vSAN 네트워크 설계

Update 3

VMware vSphere 8.0
VMware vSAN 8.0

vmware
by Broadcom

VMware by Broadcom 웹 사이트

https://docs.vmware.com/kr에서 최신 기술 문서를 찾을 수 있습니다.

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

목차

vSAN 네트워크 설계 정보

1

" vSAN 네트워크 설계" 가이드에서는 고가용성 및 확장 가능한 vSAN 클러스터를 배포하기 위한 네트워크 요구 사항, 네트워크 설계 및 구성 사례에 대해 설명합니다.

vSAN은 분산 스토리지 솔루션입니다. 다른 분산 솔루션과 마찬가지로 네트워크는 설계의 중요한 구성 요소입니다. 부적절한 네트워킹 하드웨어 및 설계를 사용하면 원치 않는 결과로 이어질 수 있으므로 최상의 결과를 얻으려면 이 문서에 제공된 지침을 준수해야 합니다.

VMware는 포용성을 중요하게 생각합니다. 고객, 파트너 및 내부 커뮤니티 내에서 이 원칙을 지원하기 위해 포괄적인 언어를 사용하여 컨텐츠를 생성합니다.

대상 사용자

이 가이드는 vSAN 클러스터를 설계, 배포 및 관리하는 모든 사용자를 대상으로 합니다. 이 가이드의 정보는 네트워크 설계 및 구성, 가상 시스템 관리, 가상 데이터 센터 작업에 익숙한 경험 많은 네트워크 관리자를 대상으로 작성되었습니다. 이 가이드에서는 또한 VMware ESXi, vCenter Server 및 vSphere Client를 비롯한 VMware vSphere에 익숙하다는 것을 전제로 합니다.

관련 문서

이 가이드 외에 다음 가이드를 참조하여 vSAN 네트워킹에 대해 자세히 알아볼 수 있습니다.

- "vSAN 계획 및 배포 가이드" : vSAN 클러스터 생성에 대한 추가 정보 알아보기
- "VMware vSAN 관리" : vSAN 클러스터를 구성하고 vSAN 기능에 대해 자세히 알아보기
- "vSAN 모니터링 및 문제 해결 가이드" : vSAN 클러스터 모니터링 및 문제 해결

vSAN 네트워크 소개

2

vSAN을 사용하여 vSphere 내에서 공유 스토리지를 프로비저닝할 수 있습니다. vSAN은 호스트 클러스터의 로컬 또는 직접 연결 스토리지 디바이스를 집계하여 vSAN 클러스터의 모든 호스트에서 공유되는 단일 스토리지 풀을 생성합니다.

vSAN은 vSAN 스토리지 트래픽을 위해 적절히 구성된 고가용성 네트워크에 의존하는 분산 및 공유 스토리지 솔루션입니다. 고성능 및 고가용성 네트워크는 성공적인 vSAN 배포에 매우 중요합니다. 이 가이드에서는 vSAN 네트워크를 설계하고 구성하는 방법에 대한 권장 사항을 제공합니다.

vSAN에는 확장 가능하고 복원력이 뛰어난 고성능 네트워크에 의존하는 분산 아키텍처가 있습니다. vSAN 클러스터 내의 모든 호스트 노드는 IP 네트워크를 통해 통신합니다. 모든 호스트는 IP 유니캐스트 연결을 유지해야 하므로 계층 2 또는 계층 3 네트워크를 통해 통신할 수 있습니다. 유니캐스트 통신에 대한 자세한 내용은 장 4 vSAN 네트워크에서 유니캐스트 사용을 참조하십시오.

vSAN 네트워킹 용어 및 정의

vSAN에는 이해하고 있어야 하는 몇 가지 중요한 용어와 정의가 포함되어 있습니다. vSAN 네트워크 설계를 시작하기 전에 주요 vSAN 네트워킹 용어 및 정의를 검토하십시오.

용어	정의
CLOM	CLOM(클러스터 수준 개체 관리자)은 개체 구성이 해당 스토리지 정책과 일치하는지 확인하는 역할을 합니다. CLOM은 해당 정책을 충족하는 데 사용할 수 있는 장애 도메인이 충분한지 아닌지를 확인합니다. 또한 클러스터에서 구성 요소 및 감시 기능을 배치할 위치를 결정합니다.
CMMDS	CMMDS(클러스터 모니터링, 멤버 자격 및 디렉토리 서비스)는 네트워크로 연결된 노드 멤버 클러스터의 복구 및 유지 보수를 담당합니다. 호스트 노드, 디바이스 및 네트워크와 같은 항목의 인벤토리를 관리합니다. 또한 vSAN 개체에 대한 정책 및 RAID 구성과 같은 메타데이터 정보도 저장합니다.
DOM	DOM(분산 개체 관리자)은 구성 요소를 생성하고 클러스터에 분산하는 역할을 합니다. DOM 개체가 생성되면 노드(호스트) 중 하나가 해당 개체에 대한 DOM 소유자로 지정됩니다. 이 호스트는 클러스터 전체에서 해당 하위 구성 요소를 찾은 후 vSAN 네트워크를 통해 해당 구성 요소로 I/O를 리디렉션함으로써 해당 DOM 개체에 대한 모든 IOPS를 처리합니다. DOM 개체에는 vdisk, snapshot, vmnamespace, vmswap, vmem 등이 포함됩니다.

용어	정의
LSOM	LSOM(로그 구조 개체 관리자)은 vSAN 파일 시스템의 데이터를 vSAN 구성 요소 또는 LSOM 개체(데이터 구성 요소 또는 감시 구성 요소)로서 로컬로 저장하는 역할을 합니다.
NIC 팀 구성	NIC(네트워크 인터페이스 카드) 팀 구성 기능은 고가용성 및 로드 밸런싱에 대해 "팀"으로 설정된 2개 이상의 네트워크 어댑터(NIC)로 정의할 수 있습니다.
NIOC	NIOC(Network I/O Control)는 여러 유형의 네트워크 트래픽이 vSphere Distributed Switch에 수신되는 대역폭을 결정합니다. 대역폭 분포는 사용자가 구성할 수 있는 매개 변수입니다. NIOC를 사용하도록 설정하면 분산 스위치 트래픽이 미리 정의된 네트워크 리소스 풀(Fault Tolerance 트래픽, iSCSI 트래픽, vMotion 트래픽, 관리 트래픽, vSphere Replication 트래픽, NFS 트래픽 및 가상 시스템 트래픽)으로 구분됩니다.
개체 및 구성 요소	각 개체는 VM 스토리지 정책에서 사용 중인 기능을 통해 결정되는 일련의 구성 요소로 이루어져 있습니다. vSAN 데이터스토어에는 몇 가지 개체 유형이 포함되어 있습니다. ■ **VM 홈 네임스페이스** - VM 홈 네임스페이스는 모든 가상 시스템 구성 파일이 저장되는 가상 시스템 홈 디렉토리입니다. 여기에는 .vmx, 로그 파일, vmdk 및 스냅샷 델타 설명 파일 등이 포함되어 있습니다. ■ **VMDK** - VMDK는 가상 시스템의 하드 디스크 드라이브 내용을 저장하는 가상 시스템 디스크 또는 .vmdk 파일입니다. ■ **VM 스왑 개체** - VM 스왑 개체는 가상 시스템의 전원을 켤 때 생성됩니다. ■ **스냅샷 델타 VMDK** - 스냅샷 델타 VMDK는 가상 시스템 스냅샷이 작성될 때 생성됩니다. ■ **메모리 개체** - 메모리 개체는 가상 시스템을 생성하거나 일시 중단할 때 스냅샷 메모리 옵션이 선택되면 생성됩니다.
RDT	RDT(신뢰할 수 있는 데이터 전송) 프로토콜은 vSAN VMkernel 포트를 통한 호스트 간 통신에 사용됩니다. 이 프로토콜은 전송 계층에서 TCP를 사용하고 요청 시 TCP 연결(소켓)을 생성 및 제거하는 일을 담당합니다. 대형 파일을 보내도록 최적화되어 있습니다.
SPBM	SPBM(스토리지 정책 기반 관리)은 광범위한 데이터 서비스와 스토리지 솔루션 간에 통합된 단일 제어 패널 역할을 하는 스토리지 정책 프레임워크를 제공합니다. 이 프레임워크는 가상 시스템의 애플리케이션 요구 사항에 맞게 스토리지를 정렬하는 데 도움을 줍니다.
VASA	VASA(스토리지 인식용 vSphere 스토리지 API)는 vCenter Server에서 스토리지 어레이의 기능을 인식할 수 있도록 하는 API(애플리케이션 프로그램 인터페이스) 집합입니다. VASA 제공자는 vCenter Server와 통신하여 정책 기반 관리, 작업 관리 및 DRS 기능을 지원하는 스토리지 토폴로지, 기능 및 상태 정보를 결정합니다.

용어	정의
VLAN	VLAN은 하나의 물리적 LAN 세그먼트를 더 세분화하여 포트 그룹이 물리적으로 다른 세그먼트에 있는 것처럼 서로 분리시킵니다.
감시 구성 요소	감시는 메타데이터만 포함하고 실제 애플리케이션 데이터는 포함하지 않는 구성 요소입니다. 이것은 잠재적 장애 후 아직 사용 가능한 데이터스토어 구성 요소의 가용성에 관해 결정을 내려야 할 때 타이브레이커 역할을 합니다. 감시 기능은 온디스크 형식 1.0 사용 시 vSAN 데이터스토어에서 약 2MB의 메타데이터 공간을 사용하고 온디스크 형식 버전 2.0 이상 사용 시 4MB를 사용합니다.

vSAN 네트워킹 이해

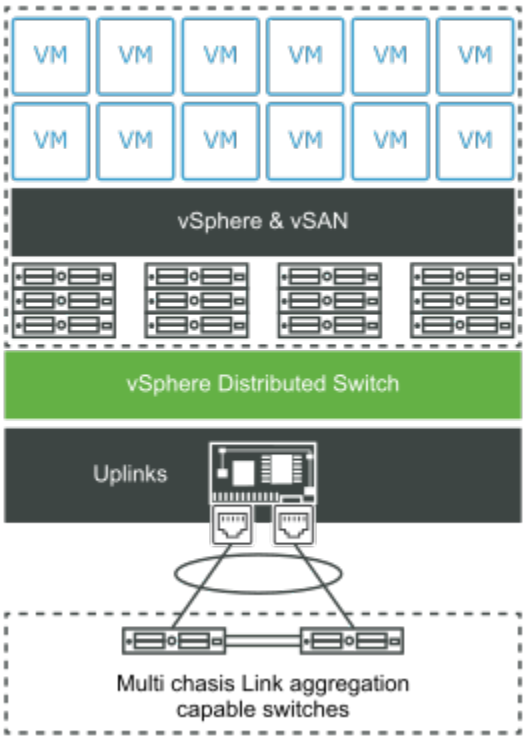
3

vSAN 네트워크는 클러스터 호스트 간의 통신을 용이하게 하며 빠른 성능, 고가용성 및 대역폭을 보장해야 합니다.

vSAN은 네트워크를 사용하여 ESXi 호스트와 가상 시스템 디스크 I/O 간에 통신을 수행합니다.

vSAN 데이터스토어의 VM(가상 시스템)은 개체 집합으로 구성되며, 각 개체는 하나 이상의 구성 요소로 이루어질 수 있습니다. 이러한 구성 요소는 드라이브 및 호스트 장애에 대해 복원력을 제공하기 위해 여러 호스트에 분산됩니다. vSAN은 vSAN 네트워크를 사용하여 이러한 구성 요소를 유지 보수하고 업데이트할 수 있습니다.

다음 다이어그램은 vSAN 네트워크에 대한 개략적인 개요입니다.



다음으로 아래 항목을 읽으십시오.

- vSAN 네트워크 특성
- ESXi 트래픽 유형
- vSAN에 대한 네트워킹 요구 사항

vSAN 네트워크 특성

vSAN은 네트워크에 따라 다릅니다. 성능 및 안정성 문제를 방지하기 위해서는 올바른 vSAN 네트워크 설정을 이해하고 구성하는 것이 중요합니다.

신뢰할 수 있는 강력한 vSAN 네트워크는 다음과 같은 특징을 갖습니다.

유니캐스트

vSAN 6.6 이상 릴리스에서는 유니캐스트 통신을 지원합니다. 유니캐스트 트래픽은 네트워크의 한 지점에서 다른 지점으로 IP 패킷을 일대일로 전송하는 것입니다. 유니캐스트는 기본 호스트에서 전송된 하트비트를 1초마다 다른 모든 호스트로 전송합니다. 이렇게 전송되면 호스트가 활성 상태고 vSAN 클러스터에 호스트가 참여하고 있는 것입니다. vSAN을 위한 단순한 유니캐스트 네트워크를 설계할 수 있습니다. 유니캐스트 통신에 대한 자세한 내용은 장 4 vSAN 네트워크에서 유니캐스트 사용을 참조하십시오.

참고 가능하면 항상 최신 버전의 vSAN을 사용하십시오.

계층 2 및 계층 3 네트워크

vSAN 클러스터의 모든 호스트는 계층 2 또는 계층 3 네트워크를 통해 연결되어야 합니다. vSAN 6.0보다 이전 버전인 vSAN 릴리스는 계층 2 네트워킹만 지원하지만 후속 릴리스에서는 계층 2 및 계층 3 프로토콜을 둘 다 지원합니다. 계층 2 또는 계층 3 네트워크를 사용하여 데이터 사이트 및 감시 사이트 간 통신을 제공합니다. 계층 2 및 계층 3 네트워크 토폴로지에 대한 자세한 내용은 표준 배포를 참조하십시오.

VMkernel 네트워크

vSAN 클러스터의 각 ESXi 호스트에는 vSAN 통신을 위한 네트워크 어댑터가 있어야 합니다. 모든 클러스터 노드 내 통신은 vSAN VMkernel 포트를 통해 수행됩니다. VMkernel 포트는 계층 2 및 계층 3 서비스를 각 vSAN 호스트 및 호스팅된 가상 시스템에 제공합니다.

vSAN 네트워크 트래픽

스토리지 트래픽 및 유니캐스트 트래픽과 같은 여러 가지 트래픽 유형을 vSAN 네트워크에서 사용할 수 있습니다. 가상 시스템의 계산 및 스토리지는 동일한 호스트에 있거나 클러스터의 서로 다른 호스트에 있을 수 있습니다. 장애를 허용하도록 구성되지 않은 VM은 한 호스트에서 실행되면서 다른 호스트에 있는 VM 개체 또는 구성 요소에 액세스할 수 있습니다. 즉, VM의 모든 I/O가 네트워크를 통해 전달된다는 것을 의미합니다. 스토리지 트래픽은 vSAN 클러스터의 트래픽 대부분을 구성합니다.

모든 ESXi 호스트 간의 클러스터 관련 통신은 vSAN 클러스터에서 트래픽을 생성합니다. 이 유니캐스트 트래픽은 vSAN 네트워크 트래픽에도 기여합니다.

가상 스위치

vSAN은 다음과 같은 가상 스위치 유형을 지원합니다.

- 표준 가상 스위치는 VM 및 VMkernel 포트에서 외부 네트워크로의 연결을 제공합니다. 이 스위치는 각 ESXi 호스트에 대해 로컬입니다.

- vSphere Distributed Switch는 여러 ESXi 호스트의 가상 스위치 관리를 중앙에서 제어합니다. 분산 스위치는 vSphere 또는 가상 네트워크에서 QoS(서비스 품질) 수준을 설정하는 데 도움이 되는 NIOC(Network I/O Control)와 같은 네트워킹 기능을 제공합니다. vSAN에는 vCenter Server 버전과 관계없이 vSphere Distributed Switch가 포함됩니다.

대역폭

vSAN 트래픽은 물리적 네트워크 어댑터를 다른 시스템 트래픽 유형(예: vSphere vMotion 트래픽, vSphere HA 트래픽 및 가상 시스템 트래픽)과 공유할 수 있습니다. 또한 vSAN, vSphere 관리, vSphere vMotion 트래픽 등이 동일한 물리적 네트워크에 있는 공유 네트워크 구성에 더 많은 대역폭을 제공합니다. vSAN에 필요한 대역폭 양을 보장하려면 분산 스위치에서 vSphere Network I/O Control을 사용합니다.

vSphere Network I/O Control에서 vSAN 송신 트래픽에 대한 예약 및 공유를 구성할 수 있습니다.

- 예약을 설정하면 Network I/O Control이 물리적 어댑터에서 vSAN에 대해 최소 대역폭을 사용할 수 있도록 보장합니다.
- 공유 값을 100으로 설정하면 vSAN에 할당된 물리적 어댑터가 포화 상태가 되는 경우 vSAN에서 특정 대역폭을 사용할 수 있습니다. 예를 들어 팀에서 다른 물리적 어댑터가 실패하고 포트 그룹의 모든 트래픽이 팀의 다른 어댑터로 전송되면 물리적 어댑터가 포화 상태가 될 수 있습니다.

vSAN 트래픽의 대역폭 할당 구성을 위한 Network I/O Control 사용에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

ESXi 트래픽 유형

ESXi 호스트는 여러 다른 네트워크 트래픽 유형을 사용하여 vSAN을 지원합니다.

다음은 vSAN에 대해 설정해야 하는 여러 트래픽 유형입니다.

표 3-1. 네트워크 트래픽 유형

트래픽 유형	설명
관리 네트워크	관리 네트워크는 VMkernel TCP/IP 스택을 사용하여 호스트 연결 및 관리를 쉽게 하는 기본 네트워크 인터페이스입니다. 또한 vMotion, iSCSI, NFS(Network File System), FCoE(Fiber Channel over Ethernet) 및 Fault Tolerance와 같은 시스템 트래픽을 처리할 수도 있습니다.
가상 시스템 네트워크	가상 네트워킹을 사용하면 가상 시스템을 네트워크로 연결하고 단일 ESXi 호스트 내에서 또는 여러 ESXi 호스트 간에 복잡한 네트워크를 구축할 수 있습니다.

표 3-1. 네트워크 트래픽 유형 (계속)

트래픽 유형	설명
vMotion 네트워크	한 호스트에서 다른 호스트로의 VM 마이그레이션을 쉽게 해 주는 트래픽 유형입니다. vMotion을 사용하여 마이그레이션하려면 소스 호스트와 대상 호스트에 올바르게 구성된 네트워크 인터페이스가 필요합니다. vMotion 네트워크가 vSAN 네트워크와 구분되는지 확인합니다.
vSAN 네트워크	vSAN 클러스터에는 데이터 교환을 위해 VMkernel 네트워크가 필요합니다. vSAN 클러스터의 각 ESXi 호스트에는 vSAN 트래픽을 위한 VMkernel 네트워크 어댑터가 있어야 합니다. 자세한 내용은 "vSAN 계획 및 배포" 에서 "수동으로 vSAN 사용"을 참조하십시오.

vSAN에 대한 네트워킹 요구 사항

vSAN은 호스트 간 통신을 위해 네트워크에 의존하는 분산 스토리지 솔루션입니다. 배포하기 이전에 vSAN 환경에 모든 네트워킹 요구 사항이 있는지 확인합니다.

물리적 NIC 요구 사항

vSAN 호스트에서 사용되는 NIC(네트워크 인터페이스 카드)는 특정 요구 사항을 충족해야 합니다. vSAN은 10Gbps, 25Gbps, 40Gbps, 50Gbps 및 100Gbps 네트워크에서 작동합니다.

호스트가 vSAN OSA(Original Storage Architecture) 또는 vSAN ESA(Express Storage Architecture)에 대한 최소 NIC 요구 사항을 충족하는지 확인합니다.

표 3-2. vSAN OSA 최소 NIC 요구 사항 및 권장 사항

토폴로지 또는 배포 모드	아키텍처	1GbE NIC 지원	10GbE NIC 지원	10GbE보다 큰 NIC 지원	노드 간 지연 시간	사이트 간 링크 대역폭 또는 지연 시간	노드 및 vSAN 감시 호스트 간 지연 시간	노드 및 vSAN 감시 호스트 간 대역폭
단일 사이트 vSAN 클러스터	하이브리드 클러스터	예(최소)	예(권장)	예	1ms RTT 미만입니다.	해당 없음	해당 없음	해당 없음
	플래시 전용 클러스터	아니요	예	예(권장)				
vSAN 확장된 클러스터	하이브리드 또는 플래시 전용 클러스터	아니요	예(최소)	예	각 사이트 내에 1ms 미만의 RTT가 있습니다.	권장되는 값은 10GbE(워크로드 종속) 및 5ms RTT 이하입니다.	200ms RTT 미만입니다. 사이트당 최대 10개의 호스트. 100ms RTT 미만입니다. 사이트당 11~15개의 호스트.	1,000개 구성 요소당 2Mbps(45000개 구성 요소가 있는 경우 최대 100Mbps).

