 경로는 슬래시("/")로 시작해야 하며 슬래시("/")로 끝나야 합니다.

'-cifs-server "server\_name'은 CIFS 서버 이름을 지정합니다. CIFS 서버 이름은 DNS 이름(예: mynetwork.cifs.server.com), IP 주소 또는 NetBIOS 이름으로 지정할 수 있습니다. NetBIOS 이름은 'vserver cifs show' 명령을 사용하여 확인할 수 있습니다. 이 선택적 매개 변수를 지정하지 않으면 로컬 CIFS 서버의 NetBIOS 이름이 기본값이 됩니다.

'-지역성'{'local'|'free'|'widelink'}은 로컬 링크, 무료 링크 또는 넓은 심볼 링크 생성 여부를 지정합니다. 로컬 심볼 링크는 로컬 SMB 공유에 매핑됩니다. 무료 심볼 링크는 로컬 SMB 서버의 어느 위치에나 매핑할 수 있습니다. 넓은 심볼 링크는 네트워크의 모든 SMB 공유에 매핑됩니다. 이 선택적 매개 변수를 지정하지 않으면 기본값은 "local"입니다.

'-home-directory'{'true'|'false'}는 타겟 공유가 홈 디렉토리인지 여부를 지정합니다. 이 매개 변수는 선택 사항이지만 타겟 공유가 홈 디렉토리로 구성될 때 이 매개 변수를 "true"로 설정해야 합니다. 기본값은 false 입니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 심볼 링크 매핑이 생성됩니다. UNIX 경로인 /src/, SMB 공유 이름 "소스", CIFS 경로, /mycompany/source/", CIFS 서버 IP 주소 123.123.123.123 등이 있으며, 이는 wizenlink입니다.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

관련 정보

[공유에서 UNIX 심볼릭 링크 지원 구성](#)

**SMB 심볼릭 링크 매핑을 관리하기 위한 ONTAP 명령**

심볼 링크 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

| 원하는 작업                 | 이 명령 사용...                    |
|------------------------|-------------------------------|
| 심볼 링크 매핑을 생성합니다        | 'vserver cifs symlink create  |
| 심볼 링크 매핑에 대한 정보를 표시합니다 | 'vserver cifs symlink show'   |
| 심볼 링크 매핑을 수정합니다        | 'vserver cifs symlink modify' |
| 심볼 링크 매핑을 삭제합니다        | 'vserver cifs symlink delete  |

에 대한 자세한 내용은 vserver cifs symlink ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

Windows에서 실행 중인 백업 응용 프로그램이 Unix 스타일의 심볼 링크(symmlink)를 발견하면 링크가 팔로우되고 데이터가 백업됩니다. ONTAP 9.15.1부터 데이터 대신 symlink를 백업할 수 있습니다. 이 기능은 ONTAP FlexGroup 볼륨과 FlexVols에서 완벽하게 지원됩니다.

## 개요

Windows 백업 작업 중에 ONTAP가 symlink를 처리하는 방식을 변경하기 전에 이점, 주요 개념 및 구성 옵션을 숙지해야 합니다.

## 이점

이 기능을 비활성화하거나 사용할 수 없는 경우 각 symlink가 통과하고 링크되는 데이터가 백업됩니다. 이로 인해 불필요한 데이터가 백업될 수 있으며 특정 상황에서는 응용 프로그램이 루프로 끝날 수 있습니다. 대신 symlink를 백업하면 이러한 문제가 발생하지 않습니다. 또한 대부분의 경우 symlink 파일은 데이터에 비해 매우 작기 때문에 백업을 완료하는 데 걸리는 시간이 줄어듭니다. IO 작업이 감소하여 클러스터의 전반적인 성능도 향상됩니다.

## Windows 서버 환경

이 기능은 Windows에서 실행되는 백업 응용 프로그램에 대해 지원됩니다. 환경을 사용하기 전에 환경의 기술적 측면을 이해해야 합니다.

## 확장 속성

Windows는 파일과 선택적으로 연결되는 추가 메타데이터를 집합적으로 형성하는 EA(확장 특성)를 지원합니다. 이러한 속성은 에 설명된 대로 Linux용 Windows 하위 시스템과 같은 다양한 응용 프로그램에서 ["WSL에 대한 파일 권한"](#) 사용됩니다. 응용 프로그램은 ONTAP에서 데이터를 읽을 때 각 파일에 대해 확장 속성을 요청할 수 있습니다.

이 기능이 설정되면 symlink가 확장 속성에서 반환됩니다. 따라서 백업 애플리케이션은 메타데이터를 저장하는 데 사용되는 표준 EA 지원을 제공해야 합니다. 일부 Windows 유틸리티는 확장 속성을 지원하고 유지합니다. 그러나 백업 소프트웨어가 확장 속성의 백업 및 복구를 지원하지 않는 경우 각 파일과 연결된 메타데이터가 보존되지 않으며 symlink를 제대로 처리하지 못합니다.

## Windows 구성

Microsoft Windows 서버에서 실행되는 백업 응용 프로그램에는 일반 파일 보안을 우회할 수 있는 특별한 권한이 부여될 수 있습니다. 이 작업은 일반적으로 Backup Operators 그룹에 응용 프로그램을 추가하여 수행합니다. 그런 다음 앱은 필요에 따라 파일을 백업 및 복원할 수 있을 뿐만 아니라 다른 관련 시스템 작업을 수행할 수 있습니다. 백업 애플리케이션에서 사용하는 SMB 프로토콜은 ONTAP에서 데이터를 읽고 쓸 때 감지할 수 있는 것처럼 약간만 변경되었습니다.

## 요구 사항

symlink 백업 기능에는 다음과 같은 몇 가지 요구 사항이 있습니다.

- 클러스터에서 ONTAP 9.15.1 이상이 실행되고 있습니다.
- 특수 백업 권한이 부여된 Windows 백업 응용 프로그램입니다.
- 또한 백업 애플리케이션은 확장 속성을 지원하고 백업 작업 중에 이를 요청해야 합니다.
- ONTAP symlink 백업 기능은 해당 데이터 SVM에 대해 활성화됩니다.

## 구성 옵션

ONTAP CLI 외에도 REST API를 사용하여 이 기능을 관리할 수 있습니다. 자세한 내용은 ["ONTAP REST API 및 자동화의 새로운 기능"](#) 참조하십시오. ONTAP가 Unix 스타일 심링크를 처리하는 방식을 결정하는 구성은 SVM별로 별도로 수행해야 합니다.

### ONTAP에서 symlink 백업 기능을 활성화합니다

ONTAP 9.15.1을 사용하는 기존 CLI 명령에 구성 옵션이 도입되었습니다. 이 옵션을 사용하여 Unix 스타일의 symlink 처리를 활성화하거나 비활성화할 수 있습니다.

시작하기 전에

기본을 [요구 사항](#) 검토합니다. 추가 사항:

- CLI 권한을 고급 수준으로 높일 수 있습니다.
- 수정할 데이터 SVM을 결정합니다. SVM `vs1` 은 예 명령에 사용됩니다.

단계

1. advanced 권한 수준을 설정합니다.

```
set privilege advanced
```

2. symlink 파일 백업을 활성화합니다.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

### BranchCache를 사용하여 지사에 SMB 공유 콘텐츠를 캐싱합니다

지점 사무실에서 **ONTAP SMB** 공유 콘텐츠를 캐싱하기 위해 **BranchCache**를 사용하는 방법에 대해 알아보세요.

BranchCache는 요청 클라이언트에 대한 로컬 컴퓨터의 콘텐츠를 캐싱할 수 있도록 Microsoft에서 개발했습니다. ONTAP의 BranchCache를 구현하면 WAN(Wide Area Network) 사용률을 줄이고, 지사의 사용자가 SMB를 사용하여 SVM(Storage Virtual Machine)에 저장된 콘텐츠에 액세스할 때 액세스 응답 시간을 향상시킬 수 있습니다.

BranchCache를 구성하는 경우 Windows BranchCache 클라이언트는 먼저 SVM에서 콘텐츠를 검색한 다음 지사 내의 컴퓨터에 콘텐츠를 캐시합니다. 지사의 다른 BranchCache 지원 클라이언트가 동일한 콘텐츠를 요청하는 경우 SVM은 먼저 요청된 사용자를 인증하고 권한을 부여합니다. 그런 다음, SVM이 캐시된 콘텐츠가 아직 최신 상태인지 확인하고 최신 상태인 경우 캐시된 콘텐츠에 대한 클라이언트 메타데이터를 보냅니다. 그런 다음 클라이언트는 메타데이터를 사용하여 로컬 기반 캐시에서 콘텐츠를 직접 검색합니다.

관련 정보

[오프라인 사용을 위해 파일을 캐싱하는 오프라인 파일 사용에 대해 알아보세요.](#)

## ONTAP SMB BranchCache 버전 지원에 대해 알아보세요

ONTAP가 지원하는 BranchCache 버전은 무엇인지 알고 있어야 합니다.

ONTAP는 BranchCache 1 및 향상된 BranchCache 2 를 지원합니다.

- SVM(스토리지 가상 시스템)에 대해 SMB 서버의 BranchCache를 구성할 때 BranchCache 1, BranchCache 2 또는 모든 버전을 사용하도록 설정할 수 있습니다.

기본적으로 모든 버전이 활성화됩니다.

- BranchCache 2만 사용하도록 설정한 경우 원격 사무소 Windows 클라이언트 시스템은 BranchCache 2를 지원해야 합니다.

SMB 3.0 이상 클라이언트만 BranchCache 2를 지원합니다.

BranchCache 버전에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

## ONTAP SMB 네트워크 프로토콜 지원 요구 사항에 대해 알아보세요.

ONTAP BranchCache를 구축하기 위한 네트워크 프로토콜 요구 사항을 알고 있어야 합니다.

SMB 2.1 이상을 사용하여 IPv4 및 IPv6 네트워크에서 ONTAP BranchCache 기능을 구현할 수 있습니다.

BranchCache 구축에 사용되는 모든 CIFS 서버 및 지사 시스템에는 SMB 2.1 이상 프로토콜이 설정되어 있어야 합니다. SMB 2.1에는 클라이언트가 BranchCache 환경에 참여할 수 있도록 하는 프로토콜 확장이 있습니다. BranchCache 지원을 제공하는 최소 SMB 프로토콜 버전입니다. SMB 2.1은 BranchCache 버전 1을 지원합니다.

BranchCache 버전 2를 사용하려면 SMB 3.0이 지원되는 최소 버전입니다. BranchCache 2 구축에 사용되는 모든 CIFS 서버 및 지사 시스템에는 SMB 3.0 이상이 활성화되어 있어야 합니다.

일부 클라이언트가 SMB 2.1만 지원하고 일부 클라이언트가 SMB 3.0을 지원하는 원격 사무소가 있는 경우 CIFS 서버에 BranchCache 1과 BranchCache 2를 모두 지원하는 BranchCache 구성을 구현할 수 있습니다.



Microsoft BranchCache 기능은 HTTP/HTTPS 및 SMB 프로토콜을 파일 액세스 프로토콜로 사용하는 것을 지원하지만 ONTAP BranchCache는 SMB의 사용만 지원합니다.

## ONTAP SMB 및 Windows 호스트 버전 요구 사항에 대해 알아보세요.

BranchCache를 구성하려면 ONTAP 및 지점 Windows 호스트가 특정 버전 요구 사항을 충족해야 합니다.

BranchCache를 구성하기 전에 클러스터 및 참여하는 지사 클라이언트의 ONTAP 버전이 SMB 2.1 이상을 지원하고 BranchCache 기능을 지원해야 합니다. Hosted Cache 모드를 구성하는 경우 캐시 서버에 지원되는 호스트를 사용해야 합니다.

BranchCache 1은 다음 ONTAP 버전 및 Windows 호스트에서 지원됩니다.

- 콘텐츠 서버: ONTAP 기반의 SVM(스토리지 가상 시스템)
- 캐시 서버: Windows Server 2008 R2 또는 Windows Server 2012 이상
- 피어 또는 클라이언트: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 또는 Windows Server 2012 이상

BranchCache 2는 다음 ONTAP 버전 및 Windows 호스트에서 지원됩니다.

- 콘텐츠 서버: ONTAP 기반의 SVM
- 캐시 서버: Windows Server 2012 이상
- 피어 또는 클라이언트: Windows 8 또는 Windows Server 2012 이상

**ONTAP SMB가 BranchCache 해시를 무효화하는 이유에 대해 알아보세요.**

BranchCache 구성을 계획할 때 ONTAP에서 해시를 무효화하는 이유를 이해하는 것이 도움이 될 수 있습니다. 구성할 운영 모드를 결정하는 데 도움이 되며 BranchCache를 활성화할 공유를 선택하는 데 도움이 될 수 있습니다.

ONTAP는 해시가 유효한지 확인하기 위해 BranchCache 해시를 관리해야 합니다. 해시가 유효하지 않은 경우 ONTAP는 해시를 무효화하고 다음에 해당 콘텐츠가 요청될 때 BranchCache가 여전히 활성화되어 있다고 가정하고 새 해시를 계산합니다.

ONTAP는 다음과 같은 이유로 해시를 무효화합니다.

- 서버 키가 수정되었습니다.

서버 키가 수정되면 ONTAP는 해시 저장소의 모든 해시를 무효화합니다.

- BranchCache 해시 저장소의 최대 크기에 도달했기 때문에 캐시에서 해시가 플러시됩니다.

이 매개 변수는 조정 가능하며 비즈니스 요구 사항에 맞게 수정할 수 있습니다.

- 파일은 SMB 또는 NFS 액세스를 통해 수정됩니다.
- 해시가 계산된 파일은 'Snap restore' 명령어를 이용하여 복구한다.
- BranchCache를 사용하는 SMB 공유가 포함된 볼륨은 'Snap restore' 명령을 사용하여 복구됩니다.

**ONTAP SMB 해시 저장소 위치 선택에 대해 알아보세요**

BranchCache를 구성할 때는 해시를 저장할 위치와 해시 저장소의 크기를 선택합니다. 해시 저장소 위치 및 크기를 선택할 때 지침을 이해하면 CIFS 지원 SVM에서 BranchCache 구성을 계획하는 데 도움이 됩니다.

- atime 업데이트가 허용되는 볼륨에서 해시 저장소를 찾아야 합니다.

해시 파일의 액세스 시간은 자주 액세스하는 파일을 해시 저장소에 유지하는 데 사용됩니다. atime 업데이트가 비활성화된 경우 생성 시간이 이 용도로 사용됩니다. 자주 사용하는 파일을 추적하기 위해 atime을 사용하는 것이 좋습니다.



- SnapMirror 대상 및 SnapLock 볼륨과 같은 읽기 전용 파일 시스템에서는 해시를 저장할 수 없습니다.
- 해시 저장소의 최대 크기에 도달하면 새 해시를 위한 공간을 확보하기 위해 이전 해시가 플러시됩니다.

해시 저장소의 최대 크기를 늘려 캐시에서 플러시되는 해시의 양을 줄일 수 있습니다.

- 해시를 저장하는 볼륨을 사용할 수 없거나 꼭 찾거나 BranchCache 서비스에서 해시 정보를 검색할 수 없는 클러스터 내 통신에 문제가 있는 경우 BranchCache 서비스를 사용할 수 없습니다.

볼륨이 오프라인 상태이거나 스토리지 관리자가 해시 저장소에 대한 새 위치를 지정했기 때문에 볼륨을 사용할 수 없습니다.

이 경우 파일 액세스에 문제가 발생하지 않습니다. 해시 저장소에 대한 액세스가 방해받으면 ONTAP는 클라이언트에 Microsoft 정의 오류를 반환하여 클라이언트가 일반 SMB 읽기 요청을 사용하여 파일을 요청하게 합니다.

#### 관련 정보

- 서버에서 [BranchCache 구성](#)
- 공유에서 [BranchCache 구성 수정](#)

#### ONTAP SMB BranchCache 권장 사항에 대해 알아보세요

BranchCache를 구성하기 전에 BranchCache 캐싱을 활성화할 SMB 공유를 결정할 때 유의해야 할 몇 가지 권장 사항이 있습니다.

사용할 운영 모드와 BranchCache를 활성화할 SMB 공유를 결정할 때 다음 권장 사항을 염두에 두어야 합니다.

- BranchCache의 이점은 원격으로 캐시되는 데이터의 변경 사항이 자주 변경되는 경우 감소합니다.
- BranchCache 서비스는 여러 원격 사무소 클라이언트에서 다시 사용하거나 단일 원격 사용자가 반복적으로 액세스하는 파일 콘텐츠에 의해 다시 사용되는 파일 콘텐츠를 포함하는 공유에 유용합니다.
- 스냅샷 및 SnapMirror 대상의 데이터와 같은 읽기 전용 콘텐츠에 대해 캐싱을 사용하도록 설정하는 것이 좋습니다.

#### BranchCache를 구성합니다

#### ONTAP SMB BranchCache 구성에 대해 알아보세요

ONTAP 명령을 사용하여 SMB 서버에서 BranchCache를 구성합니다. BranchCache를 구현하려면 클라이언트도 구성해야 하며, 콘텐츠를 캐시하려는 지사의 호스팅된 캐시 서버도 선택적으로 구성해야 합니다.

공유 단위로 캐싱을 사용하도록 BranchCache를 구성하는 경우 BranchCache 캐싱 서비스를 제공할 SMB 공유에서 BranchCache를 사용하도록 설정해야 합니다.

#### ONTAP SMB BranchCache 구성을 위한 요구 사항

몇 가지 필수 구성 요소를 충족한 후 BranchCache를 설정할 수 있습니다.

SVM용 CIFS 서버에서 BranchCache를 구성하기 전에 다음 요구 사항이 충족되어야 합니다.

- ONTAP은 클러스터의 모든 노드에 설치해야 합니다.
- CIFS에 대한 라이선스가 있어야 하며 SMB 서버를 구성해야 합니다. SMB 라이선스는 에 포함되어 ["ONTAP 1 을 참조하십시오"](#) 있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.
- IPv4 또는 IPv6 네트워크 연결을 구성해야 합니다.
- BranchCache 1의 경우 SMB 2.1 이상이 활성화되어 있어야 합니다.
- BranchCache 2의 경우 SMB 3.0을 사용하도록 설정해야 하며 원격 Windows 클라이언트가 BranchCache 2를 지원해야 합니다.

## ONTAP SMB 서버에서 BranchCache 구성

BranchCache를 구성하여 공유별로 BranchCache 서비스를 제공할 수 있습니다. 또는 BranchCache를 구성하여 모든 SMB 공유에서 캐싱을 자동으로 설정할 수 있습니다.

이 작업에 대해

SVM에서 BranchCache를 구성할 수 있습니다.

- CIFS 서버의 모든 SMB 공유 내에 포함된 모든 콘텐츠에 대해 캐싱 서비스를 제공하려는 경우 모든 공유 BranchCache 구성을 생성할 수 있습니다.
- CIFS 서버에서 선택한 SMB 공유 내에 포함된 콘텐츠에 대해 캐싱 서비스를 제공하려는 경우 공유당 BranchCache 구성을 생성할 수 있습니다.

BranchCache를 구성할 때는 다음 매개 변수를 지정해야 합니다.

| 필수 매개변수         | 설명                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| _SVM 이름 _       | BranchCache는 SVM별로 구성됩니다. BranchCache 서비스를 구성할 CIFS 지원 SVM을 지정해야 합니다.                                                                                                                                                                                                                                                                                              |
| 해시 스토어에 대한 경로 _ | <p>BranchCache 해시는 SVM 볼륨의 일반 파일에 저장됩니다. ONTAP에서 해시 데이터를 저장할 기존 디렉터리의 경로를 지정해야 합니다. BranchCache 해시 경로는 읽기/쓰기가 가능해야 합니다. 스냅샷 디렉토리나 같은 읽기 전용 경로는 허용되지 않습니다. 해시 데이터는 다른 데이터가 포함된 볼륨에 저장하거나 해시 데이터를 저장하기 위한 별도의 볼륨을 생성할 수 있습니다.</p> <p>SVM이 SVM 재해 복구 소스인 경우 해시 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨이 재해 복구 대상에 복제되지 않기 때문입니다.</p> <p>해시 경로에는 공백과 유효한 파일 이름 문자가 포함될 수 있습니다.</p> |

필요에 따라 다음 매개 변수를 지정할 수 있습니다.

| 선택적 매개 변수입니다      | 설명                                                                                                                                                                                                                                                                               |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| _ 지원되는 버전 _       | ONTAP은 BranchCache 1 및 2를 지원합니다. 버전 1, 버전 2 또는 두 버전을 모두 사용할 수 있습니다. 기본값은 두 버전을 모두 사용하는 것입니다.                                                                                                                                                                                     |
| _ 해시 저장소의 최대 크기 _ | 해시 데이터 저장소에 사용할 크기를 지정할 수 있습니다. 해시 데이터가 이 값을 초과하면 ONTAP은 이전 해시를 삭제하여 새 해시를 위한 공간을 만듭니다. 해시 저장소의 기본 크기는 1GB입니다. BranchCache는 해시가 지나치게 공격적인 방식으로 폐기되지 않을 경우 보다 효율적으로 성능을 발휘합니다. 해시 저장소가 꽉 찼기 때문에 해시가 자주 삭제되는 경우 BranchCache 구성을 수정하여 해시 저장소 크기를 늘릴 수 있습니다.                         |
| _ 서버 키 _          | BranchCache 서비스가 클라이언트가 BranchCache 서버를 가장하지 못하도록 하는 데 사용하는 서버 키를 지정할 수 있습니다. 서버 키를 지정하지 않으면 BranchCache 구성을 만들 때 서버 키가 임의로 생성됩니다. 여러 서버가 동일한 파일에 BranchCache 데이터를 제공하는 경우 클라이언트는 동일한 서버 키를 사용하는 모든 서버의 해시를 사용할 수 있도록 서버 키를 특정 값으로 설정할 수 있습니다. 서버 키에 공백이 있으면 서버 키를 따옴표로 묶어야 합니다. |
| _ 작동 모드 _         | <p>기본 설정은 공유별로 BranchCache를 사용하는 것입니다.</p> <ul style="list-style-type: none"> <li>• BranchCache 구성을 생성하여 공유별로 BranchCache를 사용하도록 설정하려면 이 선택적 매개 변수를 지정하지 않거나 "공유당"을 지정할 수 있습니다.</li> <li>• 모든 공유에서 BranchCache를 자동으로 활성화하려면 운영 모드를 '모든 공유'로 설정해야 합니다.</li> </ul>                 |

## 단계

### 1. 필요에 따라 SMB 2.1 및 3.0 활성화:

- 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
- 구성된 SVM SMB 설정을 확인하여 필요한 모든 SMB 버전이 활성화되었는지 확인합니다. 'vserver cifs options show -vserver\_vserver\_name\_'
- 필요한 경우 SMB 2.1:'vserver cifs options modify -vserver\_vserver\_name\_-SMB2-enabled true'를 설정합니다

이 명령을 사용하면 SMB 2.0 및 SMB 2.1이 모두 설정됩니다.

- 필요한 경우 SMB 3.0:'vserver cifs options modify -vserver\_vserver\_name\_-SMB3-enabled true'를 설정합니다

e. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

2. BranchCache 구성:'vserver cifs BranchCache create -vserver\_name\_ -hash-store-path path path [-hash-store-max-size{integer[KB|MB|GB|TB|PB]} [-versions{v1-enable|v2-enable|enable-all}][-server-key text] -operating-mode{per-share|all-share}}

지정된 해시 스토리지 경로가 있어야 하며 SVM에서 관리하는 볼륨에 상주해야 합니다. 경로는 읽기 쓰기 가능 볼륨에도 있어야 합니다. 경로가 읽기 전용이거나 존재하지 않으면 명령이 실패합니다.

SVM BranchCache 구성을 추가할 때 동일한 서버 키를 사용하려면 서버 키에 대해 입력한 값을 기록합니다. BranchCache 구성에 대한 정보를 표시할 때는 서버 키가 나타나지 않습니다.

3. BranchCache 구성이 올바른지 확인합니다. 'vserver cifs BranchCache show -vserver\_vserver\_name\_'

예

다음 명령을 실행하면 SMB 2.1과 3.0이 모두 활성화되어 있고 SVM VS1의 모든 SMB 공유에서 캐싱이 자동으로 활성화되도록 BranchCache가 구성됩니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled

vs1 true true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: all_shares
```

다음 명령은 SMB 2.1과 3.0이 모두 활성화되어 있는지 확인하고, SVM VS1 기반 공유별로 캐싱이 가능하도록 BranchCache를 구성하고, BranchCache 구성을 확인합니다.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled

vs1 true true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

 Vserver: vs1
 Supported BranchCache Versions: enable_all
 Path to Hash Store: /hash_data
 Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
 CIFS BranchCache Operating Modes: per_share

```

#### 관련 정보

- [BranchCache 버전 지원에 대해 알아보세요](#)
- [원격 사무실에서 BranchCache를 구성하는 방법에 대해 알아보세요.](#)
- [BranchCache 지원 SMB 공유를 생성합니다](#)
- [기존 공유에서 BranchCache 활성화](#)
- [공유에서 BranchCache 구성 수정](#)
- [공유에서 BranchCache 비활성화에 대해 알아보세요](#)
- [공유에서 BranchCache 구성을 삭제합니다.](#)

**ONTAP SMB**에서 원격 사무실에서 **BranchCache**를 구성하는 방법에 대해 알아보세요.

SMB 서버에서 BranchCache를 구성한 후에는 클라이언트 컴퓨터에 BranchCache를 설치하고 구성해야 하며, 필요에 따라 원격 사무실의 캐싱 서버에 BranchCache를 설치하고 구성해야 합니다. Microsoft는 원격 사무소에서 BranchCache를 구성하는 지침을 제공합니다.

지점 클라이언트 구성 지침 및 BranchCache를 사용할 캐싱 서버(선택 사항)는 Microsoft BranchCache 웹 사이트에 있습니다.

BranchCache 지원 SMB 공유를 구성합니다

BranchCache 지원 ONTAP SMB 공유 구성에 대해 알아보세요.

SMB 서버 및 지사에 BranchCache를 구성한 후에는 지점의 클라이언트가 캐시할 콘텐츠를 포함하는 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

BranchCache 캐싱은 SMB 서버의 모든 SMB 공유 또는 공유별로 설정할 수 있습니다.

- 공유별로 BranchCache를 사용하도록 설정한 경우 공유를 생성하거나 기존 공유를 수정하여 BranchCache를 사용하도록 설정할 수 있습니다.

기존 SMB 공유에서 캐싱을 사용하는 경우 ONTAP는 해당 공유에서 BranchCache를 사용하도록 설정하는 즉시 해시 컴퓨팅을 시작하고 콘텐츠를 요청하는 클라이언트로 메타데이터를 전송합니다.

- 이전에 SMB로 공유에 접속한 클라이언트는 이후에 BranchCache가 해당 공유에 설정된 경우 BranchCache 지원을 받지 못합니다.

ONTAP는 SMB 세션이 설정된 시간에 공유에 대한 BranchCache 지원을 알립니다. BranchCache를 사용하도록 설정할 때 이미 세션을 설정한 클라이언트는 연결을 끊고 다시 연결하여 이 공유에 캐시된 콘텐츠를 사용해야 합니다.



이후에 SMB 공유의 BranchCache가 비활성화되면 ONTAP는 요청 클라이언트로 메타데이터 전송을 중지합니다. 데이터가 필요한 클라이언트는 콘텐츠 서버(SMB 서버)에서 직접 검색합니다.

BranchCache 지원 ONTAP SMB 공유 생성

공유를 생성할 때 "BranchCache" 공유 속성을 설정하여 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SMB 공유에 BranchCache가 설정되어 있으면 공유에 수동 캐싱으로 설정된 오프라인 파일 구성이 있어야 합니다.

공유를 생성할 때 기본 설정입니다.

- BranchCache 사용 공유를 생성할 때 추가 선택적 공유 매개 변수를 지정할 수도 있습니다.
- BranchCache가 SVM(스토리지 가상 시스템)에서 구성 및 설정되지 않은 경우에도 공유에 "BranchCache" 속성을 설정할 수 있습니다.

그러나 공유 폴더에 캐시된 콘텐츠가 제공되도록 하려면 SVM에서 BranchCache를 구성하고 사용하도록 설정해야 합니다.

- '-share-properties' 매개 변수를 사용할 때 공유에 적용되는 기본 공유 속성이 없으므로 쉼표로 구분된 목록을 사용하여 "BranchCache" 공유 속성 외에도 공유에 적용할 다른 모든 공유 속성을 지정해야 합니다.
- 에 대한 자세한 내용은 `vserver cifs share create` ["ONTAP 명령 참조입니다"](#)를 참조하십시오.

단계

1. BranchCache 지원 SMB 공유 생성: + 'vserver CIFS share create -vserver \_vserver\_name\_ -share -name \_share\_name\_ -path \_path\_ -share-properties BranchCache[,...]'
2. 'vserver cifs share show' 명령을 사용하여 SMB 공유에 BranchCache 공유 속성이 설정되어 있는지 확인합니다.

예

다음 명령을 실행하면 SVM VS1 에서 "/data " 경로를 사용하여 " data " 라는 BranchCache 지원 SMB 공유가 생성됩니다. 기본적으로 오프라인 파일 설정은 '수동'으로 설정됩니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
 Vserver: vs1
 Share: data
CIFS Server NetBIOS Name: VS1
 Path: /data
 Share Properties: branchcache
 oplocks
 browsable
 changenotify
 Symlink Properties: enable
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
 File Attribute Cache Lifetime: -
 Volume Name: data
 Offline Files: manual
 Vscan File-Operations Profile: standard
```

관련 정보

[단일 공유에서 BranchCache 비활성화](#)

기존 **ONTAP SMB** 공유에서 **BranchCache** 활성화

기존 공유 속성 목록에 'BranchCache' 공유 속성을 추가하여 기존 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SMB 공유에 BranchCache가 설정되어 있으면 공유에 수동 캐싱으로 설정된 오프라인 파일 구성이 있어야 합니다.  
기존 공유의 오프라인 파일 설정이 수동 캐싱으로 설정되어 있지 않으면 공유를 수정하여 구성해야 합니다.
- BranchCache가 SVM(스토리지 가상 시스템)에서 구성 및 설정되지 않은 경우에도 공유에 "BranchCache" 속성을 설정할 수 있습니다.

그러나 공유 폴더에 캐시된 콘텐츠가 제공되도록 하려면 SVM에서 BranchCache를 구성하고 사용하도록 설정해야 합니다.

- 공유에 "BranchCache" 공유 속성을 추가하면 기존 공유 설정과 공유 속성이 유지됩니다.

BranchCache 공유 속성이 기존 공유 속성 목록에 추가됩니다. 에 대한 자세한 내용은 `vserver cifs share properties add` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

#### 단계

- 필요한 경우 수동 캐싱에 대한 오프라인 파일 공유 설정을 구성합니다.
  - '`vserver cifs share show`' 명령을 사용하여 오프라인 파일 공유 설정을 확인합니다.
  - 오프라인 파일 공유 설정이 `manual`로 설정되어 있지 않으면 필요한 값('vserver cifs share modify -vserver vserver\_name -share-name share\_name share\_name -offline-files manual')으로 변경합니다
- 기존 SMB 공유에서 BranchCache를 사용하도록 설정합니다. '`vserver cifs share properties add-vserver vserver_name -share-name share_name-share-properties BranchCache`'
- SMB 공유에서 BranchCache 공유 속성이 설정되어 있는지 확인합니다. '`vserver cifs share show -vserver vserver_name -share-name share_name`'

#### 예

다음 명령을 실행하면 SVM VS1 에서 " data2 " 라는 기존 SMB 공유에서 "/data2 " 경로를 사용하여 BranchCache를 사용할 수 있습니다.



