네트워크 관리

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/networking/networking_reference.html on February 12, 2026. Always check docs.netapp.com for the latest.

목차

네트워크 관리 . . . 1
시작하십시오 . . . 1
System Manager를 사용하여 ONTAP 네트워크를 시각화합니다 . . . 1
ONTAP 클러스터의 네트워킹 구성 요소에 대해 알아봅니다 . . . 2
ONTAP 네트워크 케이블 연결에 대한 모범 사례 . . . 4
ONTAP 네트워크에서 사용할 LIF 페일오버 정책을 결정합니다 . . . 6
NAS 경로 페일오버 워크플로우 . . . 8
ONTAP 네트워크에서 NAS 경로 페일오버를 구성합니다 . . . 8
ONTAP 네트워크에서 NAS 경로 페일오버를 위한 워크시트 . . . 9
네트워크 포트 . . . 15
ONTAP 네트워크 포트 구성에 대해 자세히 알아보십시오 . . . 15
네트워크 포트를 구성합니다 . . . 15
IPspace . . . 42
ONTAP IPspace 구성에 대해 자세히 알아보십시오 . . . 42
ONTAP 네트워크용 IPspace를 생성합니다 . . . 45
ONTAP 네트워크에서 IPspace를 확인합니다 . . . 47
ONTAP 네트워크에서 IPspace를 삭제합니다 . . . 47
브로드캐스트 도메인 . . . 48
ONTAP 브로드캐스트 도메인에 대해 알아봅니다 . . . 48
ONTAP 브로드캐스트 도메인을 생성합니다 . . . 49
ONTAP 브로드캐스트 도메인에서 포트를 추가하거나 제거합니다 . . . 52
ONTAP 포트 가용성을 복구합니다 . . . 55
ONTAP 브로드캐스트 도메인을 IPspace로 이동합니다 . . . 62
ONTAP 브로드캐스트 도메인을 분할합니다 . . . 63
ONTAP 브로드캐스트 도메인을 병합합니다 . . . 64
ONTAP 브로드캐스트 도메인의 포트에 대한 MTU 값을 변경합니다 . . . 65
ONTAP 브로드캐스트 도메인을 봅니다 . . . 67
ONTAP 브로드캐스트 도메인을 삭제합니다 . . . 68
페일오버 그룹 및 정책 . . . 69
ONTAP 네트워크에서의 LIF 페일오버에 대해 알아보십시오 . . . 69
ONTAP 페일오버 그룹을 생성합니다 . . . 70
LIF에 대한 ONTAP 페일오버 설정을 구성합니다 . . . 71
ONTAP 명령으로 페일오버 그룹 및 정책을 관리할 수 있습니다 . . . 72
서브넷(클러스터 관리자만 해당) . . . 73
ONTAP 네트워크의 서브넷에 대해 알아봅니다 . . . 73
ONTAP 네트워크에 대한 서브넷을 생성합니다 . . . 73
ONTAP 네트워크의 서브넷에서 IP 주소를 추가하거나 제거합니다 . . . 76
ONTAP 네트워크의 서브넷 속성을 변경합니다 . . . 78
ONTAP 네트워크의 서브넷을 봅니다 . . . 80

ONTAP 네트워크에서 서브넷을 삭제합니다 . . . 80
ONTAP 네트워크용 SVM을 생성합니다 . . . 81
논리 인터페이스(LIF) . . . 88
LIF 개요 . . . 88
LIF 관리 . . . 97
ONTAP 가상 IP(VIP) LIF를 구성합니다 . . . 115
네트워크 로드 밸런싱 . . . 122
DNS 로드 밸런싱을 사용하여 ONTAP 네트워크 트래픽을 최적화합니다 . . . 122
ONTAP 네트워크의 DNS 로드 밸런싱에 대해 알아봅니다 . . . 122
ONTAP 네트워크에 대한 DNS 로드 밸런싱 존을 생성합니다 . . . 123
로드 밸런싱 존에서 ONTAP LIF를 추가 또는 제거합니다 . . . 124
ONTAP 네트워크에 대한 DNS 서비스를 구성합니다 . . . 124
ONTAP 네트워크에 대한 동적 DNS 서비스를 구성합니다 . . . 127
호스트 이름 확인 . . . 128
ONTAP 네트워크의 호스트 이름 확인에 대해 알아봅니다 . . . 128
ONTAP 네트워크의 호스트 이름 확인을 위해 DNS를 구성합니다 . . . 128
ONTAP hosts 테이블을 관리하는 ONTAP 명령 . . . 130
네트워크 보안 . . . 131
모든 SSL 연결에 FIPS를 사용하여 ONTAP 네트워크 보안을 구성합니다 . . . 131
IPsec 전송 중 암호화를 구성합니다 . . . 134
ONTAP 백엔드 클러스터 네트워크 암호화 구성 . . . 143
ONTAP 네트워크에서 LIF에 대한 방화벽 정책을 구성합니다 . . . 144
방화벽 서비스 및 정책을 관리하는 ONTAP 명령 . . . 150
QoS 표시(클러스터 관리자만 해당) . . . 150
ONTAP 네트워크 QoS(Quality of Service)에 대해 알아보기 . . . 151
ONTAP 네트워크 QoS 표시 값을 수정합니다 . . . 151
ONTAP 네트워크 QoS 표시 값을 확인합니다 . . . 152
SNMP 관리(클러스터 관리자만 해당) . . . 152
ONTAP 네트워크의 SNMP에 대해 알아봅니다 . . . 152
ONTAP 네트워크용 SNMP 커뮤니티를 생성합니다 . . . 154
ONTAP 클러스터에서 SNMPv3 사용자를 구성합니다 . . . 156
ONTAP 네트워크에서 SNMP용 traphosts를 구성합니다 . . . 160
ONTAP 클러스터에서 SNMP 폴링을 확인합니다 . . . 161
SNMP, 트랩 및 traphost를 관리하는 ONTAP 명령입니다 . . . 162
SVM에서 라우팅 관리 . . . 165
ONTAP 네트워크에서의 SVM 라우팅에 대해 알아보십시오 . . . 165
ONTAP 네트워크에 대한 정적 라우트를 생성합니다 . . . 165
ONTAP 네트워크에 대해 다중 경로 라우팅을 활성화합니다 . . . 166
ONTAP 네트워크에서 정적 라우트를 삭제합니다 . . . 166
ONTAP 라우팅 정보를 봅니다 . . . 166
ONTAP 네트워크의 라우팅 테이블에서 동적 라우트를 제거합니다 . . . 168

ONTAP 네트워크 정보 . . . 169
ONTAP 네트워크 정보를 봅니다 . . . 169
ONTAP 네트워크 포트 정보를 봅니다 . . . 170
ONTAP VLAN 정보를 봅니다 . . . 171
ONTAP 인터페이스 그룹 정보를 봅니다 . . . 172
ONTAP LIF 정보 를 참조하십시오 . . . 173
ONTAP 네트워크에 대한 라우팅 정보를 봅니다 . . . 176
ONTAP DNS 호스트 테이블 항목을 봅니다 . . . 178
ONTAP DNS 도메인 구성 정보를 봅니다 . . . 178
ONTAP 페일오버 그룹 정보를 봅니다 . . . 179
ONTAP LIF 페일오버 대상을 봅니다 . . . 180
로드 밸런싱 존에서 ONTAP LIF를 확인하십시오 . . . 182
ONTAP 클러스터 연결을 봅니다 . . . 183
네트워크 문제를 진단하는 ONTAP 명령 . . . 189
Neighbor Discovery Protocol을 통한 네트워크 접속 구성 보기 . . . 190

네트워크 관리

시작하십시오

System Manager를 사용하여 ONTAP 네트워크를 시각화합니다

ONTAP 9.8부터는 System Manager를 사용하여 네트워크의 구성 요소와 구성을 보여주는 그래픽을 표시할 수 있으며, 호스트, 포트, SVM, 볼륨 등에 걸친 네트워크 연결 경로를 볼 수 있습니다. ONTAP 9.12.1부터 네트워크 인터페이스 그리드에서 LIF 및 서브넷 연결을 볼 수 있습니다.

그래픽은 * 네트워크 > 개요 * 를 선택하거나 대시보드의 * 네트워크 * 섹션에서 선택하면 표시됩니다 → .

그림에 표시된 구성 요소는 다음과 같습니다.

- 호스트
- 스토리지 포트
- 네트워크 인터페이스
- 스토리지 VM
- 데이터 액세스 구성 요소

각 섹션에는 네트워크 관리 및 구성 작업을 수행하기 위해 마우스를 가져가거나 선택할 수 있는 추가 세부 정보가 표시됩니다.

기존 시스템 관리자(ONTAP 9 .7 이하 버전에서만 사용 가능)를 사용하는 경우 를 참조하십시오."네트워크 관리"

예

다음은 각 구성 요소에 대한 세부 정보를 보거나 네트워크를 관리하기 위한 작업을 시작하기 위해 그래픽과 상호 작용할 수 있는 여러 가지 방법의 예입니다.

- 포트, 네트워크 인터페이스, 스토리지 VM 및 연결된 데이터 액세스 구성 요소와 같은 해당 구성을 보려면 호스트를 클릭합니다.
- 스토리지 VM의 볼륨 수 위에 마우스 커서를 올려 놓으면 세부 정보를 볼 볼륨을 선택할 수 있습니다.
- 지난 주 동안의 성능을 보려면 iSCSI 인터페이스를 선택합니다.
- 구성 요소 옆에 있는 을 ⋮ 클릭하여 해당 구성 요소를 수정하는 작업을 시작합니다.
- 비정상적인 구성 요소 옆에 "X"가 표시되어 네트워크에서 문제가 발생할 수 있는 위치를 빠르게 확인할 수 있습니다.

System Manager 네트워크 시각화 비디오

ONTAP 클러스터의 네트워킹 구성 요소에 대해 알아봅니다

클러스터를 설정하기 전에 클러스터의 네트워킹 구성 요소를 숙지해야 합니다. 클러스터의 물리적 네트워킹 구성 요소를 논리적 구성 요소로 구성하면 ONTAP의 유연성과 멀티 테넌시 기능을 활용할 수 있습니다.

클러스터의 다양한 네트워킹 구성 요소는 다음과 같습니다.

- 물리적 포트

  네트워크 인터페이스 카드(NIC) 및 호스트 버스 어댑터(HBA)는 각 노드에서 물리적 네트워크(관리 및 데이터 네트워크)로의 물리적(이더넷 및 파이버 채널) 연결을 제공합니다.

  사이트 요구사항, 스위치 정보, 포트 케이블 연결 정보 및 컨트롤러 온보드 포트 케이블은 에서 Hardware Universe를 참조하십시오 "hwu.netapp.com".

- 논리 포트

  VLAN(Virtual Local Area Network) 및 인터페이스 그룹은 논리 포트를 구성합니다. 인터페이스 그룹은 여러 물리적 포트를 단일 포트로 취급하며 VLAN은 물리적 포트를 여러 개의 개별 포트로 세분화합니다.

- IPspace

  IPspace를 사용하여 클러스터의 각 SVM에 대해 별개의 IP 주소 공간을 생성할 수 있습니다. 이렇게 하면 관리자가 별도의 네트워크 도메인에 있는 클라이언트가 동일한 IP 주소 서브넷 범위의 중복 IP 주소를 사용하면서 클러스터 데이터에 액세스할 수 있습니다.

- 브로드캐스트 도메인

브로드캐스트 도메인은 IPspace에 상주하며 동일한 계층 2 네트워크에 속하는 클러스터 내의 여러 노드에서 잠재적으로 네트워크 포트 그룹을 포함합니다. 그룹의 포트는 SVM에서 데이터 트래픽을 위해 사용됩니다.

- 서브넷

  서브넷은 브로드캐스트 도메인 내에서 생성되며 동일한 계층 3 서브넷에 속하는 IP 주소 풀을 포함합니다. 이 IP 주소 풀은 LIF 생성 중에 IP 주소 할당을 간소화합니다.

- 논리 인터페이스

  논리 인터페이스(LIF)는 포트에 연결된 IP 주소 또는 WWPN(Worldwide Port Name)입니다. 페일오버 그룹, 페일오버 규칙 및 방화벽 규칙과 같은 속성과 연결됩니다. LIF는 현재 바인딩된 포트(물리적 또는 논리적)를 통해 네트워크를 통해 통신합니다.

  클러스터의 다양한 LIF 유형에는 데이터 LIF, 클러스터 범위 관리 LIF, 노드 범위 관리 LIF, 인터클러스터 LIF, 클러스터 LIF 등이 있습니다. LIF의 소유권은 LIF가 상주하는 SVM에 따라 다릅니다. 데이터 LIF는 데이터 SVM, 노드 범위 관리 LIF, 클러스터 범위 관리 LIF, 인터클러스터 LIF가 관리 SVM에서 소유하며 클러스터 LIF는 클러스터 SVM에서 소유합니다.

- DNS 영역

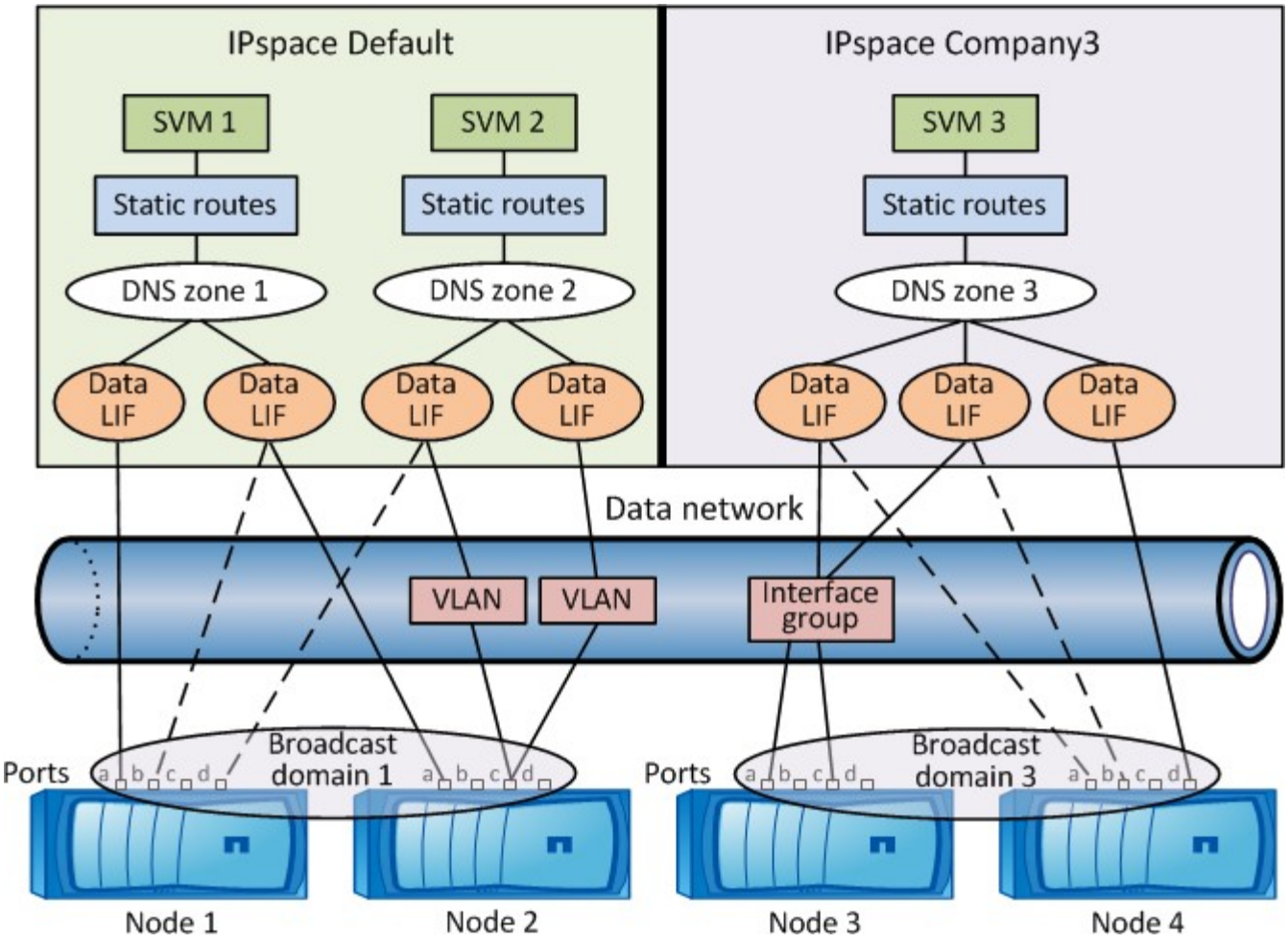
  LIF 생성 중에 DNS 존을 지정할 수 있으며, 클러스터의 DNS 서버를 통해 LIF를 내보낼 이름을 제공합니다. 여러 LIF가 동일한 이름을 공유할 수 있으므로 DNS 로드 밸런싱 기능이 로드에 따라 이름에 대한 IP 주소를 배포할 수 있습니다.

  SVM은 여러 DNS 존을 포함할 수 있습니다.

- 라우팅

  각 SVM은 네트워킹과 관련하여 자체적으로 충분합니다. SVM은 구성된 각 외부 서버에 연결할 수 있는 LIF 및 경로를 소유합니다.

  다음 그림에서는 4노드 클러스터에서 서로 다른 네트워킹 구성 요소가 연결되는 방식을 보여 줍니다.

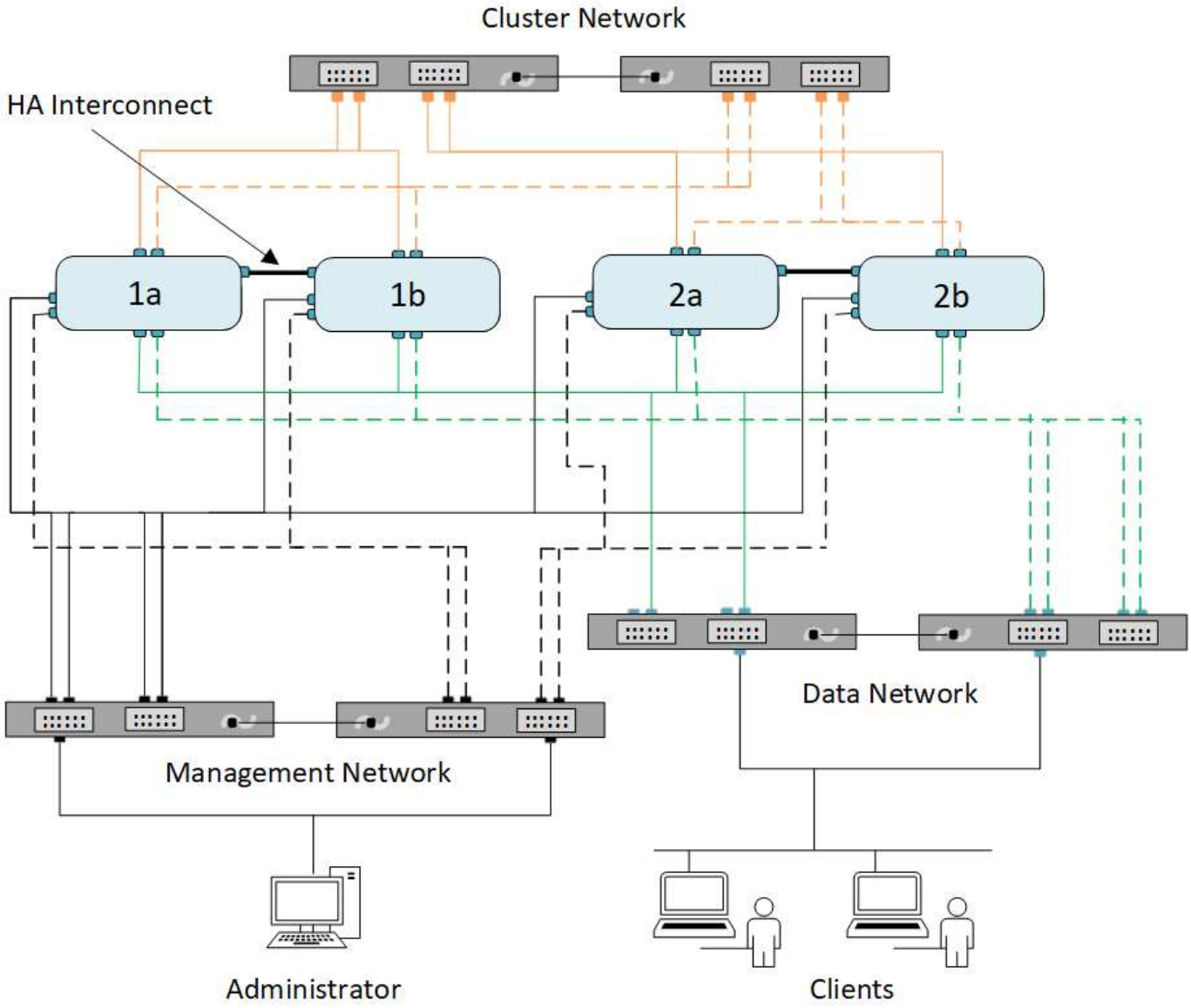


ONTAP 네트워크 케이블 연결에 대한 모범 사례

네트워크 케이블 연결 모범 사례는 트래픽을 클러스터, 관리 및 데이터와 같은 네트워크로 분리합니다.

클러스터 트래픽이 다른 모든 트래픽과 별도의 네트워크에 있도록 클러스터에 케이블을 연결해야 합니다. 이는 선택 사항이지만 데이터와 클러스터 내 트래픽과 네트워크 관리 트래픽을 분리하는 것이 좋습니다. 별도의 네트워크를 유지 관리하여 성능 향상, 관리 용이성, 노드에 대한 보안 및 관리 액세스 개선을 실현할 수 있습니다.

다음 다이어그램에서는 3개의 개별 네트워크를 포함하는 4노드 HA 클러스터의 네트워크 케이블을 연결합니다.



네트워크 연결을 연결할 때는 다음과 같은 특정 지침을 따라야 합니다.

- 각 노드는 3개의 개별 네트워크에 연결되어야 합니다.

  하나의 네트워크는 관리용으로, 하나는 데이터 액세스용으로, 다른 하나는 클러스터 간 통신용으로 사용됩니다. 관리 네트워크와 데이터 네트워크를 논리적으로 분리할 수 있습니다.

- 클라이언트(데이터) 트래픽 흐름을 개선하기 위해 각 노드에 둘 이상의 데이터 네트워크 연결을 가질 수 있습니다.
- 데이터 네트워크 연결 없이 클러스터를 생성할 수 있지만 클러스터 인터커넥트 연결이 포함되어야 합니다.
- 각 노드에 대해 항상 2개 이상의 클러스터 연결이 있어야 합니다.

네트워크 케이블 연결에 대한 자세한 내용은 를 참조하십시오 "AFF and FAS 시스템 설명서 센터 를 참조하십시오" 및 "Hardware Universe".

ONTAP 네트워크에서 사용할 LIF 페일오버 정책을 결정합니다

브로드캐스트 도메인, 페일오버 그룹 및 페일오버 정책이 함께 작동하여 LIF가 구성된 노드 또는 포트에 장애가 발생할 경우 어떤 포트가 대체할지 결정합니다.

브로드캐스트 도메인은 동일한 계층 2 이더넷 네트워크에서 연결할 수 있는 모든 포트를 나열합니다. 포트 중 하나에서 전송된 이더넷 브로드캐스트 패킷은 브로드캐스트 도메인의 다른 모든 포트에서 표시됩니다. LIF가 브로드캐스트 도메인의 다른 포트로 페일오버되더라도 원래 포트에서 연결할 수 있는 모든 로컬 및 원격 호스트에 연결할 수 있으므로 브로드캐스트 도메인의 이러한 공통 도달 가능성 특성이 LIF에 중요합니다.

페일오버 그룹은 브로드캐스트 도메인 내에서 LIF 페일오버 커버리지를 제공하는 포트를 정의합니다. 각 브로드캐스트 도메인에는 모든 포트가 포함된 하나의 페일오버 그룹이 있습니다. 브로드캐스트 도메인의 모든 포트가 포함된 이 페일오버 그룹이 LIF에 대한 기본 페일오버 그룹이며 권장되는 페일오버 그룹입니다. 브로드캐스트 도메인 내에서 동일한 링크 속도를 갖는 포트의 페일오버 그룹과 같이 사용자가 정의하는 작은 하위 집합을 사용하여 페일오버 그룹을 생성할 수 있습니다.

페일오버 정책은 노드 또는 포트가 다운될 때 LIF가 페일오버 그룹의 포트를 사용하는 방법을 결정합니다. 페일오버 정책을 페일오버 그룹에 적용되는 필터 유형으로 고려하십시오. LIF의 페일오버 타겟(LIF가 페일오버가 가능한 포트 세트)은 브로드캐스트 도메인의 LIF 페일오버 그룹에 LIF의 페일오버 정책을 적용하여 결정됩니다.

다음 CLI 명령을 사용하여 LIF의 페일오버 타겟을 볼 수 있습니다.

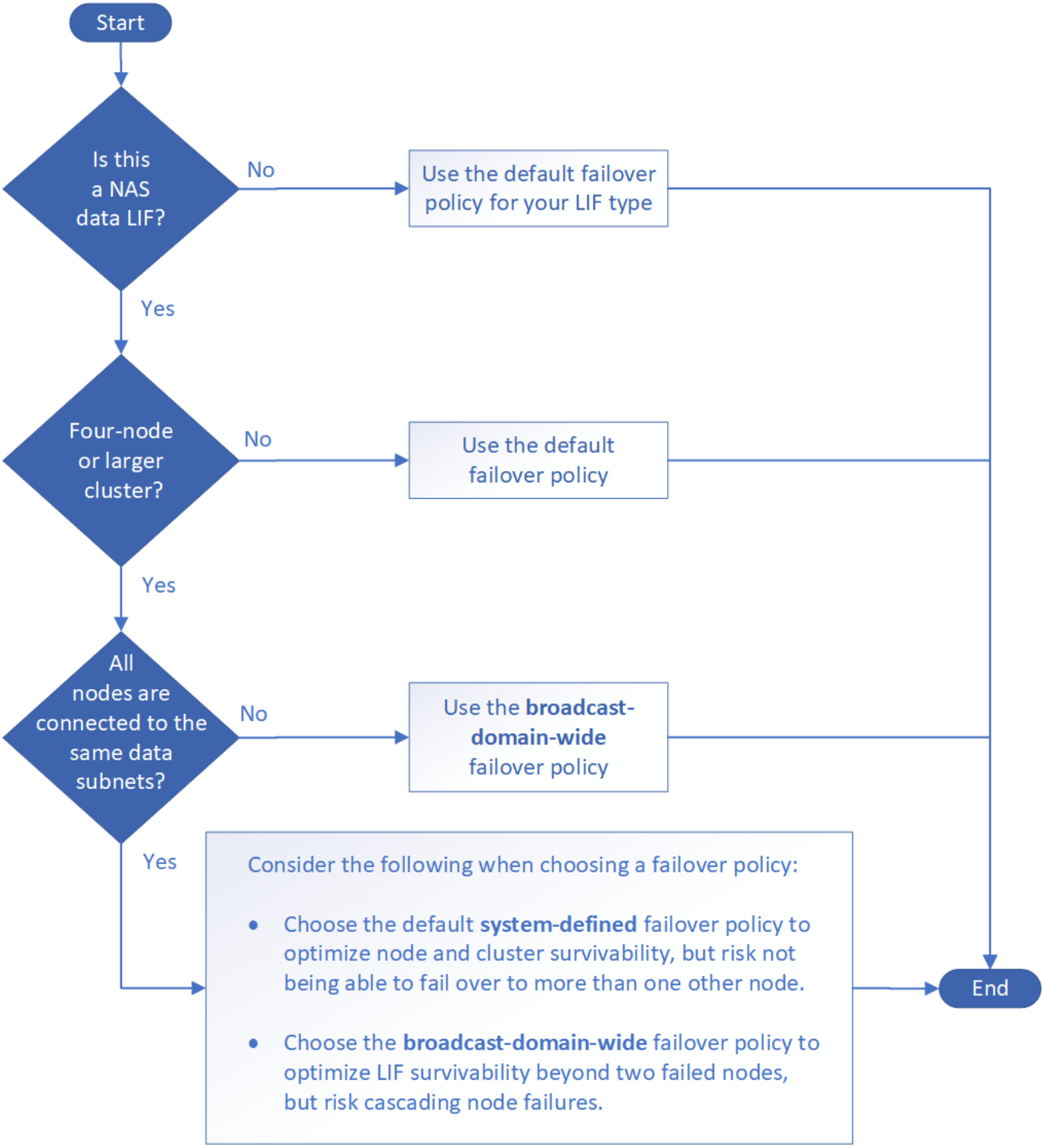
```
network interface show -failover
```

LIF 유형에 기본 페일오버 정책을 사용하는 것이 좋습니다.

사용할 **LIF** 페일오버 정책을 결정합니다

권장 기본 페일오버 정책을 사용할지, LIF 유형 및 환경에 따라 정책을 변경할지 결정합니다.

페일오버 정책 결정 트리



LIF 유형별 기본 페일오버 정책

LIF 유형입니다	기본 페일오버 정책입니다	설명
BGP LIF	사용 안 함	LIF가 다른 포트로 페일오버되지 않습니다.
클러스터 LIF	로컬 전용	LIF는 같은 노드의 포트로만 페일오버됩니다.
클러스터 관리 LIF	브로드캐스트 도메인 전체에 적용됩니다	LIF는 클러스터의 모든 노드에 있는 동일한 브로드캐스트 도메인의 포트로 페일오버됩니다.

인터클러스터 LIF	로컬 전용	LIF는 같은 노드의 포트로만 페일오버됩니다.
NAS 데이터 LIF	시스템 정의	LIF가 HA 파트너가 아닌 다른 노드 하나로 페일오버합니다.
노드 관리 LIF	로컬 전용	LIF는 같은 노드의 포트로만 페일오버됩니다.
SAN 데이터 LIF	사용 안 함	LIF가 다른 포트로 페일오버되지 않습니다.

"SFO-파트너 전용" 페일오버 정책은 기본이 아니지만 LIF가 홈 노드 또는 SFO 파트너의 포트로 페일오버되도록 하려는 경우에만 사용할 수 있습니다.

관련 정보

- "네트워크 인터페이스가 표시됩니다"

NAS 경로 페일오버 워크플로우

ONTAP 네트워크에서 NAS 경로 페일오버를 구성합니다

기본 네트워킹 개념에 이미 익숙한 경우 NAS 경로 페일오버 구성에 대한 이 "실습" 워크플로우를 검토하여 네트워크 설정 시간을 절약할 수 있습니다.

> NAS 경로 페일오버 구성을 위한 워크플로는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 NAS 페일오버를 구성해야 하는 경우 워크플로우를 "NAS 경로 페일오버 워크플로우(ONTAP 9.7 이하)"참조하십시오.

NAS LIF는 현재 포트에서 링크 장애가 발생하면 작동 가능한 네트워크 포트로 자동 마이그레이션됩니다. ONTAP 기본값을 사용하여 경로 페일오버를 관리할 수 있습니다.

> SAN LIF는 마이그레이션되지 않습니다(링크 장애 후 수동으로 이동하지 않는 경우). 대신 호스트의 다중 경로 기술은 트래픽을 다른 LIF로 전환합니다. 자세한 내용은 을 참조하십시오 "SAN 관리".

1. **"워크시트를 작성합니다"**

워크시트를 사용하여 NAS 경로 페일오버를 계획합니다.

2. **"IPspace 생성"**

클러스터의 각 SVM에 대해 고유한 IP 주소 공간을 생성합니다.

3. **"브로드캐스트 도메인을 IPspace로 이동"**

브로드캐스트 도메인을 IPspace로 이동합니다.

4. **"SVM을 생성합니다"**

SVM을 생성하여 클라이언트에 데이터 제공

5 **"LIF를 생성합니다"**

데이터에 액세스하는 데 사용할 포트에 LIF를 생성합니다.

6 **"SVM에 대한 DNS 서비스를 구성합니다"**

NFS 또는 SMB 서버를 생성하기 전에 SVM에 대한 DNS 서비스를 구성합니다.

ONTAP 네트워크에서 NAS 경로 페일오버를 위한 워크시트

NAS 경로 페일오버를 구성하기 전에 워크시트의 모든 섹션을 완료해야 합니다.

> ONTAP 네트워크의 NAS 장애 조치에 대한 정보는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 NAS 페일오버를 구성해야 하는 경우 을 참조하십시오"NAS 경로 페일오버 구성용 워크시트(ONTAP 9.7 이하)".

IPSpace 구성

IPspace를 사용하여 클러스터의 각 SVM에 대해 별개의 IP 주소 공간을 생성할 수 있습니다. 이렇게 하면 관리자가 별도의 네트워크 도메인에 있는 클라이언트가 동일한 IP 주소 서브넷 범위의 중복 IP 주소를 사용하면서 클러스터 데이터에 액세스할 수 있습니다.

정보	요구한?	당신의 가치
IPSpace 이름 IPspace의 고유 식별자입니다.	예	

브로드캐스트 도메인 구성

브로드캐스트 도메인은 동일한 계층 2 네트워크에 속한 포트를 그룹화하고 브로드캐스트 도메인 포트에 대한 MTU를 설정합니다.

브로드캐스트 도메인은 IPspace에 할당됩니다. IPspace는 하나 이상의 브로드캐스트 도메인을 포함할 수 있습니다.

> LIF가 페일오버되는 포트는 LIF의 페일오버 그룹의 구성원이어야 합니다. ONTAP에서 생성된 각 브로드캐스트 도메인에 대해 동일한 이름의 페일오버 그룹이 생성되어 브로드캐스트 도메인의 모든 포트가 포함됩니다.

정보	요구한?	당신의 가치
IPSpace 이름 브로드캐스트 도메인이 할당된 IPspace입니다. 이 IPspace가 있어야 합니다.	예	
브로드캐스트 도메인 이름 브로드캐스트 도메인의 이름입니다. 이 이름은 IPspace에서 고유해야 합니다.	예	

MTU 브로드캐스트 도메인의 최대 전송 단위 값으로, 일반적으로 * 1500 * 또는 * 9000 * 로 설정됩니다. MTU 값은 브로드캐스트 도메인의 모든 포트와 나중에 브로드캐스트 도메인에 추가된 모든 포트에 적용됩니다. MTU 값은 해당 네트워크에 연결된 모든 장치와 일치해야 합니다. e0M 포트 처리 관리 및 서비스 프로세서 트래픽은 MTU를 1500바이트 이상으로 설정해야 합니다.	예	
포트 포트는 도달 가능 여부에 따라 브로드캐스트 도메인에 할당됩니다. 포트 할당이 완료되면 네트워크 포트 도달 가능성 표시 명령을 실행하여 연결 상태를 확인합니다. 이러한 포트는 물리적 포트, VLAN 또는 인터페이스 그룹이 될 수 있습니다. 에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.	예	

서브넷 구성

서브넷에는 IP 주소 풀과 IPspace에 상주하는 SVM에서 사용하는 LIF에 할당할 수 있는 기본 게이트웨이가 포함되어 있습니다.

- SVM에서 LIF를 생성할 때 IP 주소와 서브넷을 제공하는 대신 서브넷 이름을 지정할 수 있습니다.
- 서브넷을 기본 게이트웨이로 구성할 수 있기 때문에 SVM을 생성할 때 별도의 단계에서 기본 게이트웨이를 생성할 필요가 없습니다.
- 브로드캐스트 도메인은 하나 이상의 서브넷을 포함할 수 있습니다.
- IPspace의 브로드캐스트 도메인에 하나 이상의 서브넷을 연결하여 다른 서브넷에 있는 SVM LIF를 구성할 수 있습니다.
- 각 서브넷에는 동일한 IPspace에서 다른 서브넷에 할당된 IP 주소와 중복되지 않는 IP 주소가 포함되어야 합니다.
- SVM 데이터 LIF에 특정 IP 주소를 할당하고 서브넷 대신 SVM을 위한 기본 게이트웨이를 생성할 수 있습니다.

정보	요구한?	당신의 가치
IPSpace 이름 서브넷이 할당될 IPspace입니다. 이 IPspace가 있어야 합니다.	예	

서브넷 이름 서브넷의 이름입니다. 이 이름은 IPspace에서 고유해야 합니다.	예	
브로드캐스트 도메인 이름 서브넷이 할당될 브로드캐스트 도메인입니다. 이 브로드캐스트 도메인은 지정된 IPspace에 있어야 합니다.	예	
서브넷 이름 및 IP 주소가 상주하는 서브넷 및 마스크를 마스킹합니다.	예	
게이트웨이 서브넷에 대한 기본 게이트웨이를 지정할 수 있습니다. 서브넷을 생성할 때 게이트웨이를 할당하지 않으면 나중에 할당할 수 있습니다.	아니요	
IP 주소 범위 IP 주소 또는 특정 IP 주소 범위를 지정할 수 있습니다. 예를 들어 다음과 같은 범위를 지정할 수 있습니다. 192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145 IP 주소 범위를 지정하지 않으면 지정된 서브넷의 전체 IP 주소 범위를 LIF에 할당할 수 있습니다.	아니요	
LIF 연결의 강제 업데이트 기존 LIF 연결을 강제로 업데이트할지 여부를 지정합니다. 기본적으로 서비스 프로세서 인터페이스 또는 네트워크 인터페이스가 제공된 범위의 IP 주소를 사용하는 경우 서브넷 생성이 실패합니다. 이 매개 변수를 사용하면 수동으로 주소를 지정한 모든 인터페이스를 서브넷에 연결하고 명령이 성공할 수 있습니다.	아니요	

SVM 구성

SVM을 사용하여 클라이언트 및 호스트에 데이터를 제공할 수 있습니다.

귀사가 기록하는 값은 기본 데이터 SVM을 생성하는 것입니다. MetroCluster 소스 SVM을 생성하는 경우 를 참조하십시오 "패브릭 연결 MetroCluster 설치 및 구성 가이드" 또는 을 누릅니다 "스트레치 MetroCluster 설치 및 구성 가이드".

정보	요구한?	당신의 가치
SVM은 SVM의 FQDN(정규화된 도메인 이름)을 지정합니다. 이 이름은 클러스터 리그 전체에서 고유해야 합니다.	예	
루트 볼륨 이름 SVM 루트 볼륨의 이름입니다.	예	
애그리게이트 이름 SVM 루트 볼륨을 포함하는 애그리게이트의 이름입니다. 이 집계가 있어야 합니다.	예	
보안 스타일 SVM 루트 볼륨의 보안 스타일입니다. 가능한 값은 * NTFS *, * UNIX * 및 * MIXED * 입니다.	예	
IPspace 이름 SVM이 할당된 IPspace입니다. 이 IPspace가 있어야 합니다.	아니요	
SVM 언어 SVM 및 해당 볼륨에 사용할 기본 언어를 설정합니다. 기본 언어를 지정하지 않으면 기본 SVM 언어가 * c UTF-8 * 로 설정됩니다. SVM 언어 설정에 따라 SVM의 모든 NAS 볼륨에 대한 파일 이름과 데이터를 표시하는 데 사용되는 문자 세트가 결정됩니다. SVM이 생성된 후 언어를 수정할 수 있습니다.	아니요	

LIF 구성

SVM은 하나 이상의 네트워크 논리 인터페이스(LIF)를 통해 클라이언트와 호스트에 데이터를 제공합니다.

정보	요구한?	당신의 가치
SVM은 LIF의 SVM 이름 입니다.	예	
LIF 이름 LIF의 이름입니다. 노드당 여러 개의 데이터 LIF를 할당할 수 있으며, 노드에 사용 가능한 데이터 포트가 있는 경우 클러스터의 모든 노드에 LIF를 할당할 수 있습니다. 이중화를 제공하려면 각 데이터 서브넷에 대해 최소 2개의 데이터 LIF를 생성해야 하며, 특정 서브넷에 할당된 LIF에는 서로 다른 노드의 홈 포트가 할당되어야 합니다. * 중요: * SMB를 통해 Hyper-V 또는 SQL Server를 호스팅하도록 SMB 서버를 구성하는 경우, SVM은 클러스터의 모든 노드에 하나 이상의 데이터 LIF가 있어야 합니다.	예	
LIF에 대한 서비스 정책 서비스 정책입니다. 서비스 정책은 LIF를 사용할 수 있는 네트워크 서비스를 정의합니다. 기본 제공 서비스 및 서비스 정책을 사용하여 데이터 및 시스템 SVM에서 데이터 및 관리 트래픽을 관리할 수 있습니다.	예	

허용된 프로토콜 IP 기반 LIF에는 허용되는 프로토콜이 필요하지 않습니다. 대신 서비스 정책 행을 사용하십시오. FiberChannel 포트의 SAN LIF에 대해 허용되는 프로토콜을 지정합니다. 이러한 LIF를 사용할 수 있는 프로토콜입니다. LIF가 생성된 후에는 LIF를 사용하는 프로토콜을 수정할 수 없습니다. LIF를 구성할 때 모든 프로토콜을 지정해야 합니다.	아니요	
홈 노드 LIF가 홈 포트로 되돌아갈 때 LIF가 반환되는 노드입니다. 각 데이터 LIF에 대한 홈 노드를 기록해야 합니다.	예	
홈 포트 또는 브로드캐스트 도메인이 다음 중 하나를 선택했습니다. * 포트 *: LIF가 홈 포트로 되돌아갈 때 논리 인터페이스가 반환되는 포트를 지정합니다. IPspace의 서브넷에서 첫 번째 LIF에서만 수행되었지만, 그렇지 않으면 필요하지 않습니다. * 브로드캐스트 도메인 *: 브로드캐스트 도메인을 지정하면 LIF가 홈 포트로 되돌아갈 때 논리 인터페이스가 반환될 적절한 포트가 선택됩니다.	예	
서브넷 이름 SVM에 할당할 서브넷입니다. 애플리케이션 서버에 지속적으로 사용 가능한 SMB 연결을 생성하는 데 사용되는 모든 데이터 LIF는 동일한 서브넷에 있어야 합니다.	예(서브넷을 사용하는 경우)	

DNS 구성

NFS 또는 SMB 서버를 생성하기 전에 SVM에서 DNS를 구성해야 합니다.

정보	요구한?	당신의 가치
SVM 이름 NFS 또는 SMB 서버를 생성하려는 SVM의 이름입니다.	예	
DNS 도메인 이름 호스트-IP 이름 확인을 수행할 때 호스트 이름에 추가할 도메인 이름 목록입니다. 먼저 로컬 도메인을 나열한 다음 DNS 쿼리를 가장 자주 만드는 도메인 이름을 나열합니다.	예	

DNS 서버의 IP 주소 NFS 또는 SMB 서버의 이름 확인을 제공할 DNS 서버의 IP 주소 목록입니다. 나열된 DNS 서버에는 SMB 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. SRV 레코드는 서비스 이름을 해당 서비스를 제공하는 서버의 DNS 컴퓨터 이름에 매핑하는 데 사용됩니다. ONTAP가 로컬 DNS 쿼리를 통해 서비스 위치 레코드를 가져올 수 없는 경우 SMB 서버 생성이 실패합니다. ONTAP가 Active Directory SRV 레코드를 찾을 수 있도록 하는 가장 간단한 방법은 SVM DNS 서버로 Active Directory 통합 DNS 서버를 구성하는 것입니다. DNS 관리자가 Active Directory 도메인 컨트롤러에 대한 정보가 포함된 DNS 영역에 SRV 레코드를 수동으로 추가한 경우 Active Directory 통합 DNS 서버가 아닌 서버를 사용할 수 있습니다. Active Directory 통합 SRV 레코드에 대한 자세한 내용은 항목을 참조하십시오 "Microsoft TechNet의 Active Directory에 대한 DNS 지원 방법".	예	

동적 **DNS** 구성

동적 DNS를 사용하여 Active Directory 통합 DNS 서버에 DNS 항목을 자동으로 추가하려면 SVM에서 DDNS(동적 DNS)를 구성해야 합니다.

SVM의 모든 데이터 LIF에 대해 DNS 레코드가 생성됩니다. SVM에 여러 데이터 LIF를 생성하여 할당된 데이터 IP 주소에 클라이언트 연결을 로드 밸런싱할 수 있습니다. DNS 로드는 호스트 이름을 사용하여 생성된 연결을 라운드 로빈 방식으로 할당된 IP 주소로 조정합니다.

정보	요구한?	당신의 가치
SVM은 NFS 또는 SMB 서버를 생성할 SVM의 이름을 지정합니다.	예	
DDNS 사용 여부 DDNS 사용 여부를 지정합니다. SVM에 구성된 DNS 서버가 DDNS를 지원해야 합니다. 기본적으로 DDNS는 비활성화되어 있습니다.	예	
보안 DDNS 보안 DDNS 사용 여부는 Active Directory 통합 DNS에서만 지원됩니다. Active Directory 통합 DNS에서 보안 DDNS 업데이트만 허용하는 경우 이 매개 변수의 값은 참이어야 합니다. 기본적으로 보안 DDNS는 비활성화되어 있습니다. SVM을 위해 SMB 서버 또는 Active Directory 계정을 생성한 후에만 보안 DDNS를 활성화할 수 있습니다.	아니요	
DNS 도메인의 FQDN DNS 도메인의 FQDN 입니다. SVM에서 DNS 이름 서비스로 구성된 동일한 도메인 이름을 사용해야 합니다.	아니요	

네트워크 포트

ONTAP 네트워크 포트 구성에 대해 자세히 알아보십시오

포트는 물리적 포트(NIC) 또는 인터페이스 그룹 또는 VLAN과 같은 가상 포트입니다.

VLAN(Virtual Local Area Network) 및 인터페이스 그룹은 가상 포트를 구성합니다. 인터페이스 그룹은 여러 물리적 포트를 단일 포트로 취급하며 VLAN은 물리적 포트를 여러 개의 개별 논리 포트로 세분화합니다.

- 물리적 포트: LIF는 물리적 포트에서 직접 구성할 수 있습니다.
- 인터페이스 그룹: 단일 트렁크 포트로 작동하는 2개 이상의 물리적 포트를 포함하는 포트 애그리게이트. 인터페이스 그룹은 단일 모드, 다중 모드 또는 동적 다중 모드일 수 있습니다.
- VLAN: VLAN 태그 지정(IEEE 802.1Q 표준) 트래픽을 수신 및 전송하는 논리 포트입니다. VLAN 포트 특성에는 포트의 VLAN ID가 포함됩니다. 기본 물리적 포트 또는 인터페이스 그룹 포트는 VLAN 트렁크 포트로 간주되며 연결된 스위치 포트는 VLAN ID를 트렁킹하도록 구성해야 합니다.

  VLAN 포트의 기본 물리적 포트 또는 인터페이스 그룹 포트는 태그 없는 트래픽을 전송 및 수신하는 LIF를 계속 호스팅할 수 있습니다.

- 가상 IP(VIP) 포트: VIP LIF의 홈 포트로 사용되는 논리 포트입니다. VIP 포트는 시스템에서 자동으로 생성되며 제한된 수의 작업만 지원합니다. VIP 포트는 ONTAP 9.5부터 지원됩니다.

포트 명명 규칙은 _ enumberletter _ 입니다.

- 첫 번째 문자는 포트 유형을 나타냅니다. "e"는 이더넷을 나타냅니다.
- 두 번째 문자는 포트 어댑터가 있는 번호가 매겨진 슬롯을 나타냅니다.
- 세 번째 문자는 다중 포트 어댑터의 포트 위치를 나타냅니다. "a"는 첫 번째 포트를 나타내고, "b"는 두 번째 포트를 나타냅니다.

예를 들어, "e0b"은 이더넷 포트가 노드 마더보드의 두 번째 포트임을 나타냅니다.

VLAN은 'port_name-vlan-id' 구문을 사용하여 이름을 지정해야 합니다.

port_name은 물리적 포트 또는 인터페이스 그룹을 지정합니다.

VLAN-id는 네트워크의 VLAN 식별을 지정합니다. 예를 들어, "e1c-80"은 유효한 VLAN 이름입니다.

네트워크 포트를 구성합니다

물리적 포트를 결합하여 **ONTAP** 인터페이스 그룹을 생성합니다

LAG(Link Aggregation Group)라고도 하는 인터페이스 그룹은 동일한 노드에 있는 두 개 이상의 물리적 포트를 단일 논리 포트로 결합하여 생성됩니다. 논리 포트는 향상된 복구 성능, 향상된 가용성 및 로드 공유를 제공합니다.

인터페이스 그룹 유형입니다

스토리지 시스템에서는 단일 모드, 정적 멀티모드 및 동적 멀티모드 등 세 가지 유형의 인터페이스 그룹이 지원됩니다.

각 인터페이스 그룹은 서로 다른 수준의 내결함성을 제공합니다. 다중 모드 인터페이스 그룹은 네트워크 트래픽의 로드 밸런싱을 위한 방법을 제공합니다.

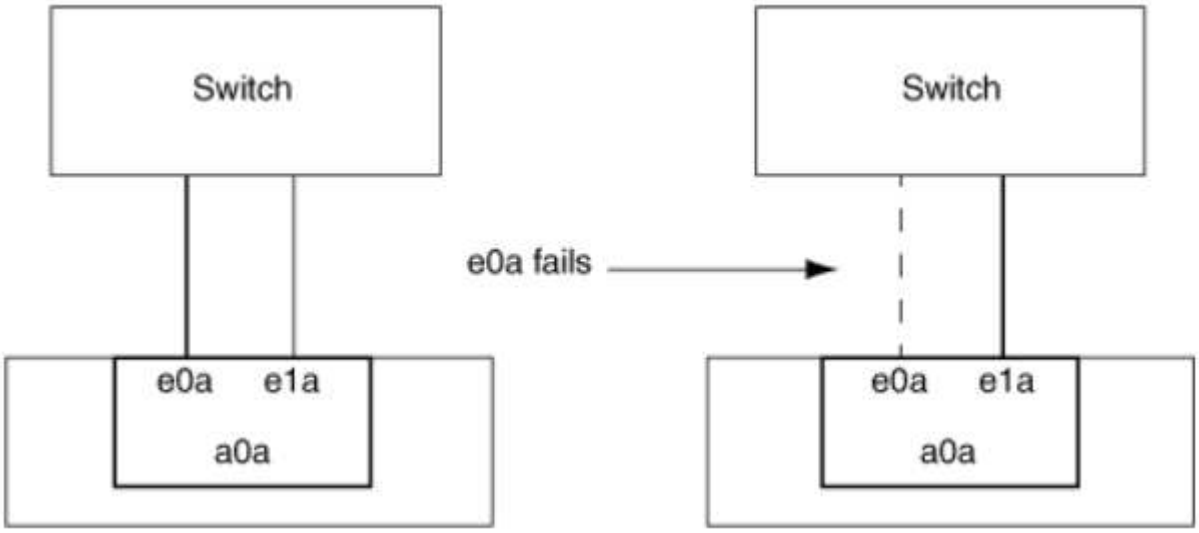
단일 모드 인터페이스 그룹의 특성

단일 모드 인터페이스 그룹에서는 인터페이스 그룹에 있는 인터페이스 중 하나만 활성화됩니다. 다른 인터페이스는 대기 상태이며 활성 인터페이스가 실패한 경우 대신 사용할 수 있습니다.

단일 모드 인터페이스 그룹의 특징:

- 페일오버의 경우 클러스터에서 액티브 링크를 모니터링하고 페일오버를 제어합니다. 클러스터가 액티브 링크를 모니터링하므로 스위치 구성이 필요하지 않습니다.
- 단일 모드 인터페이스 그룹에서 대기 중인 인터페이스가 두 개 이상 있을 수 있습니다.
- 단일 모드 인터페이스 그룹이 여러 스위치에 걸쳐 있는 경우 ISL(Inter-Switch Link)을 사용하여 스위치를 연결해야 합니다.
- 단일 모드 인터페이스 그룹의 경우 스위치 포트는 동일한 브로드캐스트 도메인에 있어야 합니다.
- 소스 주소가 0.0.0.0인 링크 모니터링 ARP 패킷은 포트를 통해 전송되어 포트가 동일한 브로드캐스트 도메인에 있는지 확인합니다.

