iSCSI 설정

E-Series storage systems

NetApp
January 20, 2026

목차

iSCSI 설정

E-Series(iSCSI)에서 Linux 구성 지원 확인

안정적인 운영을 보장하기 위해 구축 계획을 생성한 다음 NetApp 상호 운용성 매트릭스 툴(IMT)을 사용하여 전체 구성이 지원되는지 확인하십시오.

단계

1. 로 이동합니다 "NetApp 상호 운용성 매트릭스 툴".
2. 솔루션 검색 * 타일을 클릭합니다.
3. 메뉴: 프로토콜 [SAN 호스트] 영역에서 * E-Series SAN 호스트 * 옆에 있는 * 추가 * 버튼을 클릭합니다.
4. 검색 조건 구체화 보기 * 를 클릭합니다.

   검색 조건 구체화 섹션이 표시됩니다. 이 섹션에서는 적용되는 프로토콜과 운영 체제, NetApp OS 및 호스트 다중 경로 드라이버와 같은 구성의 다른 기준을 선택할 수 있습니다.

5. 구성에 대해 알고 있는 기준을 선택한 다음 어떤 호환 구성 요소가 적용되는지 확인합니다.
6. 필요한 경우 도구에 규정된 운영 체제 및 프로토콜을 업데이트합니다.

   선택한 구성에 대한 자세한 내용은 오른쪽 페이지 화살표를 클릭하여 지원되는 구성 보기 페이지에서 액세스할 수 있습니다.

E-Series-Linux(iSCSI)에서 DHCP를 사용하여 IP 주소 구성

관리 스테이션과 스토리지 어레이 간의 통신을 구성하려면 DHCP(Dynamic Host Configuration Protocol)를 사용하여 IP 주소를 제공합니다.

시작하기 전에

다음 사항을 확인하십시오.

- 스토리지 관리 포트와 동일한 서브넷에 설치 및 구성된 DHCP 서버입니다.

이 작업에 대해

각 스토리지 어레이에는 1개의 컨트롤러(단일) 또는 2개의 컨트롤러(이중)가 있으며, 각 컨트롤러에는 2개의 스토리지 관리 포트가 있습니다. 각 관리 포트에는 IP 주소가 할당됩니다.

다음 지침은 두 개의 컨트롤러가 있는 스토리지 배열(이중 구성)을 나타냅니다.

단계

1. 아직 연결하지 않은 경우 이더넷 케이블을 관리 스테이션과 각 컨트롤러(A 및 B)의 관리 포트 1에 연결하십시오.

   DHCP 서버는 각 컨트롤러의 포트 1에 IP 주소를 할당합니다.

   > 두 컨트롤러 중 하나에서 관리 포트 2를 사용하지 마십시오. 포트 2는 NetApp 기술 담당자가 사용하도록 예약되어 있습니다.

이더넷 케이블을 분리했다가 다시 연결하거나 스토리지 배열의 전원을 껐다가 켜면 DHCP는 IP 주소를 다시 할당합니다. 이 프로세스는 고정 IP 주소가 구성될 때까지 수행됩니다. 케이블을 분리하거나 배열의 전원을 껐다가 켜는 것을 피하는 것이 좋습니다.

스토리지 배열이 30초 이내에 DHCP 할당 IP 주소를 가져올 수 없는 경우, 다음의 기본 IP 주소가 설정됩니다:

- 컨트롤러 A, 포트 1: 169.254.128.101
- 컨트롤러 B, 포트 1: 169.254.128.102
- 서브넷 마스크: 255.255.0.0

2. 각 컨트롤러 뒷면에서 MAC 주소 레이블을 찾은 다음 네트워크 관리자에게 각 컨트롤러의 포트 1에 대한 MAC 주소를 제공합니다.

   네트워크 관리자는 각 컨트롤러의 IP 주소를 확인하기 위해 MAC 주소가 필요합니다. 브라우저를 통해 스토리지 시스템에 연결하려면 IP 주소가 필요합니다.

SMcli용 SANtricity Storage Manager 설치(11.53 이하) - Linux(iSCSI)

SANtricity 소프트웨어 11.53 이하를 사용하는 경우, 관리 스테이션에 SANtricity 스토리지 관리자 소프트웨어를 설치하여 어레이를 관리할 수 있습니다.

SANtricity 스토리지 관리자는 추가 관리 작업을 위한 CLI(Command Line Interface)와 I/O 경로를 통해 호스트 구성 정보를 스토리지 어레이 컨트롤러로 푸시하는 Host Context Agent를 포함합니다.

