



# iSCSI 설정

## SANtricity 11.5

NetApp  
February 12, 2024

# 목차

iSCSI 설정.....	1
개념.....	1
방법.....	2
FAQ 를 참조하십시오.....	12

# iSCSI 설정

## 개념

### iSCSI 용어

iSCSI 용어가 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

기간	설명
CHAP	CHAP(Challenge Handshake Authentication Protocol) 메시드는 초기 링크 중에 대상 및 이니시에이터의 ID를 확인합니다. 인증은 CHAPsecret이라는 공유 보안 키를 기반으로 합니다.
컨트롤러	컨트롤러는 보드, 펌웨어 및 소프트웨어로 구성됩니다. 드라이브를 제어하고 System Manager 기능을 구현합니다.
DHCP를 선택합니다	DHCP(Dynamic Host Configuration Protocol)는 IP 주소와 같은 네트워크 구성 매개 변수를 동적으로 배포하기 위해 IP(인터넷 프로토콜) 네트워크에서 사용되는 프로토콜입니다.
IB	IB(InfiniBand)는 고성능 서버와 스토리지 시스템 간의 데이터 전송을 위한 통신 표준입니다.
ICMP ping 응답	ICMP(Internet Control Message Protocol)는 네트워크 컴퓨터의 운영 체제에서 메시지를 보내는 데 사용되는 프로토콜입니다. ICMP 메시지는 호스트에 연결할 수 있는지 여부와 해당 호스트와 패킷을 주고 받는 데 걸리는 시간을 결정합니다.
IQN을 선택합니다	IQN(iSCSI Qualified Name) 식별자는 iSCSI 이니시에이터 또는 iSCSI 타겟의 고유한 이름입니다.
iSER	iSER(iSCSI Extensions for RDMA)은 InfiniBand 또는 이더넷과 같은 RDMA 전송을 통해 작동하는 iSCSI 프로토콜을 확장하는 프로토콜입니다.
iSNS를 선택합니다	iSNS(Internet Storage Name Service)는 TCP/IP 네트워크에서 iSCSI 및 Fibre Channel 디바이스를 자동으로 검색, 관리 및 구성할 수 있는 프로토콜입니다.
MAC 주소	MAC 주소(Media Access Control Identifier)는 동일한 물리적 전송 네트워크 인터페이스의 두 포트를 연결하는 별도의 논리 채널을 구분하기 위해 이더넷에서 사용됩니다.
관리 클라이언트	관리 클라이언트는 System Manager 액세스를 위해 브라우저가 설치된 컴퓨터입니다.
MTU	MTU(Maximum Transmission Unit)는 네트워크에서 전송할 수 있는 가장 큰 크기의 패킷 또는 프레임입니다.

기간	설명
RDMA 를 참조하십시오	RDMA(Remote Direct Memory Access)는 네트워크 컴퓨터가 두 컴퓨터의 운영 체제와 관계없이 주 메모리에서 데이터를 교환할 수 있도록 하는 기술입니다.
명명되지 않은 검색 세션	명명되지 않은 검색 세션 옵션이 활성화된 경우 iSCSI 초기자는 컨트롤러의 정보를 검색하기 위해 타겟 IQN을 지정할 필요가 없습니다.

## 방법

### iSCSI 포트를 구성합니다

컨트롤러에 iSCSI 호스트 연결이 포함된 경우 하드웨어 페이지 또는 시스템 페이지에서 iSCSI 포트 설정을 구성할 수 있습니다.

시작하기 전에

- 컨트롤러에 iSCSI 포트가 포함되어야 합니다. 그렇지 않으면 iSCSI 설정을 사용할 수 없습니다.
- 네트워크 속도(포트와 호스트 간의 데이터 전송 속도)를 알아야 합니다.

이 작업에 대해

이 작업은 하드웨어 페이지에서 iSCSI 포트 구성에 액세스하는 방법을 설명합니다. System(시스템) 페이지(메뉴: Settings(설정) [System](시스템))에서 구성에 액세스할 수도 있습니다.



iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 나타납니다.

단계

1. 하드웨어 \* 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 \* 셸프 뒷면 표시 \* 를 클릭합니다.

그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 구성할 iSCSI 포트가 있는 컨트롤러를 클릭합니다.

