iSCSI 서비스 관리

ONTAP 9

NetApp
September 12, 2024

목차

iSCSI 서비스 관리

iSCSI 서비스 관리

"vserver iSCSI interface enable" 또는 "vserver iscsi interface disable" 명령을 사용하여 SVM(스토리지 가상 시스템)의 iSCSI 논리 인터페이스에서 iSCSI 서비스의 가용성을 관리할 수 있습니다.

기본적으로 iSCSI 서비스는 모든 iSCSI 논리 인터페이스에서 활성화됩니다.

호스트에서 iSCSI를 구현하는 방법

iSCSI는 하드웨어 또는 소프트웨어를 사용하여 호스트에서 구현할 수 있습니다.

다음 방법 중 하나로 iSCSI를 구현할 수 있습니다.

- 호스트의 표준 이더넷 인터페이스를 사용하는 이니시에이터 소프트웨어 사용
- iSCSI HBA(호스트 버스 어댑터)를 통해: iSCSI HBA가 호스트 운영 체제에 로컬 디스크가 있는 SCSI 디스크 어댑터로 나타납니다.
- TCP/IP 처리를 오프로드하는 TOE(TCP Offload Engine) 어댑터 사용

  iSCSI 프로토콜 처리는 호스트 소프트웨어에 의해 계속 수행됩니다.

iSCSI 인증의 작동 방식

iSCSI 세션의 초기 단계 중에 이니시에이터는 iSCSI 세션을 시작하기 위해 스토리지 시스템에 로그인 요청을 보냅니다. 그러면 스토리지 시스템에서 로그인 요청을 허용하거나 거부하거나 로그인이 필요하지 않음을 확인합니다.

iSCSI 인증 방법은 다음과 같습니다.

- CHAP(Challenge Handshake Authentication Protocol) — 초기자는 CHAP 사용자 이름 및 암호를 사용하여 로그인합니다.

  CHAP 암호를 지정하거나 16진수 암호 암호를 생성할 수 있습니다. CHAP 사용자 이름과 암호는 두 가지 유형이 있습니다.

  - 인바운드 — 스토리지 시스템이 이니시에이터를 인증합니다.

    CHAP 인증을 사용하는 경우 인바운드 설정이 필요합니다.

  - 아웃바운드 — 초기자가 스토리지 시스템을 인증할 수 있도록 하는 선택적 설정입니다.

    스토리지 시스템에서 인바운드 사용자 이름과 암호를 정의한 경우에만 아웃바운드 설정을 사용할 수 있습니다.

- deny — 스토리지 시스템에 대한 액세스가 거부됩니다.

- 없음 — 스토리지 시스템은 이니시에이터에 대한 인증을 요구하지 않습니다.

이니시에이터 목록과 해당 인증 방법을 정의할 수 있습니다. 이 목록에 없는 이니시에이터에 적용되는 기본 인증 방법을 정의할 수도 있습니다.

관련 정보

"Data ONTAP를 사용하는 Windows 다중 경로 옵션: Fibre Channel 및 iSCSI"

iSCSI 초기자 보안 관리

ONTAP는 iSCSI 초기자에 대한 보안을 관리하는 다양한 기능을 제공합니다. iSCSI 초기자 목록과 각각에 대한 인증 방법을 정의하고, 인증 목록에 초기자 및 관련 인증 방법을 표시하고, 인증 목록에서 이니시에이터를 추가 및 제거하고, 목록에 없는 이니시에이터에 대한 기본 iSCSI 초기자 인증 방법을 정의할 수 있습니다.

iSCSI 엔드포인트 격리

ONTAP 9.1부터 기존 iSCSI 보안 명령이 IP 주소 범위 또는 여러 IP 주소를 사용할 수 있도록 향상되었습니다.