SANtricity 소프트웨어 11.60 이상을 사용하는 경우 다음 단계를 수행할 필요가 없습니다. SANtricity 보안 CLI(SMcli)는 SANtricity OS에 포함되어 있으며 SANtricity 시스템 관리자를 통해 다운로드할 수 있습니다. SANtricity System Manager를 통해 SMcli를 다운로드하는 방법에 대한 자세한 내용은 를 참조하십시오 "SANtricity System Manager 온라인 도움말에서 CLI(Command Line Interface) 항목을 다운로드하십시오"

SANtricity 소프트웨어 버전 11.80.1부터 호스트 컨텍스트 에이전트는 더 이상 지원되지 않습니다.

시작하기 전에

다음 사항을 확인하십시오.

- SANtricity 소프트웨어 11.53 이전 버전.
- 관리자 또는 고급 사용자 권한을 수정합니다.
- 다음과 같은 최소 요구 사항이 있는 SANtricity Storage Manager 클라이언트용 시스템:
  - RAM *: Java Runtime Engine용 2GB
  - * 디스크 공간 *: 5GB
  - * OS/아키텍처 *: 지원되는 운영 체제 버전 및 아키텍처를 결정하는 지침은 을 참조하십시오 "NetApp 지원". 다운로드 * 탭에서 다운로드 [E-Series SANtricity 스토리지 관리자] 메뉴로 이동합니다.

이 작업에 대해

이 작업에서는 데이터 호스트에 Linux를 사용할 때 Windows와 Linux가 모두 공통 관리 스테이션 플랫폼이기 때문에 Windows 및 Linux OS 플랫폼 모두에 SANtricity 스토리지 관리자를 설치하는 방법을 설명합니다.

단계

1. 에서 SANtricity 소프트웨어 릴리스를 다운로드합니다 "NetApp 지원". 다운로드 * 탭에서 다운로드 [E-Series SANtricity 스토리지 관리자] 메뉴로 이동합니다.
2. SANtricity 설치 프로그램을 실행합니다.

Windows	리눅스
SMIA*.exe 설치 패키지를 두 번 클릭하여 설치를 시작합니다.	a. SMIA*.BIN 설치 패키지가 있는 디렉터리로 이동합니다. b. temp 마운트 지점에 실행 권한이 없는 경우 'IATEMPDIR' 변수를 설정합니다. 예: "IATEMPDIR=/root./SMIA-LINUXX64-11.25.0A00.0002.BIN" c. 파일에 대한 실행 권한을 부여하려면 "chmod + x SMIA *.bin" 명령을 실행합니다. d. './SMIA *.BIN' 명령어를 실행하여 설치 프로그램을 시작한다.

3. 설치 마법사를 사용하여 관리 스테이션에 소프트웨어를 설치합니다.

SANtricity System Manager를 사용하여 스토리지 구성 - Linux(iSCSI)

스토리지 배열을 구성하려면 SANtricity System Manager에서 설치 마법사를 사용할 수 있습니다.

SANtricity 시스템 관리자는 각 컨트롤러에 내장된 웹 기반 인터페이스입니다. 사용자 인터페이스에 액세스하려면 브라우저에서 컨트롤러의 IP 주소를 가리킵니다. 설치 마법사를 사용하면 시스템 구성을 시작할 수 있습니다.

시작하기 전에

다음 사항을 확인하십시오.

- 대역 외 관리.
- 다음 브라우저 중 하나가 포함된 SANtricity System Manager에 액세스하기 위한 관리 스테이션입니다.

브라우저	최소 버전
Google Chrome	89
Microsoft Edge를 참조하십시오	90
Mozilla Firefox	80

브라우저	최소 버전
사파리	14

이 작업에 대해

iSCSI 사용자인 경우 iSCSI를 구성하는 동안 설정 마법사를 닫았습니다.

System Manager를 열거나 브라우저를 새로 고치면 마법사가 자동으로 다시 시작되고, 다음 중 _ 개 이상의 조건이 충족됩니다.

- 풀 및 볼륨 그룹이 감지되지 않습니다.
- 감지된 워크로드가 없습니다.
- 알림이 구성되지 않았습니다.

단계

1. 브라우저에서 'https://<DomainNameOrIPAddress>` URL을 입력합니다

   IPAddress는 스토리지 배열 컨트롤러 중 하나의 주소입니다.

