Dell PowerStore

NFS 구성

4.3

2025년 12월
개정 A08

DELL Technologies

참고, 주의 및 경고

노트: 참고는 제품을 보다 효과적으로 사용하는 데 도움이 되는 중요한 정보를 나타냅니다.

주의: **주의는 잠재적 하드웨어 손상이나 데이터 손실을 나타내며, 문제를 방지하는 방법을 알려줍니다.**

경고: **경고는 재산 피해, 개인 상해 또는 사망의 위험이 있음을 나타냅니다.**

목차

서문

제품군을 향상시키기 위한 노력의 일환으로 소프트웨어와 하드웨어의 개정 버전을 정기적으로 릴리스하고 있습니다. 이 문서에서 설명하는 일부 기능은 현재 사용 중인 소프트웨어 또는 하드웨어의 일부 버전에서 지원되지 않을 수 있습니다. 제품 릴리스 노트에는 제품 기능에 대한 최신 정보가 제공되어 있습니다. 제품이 올바르게 작동하지 않거나 이 문서에 설명된 대로 작동하지 않는 경우 서비스 공급업체에 문의하십시오.

노트: PowerStore X 모델 고객: 사용 중인 모델에 대한 최신 사용 방법 기술 설명서 및 가이드를 보려면 dell.com/powerstoredocs의 PowerStore 설명서 페이지에서 *PowerStore 3.2.x 설명서 세트*를 다운로드하십시오.

지원 정보

지원, 제품 및 라이선스 정보는 다음과 같이 확인할 수 있습니다.

- **제품 정보** - 제품 및 기능 설명서 또는 릴리스 노트를 보려면 dell.com/powerstoredocs에서 PowerStore 설명서 페이지를 참조하십시오.
- **문제 해결** - 제품, 소프트웨어 업데이트, 라이선싱 및 서비스에 대한 자세한 내용은 Dell 지원에서 해당 제품 지원 페이지를 참조하십시오.
- **기술 지원** - 기술 지원 및 서비스 요청의 경우 Dell 지원에서 **서비스 요청** 페이지를 참조하십시오. 서비스 요청을 개설하려면 유효한 지원 계약이 있어야 합니다. 유효한 지원 계약 체결에 대한 자세한 내용이나 계정 관련 질문에 대한 답을 얻으려면 영업 담당자에게 문의하십시오.

1

개요

이 장에서 다루는 내용은 다음과 같습니다.

주제:

NFS 지원

PowerStore T 모델 및 PowerStore Q 모델은 NFSv3 및 NFSv4를 지원합니다. 또한 이 모델들은 강력한 인증을 위해 Kerberos를 이용한 보안 NFS를 지원합니다. PowerStore T 모델 및 PowerStore Q 모델은 관련 RFC에 설명된 NFSv4 및 v4.1 기능 대부분을 지원하지만 디렉토리 위임 및 pNFS는 지원하지 않습니다. 3.0 이상에서는 PowerStore 호환성 모드에서 NFSv4.2에 대한 기본 지원도 사용할 수 있습니다. PowerStore 4.3부로 NFSv4.2 지원이 다음과 같은 추가 기능으로 향상되었습니다.

- 서버 내 복사 - 이 기능을 사용하면 클라이언트가 내부 복사 작업을 요청하여 불필요한 네트워크 트래픽을 줄일 수 있습니다.
- 스파스 파일 지원 -
  - READ_PLUS 작업은 스파스 파일의 구멍(0으로 채워진 영역)을 식별할 수 있으므로 불필요한 0 데이터를 전송할 필요가 없으며 성능이 향상됩니다.
  - SEEK 작업을 통해 클라이언트는 파일의 다음 데이터 또는 구멍의 위치를 확인할 수 있습니다.
- 레이블이 지정된 NFS - 이 기능을 사용하면 MAC Aware NFS 서버가 MAC(Mandatory Access Control) 레이블을 파일에 저장할 수 있습니다. 그런 다음 레이블을 사용하여 데이터 액세스 제어를 적용합니다.

NFS 지원은 생성 도중 또는 생성 후 NAS 서버에서 활성화되므로 해당 NAS 서버에서 NFS 사용 파일 시스템을 생성할 수 있습니다.

보안 NFS 정보

UNIX 공유를 지원하는 NAS 서버를 생성하거나 수정할 때 보안 NFS를 구성할 수 있습니다. 보안 NFS는 네트워크 데이터 무결성 및 네트워크 데이터 프라이버시를 제공할 수 있는 Kerberos 기반 사용자 인증을 제공합니다.

Kerberos는 보안 키 암호화를 사용하여 강력한 인증 기능을 제공하도록 설계된 분산 인증 서비스입니다. 안전하지 않은 네트워크를 통해 통신하는 노드가 안전한 방식으로 ID를 증명할 수 있도록 하는 "티켓"을 기반으로 작동합니다. 보안 NFS 서버 역할을 수행하도록 구성된 경우 NAS 서버는 RPCSEC_GSS 보안 프레임워크와 Kerberos 인증 프로토콜을 사용하여 사용자와 서비스를 확인합니다.

보안 옵션

보안 NFS는 다음과 같은 보안 옵션을 지원합니다.

- krb5: Kerberos 인증
- krb5i: 네트워크를 통해 전송되는 각 NFS 패킷에 서명을 추가하여 Kerberos 인증 및 데이터 무결성
- krb5p: 네트워크를 통해 데이터를 전송하기 전에 암호화하여 Kerberos 인증, 데이터 무결성 및 데이터 프라이버시 유지

  데이터를 암호화하려면 시스템 처리를 위한 추가 리소스가 필요하며 실행이 느려질 수 있습니다.

보안 NFS 환경에서는 Kerberos 보안 주체 이름을 기반으로 NFS 파일 시스템에 대한 사용자 액세스 권한이 부여됩니다. 그러나 파일 시스템 내의 공유에 대한 액세스 제어는 UNIX UID 및 GID 또는 ACL에 기반합니다.

노트: 보안 NFS는 16개가 넘는 그룹을 가진 NFS 자격 증명을 지원하며, 이는 확장된 UNIX 자격 증명 옵션과 동일합니다.

보안 NFS 구성

보안 NFS를 구현하려는 경우 다음을 구성하십시오.

- 날짜 및 시간을 동기화하려면 PowerStore 어플라이언스에서 하나 이상의 NTP 서버를 구성해야 합니다. 단일 장애 지점을 방지하려면 도메인당 두 개 이상의 NTP 서버를 설정하는 것을 적극 권장합니다.
- UDS(UNIX Directory Service)
- 하나 이상의 DNS 서버
- Kerberos 인증을 위해 AD 또는 사용자 지정 영역을 추가해야 합니다.
- Kerberos 구성에서 사용자 지정 영역을 사용하는 경우 keytab 파일을 NAS 서버에 업로드해야 합니다.

계획 시 고려 사항

NFS 내보내기를 구성하기 전에 다음 정보를 검토하십시오.

파일 스토리지 지원은 PowerStore T 모델 및 PowerStore Q 모델 어플라이언스에만 사용할 수 있습니다.

NAS 서버 네트워크

NAS 서버에 대한 네트워크 VLAN 및 IP 주소를 생성하는 것은 선택 사항입니다. NAS 서버에 대한 VLAN을 생성하려는 경우 VLAN을 PowerStore T 모델 및 PowerStore Q 모델 관리 또는 스토리지 네트워크와 공유할 수 없습니다. 또한 네트워크 관리자와 협력하여 네트워크 리소스를 예약하고 스위치에 네트워크를 구성해야 합니다. 자세한 내용은 *스토리지 서비스를 위한 PowerStore T 및 Q 네트워킹 가이드* 내용을 참조하십시오.

확장성

PowerStoreOS 3.5 이상에서는 파일 시스템 볼륨 및 vVols에 대한 공유 한도가 있습니다. 총 오브젝트 수는 세 가지 오브젝트 유형의 최대 한도에 따라 결정됩니다.

플랫폼당 파일 시스템의 한도를 보려면 PowerStore 설명서 페이지에서 *Dell Technologies PowerStore Simple Support Matrix*를 참조하십시오.

배포 요구 사항

NAS 서비스는 PowerStore T 모델 및 PowerStore Q 모델 어플라이언스에서만 사용할 수 있습니다.

PowerStore T 모델 및 PowerStore Q 모델 어플라이언스의 초기 구성 중에 **통합**을 선택해야 합니다. 초기 구성 마법사를 실행하는 동안 **Block Optimized**를 선택한 경우 NAS 서비스가 설치되지 않은 것입니다. NAS 서비스를 설치하려면 기술 지원 담당자가 시스템을 다시 초기화해야 합니다. 시스템 재초기화:

- 어플라이언스를 다시 공장 출하 상태로 설정합니다.
- **Initial Configuration Wizard**를 통해 시스템에서 수행된 모든 구성을 제거합니다.
- PowerStore의 초기 구성 후에 수행되는 모든 구성을 제거합니다.

추가 고려 사항

NAS 서버를 생성하려면 어플라이언스에서 두 노드가 모두 준비되어 있고 실행 중이어야 합니다. 어플라이언스에서 노드 중 하나가 중단되면 NAS 서버 생성이 실패합니다.

NAS 트래픽에 대한 네트워크 인터페이스 생성

LACP(Link Aggregation Control Protocol) 본드를 사용하거나 NAS 트래픽에 대한 Fail Safe Network를 생성하여 NAS 네트워크를 구성할 수 있습니다.

NAS 트래픽에 대한 LACP 본드 생성

스위치가 MC-LAG로 구성된 경우 NAS 트래픽에 대한 LAG(Link Aggregate Group)를 생성하여 네트워크 본딩을 사용할 수 있습니다.

TOR(Top-of-Rack) 스위치가 MC-LAG 상호 연결로 구성된 경우 LAG(Link Aggregation Group)를 사용하여 LACP 본드를 통해 NAS 인터페이스를 구성하는 것이 좋습니다. LACP 본딩은 2개 이상의 네트워크 인터페이스를 단일 인터페이스에 결합하는 프로세스입니다.

LACP 본딩을 사용하면 네트워크 처리량과 대역폭을 증가시켜 성능 향상 효과 및 이중화를 제공합니다. 결합된 인터페이스 중 하나가 중단되는 경우 다른 인터페이스를 사용하여 안정적인 연결을 유지합니다.

1. **하드웨어** > **[어플라이언스]** > **포트**를 선택합니다.
2. 포트 목록에서 NAS 트래픽에 서비스를 제공하기 위해 LACP(Link Aggregate Control Protocol) 본드를 집계하려는 노드에서 동일한 속도의 포트를 2~4개 선택합니다.

   노트: 구성은 피어 노드 전체에서 대칭입니다.

3. **링크 통합** > **링크 통합**을 선택합니다.
4. 필요에 따라 본드에 대한 설명을 입력합니다.
5. **통합**을 선택합니다.
6. 포트 목록을 스크롤하여 생성된 본드 이름을 찾습니다.

   노트: NAS 서버를 생성할 때 본드 이름을 선택해야 합니다.

Fail-Safe Network 생성

ToR(Top-of-Rack) 스위치가 MC-Lag 상호 연결로 구성되지 않은 경우 FSN(Fail-Safe Network)을 생성해야 합니다. FSN은 스위치 수준 이중화를 제공하여 링크 페일오버를 네트워크까지 확장합니다. 포트, Link Aggregation 또는 둘의 조합을 FSN으로 구성할 수 있습니다.

1. **하드웨어** > **[어플라이언스]** > **포트**를 선택합니다.
2. FSN에 집계된 링크를 사용하려는 경우 먼저 Link Aggregation Group을 생성합니다. 자세한 내용은 NAS 트래픽에 대한 LACP 본드 생성을 참조하십시오.
3. 목록에서 2개의 포트 또는 2개의 Link Aggregation 또는 노드 A의 FSN에 사용할 포트와 Link Aggregation Group의 조합을 선택하고 **FSN** > **Create FSN**을 선택합니다.
4. **Create FSN** 패널에서 기본(활성) 네트워크로 사용할 포트 또는 Link Aggregation을 선택합니다.

   노트: 기본 포트는 NAS 서버를 생성하는 데 사용한 후에는 수정할 수 없습니다.

5. 필요에 따라 Fail-Safe Network에 대한 설명을 추가합니다.
6. **Create**를 클릭합니다.