모든 iSCSI 초기자는 세션 또는 대상과의 연결을 설정할 때 발신 IP 주소를 제공해야 합니다. 이 새로운 기능은 원본 IP 주소가 지원되지 않거나 알려지지 않은 경우 이니시에이터가 클러스터에 로그인하지 못하도록 하여 고유한 식별 체계를 제공합니다. 지원되지 않거나 알 수 없는 IP 주소에서 시작된 모든 이니시에이터는 iSCSI 세션 계층에서 로그인이 거부되어 이니시에이터가 클러스터 내의 LUN 또는 볼륨에 액세스하지 못하게 됩니다.

두 개의 새로운 명령으로 이 새로운 기능을 구현하여 기존 항목을 관리할 수 있습니다.

이니시에이터 주소 범위를 추가합니다

"vserver iscsi security add-initiator-address-range" 명령을 사용하여 IP 주소 범위 또는 여러 IP 주소를 추가하여 iSCSI 초기자 보안 관리를 향상시킵니다.

'cluster1::> vserver iscsi security add-initiator-address-range'

이니시에이터 주소 범위를 제거합니다

vserver iscsi security remove-initiator-address-range 명령으로 IP 주소 범위 또는 여러 IP 주소를 제거합니다.

'cluster1::> vserver iscsi security remove-initiator-address-range'

CHAP 인증입니다

CHAP(Challenge Handshake Authentication Protocol)는 iSCSI 이니시에이터와 타겟 간의 인증된 통신을 활성화합니다. CHAP 인증을 사용하는 경우 이니시에이터와 스토리지 시스템 모두에서 CHAP 사용자 이름 및 암호를 정의합니다.

iSCSI 세션의 초기 단계 중에 이니시에이터는 스토리지 시스템에 로그인 요청을 보내 세션을 시작합니다. 로그인 요청에는 이니시에이터의 CHAP 사용자 이름 및 CHAP 알고리즘이 포함됩니다. 스토리지 시스템이 CHAP 챌린지에

응답합니다. 이니시에이터는 CHAP 응답을 제공합니다. 스토리지 시스템에서 응답을 확인하고 이니시에이터를 인증합니다. CHAP 암호는 응답을 계산하는 데 사용됩니다.

CHAP 인증 사용에 대한 지침입니다

CHAP 인증을 사용할 때는 특정 지침을 따라야 합니다.

- 스토리지 시스템에서 인바운드 사용자 이름과 암호를 정의하는 경우 이니시에이터에서 아웃바운드 CHAP 설정에 동일한 사용자 이름과 암호를 사용해야 합니다. 양방향 인증을 사용하도록 스토리지 시스템에 아웃바운드 사용자 이름과 암호도 정의한 경우, 이니시에이터에서 인바운드 CHAP 설정에 동일한 사용자 이름과 암호를 사용해야 합니다.
- 스토리지 시스템의 인바운드 및 아웃바운드 설정에 동일한 사용자 이름과 암호를 사용할 수 없습니다.
- CHAP 사용자 이름은 1 ~ 128바이트일 수 있습니다.

  null 사용자 이름은 허용되지 않습니다.

- CHAP 암호(암호)는 1 ~ 512바이트입니다.

  암호는 16진수 값 또는 문자열일 수 있습니다. 16진수 값의 경우 접두사 "0x" 또는 "0x"로 값을 입력해야 합니다. null 암호는 허용되지 않습니다.

> ONTAP에서는 CHAP 암호(암호)에 영어가 아닌 특수 문자, 숫자 및 공백을 사용할 수 있습니다. 그러나 호스트 제한에 따라 다릅니다. 이러한 호스트 중 특정 호스트에서 허용되지 않는 호스트는 사용할 수 없습니다.
>
> 예를 들어, Microsoft iSCSI 소프트웨어 초기자는 IPsec 암호화가 사용되지 않는 경우 초기자 및 대상 CHAP 암호를 모두 12바이트 이상 필요로 합니다. 최대 암호 길이는 IPsec의 사용 여부에 관계없이 16바이트입니다.
>
> 추가 제한 사항은 이니시에이터의 설명서를 참조하십시오.

iSCSI 인터페이스 액세스 목록을 사용하여 이니시에이터 인터페이스를 제한하는 방법은 성능과 보안을 향상시킬 수 있습니다

iSCSI 인터페이스 액세스 목록을 사용하면 이니시에이터가 액세스할 수 있는 SVM의 LIF 수를 제한하여 성능과 보안을 강화할 수 있습니다.

