



SAN 스토리지 관리

ONTAP 9

NetApp
February 20, 2026

목차

SAN 스토리지 관리	1
SAN 개념	1
iSCSI를 사용한 SAN 프로비저닝	1
iSCSI 서비스 관리	2
FC를 통한 SAN 프로비저닝	8
NVMe를 이용한 SAN 프로비저닝	9
SAN 볼륨	10
SAN 호스트측 공간 관리	15
Igroup 정보	15
igroup에 대해 이니시에이터 WWPN 및 iSCSI 노드 이름을 지정합니다	17
가상화된 SAN 환경을 사용할 때의 이점	17
ESX 호스트의 VMware VAAI 성능을 향상시킵니다	17
SAN 복사 오프로드	18
SAN 관리	22
SAN 프로비저닝	22
NVMe 프로비저닝	32
LUN 관리	44
Igroup 및 portset 관리	56
iSCSI 프로토콜을 관리합니다	62
FC 프로토콜을 관리합니다	69
NVMe 프로토콜 관리	71
FC 어댑터를 사용하여 시스템을 관리합니다	81
모든 SAN 프로토콜에 대한 LIF 관리	88
SAN 프로토콜에 ONTAP 공간 할당을 사용합니다	95
권장되는 볼륨 및 파일 또는 LUN 구성 조합	97
SAN 데이터 보호	102
SAN 환경을 위한 ONTAP 데이터 보호 방법에 대해 알아보십시오	102
ONTAP 스냅샷에서 단일 LUN을 복구합니다	103
ONTAP 스냅샷에서 볼륨의 모든 LUN을 복구합니다	105
ONTAP FlexClone LUN으로 데이터를 보호합니다	106
SAN 환경에서 SnapVault 백업을 구성하고 사용합니다	107
호스트 백업 시스템을 ONTAP에 연결하기 위한 권장 구성입니다	115
호스트 백업 시스템을 사용하여 ONTAP 스토리지 시스템의 LUN을 보호합니다	116
SAN 구성 참조	118
ONTAP SAN 구성에 대해 자세히 알아보십시오	118
iSCSI 구성	118
FC 구성	121
FCoE 구성	128
FC 및 FCoE 조닝	132

ONTAP 시스템 및 비 NetApp 시스템에 연결된 SAN 호스트의 요구 사항	135
MetroCluster 환경의 SAN 구성입니다	135
SAN 호스트 다중 경로에 대한 ONTAP 지원	138
구성 제한	139

SAN 스토리지 관리

SAN 개념

iSCSI를 사용한 SAN 프로비저닝

SAN 환경에서 스토리지 시스템은 스토리지 대상 디바이스가 있는 타겟입니다. iSCSI 및 FC의 경우 스토리지 타겟 디바이스를 LUN(논리 유닛)이라고 합니다. Fibre Channel을 통한 NVMe(Non-Volatile Memory Express)의 경우 스토리지 타겟 디바이스를 네임스페이스라고 합니다.

iSCSI 및 FC용 LUN을 생성하거나 NVMe용 네임스페이스를 생성하여 스토리지를 구성합니다. 그런 다음 iSCSI(Internet Small Computer Systems Interface) 또는 FC(Fibre Channel) 프로토콜 네트워크를 사용하여 호스트에서 LUN 또는 네임스페이스에 액세스합니다.

iSCSI 네트워크에 연결하기 위해 호스트는 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 iSCSI 호스트 버스 어댑터(HBA)를 사용할 수 있습니다.

FC 네트워크에 접속하려면 호스트에 FC HBA 또는 CNA가 필요합니다.

지원되는 FC 프로토콜은 다음과 같습니다.

- FC
- FCoE 를 참조하십시오
- NVMe를 참조하십시오

iSCSI 타겟 노드 네트워크 연결 및 이름

iSCSI 타겟 노드는 다음과 같은 여러 가지 방법으로 네트워크에 연결할 수 있습니다.

- ONTAP에 통합된 소프트웨어를 사용하는 이더넷 인터페이스를 통해.
- 다중 시스템 인터페이스, iSCSI에 사용되는 인터페이스로 SMB 및 NFS와 같은 다른 프로토콜의 트래픽을 전송할 수 있습니다.
- UTA(통합 타겟 어댑터) 또는 CNA(통합 네트워크 어댑터) 사용

모든 iSCSI 노드에는 노드 이름이 있어야 합니다.

iSCSI 노드 이름에 대한 두 형식 또는 형식 지정자는 `_iqn_` 과 `_eui_` 입니다. SVM iSCSI 타겟은 항상 `iqn`형 지정자를 사용합니다. 이니시에이터는 `iqn` 유형 또는 `eui` 유형 지정자를 사용할 수 있습니다.

스토리지 시스템 노드 이름입니다

iSCSI를 실행하는 각 SVM에는 역방향 도메인 이름과 고유한 인코딩 번호를 기반으로 하는 기본 노드 이름이 있습니다.

노드 이름은 다음 형식으로 표시됩니다.

`iqn.1992-08.com.netapp:sn.unique-encoding-number`

다음 예에서는 고유한 인코딩 번호가 있는 스토리지 시스템의 기본 노드 이름을 보여 줍니다.

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

iSCSI용 TCP 포트

iSCSI 프로토콜은 ONTAP에서 TCP 포트 번호 3260을 사용하도록 구성되어 있습니다.

ONTAP는 iSCSI의 포트 번호 변경을 지원하지 않습니다. 포트 번호 3260은 iSCSI 사양의 일부로 등록되었으며 다른 애플리케이션이나 서비스에서 사용할 수 없습니다.

관련 정보

["NetApp 설명서: ONTAP SAN 호스트 구성"](#)

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 **iSCSI**를 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

기존 iSCSI 보안 명령에서는 IP 주소 범위 또는 여러 IP 주소를 사용할 수 있습니다.

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

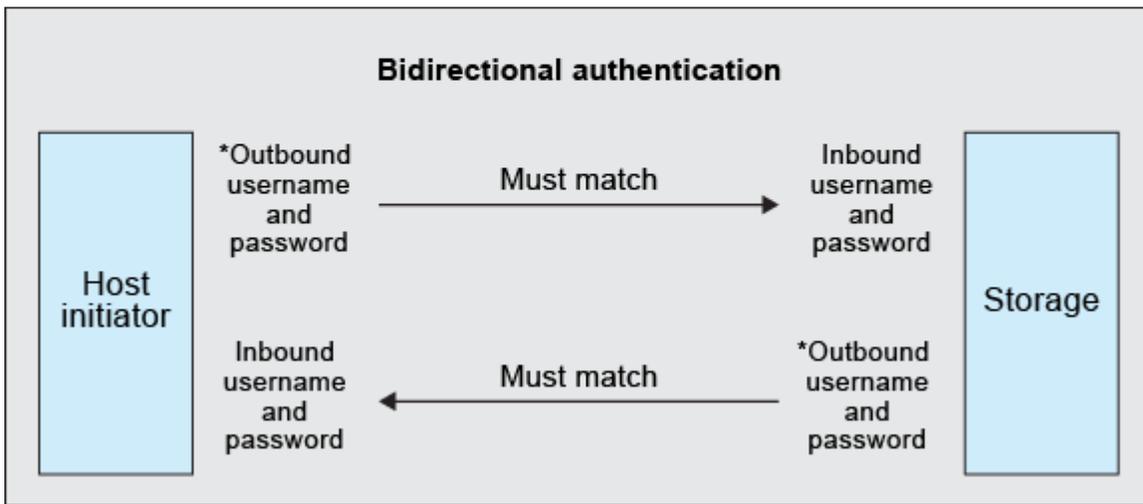
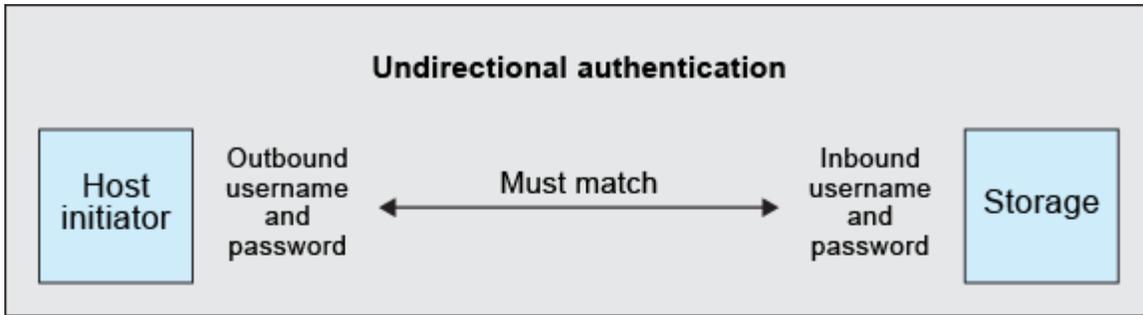
vserver iscsi security remove-initiator-address-range 명령으로 IP 주소 범위 또는 여러 IP 주소를 제거합니다.

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

ONTAP 에서 iSCSI 이니시에이터에 대한 CHAP 인증에 대해 알아보세요.

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.



*The outbound username and password for the host initiator must be different from the outbound username and password for the storage.

인증	아웃바운드	인바운드	성냥?
단방향	호스트 개시자 사용자 이름 및 비밀번호	저장소 사용자 이름 및 비밀번호	반드시 일치해야 함
양방향	호스트 개시자 사용자 이름 및 비밀번호	저장소 사용자 이름 및 비밀번호	반드시 일치해야 함
양방향	저장소 사용자 이름 및 비밀번호	호스트 개시자 사용자 이름 및 비밀번호	반드시 일치해야 함

호스트 이니시에이터의 아웃바운드 사용자 이름과 비밀번호는 스토리지 시스템의 아웃바운드 사용자 이름과 비밀번호와 달라야 합니다.

CHAP 인증 사용에 대한 지침입니다

CHAP 인증을 사용할 때 다음 지침을 따르세요.

- 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.

시스템에서는 null 사용자 이름을 허용하지 않습니다.

- CHAP 암호(암호)는 1 ~ 512바이트입니다.

비밀번호는 16진수 값이나 문자열이 될 수 있습니다. 16진수 값의 경우 "0x" 또는 "0X" 접두사를 붙여 값을 입력해야 합니다.

이 시스템은 널 비밀번호를 허용하지 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.

추가적인 제한 사항에 대해서는 개시자의 문서를 참조하세요.

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.

ONTAP의 iSNS(인터넷 저장소 이름 서비스)입니다

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.

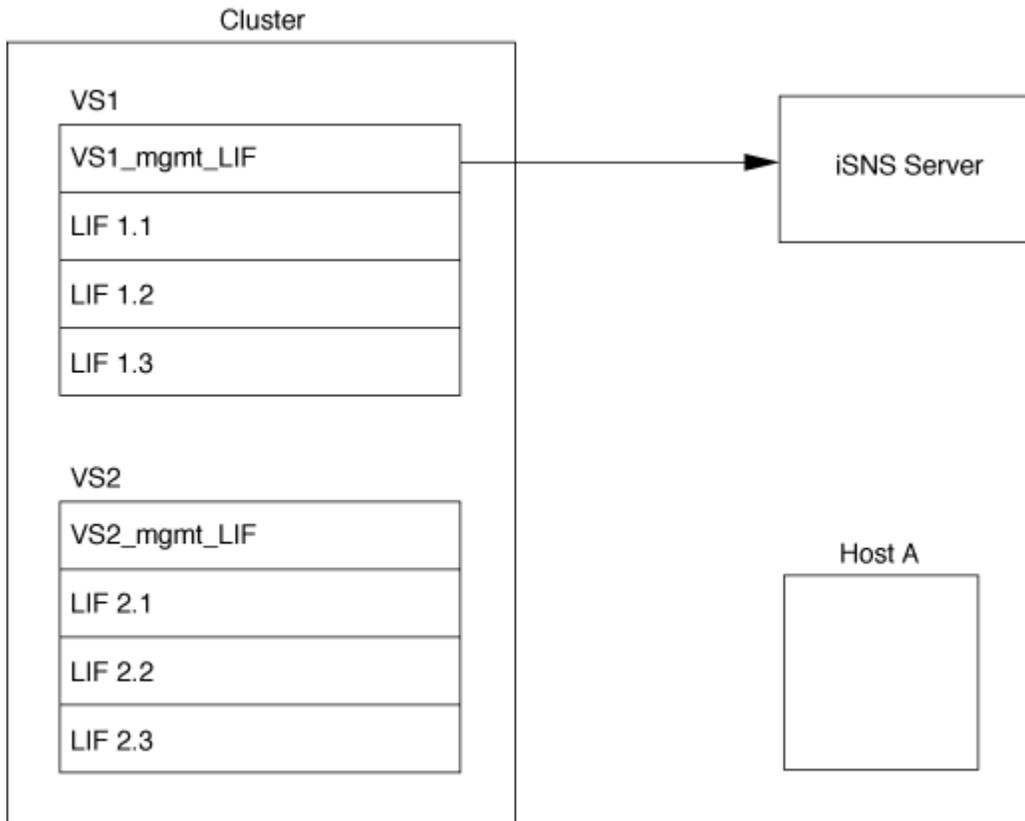
iSNS 프로토콜을 사용하면 IP 스토리지 네트워크에서 iSCSI 디바이스를 자동으로 검색하고 관리할 수 있습니다. iSCSI 이니시에이터는 iSNS 서버를 쿼리하여 iSCSI 타겟 디바이스를 검색할 수 있습니다.

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

SVM이 iSNS 서버와 상호 작용하는 방식

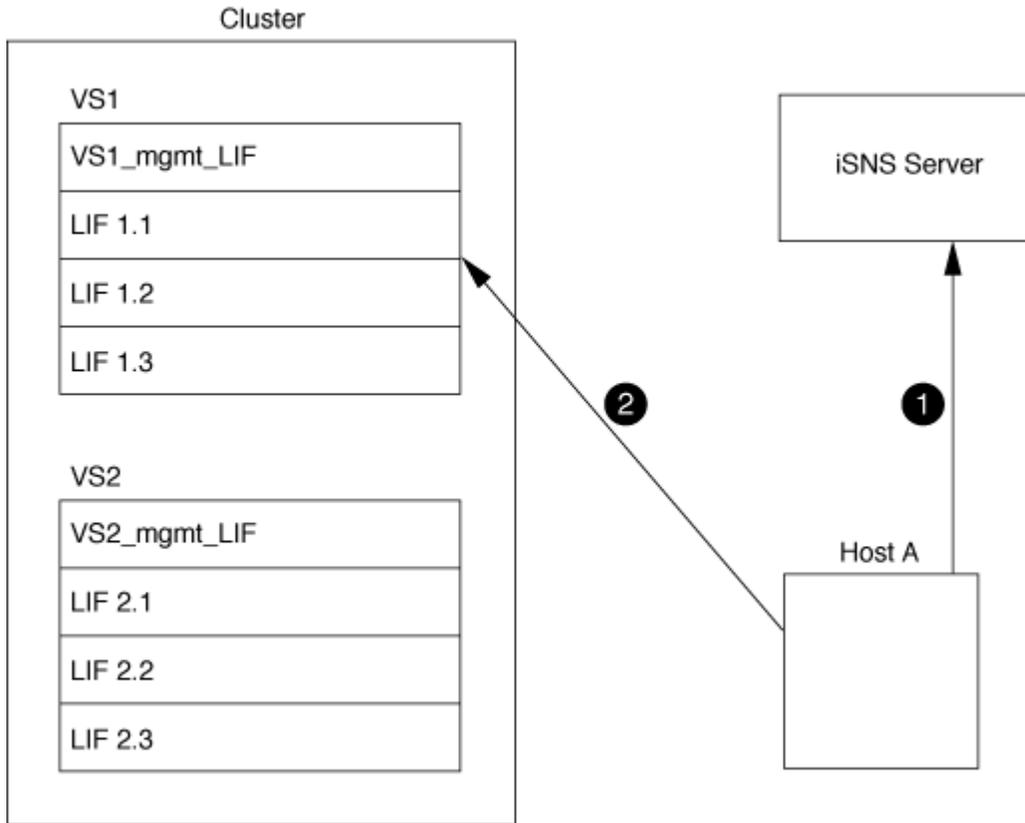
iSNS 서버는 SVM 관리 LIF를 통해 각 SVM(스토리지 가상 시스템)과 통신합니다. 관리 LIF는 특정 SVM을 위한 iSNS 서비스를 사용하여 모든 iSCSI 대상 노드 이름, 별칭 및 포털 정보를 등록합니다.

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`. 에 대한 자세한 내용은 `vserver iscsi isns update` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

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 _

에 대한 자세한 내용은 `vserver iscsi isns` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

FC를 통한 SAN 프로비저닝

ONTAP에서 FC SAN을 구축하는 방법을 이해하는 데 필요한 중요한 개념을 알아야 합니다.

FC 타겟 노드가 네트워크에 연결되는 방법

스토리지 시스템과 호스트에는 케이블이 있는 FC 스위치에 연결할 수 있는 어댑터가 있습니다.

노드가 FC SAN에 연결되면 각 SVM은 스위치 패브릭 이름 서비스에 LIF의 WWPN(World Wide Port Name)을 등록합니다. SVM의 WWNN과 각 LIF의 WWPN은 ONTAP에서 자동으로 할당됩니다.



FC를 사용하는 호스트의 노드에 대한 직접 연결은 지원되지 않습니다. NPIV가 필요하며 이 경우 스위치를 사용해야 합니다. iSCSI 세션을 사용하면 네트워크 라우팅 또는 직접 연결 중 하나의 연결에서 통신할 수 있습니다. 그러나 이러한 두 가지 방법은 모두 ONTAP에서 지원됩니다.

FC 노드의 식별 방법

FC로 구성된 각 SVM은 WWNN(Worldwide Node Name)으로 식별됩니다.

WWPN 사용 방법

WWPN은 FC를 지원하도록 구성된 SVM에서 각 LIF를 식별합니다. 이러한 LIF는 클러스터 내 각 노드에서 물리적 FC 포트를 사용합니다. 이 포트는 노드에서 FC 또는 FCoE로 구성된 FC 타겟 카드, UTA 또는 UTA2 포트일 수 있습니다.

- 이니시에이터 그룹 생성

호스트 HBA의 WWPN은 이니시에이터 그룹(igroup)을 생성하는 데 사용됩니다. igroup은 특정 LUN에 대한 호스트 액세스를 제어하는 데 사용됩니다. FC 네트워크에서 이니시에이터의 WWPN 컬렉션을 지정하여 igroup을 생성할 수 있습니다. 스토리지 시스템의 LUN을 igroup에 매핑할 때 해당 그룹의 모든 이니시에이터가 해당 LUN에 액세스할 수 있도록 허용할 수 있습니다. 호스트의 WWPN이 LUN에 매핑된 igroup에 없는 경우 해당 호스트는 LUN에 액세스할 수 없습니다. 즉, LUN이 해당 호스트의 디스크로 표시되지 않습니다.

또한 포트 세트를 생성하여 특정 타겟 포트에만 LUN을 표시할 수 있습니다. 포트 세트는 FC 타겟 포트 그룹으로 구성됩니다. igroup을 포트 세트에 바인딩할 수 있습니다. igroup 내의 모든 호스트는 포트 세트의 타겟 포트에 연결하여 LUN에 액세스할 수 있습니다.

- FC LIF의 고유 식별

WWPN은 각 FC 논리 인터페이스를 고유하게 식별합니다. 호스트 운영 체제는 WWNN과 WWPN을 함께 사용하여

SVM 및 FC LIF를 식별합니다. 일부 운영 체제에서는 LUN이 호스트에서 동일한 타겟 ID에 표시되도록 영구 바인딩이 필요합니다.

전세계적인 이름 지정 작동 방식

전 세계 이름은 ONTAP에서 순차적으로 생성됩니다. 그러나 ONTAP에서 할당된 방식 때문에 비순차적 순서로 할당된 것처럼 보일 수 있습니다.

각 어댑터에는 사전 구성된 WWPN 및 WWNN이 있지만 ONTAP는 이러한 사전 구성된 값을 사용하지 않습니다. 대신, ONTAP는 온보드 이더넷 포트의 MAC 주소를 기반으로 자체 WWPN 또는 WWNs를 할당합니다.

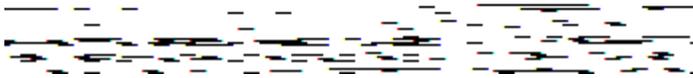
다음과 같은 이유로 전 세계 이름이 지정되면 비순차적인 것으로 보일 수 있습니다.

- 전 세계 이름은 클러스터의 모든 노드 및 SVM(스토리지 가상 머신)에 할당됩니다.
- 전 세계적으로 확보된 이름은 재활용되고 사용 가능한 이름 풀에 다시 추가됩니다.

FC 스위치의 식별 방법

파이버 채널 스위치에는 장치 자체를 위한 WWNN(Worldwide Node Name)과 각 포트에 대한 WWPN(Worldwide Port Name)이 하나씩 있습니다.

예를 들어, 다음 다이어그램에서는 16포트 Brocade 스위치의 각 포트에 WWPN을 할당하는 방법을 보여 줍니다. 특정 스위치에 대한 포트 번호 지정 방법에 대한 자세한 내용은 해당 스위치에 대해 공급업체에서 제공한 설명서를 참조하십시오.



포트 * 0 *, WWPN 20: **00**:00:60:69:51:06:B4

포트 * 1 *, WWPN 20: **01**:00:60:69:51:06:B4

포트 * 14 *, WWPN 20: **0E**:00:60:69:51:06:B4

포트 * 15 *, WWPN 20: **0f**:00:60:69:51:06:B4

NVMe를 이용한 SAN 프로비저닝

ONTAP 9.4부터는 SAN 환경에서 NVMe/FC가 지원됩니다. 스토리지 관리자는 NVMe/FC를 사용하여 네임스페이스와 서브시스템을 프로비저닝한 다음 네임스페이스를 하위 시스템에 매핑할 수 있습니다. 이는 LUN이 FC 및 iSCSI의 igroup에 용량 할당 및 매핑된 방식과 비슷합니다.

NVMe 네임스페이스는 논리 블록으로 포맷될 수 있는 비휘발성 메모리의 양입니다. 네임스페이스는 FC 및 iSCSI 프로토콜을 위한 LUN과 동일하며 NVMe 서브시스템은 igroup과 유사합니다. NVMe 하위 시스템을 이니시에이터와 연결할 수 있으므로 연결된 이니시에이터가 하위 시스템 내의 네임스페이스에 액세스할 수 있습니다.



기능에서도 유사하지만, NVMe 네임스페이스는 LUN에서 지원되는 모든 기능을 지원하지 않습니다.

ONTAP 9.5부터 NVMe를 사용한 호스트 데이터 액세스를 지원하려면 라이선스가 필요합니다. ONTAP 9.4에서 NVMe를 사용하는 경우 ONTAP 9.5로 업그레이드한 후 라이선스를 취득하기 위한 90일 유예 기간이 제공됩니다. 이 있는 "ONTAP 1 을 참조하십시오" 경우 NVMe 라이선스가 포함됩니다. 다음 명령을 사용하여 라이선스를 설정할 수 있습니다.

```
'System license add-license-code_NVMe_license_key_'
```

관련 정보

["NetApp 기술 보고서 4684: NVMe/FC를 사용하여 최신 SAN 구현 및 구성"](#)

SAN 볼륨

SAN 볼륨 개요 정보

ONTAP는 일반 프로비저닝, 씬 프로비저닝 및 반일반 프로비저닝의 세 가지 기본 볼륨 프로비저닝 옵션을 제공합니다. 각 옵션은 볼륨 공간과 ONTAP 블록 공유 기술의 공간 요구 사항을 관리하는 다양한 방법을 사용합니다. 옵션의 작동 방식을 이해하면 환경에 가장 적합한 옵션을 선택할 수 있습니다.



SAN LUN과 NAS 공유를 동일한 FlexVol 볼륨에 배치하는 것은 권장되지 않습니다. SAN LUN을 위해 특별히 별도의 FlexVol 볼륨을 프로비저닝해야 하며 NAS 공유에 별도의 FlexVol 볼륨을 프로비저닝해야 합니다. 이렇게 하면 관리 및 복제 구축이 간소화되고 FlexVol 볼륨이 Active IQ Unified Manager(이전의 OnCommand Unified Manager)에서 지원되는 방식과 유사점이 있습니다.

볼륨에 대한 씬 프로비저닝

씬 프로비저닝된 볼륨이 생성된 경우 ONTAP는 볼륨이 생성될 때 추가 공간을 예약하지 않습니다. 볼륨에 데이터가 기록될 때 볼륨은 쓰기 작업을 수용하기 위해 Aggregate에서 필요한 스토리지를 요청합니다. 씬 프로비저닝된 볼륨을 사용하면 애그리게이트를 오버 커밋할 수 있으므로 애그리게이트에 여유 공간이 부족할 때 볼륨이 필요한 공간을 확보할 수 없게 됩니다.

'-space-보증' 옵션을 '없음'으로 설정하여 씬 프로비저닝된 FlexVol 볼륨을 만듭니다.

볼륨에 대한 일반 프로비저닝입니다

썩 프로비저닝된 볼륨이 생성되면 ONTAP는 언제든지 볼륨의 블록을 쓸 수 있도록 애그리게이트에 충분한 스토리지를 남겨 둡니다. 일반 프로비저닝을 사용하도록 볼륨을 구성할 경우 압축 및 중복제거와 같은 ONTAP 스토리지 효율성 기능을 사용하여 대규모 초기 스토리지 요구사항을 상쇄할 수 있습니다.

'-space-slo'(서비스 수준 목표) 옵션을 'thick'으로 설정하여 썩 프로비저닝된 FlexVol 볼륨을 만듭니다.

볼륨에 반썩 프로비저닝

반썩 프로비저닝을 사용하는 볼륨이 생성된 경우 ONTAP에서는 애그리게이트에서 볼륨 크기를 고려하여 스토리지 공간을 별도로 설정합니다. 블록 공유 기술에서 블록을 사용하고 있기 때문에 볼륨에 여유 공간이 부족해지면 ONTAP이 보호 데이터 오브젝트(스냅샷 및 FlexClone 파일 및 LUN)를 삭제하여 보유 중인 공간을 확보하도록 시도합니다. ONTAP가 덮어쓰기 작업에 필요한 공간과 보조를 맞출 수 있을 만큼 보호 데이터 객체를 빠르게 삭제할 수 있는 한 쓰기 작업은 계속 성공합니다. 이를 '최선 노력'이라고 합니다.

- 참고: * 다음 기능은 반씩 프로비저닝을 사용하는 볼륨에서 지원되지 않습니다.
- 중복제거, 압축, 컴팩션과 같은 스토리지 효율성 기술
- Microsoft ODX(Offloaded Data Transfer)

semi-thick-provisioned FlexVol 볼륨은 '-space-slo'(서비스 수준 목표) 옵션을 'sEMI-thick'으로 설정하여 생성합니다.

공간 예약 파일 및 LUN과 함께 사용

공간 예약 파일 또는 LUN은 생성 시 스토리지가 할당되는 파일입니다. 역사적으로 NetApp은 공간 예약이 사용되지 않는 LUN(비공간 예약 LUN)을 지칭하기 위해 ""씬 프로비저닝된 LUN""이라는 용어를 사용했습니다.

- 참고: * 비공간 예약 파일은 일반적으로 ""씬 프로비저닝 파일""이라고 하지 않습니다.

다음 표에는 세 가지 볼륨 프로비저닝 옵션을 공간 예약 파일 및 LUN과 함께 사용하는 방법의 주요 차이점이 요약되어 있습니다.

볼륨 프로비저닝	LUN/파일 공간 예약	덮어쓰기	보호 데이터 ²	스토리지 효율성 ³
두껍게	지원	1을(를) 보장합니다	NetApp이 보장합니다	지원
얇음	효과 없음	없음	NetApp이 보장합니다	지원
약간 두껍습니다	지원	최선의 노력 ¹	최선을 다하세요	지원되지 않습니다

• 참고 *

1. 덮어쓰기 보장 또는 최선의 덮어쓰기 보장을 제공하려면 LUN 또는 파일에 공간 예약을 설정해야 합니다.
2. 보호 데이터에는 스냅샷, 자동 삭제로 표시된 FlexClone 파일 및 LUN(백업 클론)이 포함됩니다.
3. 스토리지 효율성에는 중복제거, 압축, 자동 삭제로 표시되지 않은 모든 FlexClone 파일 및 LUN(활성 클론), FlexClone 하위 파일(복사본 오프로드 사용)이 포함됩니다.

SCSI 씬 프로비저닝된 LUN 지원

ONTAP는 T10 SCSI 씬 프로비저닝 LUN과 NetApp 씬 프로비저닝 LUN을 지원합니다. T10 SCSI 씬 프로비저닝을 사용하면 호스트 애플리케이션에서 LUN 공간 재확보, 블록 환경의 LUN 공간 모니터링 기능 등 SCSI 기능을 지원할 수 있습니다. T10 SCSI 씬 프로비저닝은 SCSI 호스트 소프트웨어에서 지원해야 합니다.

ONTAP의 pace-allocation 설정을 사용하면 LUN에서 T10 씬 프로비저닝 지원을 활성화/비활성화할 수 있습니다. ONTAP의 pace-allocation enable 설정을 사용하여 LUN에 T10 SCSI 씬 프로비저닝을 활성화합니다.

그만큼 [-space-allocation {enabled|disabled}] 에서 명령 "ONTAP 명령 참조입니다" T10 씬 프로비저닝에 대한 지원을 활성화/비활성화하고 LUN에서 T10 SCSI 씬 프로비저닝을 활성화하는 방법에 대한 자세한 정보가 있습니다.

볼륨 프로비저닝 옵션을 구성합니다

씬 프로비저닝, 일반 프로비저닝 또는 반씩 프로비저닝을 위해 볼륨을 구성할 수 있습니다.

이 작업에 대해

'-space-slo' 옵션을 'thick'으로 설정하면 다음과 같은 이점이 있습니다.

- 전체 볼륨이 Aggregate에 사전 할당됩니다. 볼륨의 '-space-보증' 옵션을 구성하려면 'volume create' 또는 'volume modify' 명령을 사용할 수 없습니다.
- 덮어쓰기에 필요한 공간의 100%가 예약됩니다. 볼륨의 '-fractional-reserve' 옵션을 구성하려면 'volume modify' 명령을 사용할 수 없습니다.

'-space-slo' 옵션을 'EMI-thick'으로 설정하면 다음과 같은 이점이 있습니다.

- 전체 볼륨이 Aggregate에 사전 할당됩니다. 볼륨의 '-space-보증' 옵션을 구성하려면 'volume create' 또는 'volume modify' 명령을 사용할 수 없습니다.
- 덮어쓰기용으로 예약된 공간이 없습니다. 'volume modify' 명령을 사용하여 볼륨의 '-fractional-reserve' 옵션을 구성할 수 있습니다.
- 스냅샷 자동 삭제가 설정되었습니다.

단계

1. 볼륨 프로비저닝 옵션 구성:

```
'volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-space-slo none|thick|semi-thick-space-보증 없음|볼륨'
```

'-space-보증' 옵션은 AFF 시스템과 비 AFF DP 볼륨에 대해 기본적으로 '없음'으로 설정됩니다. 그렇지 않으면 볼륨(volume)으로 기본 설정됩니다. 기존 FlexVol 볼륨의 경우 'volume modify' 명령을 사용하여 프로비저닝 옵션을 구성합니다.

다음 명령은 씬 프로비저닝을 위해 SVM VS1 에서 vol1을 구성합니다.

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee none
```

다음 명령을 실행하면 일반 프로비저닝을 위해 SVM VS1 vol1에 대해 vol1이 구성됩니다.

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

다음 명령을 실행하면 반씩 프로비저닝을 위해 SVM VS1 vol1에 대해 vol1이 구성됩니다.

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-thick
```

SAN 볼륨 구성 옵션

LUN을 포함하는 볼륨에서 다양한 옵션을 설정해야 합니다. 볼륨 옵션을 설정하는 방법에 따라 볼륨의 LUN에서 사용할 수 있는 공간이 결정됩니다.

자동 확장

자동 행을 활성화 또는 비활성화할 수 있습니다. 이 기능을 사용하도록 설정하면 ONTAP에서 볼륨 크기를 미리 결정한 최대 크기까지 자동으로 늘릴 수 있습니다. 볼륨의 자동 증가를 지원하려면 포함된 애그리게이트에 사용 가능한 공간이 있어야 합니다. 따라서 자동 확장 기능을 사용하도록 설정한 경우 포함된 애그리게이트의 여유 공간을 모니터링하고 필요 시 더 많은 공간을 추가해야 합니다.

스냅샷 생성을 지원하기 위해 자동 확장을 트리거할 수 없습니다. 스냅샷을 생성하려고 하는데 볼륨에 공간이 부족하면 자동 증가가 설정된 경우에도 스냅샷 생성이 실패합니다.

자동 확장 기능을 비활성화하면 볼륨 크기는 동일하게 유지됩니다.

자동 축소

자동 축소를 사용하거나 사용하지 않도록 설정할 수 있습니다. 자동 축소를 사용하도록 설정하면 ONTAP에서 볼륨에서 사용된 공간 양이 미리 정해진 임계값을 줄일 때 볼륨의 전체 크기를 자동으로 줄일 수 있습니다. 따라서 볼륨을 트리거하여 사용되지 않는 여유 공간을 자동으로 릴리즈하여 스토리지 효율성이 향상됩니다.

스냅샷 자동 삭제

스냅샷 자동 삭제는 다음 중 하나가 발생하면 스냅샷을 자동으로 삭제합니다.

- 볼륨이 거의 꽉 찼습니다.
- 스냅샷 예약 공간이 거의 가득 찼습니다.
- 덮어쓰기 예약 공간이 가득 찼습니다.

스냅샷을 오래된 스냅샷에서 최신 스냅샷으로 또는 최신 스냅샷에서 오래된 스냅샷으로 삭제하도록 스냅샷 자동 삭제를 구성할 수 있습니다. 스냅샷 자동 삭제는 클론 복제된 볼륨 또는 LUN의 스냅샷에 연결된 스냅샷은 삭제하지 않습니다.

볼륨에 추가 공간이 필요하고 자동 확장 및 스냅샷 자동 삭제를 모두 사용하도록 설정한 경우, 기본적으로 ONTAP은 먼저 자동 확장을 트리거하여 필요한 공간을 확보하려고 시도합니다. 자동 확장을 통해 충분한 공간을 확보하지 못하면 스냅샷 자동 삭제가 트리거됩니다.

스냅샷 예비 공간입니다

스냅샷 예비 공간은 스냅샷용으로 예약된 볼륨의 공간 크기를 정의합니다. 스냅샷 예비 공간에 할당된 공간은 다른 용도로 사용할 수 없습니다. 스냅샷 예비 공간에 할당된 모든 공간이 사용되는 경우 스냅샷에서 볼륨의 추가 공간을 사용하기 시작합니다.

SAN 환경에서 볼륨을 이동하기 위한 요구사항

LUN 또는 네임스페이스가 포함된 볼륨을 이동하기 전에 특정 요구 사항을 충족해야 합니다.

- 하나 이상의 LUN이 포함된 볼륨의 경우 클러스터의 각 노드에 연결되는 LUN(LIF)당 경로가 2개 이상 있어야 합니다.

따라서 단일 장애 지점이 발생하지 않으며 시스템에서 구성 요소 장애를 극복할 수 있습니다.

- 네임스페이스가 포함된 볼륨의 경우 클러스터는 ONTAP 9.6 이상을 실행해야 합니다.

ONTAP 9.5를 실행하는 NVMe 구성에는 볼륨 이동이 지원되지 않습니다.

부분 예약 설정을 위한 고려 사항

lun 덮어쓰기 예약 _이라고도 하는 분할 예약을 통해 FlexVol 볼륨의 공간 예약 LUN 및 파일에 대한 덮어쓰기 예약 기능을 해제할 수 있습니다. 이렇게 하면 스토리지 활용률을 최대화하는 데 도움이 될 수 있지만 공간 부족으로 인한 쓰기 작업 실패로 인해 환경이 부정적인 영향을 받는 경우 이러한 구성에서 부과하는 요구사항을 이해해야 합니다.

분할 예약 설정은 백분율로 표현되며 유효한 값은 0, 100%입니다. 분할 예약 설정은 볼륨의 속성입니다.

부분 예약 공간을 '0'으로 설정하면 스토리지 활용률이 증가합니다. 그러나 볼륨 보장이 "볼륨"으로 설정되어 있더라도 볼륨에 있는 데이터에 액세스하는 응용 프로그램은 사용 가능한 공간이 부족할 경우 데이터 중단을 경험할 수 있습니다. 그러나 적절한 볼륨 구성 및 사용을 통해 쓰기 실패 가능성을 최소화할 수 있습니다. ONTAP은 다음 요구 사항 중 _ALL_ 이 충족되면 부분 예약 공간이 '0'으로 설정된 볼륨에 대해 "최선 노력" 쓰기 보장을 제공합니다.

- 중복 제거가 사용되지 않습니다
- 압축이 사용되지 않습니다
- FlexClone 하위 파일을 사용하지 않습니다
- 모든 FlexClone 파일과 FlexClone LUN이 자동으로 삭제됩니다

이 설정은 기본 설정이 아닙니다. 생성 시 또는 FlexClone 파일 또는 FlexClone LUN을 생성한 후에 이를 수정하여 자동 삭제를 명시적으로 설정해야 합니다.

- ODX 및 FlexClone 복사 오프로드가 사용되지 않습니다
- 볼륨 보장이 '볼륨'으로 설정되어 있습니다
- 파일 또는 LUN 공간 예약이 '사용'되었습니다
- 볼륨 스냅샷 예비 공간이 '0'으로 설정되어 있습니다
- 볼륨 스냅샷 자동 삭제는 의 약정 수준 destroy, 제거 목록 lun_clone, vol_clone, cifs_share, file_clone, sfsr 및 트리거로 volume 이루어집니다 enabled

이 설정은 필요한 경우 FlexClone 파일 및 FlexClone LUN도 삭제되도록 합니다.

변경률이 높은 경우 드물지만 스냅샷 자동 삭제가 지연되어 위에서 요구하는 모든 구성 설정을 사용 중이더라도 볼륨의 공간이 부족해질 수 있습니다.

또한 필요에 따라 볼륨 자동 확장 기능을 사용하여 볼륨 스냅샷이 자동으로 삭제될 가능성을 줄일 수 있습니다. 자동 확장 기능을 사용하도록 설정한 경우 연결된 애그리게이트의 여유 공간을 모니터링해야 합니다. Aggregate가 가득 차서 볼륨 증가를 막을 수 없을 경우, 볼륨의 여유 공간이 고갈되면 더 많은 스냅샷이 삭제될 수 있습니다.

위 구성 요구사항을 모두 충족하지 못할 경우 볼륨에서 공간이 부족하지 않도록 해야 하는 경우 볼륨의 분할 예약 설정을 '100'으로 설정해야 합니다. 이를 위해서는 공간을 미리 확보해야 하지만, 위에 나열된 기술이 사용 중일 때도 데이터 수정 작업이 성공하도록 보장합니다.

분할 예약 설정의 기본값 및 허용되는 값은 볼륨의 보장에 따라 다릅니다.

볼륨 보장	기본 분할 예약	허용되는 값
볼륨	100	0, 100

볼륨 보장	기본 분할 예약	허용되는 값
없음	0	0, 100

SAN 호스트측 공간 관리

썬 프로비저닝된 환경에서 호스트 측 공간 관리는 호스트 파일 시스템에서 확보된 스토리지 시스템의 공간 관리 프로세스를 완료합니다.

호스트 파일 시스템에는 새 데이터를 저장하는 데 사용할 수 있는 블록과 덮어쓰지 않아야 하는 유효한 데이터가 들어 있는 블록을 추적하는 메타데이터가 포함되어 있습니다. 이 메타데이터는 LUN 또는 네임스페이스 내에 저장됩니다. 호스트 파일 시스템에서 파일이 삭제되면 파일 시스템 메타데이터가 업데이트되어 해당 파일의 블록을 여유 공간으로 표시합니다. 그런 다음 새로 확보된 블록을 포함하도록 총 파일 시스템 여유 공간이 다시 계산됩니다. 스토리지 시스템에서 이러한 메타데이터 업데이트는 호스트에서 수행하는 다른 쓰기와 다르지 않습니다. 따라서 스토리지 시스템에서 삭제된 내용이 있는지 인식하지 못합니다.

이렇게 하면 호스트에서 보고된 사용 가능한 공간의 양과 기본 스토리지 시스템에서 보고하는 사용 가능한 공간의 양이 서로 일치하지 않습니다. 예를 들어, 스토리지 시스템에서 호스트에 할당된 새로 프로비저닝된 200GB LUN이 있다고 가정합니다. 호스트와 스토리지 시스템 모두 200GB의 사용 가능한 공간을 보고합니다. 그런 다음 호스트는 100GB 데이터를 씁니다. 이때 호스트 및 스토리지 시스템 모두 100GB 사용 공간과 100GB 사용 안 된 공간을 보고합니다.

그런 다음 호스트에서 50GB의 데이터를 삭제합니다. 이때 호스트는 50GB의 사용된 공간과 150GB의 사용되지 않은 공간을 보고합니다. 그러나 스토리지 시스템은 100GB 사용 공간과 100GB의 미사용 공간을 보고합니다.

호스트 측 공간 관리는 다양한 방법을 사용하여 호스트와 스토리지 시스템 간의 공간 차이를 조정합니다.

SnapCenter를 통한 호스트 관리 단순화

SnapCenter 소프트웨어를 사용하면 iSCSI 및 FC 스토리지와 관련된 일부 관리 및 데이터 보호 작업을 단순화할 수 있습니다. SnapCenter는 Windows 및 UNIX 호스트용 선택적 관리 패키지입니다.

SnapCenter 소프트웨어를 사용하면 여러 스토리지 시스템에 분산될 수 있는 스토리지 풀에서 가상 디스크를 손쉽게 생성하고 스토리지 프로비저닝 작업을 자동화하고 호스트 데이터와 일치하는 스냅샷에서 스냅샷 및 클론을 생성하는 프로세스를 단순화할 수 있습니다.

에 대한 자세한 내용은 NetApp 제품 설명서를 참조하십시오 **"SnapCenter"**.

관련 링크

["SAN 프로토콜에 ONTAP 공간 할당을 사용합니다"](#)

Igroup 정보

이니시에이터 그룹(igroup)은 FC 프로토콜 호스트 WWPN 또는 iSCSI 호스트 노드 이름의 테이블입니다. igroup을 정의하고 LUN에 매핑하여 LUN에 액세스할 수 있는 이니시에이터를 제어할 수 있습니다.

일반적으로 호스트의 모든 이니시에이터 포트 또는 소프트웨어 이니시에이터가 LUN에 액세스할 수 있도록 합니다. 다중 경로 소프트웨어를 사용하거나 클러스터 호스트를 사용하는 경우, 각 클러스터 호스트의 각 이니시에이터 포트 또는 소프트웨어 이니시에이터는 동일한 LUN에 대한 이중 경로를 필요로 합니다.

LUN을 생성하기 전이나 후에 LUN에 액세스할 수 있는 이니시에이터를 지정하는 igroup을 생성할 수 있지만 LUN을 igroup에 매핑하기 전에 igroup을 생성해야 합니다.

이니시에이터 그룹에 여러 이니시에이터가 있을 수 있으며, 여러 igroup이 동일한 이니시에이터를 포함할 수 있습니다. 그러나 동일한 이니시에이터가 있는 여러 igroup에 LUN을 매핑할 수 없습니다. 이니시에이터는 서로 다른 상치성 igroup의 구성원일 수 없습니다.

igroup에서 LUN 액세스를 제공하는 방법의 예

여러 igroup을 생성하여 호스트에 사용할 수 있는 LUN을 정의할 수 있습니다. 예를 들어, 호스트 클러스터가 있는 경우 igroup을 사용하여 특정 LUN이 클러스터의 한 호스트에만 또는 클러스터의 모든 호스트에 표시되는지 확인할 수 있습니다.

다음 표에서는 4개의 igroup이 스토리지 시스템에 액세스하는 4개의 서로 다른 호스트에 대한 LUN에 액세스하는 방법을 보여 줍니다. 클러스터 호스트(Host3 및 Host4)는 모두 동일한 igroup(Group3)의 구성원이며 이 igroup에 매핑된 LUN에 액세스할 수 있습니다. group4라는 igroup에는 파트너가 볼 수 없는 로컬 정보를 저장하기 위한 Host4의 WWPN이 포함되어 있습니다.