   PowerStore Manager는 "BaseEnclosure-<Node>-fsn<nextLACPbondcreated>" 형식을 사용하여 Fail-Safe Network의 이름을 자동으로 생성합니다.
   - BaseEnclosure는 상수입니다.
   - 노드는 **Node-Module-Name** 목록에 표시되는 노드입니다.
   - nextLACPbondcreated는 0부터 시작하여 PowerStore Manager에서 본드가 생성된 순서로 번호가 매겨진 값입니다.

   노드 A의 PowerStore Manager에서 생성된 첫 번째 FSN의 이름은 BaseEnclosure-NodeA-FSN0입니다.

   동일한 FSN은 반대쪽 노드에 구성됩니다. 예를 들어 노드 A에서 FSN을 구성한 경우 노드 B에 동일한 FSN이 구성됩니다.
7. Fail-Safe Network를 사용하여 NAS 서버를 생성합니다.

   PowerStore Manager에서 NAS 서버를 생성하는 동안 Fail-Safe Network가 NAS 서버에 적용됩니다. NFS 파일 시스템에 대한 NAS 서버 생성을 참조하십시오.

NFS 내보내기 생성

PowerStore에서 NFS 내보내기를 생성하려면 먼저 다음을 수행해야 합니다.

1. NFS 프로토콜을 사용하여 NAS 서버 생성
2. NFS 내보내기를 위한 파일 시스템 생성

문서 자료

추가 정보는 다음을 참조하십시오.

표 1. 문서 자료

문서	설명	위치
스토리지 서비스를 위한 PowerStore T 및Q 네트워킹 가이드	이 문서에서는 네트워크 계획 및 구성 정보를 제공합니다.	dell.com/powerstoredocs
PowerStore SMB 구성 가이드	이 문서에서는 PowerStore Manager를 사용하여 SMB 공유를 구성하는 데 필요한 정보를 제공합니다.	
PowerStore 파일 기능 백서	이 문서에서는 Dell PowerStore 파일 아키텍처에서 지원하는 특징, 기능 및 프로토콜에 대해 설명합니다.	
PowerStore 온라인 도움말	이 온라인 도움말에서는 PowerStore Manager에 열려 있는 페이지에 관하여 상황에 맞는 정보를 제공합니다.	PowerStore Manager에 내장되어 있습니다.

2

NAS 서버 생성

이 장에서 다루는 내용은 다음과 같습니다.

주제:

NAS 서버 구성 개요

스토리지 시스템에 파일 스토리지를 프로비저닝하려면 먼저 NAS 서버가 시스템에서 실행되고 있어야 합니다. NAS 서버는 SMB 프로토콜 또는 NFS 프로토콜 중 하나를 사용하거나 아니면 둘 다 사용하여 네트워크 호스트와 데이터를 공유하는 파일 서버입니다. 또한 관련 파일 시스템에 대한 읽기 및 쓰기 작업을 카탈로그화하고 구성한 후 최적화합니다.

이 문서에서는 NFS 프로토콜을 사용하여 NAS 서버를 구성하는 방법에 대해 설명합니다. 이러한 서버에서 NFS 내보내기가 있는 파일 시스템을 생성할 수 있습니다.

NFS 파일 시스템에 대한 NAS 서버 생성

파일 시스템을 생성하기 전에 NAS 서버를 생성합니다.

NAS 네트워크 정보를 사용할 수 있게 준비해 두어야 합니다.

1. **Storage** > **NAS Servers**를 선택합니다.
2. **Create**를 선택합니다.
3. **Create NAS Server** 마법사를 계속 진행합니다.

마법사 화면	설명
Details	• NAS 서버 이름 • NAS 서버 설명 • 네트워크 인터페이스 - Link Aggregation Group 또는 Fail-Safe Network를 선택합니다(NAS 트래픽에 대한 네트워크 인터페이스 생성 참조). **노트:** FSN(Fail-Safe Network)을 선택한 경우 FSN을 사용하여 NAS 서버를 구성한 후에는 기본 네트워크를 수정할 수 없습니다. • 네트워크 정보 - IP 주소, 서브넷 마스크, 게이트웨이 및 VLAN ID **노트:** 관리 및 스토리지 네트워크에 사용 중인 VLAN은 재사용할 수 없습니다. • 패킷 반영 활성화 - 대상 IP 주소에 관계없이 서버 응답이 원래 호스트 또는 라우터로 다시 전송되므로 라우팅 조회가 발생하지 않습니다. **노트:** NAS 서버 시작 통신에는 이 옵션이 적용되지 않습니다.
Sharing Protocol	**Select Sharing Protocol** NFSv3, NFSv4 또는 둘 모두를 선택합니다.

마법사 화면	설명
	노트: SMB 및 NFS 프로토콜을 선택하면 NAS 서버가 멀티 프로토콜을 지원하도록 자동으로 활성화됩니다. 멀티 프로토콜 파일 공유에 대한 자세한 내용은 설명서 페이지에서 *Dell PowerStore 멀티 프로토콜 파일 공유 구성 가이드*를 PowerStore참조하십시오. **Unix Directory Services**(이름 지정 서비스) 이름 지정 서비스는 로컬 파일과 NIS 또는 LDAP의 조합으로 구성할 수 있습니다. 구성에 관한 자세한 정보는 다음의 섹션을 참조하십시오. • 로컬 파일 사용 • NIS 포함 • LDAP 포함 여기에서 보안 NFS를 활성화하도록 선택할 수 있습니다. 보안 NFS에 필요한 사항은 다음과 같습니다. • 날짜 및 시간을 동기화하려면 PowerStore 어플라이언스에서 하나 이상의 NTP 서버를 구성해야 합니다. 단일 장애 지점을 방지하려면 도메인당 두 개 이상의 NTP 서버를 설정하는 것을 적극 권장합니다. • UDS(UNIX Directory Service) • 하나 이상의 DNS 서버 • Kerberos 인증을 위해 AD 또는 사용자 지정 영역을 추가해야 합니다. • Kerberos 구성에서 사용자 지정 영역을 사용하는 경우 keytab 파일을 NAS 서버에 업로드해야 합니다. **DNS** DNS 서버 정보는 다음과 같은 경우에 필수입니다. • AD 도메인에 연결하지만 독립 실행형 NAS 서버의 경우 선택 사항입니다. • 보안 NFS 구성 DNS는 NFS 내보내기 액세스 목록에 정의된 호스트를 확인하는 데도 사용될 수 있습니다.
보호 정책	필요에 따라 목록에서 보호 정책을 선택합니다.
파일 QoS 정책	필요에 따라 목록에서 파일 QoS 정책을 선택합니다.
요약	내용을 읽은 뒤 **Previous**를 선택하여 뒤로 돌아가거나, 수정할 사항이 있는 경우 수정합니다.

4. **Create NAS Server**를 선택하여 NAS 서버를 생성합니다.
   Status 창이 열리고, 서버가 페이지에 나열되면 **NAS Servers** 페이지로 리디렉션됩니다.

NFS를 위한 NAS 서버를 생성한 후에는 서버 설정을 계속 구성할 수 있습니다.

보안 NFS를 활성화한 경우 Kerberos를 계속 구성해야 합니다.

NAS 서버 설정을 계속 구성하거나 편집하려면 NAS 서버를 선택합니다.

노트: 원격 시스템 연결이 있는 경우 NAS 서버 구성 변경 사항을 원격 NAS 서버에 반영하려면 최대 15분이 걸릴 수 있습니다.

NAS 서버 명명 서비스 구성

NAS 서버에 대한 명명 서비스를 구성하거나 수정할 수 있습니다.

이름 지정 서비스에서는 다음 중 하나 이상을 구성해야 합니다.

- DNS
- UDS(Unix Directory Services)용 NIS
- UDS용 LDAP
- 로컬 파일

DNS 구성

DNS를 비활성화하거나 활성화할 수 있으며 NAS 서버가 DNS를 사용하도록 구성할 수 있습니다.

DNS는 NFS 내보내기 액세스 목록에 정의된 호스트를 확인하는 데에도 사용될 수 있습니다.

DNS는 다음에 필요합니다.

- Secure NFS
- AD 도메인에 연결합니다.

다음을 사용하여 구성된 NAS 서버의 DNS는 비활성화할 수 없습니다.

- 멀티 프로토콜 파일 공유
- AD(Active Directory)에 연결된 SMB 파일 공유
- Secure NFS

1. **Storage** > **NAS Servers** > **[nas server]** > **DNS**를 선택합니다.
2. DNS를 활성화하거나 비활성화합니다. DNS를 활성화한 경우 DNS 서버 정보를 입력합니다.

NIS용 NAS 서버 UNIX 디렉토리 서비스 구성

NIS용 NAS 서버 UDS(UNIX Directory Service)를 구성할 수 있습니다.

1. **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS** 카드를 선택합니다.
2. **Disabled**로 설정된 경우 버튼을 밀러 **Enabled**로 변경합니다.
3. **Unix Directory Service** 드롭다운에서 **NIS**를 선택합니다.
4. NIS **Domain**을 입력하고 NIS 서버에 대하여 IP **Addresses**를 추가합니다.
5. **Apply**를 선택합니다.

NIS를 사용한 UDS 구성 문제를 해결하려면 입력한 NIS 서버 도메인과 서버 IP 주소가 올바른지 확인합니다.

LDAP를 사용한 NAS 서버 UNIX 디렉토리 서비스 구성

LDAP를 사용하여 NAS 서버 UDS(UNIX Directory Service)를 구성할 수 있습니다.

LDAP는 IDMU, RFC2307 또는 RFC2307bis 스키마를 준수해야 합니다. 예를 들어 IDMU 기반 AD LDAP, iPlanet 및 OpenLDAP가 있습니다. 각 사용자에 대한 UID를 제공하도록 LDAP 서버를 올바르게 구성해야 합니다. 예를 들어 IDMU에서 관리자는 각 사용자의 속성으로 이동하고 UNIX 속성 탭에 UID를 추가해야 합니다.

LDAP를 구성하여 간편한 익명 Kerberos 인증을 사용할 수 있습니다. Kerberos 인증을 사용하는 경우 Kerberos를 사용하여 LDAP 구성을 계속 진행하기 전에 다음을 먼저 구성해야 합니다.

1. **Naming Services** 카드에서, Kerberos 서버를 영역에 연결하고 연결 해제하는 데 사용되는 DNS 서버를 구성합니다.
2. **Security** 카드에서, Kerberos 영역을 추가합니다.

1. **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS** 카드를 선택합니다.
2. **Disabled**로 설정된 경우 버튼을 밀러 **Enabled**로 변경합니다.
3. **Unix Directory Service** 드롭다운에서 **LDAP**를 선택합니다.
4. 기본값을 그대로 두거나 다른 **Port Number**를 입력합니다.

   노트: 기본적으로 LDAP는 포트 389를 사용하고, LDAPS(LDAP over SSL)는 포트 636을 사용합니다.

5. LDAP 서버의 IP 주소/FQDN을 추가합니다.

   NAS 서버에서 DNS 서비스 검색을 사용하여 LDAP 서버 IP 주소를 자동으로 얻도록 구성할 수 있습니다.

   노트: 이 검색 프로세스가 작동하려면 DNS 서버에 LDAP 서버에 대한 포인터가 포함되고 LDAP 서버가 동일한 인증 설정을 공유해야 합니다.

6. 다음 표에 설명된 대로 LDAP 인증을 구성합니다.

옵션	설명
익명	iPlanet/OpenLDAP 서버의 기본 DN 및 프로파일 DN을 지정합니다.

단순	다음을 지정합니다.
	• AD를 사용하는 경우 LDAP/IDMU:
	  ○ LDAP 표기 형식으로 된 바인딩 DN(예: **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**)
	  ○ X.509 형식으로 된 기본 DN(예: **dc=svt,dc=lab,dc=com**)
	  ○ 프로파일 DN.

옵션	설명
	• iPlanet/OpenLDAP 서버를 사용하는 경우: ○ LDAP 표기 형식으로 된 바인딩 DN(예: **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**) ○ Password ○ 기본 DN. 예를 들어 **svt.lab.com**을 사용하는 경우 기본 DN은 **DC=svt,DC=lab,DC=com**입니다. ○ 프로파일 DN(선택 사항) - iPlanet/OpenLDAP 서버용
Kerberos	유형에 관계없이 Kerberos 영역(Windows, MIT, Heimdal)을 가리키도록 사용자 지정 영역을 구성합니다. 이 옵션을 선택하면 NAS 서버가 NAS 서버의 **Security** 탭의 Kerberos 하위 섹션에 정의된 사용자 지정 Kerberos 영역을 사용합니다. **노트:** 맞춤 구성 영역이 있는 NFS 보안을 사용하는 경우 keytab 파일을 업로드해야 합니다.