다음 그림은 단일 모드 인터페이스 그룹의 예입니다. 그림에서 e0a 및 E1A는 a0a 단일 모드 인터페이스 그룹의 일부입니다. 활성 인터페이스인 e0a에 장애가 발생하면 대기 E1A 인터페이스가 스위치 연결을 대신 사용합니다.



> 단일 모드 기능을 수행하려면 페일오버 그룹을 사용하는 것이 좋습니다. 페일오버 그룹을 사용하면 다른 LIF에 두 번째 포트를 계속 사용할 수 있으며 사용하지 않은 상태로 둘 필요가 없습니다. 또한 페일오버 그룹은 2개 이상의 포트에 걸쳐 있을 수 있으며 여러 노드의 포트를 포괄할 수 있습니다.

정적 멀티모드 인터페이스 그룹의 특성

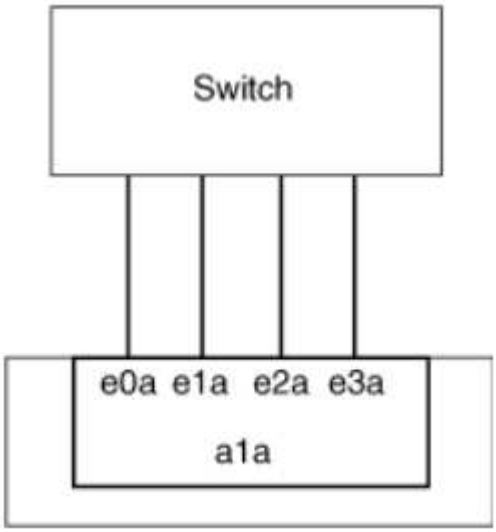
ONTAP의 정적 멀티모드 인터페이스 그룹 구현은 IEEE 802.3ad(정적)를 준수합니다. 집계를 지원하지만 집계를 구성하기 위한 제어 패킷 교환이 없는 스위치는 정적 멀티모드 인터페이스 그룹과 함께 사용할 수 있습니다.

정적 멀티모드 인터페이스 그룹은 LACP(Link Aggregation Control Protocol)라고도 하는 IEEE 802.3ad(동적)를 준수하지 않습니다. LACP는 Cisco의 독점 링크 통합 프로토콜인 PAgP(Port Aggregation Protocol)와 동일합니다.

다음은 정적 멀티모드 인터페이스 그룹의 특성입니다.

- 인터페이스 그룹의 모든 인터페이스가 활성 상태이고 단일 MAC 주소를 공유합니다.
  - 여러 개의 개별 연결이 인터페이스 그룹의 인터페이스 간에 분산됩니다.
  - 각 연결 또는 세션은 인터페이스 그룹 내에서 하나의 인터페이스를 사용합니다. 순차 로드 밸런싱 체계를 사용하면 모든 세션이 패킷 단위로 사용 가능한 링크 전체에 분산되며 인터페이스 그룹의 특정 인터페이스에 바인딩되지 않습니다.
- 정적 멀티모드 인터페이스 그룹은 최대 "n-1" 인터페이스의 오류에서 복구할 수 있습니다. 여기서 n은 인터페이스 그룹을 구성하는 총 인터페이스 수입니다.
- 포트에 장애가 발생하거나 연결이 끊어지면 장애가 발생한 링크를 통과하는 트래픽이 나머지 인터페이스 중 하나에 자동으로 재분배됩니다.
- 정적 멀티모드 인터페이스 그룹은 링크 손실을 감지할 수 있지만 연결 및 성능에 영향을 줄 수 있는 클라이언트 또는 스위치 구성 오류로 인한 연결 손실을 감지할 수 없습니다.
- 정적 멀티모드 인터페이스 그룹에는 여러 스위치 포트를 통한 Link Aggregation을 지원하는 스위치가 필요합니다. 인터페이스 그룹의 링크가 연결되는 모든 포트가 단일 논리 포트에 속하도록 스위치가 구성됩니다. 일부 스위치는 점보 프레임에 구성된 포트의 링크 집계를 지원하지 않을 수 있습니다. 자세한 내용은 스위치 공급업체의 설명서를 참조하십시오.
- 정적 멀티모드 인터페이스 그룹의 인터페이스 간에 트래픽을 분산하기 위해 몇 가지 로드 밸런싱 옵션을 사용할 수 있습니다.

다음 그림은 정적 멀티모드 인터페이스 그룹의 예입니다. 인터페이스 e0a, E1A, e2a 및 e3a는 A1A 다중 모드 인터페이스 그룹의 일부입니다. A1A 멀티모드 인터페이스 그룹의 4개 인터페이스가 모두 활성화됩니다.



단일 통합 링크의 트래픽을 여러 물리적 스위치에 분산하는 여러 기술이 존재합니다. 이 기능을 지원하는 데 사용되는 기술은 네트워킹 제품에 따라 다릅니다. ONTAP의 정적 멀티모드 인터페이스 그룹은 IEEE 802.3 표준을 준수합니다. 특정 다중 스위치 링크 통합 기술이 IEEE 802.3 표준과 상호 운용되거나 이를 준수한다고 말한다면 ONTAP와 함께 작동해야 합니다.

IEEE 802.3 표준에는 집계된 링크의 전송 장치가 전송할 물리적 인터페이스를 결정한다고 명시되어 있습니다. 따라서 ONTAP는 아웃바운드 트래픽을 분산하는 데만 책임이 있으며 인바운드 프레임이 도착하는 방식을 제어할 수 없습니다. 집계된 링크에서 인바운드 트래픽의 전송을 관리 또는 제어하려면 직접 연결된 네트워크 장치에서 해당 전송을 수정해야 합니다.

동적 멀티모드 인터페이스 그룹

동적 멀티모드 인터페이스 그룹은 직접 연결된 스위치에 그룹 구성원을 전달하기 위해 링크 통합 제어 프로토콜(LACP)을 구현합니다. LACP를 사용하면 링크 상태 손실과 노드가 직접 연결 스위치 포트와 통신할 수 없음을 감지할 수 있습니다.

ONTAP의 동적 멀티모드 인터페이스 그룹 구현은 IEEE 802.3 AD(802.1 AX)를 준수합니다. ONTAP는 Cisco의 독점 링크 집계 프로토콜인 PAgP(포트 집계 프로토콜)를 지원하지 않습니다.

동적 멀티모드 인터페이스 그룹에는 LACP를 지원하는 스위치가 필요합니다.

ONTAP는 활성 모드 또는 수동 모드로 구성된 스위치와 잘 작동하는 구성 불가능한 활성 모드에서 LACP를 구현합니다. ONTAP는 IEEE 802.3 AD(802.1ax)에 지정된 대로 긴 LACP 타이머 및 짧은 LACP 타이머(구성 불가능한 값 3초 및 90초용)를 구현합니다.

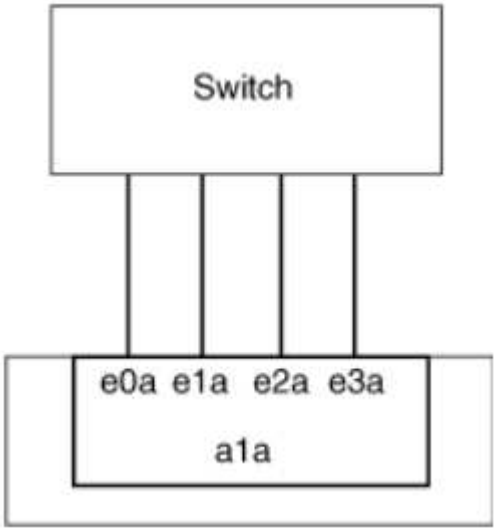
ONTAP 로드 밸런싱 알고리즘은 아웃바운드 트래픽 전송에 사용할 구성원 포트를 결정하며 인바운드 프레임 수신 방식을 제어하지 않습니다. 스위치는 스위치의 포트 채널 그룹에 구성된 로드 밸런싱 알고리즘에 따라 전송에 사용할 포트 채널 그룹의 구성원(개별 물리적 포트)을 결정합니다. 따라서 스위치 구성에 따라 트래픽을 수신할 스토리지 시스템의 구성원 포트(개별 물리적 포트)가 결정됩니다. 스위치 구성에 대한 자세한 내용은 스위치 공급업체의 설명서를 참조하십시오.

개별 인터페이스에서 연속적인 LACP 프로토콜 패킷을 수신하지 못하면 해당 개별 인터페이스는 "ifgrp status" 명령 출력에서 "lag_inactive"로 표시됩니다. 기존 트래픽은 나머지 활성 인터페이스로 자동으로 재라우팅됩니다.

동적 멀티모드 인터페이스 그룹을 사용할 때 다음 규칙이 적용됩니다.

- 동적 멀티모드 인터페이스 그룹은 포트 기반, IP 기반, MAC 기반 또는 라운드 로빈 로드 밸런싱 방법을 사용하도록 구성되어야 합니다.
- 동적 멀티모드 인터페이스 그룹에서 모든 인터페이스는 활성 상태이고 단일 MAC 주소를 공유해야 합니다.

다음 그림은 동적 멀티모드 인터페이스 그룹의 예입니다. 인터페이스 e0a, E1A, e2a 및 e3a는 A1A 다중 모드 인터페이스 그룹의 일부입니다. A1A 동적 멀티모드 인터페이스 그룹의 4개 인터페이스가 모두 활성화됩니다.



다중 모드 인터페이스 그룹의 로드 밸런싱

IP 주소, MAC 주소, 순차 또는 포트 기반 로드 밸런싱 방법을 사용하여 다중 모드 인터페이스 그룹의 네트워크 포트를 통해 네트워크 트래픽을 균등하게 분산함으로써 나가는 트래픽에 다중 모드 인터페이스 그룹의 모든 인터페이스가

동일하게 사용되도록 할 수 있습니다.

다중 모드 인터페이스 그룹에 대한 로드 밸런싱 방법은 인터페이스 그룹이 생성된 경우에만 지정할 수 있습니다.

- 모범 사례 *: 가능하면 포트 기반 로드 밸런싱이 권장됩니다. 네트워크에서 포트 기반 로드 밸런싱을 사용하는 것이 금지되는 특별한 이유 또는 제한이 없는 경우.

포트 기반 로드 밸런싱

포트 기반 로드 밸런싱이 권장되는 방법입니다.

포트 기반 로드 밸런싱 방법을 사용하여 전송 계층(TCP/UDP) 포트를 기반으로 다중 모드 인터페이스 그룹의 트래픽을 균등화할 수 있습니다.

포트 기반 로드 밸런싱 방법은 전송 계층 포트 번호와 함께 소스 및 대상 IP 주소에 대한 빠른 해싱 알고리즘을 사용합니다.

IP 주소 및 **MAC** 주소 로드 밸런싱

IP 주소 및 MAC 주소 로드 밸런싱은 다중 모드 인터페이스 그룹의 트래픽을 균등하게 조정하는 방법입니다.

이러한 로드 밸런싱 방법은 소스 및 대상 주소(IP 주소 및 MAC 주소)에서 빠른 해싱 알고리즘을 사용합니다. 해싱 알고리즘의 결과가 UP 링크 상태가 아닌 인터페이스에 매핑되면 다음 활성 인터페이스가 사용됩니다.

> 라우터에 직접 연결하는 시스템에 인터페이스 그룹을 생성할 때 MAC 주소 로드 밸런싱 방법을 선택하지 마십시오. 이러한 설정에서 모든 발신 IP 프레임에 대해 대상 MAC 주소는 라우터의 MAC 주소입니다. 따라서 인터페이스 그룹의 인터페이스가 하나만 사용됩니다.

IP 주소 로드 밸런싱은 IPv4와 IPv6 주소 모두에서 동일한 방식으로 작동합니다.

순차적 로드 밸런싱

순차 로드 밸런싱을 사용하여 라운드 로빈 알고리즘을 사용하여 여러 링크 간에 패킷을 균등하게 분산할 수 있습니다. 순차적 옵션을 사용하여 단일 연결의 트래픽을 여러 링크에서 로드 밸런싱하여 단일 연결 처리량을 높일 수 있습니다.

그러나 순차적 로드 밸런싱으로 인해 순서가 잘못된 패킷 전달이 발생할 수 있기 때문에 성능이 매우 저하될 수 있습니다. 따라서 순차적 로드 밸런싱은 일반적으로 권장되지 않습니다.

인터페이스 그룹 또는 **LAG**를 만듭니다

인터페이스 그룹 또는 LAG(단일 모드, 정적 멀티모드 또는 동적 멀티모드(LACP))를 생성하여 집계된 네트워크 포트의 기능을 결합하여 클라이언트에 단일 인터페이스를 제공할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 LAG * 를 만듭니다

단계

1. LAG를 만들려면 네트워크 > 이더넷 포트 > + Link Aggregation Group * 을 선택합니다.
2. 드롭다운 목록에서 노드를 선택합니다.
3. 다음 중에서 선택합니다.
   a. ONTAP to * automatically select broadcast domain (recommended) *.
   b. 브로드캐스트 도메인을 수동으로 선택합니다.
4. LAG를 구성할 포트를 선택합니다.
5. 모드를 선택합니다.
   a. 단일: 한 번에 하나의 포트만 사용됩니다.
   b. 다중: 모든 포트를 동시에 사용할 수 있습니다.
   c. LACP: LACP 프로토콜이 사용할 수 있는 포트를 결정합니다.
6. 로드 밸런싱 선택:
   a. IP 기반
   b. Mac 기반
   c. 포트
   d. 순차적
7. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹을 생성합니다 *

다중 모드 인터페이스 그룹을 생성할 때 다음 로드 밸런싱 방법 중 하나를 지정할 수 있습니다.

- 포트 : 네트워크 트래픽은 전송 계층(TCP/UDP) 포트를 기반으로 분산됩니다. 이것은 권장되는 로드 밸런싱 방법입니다.
- MAC 주소 기준으로 네트워크 트래픽이 분산된다.
- IP: 네트워크 트래픽은 IP 주소를 기반으로 분산됩니다.
- '등전위': 네트워크 트래픽이 수신될 때 분산됩니다.

> 인터페이스 그룹의 MAC 주소는 기본 포트의 순서 및 부팅 시 이러한 포트가 초기화되는 방식에 따라 결정됩니다. 따라서 재부팅 또는 ONTAP 업그레이드 시 ifgrp MAC 주소가 영구하다고 가정해서는 안 됩니다.

단계

interface group을 생성하기 위해 'network port ifgrp create' 명령어를 사용한다.

인터페이스 그룹의 이름은 "a<number><letter>" 구문을 사용하여 지정해야 합니다. 예를 들어, a0a, a0b, A1c 및

A2A는 유효한 인터페이스 그룹 이름입니다.

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

다음 예에서는 포트 및 다중 모드 분산 기능을 사용하여 a0a라는 인터페이스 그룹을 만드는 방법을 보여 줍니다.

'network port ifgrp create-node_cluster-1-01_-ifgrp_a0a_-Distr-func_port_-mode_multimode_'

인터페이스 그룹 또는 **LAG**에 포트를 추가합니다

모든 포트 속도에 대해 인터페이스 그룹 또는 LAG에 최대 16개의 물리적 포트를 추가할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 LAG*에 포트를 추가합니다

단계

1. LAG를 편집하려면 * 네트워크 > 이더넷 포트 > LAG * 를 선택합니다.
2. LAG에 추가할 같은 노드의 추가 포트를 선택합니다.
3. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹에 포트를 추가합니다 *

단계

인터페이스 그룹에 네트워크 포트를 추가합니다.

'network port ifgrp add-port'를 참조하십시오

다음 예에서는 a0a라는 인터페이스 그룹에 e0c 포트를 추가하는 방법을 보여줍니다.

'network port ifgrp add-port-node_cluster-1-01_-ifgrp_a0a_-port_e0c_'

ONTAP 9.8부터 인터페이스 그룹은 인터페이스 그룹에 첫 번째 물리적 포트가 추가된 후 약 1분 후에 적절한 브로드캐스트 도메인에 자동으로 배치됩니다. ONTAP가 이 작업을 수행하지 않도록 하고 ifgrp를 브로드캐스트 도메인에 수동으로 배치하려는 경우에는 '-skip-broadcast-domain-placement' 매개 변수를 'ifgrp add-port' 명령의 일부로 지정합니다.

에서 포트 인터페이스 그룹에 적용되는 및 구성 제한에 대해 자세히 `network port ifgrp add-port`"ONTAP 명령 참조입니다" 알아보십시오.

인터페이스 그룹 또는 **LAG**에서 포트를 제거합니다

인터페이스 그룹의 마지막 포트가 아닌 경우 LIF를 호스팅하는 인터페이스 그룹에서 포트를 제거할 수 있습니다. 인터페이스 그룹에서 마지막 포트를 제거하지 않는 점을 고려할 때 인터페이스 그룹이 LIF를 호스팅하거나 인터페이스 그룹이 LIF의 홈 포트가 아니어야 합니다. 그러나 마지막 포트를 제거하는 경우 먼저 인터페이스 그룹에서 LIF를 마이그레이션하거나 이동해야 합니다.

이 작업에 대해

인터페이스 그룹 또는 LAG에서 최대 16개의 포트(물리적 인터페이스)를 제거할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- 시스템 관리자를 사용하여 LAG*에서 포트를 제거합니다

단계

1. LAG를 편집하려면 * 네트워크 > 이더넷 포트 > LAG * 를 선택합니다.
2. LAG에서 제거할 포트를 선택합니다.
3. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹에서 포트를 제거합니다 *

단계

인터페이스 그룹에서 네트워크 포트 제거:

'network port ifgrp remove-port

에 대한 자세한 내용은 `network port ifgrp remove-port` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예는 a0a라는 인터페이스 그룹에서 포트 e0c를 제거하는 방법을 보여줍니다.

'network port ifgrp remove-port-node_cluster-1-01_-ifgrp_a0a_-port_e0c_'

인터페이스 그룹 또는 **LAG**를 삭제합니다

기본 물리적 포트에서 직접 LIF를 구성하거나 인터페이스 그룹, LAG 모드 또는 배포 기능을 변경하려는 경우 인터페이스 그룹 또는 LAG를 삭제할 수 있습니다.

시작하기 전에

- 인터페이스 그룹 또는 LAG가 LIF를 호스팅하지 않아야 합니다.
- 인터페이스 그룹 또는 LAG는 LIF의 홈 포트나 페일오버 타겟이 아니어야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- 시스템 관리자를 사용하여 LAG * 를 삭제합니다

단계

1. LAG를 삭제하려면 * 네트워크 > 이더넷 포트 > LAG * 를 선택합니다.
2. 제거할 LAG를 선택합니다.
3. LAG를 삭제합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹을 삭제합니다 *

단계

interface group을 삭제하려면 network port ifgrp delete 명령을 사용한다.

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

다음 예에서는 a0b라는 인터페이스 그룹을 삭제하는 방법을 보여줍니다.

'network port ifgrp delete-node_cluster-1-01_-ifgrp_a0b_'

물리적 포트를 통해 **ONTAP VLAN**을 구성합니다

ONTAP의 VLAN을 사용하여 물리적 경계에 정의된 기존 브로드캐스트 도메인과 달리 스위치 포트 단위로 정의된 별도의 브로드캐스트 도메인을 생성하여 네트워크의 논리적 분할을 제공할 수 있습니다.

VLAN은 여러 물리적 네트워크 세그먼트에 걸쳐 있을 수 있습니다. VLAN에 속한 엔드스테이션은 기능 또는 애플리케이션에 의해 관련된다.

예를 들어, VLAN의 최종 스테이션은 엔지니어링 및 회계 등의 부서 또는 릴리스1 및 릴리스2와 같은 프로젝트별로 그룹화할 수 있습니다. 최종 스테이션의 물리적 근접성이 VLAN에 반드시 필요한 것은 아니므로, 최종 스테이션을 지리적으로 분산시키고 스위치 네트워크에 브로드캐스트 도메인을 포함할 수 있습니다.

ONTAP 9.14.1 및 9.13.1에서는 논리 인터페이스(LIF)에서 사용되지 않고 연결된 스위치에서 기본 VLAN 연결이 없는 태그가 지정되지 않은 포트는 저하된 것으로 표시됩니다. 이는 사용되지 않는 포트를 식별하는 데 도움이 되며, 서비스 중단을 나타내는 것은 아닙니다. 네이티브 VLAN은 ONTAP CFM 브로드캐스트와 같은 ifgrp 기반 포트에서 태그가 지정되지 않은 트래픽을 허용합니다. 태그가 지정되지 않은 트래픽이 차단되는 것을 방지하려면 스위치에 네이티브 VLAN을 구성합니다.

VLAN에 대한 정보를 생성, 삭제 또는 표시하여 VLAN을 관리할 수 있습니다.

> 스위치의 네이티브 VLAN과 ID가 동일한 네트워크 인터페이스에 VLAN을 생성해서는 안 됩니다. 예를 들어, 네트워크 인터페이스 e0b가 네이티브 VLAN 10에 있는 경우 해당 인터페이스에 VLAN e0b-10을 생성할 수 없습니다.

VLAN을 생성합니다

System Manager 또는 'network port vlan create' 명령을 사용하여 동일한 네트워크 도메인 내에서 별도의 브로드캐스트 도메인을 유지 관리하기 위한 VLAN을 생성할 수 있습니다.

시작하기 전에

다음 요구 사항이 충족되었는지 확인합니다.

- 네트워크에 배포된 스위치는 IEEE 802.1Q 표준을 준수하거나 공급업체별로 VLAN을 구현해야 합니다.
- 여러 VLAN을 지원하려면 하나 이상의 VLAN에 속하도록 최종 스테이션을 정적으로 구성해야 합니다.
- VLAN이 클러스터 LIF를 호스팅하는 포트에 연결되어 있지 않습니다.
- VLAN이 클러스터 IPspace에 할당된 포트에 연결되어 있지 않습니다.
- VLAN은 구성원 포트가 없는 인터페이스 그룹 포트에 생성되지 않습니다.

이 작업에 대해

VLAN을 생성하면 클러스터에 있는 지정된 노드의 네트워크 포트에 VLAN이 연결됩니다.

처음으로 포트를 통해 VLAN을 구성할 때 포트가 다운되어 일시적으로 네트워크 연결이 끊길 수 있습니다. 이후에 동일한 포트에 VLAN을 추가해도 포트 상태는 영향을 받지 않습니다.

> 스위치의 네이티브 VLAN과 ID가 동일한 네트워크 인터페이스에 VLAN을 생성해서는 안 됩니다. 예를 들어, 네트워크 인터페이스 e0b가 네이티브 VLAN 10에 있는 경우 해당 인터페이스에 VLAN e0b-10을 생성할 수 없습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 VLAN * 을 생성합니다

ONTAP 9.12.0부터는 자동으로 브로드캐스트 도메인을 선택하거나 목록에서 On을 수동으로 선택할 수 있습니다. 이전에는 2계층 연결을 기반으로 브로드캐스트 도메인이 항상 자동으로 선택되었습니다. 브로드캐스트 도메인을 수동으로 선택하면 브로드캐스트 도메인을 수동으로 선택하면 연결이 끊기라는 경고가 나타납니다.

단계

1. 네트워크 > 이더넷 포트 > + VLAN * 을 선택합니다.
2. 드롭다운 목록에서 노드를 선택합니다.
3. 다음 중에서 선택합니다.
   a. ONTAP to * automatically select broadcast domain (recommended) *.
   b. 목록에서 브로드캐스트 도메인을 수동으로 선택합니다.
4. VLAN을 구성할 포트를 선택합니다.
5. VLAN ID를 지정합니다.
6. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 VLAN * 을 생성합니다

하드웨어 문제나 소프트웨어 구성 오류를 해결하지 않고 성능 저하 포트에 VLAN 포트를 생성하려면 네트워크 포트 수정 명령의 '-ignore-health-status' 매개변수를 TRUE로 설정해야 합니다.

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

단계

1. 'network port vlan create' 명령어를 사용하여 VLAN을 생성한다.
2. VLAN을 생성할 때는 VLAN-name이나 port, vlan-id 옵션을 지정해야 합니다. VLAN 이름은 포트 이름(또는 인터페이스 그룹)과 네트워크 스위치 VLAN 식별자의 조합으로, 사이에 하이픈을 사용합니다. 예를 들어, "e0c-24"와 "e1c-80"은 유효한 VLAN 이름입니다.

다음 예에서는 노드 cluster-1-01의 네트워크 포트 e1c에 연결된 VLAN e1c-80을 생성하는 방법을 보여 줍니다.

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

ONTAP 9.8부터 VLAN은 생성 후 1분 정도 적절한 브로드캐스트 도메인에 자동으로 배치됩니다. ONTAP가 이 작업을 수행하지 않고 수동으로 VLAN을 브로드캐스트 도메인에 배치하려는 경우 "VLAN create" 명령의 일부로 '-skip-broadcast-domain-placement' 매개 변수를 지정합니다.

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

VLAN을 편집합니다

브로드캐스트 도메인을 변경하거나 VLAN을 비활성화할 수 있습니다.

System Manager를 사용하여 VLAN을 편집합니다

ONTAP 9.12.0부터는 자동으로 브로드캐스트 도메인을 선택하거나 목록에서 On을 수동으로 선택할 수 있습니다. 이전의 브로드캐스트 도메인은 항상 계층 2 연결을 기반으로 자동으로 선택되었습니다. 브로드캐스트 도메인을 수동으로 선택하면 브로드캐스트 도메인을 수동으로 선택하면 연결이 끊기라는 경고가 나타납니다.

단계

1. 네트워크 > 이더넷 포트 > VLAN * 을 선택합니다.
2. 편집 아이콘을 선택합니다.
3. 다음 중 하나를 수행합니다.
    - 목록에서 다른 도메인을 선택하여 브로드캐스트 도메인을 변경합니다.
    - 사용 * 확인란의 선택을 취소합니다.
4. 변경 사항을 저장합니다.

VLAN을 삭제한다

NIC를 슬롯에서 제거하기 전에 VLAN을 삭제해야 할 수 있습니다. VLAN을 삭제하면 해당 VLAN을 사용하는 모든 페일오버 규칙 및 그룹에서 자동으로 제거됩니다.

시작하기 전에

VLAN에 연결된 LIF가 없는지 확인합니다.

이 작업에 대해

포트에서 마지막 VLAN을 삭제하면 네트워크에서 일시적으로 연결이 끊길 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 VLAN을 삭제합니다 *

단계

1. 네트워크 > 이더넷 포트 > VLAN * 을 선택합니다.
2. 제거할 VLAN을 선택합니다.
3. 삭제 * 를 클릭합니다.

CLI를 참조하십시오

- CLI를 사용하여 VLAN * 을 삭제합니다

단계

VLAN을 삭제하려면 network port vlan delete 명령을 사용한다.

다음 예에서는 노드 cluster-1-01의 네트워크 포트 e1c에서 VLAN e1c-80을 삭제하는 방법을 보여 줍니다.

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

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

ONTAP 네트워크 포트 특성을 수정합니다

물리적 네트워크 포트의 자동 협상, 이중, 흐름 제어, 속도 및 상태 설정을 수정할 수 있습니다.

시작하기 전에

수정할 포트가 LIF를 호스팅하지 않아야 합니다.

이 작업에 대해

- 100GbE, 40GbE, 10GbE 또는 1GbE 네트워크 인터페이스의 관리 설정을 수정하지 않는 것이 좋습니다.

  이중 모드 및 포트 속도에 대해 설정한 값을 관리 설정이라고 합니다. 네트워크 제한에 따라 관리 설정은 작동 설정과 다를 수 있습니다(즉, 포트가 실제로 사용하는 이중 모드 및 속도).

- 인터페이스 그룹에 있는 기본 물리적 포트의 관리 설정을 수정하지 않는 것이 좋습니다.

  '-up-admin' 매개 변수(고급 권한 수준에서 사용 가능)는 포트의 관리 설정을 수정합니다.

- 노드의 모든 포트 또는 노드의 마지막 운영 클러스터 LIF를 호스팅하는 포트에 대해 '-up-admin' 관리 설정을 false로 설정하지 않는 것이 좋습니다.
- 관리 포트 e0M의 MTU 크기를 수정하지 않는 것이 좋습니다.
- 브로드캐스트 도메인에 있는 포트의 MTU 크기는 브로드캐스트 도메인에 설정된 MTU 값에서 변경할 수 없습니다.
- VLAN의 MTU 크기는 기본 포트의 MTU 크기 값을 초과할 수 없습니다.

단계

1. 네트워크 포트의 속성을 수정합니다.

   네트워크 포트 수정

2. 시스템이 지정된 포트의 네트워크 포트 상태를 무시하도록 지정하려면 '-ignore-health-status' 필드를 true로 설정합니다.

   네트워크 포트 상태가 성능 저하에서 정상 상태로 자동으로 변경되고 이 포트를 LIF를 호스팅하는 데 사용할 수 있습니다. 클러스터 포트의 흐름 제어를 "없음"으로 설정해야 합니다. 기본적으로 흐름 제어는 'full'로 설정됩니다.

다음 명령을 실행하면 흐름 제어를 none으로 설정하여 포트 e0b의 흐름 제어가 비활성화됩니다.

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

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

40GbE NIC 포트를 변환하여 **ONTAP** 네트워크용 **10GbE** 포트를 생성합니다

X1144A-R6 및 X91440A-R6 40GbE 네트워크 인터페이스 카드(NIC)를 4개의 10GbE 포트를 지원하도록 변환할 수 있습니다.

이러한 NIC 중 하나를 지원하는 하드웨어 플랫폼을 10GbE 클러스터 인터커넥트 및 고객 데이터 연결을 지원하는 클러스터에 연결하는 경우 NIC를 변환하여 필요한 10GbE 연결을 제공해야 합니다.

시작하기 전에

지원되는 브레이크아웃 케이블을 사용해야 합니다.

이 작업에 대해

NIC를 지원하는 전체 플랫폼 목록은 를 참조하십시오 "Hardware Universe".

> X1144A-R6 NIC에서는 포트 A만 10GbE 연결 4개를 지원하도록 변환할 수 있습니다. 포트 A가 변환되면 포트 e를 사용할 수 없습니다.

단계

1. 유지보수 모드로 전환합니다.
2. NIC를 40GbE 지원에서 10GbE 지원으로 변환합니다.

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. convert 명령을 사용한 후 노드를 중단한다.
4. 케이블을 설치하거나 변경합니다.
5. 하드웨어 모델에 따라 SP(서비스 프로세서) 또는 BMC(베이스보드 관리 컨트롤러)를 사용하여 변환을 적용하기 위해 노드 전원을 껐다가 켭니다.

ONTAP 네트워크를 위해 **UTA X1143A-R6** 포트를 구성합니다

기본적으로 X1143A-R6 유니파이드 타겟 어댑터는 FC 타겟 모드로 구성되지만, 포트를 10Gb 이더넷 및 FCoE(CNA) 포트 또는 16Gb FC 이니시에이터 또는 타겟 포트로 구성할 수 있습니다. 여기에는 다른 SFP+ 어댑터가 필요합니다.

이더넷 및 FCoE용으로 구성된 경우 X1143A-R6 어댑터는 동일한 10GbE 포트에서 동시 NIC 및 FCoE 타겟 트래픽을 지원합니다. FC용으로 구성한 경우 동일한 ASIC를 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. 동일한 ASIC에 연결된 포트 쌍은 같은 모드로 구성해야 합니다.

FC 모드에서 X1143A-R6 어댑터는 최대 16Gbps의 속도를 제공하는 기존 FC 장치와 동일하게 작동합니다. CNA 모드에서 X1143A-R6 어댑터를 사용하여 동일한 10GbE 포트를 공유하는 동시 NIC 및 FCoE 트래픽을 공유할 수 있습니다. CNA 모드는 FCoE 기능에 대해 FC 타겟 모드만 지원합니다.

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

단계

1. 포트 구성 보기:

```
system hardware unified-connect show
```

2. FC(Fibre Channel) 또는 CNA(Converged Network Adapter)에 필요한 포트를 구성합니다.

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. FC 또는 10Gb 이더넷에 적합한 케이블을 연결합니다.
4. 올바른 SFP+가 설치되었는지 확인합니다.

```
network fcp adapter show -instance -node -adapter
```

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

ONTAP 네트워크에서 사용할 **UTA2** 포트를 변환합니다

UTA2 포트를 CNA(Converged Network Adapter) 모드에서 파이버 채널(FC) 모드로 전환하거나 그 반대로 전환할 수 있습니다.

포트를 네트워크에 연결하거나 FC 이니시에이터 및 타겟을 지원하는 물리적 미디어를 변경해야 하는 경우 UTA2 속성을 CNA 모드에서 FC 모드로 변경해야 합니다.

CNA 모드에서 FC 모드로 전환

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.
     - LIF를 이동하거나, ifgrp에서 포트를 제거하거나, VLAN을 각각 삭제합니다.
     - 명령을 실행하여 포트를 수동으로 삭제합니다 `network port delete`. 명령이 실패하면 `network port delete` 관리자가 오류를 해결한 다음 명령을 다시 실행해야 합니다.
   - 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 명령을 사용하여 수동으로 포트를 제거해야 `network port delete` 합니다.

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

5. 올바른 SFP+가 설치되었는지 확인합니다.

```
network fcp adapter show -instance -node -adapter
```

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

FC 모드에서 CNA 모드로 전환합니다

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 cna
```

3. 노드를 재부팅합니다
4. 올바른 SFP+가 설치되었는지 확인합니다.

   CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다.

ONTAP 네트워크의 **CNA/UTA2** 광 모듈을 변환합니다

어댑터에 대해 선택한 퍼스낼리티 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 퍼스낼리티 모드(FC 또는 CNA) 광학장치에 맞는 모듈을 삽입합니다.
4. 올바른 SFP+가 설치되었는지 확인합니다.

   ```
   network fcp adapter show -instance -node -adapter
   ```

   지원되는 SFP+ 모듈 및 Cisco Twinax(Copper) 케이블이 에 나열되어 있습니다 "NetApp Hardware Universe를 참조하십시오".

ONTAP 클러스터 노드에서 **NIC** 제거

유지 관리를 위해 결함이 있는 NIC를 슬롯에서 제거하거나 NIC를 다른 슬롯으로 이동해야 할 수 있습니다.

> NIC 제거 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 ONTAP 클러스터 노드에서 NIC를 제거해야 하는 경우 절차를 "노드에서 NIC 제거(ONTAP 9.7 이하)"참조하십시오.

단계

1. 노드 전원을 끕니다.

2. 슬롯에서 NIC를 물리적으로 분리합니다.
3. 노드의 전원을 켭니다.
4. 포트가 삭제되었는지 확인합니다.

```
network port show
```

> ONTAP는 모든 인터페이스 그룹에서 포트를 자동으로 제거합니다. 포트가 인터페이스 그룹의 유일한 구성원인 경우 인터페이스 그룹이 삭제됩니다. 에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 포트에 구성된 VLAN이 있으면 포트가 교체된 것입니다. 다음 명령을 사용하여 교체된 VLAN을 볼 수 있습니다.

```
cluster controller-replacement network displaced-vlans show
```

> dissplac된 interface show, dissplac된-vlan show, dissplac된-vLANs restore 명령은 고유하며 클러스터 컨트롤러 교체 네트워크로 시작하는 정규화된 명령 이름이 필요하지 않습니다.

6. 이러한 VLAN은 삭제되지만 다음 명령을 사용하여 복원할 수 있습니다.

```
displaced-vlans restore
```

7. 포트에 LIF가 구성되어 있는 경우 ONTAP는 동일한 브로드캐스트 도메인의 다른 포트에 있는 LIF에 대한 새 홈 포트를 자동으로 선택합니다. 동일한 파일러에 적절한 홈 포트가 없으면 해당 LIF가 교체된 것으로 간주됩니다. 다음 명령을 사용하여 교체된 LIF를 볼 수 있습니다.

   디시퍼인터페이스 쇼

8. 새 포트가 같은 노드의 브로드캐스트 도메인에 추가되면 LIF의 홈 포트가 자동으로 복원됩니다. 또는 네트워크 인터페이스 modify-home-port-home-node를 사용하여 홈 포트를 설정하거나 교체된 인터페이스 restore 명령을 사용할 수 있습니다.

관련 정보

- "클러스터 컨트롤러 교체 네트워크 - 인터페이스 삭제"
- "네트워크 인터페이스 수정"

네트워크 포트를 모니터링합니다

ONTAP 네트워크 포트의 상태를 모니터링합니다

ONTAP의 네트워크 포트 관리에는 자동 상태 모니터링 및 LIF 호스팅에 적합하지 않은 네트워크 포트를 식별하는 데 도움이 되는 상태 모니터링 세트가 포함됩니다.

이 작업에 대해

상태 모니터에서 네트워크 포트가 정상 상태가 아닌 것으로 확인되면 EMS 메시지를 통해 관리자에게 경고를

표시하거나 해당 포트를 성능 저하로 표시합니다. ONTAP는 해당 LIF에 대한 정상적인 대체 페일오버 대상이 있을 경우 성능이 저하된 네트워크 포트에서 LIF를 호스팅하지 않습니다. 링크 플래핑(링크가 위아래로 빠르게 튀어 나며 튀어 나며 튀어 나오는 경우) 또는 네트워크 파티셔닝과 같은 소프트 장애 이벤트로 인해 포트의 성능이 저하될 수 있습니다.

- 클러스터 IPspace의 네트워크 포트는 브로드캐스트 도메인의 다른 네트워크 포트에 대한 링크 플래핑 또는 L2(계층 2) 재연결이 끊어지면 성능이 저하된 것으로 표시됩니다.
- 클러스터 이외의 IPspace의 네트워크 포트는 링크 플래핑 기능이 있을 때 성능이 저하된 것으로 표시됩니다.

성능이 저하된 포트의 다음과 같은 동작을 알고 있어야 합니다.

- 성능이 저하된 포트는 VLAN 또는 인터페이스 그룹에 포함될 수 없습니다.

  인터페이스 그룹의 구성원 포트가 성능 저하로 표시되어 있지만 인터페이스 그룹이 계속 정상 상태로 표시되어 있는 경우 해당 인터페이스 그룹에서 LIF를 호스팅할 수 있습니다.

- LIF는 성능이 저하된 포트에서 정상 포트로 자동 마이그레이션됩니다.
- 페일오버 이벤트 중에 성능 저하된 포트는 페일오버 타겟으로 간주되지 않습니다. 정상 상태의 포트를 사용할 수 없는 경우 성능이 저하된 포트 호스트 LIF는 일반 페일오버 정책에 따라 작동합니다.
- LIF를 생성, 마이그레이션 또는 성능이 저하된 포트로 되돌릴 수 없습니다.

  네트워크 포트의 '상태 무시' 설정을 '참'으로 수정할 수 있습니다. 그런 다음 양호한 포트에서 LIF를 호스팅할 수 있습니다.

단계

1. 고급 권한 모드로 로그인합니다.

   ```
   set -privilege advanced
   ```

2. 네트워크 포트 상태 모니터링을 위해 활성화된 상태 모니터를 확인합니다.

   ```
   network options port-health-monitor show
   ```

   포트의 상태는 상태 모니터의 값에 의해 결정됩니다.

   ONTAP에서는 기본적으로 다음 상태 모니터를 사용할 수 있으며 사용하도록 설정되어 있습니다.

   - 링크 플래핑 상태 모니터: 링크 플래핑 모니터링

     포트에 5분 내에 두 번 이상 링크 플래핑이 있는 경우 이 포트는 성능 저하로 표시됩니다.

   - L2 연결 상태 모니터: 동일한 브로드캐스트 도메인에 구성된 모든 포트가 서로 L2 연결 가능 여부를 모니터링합니다

     이 상태 모니터는 모든 IPspace에서 L2 도달 가능성 문제를 보고하지만 클러스터 IPspace의 포트만 성능 저하로 표시합니다.

   - CRC 모니터: 포트에서 CRC 통계를 모니터링합니다

이 상태 모니터는 포트를 성능 저하로 표시하지 않지만 매우 높은 CRC 실패율이 관찰되면 EMS 메시지를 생성합니다.

에 대한 자세한 내용은 `network options port-health-monitor show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 'network options port-health-monitor modify' 명령을 사용하여 원하는 대로 IPspace에 대한 상태 모니터를 사용하거나 사용하지 않도록 설정합니다.

   에 대한 자세한 내용은 `network options port-health-monitor modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 포트의 세부 상태를 봅니다.

```
network port show -health
```

명령 출력에는 포트의 상태, '상태 무시' 설정 및 포트가 성능 저하로 표시된 이유 목록이 표시됩니다.

항만 건강상태는 건강하거나 등급이 매겨질 수 있다.

상태 무시 설정이 참이면 항만 상태가 평가됨에서 건강으로 변경되었음을 나타냅니다.

상태 무시 설정이 false이면 포트 상태는 시스템에 의해 자동으로 결정됩니다.

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

ONTAP 네트워크 포트의 연결 상태를 모니터링합니다

내후성 모니터링은 ONTAP 9.8 이상에 내장되어 있습니다. 이 모니터링을 사용하여 물리적 네트워크 토폴로지가 ONTAP 구성과 일치하지 않는 시점을 식별할 수 있습니다. 경우에 따라 ONTAP에서 포트 연결을 복구할 수 있습니다. 다른 경우에는 추가 단계가 필요합니다.

이 작업에 대해

다음 명령을 사용하여 물리적 케이블 연결 또는 네트워크 스위치 구성과 일치하지 않는 ONTAP 구성에서 비롯되는 네트워크 구성 오류를 확인, 진단 및 복구할 수 있습니다.

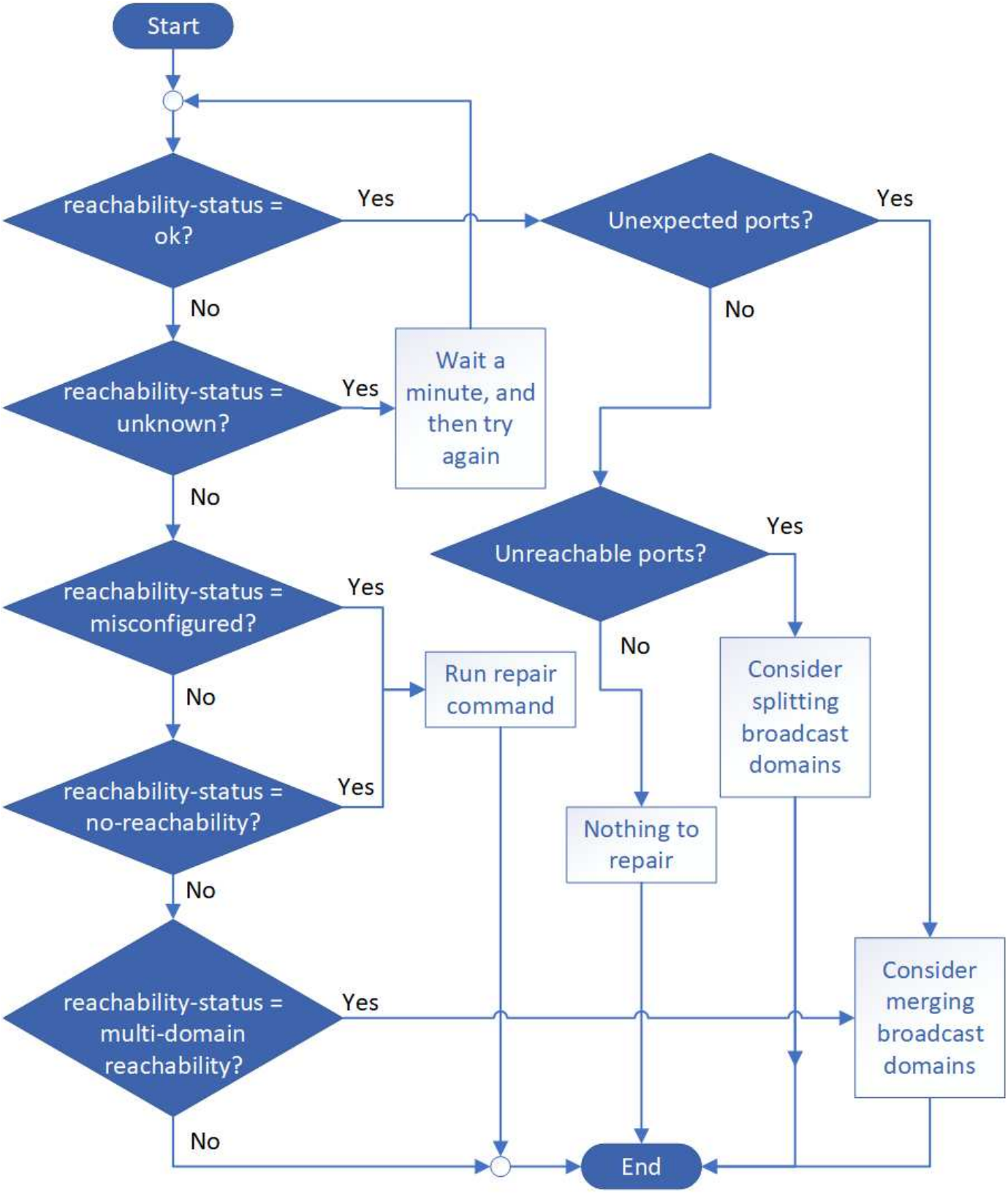
단계

1. 포트 도달 가능성 보기:

```
network port reachability show
```

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

2. 다음 진단트리와 테이블을 사용하여 다음 단계(있는 경우)를 결정합니다.


Start
reachability-status = ok?
Yes
No
Unexpected ports?
Yes
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
No
reachability-status = misconfigured?
Yes
No
Run repair command
Consider splitting broadcast domains
reachability-status = no-reachability?
Yes
No
Nothing to repair
reachability-status = multi-domain reachability?
Yes
No
Consider merging broadcast domains
End

도달 가능성 - 상태	설명

좋습니다	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 도달 가능성 - 상태가 "정상"이지만 "예상치 못한 포트"가 있는 경우 하나 이상의 브로드캐스트 도메인을 병합하는 것이 좋습니다. 자세한 내용은 다음_예기치 않은 포트_행을 참조하십시오. 도달 가능성 - 상태가 "정상"이지만 "연결할 수 없는 포트"인 경우 하나 이상의 브로드캐스트 도메인을 분할하는 것이 좋습니다. 자세한 내용은 _Unreachable ports_row를 참조하십시오. 도달 가능성 - 상태가 "정상"이고 예기치 않거나 연결할 수 없는 포트가 없는 경우 구성이 올바른 것입니다.
예기치 않은 포트	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트에 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다".
연결할 수 없는 포트	단일 브로드캐스트 도메인이 두 개의 서로 다른 도달 가능성 집합으로 분할되는 경우, 브로드캐스트 도메인을 분할하여 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다. 일반적으로 연결할 수 없는 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 다른 브로드캐스트 도메인으로 분할해야 하는 포트 집합을 정의합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 분할합니다".
잘못 구성되었습니다. - 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없지만 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템에서 해당 포트가 재연결 가능한 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 연결 복구 노드 포트 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".
아니오 - 내 상태	이 포트에는 기존 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템이 기본 IPspace에서 자동으로 생성된 새 브로드캐스트 도메인에 포트를 할당합니다. `network port reachability repair -node -port` 자세한 내용은 을 "수리 포트 도달 가능성"참조하십시오. 에 대한 자세한 내용은 `network port reachability repair` "ONTAP 명령 참조입니다"을 참조하십시오.

다중 도메인 내의 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트에 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다" 또는 "수리 포트 도달 가능성".
알 수 없음	도달 가능성 - 상태가 "알 수 없음"인 경우 몇 분 정도 기다린 후 명령을 다시 시도하십시오.

포트를 복구한 후에는 교체된 LIF 및 VLAN을 확인하고 해결해야 합니다. 포트가 인터페이스 그룹의 일부인 경우 해당 인터페이스 그룹의 변경 사항도 이해해야 합니다. 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".

ONTAP 네트워크의 포트 사용에 대해 알아봅니다

잘 알려진 여러 포트가 특정 서비스와의 ONTAP 통신용으로 예약되어 있습니다. 스토리지 네트워크 환경의 포트 값이 ONTAP 포트의 값과 같으면 포트 충돌이 발생합니다.

인바운드 트래픽

ONTAP 스토리지의 인바운드 트래픽은 다음 프로토콜 및 포트를 사용합니다.

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
TCP	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 보안 셸 액세스
TCP	80	클러스터 관리 LIF의 IP 주소에 대한 웹 페이지 액세스
TCP/UDP입니다	111	rpcbind, NFS에 대한 원격 프로시저 호출
UDP입니다	123을 선택합니다	NTP, 네트워크 시간 프로토콜
TCP	135	MSRPC, Microsoft 원격 프로시저 호출
TCP	139	NetBIOS - SSN, CIFS에 대한 NetBIOS 서비스 세션입니다
TCP/UDP입니다	161-162 을 참조하십시오	SNMP, 단순 네트워크 관리 프로토콜
TCP	443	클러스터 관리 LIF의 IP 주소에 대한 웹 페이지 액세스를 보호합니다
TCP	445	MS Active Domain Services, NetBIOS 프레이밍이 있는 TCP 기반 Microsoft SMB/CIFS
TCP/UDP입니다	635	NFS 마운트로 원격 파일 시스템이 로컬인 것처럼 상호 작용합니다
TCP	749	Kerberos
UDP입니다	953	이름 데몬입니다
TCP/UDP입니다	2049	NFS 서버 데몬

TCP	2050	NRV, NetApp 원격 볼륨 프로토콜
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP/UDP입니다	4045	NFS 잠금 데몬
TCP/UDP입니다	4046	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049	NFS RPC 견적
UDP입니다	4444	KRB524, Kerberos 524
UDP입니다	5353	멀티캐스트 DNS
TCP	10000	NDMP(Network Data Management Protocol)를 사용한 백업
TCP	11104	SnapMirror용 클러스터 간 통신 세션의 클러스터 피어링, 양방향 관리
TCP	11105	클러스터 피어링, 양방향으로 SnapMirror 데이터를 통해 인터클러스터 LIF를 사용하여 전송
SSL/TLS	30000	보안 소켓(SSL/TLS)을 통해 DMA와 NDMP 서버 간의 NDMP 보안 제어 연결을 허용합니다. 보안 스캐너는 포트 30000의 취약점을 보고할 수 있습니다.

아웃바운드 트래픽

비즈니스 요구사항에 따라 ONTAP 스토리지의 아웃바운드 트래픽은 기본 규칙 또는 고급 규칙을 사용하여 설정할 수 있습니다.

기본 아웃바운드 규칙

ICMP, TCP 및 UDP 프로토콜을 통한 모든 아웃바운드 트래픽에 모든 포트를 사용할 수 있습니다.

프로토콜	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 ONTAP의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

Active Directory를 클릭합니다

프로토콜	포트	출처	목적지	목적
TCP	88	노드 관리 LIF, 데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
UDP입니다	137	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다

UDP입니다	138	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
TCP	139	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
TCP	389	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
UDP입니다	389	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
TCP	445	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	464	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 암호 변경 및 설정(set_change)
UDP입니다	464	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
TCP	749	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 암호 변경 및 설정(RPCSEC_GSS)

AutoSupport

프로토콜	포트	출처	목적지	목적
TCP	80	노드 관리 LIF	support.netapp.com	AutoSupport(전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만 해당)

SNMP를 선택합니다

프로토콜	포트	출처	목적지	목적
TCP/UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링

SnapMirror를 참조하십시오

프로토콜	포트	출처	목적지	목적
TCP	11104	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리

기타 서비스

프로토콜	포트	출처	목적지	목적
TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고

UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다
TCP	5010	인터클러스터 LIF	엔드포인트 백업 또는 복원	S3로 백업 기능의 백업 및 복원 작업
TCP	18600 - 18699	노드 관리 LIF	대상 서버	NDMP 복제

ONTAP 내부 포트에 대해 알아봅니다

다음 표는 ONTAP이 내부적으로 사용하는 포트와 그 기능을 나열합니다. ONTAP은 이러한 포트를 클러스터 내 LIF 통신 설정과 같은 다양한 기능에 사용합니다.

이 목록은 모든 내용을 담고 있지 않으며 환경에 따라 달라질 수 있습니다.

포트/프로토콜	구성 요소/기능
514	Syslog를 클릭합니다
900	NetApp 클러스터 RPC
902	NetApp 클러스터 RPC
904	NetApp 클러스터 RPC
905	NetApp 클러스터 RPC
910	NetApp 클러스터 RPC
911	NetApp 클러스터 RPC
913	NetApp 클러스터 RPC
914	NetApp 클러스터 RPC
915	NetApp 클러스터 RPC
918	NetApp 클러스터 RPC
920	NetApp 클러스터 RPC
921)를 참조하십시오	NetApp 클러스터 RPC
924	NetApp 클러스터 RPC
925	NetApp 클러스터 RPC
927)를 참조하십시오	NetApp 클러스터 RPC
928	NetApp 클러스터 RPC
929)를 누릅니다	NetApp 클러스터 RPC

930	커널 서비스 및 관리 기능(KSMF)
931	NetApp 클러스터 RPC
932	NetApp 클러스터 RPC
933	NetApp 클러스터 RPC
934	NetApp 클러스터 RPC
935	NetApp 클러스터 RPC
936	NetApp 클러스터 RPC
937	NetApp 클러스터 RPC
939	NetApp 클러스터 RPC
940	NetApp 클러스터 RPC
951을 참조하십시오	NetApp 클러스터 RPC
954를 참조하십시오	NetApp 클러스터 RPC
955	NetApp 클러스터 RPC
956을 참조하십시오	NetApp 클러스터 RPC
958	NetApp 클러스터 RPC
961	NetApp 클러스터 RPC
963	NetApp 클러스터 RPC
964	NetApp 클러스터 RPC
966	NetApp 클러스터 RPC
967	NetApp 클러스터 RPC
975	키 관리 상호 운용성 프로토콜(KMIP)
982	NetApp 클러스터 RPC
983	NetApp 클러스터 RPC
5125	디스크의 대체 제어 포트
5133	디스크의 대체 제어 포트
5144	디스크의 대체 제어 포트
65502	노드 범위 SSH
65503	LIF 공유
7700	클러스터 세션 관리자(CSM)
7810)를 참조하십시오	NetApp 클러스터 RPC
7811	NetApp 클러스터 RPC
7812)를 참조하십시오	NetApp 클러스터 RPC
7813)를 참조하십시오	NetApp 클러스터 RPC
7814)를 참조하십시오	NetApp 클러스터 RPC

7815)를 참조하십시오	NetApp 클러스터 RPC
7816	NetApp 클러스터 RPC
7817	NetApp 클러스터 RPC
7818)를 참조하십시오	NetApp 클러스터 RPC
7819)를 참조하십시오	NetApp 클러스터 RPC
7820)를 참조하십시오	NetApp 클러스터 RPC
7821)를 참조하십시오	NetApp 클러스터 RPC
7822)를 참조하십시오	NetApp 클러스터 RPC
7823)를 참조하십시오	NetApp 클러스터 RPC
7824)를 참조하십시오	NetApp 클러스터 RPC
7835-7839 및 7845-7849	클러스터 내부 통신을 위한 TCP 포트
8023	노드 범위 텔넷
8443	Amazon FSx용 ONTAP S3 NAS 포트
8514	노드 범위 RSH
9877	KMIP 클라이언트 포트(내부 로컬 호스트만 해당)
10006	HA 상호 연결 통신을 위한 TCP 포트

IPspace

ONTAP IPspace 구성에 대해 자세히 알아보십시오

IPspace를 사용하면 단일 ONTAP 클러스터를 구성하여 클라이언트가 동일한 IP 주소 서브넷 범위를 사용 중인 경우에도 관리를 목적으로 서로 다른 여러 네트워크 도메인의 클라이언트에서 액세스할 수 있습니다. 이를 통해 개인 정보 보호와 보안을 위해 클라이언트 트래픽을 분리할 수 있습니다.

IPspace는 SVM(스토리지 가상 머신)이 상주하는 고유 IP 주소 공간을 정의합니다. IPspace에 정의된 포트 및 IP 주소는 해당 IPspace 내에서만 적용 가능합니다. IPspace 내에서 각 SVM에 대해 별개의 라우팅 테이블이 유지되므로 교차 SVM 또는 교차 IPspace 트래픽 라우팅이 발생하지 않습니다.

> IPspace는 라우팅 도메인에서 IPv4 및 IPv6 주소를 모두 지원합니다.

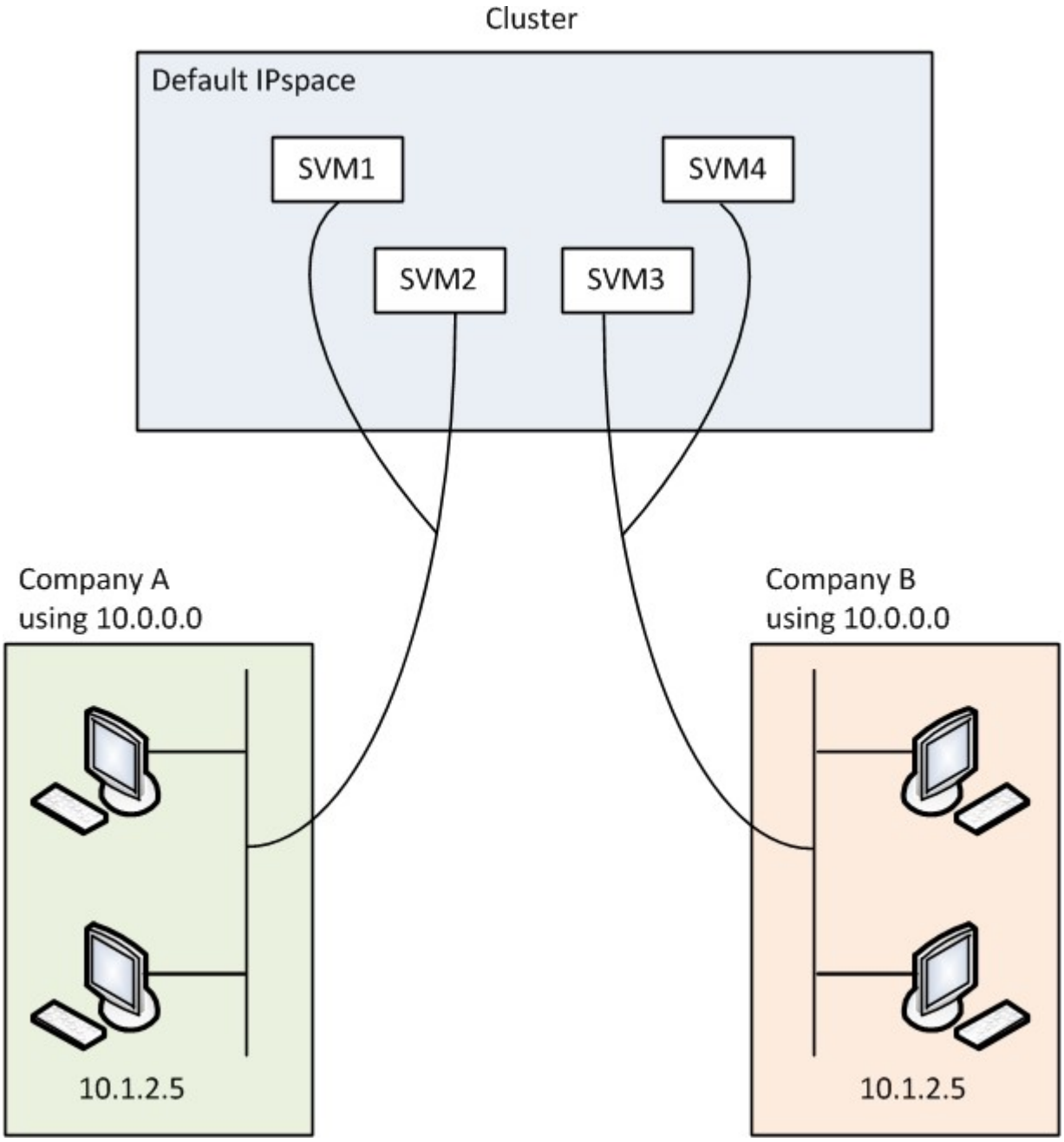
단일 조직의 스토리지를 관리하는 경우 IPspace를 구성할 필요가 없습니다. 단일 ONTAP 클러스터에서 여러 회사의 스토리지를 관리하는 경우 충돌하는 네트워킹 구성이 없을 수도 있으므로 IPspace를 사용할 필요가 없습니다. 대부분의 경우, 고유한 IP 라우팅 테이블을 사용하는 SVM(스토리지 가상 머신)을 사용하여 IPspace를 사용하는 대신 고유한 네트워킹 구성을 분리할 수 있습니다.

IPspace 사용 예

IPspace를 사용하는 일반적인 애플리케이션 은 SSP(스토리지 서비스 공급자)에서 SSP(회사 A)와 B의 고객을 SSP 단지의 ONTAP 클러스터에 연결해야 하며, 두 회사 모두 동일한 프라이빗 IP 주소 범위를 사용합니다.

SSP는 각 고객에 대해 클러스터에 SVM을 생성하고 두 SVM에서 회사 A의 네트워크 및 다른 두 SVM에서 회사 B의 네트워크로 전용 네트워크 경로를 제공합니다.

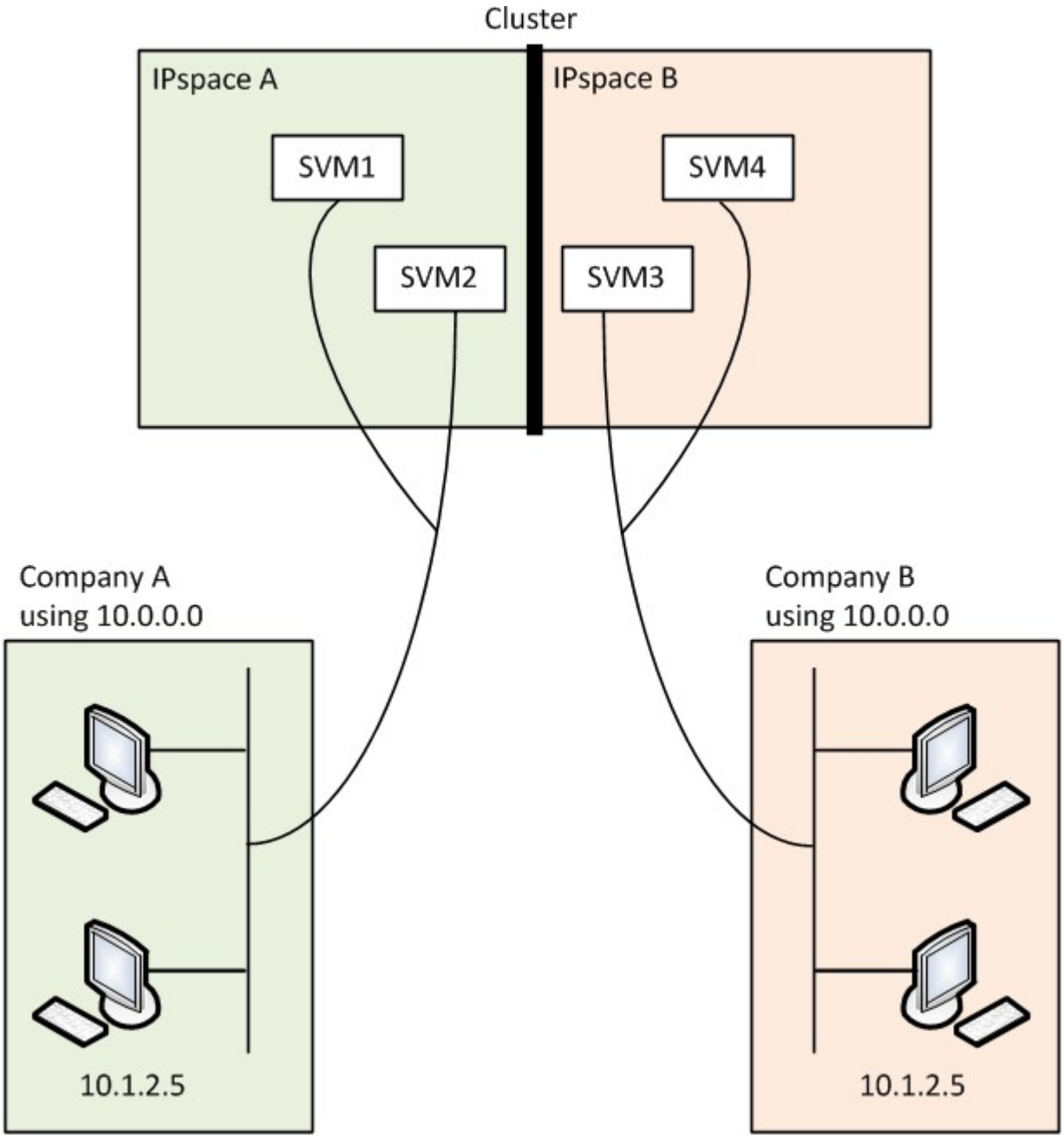
이 유형의 배포는 다음 그림에 나와 있으며 두 회사 모두 비전용 IP 주소 범위를 사용하는 경우 작동합니다. 그러나 그림에서는 문제를 일으키는 동일한 개인 IP 주소 범위를 사용하는 두 회사를 보여 줍니다.



두 회사 모두 전용 IP 주소 서브넷 10.0.0.0을 사용하므로 다음과 같은 문제가 발생합니다.

- 두 회사 모두 해당 SVM에 동일한 IP 주소를 사용하기로 결정한 경우 SSP 위치의 클러스터에 있는 SVM에서 IP 주소가 서로 충돌합니다.
- 두 회사가 SVM에 서로 다른 IP 주소를 사용하는 데 동의하더라도 문제가 발생할 수 있습니다.
- 예를 들어, A의 네트워크에 있는 클라이언트의 IP 주소가 B의 네트워크에 있는 클라이언트와 동일한 경우, A의 주소 공간에 있는 클라이언트에 대한 패킷은 B의 주소 공간에 있는 클라이언트로 라우팅될 수 있으며 그 반대의 경우도 마찬가지입니다.

- 두 회사가 상호 배타적인 주소 공간을 사용하기로 결정한 경우(예: A는 10.0.0.0, 네트워크 마스크 255.128.0.0, B는 10.128.0.0, 네트워크 마스크 255.128.0.0 사용), SSP는 트래픽을 A 및 B의 네트워크에 적절하게 라우팅하도록 클러스터의 정적 경로를 구성해야 합니다.
- 이 솔루션은 고정 경로로 인해 확장성이 뛰어나도 보안이 보장되지 않습니다.(브로드캐스트 트래픽이 클러스터의 모든 인터페이스로 전송됨) 이러한 문제를 해결하기 위해 SSP는 클러스터에서 2개의 IPspace를 정의합니다(각 회사당 하나씩). IPspace 트래픽이 라우팅되지 않기 때문에 다음 그림과 같이 모든 SVM이 10.0.0.0 주소 공간에 구성되어 있어도 각 회사의 데이터가 해당 네트워크로 안전하게 라우팅됩니다.



또한, '/etc/hosts' 파일, '/etc/hosts.equv' 파일 및 '/etc/rc' 파일과 같은 다양한 구성 파일에서 참조하는 IP 주소는 해당 IPspace와 관련이 있습니다. 따라서 IPspace를 사용하면 SSP에서 여러 SVM에 대한 구성 및 인증 데이터에 대해 충돌 없이 동일한 IP 주소를 구성할 수 있습니다.

IPspace의 표준 속성

특수 IPspace는 클러스터를 처음 생성할 때 기본적으로 생성됩니다. 또한 IPspace별로 특수 스토리지 가상 머신(SVM)을 생성합니다.

2개의 IPspace가 클러스터 초기화 시 자동으로 생성됨:

- "기본" IPspace

  이 IPspace는 포트, 서브넷 및 SVM에서 데이터를 제공하는 컨테이너입니다. 클라이언트에 대해 별도의 IPspace가 필요 없는 경우 이 IPspace에서 모든 SVM을 생성할 수 있습니다. 이 IPspace는 클러스터 관리 및 노드 관리 포트도 포함합니다.

- "클러스터" IPspace

  이 IPspace는 클러스터 내의 모든 노드에 있는 클러스터 포트를 모두 포함하고 있습니다. 이 생성된 클러스터는 클러스터 생성 시 자동으로 생성됩니다. 내부 프라이빗 클러스터 네트워크에 대한 연결을 제공합니다. 추가 노드가 클러스터에 추가될 때 해당 노드의 클러스터 포트가 "클러스터" IPspace에 추가됩니다.

IPspace별로 존재하는 "시스템" SVM IPspace를 생성하는 경우 동일한 이름의 기본 시스템 SVM이 생성됩니다.

- 내부 프라이빗 클러스터 네트워크에서 클러스터 노드 간에 클러스터 트래픽을 전달하는 "클러스터" IPspace용 시스템 SVM

  클러스터 관리자가 관리하며 "Cluster"라는 이름이 있습니다.

- 클러스터 간 트래픽을 포함하여 클러스터 및 노드에 대한 관리 트래픽을 전달하는 "기본" IPspace용 시스템 SVM

  클러스터 관리자가 관리하며 클러스터와 동일한 이름을 사용합니다.

- 생성한 사용자 지정 IPspace용 시스템 SVM은 해당 SVM에 대한 관리 트래픽을 전달

  클러스터 관리자가 관리하며 IPspace와 동일한 이름을 사용합니다.

IPspace에 클라이언트용 SVM이 하나 이상 존재할 수 있습니다. 각 클라이언트 SVM은 자체 데이터 볼륨 및 구성을 제공하며 다른 SVM과 독립적으로 관리됩니다.

ONTAP 네트워크용 **IPspace**를 생성합니다

IPspace는 SVM(스토리지 가상 머신)이 상주하는 고유 IP 주소 공간입니다. 안전한 스토리지, 관리 및 라우팅을 위해 SVM이 필요한 경우 IPspace를 생성할 수 있습니다. IPspace를 사용하여 클러스터의 각 SVM에 대해 별개의 IP 주소 공간을 생성할 수 있습니다. 이렇게 하면 관리자가 별도의 네트워크 도메인에 있는 클라이언트가 동일한 IP 주소 서브넷 범위의 중복 IP 주소를 사용하면서 클러스터 데이터에 액세스할 수 있습니다.

이 작업에 대해

512개의 IPspace를 클러스터 전체에서 사용할 수 있습니다. 6GB의 RAM이 있는 노드를 포함하는 클러스터의 경우 클러스터 전체 제한이 256개의 IPspace로 줄어듭니다. 플랫폼에 추가적인 제한이 적용되는지 확인하려면 Hardware Universe를 참조하십시오.

"NetApp Hardware Universe를 참조하십시오"

"ALL"이 시스템 예약 이름이므로 IPspace 이름은 "ALL"일 수 없습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. IPspace 생성:

```
network ipspace create -ipspace ipspace_name
```

IPSpace_name은 만들려는 IPspace의 이름입니다. 다음 명령을 실행하면 클러스터에서 IPspace ipspace1 이 생성됩니다.

```
network ipspace create -ipspace ipspace1
```

에 대한 자세한 내용은 `network ipspace create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. IPspace 표시:

네트워크 IPspace 쇼

```
IPspace             Vserver List          Broadcast Domains
------------------- --------------------- ----------------------------
Cluster             Cluster               Cluster
Default             Cluster1              Default
ipspace1            ipspace1              -
```

IPspace용 시스템 SVM과 함께 IPspace가 생성됨 시스템 SVM은 관리 트래픽을 전달합니다.

작업을 마친 후

MetroCluster 구성으로 클러스터에서 IPspace를 생성하는 경우 파트너 클러스터로 IPspace 객체를 수동으로 복제해야 합니다. IPspace가 복제되기 전에 IPspace에 생성 및 할당된 SVM은 파트너 클러스터에 복제되지 않습니다.

브로드캐스트 도메인은 "기본" IPspace에서 자동으로 생성되며 다음 명령을 사용하여 IPspace 간에 이동할 수 있습니다.

```
network port broadcast-domain move
```

예를 들어, 다음 명령을 사용하여 브로드캐스트 도메인을 "Default"에서 "IPS1"으로 이동하려는 경우:

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

ONTAP 네트워크에서 IPspace를 확인합니다

클러스터에 존재하는 IPspace 목록을 표시할 수 있으며 SVM(스토리지 가상 머신), 브로드캐스트 도메인 및 각 IPspace에 할당된 포트를 볼 수 있습니다.

단계

클러스터에서 IPspace 및 SVM 표시:

```
network ipspace show [-ipspace ipspace_name]
```

다음 명령을 실행하면 클러스터에서 모든 IPspace, SVM 및 브로드캐스트 도메인이 표시됩니다.

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  ------------------------ -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

다음 명령을 실행하면 IPspace 1의 일부인 노드 및 포트가 표시됩니다.

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

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

ONTAP 네트워크에서 IPspace를 삭제합니다

IPspace가 더 이상 필요하지 않은 경우 삭제할 수 있습니다.

시작하기 전에

삭제할 IPspace와 연결된 브로드캐스트 도메인, 네트워크 인터페이스 또는 SVM이 없어야 합니다.

시스템 정의 "기본" 및 "클러스터" IPspace는 삭제할 수 없습니다.

단계

IPspace 삭제:

```
network ipspace delete -ipspace ipspace_name
```

다음 명령을 실행하면 클러스터에서 IPspace ipspace1 이 삭제됩니다.

```
network ipspace delete -ipspace ipspace1
```

에 대한 자세한 내용은 `network ipspace delete` "ONTAP 명령 참조입니다"을 참조하십시오.

브로드캐스트 도메인

ONTAP 브로드캐스트 도메인에 대해 알아봅니다

브로드캐스트 도메인은 동일한 계층 2 네트워크에 속하는 네트워크 포트를 그룹화하는 데 사용됩니다. 그런 다음 SVM(스토리지 가상 시스템)에서 그룹의 포트를 사용하여 데이터 또는 관리 트래픽을 처리할 수 있습니다.

> 브로드캐스트 도메인의 관리는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 관리해야 하는 경우 을 참조하십시오"브로드캐스트 도메인 개요(ONTAP 9.7 이하)".

브로드캐스트 도메인은 IPspace에 상주합니다. 클러스터 초기화 중에 시스템은 두 개의 기본 브로드캐스트 도메인을 생성합니다.

- "기본" 브로드캐스트 도메인에는 "기본" IPspace에 있는 포트가 포함되어 있습니다.

  이러한 포트는 주로 데이터를 제공하는 데 사용됩니다. 클러스터 관리 및 노드 관리 포트도 이 브로드캐스트 도메인에 있습니다.

- "클러스터" 브로드캐스트 도메인에는 "클러스터" IPspace에 있는 포트가 포함되어 있습니다.

  이러한 포트는 클러스터 통신에 사용되며 클러스터의 모든 노드에 있는 모든 클러스터 포트를 포함합니다.

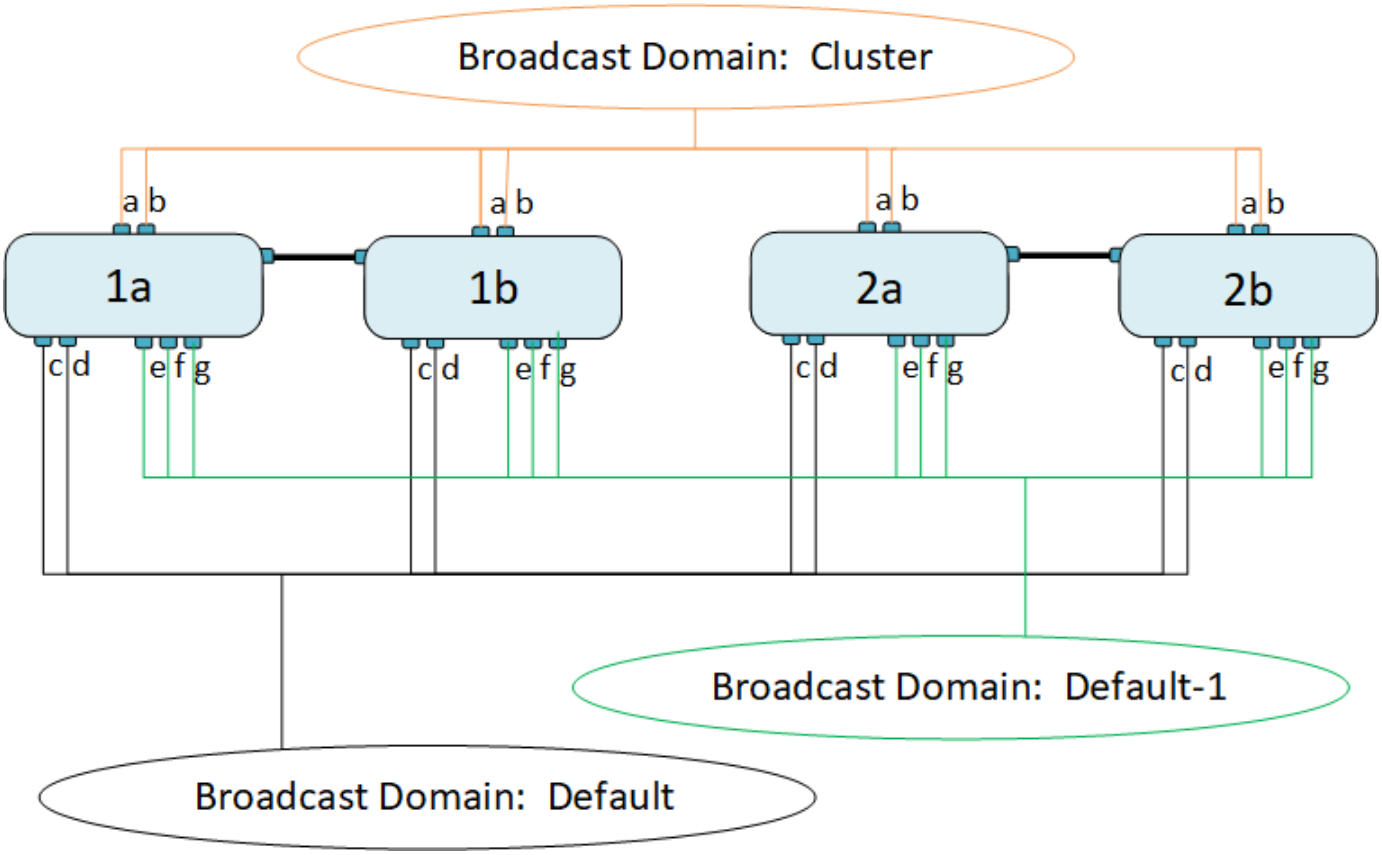
  필요한 경우 시스템이 기본 IPspace에 추가 브로드캐스트 도메인을 생성합니다. "기본" 브로드캐스트 도메인에는 관리 LIF의 홈 포트와 계층 2의 기능이 있는 다른 포트가 포함됩니다. 추가 브로드캐스트 도메인 이름은 "Default-1", "Default-2" 등으로 지정됩니다.

브로드캐스트 도메인 사용 예

브로드캐스트 도메인은 동일한 IPspace에서 네트워크 포트 집합으로, 일반적으로 클러스터에 있는 여러 노드의 포트를 포함하여 계층 2 상호 도달 기능을 가지고 있습니다.

그림에서는 4노드 클러스터의 3개 브로드캐스트 도메인에 할당된 포트를 보여 줍니다.

- "클러스터" 브로드캐스트 도메인은 클러스터 초기화 중에 자동으로 생성되며, 클러스터의 각 노드에서 포트 a와 b를 포함합니다.
- "Default" 브로드캐스트 도메인은 클러스터 초기화 중에 자동으로 생성되며, 클러스터의 각 노드에서 c 및 d 포트를 포함합니다.
- 시스템은 계층 2 네트워크 내 기능을 기반으로 클러스터 초기화 중에 추가 브로드캐스트 도메인을 자동으로 생성합니다. 이러한 추가 브로드캐스트 도메인은 Default-1, Default-2 등으로 명명됩니다.



각 브로드캐스트 도메인과 동일한 네트워크 포트를 가진 동일한 이름의 페일오버 그룹이 자동으로 생성됩니다. 이 페일오버 그룹은 시스템에서 자동으로 관리됩니다. 즉, 포트가 브로드캐스트 도메인에서 추가되거나 제거될 때 포트가 이 페일오버 그룹에서 자동으로 추가 또는 제거됩니다.

ONTAP 브로드캐스트 도메인을 생성합니다

브로드캐스트 도메인은 동일한 계층 2 네트워크에 속한 클러스터의 네트워크 포트를 그룹화합니다. 그런 다음 SVM에서 포트를 사용할 수 있습니다.

브로드캐스트 도메인은 클러스터 생성 또는 연결 작업 중에 자동으로 생성됩니다. ONTAP 9.12.0부터는 자동으로 생성된 브로드캐스트 도메인 외에도 시스템 관리자에서 수동으로 브로드캐스트 도메인을 추가할 수 있습니다.

> 브로드캐스트 도메인을 만드는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 만들어야 하는 경우 을 참조하십시오"브로드캐스트 도메인 생성(ONTAP 9.7 이하)".

시작하기 전에

브로드캐스트 도메인에 추가할 포트는 다른 브로드캐스트 도메인에 속하지 않아야 합니다. 사용하려는 포트가 다른 브로드캐스트 도메인에 속하지만 사용되지 않는 경우 원래 브로드캐스트 도메인에서 해당 포트를 제거합니다.

이 작업에 대해

- 모든 브로드캐스트 도메인 이름은 IPspace 내에서 고유해야 합니다.
- 브로드캐스트 도메인에 추가되는 포트는 물리적 네트워크 포트, VLAN 또는 링크 집계 그룹/인터페이스 그룹(LAG/ifgrp)일 수 있습니다.
- 사용하려는 포트가 다른 브로드캐스트 도메인에 속하지만 사용되지 않는 경우 새 브로드캐스트 도메인에 추가하기 전에 기존 브로드캐스트 도메인에서 제거하십시오.
- 브로드캐스트 도메인에 추가된 포트의 MTU(Maximum Transmission Unit)가 브로드캐스트 도메인에 설정된 MTU 값으로 업데이트됩니다.
- MTU 값은 e0M 포트 처리 관리 트래픽을 제외하고 해당 계층 2 네트워크에 연결된 모든 장치와 일치해야 합니다.
- IPspace 이름을 지정하지 않으면 브로드캐스트 도메인이 "기본" IPspace에 생성됩니다.

시스템 구성을 더 쉽게 하기 위해 같은 이름의 페일오버 그룹이 자동으로 생성되어 동일한 포트가 포함되어 있습니다.

시스템 관리자

단계

1. 네트워크 > 개요 > 브로드캐스트 도메인 * 을 선택합니다.
2. 을 클릭합니다 + Add
3. 브로드캐스트 도메인의 이름을 지정합니다.
4. MTU를 설정합니다.
5. IPspace를 선택합니다.
6. 브로드캐스트 도메인을 저장합니다.

브로드캐스트 도메인을 추가한 후에는 해당 도메인을 편집하거나 삭제할 수 있습니다.

CLI를 참조하십시오

ONTAP 9.8 이상을 사용 중인 경우, 레이어 2 접근성에 따라 브로드캐스트 도메인이 자동으로 생성됩니다. 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".

브로드캐스트 도메인을 수동으로 만들 수도 있습니다.

단계

1. 브로드캐스트 도메인에 현재 할당되지 않은 포트 보기:

   네트워크 포트 쇼

   디스플레이가 큰 경우 네트워크 포트 show-broadcast-domain 명령을 사용하여 할당되지 않은 포트만 봅니다.

2. 브로드캐스트 도메인 생성:

   'network port broadcast-domain create-broadcast-domain_domain_name_-MTU_MTU_value_[-IPSpace_IPSpace_name_][-ports_ports_list_]'

   a. broadcast_domain_name은 만들려는 브로드캐스트 도메인의 이름입니다.
   b. mtu_value는 IP 패킷의 MTU 크기이고 1500 및 9000은 일반적인 값입니다.

      이 값은 이 브로드캐스트 도메인에 추가되는 모든 포트에 적용됩니다.

   c. IPSpace_name은 이 브로드캐스트 도메인을 추가할 IPspace의 이름입니다.

      이 매개 변수에 값을 지정하지 않으면 "기본" IPspace가 사용됩니다.

   d. port_list는 브로드캐스트 도메인에 추가될 포트의 목록입니다.

      포트는 노드1:e0c 등의 노드_이름:포트_번호 형식으로 추가됩니다.

3. 브로드캐스트 도메인이 원하는 대로 생성되었는지 확인합니다.

   'network port show-instance-broadcast-domain new_domain'

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

예

다음 명령은 기본 IPspace에서 브로드캐스트 도메인 bcast1을 생성하고 MTU를 1500으로 설정하고 포트 4개를 추가합니다.

'network port broadcast-domain create-broadcast-domain_bcast1_-mtu_1500_-ports_cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f_'

에 대한 자세한 내용은 `network port broadcast-domain create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

서브넷을 생성하여 브로드캐스트 도메인에서 사용할 IP 주소 풀을 정의하거나, 현재 IPspace에 SVM 및 인터페이스를 할당할 수 있습니다. 자세한 내용은 을 "클러스터 및 SVM 피어링"참조하십시오.

기존 브로드캐스트 도메인의 이름을 변경해야 할 경우 'network port broadcast-domain rename' 명령어를 사용한다.

에 대한 자세한 내용은 `network port broadcast-domain rename` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 브로드캐스트 도메인에서 포트를 추가하거나 제거합니다

브로드캐스트 도메인은 클러스터 생성 또는 연결 작업 중에 자동으로 생성됩니다. 브로드캐스트 도메인에서 포트를 수동으로 제거할 필요는 없습니다.

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경되었고 네트워크 포트가 다른 브로드캐스트 도메인에 속해 있는 경우 다음 항목을 참조하십시오.

"수리 포트 도달 가능성"

> 브로드캐스트 도메인의 포트를 추가하거나 제거하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크의 브로드캐스트 도메인에서 포트를 추가하거나 제거해야 하는 경우 을 참조하십시오"브로드캐스트 도메인에서 포트 추가 또는 제거(ONTAP 9.7 이하)".

시스템 관리자

ONTAP 9.14.1부터 System Manager를 사용하여 브로드캐스트 도메인에 이더넷 포트를 재할당할 수 있습니다. 모든 이더넷 포트를 브로드캐스트 도메인에 할당하는 것이 좋습니다. 따라서 브로드캐스트 도메인에서 이더넷 포트를 할당 해제하는 경우 다른 브로드캐스트 도메인에 다시 할당해야 합니다.

단계

이더넷 포트를 재할당하려면 다음 단계를 수행하십시오.

1. 네트워크 > 개요 * 를 선택합니다.
2. 브로드캐스트 도메인 * 섹션에서 도메인 이름 옆에 있는 을 선택합니다 ⋮ .
3. 드롭다운 메뉴에서 * 편집 * 을 선택합니다.
4. 브로드캐스트 도메인 편집 * 페이지에서 다른 도메인에 재할당할 이더넷 포트를 선택 취소합니다.
5. 선택 해제된 각 포트에 대해 * 이더넷 포트 재할당 * 창이 표시됩니다. 포트를 재할당할 브로드캐스트 도메인을 선택한 다음 * 재할당 * 을 선택합니다.
6. 현재 브로드캐스트 도메인에 할당할 모든 포트를 선택하고 변경 내용을 저장합니다.

CLI를 참조하십시오

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경되었고 네트워크 포트가 다른 브로드캐스트 도메인에 속해 있는 경우 다음 항목을 참조하십시오.

"수리 포트 도달 가능성"

또는 을 사용하여 브로드캐스트 도메인에서 포트를 수동으로 추가하거나 제거할 수 있습니다 `network port broadcast-domain add-ports` 또는 을 누릅니다 `network port broadcast-domain remove-ports` 명령.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 브로드캐스트 도메인에 추가할 포트는 다른 브로드캐스트 도메인에 속하지 않아야 합니다.
- 인터페이스 그룹에 이미 속해 있는 포트는 브로드캐스트 도메인에 개별적으로 추가할 수 없습니다.

이 작업에 대해

네트워크 포트를 추가하거나 제거할 때 다음 규칙이 적용됩니다.

포트를 추가할 때…	포트를 제거할 때…
포트는 네트워크 포트, VLAN 또는 인터페이스 그룹(ifgrp)일 수 있습니다.	해당 없음
포트는 브로드캐스트 도메인의 시스템 정의 페일오버 그룹에 추가됩니다.	브로드캐스트 도메인의 모든 페일오버 그룹에서 포트가 제거됩니다.
포트의 MTU가 브로드캐스트 도메인에서 설정된 MTU 값으로 업데이트됩니다.	포트의 MTU는 변경되지 않습니다.
포트의 IPspace가 브로드캐스트 도메인의 IPspace 값으로 업데이트됩니다.	포트는 브로드캐스트 도메인 속성이 없는 '기본' IPspace로 이동됩니다.

명령을 사용하여 인터페이스 그룹의 마지막 구성원 포트를 제거하면 `network port ifgrp remove-port` 브로드캐스트 도메인에서 빈 인터페이스 그룹 포트가 허용되지 않으므로 인터페이스 그룹 포트가 브로드캐스트 도메인에서 제거됩니다. 에 대한 자세한 내용은 `network port ifgrp remove-port` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. network port show 명령을 사용하여 브로드캐스트 도메인에 현재 할당되거나 할당되지 않은 포트를 표시합니다.
2. 브로드캐스트 도메인에서 네트워크 포트 추가 또는 제거:

원하는 작업	사용...
브로드캐스트 도메인에 포트를 추가합니다	네트워크 포트 브로드캐스트 도메인 추가 포트
브로드캐스트 도메인에서 포트를 제거합니다	네트워크 포트 브로드캐스트 도메인 제거 포트

3. 브로드캐스트 도메인에서 포트가 추가되거나 제거되었는지 확인합니다.

   네트워크 포트 쇼

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

포트 추가 및 제거의 예

다음 명령을 실행하면 노드 클러스터 -1-01의 포트 e0g 및 노드 클러스터 -1-02의 포트 e0g가 기본 IPspace의 브로드캐스트 도메인 bcast1에 추가됩니다.

'cluster-1::> network port broadcast-domain add-ports-broadcast-domain bcast1-ports cluster-1-01:e0g, cluster1-02:e0g'

다음 명령을 실행하면 클러스터 IPspace의 브로드캐스트 도메인 클러스터에 클러스터 포트 2개가 추가됩니다.

'cluster-1::> network port broadcast-domain add-ports-broadcast-domain Cluster-ports cluster-2-03:e0f, cluster2-04:e0f-IPSpace Cluster'

다음 명령은 기본 IPspace의 브로드캐스트 도메인 bcast1에서 노드 cluster1-01의 포트 e0e를 제거합니다.

'cluster-1::> network port broadcast-domain remove-ports-broadcast-domain bcast1-ports cluster-1-01:e0e'

에 대한 자세한 내용은 `network port broadcast-domain remove-ports` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP 포트 가용성을 복구합니다

브로드캐스트 도메인은 자동으로 생성됩니다. 그러나 포트가 다시 설정되거나 스위치 구성이 변경되면 포트를 다른 브로드캐스트 도메인(신규 또는 기존)으로 복구해야 할 수도 있습니다.

ONTAP는 브로드캐스트 도메인 구성(이더넷 포트) 계층 2 내 기능을 기반으로 네트워크 배선 문제에 대한 솔루션을 자동으로 감지하고 추천할 수 있습니다.

동안 배선이 잘못되면 브로드캐스트 도메인 포트가 예기치 않게 할당될 수 있습니다. ONTAP 9.10.1부터 클러스터는 클러스터 설정 후 또는 새 노드가 기존 클러스터에 연결된 경우 포트 재연결을 확인하여 네트워크 배선 문제를 자동으로 확인합니다.

시스템 관리자

포트 도달 가능성 문제가 감지되면 System Manager에서 문제 해결을 위한 복구 작업을 권장합니다.

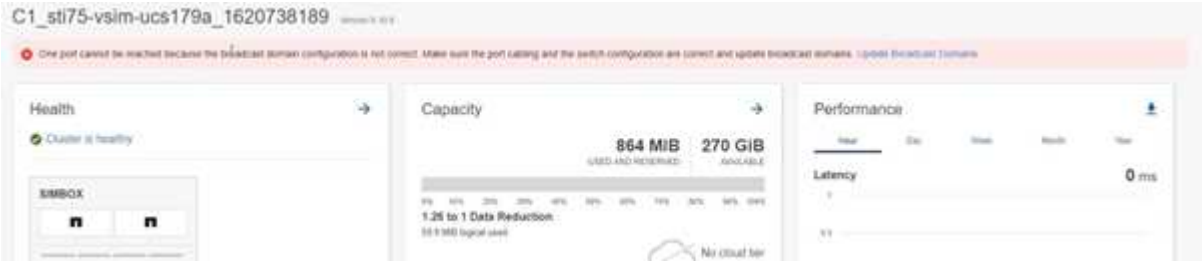
클러스터를 설정한 후 네트워크 배선 문제가 대시보드에 보고됩니다.

클러스터에 새 노드를 연결하면 노드 페이지에 네트워크 배선 문제가 나타납니다.

네트워크 다이어그램에서 네트워크 배선 상태를 볼 수도 있습니다. 포트 도달 가능성 문제는 네트워크 다이어그램에 빨간색 오류 아이콘으로 표시됩니다.

클러스터 설정 후

클러스터를 설정한 후 시스템에서 네트워크 배선 문제가 감지되면 대시보드에 메시지가 표시됩니다.



단계

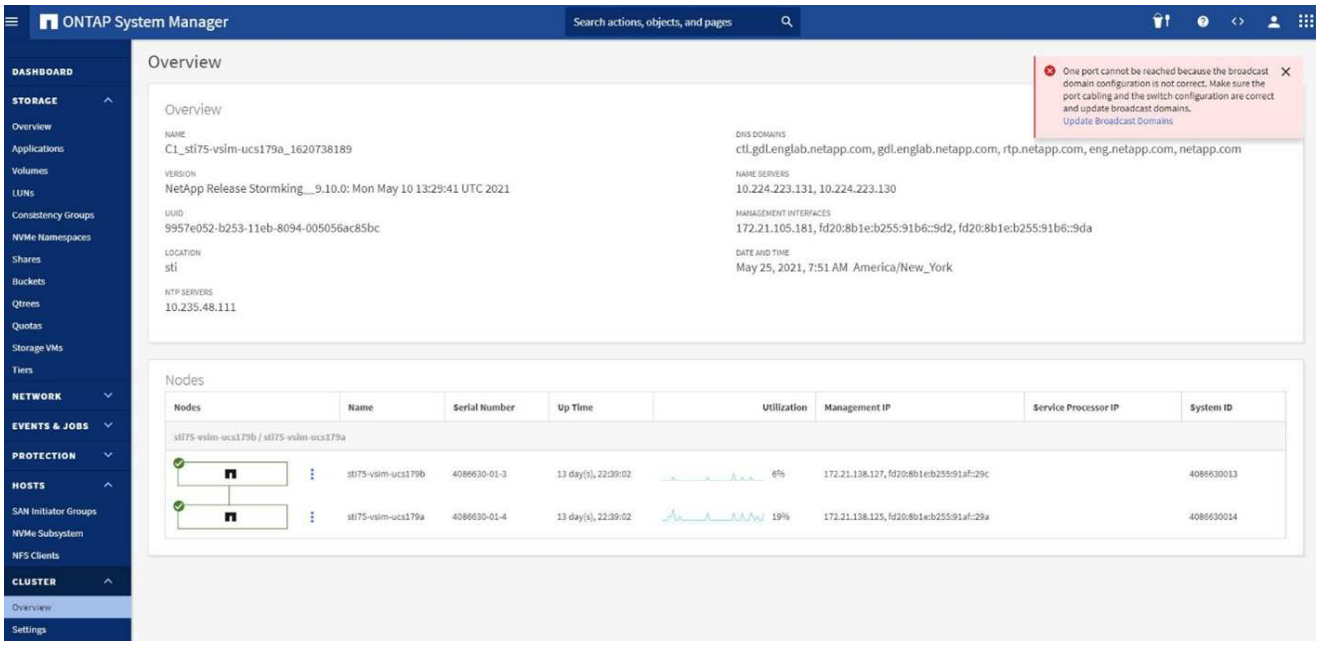
1. 메시지에 제시된 대로 배선을 수정한다.
2. 링크를 클릭하여 브로드캐스트 도메인 업데이트 대화 상자를 시작합니다. 브로드캐스트 도메인 업데이트 대화

상자가 열립니다.

3. 노드, 문제, 현재 브로드캐스트 도메인 및 예상 브로드캐스트 도메인을 포함하여 포트에 대한 정보를 검토합니다.
4. 복구할 포트를 선택하고 * Fix * 를 클릭합니다. 시스템이 현재 브로드캐스트 도메인에서 예상된 브로드캐스트 도메인으로 포트를 이동합니다.

사후 노드 조인을 선택합니다

새 노드를 클러스터에 조인 후 시스템이 네트워크 배선 문제를 감지하면 노드 페이지에 메시지가 나타납니다.



단계

1. 메시지에 제시된 대로 배선을 수정한다.
2. 링크를 클릭하여 브로드캐스트 도메인 업데이트 대화 상자를 시작합니다. 브로드캐스트 도메인 업데이트 대화

상자가 열립니다.

3. 노드, 문제, 현재 브로드캐스트 도메인 및 예상 브로드캐스트 도메인을 포함하여 포트에 대한 정보를 검토합니다.
4. 복구할 포트를 선택하고 * Fix * 를 클릭합니다. 시스템이 현재 브로드캐스트 도메인에서 예상된 브로드캐스트 도메인으로 포트를 이동합니다.

CLI를 참조하십시오

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

이 작업에 대해

ONTAP에서 감지한 계층 2 도달 가능 여부에 따라 포트에 대한 브로드캐스트 도메인 구성을 자동으로 복구하는 명령을 사용할 수 있습니다.

단계

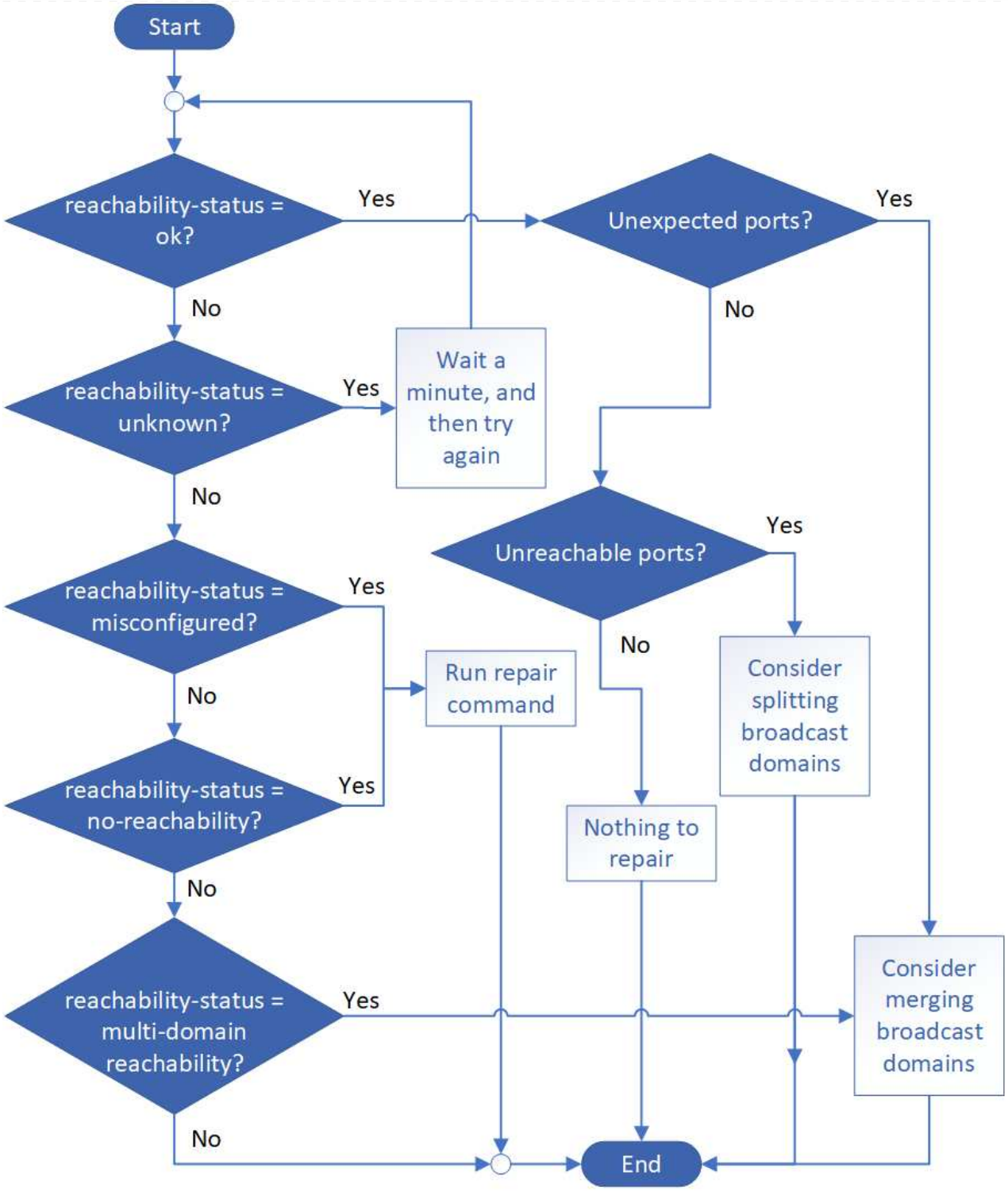
1. 스위치 구성 및 케이블 연결을 확인합니다.
2. 포트의 연결 상태를 확인합니다.

   네트워크 포트 도달 가능성 show-detail-node-port

   명령 출력에 연결 가능 결과가 포함되어 있습니다.

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

3. 다음 진단트리와 표를 사용하여 달성 가능 결과를 파악하고 다음에 수행할 작업을 결정합니다.


Start
reachability-status = ok?
Yes
No
Unexpected ports?
Yes
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
No
reachability-status = misconfigured?
Yes
No
Run repair command
Consider splitting broadcast domains
reachability-status = no-reachability?
Yes
No
Nothing to repair
reachability-status = multi-domain reachability?
Yes
No
Consider merging broadcast domains
End

도달 가능성 - 상태	설명

좋습니다	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 도달 가능성 - 상태가 "정상"이지만 "예상치 못한 포트"가 있는 경우 하나 이상의 브로드캐스트 도메인을 병합하는 것이 좋습니다. 자세한 내용은 다음_예기치 않은 포트_행을 참조하십시오. 도달 가능성 - 상태가 "정상"이지만 "연결할 수 없는 포트"인 경우 하나 이상의 브로드캐스트 도메인을 분할하는 것이 좋습니다. 자세한 내용은 _Unreachable ports_row를 참조하십시오. 도달 가능성 - 상태가 "정상"이고 예기치 않거나 연결할 수 없는 포트가 없는 경우 구성이 올바른 것입니다.
예기치 않은 포트	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트의 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다".
연결할 수 없는 포트	단일 브로드캐스트 도메인이 두 개의 서로 다른 도달 가능성 집합으로 분할되는 경우, 브로드캐스트 도메인을 분할하여 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다. 일반적으로 연결할 수 없는 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 다른 브로드캐스트 도메인으로 분할해야 하는 포트 집합을 정의합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 분할합니다".
잘못 구성되었습니다. - 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없지만 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템에서 해당 포트가 재연결 가능한 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 도달 가능성 복구 노드 포트

아니오 - 내 상태	이 포트에는 기존 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템이 기본 IPspace에서 자동으로 생성된 새 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 도달 가능성 복구 노드 포트 • 참고: * 모든 인터페이스 그룹(ifgrp) 구성원 포트가 보고되면 `no-reachability`를 실행합니다 `network port reachability repair` 각 멤버 포트의 명령은 각 멤버를 ifgrp에서 제거하고 새 브로드캐스트 도메인에 배치하도록 하여 결국 ifgrp 자체를 제거합니다. 를 실행하기 전에 `network port reachability repair` 명령을 실행하여 포트의 연결 가능한 브로드캐스트 도메인이 물리적 네트워크 토폴로지를 기준으로 예상한 것인지 확인합니다. 에 대한 자세한 내용은 `network port reachability repair` "ONTAP 명령 참조입니다"을 참조하십시오.
다중 도메인 내의 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트의 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다".
알 수 없음	도달 가능성 - 상태가 "알 수 없음"인 경우 몇 분 정도 기다린 후 명령을 다시 시도하십시오.

포트를 복구한 후에는 교체된 LIF 및 VLAN을 확인하십시오. 포트가 인터페이스 그룹의 일부인 경우 해당 인터페이스 그룹의 변경 사항도 이해해야 합니다.

LIF

포트가 복구되어 다른 브로드캐스트 도메인으로 이동되면 복구된 포트에 구성된 모든 LIF에 새 홈 포트가 자동으로 할당됩니다. 가능한 경우 동일한 노드의 동일한 브로드캐스트 도메인에서 해당 홈 포트가 선택됩니다. 또는 다른 노드의 홈 포트를 선택하거나 적합한 홈 포트가 없는 경우 홈 포트가 지워집니다.

LIF의 홈 포트를 다른 노드로 이동하거나 확보하면 LIF가 "변위"된 것으로 간주됩니다. 교체된 LIF는 다음 명령을 통해 확인할 수 있습니다.

디시퍼인터페이스 쇼

교체된 LIF가 있는 경우 다음 중 하나를 수행해야 합니다.

- 교체된 LIF의 홈을 복원합니다.

  인터페이스 복구

- LIF의 홈을 수동으로 설정합니다.

  네트워크 인터페이스 수정-홈-포트-홈-노드

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

- LIF의 현재 구성된 홈에 만족하는 경우 "교체된 인터페이스" 테이블에서 항목을 제거합니다.

  dissplac된 인터페이스 삭제

VLAN

복구된 포트에 VLAN이 있는 경우 해당 VLAN은 자동으로 삭제되지만 "교체된" VLAN으로 기록됩니다. 다음과 같은 교체된 VLAN을 볼 수 있습니다.

디세퍼드-VLAN 쇼

교체된 VLAN이 있는 경우 다음 중 하나를 수행해야 합니다.

- VLAN을 다른 포트로 복구합니다.

  디즈퍼스VLAN 복원

- "교체된 VLAN" 테이블에서 항목을 제거합니다.

  dissplac된 - vLANs delete

인터페이스 그룹

복구된 포트가 인터페이스 그룹의 일부인 경우 해당 인터페이스 그룹에서 제거됩니다. 인터페이스 그룹에 할당된 유일한 구성원 포트인 경우 인터페이스 그룹 자체가 제거됩니다.

관련 정보

- "업그레이드 후 네트워크 구성을 확인합니다"
- "네트워크 포트의 연결 상태를 모니터링합니다"
- "ONTAP 명령 참조입니다"

ONTAP 브로드캐스트 도메인을 IPspace로 이동합니다

ONTAP 9.8부터 계층 2 접근성을 기반으로 시스템이 만든 브로드캐스트 도메인을 사용자가 만든 IPspace로 이동할 수 있습니다.

브로드캐스트 도메인을 이동하기 전에 브로드캐스트 도메인의 포트 도달 가능 여부를 확인해야 합니다.

포트의 자동 스캐닝은 서로 연결할 수 있는 포트를 확인하여 동일한 브로드캐스트 도메인에 배치할 수 있지만 이 스캐닝에서 적절한 IPspace를 확인할 수 없습니다. 브로드캐스트 도메인이 기본 IPspace에 속한 경우 이 섹션의 단계를 사용하여 수동으로 이동해야 합니다.

시작하기 전에

브로드캐스트 도메인은 클러스터 생성 및 연결 작업의 일부로 자동으로 구성됩니다. ONTAP는 "기본" 브로드캐스트 도메인을 "클러스터에서 생성된 첫 번째 노드의 관리 인터페이스 홈 포트에 대한 계층 2 연결이 있는 포트 세트로 정의합니다. 필요한 경우 다른 브로드캐스트 도메인이 생성되고 이름이 * Default-1 *, * Default-2 * 등으로 지정됩니다.

노드가 기존 클러스터에 연결되면 해당 네트워크 포트는 계층 2 도달 가능 여부에 따라 기존 브로드캐스트 도메인에 자동으로 연결됩니다. 기존 브로드캐스트 도메인에 대한 도달 기능이 없는 경우 포트가 하나 이상의 새 브로드캐스트 도메인에 배치됩니다.

이 작업에 대해

- 클러스터 LIF가 있는 포트는 "클러스터" IPspace에 자동으로 배치되며
- 노드 관리 LIF의 홈 포트에 대한 연결 기능이 있는 포트는 "기본" 브로드캐스트 도메인에 배치됩니다.
- 다른 브로드캐스트 도메인은 클러스터 생성 또는 연결 작업의 일부로 ONTAP에 의해 자동으로 생성됩니다.
- VLAN 및 인터페이스 그룹을 추가하면 생성된 후 약 1분 후에 해당 브로드캐스트 도메인에 자동으로 배치됩니다.

단계

1. 브로드캐스트 도메인의 포트 도달 가능 여부를 확인합니다. ONTAP는 레이어 2 내 상태를 자동으로 모니터링합니다. 다음 명령을 사용하여 각 포트가 브로드캐스트 도메인에 추가되고 "확인" 기능이 있는지 확인합니다.

   네트워크 포트 도달 가능성 세부 정보

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

2. 필요한 경우 브로드캐스트 도메인을 다른 IPspace로 이동:

   네트워크 포트 브로드캐스트 도메인 이동

   예를 들어 브로드캐스트 도메인을 "기본값"에서 "IPS1"으로 이동하려면:

   네트워크 포트 브로드캐스트-도메인 이동-IPSpace 기본-브로드캐스트-도메인 기본-IPSpace IPS1

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 이동"

ONTAP 브로드캐스트 도메인을 분할합니다

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경된 경우 또한 단일 브로드캐스트 도메인에 이전에 구성된 네트워크 포트 그룹이 두 개의 서로 다른 도달 가능성 집합으로 분할되어 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다.

> 브로드캐스트 도메인을 분할하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 분할해야 하는 경우 을 "브로드캐스트 도메인 분할(ONTAP 9.7 이하)"참조하십시오.

네트워크 포트 브로드캐스트 도메인이 둘 이상의 연결 집합으로 분할되었는지 확인하려면 명령을 사용하여 `network port reachability show -details` 서로 연결되지 않은 포트("연결할 수 없는 포트")에 주의를 기울이십시오. 일반적으로 연결할 수 없는 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 다른 브로드캐스트 도메인으로 분할해야 하는 포트 집합을 정의합니다. 에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

브로드캐스트 도메인을 두 개의 브로드캐스트 도메인으로 분할:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- IPSpace_name은 브로드캐스트 도메인이 있는 IPSpace의 이름입니다.
- 브로드캐스트 도메인은 분할될 브로드캐스트 도메인의 이름입니다.
- 새 브로드캐스트 도메인은 생성되는 새 브로드캐스트 도메인의 이름입니다.
- 포트란 새 브로드캐스트 도메인에 추가될 노드 이름과 포트입니다.

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 분할입니다"

ONTAP 브로드캐스트 도메인을 병합합니다

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경되었고 이전에 여러 브로드캐스트 도메인에 구성된 두 개의 네트워크 포트 그룹이 이제 모두 공유 도달 가능 상태로 변경된 경우 두 개의 브로드캐스트 도메인을 병합하여 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다.

> 브로드캐스트 도메인을 병합하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 병합해야 하는 경우 을 "브로드캐스트 도메인 병합(ONTAP 9.7 이하)"참조하십시오.

여러 브로드캐스트 도메인이 하나의 도달 가능성 집합에 속하는지 확인하려면 다음을 사용하십시오. `network port reachability show -details` 명령을 내리고 다른 브로드캐스트 도메인에 구성된 포트 중 실제로 서로 연결되어 있는 포트가 무엇인지 주의 깊게 살펴보세요("예기치 않은 포트"). 일반적으로 예기치 않은 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 브로드캐스트 도메인에 병합되어야 하는 포트 집합을 정의합니다.

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

단계

한 브로드캐스트 도메인의 포트를 기존 브로드캐스트 도메인으로 병합:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- IPSpace_name은 브로드캐스트 도메인이 있는 IPSpace의 이름입니다.
- '-broadcast-domain'은 통합될 브로드캐스트 도메인의 이름입니다.
- '-브로드캐스트-도메인'은 추가 포트를 받을 브로드캐스트 도메인의 이름입니다.

관련 정보

- "네트워크 포트 브로드캐스트-도메인-병합"

ONTAP 브로드캐스트 도메인의 포트에 대한 MTU 값을 변경합니다

브로드캐스트 도메인의 MTU 값을 수정하여 해당 브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경할 수 있습니다. 이 작업은 네트워크에서 수행된 토폴로지 변경을 지원하기 위해 수행할 수 있습니다.

> 브로드캐스트 도메인 포트의 MTU 값을 변경하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인 포트의 MTU 값을 변경해야 하는 경우을 참조하십시오"브로드캐스트 도메인의 포트에 대한 MTU 값 변경(ONTAP 9.7 이하)".

시스템 관리자

ONTAP 9.12.1부터 System Manager를 사용하여 브로드캐스트 도메인의 MTU 값을 수정하면 해당 브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경할 수 있습니다.

단계

1. *Network > Broadcast Domains*를 선택합니다.
2. 브로드캐스트 도메인 섹션에서 MTU 값을 변경하려는 브로드캐스트 도메인의 이름을 선택합니다.
3. 브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경할 것인지 확인하는 메시지가 나타납니다. 변경을 진행하려면 *Yes*를 클릭하십시오.
4. 필요에 따라 MTU 값을 수정하고 변경 사항을 저장하십시오.

   시스템은 브로드캐스트 도메인의 모든 포트에 새 MTU 값을 적용하므로 해당 포트를 통한 트래픽이 잠시 중단됩니다.

CLI를 참조하십시오

시작하기 전에

MTU 값은 e0M 포트 처리 관리 트래픽을 제외하고 해당 계층 2 네트워크에 연결된 모든 장치와 일치해야 합니다.

이 작업에 대해

MTU 값을 변경하면 해당 포트를 통한 트래픽이 잠시 중단됩니다. 시스템에 메시지가 표시되며, MTU 변경을 위해서는 *y*를 입력해야 합니다.

단계

브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경합니다.

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

위치:

- broadcast_domain은 브로드캐스트 도메인의 이름입니다.
- Mtu는 IP 패킷의 MTU 크기이고 1500과 9000은 일반적인 값입니다.
- `ipspace`는 이 브로드캐스트 도메인이 상주하는 IPspace의 이름입니다. 이 옵션에 값을 지정하지 않으면 "Default" IPspace가 사용됩니다.

  다음 명령은 브로드캐스트 도메인 bcast1의 모든 포트에 대한 MTU를 9000으로 변경합니다.