HBA WWPN, IQN 또는 EUI가 포함된 호스트	igroup	WWPN, IQN, EUI가 igroup에 추가되었습니다	LUN이 igroup에 매핑되어 있습니다
호스트1, 단일 경로(iSCSI 소프트웨어 이니시에이터) iqn.1991-05.com.microsoft:host1	그룹1	iqn.1991-05.com.microsoft:host1	'/vol/vol2/lun1'
Host2, 다중 경로(HBA 2개) 10:00:00:00:C9:2b:6b:3c 10:00:00:00:C9:2b:02:3c	그룹2	10:00:00:00:C9:2b:6b:3c 10:00:00:00:C9:2b:02:3c	'/vol/vol2/lun2'
호스트 3, 다중 경로, 호스트 4로 클러스터링되었습니다 10:00:00:00:C9:2b:32:1b 10:00:00:00:C9:2b:41:02	그룹3	10:00:00:00:C9:2b:32:1b 10:00:00:00:C9:2b:41:02 10:00:00:00:C9:2b:51:2c 10:00:00:00:C9:2b:47:A2	'/vol/vol2/qtree1/lun3'
Host4, multipath, 클러스터링됨(Host3에는 표시되지 않음) 10:00:00:00:C9:2b:51:2c 10:00:00:00:C9:2b:47:A2	그룹4	10:00:00:00:C9:2b:51:2c 10:00:00:00:C9:2b:47:A2	'/vol/vol2/qtree2/lun4"/vol/vol2/qtree1/lun5'

igroup에 대해 이니시에이터 WWPN 및 iSCSI 노드 이름을 지정합니다

igroup을 생성할 때 이니시에이터의 iSCSI 노드 이름 및 WWPN을 지정하거나 나중에 추가할 수 있습니다. LUN을 생성할 때 이니시에이터 iSCSI 노드 이름과 WWPN을 지정하도록 선택한 경우 나중에 필요에 따라 제거할 수 있습니다.

Host Utilities 설명서의 지침에 따라 WWPN을 얻고 특정 호스트와 연결된 iSCSI 노드 이름을 찾습니다. ESX 소프트웨어를 실행하는 호스트의 경우 Virtual Storage Console을 사용합니다.

가상화된 SAN 환경을 사용할 때의 이점

SVM(Storage Virtual Machine)과 LIF를 사용하여 가상화 환경을 구축하면 클러스터의 모든 노드로 SAN 환경을 확장할 수 있습니다.

- 분산 관리

SVM의 모든 노드에 로그인하여 클러스터의 모든 노드를 관리할 수 있습니다.

- 데이터 액세스 증가

MPIO 및 ALUA를 사용하면 SVM을 위한 모든 활성 iSCSI 또는 FC LIF를 통해 데이터에 액세스할 수 있습니다.

- LUN 액세스를 제어합니다

SLM 및 포트 세트를 사용하는 경우 이니시에이터가 LUN에 액세스하는 데 사용할 수 있는 LIF를 제한할 수 있습니다.

ESX 호스트의 VMware VAAI 성능을 향상시킵니다

ONTAP는 ESX 호스트가 ESX 4.1 이상을 실행하는 경우 특정 VMware VAAI(vStorage APIs for Array Integration) 기능을 지원합니다. 이러한 기능은 ESX 호스트에서 스토리지 시스템으로 작업을 오프로드하고 네트워크 처리량을 늘리는 데 도움이 됩니다. ESX 호스트는 올바른 환경에서 자동으로 기능을 활성화합니다.

VAAI 기능은 다음 SCSI 명령을 지원합니다.

- "extended_copy"

이 기능을 사용하면 호스트가 데이터 전송에 참여하지 않고도 LUN 간 또는 LUN 내에서 데이터 전송을 시작할 수 있습니다. 따라서 ESX CPU 주기가 단축되고 네트워크 처리량이 증가합니다. "복사 오프로드"라고도 하는 확장된 복사 기능은 가상 머신의 클론 생성과 같은 시나리오에서 사용됩니다. ESX 호스트에서 호출하면 복제 오프로드 기능은 호스트 네트워크를 통해 이동하는 대신 스토리지 시스템 내의 데이터를 복제합니다. Copy Offload는 다음과 같은 방법으로 데이터를 전송합니다.

- 하나의 LUN 내에서

- 볼륨 내의 LUN 간

- 스토리지 가상 시스템(SVM) 내의 서로 다른 볼륨에 있는 LUN 간

- 클러스터 내의 서로 다른 SVM에 있는 LUN 간에 이 기능을 호출할 수 없는 경우 ESX 호스트는 복사 작업에

표준 읽기 및 쓰기 명령을 자동으로 사용합니다.

- 같은 글씨를 쓰십시오

이 기능은 0과 같은 반복된 패턴을 스토리지 배열에 쓰는 작업을 오프로드합니다. ESX 호스트는 파일 채우기 0과 같은 작업에서 이 기능을 사용합니다.

- 비교 및 쓰기

이 기능은 특정 파일 액세스 동시 접속 제한을 우회하여 가상 머신 부팅 등의 작업을 가속화합니다.

VAAI 환경 사용에 대한 요구 사항

VAAI 기능은 ESX 운영 체제의 일부이며 올바른 환경을 설정한 경우 ESX 호스트에서 자동으로 호출됩니다.

환경 요구 사항은 다음과 같습니다.

- ESX 호스트는 ESX 4.1 이상을 실행해야 합니다.
- VMware 데이터 저장소를 호스팅하는 NetApp 스토리지 시스템은 ONTAP를 실행 중이어야 합니다.
- (복제 오프로딩만 해당) VMware 복제 작업의 소스 및 대상은 동일한 클러스터 내의 동일한 스토리지 시스템에서 호스팅되어야 합니다.



현재 복제 오프로드 기능은 다른 스토리지 시스템에서 호스팅되는 VMware 데이터 저장소 간에 데이터 복제를 지원하지 않습니다.

VAAI 기능이 ESX에서 지원되는지 확인합니다

ESX 운영 체제에서 VAAI 기능을 지원하는지 확인하려면 vSphere Client를 확인하거나 호스트에 액세스하는 다른 방법을 사용할 수 있습니다. ONTAP는 기본적으로 SCSI 명령을 지원합니다.

ESX 호스트 고급 설정을 확인하여 VAAI 기능이 설정되었는지 여부를 확인할 수 있습니다. 표에는 ESX 제어 이름에 해당하는 SCSI 명령이 나와 있습니다.

scsi 명령	ESX 제어 이름(VAAI 기능)
Extended_copy(확장 복사)	하드하드웨어가속한이동
같은 쓰기	하드wareAcceleratedInit
Compare_and_write(비교 및 쓰기)	하드wareAcceleratedLocking

SAN 복사 오프로드

Microsoft ODX(Offloaded Data Transfer)

Microsoft ODX(Offloaded Data Transfer)는 _copy offload_ 라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고 스토리지 장치 내에서 또는 호환되는 스토리지 장치 간에 직접 데이터를 전송할 수 있습니다.

VMware와 Microsoft는 복제 오프로드 작업을 지원하여 성능과 네트워크 처리량을 높여줍니다. 개별 복제 오프로드 기능을 사용하려면 VMware 및 Windows 운영 체제 환경의 요구 사항을 충족하도록 시스템을 구성해야 합니다.

가상화된 환경에서 VMware와 Microsoft 복사 오프로드를 사용하는 경우 LUN을 정렬해야 합니다. 정렬되지 않은 LUN은 성능을 저하시킬 수 있습니다. "[정렬되지 않은 LUN에 대해 자세히 알아보세요](#)".

ONTAP은 SMB 및 SAN 프로토콜을 모두 지원하는 ODX를 지원합니다.

ODX가 아닌 파일을 전송하면 소스에서 데이터를 읽고 네트워크를 통해 호스트로 전송합니다. 호스트는 네트워크를 통해 데이터를 대상으로 다시 전송합니다. ODX 파일 전송에서는 호스트를 거치지 않고 데이터를 소스에서 대상으로 직접 복사합니다.

ODX는 오프로드된 복사본이 소스와 대상 간에 직접 수행되므로, 동일한 볼륨 내에서 복사본을 수행할 경우 동일한 볼륨 복사본의 복사 시간 단축, 클라이언트의 CPU 및 메모리 사용률 감소, 네트워크 I/O 대역폭 사용률 감소 등 상당한 성능 이점을 실현할 수 있습니다. 여러 볼륨에 걸쳐 있는 복사본에서는 호스트 기반 복사본에 비해 성능이 크게 향상되지 않을 수 있습니다.

SAN 환경의 경우 ODX는 호스트와 스토리지 시스템 모두에서 지원되는 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.

ODX 사용을 위한 요구사항

복사 오프로드를 위해 ODX를 사용할 계획이라면 볼륨 지원 고려 사항, 시스템 요구 사항 및 소프트웨어 기능 요구 사항을 잘 알고 있어야 합니다.

ODX를 사용하려면 시스템에 다음이 있어야 합니다.

- ONTAP

ODX는 지원되는 ONTAP 버전에서 자동으로 활성화됩니다.

- 최소 소스 볼륨 2GB

최적의 성능을 위해 소스 볼륨은 260GB보다 커야 합니다.

- Windows 클라이언트에서 ODX를 지원합니다

ODX는 Windows Server 2012 이상 및 Windows 8 이상에서 지원됩니다. 상호 운용성 매트릭스에는 지원되는 Windows 클라이언트에 대한 최신 정보가 포함되어 있습니다.

"[NetApp 상호 운용성 매트릭스 툴](#)"

- ODX에 대한 복사 애플리케이션 지원

데이터 전송을 수행하는 애플리케이션은 ODX를 지원해야 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 Microsoft TechNet 라이브러리에는 Windows 서버 및 클라이언트에서 지원되는 ODX 응용 프로그램에 대한 자세한 정보가 나와 있습니다.

- 압축된 볼륨을 사용하는 경우 압축 그룹 크기는 8K여야 합니다.

32K 압축 그룹 크기가 지원되지 않습니다.

ODX는 다음 볼륨 유형과 함께 작동하지 않습니다.

- 용량이 2GB 미만인 소스 볼륨
- 읽기 전용 볼륨입니다
- "FlexCache 볼륨"



ODX는 FlexCache 원본 볼륨에서 지원됩니다.

- "반씩 프로비저닝된 볼륨"

특수 시스템 파일 요구 사항

qtree에 있는 ODX 파일을 삭제할 수 있습니다. 기술 지원 부서의 지시가 없는 한 다른 ODX 시스템 파일을 제거하거나 수정하지 마십시오.

ODX 기능을 사용하면 시스템의 모든 볼륨에 ODX 시스템 파일이 존재합니다. 이러한 파일을 사용하면 ODX 전송 중에 사용된 데이터를 특정 시점으로 표시할 수 있습니다. 다음 시스템 파일은 데이터가 오프로드된 LUN 또는 파일을 포함하는 각 볼륨의 루트 레벨에 있습니다.

- '.copy-offload'(숨겨진 디렉토리)
- '.tokens'(숨겨진 파일.copy-offload' 디렉토리)

"copy-offload delete-tokens-path dir_path-node_node_name_" 명령을 사용하여 ODX 파일이 포함된 qtree를 삭제할 수 있습니다.

ODX의 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 SMB에는 적용되지 않습니다.

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 패스쓰루 를 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 패스쓰루 를 지원하지 않습니다.

NVMe 복사 오프로드에 대해 알아보세요

NVMe 복사 오프로드를 사용하면 NVMe 호스트가 CPU에서 ONTAP 스토리지 컨트롤러의 CPU로 복사 작업을 오프로드할 수 있습니다. 호스트는 애플리케이션 워크로드를 위해 CPU 리소스를 예약하는 동시에 한 NVMe 네임스페이스에서 다른 네임스페이스로 데이터를 복사할 수 있습니다.

예를 들어, 성능 분포를 개선하기 위해 스토리지 작업 부하를 재조정해야 한다고 가정해 보겠습니다. 이를 위해서는 각각 평균 크기가 500GB인 45개의 NVMe 네임스페이스를 포함하는 10개의 가상 머신(VM)을 마이그레이션해야 합니다. 즉, 약 22.5TB의 데이터를 복사해야 한다는 의미입니다. 호스트는 데이터 마이그레이션에 자체 CPU를 사용하는 대신 NVMe 복사 오프로드를 사용하여 데이터가 복사되는 동안 애플리케이션 워크로드에 대한 CPU 리소스가 감소하지 않도록 할 수 있습니다.

NVMe 복사 오프로드 지원 및 제한 사항

NVMe 복사 오프로드는 ONTAP 9.18.1부터 지원됩니다. ONTAP NVMe 복사 오프로드를 시작할 수 없습니다. 호스트에서 지원하고 시작해야 합니다.

ONTAP 사용한 NVMe 복사 오프로드 작업에는 다음과 같은 제한 사항이 적용됩니다.

- 지원되는 최대 복사 작업 크기는 16MB입니다.
- 데이터는 동일한 하위 시스템 내의 NVMe 네임스페이스 간에만 마이그레이션될 수 있습니다.
- 데이터는 동일한 HA 쌍의 노드 간에만 마이그레이션될 수 있습니다.

SAN 관리

SAN 프로비저닝

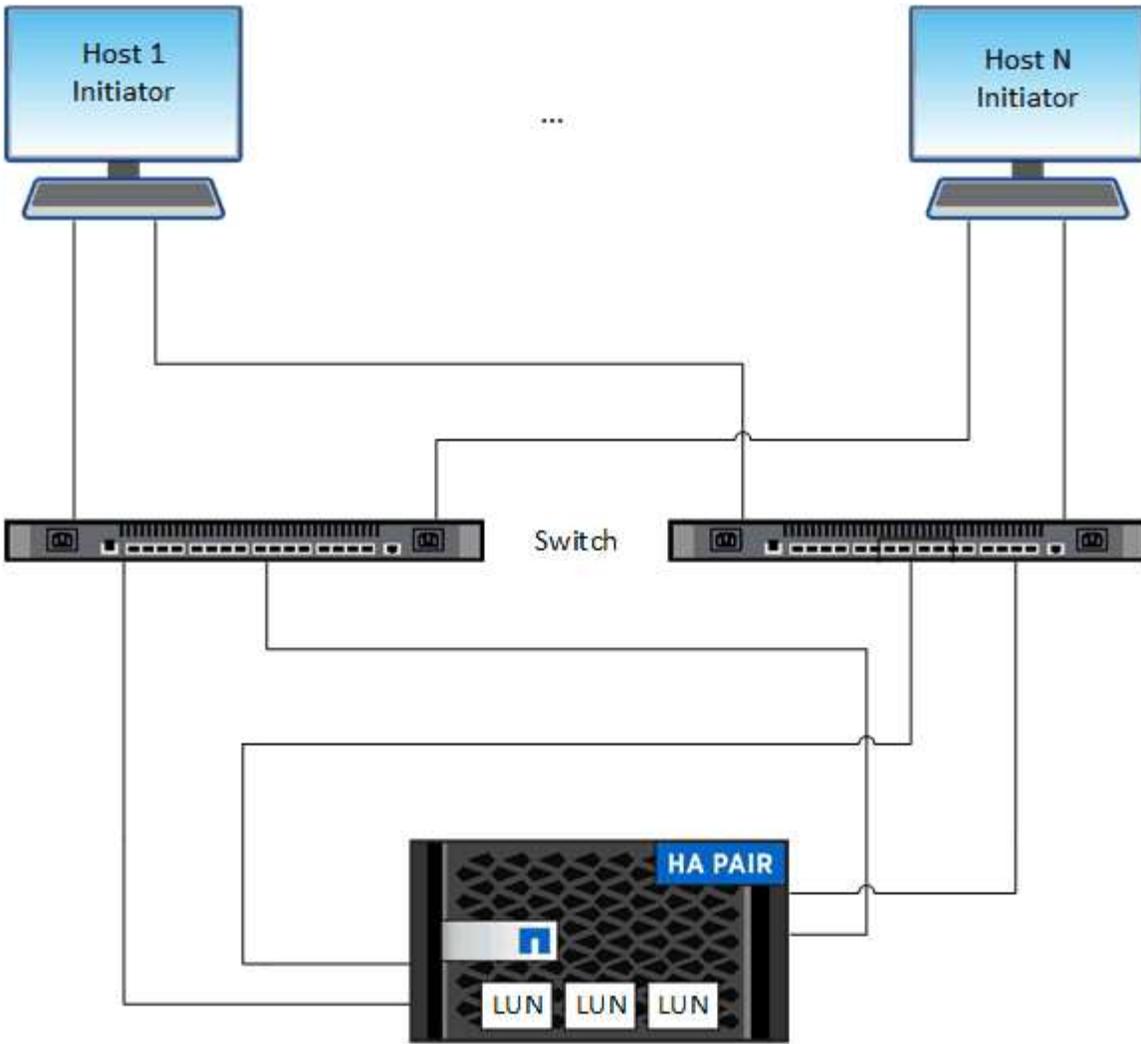
SAN 관리 개요

이 섹션의 내용은 ONTAP 9.7 이상 릴리즈에서 ONTAP CLI(Command Line Interface) 및 System Manager를 사용하여 SAN 환경을 구성하고 관리하는 방법을 보여줍니다.

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

- ["iSCSI 프로토콜"](#)
- ["FC/FCoE 프로토콜"](#)

iSCSI 및 FC 프로토콜을 사용하여 SAN 환경에 스토리지를 제공할 수 있습니다.



iSCSI 및 FC에서는 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 제공됩니다. LUN을 생성한 다음 이를 이니시에이터 그룹(igroup)에 매핑합니다. 이니시에이터 그룹은 FC 호스트 WWP 및 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 LUN을 액세스할 수 있는지 제어합니다.

FC 대상은 FC 스위치 및 호스트 측 어댑터를 통해 네트워크에 연결되며 WWPN(World Wide Port Name)으로 식별됩니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다.

를 참조하십시오

ASA R2 스토리지 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20)을 사용하는 경우 을 참조하십시오"[ASA R2 스토리지 시스템 설명서](#)".

All-Flash SAN 어레이 구성에 대해 자세히 알아보십시오

NetApp ASA(All-Flash SAN 어레이)는 ONTAP 9.7부터 사용할 수 있습니다. ASA는 검증된 AFF NetApp 플랫폼을 기반으로 하는 All-Flash SAN 전용 솔루션입니다.

ASA 플랫폼에는 다음이 포함됩니다.

- ASAA150

- ASA A250
- ASA A400
- ASA A800
- ASA A900
- ASA C250 을 참조하십시오
- ASA C400 을 참조하십시오
- ASA C800을 참조하십시오



ONTAP 9.16.0부터 ASA R2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20)에서 SAN 전용 고객을 위한 단순화된 ONTAP 환경을 이용할 수 있습니다. ASA R2 시스템을 사용하는 경우 를 "[ASA R2 시스템 설명서](#)"참조하십시오.

ASA 플랫폼은 다중 경로를 위해 대칭 액티브-액티브 를 사용합니다. 모든 경로가 액티브/최적화되어 있으므로 스토리지 페일오버 시 호스트는 I/O를 재개하기 위해 페일오버 경로의 ALUA 전환을 기다릴 필요가 없습니다 그러면 페일오버 시간이 단축됩니다.

ASA를 설정합니다

ASA(All-Flash SAN Array)는 비 ASA 시스템과 동일한 설정 절차를 따릅니다.

System Manager는 클러스터를 초기화하고, 로컬 계층을 생성하고, 프로토콜을 구성하고, ASA에 대한 스토리지를 프로비저닝하는 데 필요한 절차를 안내합니다.

ONTAP 클러스터 설정을 시작합니다.

ASA 호스트 설정 및 유틸리티

All-Flash SAN 어레이(ASA)를 설정하기 위한 호스트 설정은 다른 모든 SAN 호스트의 호스트 설정과 동일합니다.

를 다운로드할 수 있습니다 "[NetApp 호스트 유틸리티 소프트웨어](#)" 지원 사이트의 특정 호스트에 대해.

ASA 시스템을 식별하는 방법

ASA 시스템은 System Manager를 사용하거나 CLI(ONTAP Command Line Interface)를 사용하여 식별할 수 있습니다.

- * System Manager 대시보드에서 *: * 클러스터 > 개요 * 를 클릭한 다음 시스템 노드를 선택합니다.

Personality * 는 * All-Flash SAN Array * 로 표시됩니다.

- * CLI * 에서: 를 입력합니다 `san config show` 명령.

ASA 시스템에 대해 "All-Flash SAN 어레이" 값이 true로 반환됩니다.

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

관련 정보

- "[기술 보고서 4968: NetApp All-SAN 어레이 데이터 가용성 및 무결성](#)"

- ["NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례"](#)

FCoE에 대한 스위치를 구성합니다

FC 서비스를 기존 이더넷 인프라에서 실행하려면 먼저 FCoE에 대한 스위치를 구성해야 합니다.

시작하기 전에

- SAN 구성이 지원되어야 합니다.
지원되는 구성에 대한 자세한 내용은 ["NetApp 상호 운용성 매트릭스 툴"](#)을 참조하십시오.
- UTA(Unified Target Adapter)를 스토리지 시스템에 설치해야 합니다.
UTA2를 사용하는 경우 "CNA" 모드로 설정해야 합니다.
- 통합 네트워크 어댑터(CNA)가 호스트에 설치되어 있어야 합니다.

단계

1. 스위치 설명서를 참조하여 FCoE에 맞게 스위치를 구성하십시오.
2. 클러스터의 각 노드에 대한 DCB 설정이 올바르게 구성되었는지 확인합니다.

```
run -node node1 -command dcb show
```

DCB 설정이 스위치에 구성되어 있습니다. 설정이 잘못된 경우 스위치 설명서를 참조하십시오.

3. FC 타겟 포트의 온라인 상태가 일 때 FCoE 로그인 작동하는지 확인합니다 true.

```
fcip adapter show -fields node,adapter,status,state,speed,fabric-established,physical-protocol
```

FC 대상 포트의 온라인 상태가 "거짓"인 경우 스위치 설명서를 참조하십시오.

관련 정보

- ["NetApp 상호 운용성 매트릭스 툴"](#)
- ["NetApp 기술 보고서 3800: FCoE\(Fibre Channel over Ethernet\) 엔드 투 엔드 구축 가이드"](#)
- ["Cisco MDS 9000 NX-OS 및 SAN-OS 소프트웨어 구성 가이드"](#)
- ["Brocade 제품"](#)

시스템 요구 사항

LUN을 설정하려면 LUN을 생성하고, igroup을 생성하고, LUN을 igroup에 매핑해야 합니다. LUN을 설정하기 전에 시스템이 특정 사전 요구 사항을 충족해야 합니다.

- 상호 운용성 매트릭스에는 지원되는 SAN 구성이 나와 있어야 합니다.

- SAN 환경은 에 지정된 SAN 호스트 및 컨트롤러 구성 제한을 충족해야 합니다 "[NetApp Hardware Universe를 참조하십시오](#)" ONTAP 소프트웨어 버전에 적용됩니다.
- 지원되는 버전의 Host Utilities가 설치되어 있어야 합니다.

자세한 내용은 Host Utilities 설명서를 참조하십시오.

- LUN 소유 노드와 소유 노드의 HA 파트너에 SAN LIF가 있어야 합니다.

관련 정보

- "[NetApp 상호 운용성 매트릭스 툴](#)"
- "[ONTAP SAN 호스트 구성](#)"
- "[NetApp 기술 보고서 4017: 파이버 채널 SAN 모범 사례](#)"

LUN을 생성하기 전에 알아야 할 사항

클러스터에서 LUN 설정을 시작하기 전에 이러한 LUN 지침을 검토해야 합니다.

실제 LUN 크기가 약간 다른 이유

LUN의 크기와 관련하여 다음 사항에 유의하십시오.

- LUN을 생성할 때 LUN의 실제 크기는 LUN의 OS 유형에 따라 약간 다를 수 있습니다. LUN을 생성한 후에는 LUN OS 유형을 수정할 수 없습니다.
- 최대 LUN 크기로 LUN을 생성하는 경우 LUN의 실제 크기가 약간 더 작을 수 있습니다. ONTAP는 한계치를 약간 낮추어 줍니다.
- 각 LUN의 메타데이터는 포함하는 애그리게이트에서 약 64KB의 공간을 필요로 합니다. LUN을 생성할 때 포함하는 애그리게이트에 LUN의 메타데이터를 위한 충분한 공간이 있는지 확인해야 합니다. Aggregate에 LUN의 메타데이터를 위한 충분한 공간이 없을 경우 일부 호스트에서 LUN에 액세스하지 못할 수 있습니다.

LUN ID 할당 지침

일반적으로 기본 LUN ID는 0으로 시작하고 각 추가 매핑된 LUN에 대해 1씩 증분식으로 할당됩니다. 호스트는 LUN ID를 LUN의 위치 및 경로 이름과 연결합니다. 유효한 LUN ID 번호의 범위는 호스트에 따라 다릅니다. 자세한 내용은 Host Utilities와 함께 제공된 설명서를 참조하십시오.

LUN을 igroup에 매핑하기 위한 지침

- LUN을 igroup에 한 번만 매핑할 수 있습니다.
- 모범 사례로서, igroup을 통해 하나의 특정 이니시에이터에 LUN을 매핑해야 합니다.
- 한 개의 이니시에이터를 여러 igroup에 추가할 수 있지만 이니시에이터는 하나의 LUN에만 매핑할 수 있습니다.
- 동일한 igroup에 매핑된 두 LUN에 대해 동일한 LUN ID를 사용할 수 없습니다.
- Igroup 및 포트 세트에 동일한 프로토콜 유형을 사용해야 합니다.

프로토콜 FC 또는 iSCSI 라이선스를 확인하고 추가합니다

FC 또는 iSCSI를 사용하여 SVM(스토리지 가상 시스템)에 대한 블록 액세스를 활성화하려면 먼저 라이선스가 있어야 합니다. FC 및 iSCSI 라이선스는 에 포함되어 "[ONTAP 1](#) 을

참조하십시오"있습니다.

예 1. 단계

시스템 관리자

ONTAP One이 없는 경우 ONTAP System Manager(9.7 이상)를 사용하여 FC 또는 iSCSI 라이선스를 확인하고 추가합니다.

1. System Manager에서 * Cluster > Settings > Licenses * 를 선택합니다
2. 라이선스가 목록에 없으면 를 선택하고 라이선스 키를 입력합니다  .
3. 추가 * 를 선택합니다.

CLI를 참조하십시오

ONTAP One이 없는 경우 ONTAP CLI를 사용하여 FC 또는 iSCSI 라이선스를 확인하고 추가합니다.

1. FC 또는 iSCSI에 대한 활성 라이선스가 있는지 확인합니다.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. FC 또는 iSCSI에 대한 활성 라이선스가 없는 경우 라이선스 코드를 추가합니다.

```
license add -license-code <your_license_code>
```

SAN 스토리지 용량 할당

이 절차를 수행하면 FC 또는 iSCSI 프로토콜이 이미 구성된 기존 스토리지 VM에 새 LUN이 생성됩니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 저장소를 프로비저닝합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

새 스토리지 VM을 생성하고 FC 또는 iSCSI 프로토콜을 구성해야 하는 경우 를 참조하십시오 "FC용 SVM 구성" 또는 "iSCSI용 SVM을 구성합니다".

FC 라이선스가 활성화되어 있지 않으면 LIF 및 SVM이 온라인 상태로 나타나지만 운영 상태는 다운입니다.

LUN은 호스트에 디스크 디바이스로 나타납니다.



ALUA(Asymmetric Logical Unit Access)는 LUN 생성 중에 항상 사용하도록 설정됩니다. ALUA 설정은 변경할 수 없습니다.

SVM의 모든 FC LIF에서 이니시에이터를 호스팅하려면 단일 이니시에이터 조닝을 사용해야 합니다.

ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로 사용하도록 설정됩니다. 프로비저닝 프로세스 도중 또는 나중에 QoS를 사용하지 않도록 설정하거나 사용자 지정 QoS 정책을 선택할 수 있습니다.

예 2. 단계

시스템 관리자

ONTAP System Manager(9.7 이상)와 함께 FC 또는 iSCSI 프로토콜을 사용하여 SAN 호스트에 스토리지를 제공할 LUN을 생성합니다.

System Manager Classic(9.7 이하 버전에서 사용 가능)을 사용하여 이 작업을 완료하려면 [을 참조하십시오 "Red Hat Enterprise Linux용 iSCSI 구성"](#)

단계

1. 호스트에 적절한 롤 "[SAN 호스트 유틸리티](#)"설치합니다.
2. System Manager에서 * 스토리지 > LUN * 을 클릭한 다음 * 추가 * 를 클릭합니다.
3. LUN을 생성하는 데 필요한 정보를 입력합니다.
4. ONTAP 버전에 따라 * 추가 옵션 * 을 클릭하여 다음 중 하나를 수행할 수 있습니다.

옵션을 선택합니다	부터 사용할 수 있습니다
<ul style="list-style-type: none"> • 상위 볼륨 대신 LUN에 QoS 정책을 할당합니다 <ul style="list-style-type: none"> ◦ * 추가 옵션 > 스토리지 및 최적화 * 를 선택합니다 ◦ 성능 서비스 수준 * 을 선택합니다. ◦ 전체 볼륨 대신 개별 LUN에 QoS 정책을 적용하려면 * Apply these performance limits enforcement to each LUN * 을 선택합니다. <p>기본적으로 성능 제한은 볼륨 레벨에 적용됩니다.</p>	ONTAP 9.10.1
<ul style="list-style-type: none"> • 기존 이니시에이터 그룹을 사용하여 새 이니시에이터 그룹을 생성합니다 <ul style="list-style-type: none"> ◦ 추가 옵션 > 호스트 정보 * ◦ 기존 이니시에이터 그룹을 사용하여 새 이니시에이터 그룹 * 을 선택합니다. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>다른 igroup이 포함된 igroup의 OS 유형은 생성된 후에는 변경할 수 없습니다.</p> </div>	ONTAP 9.9.1
<ul style="list-style-type: none"> • igroup 또는 호스트 이니시에이터에 설명을 추가합니다 <p>이 설명은 igroup 또는 호스트 이니시에이터의 별칭으로 사용됩니다.</p> <ul style="list-style-type: none"> ◦ 추가 옵션 > 호스트 정보 * 	ONTAP 9.9.1

<ul style="list-style-type: none"> • 기존 볼륨에 LUN을 생성합니다 <p>기본적으로 새 LUN은 새 볼륨에 생성됩니다.</p> <ul style="list-style-type: none"> ◦ 추가 옵션 > LUN 추가 * 를 선택합니다 ◦ Group related LUNs * 를 선택합니다. 	<p>ONTAP 9.9.1</p>
<ul style="list-style-type: none"> • QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택합니다 ◦ * 추가 옵션 > 스토리지 및 최적화 * 를 선택합니다 ◦ 성능 서비스 수준 * 을 선택합니다. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>ONTAP 9.9.1 이상에서 사용자 지정 QoS 정책을 선택하면 지정된 로컬 계층에 수동 배치를 선택할 수도 있습니다.</p> </div>	<p>ONTAP 9.8</p>

5. FC의 경우 WWPN으로 FC 스위치를 조닝(Zoning)하십시오. 이니시에이터당 하나의 존을 사용하고 각 존에 모든 타겟 포트를 포함합니다.

6. 호스트에서 LUN을 검색합니다.

VMware vSphere의 경우 VSC(가상 스토리지 콘솔)를 사용하여 LUN을 검색하고 초기화할 수 있습니다.

7. LUN을 초기화하고 필요에 따라 파일 시스템을 생성합니다.

8. 호스트가 LUN에 데이터를 쓰고 읽을 수 있는지 확인합니다.

CLI를 참조하십시오

ONTAP CLI에서 FC 또는 iSCSI 프로토콜을 사용하여 SAN 호스트에 스토리지를 제공할 LUN을 생성합니다.

1. FC 또는 iSCSI에 대한 라이선스가 있는지 확인합니다.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. FC 또는 iSCSI 라이선스가 없는 경우 'license add' 명령을 사용합니다.

```
license add -license-code <your_license_code>
```

3. SVM에서 프로토콜 서비스 지원:

- iSCSI의 경우: *

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

- FC: *

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. 각 노드에서 SVM에 대해 2개의 LIF를 생성합니다.

```
network interface create -vserver <svm_name> -lif <lif_name> -role  
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port  
<port_name> -address <ip_address> -netmask <netmask>
```

NetApp은 각 SVM에서 데이터를 제공할 수 있도록 노드당 최소 하나의 iSCSI 또는 FC LIF를 지원합니다. 그러나 이중화를 위해서는 노드당 두 개의 LIF가 필요합니다. iSCSI의 경우 노드당 최소 두 개의 LIF를 별도의 이더넷 네트워크에 구성하는 것이 좋습니다.

5. LIF가 생성되었으며 운영 상태가 '온라인'인지 확인합니다.

```
network interface show -vserver <svm_name> <lif_name>
```

6. LUN 생성:

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>  
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

LUN 이름은 255자를 초과할 수 없으며 공백을 포함할 수 없습니다.



NVFAIL 옵션은 볼륨에 LUN이 생성될 때 자동으로 활성화됩니다.

7. Igroup 생성:

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol  
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. LUN을 igroup에 매핑:

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

9. LUN이 올바르게 구성되었는지 확인합니다.

```
lun show -vserver <svm_name>
```

10. 필요한 경우 "포트 세트를 생성하고 igroup에 바인딩합니다".

11. 호스트 설명서의 단계를 따라 특정 호스트에서 블록 액세스를 설정합니다.

12. Host Utilities를 사용하여 FC 또는 iSCSI 매핑을 완료하고 호스트에서 LUN을 검색할 수 있습니다.

관련 정보

- ["SAN 관리 개요"](#)
- ["ONTAP SAN 호스트 구성"](#)
- ["System Manager에서 SAN 이니시에이터 그룹을 보고 관리합니다"](#)
- ["NetApp 기술 보고서 4017: 파이버 채널 SAN 모범 사례"](#)

NVMe 프로비저닝

NVMe 개요

NVMe(Non-Volatile Memory Express) 프로토콜을 사용하여 SAN 환경에 스토리지를 제공할 수 있습니다. NVMe 프로토콜은 솔리드 스테이트 스토리지의 성능을 위해 최적화되어 있습니다.

NVMe의 경우 스토리지 타겟을 네임스페이스라고 합니다. NVMe 네임스페이스는 많은 비휘발성 스토리지로, 논리 블록으로 포맷되고 호스트에 표준 블록 장치로 제공될 수 있습니다. 네임스페이스와 서브시스템을 생성한 다음, 네임스페이스를 서브시스템에 매핑합니다. 이는 LUN이 FC 및 iSCSI용 igroup에 프로비저닝 및 매핑된 방식과 유사합니다.

NVMe 대상은 이더넷 스위치 및 호스트 측 어댑터를 사용하여 FC 스위치 또는 표준 TCP 인프라를 사용하여 표준 FC 인프라를 통해 네트워크에 연결됩니다.

NVMe에 대한 지원은 ONTAP 버전에 따라 다릅니다. 을 참조하십시오 ["NVMe 지원 및 제한 사항"](#) 를 참조하십시오.

NVMe란 무엇입니까

NVMe(Nonvolatile Memory Express) 프로토콜은 비휘발성 스토리지 미디어에 액세스하는 데 사용되는 전송 프로토콜입니다.

NVMe over Fabrics (NVMeoF)는 PCIe 이외의 연결을 통해 NVMe 기반 통신을 가능하게 하는 NVMe에 대한 사양 정의 확장입니다. 이 인터페이스를 통해 외부 스토리지 인클로저를 서버에 연결할 수 있습니다.

NVMe는 플래시 기술에서 고성능 영구 메모리 기술에 이르기까지 비휘발성 메모리로 구축된 스토리지 장치에 효율적으로 액세스할 수 있도록 설계되었습니다. 따라서 하드 디스크 드라이브용으로 설계된 스토리지 프로토콜과 동일한 제한이 없습니다. 플래시 및 SSD(Solid State Device)는 일종의 비휘발성 메모리(NVM)입니다. NVM은 정전 시 콘텐츠를 보관하는 메모리의 한 유형입니다. NVMe는 해당 메모리에 액세스할 수 있는 방법입니다.

NVMe의 이점으로는 데이터 전송을 위한 속도, 생산성, 처리량 및 용량이 증가합니다. 구체적인 특징은 다음과 같습니다.

- NVMe는 최대 64,000개의 대기열을 지원하도록 설계되었습니다.

또한 각 대기열에는 최대 64,000개의 동시 명령이 있을 수 있습니다.

- NVMe는 여러 하드웨어 및 소프트웨어 공급업체에서 지원합니다
- NVMe는 빠른 응답 시간을 지원하는 플래시 기술을 통해 생산성이 더 높습니다
- NVMe를 사용하면 SSD로 전송되는 각 "요청"에 대해 여러 데이터 요청을 처리할 수 있습니다.

NVMe는 "재퀘스트"를 디코딩하는 데 시간이 더 적게 걸리며 다중 스레드 프로그램에서 스레드 잠금을 요구하지 않습니다.

- NVMe는 CPU 레벨에서 병목 현상을 방지하고 시스템이 확장됨에 따라 대규모 확장성을 지원하는 기능을 지원합니다.

NVMe 네임스페이스 정보

NVMe 네임스페이스는 논리 블록으로 포맷될 수 있는 비휘발성 메모리(NVM)의 양입니다. 네임스페이스는 스토리지 가상 머신이 NVMe 프로토콜을 통해 구성되고 FC 및 iSCSI 프로토콜에 대한 LUN과 동등한 경우에 사용됩니다.

하나 이상의 네임스페이스가 프로비저닝되고 NVMe 호스트에 연결됩니다. 각 네임스페이스는 다양한 블록 크기를 지원할 수 있습니다.

NVMe 프로토콜은 여러 컨트롤러를 통해 네임스페이스에 대한 액세스를 제공합니다. 대부분의 운영 체제에서 지원되는 NVMe 드라이버를 사용하면 SSD(Solid State Drive) 네임스페이스가 수정 없이 파일 시스템과 애플리케이션을 구축할 수 있는 표준 블록 장치로 표시됩니다.

네임스페이스 ID(NSID)는 네임스페이스에서 액세스를 제공하기 위해 컨트롤러에서 사용하는 식별자입니다. 호스트 또는 호스트 그룹에 대한 NSID를 설정할 때 호스트가 볼륨에 액세스할 수 있도록 구성할 수도 있습니다. 논리적 블록은 한 번에 하나의 호스트 그룹에만 매핑할 수 있으며, 지정된 호스트 그룹에는 중복된 NSID가 없습니다.

NVMe 하위 시스템 정보

NVMe 하위 시스템에는 하나 이상의 NVMe 컨트롤러, 네임스페이스, NVM 하위 시스템 포트, NVM 스토리지 미디어 및 컨트롤러와 NVM 스토리지 미디어 간의 인터페이스가 포함되어 있습니다. NVMe 네임스페이스를 생성할 때 기본적으로 이 네임스페이스는 서브시스템에 매핑되지 않습니다. 새 하위 시스템이나 기존 하위 시스템을 매핑하도록 선택할 수도 있습니다.

관련 정보

- ["NVMe 스토리지 프로비저닝"](#) ASA, AFF 및 FAS 시스템에 대해 알아보십시오
- ["NVMe 네임스페이스를 서브시스템에 매핑합니다"](#) ASA AFF 및 FAS 시스템에 대해 알아보십시오.
- ["SAN 호스트 및 클라우드 클라이언트를 구성합니다"](#)
- ASA R2(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20) 스토리지 시스템에 대해

알아보십시오. ["SAN 스토리지 프로비저닝"](#)

NVMe 라이선스 요구 사항

ONTAP 9.5부터 NVMe를 지원하려면 라이선스가 필요합니다. ONTAP 9.4에서 NVMe를 사용하는 경우 ONTAP 9.5로 업그레이드한 후 라이선스를 취득하기 위한 90일 유예 기간이 제공됩니다.

다음 명령을 사용하여 라이선스를 설정할 수 있습니다.

```
'System license add-license-code_NVMe_license_key_'
```

NVMe 구성, 지원 및 제한 사항

ONTAP 9.4부터 **"비휘발성 메모리 익스프레스(NVMe)"** SAN 환경에서 프로토콜을 사용할 수 있습니다. FC-NVMe는 기존 FC 네트워크와 동일한 물리적 설정 및 조닝(zoning)을 사용하지만 FC-SCSI보다 더 큰 대역폭과 향상된 IOPS를 제공하며 지연 시간을 줄일 수 있습니다.

NVMe 지원 및 제한 사항은 사용 중인 ONTAP 버전, 플랫폼 및 구성에 따라 다릅니다. 특정 구성에 대한 자세한 내용을 참조하십시오 ["NetApp 상호 운용성 매트릭스 툴"](#). 지원되는 제한 사항은 을 참조하십시오 ["Hardware Universe"](#).



클러스터당 최대 노드는 * 지원되는 플랫폼 혼합 * 에서 Hardware Universe에서 사용할 수 있습니다.

구성

- 단일 패브릭 또는 멀티 패브릭을 사용하여 NVMe 구성을 설정할 수 있습니다.
- SAN을 지원하는 모든 SVM에 하나의 관리 LIF를 구성해야 합니다.
- 임베디드 블레이드 스위치의 경우를 제외하고 이기종 FC 스위치 패브릭을 사용할 수 없습니다.

특정 예외는 에 나열되어 있습니다 ["NetApp 상호 운용성 매트릭스 툴"](#).

- 캐스케이드, 부분 메시, 풀 메시, 코어 에지 및 디렉터 패브릭은 모두 FC 스위치를 패브릭에 연결하는 업계 표준 방법이며 모두 지원됩니다.

패브릭은 하나 또는 여러 개의 스위치로 구성될 수 있으며, 스토리지 컨트롤러를 여러 스위치에 연결할 수 있습니다.

피처

사용 중인 ONTAP 버전에 따라 다음 NVMe 기능이 지원됩니다.

ONTAP로 시작하는 중...	NVMe를 지원합니다
9.17.1	<ul style="list-style-type: none">• VMware 워크로드를 위한 SnapMirror 액티브 싱크 NVMe/FC 및 NVMe/TCP 호스트 액세스.
9.15.1	<ul style="list-style-type: none">• NVMe/TCP에서 4노드 MetroCluster IP 구성

9.14.1	<ul style="list-style-type: none"> 서브시스템에서 호스트 우선 순위 설정(호스트 레벨 QoS)
9.12.1	<ul style="list-style-type: none"> NVMe/FC에서 4노드 MetroCluster IP 구성 ONTAP 9.12.1 이전의 프런트 엔드 NVMe 네트워크에서는 MetroCluster 구성이 지원되지 않습니다. MetroCluster 구성은 NVMe/TCP에서 지원되지 않습니다.
9.10.1	네임스페이스 크기 조정
9.9.1	<ul style="list-style-type: none"> 네임스페이스와 LUN이 동일한 볼륨에 공존합니다
9.8	<ul style="list-style-type: none"> 프로토콜 공존 <p>SCSI, NAS 및 NVMe 프로토콜은 동일한 스토리지 가상 머신(SVM)에 존재할 수 있습니다.</p> <p>ONTAP 9.8 이전에는 SVM에서 NVMe가 유일한 프로토콜이 될 수 있습니다.</p>
9.6	<ul style="list-style-type: none"> 네임스페이스의 경우 512바이트 블록 및 4096바이트 블록입니다 <p>기본값은 4096입니다. 512는 호스트 운영 체제가 4096바이트 블록을 지원하지 않는 경우에만 사용해야 합니다.</p> <ul style="list-style-type: none"> 매핑된 네임스페이스를 사용하여 볼륨 이동
9.5	<ul style="list-style-type: none"> 다중 경로 HA 쌍 페일오버/반환

프로토콜

다음 NVMe 프로토콜이 지원됩니다.

프로토콜	ONTAP로 시작하는 중...	허용된 사용자...
TCP	9.10.1	기본값
FC	9.4	기본값

ONTAP 9.8부터 동일한 SVM(스토리지 가상 머신)에서 SCSI, NAS 및 NVMe 프로토콜을 구성할 수 있습니다. ONTAP 9.7 이하 버전에서는 NVMe가 SVM에서 유일한 프로토콜이 될 수 있습니다.

네임스페이스

NVMe 네임스페이스를 사용하여 작업할 때 다음을 숙지해야 합니다.

- ONTAP 9.15.1 이하 버전의 경우 ONTAP는 공간 재확보를 위해 NVMe와 함께 NVMe 데이터 집합 관리(할당 해제) 명령을 지원하지 않습니다.
- SnapRestore를 사용하여 LUN에서 네임스페이스를 복원하거나 그 반대로 복원할 수 없습니다.
- 네임스페이스에 대한 공간 보장은 포함하는 볼륨의 공간 보장과 동일합니다.
- 7-Mode에서 운영되는 Data ONTAP의 볼륨 전환에서는 네임스페이스를 생성할 수 없습니다.
- 네임스페이스는 다음을 지원하지 않습니다.
 - 이름 바꾸기
 - 볼륨 간 이동
 - 볼륨 간 복사
 - 온 디맨드 복사

추가 제한 사항

다음 **ONTAP** 기능은 **NVMe** 구성에서 지원되지 않습니다.