표 3-2. vSAN OSA 최소 NIC 요구 사항 및 권장 사항 (계속)

토폴로지 또는 배포 모드	아키텍처	1GbE NIC 지원	10GbE NIC 지원	10GbE보다 큰 NIC 지원	노드 간 지연 시간	사이트 간 링크 대역폭 또는 지연 시간	노드 및 vSAN 감시 호스트 간 지연 시간	노드 및 vSAN 감시 호스트 간 대역폭
2노드 vSAN 클러스터	하이브리드 클러스터	예(최대 10개의 VM)	예(권장)	예	동일한 사이트 내에 1ms 미만의 RTT가 있습니다.	권장되는 값은 10GbE 및 5ms RTT 이하입니다.	500ms RTT 미만입니다.	1,000개 구성 요소당 2Mbps(최대 1.5Mbps).
	플래시 전용 클러스터	아니요	예(최소)					

표 3-3. vSAN ESA 최소 NIC 요구 사항 및 권장 사항

배포 유형	1GbE NIC 지원	10GbE NIC 지원	10GbE보다 큰 NIC 지원	노드 간 지연 시간	사이트 간 링크 대역폭 또는 지연 시간	노드 및 vSAN 감시 호스트 간 지연 시간	노드 및 vSAN 감시 호스트 간 대역폭
단일 사이트 vSAN 클러스터	아니요	예	예	1ms RTT 미만입니다.	해당 없음	해당 없음	해당 없음
vSAN 확장된 클러스터	아니요	예	예	각 사이트 내에 1ms 미만의 RTT가 있습니다.	최소 10GbE(워크로드 종속) 및 5ms RTT.	200ms RTT 미만입니다. 사이트당 최대 10개의 호스트.	1,000개 구성 요소당 2Mbps(45000개 구성 요소가 있는 경우 최대 100Mbps).
						100ms RTT 미만입니다. 사이트당 11~15개의 호스트.	
2노드 vSAN 클러스터	아니요	예	예	동일한 사이트 내에 1ms 미만의 RTT가 있습니다.	권장되는 값은 25GbE 및 5ms RTT 이하입니다.	500ms RTT 미만입니다.	1,000개 구성 요소당 2Mbps(최대 1.5Mbps).

참고 이러한 NIC 요구 사항은 패킷 손실이 하이퍼 통합 환경에서 0.0001% 이하라고 가정합니다. 이러한 요구 사항을 초과하는 경우 vSAN 성능에 크게 영향을 미칠 수 있습니다.

vSAN 확장된 클러스터 NIC 요구 사항에 대한 자세한 내용은 "vSAN 확장된 클러스터 가이드" 를 참조하십시오.

대역폭 및 지연 시간 요구 사항

고성능 및 가용성을 보장하기 위해 vSAN 클러스터는 특정 대역폭 및 네트워크 지연 시간 요구 사항을 충족해야 합니다.

vSAN 확장된 클러스터의 기본 및 보조 사이트 간 대역폭 요구 사항은 vSAN 워크로드, 데이터의 양 및 장애를 처리하는 방법에 따라 다릅니다. 자세한 내용은 "VMware vSAN 디자인 및 크기 조정 가이드" 를 참조하십시오.

표 3-4. 대역폭 및 지연 시간 요구 사항

사이트 통신	대역폭	지연 시간
사이트 간	vSAN OSA: 최소 10Gbps vSAN ESA: 최소 10Gbps	5ms 미만 지연 시간 RTT
사이트에서 감시 기능	1000개 vSAN 구성 요소당 2Mbps	■ 사이트당 1개 호스트에 대해 500ms 미만 지연 시간 RTT ■ 사이트당 최대 10개 호스트에 대해 200ms 미만 지연 시간 RTT ■ 사이트당 11-15개 호스트에 대해 100ms 미만 지연 시간 RTT

계층 2 및 계층 3 지원

VMware는 서브넷을 공유하는 모든 vSAN 호스트 간에 계층 2 연결을 권장합니다.

vSAN은 vSAN 호스트 간에 라우팅된 계층 3 연결을 사용하는 배포도 지원합니다. 트래픽이 라우팅되는 동안 발생하는 홉 수와 추가 지연 시간을 고려해야 합니다.

표 3-5. 계층 2 및 계층 3 지원

클러스터 유형	L2 지원	L3 지원	고려 사항
하이브리드 클러스터	예	예	L2가 권장되고 L3이 지원됩니다.
플래시 전용 클러스터	예	예	L2가 권장되고 L3이 지원됩니다.
vSAN 확장된 클러스터 데이터	예	예	데이터 사이트 간에 L2와 L3이 모두 지원됩니다.
vSAN 확장된 클러스터 감시	아니요	예	L3이 지원됩니다. 데이터와 감시 사이트 간에 L2는 지원되지 않습니다.
2노드 vSAN 클러스터	예	예	데이터 사이트 간에 L2와 L3이 모두 지원됩니다.

라우팅 및 스위칭 요구 사항

vSAN 확장된 클러스터의 3개 사이트 모두는 관리 네트워크와 vSAN 네트워크를 통해 통신합니다. 모든 데이터 사이트의 VM은 공통 가상 시스템 네트워크를 통해 통신합니다.

다음은 vSAN 확장된 클러스터 라우팅 요구 사항입니다.

표 3-6. 라우팅 요구 사항

사이트 통신	배포 모델	계층	라우팅
사이트 간	기본값	계층 2	필요하지 않음
사이트 간	기본값	계층 3	정적 경로 또는 게이트웨이 재정의를 사용합니다.
사이트에서 감시 기능	기본값	계층 3	정적 경로 또는 게이트웨이 재정의를 사용합니다.
사이트에서 감시 기능	감시 트래픽 분리	계층 3	관리(vmk0) 인터페이스 이외의 인터페이스를 사용하는 경우 정적 경로 또는 게이트웨이 재정의를 사용합니다.
사이트에서 감시 기능	감시 트래픽 분리	2개 호스트 클러스터에 대한 계층 2	정적 경로는 필수가 아닙니다.

가상 스위치 요구 사항

vSphere Standard Switch 또는 vSphere Distributed Switch 중 하나를 사용하여 vSAN 네트워크를 생성할 수 있습니다. 분산 스위치를 사용하여 vSAN 트래픽의 대역폭 우선 순위를 지정합니다. vSAN은 모든 vCenter Server 버전에서 분산 스위치를 사용합니다.

다음 표에서는 표준 스위치와 분산 스위치의 장점과 이점을 비교합니다.

표 3-7. 가상 스위치 유형

설계 요구 사항	옵션 1 - vSphere Distributed Switch	옵션 2 - vSphere Standard Switch	설명
가용성	영향 없음	영향 없음	두 옵션 중 하나를 사용할 수 있습니다.
관리 용이성	긍정적인 영향	부정적인 영향	분산 스위치는 각 호스트에서 개별적으로 관리되는 표준 스위치와 달리, 모든 호스트에서 중앙 집중식으로 관리됩니다.
성능	긍정적인 영향	부정적인 영향	분산 스위치에는 vSAN 트래픽의 성능을 보장하는 데 사용할 수 있는 Network I/O Control과 같은 컨트롤이 추가되었습니다.
복구 용이성	긍정적인 영향	부정적인 영향	분산 스위치 구성을 백업 및 복원할 수 있지만 표준 스위치에는 이 기능이 없습니다.
보안	긍정적인 영향	부정적인 영향	분산 스위치에는 트래픽을 보호하는 데 도움이 되는 기본 제공 보안 컨트롤이 추가되었습니다.

vSAN 네트워크 포트 요구 사항

vSAN 배포에는 액세스 및 서비스를 제공하기 위해 특정 네트워크 포트 및 설정이 필요합니다.

vSAN은 클러스터의 각 호스트에서 특정 포트를 통해 메시지를 전송합니다. 호스트 방화벽이 이러한 포트에서 트래픽을 허용하는지 확인하십시오. 지원되는 모든 vSAN 포트 및 프로토콜 목록은 https://ports.vmware.com/에서 VMware Ports and Protocols 포털을 참조하십시오.

방화벽 고려 사항

클러스터에서 vSAN을 사용하도록 설정하면 모든 필수 포트가 ESXi 방화벽 규칙에 추가되고 자동으로 구성됩니다. 관리자가 방화벽 포트를 열거나 모든 방화벽 서비스를 수동으로 사용하도록 설정할 필요는 없습니다.

수신 및 송신 연결에 대해 열려 있는 포트를 볼 수 있습니다. ESXi 호스트를 선택하고 **구성 > 보안 프로파일**을 클릭합니다.

네트워크 방화벽 요구 사항

네트워크 방화벽을 구성할 때는 배포하려는 vSAN 버전을 고려하십시오.

클러스터에서 vSAN을 사용하도록 설정하면 모든 필수 포트가 ESXi 방화벽 규칙에 추가되고 자동으로 구성됩니다. 방화벽 포트를 열거나 모든 방화벽 서비스를 수동으로 사용하도록 설정할 필요는 없습니다. ESXi 호스트 보안 프로파일(**구성 > 보안 프로파일**)에서 수신 및 송신 연결을 위한 열린 포트를 볼 수 있습니다.

vsanEncryption 방화벽 규칙

클러스터에서 vSAN 암호화를 사용하는 경우 호스트와 KMS 서버 간의 통신을 고려합니다.

vSAN 암호화를 사용하려면 외부 KMS(키 관리 서버)가 필요합니다. vCenter Server는 KMS에서 키 ID를 가져와 ESXi 호스트에 분산합니다. KMS 서버와 ESXi 호스트는 서로 직접 통신합니다. KMS 서버는 서로 다른 포트 번호를 사용할 수 있으므로 vsanEncryption 방화벽 규칙을 사용하면 각 vSAN 호스트와 KMS 서버 간의 통신을 단순화할 수 있습니다. 이를 통해 vSAN 호스트가 KMS 서버의 모든 포트(TCP 포트 0 ~ 65535)와 직접 통신할 수 있습니다.

호스트가 KMS 서버와의 통신을 설정하면 다음 작업이 발생합니다.

- KMS 서버 IP가 vsanEncryption 규칙에 추가되고 방화벽 규칙이 사용하도록 설정됩니다.
- 교환 중에 vSAN 노드와 KMS 서버 간의 통신이 설정됩니다.
- vSAN 노드와 KMS 서버 간의 통신이 끝난 후에 IP 주소가 vsanEncryption 규칙에서 제거되고, 방화벽 규칙이 다시 비활성화됩니다.

vSAN 호스트는 동일한 규칙을 사용하여 여러 KMS 호스트와 통신할 수 있습니다.

vSAN 네트워크에서 유니캐스트 사용

4

유니캐스트 트래픽은 네트워크의 한 지점에서 다른 지점으로 일대일로 전송하는 것을 말합니다. vSAN 버전 6.6 이상에서는 유니캐스트를 사용하여 네트워크 설계 및 배포를 간소화합니다.

모든 ESXi 호스트는 유니캐스트 트래픽을 사용하고 vCenter Server는 클러스터 멤버 자격의 소스가 됩니다. vSAN 노드는 vCenter에서 제공하는 최신 호스트 멤버 자격 목록으로 자동 업데이트됩니다. vSAN은 CMMDS 업데이트를 위해 유니캐스트를 사용하여 통신합니다.

vSAN 버전 6.6의 이전 릴리스에서는 하트비트를 사용하도록 설정하고 클러스터 내의 호스트 간에 메타데이터를 교환하기 위해 멀티캐스트에 의존했습니다. vSAN 클러스터의 일부 호스트가 이전 버전의 소프트웨어를 실행 중이라면 여전히 멀티캐스트 네트워크가 필요합니다. 멀티캐스트에서 유니캐스트 네트워크로 전환하면 성능 및 네트워크 지원이 향상됩니다. 멀티캐스트에 대한 자세한 내용은 장 13 vSAN 네트워크에서 멀티캐스트 사용을 참조하십시오.

다음으로 아래 항목을 읽으십시오.

- 버전 5 이전 디스크 그룹 동작
- 버전 5 디스크 그룹 동작
- 유니캐스트 네트워크의 DHCP 지원
- 유니캐스트 네트워크의 IPv6 지원
- ESXCLI로 유니캐스트 쿼리
- 클러스터 내 트래픽

버전 5 이전 디스크 그룹 동작

vSAN 버전 6.6 디스크 그룹의 단일 버전 5 디스크 그룹이 있으면 클러스터가 유니캐스트 모드에서 영구적으로 통신하도록 트리거됩니다.

vSAN 버전 6.6 클러스터는 다음과 같은 경우에 자동으로 멀티캐스트 통신으로 전환됩니다.

- 모든 클러스터 호스트에서 vSAN 버전 6.5 이하가 실행되고 있습니다.
- 모든 디스크 그룹이 온디스크 3 이하 버전을 사용하고 있습니다.
- vSAN 6.2 또는 vSAN 6.5 같은 비 vSAN 6.6 호스트가 클러스터에 추가되었습니다.

예를 들어, vSAN 6.5 이전 버전을 실행하는 호스트를 기존 vSAN 6.6 클러스터에 추가하면 클러스터는 멀티캐스트 모드로 되돌아가고 6.5 호스트를 유효한 노드로 포함합니다. 이 동작을 피하려면 ESXi 호스트 및 온디스크 형식 모두에 대해 최신 버전을 사용하십시오. vSAN 클러스터가 계속해서 유니캐스트 모드로 통신하고 멀티캐스트로 복귀되지 않도록 하려면 vSAN 6.6 호스트의 디스크 그룹을 온디스크 버전 5.0으로 업그레이드하십시오.

참고 vSAN 버전 6.6 이상과 함께 동일한 클러스터에서 vSAN 버전 6.5 이하를 사용할 수 있는 혼합 모드 클러스터를 사용하지 마십시오.

버전 5 디스크 그룹 동작

vSAN 버전 6.6 클러스터의 단일 버전 5 디스크 그룹이 있으면 클러스터가 유니캐스트 모드에서 영구적으로 통신하도록 트리거됩니다.

vSAN 6.6 클러스터가 이미 온디스크 버전 5를 사용하고 있고 vSAN 6.5 노드가 클러스터에 추가된 환경에서는 다음 이벤트가 발생합니다.

- vSAN 6.5 노드는 자체 네트워크 파티션을 형성합니다.
- vSAN 6.5 노드는 계속 멀티캐스트 모드에서 통신하지만 유니캐스트 모드를 사용하는 vSAN 6.6 노드와는 통신할 수 없습니다.

온디스크 형식에는 하나의 노드가 이전 버전이라는 클러스터 요약 경고가 표시됩니다. 노드를 최신 버전으로 업그레이드할 수 있습니다. 클러스터가 혼합 모드일 때는 디스크 형식 버전을 업그레이드할 수 없습니다.

유니캐스트 네트워크의 DHCP 지원

vSAN 6.6 클러스터에 배포된 vCenter Server는 예약 없이 DHCP(Dynamic Host Configuration Protocol)의 IP 주소를 사용할 수 있습니다.

할당된 IP 주소는 VMkernel 포트의 MAC 주소에 연결되기 때문에 예약과 함께 DHCP를 사용할 수 있습니다.

유니캐스트 네트워크의 IPv6 지원

vSAN 6.6은 유니캐스트 통신이 있는 IPv6를 지원합니다.

IPv6를 사용하면 링크 로컬 주소는 링크 로컬 접두사를 사용하는 모든 인터페이스에서 자동으로 구성됩니다. 기본적으로 vSAN은 노드의 링크 로컬 주소를 다른 인접 클러스터 노드에 추가하지 않습니다. 따라서 vSAN 6.6은 유니캐스트 통신을 위해 IPv6 링크 로컬 주소를 지원하지 않습니다.

ESXCLI로 유니캐스트 쿼리

ESXCLI 명령을 실행하여 유니캐스트 구성을 확인할 수 있습니다.

통신 모드 보기

`esxcli vsan cluster get` 명령을 사용하여 vSAN 클러스터 노드의 CMMDS 모드(유니캐스트 또는 멀티캐스트)를 확인할 수 있습니다.

절차

- `esxcli vsan cluster get` 명령을 실행합니다.

결과

```
Cluster Information
  Enabled: true
  Current Local Time: 2020-04-09T18:19:52Z
  Local Node UUID: 5e8e3dc3-43ab-5452-795b-a03d6f88f022
  Local Node Type: NORMAL
  Local Node State: AGENT
  Local Node Health State: HEALTHY
  Sub-Cluster Master UUID: 5e8e3d3f-3015-9075-49b6-a03d6f88d426
  Sub-Cluster Backup UUID: 5e8e3daf-e5e0-ddb6-a523-a03d6f88dd4a
  Sub-Cluster UUID: 5282f9f3-d892-3748-de48-e2408dc34f72
  Sub-Cluster Membership Entry Revision: 11
  Sub_cluster Member Count: 5
  Sub-Cluster Member UUIDs: 5e8e3d3f-3015-9075-49b6-a03d6f88d426, 5e8e3daf-e5e0-ddb6-a523-
a03d6f88dd4a,
  5e8e3d73-6d1c-0b81-1305-a03d6f888d22, 5e8e3d33-5825-ee5c-013c-a03d6f88ea4c,
5e8e3dc3-43ab-5452-795b-a03d6f88f022
  Sub-Cluster Member HostNames: testbed-1.vmware.com, testbed2.vmware.com,
  testbed3.vmware.com, testbed4.vmware.com, testbed5.vmware.com
  Sub-Cluster Membership UUID: 0f438e5e-d400-1bb2-f4d1-a03d6f88d426
  유니캐스트 모드 사용: true
  Maintenance Mode State: OFF
  Config Generation: ed845022-5c08-48d0-aa1d-6b62c0022222 7 2020-04-08T22:44:14.889
```

vSAN 클러스터 호스트 확인

`esxcli vsan cluster unicastagent list` 명령을 사용하여 vSAN 클러스터 호스트가 유니캐스트 모드에서 작동하는지 확인합니다.

절차

- `esxcli vsan cluster unicastagent list` 명령을 실행합니다.

결과

```
NodeUuid                              IsWitness Supports Unicast IP Address  Port  Iface Name
Cert Thumbprint  SubClusterUuid
------------------------------------ --------- ---------------- ----------  ----- ----------
5e8e3d73-6d1c-0b81-1305-a03d6f888d22         0      true 10.198.95.10
12321
43:80:B7:A1:3F:D1:64:07:8C:58:01:2B:CE:A2:F5:DE:D6:B1:41:AB
5e8e3daf-e5e0-ddb6-a523-a03d6f88dd4a         0      true 10.198.94.240
12321
```

```
FE:39:D7:A5:EF:80:D6:41:CD:13:70:BD:88:2D:38:6C:A0:1D:36:69
5e8e3d3f-3015-9075-49b6-a03d6f88d426         0      true 10.198.94.244
12321
72:A3:80:36:F7:5D:8F:CE:B0:26:02:96:00:23:7D:8E:C5:8C:0B:E1
5e8e3d33-5825-ee5c-013c-a03d6f88ea4c         0      true 10.198.95.11
12321
5A:55:74:E8:5F:40:2F:2B:09:B5:42:29:FF:1C:95:41:AB:28:E0:57
```

출력에는 vSAN 노드 UUID, IPv4 주소, IPv6 주소, vSAN 노드가 통신하는 UDP 포트, 노드가 데이터 호스트(0)인지 또는 감시 호스트(1)인지가 포함됩니다. 이 출력을 사용하여 유니캐스트 모드에서 작동하는 vSAN 클러스터 노드를 식별하고 클러스터의 다른 호스트를 볼 수 있습니다. vCenter Server는 출력 목록을 유지합니다.

vSAN 네트워크 정보 보기

`esxcli vsan network list` 명령을 사용하여 vSAN이 통신, 유니캐스트 포트(12321) 및 vSAN 인터페이스와 연결된 트래픽 유형(vSAN 또는 감시)에 사용하는 VMkernel 인터페이스와 같은 vSAN 네트워크 정보를 볼 수 있습니다.