7. **Retrieve Current Schema**를 선택하여 ldap.conf 파일을 다운로드합니다.
8. 파일을 편집하고 저장합니다 `ldap.conf` .
9. **새 스키마 업로드**를 선택하여 업데이트된 `ldap.conf` 파일을 업로드합니다.
10. 필요에 따라 LDAP 보안(SSL 사용)을 활성화하고 CA 인증서를 업로드합니다.

LDAP를 사용한 UDS 구성 문제를 해결하려면 다음 사항을 확인합니다.

- LDAP 구성은 앞에서 설명한 대로 지원되는 스키마 중 하나를 준수합니다.
- `ldap.conf` 파일에 지정된 컨테이너가 유효한 실제 컨테이너를 가리킵니다.
- 각 LDAP 사용자가 고유한 UID로 구성되었습니다.

NAS 서버가 이름 지정 서비스에 대해 로컬 파일을 사용하도록 구성

이름 지정 서비스에서 로컬 파일을 사용하도록 구성할 수 있습니다.

- 로컬 파일은 DNS, LDAP 및 NIS 디렉토리 서비스를 대신하여 사용할 수 있으며 이러한 서비스와 함께 사용할 수도 있습니다.
- UDS(UNIX Directory Service)와 함께 로컬 파일을 구성하는 경우 스토리지 시스템은 로컬 파일을 먼저 쿼리합니다.
- NFS 서버 생성을 완료한 후에는 뒤로 돌아가 더 많은 로컬 파일을 업로드할 수 있습니다.
- NAS 서버가 생성되면 다음 단계에 설명된 대로 로컬 파일을 활성화합니다.

1. **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **Local Files**를 선택합니다.
2. 각 로컬 파일 유형마다 아래 화살표를 선택해 현재 파일을 다운로드합니다. 스토리지 시스템에 파일이 없는 경우 시스템은 파일 템플릿을 다운로드합니다.
3. 시스템 정보를 사용하여 파일을 업데이트합니다.

   FTP 액세스를 위해 로컬 파일을 사용하려면 `passwd` 파일에 사용자의 암호화된 암호가 포함되어야 합니다. 이 암호는 FTP 액세스에만 사용됩니다. `passwd` 파일은 표준 UNIX 시스템과 동일한 형식 및 구문을 사용하므로 이 암호를 활용하여 로컬 `passwd` 파일을 생성할 수 있습니다. UNIX 시스템에서 `useradd`를 사용하여 사용자를 추가하고 `passwd`를 사용하여 해당 사용자의 암호를 설정합니다. 그런 다음 `/etc/shadow` 파일에서 해시된 암호를 복사하여 `/etc/passwd` 파일의 두 번째 필드에 추가하고 `/etc/passwd` 파일을 NAS 서버에 업로드합니다.
4. 업데이트된 파일을 로컬 머신에 저장합니다.
5. **Upload Local Files**를 선택하고, 편집한 파일의 위치를 찾은 뒤 업로드할 파일을 선택합니다.
6. 각 파일 유형마다 이 단계를 반복합니다.

로컬 파일 구성 문제를 해결하려면 다음 사항을 확인합니다.

- 파일이 올바른 구문으로 생성되었습니다. (각 줄에는 6개의 콜론이 필요합니다.) 구문 및 예제에 대한 자세한 정보는 템플릿을 참조하십시오.
- 각 사용자에게 고유한 이름과 UID가 있습니다.

NAS 서버 공유 프로토콜 구성

NAS 서버에 대해 구성된 공유 프로토콜을 구성하거나 수정할 수 있습니다.

NFS에 대한 공유 프로토콜을 구성할 때는 다음 중 하나 이상을 설정해야 합니다.

- NFS 서버
- FTP

NFS 서버 구성

NAS 서버를 UNIX 전용 시스템용으로 구성하거나 NFS 서버 설정을 수정할 수 있습니다.

DNS 및 NTP는 보안 NFS 서버를 구성하기 전에 구성해야 합니다.

1. **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **NFS Server** 탭을 선택합니다.
2. **Linux/UNIX shares** 옵션을 활성화하여 UNIX 지원을 위한 NAS 서버를 정의합니다.
3. **NFSv3** 또는 **NFSv4** 중 하나를, 아니면 두 가지 모두를 활성화합니다.
4. 필요에 따라 보안 NFS를 비활성화하거나 활성화합니다.
   확장된 UNIX 자격 증명도 활성화됩니다.
5. 자격 증명에 대한 **Enable or disable Extend Unix**를 선택합니다.

   노트: 보안 NFS는 16개가 넘는 그룹을 가진 NFS 자격 증명을 지원하며, 이는 확장된 UNIX 자격 증명 옵션과 동일합니다.

   - 이 필드를 선택하면 NAS 서버는 UID(User ID)를 사용하여 기본 GID(Group ID)와 모든 소속 그룹 GID를 가져옵니다. NAS 서버는 로컬 비밀번호 파일 또는 UDS의 GID를 가져옵니다.
   - 이 필드를 선택 취소하면 프레임에 포함된 네트워크 정보에서 NFS 요청의 UNIX 자격 증명이 추출됩니다. 이 방법은 성능이 더 우수하지만 최대 16개 그룹의 GID만 포함하도록 제한됩니다.
6. 액세스 자격 증명을 캐시에 보존할 기간을 분 단위로 **Credential Cache Retention**에 입력합니다.
7. 변경 사항을 **적용**합니다.

FTP 또는 SFTP 공유 프로토콜 구성

기존 NAS 서버에만 해당하는 FTP/SFTP(FTP over SSH) 설정을 구성할 수 있습니다.

수동 모드 FTP는 지원되지 않습니다.

NFS와 동일한 방법으로 FTP 액세스를 인증할 수 있습니다. 인증이 완료된 후 보안 및 사용 권한을 위한 액세스는 NFS와 동일합니다. 형식이 `user@domain` 또는 `domain\user`가 아닌 경우 NFS 인증이 사용됩니다. NFS 인증에는 로컬 파일, LDAP, NIS 또는 LDAP나 NIS가 있는 로컬 파일이 사용됩니다.

NFS, FTP 액세스 시 로컬 파일을 사용하려면 `passwd` 파일에 사용자의 암호화된 암호가 포함되어야 합니다. 이 암호는 FTP 액세스에만 사용됩니다. `passwd` 파일은 표준 Unix 시스템과 동일한 형식과 구문을 사용하므로 이를 활용하여 로컬 `passwd` 파일을 생성할 수 있습니다. Unix 시스템에서 `useradd`를 사용하여 새 사용자를 추가하고 `passwd`를 사용하여 해당 사용자의 암호를 설정합니다. 그런 다음 `/etc/shadow` 파일에서 해시된 암호를 복사하여 `/etc/passwd` 파일의 두 번째 필드에 추가하고 `/etc/passwd` 파일을 NAS 서버에 업로드합니다. `/etc/passwd` 파일 업로드에 대한 자세한 내용은 로컬 파일을 사용하여 서비스 이름을 지정하도록 NAS 서버 구성 을 참조하십시오.

1. **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **FTP** 탭을 선택합니다.
2. **FTP**에서 Disabled로 설정된 경우 버튼을 **Enable**로 밉니다.
3. 필요에 따라 SSH FTP를 활성화합니다. **SFTP**에서 Disabled로 설정된 경우 버튼을 **Enable**로 밉니다.
4. **FTP/SFTP Server Access**에서 파일에 대한 액세스 권한이 있는 인증된 사용자 유형을 선택합니다.
5. 필요에 따라 **Home Directory and Audit** 옵션을 표시합니다.
   - **Home directory restrictions**를 선택하거나 선택 취소합니다. 비활성화된 경우 **Default home directory**를 입력합니다.
   - **Enable FTP/SFTP Auditing**을 선택하거나 선택 취소합니다. 선택한 경우 감사 파일을 저장할 디렉토리 위치와 감사 파일에 허용되는 최대 크기를 입력합니다.
6. 필요에 따라 **Show Messages**를 선택하고 기본 **Welcome message**와 **Message of the day**를 입력합니다.
7. 필요에 따라 **Show Access Control List**를 선택하여 **Filtered Users**, **Filtered Groups** 및 **Filtered hosts**에 대한 액세스 권한을 제공하거나 액세스를 거부합니다.
8. **Apply**를 클릭합니다.

NAS 서버 보안을 위한 Kerberos 구성

Kerberos를 사용하여 NAS 서버를 구성할 수 있습니다.

Kerberos는 보안 키 암호화를 사용하여 강력한 인증 기능을 제공하도록 설계된 분산 인증 서비스입니다. 안전하지 않은 네트워크를 통해 통신하는 노드가 안전한 방식으로 ID를 증명할 수 있도록 하는 "티켓"을 기반으로 작동합니다. 보안 NFS 서버 역할을 수행하도록 구성된 경우 NAS 서버는 RPCSEC_GSS 보안 프레임워크와 Kerberos 인증 프로토콜을 사용하여 사용자와 서비스를 확인합니다.

NAS 서버가 NFS만 사용하여 구성되어 있는 상태에서 Kerberos를 사용하여 보안 NFS 또는 LDAP를 구성하려는 경우, PowerStore에 보안을 구성하기 전에 먼저 맞춤 구성 영역을 사용하여 Kerberos를 구성해야 합니다.

NAS 서버가 NFS 프로토콜과 SMB 프로토콜을 모두 사용하여 구성된 경우에는 도메인에 연결된 SMB 서버가 NAS 서버에 존재하므로 AD로 상속된 Kerberos를 사용할 수 있습니다.

스토리지 시스템은 NTP 서버를 사용하여 구성해야 합니다. Kerberos는 네트워크의 클라이언트, 서버 및 KDC 간 시간 동기화가 올바르게 이루어져야 합니다.

보안 NFS용 Kerberos 구성

보안 NFS에 대한 Kerberos를 구성할 경우 다음 사항에 유의하십시오.

- NFS에만 NAS 서버를 구성하는 경우에는 사용자 지정 영역을 사용하여 NAS 서버를 구성해야 합니다. NFS 및 SMB를 사용하여 NAS 서버를 구성한 경우 AD 또는 사용자 지정 영역을 사용할 수 있습니다.
- 보안 강화를 위해 LDAPS 또는 Kerberos를 사용하는 LDAP를 사용하는 것이 좋습니다.
- DNS 서버는 NAS 서버 레벨에서 구성해야 합니다. KDC, NFS 서버, NFS 클라이언트를 포함한 Kerberos 영역의 모든 구성원을 DNS 서버에 등록해야 합니다.
- NFS 클라이언트의 호스트 이름 FQDN과 NAS 서버 FQDN을 DNS 서버에 등록해야 합니다. 클라이언트와 서버는 Kerberos 영역의 FQDN의 모든 구성원을 하나의 IP 주소에서 확인할 수 있어야 합니다.
- NFS 클라이언트의 SPN에서 FQDN 부분을 DNS 서버에 등록해야 합니다.
- 보안 NFS를 구성할 때 keytab 파일을 NAS 서버에 업로드해야 합니다.

Kerberos에 대한 사용자 지정 영역 생성

Kerberos와 함께 사용할 사용자 지정 영역을 구성할 수 있습니다.

사용자 지정 Kerberos 영역에서는 모든 종류의 KDC(MIT/Heimdal 또는 AD)를 구성할 수 있습니다. NAS 서버에 SMB 서버가 구성되지 않았거나 SMB 서버 도메인에 대해 구성된 영역이 아닌 다른 Kerberos 영역을 사용하려는 경우 이 방법을 사용하십시오.

순수 NFS 서버에 대한 맞춤 구성 영역 생성

Unix 기반 KDC를 사용하려면 PowerStore에서 Kerberos를 구성하기 전에 다음 단계를 수행하십시오. 단, 이 단계는 Kerberos 영역 linux.dellemc.com에서 NFS 서버의 호스트 이름으로 myrealm을 사용하려는 경우를 가정한 것입니다.