- 가상 스토리지 콘솔
- 영구 예약

다음은 **ONTAP 9.4**를 실행하는 노드에만 적용됩니다.

- NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
- NVMe LIF가 생성되기 전에 NVMe 서비스를 생성해야 합니다.

관련 정보

["최신 SAN의 모범 사례"](#)

NVMe용 스토리지 VM을 구성합니다

노드에서 NVMe 프로토콜을 사용하려면 NVMe용으로 특수 SVM을 구성해야 합니다.

시작하기 전에

FC 또는 이더넷 어댑터는 NVMe를 지원해야 합니다. 지원되는 어댑터가 에 나열되어 있습니다 ["NetApp Hardware Universe를 참조하십시오"](#).

예 3. 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 NVMe용 스토리지 VM을 구성합니다.

새 스토리지 VM에서 NVMe를 구성합니다	기존 스토리지 VM에서 NVMe를 구성합니다
<ol style="list-style-type: none">1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다.2. 스토리지 VM의 이름을 입력합니다.3. 액세스 프로토콜 * 에 대해 * NVMe * 를 선택합니다.4. NVMe/FC * 활성화 또는 * NVMe/TCP * 활성화 및 * 저장 * 을 선택합니다.	<ol style="list-style-type: none">1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.2. 구성할 스토리지 VM을 클릭합니다.3. 설정 * 탭을 클릭한 다음 NVMe 프로토콜 옆에 있는  을 클릭합니다.4. NVMe/FC * 활성화 또는 * NVMe/TCP * 활성화 및 * 저장 * 을 선택합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 NVMe용 스토리지 VM을 구성합니다.

1. 기존 SVM을 사용하지 않으려면 다음을 생성합니다.

```
vserver create -vserver <SVM_name>
```

- a. SVM이 생성되었는지 확인:

```
vserver show
```

2. 클러스터에 NVMe 또는 TCP 가능 어댑터가 설치되어 있는지 확인합니다.

NVMe의 경우:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

TCP의 경우:

```
network port show
```

에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. ONTAP 9.7 이하를 실행 중인 경우 SVM에서 프로토콜을 모두 제거하십시오.

```
vserver remove-protocols -vserver <SVM_name> -protocols  
iscsi, fcp, nfs, cifs, ndmp
```

ONTAP 9.8부터는 NVMe를 추가할 때 다른 프로토콜을 제거할 필요가 없습니다.

4. SVM에 NVMe 프로토콜을 추가합니다.

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. ONTAP 9.7 이하를 실행 중인 경우, NVMe가 SVM에서 허용되는 유일한 프로토콜인지 확인하십시오.

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe는 허용된 프로토콜 칼럼 아래에 표시되는 유일한 프로토콜이어야 합니다.

6. NVMe 서비스를 생성합니다.

```
vserver nvme create -vserver <SVM_name>
```

7. NVMe 서비스가 생성되었는지 확인하십시오.

```
vserver nvme show -vserver <SVM_name>
```

`Administrative Status` SVM은 **으로 나열되어야 합니다** `up`. 에 대한 자세한 내용은 `up` [link:https://docs.netapp.com/us-en/ontap-cli/up.html](https://docs.netapp.com/us-en/ontap-cli/up.html) ["ONTAP 명령 참조입니다"^]을 참조하십시오.

8. NVMe/FC LIF 생성:

- ONTAP 9.9.1 이하, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-role data -data-protocol fc-nvme -home-node <home_node> -home  
-port <home_port>
```

- ONTAP 9.10.1 이상의 경우 FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

- ONTAP 9.10.1 이상의 경우 TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

9. HA 파트너 노드에 NVMe/FC LIF 생성:

- ONTAP 9.9.1 이하, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- ONTAP 9.10.1 이상의 경우 FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-home-node <home_node> -home-port <home_port> -status-admin up
-failover-policy disabled -firewall-policy data -auto-revert
false -failover-group <failover_group> -is-dns-update-enabled
false
```

- ONTAP 9.10.1 이상의 경우 TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

10. NVMe/FC LIF가 생성되었는지 확인:

```
network interface show -vserver <SVM_name>
```

11. LIF와 동일한 노드에서 볼륨 생성:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate  
<aggregate_name> -size <volume_size>
```

자동 효율성 정책에 대한 경고 메시지가 표시되면 무시해도 됩니다.

NVMe 스토리지 프로비저닝

다음 단계를 사용하여 기존 스토리지 VM에서 NVMe 지원 호스트에 대한 네임스페이스를 생성하고 스토리지를 프로비저닝할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. ["수행할 수 있습니다"](#) 저장소를 프로비저닝합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로 사용하도록 설정됩니다. 프로비저닝 프로세스 중에 또는 나중에 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택할 수 있습니다.

시작하기 전에

스토리지 VM은 NVMe에 맞게 구성해야 하며 FC 또는 TCP 전송은 이미 설정되어 있어야 합니다.

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 NVMe 프로토콜을 사용하여 스토리지를 제공하기 위한 네임스페이스를 생성합니다.

단계

1. System Manager에서 * 스토리지 > NVMe 네임스페이스 * 를 클릭한 다음 * 추가 * 를 클릭합니다.
새 하위 시스템을 만들어야 하는 경우 * 추가 옵션 * 을 클릭합니다.
2. ONTAP 9.8 이상을 실행하고 있고 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택하려면 * 추가 옵션 * 을 클릭한 다음 * 스토리지 및 최적화 * 에서 * 성능 서비스 수준 * 을 선택합니다.
3. WWPN을 기준으로 FC 스위치를 조닝(Zoning)하십시오. 이니시에이터당 하나의 존을 사용하고 각 존에 모든 타겟 포트를 포함합니다.
4. 호스트에서 새 네임스페이스를 검색합니다.
5. 네임스페이스를 초기화하고 파일 시스템으로 포맷합니다.
6. 호스트에서 네임스페이스에서 데이터를 쓰고 읽을 수 있는지 확인합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 NVMe 프로토콜을 사용하여 스토리지를 제공하기 위한 네임스페이스를 생성합니다.

이 절차에서는 NVMe 프로토콜용으로 이미 구성된 기존 스토리지 VM에 NVMe 네임스페이스 및 서브시스템을 생성한 다음, 네임스페이스를 서브시스템에 매핑하여 호스트 시스템에서 데이터에 액세스할 수 있도록 합니다.

NVMe용 스토리지 VM을 구성해야 하는 경우 를 참조하십시오 ["NVMe를 위한 SVM 구성"](#).

단계

1. SVM이 NVMe용으로 구성되었는지 확인합니다.

```
vserver show -vserver <svm_name> -fields allowed-protocols
```

"NVMe"는 "허용된 프로토콜" 열 아래에 표시되어야 합니다.

2. NVMe 네임스페이스를 생성합니다.



매개 변수로 참조하는 볼륨이 이미 존재해야 하며, 그렇지 않으면 이 명령을 실행하기 전에 볼륨을 `-path` 생성해야 합니다.

```
vserver nvme namespace create -vserver <svm_name> -path <path> -size <size_of_namespace> -ostype <OS_type>
```

3. NVMe 하위 시스템을 생성합니다.

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

NVMe 하위 시스템 이름은 대/소문자를 구분합니다. 1 ~ 96자를 포함해야 합니다. 특수 문자를 사용할 수 있습니다.

4. 하위 시스템이 생성되었는지 확인합니다.

```
vserver nvme subsystem show -vserver <svm_name>
```

NVMe 서브시스템은 Subsystem 열에 표시되어야 한다.

5. 호스트에서 NQN을 가져옵니다.
6. 호스트 NQN을 하위 시스템에 추가합니다.

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. 네임스페이스를 하위 시스템에 매핑합니다.

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

네임스페이스는 단일 하위 시스템에만 매핑할 수 있습니다.

8. 네임스페이스가 하위 시스템에 매핑되어 있는지 확인합니다.

```
vserver nvme namespace show -vserver <svm_name> -instance
```

하위 시스템은 연결된 하위 시스템으로 나열되어야 합니다.

NVMe 네임스페이스를 하위 시스템에 매핑합니다

NVMe 네임스페이스를 하위 시스템에 매핑하면 호스트에서 데이터에 액세스할 수 있습니다. 스토리지를 프로비저닝할 때 NVMe 네임스페이스를 하위 시스템에 매핑하거나 스토리지를 프로비저닝한 후 연결할 수 있습니다.

ONTAP 9.17.1부터 SnapMirror 액티브 동기화 구성을 사용하는 경우, 호스트를 NVMe 서브시스템에 추가하는 동시에 호스트에 SVM을 근접 가상 서버로 추가할 수 있습니다. NVMe 서브시스템의 네임스페이스에 대한 액티브 최적화 경로는 근접 가상 서버로 구성된 SVM에서만 호스트에 게시됩니다.

ONTAP 9.14.1부터 특정 호스트에 대한 리소스 할당의 우선 순위를 지정할 수 있습니다. 기본적으로 호스트가 NVMe 서브시스템에 추가되면 보통 우선 순위가 부여됩니다. ONTAP CLI(명령줄 인터페이스)를 사용하여 기본 우선 순위를 보통에서 높음으로 수동으로 변경할 수 있습니다. 높은 우선 순위가 할당된 호스트에는 더 큰 입출력 대기열 수와 대기열 깊이가 할당됩니다.



ONTAP 9.13.1 이하 버전에서 하위 시스템에 추가된 호스트에 높은 우선 순위를 부여하려는 경우 다음을 수행할 수 있습니다 [호스트 우선 순위를 변경합니다](#).

시작하기 전에

네임스페이스와 하위 시스템이 이미 만들어져 있어야 합니다. 네임스페이스와 하위 시스템을 만들어야 하는 경우 를 참조하십시오 "[NVMe 스토리지 프로비저닝](#)".

NVMe 네임스페이스 매핑

단계

1. 호스트에서 NQN을 가져옵니다.
2. 호스트 NQN을 하위 시스템에 추가합니다.

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

호스트의 기본 우선 순위를 보통에서 높음으로 변경하려면 `-priority high` 옵션을 사용합니다. 이 옵션은 ONTAP 9.14.1부터 사용할 수 있습니다. 에 대한 자세한 내용은 `vserver nvme subsystem host add` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

SVM을 추가하려면 `proximal-vserver SnapMirror` 활성화 동기화 구성에서 NVMe 하위 시스템에 호스트를 추가하는 동안 호스트에 다음을 사용할 수 있습니다. `-proximal-vservers` 옵션입니다. 이 옵션은 ONTAP 9.17.1부터 사용할 수 있습니다. 소스 SVM이나 대상 SVM, 또는 둘 다를 추가할 수 있습니다. 이 명령을 실행 중인 SVM이 기본값입니다.

3. 네임스페이스를 하위 시스템에 매핑합니다.

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

네임스페이스는 단일 하위 시스템에만 매핑할 수 있습니다. 에 대한 자세한 내용은 `vserver nvme subsystem map add` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

4. 네임스페이스가 하위 시스템에 매핑되어 있는지 확인합니다.

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

하위 시스템이 로 나열되어야 `Attached subsystem` 합니다. 에 대한 자세한 내용은 `vserver nvme namespace show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

LUN 관리

LUN QoS 정책 그룹을 편집합니다

ONTAP 9.10.1부터 System Manager를 사용하여 여러 LUN에 동시에 QoS(서비스 품질) 정책을 할당하거나 제거할 수 있습니다.



볼륨 레벨에서 QoS 정책이 할당된 경우 볼륨 레벨에서 QoS 정책을 변경해야 합니다. LUN 레벨에서 원래 할당된 LUN 레벨에서만 QoS 정책을 편집할 수 있습니다.

단계

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 편집할 LUN을 선택합니다.

한 번에 둘 이상의 LUN을 편집하는 경우 LUN은 동일한 SVM(Storage Virtual Machine)에 속해야 합니다. 동일한 SVM에 속하지 않는 LUN을 선택하면 QoS 정책 그룹을 편집하는 옵션이 표시되지 않습니다.

3. More * 를 클릭하고 * Edit QoS Policy Group * 을 선택합니다.

LUN을 네임스페이스로 변환

ONTAP 9.11.1부터 ONTAP CLI를 사용하여 현재 위치에서 기존 LUN을 NVMe 네임스페이스로 변환할 수 있습니다.

시작하기 전에

- 지정한 LUN에 igroup에 대한 기존 맵이 없어야 합니다.
- LUN은 MetroCluster로 구성된 SVM이나 SnapMirror 활성 동기화 관계에 있어서는 안 됩니다.
- LUN은 프로토콜 엔드포인트이거나 프로토콜 엔드포인트에 바인딩되지 않아야 합니다.
- LUN에 0이 아닌 접두사 및/또는 접미사 스트림이 있어서는 안 됩니다.
- LUN은 스냅샷의 일부이거나 SnapMirror 관계의 대상 측에서 읽기 전용 LUN일 수 없습니다.

단계

1. LUN을 NVMe 네임스페이스로 변환:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

LUN을 오프라인 상태로 전환합니다

ONTAP 9.10.1부터 System Manager를 사용하여 LUN을 오프라인 상태로 전환할 수 있습니다. ONTAP 9.10.1 이전에는 ONTAP CLI를 사용하여 LUN을 오프라인 상태로 전환해야 합니다.

시스템 관리자

단계

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 단일 LUN 또는 여러 LUN을 오프라인 상태로 전환합니다

원하는 사항	이렇게 하십시오.
단일 LUN을 오프라인 상태로 전환합니다	LUN 이름 옆에 있는 을  클릭하고 * 오프라인 상태로 전환 * 을 선택합니다.
여러 LUN을 오프라인 상태로 전환	<ol style="list-style-type: none">1. 오프라인 상태로 전환할 LUN을 선택합니다.2. More * 를 클릭하고 * Take Offline * 을 선택합니다.

CLI를 참조하십시오

CLI를 사용할 때는 한 번에 하나의 LUN만 오프라인 상태로 전환할 수 있습니다.

단계

1. LUN을 오프라인 상태로 전환:

```
lun offline <lun_name> -vserver <SVM_name>
```

ONTAP에서 LUN 크기를 조정합니다

LUN 크기를 늘리거나 줄일 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. ["수행할 수 있습니다"](#) 저장 장치의 크기를 늘리려면. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.



Solaris LUN의 크기는 조정할 수 없습니다.

LUN의 크기를 늘립니다

LUN을 늘릴 수 있는 크기는 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	최대 LUN 크기입니다
ONTAP 9.12.1P2 이상	AFF, FAS 및 ASA 플랫폼의 경우 128TB

ONTAP 9.8 이상	<ul style="list-style-type: none"> • ASA(All-Flash SAN 어레이) 플랫폼의 경우 128TB • 비 ASA 플랫폼의 경우 16TB
ONTAP 9.5, 9.6, 9.7	16TB
ONTAP 9.4 이하	원래 LUN 크기의 10배이지만 최대 LUN 크기인 16TB를 넘지 않습니다. 예를 들어 100GB LUN을 생성하는 경우 1,000GB로만 확장할 수 있습니다. LUN의 실제 최대 크기는 정확히 16TB가 아닐 수 있습니다. ONTAP는 한계치를 약간 낮추어 줍니다.

크기를 늘리기 위해 LUN을 오프라인 상태로 전환하지 않아도 됩니다. 그러나 크기를 늘린 후에는 호스트에서 LUN을 재검색하여 크기 변경을 인식해야 합니다.

예 4. 단계

시스템 관리자

ONTAP 시스템 관리자(9.7 이상)를 사용하여 LUN의 크기를 늘립니다.

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 을  클릭하고 * 편집 * 을 선택합니다.
3. 스토리지 및 최적화 * 에서 LUN의 크기를 늘리고 * 저장 * 을 클릭합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 LUN의 크기를 늘립니다.

1. LUN 크기를 늘립니다.

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

에 대한 자세한 내용은 `lun resize` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. 늘어난 LUN 크기 확인:

```
lun show -vserver <SVM_name>
```

ONTAP 작업은 LUN의 실제 최대 크기를 반올림하여 예상 값보다 약간 작습니다. 또한 실제 LUN 크기는 LUN의 OS 유형에 따라 약간 다를 수 있습니다. 정확한 크기 조정 값을 얻으려면 고급 모드에서 다음 명령을 실행합니다.

```
set -unit B
```

```
lun show -fields max-resize-size -volume volume_name -lun lun_name
```

+

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

1. 호스트에서 LUN을 다시 검색합니다.
2. 호스트 문서에 따라 새로 생성된 LUN 크기를 호스트 파일 시스템에 표시합니다.

LUN 크기를 줄입니다

LUN 크기를 줄이기 전에 호스트는 LUN 데이터가 포함된 블록을 더 작은 LUN 크기의 바운더리로 마이그레이션해야 합니다. SnapCenter와 같은 툴을 사용하면 LUN 데이터가 포함된 블록을 잘라내지 않고도 LUN이 제대로 감소하는지 확인할 수 있습니다. LUN 크기를 수동으로 줄이는 것은 권장되지 않습니다.

LUN 크기를 줄이면 ONTAP에서 자동으로 LUN 크기가 줄어들었음을 이니시에이터에 알립니다. 그러나 호스트에서 새 LUN 크기를 인식하려면 추가 단계가 필요할 수 있습니다. 호스트 파일 구조의 크기 감소에 대한 자세한 내용은 호스트 설명서를 참조하십시오.

LUN을 이동합니다

SVM(스토리지 가상 시스템) 내의 볼륨 간에 LUN을 이동할 수 있지만 SVM 간에 LUN을 이동할 수는 없습니다. SVM 내에서 볼륨 간에 이동하는 LUN은 연결 끊김 없이 즉시 이동됩니다.

시작하기 전에

LUN이 SLM(선택적 LUN 맵)을 사용하는 경우 다음을 수행해야 합니다 "[SLM reporting-nodes 목록을 수정합니다](#)" LUN을 이동하기 전에 대상 노드 및 해당 HA 파트너를 포함해야 합니다.

이 작업에 대해

LUN 이동 중에는 중복제거, 압축, 컴팩션과 같은 스토리지 효율성 기능이 유지되지 않습니다. LUN 이동이 완료된 후 다시 적용해야 합니다.

스냅샷을 통한 데이터 보호는 볼륨 레벨에서 발생합니다. 따라서 LUN을 이동하면 대상 볼륨의 데이터 보호 체계에 따라 이동됩니다. 대상 볼륨에 대해 설정된 스냅샷이 없으면 LUN의 스냅샷이 생성되지 않습니다. 또한 LUN의 모든 스냅샷은 해당 스냅샷이 삭제될 때까지 원래 볼륨에 유지됩니다.

LUN을 다음 볼륨으로 이동할 수 없습니다.

- SnapMirror 타겟 볼륨
- SVM 루트 볼륨

다음 유형의 LUN을 이동할 수 없습니다.

- 파일에서 생성된 LUN입니다
- NVFail 상태인 LUN
- 로드 공유 관계에 있는 LUN입니다
- 프로토콜 엔드포인트 클래스 LUN

클러스터의 노드가 서로 다른 ONTAP 버전을 사용하는 경우, 소스 볼륨이 대상 볼륨보다 최신 버전인 경우에만 서로 다른 노드의 볼륨 간에 LUN을 이동할 수 있습니다. 예를 들어, 소스 볼륨의 노드가 ONTAP 9.15.1이고 대상 볼륨의

노드가 ONTAP 9.16.1인 경우 LUN을 이동할 수 없습니다. 동일한 ONTAP 버전을 사용하는 노드의 볼륨 간에는 LUN을 이동할 수 있습니다.



1TB 이상인 Solaris OS_TYPE LUN의 경우 LUN 이동 중에 호스트에서 시간 초과가 발생할 수 있습니다. 이 LUN 유형의 경우 이동을 시작하기 전에 LUN을 마운트 해제해야 합니다.

예 5. 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 LUN을 이동합니다.

ONTAP 9.10.1부터 단일 LUN을 이동할 때 시스템 관리자를 사용하여 새 볼륨을 생성할 수 있습니다. ONTAP 9.8 및 9.9.1에서는 LUN 이동을 시작하기 전에 LUN을 이동할 볼륨이 있어야 합니다.

단계

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 이동할 LUN을 마우스 오른쪽 버튼으로  클릭한 다음 * Move LUN * 을 선택합니다.

ONTAP 9.10.1에서 LUN을 * 기존 볼륨 * 또는 * 새 볼륨 * 으로 이동하려면 선택합니다.

새 볼륨을 생성하도록 선택한 경우 볼륨 사양을 제공합니다.
3. 이동 * 을 클릭합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 LUN을 이동합니다.

1. LUN 이동:

```
lun move start
```

매우 짧은 기간 동안 원본 볼륨과 대상 볼륨 모두에 LUN이 표시됩니다. 이는 예상되며 이동이 완료되면 해결됩니다.

2. 이동 상태를 추적하고 성공적으로 완료되었는지 확인합니다.

```
lun move show
```

관련 정보

- ["선택적 LUN 맵입니다"](#)

LUN을 삭제합니다

LUN이 더 이상 필요하지 않은 경우 SVM(스토리지 가상 시스템)에서 LUN을 삭제할 수

있습니다.

시작하기 전에

LUN을 삭제하기 전에 해당 igroup에서 매핑 해제해야 합니다.

단계

1. 애플리케이션 또는 호스트에서 LUN을 사용하고 있지 않은지 확인합니다.
2. igroup에서 LUN 매핑을 해제합니다.

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name> -igroup <igroup_name>
```

3. LUN을 삭제합니다.

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. LUN을 삭제했는지 확인합니다.

```
lun show -vserver <SVM_name>
```

Vserver	Path	State	Mapped	Type	Size
vs5	/vol/vol16/lun8	online	mapped	windows	10.00GB

LUN을 복제하기 전에 알아야 할 사항

LUN을 복제하기 전에 몇 가지 사항을 숙지해야 합니다.

클러스터 관리자는 'lun copy' 명령을 사용하여 클러스터 내의 SVM(스토리지 가상 머신)에서 LUN을 복제할 수 있습니다. 클러스터 관리자는 SVM 간 LUN 복사 작업을 수행하기 전에 'vserver peer create' 명령을 사용하여 SVM(스토리지 가상 시스템) 피어링 관계를 설정해야 합니다. 소스 볼륨에 SIS 클론에 대한 충분한 공간이 있어야 합니다.

스냅샷의 LUN은 명령의 소스 LUN으로 사용할 수 `lun copy` 있습니다. 명령을 사용하여 LUN을 복제하면 `lun copy` LUN 복사본을 읽기 및 쓰기 액세스에 즉시 사용할 수 있습니다. LUN 복제본을 생성해도 소스 LUN은 변경되지 않습니다. 소스 LUN과 LUN 복제본은 모두 LUN 일련 번호가 서로 다른 고유한 LUN으로 존재합니다. 소스 LUN에 대한 변경 내용은 LUN 복제본에 반영되지 않으며 LUN 복제본에 대한 변경 내용은 소스 LUN에 반영되지 않습니다. 소스 LUN의 LUN 매핑은 새 LUN에 복제되지 않으므로 LUN 복제본을 매핑해야 합니다.

스냅샷을 통한 데이터 보호는 볼륨 레벨에서 발생합니다. 따라서 LUN을 소스 LUN의 볼륨과 다른 볼륨으로 복제하는 경우 대상 LUN은 대상 볼륨의 데이터 보호 체계에 따라 달라집니다. 대상 볼륨에 대해 설정된 스냅샷이 없는 경우 LUN 복제본의 스냅샷이 생성되지 않습니다.

LUN을 복사하는 것은 무중단 운영입니다.

다음 유형의 LUN은 복제할 수 없습니다.

- 파일에서 생성된 LUN입니다
- NVFAIL 상태에 있는 LUN
- 로드 공유 관계에 있는 LUN입니다
- 프로토콜 엔드포인트 클래스 LUN

에 대한 자세한 내용은 `lun copy` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

LUN의 구성 및 사용 공간을 검사합니다

LUN에 사용된 구성된 공간과 실제 공간을 알면 공간 재확보, 데이터가 포함된 예약된 공간의 양, LUN에 사용된 실제 크기와 비교하여 재확보된 공간을 확인할 수 있습니다.

단계

1. 구성된 공간과 LUN에 사용된 실제 공간을 비교하여 확인합니다.

LUN show

다음 예에서는 vs3 스토리지 가상 시스템(SVM)에서 LUN이 사용하는 실제 공간과 구성된 공간을 비교하여 보여줍니다.

'`lun show -vserver vs3`' - 필드 경로, 크기, 사용된 크기, 공간 예약

```
vs3 /vol/vol0/lun1 50.01GB disabled 25.00GB
vs3 /vol/vol0/lun1_backup 50.01GB disabled 32.15GB
vs3 /vol/vol0/lun2 75.00GB disabled 0B
vs3 /vol/vol0/vospace/lun0 5.00GB enabled 4.50GB
4 entries were displayed.
```

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

스토리지 **QoS**를 사용하여 **LUN**에 대한 **I/O** 성능을 제어 및 모니터링합니다

스토리지 QoS 정책 그룹에 LUN을 할당하여 LUN에 대한 입출력 성능을 제어할 수 있습니다. 입출력 성능을 제어하여 워크로드가 특정 성능 목표를 달성하도록 보장하고, 다른 워크로드에 부정적인 영향을 주는 워크로드를 조절할 수 있습니다.

이 작업에 대해

정책 그룹은 최대 처리량 제한(예: 100MB/s)을 적용합니다. 최대 처리량을 지정하지 않고 정책 그룹을 생성하면 워크로드를 제어하기 전에 성능을 모니터링할 수 있습니다.

FlexVol 볼륨 및 LUN이 있는 SVM(스토리지 가상 시스템)을 정책 그룹에 할당할 수도 있습니다.

LUN을 정책 그룹에 할당하는 것에 대한 다음 요구 사항을 참고하십시오.

- LUN은 정책 그룹이 속한 SVM에 의해 포함되어야 합니다.

정책 그룹을 생성할 때 SVM을 지정합니다.

- LUN을 정책 그룹에 할당할 경우 LUN에 포함된 볼륨 또는 SVM을 정책 그룹에 할당할 수 없습니다.

스토리지 QoS를 사용하는 방법에 대한 자세한 내용은 를 참조하십시오 ["시스템 관리 참조"](#).

단계

1. QoS policy-group create 명령을 사용하여 정책 그룹을 생성합니다.

에 대한 자세한 내용은 qos policy-group create ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 정책 그룹에 LUN을 할당하려면 "lun create" 명령 또는 "lun modify" 명령과 함께 -qos-policy-group" 매개 변수를 사용합니다.

에 대한 자세한 내용은 lun ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. QoS 통계 명령어를 이용하여 성능 데이터를 확인할 수 있다.

4. 필요한 경우 QoS policy-group modify 명령을 사용하여 정책 그룹의 최대 처리량 한도를 조정합니다.

에 대한 자세한 내용은 qos policy-group modify ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

LUN을 효과적으로 모니터링하는 데 사용할 수 있는 툴입니다

툴을 사용하면 LUN을 효과적으로 모니터링하고 공간 부족 현상을 방지할 수 있습니다.

- Active IQ Unified Manager은 환경의 모든 클러스터에서 모든 스토리지를 관리할 수 있는 무료 툴입니다.
- System Manager는 ONTAP에 내장된 그래픽 사용자 인터페이스로, 클러스터 레벨에서 스토리지 요구사항을 수동으로 관리할 수 있습니다.
- OnCommand Insight은 스토리지 인프라에 대한 단일 뷰를 제공하며 LUN, 볼륨 및 애그리게이트에 스토리지 공간이 부족할 때 자동 모니터링, 경고 및 보고를 설정할 수 있습니다.

전환된 **LUN**의 기능 및 제한

SAN 환경에서는 7-Mode 볼륨을 ONTAP로 전환하는 동안 서비스 중단이 필요합니다. 전환을 완료하려면 호스트를 종료해야 합니다. 전환 후에는 ONTAP에서 데이터 제공을 시작하기 전에 호스트 구성을 업데이트해야 합니다

호스트를 종료하고 전환을 완료할 수 있는 유지 관리 기간을 예약해야 합니다.

7-Mode에서 운영되는 Data ONTAP에서 ONTAP로 전환된 LUN에는 LUN 관리 방식에 영향을 주는 특정 기능과 제한 사항이 있습니다.

전환된 LUN에서 다음을 수행할 수 있습니다.

- 'lun show' 명령을 사용하여 LUN을 확인합니다

- 'transition 7-mode show' 명령을 사용하여 7-Mode 볼륨에서 전환된 LUN의 인벤토리를 확인합니다

- 7-Mode 스냅샷에서 볼륨을 복원합니다

볼륨을 복원하면 스냅샷에 캡처된 모든 LUN이 전환됩니다

- 명령을 사용하여 7-Mode 스냅샷에서 단일 LUN을 복원합니다 `snapshot restore-file`
- 7-Mode 스냅샷에서 LUN 클론을 생성합니다
- 7-Mode 스냅샷에서 캡처된 LUN의 블록 범위를 복원합니다
- 7-Mode 스냅샷을 사용하여 볼륨의 FlexClone을 생성합니다

전환된 LUN에서는 다음을 수행할 수 없습니다.

- 볼륨에서 캡처된 스냅샷 지원 LUN 클론에 액세스합니다

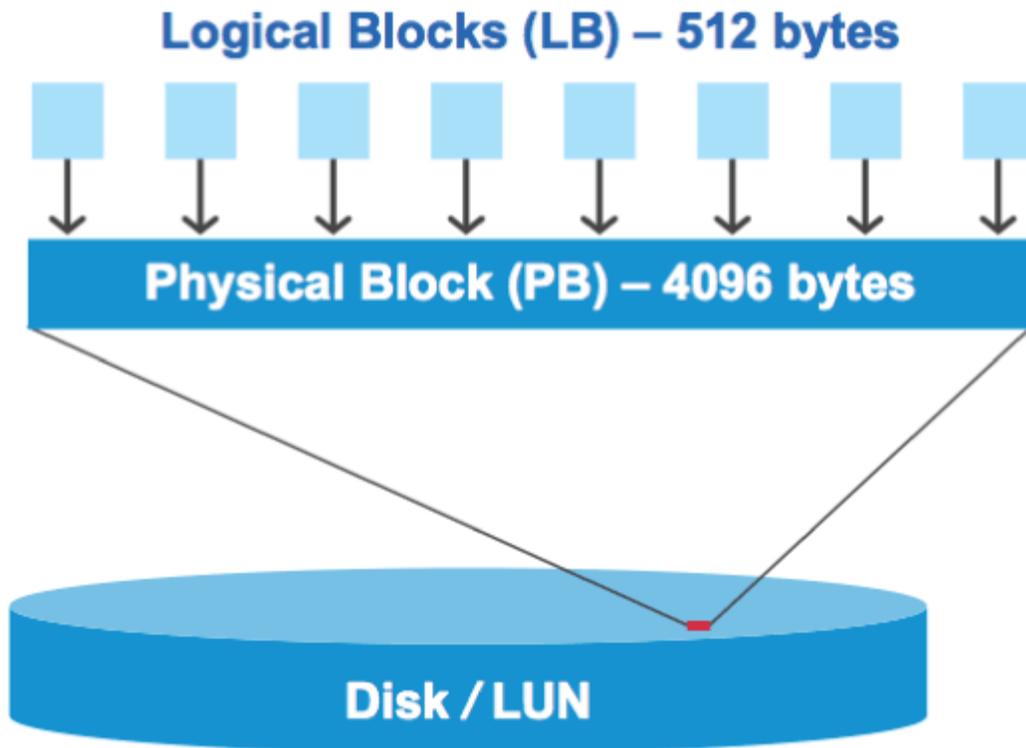
관련 정보

- ["복사 기반 전환"](#)
- ["LUN 표시"](#)

올바르게 정렬된 **LUN**의 입출력 정렬 불량 개요

ONTAP는 올바르게 정렬된 LUN에 대한 I/O 정렬 불량을 보고할 수 있습니다. 일반적으로 이 정렬 불량 경고는 LUN이 제대로 프로비저닝되고 파티셔닝 테이블이 올바른 경우에 무시할 수 있습니다.

LUN과 하드 디스크는 모두 스토리지를 블록으로 제공합니다. 호스트의 디스크에 대한 블록 크기가 512바이트이므로 LUN은 호스트에 해당 크기의 블록을 제공하는 동시에 실제로 더 큰 4KB 블록을 사용하여 데이터를 저장합니다. 호스트에서 사용되는 512바이트 데이터 블록을 논리적 블록이라고 합니다. LUN에서 데이터를 저장하는 데 사용하는 4KB 데이터 블록을 물리적 블록이라고 합니다. 즉, 각 4KB 물리적 블록에는 8개의 512바이트 논리적 블록이 있습니다.



호스트 운영 체제는 모든 논리 블록에서 읽기 또는 쓰기 I/O 작업을 시작할 수 있습니다. I/O 작업은 물리적 블록의 첫 번째 논리적 블록에서 시작될 때만 정렬되는 것으로 간주됩니다. 물리적 블록의 시작이 아닌 논리적 블록에서 I/O 작업이 시작되면 I/O가 잘못 정렬된 것으로 간주됩니다. ONTAP는 자동으로 정렬 불량을 감지하여 LUN에 보고합니다. 하지만 잘못 정렬된 I/O가 있다고 해서 LUN도 제대로 정렬되지 않은 것은 아닙니다. 잘못 정렬된 I/O가 제대로 정렬된 LUN에 보고될 수 있습니다.

추가 조사가 필요한 경우 다음을 참조하세요. ["NetApp 지식 기반: LUN에서 정렬되지 않은 IO를 식별하는 방법은 무엇입니까?"](#)

정렬 문제 해결을 위한 도구에 대한 자세한 내용은 다음 설명서를 참조하십시오: +

- ["Windows Unified Host Utilities 7.1"](#)
- ["SAN 스토리지 설명서를 프로비저닝합니다"](#)

LUN OS 유형을 사용하여 I/O를 조정할 수 있습니다

ONTAP 9.7 이하 버전의 경우 권장 ONTAP LUN을 사용해야 합니다 `ostype` OS 파티셔닝 스키마에 I/O를 정렬하기 위해 운영 체제에 가장 일치하는 값

호스트 운영 체제에서 사용되는 파티션 구조는 I/O 정렬 불량을 크게 유발하는 요소입니다. 일부 ONTAP LUN "OSType" 값에는 호스트 운영 체제에서 사용하는 기본 파티셔닝 구조를 정렬할 수 있도록 "접두사"라고 하는 특수 오프셋을 사용합니다.



경우에 따라 I/O를 정렬하기 위해 사용자 지정 파티셔닝 테이블이 필요할 수 있습니다. 그러나 접두사 값이 0보다 큰 OSType 값에서는 사용자 지정 파티션이 잘못 정렬된 I/O를 생성할 수 있습니다

ONTAP 9.7 또는 이전 버전에서 프로비저닝된 LUN에 대한 자세한 내용은 다음을 참조하세요. ["NetApp 기술 자료: LUN에서 정렬되지 않은 IO를 식별하는 방법"](#) .



기본적으로 ONTAP 9.8 이상에서 프로비저닝된 새 LUN은 모든 LUN OS 유형에 대한 접두사 및 접미사 크기가 0입니다. I/O는 기본적으로 지원되는 호스트 운영 체제에 맞춰 정렬되어야 합니다.

Linux에 대한 특수 I/O 정렬 고려 사항

Linux 배포판은 데이터베이스, 다양한 볼륨 관리자 및 파일 시스템을 위한 원시 디바이스로 LUN을 사용하는 다양한 방법을 제공합니다. 원시 디바이스로 사용하거나 논리적 볼륨에서 물리적 볼륨으로 사용할 경우 LUN에 파티션을 생성할 필요가 없습니다.

RHEL 5 이전 및 SLES 10 이전 버전의 경우, 볼륨 관리자 없이 LUN을 사용할 경우, 정렬된 오프셋에서 시작하는 하나의 파티션을 LUN에 분할해야 합니다. 이 파티션은 8개의 논리적 블록의 짝수 배수로 이루어진 섹터입니다.

Solaris LUN에 대한 특수 I/O 정렬 고려 사항

'솔리스' OSType을 사용할지, '솔리스_EFI' OSType을 사용할지 결정할 때는 다양한 요소를 고려해야 합니다.

를 참조하십시오 ["Solaris 호스트 유틸리티 설치 및 관리 가이드"](#) 을 참조하십시오.

ESX 부팅 LUN이 잘못 정렬되었습니다

ESX 부팅 LUN으로 사용되는 LUN은 일반적으로 ONTAP에서 정렬 불량이라고 보고합니다. ESX는 부팅 LUN에 여러 파티션을 생성하므로 정렬하기가 매우 어렵습니다. 잘못 정렬된 ESX 부팅 LUN은 일반적으로 성능 문제가 되지 않습니다. 잘못 정렬된 입출력의 총량이 작기 때문입니다. LUN이 VMware "OSType"으로 올바르게 프로비저닝되었다고 가정할 경우 별도의 작업이 필요하지 않습니다.

관련 정보

["VMware vSphere, 기타 가상 환경 및 NetApp 스토리지 시스템에 대한 게스트 VM 파일 시스템 파티션/디스크 정렬"](#)

LUN이 오프라인 상태가 될 때 발생하는 문제를 해결하는 방법

쓰기에 사용할 수 있는 공간이 없으면 LUN이 오프라인 상태가 되어 데이터 무결성을 유지합니다. LUN의 공간이 부족하고 다양한 이유로 인해 오프라인 상태가 될 수 있으며 문제를 해결할 수 있는 몇 가지 방법이 있습니다.

만약...	할 수 있는 일...
Aggregate가 가득 찼습니다	<ul style="list-style-type: none"> 디스크를 더 추가합니다. 'volume modify' 명령을 사용하여 사용 가능한 공간이 있는 볼륨을 축소합니다. 사용 가능한 공간이 있는 공간 보장 볼륨이 있는 경우 볼륨 수정 명령을 사용하여 볼륨 공간 보장을 "없음"으로 변경합니다.

만약...	할 수 있는 일...
볼륨이 가득 찼지만 포함된 애그리게이트에 사용 가능한 공간이 있습니다	<ul style="list-style-type: none"> 공간 보장 볼륨의 경우 볼륨 크기를 늘리려면 'volume modify' 명령을 사용하십시오. 썸 프로비저닝된 볼륨의 경우 'volume modify' 명령을 사용하여 볼륨의 최대 크기를 늘리십시오. <p>볼륨 자동 증가를 사용하지 않는 경우 'volume modify-en자동 확장 모드'를 사용하여 활성화하십시오.</p> <ul style="list-style-type: none"> 명령을 사용하여 스냅샷을 수동으로 volume snapshot delete 삭제하거나 명령을 사용하여 volume snapshot autodelete modify 스냅샷을 자동으로 삭제합니다.

관련 정보

["디스크 및 로컬 계층\(애그리게이트\) 관리"](#)

["논리적 스토리지 관리"](#)

호스트에 표시되지 않는 **iSCSI LUN** 문제를 해결합니다

iSCSI LUN은 호스트에 로컬 디스크로 표시됩니다. 스토리지 시스템 LUN을 호스트에서 디스크로 사용할 수 없는 경우 구성 설정을 확인해야 합니다.

구성 설정	할 일
케이블 연결	호스트와 스토리지 시스템 사이의 케이블이 올바르게 연결되었는지 확인합니다.
네트워크 연결	<p>호스트와 스토리지 시스템 간에 TCP/IP 접속이 설정되어 있는지 확인합니다.</p> <ul style="list-style-type: none"> 스토리지 시스템 명령줄에서 iSCSI에 사용 중인 호스트 인터페이스를 ping합니다. "ping -node_node_name_-destination_host_ip_address_for_iscsi_" 호스트 명령줄에서 iSCSI에 사용 중인 스토리지 시스템 인터페이스를 ping합니다. "ping -node_node_name_-destination_host_ip_address_for_iscsi_"
시스템 요구 사항	구성 요소의 자격 여부를 확인합니다. 또한 호스트 운영 체제(OS) 서비스 팩 수준, 이니시에이터 버전, ONTAP 버전 및 기타 시스템 요구 사항이 올바른지 확인합니다. 상호 운용성 매트릭스에는 최신 시스템 요구 사항이 포함되어 있습니다.
점보 프레임	구성에서 점보 프레임을 사용하는 경우 네트워크 경로의 모든 장치(호스트 이더넷 NIC, 스토리지 시스템 및 모든 스위치)에서 점보 프레임이 활성화되어 있는지 확인합니다.
iSCSI 서비스 상태입니다	iSCSI 서비스에 라이선스가 부여되어 스토리지 시스템에서 시작되었는지 확인합니다.

구성 설정	할 일
초기자 로그인	이니시에이터가 스토리지 시스템에 로그인되어 있는지 확인합니다. "iscsi initiator show" 명령 출력에 로그인한 이니시에이터가 없는 경우 호스트에서 이니시에이터 구성을 확인하십시오. 스토리지 시스템이 이니시에이터의 타겟으로 구성되어 있는지도 확인합니다.
iSCSI 노드 이름(IQN)	igroup 구성에서 올바른 이니시에이터 노드 이름을 사용하고 있는지 확인합니다. 호스트에서 이니시에이터 툴 및 명령을 사용하여 이니시에이터 노드 이름을 표시할 수 있습니다. igroup 및 호스트에 구성된 이니시에이터 노드 이름이 일치해야 합니다.
LUN 매핑	LUN이 igroup에 매핑되어 있는지 확인합니다. 스토리지 시스템 콘솔에서 다음 명령 중 하나를 사용할 수 있습니다. <ul style="list-style-type: none"> • LUN mapping show는 모든 LUN과 매핑된 igroup을 표시합니다. • 'lun mapping show -igroup'은 특정 igroup에 매핑된 LUN을 표시합니다.
iSCSI LIF가 사용하도록 설정합니다	iSCSI 논리 인터페이스가 활성화되었는지 확인합니다.

관련 정보

- ["NetApp 상호 운용성 매트릭스 툴"](#)
- ["LUN 매핑이 표시됩니다"](#)

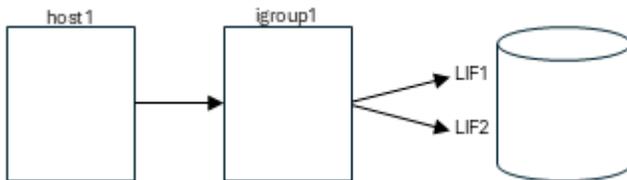
Igroup 및 portset 관리

포트 세트 및 **igroup**을 사용하여 **LUN** 액세스를 제한하는 방법

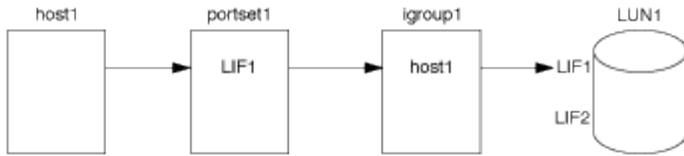
SLM(Selective LUN Map)을 사용하는 것 외에도 igroup 및 포트 세트를 통해 LUN에 대한 액세스를 제한할 수 있습니다.

Portset을 SLM과 함께 사용하여 특정 타겟에 대한 액세스를 특정 이니시에이터에 추가로 제한할 수 있습니다. 포트 세트와 함께 SLM을 사용하는 경우 LUN을 소유한 노드의 HA 파트너와 해당 노드의 포트셋 LIF 세트에서 LUN에 액세스할 수 있습니다.

다음 예에서 host1에는 포트셋이 없습니다. 포트셋이 없으면 host1은 LIF1과 LIF2를 통해 LUN1에 액세스할 수 있습니다.



포트셋을 사용하여 LUN1에 대한 액세스를 제한할 수 있습니다. 다음 예에서 host1은 LIF1을 통해서만 LUN1에 액세스할 수 있습니다. 하지만 LIF2가 portset1에 없기 때문에 host1은 LIF2를 통해 LUN1에 액세스할 수 없습니다.



관련 정보

- [선택적 LUN 맵입니다](#)
- [포트셋 및 igroup에 바인딩](#)

SAN 이니시에이터 및 igroup을 보고 관리합니다

System Manager를 사용하여 이니시에이터 그룹(igroup)과 이니시에이터를 보고 관리할 수 있습니다.

이 작업에 대해

- 이니시에이터 그룹은 스토리지 시스템의 특정 LUN에 액세스할 수 있는 호스트를 식별합니다.
- 이니시에이터 및 이니시에이터 그룹을 생성한 후 편집하거나 삭제할 수 있습니다.
- SAN 이니시에이터 그룹 및 이니시에이터를 관리하려면 다음 작업을 수행할 수 있습니다.
 - [\[view-manage-san-igroups\]](#)
 - [\[view-manage-san-inits\]](#)

SAN 이니시에이터 그룹을 보고 관리합니다

System Manager를 사용하여 이니시에이터 그룹(igroup) 목록을 볼 수 있습니다. 목록에서 추가 작업을 수행할 수 있습니다.