   구성되지 않은 어레이에서 SANtricity 시스템 관리자를 처음 열면 관리자 암호 설정 프롬프트가 나타납니다. 역할 기반 액세스 관리는 관리자, 지원, 보안 및 모니터링의 네 가지 로컬 역할을 구성합니다. 마지막 세 개의 역할에는 추측할 수 없는 임의의 암호가 있습니다. admin 역할의 암호를 설정한 후 admin 자격 증명을 사용하여 모든 암호를 변경할 수 있습니다. 4개의 로컬 사용자 역할에 대한 자세한 내용은 SANtricity System Manager 사용자 인터페이스에서 제공되는 온라인 도움말을 참조하십시오.

2. 관리자 암호 설정 및 암호 확인 필드에 관리자 역할에 대한 System Manager 암호를 입력한 다음 * 암호 설정 * 을 클릭합니다.

   구성된 풀, 볼륨 그룹, 워크로드 또는 알림이 없는 경우 설정 마법사가 시작됩니다.

3. 설정 마법사를 사용하여 다음 작업을 수행합니다.
   - * 하드웨어(컨트롤러 및 드라이브) 확인 * — 스토리지 배열의 컨트롤러 및 드라이브 수를 확인합니다. 어레이에 이름을 할당합니다.
   - * 호스트 및 운영 체제 확인 * — 스토리지 배열이 액세스할 수 있는 호스트 및 운영 체제 유형을 확인합니다.
   - * 풀 수락 * — 빠른 설치 방법에 대해 권장되는 풀 구성을 수락합니다. 풀은 드라이브의 논리적 그룹입니다.
   - * 경고 구성 * — 스토리지 배열에 문제가 발생하면 System Manager가 자동 알림을 수신할 수 있도록 합니다.
   - * AutoSupport 활성화 * — 스토리지 어레이의 상태를 자동으로 모니터링하고 기술 지원 부서에 디스패치를 보냅니다.
4. 볼륨을 아직 생성하지 않은 경우 Storage [Volumes > Create > Volume] 메뉴로 이동하여 생성합니다.

   자세한 내용은 SANtricity 시스템 관리자의 온라인 도움말을 참조하십시오.

E-Series-Linux(iSCSI)에서 다중 경로 소프트웨어 구성

스토리지 배열에 대한 중복 경로를 제공하기 위해 다중 경로 소프트웨어를 구성할 수 있습니다.

시작하기 전에

시스템에 필요한 패키지를 설치해야 합니다.

- RHEL(Red Hat) 호스트의 경우 "rpm -q device-mapper-multipath"를 실행하여 패키지가 설치되어 있는지 확인합니다.
- SLES 호스트의 경우 'rpm-q multipath-tools'를 실행하여 패키지가 설치되어 있는지 확인합니다.

운영 체제를 아직 설치하지 않은 경우 운영 체제 공급업체에서 제공한 매체를 사용하십시오.

이 작업에 대해

물리적 경로 중 하나가 중단되는 경우 다중 경로 소프트웨어가 스토리지 배열에 대한 중복 경로를 제공합니다. 다중 경로 소프트웨어는 스토리지에 대한 활성 물리적 경로를 나타내는 단일 가상 장치를 운영 체제에 제공합니다. 또한 다중 경로 소프트웨어는 가상 장치를 업데이트하는 페일오버 프로세스를 관리합니다.

Linux 설치에 DM-MP(Device Mapper MultiPath) 툴을 사용합니다. 기본적으로 DM-MP는 RHEL 및 SLES에서 비활성화됩니다. 호스트에서 DM-MP 구성 요소를 활성화하려면 다음 단계를 수행하십시오.

단계

1. multipath.conf 파일이 아직 생성되지 않은 경우 '#touch/etc/multipath.conf' 명령을 실행합니다.
2. multipath.conf 파일을 비워 두고 기본 다중 경로 설정을 사용합니다.
3. 다중 경로 서비스를 시작합니다.

```
# systemctl start multipathd
```

4. uname -r 명령을 실행하여 커널 버전을 저장합니다.

```
# uname -r
3.10.0-327.el7.x86_64
```

   호스트에 볼륨을 할당할 때 이 정보를 사용합니다.

5. 를 활성화합니다 `multipathd` 부팅 시 데몬

```
systemctl enable multipathd
```

6. /boot 디렉토리에서 "initramfs" 이미지 또는 "initrd" 이미지를 재생성합니다.

```
dracut --force --add multipath
```

7. 를 사용합니다 "호스트를 수동으로 생성합니다" 호스트가 정의되어 있는지 여부를 확인하는 온라인 도움말의 절차입니다. 각 호스트 유형 설정이 에서 수집한 커널 정보를 기반으로 하는지 확인합니다 4단계.

   자동 로드 밸런싱은 커널 3.9 이하를 실행하는 호스트에 매핑된 볼륨에 대해 비활성화됩니다.