  ```
  network port broadcast-domain modify -broadcast-domain <Default-1>
  -mtu < 9000 >
  Warning: Changing broadcast domain settings will cause a momentary
  data-serving interruption.
  Do you want to continue? {y|n}: <y>
  ```

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 수정"

ONTAP 브로드캐스트 도메인을 봅니다

클러스터의 각 IPspace 내에서 브로드캐스트 도메인 목록을 표시할 수 있습니다. 출력에는 각 브로드캐스트 도메인의 포트 목록과 MTU 값도 표시됩니다.

> 브로드캐스트 도메인을 표시하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에 브로드캐스트 도메인을 표시해야 하는 경우 을 참조하십시오"브로드캐스트 도메인 표시(ONTAP 9.7 이하)".

단계

클러스터의 브로드캐스트 도메인 및 관련 포트를 표시합니다.

```
network port broadcast-domain show
```

다음 명령을 실행하면 클러스터의 모든 브로드캐스트 도메인 및 관련 포트가 표시됩니다.

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Cluster Cluster      9000
                            cluster-1-01:e0a       complete
                            cluster-1-01:e0b       complete
                            cluster-1-02:e0a       complete
                            cluster-1-02:e0b       complete
Default Default      1500
                            cluster-1-01:e0c       complete
                            cluster-1-01:e0d       complete
                            cluster-1-02:e0c       complete
                            cluster-1-02:e0d       complete
        Default-1    1500
                            cluster-1-01:e0e       complete
                            cluster-1-01:e0f       complete
                            cluster-1-01:e0g       complete
                            cluster-1-02:e0e       complete
                            cluster-1-02:e0f       complete
                            cluster-1-02:e0g       complete
```

다음 명령을 실행하면 Default-1 브로드캐스트 도메인의 포트가 오류 상태로 표시되며, 이는 포트를 올바르게 업데이트할 수 없음을 나타냅니다.

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                    Update
Name    Domain Name  MTU   Port List                 Status Details
------- ----------- -----  ---------------------- --------------
Default Default-1   1500
                           cluster-1-02:e0g        error
```

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 표시"

ONTAP 브로드캐스트 도메인을 삭제합니다

브로드캐스트 도메인이 더 이상 필요하지 않으면 삭제할 수 있습니다. 이렇게 하면 해당 브로드캐스트 도메인과 연결된 포트가 "기본" IPspace로 이동합니다.

시작하기 전에

삭제할 브로드캐스트 도메인에 연결된 서브넷, 네트워크 인터페이스 또는 SVM이 없어야 합니다.

이 작업에 대해

- 시스템에서 생성한 "클러스터" 브로드캐스트 도메인은 삭제할 수 없습니다.
- 브로드캐스트 도메인을 삭제하면 브로드캐스트 도메인과 관련된 모든 페일오버 그룹이 제거됩니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 브로드캐스트 도메인 * 을 삭제할 수 있습니다

브로드캐스트 도메인에 포트가 포함되어 있거나 서브넷에 연결되어 있는 경우에는 삭제 옵션이 표시되지 않습니다.

단계

1. 네트워크 > 개요 > 브로드캐스트 도메인 * 을 선택합니다.
2. 제거할 브로드캐스트 도메인 옆의 * > 삭제 * 를 선택합니다 ⋮ .

CLI를 참조하십시오

- CLI를 사용하여 브로드캐스트 도메인 * 을 삭제합니다

단계

브로드캐스트 도메인 삭제:

'network port broadcast-domain delete-broadcast-domain_broadcast_domain_name_[-IPSpace_IPSpace_name_]'

다음 명령을 실행하면 IPspace ipspac1에서 브로드캐스트 도메인 Default-1이 삭제됩니다.

'network port broadcast-domain delete-broadcast-domain_Default-1_-IPSpace_ipspace1_'

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 삭제"

페일오버 그룹 및 정책

ONTAP 네트워크에서의 **LIF** 페일오버에 대해 알아보십시오

LIF 페일오버는 LIF의 현재 포트에서 링크 장애가 발생할 경우 LIF가 다른 네트워크 포트로 자동 마이그레이션되는 것을 의미합니다. 이 기능은 SVM에 대한 연결을 위한 고가용성을 제공하는 핵심 구성요소입니다. LIF 페일오버를 구성하려면 페일오버 그룹을 생성하고, 페일오버 그룹을 사용하도록 LIF를 수정하고, 페일오버 정책을 지정해야 합니다.

페일오버 그룹에는 클러스터에 있는 하나 이상의 노드의 네트워크 포트 세트(물리적 포트, VLAN 및 인터페이스 그룹)가 포함됩니다. 페일오버 그룹에 있는 네트워크 포트는 LIF에 사용할 수 있는 페일오버 타겟을 정의합니다. 페일오버 그룹은 클러스터 관리, 노드 관리, 인터클러스터 및 NAS 데이터 LIF가 할당될 수 있습니다.

> LIF가 유효한 페일오버 대상이 없이 구성되면 LIF가 페일오버를 시도할 때 중단이 발생합니다. 명령을 사용하여 페일오버 구성을 확인할 수 `network interface show -failover` 있습니다. 에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

브로드캐스트 도메인을 생성하면 동일한 네트워크 포트를 포함하는 동일한 이름의 페일오버 그룹이 자동으로 생성됩니다. 이 페일오버 그룹은 시스템에서 자동으로 관리됩니다. 즉, 포트가 브로드캐스트 도메인에서 추가되거나 제거될 때 포트가 이 페일오버 그룹에서 자동으로 추가 또는 제거됩니다. 이 기능은 고유한 페일오버 그룹을 관리하지

않으려는 관리자에게 효율적으로 제공됩니다.

ONTAP 페일오버 그룹을 생성합니다

네트워크 포트의 페일오버 그룹을 생성하면 LIF의 현재 포트에서 링크 장애가 발생할 경우 LIF가 자동으로 다른 포트로 마이그레이션할 수 있습니다. 이렇게 하면 시스템이 네트워크 트래픽을 클러스터의 사용 가능한 다른 포트로 재라우팅할 수 있습니다.

이 작업에 대해

'network interface failover-groups create' 명령을 사용하여 그룹을 생성하고 그룹에 포트를 추가합니다.

- 페일오버 그룹에 추가된 포트는 네트워크 포트, VLAN 또는 인터페이스 그룹(ifgrp)일 수 있습니다.
- 페일오버 그룹에 추가된 모든 포트는 동일한 브로드캐스트 도메인에 속해야 합니다.
- 단일 포트는 여러 페일오버 그룹에 상주할 수 있습니다.
- 다른 VLAN 또는 브로드캐스트 도메인에 LIF가 있는 경우 각 VLAN 또는 브로드캐스트 도메인에 대해 페일오버 그룹을 구성해야 합니다.
- SAN iSCSI 또는 FC 환경에서는 페일오버 그룹이 적용되지 않습니다.

단계

페일오버 그룹 생성:

'network interface failover-groups create-vserver_vserver_name_-failover-group_failover_group_name_-targets_ports_list_'

- '*vserver_name*'은 페일오버 그룹을 사용할 수 있는 SVM의 이름입니다.
- '*failover_group_name*'은 생성할 페일오버 그룹의 이름입니다.
- '*ports_list*'는 페일오버 그룹에 추가될 포트 목록입니다. 포트는 format_node_name>:<port_number>_에 추가됩니다(예: node1:e0c).

다음 명령을 실행하면 SVM vs3용 페일오버 그룹 fg3이 생성되고 2개의 포트가 추가됩니다.

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

작업을 마친 후

- 페일오버 그룹이 생성되었으므로 페일오버 그룹을 LIF에 적용해야 합니다.
- LIF에 유효한 페일오버 타겟을 제공하지 않는 페일오버 그룹을 적용하면 경고 메시지가 표시됩니다.

  유효한 페일오버 목표가 없는 LIF가 페일오버를 시도하면 운영 중단이 발생할 수 있습니다.

- 에 대한 자세한 내용은 `network interface failover-groups create` "ONTAP 명령 참조입니다"을 참조하십시오.

LIF에 대한 ONTAP 페일오버 설정을 구성합니다

페일오버 정책과 페일오버 그룹을 LIF에 적용하여 LIF를 특정 네트워크 포트 그룹으로 페일오버할 수 있습니다. LIF가 다른 포트로 페일오버되지 않도록 설정할 수도 있습니다.

이 작업에 대해

- LIF가 생성되면 LIF 페일오버가 기본적으로 활성화되며 사용 가능한 타겟 포트 목록은 LIF 유형 및 서비스 정책에 따라 기본 페일오버 그룹 및 페일오버 정책에 따라 결정됩니다.

  9.5부터 LIF를 사용할 수 있는 네트워크 서비스를 정의하는 LIF의 서비스 정책을 지정할 수 있습니다. 일부 네트워크 서비스에서는 LIF에 페일오버 제한을 적용합니다.

  > LIF의 서비스 정책이 페일오버를 더욱 제한하는 방식으로 변경되면 LIF의 페일오버 정책이 시스템에 의해 자동으로 업데이트됩니다.

- network interface modify 명령에서 -failover -group 및 -failover -policy 매개 변수의 값을 지정하여 LIF의 페일오버 동작을 수정할 수 있습니다.
- LIF가 수정되어 LIF에 유효한 페일오버 타겟이 없게 되면 경고 메시지가 표시됩니다.

  유효한 페일오버 목표가 없는 LIF가 페일오버를 시도하면 운영 중단이 발생할 수 있습니다.

- ONTAP 9.11.1부터 ASA(All-Flash SAN 어레이) 플랫폼에서는 새로 생성된 스토리지 VM에서 새로 생성된 iSCSI LIF에 대해 iSCSI LIF 페일오버가 자동으로 활성화됩니다.

  또한, 할 수 있습니다 "기존 iSCSI LIF에서 iSCSI LIF 페일오버를 수동으로 활성화합니다"는 ONTAP 9.11.1 이상으로 업그레이드하기 전에 생성된 LIF를 의미합니다.

- 다음 목록에서는 -failover-policy 설정이 페일오버 그룹에서 선택한 타겟 포트에 미치는 영향에 대해 설명합니다.

  > iSCSI LIF 페일오버의 경우 페일오버 정책 '로컬 전용', 'fo 파트너 전용', '사용 안 함'만 지원됩니다.

- 브로드캐스트 도메인 전체에 적용되는 것은 페일오버 그룹의 모든 노드에 있는 모든 포트에 적용됩니다.
- '시스템 정의'는 LIF 홈 노드의 포트와 클러스터의 다른 노드(일반적으로 SFO가 아닌 파트너)에만 적용됩니다.
- '로컬 전용'은 LIF의 홈 노드에 있는 포트에만 적용됩니다.
- 'fo 파트너 전용'은 LIF 홈 노드와 SFO 파트너에 있는 포트에만 적용됩니다.
- "사용 안 함"은 LIF가 페일오버 대상으로 구성되지 않았음을 나타냅니다.

단계

기존 인터페이스에 대한 페일오버 설정을 구성합니다.

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

페일오버 설정 구성 및 페일오버 해제의 예

다음 명령은 페일오버 정책을 브로드캐스트 도메인 전체에 설정하고 페일오버 그룹 fg3의 포트를 SVM vs3의 LIF

data1의 페일오버 타겟으로 사용합니다.

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1           broadcast-domain-wide  fg3
```

다음 명령을 실행하면 SVM vs3에서 LIF 데이터 1의 페일오버가 사용되지 않습니다.

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

관련 정보

- "네트워크 인터페이스"

ONTAP 명령으로 페일오버 그룹 및 정책을 관리할 수 있습니다

네트워크 인터페이스 페일오버 그룹 명령을 사용하여 페일오버 그룹을 관리할 수 있습니다. 'network interface modify' 명령을 사용하여 LIF에 적용되는 페일오버 그룹 및 페일오버 정책을 관리할 수 있습니다.

원하는 작업	이 명령 사용...
페일오버 그룹에 네트워크 포트를 추가합니다	네트워크 인터페이스 페일오버 그룹 추가 타겟
페일오버 그룹에서 네트워크 포트를 제거합니다	네트워크 인터페이스 페일오버 그룹 제거 대상
페일오버 그룹의 네트워크 포트를 수정합니다	네트워크 인터페이스 페일오버 그룹 수정
현재 페일오버 그룹을 표시합니다	네트워크 인터페이스 페일오버 그룹들이 보여줌
LIF에서 페일오버를 구성합니다	네트워크 인터페이스 수정-페일오버-그룹-페일오버-정책
각 LIF에서 사용 중인 페일오버 그룹 및 페일오버 정책을 표시합니다	네트워크 인터페이스 보기 필드 장애 조치 그룹 장애 조치 정책
페일오버 그룹의 이름을 바꿉니다	네트워크 인터페이스 페일오버 그룹 이름 바꾸기
페일오버 그룹을 삭제합니다	네트워크 인터페이스 페일오버 그룹 삭제

> 페일오버 그룹을 수정하여 클러스터의 모든 LIF에 유효한 페일오버 목표를 제공하지 않으면 LIF에서 페일오버를 시도할 때 운영 중단이 발생할 수 있습니다.

관련 정보

- "네트워크 인터페이스"

서브넷(클러스터 관리자만 해당)

ONTAP 네트워크의 서브넷에 대해 알아봅니다

서브넷을 사용하면 ONTAP 네트워크 구성을 위해 특정 블록 또는 IP 주소 풀을 할당할 수 있습니다. 따라서 IP 주소와 네트워크 마스크 값을 지정하지 않고 서브넷 이름을 지정하여 LIF를 더 쉽게 생성할 수 있습니다.

서브넷은 브로드캐스트 도메인 내에서 생성되며 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함됩니다. LIF가 생성될 때 서브넷의 IP 주소가 브로드캐스트 도메인의 포트에 할당됩니다. LIF가 제거되면 IP 주소가 서브넷 풀로 반환되며 향후 LIF에서 사용할 수 있습니다.

서브넷을 사용하면 IP 주소를 훨씬 쉽게 관리할 수 있으며 LIF를 더 쉽게 생성할 수 있으므로 서브넷을 사용하는 것이 좋습니다. 또한, 서브넷을 정의할 때 게이트웨이를 지정하면 해당 서브넷을 사용하여 LIF가 생성될 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.

ONTAP 네트워크에 대한 서브넷을 생성합니다

나중에 SVM에 대한 LIF를 생성할 때 사용할 IPv4 또는 IPv6 주소의 특정 블록을 할당하는 서브넷을 생성할 수 있습니다.

따라서 각 LIF에 대한 IP 주소와 네트워크 마스크 값을 지정하지 않고 서브넷 이름을 지정하여 LIF를 더 쉽게 생성할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

서브넷을 추가하려는 브로드캐스트 도메인 및 IPspace가 이미 있어야 합니다.

이 작업에 대해

- 모든 서브넷 이름은 IPspace 내에서 고유해야 합니다.
- 서브넷에 IP 주소 범위를 추가할 때 네트워크에 중복되는 IP 주소가 없는지 확인해야 합니다. 이렇게 하면 다른 서브넷 또는 호스트가 동일한 IP 주소를 사용하지 않도록 할 수 있습니다.
- 서브넷을 정의할 때 게이트웨이를 지정하면 해당 서브넷을 사용하여 LIF가 생성될 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다. 서브넷을 사용하지 않거나 서브넷을 정의할 때 게이트웨이를 지정하지 않으면 수동으로 SVM에 경로를 추가하려면 'route create' 명령을 사용해야 합니다.
- NetApp은 데이터 SVM의 모든 LIF에 대한 서브넷 개체를 생성할 것을 권장합니다. 이는 각 서브넷 객체에 연결된 브로드캐스트 도메인이 있기 때문에 ONTAP에서 대상 클러스터의 페일오버 대상을 결정할 수 있도록 서브넷 객체를 사용하는 MetroCluster 구성에서 특히 중요합니다.

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 서브넷을 생성할 수 있습니다.

시스템 관리자

ONTAP 9.12.0부터는 시스템 관리자를 사용하여 서브넷을 생성할 수 있습니다.

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 서브넷을 만들려면 + Add 클릭합니다.
3. 서브넷 이름을 지정합니다.
4. 서브넷 IP 주소를 지정합니다.
5. 서브넷 마스크를 설정합니다.
6. 서브넷을 구성하는 IP 주소의 범위를 정의합니다.
7. 유용한 경우 게이트웨이를 지정합니다.
8. 서브넷이 속한 브로드캐스트 도메인을 선택합니다.
9. 변경 사항을 저장합니다.
   a. 입력한 IP 주소 또는 범위가 이미 인터페이스에서 사용되는 경우 다음 메시지가 표시됩니다. "이 범위의 IP 주소는 LIF에서 이미 사용 중입니다. LIF를 이 서브넷과 연결하시겠습니까?"라는 문구입니다
   b. OK * 를 클릭하면 기존 LIF가 서브넷에 연결됩니다.

CLI를 참조하십시오

CLI를 사용하여 서브넷을 생성합니다.

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- 'subnet_name'은 만들려는 계층 3 서브넷의 이름입니다.

  이름은 "Mgmt"와 같은 텍스트 문자열이거나 192.0.2.0/24와 같은 특정 서브넷 IP 값일 수 있습니다.

- broadcast_domain_name은 서브넷이 상주할 브로드캐스트 도메인의 이름입니다.
- IPSpace_name은 브로드캐스트 도메인이 속한 IPspace의 이름입니다.

  이 옵션에 대한 값을 지정하지 않으면 "기본" IPspace가 사용됩니다.

- Subnet_address는 서브넷의 IP 주소와 마스크입니다(예: 192.0.2.0/24).
- gateway_address는 192.0.2.1과 같이 서브넷의 기본 라우트에 대한 게이트웨이입니다.
- IP_address_list는 서브넷에 할당할 IP 주소의 목록 또는 범위입니다.

  IP 주소는 개별 주소, IP 주소 범위 또는 쉼표로 구분된 목록의 조합이 될 수 있습니다.

- TRUE 값은 '-force-update-lif-associations' 옵션에 설정할 수 있습니다.

서비스 프로세서 또는 네트워크 인터페이스가 현재 지정된 범위의 IP 주소를 사용하는 경우 이 명령은 실패합니다. 이 값을 true 로 설정하면 수동으로 주소를 지정한 모든 인터페이스가 현재 서브넷에 연결되어 명령이 성공할 수 있습니다.

다음 명령을 실행하면 기본 IPspace에 브로드캐스트 도메인 Default-1에 서브넷 하위 1이 생성됩니다. IPv4 서브넷 IP 주소 및 마스크, 게이트웨이 및 IP 주소 범위를 추가합니다.

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

다음 명령을 실행하면 "기본" IPspace에서 브로드캐스트 도메인 Default에 서브넷 하위 2가 생성됩니다. 다음과 같은 다양한 IPv6 주소가 추가됩니다.

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

서브넷의 주소를 사용하여 SVM 및 인터페이스를 IPspace에 할당할 수 있습니다.

기존 서브넷의 이름을 변경해야 할 경우에는 네트워크 서브넷 이름 바꾸기 명령을 사용합니다.

에 대한 자세한 내용은 `network subnet rename` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크의 서브넷에서 IP 주소를 추가하거나 제거합니다

처음에 서브넷을 생성할 때 IP 주소를 추가하거나 이미 존재하는 서브넷에 IP 주소를 추가할 수 있습니다. 기존 서브넷에서 IP 주소를 제거할 수도 있습니다. 따라서 SVM에 필요한 IP 주소만 할당할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 서브넷 * 에 IP 주소를 추가하거나 제거할 수 있습니다

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 변경할 서브넷 옆의 * > 편집 * 을 선택합니다 ⋮ .
3. IP 주소를 추가하거나 제거합니다.
4. 변경 사항을 저장합니다.
   a. 입력한 IP 주소 또는 범위가 이미 인터페이스에서 사용되는 경우 다음 메시지가 표시됩니다. "이 범위의 IP 주소는 LIF에서 이미 사용 중입니다. LIF를 이 서브넷과 연결하시겠습니까?"라는 문구입니다
   b. OK * 를 클릭하면 기존 LIF가 서브넷에 연결됩니다.

CLI를 참조하십시오

- CLI를 사용하여 IP 주소를 서브넷 * 에 추가하거나 서브넷에서 제거합니다

이 작업에 대해

IP 주소를 추가할 때 서비스 프로세서 또는 네트워크 인터페이스가 추가되는 범위의 IP 주소를 사용하는 경우 오류가 발생합니다. 수동으로 주소를 지정한 인터페이스를 현재 서브넷에 연결하려면 '-force-update-lif-associations' 옵션을 'true'로 설정합니다.

IP 주소를 제거할 때 서비스 프로세서 또는 네트워크 인터페이스에서 제거 중인 IP 주소를 사용하는 경우 오류가 발생합니다. 서브넷에서 IP 주소를 제거한 후에도 인터페이스가 계속 사용하도록 하려면 "-force-update-lif-associations" 옵션을 "true"로 설정합니다.

단계

서브넷에서 IP 주소 추가 또는 제거:

원하는 작업	이 명령 사용…
IP 주소를 서브넷에 추가합니다	네트워크 서브넷 추가 범위
서브넷에서 IP 주소를 제거합니다	네트워크 서브넷 remove-range

다음 명령을 실행하면 서브넷 sub1에 IP 주소 192.0.2.82 ~ 192.0.2.85 가 추가됩니다.

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

다음 명령을 실행하면 서브넷 하위 3에서 IP 주소 198.51.100.9가 제거됩니다.

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

현재 범위에 1 ~ 10 및 20 ~ 40이 포함되어 있고 11 ~ 19 및 41 ~ 50(기본적으로 1 ~ 50을 허용)을 추가하려는 경우 다음 명령을 사용하여 기존 주소 범위와 겹칠 수 있습니다. 이 명령은 새 주소만 추가하며 기존 주소에는 영향을 주지 않습니다.

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-198.51.10.50>
```

및 `network subnet remove-ranges` 에 대한 자세한 `network subnet add-ranges` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 네트워크의 서브넷 속성을 변경합니다

기존 서브넷에서 서브넷 주소 및 마스크 값, 게이트웨이 주소 또는 IP 주소 범위를 변경할 수 있습니다.

이 작업에 대해

- IP 주소를 수정할 때 다른 서브넷 또는 호스트가 동일한 IP 주소를 사용하지 않도록 네트워크에 중복되는 IP 주소가 없는지 확인해야 합니다.
- 게이트웨이 IP 주소를 추가하거나 변경할 경우, 서브넷을 사용하여 LIF를 생성할 때 수정된 게이트웨이가 새로운 SVM에 적용됩니다. 경로가 존재하지 않을 경우 SVM을 위해 게이트웨이로 가는 기본 경로가 생성됩니다. 게이트웨이 IP 주소를 변경할 때 SVM에 새 경로를 수동으로 추가해야 할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 서브넷 속성을 변경할 수 있습니다 *

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 변경할 서브넷 옆의 * > 편집 * 을 선택합니다 ⋮.
3. 변경합니다.
4. 변경 사항을 저장합니다.
   a. 입력한 IP 주소 또는 범위가 이미 인터페이스에서 사용되는 경우 다음 메시지가 표시됩니다. "이 범위의 IP 주소는 LIF에서 이미 사용 중입니다. LIF를 이 서브넷과 연결하시겠습니까?"라는 문구입니다
   b. OK * 를 클릭하면 기존 LIF가 서브넷에 연결됩니다.

CLI를 참조하십시오

- CLI를 사용하여 서브넷 속성을 변경합니다 *

단계

서브넷 속성 수정:

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- 'subnet_name'은 수정하려는 서브넷의 이름입니다.
- IPSpace는 서브넷이 상주하는 IPspace의 이름입니다.
- 'Subnet'은 192.0.2.0/24와 같이 해당되는 경우 서브넷의 새로운 주소 및 마스크입니다.
- 게이트웨이(gateway)는 192.0.2.1과 같이 해당되는 경우 서브넷의 새로운 게이트웨이입니다. "" * 를 입력하면 게이트웨이 항목이 제거됩니다.
- IP_range는 해당되는 경우 서브넷에 할당될 IP 주소의 새 목록 또는 범위입니다. IP 주소는 개별 주소, 범위 또는 IP 주소 또는 쉼표로 구분된 목록의 조합이 될 수 있습니다. 여기에 지정된 범위가 기존 IP 주소를 대체합니다.
- IP 주소 범위를 변경할 때 'force-update-lif-associations'가 필요합니다. IP 주소 범위를 수정할 때 이 옵션에 대해 값을 * TRUE * 로 설정할 수 있습니다. 서비스 프로세서 또는 네트워크 인터페이스가 지정된 범위의 IP 주소를 사용하는 경우 이 명령은 실패합니다. 이 값을 * true * 로 설정하면 수동으로 주소를 지정한 모든 인터페이스가 현재 서브넷에 연결되어 명령이 성공할 수 있습니다.

다음 명령을 실행하면 서브넷 sub3의 게이트웨이 IP 주소가 수정됩니다.

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

에 대한 자세한 내용은 `network subnet modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크의 서브넷을 봅니다

IPspace 내의 각 서브넷에 할당된 IP 주소 목록을 표시할 수 있습니다. 출력에는 각 서브넷에서 사용할 수 있는 총 IP 주소 수와 현재 사용 중인 주소 수도 표시됩니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 서브넷 * 을 표시할 수 있습니다

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 서브넷 목록을 봅니다.

CLI를 참조하십시오

- CLI를 사용하여 서브넷 * 을 표시합니다

단계

서브넷 목록과 해당 서브넷에서 사용되는 관련 IP 주소 범위를 표시합니다.

```
network subnet show
```

다음 명령을 실행하면 서브넷 및 서브넷 속성이 표시됩니다.

```
network subnet show

IPspace: Default
Subnet                  Broadcast                Avail/
Name    Subnet          Domain    Gateway        Total    Ranges
-----   --------------- --------- ------------ --------
------------------------
sub1    192.0.2.0/24     bcast1   192.0.2.1      5/9      192.0.2.92-
192.0.2.100
sub3    198.51.100.0/24  bcast3   198.51.100.1    3/3
198.51.100.7,198.51.100.9
```

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

ONTAP 네트워크에서 서브넷을 삭제합니다

서브넷이 더 이상 필요하지 않고 서브넷에 할당된 IP 주소를 할당 해제하려는 경우 삭제할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터는 시스템 관리자를 사용하여 서브넷 * 을 삭제할 수 있습니다

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 제거하려는 서브넷 옆의 * > 삭제 * 를 선택합니다 ⋮ .
3. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 서브넷을 삭제합니다 *

이 작업에 대해

서비스 프로세서 또는 네트워크 인터페이스가 현재 지정된 범위의 IP 주소를 사용하는 경우 오류가 발생합니다. 서브넷이 삭제된 후에도 인터페이스가 IP 주소를 계속 사용하도록 하려면 -force-update-lif-associations 옵션을 true 로 설정하여 LIF와 서브넷의 연결을 제거할 수 있습니다.

단계

서브넷 삭제:

'network subnet delete -subnet-name subnet_name[-IPSpace IPSpace_name][-force-update-lif-associations true]'

다음 명령을 실행하면 IPspace ipspac1에서 서브넷 sub1이 삭제됩니다.

네트워크 서브넷 delete-subnet-name sub1-IPSpace ipspace1

에 대한 자세한 내용은 `network subnet delete` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크용 SVM을 생성합니다

SVM을 생성하여 고객에게 데이터를 제공해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- SVM 루트 볼륨에 있을 보안 스타일을 알아야 합니다.

  이 SVM에서 Hyper-V 또는 SQL Server over SMB 솔루션을 구축하려는 경우 루트 볼륨에 NTFS 보안 스타일을 사용해야 합니다. Hyper-V 파일 또는 SQL 데이터베이스 파일이 포함된 볼륨은 만들 때 NTFS 보안으로 설정되어야 합니다. 루트 볼륨 보안 스타일을 NTFS로 설정하면 실수로 UNIX 또는 혼합 보안 스타일 데이터 볼륨을 만들지 않아도 됩니다.

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 을 SVM 용량 관리참조하십시오.

시스템 관리자

System Manager를 사용하여 스토리지 VM을 생성할 수 있습니다.

단계

1. 스토리지 VM * 을 선택합니다.
2. + Add 스토리지 VM을 생성하려면 클릭하십시오.
3. 스토리지 VM의 이름을 지정합니다.
4. 액세스 프로토콜을 선택합니다.
    - SMB/CIFS, NFS를 지원합니다
    - iSCSI
    - FC
    - NVMe를 참조하십시오
        i. SMB/CIFS 활성화 * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
관리자 이름	SMB/CIFS 스토리지 VM의 관리자 사용자 이름을 지정합니다.
암호	SMB/CIFS 스토리지 VM의 관리자 암호를 지정합니다.
서버 이름	SMB/CIFS 스토리지 VM의 서버 이름을 지정합니다.
Active Directory 도메인	SMB/CIFS 스토리지 VM에 대한 사용자 인증을 제공할 Active Directory 도메인을 지정합니다.
조직 구성 단위	SMB/CIFS 서버와 연결된 Active Directory 도메인 내의 조직 단위를 지정합니다. "CN=Computers"가 기본값입니다. 이 값은 수정할 수 있습니다.
스토리지 VM의 공유에 액세스하는 동안 데이터를 암호화합니다	SMB 3.0을 사용하여 데이터를 암호화하여 SMB/CIFS 스토리지 VM의 공유에 대한 무단 파일 액세스를 방지합니다.
도메인	SMB/CIFS 스토리지 VM에 대해 나열된 도메인을 추가, 제거 또는 재정렬합니다.
이름 서버	SMB/CIFS 스토리지 VM의 이름 서버를 추가, 제거 또는 재정렬합니다.
기본 언어	스토리지 VM 및 해당 볼륨에 대한 기본 언어 인코딩 설정을 지정합니다. CLI를 사용하여 스토리지 VM 내의 개별 볼륨에 대한 설정을 변경할 수 있습니다.

네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. Enable NFS * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
NFS 클라이언트 액세스 허용 확인란을 선택합니다	NFS 스토리지 VM에서 생성된 모든 볼륨이 루트 볼륨 경로 "/"를 사용하여 마운트하고 트래버스해야 할 경우 이 확인란을 선택합니다. 엑스포트 정책 "기본값"에 규칙을 추가하여 무중단 마운트 트래버설을 허용합니다.

규칙	규칙을 만들려면 + Add 클릭하십시오. • 클라이언트 사양: 호스트 이름, IP 주소, 넷그룹 또는 도메인을 지정합니다. • 액세스 프로토콜: 다음 옵션의 조합을 선택합니다. ◦ SMB/CIFS ◦ FlexCache ◦ NFS 를 참조하십시오 ▪ NFSv3 ▪ NFSv4 • 액세스 세부 정보: 각 사용자 유형에 대해 읽기 전용, 읽기/쓰기 또는 고급 사용자 액세스 수준을 지정합니다. 사용자 유형은 다음과 같습니다. ◦ 모두 ◦ 모두(익명 사용자) ◦ Unix ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM 규칙을 저장합니다.
기본 언어	스토리지 VM 및 해당 볼륨에 대한 기본 언어 인코딩 설정을 지정합니다. CLI를 사용하여 스토리지 VM 내의 개별 볼륨에 대한 설정을 변경할 수 있습니다.
네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. iSCSI 활성화 * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. FC * 활성화 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
FC 포트를 구성합니다	스토리지 VM에 포함할 노드에서 네트워크 인터페이스를 선택합니다. 노드당 두 개의 네트워크 인터페이스를 사용하는 것이 좋습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. Enable NVMe/FC * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
FC 포트를 구성합니다	스토리지 VM에 포함할 노드에서 네트워크 인터페이스를 선택합니다. 노드당 두 개의 네트워크 인터페이스를 사용하는 것이 좋습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. NVMe/TCP * 활성화 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명

네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. 변경 사항을 저장합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 서브넷을 생성합니다.

단계

1. SVM 루트 볼륨을 포함할 Aggregate를 결정합니다.

   '스토리지 집계 show-has-mroot false'

   루트 볼륨을 포함할 최소 1GB의 여유 공간이 있는 애그리게이트를 선택해야 합니다. SVM에서 NAS 감사를 구성하려면 감사가 활성화된 경우 감사 스테이징 볼륨을 생성하는 데 사용 중인 추가 공간이 있어야 하며 루트 애그리게이트에 최소 3GB의 여유 공간이 있어야 합니다.

   > 기존 SVM에서 NAS 감사가 이미 활성화되어 있는 경우 애그리게이트 생성이 성공적으로 완료된 직후 애그리게이트의 스테이징 볼륨이 생성됩니다.

2. SVM 루트 볼륨을 생성할 애그리게이트의 이름을 기록합니다.
3. SVM을 생성할 때 언어를 지정할 계획이고 사용할 값을 모르는 경우 지정할 언어의 값을 식별하고 기록하십시오.

   "vserver create-language?

4. SVM을 생성할 때 스냅샷 정책을 지정할 계획이지만 정책 이름을 모르는 경우, 사용 가능한 정책을 나열하고 사용할 스냅샷 정책의 이름을 식별하여 기록합니다.

   '볼륨 스냅샷 정책 표시 - vserver_vserver_name_'

5. SVM을 생성할 때 할당량 정책을 지정할 계획이고 정책 이름을 모를 경우, 사용 가능한 정책을 나열하고 사용할 할당량 정책의 이름을 식별하고 기록합니다.

   '볼륨 할당량 정책 표시 - vserver_vserver_name_'

6. SVM 생성:

'vserver create-vserver_vserver_name_-aggregate_aggregate_name_-rootvolume_root_volume_name_-rootvolume-security-style{unix|ntfs|mixed}[-IPSpace_hIPspace_name_] [-language>] [-snapshot-policy_snapshot_snapshot_policy_name_] [-quota-policy_policy_name_ comment_comment_comment_comment]'] - comment_

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language
en_US.UTF-8
```

([Job 72] Job Succeeded: Vserver creation completed.

7. SVM 구성이 올바른지 확인합니다.

   'vserver show-vserver vs1'

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

이 예제에서 명령은 IPspace "ipspace1"에서 "vs1"이라는 SVM을 생성합니다. 루트 볼륨의 이름은 "VS1_root"이며 NTFS 보안 스타일로 aggr3에 생성됩니다.

ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 적응형 정책 그룹 템플릿을 설정합니다참조하십시오.

논리 인터페이스(LIF)

LIF 개요

ONTAP 클러스터의 **LIF** 구성에 대해 자세히 알아보십시오

LIF(논리 인터페이스)는 클러스터의 노드에 대한 네트워크 액세스 지점을 나타냅니다. 클러스터가 네트워크를 통해 통신을 주고받는 포트에 LIF를 구성할 수 있습니다.

클러스터 관리자는 다음을 생성, 보기, 수정, 마이그레이션, 되돌리기, 또는 LIF를 삭제합니다. SVM 관리자는 SVM과 연결된 LIF만 볼 수 있습니다.

LIF는 서비스 정책, 홈 포트, 홈 노드, 페일오버할 포트 목록, 방화벽 정책과 같은 관련 특성을 가진 IP 주소 또는 WWPN입니다. 클러스터가 네트워크를 통해 통신을 주고받는 포트에 LIF를 구성할 수 있습니다.

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

LIF는 다음 포트에서 호스팅할 수 있습니다.

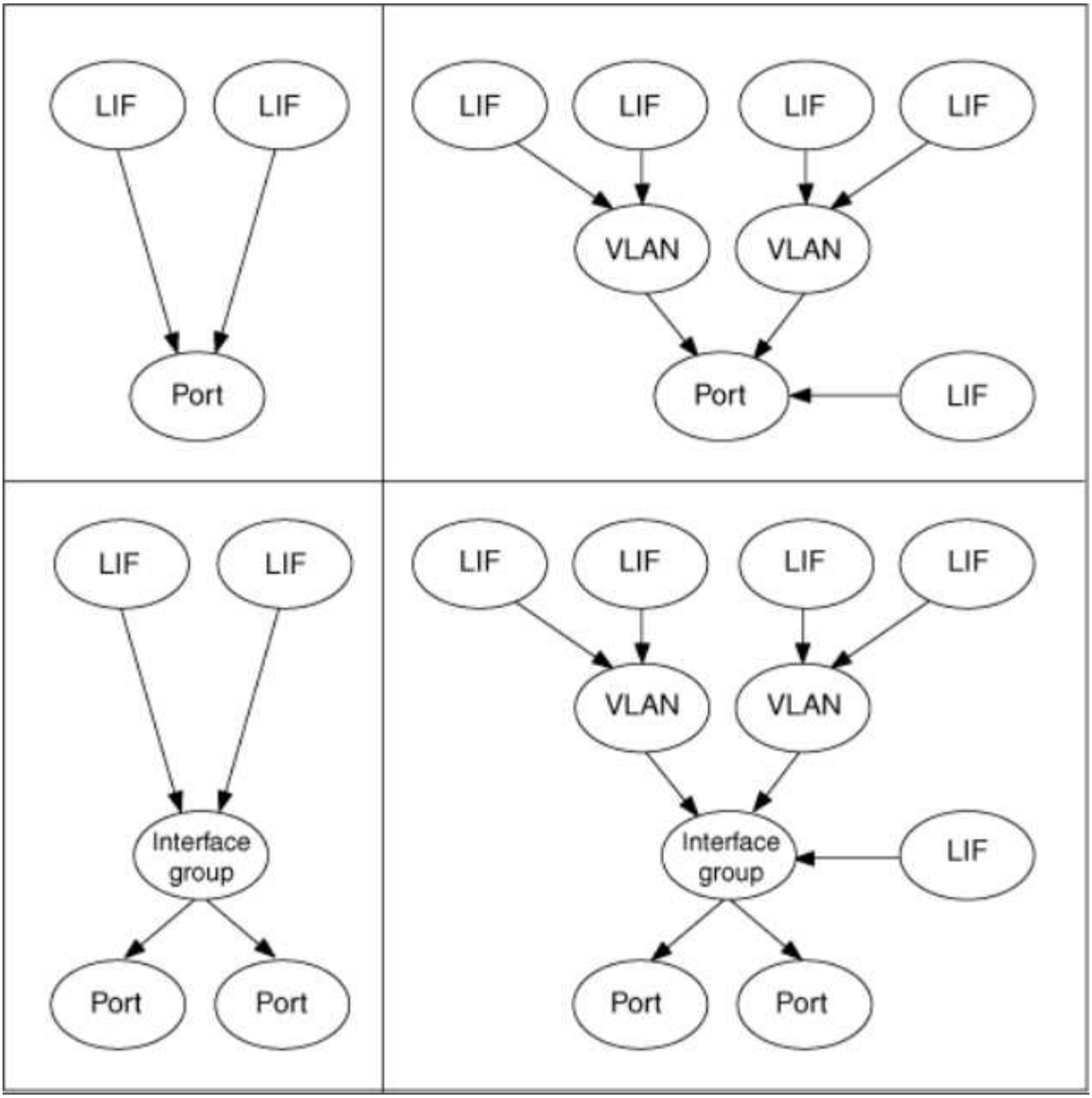
- 인터페이스 그룹에 속하지 않는 물리적 포트입니다
- 인터페이스 그룹
- VLAN
- VLAN을 호스팅하는 물리적 포트 또는 인터페이스 그룹
- 가상 IP(VIP) 포트

  ONTAP 9.5부터 VIP LIF가 지원되며 VIP 포트에서 호스팅됩니다.

LIF에서 FC와 같은 SAN 프로토콜을 구성하는 동안에는 WWPN과 연결됩니다.

"SAN 관리"

다음 그림에서는 ONTAP 시스템의 포트 계층을 보여 줍니다.