단계

1. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.

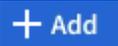
페이지에 이니시에이터 그룹(igroup) 목록이 표시됩니다. 목록이 큰 경우 페이지의 오른쪽 아래 모서리에 있는 페이지 번호를 클릭하여 목록의 추가 페이지를 볼 수 있습니다.

열에는 igroup에 대한 다양한 정보가 표시됩니다. 9.11.1부터 igroup의 연결 상태도 표시됩니다. 상태 알림 위로 마우스를 가져가면 세부 정보가 표시됩니다.

2. (선택 사항): 목록의 오른쪽 위에 있는 아이콘을 클릭하여 다음 작업을 수행할 수 있습니다.

- * 검색 *
- * 목록을 다운로드 * 합니다.
- 목록에서 * 표시 * 또는 * 숨기기 * 열을 표시합니다.
- * 필터 * 목록의 데이터.

3. 목록에서 작업을 수행할 수 있습니다.

-  **Add** igroup을 추가하려면 클릭합니다.
- igroup 이름을 클릭하여 igroup에 대한 세부 정보를 보여주는 * Overview * 페이지를 표시합니다.

개요 * 페이지에서 igroup과 연결된 LUN을 볼 수 있으며 작업을 시작하여 LUN을 생성하고 LUN을 매핑할 수 있습니다. 기본 목록으로 돌아가려면 * 모든 SAN 이니시에이터 * 를 클릭합니다.

- igroup에 마우스를 올려놓고 igroup 이름 옆에 있는 을 클릭하여 : igroup을 편집하거나 삭제합니다.
- igroup 이름 왼쪽에 있는 영역 위로 마우스를 가져간 다음 확인란을 선택합니다. 이니시에이터 그룹에 * + 추가를 클릭하면 해당 igroup을 다른 igroup에 추가할 수 있습니다.
- 스토리지 VM * 열에서 스토리지 VM의 이름을 클릭하여 해당 VM에 대한 세부 정보를 봅니다.

SAN 이니시에이터를 보고 관리합니다

System Manager를 사용하여 이니시에이터 목록을 볼 수 있습니다. 목록에서 추가 작업을 수행할 수 있습니다.

단계

1. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.

페이지에 이니시에이터 그룹(igroup) 목록이 표시됩니다.

2. 이니시에이터를 보려면 다음을 수행하십시오.

- FC 이니시에이터 * 탭을 클릭하여 FC 이니시에이터 목록을 표시합니다.
- iSCSI 초기자 목록을 보려면 * iSCSI 초기자 * 탭을 클릭합니다.

열에는 이니시에이터에 대한 다양한 정보가 표시됩니다.

9.11.1부터 초기자의 연결 상태도 표시됩니다. 상태 알림 위로 마우스를 가져가면 세부 정보가 표시됩니다.

3. (선택 사항): 목록의 오른쪽 위에 있는 아이콘을 클릭하여 다음 작업을 수행할 수 있습니다.

- * 검색 * 특정 이니시에이터 목록입니다.
- * 목록을 다운로드 * 합니다.
- 목록에서 * 표시 * 또는 * 숨기기 * 열을 표시합니다.
- * 필터 * 목록의 데이터.

중첩된 igroup을 생성합니다

ONTAP 9.9.1부터 다른 기존 igroup으로 구성된 igroup을 생성할 수 있습니다.

1. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭한 다음 * 추가 * 를 클릭합니다.

2. igroup * 이름 * 및 * 설명 * 을 입력합니다.

설명에는 igroup 별칭으로 사용됩니다.

3. 스토리지 VM * 및 * 호스트 운영 체제 * 를 선택합니다.



igroup이 생성된 후 중첩된 igroup의 OS 유형을 변경할 수 없습니다.

4. 이니시에이터 그룹 구성원 * 에서 * 기존 이니시에이터 그룹 * 을 선택합니다.

검색 * 을 사용하여 추가할 이니시에이터 그룹을 찾아서 선택할 수 있습니다.

여러 LUN에 igroup 매핑

ONTAP 9.9.1부터 igroup을 2개 이상의 LUN에 동시에 매핑할 수 있습니다.

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 매핑할 LUN을 선택합니다.
3. More * 를 클릭한 다음 * Map to Initiator Groups * 를 클릭합니다.



선택한 igroup이 선택한 LUN에 추가됩니다. 기존 매핑은 덮어쓰지 않습니다.

포트셋 및 igroup에 바인딩

또한 를 사용할 수 있습니다 "**선택적 LUN 맵(SLM)**" 포트셋 를 생성하고 포트셋 를 igroup에 바인딩하여 이니시에이터에서 LUN에 액세스하는 데 사용할 수 있는 LIF를 더 제한할 수 있습니다.

포트셋 를 igroup에 바인딩하지 않으면 igroup의 모든 이니시에이터가 LUN과 소유 노드의 HA 파트너가 소유하는 노드의 모든 LIF를 통해 매핑된 LUN에 액세스할 수 있습니다.

시작하기 전에

LIF가 하나 이상, igroup 하나가 있어야 합니다.

인터페이스 그룹을 사용하지 않는 경우 iSCSI와 FC 모두에서 중복성을 위해 두 개의 LIF가 권장됩니다. 인터페이스 그룹에서는 LIF가 하나만 권장됩니다.

이 작업에 대해

노드에 LIF가 2개 이상 있고 특정 이니시에이터를 LIF의 하위 집합으로 제한하려는 경우 SLM에 Portset을 사용하는 것이 좋습니다. 포트 세트가 없으면 LUN 및 소유 노드의 HA 파트너를 소유하는 노드를 통해 LUN에 액세스할 수 있는 모든 이니시에이터가 노드의 모든 타겟에 액세스할 수 있습니다.

예 6. 단계

시스템 관리자

ONTAP 9.10.1부터 System Manager를 사용하여 포트 세트를 생성하고 igroup에 바인딩할 수 있습니다.

9.10.1 이전의 ONTAP 릴리즈에서 포트셋 및 igroup을 바인딩해야 하는 경우 ONTAP CLI 절차를 사용해야 합니다.

ONTAP 9.12.1부터 기존 포트셋이 없으면 ONTAP CLI 프로시저를 사용하여 첫 번째 포트셋을 만들어야 합니다.

1. System Manager에서 * Network > Overview > Portsets * 를 클릭하고 * Add * 를 클릭합니다.
2. 새 포트셋 정보를 입력하고 * 추가 * 를 클릭합니다.
3. 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.
4. 포트셋 를 새 igroup에 바인딩하려면 * 추가 * 를 클릭합니다.

포트셋 을 기존 igroup에 바인딩하려면 igroup을 선택하고 를  클릭한 다음 * 이니시에이터 그룹 편집 * 을 클릭합니다.

관련 정보

["이니시에이터 및 igroup을 보고 관리합니다"](#)

CLI를 참조하십시오

1. 적절한 LIF가 포함된 포트 세트를 생성합니다.

```
' create-vserver_vserver_name_-포트셋_이름_-protocol_protocol_-port-name_port_name_ '
```

FC를 사용하는 경우 프로토콜 매개변수를 FCP로 지정합니다. iSCSI를 사용하는 경우 프로토콜 매개변수를 iSCSI로 지정합니다.

2. igroup을 포트 세트에 바인드합니다.

```
'lun igroup bind -vserver_vserver_name_-igroup_igroup_name_-포트셋_포트셋_이름_'
```

에 대한 자세한 내용은 lun igroup bind ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

3. 포트 세트와 LIF가 올바른지 확인합니다.

```
' show-vserver_vserver_name_ '
```

Vserver	Portset	Protocol	Port Names	Igroups
vs3	portset0	iscsi	lif0,lif1	igroup1

포트세트를 관리합니다

또한 ["선택적 LUN 맵\(SLM\)"](#) 포트 세트를 사용하여 이니시에이터에서 LUN에 액세스하는 데

사용할 수 있는 LIF를 추가로 제한할 수 있습니다.

ONTAP 9.10.1부터 System Manager를 사용하여 포트 세트와 관련된 네트워크 인터페이스를 변경하고 포트 세트를 삭제할 수 있습니다.

포트셋 관련 네트워크 인터페이스를 변경합니다

1. System Manager에서 * Network > Overview > Portsets * 를 선택합니다.
2. 편집할 포트셋 을 선택한 다음 * 포트세트 편집 * 을 선택합니다.

포트셋 삭제

1. System Manager에서 * Network > Overview > Portsets * 를 클릭합니다.
2. 포트셋 하나를 삭제하려면 포트셋, 선택 후 * 포트세트 삭제 * 를 선택합니다.

여러 개의 포트 세트를 삭제하려면 포트 세트를 선택하고 * Delete * (삭제 *)를 클릭합니다.

선택적 LUN 맵 개요

SLM(Selective LUN Map)은 호스트에서 LUN으로의 경로 수를 줄입니다. SLM 기능을 통해 새 LUN 맵이 생성되면 LUN 및 해당 HA 파트너를 소유하는 노드의 경로를 통해서만 LUN에 액세스할 수 있습니다.

SLM은 호스트당 단일 igroup을 관리할 수 있도록 하며, 포트셋 조작 또는 LUN 재매핑이 필요하지 않은 무중단 LUN 이동 작업도 지원합니다.

"포트 세트" SLM과 함께 사용하여 특정 타겟에 대한 액세스를 특정 이니시에이터에 더 제한할 수 있습니다. 포트 세트와 함께 SLM을 사용하는 경우 LUN을 소유한 노드의 HA 파트너와 해당 노드의 포트셋 LIF 세트에서 LUN에 액세스할 수 있습니다.

SLM은 모든 새로운 LUN 맵에서 기본적으로 활성화됩니다.

LUN 맵에서 SLM이 설정되었는지 여부를 확인합니다

환경에 ONTAP 9 릴리즈에서 생성된 LUN과 이전 버전에서 전환된 LUN의 조합이 있는 경우, 특정 LUN에 SLM(선택적 LUN 맵)이 활성화되어 있는지 여부를 확인해야 할 수 있습니다.

의 출력에 표시된 정보를 사용할 수 있습니다 `lun mapping show -fields reporting-nodes, node` 명령을 사용하여 LUN 맵에서 SLM이 활성화되어 있는지 여부를 확인합니다. SLM이 활성화되지 않은 경우 명령 출력의 "노드 재이식" 열 아래의 셀에 "-"가 표시됩니다. SLM이 활성화된 경우 ""노드" 열 아래에 표시되는 노드 목록이 "노드 재이식" 열에 복제됩니다.

에 대한 자세한 내용은 `lun mapping show` "ONTAP 명령 참조입니다"을 참조하십시오.

SLM 보고 노드 목록을 수정합니다

LUN이 포함된 LUN 또는 볼륨을 동일한 클러스터 내의 다른 고가용성(HA) 쌍으로 이동하는 경우, 이동을 시작하기 전에 선택 LUN 맵(SLM: Selective LUN Map) 보고 노드 목록을 수정하여 최적화된 활성 LUN 경로가 유지되도록 해야 합니다.

단계

1. 대상 노드와 해당 파트너 노드를 애그리게이트 또는 볼륨의 보고 노드 목록에 추가합니다.

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

일관된 명명 규칙이 있는 경우 대신 `l` 사용하여 여러 LUN 매핑을 동시에 수정할 수 있습니다 `igroup_prefix* igroup_name`.

2. 호스트를 재검색하여 새로 추가된 경로를 검색합니다.
3. OS에 필요한 경우 다중 경로 네트워크 I/O(MPIO) 구성에 새 경로를 추가합니다.
4. 필요한 이동 작업에 대해 명령을 실행하고 작업이 완료될 때까지 기다립니다.
5. Active/Optimized 경로를 통해 입출력이 서비스되고 있는지 확인합니다.

```
lun mapping show -fields reporting-nodes
```

6. 보고 노드 목록에서 이전 LUN 소유자 및 해당 파트너 노드를 제거합니다.

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. LUN이 기존 LUN 맵에서 제거되었는지 확인합니다.

```
lun mapping show -fields reporting-nodes
```

8. 호스트 OS의 오래된 디바이스 항목을 제거합니다.
9. 필요한 경우 경로 다중화 구성 파일을 변경합니다.
10. 호스트를 재검색하여 이전 경로가 제거되었는지 확인합니다. + 호스트를 재검색하는 특정 단계는 호스트 설명서를 참조하십시오.

iSCSI 프로토콜을 관리합니다

최상의 성능을 위해 네트워크를 구성합니다

이더넷 네트워크의 성능은 매우 다양합니다. 특정 구성 값을 선택하여 iSCSI에 사용되는 네트워크의 성능을 최대화할 수 있습니다.

단계

1. 호스트 및 스토리지 포트를 동일한 네트워크에 연결합니다.

동일한 스위치에 연결하는 것이 가장 좋습니다. 라우팅은 절대 사용해서는 안 됩니다.

2. 사용 가능한 최고 속도 포트를 선택하고 iSCSI에 전용으로 지정합니다.

10GbE 포트가 가장 적합합니다. 1GbE 포트는 최소 포트입니다.

3. 모든 포트에 대해 이더넷 흐름 제어를 사용하지 않도록 설정합니다.

이 표시됩니다 "네트워크 관리" CLI를 사용하여 이더넷 포트 흐름 제어를 구성하는 데 사용됩니다.

4. 점보 프레임(일반적으로 MTU 9000)을 사용하도록 설정합니다.

이니시에이터, 타겟 및 스위치를 비롯한 데이터 경로의 모든 디바이스가 점보 프레임을 지원해야 합니다. 그렇지 않으면 점보 프레임이 실제로 네트워크 성능을 크게 줄입니다.

iSCSI용 SVM을 구성합니다

iSCSI를 위한 SVM(Storage Virtual Machine)을 구성하려면 SVM용 LIF를 생성하고 이러한 LIF에 iSCSI 프로토콜을 할당해야 합니다.

이 작업에 대해

iSCSI 프로토콜로 데이터를 제공하는 SVM은 노드당 최소 하나의 iSCSI LIF가 필요합니다. 이중화를 위해서는 노드당 LIF를 2개 이상 생성해야 합니다.

예 7. 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 iSCSI용 스토리지 VM을 구성합니다.

새 스토리지 VM에서 iSCSI를 구성합니다	기존 스토리지 VM에서 iSCSI를 구성합니다
<ol style="list-style-type: none"> 1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다. 2. 스토리지 VM의 이름을 입력합니다. 3. 액세스 프로토콜 * 에 대해 * iSCSI * 를 선택합니다. 4. iSCSI 활성화 * 를 클릭하고 네트워크 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. + 각 노드에는 최소 2개의 네트워크 인터페이스가 있어야 합니다. 5. 저장 * 을 클릭합니다. 	<ol style="list-style-type: none"> 1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다. 2. 구성할 스토리지 VM을 클릭합니다. 3. 설정 * 탭을 클릭한 다음 iSCSI 프로토콜 옆에 있는  을 클릭합니다. 4. iSCSI 활성화 * 를 클릭하고 네트워크 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. + 각 노드에는 최소 2개의 네트워크 인터페이스가 있어야 합니다. 5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 iSCSI용 스토리지 VM을 구성합니다.

1. SVM이 iSCSI 트래픽을 수신하도록 설정:

```
'vserver iscsi create -vserver vserver_name -target-alias vserver_name_'
```

2. iSCSI에 사용할 SVM을 위한 LIF를 각 노드에서 생성합니다.

- ONTAP 9.6 이상:

```
network interface create -vserver vserver_name -lif lif_name -data
-protocol iscsi -service-policy default-data-iscsi -home-node node_name
-home-port port_name -address ip_address -netmask netmask
```

- ONTAP 9.5 이하:

```
network interface create -vserver vserver_name -lif lif_name -role data
-data-protocol iscsi -home-node node_name -home-port port_name -address
ip_address -netmask netmask
```

3. LIF를 올바르게 설정했는지 확인하십시오.

```
'network interface show -vserver vserver_name_'
```

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

4. iSCSI가 작동 중이고 해당 SVM의 타겟 IQN이 실행 중인지 확인합니다.

```
'vserver iscsi show -vserver vserver_name_'
```

5. 호스트에서 LIF에 iSCSI 세션을 생성합니다.

관련 정보

- ["NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례"](#)

이니시에이터에 대한 보안 정책 방법을 정의합니다

이니시에이터 목록과 해당 인증 방법을 정의할 수 있습니다. 사용자 정의 인증 방법이 없는 이니시에이터에 적용되는 기본 인증 방법을 수정할 수도 있습니다.

이 작업에 대해

제품의 보안 정책 알고리즘을 사용하여 고유한 암호를 생성하거나 사용하려는 암호를 수동으로 지정할 수 있습니다.



일부 이니시에이터는 16진수 CHAP 암호 암호를 지원하지 않습니다.

단계

1. "vserver iSCSI security create" 명령을 사용하여 이니시에이터에 대한 보안 정책 방법을 생성합니다.

```
'vserver iscsi security create-vserver vs2-initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP-user-name byby1-outbound-user-name byby2'
```

2. 화면 명령에 따라 암호를 추가합니다.

인바운드 및 아웃바운드 CHAP 사용자 이름 및 암호를 사용하여 초기자 iqn.1991-05.com.microsoft:host1 에 대한 보안 정책 방법을 만듭니다.

관련 정보

- [iSCSI 인증의 작동 방식](#)
- [CHAP 인증입니다](#)

SVM을 위한 iSCSI 서비스를 삭제합니다

더 이상 필요하지 않은 경우 SVM(스토리지 가상 머신)에 대한 iSCSI 서비스를 삭제할 수 있습니다.

시작하기 전에

iSCSI 서비스를 삭제하려면 먼저 iSCSI 서비스의 관리 상태가 "down" 상태여야 합니다. 'vserver iscsi modify' 명령을 사용하여 관리 상태를 아래로 이동할 수 있습니다.

단계

1. 'vserver iscsi modify' 명령을 사용하여 LUN에 대한 입출력을 중지합니다.

```
'vserver iscsi modify -vserver vs1-status-admin down'
```

2. SVM에서 iSCSI 서비스를 제거하려면 "vserver iSCSI delete" 명령을 사용하십시오.

```
'vserver iscsi delete - vserver vs_1'
```

3. SVM에서 iSCSI 서비스를 삭제했는지 확인하려면 'vserver iscsi show 명령'을 사용하십시오.

```
'vserver iscsi show -vserver vs1'
```

iSCSI 세션 오류 복구에 대한 자세한 내용을 확인하십시오

iSCSI 세션 오류 복구 수준을 높이면 iSCSI 오류 복구에 대한 자세한 정보를 얻을 수 있습니다. 높은 오류 복구 레벨을 사용하면 iSCSI 세션 성능이 약간 저하될 수 있습니다.

이 작업에 대해

기본적으로 ONTAP은 iSCSI 세션에 대해 오류 복구 레벨 0을 사용하도록 구성됩니다. 오류 복구 레벨 1 또는 2에 대해 검증된 이니시에이터를 사용하는 경우 오류 복구 레벨을 증가하도록 선택할 수 있습니다. 수정된 세션 오류 복구 수준은 새로 생성된 세션에만 영향을 미치며 기존 세션에는 영향을 미치지 않습니다.

ONTAP 9.4부터 iSCSI show와 iSCSI modify 명령에서는 max-error-recovery-level 옵션이 지원되지 않습니다.

단계

1. 고급 모드 진입:

세트 프리빌리지 고급

2. "iscsi show" 명령을 사용하여 현재 설정을 확인합니다.

```
'iscsi show -vserver vs3 -fields max-error-recovery-level'
```

```
vserver max-error-recovery-level
-----
vs3      0
```

3. iSCSI modify 명령을 사용하여 오류 복구 수준을 변경합니다.

```
'iscsi modify -vserver vs3 -max-error-recovery-level 2'
```

iSNS 서버를 사용하여 **SVM**을 등록합니다

"vserver iSCSI iSNS" 명령을 사용하여 iSNS 서버에 등록할 SVM(스토리지 가상 시스템)을 구성할 수 있습니다.

이 작업에 대해

'vserver iscsi iSNS create' 명령은 iSNS 서버에 등록할 SVM을 구성합니다. SVM은 iSNS 서버를 구성하거나 관리할 수 있는 명령을 제공하지 않습니다. iSNS 서버를 관리하려면 공급업체에서 제공하는 iSNS 서버 관리 도구 또는 인터페이스를 사용할 수 있습니다.

단계

1. iSNS 서버에서 iSNS 서비스가 작동 가능하고 서비스를 사용할 수 있는지 확인합니다.

2. 데이터 포트에 SVM 관리 LIF를 생성합니다.

```
'network interface create -vserver_SVM_name_-lif_lif_name_-role data-protocol none-home-  
node_home_node_name_-home-port_home_home_home_port_-address_-netmask_network_mask_'
```

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

3. SVM에 iSCSI 서비스가 없는 경우 생성합니다.

```
'vserver iscsi create-vserver_SVM_name_'
```

4. iSCSI 서비스가 성공적으로 생성되었는지 확인합니다.

```
'iscsi show -vserver_SVM_name_'
```

5. SVM에 대한 기본 경로가 있는지 확인합니다.

```
'network route show -vserver_SVM_name_'
```

6. SVM에 대한 기본 경로가 없는 경우 기본 경로를 생성합니다.

```
'network route create-vserver_SVM_name_-destination_destination_-gateway_gateway_'
```

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

7. iSNS 서비스에 등록할 SVM을 구성합니다.

```
'vserver iSCSI iSNS create -vserver_SVM_name_-address_ip_address_'
```

IPv4 및 IPv6 주소 제품군이 모두 지원됩니다. iSNS 서버의 주소 제품군은 SVM 관리 LIF의 주소 제품군과 같아야 합니다.

예를 들어, IPv6 주소를 사용하여 anSVM 관리 LIF를 IPv4 주소와 함께 iSNS 서버에 연결할 수 없습니다.

8. iSNS 서비스가 실행 중인지 확인합니다.

```
'vserver iscsi iSNS show -vserver_SVM_name_'
```

9. iSNS 서비스가 실행되고 있지 않으면 다음을 시작합니다.

```
'vserver iscsi iSNS start -vserver_SVM_name_'
```

스토리지 시스템의 **iSCSI** 오류 메시지를 해결합니다

'event log show' 명령을 사용하여 볼 수 있는 일반적인 iSCSI 관련 오류 메시지가 많이 있습니다. 이러한 메시지의 의미와 해당 메시지가 파악한 문제를 해결하기 위해 수행할 수 있는 작업을 알고 있어야 합니다.

다음 표에는 가장 일반적인 오류 메시지와 해결 지침이 나와 있습니다.

메시지	설명	할 일
'iSCSI: 네트워크 인터페이스 식별자 사용 안 함, 들어오는 연결이 삭제됨'	인터페이스에서 iSCSI 서비스가 활성화되어 있지 않습니다.	"iSCSI interface enable" 명령을 사용하여 인터페이스에서 iSCSI 서비스를 활성화할 수 있습니다. 예를 들면 다음과 같습니다. 'iSCSI interface enable - vserver vs1-lif lif liff li1'
"iSCSI: 이니시에이터 노데이름 인증에 실패했습니다.	지정된 이니시에이터에 대해 CHAP가 올바르게 구성되지 않았습니다.	CHAP 설정을 확인해야 합니다. 스토리지 시스템의 인바운드 및 아웃바운드 설정에 동일한 사용자 이름과 암호를 사용할 수 없습니다. <ul style="list-style-type: none"> • 스토리지 시스템의 인바운드 자격 증명은 이니시에이터의 아웃바운드 자격 증명과 일치해야 합니다. • 스토리지 시스템의 아웃바운드 자격 증명은 이니시에이터의 인바운드 자격 증명과 일치해야 합니다.

에 대한 자세한 내용은 `event log show "ONTAP 명령 참조입니다"`을 참조하십시오.

자동 **iSCSI LIF** 페일오버를 사용 또는 사용하지 않도록 설정합니다

ONTAP 9.11.1 이상으로 업그레이드한 후에는 ONTAP 9.10.1 이전 버전에서 생성된 모든 iSCSI LIF에서 자동 LIF 페일오버를 수동으로 사용하도록 설정해야 합니다.

ONTAP 9.11.1부터 All-Flash SAN 어레이 플랫폼에서 iSCSI LIF에 대한 자동 LIF 페일오버를 활성화할 수 있습니다. 스토리지 페일오버가 발생하는 경우 iSCSI LIF가 홈 노드나 포트에서 HA 파트너 노드 또는 포트로 자동으로 마이그레이션된 다음, 페일오버가 완료되면 다시 뒤로 마이그레이션됩니다. 또는 iSCSI LIF의 포트가 정상 상태가 아닐 경우 LIF는 자동으로 현재 홈 노드의 정상 포트로 마이그레이션된 다음, 포트가 다시 정상 상태가 되면 원래 포트로 다시 돌아갑니다. 를 사용하면 iSCSI에서 실행되는 SAN 워크로드가 페일오버가 발생한 후 I/O 서비스를 더 빠르게 재개할 수 있습니다.

ONTAP 9.11.1 이상에서는 기본적으로 새로 생성된 iSCSI LIF가 다음 조건 중 하나에 해당할 경우 자동 LIF 페일오버에 사용하도록 설정됩니다.

- SVM에 iSCSI LIF가 없습니다
- SVM의 모든 iSCSI LIF는 자동 LIF 페일오버에 사용할 수 있습니다

자동 **iSCSI LIF** 페일오버를 사용합니다

기본적으로 ONTAP 9.10.1 이전 버전에서 생성된 iSCSI LIF는 자동 LIF 페일오버에 사용되지 않습니다. 자동 LIF 페일오버에 사용되지 않는 SVM에 iSCSI LIF가 있으면 새로 생성한 LIF가 자동 LIF 페일오버 중에 사용할 수 없습니다. 자동 LIF 페일오버가 사용되도록 설정되어 있지 않고 페일오버 이벤트가 발생하면 iSCSI LIF가 마이그레이션되지 않습니다.

에 대해 자세히 ["LIF 페일오버 및 반환"](#) 알아보십시오.

단계

1. iSCSI LIF에 대해 자동 페일오버 활성화:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

SVM에서 모든 iSCSI LIF를 업데이트하려면 `l` 를 사용하십시오 `-lif*` 대신 `lif`.

자동 **iSCSI LIF** 페일오버를 해제합니다

이전에 ONTAP 9.10.1 이하 버전에서 생성된 iSCSI LIF에서 자동 iSCSI LIF 페일오버를 사용하도록 설정한 경우 이 기능을 사용하지 않도록 설정할 수 있습니다.

단계

1. iSCSI LIF에 대한 자동 페일오버 비활성화:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

SVM에서 모든 iSCSI LIF를 업데이트하려면 `l` 를 사용하십시오 `-lif*` 대신 `lif`.

관련 정보

- ["LIF를 생성합니다"](#)
- 수동 ["LIF를 마이그레이션합니다"](#)
- 수동 ["LIF를 홈 포트에 되돌립니다"](#)
- ["LIF에서 페일오버 설정을 구성합니다"](#)

FC 프로토콜을 관리합니다

FC용 SVM 구성

FC용 SVM(Storage Virtual Machine)을 구성하려면 SVM용 LIF를 생성하고 이러한 LIF에 FC 프로토콜을 할당해야 합니다.

시작하기 전에

FC 라이선스(["ONTAP One에 포함되어 있습니다"](#))가 있어야 하며 활성화해야 합니다. FC 라이선스가 활성화되지 않으면 LIF 및 SVM이 온라인 상태로 표시되지만 운영 상태는 입니다. `down` LIF 및 SVM이 작동할 수 있도록 FC 서비스를 설정해야 합니다. SVM의 모든 FC LIF에서 이니시에이터를 호스팅하려면 단일 이니시에이터 조닝을 사용해야 합니다.

이 작업에 대해

NetApp은 각 SVM에서 FC 프로토콜을 통해 데이터를 제공하는 FC LIF를 노드당 1개 이상 지원합니다. 노드당 LIF

2개와 Fabric 2개를 사용해야 하며, 연결된 노드당 LIF 1개가 있어야 합니다. 이는 노드 계층과 패브릭에서 이중화를 제공합니다.

예 8. 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 iSCSI용 스토리지 VM을 구성합니다.

새 스토리지 VM에서 FC를 구성합니다	기존 스토리지 VM에서 FC를 구성합니다
<ol style="list-style-type: none"> 1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다. 2. 스토리지 VM의 이름을 입력합니다. 3. 액세스 프로토콜 * 으로 * FC * 를 선택합니다. 4. FC * 활성화 를 클릭합니다. + FC 포트가 자동으로 할당됩니다. 5. 저장 * 을 클릭합니다. 	<ol style="list-style-type: none"> 1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다. 2. 구성할 스토리지 VM을 클릭합니다. 3. 설정 * 탭을 클릭한 다음 FC 프로토콜 옆에 있는 을 클릭합니다  . 4. FC * 활성화 를 클릭하고 네트워크 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. + FC 포트가 자동으로 할당됩니다. 5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. SVM에서 FC 서비스 활성화:

```
'vserver fcp create-vserver_vserver_name_-status-admin up'
```

2. FC를 지원하는 각 노드에서 SVM에 대해 2개의 LIF를 생성합니다.

- ONTAP 9.6 이상:

```
network interface create -vserver vserver_name -lif lif_name -data
-protocol fcp -service-policy default-data-fcp -home-node node_name
-home-port port_name -address ip_address -netmask netmask -status-admin
up
```

- ONTAP 9.5 이하:

```
'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol fcp-home-
node_node_name_-home-port_port_'
```

3. LIF가 생성되었으며 운영 상태가 '온라인'인지 확인합니다.

```
'network interface show -vserver_vserver_name__lif_name_'
```

에 대한 자세한 내용은 network interface show "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "NetApp 지원"

- "NetApp 상호 운용성 매트릭스 툴"
- 클러스터 SAN 환경의 LIF 고려 사항

SVM을 위한 **FC** 서비스를 삭제합니다

더 이상 필요하지 않은 경우 SVM(스토리지 가상 머신)에 대한 FC 서비스를 삭제할 수 있습니다.

시작하기 전에

SVM에 대한 FC 서비스를 삭제하려면 관리 상태가 "자체"여야 합니다. 'vserver fcp modify' 명령 또는 'vserver fcp stop' 명령을 사용하여 관리 상태를 down으로 설정할 수 있습니다.

단계

1. 'vserver FCP stop' 명령을 사용하여 LUN에 대한 입출력을 중지합니다.

```
'vserver fcp stop-vserver vs_1'
```

2. SVM에서 서비스를 제거하려면 'vserver FCP delete' 명령을 사용하십시오.

```
'vserver fcp delete-vserver vs_1'
```

3. SVM에서 FC 서비스를 삭제했는지 확인하려면 'vserver FCP show'를 사용하십시오.

```
'vserver fcp show -vserver vs_1'
```

FCoE 점보 프레임에 대한 권장 **MTU** 구성

FCoE(Fibre Channel over Ethernet)의 경우 CNA의 이더넷 어댑터 부분에 대한 점보 프레임을 9000 MTU로 구성해야 합니다. CNA의 FCoE 어댑터 부분에 대한 점보 프레임은 1500 MTU 이상으로 구성해야 합니다. 이니시에이터, 타겟 및 모든 중재 스위치가 점보 프레임을 지원하고 점보 프레임에 맞게 구성된 경우에만 점보 프레임을 구성합니다.

NVMe 프로토콜 관리

SVM을 위한 **NVMe** 서비스를 시작합니다

스토리지 가상 시스템(SVM)에서 NVMe 프로토콜을 사용하려면 먼저 SVM에서 NVMe 서비스를 시작해야 합니다.

시작하기 전에

NVMe는 시스템에서 프로토콜로 허용되어야 합니다.

지원되는 NVMe 프로토콜은 다음과 같습니다.

프로토콜	다음으로 시작...	허용된 사용자...
TCP	ONTAP 9.10.1	기본값
FCP	ONTAP 9.4	기본값

단계

1. 권한 설정을 고급으로 변경합니다.

세트 프리빌리지 고급

2. NVMe가 프로토콜로 허용되는지 확인합니다.

'vserver NVMe show'

3. NVMe 프로토콜 서비스를 생성합니다.

'vserver NVMe create'

4. SVM에서 NVMe 프로토콜 서비스를 시작합니다.

'vserver NVMe modify-status-admin up'을 선택합니다

SVM에서 NVMe 서비스를 삭제합니다

필요한 경우 스토리지 가상 시스템(SVM)에서 NVMe 서비스를 삭제할 수 있습니다.

단계

1. 권한 설정을 고급으로 변경합니다.

세트 프리빌리지 고급

2. SVM에서 NVMe 서비스를 중지합니다.

'vserver NVMe modify-status-admin down'

3. NVMe 서비스를 삭제합니다.

'vserver NVMe delete'

네임스페이스 크기 조정

ONTAP 9.10.1부터 ONTAP CLI를 사용하여 NVMe 네임스페이스의 크기를 늘리거나 줄일 수 있습니다. System Manager를 사용하여 NVMe 네임스페이스의 크기를 늘릴 수 있습니다.

네임스페이스의 크기를 늘립니다

시스템 관리자

1. 스토리지 > NVMe 네임스페이스 * 를 클릭합니다.
2. 늘릴 네임스페이스를 마우스 오른쪽 단추로 클릭한 **⋮** 다음 * 편집 * 을 클릭합니다.
3. capacity * 에서 네임스페이스의 크기를 변경합니다.

CLI를 참조하십시오

1. 'vserver NVMe namespace modify -vserver_SVM_name_-path_path_-size_new_size_of_namespace_' 명령을 입력합니다

네임스페이스의 크기를 줄입니다

ONTAP CLI를 사용하여 NVMe 네임스페이스의 크기를 줄여야 합니다.

1. 권한 설정을 고급으로 변경합니다.

'세트-프리빌리지 어드밴스드'

2. 네임스페이스 크기 축소:

```
'vserver NVMe namespace modify -vserver_SVM_name_-path_namespace_path_-size_new_size_of_namespace_'
```

네임스페이스를 LUN으로 변환합니다

ONTAP 9.11.1부터는 ONTAP CLI를 사용하여 데이터 이동 없이 기존 NVMe 네임스페이스를 LUN으로 변환할 수 있습니다.

시작하기 전에

- 지정된 NVMe 네임스페이스에는 하위 시스템에 대한 기존 맵이 없어야 합니다.
- 네임스페이스가 스냅샷의 일부이거나 SnapMirror 관계의 대상 측에 읽기 전용 네임스페이스로 있어서는 안 됩니다.
- NVMe 네임스페이스는 특정 플랫폼 및 네트워크 카드에서만 지원되므로 이 기능은 특정 하드웨어에서만 작동합니다.

단계

1. 다음 명령을 입력하여 NVMe 네임스페이스를 LUN으로 변환합니다.

```
'LUN convert-from-namespace-vserver-namespace-path'
```

에 대한 자세한 내용은 `lun convert-from-namespace` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

NVMe를 통해 대역 내 인증을 설정합니다

ONTAP 9.12.1부터 ONTAP CLI(명령줄 인터페이스)를 사용하여 DH-HMAC-CHAP 인증을 사용하여 NVMe/TCP 및 NVMe/FC 프로토콜을 통해 NVMe 호스트와 컨트롤러 간에 대역 내 (보안), 양방향 및 단방향 인증을 구성할 수 있습니다. ONTAP 9.14.1부터 System

Manager에서 대역 내 인증을 구성할 수 있습니다.

대역내 인증을 설정하려면 각 호스트 또는 컨트롤러가 NVMe 호스트 또는 컨트롤러의 NQN 및 관리자가 구성한 인증 비밀의 조합인 DH-HMAC-CHAP 키와 연결되어야 합니다. NVMe 호스트 또는 컨트롤러가 해당 피어를 인증하려면 피어와 연결된 키를 알고 있어야 합니다.

단방향 인증에서는 호스트에 대해 암호 키가 구성되지만 컨트롤러는 구성되지 않습니다. 양방향 인증에서 비밀 키는 호스트와 컨트롤러 모두에 대해 구성됩니다.

SHA-256은 기본 해시 함수이고 2048비트는 기본 DH 그룹입니다.

시스템 관리자

ONTAP 9.14.1부터는 System Manager를 사용하여 NVMe 서브시스템을 생성 또는 업데이트하고, NVMe 네임스페이스를 생성 또는 클론 복제하며, 새로운 NVMe 네임스페이스로 일관성 그룹을 추가하는 동안 대역 내 인증을 구성할 수 있습니다.

단계

1. System Manager에서 * Hosts > NVMe Subsystem * 을 클릭하고 * Add * 를 클릭합니다.
2. NVMe 서브시스템 이름을 추가하고 스토리지 VM 및 호스트 운영 체제를 선택합니다.
3. 호스트 NQN을 입력합니다.
4. 호스트 NQN 옆에 있는 * Use in-band authentication * 을 선택합니다.
5. 호스트 암호 및 컨트롤러 암호를 제공합니다.

DH-HMAC-CHAP 키는 NVMe 호스트 또는 컨트롤러의 NQN과 관리자가 구성한 인증 비밀의 조합입니다.

6. 각 호스트에 대해 선호하는 해시 기능과 DH 그룹을 선택합니다.

해시 함수와 DH 그룹을 선택하지 않으면 SHA-256이 기본 해시 함수로 할당되고 2048비트가 기본 DH 그룹으로 할당됩니다.

7. 선택적으로 * Add * 를 클릭하고 필요에 따라 단계를 반복하여 호스트를 추가합니다.
8. 저장 * 을 클릭합니다.
9. 대역 내 인증이 활성화되어 있는지 확인하려면 * System Manager > Hosts > NVMe Subsystem > Grid > Peek view * 를 클릭합니다.

호스트 이름 옆에 투명한 키 아이콘은 단방향 모드가 설정되어 있음을 나타냅니다. 호스트 이름 옆의 불투명 키는 양방향 모드가 활성화되었음을 나타냅니다.

CLI를 참조하십시오

단계

1. DH-HMAC-CHAP 인증을 NVMe 하위 시스템에 추가합니다.

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

에 대한 자세한 내용은 `vserver nvme subsystem host add` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. DH-HMAC CHAP 인증 프로토콜이 호스트에 추가되었는지 확인합니다.

```
vserver nvme subsystem host show
```

```
[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman Authentication
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode
```

에 대한 자세한 내용은 `vserver nvme subsystem host show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

3. NVMe 컨트롤러 생성 중에 DH-HMAC CHAP 인증이 수행되었는지 확인합니다.

```
vserver nvme subsystem controller show
```

```
[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman Authentication
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode
```

관련 정보

- "[vserver nvme 서브시스템 컨트롤러 표시](#)"

NVMe를 통한 대역 내 인증을 비활성화합니다

DH-HMAC-CHAP를 사용하여 NVMe를 통해 대역 내 인증을 구성한 경우 언제든지 비활성화할 수 있습니다.

ONTAP 9.12.1 이상에서 ONTAP 9.12.0 이하로 되돌리는 경우 되돌리기 전에 대역내 인증을 비활성화해야 합니다. DH-HMAC-CHAP를 사용한 대역내 인증이 해제되지 않은 경우 되돌리기가 실패합니다.

단계

1. DH-HMAC-CHAP 인증을 비활성화하려면 서브시스템에서 호스트를 제거합니다.

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

2. DH-HMAC-CHAP 인증 프로토콜이 호스트에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

3. 인증 없이 호스트를 하위 시스템에 다시 추가합니다.

```
vserver nvme subsystem host add vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

NVMe/TCP에 대한 TLS 보안 채널을 설정합니다

ONTAP 9.16.1 버전부터 NVMe/TCP 연결에 대해 TLS 보안 채널을 구성할 수 있습니다. 시스템 관리자 또는 ONTAP CLI를 사용하여 TLS가 활성화된 새 NVMe 서브시스템을 추가하거나 기존 NVMe 서브시스템에 대해 TLS를 활성화할 수 있습니다. ONTAP TLS 하드웨어 오프로드를 지원하지 않습니다.

시스템 관리자

ONTAP 9.16.1부터는 System Manager를 사용하여 NVMe 서브시스템을 생성 또는 업데이트하거나, NVMe 네임스페이스를 생성 또는 복제하거나, 새로운 NVMe 네임스페이스로 일관성 그룹을 추가하는 동안 NVMe/TCP 연결용 TLS를 구성할 수 있습니다.

단계

1. System Manager에서 * Hosts > NVMe Subsystem * 을 클릭하고 * Add * 를 클릭합니다.
2. NVMe 서브시스템 이름을 추가하고 스토리지 VM 및 호스트 운영 체제를 선택합니다.
3. 호스트 NQN을 입력합니다.
4. 호스트 NQN 옆에 있는 * 전송 계층 보안(TLS) 필요 * 를 선택합니다.
5. 사전 공유 키(PSK)를 제공합니다.
6. 저장 * 을 클릭합니다.
7. TLS 보안 채널이 활성화되어 있는지 확인하려면 * System Manager > 호스트 > NVMe 하위 시스템 > 그리드 > Peek view * 를 선택합니다.

CLI를 참조하십시오

단계

1. TLS 보안 채널을 지원하는 NVMe 서브시스템 호스트를 추가합니다. 다음을 사용하여 사전 공유 키(PSK)를 제공할 수 있습니다. `tls-configured-psk` 논쟁:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. NVMe 서브시스템 호스트가 TLS 보안 채널에 대해 구성되어 있는지 확인합니다. 선택적으로 인수를 사용하여 해당 키 유형을 사용하는 호스트만 표시할 수 `tls-key-type` 있습니다.

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. NVMe 서브시스템 호스트 컨트롤러가 TLS 보안 채널에 대해 구성되어 있는지 확인합니다. 선택적으로, `tls-identity` 또는 `tls-cipher` 인수를 사용하여 해당 TLS 특성이 있는 컨트롤러만 표시할 수 있습니다 `tls-key-type`.

```
vserver nvme subsystem controller show -vserver <svm_name>  
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type  
{none|configured} -tls-identity <text> -tls-cipher  
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

관련 정보

- ["SVM NVMe 서브시스템"](#)

NVMe/TCP에 대한 **TLS** 보안 채널을 비활성화합니다

ONTAP 9.16.1부터, NVMe/TCP 연결을 위해 TLS 보안 채널을 구성할 수 있습니다. NVMe/TCP 연결을 위해 TLS 보안 채널을 구성한 경우 언제든지 사용하지 않도록 설정할 수 있습니다.

단계

1. TLS 보안 채널을 비활성화하려면 서브시스템에서 호스트를 제거합니다.

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

2. TLS 보안 채널이 호스트에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

3. TLS 보안 채널이 없는 서브시스템에 호스트를 다시 추가합니다.

```
vserver nvme subsystem host add vserver <svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

관련 정보

- ["SVM NVMe 서브시스템 호스트"](#)

NVMe 호스트 우선순위를 변경합니다

ONTAP 9.14.1부터 특정 호스트에 대한 리소스 할당의 우선순위를 지정하도록 NVMe 서브시스템을 구성할 수 있습니다. 기본적으로 호스트가 서브시스템에 추가되면 보통 우선 순위가 할당됩니다. 높은 우선 순위가 할당된 호스트에는 더 큰 입출력 대기열 수와 대기열 깊이가 할당됩니다.

ONTAP CLI(명령줄 인터페이스)를 사용하여 기본 우선 순위를 보통에서 높음으로 수동으로 변경할 수 있습니다. 호스트에 할당된 우선 순위를 변경하려면 하위 시스템에서 호스트를 제거한 다음 다시 추가해야 합니다.

단계

1. 호스트 우선 순위가 Regular로 설정되어 있는지 확인합니다.

```
vserver nvme show-host-priority
```

에 대한 자세한 내용은 `vserver nvme show-host-priority` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 서버시스템에서 호스트 제거:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

에 대한 자세한 내용은 `vserver nvme subsystem host remove` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

3. 호스트가 서버시스템에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

에 대한 자세한 내용은 `vserver nvme subsystem host show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

4. 우선 순위가 높은 하위 시스템에 호스트를 다시 추가합니다.

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>  
-priority high
```

에 대한 자세한 내용은 `vserver nvme subsystem host add` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

ONTAP에서 NVMe/TCP 컨트롤러의 자동화된 호스트 검색을 관리합니다

ONTAP 9.14.1부터는 IP 기반 패브릭에서 NVMe/TCP 프로토콜을 사용하여 컨트롤러의 호스트 검색이 기본적으로 자동화됩니다.

NVMe/TCP 컨트롤러의 자동화된 호스트 검색 지원

이전에 자동 호스트 검색을 사용하지 않도록 설정했지만 필요한 사항이 변경된 경우 다시 사용하도록 설정할 수 있습니다.