컨트롤러의 상황에 맞는 메뉴가 나타납니다.

4. iSCSI 포트 구성 \* 을 선택합니다.



iSCSI 포트 구성 \* 옵션은 System Manager가 컨트롤러에서 iSCSI 포트를 감지한 경우에만 나타납니다.

iSCSI 포트 구성 대화 상자가 열립니다.

5. 드롭다운 목록에서 구성할 포트를 선택한 후 \* 다음 \* 을 클릭합니다.
6. 구성 포트 설정을 선택한 후 \* 다음 \* 을 클릭합니다.

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

필드 세부 정보

포트 설정	설명
IPv4 사용/IPv6 사용	IPv4 및 IPv6 네트워크에 대한 지원을 활성화하려면 하나 또는 두 옵션을 모두 선택하십시오. 참고: 포트 액세스를 비활성화하려면 두 확인란을 모두 선택 취소합니다.
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 클릭한 후 IPv4 설정을 선택할 수 있는 대화 상자가 열립니다. IPv6 사용 을 선택한 경우 다음 을 클릭한 후 IPv6 설정을 선택할 수 있는 대화 상자가 열립니다. 두 옵션을 모두 선택한 경우 IPv4 설정에 대한 대화 상자가 먼저 열리고 다음을 클릭하면 IPv6 설정에 대한 대화 상자가 열립니다.

7. 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. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) IPv4의 경우 네트워크 서브넷 마스크 및 게이트웨이를 포함합니다. IPv6의 경우 라우팅 가능한 IP 주소와 라우터 IP 주소를 포함합니다.
VLAN 지원을 활성화합니다(추가 설정 표시 를 클릭하여 사용 가능).	VLAN을 활성화하고 해당 ID를 입력하려면 이 옵션을 선택합니다. VLAN은 동일한 스위치, 동일한 라우터 또는 둘 다에서 지원되는 다른 물리적 LAN(가상 LAN)과 물리적으로 분리된 것처럼 동작하는 논리 네트워크입니다.
이더넷 우선 순위 활성화(추가 설정 표시 를 클릭하여 사용 가능)	네트워크 액세스 우선 순위를 결정하는 매개변수를 활성화하려면 이 옵션을 선택합니다. 슬라이더를 사용하여 1(최저)과 7(최고) 사이의 우선순위를 선택합니다.  이더넷과 같은 공유 LAN(Local Area Network) 환경에서는 많은 스테이션이 네트워크 액세스에 대해 경쟁할 수 있습니다. 액세스는 선착순으로 제공됩니다. 두 스테이션이 동시에 네트워크에 액세스하려고 시도할 수 있으며, 이로 인해 두 스테이션이 다시 꺼졌다가 다시 시도하기 전에 대기하게 됩니다. 스위치 포트에 하나의 스테이션만 연결되어 있는 스위치 이더넷의 경우 이 프로세스가 최소화됩니다.

8. 마침 \* 을 클릭합니다.

### iSCSI 인증을 구성합니다

iSCSI 네트워크의 보안을 강화하기 위해 컨트롤러(타겟)와 호스트(이니시에이터) 간에 인증을 설정할 수 있습니다. System Manager에서는 CHAP(Challenge Handshake Authentication Protocol) 방법을 사용하여 초기 링크 중에 대상 및 초기자의 ID를 확인합니다. 인증은 CHAPsecret이라는 공유 보안 키를 기반으로 합니다.

#### 시작하기 전에

타겟(컨트롤러)에 대한 CHAP 암호를 설정하기 전이나 후에 이니시에이터(iSCSI 호스트)에 대한 CHAP 암호를 설정할 수 있습니다. 이 작업의 지침을 따르기 전에 호스트가 iSCSI 연결을 먼저 수행할 때까지 기다린 다음 개별 호스트에 CHAP 암호를 설정해야 합니다. 연결이 완료되면 호스트의 IQN 이름과 해당 CHAP 암호가 iSCSI 인증 대화 상자(이 작업에 설명되어 있음)에 나열되며, 수동으로 입력할 필요가 없습니다.

이 작업에 대해

다음 인증 방법 중 하나를 선택할 수 있습니다.