8. 호스트를 재부팅합니다.

E-Series-Linux(iSCSI)에서 multipath.conf 파일 설정

multipath.conf 파일은 multipath daemon, multipathd의 구성 파일입니다.

multipath.conf 파일은 multipathd에 대한 기본 제공 구성 테이블보다 우선합니다.

SANtricity 운영 체제 8.30 이상의 경우 NetApp은 제공된 기본 설정을 사용할 것을 권장합니다.

/etc/multipath.conf를 변경할 필요가 없습니다.

E-Series-Linux(iSCSI)에서 스위치 구성

iSCSI에 대한 공급업체의 권장 사항에 따라 스위치를 구성합니다. 이러한 권장 사항에는 구성 지시문과 코드 업데이트가 모두 포함될 수 있습니다.

다음 사항을 확인해야 합니다.

- 고가용성을 위해 두 개의 별도 네트워크가 있습니다. iSCSI 트래픽을 분리하여 네트워크 세그먼트를 구분해야 합니다.
- 흐름 제어 * 엔드 투 엔드 * 를 활성화해야 합니다.
- 필요한 경우 점보 프레임을 사용하도록 설정합니다.

컨트롤러의 스위치 포트에서는 포트 채널/LACP가 지원되지 않습니다. 호스트측 LACP는 권장되지 않습니다. 다중 경로가 동일한 이점을 제공하며 경우에 따라 더 나은 이점이 있습니다.

E-Series-Linux(iSCSI)에서 네트워킹 구성

데이터 저장소 요구 사항에 따라 여러 가지 방법으로 iSCSI 네트워크를 설정할 수 있습니다.

사용자 환경에 가장 적합한 구성을 선택하는 방법은 네트워크 관리자에게 문의하십시오.

기본 이중화를 사용하여 iSCSI 네트워크를 구성하려면 각 호스트 포트와 각 컨트롤러의 포트 하나를 별도의 스위치에 연결하고 각 호스트 포트 및 컨트롤러 포트 세트를 별도의 네트워크 세그먼트 또는 VLAN에서 분할하십시오.

하드웨어 흐름 제어 전송 및 수신 * 엔드 투 엔드 * 를 활성화해야 합니다. 우선 순위 흐름 제어를 비활성화해야 합니다.

성능상의 이유로 IP SAN 내에서 점보 프레임을 사용하는 경우, 점보 프레임을 사용하도록 어레이, 스위치 및 호스트를 구성해야 합니다. 호스트와 스위치에서 점보 프레임을 활성화하는 방법에 대한 자세한 내용은 운영 체제 및 스위치 설명서를 참조하십시오. 어레이에서 점보 프레임을 활성화하려면 의 단계를 완료하십시오 "스토리지 측 네트워킹 구성".

IP 오버헤드를 위해 많은 네트워크 스위치를 9,000바이트 이상으로 구성해야 합니다. 자세한 내용은 스위치 설명서를 참조하십시오.

E-Series-Linux(iSCSI)에서 어레이측 네트워킹 구성

SANtricity 시스템 관리자 GUI를 사용하여 어레이 측에서 iSCSI 네트워킹을 구성합니다.

시작하기 전에

다음 사항을 확인하십시오.

- 스토리지 어레이 컨트롤러 중 하나의 IP 주소 또는 도메인 이름입니다.
- 스토리지 어레이에 대한 적절한 보안 액세스를 위해 구성된 System Manager GUI, 즉 역할 기반 액세스 제어(RBAC) 또는 LDAP 및 디렉토리 서비스에 대한 암호입니다. 액세스 관리에 대한 자세한 내용은 SANtricity 시스템 관리자 온라인 도움말을 참조하십시오.

이 작업에 대해

이 작업은 System Manager의 하드웨어 페이지에서 iSCSI 포트 구성에 액세스하는 방법을 설명합니다. 시스템 [설정 > iSCSI 포트 구성] 메뉴에서 구성에 액세스할 수도 있습니다.

단계

1. 브라우저에서 'https://<DomainNameOrIPAddress>` URL을 입력합니다

   IPAddress는 스토리지 배열 컨트롤러 중 하나의 주소입니다.

   구성되지 않은 어레이에서 SANtricity 시스템 관리자를 처음 열면 관리자 암호 설정 프롬프트가 나타납니다. 역할 기반 액세스 관리는 관리자, 지원, 보안 및 모니터링의 네 가지 로컬 역할을 구성합니다. 마지막 세 개의 역할에는 추측할 수 없는 임의의 암호가 있습니다. admin 역할의 암호를 설정한 후 admin 자격 증명을 사용하여 모든 암호를 변경할 수 있습니다. 4개의 로컬 사용자 역할에 대한 자세한 내용은 SANtricity System Manager 사용자 인터페이스에서 제공되는 온라인 도움말을 참조하십시오.