```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

 Vservice: vs1
 Share: data2
 CIFS Server NetBIOS Name: VS1
 Path: /data2
 Share Properties: oplocks
 browsable
 changenotify
 showsnapshot
 Symlink Properties: -
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
 Volume Name: -
 Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties add -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

 Vservice: vs1
 Share: data2
 CIFS Server NetBIOS Name: VS1
 Path: /data2
 Share Properties: oplocks
 browsable
 showsnapshot
 changenotify
 branchcache
 Symlink Properties: -
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
 Volume Name: -
 Offline Files: manual
Vscan File-Operations Profile: standard
```

- 기존 주식에 주식 속성 추가 또는 제거
- 단일 공유에서 BranchCache 비활성화

BranchCache 구성을 관리하고 모니터링합니다

## ONTAP SMB 공유에서 BranchCache 구성 수정

해시 저장소 디렉토리 경로 변경, 해시 저장소 최대 디렉토리 크기, 운영 모드 및 지원되는 BranchCache 버전을 포함하여 SVM에서 BranchCache 서비스의 구성을 수정할 수 있습니다. 해시 저장소가 포함된 볼륨의 크기를 늘릴 수도 있습니다.

단계

1. 적절한 작업을 수행합니다.

| 원하는 작업                                                                           | 다음을 입력하십시오.                                                                              |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| 해시 저장소 디렉터리 크기를 수정합니다                                                            | 'vserver cifs BranchCache modify -vserver vservice_name -hash-store -max-size{integer[KB |
| MB                                                                               | GB                                                                                       |
| TB                                                                               | PB]]'                                                                                    |
| 해시 저장소가 포함된 볼륨의 크기를 늘립니다                                                         | ``볼륨 크기 - vservice vservice_name - volume volume_name - new-size new_size [k             |
| m                                                                                | g                                                                                        |
| tb] 해시 저장소가 포함된 볼륨이 가득 차면 볼륨의 크기를 늘릴 수 있습니다. 새 볼륨 크기를 숫자로 지정한 다음 단위를 지정할 수 있습니다. | 해시 저장소 디렉터리 경로를 수정합니다                                                                    |
| 에 대해 자세히 알아보십시오 " <a href="#">FlexVol 볼륨 관리</a> "                                |                                                                                          |

|                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 원하는 작업                                                                                         | 다음을 입력하십시오.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 'vserver cifs BranchCache modify -vserver vserver_name -hash-store-path path -flush -hash{true | <p>false}' SVM이 SVM 재해 복구 소스인 경우 해시 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨이 재해 복구 대상에 복제되지 않기 때문입니다.</p> <p>BranchCache 해시 경로에는 공백과 유효한 파일 이름 문자가 포함될 수 있습니다.</p> <p>해시 경로를 수정할 경우 ONTAP가 원래 해시 저장 위치에서 해시를 플러시할지 여부를 지정하는 필수 매개 변수입니다. '-flush-hash' 파라미터에 대해 다음 값을 설정할 수 있습니다.</p> <p><b>"true"</b>를 지정하면 <b>ONTAP</b>는 원래 위치에서 해시를 삭제하고 <b>BranchCache</b> 사용 클라이언트가 새 요청을 수행할 때 새 위치에 새 해시를 만듭니다.<br/>false를 지정하면 해시가 플러시되지 않습니다.</p> <p>+</p> <p>이 경우 해시 저장소 경로를 원래 위치로 다시 변경하여 나중에 기존 해시를 다시 사용하도록 선택할 수 있습니다.</p> |
| 작동 모드를 변경합니다                                                                                   | 'vserver cifs BranchCache modify -vserver vserver_name -operating-mode{per-share                                                                                                                                                                                                                                                                                                                                                                                                                              |
| all-share                                                                                      | <p>disable}'</p> <p>작동 모드를 수정할 때 다음 사항에 유의해야 합니다.</p> <p><b>ONTAP</b>는 <b>SMB</b> 세션이 설정되어 있을 때 공유에 대한 <b>BranchCache</b> 지원을 알립니다.<br/>BranchCache를 사용하도록 설정할 때 이미 세션을 설정한 클라이언트는 연결을 끊고 다시 연결하여 이 공유에 캐시된 콘텐츠를 사용해야 합니다.</p>                                                                                                                                                                                                                                                                                |
| BranchCache 버전 지원을 변경합니다                                                                       | 'vserver cifs BranchCache modify -vserver vserver_name -versions{v1-enable                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| v2-enable                                                                                      | enable-all}'                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

2. 'vserver cifs BranchCache show' 명령을 사용하여 구성 변경 사항을 확인합니다.

## ONTAP SMB 공유에서 BranchCache 구성에 대한 정보 표시

구성을 확인하거나 구성을 수정하기 전에 현재 설정을 확인할 때 사용할 수 있는 SVM(스토리지 가상 머신)에 BranchCache 구성에 대한 정보를 표시할 수 있습니다.

### 단계

1. 다음 작업 중 하나를 수행합니다.

|                                  |                                                           |
|----------------------------------|-----------------------------------------------------------|
| 를 표시하려면...                       | 이 명령을 입력하십시오...                                           |
| 모든 SVM의 BranchCache 구성에 대한 요약 정보 | 'vserver cifs BranchCache show'를 선택합니다                    |
| 특정 SVM의 구성에 대한 자세한 정보            | 'vserver cifs BranchCache show<br>-vserver_vserver_name_' |

예

다음 예에서는 SVM VS1 BranchCache 구성에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

## ONTAP SMB BranchCache 서버 키 변경

SVM(스토리지 가상 시스템)에서 BranchCache 구성을 수정하고 다른 서버 키를 지정하여 BranchCache 서버 키를 변경할 수 있습니다.

이 작업에 대해

여러 서버가 동일한 파일에 BranchCache 데이터를 제공하는 경우 클라이언트는 동일한 서버 키를 사용하는 모든 서버의 해시를 사용할 수 있도록 서버 키를 특정 값으로 설정할 수 있습니다.

서버 키를 변경할 때는 해시 캐시도 플러시해야 합니다. 해시를 플러싱한 후 ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

단계

1. 'vserver cifs BranchCache modify -vserver vserver\_name -server -key text -flush -hash true' 명령을 사용하여 서버 키를 변경합니다

새 서버 키를 구성할 때는 -flush-hash를 지정하고 값을 true로 설정해야 합니다.

2. 'vserver cifs BranchCache show' 명령을 사용하여 BranchCache 구성이 올바른지 확인합니다.

예

다음 예에서는 공백이 포함된 새 서버 키를 설정하고 SVM VS1 의 해시 캐시를 플러시합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

## 관련 정보

[ONTAP가 BranchCache 해시를 무효화하는 이유에 대해 알아보세요.](#)

지정된 **ONTAP SMB** 경로에서 **BranchCache** 해시를 미리 계산합니다.

BranchCache 서비스를 구성하여 단일 파일, 디렉토리 또는 디렉토리 구조의 모든 파일에 대한 해시를 사전 계산할 수 있습니다. 이 방법은 사용량이 많지 않은 시간 동안 BranchCache 사용 공유의 데이터에 대한 해시를 계산할 때 유용합니다.

이 작업에 대해

해시 통계를 표시하기 전에 데이터 샘플을 수집하려면 '통계 시작' 및 '통계 중지' 옵션 명령을 사용해야 합니다.

- 사전 컴퓨팅 해시를 계산할 스토리지 가상 시스템(SVM)과 경로를 지정해야 합니다.
- 또한 해시를 재귀적으로 계산할 것인지 여부를 지정해야 합니다.
- 해시를 재귀적으로 계산하려는 경우 BranchCache 서비스는 지정된 경로 아래의 전체 디렉토리 트리를 탐색한 다음 각 대상 객체에 대한 해시를 계산합니다.

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 ["ONTAP 명령 참조입니다"](#).

## 단계

1. 원하는 대로 사전 계산 해시:

| 에서 해시를 사전 계산하려는 경우...       | 명령 입력...                                                                                                 |
|-----------------------------|----------------------------------------------------------------------------------------------------------|
| 단일 파일 또는 디렉토리입니다            | <code>'vserver cifs BranchCache hash-create-vserver vserver_name-path path-recurse false'</code>         |
| 디렉토리 구조의 모든 파일에 반복적으로 존재합니다 | <code>'vserver cifs BranchCache hash-create-vserver vserver_name-path absolute_path-recurse true'</code> |

2. '통계' 명령을 사용하여 해시가 계산되는지 확인합니다.

- a. 원하는 SVM 인스턴스에 대한 'hashd' 객체 통계 표시: `'stattisics show-object hashd-instance'`

vserver\_name'

b. 명령을 반복하여 생성된 해시 수가 증가하는지 확인합니다.

에 대한 자세한 내용은 `statistics show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

예

다음 예에서는 경로 '/data'와 SVM VS1 의 모든 포함된 파일 및 하위 디렉토리에 해시를 생성합니다.

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

| Counter                         | Value                                |
|---------------------------------|--------------------------------------|
| branchcache_hash_created        | 85                                   |
| branchcache_hash_files_replaced | 0                                    |
| branchcache_hash_rejected       | 0                                    |
| branchcache_hash_store_bytes    | 0                                    |
| branchcache_hash_store_size     | 0                                    |
| instance_name                   | vs1                                  |
| node_name                       | node1                                |
| node_uuid                       | 11111111-1111-1111-1111-111111111111 |
| process_name                    | -                                    |

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

| Counter                         | Value                                |
|---------------------------------|--------------------------------------|
| branchcache_hash_created        | 92                                   |
| branchcache_hash_files_replaced | 0                                    |
| branchcache_hash_rejected       | 0                                    |
| branchcache_hash_store_bytes    | 0                                    |
| branchcache_hash_store_size     | 0                                    |
| instance_name                   | vs1                                  |
| node_name                       | node1                                |
| node_uuid                       | 11111111-1111-1111-1111-111111111111 |
| process_name                    | -                                    |

## 관련 정보

- ["성능 모니터링 설정"](#)

## ONTAP SMB SVM BranchCache 해시 저장소에서 해시 플러시

SVM(스토리지 가상 머신)의 BranchCache 해시 저장소에서 캐시된 모든 해시를 플러시할 수 있습니다. 지사 BranchCache 구성을 변경한 경우 이 기능이 유용할 수 있습니다. 예를 들어 최근에 분산 캐싱에서 호스팅된 캐싱 모드로 캐싱 모드를 재구성한 경우 해시 저장소를 플러시해야 합니다.

이 작업에 대해

해시를 플러싱한 후 ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

단계

1. BranchCache 해시 저장소에서 해시를 플러시합니다. 'vserver cifs BranchCache hash-flush-vserver\_vserver\_name\_'

```
'vserver cifs BranchCache hash-flush-vserver vs1'
```

## ONTAP SMB BranchCache 통계 표시

BranchCache 통계를 에 표시할 수도 있습니다. 그 중에서도 캐싱을 얼마나 잘 수행하고 있는지 식별하고, 구성이 클라이언트에 캐시된 콘텐츠를 제공하고 있는지 여부를 확인하고, 해시 파일을 삭제하여 최신 해시 데이터를 저장할 공간을 확보할 수 있는지 확인할 수 있습니다.

이 작업에 대해

"hashd" 통계 객체에는 BranchCache 해시에 대한 통계 정보를 제공하는 카운터가 포함되어 있습니다. CIFS 통계 객체에는 BranchCache 관련 작업에 대한 통계 정보를 제공하는 카운터가 포함되어 있습니다. 고급 권한 수준에서 이러한 개체에 대한 정보를 수집하고 표시할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. 'istics catalog counter show' 명령을 사용하여 BranchCache 관련 카운터를 출력한다.

```
cluster1::*> statistics catalog counter show -object hashd
```

```
Object: hashd
```

| Counter | Description |
|---------|-------------|
|---------|-------------|

-----

-----

|                          |                                                                              |
|--------------------------|------------------------------------------------------------------------------|
| branchcache_hash_created | Number of times a request to generate BranchCache hash for a file succeeded. |
|--------------------------|------------------------------------------------------------------------------|



```

branchcache_hash_files_replaced Number of times a BranchCache hash file
was deleted to make room for more recent
hash data. This happens if the hash store
size is exceeded.
branchcache_hash_rejected Number of times a request to generate
branchcache_hash_store_bytes BranchCache hash data failed.
Total number of bytes used to store hash
data.
branchcache_hash_store_size Total space used to store BranchCache
hash data for the Vserver.
instance_name Instance Name
instance_uuid Instance UUID
node_name System node name
node_uuid System node id
9 entries were displayed.

```

```
cluster1::*> statistics catalog counter show -object cifs
```

```
Object: cifs
```

| Counter                     | Description                                                                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -----                       | -----                                                                                                                                                                                                      |
| active_searches             | Number of active searches over SMB and SMB2                                                                                                                                                                |
| auth_reject_too_many        | Authentication refused after too many requests were made in rapid succession                                                                                                                               |
| avg_directory_depth         | Average number of directories crossed by SMB                                                                                                                                                               |
| avg_junction_depth          | Average number of junctions crossed by SMB                                                                                                                                                                 |
| branchcache_hash_fetch_fail | Total number of times a request to fetch hash data failed. These are failures when attempting to read existing hash data. It does not include attempts to fetch hash data that has not yet been generated. |

```

branchcache_hash_fetch_ok Total number of times a request to fetch
hash data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients
 requesting hashes.
branchcache_missing_hash_bytes
to be Total number of bytes of data that had
that read by the client because the hash for
 content was not available on the server.
....Output truncated....

```

에 대한 자세한 내용은 `statistics catalog counter show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. '스타티틱스 스타트', '스타티틱스 스톱' 명령어를 사용해 BranchCache 관련 통계를 수집한다.

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 ["ONTAP 명령 참조입니다"](#).

4. 통계 표시 명령을 사용하여 수집된 BranchCache 통계를 표시합니다.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1
```

| Counter                     | Value |
|-----------------------------|-------|
| branchcache_hash_sent_bytes | 0     |
| branchcache_hash_sent_bytes | 0     |
| branchcache_hash_sent_bytes | 0     |
| branchcache_hash_sent_bytes | 0     |

```
cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1
```

| Counter                        | Value |
|--------------------------------|-------|
| branchcache_missing_hash_bytes | 0     |
| branchcache_missing_hash_bytes | 0     |
| branchcache_missing_hash_bytes | 0     |
| branchcache_missing_hash_bytes | 0     |

에 대한 자세한 내용은 `statistics show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

#### 5. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

```
cluster1::*> set -privilege admin
```

#### 관련 정보

- [통계를 표시합니다](#)
- ["성능 모니터링 설정"](#)
- ["통계 시작"](#)
- ["통계 중지"](#)

**BranchCache** 그룹 정책 개체에 대한 **ONTAP SMB** 지원에 대해 알아보세요.

ONTAP BranchCache는 특정 BranchCache 구성 매개 변수에 대한 중앙 집중식 관리를 허용하는 BranchCache GPO(그룹 정책 개체)를 지원합니다. BranchCache에는 두 가지 GPO, 즉 BranchCache GPO의 해시 게시 GPO와 BranchCache GPO의 해시 버전 지원 GPO가 사용됩니다.

- \* BranchCache GPO \* 용 해시 게시

BranchCache GPO의 해시 게시는 '-operating-mode' 매개 변수에 해당합니다. GPO 업데이트가 발생하면 이 값은 그룹 정책이 적용되는 OU(조직 구성 단위) 내에 포함된 SVM(스토리지 가상 시스템) 개체에 적용됩니다.

- \* BranchCache GPO \* 에 대한 해시 버전 지원

BranchCache GPO의 해시 버전 지원은 '-versions' 매개 변수에 해당합니다. GPO 업데이트가 발생하면 이 값은 그룹 정책이 적용되는 조직 구성 단위 내에 포함된 SVM 개체에 적용됩니다.

#### 관련 정보

[SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.](#)

#### ONTAP SMB BranchCache 그룹 정책 개체에 대한 정보 표시

CIFS 서버의 GPO(그룹 정책 개체) 구성에 대한 정보를 표시하여 BranchCache GPO가 CIFS 서버가 속한 도메인에 대해 정의되었는지 그리고 그러한 경우 허용되는 설정이 무엇인지 확인할 수 있습니다. 또한 BranchCache GPO 설정이 CIFS 서버에 적용되는지 여부를 확인할 수 있습니다.

#### 이 작업에 대해

CIFS 서버가 속한 도메인 내에서 GPO 설정이 정의되더라도 CIFS 지원 SVM(스토리지 가상 머신)이 포함된 OU(조직 구성 단위)에는 적용되지 않을 수도 있습니다. 적용된 GPO 설정은 CIFS 지원 SVM에 적용되는 정의된 모든 GPO의 하위 집합입니다. GPO를 통해 적용된 BranchCache 설정은 CLI를 통해 적용된 설정을 재정의합니다.

#### 단계

1. 'vserver cifs group-policy show-defined' 명령을 사용하여 Active Directory 도메인에 대해 정의된 BranchCache GPO 설정을 표시합니다.



이 예제에는 명령에 사용할 수 있는 출력 필드가 모두 표시되지 않습니다. 출력이 잘립니다.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```

```

```
 GPO Name: Default Domain Policy
```

```
 Level: Domain
```

```
 Status: enabled
```

```
Advanced Audit Settings:
```

```
 Object Access:
```

```
 Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
 Refresh Time Interval: 22
```

```
 Refresh Random Offset: 8
```

```
 Hash Publication Mode for BranchCache: per-share
```

```
 Hash Version Support for BranchCache: version1
```

```
[...]
```

```
 GPO Name: Resultant Set of Policy
```

```
 Status: enabled
```

```
Advanced Audit Settings:
```

```
 Object Access:
```

```
 Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
 Refresh Time Interval: 22
```

```
 Refresh Random Offset: 8
```

```
 Hash Publication for Mode BranchCache: per-share
```

```
 Hash Version Support for BranchCache: version1
```

```
[...]
```

2. 'vserver cifs group-policy show-applied' 명령을 사용하여 CIFS 서버에 적용된 BranchCache GPO 설정을 표시합니다. ``이



이 예제에는 명령에 사용할 수 있는 출력 필드가 모두 표시되지 않습니다. 출력이 잘립니다.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1

 GPO Name: Default Domain Policy
 Level: Domain
 Status: enabled
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: version1
[...]

 GPO Name: Resultant Set of Policy
 Level: RSOP
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: version1
[...]
```

#### 관련 정보

- [서버에서 GPO 지원 활성화 또는 비활성화](#)
- ["SVM CIFS 그룹 - policy show-defined"](#)
- ["SVM CIFS 그룹 - policy show-applied"](#)

**SMB 공유에서 BranchCache**를 해제합니다

**ONTAP SMB 공유에서 BranchCache 비활성화에 대해 알아보세요**

특정 SMB 공유에서 BranchCache 캐싱 서비스를 제공하지 않고 나중에 이러한 공유에 캐싱 서비스를 제공하려는 경우 공유별로 BranchCache를 사용하지 않도록 설정할 수 있습니다. BranchCache가 모든 공유에서 캐싱을 제공하도록 구성되었지만 모든 캐싱 서비스를 일시적으로 해제하려면 BranchCache 구성을 수정하여 모든 공유에서 자동 캐싱을 중지할 수 있습니다.

SMB 공유의 BranchCache가 이후에 처음 설정된 후 비활성화되면 ONTAP는 요청된 클라이언트로 메타데이터 전송을 중지합니다. 데이터가 필요한 클라이언트는 콘텐츠 서버(SVM(Storage Virtual Machine)의 CIFS 서버)에서 직접 데이터를 검색합니다.

관련 정보

[BranchCache 지원 공유 구성에 대해 알아보세요](#)

단일 **ONTAP SMB** 공유에서 **BranchCache** 비활성화

이전에 캐시된 콘텐츠를 제공한 특정 공유에 캐싱 서비스를 제공하지 않으려면 기존 SMB 공유에서 BranchCache를 사용하지 않도록 설정할 수 있습니다.

단계

1. 'vserver cifs share properties remove-vserver vservers\_name -share-name share\_name-share-properties BranchCache' 명령을 입력합니다

BranchCache 공유 속성이 제거됩니다. 다른 적용된 공유 속성은 그대로 유지됩니다.

예

다음 명령을 실행하면 이름이 "data2"인 기존 SMB 공유에서 BranchCache가 비활성화됩니다.

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

 Vservice: vs1
 Share: data2
CIFS Server NetBIOS Name: VS1
 Path: /data2
 Share Properties: oplocks
 browsable
 changenotify
 attributecache
 branchcache
 Symlink Properties: -
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
 Volume Name: -
 Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties remove -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

 Vservice: vs1
 Share: data2
CIFS Server NetBIOS Name: VS1
 Path: /data2
 Share Properties: oplocks
 browsable
 changenotify
 attributecache
 Symlink Properties: -
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
 Volume Name: -
 Offline Files: manual
Vscan File-Operations Profile: standard
```



모든 **ONTAP SMB** 공유에서 자동 캐싱 중지

BranchCache 구성에서 각 SVM(스토리지 가상 머신)의 모든 SMB 공유에 대한 캐싱을 자동으로 설정하는 경우 BranchCache 구성을 수정하여 모든 SMB 공유의 콘텐츠를 자동으로 캐싱하지 않도록 할 수 있습니다.

이 작업에 대해

모든 SMB 공유에서 자동 캐싱을 중지하려면 BranchCache 운영 모드를 공유 기준 캐싱으로 변경합니다.

단계

1. 모든 SMB 공유에서 자동 캐싱을 중지하도록 BranchCache를 구성합니다. 'vserver cifs BranchCache modify -vserver vserver\_name -operating-mode per-share'
2. BranchCache 구성이 올바른지 확인합니다. 'vserver cifs BranchCache show -vserver vserver\_name'

예

다음 명령을 실행하면 스토리지 가상 머신(SVM, 이전의 Vserver)의 BranchCache 구성이 변경되어 모든 SMB 공유에서 자동 캐싱을 중지합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

**SVM에서 BranchCache**를 비활성화하거나 활성화합니다

**ONTAP SMB** 서버에서 **BranchCache**를 비활성화하거나 다시 활성화하면 어떤 일이 발생하는지 알아보세요.

이전에 BranchCache를 구성했지만 지사 클라이언트가 캐시된 콘텐츠를 사용하지 않도록 하려면 CIFS 서버에서 캐싱을 해제할 수 있습니다. BranchCache를 사용하지 않도록 설정하면 어떤 일이 발생하는지 알고 있어야 합니다.

BranchCache를 사용하지 않도록 설정하면 ONTAP는 더 이상 해시를 계산하지 않고 요청 클라이언트로 메타데이터를 보내지 않습니다. 그러나 파일 액세스는 중단되지 않습니다. 그 후 BranchCache를 사용하는 클라이언트가 액세스할 콘텐츠에 대한 메타데이터 정보를 요청하면 ONTAP는 Microsoft 정의 오류로 응답하여 클라이언트가 실제 콘텐츠를 요청하는 두 번째 요청을 보냅니다. CIFS 서버는 콘텐츠 요청에 따라 SVM(스토리지 가상 머신)에 저장된 실제 콘텐츠를 전송합니다.

CIFS 서버에서 BranchCache를 사용하지 않도록 설정한 후 SMB 공유는 BranchCache 기능을 알리지 않습니다. 새 SMB 연결에서 데이터에 액세스하기 위해 클라이언트는 SMB 읽기 요청을 정상적으로 처리합니다.

언제든지 CIFS 서버에서 BranchCache를 다시 설정할 수 있습니다.

- BranchCache를 비활성화하면 해시 저장소가 삭제되지 않으므로 요청된 해시가 여전히 유효하다면 ONTAP는 해시 요청을 다시 활성화한 후 해시 요청에 응답할 때 저장된 해시를 사용할 수 있습니다.
- BranchCache를 사용하지 않는 동안 BranchCache 사용 공유에 SMB 연결을 설정한 클라이언트는 BranchCache를 나중에 다시 사용하도록 설정한 경우 BranchCache 지원을 받지 않습니다.

이는 ONTAP가 SMB 세션을 설정할 때 공유에 대한 BranchCache 지원을 광고하기 때문입니다. BranchCache를 사용하지 않는 동안 BranchCache 사용 공유에 세션을 설정한 클라이언트는 이 공유에 대해 캐시된 콘텐츠를 사용하려면 연결을 끊고 다시 연결해야 합니다.



CIFS 서버에서 BranchCache를 해제한 후에 해시 저장소를 저장하지 않으려면 수동으로 삭제할 수 있습니다. BranchCache를 다시 사용하도록 설정하는 경우 해시 저장소 디렉터리가 있는지 확인해야 합니다. BranchCache를 다시 사용하도록 설정한 후 BranchCache 사용 공유는 BranchCache 기능을 광고합니다. ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

## ONTAP SMB 공유에서 BranchCache 비활성화 또는 활성화

BranchCache 운영 모드를 사용 안 함으로 변경하여 SVM(스토리지 가상 시스템)에서 BranchCache를 사용하지 않도록 설정할 수 있습니다. 운영 모드를 변경하여 BranchCache 서비스를 공유당 제공하거나 모든 공유에 자동으로 제공하여 언제든지 BranchCache를 활성화할 수 있습니다.

단계

1. 적절한 명령을 실행합니다.

| 원하는 작업                             | 그런 다음 다음을 입력합니다.                                                                  |
|------------------------------------|-----------------------------------------------------------------------------------|
| BranchCache를 비활성화합니다               | 'vserver cifs BranchCache modify -vserver vserver_name -operating-mode disable'   |
| 공유당 BranchCache를 설정합니다             | 'vserver cifs BranchCache modify -vserver vserver_name -operating-mode per-share' |
| 모든 공유에 대해 BranchCache를 사용하도록 설정합니다 | 'vserver cifs BranchCache modify -vserver vserver_name -operating-mode all-공유'    |

2. BranchCache 작동 모드가 'vserver cifs BranchCache show -vserver vserver\_name' 설정으로 구성되어 있는지 확인합니다

예

다음 예에서는 SVM VS1 에서 BranchCache를 사용하지 않도록 설정합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable
```

**SVM에서 BranchCache 구성을 삭제합니다**

**ONTAP SMB 공유에서 BranchCache 구성을 삭제하면 어떤 일이 발생하는지 알아보세요.**

이전에 BranchCache를 구성했지만 SVM(스토리지 가상 시스템)이 캐시된 콘텐츠를 계속 제공하지 않도록 하려면 CIFS 서버에서 BranchCache 구성을 삭제할 수 있습니다. 구성을 삭제할 때 어떤 일이 발생하는지 알고 있어야 합니다.

구성을 삭제하면 ONTAP에서 해당 SVM에 대한 구성 정보를 클러스터에서 제거하고 BranchCache 서비스를 중지합니다. ONTAP에서 SVM의 해시 저장소를 삭제할 것인지 여부를 선택할 수 있습니다.

BranchCache 구성을 삭제해도 BranchCache 사용 클라이언트의 액세스가 중단되지 않습니다. 그 후 BranchCache를 사용하는 클라이언트가 이미 캐시된 콘텐츠에 대한 기존 SMB 연결에 대한 메타데이터 정보를 요청하면 ONTAP는 Microsoft 정의 오류로 응답하여 클라이언트가 실제 콘텐츠를 요청하는 두 번째 요청을 보냅니다. CIFS 서버는 콘텐츠 요청에 응답하여 SVM에 저장된 실제 콘텐츠를 전송합니다

BranchCache 구성이 삭제된 후 SMB 공유는 BranchCache 기능을 알리지 않습니다. 새 SMB 연결을 사용하여 이전에 캐시되지 않은 콘텐츠에 액세스하려면 클라이언트는 SMB 읽기 요청을 정상적으로 처리합니다.

**ONTAP SMB 공유에서 BranchCache 구성을 삭제합니다.**

SVM(스토리지 가상 시스템)에서 BranchCache 서비스를 삭제하는 데 사용하는 명령은 기존 해시를 삭제하거나 유지할지 여부에 따라 달라집니다.

단계

1. 적절한 명령을 실행합니다.

| 원하는 작업                               | 그런 다음 다음을 입력합니다.                                                            |
|--------------------------------------|-----------------------------------------------------------------------------|
| BranchCache 구성을 삭제하고 기존 해시를 삭제합니다    | 'vserver cifs BranchCache delete<br>-vserver_vserver_name_-flush-hash true  |
| BranchCache 구성을 삭제하지만 기존 해시는 그대로 둡니다 | 'vserver cifs BranchCache delete<br>-vserver_vserver_name_-flush-hash false |

예

다음 예에서는 SVM VS1 상의 BranchCache 구성을 삭제하고 기존 해시를 모두 삭제합니다.