- \* 단방향 인증 \* — 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하려면 이 설정을 사용합니다(단방향 인증).
- \* 양방향 인증 \* — 컨트롤러와 iSCSI 호스트가 모두 인증(양방향 인증)을 수행할 수 있도록 하려면 이 설정을 사용합니다. 이 설정은 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하고, iSCSI 호스트가 컨트롤러의 ID를 인증할 수 있도록 하여 두 번째 수준의 보안을 제공합니다.



iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 설정 페이지에 표시됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. iSCSI 설정 \* 에서 \* 인증 구성 \* 을 클릭합니다.

현재 설정된 방법을 보여 주는 Configure Authentication 대화 상자가 나타납니다. 또한 호스트에 CHAP 암호가 구성되어 있는지 여부도 표시됩니다.

3. 다음 중 하나를 선택합니다.
  - \* 인증 없음 \* — 컨트롤러가 iSCSI 호스트의 ID를 인증하지 않도록 하려면 이 옵션을 선택하고 \* 마침 \* 을 클릭합니다. 대화 상자가 닫히고 구성이 완료됩니다.
  - \* 단방향 인증 \* — 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하려면 이 옵션을 선택하고 \* 다음 \* 을 클릭하여 대상 CHAP 구성 대화 상자를 표시합니다.
  - \* 양방향 인증 \* — 컨트롤러와 iSCSI 호스트가 인증을 수행하도록 허용하려면 이 옵션을 선택하고 \* 다음 \* 을 클릭하여 대상 CHAP 구성 대화 상자를 표시합니다.
4. 단방향 또는 양방향 인증의 경우 컨트롤러의 CHAP 암호(타겟)를 입력하거나 확인합니다. CHAP 암호는 12자에서 57자 사이의 인쇄 가능한 ASCII 문자여야 합니다.



컨트롤러에 대한 CHAP 암호가 이전에 구성된 경우 필드의 문자가 마스킹됩니다. 필요한 경우 기존 문자를 바꿀 수 있습니다(새 문자는 마스킹되지 않음).

5. 다음 중 하나를 수행합니다.
  - one-way\_authentication을 구성하는 경우 \* Finish \* 를 클릭합니다. 대화 상자가 닫히고 구성이 완료됩니다.
  - two-way\_authentication을 구성하는 경우 \* Next \* 를 클릭하여 이니시에이터 CHAP 구성 대화 상자를 표시합니다.
6. 양방향 인증의 경우, 12-57자의 인쇄 가능한 ASCII 문자일 수 있는 iSCSI 호스트(이니시에이터)에 대한 CHAP 암호를 입력하거나 확인합니다. 특정 호스트에 대해 양방향 인증을 구성하지 않으려면 \* Initiator CHAP Secret \* 필드를 비워 둡니다.



호스트에 대한 CHAP 암호가 이전에 구성된 경우 필드의 문자가 마스킹됩니다. 필요한 경우 기존 문자를 바꿀 수 있습니다(새 문자는 마스킹되지 않음).

7. 마침 \* 을 클릭합니다.

결과

인증을 지정하지 않은 경우, 컨트롤러와 iSCSI 호스트 간의 iSCSI 로그인 시퀀스 중에 인증이 발생합니다.

## iSCSI 검색 설정을 활성화합니다

iSCSI 네트워크에서 스토리지 디바이스 검색과 관련된 설정을 설정할 수 있습니다. 대상 검색 설정을 사용하면 iSNS(Internet Storage Name Service) 프로토콜을 사용하여 스토리지 배열의 iSCSI 정보를 등록하고 명명되지 않은 검색 세션을 허용할지 여부를 결정할 수 있습니다

시작하기 전에

iSNS 서버가 정적 IP 주소를 사용하는 경우 iSNS 등록에 해당 주소를 사용할 수 있어야 합니다. IPv4와 IPv6가 모두 지원됩니다.

이 작업에 대해

iSCSI 검색과 관련된 다음 설정을 활성화할 수 있습니다.