절차

- `esxcli vsan network list` 명령을 실행합니다.

결과

```
Interface
   VmkNic Name: vmk1
   IP Protocol: IP
   Interface UUID: e290be58-15fe-61e5-1043-246e962c24d0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: vsan
```

이 출력에는 멀티캐스트 정보도 표시됩니다.

클러스터 내 트래픽

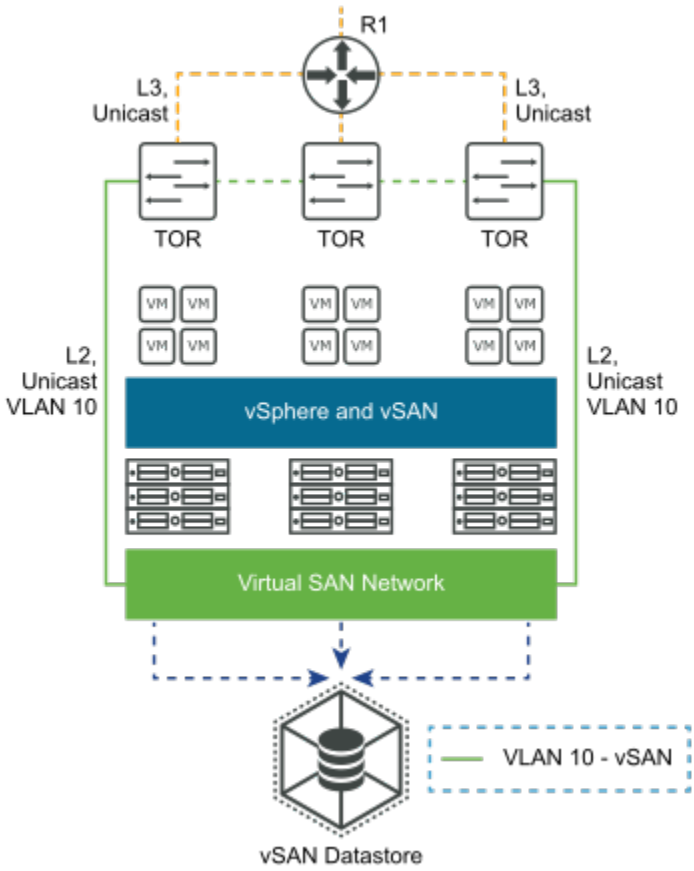
유니캐스트 모드에서 기본 노드는 클러스터의 모든 vSAN 노드에 동일한 메시지를 전송하므로 모든 클러스터 노드에 주소를 지정합니다.

예를 들어 N이 vSAN 노드의 개수인 경우 기본 노드는 메시지를 N번 전송합니다. 이로 인해 vSAN CMMDS 트래픽이 약간 증가합니다. 정상적인 안정된 상태의 작업 중에는 이러한 경미한 트래픽 증가를 알아채지 못할 수 있습니다.

단일 랙의 클러스터 내 트래픽

vSAN 클러스터의 모든 노드가 동일한 TOR(랙 상단) 스위치에 연결되어 있으면 기본 노드와 스위치 사이에서만 전체 트래픽이 증가합니다.

vSAN 클러스터가 2개 이상의 TOR 스위치에 걸쳐 있는 경우 스위치 간 트래픽이 확장됩니다. 많은 랙에 걸쳐 있는 클러스터에서 랙 인식을 위해 여러 TOR이 FD(장애 도메인)를 형성합니다. 기본 노드는 랙 또는 장애 도메인에 N개의 메시지를 전송합니다. 여기서 N은 각 장애 도메인의 호스트 수입니다.

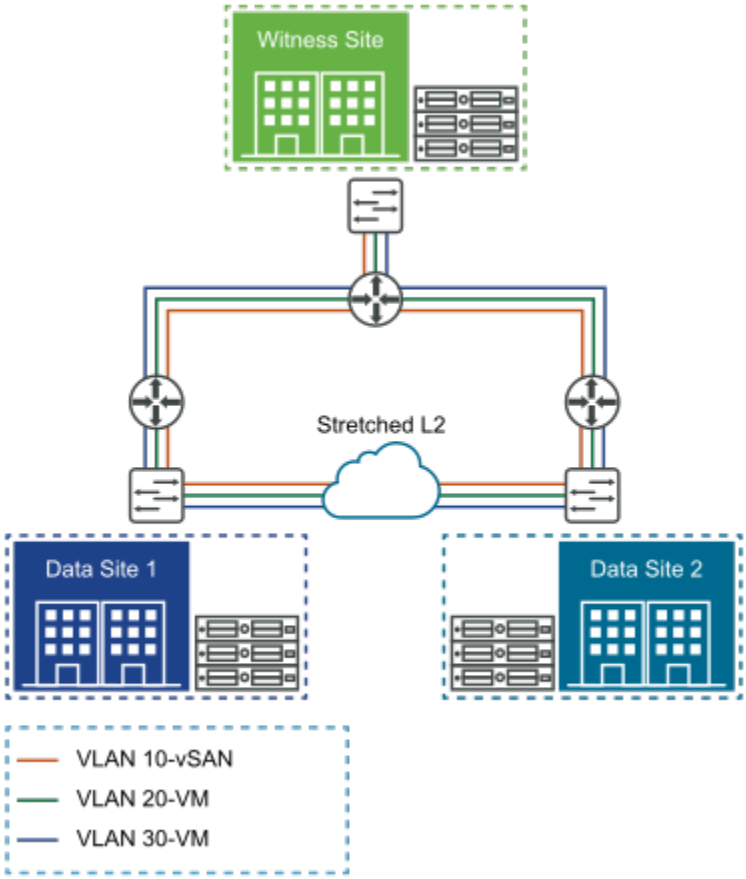


vSAN 확장된 클러스터의 클러스터 내 트래픽

vSAN 확장된 클러스터에서 기본 노드는 기본 사이트에 있습니다.

장애 도메인에서 CMMDS 데이터는 보조 사이트에서 기본 사이트로 전달되어야 합니다. vSAN 확장된 클러스터에서 트래픽을 계산하려면 보조 사이트의 노드 수, CMMDS 노드 크기(MB) 및 보조 사이트의 노드 수를 모두 곱해야 합니다.

vSAN 확장된 클러스터의 트래픽 = 보조 사이트의 노드 수 * CMMDS 노드 크기(MB) * 보조 사이트의 노드 수



유니캐스트 트래픽에도 감시 사이트 트래픽 요구 사항이 그대로 적용됩니다.

IP 네트워크 전송 구성

5

전송 프로토콜은 네트워크를 통해 통신 서비스를 제공합니다. 이러한 서비스에는 TCP/IP 스택 및 흐름 제어가 포함됩니다.

다음으로 아래 항목을 읽으십시오.

- vSphere TCP/IP 스택
- Object Missing
- IPv6 지원
- 정적 경로
- 점보 프레임

vSphere TCP/IP 스택

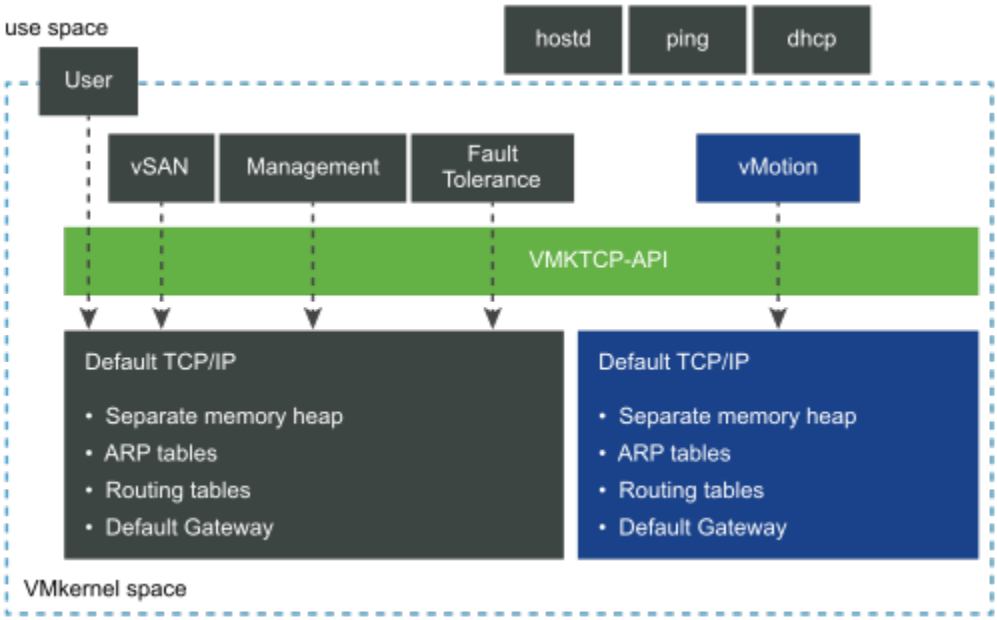
vSphere에는 vSAN 트래픽 서비스에 대한 전용 TCP/IP 스택이 포함되어 있지 않습니다. vSAN VMkernel 네트워크 인터페이스를 기본 TCP/IP 스택에 추가하고 vSAN 클러스터의 모든 호스트에 대한 고정 경로를 정의할 수 있습니다.

vSphere는 사용자 지정 vSAN TCP/IP 스택의 생성을 지원하지 않습니다. 계층 3 네트워크 토폴로지의 vSAN 트래픽이 vSAN VMkernel 네트워크 인터페이스를 통해 나가도록 보장할 수 있습니다. vSAN VMkernel 네트워크 인터페이스를 기본 TCP/IP 스택에 추가하고 vSAN 클러스터의 모든 호스트에 대한 고정 경로를 정의합니다.

참고 vSAN에는 자체 TCP/IP 스택이 없습니다. 고정 경로를 사용하여 L3 네트워크에서 vSAN 트래픽을 라우팅합니다.

vSphere 6.0에는 여러 TPC/IP 스택을 사용하여 다양한 VMkernel 네트워크 인터페이스를 관리할 수 있는 새로운 TCP/IP 스택 아키텍처가 도입되었습니다. 이 아키텍처를 사용하면 여러 기본 게이트웨이를 사용할 수 있는 분리된 TCP/IP 스택에서 vMotion, 관리 및 Fault Tolerance와 같은 트래픽 서비스를 구성할 수 있습니다.

네트워크 트래픽 분리 및 보안 요구 사항을 위해, 서로 다른 트래픽 서비스를 다른 네트워크 세그먼트 또는 VLAN에 배포합니다. 이렇게 하면 서로 다른 트래픽 서비스가 동일한 기본 게이트웨이를 통과하는 것을 방지할 수 있습니다.



별도 TCP/IP 스택에서 트래픽 서비스를 구성하는 경우 각 트래픽 서비스 유형을 자체 네트워크 세그먼트에 배포합니다. 네트워크 세그먼트는 VLAN이 세분된 물리적 네트워크 어댑터를 통해 액세스합니다. 각 세그먼트를 해당 트래픽 서비스를 사용하도록 설정한 다른 VMkernel 네트워크 인터페이스에 매핑합니다.

vSphere에서 사용 가능한 TCP/IP 스택

vSphere는 vSAN 트래픽 요구 사항을 지원하는 TCP/IP 스택을 제공합니다.

- **기본 TCP/IP 스택**. 호스트 관련 트래픽 서비스를 관리합니다. 이 스택에서는 구성된 모든 네트워크 서비스 간에 단일 기본 게이트웨이를 공유합니다.
- **vMotion TCP/IP 스택**. vMotion 트래픽을 자체 스택으로 격리합니다. 이 스택을 사용하면 기본 TCP/IP 스택에서 vMotion 트래픽이 완전히 제거되거나 비활성화됩니다.
- **프로비저닝 TPC/IP 스택**. 콜드 마이그레이션, 복제, 스냅샷 또는 NFC 트래픽과 같은 일부 가상 시스템 관련 작업을 분리합니다.
- **미러 TCP/IP 스택**. 포트 미러링 트래픽을 관리 트래픽과 분리합니다. 이 스택이 없으면 미러 트래픽은 기본 TCP/IP 스택에 바인딩됩니다.
- **운영 TCP/IP 스택**. vSphere 네트워크 흐름 데이터 수집에 대한 지원을 제공합니다.

VMkernel 인터페이스를 생성하는 동안 다른 TCP/IP 스택을 선택할 수 있습니다.

vSphere 트래픽 서비스에 대해 네트워크 격리 요구가 있는 환경에서는 동일한 기본 게이트웨이를 사용하여 트래픽을 보낼 수 없습니다. 다른 TCP/IP 스택을 사용하면 다른 기본 게이트웨이를 사용하고 고정 경로를 추가하지 않도록 할 수 있으므로 트래픽 분리를 간편하게 관리할 수 있습니다. vSAN 트래픽을 기본 게이트웨이를 통해 액세스할 수 없는 다른 네트워크로 라우팅해야 할 경우 이 방법을 사용합니다.

Object Missing

This object is not available in the repository.

IPv6 지원

vSAN 6.2 이상에서는 IPv6를 지원합니다.

vSAN은 다음 IP 버전을 지원합니다.

- IPv4
- IPv6(vSAN 6.2 이상)
- 혼합 IPv4/IPv6(vSAN 6.2 이상)

vSAN 6.2 이전 릴리스에서는 IPv4만 지원됩니다. vSAN 클러스터를 IPv4에서 IPv6로 마이그레이션할 때 혼합 모드를 사용합니다.

IPv6 멀티캐스트도 지원됩니다.

IPv6 사용에 대한 자세한 내용은 네트워크 벤더에 문의하십시오.

정적 경로

정적 경로를 사용하여 한 서브넷의 호스트에 있는 vSAN 네트워크 인터페이스가 다른 네트워크의 호스트에 도달하도록 허용할 수 있습니다.

대부분의 구성은 관리 네트워크에서 vSAN 네트워크를 분리하므로 vSAN 네트워크에는 기본 게이트웨이가 없습니다. L3 배포에서 서로 다른 서브넷 또는 서로 다른 L2 세그먼트에 있는 호스트는 일반적으로 관리 네트워크와 연결되는 기본 게이트웨이를 통해 서로 연결할 수 없습니다.

"정적 경로" 를 사용하여 한 서브넷에 있는 호스트의 vSAN 네트워크 인터페이스가 다른 네트워크의 호스트에 있는 vSAN 네트워크에 도달하도록 허용해야 합니다. 정적 경로는 기본 게이트웨이를 사용하는 대신, 인터페이스를 통해 특정 네트워크에 연결하는 방법을 호스트에 알려줍니다.

다음 예에서는 ESXi 호스트에 IPv4 정적 경로를 추가하는 방법을 보여 줍니다. 해당 게이트웨이를 통해 연결하려는 게이트웨이(-g) 및 네트워크(-n)를 지정합니다.

```
esxcli network ip route ipv4 add -g 172.16.10.253 -n 192.168.10.0/24
```

정적 경로가 추가되면 물리적 인프라에서 허용한다고 가정할 경우 모든 네트워크에서 vSAN 트래픽 연결을 사용할 수 있습니다. `vmkping` 명령을 실행하여 원격 네트워크의 IP 주소 또는 기본 게이트웨이를 ping함으로써 서로 다른 네트워크 간의 통신을 테스트하고 확인합니다. 다른 크기의 패킷을 확인하고(-s) 패킷 조각화를 방지(-d)할 수도 있습니다.

```
vmkping -I vmk3 192.168.10.253
```

점보 프레임

vSAN은 vSAN 네트워크의 점보 프레임을 완전히 지원합니다.

점보 프레임은 1500바이트 이상의 페이로드를 포함하는 이더넷 프레임입니다. 점보 프레임은 일반적으로 최대 9000바이트의 페이로드를 운반하지만 변형도 존재합니다.

점보 프레임을 사용하면 CPU 활용률을 줄이고 처리량을 높일 수 있습니다.

참고 성능 향상을 위해 vSAN Max 배포에 대해 점보 프레임 지원을 사용하도록 설정합니다.

이러한 이점이 네트워크 전체에서 점보 프레임을 구현할 때 발생하는 오버헤드보다 중요한지를 결정해야 합니다. 네트워크 인프라에서 점보 프레임을 이미 사용하도록 설정한 데이터 센터에서는 vSAN에 점보 프레임을 사용할 수 있습니다. 네트워크 전체에서 점보 프레임을 구성하는 데 드는 운영 비용은 CPU 제한 및 성능 혜택보다 클 수 있습니다.

vSAN에서 VMware NSX 사용

6

vSAN과 VMware NSX는 동일한 vSphere 인프라에 배포되고 공존할 수 있습니다.

NSX는 NSX 관리 VXLAN 또는 Geneve 오버레이를 통한 vSAN 데이터 네트워크의 구성을 지원하지 않습니다.

vSAN과 NSX는 호환됩니다. vSAN과 NSX는 기능, 리소스 및 서비스를 제공하기 위해 서로 종속되지 않습니다.

그러나 NSX 관리 VxLAN/Geneve 오버레이에 vSAN 네트워크 트래픽을 배치할 수 없습니다. NSX는 NSX 관리 VxLAN/Geneve 오버레이를 통한 vSAN 데이터 네트워크 트래픽의 구성을 지원하지 않습니다.

NSX 관리 VxLAN 오버레이를 통한 VMkernel 트래픽이 지원되지 않는 이유 중 하나는 VMkernel 네트워크와 지원되는 VxLAN 오버레이 간의 순환 종속성이 유지되지 못하기 때문입니다. NSX 관리 VxLAN 오버레이와 함께 제공되는 논리적 네트워크는 가상 시스템에서 사용되며 이로 인해 네트워크 이동성 및 유연성이 요구됩니다.

NSX에서 LACP/LAG를 구현하면 Cisco Nexus 환경에서 LAG를 vPC(가상 포트 채널)로 정의합니다.

정체 제어 및 흐름 제어 사용

7

흐름 제어를 사용하여 vSAN 네트워크에서 발신자와 수신자 간의 데이터 전송 속도를 관리합니다. 정체 제어는 네트워크의 정체를 처리합니다.

흐름 제어

흐름 제어를 사용하여 두 디바이스 간의 데이터 전송 속도를 관리할 수 있습니다.

물리적으로 연결된 두 디바이스가 자동 협상을 수행할 때 흐름 제어가 구성됩니다.

과도하게 트래픽이 발생하는 네트워크 노드는 지정된 기간에 발신자의 전송을 중지하기 위해 일시 중지 프레임을 보낼 수 있습니다. 스위치로 전송된 멀티캐스트 대상 주소가 있는 프레임은 스위치의 다른 모든 포트를 통해 전달됩니다. 일시 중지 프레임에는 다른 멀티캐스트 트래픽과 구분되는 특수한 멀티캐스트 대상 주소가 있습니다. 규격 스위치는 일시 중지 프레임을 전달하지 않습니다. 이 범위로 전송되는 프레임은 스위치 내에서만 작동합니다. 일시 중지 프레임은 기간이 제한되어 있으며, 시간 간격이 지나면 만료됩니다. 스위치를 통해 연결된 두 대의 컴퓨터는 서로에게 일시 중지 프레임을 절대 보내지 않지만 스위치에는 일시 중지 프레임을 보낼 수 있습니다.

일시 중지 프레임을 사용하는 한 가지 이유는 최대 속도 수신을 처리하기 위한 충분한 완충 능력이 없는 NIC(네트워크 인터페이스 컨트롤러)를 지원하기 위한 것입니다. 이 문제는 버스 속도와 메모리 크기가 개선된 경우에는 일반적이지 않습니다.

정체 제어

정체 제어는 네트워크의 트래픽을 제어하는 데 도움이 됩니다.

정체 제어는 주로 패킷 스위칭 네트워크에 적용됩니다. 스위치 내의 네트워크 정체는 오버로드된 스위치 간 링크로 인해 발생할 수 있습니다. 스위치 간 링크가 물리적 계층의 기능을 오버로드하는 경우 스위치는 자체 보호를 위해 일시 중지 프레임을 도입합니다.