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes true
```

**ONTAP SMB BranchCache**를 되돌릴 때 발생하는 일을 알아보세요.

ONTAP를 BranchCache를 지원하지 않는 릴리즈로 되돌릴 경우 어떤 일이 발생하는지 이해하는 것이 중요합니다.

- BranchCache를 지원하지 않는 ONTAP 버전으로 되돌릴 경우 SMB 공유는 BranchCache를 사용하는 클라이언트에 BranchCache 기능을 알리지 않으므로 클라이언트는 해시 정보를 요청하지 않습니다.

대신 일반 SMB 읽기 요청을 사용하여 실제 콘텐츠를 요청합니다. 콘텐츠 요청에 따라 SMB 서버는 SVM(스토리지 가상 머신)에 저장된 실제 콘텐츠를 전송합니다.

- 해시 저장소를 호스팅하는 노드가 BranchCache를 지원하지 않는 릴리즈로 되돌려지면 스토리지 관리자는 복원 중에 인쇄되는 명령을 사용하여 BranchCache 구성을 수동으로 되돌려야 합니다.

이 명령을 실행하면 BranchCache 구성 및 해시가 삭제됩니다.

복원이 완료된 후 스토리지 관리자는 원하는 경우 해시 저장소가 포함된 디렉토리를 수동으로 삭제할 수 있습니다.

관련 정보

[공유에서 BranchCache 구성을 삭제합니다.](#)

## Microsoft 원격 복제 성능 향상

**ONTAP SMB** 서버에서 **Microsoft** 원격 복사 성능 개선에 대해 알아보세요.

Microsoft ODX(Offloaded Data Transfer)는 `_copy offload_`라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고도 호환되는 스토리지 장치 내부 또는 간에 데이터를 직접 전송할 수 있습니다.

ONTAP은 SMB 및 SAN 프로토콜을 모두 지원하는 ODX를 지원합니다. 소스는 CIFS 서버 또는 LUN일 수 있으며 대상은 CIFS 서버 또는 LUN일 수 있습니다.

ODX가 아닌 파일을 전송하면 소스에서 데이터를 읽어 네트워크를 통해 클라이언트 컴퓨터로 전송합니다. 클라이언트 컴퓨터는 네트워크를 통해 데이터를 대상으로 다시 전송합니다. 요약하면 클라이언트 컴퓨터는 소스에서 데이터를 읽고 대상에 씁니다. ODX 파일 전송을 사용하면 데이터가 소스에서 타겟으로 직접 복사됩니다.

오프로드 복사본은 소스 및 타겟 스토리지 간에 직접 수행되므로 성능이 크게 향상됩니다. 소스 및 대상 간의 복제 시간 단축, 클라이언트의 리소스 활용률(CPU, 메모리) 감소, 네트워크 I/O 대역폭 사용률 감소 등의 성능 이점을 얻을 수 있습니다.

SMB 환경의 경우 이 기능은 클라이언트와 스토리지 서버가 모두 SMB 3.0 및 ODX 기능을 지원하는 경우에만 사용할 수 있습니다. SAN 환경의 경우 이 기능은 클라이언트와 스토리지 서버가 ODX 기능을 모두 지원하는 경우에만 사용할 수 있습니다. ODX를 지원하고 ODX를 사용하는 클라이언트 컴퓨터는 파일을 이동하거나 복사할 때 오프로드된 파일

전송을 자동으로 투명하게 사용합니다. ODX는 Windows 탐색기를 통해 파일을 끌어서 놓을지, 명령줄 파일 복사 명령을 사용하는지, 클라이언트 애플리케이션이 파일 복사 요청을 시작하는지 여부와 관계없이 사용됩니다.

#### 관련 정보

- [자동 위치 지정을 통해 자동 노드 참조를 제공하여 클라이언트 응답 시간을 개선하는 방법에 대해 알아보세요.](#)
- ["Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"](#)

#### ONTAP SMB 서버에서 ODX에 대해 알아보세요

ODX 복사 오프로드는 토큰 기반 메커니즘을 사용하여 ODX 지원 CIFS 서버 내부 또는 간에 데이터를 읽고 씁니다. CIFS 서버는 데이터를 호스트를 통해 라우팅하는 대신 데이터를 나타내는 작은 토큰을 클라이언트에 보냅니다. ODX 클라이언트는 해당 토큰을 대상 서버에 제공하고, 이 토큰을 통해 표시되는 데이터를 소스에서 타겟으로 전송할 수 있습니다.

ODX 클라이언트는 CIFS 서버가 ODX를 지원하는 서버임을 인식하면 소스 파일을 열고 CIFS 서버에서 토큰을 요청합니다. 대상 파일을 연 후 클라이언트는 토큰을 사용하여 서버에서 데이터를 소스에서 대상으로 직접 복사하도록 지시합니다.

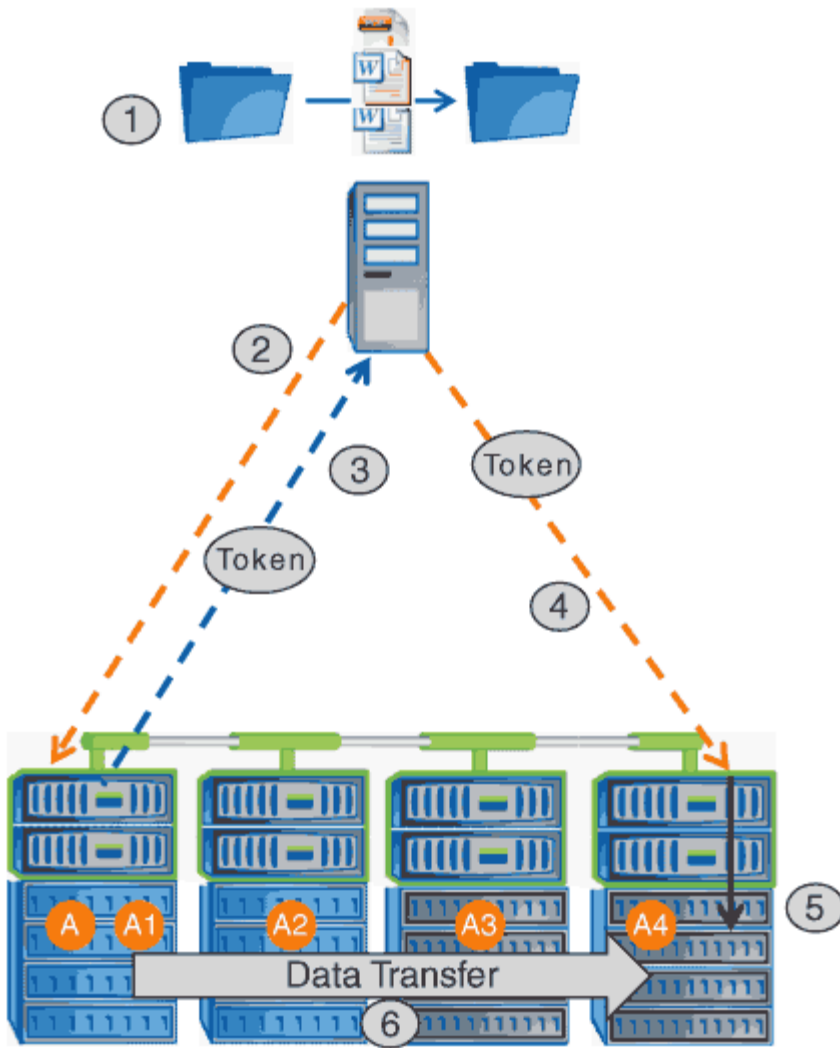


복사 작업의 범위에 따라 소스 및 대상이 동일한 SVM(스토리지 가상 머신) 또는 다른 SVM에 있을 수 있습니다.

토큰은 데이터의 시점 표현의 역할을 합니다. 예를 들어, 스토리지 위치 간에 데이터를 복사할 때 데이터 세그먼트를 나타내는 토큰이 요청 클라이언트로 반환되고, 이 클라이언트는 대상에 복사되므로 클라이언트를 통해 기본 데이터를 복사할 필요가 없습니다.

ONTAP는 8MB의 데이터를 나타내는 토큰을 지원합니다. 8MB를 초과하는 ODX 복제본은 8MB의 데이터를 나타내는 각 토큰과 함께 여러 토큰을 사용하여 수행됩니다.

다음 그림에서는 ODX 복사 작업과 관련된 단계를 설명합니다.



1. 사용자가 Windows 탐색기, 명령줄 인터페이스 또는 가상 시스템 마이그레이션의 일부로 파일을 복사 또는 이동하거나 응용 프로그램이 파일 복사 또는 이동을 시작합니다.

2. ODX 지원 클라이언트는 이 전송 요청을 ODX 요청으로 자동 변환합니다.

CIFS 서버로 전송되는 ODX 요청에 토큰에 대한 요청이 있습니다.

3. CIFS 서버에서 ODX가 설정되어 있고 연결이 SMB 3.0을 통해 설정되어 있으면 CIFS 서버가 토큰을 생성합니다. 이는 소스에서 데이터를 논리적으로 표현한 것입니다.

4. 클라이언트는 데이터를 나타내는 토큰을 받아 쓰기 요청과 함께 대상 CIFS 서버로 전송합니다.

이 데이터는 네트워크를 통해 소스에서 클라이언트로 복사한 다음 클라이언트에서 대상으로 복사하는 유일한 데이터입니다.

5. 토큰이 스토리지 서브시스템에 제공됩니다.

6. SVM은 내부적으로 복사 또는 이동을 수행합니다.

복사 또는 이동된 파일이 8MB보다 큰 경우 복제를 수행하려면 여러 토큰이 필요합니다. 필요에 따라 복사를 완료하기 위해 2-6단계를 수행합니다.



ODX 복사 작업을 오프로드하는 데 장애가 발생하면 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기 및 쓰기로 다시 이동됩니다. 마찬가지로, 대상 CIFS 서버가 ODX 또는 ODX를 지원하지 않을 경우 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기 및 쓰기로 다시 돌아갑니다.

#### ONTAP SMB 서버에서 ODX를 사용하기 위한 요구 사항

복사 오프로드를 SVM(스토리지 가상 머신)과 함께 사용하려면 먼저 특정 요구사항을 알고 있어야 합니다.

#### ONTAP 버전 요구 사항

ONTAP는 복사 오프로드를 위한 ODX를 지원합니다.

#### SMB 버전 요구 사항

- ONTAP는 SMB 3.0 이상을 지원하는 ODX를 지원합니다.
- ODX를 사용하려면 CIFS 서버에서 SMB 3.0을 설정해야 함:
  - ODX를 사용하도록 설정하면 SMB 3.0도 사용할 수 없습니다.
  - SMB 3.0을 비활성화하면 ODX도 비활성화됩니다.

#### Windows 서버 및 클라이언트 요구 사항

복사 오프로드를 위해 ODX를 사용하려면 Windows 클라이언트에서 이 기능을 지원해야 합니다.

를 클릭합니다 ["NetApp 상호 운용성 매트릭스"](#)지원되는 Windows 클라이언트에 대한 최신 정보를 제공합니다.

#### 볼륨 요구 사항

- 소스 볼륨은 최소 1.25GB여야 합니다.
  - 압축 볼륨을 사용하는 경우 압축 유형은 적응 가능해야 하며 압축 그룹 크기 8K만 지원됩니다.
- 보조 압축 유형은 지원되지 않습니다.

#### ONTAP SMB 서버에서 ODX를 사용하기 위한 지침

복사 오프로드에 ODX를 사용하려면 먼저 지침을 숙지하고 있어야 합니다. 예를 들어, ODX를 사용할 수 있는 볼륨 유형을 파악하고 클러스터 내부 및 클러스터 간 ODX 고려 사항을 파악해야 합니다.

#### 볼륨 지침

- 다음과 같은 볼륨 구성에서는 복사 오프로드에 ODX를 사용할 수 없습니다.
    - 소스 볼륨 크기가 1.25GB 미만입니다
- ODX를 사용하려면 볼륨 크기가 1.25GB 이상이어야 합니다.
- 읽기 전용 볼륨입니다

ODX는 로드 공유 미러 또는 SnapMirror 또는 SnapVault 대상 볼륨에 상주하는 파일 및 폴더에 사용되지 않습니다.

- 소스 볼륨 중복 제거가 수행되지 않은 경우
- ODX 복사본은 클러스터 내 복사본에만 지원됩니다.

ODX를 사용하여 파일 또는 폴더를 다른 클러스터의 볼륨으로 복사할 수는 없습니다.

## 기타 지침

- SMB 환경에서 복사 오프로드에 ODX를 사용하려면 파일이 256KB 이상이어야 합니다.

작은 파일은 기존 복사 작업을 사용하여 전송됩니다.

- ODX 복사 오프로드는 복제 프로세스의 일부로 중복 제거를 사용합니다.

데이터를 복사하거나 이동할 때 SVM 볼륨에서 중복 제거를 수행하지 않으려면 해당 SVM에서 ODX 복사 오프로드를 해제해야 합니다.

- ODX를 지원하려면 데이터 전송을 수행하는 애플리케이션에 데이터를 기록해야 합니다.

ODX를 지원하는 애플리케이션 작업은 다음과 같습니다.

- 가상 하드 디스크(VHD) 생성 및 변환, 스냅샷 관리, 가상 컴퓨터 간 파일 복사 등의 Hyper-V 관리 작업
- Windows 탐색기 작업
- Windows PowerShell 복사 명령
- Windows 명령 프롬프트 복사 명령

Windows 명령 프롬프트의 Robocopy는 ODX를 지원합니다.



ODX를 지원하는 Windows 서버 또는 클라이언트에서 애플리케이션이 실행되고 있어야 합니다.

+

Windows 서버 및 클라이언트에서 지원되는 ODX 애플리케이션에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

## 관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

## ONTAP SMB 서버에서 ODX 사용 사례

ODX가 성능 이점을 제공하는 상황을 파악할 수 있도록 SVM에서 ODX를 사용하는 사용 사례를 알고 있어야 합니다.

ODX를 지원하는 Windows 서버 및 클라이언트는 원격 서버 간에 데이터를 복사하는 기본 방법으로 복사 오프로드를 사용합니다. Windows 서버 또는 클라이언트가 ODX를 지원하지 않거나 ODX 복사 오프로드가 어느 시점에서든 장애가 발생하면 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기/쓰기로 다시 돌아갑니다.



ODX 복사 및 이동 사용을 지원하는 사용 사례는 다음과 같습니다.

- 체내

소스 및 대상 파일 또는 LUN이 동일한 볼륨 내에 있습니다.

- 볼륨 간, 동일한 노드, 동일한 SVM

소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- 볼륨 간, 다른 노드, 동일한 SVM

소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- SVM 간, 동일한 노드

소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- SVM 간, 다른 노드

소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- 클러스터 간

소스 및 타겟 LUN은 클러스터 전반의 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 이 기능은 SAN에만 지원되며 CIFS에는 사용할 수 없습니다.

다음과 같은 몇 가지 특별한 사용 사례가 있습니다.

- ONTAP ODX를 구현하면 ODX를 사용하여 SMB 공유와 FC 또는 iSCSI 연결 가상 드라이브 간에 파일을 복사할 수 있습니다.

SMB 공유와 LUN이 동일한 클러스터에 존재하는 경우, ODX를 지원하는 Windows 탐색기, Windows CLI 또는 PowerShell, Hyper-V 또는 기타 애플리케이션을 사용하여 SMB 공유와 연결된 LUN 간에 ODX 복사 오프로드를 사용하여 파일을 원활하게 복사 또는 이동할 수 있습니다.

- Hyper-V는 ODX 복사 오프로드를 위한 몇 가지 추가 사용 사례를 제공합니다.

- Hyper-V에서 ODX 복사 오프로드 패스스루를 사용하여 VHD(가상 하드 디스크) 파일 내부 또는 VHD 파일 간에 데이터를 복사하거나, 매핑된 SMB 공유와 동일한 클러스터 내에서 연결된 iSCSI LUN 간에 데이터를 복사할 수 있습니다.

이렇게 하면 게스트 운영 체제에서 복제본을 기본 스토리지로 전달할 수 있습니다.

- 고정 크기의 VHD를 생성할 때 ODX는 잘 알려진 제로화 토큰을 사용하여 0으로 디스크를 초기화하는 데 사용됩니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드가 가상 머신 스토리지 마이그레이션에 사용됩니다.



Hyper-V를 사용한 ODX 복사 오프로드 패스쓰루 사용 사례를 활용하려면 게스트 운영 체제가 ODX를 지원하고, 게스트 운영 체제 디스크는 ODX를 지원하는 스토리지(SMB 또는 SAN)를 통해 지원되는 SCSI 디스크여야 합니다. 게스트 운영 체제의 IDE 디스크는 ODX 패스쓰루를 지원하지 않습니다.

#### ONTAP SMB 서버에서 ODX 활성화 또는 비활성화

스토리지 가상 시스템(SVM)에서 ODX를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본적으로 SMB 3.0도 사용하도록 설정된 경우 ODX 복사 오프로드를 지원합니다.

시작하기 전에

SMB 3.0을 활성화해야 합니다.

이 작업에 대해

SMB 3.0을 비활성화하면 ONTAP도 SMB ODX를 비활성화합니다. SMB 3.0을 다시 설정하는 경우 SMB ODX를 수동으로 다시 설정해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

| ODX 복사 오프로드 기능을 사용하려면... | 명령 입력...                                                                          |
|--------------------------|-----------------------------------------------------------------------------------|
| 활성화됨                     | 'vserver cifs options modify -vserver vserver_name -copy -offload -enabled true'  |
| 사용 안 함                   | 'vserver cifs options modify -vserver vserver_name -copy -offload -enabled false' |

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 SVM VS1 에서 ODX 복사 오프로드를 활성화합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

관련 정보

## 사용 가능한 서버 옵션

자동 위치로 **SMB** 자동 노드 조회를 제공하여 클라이언트 응답 시간을 단축합니다

자동 위치 지정을 통해 **ONTAP SMB** 자동 노드 참조를 제공하여 클라이언트 응답 시간을 개선하는 방법에 대해 알아보세요.

자동 위치에서는 SMB 자동 노드 조회를 사용하여 스토리지 가상 시스템(SVM)에서 SMB 클라이언트 성능을 높입니다. 자동 노드 조수는 요청 클라이언트를 데이터가 상주하는 볼륨을 호스팅하는 노드 SVM의 LIF로 자동으로 리디렉션하여 클라이언트 응답 시간을 향상할 수 있습니다.

SMB 클라이언트가 SVM에서 호스팅된 SMB 공유에 연결할 경우, 요청된 데이터를 소유하지 않은 노드에 있는 LIF를 사용하여 연결할 수 있습니다. 클라이언트가 연결된 노드는 클러스터 네트워크를 사용하여 다른 노드가 소유한 데이터에 액세스합니다. SMB 연결이 요청된 데이터를 포함하고 있는 노드에 있는 LIF를 사용하면 클라이언트에서 더 빠른 응답 시간을 경험할 수 있습니다.

- ONTAP는 Microsoft DFS 조회를 사용하여 SMB 클라이언트에 네임스페이스에서 요청된 파일 또는 폴더가 다른 곳에 호스팅된다는 사실을 알리는 이 기능을 제공합니다.

노드가 데이터를 포함하는 노드에 SVM LIF가 있다고 판단하면 노드를 전문의에게 의뢰합니다.

- IPv4 및 IPv6 LIF IP 주소에 대해 자동 노드 조회가 지원됩니다.
- 조인은 클라이언트가 연결되는 공유 루트의 위치를 기반으로 합니다.
- SMB 협상 중에 불합격입니다.

연결이 설정되기 전에 의뢰합니다. ONTAP가 SMB 클라이언트를 타겟 노드로 참조하면 연결이 연결되고 클라이언트는 해당 시점부터 참조된 LIF 경로를 통해 데이터에 액세스합니다. 이렇게 하면 클라이언트가 데이터에 더 빠르게 액세스할 수 있고 추가 클러스터 통신을 피할 수 있습니다.



공유가 여러 연결 지점을 거치는 경우 일부 접합부가 다른 노드에 포함된 볼륨에 연결되는 경우 공유 내의 데이터가 여러 노드로 분산됩니다. ONTAP는 공유의 루트에 대해 로컬인 조회를 제공하므로 ONTAP는 이러한 비 로컬 볼륨에 포함된 데이터를 검색하기 위해 클러스터 네트워크를 사용해야 합니다. 이러한 유형의 네임스페이스 아키텍처를 사용하면 자동 노드 조회가 성능에 큰 이점을 제공하지 않을 수 있습니다.

데이터를 호스팅하는 노드에 사용 가능한 LIF가 없는 경우 ONTAP은 클라이언트가 선택한 LIF를 사용하여 연결을 설정합니다. SMB 클라이언트가 파일을 연 후에는 동일한 참조 연결을 통해 계속 파일에 액세스합니다.

어떤 이유로든 CIFS 서버가 조회를 수행할 수 없는 경우 SMB 서비스가 중단되지 않습니다. SMB 연결은 자동 노드 조회가 활성화되지 않은 것처럼 설정됩니다.

관련 정보

[Microsoft 원격 복제 성능 향상](#)

**ONTAP SMB** 서버에서 자동 노드 참조를 사용하기 위한 요구 사항 및 지침

SMB 자동 노드 조회를 사용하려면 `_autolocation_` 이라고도 하며, 이 기능을 지원하는 ONTAP 버전을 비롯한 특정 요구 사항을 알고 있어야 합니다. 또한 지원되는 SMB 프로토콜 버전 및 기타 특정 특별 지침에 대해서도 알아야 합니다.

## ONTAP 버전 및 라이선스 요구 사항

- 클러스터의 모든 노드는 자동 노드 조회를 지원하는 ONTAP 버전을 실행하고 있어야 합니다.
- 자동 위치 정보를 사용하려면 SMB 공유에서 Widelink를 활성화해야 합니다.
- CIFS에 대한 라이선스가 있어야 하며 SMB 서버가 SVM에 있어야 합니다. SMB 라이선스는 에 포함되어 ["ONTAP 1 을 참조하십시오"](#) 있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

## SMB 프로토콜 버전 요구 사항

- SVM의 경우 ONTAP는 모든 SMB 버전에서 자동 노드 조회를 지원합니다.

## SMB 클라이언트 요구 사항

ONTAP에서 지원하는 모든 Microsoft 클라이언트는 SMB 자동 노드 조회를 지원합니다.

상호 운용성 매트릭스에는 ONTAP에서 지원하는 Windows 클라이언트에 대한 최신 정보가 포함되어 있습니다.

["NetApp 상호 운용성 매트릭스 툴"](#)

## 데이터 LIF 요구사항

데이터 LIF를 SMB 클라이언트를 위한 잠재 고객으로 사용하려면 NFS와 CIFS를 모두 사용하도록 설정된 데이터 LIF를 생성해야 합니다.

타겟 노드에 NFS 프로토콜에만 사용하도록 설정된 데이터 LIF가 있거나 SMB 프로토콜에 대해서만 사용하도록 설정된 데이터 LIF가 있는 경우 자동 노드 조회가 작동하지 않을 수 있습니다.

이 요구 사항이 충족되지 않으면 데이터 액세스가 영향을 받지 않습니다. SMB 클라이언트는 클라이언트가 SVM에 연결할 때 사용한 원래 LIF를 사용하여 공유를 매핑합니다.

## 참조된 SMB 연결을 만들 때 NTLM 인증 요구 사항

NTLM 인증은 CIFS 서버가 포함된 도메인 및 자동 노드 조회를 사용하려는 클라이언트가 포함된 도메인에서 허용되어야 합니다.

SMB 서버는 조회를 수행할 때 Windows 클라이언트에 대한 IP 주소를 참조합니다. NTLM 인증은 IP 주소를 사용하여 연결할 때 사용되므로 Kerberos 인증은 참조된 연결에 대해 수행되지 않습니다.

이는 Kerberos(service/netbios name, service/FQDN) 형태의 서비스 주체 이름을 Windows 클라이언트가 생성할 수 없기 때문에 클라이언트가 Kerberos 티켓을 서비스에 요청할 수 없다는 뜻입니다.

## 홈 디렉토리 기능과 함께 자동 노드 조회를 사용하는 지침

공유가 홈 디렉토리 공유 속성을 사용하여 구성된 경우 홈 디렉토리 구성에 대해 하나 이상의 홈 디렉토리 검색 경로가 구성될 수 있습니다. 검색 경로는 SVM 볼륨을 포함하는 각 노드에 포함된 볼륨을 가리킬 수 있습니다. 클라이언트는 추천을 받으며 액티브 로컬 데이터 LIF가 사용 가능한 경우 홈 사용자의 홈 디렉토리에 로컬로 연결된 참조된 LIF를 통해 연결됩니다.

SMB 1.0 클라이언트가 자동 노드 조회가 설정된 동적 홈 디렉토리에 액세스하는 경우 지침이 있습니다. 이는 SMB 1.0 클라이언트가 인증을 받기 전에 자동 노드 조회를 필요로 하기 때문입니다. 이는 SMB 서버가 사용자 이름을 가지기 전입니다. 그러나 SMB 1.0 클라이언트에서 SMB 홈 디렉토리 액세스가 올바르게 작동하는 경우는 다음과 같습니다.

- SMB 홈 디렉토리는 ""%w"(Windows 사용자 이름) 또는 ""%u"(매핑된 UNIX 사용자 이름)와 같은 단순 이름을 사용하도록 구성되어 있으며 ""%d\%w"(domain-name\user-name)와 같은 도메인 이름 스타일 이름은 사용하지 않습니다.
- 홈 디렉토리 공유를 생성할 때 CIFS 홈 디렉토리 공유 이름은 ""home""과 같은 정적 이름이 아니라 변수("""%w" 또는 ""%u")로 구성됩니다.

SMB 2.x 및 SMB 3.0 클라이언트의 경우 자동 노드 조회를 사용하여 홈 디렉토리에 액세스할 때 특별한 지침이 없습니다.

기존에 연결된 연결이 있는 **CIFS** 서버에서 자동 노드 조회를 해제하는 지침입니다

이 옵션이 설정된 후 자동 노드 조회를 사용하지 않도록 설정하면 현재 참조된 LIF에 연결된 클라이언트가 계속 연결된 상태로 유지됩니다. ONTAP은 DFS 조회를 SMB 자동 노드 조정의 메커니즘으로 사용하므로, 클라이언트의 캐시된 DFS 참조 시간이 초과될 때까지 이 옵션을 비활성화한 후에 클라이언트가 참조된 LIF에 다시 연결할 수도 있습니다. 자동 노드 조회를 지원하지 않는 ONTAP 버전으로 되돌리는 경우에도 마찬가지입니다. 클라이언트는 클라이언트의 캐시에서 DFS 참조 시간이 초과될 때까지 계속 조회를 사용합니다.

Autolocation은 SMB 자동 노드 조회를 사용하여 SVM의 데이터 볼륨을 소유하는 노드의 LIF에 클라이언트를 위탁하여 SMB 클라이언트의 성능을 높입니다. SMB 클라이언트가 SVM에서 호스팅되는 SMB 공유에 연결할 경우, 요청된 데이터를 소유하지 않고 클러스터 인터커넥트 네트워크를 사용하여 데이터를 검색하는 노드에서 LIF를 사용하여 연결할 수 있습니다. SMB 연결이 요청된 데이터를 포함하고 있는 노드에 있는 LIF를 사용하는 경우 클라이언트는 더 빠른 응답 시간을 경험할 수 있습니다.

ONTAP은 Microsoft DFS(분산 파일 시스템) 조회를 사용하여 SMB 클라이언트에 네임스페이스에서 요청된 파일 또는 폴더가 다른 곳에 호스팅된다는 사실을 알려 주는 이 기능을 제공합니다. 노드가 데이터를 포함하는 노드에 SVM LIF가 있다고 판단하면 노드를 전문의에게 의뢰합니다. 조인은 클라이언트가 연결되는 공유 루트의 위치를 기반으로 합니다.

SMB 협상 중에 불합격입니다. 연결이 설정되기 전에 의뢰합니다. ONTAP가 SMB 클라이언트를 타겟 노드로 참조하면 연결이 연결되고 클라이언트는 해당 시점부터 참조된 LIF 경로를 통해 데이터에 액세스합니다. 이렇게 하면 클라이언트가 데이터에 더 빠르게 액세스할 수 있고 추가 클러스터 통신을 피할 수 있습니다.

**Mac OS** 클라이언트에서 자동 노드 조회를 사용하는 방법에 대한 지침입니다

Mac OS X 클라이언트는 Microsoft의 DFS(Distributed File System)를 지원하지만 SMB 자동 노드 조회를 지원하지 않습니다. Windows 클라이언트는 SMB 공유에 연결하기 전에 DFS 참조 요청을 합니다. ONTAP은 요청된 데이터를 호스팅하는 동일한 노드에 있는 데이터 LIF를 지칭하여 클라이언트 응답 시간을 개선합니다. Mac OS는 DFS를 지원하지만 Mac OS 클라이언트는 이 영역의 Windows 클라이언트와 정확히 작동하지 않습니다.

관련 정보

- [서버에서 동적 홈 디렉토리를 활성화하는 방법에 대해 알아보세요.](#)
- ["네트워크 관리"](#)
- ["NetApp 상호 운용성 매트릭스 툴"](#)

**ONTAP SMB** 자동 노드 참조 지원

SMB 자동 노드 조회를 활성화하기 전에 특정 ONTAP 기능이 조회를 지원하지 않는다는 점을 알아야 합니다.

- 다음 유형의 볼륨은 SMB 자동 노드 조회를 지원하지 않습니다.
  - 로드 공유 미러의 읽기 전용 구성원입니다

◦ 데이터 보호 미러의 타겟 볼륨입니다

- 노드 조회가 LIF 이동 옆에서 이동하지 않습니다.

클라이언트가 SMB 2.x 또는 SMB 3.0 연결을 통해 위탁된 연결을 사용 중이고 데이터 LIF가 중단 없이 이동되는 경우, LIF가 더 이상 데이터에 로컬이 아니어도 클라이언트는 계속 동일한 연결 연결을 사용합니다.

- 노드 조회가 볼륨 이동 옆에서 이동하지 않습니다.

클라이언트가 SMB 연결을 통해 참조된 연결을 사용하고 있고 볼륨 이동이 발생하는 경우, 클라이언트는 볼륨이 데이터 LIF와 같은 노드에 더 이상 존재하지 않더라도 계속해서 동일한 연결 연결을 사용합니다.

#### ONTAP SMB 자동 노드 참조 활성화 또는 비활성화

SMB 자동 노드 조회를 활성화하여 SMB 클라이언트 액세스 성능을 높일 수 있습니다. ONTAP가 SMB 클라이언트에 조회를 하지 않도록 하려면 자동 노드 조회를 사용하지 않도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버는 SVM(스토리지 가상 머신)에서 구성 및 실행해야 합니다.

이 작업에 대해

SMB 자동 노드 조회 기능은 기본적으로 비활성화되어 있습니다. 필요에 따라 각 SVM에서 이 기능을 활성화 또는 비활성화할 수 있습니다.

이 옵션은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 필요에 따라 SMB 자동 노드 조회를 설정하거나 해제합니다.

| SMB 자동 노드 조회를 원하는 경우... | 다음 명령을 입력합니다...                                                                |
|-------------------------|--------------------------------------------------------------------------------|
| 활성화됨                    | 'vserver cifs options modify -vserver vserver_name -is-referral-enabled true'  |
| 사용 안 함                  | 'vserver cifs options modify -vserver vserver_name -is-referral-enabled false' |

옵션 설정은 새 SMB 세션에 적용됩니다. 기존 연결이 있는 클라이언트는 기존 캐시 시간 제한이 만료될 때만 노드 조회를 사용할 수 있습니다.

3. 'Set-Privilege admin'으로 설정

관련 정보

[사용 가능한 서버 옵션](#)

통계를 사용하여 **ONTAP SMB** 자동 노드 참조 활동을 모니터링합니다.

SMB 연결 조회 수를 확인하려면 '통계' 명령어를 사용해 자동 노드 조회 활동을 모니터링할 수 있다. 조회를 모니터링하면 공유를 호스팅하는 노드에서 자동 조회가 접속을 찾는 범위와 CIFS 서버의 공유에 대한 로컬 액세스를 더 잘 제공할 수 있도록 데이터 LIF를 재분산해야 하는지 여부를 확인할 수 있습니다.

이 작업에 대해

"CIFS" 객체는 SMB 자동 노드 조회를 모니터링할 때 유용한 고급 권한 수준의 여러 카운터를 제공합니다.

- 'node\_referral\_발급'

공유 루트의 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 클라이언트가 연결된 후 공유 루트 노드에 대한 조회를 실행한 클라이언트 수입입니다.

- 'node\_referral\_local'

공유 루트를 호스팅하는 동일한 노드에서 호스팅되는 LIF를 사용하여 연결된 클라이언트의 수입입니다. 로컬 액세스는 일반적으로 최적의 성능을 제공합니다.

- 'node\_referral\_not\_possible'

공유 루트의 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 연결한 후 공유 루트를 호스팅하는 노드에 아직 위탁하지 않은 클라이언트 수입입니다. 이는 공유 루트의 노드에 대한 활성 데이터 LIF를 찾을 수 없기 때문입니다.

- 'node\_referral\_remote'

공유 루트를 호스팅하는 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 연결된 클라이언트 수입입니다. 원격 액세스로 인해 성능이 저하될 수 있습니다.

특정 기간(샘플)에 대한 데이터를 수집 및 확인하여 스토리지 가상 시스템(SVM)에 대한 자동 노드 참조 통계를 모니터링할 수 있습니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 성능 추세를 파악할 수 있습니다.



'통계' 명령을 통해 수집한 정보를 평가하고 사용하려면 사용자 환경에서 클라이언트의 분포를 이해해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. '통계' 명령어를 이용하여 자동 노드 조회 통계를 볼 수 있다.

이 예제에서는 샘플링된 기간에 대한 데이터를 수집하고 확인하여 자동 노드 참조 통계를 보여 줍니다.

- a. 'stantics start-object cifs-instance vs1-sample-id sample1' 컬렉션을 시작합니다

```
Statistics collection is being started for Sample-id: sample1
```

- b. 원하는 수집 시간이 경과할 때까지 기다립니다.

c. '스타티틱스 스톱-시료-ID sample1' 컬렉션을 중단한다

```
Statistics collection is being stopped for Sample-id: sample1
```

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 ["ONTAP 명령 참조입니다"](#).

d. 자동 노드 참조 통계: 'stattics show -sample-id sample1-counter \* node \*'를 봅니다

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

| Counter                    | Value |
|----------------------------|-------|
| node_name                  | node1 |
| node_referral_issued       | 0     |
| node_referral_local        | 1     |
| node_referral_not_possible | 2     |
| node_referral_remote       | 2     |
| ...                        |       |
| node_name                  | node2 |
| node_referral_issued       | 2     |
| node_referral_local        | 1     |
| node_referral_not_possible | 0     |
| node_referral_remote       | 2     |
| ...                        |       |

SVM VS1에 참여하는 모든 노드의 카운터를 출력합니다. 이 예에서는 자동 노드 조회 통계와 관련된 출력 필드만 제공합니다.

에 대한 자세한 내용은 `statistics show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

- [통계를 표시합니다](#)
- ["성능 모니터링 설정"](#)

**Windows** 클라이언트를 사용하여 클라이언트 측 **ONTAP SMB** 자동 노드 참조 정보 모니터링

클라이언트의 관점에서 어떤 조회를 수행할지 결정하려면 Windows `dutil.exe`를 사용할 수 있습니다.



Windows 7 이상의 클라이언트에서 사용할 수 있는 RSAT(원격 서버 관리 도구) 키트에는 Dsutil.exe가 포함되어 있습니다. 이 유틸리티를 사용하면 추천 캐시의 내용에 대한 정보를 표시하고 클라이언트가 현재 사용하고 있는 각 추천 정보에 대한 정보를 볼 수 있습니다. 이 유틸리티를 사용하여 클라이언트의 조희 캐시를 지울 수도 있습니다. 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

액세스 기반 열거를 사용하여 공유에 대한 폴더 보안을 제공합니다

액세스 기반 열거를 통해 공유에 **ONTAP SMB** 폴더 보안 제공

SMB 공유에서 ABE(Access-Based Enumeration)를 사용하면 공유 내에 포함된 폴더나 파일에 액세스할 수 있는 권한이 없는 사용자(개인 또는 그룹 권한 제한 사용 여부)는 공유 자체가 표시되더라도 공유 리소스가 해당 환경에 표시되지 않습니다.

일반 공유 속성을 사용하면 공유에 포함된 파일 또는 폴더를 보거나 수정할 수 있는 권한이 있는 사용자(개별 또는 그룹)를 지정할 수 있습니다. 그러나 공유 내의 폴더나 파일이 액세스 권한이 없는 사용자에게 표시되는지 여부를 제어할 수는 없습니다. 이러한 폴더 또는 공유 내의 파일 이름이 개발 중인 고객 또는 제품 이름과 같은 중요한 정보를 설명하는 경우 문제가 발생할 수 있습니다.

ABE(Access-Based Enumeration)는 공유 속성을 확장하여 공유 내의 파일 및 폴더 열거를 포함합니다. 따라서 ABE를 사용하면 사용자 액세스 권한에 따라 공유 내의 파일 및 폴더 표시를 필터링할 수 있습니다. 즉, 공유 자체는 모든 사용자에게 표시되지만 공유 내의 파일과 폴더는 지정된 사용자에게 표시되거나 숨겨집니다. 업무 공간의 중요한 정보를 보호하는 것 외에도, ABE를 사용하면 전체 콘텐츠 범위에 액세스할 필요가 없는 사용자에게 혜택을 제공하기 위해 대규모 디렉터리 구조의 표시를 단순화할 수 있습니다. 예를 들어 공유 자체는 모든 사용자에게 표시되지만 공유 내의 파일과 폴더는 표시하거나 숨길 수 있습니다.

에 대해 자세히 알아보십시오 ["SMB/CIFS 액세스 기반 열거 사용 시 성능에 미치는 영향"](#).

**ONTAP SMB** 공유에서 액세스 기반 열거 활성화 또는 비활성화

SMB 공유에서 ABE(Access-Based Enumeration)를 설정하거나 해제하여 사용자가 액세스 권한이 없는 공유 리소스를 볼 수 없도록 하거나 허용할 수 있습니다.

이 작업에 대해

기본적으로 ABE는 비활성화되어 있습니다.

단계

- 1. 다음 작업 중 하나를 수행합니다.

| 원하는 작업             | 명령 입력...                                                                                                                                                                                                                                                                                |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 새 공유에서 ABE를 활성화합니다 | <code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</code> SMB 공유를 생성할 때 추가 공유 설정 및 추가 공유 속성을 지정할 수 있습니다. 에 대한 자세한 내용은 <code>vserver cifs share create</code> <a href="#">"ONTAP 명령 참조입니다"</a> 을 참조하십시오. |

| 원하는 작업               | 명령 입력...                                                                                                                                                                       |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 기존 공유에서 ABE를 활성화합니다  | 'vserver cifs 공유 속성 add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration' 기존 공유 속성은 보존됩니다. ABE 공유 속성은 기존 공유 속성 목록에 추가됩니다.               |
| 기존 공유에서 ABE를 비활성화합니다 | 'vserver cifs share properties remove - vserver vserver_name -share-name share_name -share -properties access-based-enumeration' 다른 공유 속성은 보존됩니다. 공유 속성 목록에서 ABE 공유 속성만 제거됩니다. |

2. 'vserver cifs share show' 명령을 사용하여 공유 구성이 올바른지 확인합니다.

예

다음 예에서는 SVM VS1 에서 /sales 경로를 사용하여 "sale"이라는 이름의 ABE SMB 공유를 생성합니다. 공유는 공유 속성으로 '액세스 기반 열거'로 만들어집니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

Vserver: vs1
Share: sales
CIFS Server NetBIOS Name: VS1
Path: /sales
Share Properties: access-based-enumeration
 oplocks
 browsable
 changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

다음 예제에서는 "data2"라는 SMB 공유에 "액세스 기반 열거" 공유 속성을 추가합니다.