- \* iSNS 서버를 사용하여 타겟을 등록합니다. \* — 이 옵션을 설정하면 스토리지 어레이가 iSNS 서버의 iSCSI IQN(Qualified Name) 및 포트 정보를 등록합니다. 이 설정은 iSNS 검색을 허용하므로 이니시에이터는 iSNS 서버에서 IQN 및 포트 정보를 검색할 수 있습니다.
- \* 이름 없는 검색 세션 활성화 \* — 이름 없는 검색 세션이 활성화되면 이니시에이터(iSCSI 호스트)가 검색 유형 연결을 위한 로그인 시퀀스 중에 타겟(컨트롤러)의 IQN을 제공할 필요가 없습니다. 비활성화된 경우 호스트는 IQN을 제공하여 컨트롤러에 검색 세션을 설정해야 합니다. 하지만 정상(입출력 베어링) 세션에 대해서는 타겟 IQN이 항상 필요합니다. 이 설정을 비활성화하면 권한이 없는 iSCSI 호스트가 해당 IP 주소만 사용하여 컨트롤러에 연결하는 것을 방지할 수 있습니다.



iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 설정 페이지에 표시됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. iSCSI 설정 \* 에서 \* 대상 검색 설정 보기/편집 \* 을 클릭합니다.

대상 검색 설정 \* 대화 상자가 나타납니다. iSNS 서버 사용... 필드 아래에 컨트롤러가 이미 등록되어 있는지 여부를 나타내는 대화 상자가 나타납니다.

3. 컨트롤러를 등록하려면 \* iSNS 서버를 사용하여 대상 등록 \* 을 선택한 후 다음 중 하나를 선택합니다.
  - \* DHCP 서버에서 자동으로 구성 가져오기 \* — DHCP(Dynamic Host Configuration Protocol) 서버를 사용하여 iSNS 서버를 구성하려면 이 옵션을 선택합니다. 이 옵션을 사용하는 경우 컨트롤러의 모든 iSCSI 포트에서도 DHCP를 사용하도록 구성해야 합니다. 필요한 경우 컨트롤러 iSCSI 포트 설정을 업데이트하여 이 옵션을 활성화합니다.



DHCP 서버가 iSNS 서버 주소를 제공하려면 옵션 43 - - "공급업체 특정 정보"를 사용하도록 DHCP 서버를 구성해야 합니다. 이 옵션은 데이터 바이트 0xa-0xd(10-13)로 iSNS 서버 IPv4 주소를 포함해야 합니다.

- \* 수동으로 정적 구성 지정 \* — iSNS 서버의 정적 IP 주소를 입력하려면 이 옵션을 선택합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) 필드에 IPv4 주소 또는 IPv6 주소를 입력합니다. 둘 다 구성한 경우 IPv4가 기본값입니다. 또한 TCP 수신 대기 포트를 입력합니다(기본값 3205를 사용하거나 49152와 65535 사이의 값을 입력합니다).
4. 스토리지 배열이 명명되지 않은 검색 세션에 참여할 수 있도록 하려면 \* 명명되지 않은 검색 세션 활성화 \* 를 선택합니다.



- 이 옵션을 설정하면 컨트롤러의 정보를 검색하기 위해 타겟 IQN을 지정하는 데 iSCSI 이니시에이터가 필요하지 않습니다.
- 비활성화된 경우 이니시에이터가 타겟 IQN을 제공하지 않으면 검색 세션이 차단됩니다. 명명되지 않은 검색 세션을 비활성화하면 보안이 강화됩니다.

5. 저장 \* 을 클릭합니다.

## 결과

System Manager에서 iSNS 서버에 컨트롤러를 등록하려고 하면 진행률 표시줄이 나타납니다. 이 프로세스는 최대 5분 정도 걸릴 수 있습니다.

## iSCSI 통계 패키지를 봅니다

스토리지 배열에 대한 iSCSI 연결에 대한 데이터를 볼 수 있습니다.