우선 순위 흐름 제어

PFC(우선 순위 기반 흐름 제어)를 사용하면 정체 때문에 발생한 프레임 손실을 방지하는 데 도움이 됩니다.

우선 순위 기반 흐름 제어(IEEE 802.1Qbb)는 일시 중지 프레임과 유사한 메커니즘으로 구현되지만, 개별 우선 순위에 따라 작동합니다. PFC를 CBFC(클래스 기반 흐름 제어) 또는 PPP(우선 순위별 일시 중지)라고도 합니다.

흐름 제어 및 정체 제어

흐름 제어는 발신자와 수신자 간의 트래픽을 제어하는 종단 간 메커니즘입니다. 흐름 제어는 데이터 링크 계층과 전송 계층에서 발생합니다.

정체 제어는 네트워크에서 정체를 제어하는 데 사용됩니다. 이 문제는 버스 속도와 메모리 크기가 개선된 최신 네트워크에서는 자주 발생하지 않습니다. 스위치 내에서 네트워크가 정체될 시나리오의 가능성이 좀 더 높습니다. 정체 제어는 네트워크 계층 및 전송 계층에서 처리됩니다.

흐름 제어 설계 고려 사항

기본적으로 흐름 제어는 ESXi 호스트의 모든 네트워크 인터페이스에서 사용하도록 설정됩니다.

NIC의 흐름 제어 구성은 드라이버에 의해 수행됩니다. NIC의 네트워크 트래픽이 과도하게 발생하면 NIC는 일시 중지 프레임을 전송합니다.

일시 중지 프레임과 같은 흐름 제어 메커니즘은 vSAN 네트워크 계층의 지연 시간 증가로 인한 VM 게스트 I/O의 전반적인 지연을 트리거할 수 있습니다. 일부 네트워크 드라이버는 드라이버 내에서 흐름 제어 기능을 구성하는 모듈 옵션을 제공합니다. 일부 네트워크 드라이버를 사용하면 ESXi 호스트의 콘솔에서 `ethtool` 명령줄 유틸리티를 사용하여 구성 옵션을 수정할 수 있습니다. 지정된 드라이버의 구현 세부 정보에 따라 모듈 옵션 또는 `ethtool`을 사용합니다.

ESXi 호스트의 흐름 제어 구성에 대한 자세한 내용은 VMware KB 1013413을 참조하십시오.

1Gbps가 있는 배포에서는 ESXi 네트워크 인터페이스에서 흐름 제어를 사용하도록 설정합니다(기본값). 일시 중지 프레임이 문제인 경우에는 하드웨어 벤더 지원 또는 VMware 글로벌 지원 서비스와 함께 흐름 제어 비활성화를 신중하게 계획합니다.

수신자가 ESXi 호스트로 보내는 일시 중지 프레임의 존재 여부를 인식하는 방법을 보려면 장 12 vSAN 네트워크 문제 해결을 참조하십시오. 환경의 일시 중지 프레임 수는 일반적으로 조사해야 할 기본 네트워크 또는 전송 문제를 나타냅니다.

기본 NIC 팀 구성, 페일오버 및 로드 밸런싱

8

많은 vSAN 환경에서 어느 정도의 네트워크 이중화가 필요합니다.

NIC 팀 구성을 사용하여 네트워크 이중화를 달성할 수 있습니다. 고가용성 및 로드 밸런싱을 위해 둘 이상의 NIC(네트워크 어댑터)를 하나의 팀으로 구성할 수 있습니다. 기본 NIC 팀 구성은 vSphere 네트워킹에 사용할 수 있으며 이러한 기술은 vSAN 설계 및 아키텍처에 영향을 미칠 수 있습니다.

여러 NIC 팀 구성 옵션을 사용할 수 있습니다. 물리적 스위치 구성이 필요하거나 링크 집계와 같은 네트워킹 개념을 이해해야 하는 NIC 팀 구성 정책은 피합니다. 기본적이고 단순하고 안정적인 설정을 사용해야 최상의 결과를 얻을 수 있습니다.

NIC 팀 구성 옵션을 잘 모르는 경우 명시적 페일오버와 함께 활성/대기 구성을 사용하십시오.

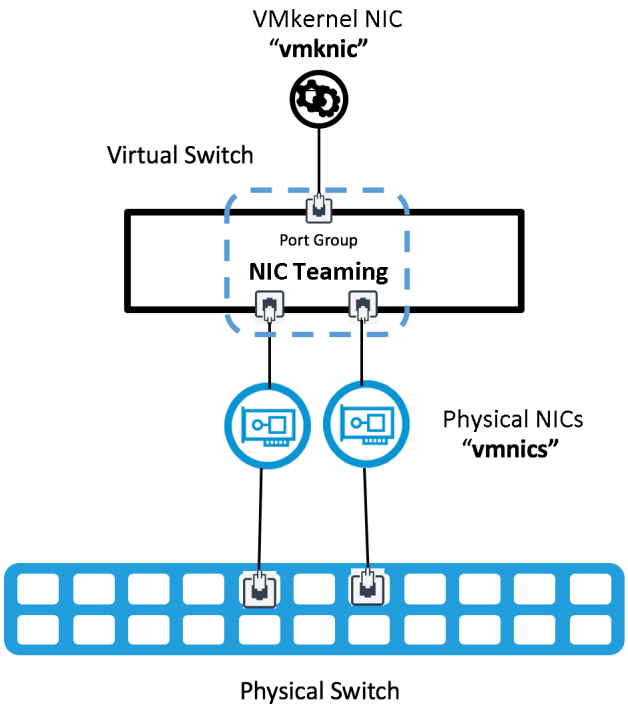
다음으로 아래 항목을 읽으십시오.

- 기본 NIC 팀 구성

기본 NIC 팀 구성

기본 NIC 팀 구성에서는 여러 물리적 업링크, 하나의 vmknic 및 단일 스위치를 사용합니다.

vSphere NIC 팀 구성에서는 단일 가상 스위치와 연결된 vmnics라는 다중 업링크 어댑터를 사용하여 팀을 구성합니다. 이것은 가장 기본적인 옵션이며 vSphere Standard Switch나 vSphere Distributed Switch를 사용하여 구성할 수 있습니다.



페일오버 및 이중화

vSAN은 vSphere에서 제공하는 기본 NIC 팀 구성 및 페일오버 정책을 사용할 수 있습니다.

vSwitch의 NIC 팀 구성에는 여러 활성 업링크 또는 활성/대기 업링크 구성이 있을 수 있습니다. 기본 NIC 팀 구성에는 물리적 스위치 계층의 특별한 구성이 필요하지 않습니다.

참고 vSAN은 로드 밸런싱을 위해 NIC 팀 구성을 사용하지 않습니다.

일반적인 NIC 팀 구성에는 다음과 같은 설정이 있습니다. 분산 스위치로 작업하는 경우 vSAN 트래픽에 사용되는 분산 포트 그룹의 설정을 편집합니다.

- 로드 밸런싱: 기존 가상 포트를 기준으로 라우팅
- 네트워크 장애 감지: 링크 상태만
- 스위치 알림: 예
- 페일백: 예

vSAN 트래픽 로드 밸런싱

- 로드 밸런싱: 기존 가상 포트를 기준으로 라우팅
- 네트워크 장애 감지: 링크 상태만
- 스위치 알림: 예
- 페일백: 예

NIC 팀에 대한 로드 밸런싱 구성

NIC 팀 구성을 위해 몇 가지 로드 밸런싱 기술을 사용할 수 있으며 각 기술에는 장단점이 있습니다.

기존 가상 포트 기준 라우팅

활성/활성 또는 활성/수동 구성에서는 기본 NIC 팀 구성을 위해 **기존 가상 포트 기준 라우팅**을 사용합니다. 이 정책이 적용되면 VMkernel 포트마다 하나의 물리적 NIC만 사용됩니다.

장점

- 물리적 스위치 구성을 최소화해야 하는 가장 간단한 NIC 팀 구성 방법입니다.
- 이 방법을 사용하려면 vSAN 트래픽에 단일 포트만 필요하므로 문제 해결이 간단해집니다.

단점

- 단일 VMkernel 인터페이스는 하나의 물리적 NIC 대역폭으로 제한됩니다. 일반적인 vSAN 환경에서는 하나의 VMkernel 어댑터를 사용하므로 팀에서 물리적 NIC가 하나만 사용됩니다.

물리적 NIC 로드 기준 라우팅

물리적 NIC 로드 기준 라우팅은 **기존 가상 포트 기준 라우팅**을 기준으로 하여 가상 스위치가 업링크의 실제 로드를 모니터링하고 오버로드된 업링크에서 로드를 줄이는 단계를 수행합니다. 이 로드 밸런싱 방법은 vSphere Standard Switch가 아닌 vSphere Distributed Switch에서만 사용할 수 있습니다.

이 Distributed Switch는 NIC 팀의 포트 ID 및 업링크 수를 사용하여 각 VMKernel 포트에 대한 업링크를 계산합니다. 이 Distributed Switch는 30초마다 업링크를 검사하고 로드가 75퍼센트를 초과하는 경우 가장 높은 I/O를 가진 VMkernel 포트의 포트 ID를 다른 업링크로 이동합니다.

장점

- 물리적 스위치 구성이 필요하지 않습니다.
- vSAN에 하나의 VMkernel 포트가 있지만, 다른 VMkernel 포트 또는 네트워크 서비스가 동일한 업링크를 공유할 수 있습니다. vSAN은 vMotion 또는 관리 등의 다른 경쟁 서비스의 다른 업링크를 사용할 수 있습니다.

단점

- vSAN에는 일반적으로 VMkernel 포트가 하나만 구성되어 있으므로 효율성이 제한됩니다.
- ESXi VMkernel은 각 시간 간격 후에 트래픽 로드를 다시 평가하므로 처리 오버헤드가 발생할 수 있습니다.

설정: 네트워크 장애 감지

기본 설정인 **링크 상태만**을 사용합니다. 링크 장애 감지를 위해 비콘 검색을 사용하지 마십시오. 분할 브레인 시나리오를 피하려면 비콘 검색을 위해 3개 이상의 물리적 NIC가 필요합니다. 자세한 내용은 VMware KB 1005577을 참조하십시오.

설정: 스위치 알림

기본 설정인 **예**를 사용합니다. 물리적 스위치는 각 MAC 주소를 물리적 스위치 포트에 연결하기 위한 MAC 주소 전달 테이블을 포함합니다. 프레임이 들어오면 스위치는 테이블에서 대상 MAC 주소를 확인하고 올바른 물리적 포트를 결정합니다.

NIC 페일오버가 발생하는 경우 ESXi 호스트는 변경된 사항이 있다는 사실을 네트워크 스위치에 알려야 합니다. 그렇지 않으면 물리적 스위치는 계속 이전 정보를 사용하고 프레임을 잘못된 포트로 보낼 수 있습니다.

스위치 알림을 **예**로 설정한 상태에서 한 물리적 NIC가 실패하고 트래픽이 팀의 다른 물리적 NIC로 재라우팅되는 경우 가상 스위치가 네트워크를 통해 알림을 전송하여 물리적 스위치의 조회 테이블을 업데이트합니다.

이 설정은 VLAN 구성 오류 또는 네트워크에서 추가적인 업스트림을 발생하게 되는 업링크 손실을 찾아내지 않습니다. vSAN 네트워크 파티션 상태 점검은 이러한 문제를 감지할 수 있습니다.

설정: 페일백

이 옵션은 물리적 어댑터가 고장을 복구한 후에 어떻게 실행 상태로 돌아가는지를 결정합니다. 페일오버 이벤트는 네트워크 트래픽이 NIC 간에 이동되도록 트리거합니다. 기존 NIC에서 **링크 실행 중** 상태가 감지되면 페일백이 **예**로 설정된 경우 트래픽이 자동으로 기존 네트워크 어댑터로 되돌아갑니다. 페일백을 **아니요**로 설정한 경우 수동 페일백이 필요합니다.

경우에 따라 페일백을 **아니요**로 설정하는 것이 유용할 수 있습니다. 예를 들어 물리적 스위치 포트가 장애로부터 복구되면 포트는 활성 상태일 수 있지만, 트래픽을 전달하기 시작하는 데 몇 초 정도 걸릴 수 있습니다. 자동 페일백은 Spanning Tree Protocol을 사용하는 특정 환경에서 문제를 발생시키는 것으로 알려졌습니다. STP(Spanning Tree Protocol)에 대한 자세한 내용은 VMware KB 1003804를 참조하십시오.

페일오버 순서 설정

페일오버 순서는 정상 작업 동안 활성 상태인 링크와 페일오버 이벤트 시 활성 상태인 링크를 결정합니다. vSAN 네트워크에 대해 지원되는 구성이 다를 수 있습니다.

활성/대기 업링크: 활성/대기 설정에서 장애가 발생하면 NIC 드라이버가 업링크 1에서 링크 종료 이벤트를 vSphere에 알립니다. 대기 업링크 2가 활성화되고 업링크 2에서 트래픽이 재개됩니다.

활성/활성 업링크: 페일오버 순서를 활성/활성으로 설정한 경우 vSAN 트래픽에 사용되는 가상 포트는 동시에 두 개의 물리적 포트를 모두 사용할 수는 없습니다.

업링크 1 및 업링크 2 둘 다의 NIC 팀 구성이 활성 상태이면 대기 업링크가 활성 상태일 필요는 없습니다.

참고 활성/활성 구성을 사용하는 경우 페일백이 **아니요**로 설정되어 있는지 확인합니다. 자세한 내용은 VMware 기술 자료 문서 2072928을 참조하십시오.

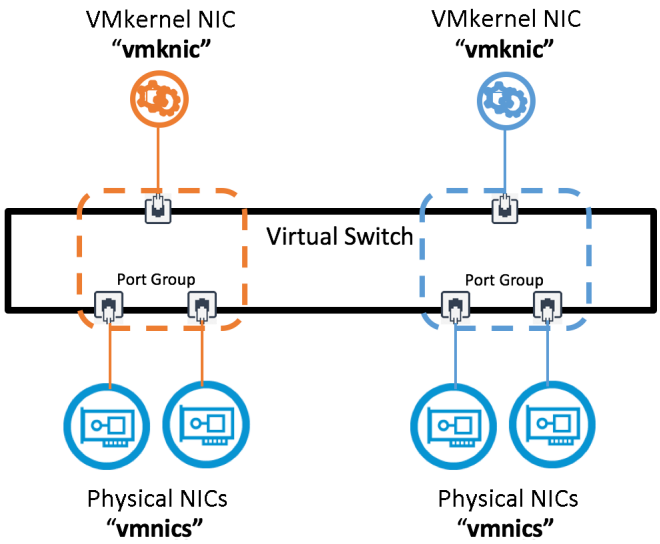
고급 NIC 팀 구성

9

다중 VMkernel 어댑터와 함께 고급 NIC 팀 구성 방법을 사용하여 vSAN 네트워크를 구성할 수 있습니다. LAG/LACP(Link Aggregation Protocol)를 사용하는 경우 단일 VMkernel 어댑터를 사용하여 vSAN 네트워크를 구성할 수 있습니다.

고급 NIC 팀 구성을 사용하여 에어갭을 구현할 수 있으므로 한 네트워크 경로에서 발생한 장애가 다른 네트워크 경로에 영향을 주지 않습니다. 한 네트워크 경로의 일부에 장애가 발생하면 다른 네트워크 경로를 통해 트래픽을 전달할 수 있습니다. 이를 위해 다른 VLAN 또는 별도의 물리적 네트워크 패브릭과 같이 서로 다른 서브넷에서 vSAN용 VMkernel NIC를 여러 개 구성합니다.

vSphere 및 vSAN은 동일한 서브넷에 있는 여러 VMkernel 어댑터(vmknic)를 지원하지 않습니다. 자세한 내용은 VMware KB 2010877을 참조하십시오.



다음으로 아래 항목을 읽으십시오.

- 링크 집계 그룹 개요
- 네트워크 에어갭 이해
- vSAN에서 에어갭 네트워크 구성을 사용할 때의 장단점

링크 집계 그룹 개요

LACP 프로토콜을 사용하면 네트워크 디바이스는 LACP 패킷을 피어로 보내 링크의 자동 번들을 협상할 수 있습니다.

LAG(링크 집계 그룹)는 IEEE 802.1AX-2008 표준에 따라 정의됩니다. 이 표준에 따르면 링크 집계를 통해 하나 이상의 링크를 함께 집계하여 링크 집계 그룹을 형성할 수 있습니다.

LACP를 통해 LAG 형성을 협상하여 LAG를 고정(수동) 또는 동적으로 구성할 수 있습니다. LACP는 다음과 같이 구성할 수 있습니다.

활성

포트가 작동하면 디바이스에서 즉시 LACP 메시지를 전송합니다. LACP가 사용되도록 설정된 최종 디바이스(예: ESXi 호스트 및 물리적 스위치)는 LACP 메시지라는 프레임을 서로 주고받으며, LAG 생성을 협상합니다.

수동

디바이스는 포트가 수신된 LACP 메시지에만 응답하고 협상을 시작하지는 않는 수동 협상 상태로 포트를 유지합니다.

참고 호스트와 스위치가 둘 다 수동 모드에 있는 경우 연결을 트리거하는 활성 부분이 필요하기 때문에 LAG는 초기화되지 않습니다. 둘 중 적어도 하나는 활성 상태여야 합니다.

vSphere 5.5 이상 릴리스에서는 이 기능을 **향상된 LACP**라고 합니다. 이 기능은 vSphere Distributed Switch 버전 5.5 이상에서만 지원됩니다.

vSphere Distributed Switch의 LACP 지원에 대한 자세한 내용은 vSphere 6 네트워킹 설명서를 참조하십시오.

참고 사용할 수 있는 LAG 수는 기본 물리적 환경의 기능과 가상 네트워크의 토폴로지에 따라 다릅니다.

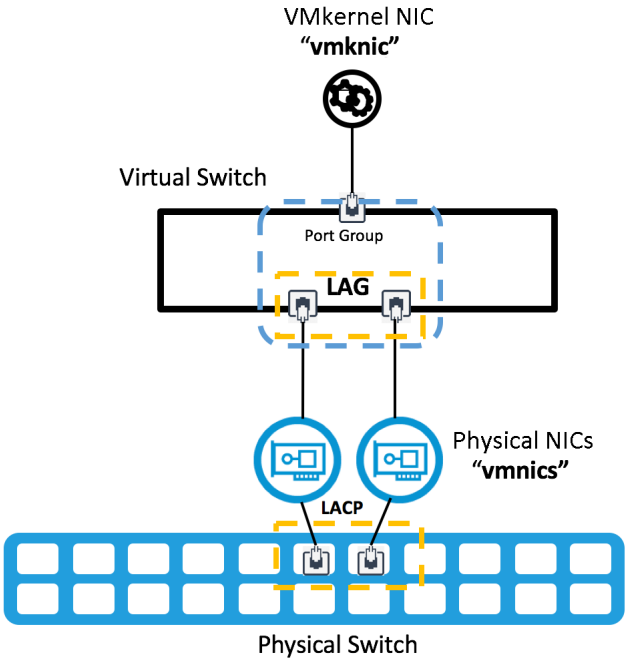
여러 다른 로드-밸런싱 옵션에 대한 자세한 내용은 KB 2051826 "" 을 참조하십시오.

고정 및 동적 링크 집계

LACP를 사용하여 여러 네트워크 연결을 결합하고 집계할 수 있습니다.

LACP가 **활성** 또는 **동적** 모드인 경우 물리적 스위치는 LACP 메시지를 ESXi 호스트와 같은 네트워크 디바이스로 보내 LAG(링크 집계 그룹) 생성을 협상합니다.

vSphere Standard Switch(및 5.5 이전 vSphere Distributed Switch)를 사용하여 호스트에서 링크 집계를 구성하려면 물리적 스위치에 고정 채널 그룹을 구성합니다. 자세한 내용은 벤더 설명서를 참조하십시오.



동적 링크 집계의 장단점

동적 링크 집계를 사용할 때 장단점을 검토하십시오.

장점

성능 및 대역폭이 개선됩니다. 한 vSAN 호스트 또는 VMkernel 포트가 여러 다른 로드 밸런싱 옵션을 사용하여 여러 다른 vSAN 호스트와 통신할 수 있습니다.