1. `kadmin.local` 툴을 실행합니다.
2. 보안 주체와 그 키를 생성합니다.

```
kadmin.local: addprinc -randkey nfs/myrealm.linux.dellemc.com
```

   및/또는

```
kadmin.local: addprinc -randkey nfs/myrealm
```

3. 보안 주체의 키를 keytab 파일 myrealm.linux.dellemc.fr에 넣습니다.

```
kadmin.local: ktadd -k myrealm.linux.dellemc.com.keytab nfs/myrealm.linux.dellemc.fr
```

멀티 프로토콜(NFS 및 SMB) NAS 서버에 대한 사용자 지정 영역 생성

NAS 서버에서 SMB 서버 계정을 사용하지 않고 Windows 기반 KDC를 사용하려면 PowerStore에서 Kerberos를 구성하기 전에 다음의 단계를 따르십시오. 단, 이 단계는 NFS 서버에 대해 myrealm.windows.dellemc.com을 FQDN으로 사용하려는 경우를 가정한 것입니다.

1. Windows 도메인 windows.dellemc.com의 AD(Active Directory)에서 NAS 서버용 계정 myrealm을 생성합니다.
2. 생성한 컴퓨터 계정에서 서비스 SPN을 등록합니다.

```
C:\setspn -S nfs/myrealm.windows.dellemc.com myrealm
```

3. SPN이 생성되었는지 확인합니다.

```
C:\setspn myrealm
```

4. SPN에 대한 keytab 파일을 생성합니다.

```
C:\ktpass -princ nfs/myrealm.windows.dellemc.com@WINDOWS.DELLEMC.COM -mapuser
WINDOWS\myrealm
 -crypto ALL +rndpass -ptype KRB5_NT_PRINCIPAL -out myrealm.windows.dellemc.com.keytab
```

NAS 서버에 대한 Kerberos 보안 구성

Kerberos 보안을 사용하여 NAS 서버를 구성할 수 있습니다.

NFS의 구성인 경우, NAS 서버에 대해 DNS와 LDAP가 구성되어 있고 Kerberos 영역의 모든 구성원이 DNS 서버에 등록되어 있어야 합니다.

SMB와 NFS 모두에 대해 구성된 NAS 서버를 사용하는 경우에는 SMB 서버를 AD 도메인에 추가해야 합니다.

1. **Storage** > **NAS Servers** > **[nas server]** > **Security** > **Kerberos**를 선택합니다.
2. Disabled로 설정된 경우 버튼을 밀러 **Enabled**로 변경합니다.
3. **Realm** 이름을 입력합니다.
4. **Kerberos IP Address**를 입력하고 **Add**를 클릭합니다.
5. 사용할 Kerberos에 대한 TCP 포트를 입력합니다. 기본값 포트는 88입니다.
6. **Apply**를 클릭합니다.

보안 NFS를 사용하여 NAS 서버를 성공적으로 생성한 후에 AD 영역을 사용자 지정 영역으로 변경하는 경우에는 다음 작업을 수행할 때까지 어떠한 NFS 내보내기도 마운트할 수 없습니다.

1. Keytab 파일을 생성합니다.
2. NAS 서버에서 AD 영역을 제거합니다.
3. AD 서버의 사용자 이름 및 암호를 입력합니다.
4. 사용자 지정 영역을 입력합니다.
5. Keytab 파일을 업로드합니다.

NAS 서버 삭제

NAS 서버를 선택하고 삭제를 확인하여 연결된 파일 시스템 또는 보호 정책이 없는지 확인합니다.

- 서버에 파일 시스템이 없는지 확인합니다.
- 서버와 연결된 보호 정책이 없는지 확인합니다.

1. **StorageNAS** > **Servers**를 선택하여 NAS Servers 목록을 엽니다.
2. 목록에서 삭제할 서버 옆의 확인란을 선택합니다.
3. **More ActionsDelete** > 를 선택합니다.

   노트: 선택한 NAS 서버에 파일 시스템이 포함되어 있거나 보호 정책과 연결되어 있는 경우 Delete 옵션을 사용할 수 없습니다. Delete 옵션 위로 마우스를 가져가면 비활성화 이유가 표시됩니다.

4. **삭제**를 선택하여 확인합니다.

선택한 NAS 서버가 삭제됩니다.

3

NFS 내보내기 구성

이 장에서 다루는 내용은 다음과 같습니다.

주제:

파일 시스템 및 NFS 내보내기 개요

파일 시스템 및 NFS 내보내기를 생성하는 동안 다음 사항에 유의하는 것이 좋습니다.

- 파일 시스템을 생성하기 전에 NFS 프로토콜을 지원하도록 NAS 서버를 구성해야 합니다.
- 파일 시스템을 처음 생성할 때 NFS 내보내기를 추가하도록 선택할 수 있습니다. 또는 NFS 내보내기를 생성한 후 파일 시스템에 추가할 수 있습니다.

NFS 내보내기를 위한 파일 시스템 생성

NFS 내보내기를 위한 파일 시스템을 생성할 수 있습니다.

NFS 프로토콜을 지원하도록 구성된 NAS 서버가 있는지 확인합니다.

1. **Storage** > **File Systems**를 선택합니다.
2. **Create**를 클릭합니다.
   Create File System 마법사가 시작됩니다.
3. **General** 또는 **VMware File System**을 파일 시스템 유형으로 선택합니다.

   노트: VMware 파일 시스템은 VMware에 최적화되고 VMware 워크로드에 사용되는 PowerStore 파일 시스템입니다. 이 옵션은 VMware NFS 데이터 저장소에 대해서만 선택해야 합니다. 다른 모든 파일 시스템의 경우 **General**을 선택합니다.

4. 파일 시스템에 대해 NFS 지원 NAS 서버를 선택합니다.
5. 파일 시스템 이름 및 크기, 최소 크기 3GB, 최대 크기 256TB를 포함한 파일 시스템 세부 정보를 지정합니다.

   노트: 크기에 관계없이 모든 씬 파일 시스템은 생성 시 메타데이터용으로 1.5GB가 예약되어 있습니다. 예를 들어 100GB 씬 파일 시스템을 생성한 후 PowerStore T 모델 및 PowerStore Q 모델에서는 1.5GB가 사용되고 있다고 표시됩니다. 파일 시스템이 호스트에 마운트되면 98.5GB의 가용 용량이 표시됩니다. 이는 메타데이터 공간이 사용 가능한 파일 시스템 용량에서 예약되기 때문입니다.

6. 필요에 따라 파일 보존 유형(일반 파일 시스템에만 사용 가능)을 선택합니다.
   - 엔터프라이즈(FLR-E) - NFS 및 FTP를 통해 사용자가 변경한 사항으로부터 콘텐츠를 보호합니다. 관리자는 보호 대상 파일이 포함된 FLR-E 파일 시스템을 삭제할 수 있습니다.
   - Compliance(FLR-C) - 사용자 및 관리자가 변경한 사항으로부터 콘텐츠를 보호하고 SEC 규칙 17a-4(f) 요구 사항을 준수합니다. FLR-C 파일 시스템은 보호 대상 파일이 없는 경우에만 삭제할 수 있습니다.

   노트: FLR 상태 및 파일 보존 유형은 파일 시스템 생성 시 설정되며 수정할 수 없습니다.

   보존 기간을 설정합니다.
   - Minimum - 파일을 잠금 설정할 수 있는 가장 짧은 기간을 지정합니다(기본값 1일).
   - Default - 파일이 잠금 설정되어 있고 보존 기간이 지정되지 않은 경우 사용됩니다.
   - Maximum - 파일을 잠금 설정할 수 있는 가장 긴 기간을 지정합니다.
7. 필요에 따라 파일 시스템의 초기 내보내기를 구성합니다.

노트: 나중에 파일 시스템에 NFS 내보내기를 추가할 수 있습니다.

8. 초기 내보내기를 구성한 경우 호스트 액세스를 구성합니다.

옵션	설명
최소 보안	비보안 NFS 또는 보안 NFS 사용자가 파일 시스템에서 마운트 및 NFS 내보내기를 수행할 수 있도록 하려면 **Sys**를 선택합니다. 보안 NFS를 구성하지 않는 경우 이 옵션을 선택해야 합니다. 보안 NFS를 사용하여 파일 시스템을 생성하는 경우 다음 옵션 중에서 선택할 수 있습니다. • 인증(krb5/krb5i/krb5p)을 위해 모든 유형의 Kerberos 보안을 허용하려면 **Kerberos**를 선택합니다. • 사용자 인증(krb5i/krb5p)을 위해 무결성을 사용하는 Kerberos와 암호화 보안을 사용하는 Kerberos를 모두 허용하려면 **Kerberos with Integrity**를 선택합니다. • 사용자 인증(krb5p)을 위해 암호화 보안을 사용하는 Kerberos만 허용하려면 **Kerberos with Encryption**을 선택합니다.
기본 액세스	기본적으로 호스트에 적용되는 액세스 유형입니다. 필요에 따라 개별 호스트를 추가할 때 호스트에 대한 다른 액세스 유형을 선택할 수 있습니다. 옵션은 다음과 같습니다. • **No Access** - 스토리지 리소스나 공유에 대한 액세스를 허용하지 않습니다. • **읽기/쓰기** - 호스트가 NFS 데이터 저장소 또는 공유에 대한 읽기 및 쓰기 권한을 갖습니다. • **읽기 전용** - 호스트가 스토리지 리소스 또는 공유 콘텐츠를 볼 수 있지만 쓸 수는 없습니다. **노트:** ESXi 호스트가 **Kerberos NFS 소유자** 인증과 NFSv4를 사용하여 NFS Datastore를 마운트하려면 **읽기//쓰기** 액세스 권한이 있어야 합니다. • **읽기/쓰기, 루트 허용** - 호스트가 스토리지 리소스나 공유를 읽고 쓸 수 있으며 스토리지를 액세스하는 다른 로그인 계정에 대한 액세스 권한(예: 특정 파일과 디렉토리 읽기, 수정 및 실행 권한)을 부여 및 취소할 수 있습니다. NFS 클라이언트의 루트는 공유에 대한 루트 액세스 권한을 갖습니다. **노트:** 호스트가 지원되는 클러스터 구성의 일부가 아닌 경우 둘 이상의 호스트에 대한 읽기/쓰기 액세스를 허용하지 마십시오. **노트:** ESXi 호스트가 NFS 소유자: root 인증과 NFSv4를 사용하여 NFS 데이터 저장소를 마운트하려면 **Read/Write, allow Root** 액세스 권한이 있어야 합니다. • **Read-Only, allow Root** — 호스트에 공유의 콘텐츠를 볼 수 있는 권한은 있지만 쓸 수 있는 권한은 없습니다. NFS 클라이언트의 루트는 공유에 대한 루트 액세스 권한을 갖습니다.
호스트 추가	호스트를 개별적으로 입력하거나 올바른 형식의 CSV 파일을 업로드하여 호스트를 추가할 수 있습니다. 먼저 CSV 파일을 다운로드하여 템플릿을 얻을 수 있습니다. CSV 파일 템플릿을 다운로드하고 편집하고 사용하려면 다음을 수행합니다. a. **Export Hosts** 아이콘을 클릭합니다. b. 호스트와 가져오려는 액세스 유형으로 CSV 파일을 업데이트합니다. c. CSV 파일을 로컬 머신에 저장합니다. d. **Import CSV file**을 클릭합니다. e. CSV 파일을 찾아 Microsoft 파일 탐색기 창에서 **Open**을 클릭합니다. CSV 파일의 호스트가 CVS 파일에서 정의한 **Access Type**과 함께 **Import Host List**에 표시됩니다.

9. 선택적으로 파일 시스템에 보호 정책을 추가합니다.
   파일 시스템에 보호 정책을 추가하는 경우 파일 시스템을 생성하기 전에 정책을 생성해야 합니다. 선택한 보호 정책에는 스냅샷 규칙과 복제 규칙이 모두 포함될 수 있습니다.
10. 필요에 따라 파일 시스템에 QoS 정책을 추가합니다.
    노트: 선택한 정책에서 설정된 대역폭이 NAS 서버에 설정된 최대 대역폭을 초과하는 경우 유효 대역폭은 서버의 최대 대역폭입니다.
11. 요약을 검토하고 **Create File System**을 클릭합니다.
    파일 시스템이 **File System** 탭에 추가됩니다. 동시에 내보내기를 생성한 경우 내보내기가 **NFS export** 탭에 표시됩니다.

NFS 내보내기 생성

파일 시스템에 NFS 내보내기를 생성할 수 있습니다.

1. **Storage** > **File Systems** > **NFS Export** 탭을 선택합니다.
2. **Create**를 클릭합니다.
   Create NFS Export 마법사가 실행됩니다.
3. 다음 사항에 주의하여 필요 정보를 입력합니다.
   - 스냅샷을 기반으로 내보내기를 생성하려면 NFS 내보내기를 생성하기 전에 스냅샷을 생성해야 합니다.
   - **Local Path**는 호스트 측에서 생성된 파일 시스템 내 기존 폴더 이름에 해당해야 합니다.
   - **NFS 내보내기 세부 정보**, **이름** 필드에 지정한 값은 NAS 서버 이름과 함께 내보내기 경로를 구성합니다.