### 이 작업에 대해

System Manager는 이러한 유형의 iSCSI 통계를 표시합니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- \* 이더넷 MAC 통계 \* — MAC(Media Access Control)에 대한 통계를 제공합니다. 또한 MAC는 실제 주소 또는 MAC 주소라는 주소 지정 메커니즘을 제공합니다. MAC 주소는 각 네트워크 어댑터에 할당된 고유한 주소입니다. MAC 주소는 하위 네트워크 내의 대상으로 데이터 패킷을 전송하는 데 도움이 됩니다.
- \* 이더넷 TCP/IP 통계 \* — TCP(Transmission Control Protocol) 및 IP(Internet Protocol)인 TCP/IP에 대한 통계를 제공합니다. TCP를 사용하면 네트워크로 연결된 호스트의 응용 프로그램이 서로 연결을 만들어 데이터를 패킷으로 교환할 수 있습니다. IP는 패킷 교환 방식의 네트워크를 통해 데이터를 전달하는 데이터 지향 프로토콜입니다. IPv4 통계 및 IPv6 통계는 별도로 표시됩니다.
- \* 로컬 대상/초기자(프로토콜) 통계 \* — iSCSI 대상에 대한 통계를 표시합니다. iSCSI 타겟은 해당 스토리지 미디어에 대한 블록 수준 액세스를 제공하고 비동기 미러링 작업에서 이니시에이터로 사용될 때 스토리지 배열에 대한 iSCSI 통계를 표시합니다.
- \* DCBX 작업 상태 통계 \* — 다양한 DCBX(Data Center Bridging Exchange) 기능의 작동 상태를 표시합니다.
- \* LLDP TLV statistics \* — LLDP(Link Layer Discovery Protocol) TLV(Type Length Value) 통계를 표시합니다.
- \* DCBX TLV 통계 \* — DCB(데이터 센터 브리징) 환경에서 스토리지 배열 호스트 포트를 식별하는 정보를 표시합니다. 이 정보는 식별 및 기능 목적으로 네트워크 피어와 공유됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

### 단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. iSCSI 통계 패키지 보기 \* 를 선택합니다.
3. 탭을 클릭하여 다양한 통계 집합을 봅니다.
4. 기준선을 설정하려면 \* Set new baseline \* 을 클릭합니다.

기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. 모든 iSCSI 통계에는 동일한 기준이 사용됩니다.

## iSCSI 세션을 종료합니다

더 이상 필요하지 않은 iSCSI 세션을 종료할 수 있습니다. iSCSI 세션은 비동기 미러 관계의 호스트 또는 원격 스토리지 시스템에서 발생할 수 있습니다.

이 작업에 대해

다음과 같은 이유로 iSCSI 세션을 종료할 수 있습니다.

- \* 무단 액세스 \* — iSCSI 초기자가 로그인되어 있고 액세스 권한이 없는 경우 iSCSI 세션을 종료하여 iSCSI 초기자를 스토리지 배열에서 강제로 끌 수 있습니다. 사용 가능한 인증 방법이 없으므로 iSCSI 초기자가 로그인할 수 있습니다.
- \* 시스템 다운타임 \* — 스토리지 배열을 중지시켜야 하고 iSCSI 초기자가 여전히 로그인 상태인 것을 볼 경우 iSCSI 세션을 종료하여 스토리지 배열에서 iSCSI 초기자를 가져올 수 있습니다.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. iSCSI 세션 보기/종료 \* 를 선택합니다.

현재 iSCSI 세션 목록이 나타납니다.

3. 종료할 세션을 선택합니다
4. 세션 종료 \* 를 클릭하고 작업을 수행할지 확인합니다.

## iSCSI 세션을 봅니다

스토리지 배열에 대한 iSCSI 연결에 대한 자세한 정보를 볼 수 있습니다. iSCSI 세션은 비동기 미러 관계의 호스트 또는 원격 스토리지 시스템에서 발생할 수 있습니다.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. iSCSI 세션 보기/종료 \* 를 선택합니다.

현재 iSCSI 세션 목록이 나타납니다.

3. 특정 iSCSI 세션에 대한 추가 정보를 보려면 세션을 선택한 다음 \* 세부 정보 보기 \* 를 클릭합니다.