네트워크 어댑터 이중화를 제공합니다. NIC가 실패하고 링크 상태가 실패해도 팀의 나머지 NIC는 계속 트래픽을 전달합니다.

트래픽 밸런싱이 개선됩니다. 장애 이후에 트래픽 밸런싱이 빠르게 자동으로 수행됩니다.

단점

유연성이 저하됩니다. 물리적 스위치 구성을 사용하려면 포트 채널 구성에서 물리적 스위치 포트를 구성해야 합니다.

더 복잡해집니다. 완전한 물리적 이중화 구성을 생성하기 위해 여러 스위치를 사용하는 것은 복잡합니다. 벤더별 구현으로 인해 복잡성이 증가합니다.

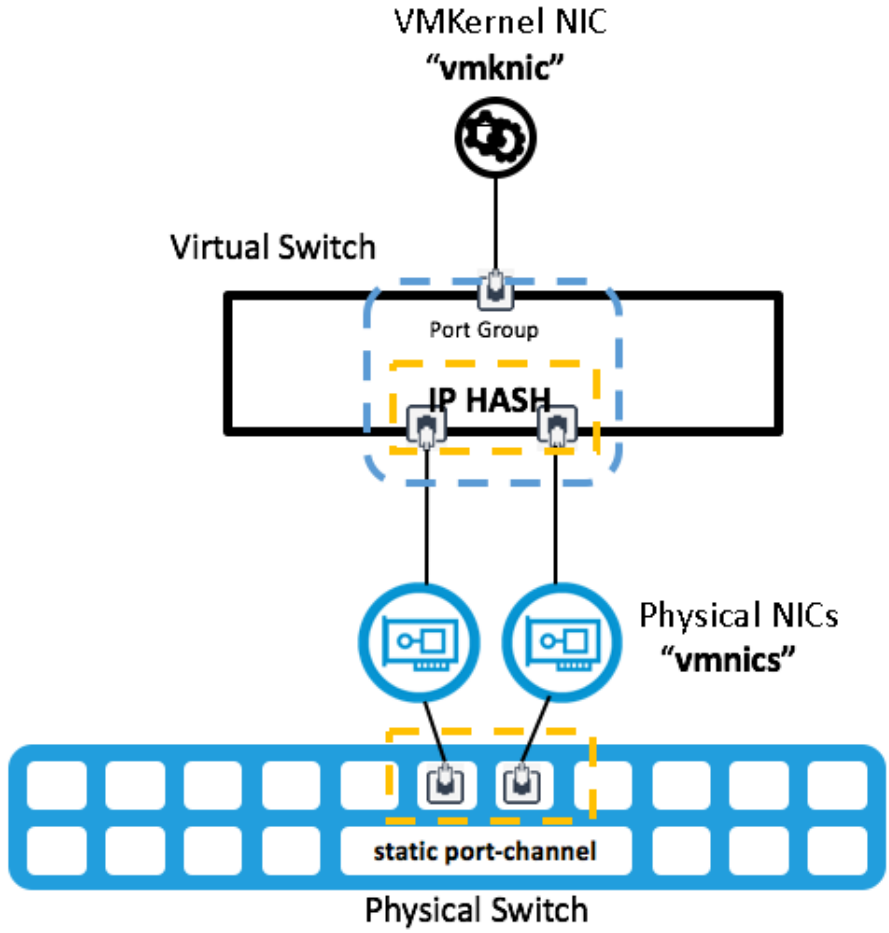
IP 해시 기준 라우팅을 사용하는 고정 LACP

IP 해시 정책에서 고정 LACP를 사용하여 vSAN 6.6 클러스터를 생성할 수 있습니다. 이 섹션에서는 vSphere Standard Switch를 중점적으로 다루지만, vSphere Distributed Switch를 사용할 수도 있습니다.

IP 해시 기준 라우팅 로드 밸런싱 정책을 사용할 수 있습니다.

vSwitch 또는 포트 그룹 수준의 **IP 해시 기준 라우팅** 로드 밸런싱 정책을 선택합니다. 고정 채널 그룹에 할당된 모든 업링크를 가상 스위치 또는 포트 그룹 수준의 팀 구성 및 페일오버 정책에 대한 활성 업링크 위치로 설정합니다.

IP 해시가 vSphere 포트 그룹에 구성된 경우 포트 그룹은 **IP 해시 기준 라우팅** 정책을 사용합니다. port-channel의 포트 수는 팀의 업링크 수와 동일해야 합니다.



IP 해시를 사용한 고정 LACP의 장단점

IP 해시와 함께 고정 LACP를 사용할 경우의 장단점을 고려하십시오.

장점

- **성능 및 대역폭이 개선됩니다**. 한 vSAN 호스트 또는 VMkernel 포트가 IP 해시 알고리즘을 사용하여 여러 다른 vSAN 호스트와 통신할 수 있습니다.
- **네트워크 어댑터 이중화를 제공합니다**. NIC가 실패하고 링크 상태가 실패해도 팀의 나머지 NIC는 계속 트래픽을 전달합니다.
- **유연성이 증가합니다**. vSphere Standard Switch 및 vSphere Distributed Switch 둘 다에서 IP 해시를 사용할 수 있습니다.

단점

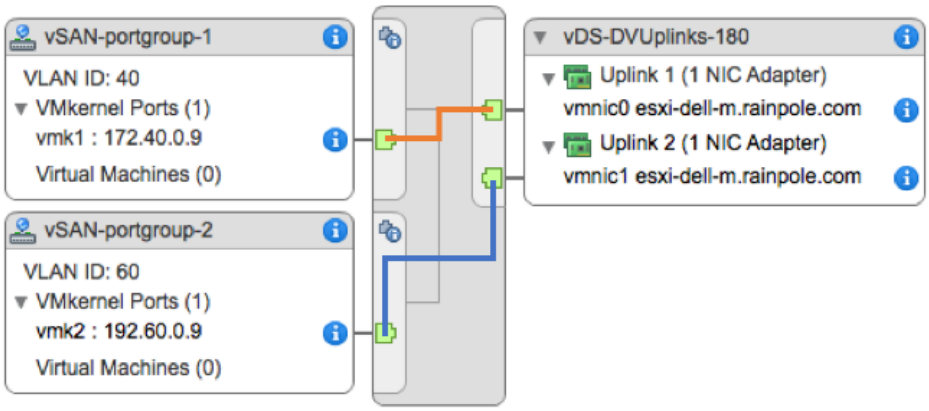
- **물리적 스위치 구성의 유연성이 저하됩니다**. 물리적 스위치 포트는 고정 포트-채널 구성으로 구성되어야 합니다.

- **구성 오류가 발생할 가능성이 커집니다**. 어느 한쪽에서도 확인 과정이 수행되지 않고 고정 포트-채널이 형성됩니다(LACP 동적 포트-채널과는 다름).
- **더 복잡해집니다**. 여러 개의 스위치를 사용할 경우 전체 물리적 이중화 구성을 도입하면 점점 복잡해집니다. 벤더별로 구현이 상당히 달라질 수 있습니다.
- **로드 밸런싱이 제한됩니다**. 환경에 소수의 IP 주소만 있는 경우에는 가상 스위치가 팀의 하나의 업링크를 통해 트래픽을 일관되게 전달할 수 있습니다. 소규모 vSAN 클러스터에서 특히 그렇습니다.

네트워크 에어갭 이해

고급 NIC 팀 구성 메서드를 사용하여 에어갭 스토리지 패브릭을 생성할 수 있습니다. 두 개의 스토리지 네트워크를 사용하여 각 스토리지 네트워크가 에어갭을 통해 물리적 및 논리적으로 다른 네트워크와 격리되는 중복 스토리지 네트워크 토폴로지를 생성합니다.

vSphere 환경에서 vSAN에 대한 네트워크 에어갭을 구성할 수 있습니다. vSAN 호스트별로 여러 VMkernel 포트를 구성합니다. 단일 vSwitch 또는 여러 가상 스위치(예: vSphere Standard Switch 또는 vSphere Distributed Switch)를 사용하여 각 VMkernel 포트를 전용 물리적 업링크에 연결합니다.



일반적으로 각 업링크는 완전히 중복된 물리적 인프라에 연결되어야 합니다.

이 토폴로지는 적절하지 않습니다. 동일한 네트워크에 있는 서로 다른 호스트의 NIC와 같은 구성 요소에서 장애가 발생하면 스토리지 I/O가 중단될 수 있습니다. 이 문제를 방지하려면 모든 호스트와 모든 네트워크 세그먼트에서 물리적 NIC 이중화를 구현합니다. 구성 예제 2에서는 이 토폴로지를 자세히 다룹니다.

이러한 구성은 유니캐스트 및 멀티캐스트 구성과 함께 L2 및 L3 토폴로지 둘 다에 적용됩니다.

vSAN에서 에어갭 네트워크 구성을 사용할 때의 장단점

네트워크 에어갭은 vSAN 트래픽을 분리하고 격리하는 데 유용할 수 있습니다. 이 토폴로지를 구성할 때는 주의하십시오.

장점

- vSAN 트래픽의 물리적 및 논리적 분리

단점

- vSAN은 동일한 서브넷에 있는 여러 VMkernel 어댑터(vmknics)를 지원하지 않습니다. 자세한 내용은 VMware 기술 자료 문서 2010877을 참조하십시오.
- 설치가 복잡하고 오류가 발생하기 쉬우므로 문제 해결이 더 복잡합니다.
- 한 호스트에서 하나의 NIC 장애가 발생하고 다른 호스트에서 다른 NIC 장애가 발생하는 경우와 같은 일부 비대칭 장애 상황에서 여러 vmknic를 사용하면 네트워크 가용성에 보장되지 않습니다.
- 물리적 NIC 간에 vSAN 트래픽 로드 밸런싱은 보장되지 않습니다.
- 여러 물리적 NIC(vmnics)를 보호하는 데 여러 VMkernel 어댑터(vmknic)가 필요할 수 있으므로 vSAN 호스트에 대한 비용이 증가합니다. 예를 들어 두 vSAN vmknic에 대해 이중화를 제공하려면 2x2 vmnic가 필요할 수 있습니다.
- VMkernel 포트, IP 주소 및 VLAN과 같은 필수 논리적 리소스는 2배가 됩니다.
- vSAN은 포트 바인딩을 구현하지 않습니다. 즉, 다중 경로 지정과 같은 기술을 사용할 수 없습니다.
- 계층 3 토폴로지는 vmknic가 여러 개인 vSAN 트래픽에 적합하지 않습니다. 이러한 토폴로지는 예상대로 작동하지 않을 수 있습니다.
- vSAN 멀티캐스트 주소를 변경하려면 명령줄 호스트 구성이 필요할 수 있습니다.

동적 LACP는 여러 네트워크 연결을 병렬로 결합하거나 집계하여 처리량을 늘리고 이중화를 제공합니다. LACP를 사용하여 NIC 팀 구성을 지정하면 여러 업링크에서 vSAN 네트워크의 로드 밸런싱이 발생합니다. 이 로드 밸런싱은 네트워크 계층에서 수행되며 vSAN을 통해 수행되지 않습니다.

참고 링크 집계를 설명하는 데 사용되는 다른 용어에는 포트 트렁킹, 링크 번들화, 이더넷/네트워크/NIC 결합, EtherChannel 등이 있습니다.

이 섹션에서는 LACP(Link Aggregation Control Protocol)를 중점적으로 다룹니다. IEEE 표준은 802.3ad이지만 일부 벤더에는 PAgP(Port Aggregation Protocol)와 같은 독점적인 LACP 기능이 있습니다. 벤더에서 권장하는 모범 사례를 따르십시오.

참고 vSphere Distributed Switch 5.1에 도입된 LACP 지원은 IP 해시 로드 밸런싱만 지원합니다. vSphere Distributed Switch 5.5 이상에서는 LACP를 완전히 지원합니다.

LACP는 포트 채널을 사용하는 업계 표준입니다. 많은 해싱 알고리즘을 사용할 수 있습니다. vSwitch 포트-그룹 정책 및 포트-채널 구성은 합의되고 일치되어야 합니다.

NIC 팀 구성 예

다음 NIC 팀 구성에서는 일반적인 vSAN 네트워킹 시나리오를 보여 줍니다.

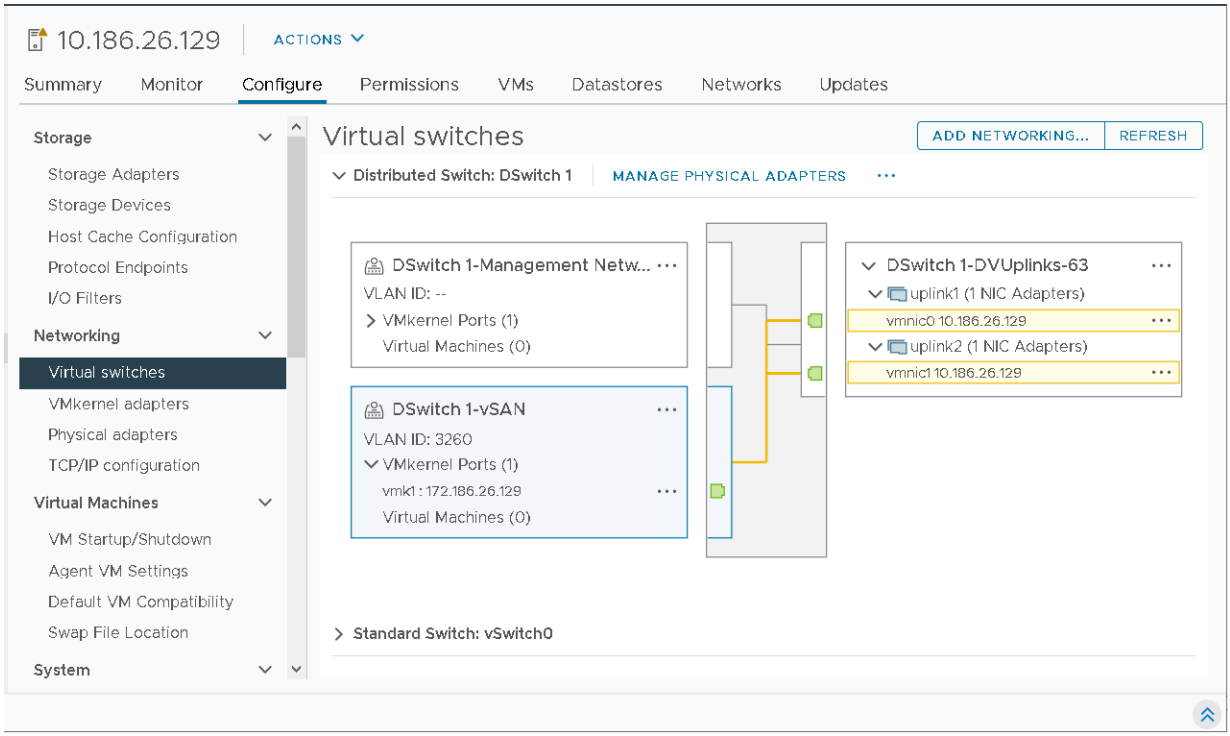
구성 1: 단일 vmknic, 물리적 NIC 로드 기준 라우팅

vSAN 호스트에 대해 **물리적 NIC 로드 기준 라우팅** 정책을 사용하여 기본 액티브/액티브 NIC 팀 구성을 지정할 수 있습니다. vDS(vSphere Distributed Switch)를 사용합니다.

이 예에서 vDS에는 각 호스트에 대해 두 개의 업링크가 구성되어야 합니다. 분산 포트 그룹은 vSAN 트래픽에 지정되고 특정 VLAN으로 분리됩니다. 점보 프레임은 MTU 값이 9000인 vDS에서 이미 사용하도록 설정되어 있습니다.

다음과 같이 vSAN 트래픽에서 분산 포트 그룹에 대한 팀 구성 및 페일오버를 구성합니다.

- 로드 밸런싱 정책을 **물리적 NIC 로드 기준 라우팅**으로 설정합니다.
- 네트워크 장애 감지를 **링크 상태만**으로 설정합니다.
- 스위치 알림을 **예**로 설정합니다.
- 페일백을 **아니요**로 설정합니다. 페일백을 **예**로 설정할 수 있지만 이 예에서는 그렇게 하지 않습니다.
- 두 업링크가 **활성 업링크** 위치에 있는지 확인합니다.



네트워크 업링크 이중화가 손실됨

링크 종료 상태가 감지되면 워크로드가 업링크 사이를 전환합니다. vSAN 클러스터 및 VM 워크로드에 미치는 명확한 영향은 없습니다.

복구 및 페일백

페일백을 **아니요**로 설정하면 트래픽이 기존 vmnic로 다시 승격되지 않습니다. **페일백**을 **예**로 설정하면 복구 시 트래픽이 기존 vmnic로 다시 승격됩니다.

로드 밸런싱

이것은 단일 VMkernel NIC이므로 **물리적 로드 기준 라우팅**을 사용해도 성능상의 이점은 없습니다.

한 번에 하나의 물리적 NIC만 사용됩니다. 다른 물리적 NIC는 유휴 상태입니다.

구성 2: 여러 vmknic, 기존 포트 ID 기준 라우팅

논리적 및 물리적으로 분리된 두 라우팅 불가능 VLAN을 사용하여 에어갭 토폴로지를 생성할 수 있습니다.

이 예에서는 vSphere Distributed Switch에 대한 구성 단계를 제공하지만 vSphere Standard Switch를 사용할 수도 있습니다. 2개의 10Gb의 물리적 NIC를 사용하고 이러한 NIC를 vSphere 네트워킹 계층에서 논리적으로 분리합니다.

각 vSAN VMkernel vmknic에 대해 두 개의 분산 포트 그룹을 생성합니다. 각 포트 그룹에는 별도의 VLAN 태그가 있습니다. vSAN VMkernel 구성의 경우 vSAN 트래픽에는 두 VLAN의 두 IP 주소가 필요합니다.

참고 실제 구현에서는 완전 이중화를 위해 일반적으로 4개의 물리적 업링크를 사용합니다.

각 포트 그룹에 대해 팀 구성 및 페일오버 정책이 기본 설정을 사용합니다.

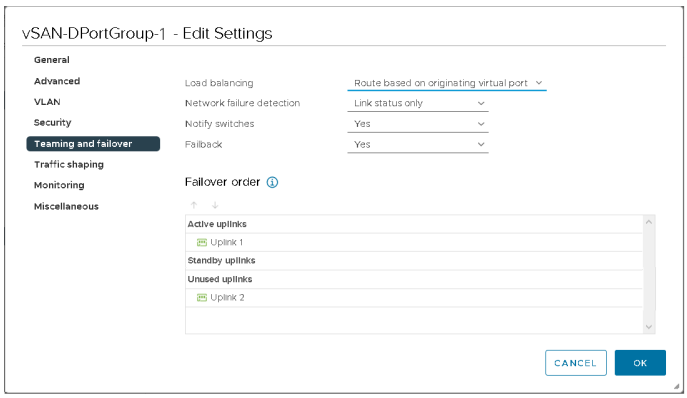
- 로드 밸런싱을 **기존 포트 ID 기준 라우팅**으로 설정합니다.
- 네트워크 장애 감지를 **링크 상태만**으로 설정합니다.
- 스위치 알림을 기본값인 **예**로 설정합니다.
- 페일백을 기본값인 **예**로 설정합니다.
- 업링크 구성에는 **활성** 위치의 업링크 1개와 **미사용** 위치의 업링크 1개가 있습니다.

한 네트워크가 다른 네트워크와 완전히 분리됩니다.

vSAN 포트 그룹 1

이 예에서는 **vSAN-DPortGroup-1**이라는 분산 포트 그룹을 사용합니다. 다음 팀 구성 및 페일오버 정책을 사용할 경우 이 포트 그룹에 **VLAN 3266**이 태그로 지정됩니다.