2. 관리자 암호 설정 및 암호 확인 필드에 관리자 역할에 대한 System Manager 암호를 입력한 다음 * 암호 설정 * 을 클릭합니다.

   구성된 풀, 볼륨 그룹, 워크로드 또는 알림이 없는 경우 설정 마법사가 시작됩니다.

3. 설정 마법사를 닫습니다.

   나중에 마법사를 사용하여 추가 설정 작업을 완료합니다.

4. 하드웨어 * 를 선택합니다.
5. 그래픽에 드라이브가 표시되면 * 쉘프 뒷면 표시 * 를 클릭합니다.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

6. 구성할 iSCSI 포트가 있는 컨트롤러를 클릭합니다.

   컨트롤러의 상황에 맞는 메뉴가 나타납니다.

7. iSCSI 포트 구성 * 을 선택합니다.

   iSCSI 포트 구성 대화 상자가 열립니다.

8. 드롭다운 목록에서 구성할 포트를 선택한 후 * 다음 * 을 클릭합니다.

9. 구성 포트 설정을 선택한 후 * 다음 * 을 클릭합니다.

   모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가 포트 설정 표시 * 링크를 클릭합니다.

포트 설정	설명
이더넷 포트 속도를 구성했습니다	원하는 속도를 선택합니다. 드롭다운 목록에 표시되는 옵션은 네트워크에서 지원할 수 있는 최대 속도(예: 10Gbps)에 따라 달라집니다. 컨트롤러에서 옵션으로 제공되는 25GB iSCSI 호스트 인터페이스 카드는 속도를 자동 협상하지 않습니다. 각 포트의 속도를 10Gb 또는 25Gb로 설정해야 합니다. 모든 포트는 동일한 속도로 설정되어야 합니다.
IPv4 사용/IPv6 사용	IPv4 및 IPv6 네트워크에 대한 지원을 활성화하려면 하나 또는 두 옵션을 모두 선택하십시오.
TCP 수신 대기 포트(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)	필요한 경우 새 포트 번호를 입력합니다. 수신 대기 포트는 컨트롤러가 호스트 iSCSI 초기자의 iSCSI 로그인을 수신 대기하기 위해 사용하는 TCP 포트 번호입니다. 기본 수신 대기 포트는 3260입니다. 3260 또는 49152와 65535 사이의 값을 입력해야 합니다.
MTU 크기(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)	필요한 경우 MTU(Maximum Transmission Unit)에 대한 새 크기를 바이트 단위로 입력합니다. 기본 MTU(Maximum Transmission Unit) 크기는 프레임당 1,500바이트입니다. 1500에서 9000 사이의 값을 입력해야 합니다.
ICMP Ping 응답을 활성화합니다	ICMP(Internet Control Message Protocol)를 활성화하려면 이 옵션을 선택합니다. 네트워크로 연결된 컴퓨터의 운영 체제는 이 프로토콜을 사용하여 메시지를 전송합니다. 이러한 ICMP 메시지는 호스트에 연결할 수 있는지 여부와 해당 호스트와 패킷을 주고 받는 데 걸리는 시간을 결정합니다.

   IPv4 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv4 설정을 선택할 수 있는 대화 상자가 열립니다. IPv6 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv6 설정을 선택할 수 있는 대화 상자가 열립니다. 두 옵션을 모두 선택한 경우 IPv4 설정에 대한 대화 상자가 먼저 열리고 * 다음 * 을 클릭하면 IPv6 설정에 대한 대화 상자가 열립니다.

10. IPv4 및/또는 IPv6 설정을 자동 또는 수동으로 구성합니다. 모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가 설정 표시 * 링크를 클릭합니다.

포트 설정	설명
자동으로 구성을 가져옵니다	구성을 자동으로 가져오려면 이 옵션을 선택합니다.
수동으로 정적 설정을 지정합니다	이 옵션을 선택한 다음 필드에 정적 주소를 입력합니다. IPv4의 경우 네트워크 서브넷 마스크 및 게이트웨이를 포함합니다. IPv6의 경우 라우팅 가능한 IP 주소와 라우터 IP 주소를 포함합니다.

11. 마침 * 을 클릭합니다.
12. System Manager를 닫습니다.

E-Series-Linux(iSCSI)에서 호스트측 네트워킹 구성

호스트측 네트워킹을 구성하려면 몇 가지 단계를 수행해야 합니다.