필드 세부 정보

항목	설명
세션 식별자(SSID)	iSCSI 이니시에이터와 iSCSI 타겟 간의 세션을 식별하는 16진수 문자열입니다. SSID는 ISID와 TPGT로 구성됩니다.
이니시에이터 세션 ID(ISID)	세션 식별자의 이니시에이터 부분입니다. 초기자는 로그인 중에 ISID를 지정합니다.
대상 포털 그룹	iSCSI 타겟입니다.
대상 포털 그룹 태그(TPGT)	세션 식별자의 대상 부분. iSCSI 대상 포털 그룹의 16비트 숫자 식별자입니다.
이니시에이터 iSCSI 이름입니다	이니시에이터의 전 세계에서 고유한 이름입니다.
이니시에이터 iSCSI 레이블	System Manager에 설정된 사용자 레이블입니다.
이니시에이터 iSCSI 별칭입니다	iSCSI 노드와 연결할 수도 있는 이름입니다. 별칭을 사용하면 조직에서 사용자에게 친숙한 문자열을 iSCSI 이름과 연결할 수 있습니다. 그러나 별칭은 iSCSI 이름을 대체하는 것이 아닙니다. 이니시에이터 iSCSI 별칭은 호스트에서만 설정할 수 있고 System Manager에서는 설정할 수 없습니다
호스트	스토리지 배열에 입력 및 출력을 전송하는 서버입니다.
연결 ID(CID)	이니시에이터와 타겟 간의 세션 내 접속에 대한 고유한 이름입니다. 초기자는 이 ID를 생성하여 로그인 요청 중에 대상에 제공합니다. 연결이 닫히라는 로그아웃 중에도 연결 ID가 표시됩니다.
이더넷 포트 식별자입니다	연결과 관련된 컨트롤러 포트입니다.
이니시에이터 IP 주소입니다	이니시에이터의 IP 주소입니다.
협상된 로그인 매개 변수	iSCSI 세션 로그인 중에 트랜잭션되는 매개 변수입니다.
인증 방법	iSCSI 네트워크에 액세스할 사용자를 인증하는 기술입니다. 유효한 값은 * CHAP * 및 * 없음 * 입니다.
헤더 다이제스트 방법입니다	iSCSI 세션에 대해 가능한 헤더 값을 표시하는 기술입니다. HeaderDigest 및 DataDigest는 * None * 또는 * CRC32C * 일 수 있습니다. 두 가지 모두 기본값은 * 없음 * 입니다.

항목	설명
데이터 다이제스트 방법입니다	iSCSI 세션에 대해 가능한 데이터 값을 표시하는 기술입니다. HeaderDigest 및 DataDigest는 * None * 또는 * CRC32C * 일 수 있습니다. 두 가지 모두 기본값은 * 없음 * 입니다.
최대 연결 수	iSCSI 세션에 허용되는 최대 연결 수입니다. 최대 연결 수는 1 ~ 4입니다. 기본값은 * 1 * 입니다.
대상 별칭	대상과 연관된 레이블입니다.
이니시에이터 별칭입니다	이니시에이터와 연결된 레이블입니다.
대상 IP 주소입니다	iSCSI 세션의 타겟의 IP 주소입니다. DNS 이름은 지원되지 않습니다.
초기 R2T	초기 전송 준비 상태입니다. 상태는 * 예 * 또는 * 아니요 * 일 수 있습니다.
최대 버스트 길이	이 iSCSI 세션의 최대 SCSI 페이로드(바이트) 최대 버스트 길이는 512에서 262,144(256KB)입니다. 기본값은 * 262,144(256KB) * 입니다.
첫 번째 버스트 길이	이 iSCSI 세션에 대한 요청되지 않은 데이터의 SCSI 페이로드입니다. 첫 번째 버스트 길이는 512에서 131,072(128KB)일 수 있습니다. 기본값은 * 65,536(64KB) * 입니다.
기본 대기 시간입니다	연결 종료 또는 연결 재설정 후 연결을 시도하기 전에 대기하는 최소 시간(초)입니다. 기본 대기 시간은 0에서 3600 사이입니다. 기본값은 * 2 * 입니다.
기본 유지 시간	연결 종료 또는 연결 재설정 후에도 연결이 가능한 최대 시간(초)입니다. 기본 유지 시간은 0에서 3600 사이입니다. 기본값은 * 20 * 입니다.
최대 미결 R2T	이 iSCSI 세션에 대해 최대 "전송 준비 완료" 수입니다. 전송 준비 완료 최대 값은 1에서 16 사이의 값일 수 있습니다. 기본값은 * 1 * 입니다.
복구 수준 오류	이 iSCSI 세션에 대한 오류 복구 수준입니다. 오류 복구 레벨 값은 항상 * 0 * 으로 설정됩니다.
최대 수신 데이터 세그먼트 길이	이니시에이터 또는 타겟이 iSCSI PDU(페이로드 데이터 유닛)에서 수신할 수 있는 최대 데이터 양입니다.
대상 이름입니다	대상의 공식 이름(별칭 아님). 대상 이름(_iqn_format)입니다.
이니시에이터 이름입니다	이니시에이터의 공식 이름(별칭 아님) <i>iqn</i> 또는 <i>_eui_format</i> 을 사용하는 이니시에이터 이름입니다.