```
cluster1::> vservers cifs share properties add -vservers vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vservers cifs share show -vservers vs1 -share-name data2 -fields
share-name,share-properties
server share-name share-properties

vs1 data2 oplocks,browsable,changeNotify,access-based-enumeration
```

## 관련 정보

### 기존 주식에 주식 속성 추가 또는 제거

**ONTAP SMB** 공유에서 **Windows** 클라이언트의 액세스 기반 열거 활성화 또는 비활성화

Windows 클라이언트에서 SMB 공유에 대해 ABE(액세스 기반 열거)를 설정하거나 해제할 수 있습니다. 그러면 CIFS 서버에 연결하지 않고도 이 공유 설정을 구성할 수 있습니다.



새 버전의 Windows Server 및 Windows 클라이언트에서는 abecmd 유틸리티를 사용할 수 없습니다. 이 제품은 Windows Server 2008의 일부로 출시되었습니다. 2020년 1월 14일에 Windows Server 2008에 대한 지원이 종료되었습니다.

## 단계

1. ABE를 지원하는 Windows 클라이언트에서 'abecmd[/enable/disable][server cifs\_server\_name[/allshare\_name]]' 명령을 입력합니다

"abecmd" 명령에 대한 자세한 내용은 Windows 클라이언트 설명서를 참조하십시오.

## NFS 및 SMB 파일 및 디렉토리 명명 종속성

**ONTAP NFS** 및 **SMB** 파일 및 디렉토리 명명 종속성에 대해 알아보세요.

파일 및 디렉토리 명명 규칙은 ONTAP 클러스터 및 클라이언트의 언어 설정과 함께 네트워크 클라이언트의 운영 체제 및 파일 공유 프로토콜에 따라 다릅니다.

운영 체제 및 파일 공유 프로토콜에는 다음이 결정됩니다.

- 문자 파일 이름에 사용할 수 있습니다
- 파일 이름의 대/소문자 구분

ONTAP는 ONTAP 릴리즈별 파일, 디렉토리 및 qtree 이름에서 멀티바이트 문자를 지원합니다.

**ONTAP SMB** 파일 또는 디렉토리 이름에 유효한 문자에 대해 알아보세요.

다른 운영 체제를 사용하는 클라이언트에서 파일 또는 디렉토리에 액세스하는 경우 두 운영 체제 모두에서 유효한 문자를 사용해야 합니다.

예를 들어 UNIX를 사용하여 파일 또는 디렉토리를 생성하는 경우 MS-DOS 파일 또는 디렉토리 이름에 콜론이 허용되지 않으므로 이름에 콜론(:)을 사용하지 마십시오. 유효한 문자의 제한 사항은 운영 체제마다 다르므로 금지된 문자에 대한 자세한 내용은 클라이언트 운영 체제 설명서를 참조하십시오.

다중 프로토콜 환경에서 **ONTAP SMB** 파일 및 디렉토리 이름의 대소문자 구분

파일 및 디렉토리 이름은 NFS 클라이언트의 경우 대/소문자를 구분하며, SMB 클라이언트의 경우 대/소문자를 구분하지 않지만 대/소문자를 구분합니다. SMB 공유를 생성하는 동안 그리고 공유 내의 데이터에 액세스할 때 경로를 지정할 때 취해야 할 조치와 멀티 프로토콜 환경에 미치는 영향을 이해해야 합니다.

SMB 클라이언트가 testdir라는 디렉토리를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 testdir로 표시합니다. 그러나 SMB 사용자가 나중에 디렉터리 이름 testdir을 만들려고 하면 해당 이름이 SMB 클라이언트에 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 "testdir"이라는 디렉토리를 생성할 경우 NFS 및 SMB 클라이언트는 다음과 같이 디렉토리 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 디렉토리 이름이 대/소문자를 구분하기 때문에 디렉토리 이름이 생성될 때 testdir와 testDir 같은 두 디렉토리 이름을 모두 볼 수 있습니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 디렉토리를 구분합니다. 한 디렉토리에 기본 파일 이름이 있습니다. 추가 디렉토리에는 8.3 파일 이름이 할당됩니다.
  - SMB 클라이언트에서는 testdir과 testDI~1이 표시됩니다.
  - ONTAP는 두 디렉토리를 구분하기 위해 'TESTDI~1' 디렉토리 이름을 생성한다.

이 경우 SVM(스토리지 가상 머신)에서 공유를 생성하거나 수정하는 동안 공유 경로를 지정할 때 8.3 이름을 사용해야 합니다.

마찬가지로 SMB 클라이언트가 test.txt를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 test.txt로 표시합니다. 그러나 SMB 사용자가 나중에 Test.txt를 생성하려고 하면 SMB 클라이언트에 해당 이름이 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 Test.txt라는 파일을 만들면 NFS 및 SMB 클라이언트는 다음과 같이 파일 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 파일 이름이 대/소문자를 구분하기 때문에 이름이 test.txt와 Test.txt로 만들어지면 두 파일 이름이 모두 표시됩니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 파일을 구분합니다. 한 파일에 기본 파일 이름이 있습니다. 8.3 파일 이름이 추가로 할당됩니다.
  - SMB 클라이언트의 경우 test.txt와 test~1.TXT가 표시됩니다.
  - ONTAP는 두 파일을 구별하기 위해 'test~1.TXT' 파일 이름을 만듭니다.



SVM CIFS 문자 매핑 명령을 사용하여 문자 매핑을 설정하거나 수정한 경우 일반적으로 대/소문자를 구분하지 않는 Windows 조회가 대/소문자를 구분합니다.

**ONTAP SMB** 파일 및 디렉토리 이름 생성에 대해 알아보세요

ONTAP는 SMB 클라이언트에서 액세스할 수 있는 디렉토리인 원래 긴 이름과 8.3 형식의 이름을 사용하여 파일 또는 디렉토리의 이름을 두 개 생성하고 유지합니다.

파일 또는 디렉토리 이름이 8자 이름 또는 3자 확장자 제한(파일의 경우)을 초과하는 경우, ONTAP는 다음과 같이 8.3

형식 이름을 생성합니다.

- 이름이 6자를 초과하면 원본 파일 또는 디렉터리 이름이 6자로 잘립니다.
- 잘려서 더 이상 고유하지 않은 파일 또는 디렉터리 이름에 물결표(~)와 숫자(1 - 5)를 추가합니다.

비슷한 이름이 5개 이상 있어 숫자가 부족하면 원래 이름과 아무런 관계가 없는 고유한 이름이 만들어집니다.

- 파일의 경우 파일 확장명이 3자로 잘립니다.

예를 들어, NFS 클라이언트가 'specifications.html'이라는 파일을 생성할 경우 ONTAP에서 생성한 8.3 형식 파일 이름은 'specif~1.htm'입니다. 이 이름이 이미 있는 경우 ONTAP에서는 파일 이름 끝에 다른 번호를 사용합니다. 예를 들어, NFS 클라이언트가 'specifications\_new.html'이라는 다른 파일을 만들 경우 'specifications\_new.html'의 8.3 형식은 'specif~2.htm'입니다.

## ONTAP SMB 다중 바이트 파일, 디렉터리 및 **qtree** 이름에 대해 알아보세요

ONTAP 9.5부터 4바이트 UTF-8 인코딩 이름을 지원하므로 BMP(기본 다국어 플레인) 외부의 유니코드 보조 문자를 포함하는 파일, 디렉터리 및 트리 이름을 만들고 표시할 수 있습니다. 이전 릴리스에서는 이러한 보조 문자가 멀티 프로토콜 환경에서 올바르게 표시되지 않았습니다.

4바이트 UTF-8 인코딩된 이름을 지원하기 위해 새 `_utf8mb4_language` 코드를 "vserver" 및 "volume" 명령 제품군에 사용할 수 있습니다.

다음 방법 중 하나로 새 볼륨을 만들어야 합니다.

- 볼륨 '-language' 옵션을 명시적으로 설정하는 것은 'volume create-language utf8mb4{...}'입니다
- 옵션을 위해 생성되거나 수정된 SVM에서 볼륨 '-language' 옵션을 상속합니다: 'vserver[create|modify] -language utf8mb4{...}"volume create{...}'
- ONTAP 9.6 이하 버전에서는 utf8mb4 지원을 위한 기존 볼륨을 수정할 수 없습니다. 새로운 utf8mb4 지원 볼륨을 생성한 다음 클라이언트 기반 복사 툴을 사용하여 데이터를 마이그레이션해야 합니다.

utf8mb4 지원을 위해 SVM을 업데이트할 수 있지만 기존 볼륨에 원래 언어 코드가 유지됩니다.

ONTAP 9.7P1 이상을 사용 중인 경우 지원 요청을 통해 utf8mb4에 대한 기존 볼륨을 수정할 수 있습니다. 자세한 내용은 을 참조하십시오 ["ONTAP에서 생성한 후 볼륨 언어를 변경할 수 있습니까?"](#).

- ONTAP 9.8부터 를 사용할 수 있습니다 [-language <Language code>] 볼륨 언어를 \*.utf-8에서 utf8mb4로 변경하는 매개 변수입니다. 볼륨의 언어를 변경하려면 에 문의하십시오 ["NetApp 지원"](#).



4바이트 UTF-8 문자를 사용하는 LUN 이름은 현재 지원되지 않습니다.

- 유니코드 문자 데이터는 일반적으로 16비트 UTF-16(Unicode Transformation Format)을 사용하는 Windows 파일 시스템 응용 프로그램과 8비트 UTF-8(Unicode Transformation Format)을 사용하는 NFS 파일 시스템에 표시됩니다.

ONTAP 9.5 이전 버전에서는 Windows 클라이언트에서 생성한 UTF-16 보조 문자를 포함한 이름이 다른 Windows 클라이언트에 올바르게 표시되었지만 NFS 클라이언트용 UTF-8로 올바르게 변환되지 않았습니다. 마찬가지로, 생성된 NFS 클라이언트에서 UTF-8 보완 문자를 사용하는 이름은 Windows 클라이언트의 UTF-16으로 올바르게 변환되지 않았습니다.

- ONTAP 9.4 이하를 실행하는 시스템에서 유효하거나 잘못된 보조 문자가 포함된 파일 이름을 만들면 ONTAP가 파일 이름을 거부하고 잘못된 파일 이름 오류를 반환합니다.

이 문제를 방지하려면 파일 이름에 BMP 문자만 사용하고 보조 문자는 사용하지 마십시오. 또는 ONTAP 9.5 이상으로 업그레이드하십시오.

ONTAP 9부터는 qtree 이름에 유니코드 문자가 허용됩니다.

- 'volume qtree' 명령군 또는 System Manager를 사용하여 qtree 이름을 설정하거나 수정할 수 있습니다.
- Qtree 이름에는 일본어 및 중국어 문자와 같은 유니코드 형식의 멀티바이트 문자가 포함될 수 있습니다.
- ONTAP 9.5 이전 버전에서는 BMP 문자(즉, 3바이트로 표현될 수 있는 문자)만 지원되었습니다.



ONTAP 9.5 이전의 릴리즈에서는 qtree 상위 볼륨의 연결 경로에 유니코드 문자가 있는 qtree 및 디렉토리 이름이 포함될 수 있습니다. 볼륨 표시 명령은 상위 볼륨에 UTF-8 언어 설정이 있는 경우 이러한 이름을 올바르게 표시합니다. 그러나 상위 볼륨 언어가 UTF-8 언어 설정 중 하나가 아닌 경우 junction-path의 일부 부분은 숫자 NFS 대체 이름을 사용하여 표시됩니다.

- 9.5 이상 릴리즈에서는 qtree 이름이 qtree 이름으로 지원되지만 qtree가 utf8mb4에 대해 활성화된 볼륨에 있습니다.

볼륨에서 **ONTAP SMB** 파일 이름 변환을 위한 문자 매핑 구성

NFS 클라이언트는 SMB 클라이언트 및 특정 Windows 애플리케이션에 유효하지 않은 문자를 포함하는 파일 이름을 생성할 수 있습니다. SMB 클라이언트가 유효하지 않은 NFS 이름의 파일에 액세스할 수 있도록 볼륨의 파일 이름 변환에 대한 문자 매핑을 구성할 수 있습니다.

이 작업에 대해

NFS 클라이언트가 생성한 파일을 SMB 클라이언트가 액세스할 때 ONTAP는 파일 이름을 찾습니다. 이름이 유효한 SMB 파일 이름이 아닌 경우(예: 포함된 콜론 ":" 문자가 있는 경우) ONTAP는 각 파일에 대해 유지되는 8.3 파일 이름을 반환합니다. 그러나 이로 인해 중요한 정보를 긴 파일 이름으로 인코딩하는 응용 프로그램에 문제가 발생합니다.

따라서 다른 운영 체제의 클라이언트 간에 파일을 공유하는 경우 두 운영 체제 모두에서 유효한 파일 이름에 문자를 사용해야 합니다.

그러나 SMB 클라이언트에 대해 유효한 파일 이름이 아닌 문자를 포함하는 파일 이름을 생성하는 NFS 클라이언트가 있는 경우, 잘못된 NFS 문자를 SMB 및 특정 Windows 애플리케이션이 허용하는 유니코드 문자로 변환하는 맵을 정의할 수 있습니다. 예를 들어, 이 기능은 CATIA MCAD 및 Mathematica 응용 프로그램과 이 요구 사항이 있는 다른 응용 프로그램을 지원합니다.

볼륨별로 문자 매핑을 구성할 수 있습니다.

볼륨에 문자 매핑을 구성할 때 다음 사항을 염두에 두어야 합니다.

- 문자 매핑이 교차점에 적용되지 않습니다.

각 집합 볼륨에 대해 문자 매핑을 명시적으로 구성해야 합니다.

- 올바르게 않거나 잘못된 문자를 나타내는 데 사용되는 유니코드 문자가 파일 이름에 일반적으로 나타나지 않는 문자인지 확인해야 합니다. 그렇지 않으면 원치 않는 매핑이 발생합니다.

예를 들어 콜론(:)을 하이픈(-)에 매핑하려고 하지만 파일 이름에 하이픈(-)이 올바르게 사용된 경우 ""a-b""라는 파일에 액세스하려는 Windows 클라이언트의 요청이 ""a:b""(원하는 결과가 아님)의 NFS 이름에 매핑됩니다.

- 문자 매핑을 적용한 후에도 매핑에 여전히 잘못된 Windows 문자가 포함되어 있으면 ONTAP는 Windows 8.3 파일 이름으로 다시 돌아갑니다.
- FPolicy 알림, NAS 감사 로그, 보안 추적 메시지에 매핑된 파일 이름이 표시됩니다.
- DP 유형의 SnapMirror 관계가 생성될 때 소스 볼륨의 문자 매핑이 대상 DP 볼륨에 복제되지 않습니다.
- 대소문자 구분: 매핑된 Windows 이름이 NFS 이름으로 전환되기 때문에 이름 조회는 NFS 의미를 따릅니다. 여기에는 NFS 조회가 대/소문자를 구분한다는 사실도 포함됩니다. 즉, 매핑된 공유에 액세스하는 응용 프로그램이 대/소문자를 구분하지 않는 Windows 동작에 의존해서는 안 됩니다. 그러나 8.3 이름은 사용할 수 있으며 대/소문자를 구분하지 않습니다.
- 부분 매핑 또는 잘못된 매핑: 이름을 매핑하여 디렉터리 열거("dir")를 수행하는 클라이언트로 반환하면 결과 유니코드 이름이 Windows 유효성을 검사합니다. 이름에 여전히 잘못된 문자가 있거나 Windows에 유효하지 않은 경우(예: "." 또는 공백으로 끝나는 경우) 잘못된 이름 대신 8.3 이름이 반환됩니다.

단계

1. 문자 매핑 구성: +

```
"vserver cifs character-mapping create -vserver_vserver_name_-volume_volume_name_-mapping_mapping_text_... 를 누릅니다
```

매핑은 ""로 구분된 소스-타겟 문자 쌍 목록으로 구성됩니다. 문자는 16진수를 사용하여 입력한 유니코드 문자입니다. 예: 3C:E03C. 를 누릅니다

콜론으로 구분된 각 mapping\_text 쌍의 첫 번째 값은 번역할 NFS 문자의 16진수 값이고 두 번째 값은 SMB가 사용하는 유니코드 값입니다. 매핑 쌍은 고유해야 합니다(일대일 매핑이 있어야 함).

- 소스 매핑+

다음 표에서는 소스 매핑에 사용할 수 있는 유니코드 문자 집합을 보여 줍니다.

를 누릅니다

| 유니코드 문자입니다 | 인쇄된 문자 | 설명                |
|------------|--------|-------------------|
| 0x01-0x19  | 해당 없음  | 인쇄할 수 없는 제어 문자입니다 |
| 0x5C       |        | 백슬래시              |
| 0x3A       | :      | 결장                |
| 0x2A       | *      | 별표                |
| 0x3F       | ?      | 물음표               |
| 0x22       | "      | 인용 부호가 있습니다       |

| 유니코드 문자입니다 | 인쇄된 문자 | 설명    |
|------------|--------|-------|
| 0x3C       | 를 누릅니다 | 보다 작음 |
| 0x3E       | 를 누릅니다 | 보다 큼  |
| 0x7C       |        |       |
| 세로선        | 0xB1   | ±     |

- 타겟 매핑

U+E0000...U+F8FF 범위의 유니코드 "전용 용도 영역"에서 대상 문자를 지정할 수 있습니다.

예

다음 명령을 실행하면 SVM(스토리지 가상 시스템) VS1 에서 "data"라는 이름의 볼륨에 대한 문자 매핑이 생성됩니다.

```
cluster1::> vservers cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vservers cifs character-mapping show
```

| Vserver | Volume Name | Character Mapping         |
|---------|-------------|---------------------------|
| vs1     | data        | 3c:e17c, 3e:f17d, 2a:f745 |

#### 관련 정보

[네임스페이스에서 데이터 볼륨을 만들고 관리하는 방법에 대해 알아보세요.](#)

#### SMB 파일 이름 변환을 위한 문자 매핑을 관리하기 위한 ONTAP 명령

FlexVol 볼륨에서 SMB 파일 이름 변환에 사용되는 파일 문자 매핑을 생성, 수정, 정보 표시 또는 삭제하여 문자 매핑을 관리할 수 있습니다.

| 원하는 작업                 | 이 명령 사용...                                       |
|------------------------|--------------------------------------------------|
| 새 파일 문자 매핑을 만듭니다       | 'vservers cifs character-mapping create'         |
| 파일 문자 매핑에 대한 정보를 표시합니다 | 'vservers cifs character-mapping show'           |
| 기존 파일 문자 매핑을 수정합니다     | 'vservers cifs character-mapping modify'를 참조하십시오 |
| 파일 문자 매핑을 삭제합니다        | 'vservers cifs character-mapping delete'         |



에 대한 자세한 내용은 `vserver cifs character-mapping` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

관련 정보

[볼륨에서 파일 이름 번역을 위한 문자 매핑 구성](#)

## NAS 데이터에 S3 클라이언트 액세스 제공

### ONTAP S3 멀티프로토콜 지원에 대해 알아보세요

ONTAP 9.12.1부터는 S3 프로토콜을 실행하는 클라이언트가 다시 포맷하지 않고 NFS 및 SMB 프로토콜을 사용하는 클라이언트에 제공되는 동일한 데이터에 액세스할 수 있도록 설정할 수 있습니다. 이 기능을 사용하면 NAS 클라이언트에서 NAS 데이터를 계속 처리하는 동시에 S3 애플리케이션(예: 데이터 마이닝 및 인공 지능)을 실행하는 S3 클라이언트에 오브젝트 데이터를 제공할 수 있습니다.

S3 멀티 프로토콜 기능은 다음과 같은 두 가지 사용 사례를 해결합니다.

#### 1. S3 클라이언트를 사용하여 기존 NAS 데이터에 액세스

기존 데이터가 기존 NAS 클라이언트(NFS 또는 SMB)를 사용하여 생성되었고 NAS 볼륨(FlexVol 또는 FlexGroup 볼륨)에 있는 경우 S3 클라이언트의 분석 도구를 사용하여 이 데이터에 액세스할 수 있습니다.

#### 2. NAS 및 S3 프로토콜을 모두 사용하여 I/O를 수행할 수 있는 최신 클라이언트를 위한 백엔드 스토리지

NAS와 S3 프로토콜을 모두 사용하여 동일한 데이터를 읽고 쓸 수 있는 Spark 및 Kafka와 같은 애플리케이션에 통합 액세스를 제공할 수 있습니다.

### S3 멀티프로토콜 지원 작동 방식

ONTAP 멀티프로토콜 지원을 통해 동일한 데이터 세트를 파일 계층 구조나 버킷의 객체로 표현할 수 있습니다. 이를 위해 ONTAP S3 클라이언트가 S3 객체 요청을 사용하여 NAS 스토리지에서 파일을 생성, 읽기, 삭제 및 열거할 수 있도록 하는 "S3 NAS 버킷"을 생성합니다. 이 매핑은 NAS 보안 구성을 준수하며, 파일 및 디렉터리 액세스 권한을 관찰하고 필요에 따라 보안 감사 추적에 기록합니다.

이 매핑은 지정된 NAS 디렉터리 계층을 S3 버킷으로 제공하여 수행됩니다. 디렉터리 계층의 각 파일은 이름이 매핑된 디렉터리에서 상대적으로 아래로 내려가는 S3 오브젝트로 표시되며 디렉터리 경계는 슬래시 문자("/")로 표시됩니다.

ONTAP 정의 S3 사용자는 NAS 디렉토리에 매핑되는 버킷에 정의된 버킷 정책에 따라 제어되는 이 스토리지에 액세스할 수 있습니다. 이를 위해서는 S3 사용자와 SMB/NFS 사용자 간에 매핑을 정의해야 합니다. SMB/NFS 사용자의 자격 증명은 NAS 권한 확인에 사용되며 이러한 액세스로 인해 발생하는 모든 감사 레코드에 포함됩니다.

SMB 또는 NFS 클라이언트가 파일을 생성하면 파일이 디렉토리에 즉시 배치되므로 데이터가 쓰기 전에 클라이언트에 표시됩니다. S3 클라이언트는 모든 데이터가 기록될 때까지 새 오브젝트가 네임스페이스에 표시되지 않는 다른 의미를 기대합니다. S3를 NAS 스토리지에 매핑하는 방식은 S3 의미를 사용하여 파일을 생성하므로 S3 생성 명령이 완료될 때까지 파일을 외부적으로 볼 수 없습니다.

### S3 NAS 버킷 용 데이터 보호

S3 NAS "버킷"은 단순히 S3 클라이언트를 위한 NAS 데이터의 매핑일 뿐이며, 표준 S3 버킷이 아닙니다. 따라서 NetApp SnapMirror S3 기능을 사용하여 S3 NAS 버킷을 보호할 필요가 없습니다. 대신 SnapMirror 비동기 볼륨

복제를 사용하여 S3 NAS 버킷이 포함된 볼륨을 보호할 수 있습니다. SnapMirror 동기 및 SVM 재해 복구는 지원되지 않습니다.

ONTAP 9.14.1부터, MetroCluster IP 및 FC 구성을 위한 미러링된 애그리게이트 및 미러링되지 않은 애그리게이트에서 S3 NAS 버킷이 지원됩니다.

에 대해 자세히 "[SnapMirror 비동기](#)"알아보십시오.

### S3 NAS 버킷에 대한 감사

S3 NAS 버킷은 기존의 S3 버킷이 아니므로 액세스 감사를 위해 S3 감사를 구성할 수 없습니다. 에 대해 자세히 알아보십시오 "[S3 감사](#)".

그럼에도 불구하고 S3 NAS 버킷에 매핑된 NAS 파일 및 디렉토리는 기존의 ONTAP 감사 절차를 사용하여 액세스 이벤트에 대한 감사를 수행할 수 있습니다. 따라서 S3 작업은 다음과 같은 예외를 제외하고 NAS 감사 이벤트를 트리거할 수 있습니다.

- S3 정책 구성(그룹 또는 버킷 정책)에 의해 S3 클라이언트 액세스가 거부되면 이벤트에 대한 NAS 감사가 시작되지 않습니다. 이는 SVM 감사 점검을 수행하기 전에 S3 권한을 확인하기 때문입니다.
- S3 GET 요청의 타겟 파일이 0 크기인 경우 0개의 콘텐츠가 GET 요청으로 반환되고 읽기 액세스가 기록되지 않습니다.
- S3 GET 요청의 타겟 파일이 사용자에게 통과 권한이 없는 폴더에 있는 경우 액세스 시도가 실패하고 이벤트가 기록되지 않습니다.

에 대해 자세히 알아보십시오 "[SVM에서 NAS 이벤트 감사](#)".

### 개체 다중 파트 업로드

ONTAP 9.16.1부터 기본 FlexGroup 볼륨에서 을 사용하도록 설정한 경우 S3 NAS 버킷에서 오브젝트 다중 부분 업로드가 "[고급 용량 밸런싱](#)"지원됩니다.

NAS 파일 스토리지에서 오브젝트 다중 부분 업로드를 사용하면 S3 프로토콜 클라이언트가 큰 오브젝트를 더 작은 부분으로 업로드할 수 있습니다. 개체 다중 파트 업로드에는 다음과 같은 이점이 있습니다.

- 객체를 병렬로 업로드할 수 있습니다.
- 업로드가 실패하거나 일시 중지되는 경우 아직 업로드되지 않은 부분만 업로드해야 합니다. 전체 개체의 업로드를 다시 시작할 필요가 없습니다.
- 개체 크기를 미리 알 수 없는 경우(예: 큰 개체가 아직 작성되는 경우), 클라이언트는 개체의 일부를 즉시 업로드하고 전체 개체가 생성된 후 업로드를 완료할 수 있습니다.



S3 NAS 버킷의 멀티파트 객체는 부분 크기가 아닌 정수 크기로 정렬되어야 합니다. 예를 들어, 파트는 4MB 또는 4GB 또는 이와 유사한 크기일 수 있습니다. 파트는 4.5MB 또는 4000.5MB와 같이 부분 크기 또는 MB 미만의 크기를 사용할 수 없습니다.

멀티파트 업로드는 다음 S3 작업을 지원합니다.

- AbortMultipartUpload 를 클릭합니다
- CompleteMultipartUpload를 클릭합니다
- CopyObject( ONTAP 9.17.1부터)

- CreateMultipartUpload 를 클릭합니다

ONTAP 9.17.1부터 CreateMultipartUpload는 태그 지정과 사용자 메타데이터 키/값 쌍을 지원합니다.

- ListMultipartUpload 를 클릭합니다
- 업로드 파트



부품 번호로 가져오기("PARTNUMBER=xx")는 S3 NAS 버킷에서 지원되지 않습니다. 대신 전체 개체가 반환됩니다.

### S3 및 NAS 상호 운용성

ONTAP S3 NAS 버킷은 여기에 나열된 기능을 제외한 표준 NAS 및 S3 기능을 지원합니다.

NAS 기능은 현재 S3 NAS 버킷에서 지원되지 않습니다

### FabricPool 용량 계층입니다

S3 NAS 버킷을 FabricPool의 용량 계층으로 구성할 수 없습니다.

현재 S3 NAS 버킷에서 지원되지 않는 S3 작업 및 기능

#### 작업

- BypassGovernanceRetention 을 참조하십시오
- DeleteBucketLifecycleConfiguration을 참조하십시오
- GetBuckLifecycleConfiguration 을 참조하십시오
- GetBucketObjectLockConfiguration 을 참조하십시오
- GetBuckketVersioning 을 참조하십시오
- GetObjectRetention을 참조하십시오
- ListBuckketVersioning을 참조하십시오
- ListObjectVersions 를 선택합니다
- PutBucketLifecycleConfiguration을 참조하십시오
- PutBucketVersioning을 참조하십시오
- PutObjectLockConfiguration 을 참조하십시오
- PutObjectRetention



이러한 S3 작업은 S3 NAS 버킷에서 S3를 사용하는 경우 특별히 지원되지 않습니다. 네이티브 S3 버킷을 사용할 때 이러한 작업은 다음과 "정상적으로 지원됩니다"같습니다.

### AWS 사용자 메타데이터

- ONTAP 9.17.1부터 다중 파트 객체가 포함된 메타데이터가 지원됩니다.
- ONTAP 9.16.1 버전부터 단일 파트 객체의 메타데이터를 지원합니다.
- ONTAP 9.15.1 이하 버전의 경우 S3 사용자 메타데이터의 일부로 수신된 키 값 쌍이 오브젝트 데이터와 함께 디스크에 저장되지 않습니다.

- ONTAP 9.15.1 이하 버전의 경우 접두사가 "x-amz-meta"인 요청 헤더는 무시됩니다.

## AWS 태그

- ONTAP 9.17.1부터 다중 파트 객체가 있는 태그가 지원됩니다.
- ONTAP 9.16.1 버전부터 단일 파트 객체를 포함하는 태그를 지원합니다.
- ONTAP 9.15.1 이하 버전의 PUT 객체 및 Multipart Initiate 요청에서는 접두사 "x-amz-tagging"이 있는 헤더가 무시됩니다.
- ONTAP 9.15.1 이하 버전의 경우 기존 파일에 대한 태그 업데이트 요청(?태깅 쿼리 문자열을 사용한 PUT, GET 및 삭제 요청)이 오류로 거부됩니다.

## 버전 관리

버킷 매핑 구성에서는 버전 관리를 지정할 수 없습니다.

- null이 아닌 버전 사양(versionId=xyz 쿼리 문자열)이 포함된 요청은 오류 응답을 받습니다.
- 버킷의 버전 관리 상태에 영향을 주는 요청은 오류와 함께 거부됩니다.

## ONTAP S3 클라이언트 액세스를 위한 NAS 데이터 요구 사항에 대해 알아보세요.

S3 액세스를 위해 NAS 파일 및 디렉토리를 매핑할 때 몇 가지 고유한 비호환성이 있다는 것을 이해하는 것이 중요합니다. S3 NAS 버킷을 사용하여 NAS 파일 계층을 서비스하기 전에 NAS 파일 계층을 조정해야 할 수 있습니다.

S3 NAS 버킷은 S3 버킷 구문을 사용하여 해당 디렉토리를 매핑함으로써 NAS 디렉토리에 대한 S3 액세스를 제공하며 디렉토리 트리의 파일은 오브젝트로 표시됩니다. 오브젝트 이름은 S3 버킷 구성에 지정된 디렉토리를 기준으로 파일의 슬래시로 구분된 경로 이름입니다.

이 매핑에서는 S3 NAS 버킷을 사용하여 파일 및 디렉토리를 제공할 경우 다음과 같은 몇 가지 요구사항이 발생합니다.

- S3 이름은 1024바이트로 제한되므로 S3를 사용하면 경로 이름이 더 긴 파일에 액세스할 수 없습니다.
- 파일 및 디렉터리 이름은 255자로 제한되므로 개체 이름은 255자 이하의 연속된 비슬래시('/') 문자를 사용할 수 없습니다
- 백슬래시('\') 문자로 구분된 SMB 경로 이름은 S3에 슬래시('/') 문자를 포함하는 객체 이름으로 표시됩니다.
- 일부 합법적인 S3 객체 이름 쌍은 매핑된 NAS 디렉토리 트리에서 공존할 수 없습니다. 예를 들어, 합법적인 S3 객체 이름인 "part1/part2"와 "part1/part2/part3"은 NAS 디렉토리 트리에서 동시에 존재할 수 없는 파일에 매핑됩니다. "part1/part2"는 첫 번째 이름에서는 파일이고 다른 이름에서는 디렉토리이기 때문입니다.
  - "part1/part2"가 기존 파일인 경우 S3에서 "part1/part2/part3"을 생성하는 데 실패합니다.
  - "part1/part2/part3"이 기존 파일인 경우 S3에서 "part1/part2"를 생성하거나 삭제하면 실패합니다.
  - 기존 오브젝트의 이름과 일치하는 S3 오브젝트 생성은 NAS에 있지만 정확히 일치해야 하는 기존 오브젝트 (버전이 지정되지 않은 버킷)를 대체합니다. 위의 예제에서는 이름이 충돌하는 동안 이름이 일치하지 않으므로 기존 개체를 제거하지 않습니다.

객체 저장소는 매우 많은 수의 임의의 이름을 지원하도록 설계되었지만, NAS 디렉토리 구조는 매우 많은 수의 이름이 하나의 디렉토리에 저장되면 성능 문제가 발생할 수 있습니다. 특히, 슬래시('/') 문자가 없는 이름은 모두 NAS 매핑의 루트 디렉토리에 배치됩니다. "NAS 친화적"이지 않은 이름을 광범위하게 사용하는 애플리케이션은 NAS 매핑보다는 실제 객체 저장소 버킷에 호스팅하는 것이 더 좋습니다.

## ONTAP SVM에서 NAS 데이터에 대한 S3 프로토콜 액세스 활성화

S3 프로토콜 액세스를 활성화하려면 NAS 지원 SVM이 오브젝트 저장소 서버 추가, 네트워킹 및 인증 요구사항 확인을 포함하여 S3 지원 서버와 동일한 요구사항을 충족하는지 확인해야 합니다.

새로운 ONTAP 설치의 경우 NAS 데이터를 클라이언트에 제공하도록 구성된 후 SVM에 대한 S3 프로토콜 액세스를 지원하는 것이 좋습니다. NAS 프로토콜 구성에 대한 자세한 내용은 다음을 참조하십시오.

- ["NFS 구성"](#)
- ["SMB 구성"](#)

시작하기 전에

S3 프로토콜을 활성화하기 전에 다음을 구성해야 합니다.

- S3 프로토콜과 NFS, SMB 또는 둘 다에 대한 라이선스가 필요합니다.
- SVM은 원하는 NAS 프로토콜을 위해 구성됩니다.
- NFS 및/또는 SMB 서버가 존재합니다.
- DNS 및 기타 필요한 서비스가 구성됩니다.
- NAS 데이터를 클라이언트 시스템으로 보내거나 공유 중입니다.

이 작업에 대해

S3 클라이언트에서 S3 기반 SVM으로 HTTPS 트래픽을 활성화하려면 CA(인증 기관) 인증서가 필요합니다. 다음 세 소스의 CA 인증서를 사용할 수 있습니다.

- SVM에서 자체 서명된 새로운 ONTAP 인증서
- SVM에 자체 서명된 기존 ONTAP 인증서
- 타사 인증서입니다.

NAS 데이터 제공에 사용하는 S3/NAS 버킷에 동일한 데이터 LIF를 사용할 수 있습니다. 특정 IP 주소가 필요한 경우를 참조하십시오 ["데이터 LIF 생성"](#). LIF에서 S3 데이터 트래픽을 활성화하려면 S3 서비스 데이터 정책이 필요합니다. S3를 포함하도록 SVM의 기존 서비스 정책을 수정할 수 있습니다.

S3 오브젝트 서버를 생성할 때 S3 서버 이름을 클라이언트가 S3 액세스에 사용할 FQDN(정규화된 도메인 이름)으로 입력할 준비를 해야 합니다. S3 서버 FQDN은 버킷 이름으로 시작하지 않아야 합니다.

## 시스템 관리자

1. NAS 프로토콜이 구성된 스토리지 VM에서 S3를 설정합니다.
  - a. 스토리지 > 스토리지 VM \* 을 클릭하고 NAS 지원 스토리지 VM을 선택한 다음 설정 을 클릭하고 S3 아래를 클릭합니다 .
  - b. 인증서 유형을 선택합니다. 시스템에서 생성한 인증서 또는 사용자 인증서 중 하나를 선택하든 클라이언트 액세스에 필요합니다.
  - c. 네트워크 인터페이스를 입력합니다.
2. 시스템에서 생성한 인증서를 선택한 경우 새 스토리지 VM 생성이 확인되면 인증서 정보가 표시됩니다. 다운로드 \* 를 클릭하고 클라이언트 액세스를 위해 저장합니다.
  - 비밀 키는 다시 표시되지 않습니다.
  - 인증서 정보가 다시 필요한 경우 \* 스토리지 > 스토리지 VM \* 을 클릭하고 스토리지 VM을 선택한 다음 \* 설정 \* 을 클릭합니다.

## CLI를 참조하십시오

1. SVM에서 S3 프로토콜이 허용되는지 확인합니다.