LIF 페일오버 및 반환

LIF 페일오버는 LIF가 홈 노드 또는 포트에서 HA 파트너 노드 또는 포트로 이동할 때 발생합니다. LIF 페일오버는 ONTAP에 의해 자동으로 트리거되거나, 클러스터 관리자가 물리적 이더넷 링크 다운 또는 복제된 데이터베이스(RDB) 쿼럼에서 노드 드롭과 같은 특정 이벤트에 대해 수동으로 트리거할 수 있습니다. LIF 페일오버가 발생할 경우 ONTAP은 페일오버 이유가 해결될 때까지 파트너 노드에서 정상 작업을 계속합니다. 홈 노드나 포트가 상태를 회복하면 LIF가 HA 파트너로부터 홈 노드 또는 포트로 되돌아갑니다. 이 재버전을 반환이라고 합니다.

LIF 페일오버 및 기브백의 경우 각 노드의 포트는 동일한 브로드캐스트 도메인에 속해야 합니다. 각 노드의 관련 포트가 동일한 브로드캐스트 도메인에 속해 있는지 확인하려면 다음을 참조하십시오.

- ONTAP 9.8 이상: "수리 포트 도달 가능성"
- ONTAP 9.7 이하: "브로드캐스트 도메인에서 포트를 추가하거나 제거합니다"

LIF 페일오버가 사용되도록 설정된 LIF의 경우(자동 또는 수동) 다음이 적용됩니다.

- 데이터 서비스 정책을 사용하는 LIF의 경우 페일오버 정책 제한 사항을 확인할 수 있습니다.
  - ONTAP 9.6 이상: "ONTAP 9.6 이상의 LIF 및 서비스 정책"
  - ONTAP 9.5 이하: "ONTAP 9.5 이전 버전에서 LIF 역할"
- LIF 자동 되돌리기는 자동 되돌리기가 로 설정된 경우 발생합니다 `true` LIF의 홈 포트가 정상 상태이고 LIF를 호스팅할 수 있는 경우,
- 계획된 또는 계획되지 않은 노드 테이크오버 경우, 테이크오버된 노드의 LIF가 HA 파트너로 페일오버됩니다. LIF가 페일오버되는 포트는 VIF Manager에 의해 결정됩니다.
- 페일오버가 완료된 후 LIF는 정상적으로 작동합니다.
- 반환이 시작되면 자동 되돌리기가 로 설정된 경우 LIF는 홈 노드와 포트로 되돌아갑니다 `true`.
- 이더넷 링크가 하나 이상의 LIF를 호스팅하는 포트에서 중지되면 VIF Manager가 LIF를 주 포트에서 같은 브로드캐스트 도메인의 다른 포트로 마이그레이션합니다. 새 포트가 같은 노드 또는 해당 HA 파트너에 있을 수 있습니다. 링크가 복구되고 자동 되돌리기가 로 설정된 경우 `true`VIF Manager가 LIF를 홈 노드와 홈 포트로 되돌립니다.
- 노드가 복제된 데이터베이스(RDB) 쿼럼에서 벗어나면 VIF Manager가 쿼럼 노드의 LIF를 HA 파트너로 마이그레이션합니다. 노드가 쿼럼으로 돌아온 후 자동 되돌리기가 로 설정된 경우 `true`VIF Manager가 LIF를 홈 노드와 홈 포트로 되돌립니다.

포트 유형별 **ONTAP LIF** 호환성에 대해 알아보십시오

LIF는 다양한 포트 유형을 지원하는 다양한 특성을 가질 수 있습니다.

> 인터클러스터 및 관리 LIF가 동일한 서브넷에 구성된 경우 관리 트래픽이 외부 방화벽에 의해 차단될 수 있으며 AutoSupport 및 NTP 연결이 실패할 수 있습니다. 'network interface modify -vserver_vserver name_-lif_인터클러스터 LIF_-status-admin up|down' 명령을 실행하여 인터클러스터 LIF를 전환하여 시스템을 복구할 수 있습니다. 그러나 이 문제를 방지하려면 인터클러스터 LIF 및 관리 LIF를 다른 서브넷에 설정해야 합니다.

LIF	설명
데이터 LIF	스토리지 가상 시스템(SVM)과 연결되고 클라이언트와 통신하는 데 사용되는 LIF 한 포트에 여러 개의 데이터 LIF가 존재할 수 있습니다. 이러한 인터페이스는 전체 클러스터에서 마이그레이션하거나 페일오버할 수 있습니다. 방화벽 정책을 관리 LIF로 수정하여 SVM 관리 LIF로 사용할 수 있습니다. NIS, LDAP, Active Directory, WINS 및 DNS 서버에 설정된 세션에서 데이터 LIF를 사용합니다.
클러스터 LIF	클러스터 내 노드 간에 클러스터 간 트래픽을 전송하는 데 사용되는 LIF. 클러스터 LIF는 항상 클러스터 포트에 생성해야 합니다. 클러스터 LIF는 동일한 노드의 클러스터 포트 간에 페일오버할 수 있으며 원격 노드로 마이그레이션하거나 페일오버할 수 없습니다. 새 노드가 클러스터에 연결되면 IP 주소가 자동으로 생성됩니다. 그러나 IP 주소를 클러스터 LIF에 수동으로 할당하려면 새 IP 주소가 기존 클러스터 LIF와 동일한 서브넷 범위에 있어야 합니다.
클러스터 관리 LIF	LIF는 전체 클러스터에 대한 단일 관리 인터페이스를 제공합니다. 클러스터 관리 LIF는 클러스터의 모든 노드로 페일오버할 수 있습니다. 클러스터 또는 인터클러스터 포트로 페일오버할 수 없습니다

인터클러스터 LIF	클러스터 간 통신, 백업 및 복제에 사용되는 LIF. 클러스터 피어링을 설정하려면 먼저 클러스터의 각 노드에 대한 인터클러스터 LIF를 생성해야 합니다. 이러한 LIF는 동일한 노드의 포트로만 페일오버할 수 있습니다. 클러스터의 다른 노드로 마이그레이션하거나 페일오버할 수 없습니다.
노드 관리 LIF	LIF는 클러스터의 특정 노드를 관리하기 위한 전용 IP 주소를 제공합니다. 노드 관리 LIF는 클러스터를 생성하거나 결합할 때 생성됩니다. 이러한 LIF는 클러스터에서 노드에 액세스할 수 없을 때와 같이 시스템 유지 관리에 사용됩니다.
VIP LIF	VIP LIF는 VIP 포트에 생성된 모든 데이터 LIF입니다. 자세한 내용은 을 참조하십시오"가상 IP(VIP) LIF를 구성합니다".

관련 정보

- "네트워크 인터페이스 수정"

ONTAP 버전에 지원되는 **LIF** 서비스 정책 및 역할

시간이 지남에 따라 ONTAP에서 LIF에서 지원되는 트래픽 유형을 관리하는 방식이 변경되었습니다.

- ONTAP 9 .5 이전 릴리즈에서는 LIF 역할 및 방화벽 서비스를 사용합니다.
- ONTAP 9 .6 이상 릴리즈에서는 LIF 서비스 정책을 사용합니다.
  - ONTAP 9 .5 릴리스에는 LIF 서비스 정책이 도입되었습니다.
  - ONTAP 9 .6은 LIF 역할을 LIF 서비스 정책으로 교체했습니다.
  - ONTAP 9.10.1은 방화벽 서비스를 LIF 서비스 정책으로 교체했습니다.

구성하는 방법은 사용 중인 ONTAP 릴리스에 따라 다릅니다.

추가 정보:

- 방화벽 정책은 "명령: firewall-policy-show"을 참조하십시오.
- LIF 역할은 를 참조하십시오"LIF 역할(ONTAP 9.5 이하)".
- LIF 서비스 정책은 을 "LIF 및 서비스 정책(ONTAP 9.6 이상)"참조하십시오.

ONTAP LIF 및 서비스 정책에 대해 자세히 알아보십시오

LIF에서 지원되는 트래픽 유형을 결정하는 LIF에 서비스 정책(LIF 역할 또는 방화벽 정책 대신)을 할당할 수 있습니다. 서비스 정책은 LIF에서 지원하는 네트워크 서비스 모음을 정의합니다. ONTAP는 LIF와 연결할 수 있는 기본 서비스 정책 세트를 제공합니다.

> 네트워크 트래픽을 관리하는 방법은 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 트래픽을 관리해야 하는 경우 을 참조하십시오"LIF 역할(ONTAP 9.5 이하)".

> FCP 및 NVMe/FCP 프로토콜은 현재 서비스 정책이 필요하지 않습니다.

네트워크 인터페이스 service-policy show 명령을 사용하여 서비스 정책과 세부 정보를 표시할 수 있습니다

에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

특정 서비스에 바인딩되지 않은 기능은 시스템 정의 동작을 사용하여 아웃바운드 연결에 대해 LIF를 선택합니다.

> 빈 서비스 정책이 있는 LIF에서 애플리케이션이 예기치 않게 동작할 수 있습니다.

시스템 **SVM**에 대한 서비스 정책

관리 SVM과 모든 시스템 SVM에는 관리 및 인터클러스터 LIF를 포함하여 해당 SVM의 LIF에 사용할 수 있는 서비스 정책이 포함되어 있습니다. 이러한 정책은 IPspace가 생성될 때 시스템에서 자동으로 생성됩니다.

다음 표에는 ONTAP 9.12.1부터 시작하는 시스템 SVM에 있는 LIF에 대한 내장 정책이 나와 있습니다. 다른 릴리즈의 경우 다음 명령을 사용하여 서비스 정책과 세부 정보를 표시합니다.

네트워크 인터페이스 서비스 정책 쇼

정책	포함된 서비스	동등한 역할	설명
기본값 - 인터클러스터	인터클러스터 코어, 관리 - https	인터클러스터	인터클러스터 트래픽을 전송하는 LIF에서 사용됩니다. 참고: 서비스 인터클러스터 코어는 net-인터클러스터 서비스 정책이라는 이름의 ONTAP 9.5에서 사용할 수 있습니다.
default-route-공지	관리 - BGP	-	BGP 피어 연결을 전달하는 LIF에서 사용됩니다. 참고: net-route-공지 서비스 정책과 함께 ONTAP 9.5에서 사용할 수 있습니다.
기본 관리	관리 코어, 관리 - https, management-http, management-ssh, management-autosupport, 관리 - EMS, 관리 - DNS - 클라이언트, 관리 - ad - 클라이언트, 관리 - LDAP - 클라이언트, 관리 - NIS - 클라이언트, 관리 - NTP - 클라이언트, 관리 - 로그 전달	노드 관리 또는 클러스터 관리	시스템 범위 관리 정책을 사용하여 시스템 SVM이 소유하는 노드 및 클러스터 범위 관리 LIF를 생성할 수 있습니다. 이러한 LIF는 DNS, AD, LDAP 또는 NIS 서버에 대한 아웃바운드 연결뿐만 아니라 전체 시스템을 대신하여 실행되는 애플리케이션을 지원하기 위한 일부 추가 연결에 사용할 수 있습니다. ONTAP 9.12.1부터 서비스를 사용하여 감사 로그를 원격 syslog 서버에 전달하는 데 사용되는 LIF를 제어할 수 `management-log-forwarding` 있습니다.

다음 표에는 ONTAP 9.11.1부터 시작하는 시스템 SVM에서 LIF가 사용할 수 있는 서비스가 나와 있습니다.

서비스	페일오버 제한 사항	설명
인터클러스터 코어	홈 노드 전용	핵심 인터클러스터 서비스
관리 코어	-	핵심 관리 서비스

관리 - ssh	-	SSH 관리 액세스를 위한 서비스
관리 - http	-	HTTP 관리 액세스를 위한 서비스입니다
관리 - https	-	HTTPS 관리 액세스를 위한 서비스
AutoSupport에 대해 설명합니다	-	AutoSupport 페이로드 게시와 관련된 서비스
관리 - BGP	홈 포트 전용	BGP 피어 상호 작용과 관련된 서비스
backup-ndmp-control입니다	-	NDMP 백업 제어를 위한 서비스
관리 - EMS	-	관리 메시징 액세스를 위한 서비스
관리 - NTP - 클라이언트	-	ONTAP 9.10.1에서 도입되었습니다. NTP 클라이언트 액세스를 위한 서비스입니다.
관리 - NTP - 서버	-	ONTAP 9.10.1에서 도입되었습니다. NTP 서버 관리 액세스를 위한 서비스입니다
관리 - portmap	-	포트맵 관리 서비스
관리 - rsh - 서버	-	rsh 서버 관리를 위한 서비스
관리 - SNMP - 서버	-	SNMP 서버 관리를 위한 서비스입니다
관리 - 텔넷 - 서버	-	텔넷 서버 관리를 위한 서비스
관리 - 로그 전달	-	ONTAP 9.12.1에서 도입되었습니다. 감사 로그 전달을 위한 서비스

데이터 **SVM**에 대한 서비스 정책

모든 데이터 SVM에는 해당 SVM의 LIF에서 사용할 수 있는 서비스 정책이 포함되어 있습니다.

다음 표에는 ONTAP 9.11.1부터 데이터 SVM에 있는 LIF에 대한 기본 제공 정책이 나와 있습니다. 다른 릴리즈의 경우 다음 명령을 사용하여 서비스 정책과 세부 정보를 표시합니다.

네트워크 인터페이스 서비스 정책 쇼

정책	포함된 서비스	등가 데이터 프로토콜	설명

기본 관리	data-core, management-https, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	없음	SVM 범위 관리 정책을 사용하여 데이터 SVM이 소유하는 SVM 관리 LIF를 생성할 수 있습니다. 이러한 LIF는 SVM 관리자에게 SSH 또는 HTTPS 액세스를 제공하는 데 사용할 수 있습니다. 필요한 경우 이러한 LIF를 외부 DNS, AD, LDAP 또는 NIS 서버에 대한 아웃바운드 연결에 사용할 수 있습니다.
default-data-blocks입니다	데이터 코어, 데이터 - iSCSI	iSCSI	블록 지향 SAN 데이터 트래픽을 전송하는 LIF에서 사용됩니다. ONTAP 9.10.1부터 "default-data-blocks" 정책은 사용되지 않습니다. 대신 "default-data-iscsi" 서비스 정책을 사용합니다.
default-data-files 를 선택합니다	데이터 코어, 데이터 -FPolicy-Client, 데이터-dns-server, 데이터-FlexCache, 데이터-cifs, 데이터 -nfs, 관리-dns-client, 관리-add-client, 관리 -ldap-client, 관리 -NIS-client	NFS, CIFS, FCache가 있습니다	기본 데이터 파일 정책을 사용하여 파일 기반 데이터 프로토콜을 지원하는 NAS LIF를 생성합니다. SVM에는 하나의 LIF만 있을 수 있으므로 이 정책을 통해 외부 DNS, AD, LDAP 또는 NIS 서버에 대한 아웃바운드 연결에 LIF를 사용할 수 있습니다. 연결 시 관리 LIF만 사용하도록 설정하려면 이 정책에서 이러한 서비스를 제거할 수 있습니다.
default-data-iscsi 를 참조하십시오	데이터 코어, 데이터 - iSCSI	iSCSI	iSCSI 데이터 트래픽을 전송하는 LIF에서 사용됩니다.
default-data-NVMe-TCP를 참조하십시오	데이터 코어, 데이터 - NVMe-TCP	NVMe-TCP	NVMe/TCP 데이터 트래픽을 전송하는 LIF에서 사용됩니다.

다음 표에는 데이터 SVM에서 사용할 수 있는 서비스와 각 서비스가 ONTAP 9.11.1부터 LIF의 페일오버 정책에 적용되는 모든 제한이 나와 있습니다.

서비스	페일오버 제한 사항	설명
관리 - ssh	-	SSH 관리 액세스를 위한 서비스
관리 - http	-	HTTP 관리 액세스를 위한 ONTAP 9.10.1 서비스에 도입되었습니다
관리 - https	-	HTTPS 관리 액세스를 위한 서비스
관리 - portmap	-	포트맵 관리 액세스를 위한 서비스
관리 - SNMP - 서버	-	SNMP 서버 관리 액세스를 위한 ONTAP 9.10.1 서비스에 도입되었습니다

데이터 코어	-	핵심 데이터 서비스
데이터 - NFS	-	NFS 데이터 서비스
데이터 - CIFS	-	CIFS 데이터 서비스
데이터 - FlexCache	-	FlexCache 데이터 서비스
데이터 - iSCSI	홈 포트 - AFF/FAS 전용, SFO 파트너 - ASA 전용	iSCSI 데이터 서비스
backup-ndmp-control입니다	-	ONTAP 9.10.1 백업 NDMP에서 도입되어 데이터 서비스를 제어합니다
data-dns-server 를 참조하십시오	-	ONTAP 9.10.1 DNS 서버 데이터 서비스에 도입되었습니다
데이터 - FPolicy - 클라이언트	-	파일 스크리닝 정책 데이터 서비스
데이터 NVMe-TCP	홈 포트 전용	ONTAP 9.10.1 NVMe TCP 데이터 서비스에 도입되었습니다
Data-S3-서버	-	S3(Simple Storage Service) 서버 데이터 서비스

서비스 정책이 데이터 SVM의 LIF에 할당되는 방식에 대해 알고 있어야 합니다.

- 데이터 서비스 목록을 사용해 데이터 SVM을 생성할 경우 지정된 서비스를 사용하여 해당 SVM에 내장된 "기본 데이터 파일" 및 "기본 데이터 블록" 서비스 정책을 생성합니다.
- 데이터 서비스 목록을 지정하지 않고 SVM 데이터 생성 시 기본 데이터 서비스 목록을 사용하여 해당 SVM에 내장된 "default-data-files" 및 "default-data-blocks" 서비스 정책이 생성됩니다.

  기본 데이터 서비스 목록에는 iSCSI, NFS, NVMe, SMB 및 FlexCache 서비스가 포함됩니다.

- LIF가 데이터 프로토콜 목록으로 작성되면 지정된 데이터 프로토콜에 해당하는 서비스 정책이 LIF에 할당됩니다.
- 동등한 서비스 정책이 없으면 사용자 지정 서비스 정책이 만들어집니다.
- 서비스 정책이나 데이터 프로토콜 목록 없이 LIF를 생성할 경우 기본적으로 기본 데이터 파일 서비스 정책이 LIF에 할당됩니다.

데이터 코어 서비스

데이터 코어 서비스는 LIF 역할(ONTAP 9.6에서 더 이상 사용되지 않음)을 사용하여 서비스 정책을 관리하는 LIF를 관리하도록 업그레이드된 클러스터에서 데이터 역할의 LIF를 사용한 구성 요소가 예상대로 작동할 수 있도록 합니다.

데이터 코어를 서비스로 지정해도 방화벽에서 어떠한 포트도 열리지 않지만 데이터 SVM의 서비스 정책에는 서비스가 포함되어야 합니다. 예를 들어 기본 데이터 파일 서비스 정책에는 기본적으로 다음 서비스가 포함됩니다.

- 데이터 코어
- 데이터 - NFS
- 데이터 - CIFS
- 데이터 - FlexCache

데이터 코어 서비스를 정책에 포함하여 LIF를 사용하는 모든 애플리케이션이 예상대로 작동하도록 해야 하지만, 필요한 경우 다른 세 서비스를 제거할 수 있습니다.

클라이언트 측 **LIF** 서비스

ONTAP는 ONTAP 9.10.1부터 여러 애플리케이션을 위한 클라이언트측 LIF 서비스를 제공합니다. 이러한 서비스를 통해 각 애플리케이션을 대신하여 아웃바운드 연결에 사용되는 LIF를 제어할 수 있습니다.

관리자는 다음과 같은 새로운 서비스를 통해 특정 애플리케이션의 소스 주소로 사용되는 LIF를 제어할 수 있습니다.

서비스	SVM 제한	설명
관리 - ad-client	-	ONTAP 9.11.1부터 ONTAP는 외부 AD 서버에 대한 아웃바운드 연결을 위한 Active Directory 클라이언트 서비스를 제공합니다.
관리 - DNS - 클라이언트	-	ONTAP는 ONTAP 9.11.1부터 외부 DNS 서버에 대한 아웃바운드 연결을 위한 DNS 클라이언트 서비스를 제공합니다.
관리 - LDAP - 클라이언트	-	ONTAP 9.11.1부터 ONTAP는 외부 LDAP 서버에 대한 아웃바운드 연결을 위한 LDAP 클라이언트 서비스를 제공합니다.
Management - NIS - 클라이언트입니다	-	ONTAP는 ONTAP 9.11.1부터 외부 NIS 서버에 대한 아웃바운드 연결을 위한 NIS 클라이언트 서비스를 제공합니다.
관리 - NTP - 클라이언트	시스템 전용	ONTAP 9.10.1부터 ONTAP는 외부 NTP 서버에 대한 아웃바운드 연결을 위한 NTP 클라이언트 서비스를 제공합니다.
데이터 - FPolicy - 클라이언트	데이터 전용	ONTAP 9.8부터 ONTAP는 아웃바운드 FPolicy 연결을 위한 클라이언트 서비스를 제공합니다.

새로운 서비스 각각은 자동으로 일부 기본 제공 서비스 정책에 포함되지만 관리자는 기본 제공 정책에서 해당 서비스를 제거하거나 사용자 지정 정책에 추가하여 각 애플리케이션을 대신하여 아웃바운드 연결에 사용되는 LIF를 제어할 수 있습니다.

관련 정보

- "네트워크 인터페이스 service-policy show를 참조하십시오"

LIF 관리

ONTAP 클러스터에 대한 LIF 서비스 정책을 구성합니다

LIF 서비스 정책을 구성하여 LIF를 사용할 단일 서비스 또는 서비스 목록을 식별할 수 있습니다.

LIF에 대한 서비스 정책을 생성합니다

LIF에 대한 서비스 정책을 생성할 수 있습니다. 하나 이상의 LIF에 서비스 정책을 할당할 수 있으므로 LIF에서 단일 서비스 또는 서비스 목록에 대한 트래픽을 전송할 수 있습니다.

'network interface service-policy create' 명령을 실행하려면 고급 권한이 필요합니다.

이 작업에 대해

기본 제공 서비스 및 서비스 정책을 사용하여 데이터 및 시스템 SVM에서 데이터 및 관리 트래픽을 관리할 수 있습니다. 대부분의 사용 사례는 사용자 지정 서비스 정책을 만들지 않고 기본 제공 서비스 정책을 사용하여 충족됩니다.

필요한 경우 이러한 기본 제공 서비스 정책을 수정할 수 있습니다.

단계

1. 클러스터에서 사용 가능한 서비스를 봅니다.

```
network interface service show
```

서비스는 LIF에서 액세스하는 애플리케이션 및 클러스터에서 지원하는 애플리케이션을 나타냅니다. 각 서비스에는 응용 프로그램이 수신 대기 중인 0개 이상의 TCP 및 UDP 포트가 포함됩니다.

다음과 같은 추가 데이터 및 관리 서비스를 사용할 수 있습니다.

```
cluster1::> network interface service show

Service                      Protocol:Ports
-------                      --------------
cluster-core                 -
data-cifs                    -
data-core                    -
data-flexcache               -
data-iscsi                   -
data-nfs                     -
intercluster-core            tcp:11104-11105
management-autosupport       -
management-bgp               tcp:179
management-core              -
management-https             tcp:443
management-ssh               tcp:22
12 entries were displayed.
```

2. 클러스터에 존재하는 서비스 정책을 확인합니다.

```
cluster1::> network interface service-policy show

Vserver   Policy                      Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster        intercluster-core: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

          default-management          management-core: 0.0.0.0/0
                                      management-autosupport: 0.0.0.0/0
                                      management-ssh: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

          default-route-announce      management-bgp: 0.0.0.0/0

Cluster
          default-cluster             cluster-core: 0.0.0.0/0

vs0
          default-data-blocks         data-core: 0.0.0.0/0
                                      data-iscsi: 0.0.0.0/0

          default-data-files          data-core: 0.0.0.0/0
                                      data-nfs: 0.0.0.0/0
                                      data-cifs: 0.0.0.0/0
                                      data-flexcache: 0.0.0.0/0

          default-management          data-core: 0.0.0.0/0
                                      management-ssh: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

7 entries were displayed.
```

3. 서비스 정책 생성:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- "service_name"은 정책에 포함되어야 하는 서비스 목록을 지정합니다.
- "ip_address/mask"는 서비스 정책의 서비스에 액세스할 수 있는 주소에 대한 서브넷 마스크 목록을 지정합니다. 기본적으로 지정된 모든 서비스는 모든 서브넷의 트래픽을 허용하는 기본 허용 주소 목록인 0.0.0.0/0으로 추가됩니다. 기본값이 아닌 허용 주소 목록이 제공되는 경우 정책을 사용하는 LIF는 지정된 마스크와 일치하지 않는 소스 주소를 가진 모든 요청을 차단하도록 구성됩니다.

  다음 예에서는 _nfs_and_smb_services를 포함하는 SVM에 대해 _svm1_data_policy_라는 데이터 서비스 정책을 생성하는 방법을 보여 줍니다.

  ```
  cluster1::> set -privilege advanced
  Warning: These advanced commands are potentially dangerous; use them
  only when directed to do so by technical support.
  Do you wish to continue? (y or n): y

  cluster1::> network interface service-policy create -vserver svm1
  -policy svm1_data_policy -services data-nfs,data-cifs,data-core
  ```

  다음 예제에서는 인터클러스터 서비스 정책을 만드는 방법을 보여 줍니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. 서비스 정책이 생성되었는지 확인합니다.

```
cluster1::> network interface service-policy show
```

다음 출력에는 사용 가능한 서비스 정책이 나와 있습니다.

```
cluster1::> network interface service-policy show

Vserver   Policy                      Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster        intercluster-core: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

          intercluster1               intercluster-core: 0.0.0.0/0

          default-management          management-core: 0.0.0.0/0
                                      management-autosupport: 0.0.0.0/0
                                      management-ssh: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

          default-route-announce      management-bgp: 0.0.0.0/0

Cluster
          default-cluster             cluster-core: 0.0.0.0/0

vs0
          default-data-blocks         data-core: 0.0.0.0/0
                                      data-iscsi: 0.0.0.0/0

          default-data-files          data-core: 0.0.0.0/0
                                      data-nfs: 0.0.0.0/0
                                      data-cifs: 0.0.0.0/0
                                      data-flexcache: 0.0.0.0/0

          default-management          data-core: 0.0.0.0/0
                                      management-ssh: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

          svm1_data_policy            data-core: 0.0.0.0/0
                                      data-nfs: 0.0.0.0/0
                                      data-cifs: 0.0.0.0/0

9 entries were displayed.
```

작업을 마친 후

서비스 정책을 생성할 때 또는 기존 LIF를 수정하여 LIF에 할당합니다.

LIF에 서비스 정책을 할당합니다

LIF를 생성할 때 또는 LIF를 수정하여 서비스 정책을 LIF에 할당할 수 있습니다. 서비스 정책은 LIF에서 사용할 수 있는 서비스 목록을 정의합니다.

이 작업에 대해

admin 및 Data SVM에서 LIF에 서비스 정책을 할당할 수 있습니다.

단계

서비스 정책을 LIF에 할당할 시기에 따라 다음 작업 중 하나를 수행합니다.

만약...	서비스 정책 할당...
LIF 생성	네트워크 인터페이스 create-vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(-address <ip_address> -netmask <ip_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
LIF 수정	네트워크 인터페이스 modify -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

LIF에 서비스 정책을 지정할 때 LIF의 데이터 프로토콜과 역할을 지정할 필요가 없습니다. 역할 및 데이터 프로토콜을 지정하여 LIF를 생성할 수도 있습니다.

> 서비스 정책은 서비스 정책을 생성할 때 지정한 SVM에 있는 LIF에서만 사용할 수 있습니다.

예

다음 예에서는 LIF의 서비스 정책을 수정하여 기본 관리 서비스 정책을 사용하는 방법을 보여 줍니다.

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

LIF 서비스 정책을 관리하는 명령입니다

네트워크 인터페이스 서비스 정책 명령을 사용하여 LIF 서비스 정책을 관리합니다.

에 대한 자세한 내용은 `network interface service-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

활성 SnapMirror 관계에서 LIF의 서비스 정책을 수정하면 복제 일정이 중단됩니다. LIF를 인터클러스터에서 비인터클러스터(또는 그 반대로)로 변환하면 해당 변경 사항이 피어링된 클러스터에 복제되지 않습니다. LIF 서비스 정책을 수정한 후 피어 클러스터를 업데이트하려면 먼저 를 수행합니다 `snapmirror abort` 작동 후 복제 관계를 다시 동기화합니다.

원하는 작업	이 명령 사용...
서비스 정책 생성(고급 권한 필요)	네트워크 인터페이스 서비스 정책 만들기

원하는 작업	이 명령 사용...
기존 서비스 정책에 추가 서비스 항목 추가(고급 권한 필요)	네트워크 인터페이스 서비스 정책 추가 서비스
기존 서비스 정책 클론 생성(고급 권한 필요)	네트워크 인터페이스 서비스 정책 클론
기존 서비스 정책의 서비스 항목 수정(고급 권한 필요)	네트워크 인터페이스 서비스 정책 수정 서비스
기존 서비스 정책에서 서비스 항목 제거(고급 권한 필요)	네트워크 인터페이스 서비스 정책 제거 서비스
기존 서비스 정책 이름 바꾸기(고급 권한 필요)	네트워크 인터페이스 서비스 정책 이름 바꾸기
기존 서비스 정책 삭제(고급 권한 필요)	네트워크 인터페이스 서비스 정책 삭제
기본 제공 서비스 정책을 원래 상태로 복원(고급 권한 필요)	네트워크 인터페이스 서비스 정책 복원 - 기본값
기존 서비스 정책을 표시합니다	네트워크 인터페이스 서비스 정책 쇼

관련 정보

- "네트워크 인터페이스 서비스가 표시됩니다"
- "네트워크 인터페이스 서비스 - 정책"
- "SnapMirror가 중단되었습니다"

ONTAP LIF를 생성합니다

SVM은 하나 이상의 네트워크 논리 인터페이스(LIF)를 통해 클라이언트에 데이터를 제공합니다. 데이터에 액세스하는 데 사용할 포트에 LIF를 생성해야 합니다. LIF(네트워크 인터페이스)는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트로 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

모범 사례

LIF 마이그레이션 중에 지연을 줄이려면 ONTAP에 연결된 스위치 포트를 스패닝 트리 에지 포트로 구성해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 기본 물리적 또는 논리적 네트워크 포트가 관리 작동 상태로 구성되어 있어야 합니다.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

  서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. System Manager나 network subnet create 명령을 사용하여 생성됩니다.

  에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

이 작업에 대해

- NAS 및 SAN 프로토콜은 동일한 LIF에 할당할 수 없습니다.

  지원되는 프로토콜은 SMB, NFS, FlexCache, iSCSI 및 FC입니다. iSCSI 및 FC는 다른 프로토콜과 결합할 수 없습니다. 그러나 NAS 및 이더넷 기반 SAN 프로토콜은 동일한 물리적 포트에 존재할 수 있습니다.

  - SMB 트래픽이 있는 LIF가 홈 노드로 자동 복구되도록 구성하지 않아야 합니다. SMB를 통해 Hyper-V 또는 SQL Server의 무중단 운영을 지원하는 솔루션을 호스팅하려는 SMB 서버의 경우 이 권장 사항이 필수입니다.
- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- SVM에서 사용하는 DNS, NIS, LDAP, Active Directory 등의 모든 이름 매핑 및 호스트 이름 확인 서비스 SVM의 데이터 트래픽을 처리하는 하나 이상의 LIF에서 연결할 수 있어야 합니다.
- 클러스터 간 노드 트래픽을 처리하는 LIF는 LIF가 관리 트래픽을 처리하거나 데이터 트래픽을 처리하는 LIF와 같은 서브넷에 있으면 안 됩니다.
- 유효한 페일오버 목표가 없는 LIF를 생성하면 경고 메시지가 표시됩니다.
- 클러스터에 LIF가 많은 경우 클러스터에서 지원되는 LIF 용량을 확인할 수 있습니다.
  - 시스템 관리자: ONTAP 9.12.0부터 네트워크 인터페이스 그리드의 처리량을 확인합니다.
  - CLI: 고급 권한 수준에서 network interface capacity details show 명령을 사용하여 각 노드에서 지원되는 LIF 용량과 network interface capacity show 명령을 사용하십시오.

    및 `network interface capacity details show` 에 대한 자세한 `network interface capacity show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.
- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

  ONTAP 9.4부터는 FC-NVMe가 지원됩니다. FC-NVMe LIF를 생성하는 경우 다음 사항을 알아야 합니다.

  - NVMe 프로토콜은 LIF가 생성된 FC 어댑터에서 지원되어야 합니다.
  - FC-NVMe는 데이터 LIF에서 유일한 데이터 프로토콜일 수 있습니다.
- SAN을 지원하는 모든 SVM(스토리지 가상 머신)에서 관리 트래픽을 처리하는 하나의 LIF를 구성해야 합니다.
- NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
- SVM당, 노드당 최대 2개의 NVMe LIF를 구성할 수 있다.
- 서브넷을 사용하여 네트워크 인터페이스를 만들면 ONTAP는 선택한 서브넷에서 사용 가능한 IP 주소를 자동으로 선택하고 네트워크 인터페이스에 할당합니다. 서브넷이 두 개 이상인 경우 서브넷을 변경할 수 있지만 IP 주소는 변경할 수 없습니다.
- 네트워크 인터페이스를 위해 SVM을 생성(추가)할 때 기존 서브넷 범위에 있는 IP 주소를 지정할 수 없습니다. 서브넷 충돌 오류가 발생합니다. 이 문제는 SVM 설정 또는 클러스터 설정에서 클러스터 간 네트워크 인터페이스를 생성하거나 수정하는 등 네트워크 인터페이스를 위한 다른 워크플로우에서 발생합니다.
- ONTAP 9.10.1부터 `network interface` CLI 명령에 RDMA 기반 NFS 구성에 대한 매개 변수가 포함됩니다 `-rdma-protocols`. RDMA 기반 NFS 구성용 네트워크 인터페이스 생성은 ONTAP 9.12.1부터 System

Manager에서 지원됩니다. 자세한 내용은 을 RDMA를 통해 NFS에 대해 LIFS를 구성합니다참조하십시오.

- ONTAP 9.11.1부터 ASA(All-Flash SAN 어레이) 플랫폼에서 자동 iSCSI LIF 페일오버를 사용할 수 있습니다.

  iSCSI LIF 페일오버가 자동으로 활성화됨(페일오버 정책은 'fo-partner-only'로 설정되고 자동 되돌리기 값은 'true'로 설정됨) 새로 생성된 iSCSI LIF에서 지정된 SVM에 iSCSI LIF가 없거나 지정된 SVM에 있는 기존 iSCSI LIF가 iSCSI LIF 페일오버로 이미 활성화되어 있는 경우.

  ONTAP 9.11.1 이상으로 업그레이드한 후 iSCSI LIF 페일오버 기능을 사용하도록 설정되지 않은 SVM에 기존 iSCSI LIF가 있고 동일한 SVM에 새 iSCSI LIF를 생성하고, 새로운 iSCSI LIF는 SVM에 있는 기존 iSCSI LIF와 동일한 페일오버 정책(비활성화)을 가정합니다.

  "ASA 플랫폼의 iSCSI LIF 페일오버"

ONTAP 9.7부터 ONTAP는 해당 IPspace의 동일한 서브넷에 이미 있는 LIF가 하나 이상 있으면 LIF의 홈 포트를 자동으로 선택합니다. ONTAP은 해당 서브넷에 있는 다른 LIF와 동일한 브로드캐스트 도메인에서 홈 포트를 선택합니다. 홈 포트는 여전히 지정할 수 있지만 더 이상 필요하지 않습니다(지정된 IPspace의 해당 서브넷에 LIF가 아직 없는 경우).

ONTAP 9.12.0부터는 — System Manager 또는 CLI를 사용하는 인터페이스에 따라 절차가 달라집니다.

시스템 관리자

- System Manager를 사용하여 네트워크 인터페이스를 추가합니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 를 선택합니다 + Add .
3. 다음 인터페이스 역할 중 하나를 선택합니다.
   a. 데이터
   b. 인터클러스터
   c. SVM 관리
4. 프로토콜을 선택합니다.
   a. SMB/CIFS 및 NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. LIF의 이름을 지정하거나 이전 선택 사항에서 생성한 이름을 그대로 사용합니다.
6. 홈 노드를 수락하거나 드롭다운을 사용하여 하나를 선택합니다.
7. 선택한 SVM의 IPspace에서 하나 이상의 서브넷이 구성된 경우 서브넷 드롭다운이 표시됩니다.
   a. 서브넷을 선택한 경우 드롭다운에서 선택합니다.
   b. 서브넷 없이 진행하면 브로드캐스트 도메인 드롭다운이 표시됩니다.
      i. IP 주소를 지정합니다. IP 주소를 사용 중인 경우 경고 메시지가 표시됩니다.
      ii. 서브넷 마스크를 지정합니다.
8. 브로드캐스트 도메인에서 홈 포트를 자동으로(권장) 선택하거나 드롭다운 메뉴에서 선택합니다. 홈 포트 컨트롤은 브로드캐스트 도메인 또는 서브넷 선택에 따라 표시됩니다.
9. 네트워크 인터페이스를 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF * 를 생성합니다

단계

1. LIF에 사용할 브로드캐스트 도메인 포트를 결정합니다.

   '네트워크 포트 브로드캐스트-도메인 쇼-IPSpace_ipspace1_'

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List   Status Details
ipspace1
            default       1500
                                  node1:e0d   complete
                                  node1:e0e   complete
                                  node2:e0d   complete
                                  node2:e0e   complete
```

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

2. LIF에 사용할 서브넷에 사용되지 않는 IP 주소가 충분히 있는지 확인합니다.

   'network subnet show - IPSpace_ipspace1_'

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

3. 데이터에 액세스하는 데 사용할 포트에 하나 이상의 LIF를 생성합니다.

   > NetApp은 데이터 SVM의 모든 LIF에 대한 서브넷 개체를 생성할 것을 권장합니다. 이는 각 서브넷 객체에 연결된 브로드캐스트 도메인이 있기 때문에 ONTAP에서 대상 클러스터의 페일오버 대상을 결정할 수 있도록 서브넷 객체를 사용하는 MetroCluster 구성에서 특히 중요합니다. 자세한 내용은 을 "서브넷을 생성합니다"참조하십시오.

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

     또한 LIF가 -auto-revert 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도 있습니다.

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

   - '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
   - IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
   - 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.
   - 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. 에 대한 자세한 내용은

`network route create` "ONTAP 명령 참조입니다"을 참조하십시오.

- '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 true로 설정할 수 있습니다.
- '-service-policy' ONTAP 9.5부터 '-service-policy' 옵션을 통해 LIF에 대한 서비스 정책을 할당할 수 있습니다. LIF에 서비스 정책을 지정한 경우, 이 정책을 사용하여 LIF에 대한 기본 역할, 페일오버 정책 및 데이터 프로토콜 목록을 구성합니다. ONTAP 9.5에서는 서비스 정책이 인터클러스터 및 BGP 피어 서비스에 대해서만 지원됩니다. ONTAP 9.6에서는 여러 데이터 및 관리 서비스에 대한 서비스 정책을 작성할 수 있습니다.
- '-data-protocol'을 사용하면 FCP 또는 NVMe/FC 프로토콜을 지원하는 LIF를 생성할 수 있습니다. IP LIF를 생성할 때는 이 옵션이 필요하지 않습니다.

4. * 선택 사항 *: -address 옵션에서 IPv6 주소 할당:

   a. network NDP prefix show 명령을 사용하여 다양한 인터페이스에서 습득한 RA prefix 목록을 볼 수 있다.

      고급 권한 수준에서 network NDP prefix show 명령을 사용할 수 있다.

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

   b. IPv6 주소를 수동으로 구성하려면 접두사::id 형식을 사용합니다.

      접두사는 다양한 인터페이스에서 습득한 접두사입니다.

   ID를 도출하려면 임의의 64비트 16진수 숫자를 선택합니다.

5. LIF 인터페이스 구성이 올바른지 확인합니다.

   네트워크 인터페이스 show-vserver vs1

```
           Logical     Status     Network          Current   Current Is
Vserver    Interface   Admin/Oper Address/Mask     Node      Port
Home
--------- ---------- ---------- --------------- --------- -------
----
vs1
            lif1        up/up      10.0.0.128/24   node1      e0d
true
```

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

6. 페일오버 그룹 구성이 원하는 대로 되어 있는지 확인합니다.

   'network interface show-failover-vserver_vs1_'

```
          Logical    Home       Failover        Failover
Vserver   interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
          lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면…	사용…
IPv4 주소입니다	네트워크 Ping
IPv6 주소입니다	네트워크 ping6

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

다음 명령은 NVMe/FC LIF를 생성하고 'NVMe-FC' 데이터 프로토콜을 지정합니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

ONTAP LIF 수정

홈 노드 또는 현재 노드, 관리 상태, IP 주소, 넷마스크, 페일오버 정책 등의 특성을 변경하여 LIF를 수정할 수 있습니다. 방화벽 정책 및 서비스 정책을 참조하십시오. LIF의 주소 제품군을 IPv4에서 IPv6로 변경할 수도 있습니다.

이 작업에 대해

- LIF의 관리 상태를 중지 상태로 수정할 때 LIF의 관리 상태가 위로 돌아갈 때까지 진행 중인 모든 NFSv4 잠금이 유지됩니다.

  다른 LIF가 잠긴 파일에 액세스하려고 할 때 발생할 수 있는 잠금 충돌을 방지하려면 관리 상태를 낮춤 으로 설정하기 전에 NFSv4 클라이언트를 다른 LIF로 이동해야 합니다.

- FC LIF에서 사용되는 데이터 프로토콜은 수정할 수 없습니다. 하지만 서비스 정책에 할당된 서비스를 수정하거나 IP LIF에 할당된 서비스 정책을 변경할 수 있습니다.

  FC LIF에서 사용되는 데이터 프로토콜을 수정하려면 LIF를 삭제하고 다시 생성해야 합니다. IP LIF에서 서비스 정책을 변경하기 위해 업데이트를 수행하는 동안 잠시 중단이 발생합니다.

- 노드 범위 관리 LIF의 홈 노드 또는 현재 노드를 수정할 수 없습니다.
- 서브넷을 사용하여 LIF의 IP 주소 및 네트워크 마스크 값을 변경할 경우, IP 주소는 지정된 서브넷에서 할당됩니다. LIF의 이전 IP 주소가 다른 서브넷에 있는 경우 IP 주소는 해당 서브넷으로 반환됩니다.
- LIF의 주소 제품군을 IPv4에서 IPv6로 수정하려면 IPv6 주소에 대한 콜론 표기법을 사용하고 '-netmask-length' 매개 변수에 새 값을 추가해야 합니다.
- 자동 구성된 링크 로컬 IPv6 주소는 수정할 수 없습니다.
- LIF가 수정되어 LIF에 유효한 페일오버 타겟이 없게 되면 경고 메시지가 표시됩니다.

  유효한 페일오버 목표가 없는 LIF가 페일오버를 시도하면 운영 중단이 발생할 수 있습니다.

- ONTAP 9.5부터 LIF와 연결된 서비스 정책을 수정할 수 있습니다.

  ONTAP 9.5에서는 서비스 정책이 인터클러스터 및 BGP 피어 서비스에 대해서만 지원됩니다. ONTAP 9.6에서는 여러 데이터 및 관리 서비스에 대한 서비스 정책을 작성할 수 있습니다.

- ONTAP 9.11.1부터 ASA(All-Flash SAN 어레이) 플랫폼에서 자동 iSCSI LIF 페일오버를 사용할 수 있습니다.

  기존 iSCSI LIF의 경우, 9.11.1 이상으로 업그레이드하기 전에 생성된 LIF를 의미하며 페일오버 정책을 로 수정할 수 있습니다 "자동 iSCSI LIF 페일오버를 사용합니다".

- ONTAP NTP(네트워크 시간 프로토콜)를 활용하여 클러스터 전체에서 시간을 동기화합니다. LIF IP 주소를 변경한 후에는 동기화 실패를 방지하기 위해 NTP 구성을 업데이트해야 할 수도 있습니다. 자세한 내용은 다음을 참조하세요."NetApp 지식 기반: LIF IP 변경 후 NTP 동기화가 실패함" .

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터는 시스템 관리자를 사용하여 네트워크 인터페이스를 편집할 수 있습니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆의 * > 편집 * 을 선택합니다 ⋮ .
3. 하나 이상의 네트워크 인터페이스 설정을 변경합니다. 자세한 내용은 을 참조하십시오 "LIF를 생성합니다".
4. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF를 수정합니다 *

단계

1. 'network interface modify' 명령을 사용하여 LIF의 특성을 수정합니다.

   다음 예에서는 서브넷 client1_sub의 IP 주소와 네트워크 마스크 값을 사용하여 LIF datalif2의 IP 주소와 네트워크 마스크를 수정하는 방법을 보여 줍니다.

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   다음 예에서는 LIF의 서비스 정책을 수정하는 방법을 보여 줍니다.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

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

2. IP 주소에 연결할 수 있는지 확인합니다.

사용 중인 경우...	그 다음에...
IPv4 주소	네트워크 핑
IPv6 주소	네트워크 핑6

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

ONTAP LIF 마이그레이션

포트에 장애가 발생하거나 유지 관리가 필요한 경우 LIF를 동일한 노드의 다른 포트 또는 클러스터 내의 다른 노드로 마이그레이션해야 할 수 있습니다. LIF 마이그레이션은 LIF

페일오버와 비슷하지만, LIF 마이그레이션은 수동 작업이며, LIF 페일오버는 LIF의 현재 네트워크 포트에서 링크 장애가 발생할 경우 LIF의 자동 마이그레이션입니다.

시작하기 전에

- LIF에 대해 페일오버 그룹을 구성해야 합니다.
- 대상 노드와 포트가 작동 중이고 소스 포트와 동일한 네트워크에 액세스할 수 있어야 합니다.

이 작업에 대해

- BGP LIF는 홈 포트에 상주하며 다른 노드 또는 포트로 마이그레이션할 수 없습니다.
- 노드에서 NIC를 제거하기 전에 NIC에 속한 포트에서 호스팅되는 LIF를 클러스터의 다른 포트로 마이그레이션해야 합니다.
- 클러스터 LIF가 호스팅된 노드에서 클러스터 LIF를 마이그레이션하기 위한 명령을 실행해야 합니다.
- 노드 범위의 관리 LIF, 클러스터 LIF, LIF와 같은 노드 범위의 LIF는 원격 인터클러스터 노드로 마이그레이션할 수 없습니다.
- NFSv4 LIF를 노드 간에 마이그레이션할 경우 LIF가 새 포트에서 사용 가능해지기 전에 최대 45초가 지연됩니다.

  이 문제를 해결하려면 지연이 발생하지 않는 NFSv4.1을 사용하십시오.

- ONTAP 9.11.1 이상을 실행하는 ASA(All-Flash SAN 어레이) 플랫폼에서 iSCSI LIF를 마이그레이션할 수 있습니다.

  iSCSI LIF 마이그레이션은 홈 노드 또는 HA 파트너의 포트로 제한됩니다.

- 사용 중인 플랫폼이 ONTAP 버전 9.11.1 이상을 실행하는 ASA(All-Flash SAN 어레이) 플랫폼이 아닌 경우 한 노드에서 다른 노드로 iSCSI LIF를 마이그레이션할 수 없습니다.

  이 제한을 해결하려면 대상 노드에 iSCSI LIF를 생성해야 합니다. 에 대해 자세히 "iSCSI LIF를 생성하는 중입니다 "알아보십시오.

- RDMA를 통해 NFS용 LIF(네트워크 인터페이스)를 마이그레이션하려면 대상 포트가 RoCE를 지원하는지 확인해야 합니다. CLI에서 LIF를 마이그레이션하려면 ONTAP 9.10.1 이상을 실행해야 하며, System Manager를 사용하여 마이그레이션하려면 ONTAP 9.12.1을 실행해야 합니다. System Manager에서 RoCE 가능 대상 포트를 선택한 후에는 * RoCE 포트 사용 * 옆의 확인란을 선택하여 마이그레이션을 성공적으로 완료해야 합니다. 에 대해 자세히 알아보십시오 "RDMA를 통해 NFS용 LIF 구성".
- 소스 또는 대상 LIF를 마이그레이션할 때 VMware VAAI 복사본 오프로드 작업이 실패합니다. Copy Off-load에 대한 자세한 내용:
  - "알아보십시오"
  - "알아보십시오"

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 네트워크 인터페이스를 마이그레이션합니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆에 있는 *>Migrate * 를 선택합니다 ⋮ .

> iSCSI LIF의 경우 * Migrate Interface * 대화 상자에서 HA 파트너의 대상 노드 및 포트를 선택합니다.

iSCSI LIF를 영구적으로 마이그레이션하려면 확인란을 선택합니다. iSCSI LIF는 영구적으로 마이그레이션되기 전에 오프라인 상태여야 합니다. 또한 iSCSI LIF를 영구적으로 마이그레이션한 후에는 취소할 수 없습니다. 되돌리기 옵션은 없습니다.

3. 마이그레이션 * 을 클릭합니다.
4. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF를 마이그레이션합니다 *

단계

특정 LIF를 마이그레이션할지 또는 모든 LIF를 마이그레이션할지 여부에 따라 적절한 작업을 수행합니다.

마이그레이션하려면…	다음 명령을 입력합니다…
특정 LIF	네트워크 인터페이스 마이그레이션
노드의 모든 데이터 및 클러스터 관리 LIF	네트워크 인터페이스 마이그레이션 모두
모든 LIF가 포트에서 해제됩니다	'network interface migrate-all-node <node> - port <port>'

다음 예제에서는 이라는 LIF를 마이그레이션하는 방법을 보여 줍니다 `datalif1` SVM에서 `vs0` 포트에 연결합니다 `e0d` 켜짐 `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

다음 예에서는 현재(로컬) 노드에서 모든 데이터 및 클러스터 관리 LIF를 마이그레이션하는 방법을 보여 줍니다.

```
network interface migrate-all -node local
```

관련 정보

- "네트워크 인터페이스 마이그레이션"

ONTAP 노드 페일오버 또는 포트 마이그레이션 후에 **LIF**를 홈 포트로 되돌립니다

LIF가 페일오버된 후 홈 포트로 되돌아가거나 수동으로 또는 자동으로 다른 포트로 마이그레이션될 수 있습니다. 특정 LIF의 홈 포트를 사용할 수 없는 경우 LIF는 현재 포트에 남아 있으며 되돌릴 수 없습니다.

이 작업에 대해

- 관리상 자동 되돌리기 옵션을 설정하기 전에 LIF의 홈 포트를 설정 상태로 전환할 경우 LIF는 홈 포트로 돌아가지 않습니다.
- "자동 되돌리기" 옵션의 값이 true로 설정되어 있지 않으면 LIF가 자동으로 복구되지 않습니다.
- LIF가 홈 포트로 되돌아가려면 "자동 되돌리기" 옵션이 설정되어 있는지 확인해야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 네트워크 인터페이스를 홈 포트로 되돌립니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆의 *>되돌리기 * 를 선택합니다 ⋮ .
3. 네트워크 인터페이스를 홈 포트로 되돌리려면 * Revert * 를 선택합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF를 홈 포트로 되돌릴 수 있습니다 *

단계

LIF를 홈 포트로 수동 또는 자동으로 되돌리기:

LIF를 홈 포트로 되돌리려면...	그런 다음 다음 다음 명령을 입력합니다.
수동	'network interface revert-vserver vserver_name-lif lif_name'
자동으로	'network interface modify -vserver vserver_name -lif lif_name -auto -revert true'

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

잘못 구성된 **ONTAP LIF**를 복구합니다

클러스터 네트워크가 스위치에 케이블로 연결되어 있지만 클러스터 IPspace에 구성된 모든 포트가 클러스터 IPspace에 구성된 다른 포트에 연결할 수 있는 것은 아닙니다.