4. 보고서를 파일에 저장하려면 \* 저장 \* 을 클릭합니다.

이 파일은 브라우저의 다운로드 폴더에 "iscsi-session-connections.txt"라는 파일 이름으로 저장됩니다.

## InfiniBand 포트를 통해 iSER 구성

컨트롤러에 InfiniBand 포트를 통한 iSER이 포함된 경우 호스트에 대한 네트워크 연결을 구성할 수 있습니다. 구성 설정은 하드웨어 페이지 또는 시스템 페이지에서 사용할 수 있습니다.

시작하기 전에

- 컨트롤러에 InfiniBand 포트를 통한 iSER이 포함되어야 합니다. 그렇지 않으면 InfiniBand를 통한 iSER 설정을 System Manager에서 사용할 수 없습니다.
- 호스트 연결의 IP 주소를 알아야 합니다.

이 작업에 대해

iSER은 \* Hardware \* 페이지 또는 메뉴에서 \* Settings[System] 메뉴에서 InfiniBand 구성을 통해 액세스할 수 있습니다. 이 작업에서는 \* 하드웨어 \* 페이지에서 포트를 구성하는 방법에 대해 설명합니다.



InfiniBand를 통한 iSER 설정 및 기능은 스토리지 어레이 컨트롤러에 InfiniBand 포트를 통한 iSER이 포함된 경우에만 나타납니다.

단계

1. 하드웨어 \* 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 \* 셀프 뒷면 표시 \* 를 클릭합니다.  
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.
3. 구성하려는 InfiniBand 포트를 통해 iSER이 있는 컨트롤러를 클릭합니다.  
컨트롤러의 상황에 맞는 메뉴가 나타납니다.
4. InfiniBand 포트를 통해 iSER 구성 \* 을 선택합니다.  
InfiniBand 포트를 통해 iSER 구성 대화 상자가 열립니다.
5. 드롭다운 목록에서 구성할 HIC 포트를 선택한 다음 호스트의 IP 주소를 입력합니다.
6. 구성 \* 을 클릭합니다.
7. 구성을 완료한 다음 \* Yes \* 를 클릭하여 iSER을 InfiniBand 포트에 재설정합니다.

## InfiniBand 통계를 통해 iSER 보기

스토리지 어레이의 컨트롤러에 InfiniBand 포트를 통한 iSER이 포함된 경우 호스트 연결에 대한 데이터를 볼 수 있습니다.

이 작업에 대해

System Manager는 InfiniBand 통계를 통해 다음과 같은 유형의 iSER을 보여 줍니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- \* 로컬 타겟(프로토콜) 통계 \* — InfiniBand 타겟에 대한 iSER 통계를 제공하며, 이 통계는 스토리지 미디어에 대한 블록 레벨 액세스를 보여줍니다.
- InfiniBand 인터페이스 통계 \* 를 통한 \* iSER — InfiniBand 인터페이스의 모든 iSER 포트에 대한 통계를 제공하며, 여기에는 각 스위치 포트와 관련된 성능 통계 및 링크 오류 정보가 포함됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

InfiniBand 통계를 통해 iSER에 액세스하려면 시스템 페이지(메뉴: 설정 [시스템]) 또는 지원 페이지에서 액세스할 수 있습니다. 다음 지침은 지원 페이지에서 통계에 액세스하는 방법을 설명합니다.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. InfiniBand 통계 \* 를 통해 iSER 보기 \* 를 선택합니다.
3. 탭을 클릭하여 다양한 통계 집합을 봅니다.
4. 기준선을 설정하려면 \* Set new baseline \* 을 클릭합니다.

기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. InfiniBand 통계에서 모든 iSER에 동일한 기준선이 사용됩니다.