이 작업에 대해

물리적 경로당 노드 세션 수 설정, 해당 iSCSI 서비스 설정, iSCSI 포트에 대한 네트워크 구성, iSCSI 얼굴 바인딩 생성 및 이니시에이터와 타겟 간의 iSCSI 세션 설정을 통해 호스트 측에서 iSCSI 네트워킹을 구성합니다.

대부분의 경우 받은 편지함 소프트웨어 - iSCSI CNA/NIC용 이니시에이터를 사용할 수 있습니다. 최신 드라이버, 펌웨어 및 BIOS는 다운로드할 필요가 없습니다. 을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴" 코드 요구 사항을 결정합니다.

단계

1. /etc/iscsi/iscsid.conf 파일에서 ' node.session.nr_sessions` 변수를 확인하여 물리적 경로당 기본 세션 수를 확인합니다. 필요한 경우 기본 세션 수를 하나의 세션으로 변경합니다.

```
node.session.nr_sessions = 1
```

2. /etc/iscsi/iscsid.conf 파일의 node.session.timeo.replacement_timeout` 변수를 기본값인 120에서 20으로 변경합니다.

```
node.session.timeo.replacement_timeout = 20
```

3. 선택적으로 을 설정할 수 있습니다 `node.startup = automatic` 를 실행하기 전에 /etc/iscsi/iscsid.conf에서 `iscsiadm` 재부팅 후 세션이 유지되는 명령입니다.
4. "iscsid" 및 "open-) iSCSI" 서비스가 부팅 및 활성화되어 있는지 확인합니다.

```
# systemctl start iscsi
# systemctl start iscsid
# systemctl enable iscsi
# systemctl enable iscsid
```

5. 호스트 IQN 이니시에이터 이름을 가져옵니다. 이 이니시에이터 이름은 호스트를 스토리지에 구성하는 데 사용됩니다.

```
# cat /etc/iscsi/initiatorname.iscsi
```

6. iSCSI 포트에 대한 네트워크를 구성합니다. 다음은 RHEL 및 SLES에 대한 지침 예입니다.

공용 네트워크 포트 외에도 iSCSI 이니시에이터는 별도의 개인 세그먼트 또는 VLAN에 둘 이상의 NIC를 사용해야 합니다.

a. ifconfig -a 명령을 사용하여 iSCSI 포트 이름을 확인합니다.

b. iSCSI 이니시에이터 포트의 IP 주소를 설정합니다. 이니시에이터 포트는 iSCSI 타겟 포트와 동일한 서브넷에 있어야 합니다.

레드햇 엔터프라이즈 리눅스 **8(RHEL 8)**

예제 파일을 만듭니다 `/etc/sysconfig/network-scripts/ifcfg-<NIC port>` 다음 내용을 참조하십시오.

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=<NIC port>
UUID=<unique UUID>
DEVICE=<NIC port>
ONBOOT=yes
IPADDR=192.168.xxx.xxx
PREFIX=24
NETMASK=255.255.255.0
NM_CONTROLLED=no
MTU=
```

IPv6과 관련한 선택적 추가 사항:

```
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=fdxx::192:168:xxxx:xxxx/32
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=eui64
```

레드햇 엔터프라이즈 리눅스 **9** 및 **10(RHEL 9** 및 **RHEL 10)** 및 **SUSE** 리눅스 엔터프라이즈 서버 **16(SLES 16)**

를 사용합니다 `nmtui` 도구를 사용하여 연결을 활성화하고 편집합니다. 도구가 을 생성합니다 `<NIC port>.nmconnection` 파일 내 `/etc/NetworkManager/system-connections/`.

- SUSE Linux Enterprise Server 12 및 15(SLES 12 및 SLES 15) *

  예제 파일을 만듭니다 `/etc/sysconfig/network/ifcfg-<NIC port>` 다음 내용을 참조하십시오.

```
IPADDR='192.168.xxx.xxx/24'
BOOTPROTO='static'
STARTMODE='auto'
```

+ IPv6에 대한 추가 옵션:

```
IPADDR_0='fdxx::192:168:xxxx:xxxx/32'
```

+

ⓘ 두 iSCSI 이니시에이터 포트의 주소를 설정해야 합니다.

a. 네트워크 서비스를 다시 시작합니다.

```
# systemctl restart network
```

b. Linux 서버가 iSCSI 대상 포트의 ping_all_을 수행할 수 있는지 확인합니다.

7. 두 가지 방법 중 하나를 사용하여 이니시에이터와 타겟 사이의 iSCSI 세션을 설정합니다(총 4개).

a. (선택 사항) ifaces를 사용하는 경우 iSCSI iface 바인딩 2개를 생성하여 iSCSI 인터페이스를 구성합니다.