단계

1. 고급 권한 모드 시작:

```
set -privilege advanced
```

2. 자동 검색 사용:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled true
```

3. NVMe/TCP 컨트롤러의 자동화된 검색이 활성화되었는지 확인합니다.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

NVMe/TCP 컨트롤러의 자동화된 호스트 검색을 사용하지 않도록 설정합니다

호스트에서 NVMe/TCP 컨트롤러를 자동으로 검색할 필요가 없고 네트워크에서 원치 않는 멀티캐스트 트래픽을 감지한 경우 이 기능을 비활성화해야 합니다.

단계

1. 고급 권한 모드 시작:

```
set -privilege advanced
```

2. 자동 검색 사용 안 함:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled false
```

3. NVMe/TCP 컨트롤러의 자동 검색이 비활성화되었는지 확인합니다.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

ONTAP에서 **NVMe** 호스트 가상 머신 식별자를 비활성화합니다

ONTAP 9.14.1부터 기본적으로 ONTAP는 NVMe/FC 호스트의 기능을 지원하여 고유 식별자로 가상 머신을 식별하고 NVMe/FC 호스트에서 가상 머신 리소스 활용률을 모니터링할 수 있도록 합니다. 또한 호스트측 보고 및 문제 해결이 향상됩니다.

bootarg를 사용하여 이 기능을 비활성화할 수 있습니다. 를 참조하십시오"[NetApp 기술 자료: ONTAP 에서 NVMe 호스트 가상 머신 식별자를 비활성화하는 방법](#)".

FC 어댑터를 사용하여 시스템을 관리합니다

FC 어댑터를 사용하여 시스템을 관리합니다

온보드 FC 어댑터 및 FC 어댑터 카드를 관리하는 데 사용할 수 있는 명령입니다. 이러한 명령을 사용하여 어댑터 모드를 구성하고 어댑터 정보를 표시하며 속도를 변경할 수 있습니다.

대부분의 스토리지 시스템에는 이니시에이터 또는 타겟으로 구성할 수 있는 온보드 FC 어댑터가 있습니다. 또한, 이니시에이터 또는 타겟으로 구성된 FC 어댑터 카드를 사용할 수도 있습니다. 개시자는 백엔드 디스크 셀프로 연결되고, 외부 스토리지 어레이에도 연결될 수 있습니다. 타겟은 FC 스위치에만 연결됩니다. FC 대상 HBA 포트와 스위치 포트 속도는 모두 동일한 값으로 설정해야 하며 자동으로 설정하면 안 됩니다.

관련 정보

"SAN 구성"

FC 어댑터를 관리하는 명령입니다

FC 명령을 사용하여 스토리지 컨트롤러에 대한 FC 타겟 어댑터, FC 이니시에이터 어댑터 및 온보드 FC 어댑터를 관리할 수 있습니다. FC 프로토콜과 FC-NVMe 프로토콜을 위해 FC 어댑터를 관리하는 데 동일한 명령이 사용됩니다.

FC 이니시에이터 어댑터 명령은 노드 레벨에서만 작동합니다. FC Initiator Adapter 명령을 사용하려면 먼저 'run-node_node_name_' 명령을 사용해야 합니다.

FC 타겟 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드에 FC 어댑터 정보를 표시합니다	네트워크 FCP 어댑터가 표시됩니다
FC 타겟 어댑터 매개 변수를 수정합니다	네트워크 FCP 어댑터 수정
FC 프로토콜 트래픽 정보를 표시합니다	'run-node_node_name_sysstat -f'
FC 프로토콜이 실행된 시간을 표시합니다	'run-node_node_name_uptime'
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'
명령에 대한 man 페이지를 봅니다	man <command_name>

FC 이니시에이터 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드의 모든 이니시에이터 및 해당 어댑터에 대한 정보를 표시합니다	'run-node_node_name_storage show adapter'입니다
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'

온보드 **FC** 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
온보드 FC 포트의 상태를 표시합니다	'run-node_node_name_system hardware unified-connect show

관련 정보

- ["네트워크 FCP 어댑터"](#)

FC 어댑터를 구성합니다

각 온보드 FC 포트는 이니시에이터 또는 타겟으로 개별적으로 구성할 수 있습니다. 특정 FC 어댑터의 포트는 온보드 FC 포트와 마찬가지로 타겟 포트 또는 이니시에이터 포트도 개별적으로 구성할 수도 있습니다. 대상 모드에 대해 구성할 수 있는 어댑터 목록은 [에서 확인할 수 있습니다 "NetApp Hardware Universe를 참조하십시오"](#).

타겟 모드는 포트를 FC 이니시에이터에 연결하는 데 사용됩니다. 이니시에이터 모드는 외부 LUN 가져오기(FLI)를 통해 포트를 테이프 드라이브, 테이프 라이브러리 또는 타사 스토리지에 연결하는 데 사용됩니다.

FC 프로토콜과 FC-NVMe 프로토콜을 위해 FC 어댑터를 구성할 때도 동일한 단계가 사용됩니다. 하지만 특정 FC 어댑터만 FC-NVMe를 지원합니다. [를 참조하십시오 "NetApp Hardware Universe를 참조하십시오"](#) FC-NVMe 프로토콜을 지원하는 어댑터 목록을 확인하십시오.

FC 어댑터를 타겟 모드로 구성합니다

단계

1. 어댑터를 오프라인 상태로 전환:

```
'node run-node_node_name_storage disable adapter_adapter_name_'
```

어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

2. 어댑터를 이니시에이터에서 타겟으로 변경합니다.

```
'system hardware unified-connect modify -t target-node_node_name_adapter_adapter_name_'
```

3. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.

4. 타겟 포트의 구성이 올바른지 확인합니다.

```
'network fcp adapter show-node_name _'
```

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

5. 어댑터를 온라인으로 전환합니다.

```
'network fcp adapter modify -node_node_name_-adapter_adapter_port_-state up
```

이니시에이터 모드에 맞게 **FC 어댑터를 구성합니다**

시작하기 전에

- 어댑터에 있는 LIF는 해당 LIF가 구성원인 포트 세트에서 제거해야 합니다.
- 물리적 포트의 속성을 타겟에서 이니시에이터로 변경하기 전에 수정할 물리적 포트를 사용하는 모든 SVM(스토리지 가상 머신)의 모든 LIF를 마이그레이션 또는 제거해야 합니다.



NVMe/FC는 이니시에이터 모드를 지원합니다.

단계

1. 어댑터에서 모든 LIF를 제거합니다.

'네트워크 인터페이스 삭제 - vserver_SVM_name_-lif_LIF_name, LIF_name_'

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

2. 어댑터를 오프라인 상태로 전환:

'network fcp adapter modify -node_node_name_-adapter_adapter_port_-status-admin down'

어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

3. 어댑터를 타겟에서 이니시에이터로 변경합니다.

'System hardware unified-connect modify -t initiator_adapter_port_'

4. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.

5. FC 포트가 구성에 맞는 올바른 상태로 구성되었는지 확인합니다.

'시스템 하드웨어 통합 접속 쇼

6. 어댑터를 다시 온라인으로 전환합니다.

'node run-node_node_name_storage enable adapter_adapter_port_'

어댑터 설정을 봅니다

특정 명령을 사용하여 FC/UTA 어댑터에 대한 정보를 볼 수 있습니다.

FC 타겟 어댑터

단계

1. 네트워크 FCP 어댑터 `show` 명령을 사용하여 어댑터 정보를 표시합니다. 네트워크 FCP 어댑터 `show-instance-node node1-adapter 0a`

출력에는 사용되는 각 슬롯의 시스템 구성 정보와 어댑터 정보가 표시됩니다.

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

UTA(Unified Target Adapter) X1143A-R6

단계

1. 케이블을 연결하지 않고 컨트롤러를 부팅합니다.
2. 'system hardware unified-connect show' 명령어를 실행하여 포트 구성 및 모듈을 확인할 수 있다.
3. CNA 및 포트를 구성하기 전에 포트 정보를 확인합니다.

UTA2 포트를 CNA 모드에서 FC 모드로 변경합니다

UTA2 포트를 CNA(Converged Network Adapter) 모드에서 FC(Fibre Channel) 모드로 변경하여 FC 이니시에이터 및 FC 타겟 모드를 지원해야 합니다. 포트를 네트워크에 연결하는 물리적 미디어를 변경해야 하는 경우 CNA 모드에서 FC 모드로 속성을 변경해야 합니다.

단계

1. 어댑터를 오프라인 상태로 전환:

```
'network fcp adapter modify -node_node_name_-adapter_adapter_name_-status-admin down'
```

2. 포트 모드를 변경합니다.

```
'ucadmin modify -node_node_name_-adapter_adapter_name_-mode fcp'
```

3. 노드를 재부팅한 다음 어댑터를 온라인 상태로 전환합니다.

```
'network fcp adapter modify -node_node_name_-adapter_adapter_name_-status-admin up'
```

4. 필요에 따라 관리자 또는 VIF 관리자에게 포트를 삭제하거나 제거하도록 알립니다.

- 포트가 LIF의 홈 포트로 사용되고, 인터페이스 그룹(ifgrp) 또는 호스트 VLAN의 구성원인 경우 관리자는 다음을 수행해야 합니다.

- i. LIF를 이동하거나, ifgrp에서 포트를 제거하거나, VLAN을 각각 삭제합니다.

- ii. 'network port delete' 명령어를 실행해 포트를 수동으로 삭제한다.

'network port delete' 명령이 실패하면 관리자가 오류를 해결한 다음 명령을 다시 실행해야 합니다.

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

- 포트가 LIF의 홈 포트로 사용되지 않고, ifgrp의 구성원이 아니며 VLAN을 호스팅하지 않는 경우, VIF 관리자는 재부팅 시 기록에서 포트를 제거해야 합니다.

VIF 관리자가 포트를 제거하지 않는 경우, 관리자는 재부팅 후 'network port delete' 명령을 사용하여 수동으로 제거해야 합니다.

```
net-f8040-34::> network port show

Node: net-f8040-34-01

Health                                                                                               Speed (Mbps)
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper
Status
-----
```

```

-----
...
e0i      Default      Default      down 1500  auto/10  -
e0f      Default      Default      down 1500  auto/10  -
...

net-f8040-34::> ucadmin show

Admin
Node          Adapter  Mode      Type      Pending  Pending
Status
-----
net-f8040-34-01  0e      cna      target    -         -
offline
net-f8040-34-01  0f      cna      target    -         -
offline
...

net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0

net-f8040-34::> network interface show -fields home-port, curr-
port

vserver lif          home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a      e0a
Cluster net-f8040-34-01_clus2 e0b      e0b
Cluster net-f8040-34-01_clus3 e0c      e0c
Cluster net-f8040-34-01_clus4 e0d      e0d
net-f8040-34
      cluster_mgmt      e0M      e0M
net-f8040-34
      m                  e0e      e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M      e0M
7 entries were displayed.

net-f8040-34::> ucadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed
to fc.

```

```

Do you want to continue? {y|n}: y
Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

net-f8040-34::> reboot local
(system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y

```

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

5. 올바른 SFP+가 설치되었는지 확인합니다.

네트워크 FCP 어댑터 `show-instance-node-adapter`입니다

CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다. FC의 경우 노드에서 구성을 변경하기 전에 8Gb SFP 또는 16Gb SFP를 사용해야 합니다.

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

관련 정보

- "[네트워크 인터페이스](#)"

CNA/UTA2 타겟 어댑터 광 모듈을 변경합니다

어댑터에 대해 선택한 퍼스널리티 모드를 지원하도록 유니파이드 타겟 어댑터(CNA/UTA2)의 광 모듈을 변경해야 합니다.

단계

1. 카드에 사용된 현재 SFP+를 확인합니다. 그런 다음 기본 설정 특성(FC 또는 CNA)에 대해 현재 SFP+를 적절한 SFP+로 교체합니다.
2. X1143A-R6 어댑터에서 현재 광 모듈을 제거합니다.
3. 기본 퍼스널리티 모드(FC 또는 CNA) 광학장치에 맞는 모듈을 삽입합니다.
4. 올바른 SFP+가 설치되었는지 확인합니다.

네트워크 FCP 어댑터 `show-instance-node-adapter`입니다

지원되는 SFP+ 모듈 및 Cisco Twinax(Copper) 케이블은 `_Hardware Universe_`에 나열되어 있습니다.

관련 정보

- "[NetApp Hardware Universe](#)를 참조하십시오"
- "[네트워크 FCP 어댑터가 표시됩니다](#)"

X1143A-R6 어댑터에 대해 지원되는 포트 구성

FC 타겟 모드는 X1143A-R6 어댑터 포트의 기본 구성입니다. 하지만 이 어댑터의 포트는 10Gb 이더넷 및 FCoE 포트 또는 16Gb FC 포트도 구성할 수 있습니다.

이더넷 및 FCoE용으로 구성된 경우 X1143A-R6 어댑터는 동일한 10GbE 포트에서 동시 NIC 및 FCoE 타겟 트래픽을 지원합니다. FC용으로 구성된 경우 동일한 ASIC을 공유하는 각 2포트 쌍은 FC 타겟 또는 FC 이니시에이터 모드에 대해 개별적으로 구성할 수 있습니다. 즉, 단일 X1143A-R6 어댑터는 하나의 2포트 쌍에서 FC 타겟 모드를, 다른 2포트 쌍에서 FC 이니시에이터 모드를 지원할 수 있습니다.

관련 정보

["NetApp Hardware Universe를 참조하십시오"](#)

["SAN 구성"](#)

포트를 구성합니다

통합 타겟 어댑터(X1143A-R6)를 구성하려면 동일한 퍼스널리티 모드에서 동일한 칩에 두 개의 인접 포트를 구성해야 합니다.

단계

1. 'system node hardware unified-connect modify' 명령을 사용하여 FC(Fibre Channel) 또는 CNA(Converged Network Adapter)에 필요한 포트를 구성합니다.
2. FC 또는 10Gb 이더넷에 적합한 케이블을 연결합니다.
3. 올바른 SFP+가 설치되었는지 확인합니다.

네트워크 FCP 어댑터 show-instance-node-adapter입니다

CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다. FC의 경우 연결 중인 FC 패브릭을 기반으로 8Gb SFP 또는 16Gb SFP를 사용해야 합니다.

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

X1133A-R6 어댑터를 사용할 경우 연결 끊김 방지

별도의 X1133A-R6 HBA에 대한 중복 경로를 사용하여 시스템을 구성하면 포트 장애 시 연결이 끊어지지 않습니다.

X1133A-R6 HBA는 2개의 2포트 쌍으로 구성된 4포트, 16Gb FC 어댑터입니다. X1133A-R6 어댑터는 타겟 모드 또는 이니시에이터 모드로 구성할 수 있습니다. 각 2포트 쌍은 단일 ASIC에서 지원됩니다(예: ASIC 1의 포트 1과 포트 2, ASIC 2의 포트 3과 포트 4). 단일 ASIC의 두 포트는 타겟 모드나 이니시에이터 모드에서 동일한 모드로 작동하도록 구성해야 합니다. ASIC에서 쌍을 지원하는 데 오류가 발생하면 페어의 두 포트가 모두 오프라인 상태가 됩니다.

이러한 접속 구성 손실을 방지하려면 X1133A-R6 HBA를 분리하는 이중 경로 또는 HBA의 다른 ASIC에서 지원되는 포트에 대한 이중 경로를 사용하여 시스템을 구성합니다.

모든 SAN 프로토콜에 대한 LIF 관리

모든 SAN 프로토콜에 대한 LIF 관리

이니시에이터는 SAN 환경의 클러스터에 대한 페일오버 기능에 MPIO(다중 경로 I/O) 및 ALUA(Asymmetric Logical Unit Access)를 사용해야 합니다. 노드에 장애가 발생할 경우 LIF는 장애가 발생한 파트너 노드의 IP 주소를 마이그레이션하거나 가정하지 않습니다. 대신, 호스트에서 ALUA를 사용하여 LIF를 통해 LUN 액세스를 위한 적절한 경로를 선택해야 합니다.

HA 쌍에서 처리하는 LUN에 대한 액세스를 허용하려면 논리 인터페이스(LIF)를 사용하여 HA 쌍의 각 노드에서 하나 이상의 iSCSI 경로를 생성해야 합니다. SAN을 지원하는 모든 SVM(스토리지 가상 머신)마다 하나의 관리 LIF를 구성해야 합니다.

직접 연결 또는 이더넷 스위치 사용이 연결에 지원됩니다. 두 가지 연결 유형에 대해 LIF를 생성해야 합니다.

- SAN을 지원하는 모든 SVM(스토리지 가상 머신)마다 하나의 관리 LIF를 구성해야 합니다. 노드당 두 개의 LIF를 구성할 수 있으며, FC와 함께 사용되는 각 패브릭과 iSCSI용 이더넷 네트워크를 각각 하나씩 구성할 수 있습니다.

LIF를 생성한 후 포트 세트에서 제거하고 SVM(스토리지 가상 머신) 내의 다른 노드로 이동한 후 삭제할 수 있습니다.

관련 정보

- ["LIF 개요 구성"](#)
- ["LIF를 생성합니다"](#)

ONTAP에서 NVMe LIF를 구성합니다

NVMe LIF를 구성할 때 특정 요구사항을 충족해야 합니다.

시작하기 전에

NVMe는 LIF를 생성하는 FC 어댑터에서 지원되어야 합니다. 지원되는 어댑터는 [여기](#) 나와 있습니다 "[Hardware Universe](#)".

이 작업에 대해

ONTAP 9.12.1 이상부터 최대 12개 노드에서 노드당 두 개의 NVMe LIF를 구성할 수 있다. ONTAP 9.11.1 이하 버전에서는 최대 2개 노드에서 노드당 두 개의 NVMe LIF를 구성할 수 있다.

NVMe LIF를 생성할 때 다음 규칙이 적용됩니다.

- NVMe는 데이터 LIF에서 유일한 데이터 프로토콜일 수 있습니다.
- SAN을 지원하는 모든 SVM에 대해 하나의 관리 LIF를 구성해야 합니다.
- ONTAP 9.5 이상의 경우 네임스페이스가 포함된 노드와 노드의 HA 파트너에 NVMe LIF를 구성해야 합니다.
- ONTAP 9.4만 해당:
 - NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
 - SVM당 하나의 NVMe 데이터 LIF만 구성할 수 있습니다.

단계

1. LIF를 생성합니다.

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```



NVMe/TCP는 ONTAP 9.10.1 이상부터 사용할 수 있습니다.

2. LIF가 생성되었는지 확인합니다.

```
network interface show -vserver <SVM_name>
```

NVMe/TCP LIF 생성 후 포트 8009에서 검색을 수신합니다.

관련 정보

- ["네트워크 인터페이스"](#)

SAN LIF를 이동하기 전에 알아야 할 사항

클러스터에 노드 추가, 클러스터에서 노드 삭제 등과 같이 클러스터의 콘텐츠를 변경하는 경우에는 LIF 이동만 수행해야 합니다. LIF 이동을 수행할 경우 FC 패브릭을 재존치하거나 클러스터의 연결된 호스트와 새로운 타겟 인터페이스 간에 새 iSCSI 세션을 생성할 필요가 없습니다.

네트워크 인터페이스 이동 명령을 사용하면 SAN LIF를 이동할 수 없습니다. SAN LIF는 LIF를 오프라인 상태로 전환하고 LIF를 다른 홈 노드 또는 포트에 이동한 다음, 새로운 위치에서 온라인 상태로 다시 전환하여 수행해야 합니다. ALUA(Asymmetric Logical Unit Access)는 모든 ONTAP SAN 솔루션의 일부로 이중 경로 및 자동 경로 선택을 제공합니다. 따라서 LIF가 이동을 위해 오프라인 상태로 전환되면 I/O 중단이 발생하지 않습니다. 호스트는 간단히 재시도하여 I/O를 다른 LIF로 이동합니다.

LIF 이동을 사용하면 다음을 중단 없이 수행할 수 있습니다.

- LUN 데이터에 액세스하는 호스트에 전혀 영향을 주지 않는 방식으로 클러스터의 HA 쌍 중 하나를 업그레이드된 HA 쌍으로 교체합니다
- 대상 인터페이스 카드를 업그레이드합니다
- SVM(스토리지 가상 시스템)의 리소스를 클러스터의 한 노드 세트에서 클러스터의 다른 노드 세트로 이동합니다

포트 세트에서 **SAN LIF**를 제거합니다

삭제하거나 이동하려는 LIF가 포트 세트에 있는 경우 LIF를 삭제하거나 이동하기 전에 포트 세트에서 LIF를 제거해야 합니다.

이 작업에 대해

다음 절차의 1단계는 하나의 LIF가 포트 세트에 있는 경우에만 수행해야 합니다. 포트 세트가 이니시에이터 그룹에 바인딩되어 있는 경우 포트 세트의 마지막 LIF를 제거할 수 없습니다. 그렇지 않으면 포트 세트에 여러 LIF가 있는 경우 2단계부터 시작할 수 있습니다.

단계

1. 포트 세트에 하나의 LIF만 있는 경우 'lun igroup unbind' 명령을 사용하여 이니시에이터 그룹에서 포트 세트를 바인딩 해제합니다.



이니시에이터 그룹을 포트 세트에서 바인딩 해제하면 이니시에이터 그룹의 모든 이니시에이터가 모든 네트워크 인터페이스의 이니시에이터 그룹에 매핑된 모든 타겟 LUN에 액세스할 수 있습니다.

```
'cluster1::> lun igroup unbind-vserver vs1-igroup ig1'
```

에 대한 자세한 내용은 `lun igroup unbind` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. 'lun 포트셋 제거' 명령을 사용하여 포트 세트에서 LIF를 제거합니다.

```
'cluster1::> port set remove-vserver vs1-포트셋 PS1-port-name lif 1'
```

에 대한 자세한 내용은 `lun portset remove` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

SAN LIF를 이동합니다

노드를 오프라인 상태로 전환해야 하는 경우 SAN LIF를 이동하여 WWPN과 같은 구성 정보를 유지하고 스위치 패브릭의 재조닝(zoning)을 방지할 수 있습니다. SAN LIF가 이동되기 전에 먼저 오프라인으로 전환되어야 하므로 호스트 트래픽은 호스트 다중 경로 소프트웨어를 통해 LUN에 대한 무중단 액세스를 제공해야 합니다. SAN LIF를 클러스터의 아무 노드로 이동할 수 있지만 SVM(스토리지 가상 머신) 간에 SAN LIF를 이동할 수 없습니다.

시작하기 전에

LIF가 포트 세트의 구성원인 경우 LIF를 다른 노드로 이동하기 전에 포트 세트에서 LIF를 제거해야 합니다.

이 작업에 대해

이동하려는 LIF의 대상 노드 및 물리적 포트는 동일한 FC 패브릭 또는 이더넷 네트워크에 있어야 합니다. LIF를 적절하게 구역이 되어 있지 않은 다른 패브릭으로 이동하거나 iSCSI 이니시에이터와 타겟 간의 연결이 없는 이더넷 네트워크로 LIF를 이동할 경우 LUN을 다시 온라인 상태로 전환할 때 LUN에 액세스할 수 없습니다.

단계

1. LIF의 관리 및 운영 상태를 봅니다.

```
'network interface show -vserver_vserver_name_'
```

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

2. LIF의 상태를 '자체'(오프라인)로 변경합니다.

```
'network interface modify -vserver_vserver_name_-lif_LIF_name_-status-admin down'
```

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

3. LIF를 새 노드 및 포트에 할당합니다.

```
'network interface modify -vserver_vserver_name_-lif_LIF_name_-home-node_node_name_-home-port_port_name_'
```

4. LIF의 상태를 '위쪽'(온라인)으로 변경합니다.

```
'network interface modify -vserver_vserver_name_-lif_LIF_name_-status-admin up
```

에 대한 자세한 내용은 [up "ONTAP 명령 참조입니다"](#)을 참조하십시오.

5. 변경 사항 확인:

```
'network interface show -vserver_vserver_name_'
```

SAN 환경에서 **LIF**를 삭제합니다

LIF를 삭제하기 전에 LIF에 연결된 호스트가 다른 경로를 통해 LUN에 액세스할 수 있는지 확인해야 합니다.

시작하기 전에

삭제하려는 LIF가 포트 세트의 구성원인 경우 LIF를 삭제하려면 먼저 포트 세트에서 LIF를 제거해야 합니다.

시스템 관리자

ONTAP 시스템 관리자(9.7 이상)가 설치된 LIF를 삭제합니다.

단계

1. System Manager에서 * Network > Overview * 를 클릭한 다음 * Network Interfaces * 를 선택합니다.
2. LIF를 삭제할 스토리지 VM을 선택합니다.
3. 을  클릭하고 * 삭제 * 를 선택합니다.

CLI를 참조하십시오

ONTAP CLI에서 LIF를 삭제합니다.

단계

1. 삭제할 LIF와 현재 포트의 이름을 확인합니다.

```
'network interface show - vserver _vserver_name _'
```

2. LIF를 삭제합니다.

네트워크 인터페이스 삭제

```
'network interface delete-vserver vs1-lif lif liff li1'
```

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

3. LIF를 삭제했는지 확인합니다.

네트워크 인터페이스 쇼

네트워크 인터페이스 show-vserver vs1

```
Logical Status      Network              Current   Current Is
Vserver Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
----
vs1
      lif2          up/up        192.168.2.72/24  node-01   e0b
true
      lif3          up/up        192.168.2.73/24  node-01   e0b
true
```

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

SAN LIF 요구사항에서 클러스터에 노드를 추가해야 합니다

클러스터에 노드를 추가할 때는 특정 고려 사항을 염두에 두어야 합니다.

- 새 노드에서 LUN을 생성하기 전에 필요에 따라 새 노드에 LIF를 생성해야 합니다.
- 호스트에서 호스트 스택 및 프로토콜에 따라 이러한 LIF를 검색해야 합니다.
- 클러스터 인터커넥트 네트워크를 사용하지 않고 LUN 및 볼륨 이동을 수행할 수 있도록 새 노드에 LIF를 생성해야 합니다.

호스트 **iSCSI SendTargets** 검색 작업에 **FQDN**을 반환하도록 **iSCSI LIF**를 구성합니다

ONTAP 9부터 호스트 OS가 iSCSI SendTargets 검색 작업을 전송할 때 FQDN(정규화된 도메인 이름)을 반환하도록 iSCSI LIF를 구성할 수 있습니다. FQDN은 호스트 OS와 스토리지 서비스 사이에 NAT(Network Address Translation) 디바이스가 있는 경우에 유용합니다.

이 작업에 대해

NAT 장치의 한 쪽에 있는 IP 주소는 다른 쪽에는 의미가 없지만 FQDN은 양쪽에서 의미를 가질 수 있습니다.



FQDN 값 상호 운용성 제한은 모든 호스트 OS에서 128자입니다.

단계

1. 권한 설정을 고급으로 변경합니다.

세트 프리빌리지 고급

2. FQDN을 반환하도록 iSCSI LIF 구성:

```
"vserver iSCSI interface modify -vserver_SVM_name_-lif_iscsi_LIF_name_-SendTargets_FQDN"
```

다음 예에서는 iSCSI LIF가 storagehost-005.example.com 를 FQDN으로 반환하도록 구성되어 있습니다.

```
'vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1-SendTargets-FQDN storagehost-005.example.com'
```

3. SendTargets가 FQDN인지 확인합니다.

```
'vserver iscsi interface show -vserver_SVM_name_-fields SendTargets-FQDN'
```

이 예제에서 storagehost-005.example.com 은 SendTargets-FQDN 출력 필드에 표시됩니다.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif          sendtargets-fqdn
-----
vs1      vs1_iscsi1  storagehost-005.example.com
vs1      vs1_iscsi2  storagehost-006.example.com
```

SAN 프로토콜에 ONTAP 공간 할당을 사용합니다

ONTAP 공간을 할당하면 LUN 또는 NVMe 네임스페이스가 공간이 부족할 때 오프라인 상태로 전환되지 않도록 방지하고 SAN 호스트에서 공간을 재확보할 수 있습니다.

ONTAP는 SAN 프로토콜과 ONTAP 버전에 따라 공간 할당을 지원합니다. ONTAP 9.16.1부터 새로 생성된 LUN 및 모든 네임스페이스에 대해 iSCSI, FC, NVMe 프로토콜에 대해 공간 할당이 기본적으로 활성화됩니다.

ONTAP 버전입니다	프로토콜	공간 할당은...
9.16.1 이상	<ul style="list-style-type: none"> • iSCSI • FC • NVMe를 참조하십시오 	새로 생성된 LUN 및 모든 네임스페이스에 대해 기본적으로 설정됩니다
9.15.1	<ul style="list-style-type: none"> • iSCSI • FC 	새로 생성된 LUN에 대해 기본적으로 설정됩니다
	NVMe를 참조하십시오	지원되지 않습니다
9.14.1 이하	<ul style="list-style-type: none"> • iSCSI • FC 	새로 생성된 LUN에 대해 기본적으로 해제되어 있습니다
	NVMe를 참조하십시오	지원되지 않습니다

공간 할당이 설정된 경우:

- LUN 또는 네임스페이스에 공간이 부족할 경우 ONTAP는 쓰기 작업에 사용할 수 있는 여유 공간이 없음을 호스트에 알립니다. 그 결과 LUN 또는 네임스페이스가 온라인 상태로 유지되고 읽기 작업이 계속 서비스됩니다. 호스트 구성에 따라 호스트가 성공할 때까지 쓰기 작업을 다시 시도하거나 호스트 파일 시스템이 오프라인이 될 때까지 재시도합니다. LUN 또는 네임스페이스에서 추가 여유 공간을 사용할 수 있게 되면 쓰기 작업이 재개됩니다.

공간 할당이 사용하도록 설정되어 있지 않은 경우 LUN 또는 네임스페이스에 공간이 부족할 때 모든 I/O 작업이 실패하고 LUN 또는 네임스페이스가 오프라인 상태가 됩니다. 정상 작업을 재개하려면 공간 문제를 해결해야 합니다. 호스트에서 LUN 디바이스를 다시 검색해야 경로 및 디바이스를 운영 상태로 복구할 수 있습니다.

- 호스트는 SCSI 또는 NVMe(일명 TRIM) 작업을 수행할 수 UNMAP 있습니다. 매핑 해제 작업을 사용하면 호스트에서 더 이상 유효한 데이터를 포함하지 않으므로 더 이상 필요하지 않은 데이터 블록을 식별할 수 있습니다. 일반적으로 파일 삭제 후 식별이 이루어집니다. 그런 다음 스토리지 시스템에서 해당 데이터 블록을 할당 해제하여 다른 곳에서 공간을 사용할 수 있도록 합니다. 이러한 할당 해제는 특히 데이터 회전율이 높은 파일 시스템에서 전반적인 스토리지 효율성을 크게 향상시킵니다.

시작하기 전에

공간 할당을 설정하려면 쓰기를 완료할 수 없는 경우 공간 할당 오류를 올바르게 처리할 수 있는 호스트 구성이 필요합니다. SCSI 또는 NVMe를 UNMAP 활용하려면 SCSI SBC-3 표준에 정의된 논리적 블록 프로비저닝을 사용할 수 있는 구성이 필요합니다.

공간 할당을 설정할 때 다음 호스트는 현재 실행 프로비저닝을 지원합니다.

- Citrix XenServer 6.5 이상
- VMware ESXi 5.0 이상
- Oracle Linux 6.2 UEK 커널 이상
- Red Hat Enterprise Linux 6.2 이상
- SUSE Linux Enterprise Server 11 이상
- Solaris 11.1 이상
- Windows

이 작업에 대해

클러스터를 ONTAP 9.15.1 이상으로 업그레이드하면 소프트웨어 업그레이드 전에 생성된 모든 LUN에 대한 공간 할당 설정은 호스트 유형에 관계없이 업그레이드 후에도 동일하게 유지됩니다. 예를 들어 공간 할당이 해제된 VMware 호스트에 대해 ONTAP 9.13.1에서 LUN을 생성한 경우 ONTAP 9.15.1로 업그레이드한 후 해당 LUN에 대한 공간 할당이 해제된 상태로 유지됩니다.

단계

1. 공간 할당 활성화:

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. 공간 할당이 설정되었는지 확인합니다.

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. 호스트 운영 체제에서 공간 할당이 활성화되어 있는지 확인합니다.



일부 버전의 VMware ESXi를 포함한 일부 호스트 구성은 설정 변경을 자동으로 인식할 수 있으며 사용자 개입이 필요하지 않습니다. 다른 구성에서는 장치를 다시 검색해야 할 수 있습니다. 일부 파일 시스템 및 볼륨 관리자는 를 사용하여 공간을 재확보하기 위해 추가적인 특정 설정이 필요할 수 있습니다. SCSI UNMAP 있습니다. 파일 시스템을 다시 마운트하거나 전체 운영 체제를 재부팅해야 할 수 있습니다. 해당 호스트의 설명서를 참조하여 지침을 확인하십시오.

VMware ESXi 8.x 이상 NVMe 호스트에 대한 호스트 구성

NVMe 프로토콜을 사용하여 ESXi 8.x 이상을 실행하는 VMware 호스트가 있는 경우 ONTAP에서 공간 할당을 설정한 후 호스트에서 다음 단계를 수행해야 합니다.

단계

1. ESXi 호스트에서 DSM이 비활성화되었는지 확인합니다.

```
esxcfg-advcfg -g /SCSI/NVmeUseDsmTp4040
```

예상 값은 0입니다.

2. NVMe DSM 활성화:

```
esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
```

3. DSM이 활성화되어 있는지 확인합니다.

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

예상 값은 1입니다.

관련 링크

에 대해 자세히 "[ONTAP를 사용하는 ESXi 8.x에 대한 NVMe-oF 호스트 구성](#)"을 살펴보십시오.

권장되는 볼륨 및 파일 또는 LUN 구성 조합

권장되는 볼륨 및 파일 또는 LUN 구성 조합 개요

애플리케이션 및 관리 요구사항에 따라 FlexVol 볼륨과 파일 또는 LUN 구성의 특정 조합이 사용할 수 있습니다. 이러한 조합을 통해 얻을 수 있는 이점과 비용을 이해하면 환경에 적합한 볼륨 및 LUN 구성의 조합을 결정하는 데 도움이 됩니다.

권장되는 볼륨 및 LUN 구성 조합은 다음과 같습니다.

- 일반 볼륨 프로비저닝이 있는 공간 예약 파일 또는 LUN
- 씬 볼륨 프로비저닝이 있는 공간 예약 파일이 아닌 LUN
- 반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 LUN

이러한 구성 조합과 함께 LUN에서 SCSI 씬 프로비저닝을 사용할 수 있습니다.

일반 볼륨 프로비저닝이 있는 공간 예약 파일 또는 LUN

- 이점: *
- 공간 예약 파일 내의 모든 쓰기 작업이 보장되며 공간 부족으로 인해 작업이 실패하지 않습니다.
- 볼륨의 스토리지 효율성 및 데이터 보호 기술에는 제한이 없습니다.
- 비용 및 제한: *
- 전체적으로 프로비저닝된 볼륨을 지원할 수 있도록 충분한 공간을 집합체로부터 충분히 미리 설정해야 합니다.
- LUN 생성 시 볼륨에서 LUN의 2배에 해당하는 공간이 할당됩니다.

씬 볼륨 프로비저닝이 있는 공간 예약 파일이 아닌 LUN

- 이점: *
- 볼륨의 스토리지 효율성 및 데이터 보호 기술에는 제한이 없습니다.
- 공간은 사용되는 경우에만 할당됩니다.

- 비용 및 제한: *
- 쓰기 작업은 보장되지 않으며, 볼륨에 여유 공간이 없을 경우 실패할 수 있습니다.
- Aggregate에 여유 공간이 부족하지 않도록 하려면 Aggregate의 여유 공간을 효과적으로 관리해야 합니다.

반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 LUN

- 이점: *

공간을 일반 볼륨 프로비저닝보다 미리 예약하므로 최선의 쓰기 보장이 제공됩니다.

- 비용 및 제한: *
- 이 옵션을 사용하면 쓰기 작업이 실패할 수 있습니다.

볼륨의 여유 공간과 데이터 휘발성의 균형을 적절하게 유지하여 이 위험을 완화할 수 있습니다.

- 스냅샷, FlexClone 파일 및 LUN과 같은 데이터 보호 객체의 보존에 의존할 수는 없습니다.
- 중복제거, 압축, ODX/복사 오프로드 등 자동으로 삭제할 수 없는 ONTAP 블록 공유 스토리지 효율성 기능은 사용할 수 없습니다.

환경에 맞는 올바른 볼륨 및 LUN 구성 조합을 결정합니다

환경에 대한 몇 가지 기본적인 질문에 답변하면 환경에 가장 적합한 FlexVol 볼륨 및 LUN 구성을 파악하는 데 도움이 됩니다.

이 작업에 대해

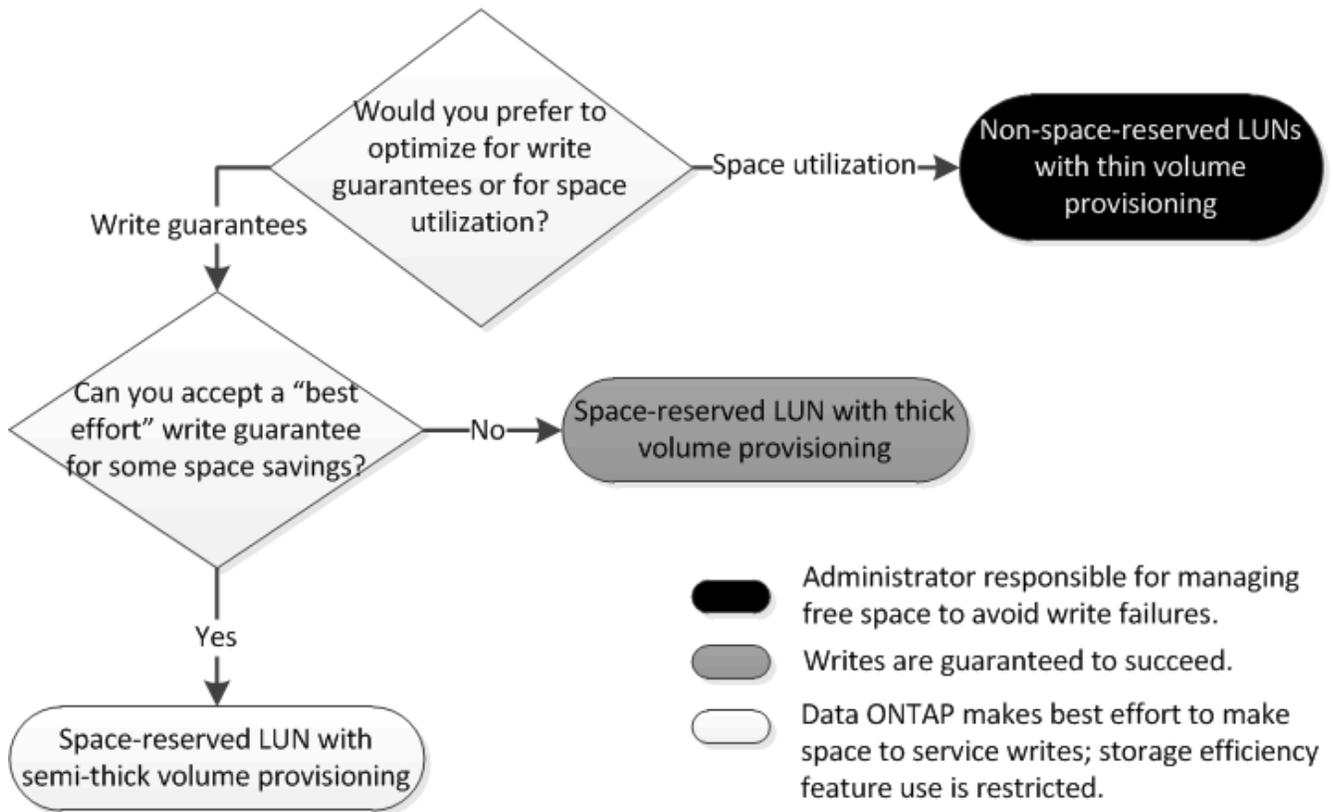
LUN 및 볼륨 구성을 최적화하여 스토리지 활용률을 극대화하거나 쓰기 보장을 극대화할 수 있습니다. 스토리지 활용률의 요구사항과 여유 공간을 신속하게 모니터링 및 보충하는 기능을 기준으로 설치에 적합한 FlexVol 볼륨 및 LUN 볼륨을 결정해야 합니다.



각 LUN에 대해 별도의 볼륨이 필요하지 않습니다.

단계

1. 다음 진단트리를 사용하여 환경에 가장 적합한 볼륨 및 LUN 구성 조합을 결정합니다.



LUN의 데이터 증가율 계산

시간이 경과하면서 LUN 데이터가 증가하는 속도를 알고 있어야 공간 예약 LUN 또는 비공간 예약 LUN을 사용해야 하는지 여부를 확인할 수 있습니다.

이 작업에 대해

지속적으로 높은 데이터 증가율을 사용하면 공간 예약 LUN이 더 나은 옵션이 될 수 있습니다. 데이터 증가율이 낮은 경우 공간이 예약되지 않은 LUN을 고려해야 합니다.

OnCommand Insight와 같은 도구를 사용하여 데이터 증가율을 계산하거나 수동으로 계산할 수 있습니다. 다음은 수동 계산에 대한 단계입니다.

단계

1. 공간 예약 LUN을 설정합니다.
2. LUN의 데이터를 1주일 등의 지정된 기간 동안 모니터링합니다.

모니터링 기간이 충분히 길어 데이터 증가 시 정기적으로 발생하는 대표적인 샘플을 형성해야 합니다. 예를 들어, 매달 말에 지속적으로 증가하는 데이터의 양이 상당히 많을 것입니다.

3. 매일 증가하는 데이터의 양을 GB 단위로 기록합니다.
4. 모니터링 기간이 끝나면 각 날짜의 합계를 더한 다음 모니터링 기간의 일 수로 나눕니다.

이 계산으로 평균 성장률을 얻을 수 있습니다.

예

이 예에서는 200GB LUN이 필요합니다. LUN을 1주일 동안 모니터링하고 다음과 같은 일일 데이터 변경 사항을 기록하기로 결정합니다.

- 일요일: 20GB
- 월요일: 18GB
- 화요일: 17GB
- 수요일: 20GB
- 목요일: 20GB
- 금요일: 23GB
- 토요일: 22GB

이 예에서 성장률(20+18+17+20+20+23+22)/7=20GB입니다.

일반 프로비저닝된 볼륨이 있는 공간 예약 파일 또는 LUN에 대한 구성 설정입니다

이 FlexVol 볼륨 및 파일 또는 LUN 구성 조합을 사용하면 스토리지 효율성 기술을 사용할 수 있으며 공간이 사전에 충분히 할당되므로 여유 공간을 능동적으로 모니터링할 필요가 없습니다.

일반 프로비저닝을 사용하여 볼륨에서 공간 예약 파일 또는 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	볼륨
부분 예약	100
스냅샷 예비 공간입니다	모두
스냅샷 자동 삭제	선택 사항
자동 확장	선택 사항: 사용하도록 설정한 경우 애그리게이트 가용 공간을 능동적으로 모니터링해야 합니다.

파일 또는 LUN 설정	값
공간 예약	활성화됨

공간이 예약되지 않은 파일 또는 썬 프로비저닝된 볼륨이 있는 LUN에 대한 구성 설정입니다

이 FlexVol 볼륨 및 파일 또는 LUN 구성 조합을 사용하려면 가장 적은 양의 스토리지를 미리 할당해야 하지만 공간 부족으로 인한 오류를 방지하기 위해 활성 여유 공간 관리가 필요합니다.

썬 프로비저닝된 볼륨에서 공간이 예약되지 않은 파일 또는 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	없음
부분 예약	0
스냅샷 예비 공간입니다	모두
스냅샷 자동 삭제	선택 사항
자동 확장	선택 사항

파일 또는 LUN 설정	값
공간 예약	사용 안 함

추가 고려 사항

볼륨 또는 애그리게이트의 공간이 부족해지면 파일 또는 LUN에 대한 쓰기 작업이 실패할 수 있습니다.

볼륨과 애그리게이트의 여유 공간을 적극적으로 모니터링하지 않으려면 볼륨에 대해 Autogrow를 활성화하고 볼륨의 최대 크기를 애그리게이트 크기로 설정해야 합니다. 이 구성에서는 aggregate 여유 공간을 적극적으로 모니터링해야 하지만, 볼륨의 여유 공간을 모니터링할 필요는 없습니다.

반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 LUN에 대한 구성 설정입니다

이 FlexVol 볼륨 및 파일 또는 LUN 구성 조합을 사용하면 완전히 프로비저닝된 조합보다 더 적은 양의 스토리지를 미리 할당할 수 있지만 볼륨에 사용할 수 있는 효율성 기술에 제한이 있습니다. 이러한 구성 조합의 경우 덮어쓰기의 작업이 가장 효율적으로 처리됩니다.

반씩 프로비저닝을 사용하여 볼륨에서 공간 예약 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	볼륨
부분 예약	0
스냅샷 예비 공간입니다	0
스냅샷 자동 삭제	제거 약속 수준에서는 모든 오브젝트, 볼륨으로 설정된 트리거, 자동 삭제를 위해 활성화된 모든 FlexClone LUN 및 FlexClone 파일이 포함된 제거 목록이 있습니다.
자동 확장	선택 사항: 사용하도록 설정한 경우 애그리게이트 가용 공간을 능동적으로 모니터링해야 합니다.

파일 또는 LUN 설정	값
공간 예약	활성화됨

기술 제한

이 구성 조합에는 다음 볼륨 스토리지 효율성 기술을 사용할 수 없습니다.

- 압축
- 중복 제거
- ODX 및 FlexClone 복사 오프로드
- FlexClone LUN 및 FlexClone 파일이 자동 삭제용으로 표시되지 않음(활성 클론)
- FlexClone 하위 파일
- ODX/복사 오프로드

추가 고려 사항

이 구성 조합을 사용할 때는 다음 사항을 고려해야 합니다.

- 해당 LUN을 지원하는 볼륨의 공간이 부족하면 보호 데이터(FlexClone LUN 및 파일, 스냅샷)가 삭제됩니다.
- 볼륨에 여유 공간이 부족하면 쓰기 작업이 시간 초과되어 실패할 수 있습니다.

압축은 AFF 플랫폼에 대해 기본적으로 사용하도록 설정되어 있습니다. AFF 플랫폼에서 반씩 프로비저닝을 사용하려는 모든 볼륨에 대해 압축을 명시적으로 해제해야 합니다.

SAN 데이터 보호

SAN 환경을 위한 ONTAP 데이터 보호 방법에 대해 알아보십시오

실수로 인한 삭제, 애플리케이션 충돌, 데이터 손상 또는 재해가 발생할 경우 복원에 사용할 수 있도록 데이터의 복사본을 만들어 데이터를 보호할 수 있습니다. ONTAP는 데이터 보호 및 백업 요구에 따라 데이터를 보호할 수 있는 다양한 방법을 제공합니다.

SnapMirror 활성화 동기화

ONTAP 9.9.1의 일반 가용성부터 SAN 환경에서 비즈니스 크리티컬 애플리케이션의 자동 페일오버를 지원하기 위해 제로 복구 시간 목표(제로 RTO) 또는 투명 애플리케이션 페일오버(TAF)를 제공합니다. SnapMirror 액티브 동기화를 사용하려면 2개의 AFF 클러스터 또는 2개의 ASA(All Flash SAN Array) 클러스터가 있는 구성으로 ONTAP Mediator 1.2를 설치해야 합니다.

"SnapMirror 활성화 동기화"

스냅샷

LUN의 여러 백업을 수동 또는 자동으로 생성, 예약 및 유지 관리할 수 있습니다. 스냅샷은 최소한의 추가 볼륨 공간만 사용하며 성능 비용이 들지 않습니다. LUN 데이터가 실수로 수정되거나 삭제된 경우 최신 스냅샷 중 하나에서 해당 데이터를 쉽고 빠르게 복원할 수 있습니다.

FlexClone LUN(FlexClone 라이선스 필요)

활성 볼륨 또는 스냅샷에 있는 다른 LUN의 쓰기 가능한 특정 시점 복사본을 제공합니다. 클론 및 상위 항목은 서로 영향을 주지 않고 독립적으로 수정할 수 있습니다.

SnapRestore(라이선스 필요)

전체 볼륨의 스냅샷에서 요청 시 데이터를 빠르고 공간 효율적으로 복구할 수 있습니다. SnapRestore를 사용하면 스토리지 시스템을 재부팅하지 않고도 LUN을 이전에 보존된 상태로 복원할 수 있습니다.

데이터 보호 미러 복사본(SnapMirror 라이선스 필요)

볼륨에 있는 데이터의 스냅샷을 주기적으로 생성하고, 로컬 또는 광역 네트워크를 통해 해당 스냅샷을 다른 클러스터에 있는 파트너 볼륨에 복사하고, 이러한 스냅샷을 보존할 수 있도록 함으로써 비동기식 재해 복구를 제공합니다. 소스 볼륨의 데이터가 손상되었거나 손실된 경우 파트너 볼륨의 미러 복사본을 사용하여 마지막 스냅샷 시점의 데이터를 빠르게 복구하고 복구할 수 있습니다.

SnapVault 백업(SnapMirror 라이선스 필요)

스토리지 효율적으로 장기 백업 보존 SnapVault 관계를 사용하면 선택한 볼륨 스냅샷을 대상 볼륨에 백업하고 백업을 유지할 수 있습니다.

테이프 백업 및 아카이브 작업을 수행하는 경우 SnapVault 보조 볼륨에 이미 백업된 데이터에 대해 수행할 수 있습니다.

기본 테이프 백업 및 복구

대부분의 기존 테이프 드라이브 지원은 ONTAP에 포함되어 있으며 테이프 공급업체가 새 디바이스에 대한 지원을 동적으로 추가하는 방법도 포함되어 있습니다. 또한 ONTAP는 RMT(Remote Magnetic Tape) 프로토콜을 지원하여 모든 가능 시스템에 백업 및 복구를 수행할 수 있습니다.

관련 정보

["테이프 백업을 사용한 데이터 보호"](#)

ONTAP 스냅샷에서 단일 LUN을 복구합니다

단일 LUN이 포함된 전체 볼륨을 복원하지 않고 스냅샷에서 단일 LUN을 복구할 수 있습니다. LUN을 제자리에서 또는 볼륨의 새 경로로 복원할 수 있습니다. 이 작업은 볼륨의 다른 파일 또는 LUN에 영향을 주지 않고 단일 LUN만 복구합니다. 스트림을 사용하여 파일을 복원할 수도 있습니다.

시작하기 전에

- 복원 작업을 완료하려면 볼륨에 충분한 공간이 있어야 합니다.
 - 부분 예약 공간이 0%인 공간 예약 LUN을 복원하는 경우 복원된 LUN 크기의 1배가 필요합니다.
 - 부분 예약 공간이 100%인 공간 예약 LUN을 복원하는 경우 복원된 LUN의 크기의 2배가 필요합니다.
 - 공간이 예약되지 않은 LUN을 복원하는 경우 복원된 LUN에 사용된 실제 공간만 필요합니다.
- 대상 LUN의 스냅샷이 생성되어야 합니다.

복구 작업이 실패하면 대상 LUN이 잘릴 수 있습니다. 이러한 경우 스냅샷을 사용하여 데이터 손실을 방지할 수 있습니다.

- 소스 LUN의 스냅샷이 생성되어야 합니다.

드물지만 LUN 복구가 실패하여 소스 LUN을 사용할 수 없게 되는 경우가 있습니다. 이 경우 스냅샷을 사용하여 LUN을 복구 시도 바로 전 상태로 되돌릴 수 있습니다.

- 대상 LUN과 소스 LUN의 OS 유형이 같아야 합니다.

대상 LUN의 OS 유형이 소스 LUN과 다른 경우 복구 작업 후 호스트가 대상 LUN에 대한 데이터 액세스를 잃을 수 있습니다.

단계

1. 호스트에서 LUN에 대한 모든 호스트 액세스를 중지합니다.
2. 호스트에서 LUN을 액세스할 수 없도록 해당 호스트에서 LUN을 마운트 해제합니다.
3. LUN 매핑을 해제합니다.

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

4. LUN을 복구할 스냅샷을 결정합니다.

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. LUN을 복구하기 전에 LUN의 스냅샷을 생성합니다.

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>  
-snapshot <snapshot_name>
```