     노트: NAS 서버 IP 및 로컬 경로를 사용하여 내보내기를 마운트할 수도 있습니다.

   - NFS 내보내기 이름은 프로토콜별로 NAS 서버 수준에서 고유한 값이어야 합니다. SMB 공유 및 NFS 내보내기에 대해 같은 이름을 지정할 수는 있습니다.
4. 설정을 승인한 후 **Create NFS Export**를 클릭합니다.
   NFS 내보내기가 **NFS Export** 페이지에 표시됩니다.

FLR(File Level Retention)

FLR(File Level Retention)을 사용하면 지정된 보존 기간 동안 파일의 수정 또는 삭제를 방지할 수 있습니다. FLR을 사용하여 파일 시스템을 보호하면 영구적이고 변경 불가능한 파일 및 디렉토리 세트를 생성할 수 있습니다. FLR은 데이터 무결성과 접근성을 보장하고, 관리자를 위한 아카이빙 절차를 간소화하며, 스토리지 관리 유연성을 향상시킵니다.

파일 레벨 보존에는 두 가지 유형이 있습니다.

- Enterprise(FLR-E) - SMB, NFS 및 FTP를 사용하여 사용자 및 스토리지 관리자가 변경한 사항으로부터 데이터를 보호합니다. 관리자는 잠긴 파일이 포함된 FLR-E 파일 시스템을 삭제할 수 있습니다.
- Compliance(FLR-C) - SMB, NFS 및 FTP를 사용하여 사용자 및 스토리지 관리자가 변경한 사항으로부터 데이터를 보호합니다. 관리자는 잠긴 파일이 포함된 FLR-C 파일 시스템을 삭제할 수 없습니다. FLR-C는 SEC 규칙 17a-4(f)를 준수합니다.

다음과 같은 제한 사항이 적용됩니다.

- FLR은 통합 PowerStore 시스템 3.0 이상에서 사용할 수 있습니다.
- FLR은 VMware 파일 시스템에서 지원되지 않습니다.
- 파일 시스템에 FLR 활성화 및 FLR 유형은 파일 시스템 생성 시 설정되며 수정할 수 없습니다.
- FLR-C는 스냅샷에서의 복원을 지원하지 않습니다.
- 스냅샷을 사용하여 새로 고치는 경우 두 파일 시스템의 FLR 유형이 동일해야 합니다.
- 파일 시스템을 복제할 때 소스 및 대상 파일 시스템은 FLR 유형이 동일해야 합니다.
- 클론 생성된 파일 시스템의 FLR 유형은 소스와 동일합니다(수정할 수 없음).

FLR 모드는 File Systems 테이블의 **FLR Mode** 열에 표시됩니다.

DHSM 서버 구성

FLR(File Level Retention)에는 DHSM 서버 자격 증명이 필요합니다.

DHSM 서버는 FLR을 사용하려는 Window 호스트에도 필요하며 DHSM 서버를 사용하려면 FLR 지원 파일 시스템을 관리할 수 있는 FLR 툴킷을 설치해야 합니다.

1. **Storage** > **NAS Servers** > **[NAS server]** > **Protection** > **DHSM**을 선택합니다.
2. 비활성화된 경우 버튼을 밀어 **Enabled**로 변경합니다.
3. DHSM 서버의 사용자 이름과 암호를 입력하고 암호를 확인합니다.
4. **Apply**를 선택합니다.

FLR(File Level Retention) 구성

FLR(File Level Retention)은 파일 시스템 생성 시 구성됩니다. 자세한 내용은 파일 시스템 생성을 참조하십시오.

노트: 파일 레벨 보존 및 해당 레벨은 파일 시스템 생성 시 결정되며 수정할 수 없지만 보존 기간 매개변수는 수정할 수 있습니다.

FLR(File Level Retention) 수정

보존 기간 매개변수는 파일 시스템 생성 시 또는 그 이후에 설정할 수 있으며 수정할 수 있습니다.

노트: 보존 기간 매개변수를 수정해도 이미 잠긴 파일에는 영향을 주지 않습니다.

1. **Storage** > **File Systems** > **[file system]** > **Security & Events** > **File-Level Retention**을 선택합니다.
2. 보존 기간 매개변수를 설정합니다.
   - 최소 보존 기간 - FLR 지원 파일 시스템을 보호할 수 있는 가장 짧은 기간을 지정합니다(기본값 1일).
   - 기본 보존 기간 - 파일이 잠겨 있고 보존 기간이 지정되지 않은 경우 사용됩니다(기본값 1년).
   - 최대 보존 기간 - FLR 지원 파일 시스템을 보호할 수 있는 가장 긴 기간을 지정합니다(기본값 무제한).
3. 필요한 경우 고급 설정을 지정합니다.
   - 자동 파일 잠금 - FLR 지원 파일 시스템에서 파일을 자동으로 잠글 것인지 여부를 지정하고 파일 수정과 자동 잠금 사이의 기간을 결정하는 정책 간격을 설정할 수 있습니다(정책 간격 기본값은 1시간).
   - 자동 파일 삭제 - 보존 기간이 만료된 후 잠긴 파일을 자동으로 삭제할지 여부를 지정할 수 있습니다. 삭제할 파일을 찾기 위한 첫 번째 스캔은 기능이 활성화된 후 7일입니다.
4. **Apply**를 선택합니다.

4

추가 NAS 서버 기능

이 장에서 다루는 내용은 다음과 같습니다.

주제:

기본 UNIX 디렉토리 서비스 설정

NAS 서버를 생성한 후 사용자 액세스를 위한 기본 UDS(UNIX Directory Services) 검색 순서를 설정할 수 있습니다.

1. **Storage** > **NAS Servers**를 선택합니다.
2. NAS 서버의 왼쪽에 있는 **Name** 열에서 확인란을 선택합니다.
3. **Modify**를 클릭합니다.
4. **Unix Directory Service Search Order** 드롭다운 목록에서 사용할 기본 UDS 검색 순서를 선택합니다.
5. **Apply**를 클릭합니다.

NAS 서버 네트워크 구성

NAS 서버 네트워크를 수정하거나 구성할 수 있습니다.

NAS 서버 네트워크에 대해 다음을 구성하십시오.

- 파일 인터페이스
- 호스트 같은 외부 서비스에 대한 경로

NAS 서버에 대한 파일 인터페이스 구성

PowerStore에 서버를 추가한 후 NAS 서버에 대한 파일 인터페이스를 구성할 수 있습니다.

더 많은 파일 인터페이스를 추가하고, 사용할 기본 인터페이스를 정의할 수 있습니다. 또한, 운영 및 백업이나 IPv4 또는 IPv6에 사용할 인터페이스를 정의할 수 있습니다.

1. **Storage** > **NAS Servers** > **[nas server]**를 선택합니다.
2. **Network** 페이지에서 **Add**를 클릭하여 NAS 서버에 다른 파일 인터페이스를 추가합니다.
3. 파일 인터페이스 속성을 입력합니다.

   노트: 관리 및 스토리지 네트워크에 사용 중인 VLAN을 재사용하지 마십시오.

4. 목록에서 파일 인터페이스를 선택하여 파일 인터페이스에서 다음 작업을 수행할 수 있습니다. 선택:

옵션	설명
수정	파일 인터페이스 속성을 변경합니다.
삭제	NAS 서버에서 파일 인터페이스를 삭제합니다.
Ping	NAS 서버에서 외부 IP 주소로의 접속을 테스트합니다.
기본 인터페이스	여러 운영 및 백업 인터페이스가 정의되어 있을 때 어떤 인터페이스 PowerStore를 기본값으로 사용할지 정의합니다.

외부 연결용 파일 인터페이스에 대한 경로 구성

파일 시스템이 외부 연결에 사용하는 경로를 구성할 수 있습니다.

File Interface 카드에서 **Ping** 옵션을 사용하여, 파일 인터페이스가 외부 리소스에 대한 액세스 권한이 있는지 여부를 확인할 수 있습니다.

대개는 NAS 서버 인터페이스는 NAS 서버의 인터페이스에서 외부 서비스로 요청을 라우팅하는 데 사용되는 기본 게이트웨이로 구성됩니다.

다음 단계를 따르십시오.

- 외부 서비스에 대해 보다 세분화된 경로를 구성해야 하는 경우
- 특정 게이트웨이를 통해 특정 인터페이스에서 서버에 액세스하기 위한 경로를 추가해야 하는 경우.

1. **Storage** > **NAS Servers** > **[nas server]** > **Network** > **Routes to External Services**를 선택합니다.
2. **Add**를 클릭하여 **Add Route** 마법사에 경로 정보를 입력합니다.

NDMP 백업 활성화

NDMP를 사용하여 NAS 서버에 대한 표준 백업을 구성할 수 있습니다.NDMP(Network Data Management Protocol)는 네트워크에서 파일 서버를 백업하기 위한 표준을 제공합니다. NDMP가 활성화되면 Dell Networker와 같은 타사 DMA(Data Management Application)에서 NAS 서버 IP 주소를 사용하여 PowerStore NDMP를 감지할 수 있습니다.

NDMP 활성화는 NAS 서버가 생성된 후에 수행됩니다.

PowerStore는 다음을 지원합니다.

- 3방향 NDMP - 데이터는 LAN(local area network) 또는 WAN(Wide Area Network)에서 DMA를 통해 전송됩니다.
- 전체 및 증분 백업

1. **Storage** > **NAS Servers** > **[nas server]** > **Protection**을 선택합니다.
2. **NDMP Backup**에서 **Disabled**로 설정된 경우 버튼을 밀어 **Enable**로 변경합니다.
3. **New Password**에 암호를 입력합니다.
   사용자 이름은 항상 `ndmp`입니다.
4. **Verify Password**에 새 암호와 동일한 암호를 다시 입력합니다.
5. **Apply**를 클릭합니다.

NDMP 페이지에서 나가 NDMP 페이지로 되돌아간 뒤 NDMP가 활성화되어 있는지 검증합니다.

5

기타 파일 시스템 기능

이 장에서 다루는 내용은 다음과 같습니다.

주제:

파일 시스템 할당량

파일 시스템에서 또는 디렉토리 레벨에서 파일 시스템에 대한 할당량을 구성하여 드라이브 공간 사용을 추적 및 제한할 수 있습니다. 할당량 활성화 또는 비활성화는 언제든지 가능하지만 파일 시스템 작업에 영향을 미치지 않도록 사용량이 적은 운영 시간에 활성화하거나 비활성화하는 것이 좋습니다.

노트: 읽기 전용 파일 시스템에 대한 할당량을 활성화할 수 없습니다.

노트: 할당량은 VMware 파일 시스템에서 지원되지 않습니다.

노트: 복제 세션을 생성할 때 소스 시스템에서 할당량이 활성화되어 있더라도 대상 시스템에는 할당량이 표시되지 않습니다.

할당량 유형

파일 시스템에 적용할 수 있는 할당량에는 세 가지 유형이 있습니다.

표 2. 할당량 유형

유형	설명
사용자 할당량	개별 사용자가 파일 시스템에 데이터를 저장하여 소비하는 스토리지의 양을 제한합니다.
트리 할당량	트리 할당량은 특정 디렉토리 트리에서 사용하는 총 스토리지 양을 제한합니다. 트리 할당량을 사용하여 다음을 수행할 수 있습니다. • 프로젝트 기반 스토리지 제한값을 설정합니다. 예를 들어 여러 사용자가 파일을 공유 및 생성하는 프로젝트 디렉토리에 대해 트리 할당량을 설정할 수 있습니다. • 트리 할당량의 고정적 제한 및 유동적 제한을 0으로 설정하여 디렉토리 사용량을 추적합니다. **노트:** 트리 할당량의 제한을 변경하는 경우 해당 변경 사항은 파일 시스템 작업의 중단 없이 즉시 적용됩니다.
할당량 트리의 사용자 할당량	할당량 트리에 데이터를 저장하여 개별 사용자가 소비하는 스토리지의 양을 제한합니다.