```
# iscsiadm -m iface -I iface0 -o new
# iscsiadm -m iface -I iface0 -o update -n iface.net_ifacename -v
<NIC port1>
```

```
# iscsiadm -m iface -I iface1 -o new
# iscsiadm -m iface -I iface1 -o update -n iface.net_ifacename -v
<NIC port2>
```

ⓘ 인터페이스를 나열하려면 iscsiadm -m iface를 사용합니다.

b. iSCSI 대상을 검색합니다. 다음 단계를 위해 워크시트에 IQN(각 검색과 동일함)을 저장합니다.

- 방법 1(ifaces 사용) *

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port> -I iface0
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260 -I
iface0
```

- 방법 2(ifaces 없음) *

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port>
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260
```

ⓘ IQN은 다음과 같습니다.

```
iqn.1992-01.com.netapp:2365.60080e50001bf1600000000531d7be3
```

c. iSCSI 이니시에이터와 iSCSI 타겟 간의 접속을 생성합니다.

- 방법 1(ifaces 사용) *

```
# iscsiadm -m node -T <target_iqn> -p
<target_ip_address>:<target_tcp_listening_port> -I iface0 -l
# iscsiadm -m node -T iqn.1992-
01.com.netapp:2365.60080e50001bf1600000000531d7be3 -p
192.168.0.1:3260 -I iface0 -l
```

+

- 방법 2(ifaces 없음) *

```
# iscsiadm -m node -L all
```

a. 호스트에 설정된 iSCSI 세션을 나열합니다.

```
# iscsiadm -m session
```

E-Series-Linux(iSCSI)에서 IP 네트워크 연결 확인

ping 테스트를 사용하여 호스트와 어레이가 통신할 수 있는지 확인하여 IP(인터넷 프로토콜)

네트워크 연결을 확인합니다.

단계

1. 호스트에서 점보 프레임이 활성화되었는지 여부에 따라 다음 명령 중 하나를 실행합니다.

   ◦ 점보 프레임이 활성화되어 있지 않으면 다음 명령을 실행합니다.

   ```
   ping -I <hostIP\> <targetIP\>
   ```

   ◦ 점보 프레임이 활성화된 경우 페이로드 크기가 8,972바이트인 ping 명령을 실행합니다. IP 및 ICMP 결합된 헤더는 28바이트로, 페이로드에 추가되면 9,000바이트입니다. s 스위치는 패킷 크기 비트를 설정합니다. d 스위치는 디버그 옵션을 설정합니다. 이러한 옵션을 사용하면 9,000바이트의 점보 프레임을 iSCSI 이니시에이터와 타겟 간에 성공적으로 전송할 수 있습니다.

   ```
   ping -I <hostIP\> -s 8972 -d <targetIP\>
   ```

   이 예에서 iSCSI 대상 IP 주소는 192.0.2.8 입니다.

```
#ping -I 192.0.2.100 -s 8972 -d 192.0.2.8
Pinging 192.0.2.8 with 8972 bytes of data:
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Ping statistics for 192.0.2.8:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. 각 호스트의 이니시에이터 주소(iSCSI에 사용되는 호스트 이더넷 포트의 IP 주소)에서 각 컨트롤러의 iSCSI 포트로 'ping' 명령을 실행합니다. 구성에 있는 각 호스트 서버에서 이 작업을 수행하고 필요에 따라 IP 주소를 변경합니다.

   명령이 실패한 경우(예: 패킷이 조각화되어야 하지만 DF 집합을 반환함) 호스트 서버, 스토리지 컨트롤러 및 스위치 포트의 이더넷 인터페이스에 대한 MTU 크기(점보 프레임 지원)를 확인합니다.

E-Series-Linux(iSCSI)에서 파티션 및 파일 시스템 생성

Linux 호스트가 처음 LUN을 검색할 때 새 LUN에 파티션이나 파일 시스템이 없으므로 LUN을 사용하려면 먼저 LUN을 포맷해야 합니다. 선택적으로 LUN에 파일 시스템을 생성할 수 있습니다.

시작하기 전에

다음 사항을 확인하십시오.

- 호스트에서 검색된 LUN입니다.
- 사용 가능한 디스크 목록입니다. 사용 가능한 디스크를 보려면 /dev/mapper 폴더에서 "ls" 명령을 실행합니다.