초기자가 iSCSI 'endTargets' 명령을 사용하여 검색 세션을 시작하면 액세스 목록에 있는 LIF(네트워크 인터페이스)와 연결된 IP 주소를 수신합니다. 기본적으로 모든 이니시에이터는 SVM의 모든 iSCSI LIF에 액세스할 수 있습니다. 액세스 목록을 사용하여 이니시에이터가 액세스할 수 있는 SVM의 LIF 수를 제한할 수 있습니다.

iSNS(Internet Storage Name Service)

iSNS(Internet Storage Name Service)는 TCP/IP 스토리지 네트워크에서 iSCSI 디바이스를 자동으로 검색하고 관리할 수 있도록 하는 프로토콜입니다. iSNS 서버는 IP 주소, iSCSI 노드 이름 IQN 및 포털 그룹을 포함하여 네트워크의 활성 iSCSI 장치에 대한 정보를 유지합니다.

타사 공급업체에서 iSNS 서버를 가져올 수 있습니다. 네트워크에 iSNS 서버가 구성되어 이니시에이터 및 타겟에

사용하도록 설정되어 있는 경우 SVM(스토리지 가상 머신)에 관리 LIF를 사용하여 iSNS 서버에 해당 SVM에 대한 모든 iSCSI LIF를 등록할 수 있습니다. 등록이 완료되면 iSCSI 이니시에이터가 iSNS 서버를 쿼리하여 해당 SVM에 대한 모든 LIF를 검색할 수 있습니다.

iSNS 서비스를 사용하려는 경우 iSNS(Internet Storage Name Service) 서버에 스토리지 가상 시스템(SVM)이 올바르게 등록되어 있는지 확인해야 합니다.

네트워크에 iSNS 서버가 없는 경우 호스트에 표시되도록 각 타겟을 수동으로 구성해야 합니다.

iSNS 서버의 기능

iSNS 서버는 iSNS(Internet Storage Name Service) 프로토콜을 사용하여 IP 주소, iSCSI 노드 이름(IQN) 및 포털 그룹을 포함하여 네트워크의 활성 iSCSI 장치에 대한 정보를 유지합니다.