## FAQ 를 참조하십시오

등록을 위해 **iSNS** 서버를 사용하면 어떻게 됩니까?

iSNS(Internet Storage Name Service) 서버 정보를 사용하는 경우 iSNS 서버를 쿼리하여 타겟(컨트롤러)에서 정보를 검색하도록 호스트(이니시에이터)를 구성할 수 있습니다.

이 등록을 통해 iSNS 서버에 컨트롤러의 IQN(iSCSI Qualified Name) 및 포트 정보를 제공하고 이니시에이터(iSCSI 호스트)와 타겟(컨트롤러) 간의 쿼리를 허용합니다.

**iSCSI**에 대해 자동으로 지원되는 등록 방법은 무엇입니까?

iSCSI 구현에서는 iSNS(Internet Storage Name Service) 검색 방법이나 대상 보내기 명령을 사용할 수 있습니다.

iSNS 방법을 사용하면 이니시에이터(iSCSI 호스트)와 타겟(컨트롤러) 간에 iSNS 검색을 수행할 수 있습니다. iSNS 서버에 컨트롤러의 IQN(iSCSI Qualified Name) 및 포트 정보를 제공하기 위해 타겟 컨트롤러를 등록합니다.

iSNS를 구성하지 않으면 iSCSI 호스트가 iSCSI 검색 세션 중에 대상 보내기 명령을 전송할 수 있습니다. 이에 따라 컨트롤러는 포트 정보(예: 대상 IQN, 포트 IP 주소, 수신 포트 및 대상 포트 그룹)를 반환합니다. iSNS를 사용하는 경우 호스트 이니시에이터가 iSNS 서버에서 대상 IP를 검색할 수 있으므로 이 검색 방법은 필요하지 않습니다.

**InfiniBand** 통계를 통해 **iSER**을 어떻게 해석합니까?

InfiniBand 통계 \* 를 통해 iSER 보기 대화 상자에는 로컬 대상(프로토콜) 통계와 iSER over InfiniBand(IB) 인터페이스 통계가 표시됩니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- \* 로컬 타겟(프로토콜) 통계 \* — InfiniBand 타겟에 대한 iSER 통계를 제공하며, 이 통계는 스토리지 미디어에 대한 블록 레벨 액세스를 보여줍니다.
- InfiniBand 인터페이스 통계 \* 를 통한 \* iSER — InfiniBand 인터페이스의 InfiniBand 포트를 통해 모든 iSER에 대한 통계를 제공하며, 여기에는 각 스위치 포트와 관련된 성능 통계 및 링크 오류 정보가 포함됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

## InfiniBand를 통해 iSER을 구성하거나 진단하려면 어떻게 해야 합니까?

다음 표에는 InfiniBand 세션을 통해 iSER을 구성 및 관리하는 데 사용할 수 있는 System Manager 기능이 나와 있습니다.



InfiniBand를 통한 iSER 설정은 스토리지 어레이의 컨트롤러에 InfiniBand 호스트 관리 포트를 통한 iSER이 포함된 경우에만 사용할 수 있습니다.

### InfiniBand를 통해 iSER 구성 및 진단

조치	위치
InfiniBand 포트를 통해 iSER 구성	<ol style="list-style-type: none"> <li>1. 하드웨어 * 를 선택합니다.</li> <li>2. Show back of shelf * 를 선택합니다.</li> <li>3. 컨트롤러를 선택합니다.</li> <li>4. InfiniBand 포트를 통해 iSER 구성 * 을 선택합니다.</li> </ol> <p>또는</p> <ol style="list-style-type: none"> <li>1. 설정 [시스템] 메뉴를 선택합니다.</li> <li>2. InfiniBand 설정을 통해 * iSER * 로 스크롤한 다음 * InfiniBand 포트를 통해 iSER 구성 * 을 선택합니다.</li> </ol>
InfiniBand 통계를 통해 iSER 보기	<ol style="list-style-type: none"> <li>1. 설정 [시스템] 메뉴를 선택합니다.</li> <li>2. InfiniBand 설정 * 을 통해 * iSER로 스크롤한 다음 * InfiniBand 통계 * 를 통해 iSER 보기 * 를 선택합니다.</li> </ol>

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 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.