```
vserver show -fields allowed-protocols
```
2. 이 SVM에 대한 공개 키 인증서를 기록합니다. + 새로운 ONTAP 자체 서명 인증서가 필요한 경우 를 참조하십시오 ["SVM에서 CA 인증서를 생성하고 설치합니다"](#).
3. 서비스 데이터 정책을 업데이트합니다
  - a. SVM+에 대한 서비스 데이터 정책을 표시합니다

```
network interface service-policy show -vserver svm_name
```

에 대한 자세한 내용은 `network interface service-policy show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.
  - b. 및 가 없는 경우 를 `data-core data-s3-server services` 추가합니다.

```
network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server
```
4. SVM에 있는 데이터 LIF가 귀사의 요구사항을 충족하는지 확인하십시오.

```
network interface show -vserver svm_name
```

에 대한 자세한 내용은 `network interface show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.
5. S3 서버 생성:

```
vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]
```

S3 서버를 생성할 때 또는 나중에 언제든지 추가 옵션을 지정할 수 있습니다.

- HTTPS는 기본적으로 포트 443에서 활성화됩니다. `secure-listener-port` 옵션을 사용하여 포트 번호를 변경할 수 있습니다. 를 누릅니다  
HTTPS가 활성화된 경우 SSL/TLS와의 올바른 통합을 위해 CA 인증서가 필요합니다. ONTAP 9.15.1부터 TLS 1.3은 S3 오브젝트 스토리지에서 지원됩니다.
- HTTP는 기본적으로 사용되지 않으며, 이 옵션을 설정하면 서버가 포트 80에서 수신 대기합니다. `is-http-`

enabled 옵션을 사용하여 설정하거나 -listener-port 옵션을 사용하여 포트 번호를 변경할 수 있습니다. + HTTP가 활성화되면 모든 요청과 응답이 일반 텍스트로 네트워크를 통해 전송됩니다.

1. S3이 원하는 대로 구성되었는지 확인합니다

```
vserver object-store-server show
```

- example \* + 다음 명령은 모든 오브젝트 스토리지 서버의 구성 값을 확인합니다.

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

#### 관련 정보

- ["네트워크 인터페이스 서비스 정책 추가 서비스"](#)

## ONTAP S3 NAS 버킷 생성

S3 NAS 버킷은 S3 버킷 이름과 NAS 경로를 매핑한 것입니다. S3 NAS 버킷을 사용하면 기존 볼륨과 디렉터리 구조를 가진 SVM 네임스페이스의 모든 부분에 대한 S3 액세스를 제공할 수 있습니다.

#### 시작하기 전에

- S3 오브젝트 서버는 NAS 데이터를 포함하는 SVM으로 구성됩니다.
- NAS 데이터는 에 부합합니다 ["S3 클라이언트 액세스에 대한 요구 사항"](#).

#### 이 작업에 대해

SVM의 루트 디렉터리 내에 모든 파일 및 디렉터리 세트를 지정하도록 S3 NAS 버킷을 구성할 수 있습니다.

다음 매개 변수의 조합을 기반으로 NAS 데이터에 대한 액세스를 허용하거나 허용하지 않는 버킷 정책을 설정할 수도 있습니다.

- 파일 및 디렉터리
- 사용자 및 그룹 권한
- S3 작업

예를 들어, 많은 사용자에게 읽기 전용 데이터 액세스 권한을 부여하는 버킷 정책과, 제한된 사용자 그룹이 해당 데이터의 일부에 대해 작업을 수행할 수 있도록 허용하는 또 다른 버킷 정책을 설정할 수 있습니다.

ONTAP 9.18.1부터 애플리케이션이 S3 프로토콜을 사용하여 FlexCache 볼륨의 데이터에 액세스할 수 있도록 하는 NAS 버킷을 생성할 수 있습니다. 클러스터의 모든 노드는 ONTAP 9.18.1 이상을 실행해야 합니다. S3 프로토콜을 사용하여 FlexCache 볼륨에 액세스하려면 먼저 `-is-s3-enabled` 옵션을 `true` "[FlexCache 볼륨에서](#)"로 설정해야 합니다. 이 매개변수는 기본적으로 `false`로 설정되어 있습니다.

ONTAP 9.17.1부터 S3 NAS 버킷을 연결 경로가 아닌 볼륨에 직접 연결할 수 있습니다. 기본적으로 NAS 볼륨의 S3 버킷은 연결 경로와 연결되며, ONTAP 관리자는 언제든지 이 경로를 변경할 수 있습니다. 이러한 변경으로 인해 S3 버킷 작업이 중단될 수 있습니다. ONTAP 9.17.1부터는 `-is-nas-path-mutable false` 옵션과 함께 `vserver object-store-server bucket create` ONTAP CLI에서 명령을 사용하여 S3 NAS 버킷을 볼륨에 연결할 수 있습니다. 기본적으로 `-is-nas-path-mutable` 로 설정됩니다 `true`.

S3 NAS "버킷"은 매핑이지 S3 버킷이 아니므로 표준 S3 버킷의 다음 속성은 S3 NAS 버킷에 적용되지 않습니다.

- `* aggr-list\aggr-list-multiplier\storage-service-level\volume\size\exclude-aggr-list\QoS-policy-group *` + S3 NAS 버킷을 구성할 때 볼륨 또는 `qtree`가 생성되지 않습니다.
- 역할 \은 **-protected**입니다 \은 **-protected-on-ontap**입니다 \은 **-protected-on-cloud**입니다 + S3 NAS 버킷은 SnapMirror S3를 사용하여 보호되거나 미러링되지 않고 대신 볼륨 세분성에서 사용 가능한 일반 SnapMirror 보호 기능을 사용합니다.
- **versioning-state**+ NAS 볼륨에는 일반적으로 다른 버전을 저장할 수 있는 스냅샷 기술이 있습니다. 그러나 버전 관리는 현재 S3 NAS 버킷에서 사용할 수 없습니다.
- 볼륨 명령을 통해 NAS 볼륨에 대해 `* logical-used\object-count *` + 등가 통계를 사용할 수 있습니다.
- **multipart** 객체 + ONTAP 9.16.1부터 S3 NAS 버킷에서 multipart 객체가 지원됩니다. "[고급 용량 밸런싱](#)" 기본 FlexGroup 볼륨에서 활성화되어 있습니다. 고급 용량 분산은 FlexGroup 볼륨에서만 활성화할 수 있습니다. FlexVol 볼륨에서는 활성화할 수 없습니다.

단계

시스템 관리자나 ONTAP CLI를 사용하여 NAS 버킷을 생성할 수 있습니다.



시스템 관리자

NAS가 활성화된 스토리지 VM에 새 S3 NAS 버킷을 추가합니다.

1. 스토리지 > 버킷 \* 을 클릭한 다음 \* 추가 \* 를 클릭합니다.
2. S3 NAS 버킷의 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력하지 말고 \* More Options \* 를 클릭합니다.
3. 유효한 경로 이름을 입력하거나 찾아보기를 클릭하여 유효한 경로 이름 목록에서 선택합니다. + 올바른 경로 이름을 입력하면 S3 NAS 구성과 관련이 없는 옵션이 숨겨집니다.
4. S3 사용자를 NAS 사용자 및 생성된 그룹에 이미 매핑한 경우 해당 사용 권한을 구성한 다음 \* 저장 \* 을 클릭합니다. +이 단계에서 사용 권한을 구성하기 전에 S3 사용자를 NAS 사용자에게 이미 매핑해야 합니다.

그렇지 않으면 \* 저장 \* 을 클릭하여 S3 NAS 버킷 구성을 완료합니다.

CLI를 참조하십시오

1. NAS 파일 시스템이 포함된 SVM에 S3 NAS 버킷을 만듭니다.

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
true|false [-comment <text>]
```

예제 1: S3 NAS 버킷 만들기

```
cluster1::> vserver object-store-server bucket create -bucket testbucket
-type nas -path /vol1
```

예제 2: S3 NAS 버킷을 생성하고 버킷을 볼륨에 연결

```
vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
-type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
```

## ONTAP S3 클라이언트 사용자 활성화

S3 클라이언트 사용자가 NAS 데이터에 액세스할 수 있도록 하려면 S3 사용자 이름을 해당 NAS 사용자에게 매핑한 다음 버킷 서비스 정책을 사용하여 NAS 데이터에 대한 액세스 권한을 부여해야 합니다.

시작하기 전에

클라이언트 액세스를 위한 사용자 이름(LINUX/UNIX, Windows 및 S3 클라이언트 사용자)이 이미 존재해야 합니다.

일부 S3 기능은 에 대해 알고 "S3 NAS 버킷에서 지원되지 않음"있어야 합니다.

이 작업에 대해

S3 사용자 이름을 해당 Linux/UNIX 또는 Windows 사용자에게 매핑하면 S3 클라이언트가 NAS 파일에 액세스할 때 NAS 파일에 대한 권한 부여 검사를 수행할 수 있습니다. S3-NAS 매핑은 단일 이름 또는 POSIX 정규식으로 표현될 수 있는 S3 사용자 이름\_Pattern\_과 Linux/UNIX 또는 Windows 사용자 이름\_Replacement\_를 제공하여 지정합니다.

이름 매핑이 없는 경우 기본 이름 매핑이 사용됩니다. 여기서 S3 사용자 이름 자체는 UNIX 사용자 이름 및 Windows

사용자 이름으로 사용됩니다. 를 사용하여 UNIX 및 Windows 기본 사용자 이름 매핑을 수정할 수 있습니다 `vserver object-store-server modify` 명령.

로컬 이름 매핑 구성만 지원되며 LDAP는 지원되지 않습니다.

S3 사용자를 NAS 사용자에게 매핑한 후에는 액세스 권한이 있는 리소스(디렉토리 및 파일)와 해당 사용자가 액세스할 수 있거나 수행할 수 없는 작업을 지정하는 권한을 사용자에게 부여할 수 있습니다.

## 시스템 관리자

1. UNIX 또는 Windows 클라이언트(또는 둘 다)에 대한 로컬 이름 매핑을 생성합니다.
  - a. 스토리지 > 버킷 \* 을 클릭한 다음 S3/NAS 지원 스토리지 VM을 선택합니다.
  - b. Settings \* 를 선택한 다음 \* Name Mapping \* (\* Host Users and Groups \* 아래)을 클릭합니다 → .
  - c. S3 to Windows \* 또는 \* S3 to UNIX \* 타일(또는 둘 다)에서 \* 추가 \* 를 클릭한 다음 원하는 \* 패턴 \* (S3) 및 \* 교체 \* (NAS) 사용자 이름을 입력합니다.
2. 버킷 정책을 생성하여 클라이언트 액세스를 제공합니다.
  - a. 스토리지 > Bucket \* 을 클릭하고 원하는 S3 버킷 옆에 있는 을  클릭한 다음 \* Edit \* 를 클릭합니다.
  - b. 추가 \* 를 클릭하고 원하는 값을 입력합니다.
    - \* Principal \* - S3 사용자 이름을 제공하거나 기본값(모든 사용자)을 사용합니다.
    - \* 효과 \* - \* 허용 \* 또는 \* 거부 \* 를 선택합니다.
    - \* 조치 \* - 이러한 사용자 및 리소스에 대한 조치를 입력합니다. 현재 오브젝트 저장소 서버가 S3 NAS 버킷에 대해 지원하는 리소스 작업 집합은 GetObject , PutObject , DeleteObject , ListBucket , GetBucketAcl 입니다. GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning 및 ListBucketVersions. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.
    - \* 리소스 \* - 작업이 허용 또는 거부된 폴더나 파일 경로를 입력하거나 기본(버킷의 루트 디렉터리)을 사용합니다.

## CLI를 참조하십시오

1. UNIX 또는 Windows 클라이언트(또는 둘 다)에 대한 로컬 이름 매핑을 생성합니다. 를 누릅니다  
`vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix}  
-position integer -pattern s3_user_name -replacement nas_user_name`
  - ° -position 매핑 평가의 우선 순위 번호입니다. 1 또는 2를 입력합니다.
  - ° -pattern - S3 사용자 이름 또는 정규식입니다
  - ° -replacement - Windows 또는 UNIX 사용자 이름입니다

## 예

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. 버킷 정책을 생성하여 클라이언트 액세스를 제공합니다. 를 누릅니다  
`vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {deny|allow} -action list_of_actions -principal  
list_of_users_or_groups -resource [-sid alphanumeric_text]`
  - ° -effect {deny|allow} - 사용자가 작업을 요청할 때 액세스를 허용할지 또는 거부할지 여부를 지정합니다.
  - ° -action <Action>, ... - 허용되거나 거부되는 리소스 작업을 지정합니다. 개체 저장소 서버에서 S3 NAS 버킷에 대해 현재 지원하는 리소스 작업 집합은 GetObject, PutObject, DeleteObject, ListBucketAcl, GetObjectAcl 및 GetBucketLocation입니다. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.

- `-principal <Objectstore Principal>`, ... - 이 매개 변수에 지정된 개체 저장소 서버 사용자 또는 그룹에 대해 액세스를 요청하는 사용자의 유효성을 검사합니다.
  - 개체 저장소 서버 그룹은 그룹 이름에 접두사 `그룹 /` 을 추가하여 지정합니다.
  - `-principal -(하이픈 문자)`는 모든 사용자에게 액세스 권한을 부여합니다.
- `-resource <text>`, ... - 허용/거부 권한이 설정된 버킷, 폴더 또는 개체를 지정합니다. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.
- `[-sid <SID>]` - 오브젝트 저장소 서버 버킷 정책 문에 대한 선택적 텍스트 설명을 지정합니다.