이 작업에 대해

전환된 클러스터에서 클러스터 네트워크 인터페이스(LIF)가 잘못된 포트에 구성되어 있거나 클러스터 포트가 잘못된

네트워크에 연결되어 있는 경우 "cluster create" 명령이 실패하고 다음 오류가 표시될 수 있습니다.

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

에 대한 자세한 내용은 `cluster create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 `network port show` 명령의 결과는 여러 포트가 클러스터 LIF로 구성된 포트에 연결되기 때문에 클러스터 IPspace에 추가된 것을 보여 줄 수 있습니다. 그러나 결과는 `network port reachability show -detail` 명령어는 어떤 포트가 서로 연결되지 않았는지 보여줍니다.

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

클러스터 LIF로 구성된 다른 포트에 연결할 수 없는 포트에 구성된 클러스터 LIF에서 복구하려면 다음 단계를 수행하십시오.

단계

1. 클러스터 LIF의 홈 포트를 올바른 포트로 재설정합니다.

   ```
   network port modify -home-port
   ```

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

2. 클러스터 LIF가 구성되어 있지 않은 포트를 클러스터 브로드캐스트 도메인에서 제거합니다.

   ```
   network port broadcast-domain remove-ports
   ```

   에 대한 자세한 내용은 `network port broadcast-domain remove-ports` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 클러스터를 생성합니다.

   ```
   cluster create
   ```

결과

클러스터 생성을 완료하면 시스템이 올바른 구성을 감지하고 포트를 올바른 브로드캐스트 도메인에 배치합니다.

관련 정보

- "네트워크 포트 도달 가능성 표시"

ONTAP LIF를 삭제합니다

더 이상 필요하지 않은 네트워크 인터페이스(LIF)를 삭제할 수 있습니다.

시작하기 전에

삭제할 LIF는 사용 중이 아니어야 합니다.

단계

1. 다음 명령을 사용하여 삭제할 LIF를 관리 목적으로 사용 중지하도록 표시합니다.

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. "network interface delete" 명령을 사용하여 하나 또는 모든 LIF를 삭제합니다.

삭제하려면…	명령 입력…
특정 LIF	'network interface delete -vserver vserver_name -lif lif_name'
모든 LIF	'network interface delete-vserver vserver_name-lif *'

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

다음 명령을 실행하면 LIF mgmtd LIF가 삭제됩니다. 2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. LIF가 삭제되었는지 확인하려면 'network interface show' 명령을 사용하십시오.

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

ONTAP 가상 IP(VIP) LIF를 구성합니다

일부 차세대 데이터 센터에서는 여러 서브넷에서 LIF를 페일오버해야 하는 계층 3(IP) 네트워크 메커니즘을 사용합니다. ONTAP는 이러한 차세대 네트워크의 페일오버 요구사항을 충족하기 위해 VIP(가상 IP) 데이터 LIF와 관련 라우팅 프로토콜, BGP(Border Gateway Protocol)를 지원합니다.

이 작업에 대해

VIP 데이터 LIF는 서브넷의 일부가 아닌 LIF로, 동일한 IPspace에서 BGP LIF를 호스팅하는 모든 포트에서 연결할 수 있습니다. VIP 데이터 LIF는 개별 네트워크 인터페이스에 대한 호스트의 종속성을 제거합니다. 여러 개의 물리적 어댑터가 데이터 트래픽을 전달하므로 전체 로드가 단일 어댑터와 관련 서브넷에 집중되지 않습니다. VIP 데이터 LIF는 라우팅 프로토콜인 BGP(Border Gateway Protocol)를 통해 피어 라우터에 보급됩니다.

VIP 데이터 LIF는 다음과 같은 이점을 제공합니다.

- 브로드캐스트 도메인 또는 서브넷 이상의 LIF 이동성: VIP 데이터 LIF는 BGP를 통해 각 VIP 데이터 LIF의 현재 위치를 공유함으로써 네트워크의 모든 서브넷에 페일오버할 수 있습니다.
- 총 처리량: VIP 데이터 LIF는 여러 서브넷 또는 포트에서 데이터를 동시에 송수신할 수 있으므로 개별 포트의

대역폭을 초과하는 총 처리량을 지원할 수 있습니다.

BGP(Border Gateway Protocol) 설정

VIP LIF를 생성하기 전에 피어 라우터에 대한 VIP LIF의 존재를 알리는 데 사용되는 라우팅 프로토콜인 BGP를 설정해야 합니다.

ONTAP 9.9.1부터 VIP는 BGP 피어 그룹을 사용하여 기본 경로 자동화를 옵션으로 제공하여 구성을 간소화합니다.

ONTAP는 BGP 피어가 동일한 서브넷에 있을 때 BGP 피어를 다음 홉 라우터로 사용하여 기본 라우트를 학습할 수 있는 간단한 방법을 제공합니다. 이 기능을 사용하려면 '-use-peer-as-next-hop' 속성을 true로 설정합니다. 기본적으로 이 속성은 false 입니다.

정적 라우트가 구성된 경우 이러한 자동 기본 라우트보다 더 선호됩니다.

시작하기 전에

ASN(Autonomous System Number)이 구성된 BGP LIF에서 BGP 연결을 허용하도록 피어 라우터를 구성해야 합니다.

> ONTAP는 라우터에서 수신되는 라우트 알림을 처리하지 않으므로, 피어 라우터가 클러스터에 대한 라우트 업데이트를 보내지 않도록 구성해야 합니다. 이렇게 하면 피어와 통신하는 데 걸리는 시간이 단축되고 ONTAP 내의 내부 메모리 사용량이 줄어듭니다.

이 작업에 대해

BGP를 설정하려면 선택적으로 BGP 구성을 생성하고, BGP LIF를 생성하고, BGP 피어 그룹을 생성해야 합니다. ONTAP는 특정 노드에서 첫 번째 BGP 피어 그룹이 생성될 때 기본값으로 기본 BGP 구성을 자동으로 생성합니다.

BGP LIF는 피어 라우터를 사용하여 BGP TCP 세션을 설정하는 데 사용됩니다. 피어 라우터의 경우 BGP LIF는 VIP LIF에 도달하기 위한 다음 홉입니다. BGP LIF에서 페일오버가 비활성화되었습니다. BGP 피어 그룹은 피어 그룹이 사용하는 IPspace의 모든 SVM에 대한 VIP 경로를 알립니다. 피어 그룹에서 사용하는 IPspace는 BGP LIF에서 상속됩니다.

ONTAP 9.16.1부터는 BGP 피어 그룹에서 MD5 인증이 지원되어 BGP 세션을 보호합니다. MD5가 활성화되면 승인된 피어 사이에서만 BGP 세션을 설정 및 처리할 수 있으므로 권한이 없는 행위자에 의한 세션 중단을 방지할 수 있습니다.

및 `network bgp peer-group modify` 명령에 다음 필드가 `network bgp peer-group create` 추가되었습니다.

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

이러한 매개 변수를 사용하면 보안을 강화하기 위해 MD5 서명을 사용하여 BGP 피어 그룹을 구성할 수 있습니다. MD5 인증 사용에 적용되는 요구 사항은 다음과 같습니다.

- 매개 변수가 (으)로 설정된 `true` 경우에만 매개 변수를 `-md5-enabled` 지정할 수 `-md5-secret` 있습니다.
- MD5 BGP 인증을 활성화하려면 IPsec을 전역적으로 활성화해야 합니다. BGP LIF는 활성 IPsec 구성을 가질 필요가 없습니다. 을 "유선 암호화를 통해 IP 보안(IPsec)을 구성합니다"참조하십시오.
- NetApp는 ONTAP 컨트롤러에서 MD5를 구성하기 전에 라우터에 MD5를 구성하는 것이 좋습니다.

ONTAP 9.9.1부터 다음 필드가 추가되었습니다.

- `-asn` 또는 `-peer-asn` (4바이트 값) 특성 자체는 새로운 것이 아니지만 4바이트 정수를 사용합니다.
- `-med`
- `-use-peer-as-next-hop`

경로 우선 순위 지정을 위해 MED(Multi-Exit Discriminator) 지원을 통해 고급 경로 선택을 수행할 수 있습니다. Med는 라우터에 트래픽에 가장 적합한 경로를 선택하도록 지시하는 BGP 업데이트 메시지의 선택적 속성입니다. MED는 부호 없는 32비트 정수(0-4294967295)이며 더 낮은 값을 사용하는 것이 좋습니다.

ONTAP 9.8부터 이러한 필드는 'network BGP peer-group' 명령에 추가되었습니다.

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

이러한 BGP 특성을 사용하면 를 BGP 피어 그룹에 대한 경로 및 커뮤니티 속성으로 구성할 수 있습니다.

> ONTAP는 위의 BGP 속성을 지원하지만 라우터는 이를 인정할 필요가 없습니다. NetApp은 라우터에서 지원하는 속성을 확인하고 그에 따라 BGP 피어 그룹을 구성할 것을 적극 권장합니다. 자세한 내용은 라우터에서 제공한 BGP 설명서를 참조하십시오.

단계

1. 고급 권한 레벨에 로그인합니다.

   세트 프리빌리지 고급

2. 선택 사항: 다음 작업 중 하나를 수행하여 BGP 구성을 생성하거나 클러스터의 기본 BGP 구성을 수정합니다.

   a. BGP 구성 생성:

   ```
   network bgp config create -node {node_name | local} -asn <asn_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

   > - 이 `-routerid` 매개 변수는 AS 도메인 내에서만 고유해야 하는 점분리 십진수 32비트 값을 허용합니다. NetApp은 고유성을 보장하는 노드 관리 IP(v4) 주소를 사용할 것을 `<router_id>` 권장합니다.
   > - ONTAP BGP는 32비트 ASN 숫자를 지원하지만 표준 10진수 표기법만 지원됩니다. 사설 ASN에 대해 4259840001 대신 65000.1과 같은 점선 ASN 표기법은 지원되지 않습니다.

   2바이트 ASN이 포함된 샘플:

   ```
   network bgp config create -node node1 -asn 65502 -holdtime 180
   -routerid 1.1.1.1
   ```

   4바이트 ASN이 포함된 샘플:

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. 기본 BGP 구성을 수정합니다.

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` ASN 번호를 지정합니다. ONTAP 9.8부터 BGP의 ASN은 2바이트 비음수를 지원합니다. 16비트 숫자입니다(1 - 65534 사용 가능한 값). ONTAP 9.9.1부터 BGP용 ASN은 4바이트 비음의 정수(1 ~ 4294967295)를 지원합니다. 기본 ASN은 65501입니다. ASN 23456은 4바이트 ASN 기능을 발표하지 않는 피어와의 ONTAP 세션 설정을 위해 예약되어 있습니다.
- `<hold_time>` 보류 시간을 초 단위로 지정합니다. 기본값은 180입니다.

> ONTAP는 여러 IPspaces에 대해 BGP를 구성한 경우에도 하나의 글로벌, `<hold_time>` 및 `<router_id>` 만 `<asn_number>` 지원합니다. BGP와 모든 IP 라우팅 정보는 하나의 IPspace 내에서 완전히 격리된다. IPspace는 가상 라우팅 및 전달(VRF) 인스턴스와 같습니다.

3. 시스템 SVM을 위한 BGP LIF 생성:

   기본 IPspace의 경우 SVM 이름은 클러스터 이름입니다. 추가 IPspace의 경우 SVM 이름은 IPspace 이름과 동일합니다.

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

   BGP LIF에 대한 'default-route-공지' 서비스 정책 또는 "management-BGP" 서비스가 포함된 사용자 지정 서비스 정책을 사용할 수 있습니다.

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. 원격 피어 라우터로 BGP 세션을 설정하고 피어 라우터에 보급된 VIP 라우트 정보를 구성하는 데 사용되는 BGP 피어 그룹을 생성합니다.

   샘플 1: 자동 기본 경로 없이 피어 그룹을 생성합니다

   이 경우 관리자는 BGP 피어에 대한 정적 경로를 생성해야 합니다.

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

샘플 2: 자동 기본 라우트가 있는 피어 그룹을 생성합니다

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

샘플 3: MD5가 활성화된 피어 그룹을 만듭니다

a. IPsec 활성화:

   보안 IPsec config modify -is -enabled true

b. MD5가 활성화된 BGP 피어 그룹을 생성합니다.

   ```
   network bgp peer-group create -ipspace Default -peer-group
   <group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
   {-md5-enabled true}{-md5-secret <md5 secret in string or hex format>}
   ```

   16진수 키 사용 예:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657 4
```

문자열 사용 예:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

> BGP 피어 그룹을 생성한 후 명령을 실행하면 가상 이더넷 포트(v0a..v0z, v1a… 로 시작)가 `network port show` 나열됩니다. 이 인터페이스의 MTU는 항상 1500으로 보고됩니다. 트래픽에 사용되는 실제 MTU는 트래픽을 전송할 때 결정되는 물리적 포트(BGP LIF)에서 파생됩니다. 에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

가상 **IP(VIP)** 데이터 **LIF**를 생성합니다

VIP 데이터 LIF는 라우팅 프로토콜인 BGP(Border Gateway Protocol)를 통해 피어 라우터에 보급됩니다.

시작하기 전에

- BGP 피어 그룹을 설정하고 LIF를 생성할 SVM을 위한 BGP 세션을 활성화해야 합니다.
- SVM의 나가는 VIP 트래픽에 대해 BGP 라우터 또는 BGP LIF 서브넷의 다른 라우터에 대한 정적 경로를 생성해야 합니다.
- 나가는 VIP 트래픽이 사용 가능한 모든 경로를 사용할 수 있도록 다중 경로 라우팅을 켜야 합니다.

  다중 경로 라우팅이 활성화되지 않은 경우 나가는 모든 VIP 트래픽은 단일 인터페이스에서 이동합니다.

단계

1. VIP 데이터 LIF 생성:

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

   네트워크 인터페이스 생성 명령으로 홈 포트를 지정하지 않으면 VIP 포트가 자동으로 선택됩니다.

   기본적으로 VIP 데이터 LIF는 각 IPspace에 대해 'VIP'라는 시스템 생성 브로드캐스트 도메인에 속해 있습니다. VIP 브로드캐스트 도메인은 수정할 수 없습니다.

   VIP 데이터 LIF는 IPspace의 BGP LIF를 호스팅하는 모든 포트에서 동시에 연결할 수 있습니다. 로컬 노드에서 VIP의 SVM을 위한 활성 BGP 세션이 없는 경우, VIP 데이터 LIF는 해당 SVM을 위해 BGP 세션이 설정된 노드에서 다음 VIP 포트로 페일오버됩니다.

2. BGP 세션이 VIP 데이터 LIF의 SVM에 대한 UP 상태인지 확인합니다.

```
network bgp vserver-status show

Node        Vserver  bgp status
        ----------  -------- ---------
        node1       vs1      up
```

노드의 SVM에 대해 BGP 상태가 'down'이면 VIP 데이터 LIF가 SVM에 대해 BGP 상태가 가동 중인 다른 노드로 페일오버됩니다. 모든 노드에서 BGP 상태가 '소유'인 경우 VIP 데이터 LIF는 어느 곳에서나 호스팅할 수 없으며 LIF 상태가 '다운'입니다.

BGP 관리를 위한 명령입니다

ONTAP 9.5부터 ONTAP에서 BGP 세션을 관리하기 위해 'network BGP' 명령어를 사용한다.

BGP 구성 관리

원하는 작업	이 명령 사용...
BGP 구성을 생성합니다	`network bgp config create`
BGP 구성을 수정합니다	`network bgp config modify`
BGP 구성을 삭제합니다	`network bgp config delete`
BGP 구성을 표시합니다	`network bgp config show`
VIP LIF의 SVM에 대한 BGP 상태를 표시합니다	`network bgp vserver-status show`

BGP 기본값을 관리합니다

원하는 작업	이 명령 사용...
BGP 기본값을 수정합니다	`network bgp defaults modify`
BGP 기본값을 표시합니다	`network bgp defaults show`

BGP 피어 그룹을 관리합니다

원하는 작업	이 명령 사용...
BGP 피어 그룹을 생성합니다	`network bgp peer-group create`
BGP 피어 그룹을 수정합니다	`network bgp peer-group modify`
BGP 피어 그룹을 삭제합니다	`network bgp peer-group delete`
BGP 피어 그룹 정보를 표시합니다	`network bgp peer-group show`
BGP 피어 그룹의 이름을 바꿉니다	`network bgp peer-group rename`

MD5를 사용하여 **BGP** 피어 그룹을 관리합니다

ONTAP 9.16.1부터 기존 BGP 피어 그룹에서 MD5 인증을 사용하거나 사용하지 않도록 설정할 수 있습니다.

> 기존 BGP 피어 그룹에서 MD5를 활성화 또는 비활성화하면 BGP 연결이 종료되고 MD5 구성 변경 사항을 적용하기 위해 다시 생성됩니다.

원하는 작업	이 명령 사용...
기존 BGP 피어 그룹에서 MD5를 활성화합니다	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
기존 BGP 피어 그룹에서 MD5를 비활성화합니다	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

관련 정보

- "ONTAP 명령 참조입니다"
- "네트워크 BGP"
- "네트워크 인터페이스"
- "보안 IPsec 구성 수정"

네트워크 로드 밸런싱

DNS 로드 밸런싱을 사용하여 **ONTAP** 네트워크 트래픽을 최적화합니다

적절하게 로드된 LIF의 클라이언트 요청을 처리하도록 클러스터를 구성할 수 있습니다. 그 결과, LIF 및 포트의 활용률이 더욱 높아질수록 클러스터의 성능이 향상됩니다.

DNS 로드 밸런싱은 적절하게 로드된 데이터 LIF를 선택하고 사용 가능한 모든 포트(물리적, 인터페이스 그룹 및 VLAN)에서 사용자 네트워크 트래픽의 균형을 조정하는 데 도움이 됩니다.

DNS 로드 밸런싱을 통해 LIF는 SVM의 로드 밸런싱 영역과 연결됩니다. 사이트 전체의 DNS 서버는 모든 DNS 요청을 전달하고 네트워크 트래픽과 포트 리소스의 가용성(CPU 사용량, 처리량, 개방형 연결 등)을 기준으로 가장 적게 로드된 LIF를 반환하도록 구성됩니다. DNS 로드 밸런싱은 다음과 같은 이점을 제공합니다.

- 사용 가능한 리소스 간에 새 클라이언트 연결이 균형 있게 조정됩니다.
- 특정 SVM을 마운트할 때 사용할 LIF를 결정하기 위해 수작업이 필요하지 않습니다.
- DNS 로드 밸런싱이 NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0 및 S3.

ONTAP 네트워크의 **DNS** 로드 밸런싱에 대해 알아봅니다

클라이언트는 IP 주소(LIF와 연결) 또는 호스트 이름(여러 IP 주소와 연결)을 지정하여 SVM을

마운트합니다. 기본적으로 LIF는 라운드 로빈 방식으로 사이트 전체 DNS 서버에서 선택되어 있으며, 이 방식을 통해 모든 LIF에서 워크로드의 균형을 조정할 수 있습니다.

라운드 로빈 로드 밸런싱으로 인해 일부 LIF가 오버로드될 수 있으므로 SVM에서 호스트 이름 확인을 처리하는 DNS 로드 밸런싱 존을 사용할 수 있습니다. DNS 로드 밸런싱 존을 사용하면 사용 가능한 리소스 전체에서 새 클라이언트 연결의 균형을 보다 효율적으로 유지할 수 있어 클러스터의 성능이 향상됩니다.

DNS 로드 밸런싱 존은 클러스터 내의 DNS 서버로서 모든 LIF의 로드를 동적으로 평가하고 적절하게 로드된 LIF를 반환합니다. 로드 밸런싱 영역에서 DNS는 각 LIF에 로드(메트릭)를 기준으로 가중치를 할당합니다.

모든 LIF에는 홈 노드의 포트 로드 및 CPU 활용률을 기준으로 가중치가 할당됩니다. 로드가 적은 포트에 있는 LIF는 DNS 쿼리에서 반환될 가능성이 높습니다. 가중치는 수동으로 지정할 수도 있습니다.

ONTAP 네트워크에 대한 **DNS** 로드 밸런싱 존을 생성합니다

DNS 로드 밸런싱 영역을 생성하여 LIF에 마운트된 클라이언트 수, 즉 로드를 기반으로 LIF를 동적으로 선택할 수 있습니다. 데이터 LIF를 생성하는 동안 로드 밸런싱 존을 생성할 수 있습니다.

시작하기 전에

로드 밸런싱 존에 대한 모든 요청을 구성된 LIF로 전달하도록 사이트 전체 DNS 서버의 DNS 전달자를 구성해야 합니다.

그만큼"NetApp 지식 기반: 클러스터 모드에서 DNS 부하 분산을 설정하는 방법" 조건부 전달을 사용하여 DNS 부하 분산을 구성하는 방법에 대한 자세한 정보가 포함되어 있습니다.

이 작업에 대해

- 모든 데이터 LIF는 DNS 로드 밸런싱 존 이름에 대한 DNS 쿼리에 응답할 수 있습니다.
- DNS 로드 밸런싱 존은 클러스터에서 고유한 이름을 가져야 하며 영역 이름은 다음 요구 사항을 충족해야 합니다.
  - 256자를 초과하면 안 됩니다.
  - 최소 하나의 기간을 포함해야 합니다.
  - 첫 번째 문자와 마지막 문자는 마침표 또는 기타 특수 문자여야 합니다.
  - 문자 사이에 공백을 포함할 수 없습니다.
  - DNS 이름의 각 레이블은 63자를 초과할 수 없습니다.

    레이블은 기간 전후에 나타나는 텍스트입니다. 예를 들어 storage.company.com 이라는 DNS 영역에는 세 개의 레이블이 있습니다.

단계

명령을 옵션과 함께 `dns-zone` 사용하여 `network interface create` DNS 로드 밸런싱 존을 생성합니다. 에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

로드 밸런싱 영역이 이미 존재하는 경우 LIF가 이 영역에 추가됩니다.

다음 예제에서는 LIF 'lif1'을 생성하는 동안 storage.company.com 이라는 DNS 로드 밸런싱 존을 생성하는 방법을 보여 줍니다.

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

로드 밸런싱 존에서 **ONTAP LIF**를 추가 또는 제거합니다

SVM(가상 머신)의 DNS 로드 밸런싱 영역에서 LIF를 추가하거나 제거할 수 있습니다. 로드 밸런싱 영역에서 모든 LIF를 동시에 제거할 수도 있습니다.

시작하기 전에

- 로드 밸런싱 존의 모든 LIF는 동일한 SVM에 속해야 합니다.
- LIF는 하나의 DNS 로드 밸런싱 존에 포함될 수 있습니다.
- LIF가 다른 서브넷에 속한 경우 각 서브넷에 대한 페일오버 그룹을 설정해야 합니다.

이 작업에 대해

관리 다운 상태인 LIF는 DNS 로드 밸런싱 영역에서 일시적으로 제거됩니다. LIF가 관리 설정 상태로 돌아가면 LIF가 DNS 로드 밸런싱 존에 자동으로 추가됩니다.

단계

LIF를 로드 밸런싱 존에 추가하거나 LIF에서 제거합니다.

원하는 작업	입력…
LIF를 추가합니다	'network interface modify -vserver_vserver_name_-lif_lif_name_-dns -zone_zone_name_' 예: 'network interface modify -vserver vs1-lif data1-dns-zone cifs.company.com`
단일 LIF를 제거합니다	'network interface modify -vserver_vserver_name_-lif_lif_name_-dns-zone none' 예: 'network interface modify -vserver vs1-lif data1-dns-zone none
모든 LIF를 제거합니다	'network interface modify -vserver_vserver_name_-lif * -dns-zone none' 예: 'network interface modify -vs0 -lif * -dns-zone none' SVM의 모든 LIF를 해당 영역에서 제거하여 로드 밸런싱 영역에서 SVM을 제거할 수 있습니다.

관련 정보

- "네트워크 인터페이스 수정"

ONTAP 네트워크에 대한 **DNS** 서비스를 구성합니다

NFS 또는 SMB 서버를 생성하기 전에 SVM을 위한 DNS 서비스를 구성해야 합니다. 일반적으로 DNS 이름 서버는 NFS 또는 SMB 서버가 연결할 도메인의 Active Directory 통합 DNS 서버입니다.

이 작업에 대해

Active Directory 통합 DNS 서버에는 도메인 LDAP 및 도메인 컨트롤러 서버에 대한 SRV(서비스 위치 레코드)가

포함되어 있습니다. SVM이 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾을 수 없는 경우 NFS 또는 SMB 서버 설정에 실패합니다.

SVM은 hosts name services ns-switch 데이터베이스를 사용하여 호스트에 대한 정보를 찾을 때 사용할 이름 서비스와 순서를 결정합니다. 호스트 데이터베이스에 대해 지원되는 두 가지 이름 서비스는 파일과 DNS입니다.

SMB 서버를 생성하기 전에 DNS가 소스 중 하나인지 확인해야 합니다.

> mgwd 프로세스 및 SecD 프로세스의 DNS 이름 서비스에 대한 통계를 보려면 통계 UI를 사용합니다.

단계

1. 호스트 이름 서비스 데이터베이스에 대한 현재 구성을 확인합니다. 이 예에서는 호스트 이름 서비스 데이터베이스가 기본 설정을 사용합니다.

   'vserver services name-service_ns-switch_show-vserver_vs1_-database_hosts_'

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. 필요한 경우 다음 작업을 수행합니다.

   a. DNS 이름 서비스를 호스트 이름 서비스 데이터베이스에 원하는 순서로 추가하거나 소스를 다시 정렬합니다.

      이 예에서는 호스트 데이터베이스가 DNS 및 로컬 파일을 순서대로 사용하도록 구성되어 있습니다.

      'vserver services name-service_ns-switch_modify -vserver_vs1_-database_hosts_-sources_dns, files_'

   b. 이름 서비스 구성이 올바른지 확인합니다.

      'vserver services name-service_ns-switch_show-vserver_vs1_-database_hosts_'

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Name Service Source Order: dns, files
   ```

3. DNS 서비스를 구성합니다.

   'vserver services name-service dns create-vserver_vs1_-domain *example.com,example2.com* -name -servers_10.0.0.50,10.0.0.51_'

   > vserver services name-service dns create 명령은 자동 구성 검증을 수행하고 ONTAP가 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

4. DNS 구성이 올바르고 서비스가 활성화되었는지 확인합니다.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. 이름 서버의 상태를 확인합니다.

   'vserver services name-service dns check-vserver_vs1_'

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

SVM에서 동적 **DNS**를 구성합니다

Active Directory 통합 DNS 서버가 DNS에 있는 NFS 또는 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SVM에서 DDNS(동적 DNS)를 구성해야 합니다.

시작하기 전에

SVM에서 DNS 이름 서비스를 구성해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서버를 사용해야 하며 SVM을 위해 NFS 또는 SMB 서버 또는 Active Directory 계정을 생성해야 합니다.

이 작업에 대해

지정된 FQDN(정규화된 도메인 이름)은 고유해야 합니다.

지정된 FQDN(정규화된 도메인 이름)은 고유해야 합니다.

- NFS의 경우 'vserver services name-service dns dynamic-update' 명령의 일부로 '-vserver-FQDN'에 지정된 값이 LIF의 등록 FQDN이 됩니다.
- SMB의 경우 CIFS 서버 NetBIOS 이름 및 CIFS 서버 정규화된 도메인 이름으로 지정된 값이 LIF의 등록 FQDN이 됩니다. ONTAP에서는 구성할 수 없습니다. 다음 시나리오에서 LIF FQDN은 "CIFS_VS1.EXAMPLE.COM": 입니다

```
cluster1::> cifs server show -vserver vs1

                                            Vserver: vs1
                         CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

DDNS 업데이트에 대한 RFC 규칙을 준수하지 않는 SVM FQDN의 구성 오류를 방지하려면 RFC와 호환되는 FQDN 이름을 사용합니다. 자세한 내용은 을 참조하십시오 "RFC 1123".

단계

1. SVM에서 DDNS 구성:

   'vserver services name-service dns dynamic-update modify -vserver_vserver_name_-is-enabled_true_[-use-secure{true|false}-vserver-FQDN_FQDN_used_for_dns_updates_'

   'vserver services name-service dns dynamic-update modify -vserver_vs1_-is-enabled_true_-use -secure_true_-vserver-FQDN *vs1.example.com*`

   별표는 사용자 지정 FQDN의 일부로 사용할 수 없습니다. 예를 들어, '* .netapp.com'은(는) 유효하지 않습니다.

2. DDNS 구성이 올바른지 확인합니다.

   'vserver services name-service dns dynamic-update show'

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

ONTAP 네트워크에 대한 동적 DNS 서비스를 구성합니다

Active Directory 통합 DNS 서버가 DNS에 있는 NFS 또는 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SVM에서 DDNS(동적 DNS)를 구성해야 합니다.

시작하기 전에

SVM에서 DNS 이름 서비스를 구성해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서버를 사용해야 하며 SVM을 위해 NFS 또는 SMB 서버 또는 Active Directory 계정을 생성해야 합니다.

이 작업에 대해

지정된 FQDN은 고유해야 합니다.

> DDNS 업데이트에 대한 RFC 규칙을 준수하지 않는 SVM FQDN의 구성 오류를 방지하려면 RFC와 호환되는 FQDN 이름을 사용합니다.

단계

1. SVM에서 DDNS 구성:

   'vserver services name-service dns dynamic-update modify -vserver_vserver_name_-is-enabled_true_[-use-secure{true|false}-vserver-FQDN_FQDN_used_for_dns_updates_'

   'vserver services name-service dns dynamic-update modify -vserver_vs1_-is-enabled_true_-use -secure_true_-vserver-FQDN *vs1.example.com*`

   별표는 사용자 지정 FQDN의 일부로 사용할 수 없습니다. 예를 들어, '* .netapp.com'은(는) 유효하지 않습니다.

2. DDNS 구성이 올바른지 확인합니다.

   'vserver services name-service dns dynamic-update show'

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

호스트 이름 확인

ONTAP 네트워크의 호스트 이름 확인에 대해 알아봅니다

클라이언트에 대한 액세스를 제공하고 서비스에 액세스하려면 ONTAP가 호스트 이름을 숫자 IP 주소로 변환할 수 있어야 합니다. 로컬 또는 외부 이름 서비스를 사용하여 호스트 정보를 확인하도록 SVM(스토리지 가상 시스템)을 구성해야 합니다. ONTAP에서는 외부 DNS 서버 구성 또는 호스트 이름 확인을 위한 로컬 호스트 파일 구성을 지원합니다.

외부 DNS 서버를 사용하는 경우 DDNS(동적 DNS)를 구성하여 스토리지 시스템에서 DNS 서버로 새 DNS 정보 또는 변경된 DNS 정보를 자동으로 전송할 수 있습니다. 동적 DNS 업데이트가 없으면 새 시스템을 온라인으로 연결하거나 기존 DNS 정보가 변경될 때 DNS 정보(DNS 이름 및 IP 주소)를 식별된 DNS 서버에 수동으로 추가해야 합니다. 이 프로세스는 느리고 오류가 발생하기 쉽습니다. 재해 복구 중에 수동 구성으로 인해 다운타임이 오래 발생할 수 있습니다.

ONTAP 네트워크의 호스트 이름 확인을 위해 **DNS**를 구성합니다

DNS를 사용하여 로컬 또는 원격 소스에 액세스하여 호스트 정보를 확인할 수 있습니다. 이러한 소스 중 하나 또는 둘 다에 액세스하려면 DNS를 구성해야 합니다.

ONTAP는 클라이언트에 대한 적절한 액세스를 제공하기 위해 호스트 정보를 조회해야 합니다. 호스트 정보를 얻기 위해 ONTAP가 로컬 또는 외부 DNS 서비스에 액세스하도록 이름 서비스를 구성해야 합니다.

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다.

외부 **DNS** 서버를 사용하여 호스트 이름 확인을 위해 **SVM** 및 데이터 **LIF**를 구성합니다

SVM에서 DNS를 사용하도록 설정하려면 'vserver services name-service dns' 명령을 사용하고, 호스트 이름 확인을 위해 DNS를 사용하도록 구성할 수 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. DNS 서버 이름을 하나만 입력하면 'vserver services name-service dns create' 명령이 경고를 보냅니다.

이 작업에 대해

을 참조하십시오 동적 DNS 서비스를 구성합니다 SVM에서 동적 DNS 구성에 대한 자세한 내용은 를 참조하십시오.

단계

1. SVM에서 DNS 활성화:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> 를 클릭합니다 `vserver services name-service dns create` Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com
                                      Name Server
Vserver             Name Server      Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50        up           Response time (msec): 2
vs1.example.com     10.0.0.51        up           Response time (msec): 2
```

DNS와 관련된 서비스 정책에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9.6 이상의 LIF 및 서비스 정책".

호스트 이름 확인을 위해 이름 서비스 스위치 테이블을 구성합니다

ONTAP가 로컬 또는 외부 이름 서비스에 문의하여 호스트 정보를 검색할 수 있도록 이름 서비스 스위치 테이블을 올바르게 구성해야 합니다.

시작하기 전에

사용자 환경에서 호스트 매핑에 사용할 이름 서비스를 결정해야 합니다.

단계

1. 이름 서비스 스위치 테이블에 필요한 항목을 추가합니다.

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. 이름 서비스 스위치 테이블에 원하는 순서대로 필요한 항목이 포함되어 있는지 확인합니다.

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

예

다음 예에서는 SVM VS1에 대한 이름 서비스 스위치 테이블의 항목을 수정하여 먼저 로컬 호스트 파일을 사용한 다음 외부 DNS 서버를 사용하여 호스트 이름을 확인합니다.

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

ONTAP hosts 테이블을 관리하는 ONTAP 명령

클러스터 관리자는 SVM(관리 스토리지 가상 시스템)의 호스트 테이블에 있는 호스트 이름 항목을 추가, 수정, 삭제 및 볼 수 있습니다. SVM 관리자는 할당된 SVM에 대해서만 호스트 이름 항목을 구성할 수 있습니다.

로컬 호스트 이름 항목을 관리하는 명령입니다

'vserver services name-service dns hosts' 명령을 사용하여 DNS 호스트 테이블 항목을 생성, 수정 또는 삭제할 수 있습니다.

DNS 호스트 이름 항목을 만들거나 수정할 때 쉼표로 구분된 여러 개의 별칭 주소를 지정할 수 있습니다.

원하는 작업	이 명령 사용…
DNS 호스트 이름 항목을 생성합니다	'vserver services name-service DNS hosts create'

DNS 호스트 이름 항목을 수정합니다	'vserver services name-service dns hosts modify'
DNS 호스트 이름 항목을 삭제합니다	'vserver services name-service DNS hosts delete'

명령에 대한 자세한 `vserver services name-service dns hosts` 내용은 를 참조하십시오 "ONTAP 명령 참조입니다".

네트워크 보안

모든 **SSL** 연결에 **FIPS**를 사용하여 **ONTAP** 네트워크 보안을 구성합니다

ONTAP 모든 SSL 연결에 대해 연방 정보 처리 표준(FIPS) 140-2를 준수합니다. ONTAP 내에서 SSL FIPS 모드를 켜고 끌 수 있고, SSL 프로토콜을 전역적으로 설정하고, 취약한 암호를 끌 수 있습니다.

기본적으로 ONTAP의 SSL은 FIPS 준수가 비활성화되고 다음 TLS 프로토콜이 활성화된 상태로 설정됩니다.

- TLSv1.3(ONTAP 9.11.1부터 시작)
- TLSv1.2

이전 ONTAP 릴리스에는 기본적으로 다음과 같은 TLS 프로토콜이 활성화되어 있었습니다.

- TLSv1.1(ONTAP 9.12.1부터 기본적으로 비활성화됨)
- TLSv1(ONTAP 9.8부터 기본적으로 비활성화됨)

SSL FIPS 모드가 활성화되면 ONTAP에서 외부 클라이언트 또는 ONTAP 외부의 서버 구성 요소로의 SSL 통신은 SSL에 FIPS 호환 암호화를 사용합니다.

관리자 계정이 SSH 공개 키로 SVM에 액세스하려면 SSL FIPS 모드를 활성화하기 전에 호스트 키 알고리즘이 지원되는지 확인해야 합니다.

- 참고: * ONTAP 9.11.1 이상 릴리스에서 호스트 키 알고리즘 지원이 변경되었습니다.

ONTAP 릴리즈	지원되는 키 유형	지원되지 않는 키 유형입니다
9.11.1 이상	ECDSA-SHA2-nistp256	RSA-SHA2-512 + RSA - SHA2-256 + ssh-ed25519 + ssh-dss+ssh-rssh-rsa
9.10.1 이하	ECDSA-SHA2-nistp256+ssh-ed25519	SSH-DSS+ssh-rsa를 사용합니다

FIPS를 활성화하기 전에 지원되는 키 알고리즘이 없는 기존 SSH 공개 키 계정을 지원되는 키 유형으로 재구성해야 합니다. 그렇지 않으면 관리자 인증이 실패합니다.

자세한 내용은 을 참조하십시오 "SSH 공개 키 계정을 활성화합니다".

ONTAP 9.18.1은 SSL을 위한 ML-KEM, ML-DSA 및 SLH-DSA 포스트 양자 컴퓨팅 암호화 알고리즘에 대한 지원을 도입하여 향후 발생할 수 있는 양자 컴퓨터 공격에 대비한 보안 계층을 추가로 제공합니다. 이러한 알고리즘은 다음과 같은 경우에만 사용할 수 있습니다.FIPS가 비활성화되었습니다 . FIPS가 비활성화되어 있고 피어가 이를 지원하는 경우 포스트 양자 암호화 알고리즘이 협상됩니다.

FIPS를 사용하도록 설정합니다

모든 보안 사용자는 시스템 설치 또는 업그레이드 직후 보안 구성을 조정하는 것이 좋습니다. SSL FIPS 모드가 활성화되면 ONTAP에서 외부 클라이언트 또는 ONTAP 외부의 서버 구성 요소로의 SSL 통신은 SSL에 FIPS 호환 암호화를 사용합니다.

> FIPS가 설정되어 있으면 RSA 키 길이 4096으로 인증서를 설치하거나 생성할 수 없습니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. FIPS 활성화:

   ```
   security config modify * -is-fips-enabled true
   ```

3. 계속하라는 메시지가 나타나면 y를 입력합니다
4. ONTAP 9.9.1부터 재부팅이 필요하지 않습니다. ONTAP 9.8 또는 이전 버전을 사용하는 경우 클러스터의 각 노드를 하나씩 수동으로 재부팅하세요.

예

ONTAP 9.9.1 이상을 실행 중인 경우 경고 메시지가 표시되지 않습니다.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

및 SSL FIPS 모드 구성에 대한 자세한 `security config modify` 내용은 를 "ONTAP 명령 참조입니다 "참조하십시오.

FIPS를 비활성화합니다

ONTAP 9.18.1부터 ONTAP 의 SSL은 ML-KEM, ML-DSA, SLH-DSA 포스트 양자 컴퓨팅 암호화 알고리즘을 지원합니다. 이러한 알고리즘은 FIPS가 비활성화되어 있고 피어가 이를 지원하는 경우에만 사용할 수 있습니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 다음을 입력하여 FIPS를 비활성화합니다.

   ```
   security config modify -is-fips-enabled false
   ```

3. 계속하라는 메시지가 나타나면 y를 입력합니다.
4. ONTAP 9.9.1부터 재부팅이 필요하지 않습니다. ONTAP 9.8 또는 이전 버전을 사용하는 경우 클러스터의 각 노드를 수동으로 재부팅하세요.

SSLv3 프로토콜을 사용해야 하는 경우 위의 절차에 따라 FIPS를 비활성화해야 합니다. FIPS가 비활성화된 경우에만 SSLv3를 활성화할 수 있습니다.

다음 명령을 사용하여 SSLv3를 활성화할 수 있습니다. ONTAP 9.9.1 이상을 실행 중인 경우 경고 메시지가 나타나지 않습니다.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

FIPS 준수 상태를 봅니다

전체 클러스터에서 현재 보안 구성 설정이 실행되고 있는지 확인할 수 있습니다.

단계

1. ONTAP 9.8 또는 이전 버전을 사용하는 경우 클러스터의 각 노드를 하나씩 수동으로 재부팅하세요.
2. 현재 준수 상태 보기:

   '보안 구성 쇼'

```
cluster1::> security config show
Cluster     Supported
FIPS Mode   Protocols Supported Cipher Suites
---------- ---------
-------------------------------------------------------------
false       TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
            TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                      TLS_RSA_WITH_AES_128_CBC_SHA,
                      TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                      TLS_RSA_WITH_AES_256_CCM_8,
                      ...
```

에 대한 자세한 내용은 `security config show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "FIPS 203: 모듈 격자 기반 키 캡슐화 메커니즘 표준(ML-KEM)"
- "FIPS 204: 모듈 격자 기반 디지털 서명 표준(ML-DSA)"
- "FIPS 205: 상태 비저장 해시 기반 디지털 서명 표준(SLH-DSA)"

IPsec 전송 중 암호화를 구성합니다

ONTAP 네트워크에서 IP 보안 사용을 준비합니다

ONTAP 9.8부터 IP 보안(IPsec)을 사용하여 네트워크 트래픽을 보호할 수 있습니다. IPsec은 ONTAP에서 사용할 수 있는 여러 가지 데이터 이동 중 또는 전송 중 암호화 옵션 중 하나입니다. IPsec을 프로덕션 환경에서 사용하기 전에 구성할 준비를 해야 합니다.

ONTAP에서 IP 보안 구현

IPSec은 IETF에서 관리하는 인터넷 표준입니다. IP 레벨에서 네트워크 엔드포인트 간에 흐르는 트래픽에 대한 인증뿐 아니라 데이터 암호화 및 무결성을 제공합니다.

ONTAP를 통해 IPsec은 ONTAP와 NFS, SMB 및 iSCSI 프로토콜을 포함한 다양한 클라이언트 간의 모든 IP 트래픽을 보호합니다. 네트워크 트래픽은 개인 정보 보호 및 데이터 무결성 외에도 재생 및 메시지 가로채기 공격과 같은 여러 공격으로부터 보호됩니다. ONTAP는 IPsec 전송 모드 구현을 사용합니다. IPv4 또는 IPv6를 사용하여 ONTAP와 클라이언트 간의 키 자료를 협상하는 데 IKE(인터넷 키 교환) 프로토콜 버전 2를 활용합니다.

클러스터에서 IPsec 기능이 활성화된 경우 네트워크에는 다양한 트래픽 특성과 일치하는 ONTAP SPD(보안 정책 데이터베이스)에 하나 이상의 항목이 필요합니다. 이러한 항목은 데이터를 처리하고 전송하는 데 필요한 특정 보호 세부 정보(예: 암호 그룹 및 인증 방법)에 매핑됩니다. 각 클라이언트에는 해당 SPD 항목도 필요합니다.

특정 트래픽 유형의 경우 다른 이동 중인 데이터 암호화 옵션이 더 선호될 수 있습니다. 예를 들어, NetApp SnapMirror 및 클러스터 피어링 트래픽의 암호화를 위해 일반적으로 IPsec 대신 TLS(전송 계층 보안) 프로토콜을 사용하는 것이 좋습니다. TLS는 대부분의 상황에서 더 나은 성능을 제공하기 때문입니다.

관련 정보

- "Internet Engineering Task Force의 약어입니다"
- "RFC 4301: 인터넷 프로토콜에 대한 보안 아키텍처"

ONTAP IPsec 구현의 진화

IPsec은 ONTAP 9.8에서 처음 도입되었습니다. 이후 ONTAP 릴리스에서는 아래에 설명된 대로 구현 방식이 지속적으로 발전해 왔습니다.

ONTAP 9.18.1

IPsec 하드웨어 오프로드에 대한 지원이 IPv6 트래픽으로 확장되었습니다.

ONTAP 9.17.1

IPsec 하드웨어 오프로드에 대한 지원이 확장되었습니다. "링크 집계 그룹" . "포스트퀀텀 사전 공유 키(PPK)" IPsec 사전 공유 키(PSK) 인증이 지원됩니다.

ONTAP 9.16.1

암호화 및 무결성 검사와 같은 여러 암호화 작업을 지원되는 NIC 카드로 오프로드할 수 있습니다. 자세한 내용은 을 IPsec 하드웨어 오프로드 기능 참조하십시오.

ONTAP 9.12.1

MetroCluster IP 및 MetroCluster 패브릭 연결 구성에서 IPsec 프런트엔드 호스트 프로토콜 지원을 사용할 수 있습니다. MetroCluster 클러스터와 함께 제공되는 IPsec 지원은 프런트 엔드 호스트 트래픽으로 제한되며 MetroCluster 인터클러스터 LIF에서는 지원되지 않습니다.

ONTAP 9.10.1

PSK 외에도 인증서를 사용하여 IPsec 인증을 수행할 수 있습니다. ONTAP 9.10.1 이전에는 PSK만 인증에 지원되었습니다.

ONTAP 9.9.1

IPsec에 사용되는 암호화 알고리즘은 FIPS 140-2 검증을 거쳤습니다. 이러한 알고리즘은 FIPS 140-2 검증을 수행하는 ONTAP의 NetApp 암호화 모듈에 의해 처리됩니다.

ONTAP 9.8

IPsec에 대한 지원은 처음에 전송 모드 구현에 따라 사용할 수 있습니다.

IPsec 하드웨어 오프로드 기능

ONTAP 9.16.1 이상을 사용하는 경우 암호화 및 무결성 검사와 같은 계산 집약적인 특정 작업을 스토리지 노드에 설치된 NIC(Network Interface Controller) 카드로 오프로드할 수 있습니다. NIC 카드로 오프로드된 작업의 처리량은 약 5% 이하입니다. 이를 통해 IPsec으로 보호되는 네트워크 트래픽의 성능과 처리량을 크게 향상시킬 수 있습니다.

요구 사항 및 권장 사항

IPsec 하드웨어 오프로드 기능을 사용하기 전에 고려해야 할 몇 가지 요구 사항이 있습니다.

지원되는 이더넷 카드

지원되는 이더넷 카드만 설치하고 사용해야 합니다. ONTAP 9.16.1부터 지원되는 이더넷 카드는 다음과 같습니다.

- X50131A(2p, 40G/100G/200g/400G 이더넷 컨트롤러)

- X60132A(4P, 10G/25G 이더넷 컨트롤러)

ONTAP 9.17.1에서는 다음 이더넷 카드에 대한 지원이 추가되었습니다.

- X50135A(2p, 40G/100G 이더넷 컨트롤러)
- X60135A(2p, 40G/100G 이더넷 컨트롤러)

X50131A 및 X50135A 카드는 다음 플랫폼에서 지원됩니다.

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K 를 참조하십시오
- AFF A90 를 참조하십시오
- AFF A70 를 참조하십시오

X60132A 및 X60135A 카드는 다음 플랫폼에서 지원됩니다.

- ASA A50
- ASA A30
- ASA A20
- AFF A50 를 참조하십시오
- AFF A30 를 참조하십시오
- AFF A20 를 참조하십시오

를 참조하십시오 "NetApp Hardware Universe를 참조하십시오" 지원되는 플랫폼과 카드에 대한 자세한 내용은 여기를 참조하세요.

클러스터 범위

IPsec 하드웨어 오프로드 기능은 클러스터에 대해 전역적으로 구성됩니다. 예를 들어, 명령은 `security ipsec config` 클러스터의 모든 노드에 적용됩니다.

일관된 구성

지원되는 NIC 카드는 클러스터의 모든 노드에 설치되어야 합니다. 지원되는 NIC 카드를 일부 노드에서만 사용할 수 있는 경우 일부 LIF가 오프로드 지원 NIC에 호스팅되지 않으면 페일오버 후 성능이 크게 저하될 수 있습니다.

다시 재생 안 함

ONTAP(기본 구성) 및 IPsec 클라이언트에서 IPsec 재생 방지 보호를 비활성화해야 합니다. 비활성화하지 않으면 조각화 및 다중 경로(중복 경로)가 지원되지 않습니다.

ONTAP IPsec 구성이 기본값에서 재생 방지 보호를 사용하도록 변경된 경우 다음 명령을 사용하여 사용하지 않도록 설정합니다.