- VLAN 3266으로 태그가 지정된 포트 그룹의 트래픽
- 로드 밸런싱을 **기존 포트 ID 기준 라우팅**으로 설정합니다.
- 네트워크 장애 감지를 **링크 상태만**으로 설정합니다.
- 스위치 알림을 기본값인 **예**로 설정합니다.
- 페일백을 기본값인 **예**로 설정합니다.
- 업링크 구성에는 **활성** 위치의 **업링크 1**과 **미사용** 위치의 **업링크 2**가 있습니다.



vSAN 포트 그룹 2

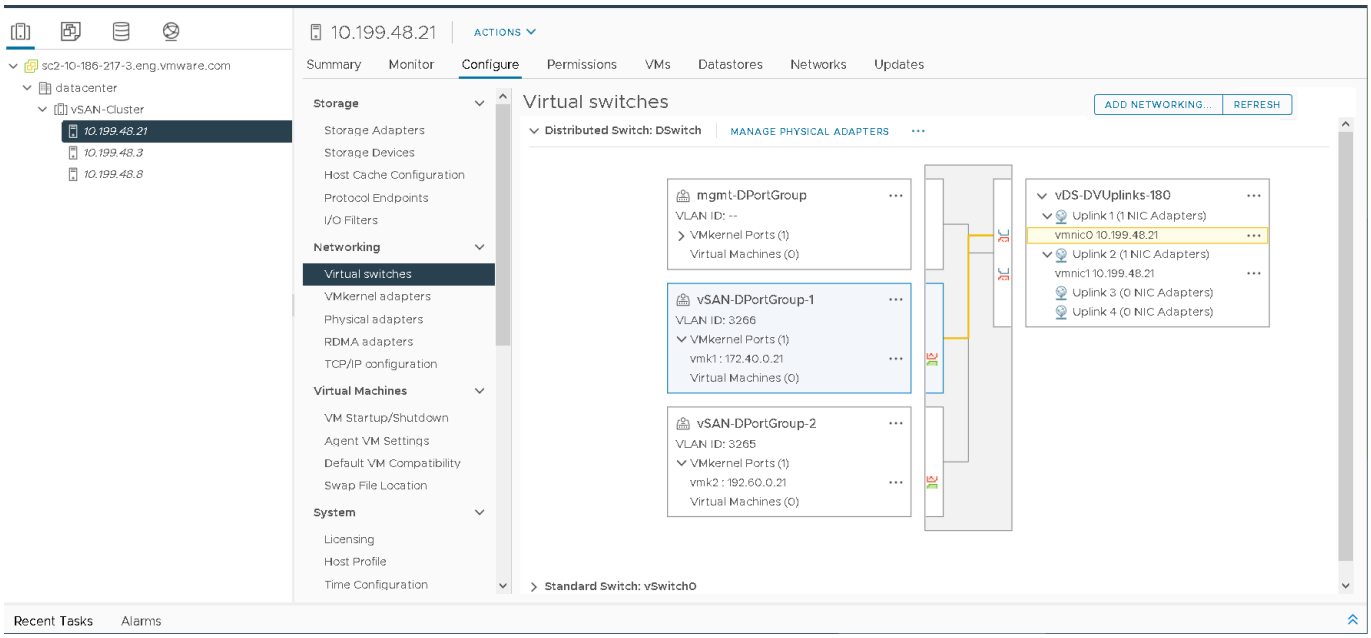
vSAN 포트 그룹 1을 보완하려면 다음과 같은 차이점을 적용하여 **vSAN-portgroup-2**라는 두 번째 분산 포트 그룹을 구성합니다..

- VLAN 3265으로 태그가 지정된 포트 그룹의 트래픽
- 업링크 구성에는 **활성** 위치의 **업링크 2**와 **미사용** " " 위치의 **업링크 1**가 있습니다.

vSAN VMkernel 포트 구성

2개의 vSAN VMkernel 인터페이스를 두 포트 그룹 모두에서 생성합니다. 이 예에서 포트 그룹의 이름은 **vmk1** 및 **vmk2**입니다.

- **vmk1**은 VLAN 3266(172.40.0.xx)과 연결되며, 결과 포트 그룹 **vSAN-DPortGroup-1**로 지정됩니다.
- **vmk2**는 VLAN 3265(192.60.0.xx)과 연결되며, 결과 포트 그룹 **vSAN-DPortGroup-2**로 지정됩니다.



로드 밸런싱

vSAN에는 여러 vmknic를 구분하는 로드 밸런싱 메커니즘이 없으므로 선택한 vSAN I/O 경로가 물리적 NIC에서 확정적이지 않습니다. vSphere 성능 차트는 하나의 물리적 NIC가 다른 NIC보다 더 많이 사용되는 것을 보여 줍니다. 4개 호스트의 전체 플래시 vSAN 클러스터에서 64K 블록 크기를 사용하며 읽기/쓰기 비율이 70:30인 120개 VM으로 랩에서 수행되는 간단한 I/O 테스트에 따르면 NIC 간의 불균형 로드가 확인되었습니다.

vSphere 성능 그래프는 NIC 간의 불균형 로드를 표시합니다.

네트워크 업링크 이중화가 손실됨

이 구성에 도입된 네트워크 장애를 고려하십시오. vmnic1이 지정된 vSAN 호스트에서 사용하지 않도록 설정되었습니다. 결과적으로 포트 **vmk2**가 영향을 받습니다. 실패한 NIC는 네트워크 연결 경보 및 이중화 경보를 둘 다 트리거합니다.

vSAN의 경우 이 페일오버 프로세스는 CMMDS(클러스터 모니터링, 멤버 자격 및 디렉토리 서비스)가 실패를 감지하고 약 **10초** 후에 트리거됩니다. 페일오버 및 복구 시 vSAN은 장애가 발생한 네트워크에서 모든 활성 연결을 중지하고 작동하는 나머지 네트워크에서 연결을 다시 설정하려고 시도합니다.

분리된 VLAN에서 두 개의 별도 vSAN VMkernel 포트가 통신하기 때문에 vSAN 상태 점검 실패가 트리거될 수 있습니다. **vmk2**가 더는 VLAN 3265에서 해당 피어와 통신할 수 없기 때문에 이러한 동작이 예상됩니다.

성능 차트는 vmnic1의 장애로 인해 영향을 받은 워크로드가 vmnic0에서 다시 시작되었음을 보여 줍니다. 이 테스트에서는 vSphere NIC 팀 구성과 이 토폴로지 간의 중요한 차이점을 보여 줍니다. vSAN은 나머지 네트워크에서 연결을 다시 설정하거나 다시 시작하려고 합니다.

그러나 일부 실패 시나리오에서 영향을 받은 연결 복구를 완료하려면 ESXi TCP 연결 시간 초과로 인해 최대 **90초**가 필요할 수 있습니다. 후속 연결 시도는 실패할 수 있지만 연결 시도는 5초 후에 시간 초과하고 가능한 모든 IP 주소를 순환합니다. 이 동작은 가상 시스템 게스트 I/O에 영향을 줄 수 있습니다. 따라서 애플리케이션 및 가상 시스템 I/O를 다시 시도해야 할 수 있습니다.

예를 들어 Windows Server 2012 VM에서 페일오버 및 복구 프로세스 중에 이벤트 ID 153(디바이스 재설정) 및 129(재시도 이벤트)가 기록될 수 있습니다. 이 예에서 이벤트 ID 129는 I/O가 복구될 때까지 약 90초 동안 로깅되었습니다.

일부 게스트 운영 체제의 디스크 시간 초과 설정을 수정하여 심각하게 영향을 받지 않도록 해야 할 수 있습니다. 디스크 시간 초과 값은 VMware Tools가 있는지와 특정 게스트 운영 체제 유형 및 버전에 따라 다를 수 있습니다. 게스트 운영 체제 디스크 시간 초과 값 변경에 대한 자세한 내용은 VMware KB 1009465로 이동하십시오.

복구 및 페일백

네트워크가 복구되면 다른 오류로 인해 워크로드가 강제로 발생하는 경우가 아니면 워크로드가 자동으로 재조정되지 않습니다. 영향을 받는 네트워크가 복구되는 즉시, 새 TCP 연결에 사용할 수 있게 됩니다.

구성 3: 동적 LACP

스위치에 2개 포트 LACP 포트 채널을 구성하고 vSphere Distributed Switch에 2개 업링크 링크 집계 그룹을 구성할 수 있습니다.

이 예에서는 서버당 2개의 물리적 업링크가 있는 10Gb 네트워킹을 사용합니다.

참고 RDMA를 통한 vSAN은 이 구성을 지원하지 않습니다.

네트워크 스위치 구성

다음 설정을 사용하여 vSphere Distributed Switch를 구성합니다.

- vSAN 호스트가 연결될 포트를 확인합니다.
- 포트 채널을 생성합니다.
- VLAN을 사용하는 경우 올바른 VLAN을 포트 채널로 다시 트렁크합니다.
- 원하는 배포 또는 로드 밸런싱 옵션(해시)을 구성합니다.
- LACP 모드를 활성/동적으로 설정합니다.
- MTU 구성을 확인합니다.

vSphere 구성

다음 설정을 사용하여 vSphere 네트워크를 구성합니다.

- 올바른 MTU를 사용하여 vDS를 구성합니다.
- vDS에 호스트를 추가합니다.
- 포트 채널에 대해 올바른 수의 업링크와 일치하는 특성을 사용하여 LAG를 생성합니다.
- 물리적 업링크를 LAG에 할당합니다.
- vSAN 트래픽에 대한 분산 포트 그룹을 생성하고 올바른 VLAN을 할당합니다.
- 올바른 MTU를 사용하여 vSAN에 대한 VMkernel 포트를 구성합니다.

물리적 스위치 설정

다음 설정을 사용하여 물리적 스위치를 구성합니다. Dell 서버에서 이 구성을 설정하는 방법에 대한 지침은 http://www.dell.com/Support/Article/kr/ko/19/HOW10364 "를 참조하십시오."

2개의 업링크 LAG를 구성합니다.

- 스위치 포트 36 및 18을 사용합니다.
- 이 구성은 VLAN 트렁킹을 사용하므로 포트 채널은 해당 VLAN이 트렁킹된 VLAN 트렁크 모드에 있습니다.
- 로드 밸런싱 또는 로드 배포에 **소스 및 대상 IP 주소, TCP/UDP 포트 및 VLAN** "" 방법을 사용합니다.
- LACP 모드가 활성 **활성**(동적)인지 확인합니다.

다음 명령을 사용하여 Dell 스위치에서 개별 포트 채널을 구성합니다.

- 포트 채널을 생성합니다.

```
#interface port-channel 1
```

- 포트-채널을 VLAN 트렁크 모드로 설정합니다.

```
#switchport mode trunk
```

- VLAN 액세스를 허용합니다.

```
#switchport trunk allowed vlan 3262
```

- 로드 밸런싱 옵션을 구성합니다.

```
#hashing-mode 6
```

- 포트-채널에 올바른 포트를 할당하고 모드를 활성으로 설정합니다.
- 포트 채널이 올바르게 구성되어 있는지 확인합니다.

```
#show interfaces port-channel 1


Channel Ports Ch-Type Hash Type Min-links Local Prf

------- ------------------------------ -------- --------- --------- ---------

Po1 Active: Te1/0/36, Te1/0/18 Dynamic 6 1 Disabled

Hash Algorithm Type

1 - Source MAC, VLAN, EtherType, source module and port Id

2 - Destination MAC, VLAN, EtherType, source module and port Id

3 - Source IP and source TCP/UDP port

4 - Destination IP and destination TCP/UDP port

5 - Source/Destination MAC, VLAN, EtherType, source MODID/port

6 - Source/Destination IP and source/destination TCP/UDP port

7 - Enhanced hashing mode
```

```
#interface range Te1/0/36, Te1/0/18

#channel-group 1 mode active
```

전체 구성:

```
#interface port-channel 1

#switchport mode trunk

#switchport trunk allowed vlan 3262

#hashing-mode 6

#exit

#interface range Te1/0/36,Te1/018
```

```
#channel-group 1 mode active

#show interfaces port-channel 1
```

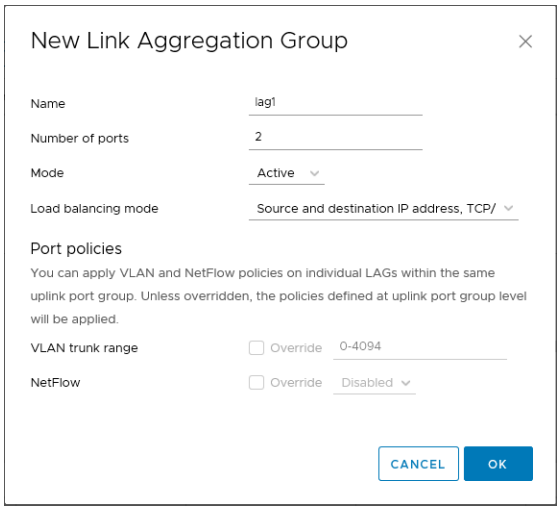
참고 vSAN 호스트에 연결된 모든 참여 스위치 포트에 대해 이 절차를 반복합니다.

vSphere Distributed Switch 설정

시작하기 전에 vDS가 LACP를 지원하는 버전으로 업그레이드되었는지 확인합니다. 확인하려면 vDS를 마우스 오른쪽 버튼으로 클릭하고 [업그레이드] 옵션을 사용할 수 있는지 확인합니다. LACP를 지원하는 버전으로 vDS를 업그레이드해야 할 수 있습니다.

vDS에서 LAG 생성

분산 스위치에 대해 LAG를 생성하려면 vDS를 선택하고 **구성** 탭을 클릭한 다음, **LACP**를 선택합니다. 새 LAG를 추가합니다.



다음 속성을 사용하여 LAG를 구성합니다.

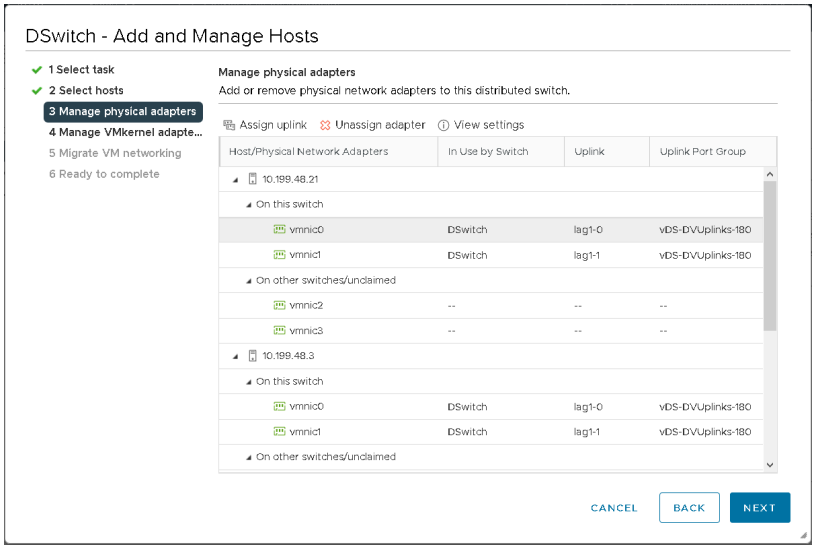
- LAG 이름: **lag1**
- 포트 수: **2**(스위치의 포트 채널과 일치하도록 지정)
- 모드: 물리적 스위치와 일치하도록 **활성**으로 지정합니다.
- 로드 밸런싱 모드: **소스 및 대상 IP 주소, TCP/UDP 포트 및 VLAN**

물리적 업링크를 LAG에 추가

vSAN 호스트가 vDS에 추가되었습니다. 개별 vmnic를 적절한 LAG 포트에 할당합니다.

- vDS를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리...**를 선택합니다.
- **호스트 네트워킹 관리**를 선택하고 연결된 호스트를 추가합니다.
- **물리적 어댑터 관리**에서 해당 어댑터를 선택하고 LAG 포트에 할당합니다.
- LAG1에서 업링크 1 위치의 vmnic0를 포트 0으로 마이그레이션합니다.

vmnic1에 대한 절차를 두 번째 LAG 포트 위치 lag1-1에 대해 반복합니다.



분산 포트 그룹 팀 구성 및 페일오버 정책 구성

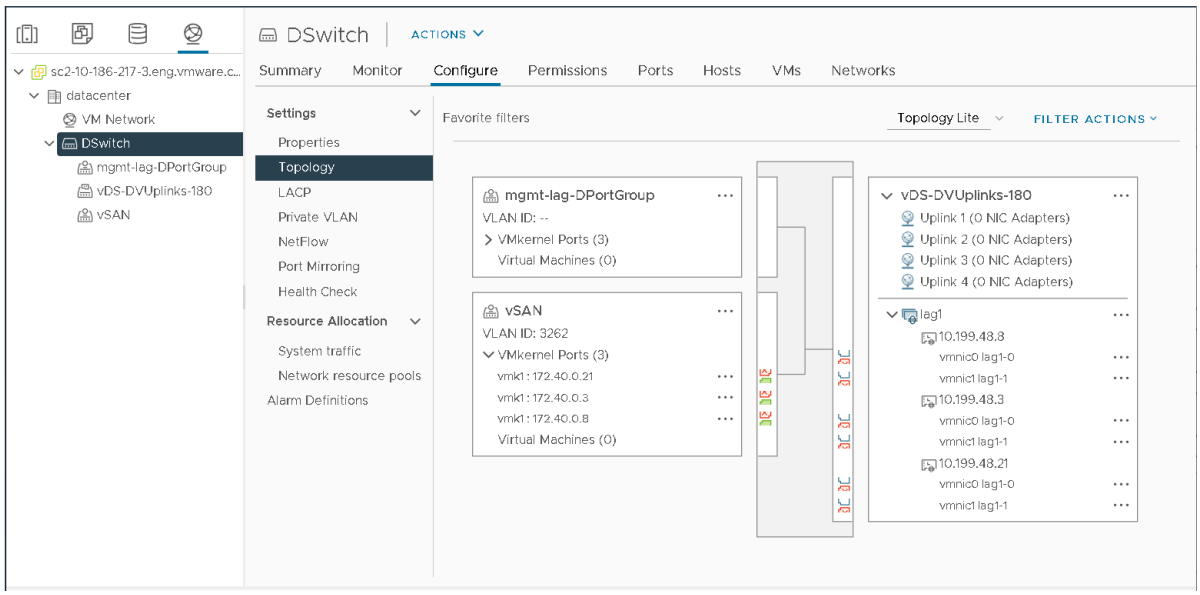
분산 포트 그룹 팀 구성 및 페일오버 정책에서 LAG 그룹을 **활성 업링크**로 할당합니다. vSAN 트래픽에 지정된 분산 포트 그룹을 선택하거나 생성합니다. 이 구성에서는 VLAN ID 3262 태그가 지정된 **vSAN**이라는 vSAN 포트 그룹을 사용합니다. 포트 그룹을 편집하고 새 LAG 구성을 반영하도록 팀 구성 및 페일오버 정책을 구성할 수 있습니다.

LAG 그룹 **lag1**이 활성 업링크 위치에 있는지 확인하고 남은 업링크가 **미사용** 위치에 있는지 확인합니다.

참고 LAG(링크 집계 그룹)가 유일한 활성 업링크로 선택되면 LAG의 로드 밸런싱 모드가 포트 그룹의 로드 밸런싱 모드를 재정의합니다. 따라서 **기존 가상 포트 기준 라우팅** 정책은 아무런 역할도 수행하지 않습니다.

VMkernel 인터페이스 생성

마지막 단계는 새 분산 포트 그룹을 사용하기 위한 VMkernel 인터페이스를 생성하여 vSAN 트래픽용으로 태그를 지정하는 것입니다. 각 vSAN vmknic가 LAG 그룹의 vmnic0 및 vmnic1을 통해 통신하여 로드 밸런싱 및 페일오버를 제공할 수 있는지 확인합니다.



로드 밸런싱 구성

로드 밸런싱 측면에서, 이 LAG 설정의 모든 vmnics에 있는 모든 호스트에서 트래픽이 일관되게 분산되지 않지만, 구성 1의 **물리적 NIC 로드 기준 라우팅**과 구성 2에서 사용되는 에어갭/다중 vmknic 방법과 비교하면 훨씬 더 일관됩니다.

개별 호스트의 vSphere 성능 그래프에 향상된 로드 밸런싱이 표시됩니다.