예

```
cluster1::> vservers object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vservers object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

## Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성

### Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 개요

ONTAP 기능을 사용하면 Microsoft Hyper-V와 Microsoft SQL Server라는 SMB 프로토콜을 통해 두 Microsoft 애플리케이션의 무중단 운영을 실현할 수 있습니다.

다음과 같은 상황에서 SMB 무중단 운영을 구현하려는 경우 다음 절차를 따라야 합니다.

- 기본 SMB 프로토콜 파일 액세스가 구성되었습니다.
- SVM에 상주하는 SMB 3.0 이상 파일 공유를 활성화하여 다음 오브젝트를 저장하려고 합니다.
  - Hyper-V 가상 머신 파일
  - SQL Server 시스템 데이터베이스

#### 관련 정보

ONTAP 기술 및 외부 서비스와의 상호 작용에 대한 자세한 내용은 다음 기술 보고서(TR)를 참조하십시오 ["NetApp 기술 보고서 4172: ONTAP 모범 사례를 사용한 SMB 3.0 기반 Microsoft Hyper-V"](#).\*\* ["NetApp 기술 보고서 4369: clustered Data ONTAP을 사용한 Microsoft SQL Server의 모범 사례 및 SQL Server의 SnapManager 7.2"](#)

### SMB 솔루션을 통해 Microsoft Hyper-V 및 SQL Server용 ONTAP를 구성합니다

지속적으로 사용 가능한 SMB 3.0 이상 파일 공유를 사용하여 Hyper-V 가상 머신 파일 또는 SQL Server 시스템 데이터베이스와 사용자 데이터베이스를 SVM에 상주하는 볼륨에 저장하는 동시에 계획된 이벤트와 계획되지 않은 이벤트 모두에 무중단 운영(NDO)을 제공할 수 있습니다.

## SMB를 통한 Microsoft Hyper-V

SMB를 통한 Hyper-V 솔루션을 생성하려면 먼저 ONTAP를 구성하여 Microsoft Hyper-V 서버에 스토리지 서비스를 제공해야 합니다. 또한 Microsoft 클러스터(클러스터 구성을 사용하는 경우), Hyper-V 서버, CIFS 서버에서 호스팅하는 공유에 대한 지속적인 SMB 3.0 연결, SVM 볼륨에 저장된 가상 시스템 파일을 보호하기 위한 백업 서비스도 구성해야 합니다.



Hyper-V 서버는 Windows 2012 Server 이상에서 구성해야 합니다. 독립 실행형 및 클러스터링된 Hyper-V 서버 구성이 모두 지원됩니다.

- Microsoft 클러스터 및 Hyper-V 서버 생성에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- SnapManager for Hyper-V는 SMB 구성을 통한 Hyper-V와 통합되도록 설계된 신속한 스냅샷 기반 백업 서비스를 지원하는 호스트 기반 애플리케이션입니다.

SMB 구성을 통한 Hyper-V에서 SnapManager를 사용하는 방법에 대한 자세한 내용은 [\\_SnapManager for Hyper-V 설치 및 관리 가이드\\_](#)를 참조하십시오.

## SMB를 통한 Microsoft SQL Server

SMB를 통한 SQL Server 솔루션을 생성하려면 먼저 Microsoft SQL Server 애플리케이션에 스토리지 서비스를 제공하도록 ONTAP를 구성해야 합니다. 또한 클러스터된 구성을 사용하는 경우 Microsoft 클러스터도 구성해야 합니다. 그런 다음 Windows 서버에 SQL Server를 설치 및 구성하고 CIFS 서버에서 호스팅하는 공유에 대해 지속적으로 사용 가능한 SMB 3.0 연결을 생성합니다. 필요에 따라 SVM 볼륨에 저장된 데이터베이스 파일을 보호하도록 백업 서비스를 구성할 수 있습니다.



SQL Server는 Windows 2012 Server 이상에서 설치 및 구성해야 합니다. 독립 실행형 구성과 클러스터 구성이 모두 지원됩니다.

- Microsoft 클러스터 만들기 및 SQL Server 설치 및 구성에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- Microsoft SQL Server용 SnapCenter 플러그인은 SMB 구성을 통해 SQL Server와 통합하도록 설계된 호스트 기반 애플리케이션으로, 신속한 스냅샷 기반 백업 서비스를 지원합니다.

Microsoft SQL Server용 SnapCenter 플러그인 사용에 대한 자세한 내용은 ["Microsoft SQL Server용 SnapCenter 플러그인"](#) 문서를 참조하십시오.

## SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영

Hyper-V 및 SQL Server over SMB의 무중단 운영은 무엇을 의미하는지

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영은 애플리케이션 서버와 포함된 가상 머신 또는 데이터베이스를 온라인 상태로 유지하고 다양한 관리 작업 중에 지속적인 가용성을 제공할 수 있는 기능의 조합을 의미합니다. 여기에는 스토리지 인프라의 계획된 다운타임과 계획되지 않은 다운타임이 모두 포함됩니다.

SMB를 통해 애플리케이션 서버에서 지원되는 무중단 운영은 다음과 같습니다.

- 계획된 테이크오버 및 반환

- 계획되지 않은 테이크오버
- 업그레이드
- 계획된 애그리게이트 재배포치(ARL)
- LIF 마이그레이션 및 페일오버
- 계획된 볼륨 이동

프로토콜을 지원하여 **SMB**를 통해 무중단 운영을 실현합니다

Microsoft는 SMB 3.0 릴리스와 함께 SMB를 통해 Hyper-V 및 SQL Server의 무중단 운영을 지원하는 데 필요한 기능을 제공하는 새로운 프로토콜을 출시했습니다.

ONTAP은 SMB를 통해 애플리케이션 서버에 무중단 운영을 제공할 때 다음과 같은 프로토콜을 사용합니다.

- SMB 3.0
- 증인

**SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영에 대한 주요 개념입니다**

SMB 솔루션을 통해 Hyper-V 또는 SQL Server를 구성하기 전에 알아야 하는 무중단 운영(NDO)에 대한 몇 가지 개념이 있습니다.

- \* 지속적으로 사용 가능한 공유 \*

지속적으로 사용 가능한 공유 속성이 설정된 SMB 3.0 공유입니다. 지속적으로 사용 가능한 공유를 통해 연결하는 클라이언트는 테이크오버, 반환 및 애그리게이트 재배포치와 같은 운영 중단 이벤트를 견딜 수 있습니다.

- \* 노드 \*

클러스터의 구성원인 단일 컨트롤러입니다. SFO 쌍의 두 노드를 구별하기 위해 한 노드는 `_local node_`라고도 하며 다른 노드는 `_partner node_` 또는 `_remote node_`라고도 합니다. 스토리지의 기본 소유자는 로컬 노드입니다. 기본 소유자가 실패하는 경우 스토리지를 제어하는 보조 소유자가 파트너 노드입니다. 각 노드는 해당 스토리지의 기본 소유자이며 파트너의 스토리지를 위한 2차 소유자입니다.

- \* 무중단 애그리게이트 재배포치 \*

클라이언트 애플리케이션을 중단하지 않고 클러스터에서 SFO 쌍 내의 파트너 노드 간에 애그리게이트를 이동할 수 있습니다.

- 무중단 페일오버 \* 를 지원합니다

테이크오버를 참조하십시오.

- \* 무중단 LIF 마이그레이션 \*

LIF를 통해 클러스터에 연결된 클라이언트 애플리케이션을 중단하지 않고 LIF 마이그레이션을 수행할 수 있습니다. SMB 연결의 경우 SMB 2.0 이상을 사용하여 연결하는 클라이언트에만 가능합니다.

- 무중단 운영 \*

주요 ONTAP 관리 및 업그레이드 작업을 수행할 뿐만 아니라 클라이언트 애플리케이션을 중단하지 않고 노드 장애를 견딜 수 있는 기능 이때 무중단 테이크오버, 무중단 업그레이드, 무중단 마이그레이션 기능이 전반적으로 사용됩니다.

- 무중단 업그레이드 \*

애플리케이션 중단 없이 노드 하드웨어 또는 소프트웨어를 업그레이드할 수 있는 기능

- \* 무중단 볼륨 이동 \*

볼륨을 사용하는 애플리케이션을 중단하지 않고 클러스터 전체에서 볼륨을 자유롭게 이동할 수 있습니다. SMB 연결의 경우, 모든 버전의 SMB가 무중단 볼륨 이동을 지원합니다.

- \* 영구 핸들 \*

연결이 끊길 경우 지속적으로 사용 가능한 연결을 통해 CIFS 서버에 투명하게 다시 연결할 수 있도록 하는 SMB 3.0의 속성입니다. 내구성이 뛰어난 핸들과 마찬가지로 연결 클라이언트와의 통신이 끊긴 후 CIFS 서버가 일정 시간 동안 영구 핸들을 유지합니다. 그러나 지속적인 핸들은 내구성 있는 핸들보다 뛰어난 복원력을 제공합니다. 다시 연결한 후 60초 이내에 클라이언트에서 핸들을 다시 확보할 수 있는 기회를 제공할 뿐 아니라 CIFS 서버는 60초 동안 파일에 대한 액세스를 요청하는 다른 클라이언트에 대한 액세스를 거부합니다.

영구 핸들에 대한 정보는 SFO 파트너의 영구 스토리지에 미러링되므로, 영구 핸들이 분리된 클라이언트는 SFO 파트너가 노드 스토리지에 대한 소유권을 갖게 된 후 내구성 있는 핸들을 다시 확보할 수 있습니다. 지속적인 핸들은 LIF 이동 시 무중단 운영(내구성이 뛰어난 핸들 지원)을 제공할 뿐만 아니라 테이크오버, 반환 및 애그리게이트 재배치를 위한 무중단 운영을 제공합니다.

- SFO 반환 \*

테이크오버 이벤트에서 복구할 때 애그리게이트를 홈 위치로 반환

- SFO 쌍 \*

두 노드 중 하나가 작동을 중지할 경우 컨트롤러가 상호 데이터를 제공하도록 구성된 노드 쌍입니다. 시스템 모델에 따라 두 컨트롤러 모두 단일 쉘 내에 있거나 컨트롤러가 별도 쉘에 있을 수 있습니다. 2노드 클러스터에서 HA 쌍이라고 합니다.

- \* 테이크오버 \*

해당 스토리지의 기본 소유자가 실패한 경우 파트너가 스토리지를 제어하는 프로세스입니다. SFO 맥락에서 파일오버 및 테이크오버는 동의어입니다.

### **SMB 3.0 기능이 SMB 공유에서 무중단 운영을 지원하는 방법**

SMB 3.0은 SMB 공유를 통해 Hyper-V 및 SQL Server의 무중단 운영을 지원하는 중요한 기능을 제공합니다. 여기에는 SMB 클라이언트가 파일 열기 상태를 재확보하고 SMB 연결을 투명하게 다시 설정할 수 있도록 하는 '연속 사용 가능' 공유 속성과 '영구 핸들'이라는 파일 핸들 유형이 포함됩니다.

지속적으로 사용 가능한 공유 속성 집합을 사용하여 공유에 연결하는 SMB 3.0 지원 클라이언트에 영구 핸들을 부여할 수 있습니다. SMB 세션의 연결이 끊기면 CIFS 서버는 영구 처리 상태에 대한 정보를 유지합니다. CIFS 서버는 클라이언트가 다시 연결될 수 있는 60초 동안 다른 클라이언트 요청을 차단하여, 영구 핸들이 있는 클라이언트가 네트워크 연결 해제 후 핸들을 다시 확보할 수 있도록 합니다. 핸들을 지속적으로 사용하는 클라이언트는 SVM(스토리지

가상 머신)의 데이터 LIF 중 하나를 사용하여 다시 연결할 수 있습니다. 즉, 동일한 LIF를 통해 다시 연결하거나 다른 LIF를 통해 다시 연결할 수 있습니다.

애그리게이트 재배포, 테이크오버 및 반환은 모두 SFO 쌍 간에 발생합니다. 영구 핸들이 있는 파일을 사용하여 세션의 분리 및 재연결을 원활하게 관리하기 위해 파트너 노드는 모든 영구 핸들 잠금 정보의 복사본을 유지 관리합니다. SFO 파트너는 이벤트의 계획인지 계획되지 않는지에 관계없이 영구 핸들 연결을 중단 없이 관리할 수 있습니다. 이 새로운 기능을 통해 CIFS 서버에 대한 SMB 3.0 연결이 예전부터 운영 중단 없이 할당된 SVM에 할당된 다른 데이터 LIF로 투명하게 페일오버할 수 있습니다.

영구 핸들을 사용하면 CIFS 서버가 SMB 3.0 연결을 투명하게 페일오버할 수 있지만 장애가 발생하여 Hyper-V 애플리케이션이 Windows Server 클러스터의 다른 노드로 페일오버될 경우 클라이언트는 연결이 끊어진 핸들의 파일 핸들을 다시 확보할 수 없습니다. 이 시나리오에서는 연결이 끊긴 상태의 파일 핸들이 다른 노드에서 다시 시작될 경우 Hyper-V 응용 프로그램의 액세스를 차단할 수 있습니다. ""장애 조치 클러스터링""은 SMB 3.0의 일부이며, 이러한 시나리오를 해결하기 위해 오래되고 충돌하는 핸들을 무효화하는 메커니즘을 제공합니다. 이 메커니즘을 사용하면 Hyper-V 클러스터 노드에 장애가 발생할 경우 Hyper-V 클러스터가 신속하게 복구될 수 있습니다.

**Witness** 프로토콜이 투명한 장애 조치를 강화하기 위해 수행하는 조치

Witness 프로토콜은 SMB 3.0에서 지속적으로 사용 가능한 공유(CA 공유)를 위한 향상된 클라이언트 페일오버 기능을 제공합니다. 입회자는 LIF 페일오버 복구 기간을 거치지 않으므로 더 빠른 페일오버를 촉진합니다. SMB 3.0 연결이 시간 초과될 때까지 기다리지 않고 노드를 사용할 수 없을 때 애플리케이션 서버에 알립니다.

클라이언트에서 실행 중인 애플리케이션이 페일오버가 발생했는지 알지 못하면서 페일오버가 원활하게 이루어집니다. Witness를 사용할 수 없는 경우에도 페일오버 작업은 성공적으로 수행되지만 Witness를 사용하지 않는 페일오버는 효율성이 떨어집니다.

다음 요구 사항이 충족되면 감시 강화 장애 조치가 가능합니다.

- SMB 3.0이 활성화된 SMB 3.0 지원 CIFS 서버에서만 사용할 수 있습니다.
- 공유는 지속적인 가용성 공유 속성 세트와 함께 SMB 3.0을 사용해야 합니다.
- 애플리케이션 서버가 연결되는 노드의 SFO 파트너는 애플리케이션 서버의 데이터를 호스팅하는 SVM(스토리지 가상 머신)에 적어도 하나의 운영 데이터 LIF가 할당되어 있어야 합니다.



Witness 프로토콜은 SFO 쌍 사이에서 작동합니다. LIF가 클러스터 내의 노드로 마이그레이션할 수 있으므로 모든 노드가 SFO 파트너의 증인이 될 수 있습니다. 애플리케이션 서버용 데이터를 호스팅하는 SVM이 파트너 노드에 활성 데이터 LIF가 없는 경우 Witness 프로토콜은 특정 노드에서 SMB 연결을 빠르게 페일오버할 수 없습니다. 따라서 클러스터의 모든 노드는 이러한 구성 중 하나를 호스팅하는 각 SVM에 대해 적어도 하나의 데이터 LIF를 가져야 합니다.

- 애플리케이션 서버는 개별 LIF IP 주소를 사용하는 대신 DNS에 저장된 CIFS 서버 이름을 사용하여 CIFS 서버에 연결해야 합니다.

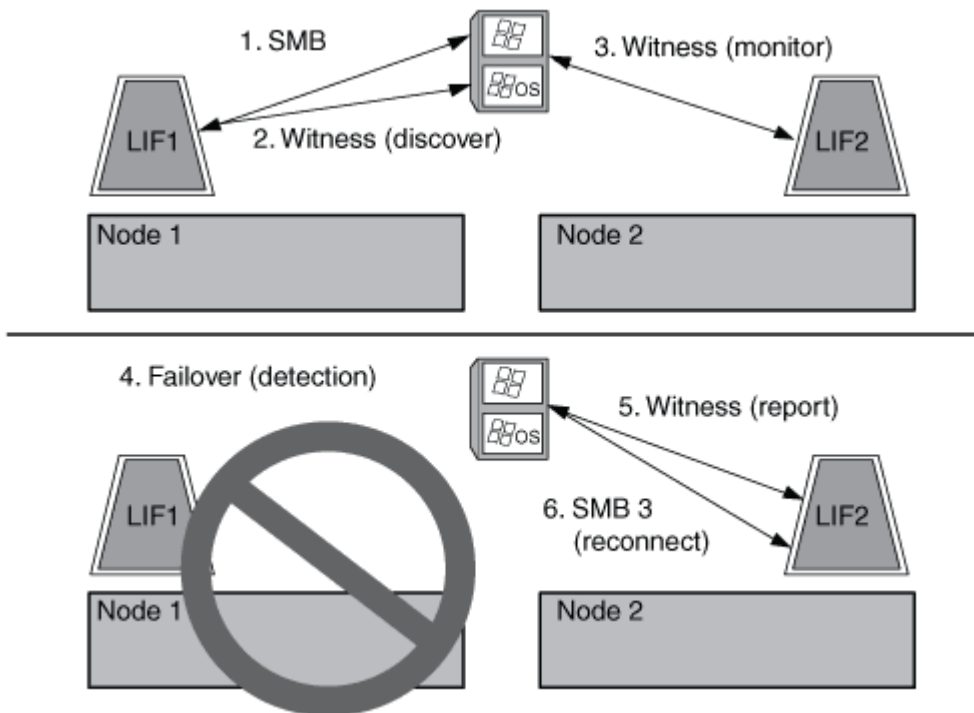
**Witness** 프로토콜 작동 방식

ONTAP는 노드의 SFO 파트너를 증인으로 사용하여 Witness 프로토콜을 구현합니다. 장애가 발생할 경우 파트너는 빠르게 장애를 감지하고 SMB 클라이언트에 알립니다.

Witness 프로토콜은 다음 프로세스를 사용하여 향상된 장애 조치를 제공합니다.



1. 애플리케이션 서버가 Node1에 대한 지속적으로 사용 가능한 SMB 연결을 설정하면 CIFS 서버가 애플리케이션 서버에 Witness를 사용할 수 있음을 알립니다.
2. 애플리케이션 서버는 Node1에서 Witness 서버의 IP 주소를 요청하고, 스토리지 가상 시스템(SVM)에 할당된 Node2(SFO 파트너) 데이터 LIF IP 주소 목록을 수신합니다.
3. 애플리케이션 서버는 IP 주소 중 하나를 선택하고 Node2에 대한 Witness 연결을 생성하며, Node1에서 계속 사용 가능한 연결이 이동해야 하는 경우 알림을 받을 레지스터를 생성합니다.
4. Node1에서 페일오버 이벤트가 발생할 경우 Witness는 페일오버 이벤트를 발생하지만 반환과 관련이 없습니다.
5. 감시 기능은 장애 조치 이벤트를 감지하고 Witness 연결을 통해 애플리케이션 서버에 SMB 연결이 Node2로 이동해야 함을 알립니다.
6. 애플리케이션 서버는 SMB 세션을 Node2로 이동하고 클라이언트 액세스를 중단하지 않고 연결을 복구합니다.



## 원격 VSS와 공유 기반 백업

원격 VSS를 사용한 공유 기반 백업 개요

원격 VSS를 사용하여 CIFS 서버에 저장된 Hyper-V 가상 머신 파일의 공유 기반 백업을 수행할 수 있습니다.

Microsoft 원격 VSS(Volume Shadow Copy Services)는 기존 Microsoft VSS 인프라의 확장입니다. Microsoft는 원격 VSS를 통해 VSS 인프라를 확장하여 SMB 공유의 새도우 복제를 지원하고 있습니다. 또한 Hyper-V와 같은 서버 애플리케이션에서 SMB 파일 공유에 VHD 파일을 저장할 수 있습니다. 이러한 확장을 사용하면 데이터 및 구성 파일을 공유에 저장하는 가상 시스템에 대해 애플리케이션 정합성이 보장되는 새도우 복제본을 가져올 수 있습니다.

## 원격 VSS 개념

SMB를 통한 Hyper-V 구성의 백업 서비스에서 원격 VSS(Volume Shadow Copy Service)를 사용하는 방법을 이해하는 데 필요한 특정 개념을 이해해야 합니다.

- \* VSS(Volume Shadow Copy Service) \*

특정 시점에 특정 볼륨에 있는 데이터의 백업 복사본 또는 스냅샷을 생성하는 데 사용되는 Microsoft 기술입니다. VSS는 데이터 서버, 백업 애플리케이션 및 스토리지 관리 소프트웨어 사이에서 조정을 수행하여 일관된 백업의 생성 및 관리를 지원합니다.

- \* 원격 VSS(원격 볼륨 새도 복사본 서비스) \*

SMB 3.0 공유를 통해 데이터에 액세스할 수 있는 특정 시점의 데이터 정합성 보장 상태에 있는 데이터의 공유 기반 백업 복사본을 생성하는 데 사용되는 Microsoft 기술입니다. 볼륨 새도 복사본 서비스 \_ 라고도 합니다.

- \* 새도 복사본 \*

공유에 포함된 중복 데이터 집합을 적절하게 정의된 즉시 사용합니다. 새도우 복제본은 데이터의 일관된 시점 백업을 생성하는 데 사용되므로 시스템이나 애플리케이션에서 원래 볼륨의 데이터를 계속 업데이트할 수 있습니다.

- \* 새도 복사본 세트 \*

한 공유에 해당하는 각 새도 복사본을 포함하는 하나 이상의 새도 복사본 모음입니다. 새도우 복제본 세트 내의 새도우 복제본은 동일한 작업에서 백업해야 하는 모든 공유를 나타냅니다. VSS 지원 애플리케이션의 VSS 클라이언트는 세트에 포함할 새도우 복제본을 식별합니다.

- \* 새도우 복제본 세트 자동 복구 \*

새도우 복제본이 포함된 복제본 디렉토리가 시점 정합성이 보장되는 원격 VSS 지원 백업 애플리케이션에 대한 백업 프로세스의 일부입니다. 백업을 시작할 때 애플리케이션의 VSS 클라이언트는 백업 예약된 데이터(Hyper-V의 경우 가상 머신 파일)에서 소프트웨어 체크포인트를 생성하도록 애플리케이션을 트리거합니다. 그러면 VSS 클라이언트가 응용 프로그램을 계속할 수 있습니다. 새도우 복제본 세트가 생성된 후 원격 VSS는 새도우 복제본 세트를 쓰기 가능하게 만들고 쓰기 가능한 복제본을 애플리케이션에 노출합니다. 애플리케이션은 앞서 생성한 소프트웨어 체크포인트를 사용하여 자동 복구를 수행하여 새도우 복제본 세트를 백업할 준비를 합니다. 자동 복구는 체크포인트가 생성된 이후 파일 및 디렉토리의 변경 사항을 언롤링함으로써 새도우 복제본을 정합성 보장 상태로 만듭니다. 자동 복구는 VSS 지원 백업을 위한 선택적 단계입니다.

- \* 새도 복사본 ID \*

새도우 복제본을 고유하게 식별하는 GUID입니다.

- \* 새도 복사본 세트 ID \*

동일한 서버에 대한 새도우 복제본 ID의 컬렉션을 고유하게 식별하는 GUID입니다.

- \* Hyper-V \* 용 SnapManager

Microsoft Windows Server 2012 Hyper-V의 백업 및 복원 작업을 자동화하고 단순화하는 소프트웨어입니다. SnapManager for Hyper-V는 원격 VSS와 자동 복구를 사용하여 SMB 공유를 통해 Hyper-V 파일을 백업합니다.

## 관련 정보

[SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영에 대한 주요 개념입니다](#)

[원격 VSS와 공유 기반 백업](#)

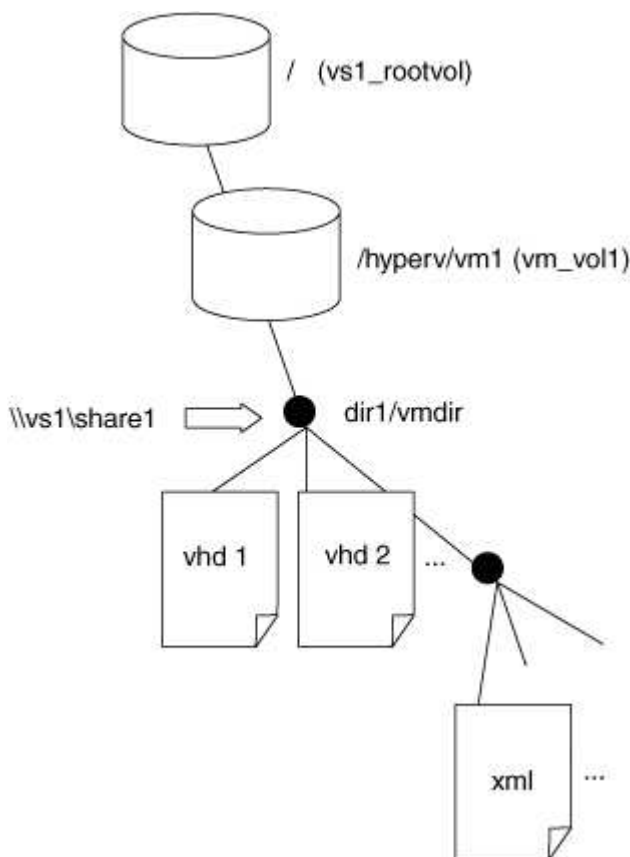
원격 VSS에서 사용하는 디렉토리 구조의 예

원격 VSS는 새도우 복제본을 생성할 때 Hyper-V 가상 머신 파일을 저장하는 디렉토리 구조를 통과합니다. 가상 머신 파일의 백업을 성공적으로 생성할 수 있도록 적절한 디렉토리 구조가 무엇인지 이해하는 것이 중요합니다.

새도우 복제본을 성공적으로 생성하기 위해 지원되는 디렉토리 구조는 다음 요구 사항을 따릅니다.

- 가상 머신 파일을 저장하는 데 사용되는 디렉토리 구조 내에는 디렉토리와 일반 파일만 있습니다.  
디렉토리 구조에는 연결 지점, 링크 또는 비정규 파일이 포함되어 있지 않습니다.
- 가상 머신의 모든 파일은 단일 공유 내에 있습니다.
- 가상 머신 파일을 저장하는 데 사용되는 디렉토리 구조가 새도 복사본 디렉토리의 구성된 깊이를 초과하지 않습니다.
- 공유의 루트 디렉토리에는 가상 머신 파일 또는 디렉토리만 포함됩니다.

다음 그림에서는 vm\_vol1이라는 이름의 볼륨이 SVM(Storage Virtual Machine) VS1의 '/hyperv/vm1'에 있는 접합 지점으로 생성됩니다. 가상 머신 파일을 포함하는 하위 디렉토리는 교차점 아래에 생성됩니다. Hyper-V 서버의 가상 머신 파일은 "/hyperv/vm1/dir1/vmdir" 경로가 있는 share1을 통해 액세스합니다. 새도 복사본 서비스는 share1 아래의 디렉토리 구조 내에 포함된 모든 가상 머신 파일의 새도 복사본을 만듭니다(새도우 복제본 디렉토리의 구성된 깊이까지).



**SnapManager for Hyper-V가 SMB를 통해 Hyper-V에 대한 원격 VSS 기반 백업을 관리하는 방법**

SnapManager for Hyper-V를 사용하여 원격 VSS 기반 백업 서비스를 관리할 수 있습니다. SnapManager for Hyper-V 관리 백업 서비스를 사용하면 공간 효율적인 백업 세트를 생성할 수

있다는 이점이 있습니다.

Hyper-V 관리 백업을 위한 SnapManager 최적화 기능은 다음과 같습니다.

- ONTAP과 SnapDrive의 통합은 SMB 공유 위치를 검색할 때 성능을 최적화합니다.

ONTAP는 공유가 상주하는 볼륨의 이름을 SnapDrive에 제공합니다.

- SnapManager for Hyper-V는 새도우 복제본 서비스를 복제해야 하는 SMB 공유의 가상 머신 파일 목록을 지정합니다.

가상 머신 파일의 타겟 목록을 제공함으로써 새도우 복제본 서비스는 공유에 있는 모든 파일의 새도우 복제본을 생성할 필요가 없습니다.

- 스토리지 가상 머신(SVM)에 복원에 사용할 SnapManager for Hyper-V의 스냅샷이 보존됩니다.

백업 단계가 없습니다. 백업은 공간 효율성이 뛰어난 스냅샷입니다.

SnapManager for Hyper-V는 다음 프로세스를 사용하여 SMB를 통한 Hyper-V의 백업 및 복원 기능을 제공합니다.

#### 1. 새도 복사본 작업을 준비하는 중입니다

SnapManager for Hyper-V 애플리케이션의 VSS 클라이언트는 새도우 복제본 세트를 설정합니다. VSS 클라이언트는 새도 복사본 세트에 포함할 공유에 대한 정보를 수집하고 이 정보를 ONTAP에 제공합니다. 세트에는 하나 이상의 새도 복사본이 포함될 수 있으며 하나의 새도 복사본은 하나의 공유에 해당합니다.

#### 2. 새도 복사본 세트 생성(자동 복구가 사용되는 경우)

새도 복사본 세트에 포함된 모든 공유에서 ONTAP는 새도 복사본을 만들고 새도 복사본을 쓰기 가능하게 만듭니다.

#### 3. 새도우 복제본 세트를 노출합니다

ONTAP에서 새도우 복제본을 생성한 후 SnapManager for Hyper-V에 노출되므로 애플리케이션의 VSS 작성기가 자동 복구를 수행할 수 있습니다.

#### 4. 새도우 복제본 세트를 자동으로 복구합니다

새도우 복제본 세트를 생성하는 동안 백업 세트에 포함된 파일에 대한 활성 변경이 발생하는 기간이 있습니다. 애플리케이션의 VSS 작성자는 새도우 복제본을 업데이트하여 백업 전에 정합성이 완벽하게 보장되는 상태인지 확인해야 합니다.



자동 복구를 수행하는 방법은 애플리케이션에 따라 다릅니다. 원격 VSS가 이 단계에 없습니다.

#### 5. 새도 복사본 세트 완료 및 정리

VSS 클라이언트는 자동 복구를 완료한 후 ONTAP에 알립니다. 새도 복사본 세트는 읽기 전용으로 만들어져 백업할 준비가 된 상태입니다. 백업에 SnapManager for Hyper-V를 사용하면 스냅샷의 파일이 백업이 되므로 백업 단계의 경우 백업 세트의 공유를 포함하는 모든 볼륨에 대해 스냅샷이 생성됩니다. 백업이 완료되면 CIFS 서버에서 새도우 복제본 세트가 제거됩니다.

## SMB 공유를 통해 Hyper-V 및 SQL Server에서 ODX 복사 오프로드를 사용하는 방법

ODX(Offloaded Data Transfer)는 \_copy offload\_라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고도 호환되는 스토리지 장치 내부 또는 간에 직접 데이터를 전송할 수 있습니다. ONTAP ODX 복사 오프로드를 사용하면 SMB 설치를 통해 애플리케이션 서버에서 복사 작업을 수행할 때 성능 이점을 얻을 수 있습니다.

ODX가 아닌 파일 전송에서는 소스 CIFS 서버에서 데이터를 읽고 네트워크를 통해 클라이언트 컴퓨터로 전송합니다. 클라이언트 컴퓨터는 네트워크를 통해 대상 CIFS 서버로 데이터를 다시 전송합니다. 요약하면 클라이언트 컴퓨터는 소스에서 데이터를 읽고 대상에 씁니다. ODX 파일 전송을 사용하면 데이터가 소스에서 타겟으로 직접 복사됩니다.

오프로드 복사본은 소스 및 타겟 스토리지 간에 직접 수행되므로 성능이 크게 향상됩니다. 소스 및 대상 간의 복제 시간 단축, 클라이언트의 리소스 활용률(CPU, 메모리) 감소, 네트워크 I/O 대역폭 사용률 감소 등의 성능 이점을 얻을 수 있습니다.

ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

ODX 복사 및 이동 사용을 지원하는 사용 사례는 다음과 같습니다.

- 체내

소스 및 대상 파일 또는 LUN이 동일한 볼륨 내에 있습니다.

- 볼륨 간, 동일한 노드, 동일한 SVM(스토리지 가상 머신)

소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- 볼륨 간, 다른 노드, 동일한 SVM

소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- SVM 간, 동일한 노드

소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- SVM 간, 다른 노드

소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

Hyper-V 솔루션을 사용한 ODX 복사 오프로드의 구체적인 사용 사례는 다음과 같습니다.

- Hyper-V에서 ODX 복사 오프로드 패스스루를 사용하여 VHD(가상 하드 디스크) 파일 내부 또는 VHD 파일 간에 데이터를 복사하거나, 매핑된 SMB 공유와 동일한 클러스터 내에서 연결된 iSCSI LUN 간에 데이터를 복사할 수 있습니다.

이렇게 하면 게스트 운영 체제에서 복제본을 기본 스토리지로 전달할 수 있습니다.

- 고정 크기의 VHD를 생성할 때 ODX는 잘 알려진 제로화 토큰을 사용하여 0으로 디스크를 초기화하는 데 사용됩니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드가 가상 머신 스토리지 마이그레이션에 사용됩니다.



Hyper-V를 사용한 ODX 복사 오프로드 패스쓰루 사용 사례를 활용하려면 게스트 운영 체제가 ODX를 지원하고, 게스트 운영 체제 디스크는 ODX를 지원하는 스토리지(SMB 또는 SAN)를 통해 지원되는 SCSI 디스크여야 합니다. 게스트 운영 체제의 IDE 디스크는 ODX 패스쓰루를 지원하지 않습니다.

SQL Server 솔루션을 사용한 ODX 복사 오프로드의 구체적인 사용 사례는 다음과 같습니다.

- ODX 복사 오프로드를 사용하여 매핑된 SMB 공유 간에 또는 동일한 클러스터 내에서 SMB 공유와 연결된 iSCSI LUN 간에 SQL Server 데이터베이스를 내보내고 가져올 수 있습니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드를 사용하여 데이터베이스를 내보내고 가져올 수 있습니다.

## 구성 요구 사항 및 고려 사항

### ONTAP 및 라이선스 요구 사항

SVM에서 무중단 운영을 위해 SQL Server 또는 Hyper-V over SMB 솔루션을 생성할 때 특정 ONTAP 및 라이선스 요구사항을 알아야 합니다.

#### ONTAP 버전 요구 사항

- SMB를 통한 Hyper-V

ONTAP는 Windows 2012 이상에서 실행되는 Hyper-V에 대해 SMB 공유를 통한 무중단 운영을 지원합니다.

- SMB를 통한 SQL Server

ONTAP는 Windows 2012 이상에서 실행되는 SQL Server 2012 이상에 대해 SMB 공유를 통한 무중단 운영을 지원합니다.

SMB 공유에서 무중단 운영을 지원하는 ONTAP, Windows Server 및 SQL Server의 지원되는 버전에 대한 최신 정보는 상호 운용성 매트릭스를 참조하십시오.

#### "NetApp 상호 운용성 매트릭스 툴"

#### 라이선스 요구 사항

다음 라이선스가 필요합니다.

- CIFS를 선택합니다
- FlexClone(SMB를 통한 Hyper-V만 해당)

원격 VSS를 백업에 사용하는 경우 이 라이선스가 필요합니다. 새도 복사본 서비스는 FlexClone을 사용하여 백업을 만들 때 사용되는 파일의 시점 복사본을 만듭니다.

FlexClone 라이선스는 원격 VSS를 사용하지 않는 백업 방법을 사용하는 경우 선택 사항입니다.

FlexClone 라이선스는 에 포함되어 **"ONTAP 1 을 참조하십시오"** 있습니다. ONTAP One이 없는 경우, **"필요한 라이선스가 설치되어 있는지 확인합니다"** 그리고 필요한 경우, 를 수행해야 **"설치합니다"** 합니다.

#### 네트워크 및 데이터 LIF 요구사항

무중단 운영을 위해 SQL Server 또는 SMB를 통한 Hyper-V 구성을 생성할 때 특정 네트워크 및 데이터 LIF 요구사항을 알고 있어야 합니다.

#### 네트워크 프로토콜 요구 사항

- IPv4 및 IPv6 네트워크가 지원됩니다.
- SMB 3.0 이상이 필요합니다.

SMB 3.0은 무중단 운영을 제공하는 데 필요한 지속적으로 사용 가능한 SMB 연결을 생성하는 데 필요한 기능을 제공합니다.

- DNS 서버에는 SVM(Storage Virtual Machine)의 데이터 LIF에 할당된 IP 주소에 CIFS 서버 이름을 매핑하는 항목이 포함되어 있어야 합니다.

Hyper-V 또는 SQL Server 애플리케이션 서버는 일반적으로 가상 머신 또는 데이터베이스 파일에 액세스할 때 여러 데이터 LIF를 통해 여러 개의 연결을 생성합니다. 적절한 기능을 위해 애플리케이션 서버는 여러 고유 IP 주소에 여러 번 연결하는 대신 CIFS 서버 이름을 사용하여 이러한 여러 SMB 연결을 설정해야 합니다.

또한 감시 기능을 사용하려면 개별 LIF IP 주소 대신 CIFS 서버의 DNS 이름을 사용해야 합니다.

ONTAP 9.4부터 SMB 멀티 채널을 활성화하여 SMB 구성에서 Hyper-V 및 SQL Server의 처리량과 내결함성을 향상시킬 수 있습니다. 이렇게 하려면 클러스터 및 클라이언트에 1G, 10G 또는 더 큰 NIC가 여러 개 설치되어 있어야 합니다.

#### 데이터 LIF 요구사항

- SMB 솔루션을 통해 애플리케이션 서버를 호스팅하는 SVM은 클러스터의 모든 노드에 운영 데이터 LIF가 하나 이상 있어야 합니다.

SVM 데이터 LIF는 애플리케이션 서버에서 액세스하는 데이터를 현재 호스팅하지 않는 노드를 비롯하여 클러스터 내의 다른 데이터 포트에 페일오버할 수 있습니다. 또한 Witness 노드는 항상 애플리케이션 서버가 접속된 노드의 SFO 파트너이므로 클러스터의 모든 노드가 잠재적인 Witness 노드입니다.

- 데이터 LIF가 자동으로 복구되도록 구성하지 않아야 합니다.

테이크오버 또는 반환 이벤트가 발생한 후에는 데이터 LIF를 홈 포트에 수동으로 되돌려야 합니다.

- 모든 데이터 LIF IP 주소에는 DNS에 항목이 있어야 하며 모든 항목이 CIFS 서버 이름으로 확인되어야 합니다.

애플리케이션 서버는 CIFS 서버 이름을 사용하여 SMB 공유에 접속해야 합니다. LIF IP 주소를 사용하여 연결되도록 애플리케이션 서버를 구성하지 마십시오.

- CIFS 서버 이름이 SVM 이름과 다른 경우 DNS 항목이 CIFS 서버 이름으로 확인되어야 합니다.

## SMB를 통한 Hyper-V의 SMB 서버 및 볼륨 요구 사항

무중단 운영을 위해 SMB를 통한 Hyper-V 구성을 생성할 때 특정 SMB 서버 및 볼륨 요구사항을 알고 있어야 합니다.

### SMB 서버 요구 사항

- SMB 3.0을 활성화해야 합니다.

이 기능은 기본적으로 활성화되어 있습니다.

- 기본 UNIX 사용자 CIFS 서버 옵션은 유효한 UNIX 사용자 계정으로 구성해야 합니다.

애플리케이션 서버는 SMB 연결을 생성할 때 컴퓨터 계정을 사용합니다. 모든 SMB 액세스를 위해서는 Windows 사용자가 UNIX 사용자 계정 또는 기본 UNIX 사용자 계정에 성공적으로 매핑되어야 하므로 ONTAP는 애플리케이션 서버의 컴퓨터 계정을 기본 UNIX 사용자 계정에 매핑할 수 있어야 합니다.

- 자동 노드 조회를 비활성화해야 합니다(이 기능은 기본적으로 비활성화되어 있습니다).

Hyper-V 시스템 파일 이외의 데이터에 액세스하기 위해 자동 노드 조회를 사용하려면 해당 데이터에 대해 별도의 SVM을 생성해야 합니다.

- Kerberos 및 NTLM 인증은 SMB 서버가 속한 도메인에서 모두 허용되어야 합니다.

ONTAP는 원격 VSS에 대한 Kerberos 서비스를 광고하지 않으므로 NTLM을 허용하도록 도메인을 설정해야 합니다.

- 새도 복사본 기능이 활성화되어 있어야 합니다.

이 기능은 기본적으로 활성화되어 있습니다.

- 새도 복사본을 만들 때 새도 복사본 서비스가 사용하는 Windows 도메인 계정은 SMB 서버 로컬 BUILTIN\Administrators 또는 BUILTIN\Backup Operators 그룹의 구성원이어야 합니다.

### 볼륨 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

지속적으로 사용 가능한 SMB 연결을 사용하여 애플리케이션 서버에 NDO를 제공하려면 공유가 포함된 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 새도 복사본 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다.

사용 가능한 공간은 새도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다. 이 요구 사항은 자동 복구를 사용하는 새도우 복제본에만 적용됩니다.



## SMB를 통한 SQL Server의 SMB 서버 및 볼륨 요구 사항

무중단 운영을 위해 SMB를 통한 SQL Server 구성을 생성할 때 특정 SMB 서버 및 볼륨 요구사항을 알고 있어야 합니다.

### SMB 서버 요구 사항

- SMB 3.0을 활성화해야 합니다.

이 기능은 기본적으로 활성화되어 있습니다.

- 기본 UNIX 사용자 CIFS 서버 옵션은 유효한 UNIX 사용자 계정으로 구성해야 합니다.

애플리케이션 서버는 SMB 연결을 생성할 때 컴퓨터 계정을 사용합니다. 모든 SMB 액세스를 위해서는 Windows 사용자가 UNIX 사용자 계정 또는 기본 UNIX 사용자 계정에 성공적으로 매핑되어야 하므로 ONTAP는 애플리케이션 서버의 컴퓨터 계정을 기본 UNIX 사용자 계정에 매핑할 수 있어야 합니다.

또한 SQL Server에서는 도메인 사용자를 SQL Server 서비스 계정으로 사용합니다. 서비스 계정도 기본 UNIX 사용자에게 매핑되어야 합니다.

- 자동 노드 조회를 비활성화해야 합니다(이 기능은 기본적으로 비활성화되어 있습니다).

SQL Server 데이터베이스 파일 이외의 데이터에 액세스하기 위해 자동 노드 조회를 사용하려면 해당 데이터에 대해 별도의 SVM을 생성해야 합니다.

- ONTAP에 SQL Server를 설치하는 데 사용되는 Windows 사용자 계정에 SeSecurityPrivilege 권한이 할당되어야 합니다.

이 권한은 SMB 서버 로컬 BUILTINAdministrators 그룹에 할당됩니다.

### 볼륨 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

지속적으로 사용 가능한 SMB 연결을 사용하여 애플리케이션 서버에 NDO를 제공하려면 공유가 포함된 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함한 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 데이터베이스 파일이 포함된 볼륨에는 접합부가 포함될 수 있지만 SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 접합을 교차하지 않습니다.
- Microsoft SQL Server용 SnapCenter 플러그인 백업 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다.

SQL Server 데이터베이스 파일이 있는 볼륨은 데이터베이스 디렉토리 구조와 공유 내에 있는 모든 포함된 파일을 저장할 수 있을 만큼 커야 합니다.

## SMB를 통한 Hyper-V의 지속적인 가용성 공유 요구 사항 및 고려 사항

무중단 운영을 지원하는 SMB 구성을 통해 Hyper-V에서 지속적으로 사용 가능한 공유를 구성할 때 특정 요구사항과 고려 사항을 알고 있어야 합니다.

### 공유 요구 사항

- 응용 프로그램 서버에서 사용하는 공유는 지속적으로 사용 가능한 속성 집합을 사용하여 구성해야 합니다.

지속적으로 사용 가능한 공유에 연결되는 애플리케이션 서버에는 SMB 공유에 중단 없이 다시 연결할 수 있는 영구 핸들이 제공되며, 테이크오버, 반환, 애그리게이트 재배포와 같은 운영 중단 이벤트가 발생한 후 파일 잠금을 재확보할 수 있습니다.

- 원격 VSS 지원 백업 서비스를 사용하려는 경우 집합을 포함하는 공유에 Hyper-V 파일을 넣을 수 없습니다.

자동 복구 사례에서는 공유를 이동하는 동안 분기점이 발생하면 새도우 복제본 생성이 실패합니다. 자동 복구가 아닌 경우 새도우 복제본 생성이 실패하지는 않지만 교차점은 아무 것도 가리키지 않습니다.

- 자동 복구와 함께 원격 VSS 지원 백업 서비스를 사용하려는 경우 다음을 포함하는 공유에 Hyper-V 파일을 넣을 수 없습니다.

- symlinks, hardlinks 또는 wdelink
- 일반 파일이 아닙니다

공유에 새도우 복제본으로 연결되는 링크나 비정규 파일이 있는 경우 새도우 복제본 생성이 실패합니다. 이 요구 사항은 자동 복구를 사용하는 새도우 복제본에만 적용됩니다.

- 새도 복사본 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다(SMB를 통한 Hyper-V만 해당).

사용 가능한 공간은 새도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다. 이 요구 사항은 자동 복구를 사용하는 새도우 복제본에만 적용됩니다.

- 애플리케이션 서버에서 계속 사용 가능한 공유에 대해 다음 공유 속성을 설정하지 않아야 합니다.

- 더 높여 줍니다
- 특성 캐싱
- BranchCache입니다

### 고려 사항

- 할당량은 지속적으로 사용 가능한 공유에서 지원됩니다.
- SMB를 통한 Hyper-V 구성에서는 다음 기능이 지원되지 않습니다.

- 감사
- FPolicy를 참조하십시오

- '연속 가용성' 매개변수가 '예'로 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.

## SMB를 통한 SQL Server의 지속적인 가용성 공유 요구 사항 및 고려 사항

무중단 운영을 지원하는 SMB 구성을 통해 SQL Server에 대해 지속적으로 사용 가능한 공유를 구성할 때 특정 요구사항과 고려 사항을 알고 있어야 합니다.

### 공유 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

지속적으로 사용 가능한 SMB 연결을 통해 애플리케이션 서버에 무중단 운영을 제공하려면 공유를 포함하는 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통한 무중단 운영에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통한 무중단 작업에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 응용 프로그램 서버에서 사용하는 공유는 지속적으로 사용 가능한 속성 집합을 사용하여 구성해야 합니다.

지속적으로 사용 가능한 공유에 연결되는 애플리케이션 서버에는 SMB 공유에 중단 없이 다시 연결할 수 있는 영구 핸들이 제공되며, 테이크오버, 반환, 애그리게이트 재배포와 같은 운영 중단 이벤트가 발생한 후 파일 잠금을 재확보할 수 있습니다.

- 데이터베이스 파일이 포함된 볼륨에는 접합부가 포함될 수 있지만 SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 접합을 교차하지 않습니다.
- Microsoft SQL Server용 SnapCenter 플러그인을 성공적으로 사용하려면 볼륨에 충분한 공간이 있어야 합니다.

SQL Server 데이터베이스 파일이 있는 볼륨은 데이터베이스 디렉토리 구조와 공유 내에 있는 모든 포함된 파일을 저장할 수 있을 만큼 커야 합니다.

- 애플리케이션 서버에서 계속 사용 가능한 공유에 대해 다음 공유 속성을 설정하지 않아야 합니다.
  - 더 높여 줍니다
  - 특성 캐싱
  - BranchCache입니다

### 공유 고려 사항

- 할당량은 지속적으로 사용 가능한 공유에서 지원됩니다.
- SMB를 통한 SQL Server 구성에서는 다음 기능이 지원되지 않습니다.
  - 감사
  - FPolicy를 참조하십시오
- 지속적으로 사용 가능한 공유 자산이 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.

## SMB 구성을 통한 Hyper-V에 대한 원격 VSS 고려 사항

SMB를 통한 Hyper-V 구성에 대해 원격 VSS 지원 백업 솔루션을 사용할 때는 특정 고려 사항을 염두에 두어야 합니다.

## 일반 원격 VSS 고려 사항

- Microsoft 애플리케이션 서버당 최대 64개의 공유를 구성할 수 있습니다.

새도우 복제본 세트에 64개 이상의 공유가 있는 경우 새도우 복제본 작업이 실패합니다. 이는 Microsoft의 요구 사항입니다.

- CIFS 서버당 하나의 활성 새도 복사본 세트만 허용됩니다.

동일한 CIFS 서버에 새도우 복제본 작업이 진행 중인 경우 새도우 복제본 작업이 실패합니다. 이는 Microsoft의 요구 사항입니다.

- 원격 VSS가 새도우 복제본을 생성하는 디렉토리 구조 내에서는 접합을 수행할 수 없습니다.
  - 자동 복구 사례에서는 공유를 이동하는 동안 분기점이 발생하면 새도우 복제본 생성이 실패합니다.
  - 비자동 복구 사례에서는 새도우 복제본 생성이 실패하지 않지만 접합은 아무 것도 가리키지 않습니다.

## 자동 복구를 사용하는 새도우 복제본에만 적용되는 원격 VSS 고려 사항

자동 복구를 사용하는 새도 복사본에만 특정 제한사항이 적용됩니다.

- 새도우 복제본 생성에는 하위 디렉토리 5개의 최대 디렉토리 수준이 허용됩니다.

새도우 복제본 서비스가 새도우 복제본 백업 세트를 생성하는 디렉토리 깊이입니다. 가상 머신 파일이 포함된 디렉토리가 5개 수준 이상 중첩되면 새도우 복제본 생성이 실패합니다. 이는 공유를 복제할 때 디렉토리 트래버설을 제한하기 위한 것입니다. 최대 디렉토리 깊이는 CIFS 서버 옵션을 사용하여 변경할 수 있습니다.

- 볼륨의 사용 가능한 공간이 적절해야 합니다.

사용 가능한 공간은 새도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다.

- 원격 VSS가 새도우 복제본을 생성하는 디렉토리 구조 내에서 링크나 일반 파일이 허용되지 않습니다.

공유에 새도 복사본에 대한 링크 또는 비정규 파일이 있는 경우 새도 복사본 생성이 실패합니다. 클론 프로세스에서 이를 지원하지 않습니다.

- 디렉토리에는 NFSv4 ACL이 허용되지 않습니다.

새도우 복제본 생성이 파일에 NFSv4 ACL을 유지하지만 디렉토리의 NFSv4 ACL이 손실됩니다.

- 새도 복사본 세트를 생성할 수 있는 시간은 최대 60초입니다.

Microsoft 사양은 새도 복사본 세트를 생성하는 데 최대 60초를 허용합니다. VSS 클라이언트가 이 시간 내에 새도우 복제본 세트를 생성할 수 없는 경우 새도우 복제본 작업이 실패하므로 새도우 복제본 세트의 파일 수가 제한됩니다. 백업 세트에 포함될 수 있는 실제 파일 또는 가상 머신 수는 서로 다르며, 이 수는 여러 요인에 따라 달라지며 각 고객 환경에 따라 결정되어야 합니다.

## ODX SMB를 통한 SQL Server 및 Hyper-V의 복사 오프로드 요구 사항

가상 머신 파일을 마이그레이션하거나 애플리케이션 서버를 통해 데이터를 전송하지 않고 데이터베이스 파일을 소스에서 대상 스토리지 위치로 직접 내보내고 가져오려면 ODX 복사

오프로드를 활성화해야 합니다. SQL Server에서 ODX 복사 오프로드를 사용하고 SMB 솔루션을 통해 Hyper-V를 사용하는 것에 대해 이해해야 하는 특정 요구사항이 있습니다.

ODX 복사 오프로드를 사용하면 성능을 대폭 향상할 수 있습니다. 이 CIFS 서버 옵션은 기본적으로 설정되어 있습니다.

- ODX 복사 오프로드를 사용하려면 SMB 3.0을 설정해야 합니다.
- 소스 볼륨은 최소 1.25GB여야 합니다.
- 복사본 오프로드와 함께 사용되는 볼륨에 대해 중복제거를 활성화해야 합니다.
- 압축 볼륨을 사용하는 경우 압축 유형은 적용 가능해야 하며 압축 그룹 크기 8K만 지원됩니다.

보조 압축 유형은 지원되지 않습니다

- ODX 복사 오프로드를 사용하여 디스크 내부 및 디스크 간에 Hyper-V 게스트를 마이그레이션하려면 SCSI 디스크를 사용하도록 Hyper-V 서버를 구성해야 합니다.

기본값은 IDE 디스크를 구성하는 것이지만, 디스크가 IDE 디스크를 사용하여 생성된 경우 게스트가 마이그레이션될 때 ODX 복사 오프로드가 작동하지 않습니다.

## SMB 구성을 통한 SQL Server 및 Hyper-V 권장 사항

SQL Server 및 Hyper-V over SMB 구성이 강력하고 작동 가능한지 확인하려면 솔루션 구성 시 권장 모범 사례를 숙지해야 합니다.

### 일반 권장 사항

- 일반 사용자 데이터와 애플리케이션 서버 파일을 분리합니다.  
가능하면 전체 SVM(스토리지 가상 시스템)과 해당 스토리지를 애플리케이션 서버의 데이터에 사용합니다.
- 최상의 성능을 위해 SVM에서 애플리케이션 서버의 데이터를 저장하는 데 사용되는 SMB 서명을 활성화하지 마십시오.
- 최상의 성능과 향상된 내결함성을 위해 SMB 멀티 채널을 통해 단일 SMB 세션에서 ONTAP과 클라이언트 간에 여러 개의 연결을 제공할 수 있습니다.
- Hyper-V 또는 SQL Server over SMB 구성에서 사용되는 공유 이외의 공유에 대해 지속적으로 사용 가능한 공유를 생성하지 마십시오.
- 지속적인 가용성에 사용되는 공유에 대한 변경 알림을 해제합니다.
- ARL에는 일부 작업을 일시 중지하는 단계가 있으므로 ARL(Aggregate relocation)과 동시에 볼륨 이동을 수행하지 마십시오.
- SMB를 통한 Hyper-V 솔루션의 경우 클러스터 가상 머신을 생성할 때 게스트 내 iSCSI 드라이브를 사용합니다. 공유 '.vHDX' 파일은 ONTAP SMB 공유에서 SMB를 통한 Hyper-V에 지원되지 않습니다.

## SMB를 통한 Hyper-V 또는 SQL Server 구성 계획

볼륨 구성 워크시트를 작성합니다

이 워크시트는 SMB 구성을 통해 SQL Server 및 Hyper-V용 볼륨을 생성할 때 필요한 값을 쉽게

기록할 수 있는 방법을 제공합니다.

각 볼륨에 대해 다음 정보를 지정해야 합니다.

- 스토리지 가상 시스템(SVM) 이름

SVM 이름은 모든 볼륨에서 동일합니다.

- 볼륨 이름입니다
- 애그리게이트 이름입니다

클러스터의 노드에 있는 애그리게이트에 볼륨을 생성할 수 있습니다.

- 크기
- 접합 경로

애플리케이션 서버 데이터를 저장하는 데 사용되는 볼륨을 생성할 때 다음 사항을 염두에 두어야 합니다.

- 루트 볼륨에 NTFS 보안 스타일이 없는 경우 볼륨을 생성할 때 보안 스타일을 NTFS로 지정해야 합니다.

기본적으로 볼륨은 SVM 루트 볼륨의 보안 스타일을 상속합니다.

- 볼륨은 기본 볼륨 공간 보장으로 구성해야 합니다.
- 필요에 따라 공간 자동 크기 조정 관리 설정을 구성할 수 있습니다.
- 스냅샷 공간 예비 공간을 결정하는 옵션을 로 '0' 설정해야 합니다.
- 볼륨에 적용된 스냅샷 정책을 해제해야 합니다.

SVM 스냅샷 정책이 해제되어 있으면 볼륨에 대한 스냅샷 정책을 지정할 필요가 없습니다. 볼륨은 SVM에 대한 스냅샷 정책을 상속합니다. SVM에 대한 스냅샷 정책이 해제되지 않고 스냅샷을 생성하도록 구성된 경우 볼륨 레벨에서 스냅샷 정책을 지정해야 하며 해당 정책을 비활성화해야 합니다. 새도 복사본 서비스 가능 백업 및 SQL Server 백업은 스냅샷 생성 및 삭제를 관리합니다.

- 볼륨에 대한 로드 공유 미러는 구성할 수 없습니다.

공유 진입점 아래에 접합된 볼륨이 없도록 애플리케이션 서버가 사용하는 공유를 생성하려는 연결 경로를 선택해야 합니다.

예를 들어, 가상 시스템 파일을 ""vol1"", ""vol2", ""vol3"" 및 ""vol4""라는 네 개의 볼륨에 저장하려면 예제에 표시된 네임스페이스를 생성할 수 있습니다. 그런 다음 '/data1/vol1', '/data1/vol2', '/data2/vol3', '/data2/vol4' 경로에서 애플리케이션 서버에 대한 공유를 생성할 수 있습니다.

| Vserver | Volume | Junction |  | Junction Path | Junction Path Source |
|---------|--------|----------|--|---------------|----------------------|
|         |        | Active   |  |               |                      |
| vs1     | data1  | true     |  | /data1        | RW_volume            |
| vs1     | vol1   | true     |  | /data1/vol1   | RW_volume            |
| vs1     | vol2   | true     |  | /data1/vol2   | RW_volume            |
| vs1     | data2  | true     |  | /data2        | RW_volume            |
| vs1     | vol3   | true     |  | /data2/vol3   | RW_volume            |
| vs1     | vol4   | true     |  | /data2/vol4   | RW_volume            |

| 정보 유형                                 | 값 |
|---------------------------------------|---|
| _Volume 1: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _ |   |
| _Volume 2: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _ |   |
| _Volume 3: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _ |   |
| _Volume 4: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _ |   |
| _Volume 5: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _ |   |
| _Volume 6: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _ |   |
| _추가 볼륨: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _    |   |

**SMB** 공유 구성 워크시트를 작성합니다

이 워크시트를 사용하여 SMB 구성에서 SQL Server 및 Hyper-V에 대해 지속적으로 사용 가능한 SMB 공유를 생성할 때 필요한 값을 기록하십시오.

**SMB** 공유 속성 및 구성 설정에 대한 정보입니다

각 공유에 대해 다음 정보를 지정해야 합니다.

- 스토리지 가상 시스템(SVM) 이름

SVM 이름은 모든 공유에서 동일합니다

- 공유 이름
- 경로
- 공유 속성

다음 두 공유 속성을 구성해야 합니다.

- oplocks
- "계속 사용할 수 있습니다.

다음 공유 속성을 설정하지 않아야 합니다.

- 홈디렉토리 attributecache
- 브랜치캐시
- '액세스 기반 열거'
  - symlinks를 비활성화해야 합니다('symlink-properties' 매개 변수의 값은 null [""] 이어야 함).

공유 경로에 대한 정보입니다

원격 VSS를 사용하여 Hyper-V 파일을 백업하는 경우 Hyper-V 서버에서 가상 머신 파일이 저장된 스토리지 위치로 SMB 연결을 설정할 때 사용할 공유 경로를 선택해야 합니다. 네임스페이스에서 어느 지점에서나 공유를 생성할 수 있지만 Hyper-V 서버가 사용하는 공유의 경로에 접합된 볼륨이 포함되어서는 안 됩니다. 교차점이 포함된 공유 경로에서는 새도 복사본 작업을 수행할 수 없습니다.

SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 교차점을 교차할 수 없습니다. 교차점이 포함된 SQL Server에 대한 공유 경로를 생성할 수 없습니다.

예를 들어, 표시된 네임스페이스를 사용할 경우 가상 머신 파일 또는 데이터베이스 파일을 볼륨 ""vol1"", ""vol2"", ""vol3"", ""vol4""에 저장하려면 "/data1/vol1", "/data1/vol2", "/data2/data4" 경로에 애플리케이션 서버의 공유를 생성해야 합니다.

| Vserver | Volume | Junction |               | Junction Path Source |
|---------|--------|----------|---------------|----------------------|
|         |        | Active   | Junction Path |                      |
| vs1     | data1  | true     | /data1        | RW_volume            |
| vs1     | vol1   | true     | /data1/vol1   | RW_volume            |
| vs1     | vol2   | true     | /data1/vol2   | RW_volume            |
| vs1     | data2  | true     | /data2        | RW_volume            |
| vs1     | vol3   | true     | /data2/vol3   | RW_volume            |
| vs1     | vol4   | true     | /data2/vol4   | RW_volume            |



관리 관리를 위해 및 /data2 경로에 공유를 만들 수 있지만 /data1, 애플리케이션 서버가 이러한 공유를 사용하여 데이터를 저장하도록 구성하지 마십시오.

계획 워크시트

| 정보 유형                       | 값 |
|-----------------------------|---|
| _볼륨 1: SMB 공유 이름 및 경로 _     |   |
| _Volume 2: SMB 공유 이름 및 경로 _ |   |
| _Volume 3: SMB 공유 이름 및 경로 _ |   |



| 정보 유형                       | 값 |
|-----------------------------|---|
| _Volume 4: SMB 공유 이름 및 경로 _ |   |
| _Volume 5: SMB 공유 이름 및 경로 _ |   |
| _Volume 6: SMB 공유 이름 및 경로 _ |   |
| _Volume 7: SMB 공유 이름 및 경로 _ |   |
| _추가 볼륨: SMB 공유 이름 및 경로 _    |   |

## SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 생성

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 개요를 제공합니다

SMB를 통한 무중단 운영을 제공하는 Hyper-V 및 SQL Server 설치를 준비하기 위해 수행해야 하는 몇 가지 ONTAP 구성 단계가 있습니다.

SMB를 통해 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성을 생성하기 전에 다음 작업을 완료해야 합니다.

- 클러스터에서 시간 서비스를 설정해야 합니다.
- SVM에 대해 네트워킹을 설정해야 합니다.
- SVM을 생성해야 합니다.
- 데이터 LIF 인터페이스는 SVM에서 구성해야 합니다.
- SVM에서 DNS를 구성해야 합니다.
- SVM에 대해 원하는 이름 서비스를 설정해야 합니다.
- SMB 서버를 생성해야 합니다.

관련 정보

[SMB를 통한 Hyper-V 또는 SQL Server 구성 계획](#)

[구성 요구 사항 및 고려 사항](#)

### Kerberos 및 NTLMv2 인증이 모두 허용되는지 확인(SMB 공유를 통한 Hyper-V)

SMB를 통한 Hyper-V의 무중단 운영에서는 데이터 SVM 및 Hyper-V 서버의 CIFS 서버가 Kerberos 및 NTLMv2 인증을 모두 허용해야 합니다. 허용되는 인증 방법을 제어하는 CIFS 서버와 Hyper-V 서버 모두에서 설정을 확인해야 합니다.

이 작업에 대해

지속적으로 사용 가능한 공유 연결을 만들 때는 Kerberos 인증이 필요합니다. 원격 VSS 프로세스의 일부는 NTLMv2 인증을 사용합니다. 따라서 SMB를 통한 Hyper-V 구성에서는 두 인증 방법을 모두 사용하는 연결이 지원되어야 합니다.

Kerberos 및 NTLMv2 인증을 모두 허용하도록 다음 설정을 구성해야 합니다.

- 스토리지 가상 시스템(SVM)에서 SMB를 위한 익스포트 정책을 사용하지 않도록 설정해야 합니다.

Kerberos 및 NTLMv2 인증은 항상 SVM에서 활성화되지만, 익스포트 정책을 사용하여 인증 방법에 따라 액세스를 제한할 수 있습니다.

SMB에 대한 익스포트 정책은 선택 사항이며 기본적으로 비활성화되어 있습니다. 내보내기 정책을 사용하지 않도록 설정하면 기본적으로 CIFS 서버에서 Kerberos 및 NTLMv2 인증이 모두 허용됩니다.

- CIFS 서버 및 Hyper-V 서버가 속하는 도메인은 Kerberos 및 NTLMv2 인증을 모두 허용해야 합니다.

Kerberos 인증은 Active Directory 도메인에서 기본적으로 활성화됩니다. 그러나 보안 정책 설정 또는 그룹 정책을 사용하여 NTLMv2 인증을 허용하지 않을 수 있습니다.

단계

1. SVM에서 익스포트 정책이 비활성화되어 있는지 확인하려면 다음을 수행하십시오.

- a. 권한 수준을 고급으로 설정합니다.