```
security ipsec config modify -replay-window 0
```

클라이언트에서 IPsec 재생 방지 보호가 해제되어 있는지 확인해야 합니다. 재생 방지 보호를 비활성화하려면 클라이언트에 대한 IPsec 설명서를 참조하십시오.

제한 사항

IPsec 하드웨어 오프로드 기능을 사용하기 전에 고려해야 할 몇 가지 제한 사항이 있습니다.

IPv6를 참조하십시오

ONTAP 9.18.1부터 IPsec 하드웨어 오프로드 기능에 IPv6가 지원됩니다. ONTAP 9.18.1 이전에는 IPsec 하드웨어 오프로드가 IPv6를 지원하지 않았습니다.

확장 순서 번호

IPsec 확장 시퀀스 번호는 하드웨어 오프로드 기능에서 지원되지 않습니다. 일반적인 32비트 시퀀스 번호만 사용됩니다.

Link Aggregation

ONTAP 9.17.1부터 IPsec 하드웨어 오프로드 기능을 사용할 수 있습니다. "링크 집계 그룹" .

9.17.1 이전 버전에서는 IPsec 하드웨어 오프로드 기능이 링크 집계를 지원하지 않습니다. 다음에서 관리하는 인터페이스 또는 링크 집계 그룹과 함께 사용할 수 없습니다. `network port ifgrp` ONTAP CLI에서 명령을 실행합니다.

ONTAP CLI에서 구성을 지원합니다

ONTAP 9.16.1에서는 아래와 같이 IPsec 하드웨어 오프로드 기능을 지원하도록 기존 CLI 명령 세 개가 업데이트됩니다. 자세한 내용은 를 "ONTAP에서 IP 보안을 구성합니다"참조하십시오.

ONTAP 명령	업데이트
'보안 IPsec 구성 표시'	부울 매개 변수는 `Offload Enabled` 현재 NIC 오프로드 상태를 표시합니다.
`security ipsec config modify`	매개 변수는 `is-offload-enabled` NIC 오프로드 기능을 활성화 또는 비활성화하는 데 사용할 수 있습니다.
`security ipsec config show-ipsecsa`	인바운드와 아웃바운드 트래픽을 바이트 및 패킷으로 표시하기 위해 새로운 카운터 4개가 추가되었습니다.

ONTAP REST API에서 구성 지원

아래에 설명된 대로 IPsec 하드웨어 오프로드 기능을 지원하도록 ONTAP 9.16.1에서 두 개의 기존 REST API 끝점이 업데이트되었습니다.

REST 엔드포인트	업데이트
`/api/security/ipsec`	매개 변수가 `offload_enabled` 추가되었으며 패치 메서드에서 사용할 수 있습니다.
`/api/security/ipsec/security_association`	오프로드 기능에 의해 처리된 총 바이트 및 패킷을 추적하기 위해 두 개의 새로운 카운터 값이 추가되었습니다.

를 비롯한 ONTAP REST API에 대한 자세한 내용은 ONTAP 자동화 설명서 를 "ONTAP REST API의 새로운 기능" 참조하십시오. 에 대한 자세한 내용은 ONTAP 자동화 설명서를 검토해야 "IPsec 끝점" 합니다.

관련 정보

- "보안 ipsec"

ONTAP 네트워크에 대한 **IP** 보안을 구성합니다

ONTAP 클러스터에서 IPsec 전송 중 암호화를 구성하고 활성화하려면 몇 가지 작업을 수행해야 합니다.

> IPsec을 구성하기 전에 반드시 "IP 보안 사용을 준비합니다"검토하십시오. 예를 들어, ONTAP 9.16.1부터 사용 가능한 IPsec 하드웨어 오프로드 기능을 사용할지 여부를 결정해야 할 수 있습니다.

클러스터에서 **IPsec**을 활성화합니다

클러스터에서 IPsec을 활성화하여 전송 중에 데이터가 지속적으로 암호화되고 안전하게 보호되도록 할 수 있습니다.

단계

1. IPsec이 이미 활성화되어 있는지 확인:

   '보안 IPsec 구성 표시'

   결과에 "IPsec 사용: 거짓"이 포함된 경우 다음 단계를 진행합니다.

2. IPsec 활성화:

   보안 IPsec config modify -is -enabled true

   부울 매개 변수를 사용하여 IPsec 하드웨어 오프로드 기능을 활성화할 수 `is-offload-enabled` 있습니다.

3. 검색 명령을 다시 실행합니다.

   '보안 IPsec 구성 표시'

   그 결과에는 이제 "IPsec 사용: 참"이 포함됩니다.

인증서 인증을 사용하여 **IPsec** 정책 생성을 준비합니다

인증을 위해 사전 공유 키(PSK)만 사용하고 인증서 인증을 사용하지 않는 경우 이 단계를 건너뛸 수 있습니다.

인증을 위해 인증서를 사용하는 IPsec 정책을 만들기 전에 다음 필수 구성 요소가 충족되었는지 확인해야 합니다.

- ONTAP와 클라이언트 모두 최종 엔터티(ONTAP 또는 클라이언트) 인증서를 양쪽 모두에서 확인할 수 있도록 타사의 CA 인증서가 설치되어 있어야 합니다
- 정책에 참여하는 ONTAP LIF에 대해 인증서가 설치됩니다

> ONTAP LIF는 인증서를 공유할 수 있습니다. 인증서와 LIF 간 일대일 매핑은 필요하지 않습니다.

단계

1. 상호 인증 중에 사용되는 모든 CA 인증서(ONTAP 측 CA와 클라이언트측 CA 모두 포함)를 ONTAP 인증서 관리에 설치합니다(ONTAP 자체 서명 루트 CA의 경우처럼).

- 샘플 명령 *
  `cluster::> security certificate install -vserver svm_name -type server-ca -cert-name my_ca_cert`

2. 설치된 CA가 인증 중에 IPsec CA 검색 경로 내에 있는지 확인하려면 를 사용하여 ONTAP 인증서 관리 CA를 IPsec 모듈에 추가합니다 `security ipsec ca-certificate add` 명령.
   - 샘플 명령 *
     `cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs my_ca_cert`
3. ONTAP LIF에서 사용할 인증서를 생성하고 설치합니다. 이 인증서의 발급자 CA가 이미 ONTAP에 설치되어 있고 IPsec에 추가되어야 합니다.
   - 샘플 명령 *
     `cluster::> security certificate install -vserver svm_name -type server -cert -name my_nfs_server_cert`

ONTAP의 인증서에 대한 자세한 내용은 ONTAP 9 설명서의 보안 인증서 명령을 참조하십시오.

보안 정책 데이터베이스**(SPD)** 정의

IPsec은 네트워크에서 트래픽이 흐르도록 허용하기 전에 SPD 항목을 필요로 합니다. PSK 또는 인증서를 인증에 사용하는지에 관계없이 적용됩니다.

단계

1. '보안 IPsec 정책 만들기' 명령을 사용하여 다음을 수행합니다.
   a. IPsec 전송에 참여할 IP 주소의 ONTAP IP 주소 또는 서브넷을 선택합니다.
   b. ONTAP IP 주소에 연결할 클라이언트 IP 주소를 선택합니다.

      클라이언트는 미리 공유된 키(PSK)가 있는 인터넷 키 교환 버전 2(IKEv2)를 지원해야 합니다.

   c. 선택적으로 상위 계층 프로토콜(UDP, TCP, ICMP 등), 로컬 포트 번호, 원격 포트 번호 등 트래픽을 보호하기 위한 세부적인 트래픽 매개변수를 선택할 수 있습니다. 해당 매개변수는 다음과 같습니다. `protocols` , `local-ports` 그리고 `remote-ports` 각기.

      ONTAP IP 주소와 클라이언트 IP 주소 사이의 모든 트래픽을 보호하려면 이 단계를 건너뜁니다. 모든 트래픽을 보호하는 것이 기본값입니다.

   d. 에 대한 PSK 또는 PKI(공개 키 인프라)를 입력합니다 `auth-method` 원하는 인증 방법에 대한 매개변수입니다.
      i. PSK를 입력한 경우 매개변수를 포함시킨 다음 <enter> 키를 눌러 미리 공유된 키를 입력하고 확인합니다.

         `local-identity`` 및 ``remote-identity` 매개 변수는 호스트와 클라이언트 모두 strongSwan을 사용하고 호스트 또는 클라이언트에 대해 와일드카드 정책을 선택하지 않은 경우 선택 사항입니다.

      ii. PKI를 입력하는 경우 도 입력해야 합니다 `cert-name`, `local-identity`, `remote-identity` 매개변수. 원격 측 인증서 ID를 알 수 없거나 여러 클라이언트 ID가 필요한 경우 특수 ID를 입력합니다 `ANYTHING`.

e. ONTAP 9.17.1부터 선택적으로 포스트퀀텀 사전 공유 키(PPK) ID를 입력합니다. `ppk-identity` 매개변수. PPK는 향후 발생할 수 있는 양자 컴퓨터 공격에 대비하여 추가적인 보안 계층을 제공합니다. PPK ID를 입력하면 PPK 비밀번호를 입력하라는 메시지가 표시됩니다. PPK는 PSK 인증에만 지원됩니다.

자세히 알아보세요 `security ipsec policy create` 에서 "ONTAP 명령 참조입니다" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAP와 클라이언트 모두 일치하는 IPsec 정책을 설정하고 인증 자격 증명(PSK 또는 인증서)이 양쪽 모두에 적용될 때까지 IP 트래픽은 클라이언트와 서버 간에 이동할 수 없습니다.

IPsec ID를 사용합니다

사전 공유 키 인증 방법의 경우 호스트와 클라이언트 모두 strongSwan을 사용하고 호스트 또는 클라이언트에 대해 와일드카드 정책을 선택하지 않은 경우 로컬 및 원격 ID는 선택 사항입니다.

PKI/인증서 인증 방법의 경우 로컬 및 원격 ID가 모두 필수입니다. ID는 각 측의 인증서 내에서 인증되고 확인 프로세스에 사용되는 ID를 지정합니다. 원격 ID를 알 수 없거나 다른 ID가 많을 수 있는 경우 특수 ID를 사용하십시오 `ANYTHING`.

이 작업에 대해

ONTAP 내에서 SPD 항목을 수정하거나 SPD 정책을 생성하는 동안 ID를 지정합니다. SPD는 IP 주소 또는 문자열 형식 ID 이름일 수 있습니다.

단계

1. 다음 명령을 사용하여 기존 SPD ID 설정을 수정합니다.

보안 IPsec 정책 수정

샘플 명령

'보안 IPsec 정책 수정 - vserver_vs1_-name_test34_-local-identity_192.168.134.34_-remote-identity *client.fooboo.com*`

IPsec 다중 클라이언트 구성

적은 수의 클라이언트가 IPsec을 활용해야 하는 경우 각 클라이언트에 대해 단일 SPD 항목을 사용하는 것이 충분합니다. 하지만 수백 또는 수천 개의 클라이언트가 IPsec을 활용해야 하는 경우 NetApp은 IPsec 다중 클라이언트 구성을 사용할 것을 권장합니다.

이 작업에 대해

ONTAP는 IPsec을 사용하여 여러 네트워크의 여러 클라이언트를 단일 SVM IP 주소에 연결할 수 있도록 지원합니다. 다음 방법 중 하나를 사용하여 이 작업을 수행할 수 있습니다.

- * 서브넷 구성 *

  특정 서브넷(예: 192.168.134.0/24)의 모든 클라이언트가 단일 SPD 정책 항목을 사용하여 단일 SVM IP 주소에 연결되도록 하려면 을 지정해야 합니다 `remote-ip-subnets` 서브넷 형식으로 표시됩니다. 또한 를 지정해야 합니다 `remote-identity` 올바른 클라이언트 측 ID를 가진 필드입니다.

  > 서브넷 구성에서 단일 정책 항목을 사용하는 경우 해당 서브넷의 IPsec 클라이언트는 IPsec ID 및 미리 공유된 키(PSK)를 공유합니다. 그러나 인증서 인증에서는 그렇지 않습니다. 인증서를 사용할 때 각 클라이언트는 고유한 인증서 또는 공유 인증서를 사용하여 인증할 수 있습니다. ONTAP IPsec은 로컬 트러스트 저장소에 설치된 CA를 기반으로 인증서의 유효성을 검사합니다. ONTAP는 CRL(인증서 해지 목록) 검사도 지원합니다.

- * 모든 클라이언트 구성 허용 *

  소스 IP 주소와 관계없이 모든 클라이언트가 SVM IPsec 지원 IP 주소에 연결되도록 하려면 을 사용합니다 `0.0.0.0/0` 를 지정할 때 와일드카드입니다 `remote-ip-subnets` 필드에 입력합니다.

  또한 를 지정해야 합니다 `remote-identity` 올바른 클라이언트 측 ID를 가진 필드입니다. 인증서 인증의 경우 를 입력할 수 있습니다 `ANYTHING`.

  또한, 가 있는 경우 `0.0.0.0/0` 와일드카드를 사용하는 경우 사용할 특정 로컬 또는 원격 포트 번호를 구성해야 합니다. 예를 들면, 다음과 같습니다. `NFS port 2049`.

  단계

  a. 다음 명령 중 하나를 사용하여 여러 클라이언트에 대해 IPsec을 구성합니다.

     i. 여러 IPsec 클라이언트를 지원하기 위해 * 서브넷 구성 * 을 사용하는 경우:

        '보안 IPsec 정책 생성 - vserver_vserver_name_-name_policy_name_-local-ip-subnets_ipsec_ip_address /32_-remote-ip_subnets_ip_address/subnet_-local-identity_local_id_-remote-identity_remote_id_'

     샘플 명령

     '보안 IPsec 정책 생성 - vserver_vs1_-name_subnet134_-local-ip-subnet134_-local_192.168.134.34 /32_-remote-ip-subnets_192.168.134.0 /24_-local-identity_ontaity_-remote-identity_client_side_identity_'

     i. 을(를) 사용하여 여러 IPsec 클라이언트를 지원하도록 모든 클라이언트 구성 * 허용 을 사용하는 경우:

        '보안 IPsec 정책 생성 - vserver_vserver_name_-name_policy_name_-local-ip-subnets_ipsec_ip_address /32_-remote-ip-subnets_0.0.0.0/0_-local-ports_port_number_-local-identity_local_id_-remote_identity_remote_id_'입니다

  샘플 명령

  '보안 IPsec 정책 생성 - vserver_vs1_-name_test35_-local-ip-subnets_ipsec_ip_address/32_-remote-ip-subnets_0.0.0.0/0_-local-ports_2049_-local-identity_side_identity_-remote-identity_client_side_identity_'입니다

협상을 통해 ONTAP SVM IP 주소와 클라이언트 IP 주소 간에 IKE SA(Security Association)라는 보안 채널을 설정할 수 있습니다. IPsec SAS는 실제 데이터 암호화 및 암호 해독 작업을 수행할 수 있도록 두 엔드포인트 모두에 설치됩니다. 통계 명령을 사용하여 IPsec SAS 및 IKE SAS의 상태를 확인할 수 있습니다.

> IPsec 하드웨어 오프로드 기능을 사용하는 경우 명령과 함께 여러 개의 새 카운터가 표시됩니다 `security ipsec config show-ipsecsa`.

샘플 명령

IKE SA 샘플 명령:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA 샘플 명령 및 출력:

SECURN IPSEC show -ipsecsa -node_hosting_node_name_for_svm_ip _'

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA 샘플 명령 및 출력:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

관련 정보

- "보안 인증서 설치"
- "보안 ipsec"

ONTAP 백엔드 클러스터 네트워크 암호화 구성

ONTAP 9.18.1부터 백엔드 클러스터 네트워크에서 전송 중인 데이터에 대한 TLS(전송 계층 보안) 암호화를 구성할 수 있습니다. 이 암호화는 백엔드 클러스터 네트워크의 ONTAP 노드 간에 전송될 때 ONTAP 에 저장된 고객 데이터를 보호합니다.

이 작업에 대해

- 백엔드 클러스터 네트워크 암호화는 기본적으로 비활성화되어 있습니다.
- 백엔드 클러스터 네트워크 암호화가 활성화되면 ONTAP 에 저장된 모든 고객 데이터는 백엔드 클러스터 네트워크의 ONTAP 노드 간에 전송될 때 암호화됩니다. 제어 경로 데이터와 같은 일부 클러스터 네트워크 트래픽은 암호화되지 않습니다.
- 기본적으로 백엔드 클러스터 네트워크 암호화는 클러스터의 각 노드에 대해 자동 생성된 인증서를 사용합니다. 당신은 할 수 있습니다클러스터 네트워크 암호화 인증서 관리 각 노드에서 사용자 정의 설치 인증서를 사용합니다.

시작하기 전에

- 당신은 ONTAP 관리자여야 합니다. `admin` 다음 작업을 수행하기 위한 권한 수준입니다.
- 백엔드 클러스터 네트워크 암호화를 활성화하려면 클러스터의 모든 노드에서 ONTAP 9.18.1 이상을 실행해야 합니다.

클러스터 네트워크 통신에 대한 암호화를 활성화하거나 비활성화합니다.

단계

1. 현재 클러스터 네트워크 암호화 상태를 확인하세요.

   ```
   security cluster-network show
   ```

   이 명령은 클러스터 네트워크 암호화의 현재 상태를 보여줍니다.

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. TLS 백엔드 클러스터 네트워크 암호화를 활성화하거나 비활성화합니다.

   ```
   security cluster-network modify -enabled <true|false>
   ```

   이 명령은 백엔드 클러스터 네트워크에서 전송 중인 고객 데이터에 대한 암호화된 통신을 활성화하거나 비활성화합니다.

클러스터 네트워크 암호화 인증서 관리

1. 현재 클러스터 네트워크 암호화 인증서 정보를 확인하세요.

```
security cluster-network certificate show
```

이 명령은 현재 클러스터 네트워크 암호화 인증서 정보를 보여줍니다.

```
security cluster-network certificate show
Node                    Certificate Name                      CA
--------------------- ------------------------------------
--------------
node1                   -                                     Cluster-
1_Root_CA
node2                   -                                     Cluster-
1_Root_CA
node3                   google_issued_cert1                   Google_CA1
node4                   google_issued_cert2                   Google_CA1
```

클러스터의 각 노드에 대한 인증서 및 인증 기관(CA) 이름이 표시됩니다.

2. 노드의 클러스터 네트워크 암호화 인증서를 수정합니다.

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

이 명령은 특정 노드에 대한 클러스터 네트워크 암호화 인증서를 수정합니다. 이 명령을 실행하기 전에 인증서를 설치하고 설치된 CA에서 서명해야 합니다. 인증서 관리에 대한 자세한 내용은 다음을 참조하세요."System Manager를 사용하여 ONTAP 인증서를 관리합니다" . 만약에 `-name` 지정하지 않으면 자동 생성된 기본 인증서가 사용됩니다.

ONTAP 네트워크에서 LIF에 대한 방화벽 정책을 구성합니다

방화벽을 설정하면 클러스터의 보안이 강화되고 스토리지 시스템에 대한 무단 액세스가 방지됩니다. 기본적으로 온보드 방화벽은 데이터, 관리 및 인터클러스터 LIF에 대한 특정 IP 서비스 세트에 대한 원격 액세스를 허용하도록 구성됩니다.

ONTAP 9.10.1 시작:

- 방화벽 정책은 더 이상 사용되지 않으며 LIF 서비스 정책으로 교체됩니다. 이전에는 방화벽 정책을 사용하여 온보드 방화벽을 관리했습니다. 이 기능은 이제 LIF 서비스 정책을 사용하여 구현됩니다.
- 모든 방화벽 정책이 비어 있으며 기본 방화벽에서 포트를 열지 않습니다. 대신 LIF 서비스 정책을 사용하여 모든 포트를 열어야 합니다.
- 방화벽 정책에서 LIF 서비스 정책으로 전환하기 위해 9.10.1 이상으로 업그레이드한 후에는 작업이 필요하지

않습니다. 이전 ONTAP 릴리즈에서 사용 중인 방화벽 정책과 일치하는 LIF 서비스 정책이 자동으로 구성됩니다. 사용자 지정 방화벽 정책을 만들고 관리하는 스크립트나 기타 도구를 사용하는 경우 대신 해당 스크립트를 업그레이드하여 사용자 지정 서비스 정책을 만들어야 할 수 있습니다.

자세한 내용은 을 참조하십시오 "ONTAP 9.6 이상의 LIF 및 서비스 정책".

방화벽 정책을 사용하여 SSH, HTTP, HTTPS, Telnet, NTP 등의 관리 서비스 프로토콜에 대한 액세스를 제어할 수 있습니다. NDMP, NDMPS, RSH, DNS 또는 SNMP NFS 또는 SMB와 같은 데이터 프로토콜에 대해 방화벽 정책을 설정할 수 없습니다.

다음과 같은 방법으로 방화벽 서비스 및 정책을 관리할 수 있습니다.

- 방화벽 서비스 활성화 또는 비활성화
- 현재 방화벽 서비스 구성을 표시합니다
- 지정된 정책 이름 및 네트워크 서비스를 사용하여 새 방화벽 정책 생성
- 방화벽 정책을 논리 인터페이스에 적용합니다
- 기존 정책의 정확한 사본인 새 방화벽 정책을 생성합니다

  이를 사용하여 동일한 SVM 내에서 유사한 특성을 갖는 정책을 생성하거나 정책을 다른 SVM으로 복사할 수 있습니다.

- 방화벽 정책에 대한 정보 표시
- 방화벽 정책에서 사용하는 IP 주소 및 넷마스크 수정
- LIF에서 사용되지 않는 방화벽 정책을 삭제합니다

방화벽 정책 및 **LIF**

LIF 방화벽 정책을 사용하여 각 LIF에서 클러스터에 대한 액세스를 제한합니다. 기본 방화벽 정책이 각 LIF 유형에 대한 시스템 액세스에 미치는 영향과 LIF에 대한 보안을 늘리거나 줄일 수 있도록 방화벽 정책을 사용자 지정하는 방법을 이해해야 합니다.

또는 `network interface modify` 명령을 사용하여 LIF를 구성할 때 `network interface create` 매개변수에 지정된 `-firewall-policy` 값에 따라 LIF에 대한 액세스가 허용된 서비스 프로토콜과 IP 주소가 결정됩니다. 에 대한 자세한 내용은 `network interface` "ONTAP 명령 참조입니다"을 참조하십시오.

대부분의 경우 기본 방화벽 정책 값을 적용할 수 있습니다. 다른 경우에는 특정 IP 주소 및 특정 관리 서비스 프로토콜에 대한 액세스를 제한해야 할 수도 있습니다. 사용 가능한 관리 서비스 프로토콜에는 SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS 및 SNMP를 지원합니다.

모든 클러스터 LIF의 방화벽 정책은 기본적으로 ""로 설정되며 수정할 수 없습니다.

다음 표에서는 LIF를 생성할 때 역할(ONTAP 9.5 이하) 또는 서비스 정책(ONTAP 9.6 이상)에 따라 각 LIF에 할당되는 기본 방화벽 정책을 설명합니다.

방화벽 정책	기본 서비스 프로토콜	기본 액세스	LIF가 에 적용되었습니다
관리	DNS, http, https, NDMP, ndmps, NTP, SNMP, ssh	모든 주소(0.0.0.0/0)	클러스터 관리, SVM 관리, 노드 관리 LIF

관리 - NFS	DNS, http, https, NDMP, ndmps, NTP, 포트 맵, SNMP, ssh	모든 주소(0.0.0.0/0)	데이터 LIF: SVM 관리 액세스도 지원합니다
인터클러스터	HTTPS, NDMP, ndmps	모든 주소(0.0.0.0/0)	모든 인터클러스터 LIF
데이터	DNS, NDMP, ndmps, portmap	모든 주소(0.0.0.0/0)	모든 데이터 LIF

portmap 서비스 구성

portmap 서비스는 RPC 서비스를 수신 대기 포트에 매핑합니다.

포트맵 서비스는 ONTAP 9.3 이전 버전에서 항상 액세스할 수 있었고 ONTAP 9.4에서 ONTAP 9.6까지 구성할 수 있었고 ONTAP 9.7부터 자동으로 관리됩니다.

- ONTAP 9.3 및 이전 버전에서는 타사 방화벽이 아닌 내장 ONTAP 방화벽에 의존하는 네트워크 구성의 포트 111에서 포트맵 서비스(rpcbind)에 항상 액세스할 수 있었습니다.
- ONTAP 9.4에서 ONTAP 9.6까지 방화벽 정책을 수정하여 특정 LIF에서 포트맵 서비스에 액세스할 수 있는지 여부를 제어할 수 있습니다.
- ONTAP 9.7부터 포트 맵 방화벽 서비스가 제거됩니다. 대신, NFS 서비스를 지원하는 모든 LIF에 대해 포트맵 포트가 자동으로 열립니다.
- Portmap 서비스는 ONTAP 9.4 ~ ONTAP 9.6 * 의 방화벽에서 구성할 수 있습니다

이 항목의 나머지 부분에서는 ONTAP 9.4에서 ONTAP 9.6 릴리스까지 포트맵 방화벽 서비스를 구성하는 방법을 설명합니다.

구성에 따라 특정 LIF 유형, 일반적으로 관리 및 인터클러스터 LIF에 대한 서비스에 대한 액세스를 허용하지 않을 수 있습니다. 경우에 따라 데이터 LIF에 대한 액세스를 허용하지 않을 수도 있습니다.

어떤 행동을 기대할 수 있습니까

ONTAP 9.4 ~ ONTAP 9.6 동작은 업그레이드 시 원활한 전환을 제공하도록 설계되었습니다. 특정 유형의 LIF에서 portmap 서비스에 이미 액세스하고 있는 경우 이러한 유형의 LIF에서 계속 액세스할 수 있습니다. ONTAP 9.3 이하 버전에서와 마찬가지로 LIF 유형에 대한 방화벽 정책에서 방화벽 내에서 액세스할 수 있는 서비스를 지정할 수 있습니다.

이 동작이 적용되려면 클러스터의 모든 노드에서 ONTAP 9.4~ONTAP 9.6을 실행해야 합니다. 인바운드 트래픽만 영향을 받습니다.

새로운 규칙은 다음과 같습니다.

- 릴리스 9.4 ~ 9.6으로 업그레이드할 때 ONTAP는 포트맵 서비스를 기존의 모든 방화벽 정책(기본값 또는 사용자 정의)에 추가합니다.
- 새 클러스터 또는 새 IPspace를 생성하는 경우 ONTAP는 기본 관리 또는 인터클러스터 정책이 아니라 기본 데이터 정책에만 포트맵 서비스를 추가합니다.
- 필요에 따라 포트맵 서비스를 기본 또는 사용자 지정 정책에 추가하고 필요에 따라 서비스를 제거할 수 있습니다.

포트맵 서비스를 추가하거나 제거하는 방법

포트맵 서비스를 SVM 또는 클러스터 방화벽 정책에 추가하려면(방화벽 내에서 액세스 가능) 다음을 입력합니다.

'시스템 서비스 방화벽 정책 생성 - vserver SVM-policy mgmt | 인터클러스터 | data | custom-service portmap'

SVM 또는 클러스터 방화벽 정책에서 portmap 서비스를 제거하려면(방화벽 내에서 액세스할 수 없도록 설정) 다음을 입력합니다.

'시스템 서비스 방화벽 정책 삭제 - vserver SVM-policy mgmt | 인터클러스터 | data | custom-service portmap

네트워크 인터페이스 수정 명령을 사용하여 기존 LIF에 방화벽 정책을 적용할 수 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

방화벽 정책을 생성하여 **LIF**에 할당합니다

LIF를 생성할 때 각 LIF에 기본 방화벽 정책이 할당됩니다. 대부분의 경우 기본 방화벽 설정이 잘 작동하고 변경할 필요가 없습니다. LIF에 액세스할 수 있는 네트워크 서비스 또는 IP 주소를 변경하려면 사용자 지정 방화벽 정책을 생성하여 LIF에 할당할 수 있습니다.

이 작업에 대해

- 정책 이름 data, 클러스터 클러스터 클러스터 또는 mGMT로 방화벽 정책을 만들 수 없습니다.

  이러한 값은 시스템 정의 방화벽 정책용으로 예약되어 있습니다.

- 클러스터 LIF에 대한 방화벽 정책을 설정하거나 수정할 수 없습니다.

  클러스터 LIF의 방화벽 정책은 모든 서비스 유형에 대해 0.0.0.0/0 으로 설정됩니다.

- 정책에서 서비스를 제거해야 하는 경우 기존 방화벽 정책을 삭제하고 새 정책을 생성해야 합니다.
- 클러스터에 IPv6이 설정되어 있으면 IPv6 주소를 사용하여 방화벽 정책을 생성할 수 있습니다.

  IPv6을 사용하도록 설정한 후, "데이터", "인터클러스터" 및 "GMT" 방화벽 정책에는 IPv6 와일드카드인 /0이 허용된 주소 목록에 포함됩니다.

- System Manager를 사용하여 클러스터 간에 데이터 보호 기능을 구성하는 경우 LIF IP 주소가 허용 목록에 포함되어 있고 인터클러스터 LIF와 회사 소유 방화벽 모두에 HTTPS 서비스가 허용되는지 확인해야 합니다.

  기본적으로 '인터클러스터' 방화벽 정책은 모든 IP 주소(IPv6의 경우 0.0.0.0/0 또는:/0)의 액세스를 허용하고 HTTPS, NDMP 및 NDMPS 서비스를 활성화합니다. 이 기본 정책을 수정하거나 인터클러스터 LIF에 대한 자체 방화벽 정책을 만드는 경우 각 인터클러스터 LIF IP 주소를 허용된 목록에 추가하고 HTTPS 서비스를 활성화해야 합니다.

- ONTAP 9.6부터는 HTTPS 및 SSH 방화벽 서비스가 지원되지 않습니다.

  ONTAP 9.6에서는 HTTPS 및 SSH 관리 액세스를 위해 관리 https와 관리 ssh LIF 서비스를 사용할 수 있습니다.

단계

1. 특정 SVM의 LIF에서 사용할 수 있는 방화벽 정책을 생성합니다.

   '시스템 서비스 방화벽 정책 생성 - vserver_vserver_name_-policy_policy_name_-service_network_service_-allow-list_ip_address/mask_'

이 명령을 여러 번 사용하여 방화벽 정책에서 각 서비스에 대해 둘 이상의 네트워크 서비스 및 허용된 IP 주소 목록을 추가할 수 있습니다.

2. System services firewall policy show 명령을 사용하여 정책이 올바르게 추가되었는지 확인합니다.
3. 방화벽 정책을 LIF에 적용합니다.

   'network interface modify -vserver_vserver_name_-lif_lif_name_-firewall-policy_policy_name_'

4. 'network interface show-fields firewall -policy' 명령을 사용하여 LIF에 정책이 올바르게 추가되었는지 확인합니다.

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

방화벽 정책을 생성하여 **LIF**에 할당하는 예입니다

다음 명령을 실행하면 10.10 서브넷의 IP 주소에서 HTTP 및 HTTPS 프로토콜 액세스를 지원하는 data_http라는 방화벽 정책이 생성되어 SVM VS1의 data1이라는 LIF에 해당 정책이 적용되고 클러스터의 모든 방화벽 정책이 표시됩니다.

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

방화벽 서비스 및 정책을 관리하는 **ONTAP** 명령

'system services firewall' 명령어를 이용하여 방화벽 서비스를 관리하고, 'system services firewall policy' 명령을 이용하여 방화벽 정책을 관리하고, 'network interface modify' 명령을 사용하여 LIF의 방화벽 설정을 관리할 수 있다.

ONTAP 9.10.1 시작:

- 방화벽 정책은 더 이상 사용되지 않으며 LIF 서비스 정책으로 교체됩니다. 이전에는 방화벽 정책을 사용하여 온보드 방화벽을 관리했습니다. 이 기능은 이제 LIF 서비스 정책을 사용하여 구현됩니다.
- 모든 방화벽 정책이 비어 있으며 기본 방화벽에서 포트를 열지 않습니다. 대신 LIF 서비스 정책을 사용하여 모든 포트를 열어야 합니다.
- 방화벽 정책에서 LIF 서비스 정책으로 전환하기 위해 9.10.1 이상으로 업그레이드한 후에는 작업이 필요하지 않습니다. 이전 ONTAP 릴리즈에서 사용 중인 방화벽 정책과 일치하는 LIF 서비스 정책이 자동으로 구성됩니다. 사용자 지정 방화벽 정책을 만들고 관리하는 스크립트나 기타 도구를 사용하는 경우 대신 해당 스크립트를 업그레이드하여 사용자 지정 서비스 정책을 만들어야 할 수 있습니다.

자세한 내용은 을 참조하십시오 "ONTAP 9.6 이상의 LIF 및 서비스 정책".

원하는 작업	이 명령 사용...
방화벽 서비스를 활성화 또는 비활성화합니다	시스템 서비스 방화벽 수정
방화벽 서비스의 현재 구성을 표시합니다	'시스템 서비스 방화벽 쇼'
방화벽 정책을 생성하거나 기존 방화벽 정책에 서비스를 추가합니다	'시스템 서비스 방화벽 정책 생성
LIF에 방화벽 정책을 적용합니다	네트워크 인터페이스 수정-lif lifname-firewall-policy
방화벽 정책과 연결된 IP 주소 및 넷마스크를 수정합니다	시스템 서비스 방화벽 정책 수정
방화벽 정책에 대한 정보를 표시합니다	'시스템 서비스 방화벽 정책 표시
기존 정책의 정확한 사본인 새 방화벽 정책을 생성합니다	'시스템 서비스 방화벽 정책 클론
LIF에서 사용되지 않는 방화벽 정책을 삭제합니다	'시스템 서비스 방화벽 정책 삭제

관련 정보

- "시스템 서비스 방화벽"
- "네트워크 인터페이스 수정"

QoS 표시(클러스터 관리자만 해당)

ONTAP 네트워크 QoS(Quality of Service)에 대해 알아보기

네트워크 서비스 품질(QoS) 표시를 사용하면 네트워크 상태에 따라 서로 다른 트래픽 유형의 우선 순위를 지정하여 네트워크 리소스를 효과적으로 사용할 수 있습니다. IPspace별로 지원되는 트래픽 유형에 대해 나가는 IP 패킷의 DSCP(Differentiated Services Code Point) 값을 설정할 수 있다.

UC 규정 준수를 위한 DSCP 표시

기본 또는 사용자가 제공한 DSCP 코드를 사용하여 지정된 프로토콜에 대해 발신(송신) IP 패킷 트래픽에 DSCP(Differentiated Services Code Point) 표시를 활성화할 수 있습니다. DSCP 마킹은 네트워크 트래픽을 분류 및 관리하는 메커니즘으로 통합 기능(UC) 규정 준수의 구성 요소입니다.

IPspace, Protocol, DSCP 값을 제공하여 DSCP marking(*Qos marking_or_quality of service marking* 이라고도 함)을 설정할 수 있다. DSCP 마킹을 적용할 수 있는 프로토콜은 NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet 및 SNMP를 지원합니다.

해당 프로토콜에 대해 DSCP marking을 설정할 때 DSCP 값을 제공하지 않으면 default를 사용한다.

- 데이터 프로토콜/트래픽의 기본값은 0x0A(10)입니다.
- 제어 프로토콜/트래픽의 기본값은 0x30(48)입니다.

ONTAP 네트워크 QoS 표시 값을 수정합니다

IPspace별로 다양한 프로토콜에 대한 QoS(서비스 품질) 표시 값을 수정할 수 있습니다.

시작하기 전에

클러스터의 모든 노드에서 동일한 버전의 ONTAP를 실행해야 합니다.

단계

network QoS-marking modify 명령을 사용하여 QoS marking 값을 수정한다.

- '–IPSpace' 매개변수는 QoS 마킹 항목을 수정할 IPspace를 지정합니다.
- `–protocol`매개 변수는 QoS 표시 항목을 수정할 프로토콜을 지정합니다.
- '–DSCP' 파라미터는 DSCP(Differentiated Services Code Point) 값을 지정한다. 가능한 값의 범위는 0 ~ 63입니다.
- '-is-enabled' 매개 변수는 '–IPSpace' 매개 변수에서 제공하는 IPspace에서 지정된 프로토콜에 대한 QoS 마킹을 활성화 또는 비활성화하는 데 사용됩니다.

다음 명령을 실행하면 기본 IPspace에서 NFS 프로토콜에 대한 QoS 마킹이 설정됩니다.

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

다음 명령을 실행하면 기본 IPspace에서 NFS 프로토콜에 대한 DSCP 값이 20으로 설정됩니다.

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

에서 프로토콜의 가능한 값과 에 대해 자세히 `network qos-marking modify`"ONTAP 명령 참조입니다" 알아보십시오.

ONTAP 네트워크 QoS 표시 값을 확인합니다

IPspace별로 다양한 프로토콜에 대한 QoS 표시 값을 표시할 수 있습니다.

단계

'network QoS-marking show' 명령어를 이용하여 QoS marking 값을 출력한다.

다음 명령을 실행하면 기본 IPspace의 모든 프로토콜에 대한 QoS 마킹이 표시됩니다.

```
network qos-marking show -ipspace Default
IPspace              Protocol            DSCP  Enabled?
------------------- ----------------- -----  --------
Default
                     CIFS                  10  false
                     FTP                   48  false
                     HTTP-admin            48  false
                     HTTP-filesrv          10  false
                     NDMP                  10  false
                     NFS                   10  true
                     SNMP                  48  false
                     SSH                   48  false
                     SnapMirror            10  false
                     Telnet                48  false
                     iSCSI                 10  false
11 entries were displayed.
```

에 대한 자세한 내용은 `network qos-marking show` "ONTAP 명령 참조입니다"을 참조하십시오.

SNMP 관리(클러스터 관리자만 해당)

ONTAP 네트워크의 SNMP에 대해 알아봅니다

문제가 발생하기 전에 이를 방지하고 문제가 발생할 경우 대응하도록 SNMP를 클러스터의 SVM을 모니터링할 수 있습니다. SNMP를 관리하려면 SNMP 사용자를 구성하고 모든 SNMP 이벤트에 대해 SNMP 트라프호스트 대상(관리 워크스테이션)을 구성해야 합니다. 데이터 LIF에서 SNMP는 기본적으로 해제되어 있습니다.

데이터 SVM에서 읽기 전용 SNMP 사용자를 생성하고 관리할 수 있습니다. SVM에서 SNMP 요청을 받도록 데이터 LIF를 구성해야 합니다.

SNMP 네트워크 관리 워크스테이션 또는 관리자는 SVM SNMP 에이전트에 정보를 쿼리할 수 있습니다. SNMP 에이전트는 정보를 수집하여 SNMP 관리자에게 전달합니다. SNMP 에이전트는 또한 특정 이벤트가 발생할 때마다 트랩 알림을 생성합니다. SVM의 SNMP 에이전트는 읽기 전용 권한을 가지고 있으며 설정된 작업에 사용하거나 트랩에 대한 응답으로 수정 조치를 취하는 데 사용할 수 없습니다. ONTAP는 SNMP 버전 v1, v2c 및 v3과 호환되는 SNMP 에이전트를 제공합니다. SNMPv3는 암호 구문 및 암호화를 사용하여 고급 보안을 제공합니다.

ONTAP 시스템의 SNMP 지원에 대한 자세한 내용은 를 참조하십시오 "TR-4220: Data ONTAP에서 SNMP 지원".

MIB 개요

MIB(Management Information Base)는 SNMP 객체 및 트랩을 설명하는 텍스트 파일입니다.

MIB는 스토리지 시스템의 관리 데이터 구조를 설명하며 OID(객체 식별자)가 포함된 계층적 네임스페이스를 사용합니다. 각 OID는 SNMP를 사용하여 읽을 수 있는 변수를 식별합니다.

MIB는 구성 파일이 아니며 ONTAP는 이러한 파일을 읽지 않기 때문에 MIB 기능은 MIB의 영향을 받지 않습니다. ONTAP는 다음과 같은 MIB 파일을 제공합니다.

- NetApp 맞춤형 MIB('NetApp.MIB')

ONTAP는 IPv6(RFC 2465), TCP(RFC 4022), UDP(RFC 4113) 및 IPv4 및 IPv6 데이터를 모두 표시하는 ICMP(RFC 2466) MIB를 지원합니다.

또한 ONTAP는 "trap.dat" 파일에서 OID(개체 식별자)와 개체 약식 이름 간의 짧은 상호 참조를 제공합니다.

> ONTAP MIB 및 traps.dat 파일의 최신 버전은 NetApp Support 사이트에서 확인할 수 있습니다. 그러나 지원 사이트에 있는 이러한 파일의 버전이 ONTAP 버전의 SNMP 기능과 일치하지 않을 수도 있습니다. 이러한 파일은 최신 ONTAP 버전에서 SNMP 기능을 평가하는 데 도움이 됩니다.

SNMP 트랩

SNMP 트랩은 SNMP 에이전트에서 SNMP 관리자로 보내는 비동기 알림으로 전송되는 시스템 모니터링 정보를 캡처합니다.

SNMP 트랩에는 표준, 기본 제공 및 사용자 정의 세 가지 유형이 있습니다. 사용자 정의 트랩은 ONTAP에서 지원되지 않습니다.

트랩을 사용하여 MIB에 정의된 작동 임계값 또는 오류를 정기적으로 확인할 수 있습니다. 임계값에 도달하거나 장애가 감지되면 SNMP 에이전트는 해당 이벤트를 알리는 메시지(트랩)를 Traphosts에 보냅니다.

> ONTAP는 SNMPv1 및 SNMPv3 트랩을 지원합니다. ONTAP는 SNMPv2c 트랩 및 정보를 지원하지 않습니다.

표준 **SNMP** 트랩

이러한 트랩은 RFC 1215에 정의되어 있습니다. ONTAP에서 지원하는 5개의 표준 SNMP 트랩은 coldstart, 웜스타트, Linkdown, Linkup 및 authenticationFailure입니다.

> authenticationFailure 트랩은 기본적으로 해제되어 있습니다. 명령을 사용하여 트랩을 활성화해야 `system snmp authtrap` 합니다. 에 대한 자세한 내용은 `system snmp authtrap` "ONTAP 명령 참조입니다"을 참조하십시오.

기본 제공 **SNMP** 트랩

내장 트랩은 ONTAP에서 미리 정의되며 이벤트가 발생하면 Traphost 목록의 네트워크 관리 스테이션으로 자동으로 전송됩니다. diskFailedShutdown, cpuTooBusy 및 volumeNearlyFull과 같은 이러한 트랩은 사용자 지정 MIB에 정의되어 있습니다.

각 내장 트랩은 고유한 트랩 코드로 식별됩니다.

ONTAP 네트워크용 **SNMP** 커뮤니티를 생성합니다

SNMPv1 및 SNMPv2c를 사용할 때 관리 스테이션과 SVM(스토리지 가상 머신) 간의 인증 메커니즘 역할을 하는 SNMP 커뮤니티를 생성할 수 있습니다.

데이터 SVM에서 SNMP 커뮤니티를 생성하여 데이터 LIF에서 'snmpwalk', 'snmpget' 등의 명령을 실행할 수 있습니다.

이 작업에 대해

- ONTAP를 새로 설치하면 SNMPv1 및 SNMPv2c가 기본적으로 비활성화됩니다.

  SNMP 커뮤니티를 생성한 후에는 SNMPv1 및 SNMPv2c가 활성화됩니다.

- ONTAP는 읽기 전용 커뮤니티를 지원합니다.
- 기본적으로 데이터 LIF에 할당되는 "데이터" 방화벽 정책은 SNMP 서비스를 "설정"으로 설정합니다.

  데이터 SVM용 SNMP 사용자를 생성할 때 SNMP 서비스 세트가 "허용"인 새 방화벽 정책을 생성해야 합니다.

  ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

- 관리 SVM과 데이터 SVM 모두에 대해 SNMPv1 및 SNMPv2c 사용자를 위한 SNMP 커뮤니티를 생성할 수 있습니다.
- SVM은 SNMP 표준의 일부가 아니므로 데이터 LIF에 대한 쿼리에는 'smpwalk-v 2c-c snmpNFS 10.238.19.14 1.3.6.1.4.1.789'와 같은 NetApp 루트 OID(1.3.6.1.4.1.789)가 포함되어야 합니다.

단계

1. '시스템 SNMP community add' 명령어를 사용하여 SNMP community를 생성한다. 다음 명령을 실행하면 관리 SVM 클러스터-1에서 SNMP 커뮤니티를 생성하는 방법이 표시됩니다.

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   다음 명령을 실행하면 SVM VS1 데이터에 SNMP 커뮤니티를 생성하는 방법이 표시됩니다.

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. system snmp community show 명령을 사용하여 커뮤니티가 생성되었는지 확인합니다.

다음 명령을 실행하면 SNMPv1 및 SNMPv2c에 대해 생성된 두 개의 커뮤니티가 표시됩니다.

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. System services firewall policy'show' 명령어를 이용하여 "data" 방화벽 정책에서 SNMP를 서비스로 허용할 수 있는지 확인한다.

   다음 명령을 실행하면 기본 "데이터" 방화벽 정책에서 SNMP 서비스가 허용되지 않습니다(SNMP 서비스는 "관리" 방화벽 정책에서만 허용됨).

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. '시스템 서비스 방화벽 정책 생성' 명령을 사용하여 'NMP' 서비스를 사용하여 액세스할 수 있는 새 방화벽 정책을 만듭니다.

   다음 명령을 실행하면 'data1'이라는 새 데이터 방화벽 정책이 생성되어 'snmp'를 사용할 수 있습니다

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                       snmp       0.0.0.0/0
vs1
         data1
                       snmp       0.0.0.0/0
```

5. 명령을 -firewall-policy 매개 변수와 함께 사용하여 데이터 LIF에 방화벽 정책을 `network interface modify` 적용합니다.

   다음 명령을 실행하면 새 "data1" 방화벽 정책이 LIF "datalif1"에 할당됩니다.

   ```
   network interface modify -vserver vs1 -lif datalif1 -firewall-policy
   data1
   ```

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

ONTAP 클러스터에서 SNMPv3 사용자를 구성합니다

SNMPv3는 SNMPv1 및 SNMPv2c와 비교할 때 보안 프로토콜입니다. SNMPv3을 사용하려면 SNMP 관리자에서 SNMP 유틸리티를 실행하도록 SNMPv3 사용자를 구성해야 합니다.

단계

사용하세요 `security login create` SNMPv3 사용자를 생성하는 명령입니다.

다음 정보를 제공하라는 메시지가 표시됩니다.

- 엔진 ID: 기본값과 권장 값은 로컬 엔진 ID입니다
- 인증 프로토콜
- 인증 암호입니다
- 개인 정보 보호 프로토콜
- 개인 정보 프로토콜 암호

결과

SNMPv3 사용자는 사용자 이름 및 암호를 사용하여 SNMP 관리자에서 로그인하고 SNMP 유틸리티 명령을 실행할 수 있습니다.

SNMPv3 보안 매개 변수

SNMPv3에는 사용자가 명령을 호출할 때 이름, 인증 프로토콜, 인증 키 및 원하는 보안 수준을 입력해야 하는 인증 기능이 포함되어 있습니다.

다음 표에는 SNMPv3 보안 매개 변수가 나열되어 있습니다.

매개 변수	명령줄 옵션입니다	설명
엔진 ID	-e 엔지니어링 ID	SNMP 에이전트의 엔진 ID입니다. 기본값은 Local EngineID(권장)입니다.
보안 이름	-u 이름	사용자 이름은 32자를 초과할 수 없습니다.
authProtocol의 약어입니다	-a {none	MD5
SHA	SHA-256}	인증 유형은 없음, MD5, SHA 또는 SHA-256일 수 있습니다.
인증 키	• 암호문	최소 8자의 암호 구문
보안 수준	-l {authNo암호화	Auth암호화
noAuthNo암호화}	보안 수준은 인증, 개인 정보 보호 없음, 인증, 개인 정보 보호 또는 인증 없음일 수 있습니다. 개인 정보 보호.	개인 프로토콜
-x{none	des	aes128}
개인 정보 보호 프로토콜은 없음, des 또는 aes128일 수 있습니다	privPassword(비밀 번호)	-X 암호

다양한 보안 수준에 대한 예

이 예에서는 서로 다른 보안 수준으로 생성된 SNMPv3 사용자가 'snmpwalk'와 같은 SNMP 클라이언트 측 명령을 사용하여 클러스터 객체를 쿼리하는 방법을 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

> 인증 프로토콜이 SHA 인 경우 'snmpwalk' 5.3.1 이상을 사용해야 합니다.

보안 수준**: auth**암호화

다음 출력에서는 auth암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS 모드

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

보안 수준: **authNo**암호화

다음 출력에서는 authNo암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS 모드

FIPS에서는 개인 정보 프로토콜에 대해 * 없음 * 을 선택할 수 없습니다. 따라서 FIPS 모드에서 authNoSNMPv3 사용자를 구성할 수 없습니다.

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

보안 수준: **noAuthNo**암호화

다음 출력에서는 NOAuthNo암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS 모드

FIPS에서는 개인 정보 프로토콜에 대해 * 없음 * 을 선택할 수 없습니다.

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에서 SNMP용 traphosts를 구성합니다

클러스터에서 SNMP 트랩이 생성될 때 알림(SNMP 트랩 PDU)을 받도록 Traphost(SNMP 관리자)를 구성할 수 있습니다. SNMP traphost의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정할 수 있습니다.

시작하기 전에

- 클러스터에서 SNMP 및 SNMP 트랩을 활성화해야 합니다.

> SNMP 및 SNMP 트랩은 기본적으로 사용하도록 설정됩니다.

- traphost 이름을 확인하기 위해 클러스터에서 DNS를 구성해야 합니다.
- IPv6 주소를 사용하여 SNMP traaphosts를 구성하려면 클러스터에서 IPv6을 활성화해야 합니다.
- traphost를 생성할 때 미리 정의된 USM(사용자 기반 보안 모델) 인증 및 개인 정보 보호 자격 증명을 지정해야 합니다.

단계

SNMP traaphost 추가:

```
system snmp traphost add
```

> 트랩은 하나 이상의 SNMP 관리 스테이션이 트랩 호스트로 지정된 경우에만 보낼 수 있습니다.

다음 명령을 실행하면 알려진 USM 사용자와 함께 yyy.example.com 이라는 새로운 SNMPv3 traphost가 추가됩니다.

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

다음 명령을 실행하면 호스트의 IPv6 주소를 사용하는 traphost가 추가됩니다.

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

ONTAP 클러스터에서 SNMP 폴링을 확인합니다

SNMP를 구성한 후에는 클러스터를 폴링할 수 있는지 확인해야 합니다.

이 작업에 대해

클러스터를 폴링하려면 과 같은 타사 명령을 사용해야 합니다 `snmpwalk`.

단계

1. SNMP 명령을 전송하여 다른 클러스터에서 클러스터를 폴링합니다.

   SNMPv1을 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v version -c community_stringip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

   이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

   ```
   C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

   SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
               Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
   SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
   DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
   19:47:24.48
   SNMPv1-MIB::sysContact.0 = STRING:
   SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
   SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
   SNMPv1-MIB::sysServices.0 = INTEGER: 72
   ```

   SNMPv2c를 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v version -c community_stringip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

   이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

SNMPv3를 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

SNMP, 트랩 및 traphost를 관리하는 ONTAP 명령입니다

'시스템 SNMP' 명령어를 이용하여 SNMP, 트랩, Traphosts를 관리할 수 있다. SVM별로 SNMP 사용자를 관리하기 위해 '보안' 명령을 사용할 수 있다. 이벤트 명령을 사용하여 SNMP 트랩과 관련된 이벤트를 관리할 수 있습니다.

SNMP를 구성하는 명령입니다

원하는 작업	이 명령 사용...

클러스터에서 SNMP를 설정합니다	'options-option-name snmp.enable-option-value on'입니다 관리(관리) 방화벽 정책에서 SNMP 서비스를 허용해야 합니다. 시스템 서비스 방화벽 policy show 명령을 사용하여 SNMP가 허용되는지 여부를 확인할 수 있습니다.
클러스터에서 SNMP를 해제합니다	'options-option-name snmp.enable-option-value off'

SNMP v1, v2c 및 **v3** 사용자를 관리하는 명령입니다

원하는 작업	이 명령 사용…
SNMP 사용자를 구성합니다	'보안 로그인 생성'
SNMP 사용자를 표시합니다	`security snmpusers`그리고 `security login show -application snmp`
SNMP 사용자를 삭제합니다	'보안 로그인 삭제
SNMP 사용자에 대한 로그인 방법의 액세스 제어 역할 이름을 수정합니다	보안 로그인 수정

연락처 및 위치 정보를 제공하는 명령입니다

원하는 작업	이 명령 사용…
클러스터의 연락처 정보를 표시하거나 수정합니다	'시스템 SNMP 연락처'
클러스터의 위치 세부 정보를 표시하거나 수정합니다	'시스템 SNMP 위치'

SNMP 커뮤니티 관리를 위한 명령입니다

원하는 작업	이 명령 사용…
SVM이나 클러스터의 모든 SVM에 대해 읽기 전용(ro) 커뮤니티를 추가할 수 있습니다	'시스템 SNMP 커뮤니티 추가'
커뮤니티 또는 모든 커뮤니티를 삭제합니다	시스템 SNMP community delete
모든 커뮤니티 목록을 표시합니다	'시스템 SNMP 커뮤니티 쇼'

SVM은 SNMP 표준의 일부가 아니므로 데이터 LIF에 대한 쿼리에는 'snmpwalk-v 2c-c snmpNFS 10.238.19.14 1.3.6.1.4.1.789'와 같은 NetApp 루트 OID(1.3.6.1.4.1.789)가 포함되어야 합니다.

SNMP 옵션 값을 표시하는 명령입니다

원하는 작업	이 명령 사용…
클러스터 연락처, 연락처 위치, 클러스터가 트랩을 전송하도록 구성되었는지 여부, 트랩 목록, 커뮤니티 및 액세스 제어 유형 목록을 포함한 모든 SNMP 옵션의 현재 값을 표시합니다	'시스템 SNMP 쇼'

SNMP 트랩 및 트랩 호스트를 관리하는 명령입니다

원하는 작업	이 명령 사용…
클러스터에서 보낸 SNMP 트랩을 설정합니다	'시스템 SNMP init-init 1'
클러스터에서 보낸 SNMP 트랩을 해제합니다	'시스템 SNMP init-init 0'
클러스터의 특정 이벤트에 대해 SNMP 알림을 수신하는 Traphost를 추가합니다	'시스템 SNMP traaphost add'
traphost를 삭제합니다	'시스템 SNMP traaphost delete
Traphosts 목록을 표시합니다	'시스템 SNMP traaphost show'

SNMP 트랩과 관련된 이벤트를 관리하는 명령입니다

원하는 작업	이 명령 사용…
SNMP 트랩(기본 제공)이 생성되는 이벤트를 표시합니다	이벤트 루트쇼 SNMP 관련 이벤트만 보려면 '-snmp-support true' 매개변수를 사용하십시오. 'instance-messagename<message>' 매개 변수를 사용하여 이벤트가 발생한 이유와 수정 조치에 대해 자세히 설명합니다. 개별 SNMP 트랩 이벤트를 특정 트랩 호스트 대상으로 라우팅하는 것은 지원되지 않습니다. 모든 SNMP 트랩 이벤트가 모든 트랩 호스트 대상으로 전송됩니다.
SNMP 트랩으로 전송된 이벤트 알림인 SNMP 트랩 기록 레코드 목록을 표시합니다	이벤트 스내피스토리 쇼
SNMP 트랩 기록 레코드를 삭제합니다	이벤트 스내피스토리 삭제

관련 정보

- "시스템 SNMP"
- "보안 snmpusers"
- "보안"
- "이벤트"
- "보안 로그인"

SVM에서 라우팅 관리

ONTAP 네트워크에서의 SVM 라우팅에 대해 알아보십시오

SVM을 위한 라우팅 테이블은 SVM이 대상과 통신하는 데 사용하는 네트워크 경로를 결정합니다. 라우팅 테이블이 작동하는 방식을 이해하여 네트워크 문제가 발생하기 전에 이를 방지하는 것이 중요합니다.