이 작업에 대해

GPT(GUID Partition Table) 또는 MBR(Master Boot Record)을 사용하여 디스크를 기본 디스크로 초기화할 수 있습니다.

ext4 같은 파일 시스템으로 LUN을 포맷합니다. 일부 응용 프로그램에는 이 단계가 필요하지 않습니다.

단계

1. 'sanlun lun show -p' 명령을 실행하여 매핑된 디스크의 SCSI ID를 검색합니다.

   SCSI ID는 3부터 시작하는 33자의 16진수 문자열입니다. 사용자 친화적인 이름이 활성화되면 장치 매퍼(Device Mapper)는 SCSI ID가 아닌 mpath로 디스크를 보고합니다.

```
# sanlun lun show -p

                E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
                   Volume Name:
               Preferred Owner: Controller in Slot B
                 Current Owner: Controller in Slot B
                          Mode: RDAC (Active/Active)
                      UTM LUN: None
                          LUN: 116
                     LUN Size:
                      Product: E-Series
                   Host Device:
mpathr(360080e50004300ac000007575568851d)
              Multipath Policy: round-robin 0
            Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      controller                      controller
path      path       /dev/   host         target
state     type       node    adapter      port
--------- ---------- ------- ------------
----------------------------------------------
up        secondary  sdcx    host14       A1
up        secondary  sdat    host10       A2
up        secondary  sdbv    host13       B1
```

2. Linux OS 릴리스에 적합한 방법에 따라 새 파티션을 만듭니다.

   일반적으로 디스크 파티션을 식별하는 문자는 SCSI ID(예: 숫자 1 또는 P3)에 추가됩니다.

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. 파티션에 파일 시스템을 생성합니다.

   파일 시스템을 생성하는 방법은 선택한 파일 시스템에 따라 다릅니다.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. 새 파티션을 마운트할 폴더를 생성합니다.

```
# mkdir /mnt/ext4
```

5. 파티션을 마운트합니다.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

iSCSI(E-Series-Linux)에서 호스트에서 스토리지 액세스 확인

볼륨을 사용하기 전에 호스트에서 볼륨에 데이터를 쓰고 다시 읽을 수 있는지 확인합니다.

시작하기 전에

다음 사항을 확인하십시오.

- 파일 시스템으로 포맷된 초기화된 볼륨입니다.

단계

1. 호스트에서 하나 이상의 파일을 디스크의 마운트 지점으로 복사합니다.
2. 파일을 원래 디스크의 다른 폴더로 다시 복사합니다.
3. "IFF" 명령을 실행하여 복사된 파일을 원본과 비교합니다.

작업을 마친 후

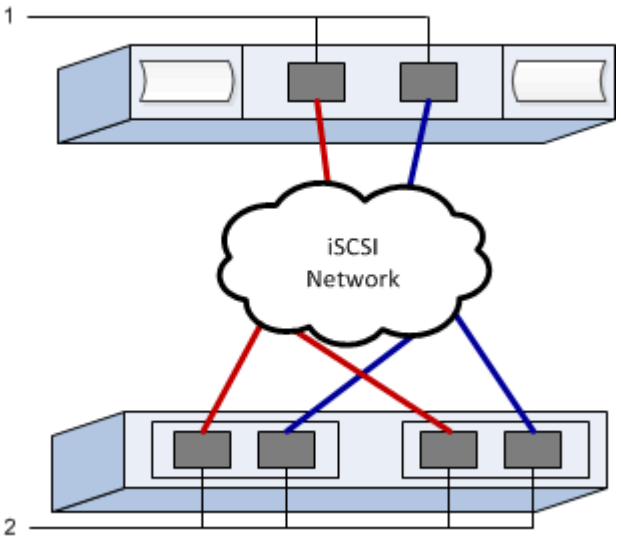
복사한 파일 및 폴더를 제거합니다.

E-Series-Linux에 iSCSI 구성을 기록합니다

이 페이지의 PDF를 생성하여 인쇄한 다음 다음 워크시트를 사용하여 iSCSI 스토리지 구성 정보를 기록할 수 있습니다. 프로비저닝 작업을 수행하려면 이 정보가 필요합니다.

권장 구성

권장 구성은 2개의 이니시에이터 포트와 1개 이상의 VLAN이 있는 4개의 타겟 포트로 구성됩니다.



타겟 **IQN**입니다

속성 표시기 번호	대상 포트 연결입니다	**IQN**을 선택합니다
2	대상 포트	

호스트 이름 매핑 중

속성 표시기 번호	호스트 정보입니다	이름 및 유형
1	호스트 이름 매핑 중	
	호스트 OS 유형입니다	