6. 볼륨에 지정된 LUN을 복구합니다.

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>  
-snapshot <snapshot_name> -path <lun_path>
```

7. 화면의 단계를 따릅니다.
8. 필요한 경우 LUN을 온라인 상태로 전환합니다.

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. 필요한 경우 LUN을 다시 매핑합니다.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

10. 호스트에서 LUN을 다시 마운트합니다.
11. 호스트에서 LUN에 대한 액세스를 다시 시작합니다.

ONTAP 스냅샷에서 볼륨의 모든 LUN을 복구합니다

명령을 사용하여 스냅샷에서 지정된 볼륨의 모든 LUN을 복원할 수 `volume snapshot restore` 있습니다.

단계

1. 호스트에서 LUN에 대한 모든 호스트 액세스를 중지합니다.

볼륨에 있는 LUN에 대한 모든 호스트 액세스를 중지하지 않고 SnapRestore를 사용하면 데이터 손상 및 시스템 오류가 발생할 수 있습니다.

2. 호스트에서 LUN을 액세스할 수 없도록 해당 호스트에서 LUN을 마운트 해제합니다.
3. LUN 매핑 해제:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. 볼륨을 복원할 스냅샷을 결정합니다.

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. 권한 설정을 고급으로 변경합니다.

```
set -privilege advanced
```

6. 데이터 복원:

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

7. 화면의 지침을 따릅니다.
8. LUN을 다시 매핑합니다.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun <lun_name> -igroup <igroup_name>
```

9. LUN이 온라인 상태인지 확인합니다.

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. LUN이 온라인 상태가 아닌 경우 온라인 상태로 전환합니다.

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. 권한 설정을 admin으로 변경합니다.

```
set -privilege admin
```

12. 호스트에서 LUN을 다시 마운트합니다.

13. 호스트에서 LUN에 대한 액세스를 다시 시작합니다.

ONTAP FlexClone LUN으로 데이터를 보호합니다

FlexClone LUN은 활성 볼륨 또는 스냅샷에 있는 다른 LUN의 쓰기 가능한 시점 복제본입니다. 클론 및 상위 항목은 서로 영향을 주지 않고 독립적으로 수정할 수 있습니다.

FlexClone LUN을 사용하여 LUN의 읽기/쓰기 복사본을 여러 개 생성할 수 있습니다.

FlexClone LUN을 생성하는 이유

- 테스트를 위해 LUN의 임시 복사본을 생성해야 합니다.
- 운영 데이터에 대한 액세스 권한을 부여하지 않고 추가 사용자가 데이터 복사본을 사용할 수 있도록 해야 합니다.
- 원본 데이터는 변경되지 않은 형식으로 유지하면서 조작 및 예상 작업에 사용할 데이터베이스 복제본을 만들려는 경우
- LUN의 특정 데이터 하위 집합(볼륨 그룹 내의 특정 논리 볼륨 또는 파일 시스템, 또는 파일 시스템 내의 특정 파일 또는 파일 집합)에 액세스하여 원래 LUN에 복사하되, 원래 LUN의 나머지 데이터는 복원하지 않으려는 경우 이 기능을 사용할 수 있습니다. 이 기능은 LUN과 LUN 복제본을 동시에 마운트할 수 있는 운영 체제에서 작동합니다.
- 동일한 운영 체제를 사용하는 여러 SAN 부팅 호스트가 필요합니다.

FlexClone LUN은 처음에 부모 LUN과 공간을 공유합니다. 기본적으로 FlexClone LUN은 상위 LUN의 공간 예약 속성을 상속합니다. 예를 들어, 상위 LUN이 공간이 예약되지 않은 경우 FlexClone LUN도 기본적으로 공간이 예약되지 않습니다. 그러나 공간 예약 LUN인 상위에서 공간 예약 FlexClone LUN을 생성할 수 있습니다.

LUN을 클론 복제하면 블록 공유가 백그라운드에서 수행되며 블록 공유가 완료될 때까지 볼륨 스냅샷을 생성할 수 없습니다.

'볼륨 스냅샷 자동 삭제 수정' 명령을 사용하여 FlexClone LUN 자동 삭제 기능을 사용하도록 볼륨을 구성해야 합니다. 그렇지 않으면 FlexClone LUN이 자동으로 삭제되지만 FlexClone 자동 삭제에 대해 볼륨이 구성되지 않은 경우 FlexClone LUN이 삭제되지 않습니다.

FlexClone LUN을 생성할 때 FlexClone LUN 자동 삭제 기능은 기본적으로 해제되어 있습니다. FlexClone LUN을 자동으로 삭제하려면 먼저 모든 FlexClone LUN에서 수동으로 활성화해야 합니다. 반씩 볼륨 프로비저닝을 사용하고 이 옵션으로 제공되는 "최선 노력" 쓰기 보장을 원하는 경우, `_ALL_FlexClone LUN`을 자동 삭제할 수 있도록 해야 합니다.



스냅샷에서 FlexClone LUN을 생성할 때 LUN은 공간 효율적인 백그라운드 프로세스를 사용하여 스냅샷에서 자동으로 분할되므로 LUN이 계속해서 스냅샷에 의존하거나 추가 공간을 소비하지 않습니다. 이 백그라운드 분할이 완료되지 않고 이 스냅샷이 자동으로 삭제되면 해당 FlexClone LUN에 대한 FlexClone 자동 삭제 기능을 해제했더라도 해당 FlexClone LUN이 삭제됩니다. 백그라운드 분할이 완료된 후 해당 스냅샷이 삭제되더라도 FlexClone LUN은 삭제되지 않습니다.

관련 정보

- ["FlexClone LUN을 생성합니다"](#)
- ["FlexClone LUN을 자동으로 삭제하도록 FlexVol volume을 구성합니다"](#)
- ["FlexClone LUN이 자동으로 삭제되지 않도록 방지합니다"](#)

SAN 환경에서 SnapVault 백업을 구성하고 사용합니다

SAN 환경에서의 ONTAP SnapVault 백업에 대해 알아보십시오

SAN 환경에서 SnapVault 구성 및 사용은 NAS 환경에서 구성 및 사용과 매우 유사하지만, SAN 환경에서 LUN을 복원하려면 몇 가지 특별한 절차가 필요합니다.

SnapVault 백업에는 소스 볼륨의 읽기 전용 복제본 세트가 포함됩니다. SAN 환경에서는 개별 LUN이 아닌 전체 볼륨을 SnapVault 2차 볼륨에 항상 백업합니다.

LUN이 포함된 운영 볼륨과 SnapVault 백업 역할을 하는 보조 볼륨 간의 SnapVault 관계를 생성하고 초기화하는 절차는 파일 프로토콜에 사용되는 FlexVol 볼륨에서 사용되는 절차와 동일합니다. 이 절차는 에 자세히 설명되어 있습니다 ["데이터 보호"](#).

스냅샷이 생성되고 SnapVault 보조 볼륨에 복제되기 전에 백업되는 LUN이 정합성 보장 상태로 유지되도록 하는 것이 중요합니다. SnapCenter를 사용하여 스냅샷 생성을 자동화하면 백업된 LUN이 완료되어 원래 애플리케이션에서 사용할 수 있습니다.

SnapVault 2차 볼륨에서 LUN을 복구하는 기본적인 세 가지 선택 사항은 다음과 같습니다.

- SnapVault 2차 볼륨에서 LUN을 직접 매핑하고 호스트를 LUN에 연결하여 LUN의 콘텐츠를 액세스할 수 있습니다.

LUN은 읽기 전용이며 SnapVault 백업의 최신 스냅샷에서만 매핑할 수 있습니다. 영구 예약 및 기타 LUN 메타데이터가 손실됩니다. 필요한 경우 호스트에서 복제 프로그램을 사용하여 LUN 콘텐츠를 원래 LUN에 다시 복제할 수 있습니다(액세스할 수 있는 경우).

LUN의 일련 번호가 소스 LUN과 다릅니다.

- SnapVault 보조 볼륨의 모든 스냅샷을 새로운 읽기-쓰기 볼륨에 복제할 수 있습니다.

그런 다음 볼륨에 있는 LUN을 매핑하고 호스트를 LUN에 연결하여 LUN의 콘텐츠를 액세스할 수 있습니다. 필요한

경우 호스트에서 복제 프로그램을 사용하여 LUN 콘텐츠를 원래 LUN에 다시 복제할 수 있습니다(액세스할 수 있는 경우).

- SnapVault 2차 볼륨의 모든 스냅샷에서 LUN이 포함된 전체 볼륨을 복원할 수 있습니다.

전체 볼륨을 복원하면 볼륨에 있는 모든 LUN과 파일이 교체됩니다. 스냅샷이 생성된 이후에 생성된 모든 새 LUN은 손실됩니다.

LUN은 매핑, 일련 번호, UUID 및 영구 예약을 보유합니다.

ONTAP SnapVault 백업에서 읽기 전용 LUN 복사본에 액세스합니다

SnapVault 백업의 최신 스냅샷에서 LUN의 읽기 전용 복사본에 액세스할 수 있습니다. LUN ID, 경로 및 일련 번호는 소스 LUN과 다르며 먼저 매핑해야 합니다. 영구 예약, LUN 매핑 및 igroup은 SnapVault 2차 볼륨에 복제되지 않습니다.

시작하기 전에

- SnapVault 관계를 초기화해야 하며 SnapVault 2차 볼륨의 최신 스냅샷에 원하는 LUN이 포함되어 있어야 합니다.
- SnapVault 백업을 포함하는 SVM(스토리지 가상 머신)에는 LUN 복사본에 액세스하는 데 사용되는 호스트에서 액세스할 수 있는 원하는 SAN 프로토콜을 갖춘 하나 이상의 LIF가 있어야 합니다.
- SnapVault 2차 볼륨에서 LUN 복사본에 직접 액세스할 계획이라면 미리 SnapVault SVM에 igroup을 생성해야 합니다.

먼저 LUN이 포함된 볼륨을 복원하거나 클론 복제하지 않고도 SnapVault 2차 볼륨에서 LUN에 직접 액세스할 수 있습니다.

이 작업에 대해

이전 스냅샷에서 매핑된 LUN이 있는 동안 새 스냅샷이 SnapVault 보조 볼륨에 추가되면 매핑된 LUN의 콘텐츠가 변경됩니다. LUN은 여전히 동일한 식별자로 매핑되지만 데이터는 새 스냅샷에서 가져옵니다. LUN 크기가 변경되면 일부 호스트는 자동으로 크기 변경을 감지합니다. 크기 변경을 확인하려면 Windows 호스트에서 디스크를 재검색해야 합니다.

단계

1. SnapVault 2차 볼륨에서 사용 가능한 LUN을 나열합니다.

```
lun show
```

이 예에서는 운영 볼륨의 원래 LUN과 SnapVault 보조 볼륨 dstvolB의 복사본을 모두 볼 수 있습니다.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

```
6 entries were displayed.
```

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

- 원하는 호스트의 `igroup`이 SnapVault 2차 볼륨이 포함된 SVM에 이미 없으면 `igroup`을 생성합니다.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol  
<protocol> -ostype <ostype> -initiator <initiator_name>
```

이 명령은 iSCSI 프로토콜을 사용하는 Windows 호스트에 대한 `igroup`을 생성합니다.

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup  
-protocol iscsi -ostype windows  
-initiator iqn.1991-05.com.microsoft:hostA
```

- 원하는 LUN 복사본을 `igroup`에 매핑합니다.

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup  
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A  
-igroup temp_igroup
```

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

- 호스트를 LUN에 연결하고 필요에 따라 LUN의 콘텐츠를 액세스합니다.

ONTAP SnapVault 백업에서 단일 LUN을 복원합니다

단일 LUN을 새 위치 또는 원래 위치로 복구할 수 있습니다. SnapVault 2차 볼륨의 모든

스냅샷에서 복원할 수 있습니다. LUN을 원래 위치로 복구하려면 먼저 LUN을 새 위치로 복원한 다음 복사합니다.

시작하기 전에

- SnapVault 관계를 초기화해야 하며 SnapVault 보조 볼륨에 복구할 적절한 스냅샷이 포함되어 있어야 합니다.
- SnapVault 2차 볼륨을 포함하는 SVM(스토리지 가상 머신)에는 LUN 복사본에 액세스하는 데 사용되는 호스트에서 액세스할 수 있는 원하는 SAN 프로토콜을 갖춘 하나 이상의 LIF가 있어야 합니다.
- SnapVault SVM에 igroup이 이미 있어야 합니다.

이 작업에 대해

이 프로세스에는 SnapVault 2차 볼륨의 스냅샷에서 읽기-쓰기 볼륨 클론 생성이 포함됩니다. 클론에서 LUN을 직접 사용하거나 필요에 따라 LUN 콘텐츠를 원래 LUN 위치로 다시 복제할 수 있습니다.

클론의 LUN의 경로와 일련 번호가 원래 LUN과 다릅니다. 영구 예약은 유지되지 않습니다.

단계

1. SnapVault 백업이 포함된 보조 볼륨을 확인합니다.

```
snapmirror show
```

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

2. LUN을 복구할 스냅샷을 식별합니다.

```
volume snapshot show
```

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB					
		snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

3. 원하는 스냅샷에서 읽기-쓰기 클론을 생성합니다

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>  
-type <type> -parent-volume <parent_volume_name> -parent-snapshot  
<snapshot_name>
```

볼륨 클론은 SnapVault 백업과 동일한 애그리게이트에 생성됩니다. 클론을 저장할 공간이 Aggregate에 있어야 합니다.

```
cluster::> volume clone create -vserver vserverB  
-flexclone dstvolB_clone -type RW -parent-volume dstvolB  
-parent-snapshot daily.2013-02-10_0010  
[Job 108] Job succeeded: Successful
```

4. 볼륨 클론의 LUN을 나열합니다.

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone
```

Vserver	Path	State	Mapped	Type
vserverB	/vol/dstvolB_clone/lun_A	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_B	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_C	online	unmapped	windows

3 entries were displayed.

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

5. 원하는 호스트의 igroup이 SnapVault 백업이 포함된 SVM에 이미 없으면 igroup을 생성합니다.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

이 예는 iSCSI 프로토콜을 사용하는 Windows 호스트에 대한 igroup을 생성합니다.

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
-protocol iscsi -ostype windows
-initiator iqn.1991-05.com.microsoft:hostA
```

6. 원하는 LUN 복사본을 igroup에 매핑합니다.

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
-path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

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

7. 호스트를 LUN에 연결하고 필요에 따라 LUN의 콘텐츠를 액세스합니다.

LUN은 읽기/쓰기이며 원래 LUN 대신 사용할 수 있습니다. LUN 일련 번호가 다르므로 호스트는 이 일련 번호를 원본과 다른 LUN으로 해석합니다.

8. 호스트에서 복제 프로그램을 사용하여 LUN 콘텐츠를 원래 LUN에 다시 복제합니다.

관련 정보

- "[스냅미러 쇼](#)"

ONTAP SnapVault 백업에서 볼륨의 모든 LUN을 복원합니다

SnapVault 백업에서 볼륨에 있는 하나 이상의 LUN을 복원해야 하는 경우 전체 볼륨을 복원할 수 있습니다. 볼륨을 복원하면 볼륨의 모든 LUN에 영향을 줍니다.

시작하기 전에

SnapVault 관계를 초기화해야 하며 SnapVault 보조 볼륨에 복구할 적절한 스냅샷이 포함되어 있어야 합니다.

이 작업에 대해

전체 볼륨을 복원하면 볼륨이 스냅샷이 생성된 시점의 상태로 돌아갑니다. 스냅샷 후에 LUN이 볼륨에 추가된 경우 복구 프로세스 중에 해당 LUN이 제거됩니다.

볼륨을 복원한 후 LUN은 복원 직전에 매핑된 igroup에 계속 매핑됩니다. LUN 매핑은 스냅샷 시점의 매핑과 다를 수 있습니다. 호스트 클러스터의 LUN에 대한 영구 예약이 유지됩니다.

단계

1. 볼륨에 있는 모든 LUN에 대한 입출력을 중지합니다.
2. SnapVault 2차 볼륨이 포함된 2차 볼륨을 확인합니다.

```
snapmirror show
```

```
cluster::> snapmirror show
```

Source Path	Dest Type	Mirror Path	Relation State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

3. 복원할 스냅샷을 식별합니다.

```
volume snapshot show
```

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

4. 사용할 스냅샷을 지정합니다.

```
snapmirror restore -destination-path <destination_path> -source-path <source_path> -source-snapshot <snapshot_name>
```

복원을 위해 지정하는 대상은 복원 중인 원본 볼륨입니다.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
      -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. 호스트 클러스터에서 LUN을 공유하는 경우 영향을 받는 호스트에서 LUN의 영구 예약을 복원합니다.

SnapVault 백업에서 볼륨 복원

다음 예에서는 스냅샷이 생성된 후에 LUN_D라는 LUN이 볼륨에 추가되었습니다. 스냅샷에서 전체 볼륨을 복구한 후 LUN_D가 더 이상 나타나지 않습니다.

'lun show' 명령 출력에서 운영 볼륨의 srcvolA 및 SnapVault 보조 볼륨 dstvolB에서 해당 LUN의 읽기 전용 복제본을 확인할 수 있습니다. SnapVault 백업에는 LUN_D의 복제본이 없습니다.

```
cluster::> lun show
Vserver    Path                               State  Mapped  Type        Size
-----
vserverA   /vol/srcvolA/lun_A                online mapped    windows    300.0GB
vserverA   /vol/srcvolA/lun_B                online mapped    windows    300.0GB
vserverA   /vol/srcvolA/lun_C                online mapped    windows    300.0GB
vserverA   /vol/srcvolA/lun_D                online mapped    windows    250.0GB
vserverB   /vol/dstvolB/lun_A                online unmapped  windows    300.0GB
vserverB   /vol/dstvolB/lun_B                online unmapped  windows    300.0GB
vserverB   /vol/dstvolB/lun_C                online unmapped  windows    300.0GB
```

7 entries were displayed.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
-sources-path vserverB:dstvolB
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than snapshot hourly.2013-02-11_1205 on volume vserverA:src_volA will be deleted.

Do you want to continue? {y|n}: y

[Job 98] Job is queued: snapmirror restore from source "vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

```
cluster::> lun show
Vserver    Path                               State  Mapped  Type        Size
-----
vserverA   /vol/srcvolA/lun_A                online mapped    windows    300.0GB
vserverA   /vol/srcvolA/lun_B                online mapped    windows    300.0GB
vserverA   /vol/srcvolA/lun_C                online mapped    windows    300.0GB
vserverB   /vol/dstvolB/lun_A                online unmapped  windows    300.0GB
vserverB   /vol/dstvolB/lun_B                online unmapped  windows    300.0GB
vserverB   /vol/dstvolB/lun_C                online unmapped  windows    300.0GB
```

6 entries were displayed.

SnapVault 보조 볼륨에서 볼륨을 복구한 후에는 소스 볼륨에 LUN_D가 더 이상 포함되지 않습니다 복구 후 소스 볼륨의 LUN은 여전히 매핑되므로 LUN을 다시 매핑할 필요가 없습니다.

관련 정보

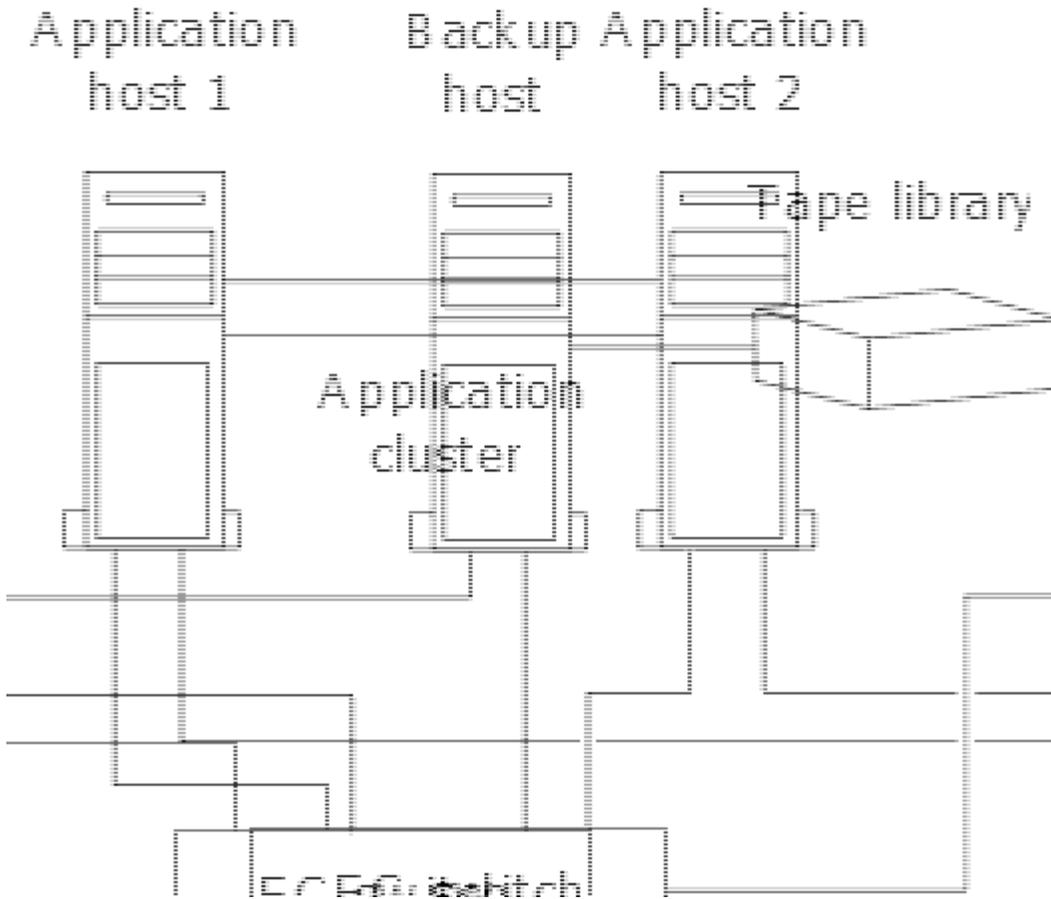
- ["SnapMirror 복원"](#)
- ["스냅미러 쇼"](#)

호스트 백업 시스템을 **ONTAP**에 연결하기 위한 권장 구성입니다

별도의 백업 호스트를 통해 SAN 시스템을 테이프 백업하여 애플리케이션 호스트의 성능

저하를 방지할 수 있습니다.

백업을 위해 SAN 및 NAS 데이터를 별도로 유지해야 합니다. 아래 그림은 운영 스토리지 시스템에 대한 호스트 백업 시스템의 권장 물리적 구성을 보여 줍니다. 볼륨을 SAN 전용으로 구성해야 합니다. LUN은 단일 볼륨으로 제한하거나 여러 볼륨 또는 스토리지 시스템에 분산할 수 있습니다.



호스트의 볼륨은 스토리지 시스템에서 매핑된 단일 LUN 또는 HP-UX 시스템의 VxVM과 같은 볼륨 관리자를 사용하여 여러 LUN으로 구성될 수 있습니다.

호스트 백업 시스템을 사용하여 **ONTAP** 스토리지 시스템의 **LUN**을 보호합니다

스냅샷에서 클론 생성된 LUN을 호스트 백업 시스템의 소스 데이터로 사용할 수 있습니다.

시작하기 전에

프로덕션 LUN이 존재해야 하며 애플리케이션 서버의 WWPN 또는 이니시에이터 노드 이름을 포함하는 igroup에 매핑되어야 합니다. 또한 LUN은 포맷되어 호스트에서 액세스할 수 있어야 합니다.

단계

1. 호스트 파일 시스템 버퍼의 내용을 디스크에 저장합니다.

호스트 운영 체제에서 제공하는 명령어를 사용할 수 있습니다. 또는 이 단계를 SAN 백업 사전 처리 스크립트에 포함시킬 수도 있습니다.

2. 운영 LUN의 스냅샷을 생성합니다.

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot> -comment <comment> -foreground false
```

3. 운영 LUN의 클론을 생성합니다.

```
volume file clone create -vserver <SMV_name> -volume <volume> -source
-path <path> -snapshot-name <snapshot> -destination-path
<destination_path>
```

4. 백업 서버의 WWPN을 포함하는 igroup을 생성합니다.

```
lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
<protocol> -ostype <os_type> -initiator <initiator>
```

5. 3단계에서 생성한 LUN 클론을 백업 호스트에 매핑합니다.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup>
```

이 단계를 SAN 백업 애플리케이션의 사후 처리 스크립트에 포함하도록 선택할 수 있습니다.

6. 호스트에서 새 LUN을 검색하고 호스트에서 파일 시스템을 사용할 수 있도록 설정합니다.

이 단계를 SAN 백업 애플리케이션의 사후 처리 스크립트에 포함하도록 선택할 수 있습니다.

7. SAN 백업 애플리케이션을 사용하여 백업 호스트에서 테이프에 LUN 클론의 데이터를 백업합니다.

8. LUN 클론을 오프라인 상태로 전환합니다.

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. LUN 클론을 제거합니다.

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. 스냅샷을 제거합니다.

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

SAN 구성 참조

ONTAP SAN 구성에 대해 자세히 알아보십시오

SAN(Storage Area Network)은 iSCSI 또는 FC와 같은 SAN 전송 프로토콜을 통해 호스트에 연결된 스토리지 솔루션으로 구성됩니다. 스토리지 솔루션이 하나 이상의 스위치를 통해 호스트에 연결되도록 SAN을 구성할 수 있습니다. iSCSI를 사용하는 경우 스위치를 사용하지 않고 스토리지 솔루션을 호스트에 직접 연결하도록 SAN을 구성할 수도 있습니다.

SAN에서는 Windows, Linux 또는 UNIX와 같은 서로 다른 운영 체제를 사용하는 여러 호스트가 동시에 스토리지 솔루션에 액세스할 수 있습니다. 을 사용할 수 있습니다 ["선택적 LUN 매핑"](#) 및 ["포트 세트"](#) 호스트와 스토리지 간의 데이터 액세스를 제한합니다.

iSCSI의 경우 스토리지 솔루션과 호스트 간의 네트워크 토폴로지를 네트워크라고 합니다. FC, FC/NVMe 및 FCoE의 경우 스토리지 솔루션과 호스트 사이의 네트워크 토폴로지를 패브릭이라고 합니다. 데이터 액세스 손실로부터 시스템을 보호하는 이중화를 생성하려면 다중 네트워크 또는 다중 패브릭 구성에서 HA 쌍으로 SAN을 설정해야 합니다. 단일 노드 또는 단일 네트워크/패브릭을 사용하는 구성은 완전히 중복되지 않으므로 권장되지 않습니다.

SAN을 구성한 후 수행할 수 있습니다 ["iSCSI 또는 FC용 스토리지를 프로비저닝합니다"](#) 또는 직접 할 수 있습니다 ["FC/NVMe용 스토리지를 프로비저닝합니다"](#). 그런 다음 호스트에 연결하여 데이터 서비스를 시작할 수 있습니다.

SAN 프로토콜 지원은 ONTAP 버전, 플랫폼 및 구성에 따라 다릅니다. 특정 구성에 대한 자세한 내용은 를 참조하십시오 ["NetApp 상호 운용성 매트릭스 툴"](#).

관련 정보

- ["SAN 관리 개요"](#)
- ["NVMe 구성, 지원 및 제한 사항"](#)

iSCSI 구성

ONTAP 시스템으로 iSCSI 네트워크를 구성합니다

iSCSI SAN 호스트에 직접 연결하거나 하나 이상의 IP 스위치를 통해 호스트에 연결하는 고가용성(HA) 쌍을 사용하여 iSCSI 구성을 설정해야 합니다.

["HA 쌍"](#) 는 호스트가 LUN을 액세스하는 데 사용할 Active/Optimized 및 Active/Unoptimized 경로에 대한 보고 노드로 정의됩니다. Windows, Linux 또는 UNIX와 같은 서로 다른 운영 체제를 사용하는 여러 호스트가 스토리지를 동시에 액세스할 수 있습니다. 호스트는 ALUA를 지원하는 지원되는 다중 경로 솔루션을 설치 및 구성해야 합니다. 지원되는 운영 체제 및 다중 경로 솔루션은 에서 확인할 수 있습니다 ["NetApp 상호 운용성 매트릭스 툴"](#).

다중 네트워크 구성에서는 호스트를 스토리지 시스템에 연결하는 스위치가 두 개 이상 있습니다. 다중 네트워크 구성은 완전히 중복되므로 권장됩니다. 단일 네트워크 구성에는 호스트를 스토리지 시스템에 연결하는 스위치 하나가 있습니다. 단일 네트워크 구성은 완전히 중복되지 않습니다.



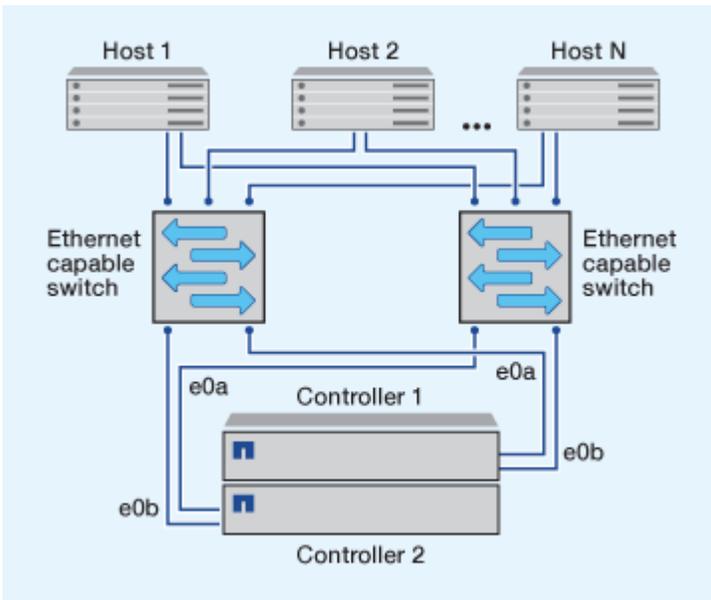
["단일 노드 구성"](#) 내결함성 및 무중단 운영을 지원하는 데 필요한 이중화를 제공하지 않기 때문에 권장되지 않습니다.

관련 정보

- HA Pair 소유의 LUN에 액세스하는 데 사용되는 경로를 제한하는 방법에 대해 "[선택적 LUN 매핑 \(SLM\)](#)"알아보십시오.
- 에 대해 자세히 알아보십시오 "[SAN LIF](#)".
- 에 대해 자세히 알아보십시오 "[iSCSI에서 VLAN의 이점](#)".

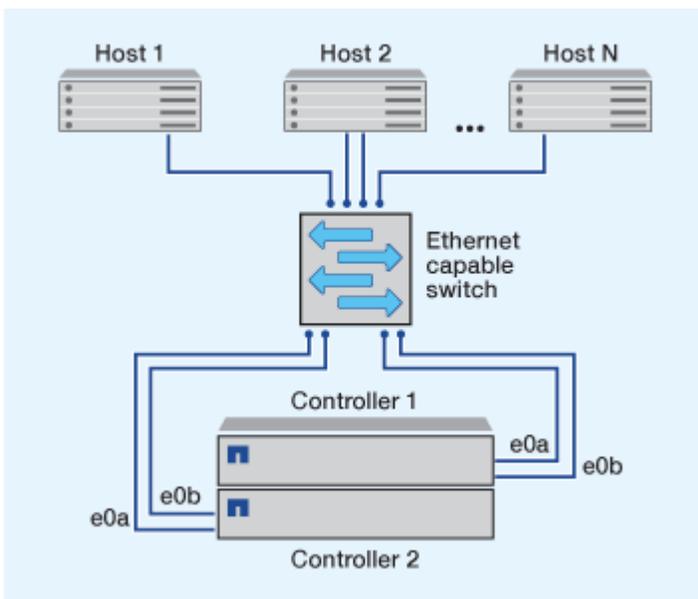
다중 네트워크 iSCSI 구성

다중 네트워크 HA 쌍 구성에서는 2개 이상의 스위치가 하나 이상의 호스트에 HA 쌍을 연결합니다. 스위치가 여러 개 있으므로 이 구성은 완전히 중복됩니다.



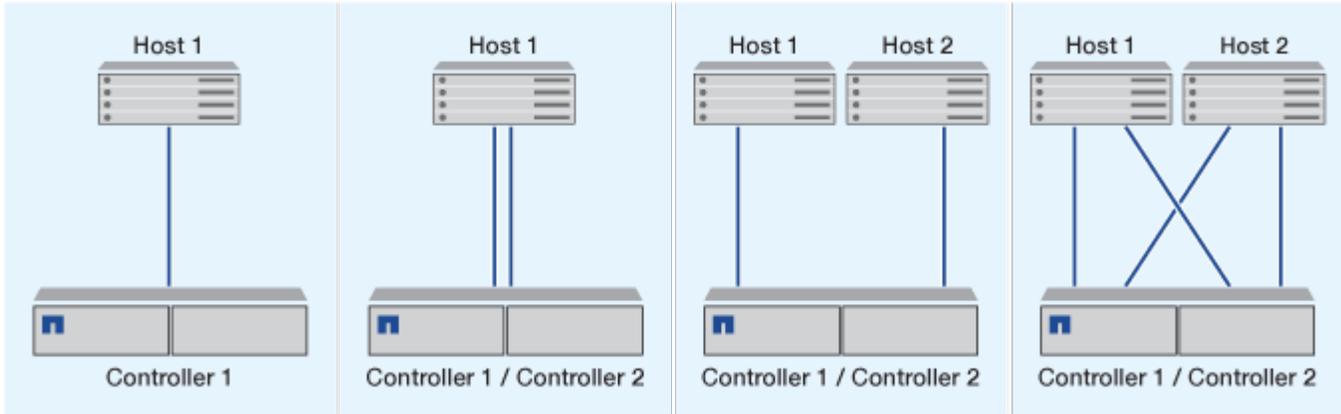
단일 네트워크 iSCSI 구성

단일 네트워크 HA Pair 구성에서 1개의 스위치는 HA 쌍을 하나 이상의 호스트에 연결합니다. 단일 스위치가 있으므로 이 구성은 완전히 중복되지 않습니다.



직접 연결 iSCSI 구성

직접 연결 구성에서는 하나 이상의 호스트가 컨트롤러에 직접 연결됩니다.



iSCSI 구성에서 ONTAP 시스템과 함께 VLAN을 사용할 때의 이점

VLAN은 브로드캐스트 도메인으로 그룹화된 스위치 포트 그룹으로 구성됩니다. VLAN은 단일 스위치에 있거나 여러 스위치 샤페에 걸쳐 있을 수 있습니다. 정적 및 동적 VLAN을 사용하면 IP 네트워크 인프라 내에서 보안을 강화하고, 문제를 격리하고, 사용 가능한 경로를 제한할 수 있습니다.

대규모 IP 네트워크 인프라에서 VLAN을 구현할 경우 다음과 같은 이점을 얻을 수 있습니다.

- 보안 강화:

VLAN을 사용하면 이더넷 네트워크 또는 IP SAN의 여러 노드 간 액세스를 제한하므로 기존 인프라를 활용하는 동시에 보안을 강화할 수 있습니다.

- 문제를 격리하여 이더넷 네트워크 및 IP SAN 안정성 향상
- 문제 공간을 제한하여 문제 해결 시간 단축
- 특정 iSCSI 타겟 포트에 대한 사용 가능한 경로 수 감소
- 호스트에서 사용하는 최대 경로 수 감소

경로가 너무 많으면 재연결 시간이 느려집니다. 호스트에 다중 경로 솔루션이 없는 경우 VLAN을 사용하여 하나의 경로만 허용할 수 있습니다.

동적 VLAN

동적 VLAN은 MAC 주소를 기반으로 합니다. 포함할 멤버의 MAC 주소를 지정하여 VLAN을 정의할 수 있습니다.

동적 VLAN은 유연성을 제공하며 장치가 물리적으로 스위치에 연결되어 있는 물리적 포트에 매핑하지 않아도 됩니다. VLAN을 재구성하지 않고도 한 포트에서 다른 포트에 케이블을 이동할 수 있습니다.

정적 VLAN

정적 VLAN은 포트 기반입니다. 스위치 및 스위치 포트는 VLAN 및 해당 구성원을 정의하는 데 사용됩니다.

정적 VLAN은 MAC(Media Access Control) 스푸핑을 사용하여 VLAN을 위반할 수 없기 때문에 보안이 향상됩니다. 그러나 다른 사람이 스위치에 물리적으로 액세스할 수 있는 경우 케이블을 교체하고 네트워크 주소를 다시 구성하면 액세스가 허용됩니다.

일부 환경에서는 동적 VLAN보다 정적 VLAN을 쉽게 생성하고 관리할 수 있습니다. 정적 VLAN은 48비트 MAC 주소 대신 스위치 및 포트 식별자만 지정할 수 있기 때문입니다. 또한 스위치 포트 범위에 VLAN 식별자를 사용하여 레이블을 지정할 수 있습니다.