할당량 제한

표 3. 고정적 제한 및 유동적 제한

유형	설명
Hard	하드 제한은 스토리지 사용에 대한 절대 제한입니다. 파일 시스템 또는 할당량 트리의 사용자 할당량이 고정적 제한에 도달하면 추가 공간이 제공되기 전까지 사용자가 파일 시스템 또는 트리에 데이터를 쓸 수 없습니다. 할당량 트리가 고정적 제한에 도달하면 추가 공간이 제공되기 전까지 사용자가 트리에 데이터를 쓸 수 없습니다.

표 3. 고정적 제한 및 유동적 제한 (계속)

유형	설명
유동적 제한	유동적 제한은 스토리지 사용량의 기본 제한값입니다. 사용자는 유예 기간에 도달할 때까지 공간을 사용할 수 있습니다. 유예 기간이 끝날 때까지 유동적 제한에 도달하면 사용자에게 경고가 표시됩니다. 그 후 사용자가 유동적 제한 아래로 돌아올 때 공간 부족 상태에 도달합니다.

할당량 유예 기간

할당량 유예 기간을 사용하면 파일 시스템의 각 트리 할당량에 특정 유예 기간을 설정할 수 있습니다. 유예 기간은 유동적 제한과 고정적 제한 사이의 시간을 카운트다운하고 고정적 제한에 도달하기 전에 남은 시간을 사용자에게 알립니다. 유예 기간이 만료되면 고정적 제한에 도달하지 않아도 추가 공간이 제공되기 전까지 사용자가 파일 시스템에 쓸 수 없습니다.

유예 기간의 만료 날짜를 설정할 수 있습니다. 기본값은 7일입니다. 또는 유예 기간 만료 날짜를 무기한으로 설정하거나(유예 기간이 만료되지 않음) 지정된 일, 시간 또는 분 동안 유예하도록 설정할 수도 있습니다. 유예 기간 만료 날짜가 되면 유예 기간이 더 이상 파일 시스템 디렉토리에 적용되지 않습니다.

추가 정보

할당량에 대한 자세한 내용은 *Dell PowerStore 파일 기능 백서*를 참조하십시오.

사용자 할당량 활성화

할당량을 활성화하고 사용자 할당량 기본값을 설정해야 파일 시스템에 사용자 할당량을 추가할 수 있습니다.

1. **Storage** > **File Systems** > **[file system]** > **Quotas**를 선택합니다.
2. **Storage** > **File Systems** > **[file system]** > **Quotas** > **Properties**를 선택합니다.
3. **비활성화됨** 버튼을 **활성화됨**으로 밉니다.
4. 파일 시스템의 사용자 할당량에 대한 기본 **유예 기간**을 입력합니다. 이는 유동적 제한이 충족된 후 고정적 제한이 충족될 때까지의 시간을 계산합니다.
5. 기본 **Soft Limit** 및 기본 **Hard Limit**를 입력하고 **Update**를 클릭합니다.

파일 시스템에 사용자 할당량 추가

파일 시스템에 사용자 할당량을 생성하여 개별 사용자가 해당 파일 시스템에서 사용하는 스토리지 공간의 양을 제한하거나 추적합니다. 사용자 할당량을 생성하거나 수정할 때, 파일 시스템 레벨에서 설정된 기본 고정적 및 유동적 제한값을 사용할 수 있습니다.

할당량을 활성화하고 사용자 할당량 기본값을 설정해야 파일 시스템에 사용자 할당량을 추가할 수 있습니다. 사용자 할당량 활성화를 참조하십시오.

노트: 읽기 전용 파일 시스템에 대한 할당량을 생성할 수 없습니다.

1. **Storage** > **File Systems** > **[file system]** > **Quotas** > **User**를 선택합니다.
2. **User Quota** 페이지에서 **Add**를 클릭합니다.
3. **Add User Quota** 마법사에서 요청된 정보를 입력합니다. 제한을 설정하지 않고 공간 사용을 추적하려면 **Soft Limit** 및 **Hard Limit**를 제한 없음을 나타내는 0으로 설정합니다.
4. **Add**를 선택합니다.

파일 시스템에 할당량 트리 추가

파일 시스템 디렉토리 레벨에서 할당량 트리를 생성하여 해당 디렉토리에 사용되는 총 스토리지 공간을 제한하거나 추적할 수 있습니다.

1. **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**를 선택합니다.
2. **Add**를 선택합니다.

3. **Enforce User Quota**를 오른쪽으로 밀어 트리 할당량에서 사용자 할당량 기본값을 활성화합니다.
4. 요청된 정보를 제공합니다.
   - **Grace Period**를 입력하여 유동적 제한과 고정적 제한 사이의 시간을 계산합니다. 유예 기간에 도달하면 알림 수신이 시작됩니다.
   - 제한을 설정하지 않고 공간 사용을 추적하려면 **Soft Limit** 및 **Hard Limit** 필드를 제한 없음을 나타내는 0으로 설정합니다.
5. **Add**를 선택합니다.

할당량 트리에 사용자 할당량 추가

할당량 트리에 사용자 할당량을 생성하여 개별 사용자가 해당 목록에서 사용하는 스토리지 공간의 양을 제한하거나 추적합니다. 트리에서 사용자 할당량을 생성할 때, 트리 할당량 레벨에서 설정된 기본 유예 기간과 기본 고정적 및 유동적 제한을 사용할 수 있습니다.

1. **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**를 선택합니다.
2. 경로를 선택하고 **Add User Quota**를 클릭합니다.
3. **Add User Quota** 화면에서 요청된 정보를 입력합니다. 제한을 설정하지 않고 공간 사용을 추적하려면 **Soft Limit** 및 **Hard Limit** 필드를 제한 없음을 나타내는 0으로 설정합니다.

파일 QoS(Quality of Service)

예측 불가능한 요구 사항으로 다양한 워크로드를 실행하는 시스템에서 QoS(Quality of Service)는 중요한 애플리케이션이 우선순위를 갖도록 보장하고 각 애플리케이션에 대해 예측 가능한 성능을 제공합니다.

QoS(Quality of Service) 정책을 적용하여 NAS 서버 및 파일 시스템에 대한 최대 대역폭을 설정할 수 있습니다.

NAS 서버 또는 파일 시스템에 QoS 정책을 할당하면 SDNAS가 NFS/SMB 서비스에 정책을 적용합니다.

대역폭 제한은 NFS/SMB 및 SFTP/FTP 프로토콜을 기반으로 적용됩니다.

설정된 대역폭이 NAS 서버에 설정된 최대 대역폭을 초과하는 경우 유효 대역폭은 서버의 최대 대역폭입니다.

노트: QoS 정책을 적용하는 데 다소 시간이 걸릴 수 있습니다.

노트: NAS 서버 클론, 파일 시스템 클론, 스냅샷, 스냅샷 클론 및 스냅샷 새로 고침에서는 QoS가 지원되지 않습니다.

노트: 할당된 QoS 정책의 일부로 NAS 서버 및 파일 시스템에 적용되는 대역폭은 10% 이내의 허용 범위 내에서 변동할 수 있습니다.

파일 QoS 제한 사항:

- QoS 정책에는 하나의 I/O 제한 규칙이 포함될 수 있습니다.
- 최대 100개의 파일 QoS 정책을 정의할 수 있습니다.
- 최대 100개의 파일 QoS 규칙을 정의할 수 있습니다.
- NAS 서버 또는 파일 시스템에는 하나의 QoS 정책만 적용할 수 있습니다.
- 동일한 QoS 정책을 여러 NAS 서버 및 파일 시스템에 할당할 수 있습니다.

QoS 및 파일 복제:

- NAS 서버에 복제 규칙이 있는 경우 할당된 QoS 정책이 대상 서버에 복제됩니다.
- NAS 서버에 할당된 QoS 정책을 수정하면 변경 사항이 대상 서버에 복제됩니다.
- 대상 서버에서는 복제된 QoS 정책 구성을 수정할 수 없습니다.
- 대상 서버의 NAS 서버 또는 파일 시스템에 QoS 정책을 할당할 수 없습니다.
- 소스 서버의 NAS 서버 또는 파일 시스템에 QoS 정책을 할당한 후에는 대상 서버에서 정책을 할당 취소할 수 없습니다.
- NAS 서버에서 QoS 정책 할당을 취소한 후에는 대상에서도 정책의 할당을 취소해야 합니다.
- 페일오버 후에는 복제된 QoS 정책을 할당, 할당 취소 및 수정할 수 있습니다.

파일 QoS 제한 사항

NAS 서버 및 파일 시스템에 대한 I/O 제한 규칙을 생성할 수 있습니다. I/O 제한 규칙은 허용되는 최대 대역폭을 정의합니다.

- 각 NAS 서버 또는 파일 시스템은 하나의 제한 규칙에만 연결할 수 있습니다.
- 각 정책에는 하나의 규칙만 포함될 수 있습니다.

- 최대 100개의 규칙을 정의할 수 있습니다.

노트: 관찰된 대역폭은 특히 더 낮은 설정 한계에서 설정 값을 초과할 수 있습니다.

I/O 제한 규칙은 외부 호스트의 I/O에만 적용되며 내부 비동기식 또는 동기식 복제 작업 또는 마이그레이션 I/O에는 적용되지 않습니다.

입출력 제한 규칙은 SDNAS의 NDMP 서버에서 제공하는 NDMP 백업과 같이 내부적으로 생성된 오브젝트에는 적용되지 않습니다.

파일 QoS 제한에 대한 특정 알림은 지원되지 않습니다. 설정된 제한에 조정이 필요한지 알아보려면 각 NAS 서버 및 파일 시스템에 대한 레이턴시, IOPS 및 대역폭 차트를 모니터링할 수 있습니다.

QoS(Quality of Service) 대역폭 제한 규칙 및 정책 생성

대역폭 제한 규칙을 생성하여 QoS 정책에 추가할 수 있습니다.

1. **Storage** > **Quality of Service (QoS)** > **File I/O Limit Rules**를 선택합니다.
2. **Create**를 선택합니다.
3. **Create File I/O Limit Rule** 슬라이드 아웃에서 규칙 이름과 최대 대역폭(MB/s)을 설정합니다.
4. **Create**를 선택합니다.
   규칙이 파일 I/O 제한 규칙 테이블에 추가됩니다.
5. **File QoS Policies**를 선택합니다.
6. **Create**를 선택합니다.
7. **Create File QoS Policy** 슬라이드 아웃에서 정책 이름을 설정합니다. 설명도 추가할 수 있습니다.
8. 규칙 목록에서 정책에 추가할 규칙을 선택합니다.
9. **Create**를 선택합니다.
   정책이 파일 QoS 정책 테이블에 추가됩니다.

파일 QoS 정책 할당

I/O 제한 규칙을 파일 QoS 정책의 일부로 정의한 후 NAS 서버 또는 파일 시스템에 할당할 수 있습니다. 할당된 QoS 정책을 수정할 수도 있습니다.

노트: NAS 서버 또는 파일 시스템을 생성하는 절차의 일부로 QoS 정책을 할당할 수도 있습니다.

1. **Storage** > **NAS Servers** or **Storage** > **File Systems**를 선택합니다.
2. 관련 NAS 서버 또는 파일 시스템 옆의 확인란을 선택합니다.
3. **More Actions** > **Change QoS Policy**를 선택합니다.
4. **QoS 정책 변경** 슬라이드 아웃에서 파일 QoS 정책을 선택한 다음 **Apply**를 선택합니다.
   정책이 할당됩니다. NAS 서버 및 파일 시스템 테이블의 **QoS 정책** 열에서 할당된 정책 이름을 볼 수 있습니다. **Storage** > **NAS Servers** > **[NAS server]** > **Performance** or **Storage** > **File Systems** > **[file system]** > **Performance**를 선택하여 할당된 정책이 성능에 미치는 영향을 볼 수 있습니다.

   노트: 관련 NAS 서버 또는 파일 시스템을 선택한 다음 **Modify**를 선택하여 QoS 정책을 설정할 수도 있습니다.

파일 QoS 정책 수정

다른 I/O 제한 규칙을 선택하여 QoS 정책을 수정할 수 있습니다.

NAS 서버 또는 파일 시스템에 할당된 정책은 수정할 수 없습니다.

1. **Storage** > **Quality of Service (QoS)**를 선택합니다.
2. **File QoS Policies** 테이블에서 수정할 QoS 정책 옆의 확인란을 선택합니다.
3. **Modify**를 선택합니다.
4. **Modify QoS Policy** 창에서 정책의 이름과 설명을 수정하고 다른 I/O 제한 규칙을 선택할 수 있습니다.
5. **적용**을 선택합니다.