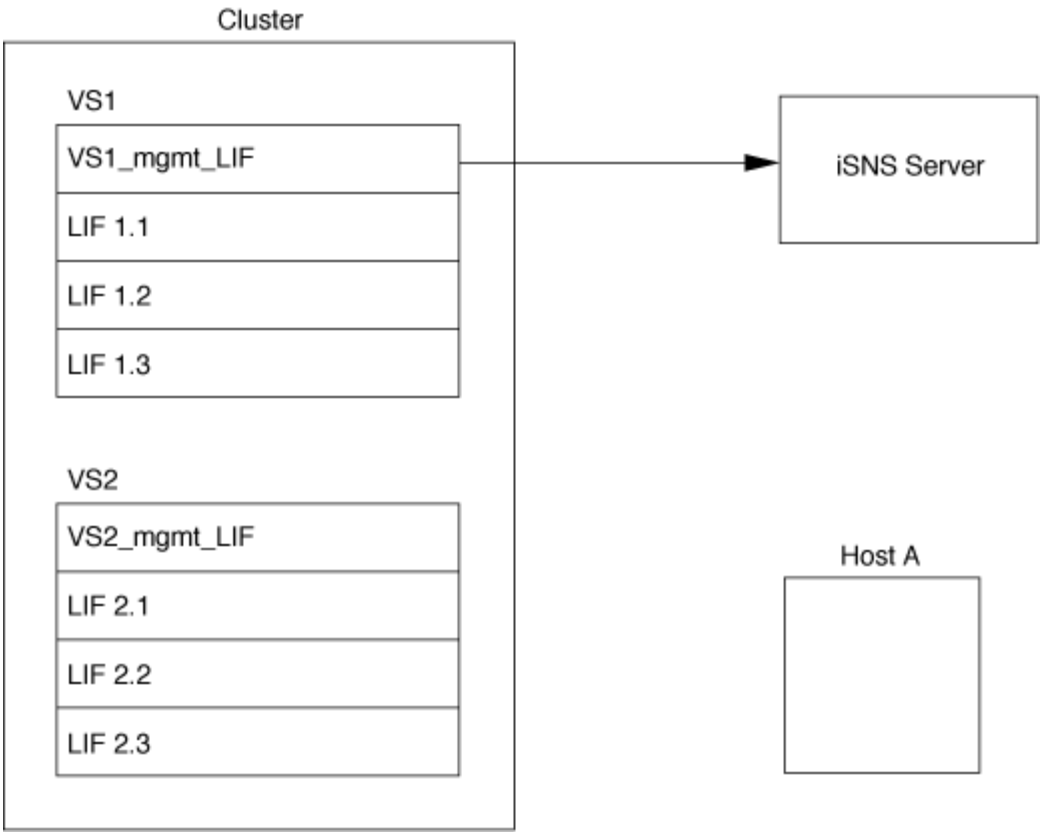
iSNS 프로토콜을 사용하면 IP 스토리지 네트워크에서 iSCSI 디바이스를 자동으로 검색하고 관리할 수 있습니다. iSCSI 이니시에이터는 iSNS 서버를 쿼리하여 iSCSI 타겟 디바이스를 검색할 수 있습니다.

NetApp은 iSNS 서버를 제공하거나 재판매하지 않습니다. NetApp에서 지원하는 공급업체로부터 이러한 서버를 받을 수 있습니다.