```
' * set-Privilege advanced * '
```

- b. '-is-exportpolicy-enabled' CIFS server 옵션이 'false'로 설정되어 있는지 확인합니다.

```
* vserver cifs options show -vserver_vserver_name_fields vserver, is-exportpolicy-enabled *
```

- c. 관리자 권한 레벨로 돌아갑니다.

```
' * set-privilege admin * '
```

2. SMB에 대한 익스포트 정책이 비활성화되어 있지 않으면 다음을 비활성화하십시오.

```
* vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled false *
```

3. 도메인에서 NTLMv2 및 Kerberos 인증이 모두 허용되는지 확인합니다.

도메인에서 허용되는 인증 방법을 결정하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

4. 도메인이 NTLMv2 인증을 허용하지 않는 경우 Microsoft 설명서에 설명된 방법 중 하나를 사용하여 NTLMv2 인증을 사용하도록 설정합니다.

예

다음 명령을 실행하면 SVM VS1 에서 SMB용 익스포트 정책이 비활성화되어 있는지 확인할 수 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vservers cifs options show -vservers vs1 -fields vservers,is-
exportpolicy-enabled

vservers is-exportpolicy-enabled
----- -
vs1 false

cluster1::*> set -privilege admin
```

도메인 계정이 **ONTAP**의 기본 **UNIX** 사용자에게 매핑되는지 확인합니다

Hyper-V 및 SQL Server는 도메인 계정을 사용하여 지속적으로 사용 가능한 공유에 대한 SMB 연결을 생성합니다. 연결을 성공적으로 생성하려면 컴퓨터 계정이 UNIX 사용자에게 성공적으로 매핑되어야 합니다. 이 작업을 수행하는 가장 편리한 방법은 컴퓨터 계정을 기본 UNIX 사용자에게 매핑하는 것입니다.

이 작업에 대해

Hyper-V 및 SQL Server는 도메인 컴퓨터 계정을 사용하여 SMB 연결을 만듭니다. 또한 SQL Server는 도메인 사용자 계정을 서비스 계정으로 사용하여 SMB 연결을 만듭니다.

스토리지 가상 머신(SVM)을 생성하면 ONTAP에서 자동으로 기본 사용자 이름을 생성합니다. pcuser (UID가 있는 65534) 및 그룹 이름 pcuser (GID가 있는 65534), 그리고 기본 사용자를 추가합니다. pcuser 그룹. 클러스터를 Data ONTAP 8.2로 업그레이드하기 전에 존재했던 SVM에서 SMB를 통한 Hyper-V 솔루션을 구성하는 경우 기본 사용자 및 그룹이 없을 수 있습니다. 그렇지 않으면 CIFS 서버의 기본 UNIX 사용자를 구성하기 전에 생성해야 합니다.

단계

1. 기본 UNIX 사용자가 있는지 확인합니다.

```
vservers cifs options show -vservers <vservers_name>
```

2. 기본 사용자 옵션이 설정되지 않은 경우 기본 UNIX 사용자로 지정할 수 있는 UNIX 사용자가 있는지 확인합니다.

```
vservers services unix-user show -vservers <vservers_name>
```

3. 기본 사용자 옵션이 설정되어 있지 않고 기본 UNIX 사용자로 지정할 수 있는 UNIX 사용자가 없는 경우, 기본 그룹과 기본 UNIX 사용자를 만들고, 기본 사용자를 그룹에 추가합니다.
4. 기본 그룹에는 일반적으로 "pcuser"라는 그룹 이름이 지정됩니다 그룹에 할당된 GID는 65534 이어야 합니다.
  - a. 기본 그룹을 만듭니다.

```
vserver services unix-group create -vserver <vserver_name> -name pcuser -id 65534
```

- b. 기본 사용자를 만들고 기본 그룹에 기본 사용자를 추가합니다.

```
vserver services unix-user create -vserver <vserver_name> -user pcuser -id 65534 -primary-gid 65534
```

- c. 기본 사용자와 기본 그룹이 올바르게 구성되었는지 확인하세요.

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

5. CIFS 서버의 기본 사용자가 구성되지 않은 경우 다음을 수행합니다.

- a. 기본 사용자를 구성합니다.

```
vserver cifs options modify -vserver <vserver_name> -default-unix -user pcuser
```

- b. 기본 UNIX 사용자가 올바르게 구성되었는지 확인합니다.

```
vserver cifs options show -vserver <vserver_name>
```

6. 애플리케이션 서버의 컴퓨터 계정이 기본 사용자에게 올바르게 매핑되었는지 확인하려면 SVM에 상주하는 공유에 드라이브를 매핑하고 "vserver cifs session show" 명령을 사용하여 Windows 사용자를 UNIX 사용자 매핑으로 확인합니다.

에 대한 자세한 내용은 vserver cifs options ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

예

존재합니다. pcuser 사용자는 SVM vs1에서 CIFS 서버의 기본 사용자로 지정됩니다.

```
cluster1::> vserver cifs options show

Vserver: vs1

Client Session Timeout : 900
Default Unix Group : -
```

```

Default Unix User : -
Guest Unix User : -
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -

```

```
cluster1::> vservice unix-user show
```

| Vserver | User Name | User ID | Group ID | Full Name |
|---------|-----------|---------|----------|-----------|
| vs1     | nobody    | 65535   | 65535    | -         |
| vs1     | pcuser    | 65534   | 65534    | -         |
| vs1     | root      | 0       | 1        | -         |

```
cluster1::> vservice unix-group show -members
```

| Vserver | Name     | ID    |
|---------|----------|-------|
| vs1     | daemon   | 1     |
|         | Users: - |       |
| vs1     | nobody   | 65535 |
|         | Users: - |       |
| vs1     | pcuser   | 65534 |
|         | Users: - |       |
| vs1     | root     | 0     |
|         | Users: - |       |

```
cluster1::> vservice cifs options modify -vserver vs1 -default-unix-user pcuser
```

```
cluster1::> vservice cifs options show
```

```
Vserver: vs1
```

```

Client Session Timeout : 900
Default Unix Group : -
Default Unix User : pcuser
Guest Unix User : -
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -

```

**SVM** 루트 볼륨의 보안 스타일이 **NTFS**로 설정되어 있는지 확인합니다

Hyper-V 및 SQL Server over SMB의 무중단 운영이 성공하려면 NTFS 보안 스타일로 볼륨을 만들어야 합니다. 루트 볼륨의 보안 스타일은 SVM(스토리지 가상 머신)에서 생성된 볼륨에

기본적으로 적용되므로 루트 볼륨의 보안 스타일을 NTFS로 설정해야 합니다.

이 작업에 대해

- SVM을 생성할 때 루트 볼륨 보안 스타일을 지정할 수 있습니다.
- 루트 볼륨이 NTFS 보안 스타일로 설정되어 있는 SVM이 생성되지 않으면 나중에 'volume modify' 명령을 사용하여 보안 스타일을 변경할 수 있습니다.

단계

1. SVM 루트 볼륨의 현재 보안 유형을 확인합니다.

```
* volume show -vserver _vserver_name_ - 필드 vserver, 볼륨, 보안 스타일 *
```

2. 루트 볼륨이 NTFS 보안 스타일 볼륨이 아닌 경우 보안 스타일을 NTFS로 변경합니다.

```
* volume modify -vserver _vserver_name_ -volume root_volume_name -security-style NTFS *
```

3. SVM 루트 볼륨이 NTFS 보안 스타일로 설정되었는지 확인합니다.

```
* volume show -vserver _vserver_name_ - 필드 vserver, 볼륨, 보안 스타일 *
```

예

다음 명령은 SVM VS1 에서 루트 볼륨 보안 스타일이 NTFS인지 확인합니다.

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver volume security-style

vs1 vs1_root unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver volume security-style

vs1 vs1_root ntfs
```

필요한 **CIFS** 서버 옵션이 구성되었는지 확인합니다

필요한 CIFS 서버 옵션이 Hyper-V 및 SQL Server over SMB의 무중단 운영 요구 사항에 따라 설정 및 구성되었는지 확인해야 합니다.

이 작업에 대해

- SMB 2.x 및 SMB 3.0을 활성화해야 합니다.
- ODX 복사 오프로드를 사용하여 성능을 향상시키려면 ODX 복사 오프로드를 활성화해야 합니다.
- Hyper-V over SMB 솔루션에서 원격 VSS 지원 백업 서비스를 사용하는 경우 VSS Shadow Copy 서비스를 활성화해야 합니다(Hyper-V만 해당).

## 단계

1. 필요한 CIFS 서버 옵션이 SVM(스토리지 가상 시스템)에서 설정되었는지 확인합니다.

a. 권한 수준을 고급으로 설정합니다.

```
' * set-Privilege advanced * '
```

b. 다음 명령을 입력합니다.

```
* vserver CIFS options show -vserver_vserver_name_ *
```

다음 옵션은 "참"으로 설정해야 합니다.

- '-SMB2-ENABLED'입니다
- '-SMB3-enabled'입니다
- '-copy-offload-enabled'
- '-shadowcopy -enabled'(Hyper-V만 해당)

2. "참"으로 설정되어 있지 않은 옵션이 있는 경우 다음을 수행하십시오.

a. vserver cifs options modify 명령을 사용하여 "true"로 설정합니다.

b. vserver cifs options show 명령을 사용하여 옵션이 "true"로 설정되어 있는지 확인합니다.

3. 관리자 권한 레벨로 돌아갑니다.

```
' * set-privilege admin * '
```

## 예

다음 명령은 SVM VS1 기반 Hyper-V 구성에 필요한 옵션이 설정되어 있는지 확인합니다. 이 예에서는 옵션 요구 사항을 충족하도록 ODX 복사 오프로드를 활성화해야 합니다.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vservers cifs options show -vservers vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vservers smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled

vs1 true true false true

cluster-1::*> vservers cifs options modify -vservers vs1 -copy-offload
-enabled true

cluster-1::*> vservers cifs options show -vservers vs1 -fields copy-offload-
enabled
vservers copy-offload-enabled

vs1 true

cluster1::*> set -privilege admin

```

성능 및 이중화를 위해 **SMB** 멀티 채널을 구성합니다

ONTAP 9.4부터 SMB 다중 채널을 구성하여 단일 SMB 세션에서 ONTAP과 클라이언트 간에 여러 연결을 제공할 수 있습니다. 이렇게 하면 SMB 구성에서 Hyper-V 및 SQL Server의 처리량과 내결함성을 향상시킬 수 있습니다.

시작하기 전에

SMB 3.0 이상 버전에서 클라이언트가 협상하는 경우에만 SMB 멀티 채널 기능을 사용할 수 있습니다. SMB 3.0 이상은 기본적으로 ONTAP SMB 서버에서 사용하도록 설정됩니다.

이 작업에 대해

ONTAP 클러스터에서 적절한 구성이 식별되는 경우 SMB 클라이언트가 자동으로 여러 네트워크 연결을 감지하고 사용합니다.

SMB 세션의 동시 연결 수는 구축한 NIC에 따라 달라집니다.

- \* 클라이언트와 ONTAP 클러스터의 1G NIC \*

클라이언트는 NIC당 하나의 연결을 설정하고 모든 연결에 세션을 바인딩합니다.

- \* 클라이언트 및 ONTAP 클러스터에 10G 이상의 대용량 NIC \*

클라이언트는 NIC당 최대 4개의 연결을 설정하고 모든 연결에 세션을 바인딩합니다. 클라이언트는 여러 개의 10G 및 대용량 NIC에 연결을 설정할 수 있습니다.



다음 매개 변수(고급 권한)도 수정할 수 있습니다.

- `-max-connections-per-session`

다중 채널 세션당 허용되는 최대 연결 수입니다. 기본값은 32개 연결입니다.

기본값보다 더 많은 연결을 설정하려면 기본값인 32개의 연결을 사용하는 클라이언트 구성을 동일하게 조정해야 합니다.

- `-max-lifs-per-session`

Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 기본값은 256개의 네트워크 인터페이스입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. SMB 서버에서 SMB 멀티 채널 활성화:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAP가 SMB 멀티 채널 세션을 보고하는지 확인합니다.

```
vserver cifs session show
```

4. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

예

다음 예에서는 모든 SMB 세션에 대한 정보를 표시하며 단일 세션에 대해 여러 개의 연결을 표시합니다.

```
cluster1::> vserver cifs session show
Node: node1
Vserver: vs1
Connection Session Open
Idle
IDs ID Workstation Windows User Files
Time

138683,
138684,
138685 1 10.1.1.1 DOMAIN\
4s Administrator
0
```

다음 예에서는 세션 ID 1이 있는 SMB 세션에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

**NTFS** 데이터 볼륨을 생성합니다

Hyper-V 또는 SQL Server over SMB 애플리케이션 서버에서 사용할 수 있도록 지속적으로 사용 가능한 공유를 구성하려면 먼저 SVM(스토리지 가상 머신)에 NTFS 데이터 볼륨을

생성해야 합니다. 볼륨 구성 워크시트를 사용하여 데이터 볼륨을 생성합니다.

이 작업에 대해

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 선택적 매개 변수가 있습니다. 볼륨 사용자 지정에 대한 자세한 내용은 [참조하십시오 "논리적 스토리지 관리"](#).

데이터 볼륨을 생성할 때 다음을 포함하는 볼륨 내에 교차점을 생성해서는 안 됩니다.

- ONTAP에서 새도 복사본을 만드는 Hyper-V 파일입니다
- SQL Server를 사용하여 백업되는 SQL Server 데이터베이스 파일입니다



혼합 또는 UNIX 보안 스타일을 사용하는 볼륨을 실수로 만든 경우 볼륨을 NTFS 보안 스타일 볼륨으로 변경한 다음 이 볼륨을 직접 사용하여 무중단 운영을 위해 지속적으로 사용 가능한 공유를 생성할 수 없습니다. Hyper-V 및 SQL Server over SMB의 무중단 운영은 구성에 사용된 볼륨이 NTFS 보안 스타일 볼륨으로 만들어지지 않는 한 제대로 작동하지 않습니다. 볼륨을 삭제하고 NTFS 보안 스타일로 볼륨을 다시 생성해야 합니다. 또는 Windows 호스트에서 볼륨을 매핑하고 볼륨 상단에 ACL을 적용하고 볼륨의 모든 파일 및 폴더에 ACL을 전파할 수 있습니다.

단계

1. 적절한 명령을 입력하여 데이터 볼륨을 생성합니다.

|                                              |                                                                                                                                                                    |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SVM</b> 에서 루트 볼륨 보안 유형이 인 볼륨을 생성하려는 경우... | 명령 입력...                                                                                                                                                           |
| NTFS입니다                                      | <code>* volume create -vserverserver_name -volume volume_name - aggregate aggregate_name -size 정수 [KB MB GB TB PB]-junction-path_path_ *</code>                    |
| NTFS가 아닙니다                                   | <code>* volume create -vserverserver_name -volume volume_name - aggregate aggregate_name -size integer [KB MB GB TB PB]-security-style NTFS-junction-path *</code> |

2. 볼륨 구성이 올바른지 확인합니다.

`* volume show -vserverserver_name -volume volume_name *`

지속적으로 사용 가능한 **SMB** 공유를 생성합니다

데이터 볼륨을 생성한 후 애플리케이션 서버가 Hyper-V 가상 머신 및 구성 파일, SQL Server 데이터베이스 파일에 액세스하는 데 사용하는 연속 사용 가능한 공유를 생성할 수 있습니다. SMB 공유를 생성할 때 공유 구성 워크시트를 사용해야 합니다.

단계

1. 기존 데이터 볼륨 및 연결 경로에 대한 정보를 표시합니다.

`* volume show -vserverserver_name -junction *`

2. 지속적으로 사용 가능한 SMB 공유 생성:

```
* vserver CIFS 공유 create-vserver_vserver_name_-share-name_share_name_-path_path_-share-
properties oplocks, Continuously-available-symlink""[-comment text] *
```

- 필요에 따라 공유 구성에 주석을 추가할 수 있습니다.
- 기본적으로 오프라인 파일 공유 속성은 공유에서 구성되며 '수동'으로 설정됩니다.
- ONTAP는 Everyone/Full Control의 Windows 기본 공유 권한으로 공유를 생성합니다.

3. 공유 구성 워크시트의 모든 공유에 대해 이전 단계를 반복합니다.

4. 'vserver cifs share show' 명령을 사용하여 구성이 올바른지 확인하십시오.

5. 드라이브를 각 공유에 매핑하고 \* Windows 속성 \* 창을 사용하여 파일 권한을 구성하여 지속적으로 사용 가능한 공유에서 NTFS 파일 권한을 구성합니다.

예

다음 명령을 실행하면 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 에 "data2"라는 이름의 연속 사용 가능한 공유가 생성됩니다. '-symlink' 매개변수를 ""로 설정하면 Symlink가 비활성화됩니다.

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Active | Junction Path | Junction Path Source |
|---------|----------|--------|---------------|----------------------|
| vs1     | data     | true   | /data         | RW_volume            |
| vs1     | data1    | true   | /data/data1   | RW_volume            |
| vs1     | data2    | true   | /data/data2   | RW_volume            |
| vs1     | vs1_root | -      | /             | -                    |

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
 continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

**seSecurityPrivilege** 권한을 사용자 계정에 추가합니다(**SMB** 공유의 **SQL Server**에 해당).

SQL Server 설치에 사용되는 도메인 사용자 계정에는 "**seSecurityPrivilege**" 권한이 할당되어 있어야 도메인 사용자에게 기본적으로 할당되지 않은 권한이 필요한 CIFS 서버에서 특정 작업을 수행할 수 있습니다.

시작하기 전에

SQL Server 설치에 사용되는 도메인 계정이 이미 있어야 합니다.

이 작업에 대해

SQL Server 설치 관리자의 계정에 권한을 추가할 때 ONTAP은 도메인 컨트롤러에 연락하여 계정의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

단계

1. "**seSecurityPrivilege**" 권한 추가:

```
* vserver cifs users-and-groups 권한 add-privilege-vserver_vserver_name_-user-or-group-
name_account_name_-Privileges SeSecurityPrivilege*
```

'-user-or-group-name' 매개 변수의 값은 SQL Server 설치에 사용되는 도메인 사용자 계정의 이름입니다.