   노트: 스토리지 리소스 **속성** 화면에서 QoS 정책을 수정할 수도 있습니다.

파일 QoS 정책 삭제

삭제하려는 QoS 정책이 NAS 서버 또는 파일 시스템에 할당되지 않았는지 확인합니다.

1. **Storage** > **Quality of Service (QoS)**를 선택합니다.
2. **File QoS Policies** 테이블에서 삭제할 QoS 정책을 선택합니다.
3. **More Actions** > **Delete**를 선택합니다.
4. **삭제**를 선택하여 확인합니다.

6

NAS 서버 복제

이 장에서 다루는 내용은 다음과 같습니다.

주제:

개요

데이터 손실이 발생할 경우 향상된 이중화 및 복구를 위해 PowerStore에서는 NAS 서버를 로컬 시스템에서 원격 시스템으로 복제할 수 있습니다.

기본적으로 복제는 NAS 서버 수준에서 발생합니다. 복제된 NAS 서버 내의 모든 파일 시스템은 원격 시스템에 복제됩니다. 복제 세션의 일부인 경우 NAS 서버에서 파일 시스템을 추가하거나 파일 시스템을 삭제하도록 선택할 수 있습니다.

정의된 RPO에 따라 시스템이 동기화되는 비동기식 복제를 선택하거나, 변경 사항이 발생하면 소스 시스템에서 대상 시스템으로 즉시 복제되는 동기식 복제를 선택할 수 있습니다.

파일 복제를 활성화하려면 다음과 같은 사전 요구 사항이 필요합니다.

- 파일 원격 시스템
- 파일 이동성 네트워크를 구성하고 매핑해야 합니다(PowerStore 설명서 페이지에서 *스토리지 서비스를 위한 PowerStore T 및 Q 네트워킹 가이드* 참조).
- 복제 규칙을 포함하는 보호 정책

NAS 서버 복제에 대해 다음을 고려하십시오.

- NAS 서버에 대한 별도의 보호 정책을 정의할 필요는 없습니다. 블록 및 파일 복제 모두에 동일한 보호 정책을 적용할 수 있습니다.
- 복제 세션의 소스 시스템에서 파일 시스템을 삭제할 수 있습니다. 삭제 후에는 나머지 파일 시스템만 대상으로 복제됩니다. 파일 시스템 삭제 후 대상 시스템의 상태는 영향을 받지 않습니다. 복제 소스 NAS 서버에서 파일 시스템을 삭제한 다음 대상 시스템으로 페일오버하는 경우 새 소스는 이전 소스에서 삭제된 파일 시스템을 복제하지 않습니다. 이러한 파일 시스템을 복제하려면 복제 가능한 클론을 생성하고 파일 시스템을 삭제합니다.
- 복제 세션을 원격 시스템으로 페일오버할 수 있습니다. 페일오버는 페일오버 NAS 서버 내의 모든 파일 시스템에 대해 발생합니다.
- 복제 세션을 생성할 때 소스 시스템에서 할당량이 활성화되어 있더라도 대상 시스템에는 할당량이 표시되지 않습니다.
- 비동기식 복제의 경우 RPO는 NAS 서버 수준에서 구성되며 연결된 모든 파일 시스템에서 동일합니다.
- 동기식 복제의 경우 복제 중인 파일 시스템의 크기를 늘리려면 먼저 복제 세션을 일시 중지해야 합니다. 파일 시스템 크기를 줄이기 위해서는 복제 세션을 일시 중지할 필요가 없습니다.
- 동기식 복제의 경우 동기식 복제 세션이 정의되어 있을 때 복제 시스템 쌍의 네트워크 레이턴시를 5밀리초보다 큰 값으로 변경할 수 없습니다.
- 파일 복제의 경우 동기식 복제와 비동기식 복제 간의 전환이 지원되지 않습니다.

NAS 서버 복제 절차에 대한 자세한 내용은 설명서 페이지의 *데이터 보호 가이드를* PowerStore참조하십시오.

복제 중인 NAS 서버에 대한 재해 복구 테스트

재해 복구 테스트는 재해가 발생할 경우 시스템이 데이터와 작업을 복구하고 복원할 수 있는지 확인하기 위한 재해 복구 계획을 수행합니다.

PowerStore는 재해로부터 복구하고 기능을 회복하는 시스템의 기능을 테스트하는 몇 가지 옵션을 제공합니다.

- 재해 복구 테스트를 위해 고유한 IP 주소를 사용하여 NAS 서버의 클론을 생성합니다.
- 재해 복구 테스트를 위해 중복 IP 주소로 격리된 네트워크를 사용하여 NAS 서버의 클론을 생성합니다.
- 계획된 페일오버를 수행합니다.

재해 복구 테스트를 위해 고유한 IP 주소를 사용하여 NAS 서버의 클론 생성

DR 테스트를 위한 권장 옵션은 NAS 서버의 클론을 생성하는 것입니다. PowerStore Manager를 사용하면 NAS 서버의 클론을 생성하고 운영에 대한 영향 없이 테스트할 수 있습니다. 새로 복제된 NAS 서버에 대한 액세스를 활성화하려면 고유한 새 네트워크 인터페이스를 구성해야 합니다. 구성한 IP 주소는 소스 또는 대상 NAS 서버에서 사용할 수 없습니다. 서버를 AD 도메인에 연결하려면 고유 설정이 필요합니다.

복제된 파일 시스템과 운영 파일 시스템에 수행된 변경 사항은 서로에 영향을 미치지 않습니다. DR 테스트가 완료되면 복제된 서버를 삭제할 수 있습니다.

다음 옵션 중 하나를 선택할 수 있습니다.

- 소스 시스템에 NAS 서버의 클론을 생성하고 대상에 복제한 후 대상 시스템으로 계획된 페일오버를 수행합니다.
- 대상 시스템에 NAS 서버의 클론을 생성하고 데이터에 액세스합니다(복제된 리소스를 대상 시스템에서 이미 액세스할 수 있으므로 페일오버가 필요하지 않음).

1. PowerStore Manager에서 **스토리지** > **NAS 서버**를 선택합니다.
2. 클론을 생성할 NAS 서버를 선택한 다음 **용도 변경** > **NAS 서버 클론 생성**을 선택합니다.
3. **클론 생성** 창에 클론의 이름을 입력하고 클론을 생성할 파일 시스템을 선택합니다.
4. **Create**를 선택합니다.
   복제된 NAS 서버가 서버 목록에 추가됩니다.
5. 복제된 NAS 서버 이름을 선택하여 서버 세부 정보 창을 엽니다.
6. 파일 인터페이스를 추가하려면 다음을 수행합니다.
   a. **네트워크** 탭을 선택합니다.
   b. **파일 인터페이스**에서 **추가**를 선택합니다.
   c. 인터페이스 정보를 제공하고 **추가**를 선택합니다.
7. 공유 프로토콜을 설정하려면 다음을 수행합니다.
   a. **공유 프로토콜** 탭을 선택합니다.
   b. 해당 프로토콜(SMB, NFS 또는 FTP)을 선택합니다.
   c. 필요한 정보를 구성하고 **적용**을 선택합니다.
8. 소스 NAS 서버의 클론을 생성한 경우 다음을 수행합니다.
   a. NAS 서버를 대상 시스템에 복제합니다. 자세한 내용은 NAS 서버 복제를 참조하십시오.
   b. 대상으로 계획된 페일오버를 수행합니다. 자세한 내용은 계획된 페일오버를 참조하십시오.
   c. 호스트가 데이터에 액세스할 수 있는지 확인합니다.
9. 대상 시스템에 복제된 운영 서버의 클론을 생성한 경우 페일오버가 필요 없습니다. 호스트 액세스를 확인합니다.

재해 복구 테스트를 위해 중복 IP 주소로 격리된 네트워크를 사용하여 NAS 서버 클론 생성

운영 환경과 같은 구성으로 재해 복구를 테스트할 수 있습니다. 같은 설정을 사용하면 장애 시나리오의 위험은 줄이고 재현성은 높일 수 있습니다. 그러나 중복 IP 주소를 사용하면 충돌이 발생합니다. 운영 환경과 격리된 환경에서 DR 테스트를 실행하면 이러한 충돌을 방지할 수 있습니다.

OS 3.6 이상에서는 PowerStore재해에 대비하는 데 도움이 되는 격리된 DRT(재해 복구 테스트 환경)를 만들 수 있습니다.

격리된 환경을 생성하면 운영 시스템과 같은 IP 주소와 호스트 이름을 사용하여 운영 환경에 영향을 미치지 않고 복제 중인 NAS 서버에 대해 DRT를 수행할 수 있습니다.

DRT 환경을 생성하려면 별도의 DRT 라우터로 격리된 네트워크를 설정하고 네트워크 I/O 포트로 링크 통합을 생성해야 합니다.

PSTCLI 또는 REST API를 사용하여 대상 PowerStore 시스템의 복제에 NAS 서버의 클론을 생성함으로써 대상 서버에 전용 네트워킹 환경을 생성합니다. 클론은 운영 환경의 전체 복제본이며 운영 환경과 격리된 전용 테스트 환경입니다. 격리된 네트워킹 환경을 생성하고 운영 시스템과 같은 IP 주소와 호스트 이름으로 테스트 환경을 구성할 수 있습니다. DRT NAS 서버는 운영 환경에 영향을 미치지 않으며 복제 NAS 서버에서 페일오버 및 페일백이 발생할 때 IP 주소 충돌 없이 실행할 수 있습니다.

격리된 테스트 환경을 사용하여 DR을 테스트하려면 다음을 수행합니다.

1. 대상에 NAS 서버 클론을 생성합니다. `is_dr_test` 플래그를 사용합니다.
2. 소스 NAS 서버와 같은 IP 주소를 사용하여 NAS를 위한 사용자 본드 인터페이스를 생성합니다.
3. 클론을 AD에 연결합니다(필요한 경우).

4. 호스트가 데이터에 액세스할 수 있는지 확인합니다.

노트: 독립 실행형 NAS 서버에서도 DRT를 사용할 수 있습니다.

사전 요구 사항 및 제한 사항

DRT 환경을 생성하려면 다음 요구 사항이 충족되는지 확인하십시오.

- 개인 네트워크 정보를 획득합니다.
  - 게이트웨이
  - 넷마스크
  - VLAN ID(선택 사항)
- 격리된 네트워크의 네트워크 포트와 운영 네트워크의 네트워크 포트를 식별합니다.

DRT 환경을 생성할 때는 다음과 같은 제한 사항에 유의하십시오.

- DRT 전용 본드 인터페이스는 다른 운영 NAS 서버를 생성하는 데 사용할 수 없습니다.
- 운영 환경으로 구성된 NAS 서버는 DRT의 일부로 재구성할 수 없습니다.
- DRT의 일부로 구성된 NAS 서버는 운영 서버로 재구성할 수 없습니다.
- 더는 DRT의 일부가 아닌 NAS 서버는 재구성할 수 없으며 삭제해야 합니다.
- NAS 서버가 활성 상태이고 네트워크 정보로 구성된 후에는 추가 구성(예: DNS, CAVA 및 Kerberos)을 수동으로 수행해야 합니다.
- DRT가 활성화된 NAS 서버는 복제할 수 없습니다.
- PowerStore Manager를 사용하여 NAS 서버를 수정하고 삭제할 수 있습니다.

PSTCLI를 사용하여 재해 복구 테스트 환경 구성

1. 클론을 생성할 대상 사이트의 NAS 서버 이름을 가져옵니다.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+------------+--------+--------------------+------------------
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. 클론의 새 이름을 제공하고 `-is_dr_test true` 스위치를 사용하여 NAS 서버의 클론을 생성합니다.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. 격리된 네트워크에 연결된 NAS 파일 본드의 IP 포트 ID를 찾습니다.