네트워크 업링크 이중화가 손실됨

지정된 vSAN 호스트에서 vmnic1이 사용하지 않도록 설정되면 네트워크 이중화 경보가 트리거됩니다.

vSAN 상태 경보는 트리거되지 않으며 게스트 I/O에 대한 영향은 에어갭이 적용된 다중 vmknic 구성과 비교할 때 최소로 유지됩니다. 이 구성에서 LACP가 구성된 모든 TCP 세션을 중지할 필요는 없습니다.

복구 및 페일백

페일백 시나리오에서는 vSAN 환경의 로드 기반 팀 구성, 다중 vmknic 및 LACP 사이에서 다른 동작을 보입니다. vmnic1이 복구된 이후 두 활성 업링크 모두에서 트래픽이 자동으로 분산됩니다. 이 동작은 vSAN 트래픽에 유용할 수 있습니다.

페일백을 예 또는 아니요 중 무엇으로 설정하시겠습니까?

LAG 로드 밸런싱 정책은 vSphere Distributed 포트 그룹에 대한 팀 구성 및 페일오버 정책을 재정의합니다. 또한 페일백 값에 대한 지침도 고려하십시오. 랩 테스트에 따르면 LACP를 사용하여 페일백을 **예** 또는 **아니요**로 설정하는 경우 명확한 동작 차이는 나타나지 않습니다. LAG 설정은 포트 그룹 설정보다 우선적으로 적용됩니다.

참고 LACP에서는 비콘 검색이 지원되지 않으므로 네트워크 장애 감지 값은 **링크 상태만**으로 유지됩니다. VMware KB IP 해시 로드 밸런싱 이해(2006129)를 참조하십시오.

구성 4: 고정 LACP – IP 해시 기준 라우팅

스위치에서 2 포트 LACP 고정 포트 채널을 사용하고 vSphere Standard Switch에서 2개의 활성 업링크를 사용할 수 있습니다.

이 구성에서는 서버당 2개의 물리적 업링크가 있는 10Gb 네트워킹을 사용합니다. 각 호스트에 vSAN에 대한 단일 VMkernel 인터페이스(vmknic)가 있습니다.

호스트 요구 사항 및 구성 예제에 대한 자세한 내용은 다음 VMware 기술 자료 문서를 참조하십시오.

- ESXi 및 ESX의 링크 집계에 대한 호스트 요구 사항(1001938)
- ESXi/ESX 및 Cisco/HP 스위치를 사용한 EtherChannel/LACP(Link Aggregation Control Protocol)의 샘플 구성(KB 1004048)

참고 RDMA를 통한 vSAN은 이 구성을 지원하지 않습니다.

물리적 스위치 구성

다음과 같이 2 업링크 고정 포트-채널을 구성합니다.

- 스위치 포트 43 및 44
- VLAN 트렁킹(포트 채널은 VLAN 트렁크 모드)이 트렁킹된 해당 VLAN 트렁크 모드에 있습니다.
- 포트-채널 그룹에 대해 로드 밸런싱 정책을 지정하지 마십시오.

이러한 단계는 스위치에서 개별 포트-채널을 구성하는 데 사용할 수 있습니다.

1단계: 포트-채널을 생성합니다.

```
#interface port-channel 13
```

2단계: 포트-채널을 VLAN 트렁크 모드로 설정합니다.

```
#switchport mode trunk
```

3단계: 해당 VLAN을 허용합니다.

```
#switchport trunk allowed vlan 3266
```

4단계: 포트-채널에 올바른 포트를 할당하고 모드를 활성으로 설정합니다.

```
#interface range Te1/0/43, Te1/0/44

#channel-group 1 mode on
```

5단계: 포트-채널이 고정 포트-채널로 구성되어 있는지 확인합니다.

```
#show interfaces port-channel 13


Channel Ports Ch-Type Hash Type Min-links Local Prf

------- ---------------------------- -------- --------- --------- --
```

```
Po13 Active: Te1/0/43, Te1/0/44 Static 7 1 Disabled

Hash Algorithm Type

1 - Source MAC, VLAN, EtherType, source module and port Id

2 - Destination MAC, VLAN, EtherType, source module and port Id

3 - Source IP and source TCP/UDP port

4 - Destination IP and destination TCP/UDP port

5 - Source/Destination MAC, VLAN, EtherType, source MODID/port

6 - Source/Destination IP and source/destination TCP/UDP port

7 - Enhanced hashing mode
```

vSphere Standard Switch 구성

이 예에서는 vSphere Standard Switch의 구성 및 생성을 이해하고 있다고 가정합니다.

이 예에서는 다음 구성을 사용합니다.

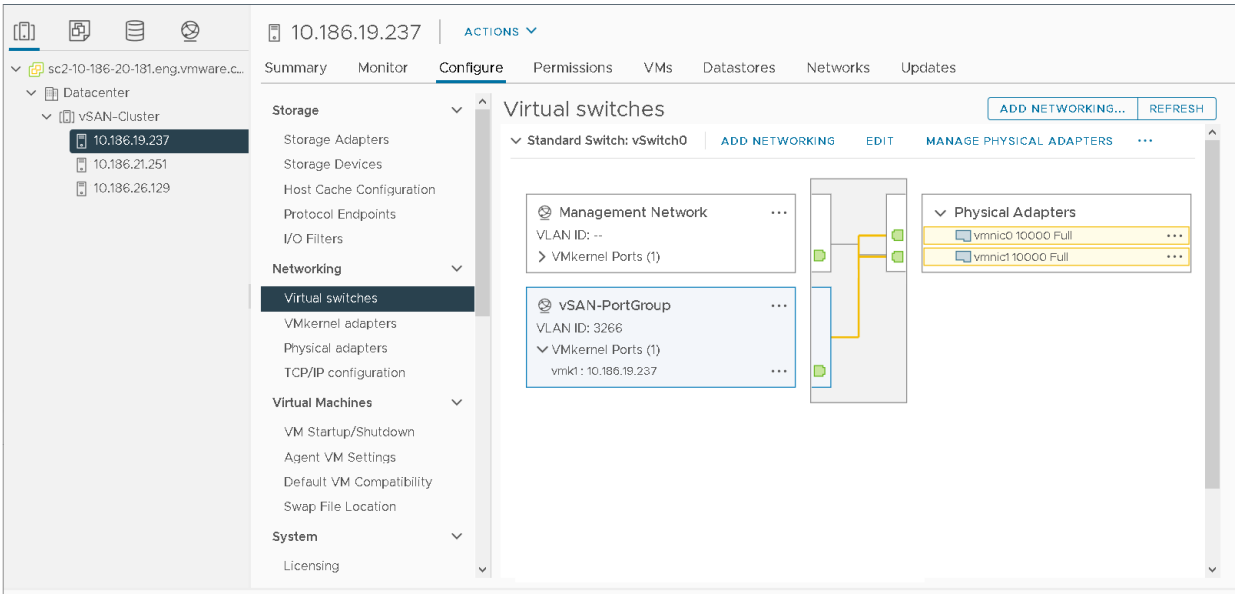
- 동일한 vSAN 호스트
- vmnic0 및 vmnic1이라는 업링크
- 스위치 포트 및 포트-채널에 트렁킹된 VLAN 3266
- 점보 프레임

각 호스트에서 MTU를 9000으로 설정하고, vSwitch에 vmnic0 및 vmnic1을 추가하여 **vSwitch1**을 생성합니다. 팀 구성 및 페일오버 정책에서 두 어댑터를 **활성** 위치로 설정합니다. 로드 밸런싱 정책 설정을 **IP 해시 기준 라우팅**으로 합니다.

다음과 같이 vSAN 트래픽에서 분산 포트 그룹에 대한 팀 구성 및 페일오버를 구성합니다.

- 로드 밸런싱 정책을 **IP 해시 기준 라우팅**으로 설정합니다.
- 네트워크 장애 감지를 **링크 상태만**으로 설정합니다.
- 스위치 알림을 **예**로 설정합니다.
- 페일백을 **예**로 설정합니다.
- 두 업링크가 **활성 업링크** 위치에 있는지 확인합니다.

네트워크 감지, 스위치 알림 및 페일백에 기본값을 사용합니다. 모든 포트 그룹은 vSwitch 수준에서 설정된 팀 구성 및 페일오버 정책을 상속합니다. 개별 포트 그룹 팀 구성 및 페일오버 정책을 상위 vSwitch와 다르게 재정의할 수 있지만, 모든 포트 그룹의 IP 해시 로드 밸런싱에 동일한 업링크 집합을 사용해야 합니다.



로드 밸런싱 구성

두 물리적 업링크가 모두 사용되지만, 모든 물리적 vmnic에서 트래픽이 일관되게 분산되지는 않습니다. 이 그림에서는 유일한 활성 트래픽이 기본적으로 4개의 vmknic 또는 IP 주소를 포함하는 vSAN 트래픽이라는 사실을 보여줍니다. 해당 동작은 IP 주소 수가 적고 해시가 가능한 경우에 발생할 수 있습니다. 그러나 일부 상황에서는 가상 스위치가 팀의 단일 업링크를 통해 트래픽을 일관되게 전달할 수 있습니다. IP 해시 알고리즘에 대한 자세한 내용은 "IP 해시 기준 라우팅" 에 대한 공식적인 vSphere 설명서를 참조하십시오.

네트워크 이중화

이 예에서는 장애 및 이중화 동작을 중점적으로 보여 주기 위해 vmnic1이 스위치에서 사용되지 않도록 설정된 포트에 연결되어 있습니다. 네트워크 업링크 이중화 경보가 트리거되었습니다.

vSAN 상태 경보는 트리거되지 않았습니다. 클러스터 및 VM 구성 요소는 영향을 받지 않으며 이 장애로 인해 게스트 스토리지 I/O가 중단되지 않습니다.

복구 및 페일백

vmnic1이 복구되면 두 활성 업링크 모두에서 트래픽이 자동으로 분산됩니다.

Network I/O Control

10

vSphere Network I/O Control을 사용하여 네트워크 트래픽의 QoS(서비스 품질) 수준을 설정합니다.

vSphere Network I/O Control은 vSphere Distributed Switch에서 사용할 수 있는 기능입니다. 이 기능을 사용하여 네트워크 트래픽에 대해 QoS(서비스 품질)를 구현합니다. vSAN 트래픽이 물리적 NIC를 vMotion, 관리, 가상 시스템 등의 다른 트래픽 유형과 공유해야 하는 경우 이 기능은 vSAN에 유용할 수 있습니다.

예약, 공유 및 제한

예약을 설정하여 Network I/O Control이 물리적 어댑터에서 vSAN에 대해 최소 대역폭을 사용할 수 있게 보장하도록 할 수 있습니다.

예약은 vMotion 또는 전체 호스트 제거와 같은 "버스트" 트래픽이 vSAN 트래픽에 영향을 줄 수 있는 경우에 유용합니다. 예약은 네트워크 대역폭에 대한 경합이 있는 경우에만 호출됩니다. Network I/O Control에서 예약을 사용할 때의 한 가지 단점은 사용되지 않은 예약 대역폭을 가상 시스템 트래픽에 할당할 수 없다는 것입니다. 모든 시스템 트래픽 유형 간에 예약된 총 대역폭은 최저 용량을 가진 물리적 네트워크 어댑터가 제공할 수 있는 대역폭의 75%를 초과할 수 없습니다.

vSAN 예약 모범 사례. vSAN용으로 예약된 트래픽을 가상 시스템 트래픽에 할당할 수 없으므로 vSAN 환경에서는 NIOC 예약을 사용하지 마십시오.

공유를 설정하면 vSAN용으로 할당된 물리적 어댑터가 포화될 때 vSAN에서 특정 대역폭을 사용할 수 있게 됩니다. 이로 인해 vSAN에서는 재구축 및 동기화 작업 중에 물리적 어댑터의 전체 용량을 사용하지는 못하게 됩니다. 예를 들어 팀에서 다른 물리적 어댑터가 실패하고 포트 그룹의 모든 트래픽이 팀의 나머지 어댑터로 전송되면 물리적 어댑터가 포화 상태가 될 수 있습니다. **공유** 옵션은 다른 트래픽이 vSAN 네트워크에 영향을 미치지 않도록 합니다.

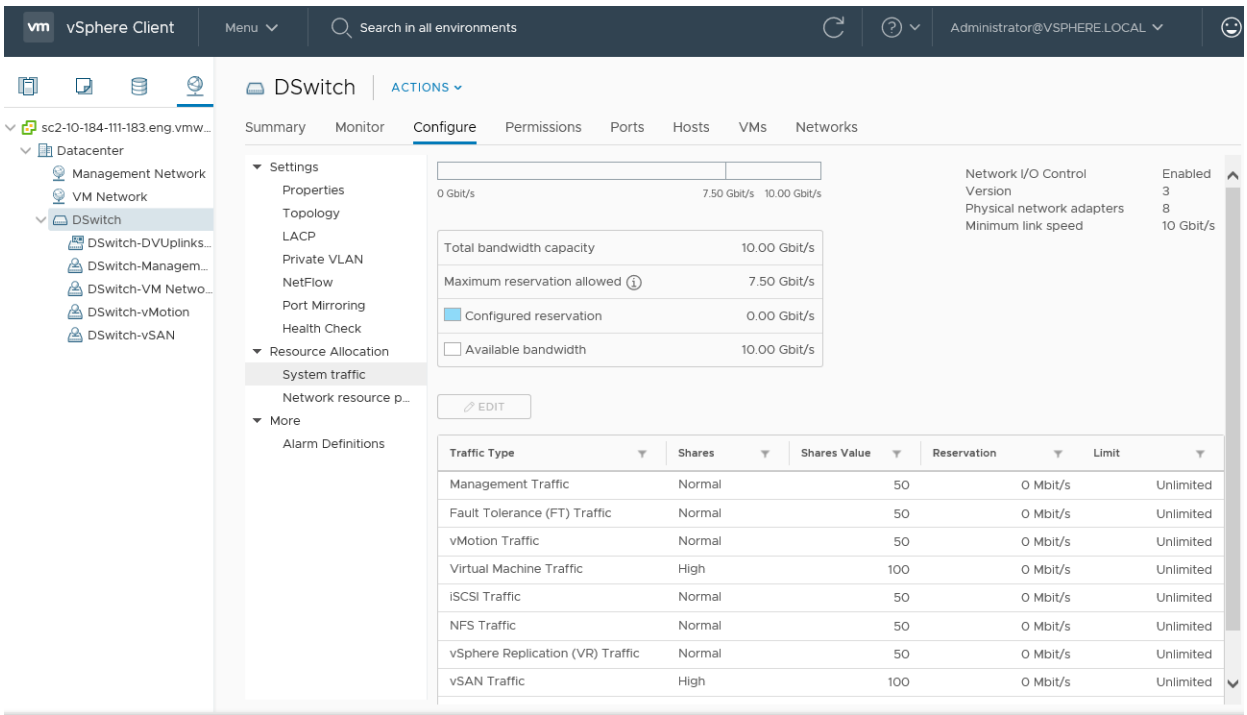
vSAN 공유 권장 사항. NIOC에서 가장 공정한 대역폭 할당 기술이며 vSAN 환경에서 사용하는 것이 좋습니다.

제한을 설정하면 특정 트래픽 유형이 어댑터에서 사용할 수 있는 최대 대역폭이 지정됩니다. 다른 사용자가 추가 대역폭을 사용하지 않는 경우에도 해당 제한이 설정된 트래픽 유형은 이러한 추가 대역폭을 사용할 수 없습니다.

vSAN 제한 권장 사항. 제한이 있는 트래픽 유형은 추가 대역폭을 사용할 수 없으므로 vSAN 환경에서는 NIOC 제한을 사용하지 마십시오.

네트워크 리소스 풀

Network I/O Control로 제어할 수 있는 모든 시스템 트래픽 유형을 볼 수 있습니다. 가상 시스템 네트워크가 여러 개 있는 경우 가상 시스템 트래픽에 특정 대역폭을 할당할 수 있습니다. 네트워크 리소스 풀을 사용하여 가상 시스템 포트 그룹을 기준으로 해당 대역폭의 일부를 사용합니다.



Network I/O Control 사용

vDS의 구성 속성에서 Network I/O Control을 사용하도록 설정할 수 있습니다. vSphere Client에서 vDS를 마우스 오른쪽 버튼으로 클릭하고 **설정 > 설정 편집** 메뉴를 선택합니다.

참고 Network I/O Control은 Standard vSwitch가 아닌 vSphere Distributed Switch에서만 사용할 수 있습니다.

Network I/O Control을 사용하여 호스트의 물리적 어댑터 용량을 기준으로 네트워크 트래픽에 대한 대역폭을 예약할 수 있습니다. 예를 들어 vSAN 트래픽이 10개의 GbE 물리적 네트워크 어댑터를 사용하며 해당 어댑터를 다른 시스템 트래픽 유형과 공유하는 경우 vSphere Network I/O Control을 사용하여 vSAN에 대해 특정 양의 대역폭을 보장할 수 있습니다. 이 방식은 vSphere vMotion, vSphere HA 및 가상 시스템 트래픽과 같은 트래픽이 vSAN 네트워크와 동일한 물리적 NIC를 공유할 때 유용할 수 있습니다.

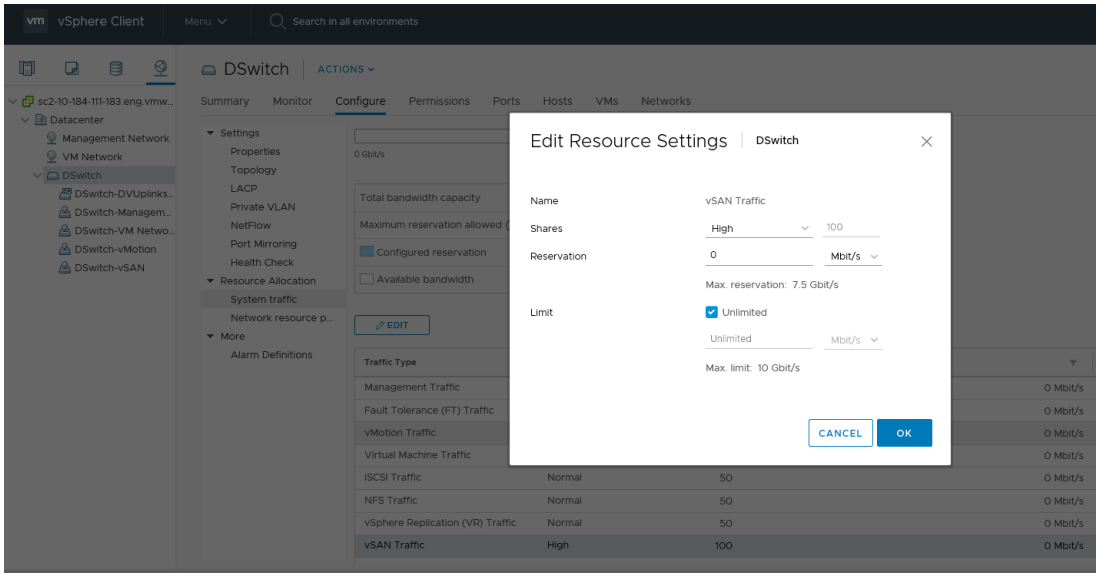
다음으로 아래 항목을 읽으십시오.

- Network I/O Control 구성 예

Network I/O Control 구성 예

vSAN 클러스터에 대해 Network I/O Control을 구성할 수 있습니다.

10GbE 물리적 어댑터가 1개 있는 vSAN 클러스터를 고려합니다. 이 NIC는 vSAN, vSphere vMotion 및 가상 시스템의 트래픽을 처리합니다. 트래픽 유형에 대한 공유 값을 변경하려면 시스템 트래픽 보기(**VDS > 구성 > 리소스 할당 > 시스템 트래픽**)에서 해당 트래픽 유형을 선택하고 **편집**을 클릭합니다. vSAN 트래픽의 공유 값이 기본값인 정상/50에서 높음/100으로 변경되었습니다.



표에 표시된 공유 값과 일치하도록 다른 트래픽 유형을 편집하십시오.