2. 계정에 권한이 적용되는지 확인합니다.

```
* vserver cifs users-and-groups 권한 show -vserver_vserver_name_-user-or-group
-name_account_name_*
```

예

다음 명령을 실행하면 SVM(Storage Virtual Machine) VS1 예제 도메인의 SQL Server 설치 관리자 계정에 "**seSecurityPrivilege**" 권한이 추가됩니다.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 EXAMPLE\SQLinstaller SeSecurityPrivilege
```

**VSS** 새도우 복제본 디렉토리 깊이 구성(**SMB** 공유를 통한 **Hyper-V**의 경우)

필요에 따라 **SMB** 공유 내에서 새도우 복제본을 생성할 디렉토리의 최대 깊이를 구성할 수 있습니다. 이 매개 변수는 ONTAP에서 새도 복사본을 만들어야 하는 하위 디렉토리의 최대 수준을 수동으로 제어하려는 경우에 유용합니다.

시작하기 전에

VSS 새도우 복제본 기능을 활성화해야 합니다.

이 작업에 대해

기본값은 최대 5개의 하위 디렉토리에 대한 새도우 복제본을 생성하는 것입니다. 이 값이 '0'으로 설정되면 ONTAP는 모든 하위 디렉토리에 대한 새도우 복제본을 만듭니다.



새도우 복제본 세트 디렉토리 깊이에 5개 이상의 하위 디렉토리나 모든 하위 디렉토리가 포함되도록 지정할 수 있지만 새도우 복제본 세트 생성이 60초 이내에 완료되어야 한다는 Microsoft 요구 사항이 있습니다. 이 시간 내에 완료할 수 없는 경우 새도우 복제본 세트 생성이 실패합니다. 선택한 새도 복사본 디렉토리 깊이로 인해 생성 시간이 시간 제한을 초과하지 않아야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
' * set-Privilege advanced * '
```

2. VSS 새도우 복제본 디렉토리 깊이를 원하는 레벨로 설정합니다.

```
`vserver cifs options modify -vserver_vserver_name_-shadowcopy -dir -depth integer*'
```

```
`vserver cifs options modify -vserver vs1-shadowcopy -dir-depth 6 *'
```

3. 관리자 권한 레벨로 돌아갑니다.

```
' * set-privilege admin * '
```

## SMB 구성을 통해 Hyper-V 및 SQL Server 관리

지속적인 가용성을 위해 기존 공유를 구성합니다

Hyper-V 및 SQL Server 애플리케이션 서버에서 Hyper-V 가상 머신 및 구성 파일, SQL Server 데이터베이스 파일에 중단 없이 액세스하는 데 사용하는 공유를 계속 사용할 수 있도록 기존 공유를 수정할 수 있습니다.

이 작업에 대해

공유에 다음과 같은 특성이 있는 경우 SMB를 통해 애플리케이션 서버와 무중단 운영을 위해 기존 공유를 지속적으로 사용할 수 있는 공유로 사용할 수 없습니다.

- 이 공유에 homedory 공유 속성이 설정되어 있으면
- 공유에 활성화된 symlink 또는 widelink가 포함된 경우
- 공유에 공유의 루트 아래에 접합된 볼륨이 포함되어 있는 경우

다음 두 공유 매개 변수가 올바르게 설정되었는지 확인해야 합니다.

- '-offline-files' 매개 변수는 수동(기본값) 또는 없음(없음)으로 설정됩니다.
- Symlink를 비활성화해야 합니다.

다음 공유 속성을 구성해야 합니다.

- "계속 사용할 수 있습니다.

- oplocks

다음 공유 속성을 설정하지 않아야 합니다. 현재 공유 속성 목록에 있는 경우 지속적으로 사용 가능한 공유에서 제거해야 합니다.

- 'attributecache
- 브랜치캐시

단계

1. 현재 공유 매개 변수 설정 및 구성된 공유 속성의 현재 목록을 표시합니다.

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. 필요한 경우 명령을 사용하여 공유 매개 변수를 수정하여 symlink를 비활성화하고 오프라인 파일을 manual로 vserver cifs share modify 설정합니다.

- '-symlink' 매개 변수의 값을 ""로 설정하여 symlink를 비활성화할 수 있습니다.
- '-offline-files' 파라미터는 'Manual'을 지정하여 올바른 설정으로 설정할 수 있습니다.

3. 공유 속성을 추가하고 필요한 경우 공유 속성을 추가합니다 continuously-available oplocks .

```
vserver cifs share properties add -vserver <vserver_name> -share-name <share_name> -share-properties continuously-available[,oplock]
```

oplocks 공유 속성이 아직 설정되지 않은 경우 계속 사용 가능한 공유 속성과 함께 추가해야 합니다.

4. 지속적으로 사용 가능한 공유에서 지원되지 않는 공유 속성을 제거합니다.

```
vserver cifs share properties remove -vserver <vserver_name> -share-name <share_name> -share-properties properties[,...]
```

심표로 구분된 목록으로 공유 속성을 지정하여 하나 이상의 공유 속성을 제거할 수 있습니다.

5. '-symlink' 및 '-offline-files' 매개 변수가 올바르게 설정되었는지 확인합니다.

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name> -fields symlink-properties,offline-files
```

6. 구성된 공유 속성 목록이 올바른지 확인합니다.

```
vserver cifs share properties show -vserver <vserver_name> -share-name <share_name>
```

예

다음 예에서는 SMB를 통해 애플리케이션 서버가 있는 NDOs에 대해 SVM(스토리지 가상 머신) "VS1"이라는 기존 공유를 구성하는 방법을 보여 줍니다.

- 매개 변수를 로 설정하면 공유에서 symlink가 `-symlink `""`` 비활성화됩니다.
- `'-offline-file'` 파라미터가 수정되어 `'manual'`로 설정됩니다.
- 이 공유에 계속 이용 가능한 공유자산이 추가됩니다.
- `oplocks` 공유 속성은 이미 공유 속성 목록에 있으므로 추가할 필요가 없습니다.
- 이 지분에서는 `attributecache` 공유재산을 빼내기도 합니다.
- "탐색 가능" 공유 속성은 SMB를 통해 애플리케이션 서버와 NDO에 사용되는 지속적인 사용 가능 공유에 대한 선택 사항이며 공유 속성 중 하나로 유지됩니다.



```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
```

```

 Vserver: vs1
 Share: share1
CIFS Server NetBIOS Name: vs1
 Path: /data
 Share Properties: oplocks
 browsable
 attributecache
 Symlink Properties: enable
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
 Volume Name: data
 Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vsriver cifs share modify -vsriver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vsriver cifs share properties add -vsriver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
-fields symlink-properties,offline-files
vsriver share-name symlink-properties offline-files
```

```

vs1 share1 - manual
```

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
```

```

 Vserver: vs1
 Share: share1
Share Properties: oplocks
 browsable
 continuously-available
```

**SMB** 백업을 통해 **Hyper-V**에 대한 **VSS** 새도우 복제본을 설정하거나 해제합니다

VSS 인식 백업 애플리케이션을 사용하여 SMB 공유에 저장된 Hyper-V 가상 머신 파일을 백업하는 경우 VSS 새도우 복제본을 설정해야 합니다. VSS 인식 백업 애플리케이션을 사용하지 않는 경우 VSS 새도우 복제본을 비활성화할 수 있습니다. 기본값은 VSS 새도우 복제본을 설정하는 것입니다.

이 작업에 대해

언제든지 VSS 새도우 복제본을 설정하거나 해제할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
' * set-Privilege advanced * '
```

2. 다음 작업 중 하나를 수행합니다.

| VSS 새도우 복제본을 만들려는 경우... | 명령 입력...                                                                                             |
|-------------------------|------------------------------------------------------------------------------------------------------|
| 활성화됨                    | <pre>``vserver cifs options modify<br/>-vserver _vserver_name_-shadowcopy -enabled true<br/>*`</pre> |
| 사용 안 함                  | <pre>* vserver cifs options modify<br/>-vserver _vserver_name_-shadowcopy -enabled<br/>false *</pre> |

3. 관리자 권한 레벨로 돌아갑니다.

```
' * set-privilege admin * '
```

예

다음 명령을 실행하면 SVM VS1 에서 VSS 새도우 복제본이 활성화됩니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

통계를 사용하여 **SMB** 작업을 통해 **Hyper-V** 및 **SQL Server**를 모니터링합니다

**ONTAP**에서 사용할 수 있는 통계 개체 및 카운터를 확인합니다

CIFS, SMB, 감사 및 BranchCache 해시 통계에 대한 정보를 얻고 성능을 모니터링하려면 데이터를 가져올 수 있는 개체와 카운터를 알고 있어야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

| 다음 사항을 확인하고자 하는 경우: | 입력...                                                                   |
|---------------------|-------------------------------------------------------------------------|
| 사용할 수 있는 개체         | '통계 카탈로그 개체 쇼'                                                          |
| 사용할 수 있는 특정 개체입니다   | <code>statistics catalog object show -object <i>object_name</i></code>  |
| 사용할 수 있는 카운터        | <code>statistics catalog counter show -object <i>object_name</i></code> |

자세히 알아보세요 `statistics catalog object show` 그리고 `statistics catalog counter show` 에서 ["ONTAP 명령 참조입니다"](#).

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

예

다음 명령을 실행하면 고급 권한 수준에 표시된 대로 클러스터에서 CIFS 및 SMB 액세스와 관련된 선택한 통계 개체에 대한 설명이 표시됩니다.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
 audit_ng CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
 cifs The CIFS object reports activity of the
 Common Internet File System protocol
 ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
 nblade_cifs The Common Internet File System (CIFS)
 protocol is an implementation of the
Server
 ...
```

```
cluster1::*> statistics catalog object show -object smb1
 smb1 These counters report activity from the
SMB
 revision of the protocol. For information
 ...
```

```
cluster1::*> statistics catalog object show -object smb2
 smb2 These counters report activity from the
 SMB2/SMB3 revision of the protocol. For
 ...
```

```
cluster1::*> statistics catalog object show -object hashd
 hashd The hashd object provides counters to
measure
 the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

다음 명령을 실행하면 고급 권한 수준에서 표시되는 "CIFS" 객체의 일부 카운터에 대한 정보가 표시됩니다.



이 예제에서는 "CIFS" 객체에 대해 사용 가능한 카운터를 모두 표시하지 않고 출력이 잘립니다.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

| Counter              | Description                                                                  |
|----------------------|------------------------------------------------------------------------------|
| active_searches      | Number of active searches over SMB and SMB2                                  |
| auth_reject_too_many | Authentication refused after too many requests were made in rapid succession |
| avg_directory_depth  | Average number of directories crossed by SMB and SMB2 path-based commands    |
| ...                  | ...                                                                          |

```
cluster2::> statistics start -object client -sample-id
```

Object: client

| Counter              | Value                   |
|----------------------|-------------------------|
| cifs_ops             | 0                       |
| cifs_read_ops        | 0                       |
| cifs_read_recv_ops   | 0                       |
| cifs_read_recv_size  | 0B                      |
| cifs_read_size       | 0B                      |
| cifs_write_ops       | 0                       |
| cifs_write_recv_ops  | 0                       |
| cifs_write_recv_size | 0B                      |
| cifs_write_size      | 0B                      |
| instance_name        | vserver_1:10.72.205.179 |
| instance_uuid        | 2:10.72.205.179         |
| local_ops            | 0                       |
| mount_ops            | 0                       |

[...]

에 대한 자세한 내용은 `statistics start` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

ONTAP에서 SMB 통계를 표시합니다

다양한 SMB 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. '통계 시작' 및 '통계 중지' 옵션 명령을 사용하여 데이터 샘플을 수집합니다.
2. 다음 작업 중 하나를 수행합니다.

| 에 대한 통계를 표시하려면... | 다음 명령을 입력합니다...                             |
|-------------------|---------------------------------------------|
| 모든 SMB 버전         | ' * statistics show-object cifs * '         |
| SMB 1.0           | ' * statistics show-object SMB1 * '         |
| SMB 2.x 및 SMB 3.0 | ' * statistics show-object SMB2 * '         |
| 노드의 SMB 하위 시스템입니다 | ' * statistics show -object nblade_cifs * ' |

관련 정보

- ["통계에 따르면"](#)
- ["통계 시작"](#)
- ["통계 중지"](#)

구성이 무중단 운영이 가능한지 확인합니다

상태 모니터링을 사용하여 무중단 운영 상태가 정상인지 확인하십시오

상태 모니터링에서는 클러스터 전체의 시스템 상태에 대한 정보를 제공합니다. 상태 모니터는 SMB 구성을 통해 Hyper-V 및 SQL Server를 모니터링하여 애플리케이션 서버에 대한 무중단 운영(NDO)을 보장합니다. 상태가 성능 저하인 경우 가능한 원인 및 권장 복구 조치를 포함하여 문제에 대한 세부 정보를 볼 수 있습니다.

여러 개의 상태 모니터가 있습니다. ONTAP는 개별 상태 모니터의 전체 시스템 상태와 상태를 모두 모니터링합니다. 노드 연결 상태 모니터에는 CIFS-NDO 서브시스템이 포함되어 있습니다. 모니터에는 특정 물리적 조건으로 인해 운영 중단이 발생할 수 있는 경우 알림을 트리거하는 상태 정책이 있으며, 중단 상태가 있을 경우 알림을 생성하고 수정 조치에 대한 정보를 제공합니다. SMB 구성을 통한 NDO의 경우 다음 두 가지 조건에 대한 경고가 생성됩니다.

| 경고 ID                       | 심각도입니다 | 조건                                                                                                                   |
|-----------------------------|--------|----------------------------------------------------------------------------------------------------------------------|
| ``HaNotReadyCifsNdo_Alert*` | 전공     | 노드에서 애그리게이트에서 볼륨에 호스팅되는 하나 이상의 파일이 장애 발생 시 지속성을 약속하는 지속적으로 사용 가능한 SMB 공유를 통해 열렸습니다. 파트너와의 HA 관계는 구성되지 않았거나 상태가 아닙니다. |

| 경고 ID                            | 심각도입니다 | 조건                                                                                                                                      |
|----------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| '* NoStandbyLifcifsNdo_Alert * ' | 경미합니다  | SVM(스토리지 가상 머신)은 노드를 통해 SMB를 통해 데이터를 능동적으로 제공하고, 지속적으로 사용 가능한 공유를 통해 지속적으로 열려 있는 SMB 파일이 있지만, 해당 파트너 노드가 SVM을 위한 활성 데이터 LIF를 노출하지 않습니다. |

시스템 상태 모니터링을 사용하여 무중단 운영 상태를 표시합니다

'시스템 상태' 명령을 사용하면 클러스터의 전체 시스템 상태 및 CIFS-NDO 하위 시스템의 상태에 대한 정보를 표시하고, 알림에 응답하고, 향후 알림을 구성하고, 상태 모니터링 구성 방법에 대한 정보를 표시할 수 있습니다.

단계

1. 적절한 작업을 수행하여 상태 모니터링:

| 를 표시하려면...                        | 명령 입력...                                       |
|-----------------------------------|------------------------------------------------|
| 개별 상태 모니터의 전체 상태를 반영하는 시스템의 상태입니다 | * 시스템 상태 표시 *                                  |
| CIFS-NDO 서브시스템의 상태에 대한 정보입니다      | * 시스템 상태 하위 시스템 표시 - 하위 시스템 cifs-NDO-instance* |

2. 적절한 작업을 수행하여 CIFS-NDO 알림 모니터링을 구성하는 방법에 대한 정보를 표시합니다.

| 다음에 대한 정보를 표시하려면...                                              | 명령 입력...                                 |
|------------------------------------------------------------------|------------------------------------------|
| 모니터링되는 노드, 초기화 상태 및 상태와 같은 CIFS-NDO 서브시스템에 대한 상태 모니터의 구성 및 상태입니다 | * 시스템 상태 구성 show-subsystem cifs-NDO *    |
| 상태 모니터에서 잠재적으로 생성할 수 있는 CIFS-NDO 알림을 나타냅니다                       | * 시스템 상태 경고 정의 show-subsystem cifs-NDO * |
| CIFS-NDO 상태 모니터링 정책으로 알림이 발생하는 시기를 결정합니다                         | * 시스템 상태 정책 정의 표시 - 모니터 노드 연결 * '        |



자세한 정보를 표시하려면 '-instance' 매개 변수를 사용합니다.

예

다음 출력에는 클러스터 및 CIFS-NDO 서브시스템의 전체 상태에 대한 정보가 표시됩니다.

```
cluster1::> system health status show
Status

ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

 Subsystem: CIFS-NDO
 Health: ok
 Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
 Node: node2
 Subsystem Refresh Interval: 5m
```

다음 출력에는 CIFS-NDO 서브시스템의 상태 모니터 구성 및 상태에 대한 자세한 정보가 나와 있습니다.



```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

지속적으로 사용 가능한 **SMB** 공유 구성을 확인합니다

무중단 운영을 지원하려면 Hyper-V 및 SQL Server SMB 공유를 지속적으로 사용 가능한 공유로 구성해야 합니다. 또한 확인해야 할 다른 공유 설정도 있습니다. 계획된 또는 계획되지 않은 중단 이벤트가 있는 경우 공유가 애플리케이션 서버에 무중단 운영을 원활하게 제공하도록 올바르게 구성되었는지 확인해야 합니다.

이 작업에 대해

다음 두 공유 매개 변수가 올바르게 설정되었는지 확인해야 합니다.

- '-offline-files' 매개 변수는 수동(기본값) 또는 없음(없음)으로 설정됩니다.

- Symlink를 비활성화해야 합니다.

적절한 무중단 운영을 위해서는 다음 공유 속성을 설정해야 합니다.

- "계속 사용할 수 있습니다.
- oplocks

다음 공유 속성을 설정하지 않아야 합니다.

- 홈디렉토리
- 'attributecache
- 브랜치캐시
- '엑세스 기반 열거'

단계

1. 오프라인 파일이 '수동' 또는 '사용 안 함'으로 설정되어 있고 symlink가 비활성화되어 있는지 확인합니다.

```
* vsver CIFS 공유 show -vsver_vsver_name_*
```

2. SMB 공유가 무중단 가용성을 위해 구성되었는지 확인합니다.

```
* vsver cifs 공유 속성 표시 - vsver_vsver_name_*
```

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 의 "shay1"이라는 공유 설정을 표시합니다. 오프라인 파일은 '수동'으로 설정되고 symlink는 비활성화됩니다('대칭 링크 속성' 필드 출력에서 하이픈으로 지정됨).

```
cluster1::> vsver cifs share show -vsver vs1 -share-name share1
 Vserver: vs1
 Share: share1
 CIFS Server NetBIOS Name: VS1
 Path: /data/share1
 Share Properties: oplocks
 continuously-available
 Symlink Properties: -
 File Mode Creation Mask: -
 Directory Mode Creation Mask: -
 Share Comment: -
 Share ACL: Everyone / Full Control
 File Attribute Cache Lifetime: -
 Volume Name: -
 Offline Files: manual
 Vscan File-Operations Profile: standard
```

다음 예에서는 SVM VS1 에서 "shay1"이라는 이름의 공유에 대한 공유 속성을 표시합니다.

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
Vserver Share Properties

vs1 share1 oplocks
 continuously-available
```

**LIF** 상태를 확인합니다

Hyper-V와 SQL Server over SMB 구성을 통해 SVM(스토리지 가상 시스템)을 구성하여 클러스터의 각 노드에 LIF를 갖는 일상적인 작업을 수행하는 경우에도 일부 LIF는 다른 노드의 포트로 이동할 수 있습니다. LIF 상태를 확인하고 필요한 수정 조치를 취해야 합니다.

이 작업에 대해

원활한 무중단 운영 지원을 제공하려면 클러스터의 각 노드에 SVM을 위한 LIF가 하나 이상 있어야 하며 모든 LIF가 홈 포트와 연결되어야 합니다. 구성된 LIF 중 일부가 현재 홈 포트에 연결되어 있지 않으면 포트 문제를 해결한 다음 LIF를 홈 포트에 되돌려야 합니다.

단계

1. SVM을 위해 구성된 LIF 정보 표시:

\* 네트워크 인터페이스 show -vsriver\_vserver\_name\_\*

이 예에서 "lif1"은 홈 포트에 없습니다.

네트워크 인터페이스 show-vsriver vs1

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|---------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home    |                   |                   |                      |              |                 |
| vs1     | lif1              | up/up             | 10.0.0.128/24        | node2        | e0d             |
| false   | lif2              | up/up             | 10.0.0.129/24        | node2        | e0d             |
| true    |                   |                   |                      |              |                 |

에 대한 자세한 내용은 network interface show ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 일부 LIF가 홈 포트에 없는 경우 다음 단계를 수행하십시오.

- a. 각 LIF에서 LIF의 홈 포트가 무엇인지 확인합니다.

\* 네트워크 인터페이스 show -vsriver\_vserver\_name\_lif\_lif\_name\_-fields home-node, home-port \*

\* network interface show -vserver vs1-lif lif1-fields home-node, home-port \*

| vserver | lif  | home-node | home-port |
|---------|------|-----------|-----------|
| -----   | ---- | -----     | -----     |
| vs1     | lif1 | node1     | e0d       |

b. 각 LIF에서 LIF의 홈 포트가 작동하는지 확인합니다.

\* 네트워크 포트 show-node\_node\_name\_-port\_port\_- 필드 포트, 링크 \*

'network port show-node node1-port e0d-fields port, link

| node  | port | link |
|-------|------|------|
| ----- | ---- | ---- |
| node1 | e0d  | up   |

이 예에서는 "lif1"을 홈 포트인 node1:e0d로 다시 마이그레이션해야 합니다.

에 대한 자세한 내용은 network port show ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. LIF와 연결되어야 하는 홈 포트 네트워크 인터페이스 중 하나가 상태에 있지 않은 경우 up, 이러한 인터페이스가 작동하도록 문제를 해결하십시오. 에 대한 자세한 내용은 up ["ONTAP 명령 참조입니다"](#)을 참조하십시오.
4. 필요한 경우 LIF를 홈 포트에 되돌립니다.

\* 네트워크 인터페이스 되돌리기 - vserver\_vserver\_name\_-lif\_lif\_name\_\*

\* 네트워크 인터페이스 되돌리기 - vserver vs1-lif lif1-lif li1\*

에 대한 자세한 내용은 network interface revert ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

5. 클러스터의 각 노드에 SVM을 위한 액티브 LIF가 있는지 확인합니다.

\* 네트워크 인터페이스 show -vserver\_vserver\_name\_\*

\* 네트워크 인터페이스 show-vserver vs1\*

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is    |
|---------|-------------------|-------------------|----------------------|--------------|--------------|-------|
| Home    |                   |                   |                      |              |              |       |
| -----   | -----             | -----             | -----                | -----        | -----        | ----- |
| vs1     |                   |                   |                      |              |              |       |
|         | lif1              | up/up             | 10.0.0.128/24        | node1        | e0d          |       |
| true    |                   |                   |                      |              |              |       |
|         | lif2              | up/up             | 10.0.0.129/24        | node2        | e0d          |       |
| true    |                   |                   |                      |              |              |       |

**SMB** 세션을 지속적으로 사용할 수 있는지 확인합니다

**SMB** 세션 정보를 표시합니다

SMB 연결 및 세션 ID와 세션을 사용하는 워크스테이션의 IP 주소를 포함하여 설정된 SMB 세션에 대한 정보를 표시할 수 있습니다. 세션의 SMB 프로토콜 버전 및 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시하여 세션이 무중단 운영을 지원하는지 여부를 확인할 수 있습니다.

이 작업에 대해

SVM의 모든 세션에 대한 정보를 요약 형식으로 표시할 수 있습니다. 그러나 대부분의 경우 반환되는 출력량이 큼니다. 옵션 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다.

- 옵션 '-fields' 매개 변수를 사용하여 선택한 필드에 대한 출력을 표시할 수 있습니다.

필드를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

- '-instance' 매개 변수를 사용하면 설정된 SMB 세션에 대한 자세한 정보를 표시할 수 있습니다.
- '-fields' 매개 변수 또는 '-instance' 매개 변수를 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

|                             |                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------|
| <b>SMB</b> 세션 정보를 표시하려면...  | 다음 명령을 입력합니다...                                                                                  |
| SVM의 모든 세션에 대해 요약 양식을 작성합니다 | <code>* vserver cifs session show -vserver_vserver_name_*</code>                                 |
| 지정된 연결 ID에 있습니다             | <code>* vserver cifs session show -vserver_vserver_name_-connection-id integer *</code>          |
| 지정된 워크스테이션 IP 주소에서          | <code>* vserver cifs session show -vserver_vserver_name_-address_workstation_ip_address_*</code> |

|                                                                                                                                                                                                                                                                               |                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>SMB</b> 세션 정보를 표시하려면...                                                                                                                                                                                                                                                    | 다음 명령을 입력합니다...                                                                               |
| 지정된 LIF IP 주소입니다                                                                                                                                                                                                                                                              | <code>* vserver cifs session show -vserver_vserver_name_-lif-address_LIF_ip_address_ *</code> |
| 지정된 노드에서                                                                                                                                                                                                                                                                      | <code>* vserver cifs session show -vserver_vserver_name_-node{node_name</code>                |
| <code>local} *</code>                                                                                                                                                                                                                                                         | 지정된 Windows 사용자로부터                                                                            |
| <code>* vserver cifs session show -vserver_vserver_name_-windows -user_user_name_ *</code><br><br>user_name 형식은 '[domain]\user'입니다.                                                                                                                                           | 지정된 인증 메커니즘을 사용합니다                                                                            |
| <code>* vserver cifs session show -vserver_vserver_name_-auth-mechanism authentication_mechanism *</code><br><br>'-auth-mechanism'의 값은 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> <li>• "NTLMv1"입니다</li> <li>• NTLMv2</li> <li>• Kerberos</li> <li>• '익명'</li> </ul> | 지정된 프로토콜 버전을 사용하여                                                                             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>SMB 세션 정보를 표시하려면...</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 다음 명령을 입력합니다...                                                            |
| <div data-bbox="168 195 495 363"> <pre> * vserver cifs session show -vserver_vserver_name_ -protocol-version protocol_version *' </pre> </div> <div data-bbox="168 401 495 499"> <p>'-protocol-version'의 값은 다음 중 하나일 수 있습니다.</p> </div> <div data-bbox="207 537 378 772"> <ul style="list-style-type: none"> <li>• 'MB1'입니다</li> <li>• MB2</li> <li>• MB2_1</li> <li>• MB3</li> <li>• 'MB3_1'</li> </ul> </div> <div data-bbox="256 1360 316 1423">  </div> <div data-bbox="370 821 462 1969"> <p>지속적으로 사용 가능한 보호 수준과 기능과 SMB 멀티 채널은 SMB 3.0 이상 세션에서만 사용할 수 있습니다. 모든 적격 세션에서 해당 상태를 보려면 이 매개 변수를 'MB3' 이상으로 설정한 값으로 지정해야 합니다.</p> </div> | <div data-bbox="505 195 1068 226"> <p>지속적으로 사용 가능한 보호 수준을 지정합니다</p> </div> |

|                                                                                                                                                                                                                                                                  |                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <b>SMB 세션 정보를 표시하려면...</b>                                                                                                                                                                                                                                       | 다음 명령을 입력합니다...  |
| <pre> '* vserver cifs session show -vserver_vserver_name_ -Continuously -available_Continuously_ available_protection_level_ *' </pre> <p>'-연속 사용 가능'의 값은 다음 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 아니</li> <li>• 네</li> <li>• 부분</li> </ul> | 지정된 SMB 서명 세션 상태 |



예

다음 명령을 실행하면 IP 주소가 10.1.1.1인 워크스테이션에서 설정된 SVM VS1 세션의 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node: node1
Vserver: vs1
Connection Session
ID ID Workstation Windows User Open Idle

3151272279,
3151272280,
3151272281 1 10.1.1.1 DOMAIN\joe 2 23s
```

다음 명령을 실행하면 SVM VS1에서 지속적으로 사용 가능한 보호 기능을 지원하는 세션에 대한 자세한 세션 정보가 표시됩니다. 도메인 계정을 사용하여 연결을 만들었습니다.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

다음 명령을 실행하면 SVM VS1 기반 SMB 3.0 및 SMB 멀티 채널을 사용하는 세션에 대한 세션 정보가 표시됩니다. 이 예에서 사용자는 LIF IP 주소를 사용하여 SMB 3.0 지원 클라이언트에서 이 공유에 연결했습니다. 따라서 인증 메커니즘은 NTLMv2로 기본값입니다. 지속적으로 사용 가능한 보호 기능을 사용하여 연결하려면 Kerberos 인증을 사용하여 연결해야 합니다.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```
Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

ONTAP에서 열린 **SMB** 파일에 대한 정보를 표시합니다

SMB 연결 및 세션 ID, 호스팅 볼륨, 공유 이름 및 공유 경로를 포함하여 열려 있는 SMB 파일에 대한 정보를 표시할 수 있습니다. 또한 파일의 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시할 수도 있습니다. 이 정보는 열려 있는 파일이 무중단 작업을 지원하는 상태에 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

설정된 SMB 세션에서 열린 파일에 대한 정보를 표시할 수 있습니다. 표시된 정보는 SMB 세션 내의 특정 파일에 대한 SMB 세션 정보를 확인해야 할 때 유용합니다.

예를 들어, 열린 파일 중 일부가 지속적으로 사용 가능한 보호 기능을 통해 열려 있고 일부는 지속적으로 사용 가능한 보호 기능을 통해 열려 있지 않은 SMB 세션이 있는 경우(vserver cifs session show 명령의 출력 값이 부분(Partial)인 경우), 이 명령을 사용하여 계속 사용할 수 없는 파일을 확인할 수 있습니다.

선택적 매개 변수 없이 'vserver cifs session file show' 명령을 사용하면 SVM(스토리지 가상 시스템)에서 설정된 SMB 세션의 모든 열려 있는 파일에 대한 정보를 요약 형식으로 표시할 수 있습니다.

그러나 대부분의 경우 반환되는 출력량이 큼니다. 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다. 이 기능은 열려 있는 파일의 작은 하위 집합에 대한 정보만 보려는 경우에 유용합니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 출력을 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

- '-instance' 매개 변수를 사용하여 열려 있는 SMB 파일에 대한 자세한 정보를 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

## 단계

1. 다음 작업 중 하나를 수행합니다.

| 열려 있는 <b>SMB</b> 파일을 표시하려면...                                                                            | 다음 명령을 입력합니다...                                                                  |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| SVM에 대해 요약 형식으로 표시됩니다                                                                                    | <code>* vserver cifs 세션 파일 표시 -<br/>vserver_vserver_name_*</code>                |
| 지정된 노드에서                                                                                                 | <code>* vserver CIFS 세션 파일 show<br/>-vserver_vserver_name_-node{node_name</code> |
| local} *                                                                                                 | 지정된 파일 ID에 있습니다                                                                  |
| <code>* vserver cifs 세션 파일 표시 -<br/>vserver_vserver_name_-file-id integer*</code>                        | 지정된 SMB 연결 ID에서                                                                  |
| <code>* vserver cifs 세션 파일 표시 -<br/>vserver_vserver_name_-connection-id integer*</code>                  | 지정된 SMB 세션 ID에서                                                                  |
| <code>* vserver cifs 세션 파일 표시 -<br/>vserver_vserver_name_-session-id integer*</code>                     | 지정된 호스팅 집계에서                                                                     |
| <code>* vserver cifs 세션 파일 표시 -<br/>vserver_vserver_name_-hosting-<br/>aggregate_aggregate_name_*</code> | 지정된 볼륨에서                                                                         |
| <code>* vserver cifs 세션 파일 표시 -<br/>vserver_vserver_name_-hosting-<br/>volume_volume_name_*</code>       | 지정된 SMB 공유에서                                                                     |
| <code>* vserver CIFS 세션 파일 표시 -<br/>vserver_vserver_name_-share_share_name_*</code>                      | 지정된 SMB 경로에 있어야 합니다                                                              |
| <code>* vserver CIFS 세션 파일 표시 -<br/>vserver_vserver_name_-path_path_*</code>                             | 지속적으로 사용 가능한 보호 수준을 지정합니다                                                        |

| 열려 있는 <b>SMB</b> 파일을 표시하려면...                                                                                                                                                                                                                                                                                                                                                                                                                                    | 다음 명령을 입력합니다... |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <pre>* vserver cifs 세션 파일 표시 - vserver_vserver_name_-Continuously- available_Continuously_available_status_*</pre> <p>'-연속 사용 가능'의 값은 다음 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 아니</li> <li>• 네</li> </ul> <div>  <p>계속 사용 가능한 상태가 '아니요'인 경우 열려 있는 파일은 Takeover와 Giveback에서 중단 없이 복구할 수 없습니다. 또한, 고가용성 관계에 있는 파트너 간의 일반 애그리게이트 재배치에서 복구할 수 없습니다.</p> </div> | 지정된 다시 연결된 상태에서 |

출력 결과를 구체화하는 데 사용할 수 있는 추가 선택적 매개 변수가 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

예

다음 예에서는 SVM VS1 에서 열린 파일에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1
Node: node1
Vserver: vs1
Connection: 3151274158
Session: 1
File File Open Hosting Continuously
ID Type Mode Volume Share Available

41 Regular r data data Yes
Path: \mytest.rtf
```

다음 예에서는 SVM VS1에서 파일 ID 82가 있는 개방형 SMB 파일에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance
```

```
 Node: node1
 Vserver: vs1
 File ID: 82
 Connection ID: 104617
 Session ID: 1
 File Type: Regular
 Open Mode: rw
Aggregate Hosting File: aggr1
 Volume Hosting File: data1
 CIFS Share: data1
 Path from CIFS Share: windows\win8\test\test.txt
 Share Mode: rw
 Range Locks: 1
Continuously Available: Yes
 Reconnected: No
```

## 저작권 정보

Copyright © 2026 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.