노트: NAS 파일 본드가 생성되지 않은 경우 PSTCLI 또는 PowerStore Manager를 사용하여 생성할 수 있습니다.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:  id =IP_PORT23
    current_usages =
    ip_pool_addresses =
    bond:
    name=BaseEnclosure-NodeA-bond1
```

4. 복제된 NAS 서버에 대한 파일 인터페이스를 생성합니다.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+------------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. 파일 인터페이스를 봅니다.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+-------------+--------+-------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

REST API를 사용하여 DRT 환경에 NAS 서버 구성

노트: REST API를 사용하지 않는 경우 이 섹션을 건너뜁니다.

1. 지정된 네임스페이스에서 NAS 서버의 클론을 생성하려면 `/nas_server/{id}/clone`을 실행하고 `is_dr_test`를 true로 지정합니다.
2. 네트워크 인터페이스를 생성하려면 `/file_interface`를 실행하고 전용 네트워크 매개변수를 지정합니다.

   노트: 이 단계에서는 운영 NAS 서버와 같은 IP 주소, 넷마스크 및 게이트웨이를 사용하여 클론 생성된 NAS 서버에 대한 파일 인터페이스를 만듭니다. 개인 네트워크와 연결된 본드 인터페이스/IP_Port를 사용합니다.

NAS 서버가 작동 중이며 격리된 네트워크에서 DRT에 사용될 수 있습니다.

계획된 페일오버 수행

계획된 페일오버를 사용하여 재해 복구를 테스트할 수 있습니다. 계획된 페일오버를 수행하는 경우 NAS 서버 복제 세션은 소스 시스템에서 대상 시스템으로 수동으로 페일오버됩니다. 페일오버를 수행하기 전에 대상 시스템이 소스 시스템과 동기화되므로 데이터 손실은 발생하지 않습니다.

노트: 운영 NAS 서버를 대상 시스템으로 페일오버하면 운영 환경에 영향을 미칠 수 있습니다.

계획된 페일오버를 수행하기 전에 모든 애플리케이션과 호스트의 I/O 작업을 중지해야 합니다. 계획된 페일오버 중인 복제 세션은 일시 중지할 수 없습니다.

정상적으로 작동되는 경우 DR 테스트 중 NAS 서버 및 파일 시스템에 대한 변경 사항은 보존되고 (수동 또는 자동으로) 다시 보호가 시작되면 원래 소스로 다시 복제됩니다. 그러나 DR 테스트 중에 변경한 사항(데이터 또는 구성)을 저장하지 않으려면 REST API 또는 PSTCLI 명령을 사용하여 변경 사항을 취소하도록 선택할 수 있습니다.

- REST API - `POST /replication_session/{id}/reprotect discard_changes_after_failover`
- PSTCLI - `replication_session -id <value> reprotect [-discard_changes_after_failover]`

취소되는 변경 사항:

- NAS 서버:
  - 구성 변경
- 파일 시스템:
  - 구성 변경
  - 파일 시스템 데이터 변경
  - 스냅샷 리소스
  - 파일 시스템 크기 변경
  - 할당량 변경
- 내보내기 및 공유:
  - NFS 내보내기 변경
  - SMB 공유 변경

노트: 이 옵션은 비동기식 복제에만 지원됩니다.

페일오버 후 REST API 및 CLI를 사용하여 변경 사항을 취소하는 자세한 방법은 dell.com/powerstoredocs에서 *Dell PowerStore REST API 참조 가이드* 및 *Dell PowerStore CLI 참조 가이드*를 참조하십시오.

NAS 서버가 다시 보호된 후, 계획된 페일오버를 다시 시작하여 원래 소스 시스템의 리소스를 온라인으로 전환할 수 있습니다.

노트: 재해 복구 목적으로 계획되지 않은 페일오버를 수행하지 마십시오. 계획되지 않은 페일오버는 소스 시스템에 액세스할 수 없는 경우에만 사용해야 합니다.

노트: SMB 환경에서 데이터에 대한 무중단 액세스를 지원하려면 SMB 공유에 대한 무중단 가용성을 구성하고 연결을 재설정한 후 공유를 다시 마운트하는 것이 좋습니다.

계획된 페일오버를 시작하는 방법에는 두 가지가 있습니다.

- **Protection** > **Replication**에서 관련 복제 세션을 선택한 후 **Planned Failover**를 선택합니다.
- 리소스의 **Protection** 탭에서 **Replication**을 선택한 후 **Planned Failover**를 선택합니다.

계획된 페일오버 후에는 복제 세션이 비활성 상태가 됩니다. 대상 스토리지 리소스를 동기화하고 복제 세션을 재개하려면 **재보호** 작업을 사용합니다. 또한 페일오버 전에 자동 재보호 옵션을 선택할 수 있습니다. 이 옵션은 페일오버가 완료된 후 반대 방향(다음 RPO에서)으로 동기화를 자동으로 시작하고 소스 및 타겟 시스템을 정상 상태로 되돌립니다.

노트: 페일오버 후에는 새 소스가 된 대상 시스템에 사용자 할당량이 표시되지 않습니다. 사용자 할당량을 보려면 **스토리지** > **파일 시스템**을 선택하고 관련 파일 시스템 옆의 확인란을 선택한 다음 **추가 작업** > **할당량 새로 고침**을 선택하여 할당량을 수동으로 새로 고칩니다.

DRT 중 네트워크 연결 해제

DRT를 수행할 때 로컬 시스템과 원격 시스템 간의 네트워크 장애를 시뮬레이션한 다음, 대상 시스템으로 계획되지 않은 페일오버를 수행하여 DR NAS 서버에 대한 액세스를 활성화하는 것은 권장되지 않습니다. 시스템 PowerStore 간에 통신이 없으므로 에서 두 NAS 서버가 호환되는 상태인지 확인할 수 없습니다. 연결이 복원된 후 두 NAS 서버가 모두 운영 모드(스플릿 브레인)가 됩니다. 따라서 데이터가 두 위치에 기록되지 않도록 두 시스템이 모두 대상 모드로 전환됩니다.

이 상태를 해결하려면 기술 지원 부서의 개입이 필요합니다.

자세한 내용은 Dell Knowledge 기술 자료 문서 000215482(사이트 간 네트워크 연결 끊기)를 참조하십시오.

7

PowerStore에 CEPA 사용

이 장에서 다루는 내용은 다음과 같습니다.

주제:

이벤트 게시

CEE를 사용하면 타사 애플리케이션이 파일 시스템에 액세스할 때 스토리지 시스템에서 이벤트 정보를 수신할 수 있습니다.

CEE(Common Event Enabler)는 타사 애플리케이션이 파일 시스템에 액세스할 때 스토리지 시스템에서 이벤트 알림 및 컨텍스트를 등록하고 수신할 수 있도록 PowerStore 클라이언트를 위한 이벤트 게시 솔루션을 제공합니다. 이벤트 알림을 수신하면 랜섬웨어 또는 무단 액세스와 같은 보안 위협을 방지하기 위해 스토리지에서 이벤트 중심의 작업을 수행할 수 있습니다.

CEE CEPA(Common Events Publishing Agent)는 SMB 및 NFS 파일 및 디렉토리 이벤트 알림을 처리하도록 설계된 애플리케이션으로 구성됩니다. CEPA는 하나의 메시지로 애플리케이션에 이벤트 알림 및 관련 컨텍스트를 모두 제공합니다. 컨텍스트는 비즈니스 정책을 결정하는 데 필요한 파일 메타데이터 또는 디렉토리 메타데이터로 구성될 수 있습니다.

CEE CEPA 지원을 활성화하려면 CEE CEPA를 활성화하고 NAS 서버에 이벤트 게시 풀을 생성해야 합니다.

이벤트 게시 풀은 CEPA 서버와 알림을 트리거하는 특정 이벤트를 정의합니다.

NAS 서버를 구성한 후 이벤트를 수신하려는 파일 시스템에서 이벤트 게시를 활성화할 수 있습니다. 호스트가 SMB 또는 NFS를 통해 파일 시스템에 대한 이벤트를 생성하는 경우 이 정보는 HTTP 연결을 통해 CEPA 서버로 전달됩니다. 서버의 CEE CEPA 소프트웨어는 이벤트를 수신하여 게시하므로 타사 소프트웨어가 이를 처리할 수 있습니다.

이벤트 게시 에이전트를 사용하려면 하나 이상의 NAS 서버가 네트워크에 구성된 PowerStore 시스템이 있어야 합니다.

CEE(Common Event Enabler)의 일부인 CEPA에 대한 자세한 내용은 Dell Technologies 지원 사이트에서 *Windows 플랫폼에서 Common Event Enabler 사용*을 참조하십시오.

게시 풀 생성

이벤트 게시 풀을 생성하려면 이벤트 게시(CEPA) 서버 FQDN이 있어야 합니다.

이벤트 게시 풀은 CEPA 서버와 알림을 트리거하는 특정 이벤트를 정의합니다. 다음 이벤트 옵션을 하나 이상 정의합니다.

- 사전 이벤트 - 처리하기 전에 승인을 위해 CEPA 서버로 전송되는 이벤트입니다.
- 사후 이벤트 – 이벤트가 발생한 후 로깅 또는 감사를 위해 CEPA 서버로 전송되는 이벤트입니다.
- 사후 오류 이벤트 - 오류 이벤트가 발생한 후 로깅 또는 감사를 위해 CEPA 서버로 전송되는 오류 이벤트입니다.

1. **Storage** > **NAS Servers**를 선택합니다.
2. **NAS Settings**를 선택합니다.
3. **Event Publishing** 창에서 **Publishing Pools**를 선택한 다음 **Create**를 선택합니다.
4. **Pool Name**을 입력합니다.
5. CEPA Server FQDN을 입력합니다.
6. 이벤트 구성 섹션에서 이벤트 유형을 클릭하고 풀에 추가할 이벤트를 선택합니다.
7. **Apply**를 클릭하여 이벤트 게시 풀을 생성합니다.

이벤트 게시자 생성

게시 풀을 구성한 후 이벤트 게시자를 생성하여 다양한 이벤트 유형에 대한 응답을 설정합니다.

노트: 이벤트 게시자는 시스템 수준에서 생성되며 하나의 이벤트 게시자를 여러 NAS 서버에 연결할 수 있습니다.

1. **Storage** > **NAS Servers**를 선택합니다.
2. **NAS Settings**를 선택합니다.
3. **Event Publishers**를 선택한 다음 **Create**를 선택합니다.
4. **Create Event Publisher** 마법사를 계속 진행합니다.

마법사 화면	설명
게시 풀 선택	• 이름을 입력합니다. • 최대 3개의 게시 풀을 선택합니다. 새 게시 풀을 생성하려면 **Create**를 클릭합니다.
이벤트 게시자 구성	• 사전 이벤트 실패 정책 - 사전 이벤트에 대해 모든 CEPA 서버가 오프라인 상태일 때 원하는 동작을 선택합니다. ○ 무시(기본값) - 모든 이벤트가 확인된다고 가정합니다. ○ 거부 - CEPA 서버가 온라인 상태가 될 때까지 승인이 필요한 이벤트를 거부합니다. • 사후 이벤트 실패 정책 - 사후 이벤트에 대해 모든 CEPA 서버가 오프라인 상태일 때 원하는 동작을 선택합니다. ○ 무시(기본값) - 계속 작업합니다. CEPA 서버가 다운되었을 때 발생한 이벤트는 손실됩니다. ○ 누적 - 계속 작업하여 이벤트를 로컬 버퍼(최대 500MB)에 저장합니다. ○ 보장 - 계속 작업하여 이벤트를 로컬 버퍼(최대 500MB)에 저장합니다. 버퍼가 가득 찼을 때 액세스를 거부합니다. ○ 거부 - CEPA 서버가 오프라인 상태일 때 파일 시스템에 대한 액세스를 거부합니다. • HTTP/Microsoft RPC • HTTP 포트

5. **Apply**를 선택하여 이벤트 게시자를 생성합니다.

NAS 서버에 대한 이벤트 게시자 활성화

이벤트 게시자를 구성한 후 NAS 서버와 해당 서버에 정의된 모든 파일 시스템에 대해 활성화합니다.

1. **Storage** > **NAS Servers** > **[nas server]**를 선택합니다.
2. **Security & Events** 페이지에서 **Events Publishing**를 선택합니다.
3. 목록에서 이벤트 게시자를 선택하고 활성화합니다.
4. NAS 서버에 정의된 모든 파일 시스템에 대해 이벤트 게시자를 활성화할지 여부를 선택합니다.
   또는 특정 파일 시스템에 대해 이벤트 게시자를 활성화하도록 선택할 수 있습니다. 자세한 내용은 파일 시스템에 대한 이벤트 게시자 활성화를 참조하십시오.
5. **Apply**를 클릭합니다.

파일 시스템에 대한 이벤트 게시자 활성화

선택한 파일 시스템에 대해 이벤트 게시자를 활성화할 수 있습니다.

1. **Storage** > **File Systems** > **[file system]**을 선택합니다.
2. **Protection** 페이지에서 **Events Publishing**을 선택합니다.
3. 파일 시스템에 대해 이벤트 게시자를 활성화하고 프로토콜을 선택합니다.
4. **Apply**를 클릭합니다.