FC 구성

ONTAP 시스템으로 **FC** 또는 **FC-NVMe** 패브릭을 구성합니다

HA 쌍과 최소 2개의 스위치를 사용하여 FC 및 FC-NVMe SAN 호스트를 구성하는 것이 좋습니다. 따라서 패브릭 및 스토리지 시스템 계층에서 이중화를 제공하여 내결함성과 무중단 운영을 지원합니다. 스위치를 사용하지 않고 FC 또는 FC-NVMe SAN 호스트를 HA 쌍에 직접 연결할 수 없습니다.

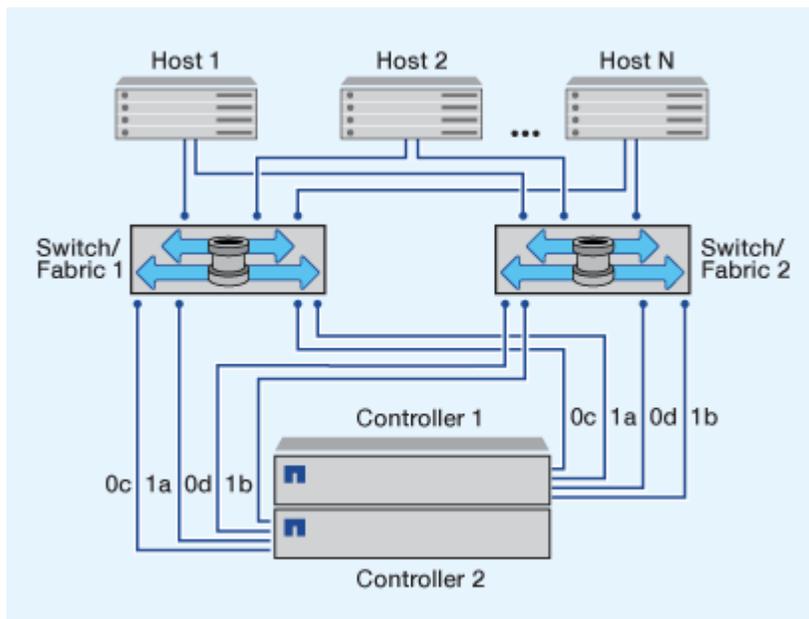
캐스케이드, 부분 메시, 풀 메시, 코어 에지 및 디렉터 패브릭은 모두 FC 스위치를 패브릭에 연결하는 업계 표준 방법이며 모두 지원됩니다. 임베디드 블레이드 스위치의 경우를 제외하고 이기종 FC 스위치 패브릭을 사용할 수 없습니다. 특정 예외는 에 나열되어 있습니다 "[상호 운용성 매트릭스 툴](#)". 패브릭은 하나 또는 여러 개의 스위치로 구성될 수 있으며, 스토리지 컨트롤러를 여러 스위치에 연결할 수 있습니다.

Windows, Linux 또는 UNIX와 같은 서로 다른 운영 체제를 사용하는 여러 호스트가 스토리지 컨트롤러에 동시에 액세스할 수 있습니다. 호스트에서는 지원되는 다중 경로 솔루션을 설치하고 구성해야 합니다. 지원되는 운영 체제 및 다중 경로 솔루션은 상호 운용성 매트릭스 툴에서 확인할 수 있습니다.

Multifabric FC 및 FC-NVMe 구성

멀티패브릭 HA 쌍 구성에서는 HA 쌍을 하나 이상의 호스트에 연결하는 스위치가 2개 이상 있습니다. 다음 멀티 패브릭 HA 쌍 그림은 2개의 패브릭만 보여주지만, 모든 멀티 패브릭 구성에 2개 이상의 패브릭을 사용할 수 있습니다.

그림에 표시된 FC 대상 포트 번호(0c, 0d, 1a, 1b)가 예시입니다. 실제 포트 번호는 스토리지 노드의 모델 및 확장 어댑터를 사용하고 있는지에 따라 다릅니다.

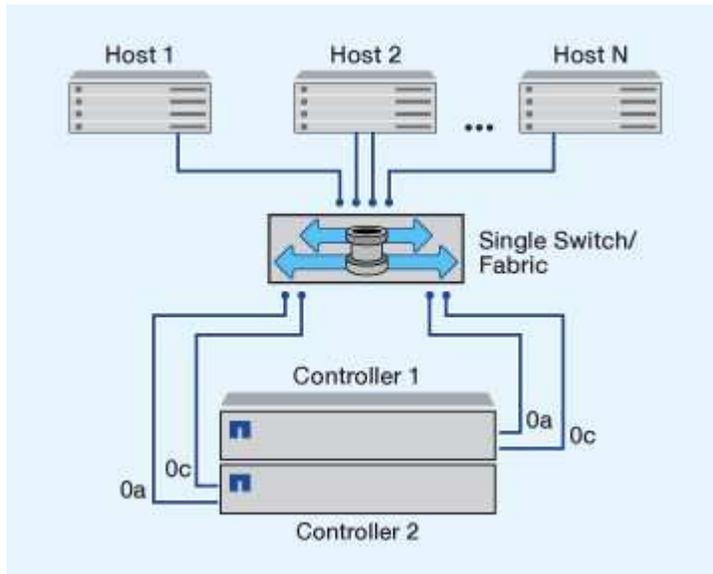


단일 패브릭 FC 및 FC-NVMe 구성

단일 패브릭 HA 쌍 구성에서는 HA 쌍의 두 컨트롤러를 하나 이상의 호스트에 연결하는 하나의 패브릭이 있습니다. 호스트와 컨트롤러가 단일 스위치를 통해 연결되므로 단일 패브릭 HA 쌍 구성은 완전히 이중화되지 않습니다.

그림에 표시된 FC 타겟 포트 번호(0a, 0c)가 예입니다. 실제 포트 번호는 스토리지 노드의 모델 및 확장 어댑터를 사용하고 있는지에 따라 다릅니다.

FC 구성을 지원하는 모든 플랫폼은 단일 패브릭 HA 쌍 구성을 지원합니다.



"단일 노드 구성" 내결함성 및 무중단 운영을 지원하는 데 필요한 이중화를 제공하지 않기 때문에 권장되지 않습니다.

관련 정보

- HA Pair 소유의 LUN에 액세스하는 데 사용되는 경로를 제한하는 방법에 대해 "[선택적 LUN 매핑 \(SLM\)](#)" 알아보십시오.
- 에 대해 자세히 알아보십시오 "[SAN LIF](#)".

ONTAP 시스템으로 FC 스위치를 구성하는 모범 사례

최상의 성능을 얻으려면 FC 스위치를 구성할 때 특정 모범 사례를 고려해야 합니다.

고정 링크 속도 설정은 FC 스위치 구성의 모범 사례이며, 특히 대규모 패브릭의 경우 패브릭 리빌드에 최고의 성능을 제공하고 시간을 크게 단축할 수 있기 때문에 그렇습니다. 자동 협상은 유연성이 높지만 FC 스위치 구성이 예전처럼 수행하지 않기 때문에 전체적인 패브릭 구성 시퀀스의 시간이 길어집니다.

Fabric에 연결된 모든 스위치는 NPIV(N_Port ID Virtualization)를 지원해야 하며 NPIV를 설정해야 합니다. ONTAP는 NPIV를 사용하여 패브릭에 FC 대상을 제공합니다.

지원되는 환경에 대한 자세한 내용은 를 참조하십시오 "[NetApp 상호 운용성 매트릭스 툴](#)".

FC 및 iSCSI 모범 사례는 를 참조하십시오 "[NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례](#)".

ONTAP 시스템에 권장되는 FC 타겟 포트 구성 및 속도

FC 타겟 포트는 FC 프로토콜에 대해 구성 및 사용되는 것과 정확히 동일한 방법으로 FC-NVMe 프로토콜에 대해 구성하고 사용할 수 있습니다. FC-NVMe 프로토콜에 대한 지원은 사용하는 플랫폼과 ONTAP 버전에 따라 다릅니다. NetApp Hardware Universe를 사용하여 지원을 확인합니다.

최상의 성능과 가용성을 얻으려면 특정 플랫폼에 대해 나와 있는 권장 대상 포트 구성을 사용하여 "[NetApp Hardware Universe](#)를 참조하십시오" 합니다.

공유 ASIC를 통한 FC 타겟 포트 구성

다음 플랫폼에는 공유 ASIC(Application-Specific Integrated Circuits)와 포트 쌍이 있습니다. 확장 어댑터를 이러한 플랫폼에 사용할 경우 연결에 동일한 ASIC를 사용하지 않도록 FC 포트를 구성해야 합니다.

컨트롤러	공유 ASIC가 있는 포트 쌍	대상 포트 수: 권장 포트 수
<ul style="list-style-type: none"> FAS8200를 참조하십시오 AFF A300 	0g + 0h	1:0g 2:0g, 0h
<ul style="list-style-type: none"> FAS2720 FAS2750 AFF A220 	0C+0d 0e+0f	1:0c 2:0c, 0e 3:0c, 0e, 0d 4:0c, 0e, 0d, 0f

FC 타겟 포트의 지원 속도입니다

FC 타겟 포트는 다른 속도로 실행되도록 구성할 수 있습니다. 지정된 호스트에서 사용하는 모든 타겟 포트는 동일한 속도로 설정되어야 합니다. 대상 포트 속도를 연결할 장치의 속도와 일치하도록 설정해야 합니다. 포트 속도에 자동 협상을 사용하지 마십시오. autonegotiation으로 설정된 포트는 Takeover/Giveback 또는 기타 중단 후 다시 연결하는 데 더 오래 걸릴 수 있습니다.

다음과 같은 속도로 실행되도록 온보드 포트 및 확장 어댑터를 구성할 수 있습니다. 필요에 따라 각 컨트롤러 및 확장 어댑터 포트를 각기 다른 속도로 구성할 수 있습니다.

4Gb 포트	8Gb 포트	16Gb 포트	32 Gb 포트
<ul style="list-style-type: none"> 4Gb 2Gb 1Gb 	<ul style="list-style-type: none"> 8Gb 4Gb 2Gb 	<ul style="list-style-type: none"> 16Gb 8Gb 4Gb 	<ul style="list-style-type: none"> 32Gb 16Gb 8Gb

지원되는 어댑터 및 지원되는 속도의 전체 목록은 를 참조하십시오 "[NetApp Hardware Universe를 참조하십시오](#)".

ONTAP FC 어댑터 포트를 구성합니다

온보드 FC 어댑터 및 일부 FC 확장 어댑터 카드는 이니시에이터 또는 대상 포트에 개별적으로 구성할 수 있습니다. 다른 FC 확장 어댑터는 출고 시 이니시에이터 또는 대상으로 구성되므로 변경할 수 없습니다. FC SFP+ 어댑터로 구성된 지원 UTA2 카드를 통해서도 추가 FC 포트를

사용할 수 있습니다.

이니시에이터 포트를 사용하여 백엔드 디스크 쉘프 및 외부 스토리지 어레이에 직접 연결할 수 있습니다. 타겟 포트는 FC 스위치에만 연결할 수 있습니다.

FC용으로 구성된 온보드 포트 및 CNA/UTA2 포트의 수는 컨트롤러의 모델에 따라 다릅니다. 지원되는 타겟 확장 어댑터도 컨트롤러 모델에 따라 다릅니다. 컨트롤러 모델에 지원되는 온보드 FC 포트 및 타겟 확장 어댑터의 전체 목록은 ["NetApp Hardware Universe를 참조하십시오"](#).

이니시에이터 모드에 맞게 **FC** 어댑터를 구성합니다

이니시에이터 모드는 외부 LUN 가져오기(FLI)를 통해 포트를 테이프 드라이브, 테이프 라이브러리 또는 타사 스토리지에 연결하는 데 사용됩니다.

시작하기 전에

- 어댑터에 있는 LIF는 해당 LIF가 구성원인 포트 세트에서 제거해야 합니다.
- 물리적 포트의 속성을 타겟에서 이니시에이터로 변경하기 전에 수정할 물리적 포트를 사용하는 모든 SVM(스토리지 가상 머신)의 모든 LIF를 마이그레이션 또는 제거해야 합니다.



NVMe/FC는 이니시에이터 모드를 지원합니다.

단계

1. 어댑터에서 모든 LIF를 제거합니다.

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. 어댑터를 오프라인 상태로 전환:

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_ -status-admin down
```

어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

3. 어댑터를 타겟에서 이니시에이터로 변경합니다.

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.
5. FC 포트가 구성에 맞는 올바른 상태로 구성되었는지 확인합니다.

```
system hardware unified-connect show
```

6. 어댑터를 다시 온라인으로 전환합니다.

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

FC 어댑터를 타겟 모드로 구성합니다

타겟 모드는 포트를 FC 이니시에이터에 연결하는 데 사용됩니다.

FC 프로토콜 및 FC-NVMe 프로토콜에 사용할 FC 어댑터를 구성하는 데 동일한 단계가 사용됩니다. 하지만 특정 FC 어댑터만 FC-NVMe를 지원합니다. FC-NVMe 프로토콜을 지원하는 어댑터 목록은 ["NetApp Hardware Universe를 참조하십시오"](#).

단계

1. 어댑터를 오프라인 상태로 전환:

```
node run -node _node_name_ storage disable adapter _adapter_name_
```

어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

2. 어댑터를 이니시에이터에서 타겟으로 변경합니다.

```
system node hardware unified-connect modify -t target -node _node_name_ adapter _adapter_name_
```

3. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.
4. 타겟 포트의 구성이 올바른지 확인합니다.

```
network fcp adapter show -node _node_name_
```

5. 어댑터를 온라인으로 전환합니다.

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_ -state up
```

FC 어댑터 속도를 구성합니다

자동 협상을 사용하는 대신 어댑터 대상 포트 속도를 연결할 장치의 속도와 일치하도록 구성해야 합니다. autonegotiation으로 설정된 포트는 Takeover/Giveback 또는 기타 중단 후 다시 연결하는 데 더 오랜 시간이 걸릴 수 있습니다.

이 작업에 대해

이 작업에는 클러스터의 모든 SVM(Storage Virtual Machine)과 모든 LIF가 포함되므로 이 작업의 범위를 제한하려면 '-home-port' 및 '-home-lif' 매개 변수를 사용해야 합니다. 이러한 매개 변수를 사용하지 않으면 클러스터에 있는 모든 LIF에 작업이 적용되며, 이는 바람직하지 않을 수 있습니다.

시작하기 전에

이 어댑터를 홈 포트에 사용하는 모든 LIF는 오프라인 상태여야 합니다.

단계

1. 이 어댑터의 모든 LIF를 오프라인 상태로 전환:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c } -status-admin down
```

2. 어댑터를 오프라인 상태로 전환:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

3. 포트 어댑터의 최대 속도를 확인합니다.

```
fcp adapter show -instance
```

어댑터 속도를 최대 속도 이상으로 수정할 수 없습니다.

4. 어댑터 속도를 변경합니다.

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. 어댑터를 온라인으로 전환합니다.

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. 어댑터에 있는 모든 LIF를 온라인으로 전환합니다.

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c } -status-admin up
```

FC 어댑터를 관리하기 위한 ONTAP 명령입니다

FC 명령을 사용하여 스토리지 컨트롤러에 대한 FC 타겟 어댑터, FC 이니시에이터 어댑터 및 온보드 FC 어댑터를 관리할 수 있습니다. FC 프로토콜과 FC-NVMe 프로토콜을 위해 FC 어댑터를 관리하는 데 동일한 명령이 사용됩니다.

FC 이니시에이터 어댑터 명령은 노드 레벨에서만 작동합니다. FC Initiator Adapter 명령을 사용하려면 먼저 'run-node_node_name_' 명령을 사용해야 합니다.

FC 타겟 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드에 FC 어댑터 정보를 표시합니다	네트워크 FCP 어댑터가 표시됩니다
FC 타겟 어댑터 매개 변수를 수정합니다	네트워크 FCP 어댑터 수정
FC 프로토콜 트래픽 정보를 표시합니다	'run-node_node_name_sysstat -f'
FC 프로토콜이 실행된 시간을 표시합니다	'run-node_node_name_uptime'
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'
명령에 대한 man 페이지를 봅니다	man command_name'입니다

FC 이니시에이터 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드의 모든 이니시에이터 및 해당 어댑터에 대한 정보를 표시합니다	'run-node_node_name_storage show adapter'입니다
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'

온보드 **FC** 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
온보드 FC 포트의 상태를 표시합니다	'시스템 노드 하드웨어 통합 접속 쇼

관련 정보

- ["네트워크 FCP 어댑터"](#)

X1133A-R6 어댑터를 사용하는 **ONTAP** 시스템에 대한 연결 손실을 방지합니다

별도의 X1133A-R6 HBA에 대한 중복 경로를 사용하여 시스템을 구성하면 포트 장애 시 연결이 끊어지지 않습니다.

X1133A-R6 HBA는 2개의 2포트 쌍으로 구성된 4포트, 16Gb FC 어댑터입니다. X1133A-R6 어댑터는 타겟 모드 또는 이니시에이터 모드로 구성할 수 있습니다. 각 2포트 쌍은 단일 ASIC에서 지원됩니다(예: ASIC 1의 포트 1과 포트 2, ASIC 2의 포트 3과 포트 4). 단일 ASIC의 두 포트는 타겟 모드나 이니시에이터 모드에서 동일한 모드로 작동하도록 구성해야 합니다. ASIC에서 쌍을 지원하는 데 오류가 발생하면 페어의 두 포트가 모두 오프라인 상태가 됩니다.

이러한 접속 구성 손실을 방지하려면 X1133A-R6 HBA를 분리하는 이중 경로 또는 HBA의 다른 ASIC에서 지원되는 포트에 대한 이중 경로를 사용하여 시스템을 구성합니다.

FCoE 구성

ONTAP 시스템으로 **FCoE** 패브릭을 구성합니다

FCoE는 다양한 방법으로 FCoE 스위치를 사용하여 구성할 수 있습니다. 직접 연결 구성은 FCoE에서 지원되지 않습니다.

모든 FCoE 구성은 이중 패브릭이며 완전히 이중화되며 호스트측 다중 경로 소프트웨어가 필요합니다. 모든 FCoE 구성에서는 이니시에이터와 타겟 사이의 경로에 최대 홉 수 제한까지 여러 FCoE 및 FC 스위치를 포함할 수 있습니다. 스위치를 서로 연결하려면 스위치가 이더넷 ISL을 지원하는 펌웨어 버전을 실행해야 합니다. 모든 FCoE 구성의 각 호스트는 다른 운영 체제로 구성할 수 있습니다.

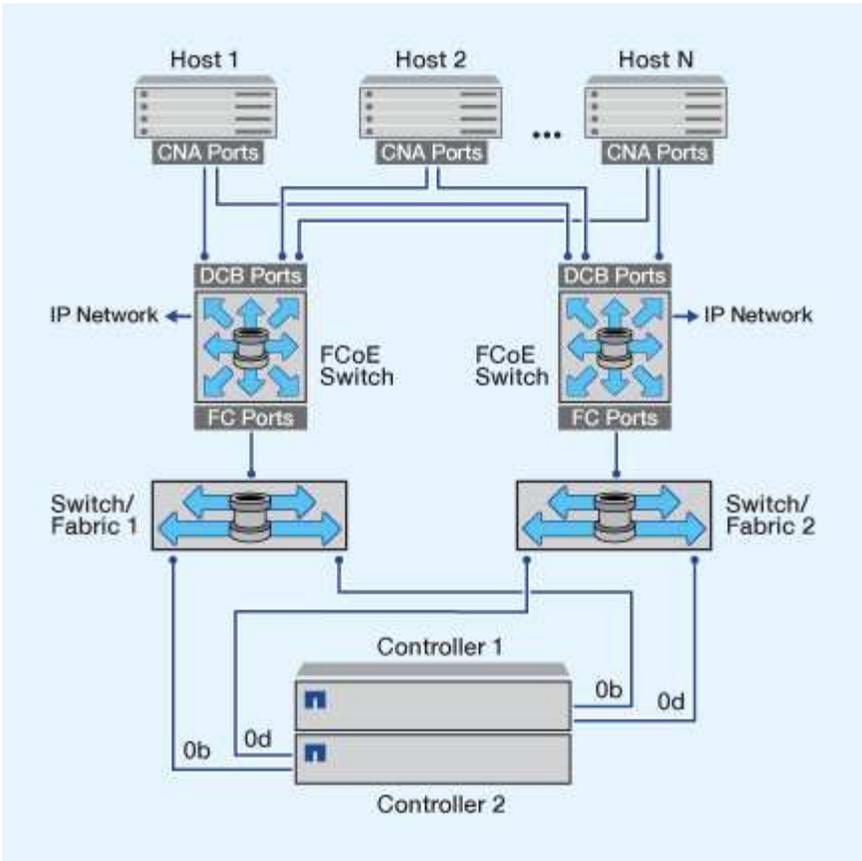
FCoE 구성에는 FCoE 기능을 명시적으로 지원하는 이더넷 스위치가 필요합니다. FCoE 구성은 FC 스위치와 동일한 상호 운용성 및 품질 보증 프로세스를 통해 검증되었습니다. 지원되는 구성은 상호 운용성 매트릭스에 나와 있습니다. 이러한 지원되는 구성에 포함된 매개 변수 중 일부는 스위치 모델, 단일 Fabric에 구축할 수 있는 스위치 수 및 지원되는 스위치 펌웨어 버전입니다.

그림에 나와 있는 FC 타겟 확장 어댑터 포트 번호의 예가 나와 있습니다. 실제 포트 번호는 FCoE 대상 확장 어댑터가 설치된 확장 슬롯에 따라 다를 수 있습니다.

FCoE 이니시에이터에서 **FC** 타겟으로

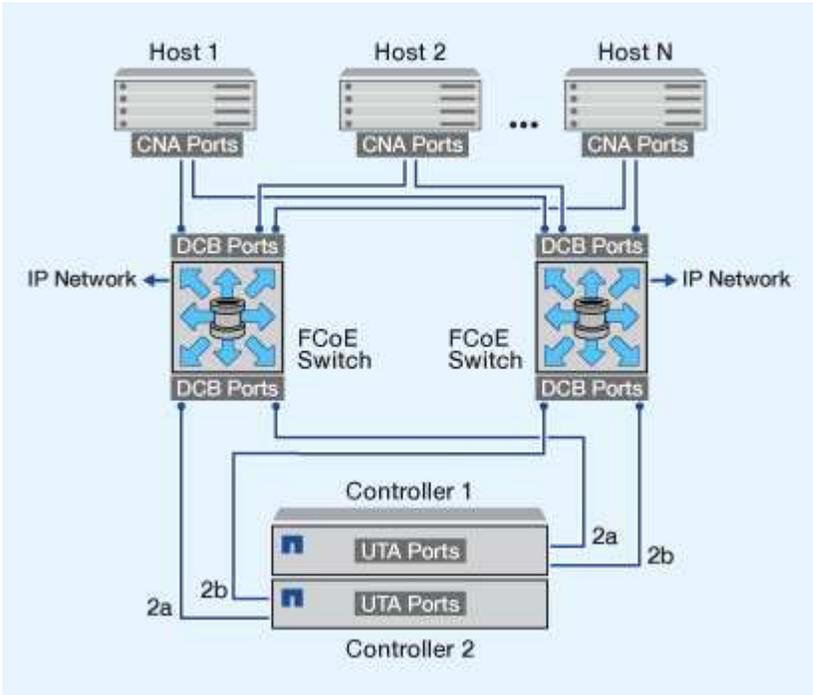
CNA(FCoE 이니시에이터)를 사용하면 FCoE 스위치를 FC 타겟 포트에 연결하여 HA 쌍의 두 컨트롤러에 호스트를 연결할 수 있습니다. FCoE 스위치에도 FC 포트가 있어야 합니다. 호스트 FCoE 이니시에이터는 항상 FCoE 스위치에 연결됩니다. FCoE 스위치는 FC 타겟에 직접 연결하거나 FC 스위치를 통해 FC 타겟에 연결할 수 있습니다.

다음 그림에서는 FCoE 스위치에 연결된 호스트 CNA와 HA 쌍에 연결하기 전에 FC 스위치에 연결하는 방법을 보여 줍니다.



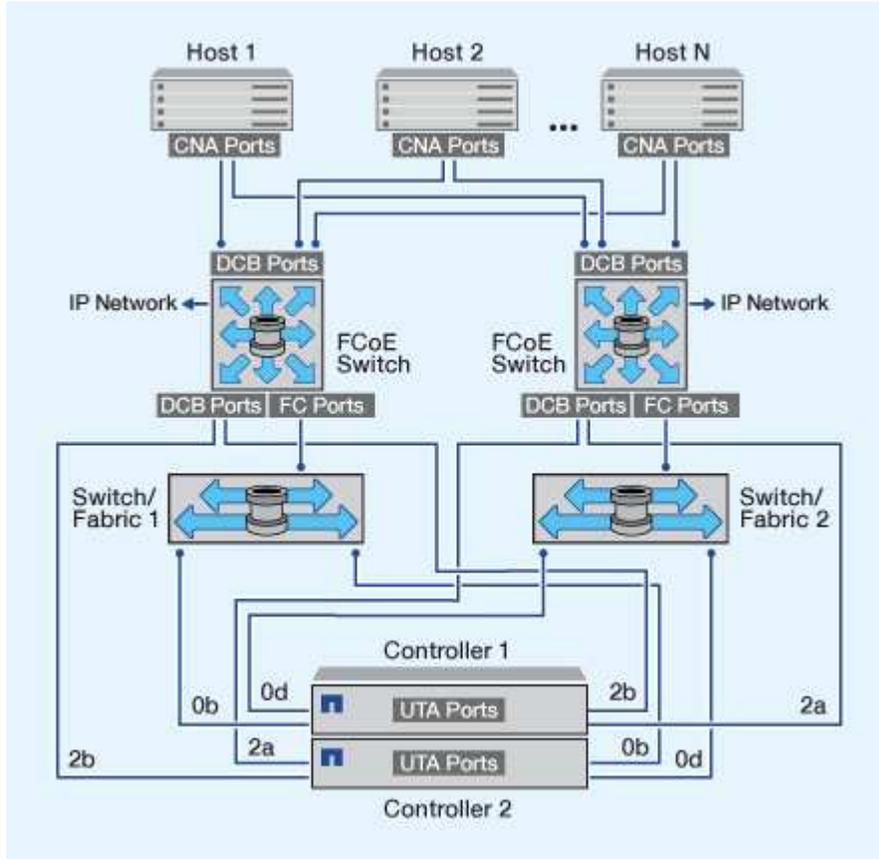
FCoE 이니시에이터에서 **FCoE** 타겟으로

CNA(호스트 FCoE 이니시에이터)를 사용하면 HA 쌍의 두 컨트롤러에 호스트를 FCoE 스위치를 통해 FCoE 타겟 포트(UTA 또는 UTA2)에 연결할 수 있습니다.



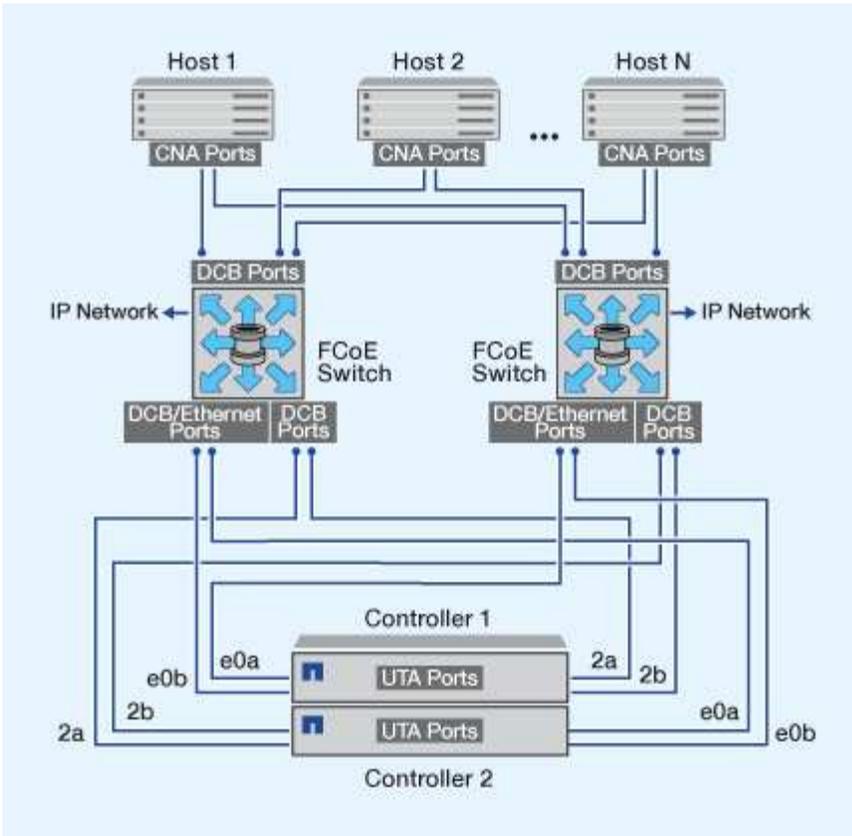
FCoE 이니시에이터에서 FCoE 및 FC 타겟으로

CNA(호스트 FCoE 이니시에이터)를 사용하면 HA 쌍의 두 컨트롤러에 호스트를 FCoE 스위치를 통해 FCoE 및 FC 타겟 포트(UTA 또는 UTA2)에 연결할 수 있습니다.



IP 스토리지 프로토콜과 혼합된 FCoE

CNA(호스트 FCoE 이니시에이터)를 사용하면 HA 쌍의 두 컨트롤러에 호스트를 FCoE 스위치를 통해 FCoE 타겟 포트(UTA 또는 UTA2)에 연결할 수 있습니다. FCoE 포트는 단일 스위치에 대한 기존 링크 집계를 사용할 수 없습니다. Cisco 스위치는 FCoE를 지원하는 특수한 유형의 Link Aggregation(가상 포트 채널)을 지원합니다. 가상 포트 채널은 두 스위치에 대한 개별 링크를 집계합니다. 다른 이더넷 트래픽에 가상 포트 채널을 사용할 수도 있습니다. NFS, SMB, iSCSI 및 기타 이더넷 트래픽을 포함하여 FCoE 이외의 트래픽에 사용되는 포트는 FCoE 스위치에서 일반 이더넷 포트를 사용할 수 있습니다.



ONTAP는 FCoE 이니시에이터 및 타겟 포트 조합을 지원합니다

FCoE와 기존 FC Initiator와 타겟의 특정 조합이 지원됩니다.

FCoE 이니시에이터

호스트 컴퓨터에서 FCoE 이니시에이터와 스토리지 컨트롤러의 기존 FC 타겟을 모두 사용할 수 있습니다. 호스트 FCoE 초기자는 FCoE DCB(데이터 센터 브리징) 스위치에 연결해야 합니다. 대상에 대한 직접 연결은 지원되지 않습니다.

다음 표에는 지원되는 조합이 나와 있습니다.

이니시에이터	타겟	지원 여부
FC	FC	예
FC	FCoE 를 참조하십시오	예
FCoE 를 참조하십시오	FC	예
FCoE 를 참조하십시오	FCoE 를 참조하십시오	예

FCoE 타겟

FC 포트가 추가 대상 어댑터인지 온보드 포트인지에 관계없이 스토리지 컨트롤러의 4Gb, 8Gb 또는 16Gb FC 포트와 FCoE 타겟 포트를 혼합할 수 있습니다. 동일한 스토리지 컨트롤러에 FCoE 및 FC 타겟 어댑터를 둘 다 사용할 수

있습니다.



온보드 및 확장 FC 포트의 결합에 대한 규칙이 계속 적용됩니다.

FC 및 FCoE 조닝

ONTAP 시스템을 통한 FC 및 FCoE 조닝에 대해 알아보십시오

FC, FC-NVMe 또는 FCoE 존은 패브릭 내 하나 이상의 포트를 논리적으로 그룹화한 것입니다. 장치가 서로 보고, 연결하고, 세션을 만들고, 통신할 수 있으려면 두 포트가 모두 같은 존의 구성원이어야 합니다.

조닝을 사용하면 공통 영역을 공유하는 엔드 포인트에 대한 액세스 및 연결을 제한하여 보안을 강화할 수 있습니다. 같은 존에 없는 포트는 서로 통신할 수 없습니다. 이렇게 하면 이니시에이터 HBA 간의 `_crosstalk_`가 감소되거나 제거됩니다. 연결 문제가 발생할 경우 조닝(zoning)을 통해 문제를 특정 포트 세트와 격리하여 해결 시간을 단축할 수 있습니다.

조닝으로 인해 특정 포트에 대해 사용 가능한 경로 수가 감소하고 호스트와 스토리지 시스템 사이의 경로 수가 감소합니다. 예를 들어, 일부 호스트 OS 다중 경로 솔루션에는 관리 가능한 경로 수에 제한이 있습니다. 조닝을 통해 호스트에 표시되는 경로 수를 줄일 수 있으므로 호스트에 대한 경로가 호스트 운영 체제에서 허용하는 최대 경로를 초과하지 않도록 할 수 있습니다.

World Wide Name 기반 조닝

WWN(World Wide Name)을 기반으로 하는 조닝은 영역 내에 포함할 구성원의 WWN을 지정합니다. 일부 스위치 공급업체에서는 WWNN(World Wide Node Name) 조닝을 사용할 수 있지만, ONTAP에서 조닝(Zoning)을 사용하면 WWPN(World Wide Port Name) 조닝을 사용해야 합니다.

특정 포트를 올바르게 정의하고 NPIV를 효과적으로 사용하려면 WWPN 조닝이 필요합니다. FC 스위치는 노드에 있는 물리적 포트의 WWPN이 아니라 대상 LIF(논리 인터페이스)의 WWPN을 사용하여 조닝되어야 합니다. 물리적 포트의 WWPN은 `"50"`으로 시작하고 LIF의 WWPN은 `"20"`으로 시작합니다.

WWPN 조닝을 사용하면 디바이스가 Fabric에 물리적으로 연결된 위치에 따라 액세스가 결정되지 않으므로 유연성이 제공됩니다. 영역을 재구성하지 않고도 한 포트에서 다른 포트에 케이블을 이동할 수 있습니다.

ONTAP 시스템에 권장되는 FC 및 FCoE 조닝 구성

호스트에 경로 다중화 솔루션이 설치되어 있지 않거나, 네 개 이상의 호스트가 SAN에 연결되어 있거나, 선택적 LUN 매핑이 클러스터의 노드에 구현되지 않은 경우 조닝 구성을 생성해야 합니다.

권장 FC 및 FCoE 조닝 구성에서 각 존에는 이니시에이터 포트와 하나 이상의 타겟 LIF가 포함됩니다. 이렇게 구성하면 각 호스트 이니시에이터가 모든 노드에 액세스할 수 있고 동일한 노드에 액세스하는 호스트가 서로의 포트를 볼 수 없습니다.

호스트 이니시에이터가 있는 존에 스토리지 가상 머신(SVM)의 모든 LIF를 추가합니다. 따라서 기존 영역을 편집하거나 새 영역을 생성하지 않고 볼륨 또는 LUN을 이동할 수 있습니다.

이중 패브릭 조닝 구성

이중 패브릭 조닝 구성은 단일 구성 요소 장애로 인한 데이터 손실을 방지하기 위해 권장됩니다. 이중 패브릭 구성에서

각 호스트 이니시에이터는 다양한 스위치를 사용하여 클러스터의 각 노드에 연결됩니다. 하나의 스위치를 사용할 수 없게 되더라도 나머지 스위치를 통해 데이터 액세스가 유지됩니다. 다중 경로를 관리하려면 호스트에 다중 경로 소프트웨어가 필요합니다.

다음 그림에서는 두 개의 이니시에이터가 있고 다중 경로 소프트웨어가 실행 중인 호스트를 보여 줍니다. 두 개의 구역이 있습니다. "선택적 LUN 매핑(SLM)" 모든 노드가 보고 노드로 간주되도록 구성됩니다.



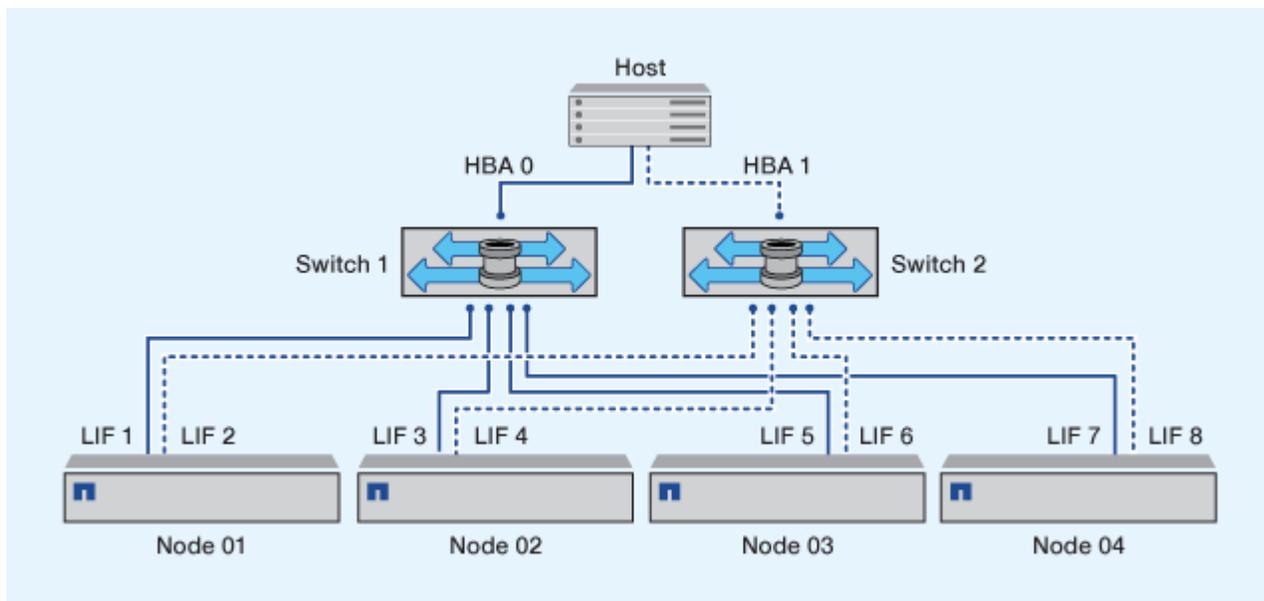
이 그림에 사용된 명명 규칙은 ONTAP 솔루션에 사용할 수 있는 명명 규칙 중 하나에 불과합니다.

- 존 1: HBA 0, LIF_1, LIF_3, LIF_5 및 LIF_7
- 구역 2: HBA 1, LIF_2, LIF_4, LIF_6 및 LIF_8

각 호스트 이니시에이터는 다른 스위치를 통해 조닝됩니다. 구역 1은 스위치 1을 통해 액세스합니다. 구역 2는 스위치 2를 통해 액세스합니다.

각 호스트는 모든 노드의 LIF에 액세스할 수 있습니다. 따라서 노드에 장애가 발생하더라도 호스트가 LUN에 액세스할 수 있습니다. SVM은 SLM 보고 노드 구성을 기반으로 클러스터의 모든 노드에서 모든 iSCSI 및 FC LIF에 액세스할 수 있습니다. SLM, 포트 세트 또는 FC 스위치 조닝을 사용하여 SVM에서 호스트로의 경로 수와 SVM에서 LUN으로의 경로 수를 줄일 수 있습니다.

구성에 더 많은 노드가 포함된 경우, 추가 노드의 LIF가 이 영역에 포함됩니다.



호스트 운영 체제 및 다중 경로 소프트웨어는 노드의 LUN에 액세스하는 데 사용되는 경로 수를 지원해야 합니다.

단일 패브릭 조닝

단일 패브릭 구성에서는 단일 스위치를 통해 각 호스트 이니시에이터를 각 스토리지 노드에 연결합니다. 단일 패브릭 조닝 구성은 단일 구성 요소 장애로 인한 데이터 손실에 대한 보호를 제공하지 않으므로 권장하지 않습니다. 단일 패브릭 조닝을 구성하는 경우 솔루션에서 복원력을 제공하려면 각 호스트에 두 개의 이니시에이터를 구성하여 다중 경로를 구현해야 합니다. 다중 경로를 관리하려면 호스트에 다중 경로 소프트웨어가 필요합니다.

각 호스트 이니시에이터에는 이니시에이터가 액세스할 수 있는 각 노드에서 LIF가 하나 이상 있어야 합니다. 조닝을

사용하면 호스트 이니시에이터에서 클러스터의 HA 노드 쌍에 대한 경로를 하나 이상 허용하여 LUN 접속 경로를 제공할 수 있어야 합니다. 즉, 호스트의 각 이니시에이터에는 자신의 존 구성 내 노드당 하나의 대상 LIF만 있을 수 있음을 의미합니다. 클러스터에서 동일한 노드 또는 여러 노드에 대한 다중 경로가 필요한 경우 각 노드의 존 구성에 노드당 여러 개의 LIF가 존재하게 됩니다. 따라서 노드에 장애가 발생하거나 LUN이 포함된 볼륨이 다른 노드로 이동되는 경우에도 호스트는 계속 LUN에 액세스할 수 있습니다. 또한 보고 노드를 적절하게 설정해야 합니다.

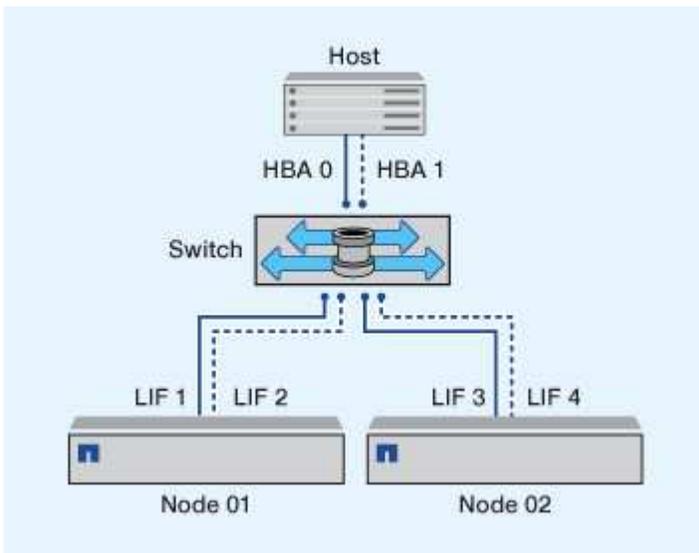
Cisco FC 및 FCoE 스위치를 사용할 때 단일 패브릭 영역에는 동일한 물리적 포트에 대해 둘 이상의 대상 LIF가 포함될 수 없습니다. 같은 포트에 여러 LIF가 있는 경우 LIF 포트가 연결 손실로부터 복구되지 못할 수 있습니다.

다음 그림에서는 두 개의 이니시에이터가 있고 다중 경로 소프트웨어가 실행 중인 호스트를 보여 줍니다. 두 개의 영역이 있습니다.

i 이 그림에 사용된 명명 규칙은 ONTAP 솔루션에 사용할 수 있는 명명 규칙 중 하나에 불과합니다.

- 구역 1: HBA 0, LIF_1 및 LIF_3
- 구역 2: HBA 1, LIF_2 및 LIF_4

구성에 더 많은 노드가 포함된 경우, 추가 노드의 LIF가 이 존에 포함됩니다



이 예제에서는 각 영역에 4개의 LIF를 모두 가질 수도 있습니다. 이 경우 영역은 다음과 같습니다.

- 존 1: HBA 0, LIF_1, LIF_2, LIF_3 및 LIF_4
- 존 2: HBA 1, LIF_1, LIF_2, LIF_3 및 LIF_4

i 호스트 운영 체제 및 다중 경로 소프트웨어는 노드의 LUN에 액세스하는 데 사용되는 지원되는 경로 수를 지원해야 합니다. 노드의 LUN에 액세스하는 데 사용되는 경로 수를 확인하려면 SAN 구성 제한 섹션을 참조하십시오.

Cisco FC 및 FCoE 스위치에 대한 조닝 제한 사항

Cisco FC 및 FCoE 스위치를 사용할 경우 영역의 물리적 포트 및 논리 인터페이스(LIF) 사용에 특정 제한이 적용됩니다.

물리적 포트

- FC-NVMe 및 FC는 동일한 32Gb 물리적 포트를 공유할 수 있습니다

- FC-NVMe 및 FCoE는 동일한 물리적 포트를 공유할 수 없습니다
- FC와 FCoE는 같은 물리적 포트를 공유할 수 있지만 프로토콜 LIF는 별도의 영역에 있어야 합니다.