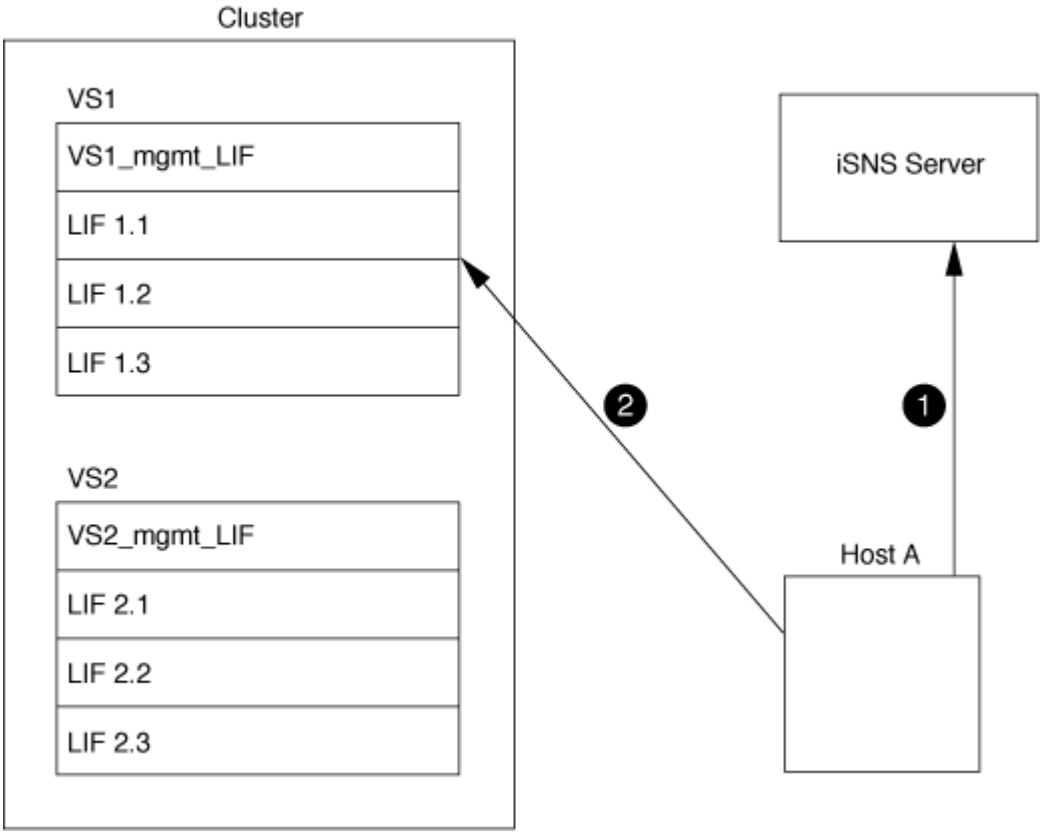
SVM이 iSNS 서버와 상호 작용하는 방식

iSNS 서버는 SVM 관리 LIF를 통해 각 SVM(스토리지 가상 시스템)과 통신합니다. 관리 LIF는 특정 SVM을 위한 iSNS 서비스를 사용하여 모든 iSCSI 대상 노드 이름, 별칭 및 포털 정보를 등록합니다.

다음 예에서는 SVM ""VS1""이 SVM 관리 LIF ""VS1_mgmt_lif""를 사용하여 iSNS 서버에 등록합니다. iSNS 등록 중에 SVM은 SVM 관리 LIF를 통해 모든 iSCSI LIF를 iSNS 서버에 보냅니다. iSNS 등록이 완료되면 iSNS 서버에 ""VS1""에서 iSCSI를 지원하는 모든 LIF 목록이 있습니다. 클러스터에 SVM이 여러 개 포함된 경우 각 SVM은 iSNS 서버에 개별적으로 등록하여 iSNS 서비스를 사용해야 합니다.



다음 예에서는 iSNS 서버가 타겟과의 등록을 완료한 후 호스트 A가 1단계에서 설명한 대로 iSNS 서버를 통해 ""VS1""에 대한 모든 LIF를 검색할 수 있습니다. 호스트 A가 ""VS1""에 대한 LIF 검색을 완료한 후 호스트 A는 2단계에 표시된 ""VS1""에 있는 LIF와 연결을 설정할 수 있습니다. 호스트 A는 관리 LIF가 ""VS2"에 ""VS2""에 ""VS2""에 등록될 때까지 ""VS2""에 있는 LIF를 인식하지 못합니다.



그러나 인터페이스 액세스 목록을 정의하는 경우 호스트는 인터페이스 액세스 목록에 정의된 LIF만 사용하여 타겟에 액세스할 수 있습니다.

iSNS를 처음 구성한 후 SVM 구성 설정이 변경되면 ONTAP에서 iSNS 서버를 자동으로 업데이트합니다.

구성을 변경하는 시간과 ONTAP가 iSNS 서버에 업데이트를 보내는 시간 사이에 몇 분 정도 지연될 수 있습니다. iSNS 서버에서 iSNS 정보를 즉시 업데이트합니다. `vserver iscsi isns update`

iSNS 관리 명령입니다

ONTAP는 iSNS 서비스를 관리하는 명령을 제공합니다.

원하는 작업	이 명령 사용…
iSNS 서비스를 구성합니다	'SVM iSCSI iSNS create'
iSNS 서비스를 시작합니다	가상 iSCSI iSNS 시작
iSNS 서비스를 수정합니다	'SVM iSCSI iSNS modify(iSCSI iSNS 수정)'
iSNS 서비스 구성을 표시합니다	SVM iSCSI iSNS show
등록된 iSNS 정보를 강제로 업데이트합니다	가상 iSCSI iSNS 업데이트
iSNS 서비스를 중지합니다	가상 iSCSI iSNS 중지
iSNS 서비스를 제거합니다	가상 iSCSI iSNS 삭제
명령에 대한 man 페이지를 봅니다	man_command name _

자세한 내용은 각 명령에 대한 man 페이지를 참조하십시오.