라우팅 규칙은 다음과 같습니다.

- ONTAP는 가장 구체적인 사용 가능한 경로를 통해 트래픽을 라우팅합니다.
- ONTAP는 더 구체적인 경로를 사용할 수 없는 경우 기본 게이트웨이 경로(넷마스크 0비트)를 통해 트래픽을 마지막 수단으로 라우팅합니다.

동일한 대상, 넷마스크 및 메트릭이 있는 라우트의 경우, 재부팅 후 또는 업그레이드 후에 시스템이 동일한 경로를 사용할 것이라는 보장은 없습니다. 이는 여러 기본 경로를 구성한 경우 특히 문제가 됩니다.

SVM에 대해서는 기본 경로를 하나만 구성하는 것이 가장 좋습니다. 중단을 방지하려면 기본 경로가 보다 구체적인 경로로는 도달할 수 없는 모든 네트워크 주소에 도달할 수 있는지 확인해야 합니다. 자세한 내용은 다음을 참조하세요 ."NetApp 기술 자료: SU134 - 클러스터형 ONTAP 에서 잘못된 라우팅 구성으로 인해 네트워크 액세스가 중단될 수 있음"

ONTAP 네트워크에 대한 정적 라우트를 생성합니다

SVM(Storage Virtual Machine) 내에서 정적 경로를 생성하여 LIF가 아웃바운드 트래픽에 네트워크를 사용하는 방법을 제어할 수 있습니다.

SVM과 관련된 경로 항목을 생성하면 해당 경로가 지정된 SVM이 소유하고 게이트웨이와 동일한 서브넷에 있는 모든 LIF에서 사용됩니다.

단계

'network route create' 명령어를 이용하여 경로를 생성한다.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

에 대한 자세한 내용은 `network route create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에 대해 다중 경로 라우팅을 활성화합니다

여러 루트가 목적지에 대해 동일한 메트릭을 가지고 있는 경우, 나가는 트래픽에 대해 하나의 라우트만 선택됩니다. 이로 인해 다른 라우트가 발신 트래픽을 전송하는 데 사용되지 않습니다. 동일한 메트릭의 사용 가능한 라우트에 걸쳐 로드 밸런싱을 수행하는 ECMP 라우팅과 달리, 다중 경로 라우팅을 활성화하여 사용 가능한 모든 라우트에 대한 로드 밸런싱을 수행할 수 있습니다.

단계

1. 고급 권한 레벨에 로그인합니다.

   세트 프리빌리지 고급

2. 다중 경로 라우팅 활성화:

   '네트워크 옵션 다중 경로 라우팅 수정 - 활성화 true'

   클러스터의 모든 노드에 대해 다중 경로 라우팅이 활성화됩니다.

   ```
   network options multipath-routing modify -is-enabled true
   ```

   에 대한 자세한 내용은 `network options multipath-routing modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에서 정적 라우트를 삭제합니다

SVM(스토리지 가상 머신)에서 불필요한 정적 경로를 삭제할 수 있습니다.

단계

정적 라우트를 삭제하려면 network route delete 명령을 사용한다.

다음 예제에서는 게이트웨이 10.63.0.1 및 대상 IP 주소가 0.0.0.0/0인 SVM vs0과 연관된 정적 경로를 삭제합니다.

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

에 대한 자세한 내용은 `network route delete` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 라우팅 정보를 봅니다

클러스터의 각 SVM에 대한 라우팅 구성 정보를 표시할 수 있습니다. 이를 통해 클라이언트 애플리케이션 또는 서비스 간 연결 문제와 클러스터의 노드 LIF 간 연결 문제를 진단할 수 있습니다.

단계

1. "network route show" 명령을 사용하여 하나 이상의 SVM 내에 경로를 표시합니다. 다음 예는 vs0 SVM에 구성된

경로를 보여줍니다.

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. "network route show -lifs" 명령을 사용하여 하나 이상의 SVM 내에 있는 경로 및 LIF의 연결을 표시합니다.

   다음 예에서는 vs0 SVM이 소유하는 라우트가 있는 LIF를 보여 줍니다.

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   및 `network route show-lifs` 에 대한 자세한 `network route show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

3. "network route active-entry show" 명령을 사용하여 하나 이상의 노드, SVM, 서브넷 또는 지정된 목적지를 가진 경로에 설치된 경로를 표시할 수 있습니다.

   다음 예는 특정 SVM에 설치된 모든 경로를 보여줍니다.

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
```

```
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

에 대한 자세한 내용은 `network route active-entry show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크의 라우팅 테이블에서 동적 라우트를 제거합니다

IPv4 및 IPv6에 대한 ICMP redirect를 수신하면, 동적 route를 라우팅 테이블에 추가한다. 기본적으로 동적 루트는 300초 후에 제거됩니다. 동적 경로를 다른 시간 동안 유지하려면 시간 초과 값을 변경할 수 있습니다.

이 작업에 대해

시간 초과 값은 0에서 65,535초로 설정할 수 있습니다. 값을 0으로 설정하면 루트가 만료되지 않습니다. 동적 경로를 제거하면 잘못된 경로의 지속성으로 인한 연결 손실을 방지할 수 있습니다.

단계

1. 현재 시간 초과 값을 표시합니다.
   - IPv4의 경우:

     ```
     network tuning icmp show
     ```

   - IPv6의 경우:

     ```
     network tuning icmp6 show
     ```

2. 시간 초과 값을 수정합니다.
   - IPv4의 경우:

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - IPv6의 경우:

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. 시간 초과 값이 올바르게 수정되었는지 확인합니다.
   - IPv4의 경우:

     ```
     network tuning icmp show
     ```

   - IPv6의 경우:

     ```
     network tuning icmp6 show
     ```

에 대한 자세한 내용은 `network tuning icmp` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크 정보

ONTAP 네트워크 정보를 봅니다

CLI를 사용하면 포트, LIF, 경로, 페일오버 규칙, 페일오버 그룹과 관련된 정보를 방화벽 규칙, DNS, NIS 및 연결 ONTAP 9.8부터 System Manager에 표시되는 네트워크 관련 데이터를

다운로드할 수도 있습니다.

이 정보는 네트워킹 설정을 재구성하거나 클러스터 문제를 해결하는 데 유용할 수 있습니다.

클러스터 관리자는 사용 가능한 모든 네트워킹 정보를 볼 수 있습니다. SVM 관리자는 할당된 SVM과 관련된 정보만 볼 수 있습니다.

System Manager에서 _ 목록 보기 _ 에 정보를 표시할 때 * 다운로드 * 를 클릭하면 표시되는 개체 목록이 다운로드됩니다.

- 목록은 CSV(쉼표로 구분된 값) 형식으로 다운로드됩니다.
- 표시된 열의 데이터만 다운로드됩니다.
- CSV 파일 이름의 형식은 개체 이름과 타임 스탬프로 지정됩니다.

ONTAP 네트워크 포트 정보를 봅니다

클러스터의 모든 노드에 있는 특정 포트 또는 모든 포트에 대한 정보를 표시할 수 있습니다.

이 작업에 대해

다음 정보가 표시됩니다.

- 노드 이름
- 포트 이름입니다
- IPspace 이름입니다
- 브로드캐스트 도메인 이름
- 링크 상태(위 또는 아래)
- MTU 설정
- 포트 속도 설정 및 작동 상태(초당 1기가비트 또는 10기가비트)
- 자동 협상 설정(참 또는 거짓)
- 이중 모드 및 작동 상태(반이중 또는 전이중)
- 해당되는 경우 포트의 인터페이스 그룹입니다
- 해당되는 경우 포트의 VLAN 태그 정보입니다
- 포트의 상태(상태 또는 성능 저하)
- 포트가 성능 저하로 표시된 이유

필드에 대한 데이터를 사용할 수 없는 경우(예: 비활성 포트에 대한 작동 이중화 및 속도를 사용할 수 없음) 필드 값이 로 표시됩니다 –.

단계

network port show 명령을 사용하여 네트워크 포트 정보를 표시합니다.

instance 매개변수를 지정하여 각 포트에 대한 상세 정보를 표시하거나 '-fields' 매개변수를 사용하여 필드 이름을 지정하여 특정 정보를 가져올 수 있습니다.

```
network port show
Node: node1

Ignore
                                                     Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                     Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

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

ONTAP VLAN 정보를 봅니다

특정 VLAN에 대한 정보 또는 클러스터의 모든 VLAN에 대한 정보를 표시할 수 있습니다.

이 작업에 대해

`-instance' 매개변수를 지정하여 각 VLAN에 대한 세부 정보를 표시할 수 있습니다. '-fields' 매개 변수를 사용하여 필드

이름을 지정하여 특정 정보를 표시할 수 있습니다.

단계

네트워크 포트 vlan show 명령을 사용하여 VLAN에 대한 정보를 표시합니다. 다음 명령을 실행하면 클러스터의 모든 VLAN에 대한 정보가 표시됩니다.

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

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

ONTAP 인터페이스 그룹 정보를 봅니다

인터페이스 그룹에 대한 정보를 표시하여 해당 구성을 확인할 수 있습니다.

이 작업에 대해

다음 정보가 표시됩니다.

- 인터페이스 그룹이 있는 노드입니다
- 인터페이스 그룹에 포함된 네트워크 포트 목록입니다
- 인터페이스 그룹의 이름입니다
- 분배 기능(MAC, IP, 포트 또는 순차)
- 인터페이스 그룹의 MAC(Media Access Control) 주소입니다
- 포트 활동 상태, 즉 모든 집계된 포트가 활성(전체 참여) 상태인지 여부, 일부 포트가 활성(부분 참여) 상태인지 여부 또는 활성 포트가 없는지 여부

단계

network port ifgrp show 명령을 사용하여 interface group에 대한 정보를 출력한다.

'-instance' 매개 변수를 지정하여 각 노드에 대한 세부 정보를 표시할 수 있습니다. '-fields' 매개 변수를 사용하여 필드 이름을 지정하여 특정 정보를 표시할 수 있습니다.

다음 명령을 실행하면 클러스터의 모든 인터페이스 그룹에 대한 정보가 표시됩니다.

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

다음 명령을 실행하면 단일 노드에 대한 상세한 인터페이스 그룹 정보가 표시됩니다.

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

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

ONTAP LIF 정보 를 참조하십시오

LIF에 대한 자세한 정보를 보고 해당 구성을 확인할 수 있습니다.

또한 이 정보를 확인하여 중복 IP 주소 확인 또는 네트워크 포트가 올바른 서브넷에 속하는지 확인하는 등의 기본 LIF 문제를 진단할 수도 있습니다. SVM(Storage Virtual Machine) 관리자는 SVM과 연결된 LIF에 대한 정보만 볼 수 있습니다.

이 작업에 대해

다음 정보가 표시됩니다.

- LIF와 연결된 IP 주소입니다
- LIF의 관리 상태입니다

- LIF의 운영 상태입니다

  데이터 LIF의 운영 상태는 데이터 LIF가 연결된 SVM의 상태에 따라 결정됩니다. SVM이 중지되면 LIF의 운영 상태가 아래로 변경됩니다. SVM이 다시 시작되면 운영 상태가 가동으로 바뀝니다

- 노드 및 LIF가 상주하는 포트입니다

필드의 데이터를 사용할 수 없는 경우(예: 확장 상태 정보가 없는 경우) 필드 값은 '-'로 표시됩니다.

단계

명령을 사용하여 LIF 정보를 `network interface show` 표시합니다.

instance 매개 변수를 지정하여 각 LIF에 대한 자세한 정보를 보거나 -fields 매개 변수를 사용하여 필드 이름을 지정하여 특정 정보를 얻을 수 있습니다.

다음 명령을 실행하면 클러스터의 모든 LIF에 대한 일반 정보가 표시됩니다.

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

다음 명령을 실행하면 단일 LIF에 대한 자세한 정보가 표시됩니다.

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
             Bits in the Netmask: 18
                  IPv4 Link Local: -
                      Subnet Name: -
           Administrative Status: up
                 Failover Policy: local-only
                 Firewall Policy: data
                     Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

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

ONTAP 네트워크에 대한 라우팅 정보를 봅니다

SVM 내에서 경로에 대한 정보를 표시할 수 있습니다.

단계

보려는 라우팅 정보의 유형에 따라 해당 명령을 입력합니다.

에 대한 정보를 보려면...	입력...
SVM당 정적 경로	네트워크 라우트 쇼

SVM당 각 경로에 LIF가 있습니다	네트워크 라우트 show-lifs

'-instance' 파라미터를 지정하여 각 라우트에 대한 세부 정보를 표시할 수 있습니다. 다음 명령을 실행하면 SVM 내의 정적 경로가 클러스터-1에 표시됩니다.

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

다음 명령을 실행하면 클러스터 1의 모든 SVM에 있는 정적 라우트 및 논리 인터페이스(LIF) 연결이 표시됩니다.

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

및 `network route show-lifs` 에 대한 자세한 `network route show` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP DNS 호스트 테이블 항목을 봅니다

DNS 호스트 테이블 항목은 호스트 이름을 IP 주소에 매핑합니다. 클러스터의 모든 SVM에 대해 매핑되는 호스트 이름 및 별칭 이름과 IP 주소를 표시할 수 있습니다.

단계

vserver services name-service dns hosts show 명령을 사용하여 모든 SVM에 대한 호스트 이름 항목을 표시합니다.

다음 예는 호스트 테이블 항목을 표시합니다.

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ----------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

SVM에서 DNS를 사용하도록 설정하려면 'vserver services name-service dns' 명령을 사용하고, 호스트 이름 확인을 위해 DNS를 사용하도록 구성할 수 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다.

ONTAP DNS 도메인 구성 정보를 봅니다

클러스터에 있는 하나 이상의 SVM(스토리지 가상 머신)의 DNS 도메인 구성을 표시하여 올바르게 구성되었는지 확인할 수 있습니다.

단계

'vserver services name-service dns show' 명령을 사용하여 DNS 도메인 구성을 봅니다.

다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

```
vserver services name-service dns show
                                                  Name
Vserver         State     Domains                 Servers
--------------- --------- ------------------------- -------------
cluster-1        enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs1             enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs2             enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs3             enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
```

다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

ONTAP 페일오버 그룹 정보를 봅니다

각 페일오버 그룹의 노드 및 포트 목록, 페일오버 설정 또는 해제, 각 LIF에 적용되는 페일오버 정책 유형 등 페일오버 그룹에 대한 정보를 볼 수 있습니다.

단계

1. network interface failover-groups show 명령을 사용하여 각 페일오버 그룹의 타겟 포트를 표시합니다.

   다음 명령을 실행하면 2노드 클러스터의 모든 페일오버 그룹에 대한 정보가 표시됩니다.

   ```
   network interface failover-groups show
                                 Failover
   Vserver        Group          Targets
   -------------- -------------- ---------------------------------
   Cluster
                  Cluster
                                 cluster1-01:e0a, cluster1-01:e0b,
                                 cluster1-02:e0a, cluster1-02:e0b
   vs1
                  Default
                                 cluster1-01:e0c, cluster1-01:e0d,
                                 cluster1-01:e0e, cluster1-02:e0c,
                                 cluster1-02:e0d, cluster1-02:e0e
   ```

   에 대한 자세한 내용은 `network interface failover-groups show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. network interface failover-groups show 명령을 사용하여 특정 페일오버 그룹의 대상 포트와 브로드캐스트 도메인을 표시합니다.

   다음 명령을 실행하면 SVM VS4 용 페일오버 그룹 data12에 대한 자세한 정보가 표시됩니다.

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. network interface show 명령을 사용하여 모든 LIF에서 사용되는 페일오버 설정을 표시합니다.

   다음 명령을 실행하면 각 LIF에서 사용 중인 페일오버 정책과 페일오버 그룹이 표시됩니다.

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  -------------------  ----------------------  --------------
Cluster   cluster1-01_clus_1  local-only             Cluster
Cluster   cluster1-01_clus_2  local-only             Cluster
Cluster   cluster1-02_clus_1  local-only             Cluster
Cluster   cluster1-02_clus_2  local-only             Cluster
cluster1  cluster_mgmt        broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1   local-only             Default
cluster1  cluster1-02_mgmt1   local-only             Default
vs1       data1               disabled               Default
vs3       data2               system-defined         group2
```

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

ONTAP LIF 페일오버 대상을 봅니다

페일오버 정책과 LIF의 페일오버 그룹이 올바르게 구성되었는지 확인해야 할 수 있습니다. 페일오버 규칙의 구성 오류를 방지하기 위해 단일 LIF 또는 모든 LIF의 페일오버 목표를 표시할 수 있습니다.

이 작업에 대해

LIF 페일오버 타겟을 디스플레이하면 다음을 확인할 수 있습니다.

- LIF가 올바른 페일오버 그룹 및 페일오버 정책으로 구성되었는지 여부를 나타냅니다
- 페일오버 타겟 포트의 결과 목록이 각 LIF에 적합한지 여부
- 데이터 LIF의 페일오버 목표가 관리 포트(e0M)가 아닌지 여부

단계

network interface show 명령의 페일오버 옵션을 사용하여 LIF의 페일오버 타겟을 표시합니다.

다음 명령을 실행하면 2노드 클러스터의 모든 LIF에 대한 페일오버 타겟에 대한 정보가 표시됩니다. 페일오버 타겟 행은 해당 LIF에 대한 노드 포트 조합의 (우선 순위) 목록을 표시합니다.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------- --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

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

로드 밸런싱 존에서 **ONTAP LIF**를 확인하십시오

로드 밸런싱 영역이 올바르게 구성되었는지 확인하려면 해당 LIF에 속하는 모든 LIF를 표시할 수 있습니다. 또한 특정 LIF의 로드 밸런싱 존 또는 모든 LIF의 로드 밸런싱 존(Zone)을 볼 수도 있습니다.

단계

다음 명령 중 하나를 사용하여 원하는 LIF 및 로드 밸런싱 세부 정보를 표시합니다

표시 방법	입력...
특정 로드 밸런싱 구역에 있는 LIF입니다	네트워크 인터페이스 show-dns-zone zone zone_name zone_name은 load balancing zone의 이름을 지정한다.
특정 LIF의 로드 밸런싱 존	네트워크 인터페이스 show-lif lif_name-fields DNS-zone
모든 LIF의 로드 밸런싱 존	네트워크 인터페이스 보기 필드 DNS-존

LIF의 로드 밸런싱 존 표시 예

다음 명령을 실행하면 SVM vs0에 대한 로드 밸런싱 존 storage.company.com 에 있는 모든 LIF의 세부 정보가 표시됩니다.

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
-------- ---------- ---------- ----------------- --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20  ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20   ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20   ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20   ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20   ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20   ndeux-21  e0c     true
```

다음 명령을 실행하면 LIF 데이터의 DNS 존 세부 정보가 표시됩니다.3

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

다음 명령을 실행하면 클러스터에 있는 모든 LIF와 해당 DNS 존 목록이 표시됩니다.

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

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

ONTAP 클러스터 연결을 봅니다

클러스터의 모든 활성 연결 또는 클라이언트, 논리 인터페이스, 프로토콜 또는 서비스별로 노드의 활성 연결 수를 표시할 수 있습니다. 클러스터의 모든 수신 대기 연결을 표시할 수도 있습니다.

클라이언트별 활성 연결 표시(클러스터 관리자만 해당)

클라이언트별로 활성 연결을 확인하여 특정 클라이언트가 사용 중인 노드를 확인하고 노드당 클라이언트 수 간의 불균형을 확인할 수 있습니다.

이 작업에 대해

클라이언트별 활성 연결 수는 다음 시나리오에서 유용합니다.

- 사용 중이거나 과부하 상태인 노드 찾기
- 특정 클라이언트의 볼륨 액세스 속도가 느린 이유 파악

  클라이언트가 액세스하는 노드에 대한 세부 정보를 확인한 다음 볼륨이 상주하는 노드와 비교할 수 있습니다. 볼륨에 액세스해야 할 경우 초과 할당된 원격 노드의 볼륨에 대한 원격 액세스로 인해 클라이언트 성능이 저하될 수 있습니다.

- 모든 노드가 데이터 액세스에 동등하게 사용되는지 확인
- 예기치 않게 많은 수의 연결이 있는 클라이언트를 찾는 중입니다.
- 특정 클라이언트에 노드에 대한 연결이 있는지 확인

단계

network connections active show-clients 명령을 사용하여 노드의 클라이언트별 활성 연결 수를 표시합니다.

에 대한 자세한 내용은 `network connections active show-clients` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-clients
Node     Vserver Name     Client IP Address      Count
------   --------------   -----------------      ------
node0    vs0              192.0.2.253                 1
         vs0              192.0.2.252                 2
         Cluster          192.10.2.124                5
node1    vs0              192.0.2.250                 1
         vs0              192.0.2.252                 3
         Cluster          192.10.2.123                4
node2    vs1              customer.example.com        1
         vs1              192.0.2.245                 3
         Cluster          192.10.2.122                4
node3    vs1              customer.example.org        1
         vs1              customer.example.net        3
         Cluster          192.10.2.121                4
```

프로토콜별 활성 연결 표시(클러스터 관리자만 해당)

노드의 프로토콜(TCP 또는 UDP)별로 활성 연결 수를 표시하여 클러스터 내의 프로토콜 사용량을 비교할 수 있습니다.

이 작업에 대해

프로토콜별 활성 연결 수는 다음 시나리오에서 유용합니다.

- 연결을 끊는 UDP 클라이언트를 찾습니다.

  노드가 연결 제한에 근접하면 UDP 클라이언트가 가장 먼저 삭제됩니다.

- 사용 중인 다른 프로토콜이 없는지 확인

단계

network connections active show-protocols 명령을 사용하여 노드의 프로토콜별 활성 연결 수를 표시합니다.

에 대한 자세한 내용은 `network connections active show-protocols` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-protocols
Node      Vserver Name  Protocol   Count
-------   ------------  ---------  ------
node0
          vs0           UDP            19
          Cluster       TCP            11
node1
          vs0           UDP            17
          Cluster       TCP             8
node2
          vs1           UDP            14
          Cluster       TCP            10
node3
          vs1           UDP            18
          Cluster       TCP             4
```

서비스별 활성 연결 표시(클러스터 관리자만 해당)

클러스터의 각 노드에 대해 서비스 유형(예: NFS, SMB, 마운트 등)별로 활성 연결 수를 표시할 수 있습니다. 이 기능은 클러스터 내의 서비스 사용을 비교하여 노드의 운영 워크로드를 확인하는 데 유용합니다.

이 작업에 대해

서비스별 활성 연결 수는 다음 시나리오에서 유용합니다.

- 모든 노드가 적절한 서비스에 사용되고 있는지, 그리고 해당 서비스에 대한 로드 밸런싱이 작동하는지 확인합니다.
- 사용 중인 다른 서비스가 없는지 확인 network connections active show-services 명령을 사용하여 노드의 service별 활성 접속 수를 출력한다.

에 대한 자세한 내용은 `network connections active show-services` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
           vs0             mount           3
           vs0             nfs            14
           vs0             nlm_v4          4
           vs0             cifs_srv        3
           vs0             port_map       18
           vs0             rclopcp        27
           Cluster         ctlopcp        60
node1
           vs0             cifs_srv        3
           vs0             rclopcp        16
           Cluster         ctlopcp        60
node2
           vs1             rclopcp        13
           Cluster         ctlopcp        60
node3
           vs1             cifs_srv        1
           vs1             rclopcp        17
           Cluster         ctlopcp        60
```

LIF를 사용하여 노드 및 **SVM**에 활성 연결을 표시합니다

노드 및 SVM(스토리지 가상 머신)별로 각 LIF의 활성 연결 수를 표시하여 클러스터 내 LIF 간 연결 불균형을 확인할 수 있습니다.

이 작업에 대해

LIF에 의한 활성 연결 수는 다음 시나리오에서 유용합니다.

- 각 LIF의 연결 수를 비교하여 오버로드된 LIF를 찾습니다.
- 모든 데이터 LIF에서 DNS 로드 밸런싱이 작동하는지 확인
- 다양한 SVM에 대한 연결 수를 비교하여 가장 많이 사용되는 SVM을 찾습니다.

단계

'network connections active show-liff' 명령을 사용하여 SVM과 노드에서 각 LIF의 활성 연결 수를 표시합니다.

에 대한 자세한 내용은 `network connections active show-lifs` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

클러스터의 활성 연결을 표시합니다

클러스터의 활성 연결에 대한 정보를 표시하여 개별 연결에 사용되는 LIF, 포트, 원격 호스트, 서비스, SVM(스토리지 가상 머신) 및 프로토콜을 볼 수 있습니다.

이 작업에 대해

클러스터에서 활성 연결을 보는 것은 다음 시나리오에서 유용합니다.

- 개별 클라이언트가 올바른 노드에서 올바른 프로토콜 및 서비스를 사용하고 있는지 확인
- 클라이언트가 특정 노드, 프로토콜 및 서비스 조합을 사용하여 데이터에 액세스하는 데 문제가 있는 경우 이 명령을 사용하여 구성 또는 패킷 추적 비교를 위한 유사한 클라이언트를 찾을 수 있습니다.

단계

network connections active show 명령을 사용하여 클러스터의 활성 연결을 표시합니다.

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

다음 명령을 실행하면 노드 노드 1의 활성 연결이 표시됩니다.

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ----------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

다음 명령을 실행하면 SVM VS1 에서의 활성 연결이 표시됩니다.

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ----------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

클러스터의 수신 대기 연결을 표시합니다

클러스터에서 수신 대기 중인 연결에 대한 정보를 표시하여 지정된 프로토콜 및 서비스의 연결을 수락하는 LIF 및 포트를 볼 수 있습니다.

이 작업에 대해

클러스터에서 청취 연결을 보는 것은 다음 시나리오에서 유용합니다.

- 클라이언트가 해당 LIF에 일관되게 연결할 수 없을 경우, 원하는 프로토콜 또는 서비스가 LIF에서 청취 가능한지 확인하십시오.
- 다른 노드의 LIF를 통해 한 노드의 볼륨에 대한 원격 데이터 액세스가 장애가 발생할 경우 각 클러스터 LIF에서 UDP/rclopcp 수신기가 열려 있는지 확인합니다.
- SnapMirror가 동일한 클러스터의 두 노드 간에 전송 실패 시 각 클러스터 LIF에서 UDP/rclopcp 수신기가 열렸는지 확인
- SnapMirror가 서로 다른 클러스터에 있는 두 노드 간에 전송하는 데 실패할 경우 각 인터클러스터 LIF에서 TCP/ctlpcp 수신기가 열렸는지 확인합니다.

단계

Network connections listening show 명령을 사용하여 노드별 listening connection을 출력한다.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

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

네트워크 문제를 진단하는 **ONTAP** 명령

ping, traceroute, NDP, tcpdump 등의 명령어를 이용하여 네트워크 문제를 진단할 수 있다. 또한 ping6, tracerout6 등의 명령을 사용하여 IPv6 문제를 진단할 수도 있습니다.

원하는 작업	이 명령을 입력하십시오...
노드가 네트워크의 다른 호스트에 도달할 수 있는지 테스트합니다	네트워크 핑
노드가 IPv6 네트워크의 다른 호스트에 도달할 수 있는지 테스트합니다	네트워크 핑6
IPv4 패킷이 네트워크 노드에 취하는 경로를 추적한다	네트워크 추적 경로
IPv6 패킷이 네트워크 노드로 전송하는 경로를 추적한다	네트워크 tracerout6
NDP(Neighbor Discovery Protocol) 관리	네트워크 NDP
지정된 네트워크 인터페이스 또는 모든 네트워크 인터페이스에서 수신 및 전송된 패킷에 대한 통계를 표시합니다	'run-node_node_name_ifstat' * 참고 *: 이 명령은 노드 쉘에서 사용할 수 있습니다.
원격 디바이스 유형 및 디바이스 플랫폼을 포함하여 클러스터의 각 노드 및 포트에서 검색된 인접 디바이스에 대한 정보를 표시합니다	네트워크 디바이스 발견 쇼
노드의 CDP 인접 항목 보기(ONTAP는 CDPv1 광고만 지원)	'run-node_node_name_CDPD show -neighbors' * 참고 *: 이 명령은 노드 쉘에서 사용할 수 있습니다.

네트워크에서 송수신되는 패킷을 추적합니다	"network tcpdump start-node_node-name_-port_port_name_' * 참고 *: 이 명령은 노드 쉘에서 사용할 수 있습니다.
클러스터 간 또는 클러스터 간 노드 간의 지연 시간 및 처리량 측정	'network test-path-source-node_source_nodename local_-destination-cluster_destination_clustername_-destination-node_destination_nodename_-session-type_Default_,*AsyncMirrorLocal*,*AsyncMirrorRemote*, *SyncMirrorRemote* 또는 *RemoteDataTransfer*'를 참조하십시오 "성능 관리".

관련 정보

- "ONTAP 명령 참조입니다"
- "네트워크 Ping"
- "네트워크 경로 추적"
- "네트워크 장치 검색 표시"
- "네트워크 NDP"

Neighbor Discovery Protocol을 통한 네트워크 접속 구성 보기

Neighbor Discovery Protocol을 통해 **ONTAP** 네트워크 연결을 확인하십시오

데이터 센터에서 인접 검색 프로토콜을 사용하여 물리적 또는 가상 시스템 쌍과 해당 네트워크 인터페이스 간의 네트워크 연결을 볼 수 있습니다. ONTAP는 CDP(Cisco Discovery Protocol) 및 LLDP(Link Layer Discovery Protocol)라는 두 개의 인접 검색 프로토콜을 지원합니다.

인접 검색 프로토콜을 사용하면 네트워크에서 직접 연결된 프로토콜 지원 장치에 대한 정보를 자동으로 검색하고 볼 수 있습니다. 각 장치는 ID, 용량 및 연결 정보를 네트워크에 알립니다. 이 정보는 이더넷 프레임에서 멀티캐스트 MAC 주소로 전송되며, 인접한 모든 프로토콜 지원 장치에서 수신됩니다.

두 개의 장치가 이웃이 되려면 각각 프로토콜이 활성화되어 있고 올바르게 구성되어 있어야 합니다. 검색 프로토콜 기능은 직접 연결된 네트워크로 제한됩니다. 이웃에는 스위치, 라우터, 브리지 등과 같은 프로토콜 지원 장치가 포함될 수 있습니다. ONTAP는 개별적으로 또는 함께 사용할 수 있는 두 개의 인접 검색 프로토콜을 지원합니다.

- CDP(Cisco Discovery Protocol) *

CDP는 Cisco Systems에서 개발한 독점 링크 계층 프로토콜입니다. 이 기능은 클러스터 포트에 대해 ONTAP에서 기본적으로 활성화되지만 데이터 포트에 대해 명시적으로 설정해야 합니다.

LLDP(Link Layer Discovery Protocol) *

LLDP는 표준 문서 IEEE 802.1AB에 지정된 공급업체 중립적인 프로토콜입니다. 모든 포트에 대해 명시적으로 활성화해야 합니다.

CDP를 사용하여 **ONTAP** 네트워크 연결을 감지합니다

CDP를 사용하여 네트워크 연결을 감지하는 것은 배포 고려 사항 검토, 데이터 포트에서 활성화, 인접 장치 보기 및 필요에 따라 CDP 구성 값 조정으로 구성됩니다. CDP는 클러스터 포트에서 기본적으로 사용하도록 설정됩니다.

인접 장치에 대한 정보를 표시하려면 모든 스위치 및 라우터에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 릴리즈	설명
9.10.1 이하	CDP는 클러스터 스위치 상태 모니터에서 클러스터 및 관리 네트워크 스위치를 자동으로 검색하는 데 사용됩니다.
9.11.1 이상	CDP는 클러스터 스위치 상태 모니터에서 클러스터, 스토리지 및 관리 네트워크 스위치를 자동으로 검색하는 데 사용됩니다.

관련 정보

"시스템 관리"

CDP 사용 시 고려 사항

기본적으로 CDP 호환 장치는 CDPv2 광고를 보냅니다. CDP 호환 장치는 CDPv1 광고를 수신할 때만 CDPv1 광고를 보냅니다. ONTAP는 CDPv1만 지원합니다. 따라서 ONTAP 노드가 CDPv1 광고를 전송할 때 CDP 호환 인접 장치는 CDPv1 광고를 다시 보냅니다.

노드에서 CDP를 사용하도록 설정하기 전에 다음 정보를 고려해야 합니다.

- CDP는 모든 포트에서 지원됩니다.
- CDP 광고는 UP 상태인 포트를 통해 송수신합니다.
- CDP 광고를 보내고 받으려면 전송 및 수신 장치 모두에서 CDP를 사용하도록 설정해야 합니다.
- CDP 광고는 일정한 간격으로 전송되며 시간 간격을 구성할 수 있습니다.
- LIF의 IP 주소가 변경되면 노드는 다음 CDP 광고에서 업데이트된 정보를 보냅니다.
- ONTAP 9.10.1 이하:
  - CDP는 클러스터 포트에서 항상 사용하도록 설정됩니다.
  - CDP는 기본적으로 모든 비클러스터 포트에서 사용할 수 없습니다.
- ONTAP 9.11.1 이상:
  - CDP는 항상 클러스터 및 스토리지 포트에서 사용하도록 설정됩니다.
  - CDP는 기본적으로 모든 비 클러스터 및 비 스토리지 포트에서 사용할 수 없습니다.

> 노드에서 LIF가 변경되는 경우 CDP 정보는 수신 디바이스 측(예: 스위치)에서 업데이트되지 않는 경우가 있습니다. 이러한 문제가 발생하는 경우 노드의 네트워크 인터페이스를 DOWN 상태로 구성한 다음 UP 상태로 구성해야 합니다.

- CDP 광고에서는 IPv4 주소만 보급됩니다.
- VLAN이 있는 물리적 네트워크 포트의 경우 해당 포트의 VLAN에 구성된 모든 LIF가 보급됩니다.
- 인터페이스 그룹에 속한 물리적 포트의 경우 해당 인터페이스 그룹에 구성된 모든 IP 주소가 각 물리적 포트에 공고됩니다.
- VLAN을 호스팅하는 인터페이스 그룹의 경우 인터페이스 그룹과 VLAN에 구성된 모든 LIF가 각 네트워크 포트에 공고됩니다.

- CDP 패킷이 1500바이트 이하로 제한되기 때문에 많은 수의 LIF로 구성된 포트에서 이러한 IP 주소 중 일부만 인접 스위치에 보고됩니다.

CDP를 사용하거나 사용하지 않도록 설정합니다

CDP를 준수하는 인접 장치를 검색하고 알림을 보내려면 클러스터의 각 노드에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 9.10.1 이하 버전에서는 기본적으로 CDP가 노드의 모든 클러스터 포트에서 활성화되고 노드의 모든 비클러스터 포트에서 비활성화됩니다.

기본적으로 ONTAP 9.11.1 이상에서는 CDP가 노드의 모든 클러스터 및 스토리지 포트에서 활성화되고 노드의 모든 비클러스터 및 비스토리지 포트에서 비활성화됩니다.

이 작업에 대해

CDPD.ENABLE 옵션은 노드 포트에서 CDP가 활성화 또는 비활성화되는지 여부를 제어합니다.

- ONTAP 9.10.1 이하의 경우, On은 비 클러스터 포트에서 CDP를 사용하도록 설정합니다.
- ONTAP 9.11.1 이상의 경우, On은 비 클러스터 및 비 스토리지 포트에서 CDP를 사용하도록 설정합니다.
- ONTAP 9.10.1 이하 버전의 경우, 클러스터 포트가 아닌 경우 CDP가 사용되지 않으므로 클러스터 포트에서 CDP를 사용하지 않도록 설정할 수 없습니다.
- ONTAP 9.11.1 이상의 경우, OFF는 클러스터링되지 않은 포트와 비스토리지 포트에서 CDP를 사용하지 않도록 설정합니다. 클러스터 포트에서 CDP를 사용하지 않도록 설정할 수 없습니다.

CDP 호환 장치에 연결된 포트에서 CDP가 비활성화되어 있으면 네트워크 트래픽이 최적화되지 않을 수 있습니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 CDP 설정을 표시합니다.

CDP 설정을 보려면…	입력…
노드	'run-node <node_name> options CDPD.enable'
클러스터의 모든 노드	옵션 CDPD.ENABLE

2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에서 CDP를 사용하거나 사용하지 않도록 설정:

에서 CDP를 활성화 또는 비활성화하려면…	입력…
노드	'run-node node_name options CDPD.enable{on or off}'
클러스터의 모든 노드	'options CDPD.enable{on or off}'

CDP 인접 항목 정보를 봅니다

포트가 CDP 호환 장치에 연결되어 있는 경우, 클러스터 노드의 각 포트에 연결된 인접 장치에 대한 정보를 볼 수 있습니다. 명령을 사용하여 Neighbor 정보를 볼 수 있다 `network device-discovery show -protocol cdp`. 에 대한 자세한 내용은 `network device-discovery show` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

ONTAP 9.10.1 이하 버전에서는 클러스터 포트에 대해 CDP가 항상 활성화되어 있기 때문에 해당 포트에 대해 CDP 인접 항목 정보가 항상 표시됩니다. 해당 포트에 대한 인접 정보가 표시되도록 비 클러스터 포트에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 9.11.1 이상에서는 CDP가 항상 클러스터 및 스토리지 포트에 대해 활성화되므로 해당 포트에 대해 CDP 인접 항목 정보가 항상 표시됩니다. 해당 포트에 대해 인접 정보가 표시되도록 클러스터링되지 않은 포트와 비스토리지 포트에서 CDP가 활성화되어 있어야 합니다.

단계

클러스터의 노드의 포트에 연결된 모든 CDP 호환 디바이스에 대한 정보를 표시합니다.

```
network device-discovery show -node node -protocol cdp
```

다음 명령을 실행하면 노드 sti2650-212의 포트에 연결된 인접 항목이 표시됩니다.

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

출력에는 지정된 노드의 각 포트에 연결된 Cisco 장치가 나열됩니다.

CDP 메시지의 보류 시간을 구성합니다

보류 시간은 CDP 광고가 인접한 CDP 준수 장치의 캐시에 저장되는 기간입니다. 보류 시간은 각 CDPv1 패킷에 공고되며 노드에서 CDPv1 패킷을 수신할 때마다 업데이트됩니다.

- 'CDPD.HoldTime' 옵션의 값은 HA 쌍의 양쪽 노드에서 동일한 값으로 설정해야 합니다.
- 기본 유지 시간 값은 180초이지만 10초에서 255초 사이의 값을 입력할 수 있습니다.
- 보류 시간이 만료되기 전에 IP 주소를 제거하면 보류 시간이 만료될 때까지 CDP 정보가 캐싱됩니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 CDP 보류 시간을 표시합니다.

보류 시간을 보려면…	입력…
노드	'run-node node_name options CDPD.HoldTime'
클러스터의 모든 노드	옵션 CDPD.HoldTime

2. 클러스터의 모든 포트 또는 클러스터의 모든 노드에 있는 모든 포트에 대해 CDP 보류 시간을 구성합니다.

보류 시간을 설정하려면…	입력…
노드	'run-node node_name options CDPD.HoldTime HoldTime'
클러스터의 모든 노드	옵션 CDPD.HoldTime HoldTime

CDP 광고 전송 간격을 설정합니다

CDP 광고는 CDP 이웃에게 정기적으로 전송됩니다. 네트워크 트래픽과 네트워크 토폴로지의 변경 내용에 따라 CDP 광고 전송 간격을 늘리거나 줄일 수 있습니다.

- "cdpd.interval` 옵션 값은 HA 쌍의 두 노드에서 같은 값으로 설정해야 합니다.
- 기본 간격은 60초이지만 5초에서 900초 사이의 값을 입력할 수 있습니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 CDP 광고 시간 간격을 표시합니다.

간격을 보려면…	입력…
노드	'run-node node_name options cdpd.interval`
클러스터의 모든 노드	옵션 cdpd.interval`

2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에 대해 CDP 알림을 보내는 간격을 구성합니다.

간격을 설정하려면…	입력…
노드	'run-node node_name options cdpd.interval interval
클러스터의 모든 노드	옵션 cdpd.interval 간격

CDP 통계를 보거나 지웁니다

각 노드의 클러스터 및 비클러스터 포트에 대한 CDP 통계를 보고 잠재적인 네트워크 연결 문제를 감지할 수 있습니다. CDP 통계는 마지막 삭제 시점으로부터 누적됩니다.

이 작업에 대해

ONTAP 9.10.1 이하 버전에서는 포트에 대해 CDP가 항상 활성화되어 있기 때문에 해당 포트의 트래픽에 대해 CDP 통계가 항상 표시됩니다. 해당 포트에 대한 통계를 표시하려면 포트에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 9.11.1 이상에서는 CDP가 항상 클러스터 및 스토리지 포트에 대해 활성화되므로 해당 포트의 트래픽에 대해 CDP 통계가 항상 표시됩니다. 이러한 포트에 대한 통계를 표시하려면 클러스터링되지 않은 포트 또는 비스토리지 포트에서 CDP가 활성화되어 있어야 합니다.

단계

노드의 모든 포트에 대한 현재 CDP 통계를 표시하거나 지웁니다.

원하는 작업	입력…
CDP 통계를 봅니다	'run-node_name CDPD show-stats'
CDP 통계를 지웁니다	'run-node_name CDPD zero-stats'

통계 표시 및 지우기 예

다음 명령을 실행하면 CDP 통계가 지워지기 전에 표시됩니다. 마지막 통계 삭제 이후 송수신된 총 패킷 수가 출력에 표시됩니다.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

다음 명령을 실행하면 CDP 통계가 지워집니다.

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:            0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:     0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:            0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:      0
```

통계를 지운 후에는 다음 CDP 보급 알림이 전송되거나 수신된 후에 누적되기 시작합니다.

CDP를 지원하지 않는 이더넷 스위치에 연결 중입니다

여러 공급업체 스위치는 CDP를 지원하지 않습니다. 를 참조하십시오"NetApp 지식 기반: ONTAP 장치 검색 시 스위치 대신 노드가 표시됨" 자세한 내용은.

이 문제를 해결하는 방법에는 두 가지가 있습니다.

- 지원되는 경우 CDP를 사용하지 않도록 설정하고 LLDP를 사용하도록 설정합니다. 을 참조하십시오 "LLDP를 사용하여 네트워크 연결을 감지합니다" 를 참조하십시오.
- CDP 광고를 삭제하도록 스위치에서 MAC 주소 패킷 필터를 구성합니다.

LLDP를 사용하여 ONTAP 네트워크 연결을 검색합니다

LLDP를 사용하여 네트워크 연결을 탐지하는 작업은 배포 고려 사항을 검토하고, 모든 포트에서 활성화하고, 인접 장치를 보고, 필요에 따라 LLDP 구성 값을 조정하는 것으로 구성됩니다.

인접 장치에 대한 정보를 표시하려면 모든 스위치 및 라우터에서 LLDP를 활성화해야 합니다.

ONTAP는 현재 다음과 같은 TLV(type-length-value structures)를 보고합니다.

- 섀시 ID입니다
- 포트 ID입니다
- TTL(Time-to-Live)
- 시스템 이름입니다

  시스템 이름 TLV는 CNA 장치에서 전송되지 않습니다.

X1143 어댑터 및 UTA2 온보드 포트와 같은 특정 통합 네트워크 어댑터(CNA)에는 LLDP에 대한 오프로드 지원 기능이 포함되어 있습니다.

- LLDP 오프로드는 DCB(데이터 센터 브리징)에 사용됩니다.
- 표시된 정보는 클러스터와 스위치 간에 다를 수 있습니다.

  스위치에 표시되는 섀시 ID 및 포트 ID 데이터는 CNA 및 비 CNA 포트에 대해 다를 수 있습니다.

예를 들면 다음과 같습니다.

- 비 CNA 포트의 경우:
  - 섀시 ID는 노드에 있는 포트 중 하나의 고정 MAC 주소입니다
  - 포트 ID는 노드에 있는 해당 포트의 포트 이름입니다
- CNA 포트의 경우:
  - 섀시 ID와 포트 ID는 노드에 있는 각 포트의 MAC 주소입니다.

그러나 클러스터에서 표시하는 데이터는 이러한 포트 유형에 대해 일관적입니다.

> LLDP 사양은 SNMP MIB를 통해 수집된 정보에 대한 액세스를 정의합니다. 그러나 ONTAP는 현재 LLDP MIB를 지원하지 않습니다.

LLDP를 활성화 또는 비활성화합니다

LLDP 호환 인접 장치를 검색하고 보급을 보내려면 클러스터의 각 노드에서 LLDP를 활성화해야 합니다. ONTAP 9.7부터 LLDP는 기본적으로 노드의 모든 포트에서 활성화됩니다.

이 작업에 대해

ONTAP 9.10.1 이하 버전의 경우, 노드 포트에서 LLDP가 활성화 또는 비활성화되는지 여부를 제어하는 LAll DP.enable 옵션:

- On은 모든 포트에서 LLDP를 활성화합니다.
- OFF는 모든 포트에서 LLDP를 비활성화합니다.

ONTAP 9.11.1 이상의 경우, "LI DP.enable" 옵션은 노드의 비클러스터 및 비스토리지 포트에서 LLDP가 활성화될지 여부를 제어합니다.

- On은 모든 비 클러스터 및 비 스토리지 포트에서 LLDP를 활성화합니다.
- "off"는 모든 비 클러스터 및 비 스토리지 포트에서 LLDP를 비활성화합니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 LLDP 설정을 표시합니다.
   - 단일 노드: 'run-node_name options lldp.enable'
   - 모든 노드: 옵션 ll dp.enable
2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에서 LLDP를 사용하거나 사용하지 않도록 설정합니다.

에서 LLDP를 활성화 또는 비활성화하려면…	입력…

노드	'run-node node_name options lldp.enable{on
off}'	클러스터의 모든 노드
'options lldp.enable{on	off}'

- 단일 노드:

```
run -node node_name options lldp.enable {on|off}
```

- 모든 노드:

```
options lldp.enable {on|off}
```

LLDP 인접 정보를 봅니다

포트가 LLDP 호환 장치에 연결되어 있는 경우, 클러스터 노드의 각 포트에 연결된 인접 장치에 대한 정보를 볼 수 있습니다. network device-discovery show 명령을 사용하여 인접 항목 정보를 볼 수 있습니다.

단계

1. 클러스터의 노드의 포트에 연결된 모든 LLDP 호환 장치에 대한 정보를 표시합니다.

```
network device-discovery show -node node -protocol lldp
```

다음 명령을 실행하면 노드 클러스터-1_01의 포트에 연결된 인접 항목이 표시됩니다. 출력에는 지정된 노드의 각 포트에 연결된 LLDP 지원 디바이스가 나열됩니다. '-protocol' 옵션을 생략하면 출력에 CDP 지원 디바이스도 나열됩니다.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

LLDP 광고 전송 간격을 조정합니다

LLDP 광고는 주기적으로 LLDP 이웃에게 전송됩니다. 네트워크 트래픽과 네트워크 토폴로지의 변경 내용에 따라 LLDP 광고 전송 간격을 늘리거나 줄일 수 있습니다.

이 작업에 대해

IEEE에서 권장하는 기본 간격은 30초이지만 5초에서 300초까지 값을 입력할 수 있습니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 LLDP 광고 시간 간격을 표시합니다.
   - 단일 노드:

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - 모든 노드:

     ```
     options lldp.xmit.interval
     ```

2. 노드의 모든 포트 또는 클러스터의 모든 노드에 대해 LLDP 광고를 전송하는 간격을 조정합니다.
   - 단일 노드:

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - 모든 노드:

     ```
     options lldp.xmit.interval <interval>
     ```

LLDP 광고의 실시간 값을 조정합니다

TTL(Time-to-Live)은 인접 LLDP 호환 장치의 캐시에 LLDP 광고가 저장되는 기간입니다. TTL은 각 LLDP 패킷에서 공고되며 LLDP 패킷이 노드에 수신될 때마다 업데이트됩니다. TTL은 나가는 LLDP 프레임에서 수정할 수 있습니다.

이 작업에 대해

- TTL은 전송 간격(모든 dp.xmit.interval`) 및 보류 승수(모든 dP.xmit.hold)에 1을 더한 계산된 값입니다.
- 기본 보압 승수 값은 4이지만 1에서 100 사이의 값을 입력할 수 있습니다.
- 따라서 기본 TTL은 IEEE에서 권장하는 121초이지만 전송 간격 및 고정 승수 값을 조정하여 발신 프레임의 값을 6초에서 30001초로 지정할 수 있습니다.
- TTL이 만료되기 전에 IP 주소를 제거하면 TTL이 만료될 때까지 LLDP 정보가 캐싱됩니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 보류 승수 값을 표시합니다.

- 단일 노드:

```
run -node <node_name> options lldp.xmit.hold
```

- 모든 노드:

```
options lldp.xmit.hold
```

2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에서 고정 승수 값을 조정합니다.
   - 단일 노드:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

   - 모든 노드:

```
options lldp.xmit.hold <hold_value>
```

LLDP 통계를 보거나 지웁니다

각 노드의 클러스터 및 비 클러스터 포트에 대한 LLDP 통계를 보고 잠재적인 네트워크 연결 문제를 감지할 수 있습니다. LLDP 통계는 마지막 삭제 시점으로부터 누적됩니다.

이 작업에 대해

ONTAP 9.10.1 이하의 경우 클러스터 포트에 대해 LLDP가 항상 활성화되므로 해당 포트의 트래픽에 대해 LLDP 통계가 항상 표시됩니다. 해당 포트에 대한 통계가 표시되도록 비 클러스터 포트에서 LLDP가 활성화되어 있어야 합니다.

ONTAP 9.11.1 이상에서는 클러스터 및 스토리지 포트에 대해 LLDP가 항상 활성화되므로 해당 포트의 트래픽에 대해 LLDP 통계가 항상 표시됩니다. 해당 포트에 대한 통계가 표시되도록 클러스터 이외의 포트와 스토리지 이외의 포트에서 LLDP가 활성화되어 있어야 합니다.

단계

노드의 모든 포트에 대한 현재 LLDP 통계를 표시하거나 지웁니다.

원하는 작업	입력…
LLDP 통계를 봅니다	'run-node_name lldp stats'
LLDP 통계를 지웁니다	'run-node_name lldp stats-z'를 선택합니다

통계 예제를 표시하고 지웁니다

다음 명령을 실행하면 LLDP 통계가 지워지기 전에 표시됩니다. 마지막 통계 삭제 이후 송수신된 총 패킷 수가 출력에

표시됩니다.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

다음 명령을 실행하면 LLDP 통계가 지워집니다.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

통계를 지운 후 다음 LLDP 보급 알림이 전송되거나 수신된 후에 누적되기 시작합니다.

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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.