논리 인터페이스(LIF)

- 존에는 클러스터의 모든 타겟 포트의 LIF가 포함될 수 있습니다.
호스트에 허용되는 최대 경로 수를 초과하지 않도록 SLM 구성을 확인하십시오.
- 특정 포트의 각 LIF는 해당 포트의 다른 LIF와 다른 영역에 있어야 합니다
- 다른 물리적 포트에 있는 LIF는 동일한 존에 있을 수 있습니다.

ONTAP 시스템 및 비 NetApp 시스템에 연결된 SAN 호스트의 요구 사항

공유 SAN 구성은 ONTAP 스토리지 시스템과 다른 공급업체의 스토리지 시스템에 모두 연결되는 호스트로 정의됩니다. 여러 요구사항을 충족할 경우, 단일 호스트에서 ONTAP 스토리지 시스템 및 다른 공급업체의 스토리지 시스템에 액세스할 수 있습니다.

모든 호스트 운영 체제에서 별도의 어댑터를 사용하여 각 공급업체의 스토리지 시스템에 연결하는 것이 좋습니다. 별도의 어댑터를 사용하면 드라이버와 설정이 충돌할 가능성이 줄어듭니다. ONTAP 스토리지 시스템에 연결하려면 어댑터 모델, BIOS, 펌웨어 및 드라이버가 NetApp 상호 운용성 매트릭스 툴에 지원되는 것으로 표시되어야 합니다.

호스트에 대해 필수 또는 권장 시간 초과 값과 기타 스토리지 매개 변수를 설정해야 합니다. 항상 NetApp 소프트웨어를 설치하거나 NetApp 설정을 마지막으로 적용해야 합니다.

- AIX의 경우 구성의 상호 운용성 매트릭스 툴에 나열된 AIX Host Utilities 버전의 값을 적용해야 합니다.
- ESX의 경우 VMware vSphere용 Virtual Storage Console을 사용하여 호스트 설정을 적용해야 합니다.
- HP-UX의 경우 HP-UX 기본 스토리지 설정을 적용해야 합니다.
- Linux의 경우 구성의 상호 운용성 매트릭스 툴에 나열된 Linux Host Utilities 버전의 값을 적용해야 합니다.
- Solaris의 경우, 구성의 상호 운용성 매트릭스 툴에 나열된 Solaris Host Utilities 버전의 값을 적용해야 합니다.
- Windows의 경우 구성의 상호 운용성 매트릭스 툴에 나열된 Windows Host Utilities 버전을 설치해야 합니다.

관련 정보

["NetApp 상호 운용성 매트릭스 툴"](#)

MetroCluster 환경의 SAN 구성입니다

ONTAP MetroCluster 환경에서 지원되는 SAN 구성

MetroCluster 환경에서 SAN 구성을 사용할 때는 몇 가지 고려 사항을 염두에 두어야 합니다.

- MetroCluster 구성은 프론트엔드 FC 패브릭 ""라우팅된" vSAN 구성을 지원하지 않습니다.
- ONTAP 9.15.1부터 NVMe/TCP에서 4노드 MetroCluster IP 구성이 지원됩니다.
- ONTAP 9.12.1부터 4노드 MetroCluster IP 구성이 NVMe/FC에서 지원됩니다. ONTAP 9.12.1 이전의 프론트엔드 NVMe 네트워크에서는 MetroCluster 구성이 지원되지 않습니다.
- iSCSI, FC, FCoE 등의 다른 SAN 프로토콜은 MetroCluster 구성에서 지원됩니다.

- SAN 클라이언트 구성을 사용할 때는 에 제공된 노트에 MetroCluster 구성에 대한 특별한 고려 사항이 포함되어 있는지 확인해야 합니다 "[NetApp 상호 운용성 매트릭스 툴](#)" (IMT).
- 운영 체제 및 애플리케이션은 MetroCluster의 자동 계획되지 않은 전환 및 Tiebreaker 또는 중재자 시작 전환을 지원하기 위해 120초의 I/O 복원력을 제공해야 합니다.
- MetroCluster 구성은 프런트 엔드 FC 패브릭의 양쪽에서 동일한 WWNN 및 WWPN을 사용합니다.

관련 정보

- "[MetroCluster 데이터 보호 및 재해 복구 이해](#)"
- "[NetApp 지식 기반: MetroCluster 구성에서 AIX 호스트 지원에 대한 고려 사항은 무엇입니까?](#)"
- "[NetApp 지식 기반: MetroCluster 구성에서 Solaris 호스트 지원 고려 사항](#)"

ONTAP MetroCluster 스위치오버 및 스위치백 중에는 포트 중첩을 방지합니다

SAN 환경에서는 이전 포트가 오프라인이 되고 새 포트가 온라인 상태가 될 때 겹치지 않도록 프런트엔드 스위치를 구성할 수 있습니다.

스위치오버 중에 정상적인 사이트의 FC 포트가 패브릭에 로그인한 후 패브릭에서 재해 사이트의 FC 포트가 오프라인이며 이름 및 디렉토리 서비스에서 이 포트를 제거했습니다.

재해의 FC 포트가 아직 제거되지 않은 경우 중복 WWPN으로 인해 정상적인 사이트에서 FC 포트의 패브릭 로그인 시도가 거부될 수 있습니다. FC 스위치의 이러한 동작은 기존 디바이스가 아닌 이전 디바이스의 로그인을 사용하도록 변경할 수 있습니다. 이 동작이 다른 패브릭 디바이스에 미치는 영향을 확인해야 합니다. 자세한 내용은 스위치 공급업체에 문의하십시오.

스위치 유형에 따라 올바른 절차를 선택하십시오.

예 9. 단계

Cisco 스위치

1. 스위치에 연결하고 로그인합니다.
2. 구성 모드 시작:

```
switch# config t
switch(config)#
```

3. 이름 서버 데이터베이스의 첫 번째 장치 항목을 새 장치로 덮어씁니다.

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. NX-OS 8.x를 실행 중인 스위치에서 flogi 일시 중지 시간 초과가 0으로 설정되었는지 확인합니다.
 - a. 일시 중지 시간 표시:

```
switch(config)# show flogi interval info \\\ i quiesce
```

```
Stats:  fs flogi quiesce timerval:  0
```

- b. 이전 단계의 출력이 시간 간격이 0임을 나타내지 않으면 0으로 설정합니다.

```
'Switch (config)#flogi scale enable'
```

```
'스위치(config)$flogi 시간 제한 0'
```

Brocade 스위치

1. 스위치에 연결하고 로그인합니다.
2. 'witchDisable' 명령어를 입력한다.
3. configure 명령을 입력하고 프롬프트에 y를 누릅니다.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. 설정 1 선택:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 나머지 프롬프트에 응답하거나 * Ctrl+D * 를 누릅니다.

6. 'witchEnable' 명령어를 입력한다.

관련 정보

["테스트 또는 유지 관리를 위한 전환 수행"](#)

SAN 호스트 다중 경로에 대한 ONTAP 지원

ONTAP는 FC와 iSCSI 호스트의 다중 경로에 대해 ALUA(Asymmetric Logical Unit Access) 소프트웨어를 사용합니다.

ONTAP 9.5부터 ANA(Asynchronous Namespace Access)를 사용하는 NVMe 호스트에 대해 다중 경로 HA(고가용성) 쌍 페일오버/반환이 지원됩니다. ONTAP 9.4에서 NVMe는 호스트에서 타겟으로의 경로를 하나만 지원하므로 애플리케이션 호스트는 HA 파트너에 대한 경로 페일오버를 관리해야 합니다.

SAN 호스트가 둘 이상의 경로를 통해 LUN 또는 NVMe 네임스페이스에 액세스할 수 있는 경우 다중 경로 소프트웨어가 필요합니다. LUN 또는 NVMe 네임스페이스에 대한 모든 경로에 대해 운영 체제에 단일 디스크를 제공합니다. 이 기능이 없으면 운영 체제는 각 경로를 별도의 디스크로 처리하여 데이터 손상이 발생할 수 있습니다.

다음 중 하나가 있는 경우 솔루션은 여러 경로를 포함하는 것으로 간주됩니다.

- 호스트의 단일 이니시에이터 포트에서 SVM의 여러 SAN LIF에 연결됩니다
- 여러 이니시에이터 포트를 SVM의 단일 SAN LIF에 연결합니다
- 여러 이니시에이터 포트를 SVM의 여러 SAN LIF에 연결합니다

MPIO(다중 경로 I/O) 소프트웨어라고도 하는 다중 경로 소프트웨어가 HA 구성에 권장됩니다. 선택적 LUN 맵 이외에도 LUN에 액세스하는 데 사용되는 경로를 제한하기 위해 FC 스위치 조닝 또는 포트 세트를 사용하는 것이 좋습니다.

ALUA 또는 ANA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 ["NetApp 상호 운용성 매트릭스 툴"](#) 및 ["ONTAP SAN 호스트 구성"](#) 호스트 운영 체제를 위한 것입니다.

클러스터의 호스트에서 노드까지 권장되는 경로 수입입니다

호스트에서 클러스터의 각 노드로 이어지는 경로가 8개를 초과할 수 없습니다. 또한 호스트 OS 및 호스트에서 사용되는 다중 경로에 대해 지원할 수 있는 총 경로 수를 초과하지 않아야 합니다.

클러스터의 SVM(스토리지 가상 머신)에서 사용하는 동안 각 보고 노드에 연결되는 LUN당 최소 2개의 경로를 보유해야 ["선택적 LUN 맵\(SLM\)"](#)합니다. 따라서 단일 장애 지점이 발생하지 않으며 시스템에서 구성 요소 장애를 극복할 수 있습니다.

클러스터에 4개 이상의 노드가 있거나 모든 노드에서 SVM이 사용하는 4개 이상의 타겟 포트가 있는 경우 다음 방법을 사용하여 노드의 LUN에 액세스하는 데 사용할 수 있는 경로 수를 제한하여 권장되는 최대 8개 경로를 초과하지 않도록 할 수 있습니다.

- SLM

SLM은 호스트에서 LUN으로의 경로 수를 LUN과 소유 노드의 HA 파트너가 있는 노드의 경로로만 줄여줍니다. SLM은 기본적으로 활성화되어 있습니다.

- "iSCSI에 대한 Portset입니다"
- 호스트에서 FC igroup 매핑
- FC 스위치 조닝

구성 제한

ONTAP 클러스터당 지원되는 최대 노드 및 **SAN** 호스트를 결정합니다

클러스터당 지원되는 노드 수는 ONTAP 버전, 컨트롤러 모델 및 클러스터 노드의 프로토콜에 따라 다릅니다. 클러스터에 연결할 수 있는 최대 SAN 호스트 수도 사용자의 특정 구성에 따라 다릅니다.

클러스터당 지원되는 최대 노드를 확인합니다

클러스터의 노드가 FC, FC-NVMe, FCoE 또는 iSCSI에 대해 구성된 경우 해당 클러스터는 SAN 노드 제한으로 제한됩니다. 클러스터의 컨트롤러에 기반한 노드 제한은 `_Hardware Universe_`에 나열되어 있습니다.

단계

1. 로 이동합니다 "[NetApp Hardware Universe를 참조하십시오](#)".
2. 왼쪽 위에서 * 홈 * 옆에 있는 * 플랫폼 * 을 선택한 다음 플랫폼 유형을 선택합니다.
3. 사용 중인 ONTAP 버전을 선택합니다.

플랫폼을 선택할 수 있는 새 열이 표시됩니다.

4. 솔루션에 사용되는 플랫폼을 선택하십시오.
5. Choose your Specifications(사양 선택) * 에서 * Select All(모두 선택) * 을 선택 취소합니다.
6. Max Nodes per Cluster(NAS/SAN) * 를 선택합니다.
7. 결과 표시 * 를 클릭합니다.

결과

선택한 플랫폼에 대한 클러스터당 최대 노드가 표시됩니다.

클러스터에서 더 많은 **FC** 호스트를 지원할 수 있는지 확인합니다

FC 및 FC-NVMe 구성의 경우 시스템에서 이니시에이터-타겟 nexuse(ITN) 수를 사용하여 클러스터에 호스트를 더 추가할 수 있는지 확인해야 합니다.

ITN은 호스트의 이니시에이터에서 스토리지 시스템의 타겟으로 연결되는 하나의 경로를 나타냅니다. FC 및 FC-NVMe 구성의 노드당 최대 ITN 수는 2,048개입니다. 최대 ITN 수 미만이면 계속해서 클러스터에 호스트를 추가할 수 있습니다.

클러스터에서 사용되는 ITN 수를 확인하려면 클러스터의 각 노드에 대해 다음 단계를 수행하십시오.

단계

1. 특정 노드에서 모든 LIF를 식별합니다.
2. 노드의 모든 LIF에 대해 다음 명령을 실행합니다.

```
fcp initiator show -fields wwpn, lif
```

명령 출력의 하단에 표시되는 항목 수는 해당 LIF의 ITN 수를 나타냅니다.

3. 각 LIF에 대해 표시되는 ITN 수를 기록합니다.
4. 클러스터의 모든 노드에 있는 각 LIF의 ITN 수를 추가합니다.

이 합계는 클러스터의 ITN 수를 나타냅니다.

클러스터에서 더 많은 **iSCSI** 호스트를 지원할 수 있는지 확인합니다

노드에 직접 연결할 수 있거나 하나 이상의 스위치를 통해 연결할 수 있는 호스트의 수는 사용 가능한 이더넷 포트의 수에 따라 달라집니다. 사용 가능한 이더넷 포트 수는 컨트롤러의 모델 및 컨트롤러에 설치된 어댑터의 수와 유형에 따라 결정됩니다. 컨트롤러 및 어댑터에 지원되는 이더넷 포트 수는 `_Hardware Universe_`에서 확인할 수 있습니다.

모든 다중 노드 클러스터 구성의 경우, 클러스터에 호스트를 더 추가할 수 있는지 여부를 알 수 있도록 노드당 iSCSI 세션 수를 결정해야 합니다. 클러스터가 노드당 최대 iSCSI 세션 수보다 많은 경우 계속해서 클러스터에 호스트를 추가할 수 있습니다. 노드당 최대 iSCSI 세션 수는 클러스터의 컨트롤러 유형에 따라 달라집니다.

단계

1. 노드에서 모든 타겟 포털 그룹을 식별합니다.
2. 노드의 모든 타겟 포털 그룹에 대한 iSCSI 세션 수를 확인합니다.

```
iscsi session show -tpgroup _tpgroup_
```

명령 출력 하단에 표시되는 항목 수는 해당 타겟 포털 그룹에 대한 iSCSI 세션 수를 나타냅니다.

3. 각 타겟 포털 그룹에 대해 표시되는 iSCSI 세션 수를 기록합니다.
4. 노드의 각 타겟 포털 그룹에 대한 iSCSI 세션 수를 추가합니다.

총계 는 노드의 iSCSI 세션 수를 나타냅니다.

All-Flash SAN 어레이 구성 제한 및 지원

ASA(All-Flash SAN 어레이)의 구성 제한 및 지원은 ONTAP 버전에 따라 다릅니다.

지원되는 구성 제한에 대한 최신 정보는 에서 확인할 수 있습니다 "[NetApp Hardware Universe를 참조하십시오](#)".



이러한 제한은 ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 참조하세요. "[ASA R2 시스템 스토리지 제한](#)"

SAN 프로토콜 및 클러스터당 지원되는 노드 수

지원되는 SAN 프로토콜과 클러스터당 최대 노드 수는 MetroCluster가 아닌 구성인지 MetroCluster 구성이 있는지에 따라 달라집니다.

MetroCluster 구성이 아닌 경우

다음 표는 MetroCluster가 아닌 구성에서 SAN 프로토콜에 대한 ASA 지원 과 클러스터당 지원되는 노드 수를 보여줍니다.

ONTAP로 시작하는 중...	프로토콜 지원	클러스터당 최대 노드 수
9.11.1	<ul style="list-style-type: none"> • NVMe/TCP • NVMe/FC 	12
9.10.1	<ul style="list-style-type: none"> • NVMe/TCP 	2
9.9.1	<ul style="list-style-type: none"> • NVMe/FC 	2
	<ul style="list-style-type: none"> • FC • iSCSI 	12
9.7	<ul style="list-style-type: none"> • FC • iSCSI 	2

MetroCluster IP 구성

다음 표는 MetroCluster IP 구성에서 SAN 프로토콜에 대한 ASA 지원과 클러스터당 지원되는 노드 수를 보여줍니다.

ONTAP로 시작하는 중...	프로토콜 지원	클러스터당 최대 노드 수
9.15.1	<ul style="list-style-type: none"> • NVMe/TCP 	4노드 MetroCluster IP 구성에서 클러스터당 2개 노드
9.12.1	<ul style="list-style-type: none"> • NVMe/FC 	4노드 MetroCluster IP 구성에서 클러스터당 2개 노드
9.9.1	<ul style="list-style-type: none"> • FC • iSCSI 	8노드 MetroCluster IP 구성으로 클러스터당 4개 노드
9.7	<ul style="list-style-type: none"> • FC • iSCSI 	4노드 MetroCluster IP 구성에서 클러스터당 2개 노드

영구 포트 지원

ONTAP 9.8부터는 FC 프로토콜을 사용하도록 구성된 ASA(All-Flash SAN Array)에서 영구 포트가 기본적으로 활성화됩니다. 영구 포트는 FC에만 사용할 수 있으며 WWPN(World Wide Port Name)으로 식별되는 영역 구성원이 필요합니다.

영구 포트는고가용성(HA) 파트너의 해당 물리적 포트에 새도 LIF를 생성하여 테이크오버의 영향을 줄입니다. 노드가 되면 파트너 노드의 새도 LIF는 WWPNe를 포함하여 원래 LIF의 ID를 가정합니다. 가져온 오버 노드의 경로 상태가

장애 발생으로 변경되기 전에 새도우 LIF는 호스트 MPIO 스택에 대한 Active/Optimized 경로로 표시되고 I/O가 이동됩니다. 따라서 스토리지 페일오버 작업 중에도 호스트가 항상 동일한 수의 경로를 타겟으로 인식하기 때문에 I/O 중단이 줄어듭니다.

영구 포트의 경우 HA 쌍 내에서 다음과 같은 FCP 포트 특성이 동일해야 합니다.

- FCP 포트의 개수
- FCP 포트 이름
- FCP 포트의 속도입니다
- FCP LIF WWPN 기반 조닝

HA Pair 내에서 동일 특성이 아닌 경우, 다음과 같은 EMS 메시지가 발생한다.

"EMS: scsiblade.lif.persistent.ports.fcp.init.error"

영구 포트에 대한 자세한 내용은 을 참조하십시오"[NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례](#)".

ONTAP 시스템에서 사용되는 FC 스위치의 구성 제한

파이버 채널 스위치에는 포트, 포트 그룹, 블레이드 및 스위치별로 지원되는 로그인 수를 포함한 최대 구성 제한이 있습니다. 지원되는 제한은 스위치 벤더에서 문서로 제공합니다.

각 FC 논리 인터페이스(LIF)는 FC 스위치 포트에 로그인합니다. 노드에서 단일 타겟의 총 로그인 수는 LIF 수에 기본 물리적 포트의 로그인 수 1을 더한 값과 같습니다. 로그인 또는 기타 구성 값에 대한 스위치 공급업체의 구성 제한을 초과하지 마십시오. 또한 NPIV가 활성화된 가상화 환경에서 호스트 측에서 사용되는 초기자에 대해서도 마찬가지입니다. 솔루션에서 사용 중인 타겟 또는 이니시에이터에 대한 스위치 공급업체의 로그인 구성 제한을 초과하지 마십시오.

Brocade 스위치 제한

Brocade 스위치에 대한 구성 제한은 _ Brocade 확장성 지침 _ 에서 확인할 수 있습니다.

Cisco Systems 스위치 제한

에서 Cisco 스위치에 대한 구성 제한을 찾을 수 있습니다 "[Cisco 구성 제한](#)" 사용 중인 Cisco 스위치 소프트웨어 버전에 대한 안내서입니다.

ONTAP에서 지원되는 최대 FC 및 FCoE 홉 수

홉 수는 이니시에이터(호스트)와 타겟(스토리지 시스템) 사이의 경로에 있는 스위치의 수로 정의됩니다. 호스트와 스토리지 시스템 간에 지원되는 최대 FC 홉 수는 스위치 공급업체에 따라 다릅니다.

Cisco Systems의 설명서에서는 이 값을 SAN fabric_의 _diameter로 참조합니다.

FCoE의 경우 FC 스위치에 FCoE 스위치를 연결할 수 있습니다. 엔드 투 엔드 FCoE 연결의 경우 FCoE 스위치는 이더넷 ISL(Inter-Switch Link)을 지원하는 펌웨어 버전을 실행해야 합니다.

공급업체를 전환합니다	지원되는 홉 수입니다
모든 정보를 제공합니다	<ul style="list-style-type: none"> • FC의 경우 7 • FCoE의 경우 5입니다
Cisco의	<ul style="list-style-type: none"> • FC의 경우 7 • 최대 3개의 스위치가 FCoE 스위치일 수 있습니다.

ONTAP FC 호스트의 큐 길이를 계산합니다

노드별 및 FC 포트 팬인 당 ITNs의 최대 값을 얻으려면 호스트에서 FC 큐 길이를 조정해야 할 수 있습니다. FC 포트에 연결할 수 있는 HBA의 수와 LUN의 최대 수는 FC 타겟 포트에서 사용 가능한 큐 길이로 제한됩니다.

이 작업에 대해

큐 길이는 스토리지 컨트롤러에서 한 번에 대기열에 넣을 수 있는 입출력 요청(SCSI 명령)의 수입입니다. 호스트의 이니시에이터 HBA에서 스토리지 컨트롤러의 타겟 어댑터로 연결되는 각 입출력 요청은 대기열 항목을 사용합니다. 일반적으로 큐 길이가 클수록 성능이 향상됩니다. 그러나 스토리지 컨트롤러의 최대 큐 수준에 도달하면 해당 스토리지 컨트롤러는 QFULL 응답을 반환하여 들어오는 명령을 거부합니다. 많은 수의 호스트가 스토리지 컨트롤러에 액세스하고 있는 경우, 시스템 성능이 크게 저하되어 일부 시스템에서 오류가 발생할 수 있는 QFULL 조건을 피할 수 있도록 신중하게 계획해야 합니다.

여러 이니시에이터(호스트)가 있는 구성에서는 모든 호스트에 유사한 대기열 길이가 있어야 합니다. 동일한 타겟 포트를 통해 스토리지 컨트롤러에 접속된 호스트 간의 큐 크기가 서로 다르기 때문에 큐 크기가 작은 호스트는 큐 크기가 큰 호스트에 의해 리소스에 액세스할 수 없습니다.

다음과 같은 일반적인 권장 사항은 ""조정"" 대기열 길이에 대해 만들 수 있습니다.

- 중소 규모 시스템의 경우 HBA 대기열 길이가 32인 HBA를 사용합니다.
- 대규모 시스템의 경우 HBA 대기열 길이가 128인 HBA를 사용합니다.
- 예외 케이스 또는 성능 테스트의 경우 큐 처리 문제가 발생하지 않도록 256개의 큐 길이를 사용하십시오.
- 모든 호스트는 모든 호스트에 동일한 액세스를 제공하기 위해 유사한 값으로 설정된 대기열 길이를 가져야 합니다.
- 성능 패널이나 오류를 방지하려면 스토리지 컨트롤러 타겟 FC 포트 큐 길이를 초과하지 않아야 합니다.

단계

1. 하나의 FC 타겟 포트에 연결되는 모든 호스트의 총 FC 이니시에이터 수를 계산합니다.
2. 128을 곱합니다.
 - 결과가 2,048보다 작으면 모든 이니시에이터에 대한 대기열 길이를 128로 설정합니다. 스토리지 컨트롤러의 각 타겟 포트 2개에 하나의 이니시에이터가 접속된 호스트 15개가 있습니다. $15 \times 128 = 1,920$. 1,920은 총 대기열 길이 제한인 2,048보다 작기 때문에 모든 이니시에이터에 대한 대기열 길이를 128로 설정할 수 있습니다.
 - 결과가 2,048보다 크면 3단계로 이동합니다. 스토리지 컨트롤러의 각 타겟 포트 2개에 하나의 이니시에이터가 연결된 30개의 호스트가 있습니다. $30 \times 128 = 3,840$. 3,840이 총 대기열 길이 제한인 2,048보다 크기 때문에 3단계에서 해결 방법 중 하나를 선택해야 합니다.
3. 다음 옵션 중 하나를 선택하여 스토리지 컨트롤러에 호스트를 더 추가합니다.

◦ 옵션 1:

- i. FC 타겟 포트를 추가합니다.
- ii. FC 이니시에이터를 재배포합니다.
- iii. 1단계와 2단계를 반복합니다. + 원하는 큐 길이 3,840이 포트당 사용 가능한 큐 길이를 초과합니다. 이를 해결하기 위해 각 컨트롤러에 2포트 FC 타겟 어댑터를 추가한 다음, 30개 호스트 중 15개가 1개의 포트 세트에 연결되고 나머지 15개 호스트는 2번째 포트 세트에 연결되도록 FC 스위치를 재존할 수 있습니다. 그런 다음 포트당 큐 길이가 $15 \times 128 = 1,920$ 으로 줄어듭니다.

◦ 옵션 2:

- i. 예상되는 I/O 요구 사항에 따라 각 호스트를 "대형" 또는 "소형"으로 지정합니다.
- ii. 큰 이니시에이터 수에 128을 곱합니다.
- iii. 작은 이니시에이터 수에 32를 곱합니다.
- iv. 두 결과를 함께 추가합니다.
- v. 결과가 2,048보다 작으면 큰 호스트의 대기열 길이를 128로, 작은 호스트의 대기열 길이를 32로 설정합니다.
- vi. 결과가 포트당 2,048보다 크면 총 대기열 길이가 2,048보다 작거나 같을 때까지 이니시에이터당 대기열 길이를 줄입니다.

초당 특정 I/O 처리량을 달성하는 데 필요한 큐 길이를 예측하려면 다음 수식을 사용합니다.



필요한 대기열 길이 = (초당 I/O 수) × (응답 시간)

예를 들어, 응답 시간이 3밀리초인 초당 40,000회의 I/O가 필요한 경우 필요한 큐 길이는 $40,000 \times (.003) = 120$ 입니다.

대기열 길이를 기본 권장 사항 32로 제한하려면 대상 포트에 연결할 수 있는 최대 호스트 수는 64개입니다. 그러나 큐 크기가 128로 결정되면 최대 16개의 호스트를 하나의 타겟 포트에 연결할 수 있습니다. 대기열 길이가 클수록 단일 타겟 포트에서 지원할 수 있는 호스트 수가 줄어듭니다. 대기열 길이를 손상시키지 않는 요구 사항이 있는 경우 더 많은 대상 포트를 얻을 수 있습니다.

원하는 큐 길이 3,840이 포트당 사용 가능한 큐 길이를 초과합니다. 스토리지 I/O 요구 사항이 높은 10개의 "대용량" 호스트와 I/O 요구 사항이 낮은 20개의 "소규모" 호스트가 있습니다. 큰 호스트의 이니시에이터 큐 길이를 128로, 작은 호스트의 이니시에이터 큐 길이를 32로 설정합니다.

총 큐 길이는 $(10 \times 128) + (20 \times 32) = 1,920$ 입니다.

사용 가능한 대기열 길이를 각 이니시에이터에 균등하게 분산시킬 수 있습니다.

결과적인 이니시에이터당 대기열 길이는 $2,048 \div 30 = 68$ 입니다.

ONTAP SAN 호스트의 큐 길이를 수정합니다

노드별 ITN 및 FC 포트 팬인에 대한 최대 값을 달성하려면 호스트의 대기열 길이를 변경해야 할 수 있습니다. 환경에 맞게 가능합니다. **"최적의 대기열 길이를 계산합니다"**

AIX 호스트

"chdev" 명령을 사용하여 AIX 호스트의 대기열 길이를 변경할 수 있습니다. "chdev" 명령을 사용하여 변경한 사항은 재부팅 후에도 유지됩니다.

예:

- hdisk7 디바이스의 대기열 길이를 변경하려면 다음 명령을 사용합니다.

```
chdev -l hdisk7 -a queue_depth=32
```

- fcs0 HBA의 대기열 길이를 변경하려면 다음 명령을 사용하십시오.

```
"chdev -l fcs0 -a num_cmd_elems=128"
```

num_cmd_elems의 기본값은 200입니다. 최대값은 2,048입니다.



num_cmd_elems를 변경하려면 HBA를 오프라인 상태로 전환한 다음 rmdev-l fcs0-R 및 makdev-l fcs0-P 명령을 사용하여 다시 온라인 상태로 전환해야 할 수도 있습니다.

HP-UX 호스트

커널 매개 변수 'scsi_max_qdepth'를 사용하여 HP-UX 호스트에서 LUN 또는 디바이스 대기열 길이를 변경할 수 있습니다. 커널 매개 변수 max_fcp_reqs를 사용하여 HBA 대기열 길이를 변경할 수 있습니다.

- 'scsi_max_qdepth'의 기본값은 8입니다. 최대값은 255입니다.

'kmtune' 명령의 '-u' 옵션을 사용하면 실행 중인 시스템에서 'scsi_max_qdepth'를 동적으로 변경할 수 있습니다. 이 변경 사항은 시스템의 모든 장치에 적용됩니다. 예를 들어, 다음 명령을 사용하여 LUN 대기열 길이를 64로 늘릴 수 있습니다.

```
"kmtune -u -s scsi_max_qdepth=64"
```

'csictl' 명령어를 이용하여 개별 장치 파일의 대기열 길이를 변경할 수 있다. 'csictl' 명령을 사용한 변경 사항은 시스템 재부팅 시에도 지속되지 않습니다. 특정 장치 파일의 대기열 길이를 보고 변경하려면 다음 명령을 실행합니다.

```
'csictl -a /dev/rdisk/c2t2d0'
```

```
'csictl -m queue_depth=16/dev/rdisk/c2t2d0'
```

- max_fcp_reqs의 기본값은 512입니다. 최대값은 1024입니다.

'max_fcp_reqs'의 변경 사항을 적용하려면 커널을 재구축하고 시스템을 재부팅해야 합니다. 예를 들어 HBA 대기열 길이를 256으로 변경하려면 다음 명령을 사용합니다.

```
"kmtune -u -s max_fcp_reqs=256"
```

Solaris 호스트

Solaris 호스트에 대한 LUN 및 HBA 대기열 길이를 설정할 수 있습니다.

- LUN 큐 깊이의 경우: 호스트에서 사용 중인 LUN 수에 LUN당 스토틀(LUN-대기열-깊이)을 곱한 값은 호스트의 tgt-queue-depth 값보다 작거나 같아야 합니다.
- Sun 스택의 대기열 깊이의 경우: 기본 드라이버는 HBA 레벨에서 LUN 단위 또는 대상 max_throttle에 대한 설정을 허용하지 않습니다. 기본 드라이버에 대해 max_throttle 값을 설정하는 데 권장되는 방법은 '/kernel/drv/sd.conf' 및 '/kernel/drv/ssd.conf' 파일의 장치별 유형(VID_PID) 수준에 있습니다. 호스트 유틸리티는 MPxIO 구성의 경우 이 값을 64로, Veritas DMP 구성의 경우 8로 설정합니다.

단계

1. '#cd/kernel/drv'
2. '#vi lpfc.conf'
3. '/TFT-queue(/tgt-queue)'를 검색합니다

```
tgt-queue-depth=32
```



기본값은 설치 시 32로 설정됩니다.

4. 환경 구성에 따라 원하는 값을 설정합니다.
5. 파일을 저장합니다.
6. 'sync;sync;sync;reboot---r' 명령을 사용하여 호스트를 재부팅합니다.

QLogic HBA의 VMware 호스트입니다

'esxcfg-module' 명령을 사용하여 HBA 시간 제한 설정을 변경합니다. ESX.conf 파일을 수동으로 업데이트하는 것은 권장되지 않습니다.

단계

1. 서비스 콘솔에 루트 사용자로 로그인합니다.
2. 현재 로드된 Qlogic HBA 모듈을 확인하려면 '#vmkload_mod -l' 명령을 사용합니다.
3. Qlogic HBA의 단일 인스턴스의 경우 다음 명령을 실행합니다.

```
'#esxcfg-module-s ql2xmaxqdepth=64 qla2300_707'
```



이 예에서는 qla2300_707 모듈을 사용합니다. "vmkload_mod -l"의 출력에 따라 적절한 모듈을 사용합니다.

4. 다음 명령을 사용하여 변경 내용을 저장합니다.

```
'#/usr/sbin/esxcfg-boot -b'
```

5. 다음 명령을 사용하여 서버를 재부팅합니다.

```
'#reboot'
```

6. 다음 명령을 사용하여 변경 사항을 확인합니다.

- a. '#esxcfg-module-g qla2300_707'

- b. ``qla2300_707 활성화됨 = 1 옵션 = 'ql2xmaxqdepth=64'`

Emulex HBA용 VMware 호스트

'esxcfg-module' 명령을 사용하여 HBA 시간 제한 설정을 변경합니다. ESX.conf 파일을 수동으로 업데이트하는 것은 권장되지 않습니다.

단계

1. 서비스 콘솔에 루트 사용자로 로그인합니다.
2. 현재 어떤 Emulex HBA가 로드되었는지 확인하려면 '#vmkload_mod -l grep lpfc' 명령을 사용합니다.
3. Emulex HBA의 단일 인스턴스의 경우 다음 명령을 입력합니다.

```
#esxcfg-module-s lpfc0_lun_queue_depth=16 lpfcdd_7xx'
```



HBA 모델에 따라 모듈은 lpfcdd_7xx 또는 lpfcdd_732일 수 있습니다. 위 명령은 lpfcdd_7xx 모듈을 사용합니다. vmkload_mod-의 결과에 따라 적절한 모듈을 사용해야 합니다.

이 명령을 실행하면 LUN 대기열 길이가 lpfc0으로 표시된 HBA에 대해 16으로 설정됩니다.

4. Emulex HBA의 여러 인스턴스의 경우 다음 명령을 실행합니다.

```
"a esxcfg-module-s" lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"lpfcdd_7xx"
```

lpfc0에 대한 LUN 큐 길이 및 lpfc1에 대한 LUN 큐 크기는 16으로 설정됩니다.

5. 다음 명령을 입력합니다.

```
#esxcfg-boot-b'
```

6. reboot를 사용하여 재부팅합니다.

Emulex HBA용 Windows 호스트

Windows 호스트에서는 "LPUTILNT" 유틸리티를 사용하여 Emulex HBA의 대기열 길이를 업데이트할 수 있습니다.

단계

1. C:\WINNT\system32 디렉토리에 있는 LPUTILNT 유틸리티를 실행합니다.
2. 오른쪽의 메뉴에서 * Drive Parameters * 를 선택합니다.
3. 아래로 스크롤하여 * QueueDepth * 를 두 번 클릭합니다.



QueueDepth * 를 150보다 크게 설정하는 경우 다음 Windows 레지스트리 값도 적절하게 늘려야 합니다.

```
'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxn\Parameters\Device\NumberOfRequests'
```

Qlogic HBA에 대한 Windows 호스트입니다

Windows 호스트에서는 및 'sansurfer' HBA 관리자 유틸리티를 사용하여 Qlogic HBA의 대기열 깊이를 업데이트할 수 있습니다.

단계

1. '서퍼' HBA 매니저 유틸리티를 실행합니다.
2. HBA 포트 * > * 설정 * 을 클릭합니다.
3. 목록 상자에서 * 고급 HBA 포트 설정 * 을 클릭합니다.
4. Execution Throttle 파라미터를 업데이트한다.

Emulex HBA용 Linux 호스트

Linux 호스트에서 Emulex HBA의 대기열 깊이를 업데이트할 수 있습니다. 재부팅 후에도 업데이트가 지속되도록 하려면 새 RAM 디스크 이미지를 생성하고 호스트를 재부팅해야 합니다.

단계

1. 수정할 대기열 길이 매개 변수를 식별합니다.

```
Modinfo lpfc | grep queue_depth(Modinfo lpfc | grep queue_depth
```

설명이 포함된 대기열 길이 매개 변수 목록이 표시됩니다. 운영 체제 버전에 따라 다음 대기열 길이 매개 변수 중 하나 이상을 수정할 수 있습니다.

- 'lpfc_lun_queue_depth': 특정 LUN에 대기할 수 있는 최대 FC 명령어 수(uint)
- 'lpfc_hba_queue_depth': lpfc HBA(uint)에 대기할 수 있는 최대 FC 명령어 수
- 'lpfc_tgt_queue_depth': 특정 대상 포트에 대기할 수 있는 최대 FC 명령어 수(uint)

"lpfc_tgt_queue_depth" 매개변수는 Red Hat Enterprise Linux 7.x 시스템, SUSE Linux Enterprise Server 11 SP4 시스템 및 12.x 시스템에만 적용됩니다.

2. Red Hat Enterprise Linux 5.x 시스템에 대한 '/etc/modprobe.conf' 파일과 Red Hat Enterprise Linux 6.x 또는 7.x 시스템에 대한 '/etc/modprobe.d/scsi.conf' 파일 또는 SUSE Linux Enterprise Server 11.x 또는 12.x 시스템에 대기열 길이 매개 변수를 추가하여 대기열 깊이를 업데이트합니다.

운영 체제 버전에 따라 다음 명령 중 하나 이상을 추가할 수 있습니다.

- 'options lpfc lpfc_hba_queue_depth=new_queue_depth'
- 'options lpfc lpfc_lun_queue_depth=new_queue_depth'
- 'options lpfc lpfc_tgt_queue_depth=new_queue_depth'

3. 새 RAM 디스크 이미지를 만든 다음 호스트를 재부팅하여 재부팅 후에도 업데이트가 지속되도록 합니다.

자세한 내용은 를 참조하십시오 "[시스템 관리](#)" Linux 운영 체제 버전용.

4. 수정한 각 대기열 길이 매개 변수에 대해 대기열 길이 값이 업데이트되었는지 확인합니다.

```
'cat/sys/class/scsi_host/host_number/lpfc_lun_queue_depth"cat/sys/class/scsi_host/host_number/lpfc_tgt_queue_depth"cat/sys/class/scsi_host/host_number/lpfc_hba_queue_depth'
```

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```

대기열 깊이의 현재 값이 표시됩니다.

QLogic HBA용 Linux 호스트

Linux 호스트에서 QLogic 드라이버의 장치 대기열 길이를 업데이트할 수 있습니다. 재부팅 후에도 업데이트가 지속되도록 하려면 새 RAM 디스크 이미지를 생성하고 호스트를 재부팅해야 합니다. QLogic HBA 관리 GUI 또는 CLI(명령줄 인터페이스)를 사용하여 QLogic HBA 대기열 길이를 수정할 수 있습니다.

이 작업은 QLogic HBA CLI를 사용하여 QLogic HBA 대기열 길이를 수정하는 방법을 보여줍니다

단계

1. 수정할 장치 대기열 길이 매개 변수를 식별합니다.

```
'modinfo qla2xxx | grep ql2xmaxqdepth'
```

각 LUN에 대해 설정할 수 있는 최대 대기열 길이를 나타내는 "ql2xmaxqdepth" 대기열 길이 매개변수만 수정할 수 있습니다. RHEL 7.5 이상의 경우 기본값은 64입니다. 기본값은 RHEL 7.4 이전 버전의 경우 32입니다.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:          ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. 장치 대기열 깊이 값 업데이트:

- 수정 사항을 영구적으로 만들려면 다음 단계를 수행하십시오.

- i. Red Hat Enterprise Linux 5.x 시스템에 대한 '/etc/modprobe.conf' 파일과 Red Hat Enterprise Linux 6.x 또는 7.x 시스템에 대한 '/etc/modprobe.d/scsi.conf' 파일에 대기열 깊이 매개 변수를 추가하거나 SUSE Linux Enterprise Server 11.x 또는 12.x 시스템에 대한 '/etc/modprobe.conf' 파일에 대기열 깊이를 업데이트합니다. laq2xxx.options
- ii. 새 RAM 디스크 이미지를 만든 다음 호스트를 재부팅하여 재부팅 후에도 업데이트가 지속되도록 합니다.

자세한 내용은 를 참조하십시오 ["시스템 관리"](#) Linux 운영 체제 버전용.

- 현재 세션에 대해서만 매개 변수를 수정하려면 다음 명령을 실행합니다.

```
'echo new_queue_depth>/sys/module/qla2xxx/parameters/ql2xmaxqdepth'
```

다음 예제에서 대기열 길이는 128로 설정됩니다.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. 대기열 길이 값이 업데이트되었는지 확인합니다.

```
'cat/sys/module/qla2xxx/parameters/ql2xmaxqdepth'
```

대기열 깊이의 현재 값이 표시됩니다.

4. QLogic HBA BIOS에서 펌웨어 매개변수 "실행 스토를"을 업데이트하여 QLogic HBA 대기열 길이를 수정합니다.

a. QLogic HBA 관리 CLI에 로그인합니다.

```
'/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli'
```

b. 주 메뉴에서 "어댑터 구성" 옵션을 선택합니다.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

          CLI - Version 2.2.0 (Build 15)

Main Menu

1:  Adapter Information
**2: Adapter Configuration**
3:  Adapter Updates
4:  Adapter Diagnostics
5:  Monitoring
6:  FabricCache CLI
7:  Refresh
8:  Help
9:  Exit

Please Enter Selection: 2
```

c. 어댑터 구성 매개 변수 목록에서 'HBA Parameters' 옵션을 선택합니다.

```

1: Adapter Alias
2: Adapter Port Alias
**3: HBA Parameters**
4: Persistent Names (udev)
5: Boot Devices Configuration
6: Virtual Ports (NPIV)
7: Target Link Speed (iidDMA)
8: Export (Save) Configuration
9: Generate Reports
10: Personality
11: FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 3

```

d. HBA 포트 목록에서 필요한 HBA 포트를 선택합니다.

```

Fibre Channel Adapter Configuration

HBA Model QLE2562 SN: BFD1524C78510
  1: Port 1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
  2: Port 2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
HBA Model QLE2672 SN: RFE1241G81915
  3: Port 1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
  4: Port 2: WWPN: 21-00-00-0E-1E-09-B7-63 Online

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 1

```

HBA 포트의 세부 정보가 표시됩니다.

e. HBA Parameters(HBA 매개변수) 메뉴에서 Display HBA Parameters(HBA 매개변수 표시) 옵션을 선택하여 "Execution Throttle(실행 스로틀)" 옵션의 현재 값을 확인합니다.

실행 스로틀 옵션의 기본값은 65535입니다.

```

HBA Parameters Menu

=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02

```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
```

=====

- 1: Display HBA Parameters
- 2: Configure HBA Parameters
- 3: Restore Defaults

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)

Please Enter Selection: 1

HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-07-00

Link: Online


```
Connection Options          : 2 - Loop Preferred, Otherwise Point-to-Point
Data Rate                   : Auto
Frame Size                   : 2048
Hard Loop ID                 : 0
Loop Reset Delay (seconds)  : 5
Enable Host HBA BIOS        : Enabled
Enable Hard Loop ID         : Disabled
Enable FC Tape Support      : Enabled
Operation Mode               : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us) : 0
**Execution Throttle       : 65535**
Login Retry Count           : 8
Port Down Retry Count       : 30
Enable LIP Full Login       : Enabled
Link Down Timeout (seconds) : 30
Enable Target Reset         : Enabled
LUNs Per Target             : 128
Out Of Order Frame Assembly : Disabled
Enable LR Ext. Credits      : Disabled
Enable Fabric Assigned WWN  : N/A
```

Press <Enter> to continue:

- a. 계속하려면 * Enter * 를 누르십시오.
- b. HBA Parameters(HBA 매개변수) 메뉴에서 Configure HBA Parameters(HBA 매개변수 구성) 옵션을 선택하여 HBA 매개변수를 수정합니다.

c. Configure Parameters 메뉴에서 'Execute Throttle' 옵션을 선택하고 이 매개 변수의 값을 업데이트합니다.

```
Configure Parameters Menu

=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====

1: Connection Options
2: Data Rate
3: Frame Size
4: Enable HBA Hard Loop ID
5: Hard Loop ID
6: Loop Reset Delay (seconds)
7: Enable BIOS
8: Enable Fibre Channel Tape Support
9: Operation Mode
10: Interrupt Delay Timer (100 microseconds)
11: Execution Throttle
12: Login Retry Count
13: Port Down Retry Count
14: Enable LIP Full Login
15: Link Down Timeout (seconds)
16: Enable Target Reset
17: LUNs per Target
18: Enable Receive Out Of Order Frame
19: Enable LR Ext. Credits
20: Commit Changes
21: Abort Changes

      (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
      Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. 계속하려면 * Enter * 를 누르십시오.

e. Configure Parameters 메뉴에서 'Commit Changes' 옵션을 선택하여 변경 사항을 저장합니다.

f. 메뉴를 종료합니다.

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.