표 10-1. 샘플 NIOC 설정

트래픽 유형	공유	값
vSAN	높음	100
vSphere vMotion	낮음	25
가상 시스템	정상	50
iSCSI/NFS	낮음	25

10GbE 어댑터가 포화되면 Network I/O Control은 물리적 어댑터에서 vSAN에 5Gbps, 가상 시스템 트래픽에 3.5Gbps, vMotion에 1.5Gbps를 할당합니다. 이러한 값을 시작점으로 사용하여 vSAN 네트워크에서 NIOC 구성을 지정합니다. vSAN이 모든 프로토콜에서 우선 순위가 가장 높은지 확인합니다.

대역폭 할당의 다양한 매개 변수에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

vSAN의 각 vSphere 버전에서 vSphere Distributed Switch가 해당 버전의 일부로 제공됩니다. Network I/O Control은 모든 vSAN 버전에서 구성할 수 있습니다.

vSAN 네트워크 토폴로지 이해

11

vSAN 아키텍처는 여러 다른 네트워크 토폴로지를 지원합니다. 이러한 토폴로지는 vSAN의 전반적인 배포 및 관리에 영향을 줍니다.

vSAN 6.6에서 유니캐스트 지원이 도입되었으므로 네트워크를 간단하게 설계할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- 표준 배포
- vSAN 확장된 클러스터 배포
- 2노드 vSAN 배포
- 데이터 사이트에서 감시 호스트로의 네트워크 구성
- 복합 경계 조건 배포

표준 배포

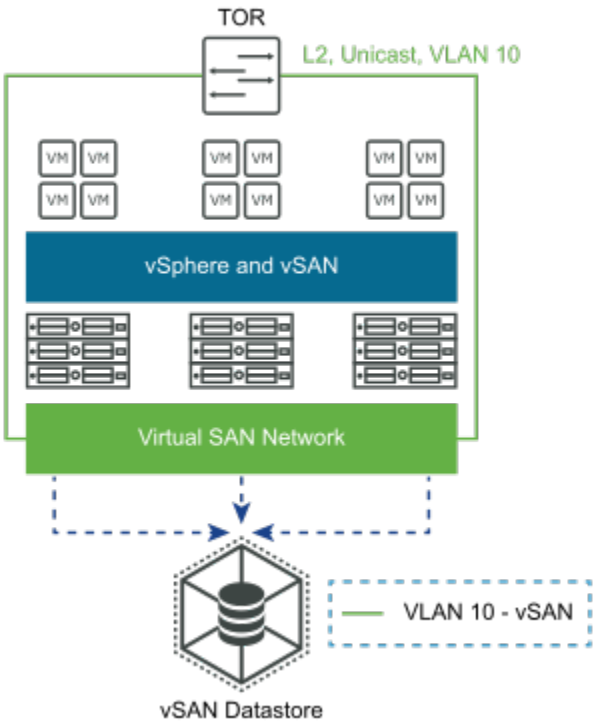
vSAN은 여러 단일 사이트 배포 유형을 지원합니다.

계층 2, 단일 사이트, 단일 랙

이 네트워크 토폴로지는 호스트, 브리지 또는 스위치와 같은 중간 계층 2 디바이스를 통해 패킷을 전달하는 역할을 합니다.

계층 2 네트워크 토폴로지는 vSAN의 가장 간단한 구현 및 관리를 제공합니다. 네트워크에서 불필요한 멀티캐스트 트래픽을 보내지 않도록 IGMP 스누핑 구성을 사용하는 것이 좋습니다. 이 첫 번째 예에서는 단일 사이트, vSAN 6.5 또는 이전 버전을 사용하는 단일 서버 랙을 살펴보겠습니다. 이 버전은 멀티캐스트를 사용하므로 IGMP 스누핑을 사용하도록 설정합니다. 모든 항목이 동일한 L2에 있으므로 멀티캐스트 트래픽에 대한 라우팅을 구성하지 않아도 됩니다.

vSAN 6.6 이상으로 계층 2 구현을 좀 더 단순화되면서 유니캐스트 지원이 도입되었습니다. IGMP 스누핑은 필요하지 않습니다.



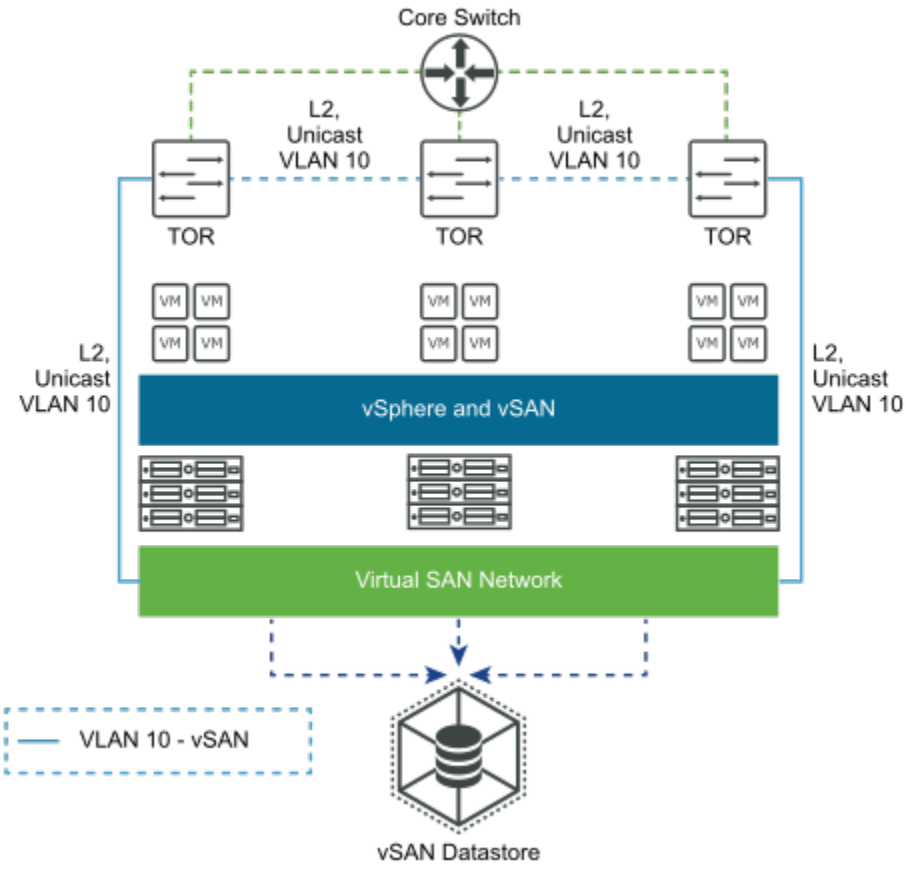
계층 2, 단일 사이트, 다중 랙

이 네트워크 토폴로지는 여러 개의 랙, 여러 개의 TOR(랙 상단) 스위치가 코어 스위치에 연결된 계층 2 구현에서 작동합니다.

다음 그림에서 TOR 사이의 파란색 점선은 vSAN 네트워크를 사용할 수 있으며 vSAN 클러스터의 모든 호스트에서 액세스할 수 있음을 보여 줍니다. 그러나 서로 다른 랙에 있는 호스트는 계층 3을 통해 서로 통신하며, 이것은 PIM을 사용하여 호스트 간에 멀티캐스트 트래픽을 라우팅하는 것을 의미합니다. TOR은 물리적으로 서로 연결되어 있지 않습니다.

네트워크의 불필요한 멀티캐스트 트래픽을 방지하기 위해 모든 TOR을 IGMP 스누핑용으로 구성하는 것이 좋습니다. 트래픽의 라우팅이 없으므로 멀티캐스트 트래픽을 라우팅하도록 PIM을 구성할 필요가 없습니다.

이 구현은 vSAN 트래픽이 유니캐스트이기 때문에 vSAN 6.6 이상에서 더 쉽습니다. 유니캐스트 트래픽을 사용하면 스위치에 IGMP 스누핑을 구성할 필요가 없습니다.



계층 3, 단일 사이트, 다중 랙

이 네트워크 토폴로지는 계층 3을 사용하여 vSAN 트래픽을 라우팅하는 vSAN 배포에 작동합니다.

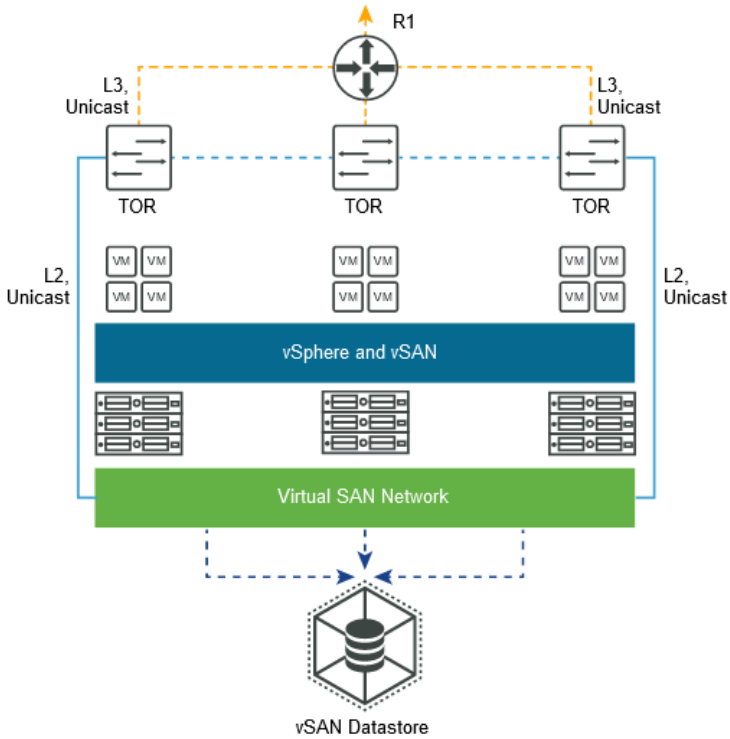
이 간단한 계층 3 네트워크 토폴로지는 각각 고유한 TOR 스위치를 사용하여 동일한 데이터 센터에서 여러 개의 랙을 사용합니다. vSAN 클러스터의 모든 호스트가 통신할 수 있도록 vSAN 네트워크를 L3를 통해 서로 다른 랙으로 라우팅합니다. 각 vSAN VMkernel 포트를 서로 다른 서브넷 또는 VLAN에 배치하고 각 랙에 대해 별도의 서브넷 또는 VLAN을 사용합니다.

이 네트워크 토폴로지는 라우터 및 계층 3 지원 스위치와 같은 중간 계층 3 지원 디바이스를 통해 패킷을 라우팅합니다. 호스트가 서로 다른 계층 3 네트워크 세그먼트에 걸쳐 배포될 때마다 라우팅된 네트워크 토폴로지가 생성됩니다.

vSAN 6.5 이하 버전에서는 이러한 배포에 멀티캐스트가 필요하기 때문에 IGMP 스누핑을 구성하고 사용하는 것이 좋습니다. 멀티캐스트 트래픽의 라우팅을 쉽게 하기 위해 물리적 스위치에 PIM을 구성합니다.

vSAN 6.6 이상에서는 이 토폴로지가 간소해집니다. 멀티캐스트 트래픽이 없기 때문에 IGMP 스누핑을 구성할 필요가 없습니다. 멀티캐스트 트래픽을 라우팅하도록 PIM을 구성할 필요가 없습니다.

다음은 L3를 통한 vSAN 6.6 배포 예를 대략적으로 나타낸 것입니다. 멀티캐스트 트래픽이 없기 때문에 IGMP 스누핑 또는 PIM에 대한 요구 사항은 없습니다.



vSAN 확장된 클러스터 배포

vSAN은 두 위치에 걸쳐 있는 확장된 클러스터 배포를 지원합니다.

vSAN 6.5 이하에서 데이터 사이트 간의 vSAN 트래픽은 메타데이터에 대해서는 **멀티캐스트**이고 I/O에 대해서는 **유니캐스트**입니다.

vSAN 6.6 이상에서는 모든 트래픽이 **유니캐스트**입니다. 모든 vSAN 버전에서 데이터 사이트와 감시 호스트 간의 감시 트래픽은 유니캐스트입니다.

계층 2 Everywhere

계층 2 네트워크에서 vSAN 확장 클러스터를 구성할 수 있지만 이 구성은 권장되지 않습니다.

vSAN 확장된 클러스터가 단일 대규모 계층 2 설계에서 구성되는 방식을 고려하십시오. 데이터 사이트 1 및 사이트 2에는 가상 시스템이 배포됩니다. 사이트 3에는 감시 호스트가 포함되어 있습니다.

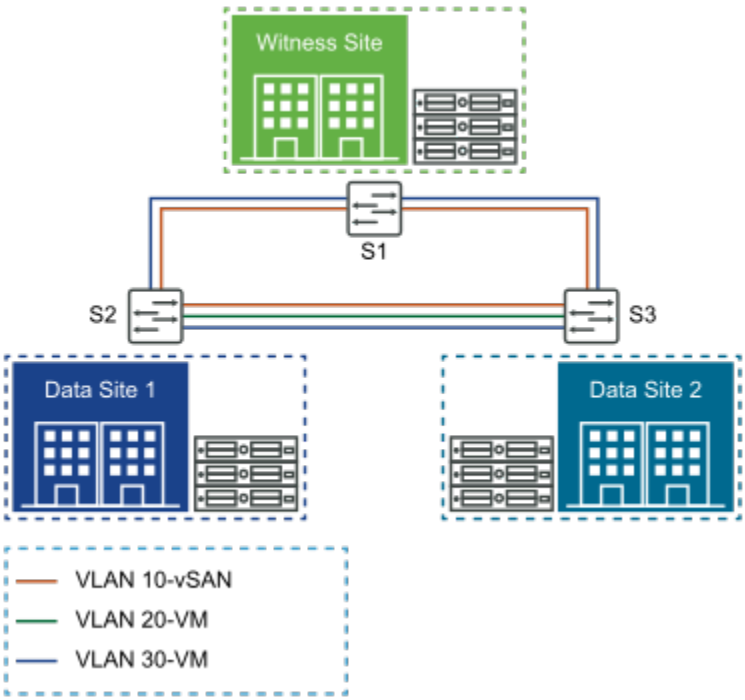
참고 최상의 결과를 얻으려면 확장 계층 2 네트워크를 전체 사이트에 걸쳐 사용하지 않도록 합니다.

계층 2 Everywhere를 최대한 간단히 예시하기 위해 토폴로지에서 스위치(라우터 아님)를 사용합니다.

계층 2 네트워크에는 루프(다중 경로)가 있을 수 없으므로, 사이트 1과 사이트 2 간의 연결 중 하나를 차단하기 위해 STP(Spanning Tree Protocol)와 같은 기능이 필요합니다. 이제 사이트 2와 사이트 3 간의 링크가 끊어진 상황(사이트 1과 사이트 2 간의 링크)을 살펴보겠습니다. 이제 네트워크 트래픽이 사이트 3의 감시 호스트를 통해 사이트 1에서 사이트 2로 전환될 수 있습니다. VMware는 감시 호스트에 대해 훨씬 더 낮은 대역폭과 더 높은 지연 시간을 지원하므로 데이터 네트워크 트래픽이 더 낮은 규격의 감시 사이트를 통과하는 경우 성능이 크게 저하되는 것을 볼 수 있습니다.

데이터 사이트 간의 트래픽이 감시 사이트를 통과하도록 전환되어 애플리케이션 지연 시간에 영향을 주지 않고 대역폭이 허용 수준을 유지할 경우 사이트 간에 확장 L2 구성이 가능할 수 있습니다. 대부분의 경우 이러한 구성은 적합하지 않으며 네트워킹 요구 사항이 더 복잡해집니다.

멀티캐스트 트래픽을 사용하는 vSAN 6.5 또는 이전 버전에서는 스위치에 IGMP 스누핑을 구성해야 합니다. vSAN 6.6 이상에서는 이 작업을 꼭 수행할 필요가 없습니다. 멀티캐스트 트래픽의 라우팅이 없기 때문에 PIM이 필요하지 않습니다.



지원되는 vSAN 확장된 클러스터 구성

vSAN은 확장된 클러스터 구성을 지원합니다.

다음 구성은 데이터 사이트의 네트워크에서 장애가 발생하는 경우 사이트 1의 트래픽이 감시 호스트를 통해 사이트 2로 라우팅되는 것을 방지합니다. 이 구성은 성능 저하를 방지합니다. 데이터 트래픽이 감시 호스트로 연결되지 않도록 하려면 다음 네트워크 토폴로지를 사용합니다.

사이트 1과 사이트 2 사이에서 확장 계층 2 전환 구성 또는 계층 3 라우팅 구성을 구현합니다. 두 구성이 모두 지원됩니다.

사이트 1과 감시 호스트 간에 계층 3 라우팅 구성을 구현합니다.

사이트 2와 감시 호스트 간에 계층 3 라우팅 구성을 구현합니다.

이러한 구성(L2+L3 및 L3 Everywhere)은 vSAN 6.5 이하 버전의 멀티캐스트와 vSAN 6.6에서 사용할 수 있는 유니캐스트에 대해서만 지정되는 고려 사항과 함께 설명됩니다. 멀티캐스트 트래픽은 IGMP 스누핑을 위해 추가적인 구성 단계와 멀티캐스트 트래픽 라우팅을 위한 PIM을 요구합니다.

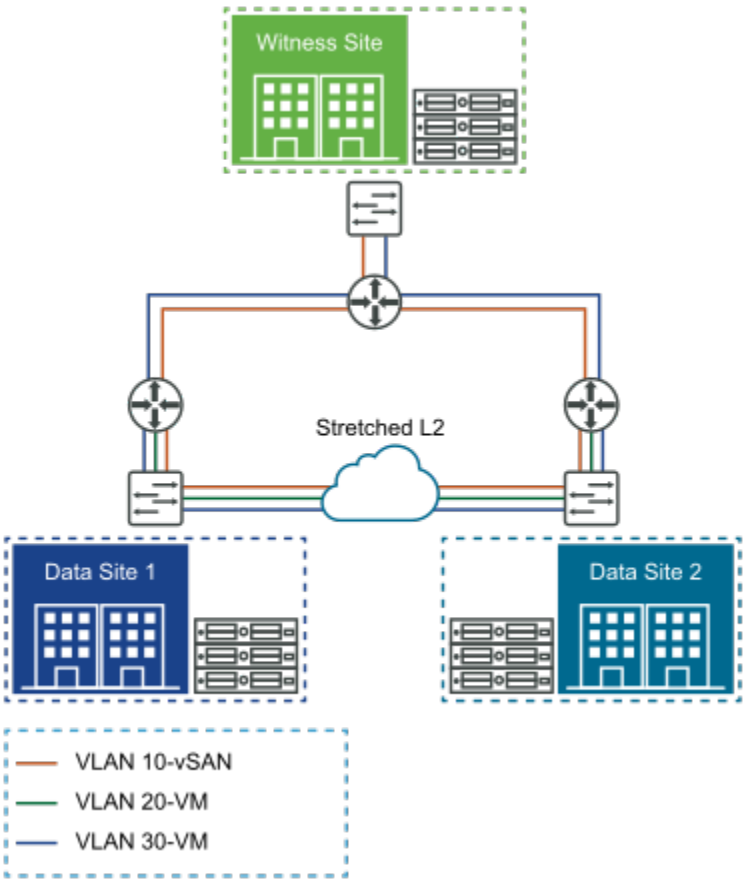
데이터 사이트 간의 확장 계층 2 네트워크와 감시 사이트로의 계층 3 라우팅 네트워크를 검토해야 합니다. 계층 2와 계층 3의 조합을 가능한 한 간단히 나타내기 위해 토폴로지의 스위치 및 라우터 조합을 사용하십시오.

데이터 사이트 간 확장 계층 2, 감시 호스트로의 계층 3

vSAN은 데이터 사이트 간에 확장 계층 2 구성을 지원합니다.

이 경우 라우팅된 트래픽은 감시 트래픽뿐입니다. 멀티캐스트를 사용하는 vSAN 6.5 이하 버전에서는 데이터 사이트 간 확장 L2 vSAN에서 멀티캐스트 트래픽에 IGMP 스누핑을 사용합니다. 그러나 감시 트래픽이 유니캐스트이기 때문에 계층 3 세그먼트에서 PIM을 구현할 필요가 없습니다.

유니캐스트를 사용하는 vSAN 6.6의 경우에는 IGMP 스누핑 또는 PIM을 고려할 필요가 없습니다.



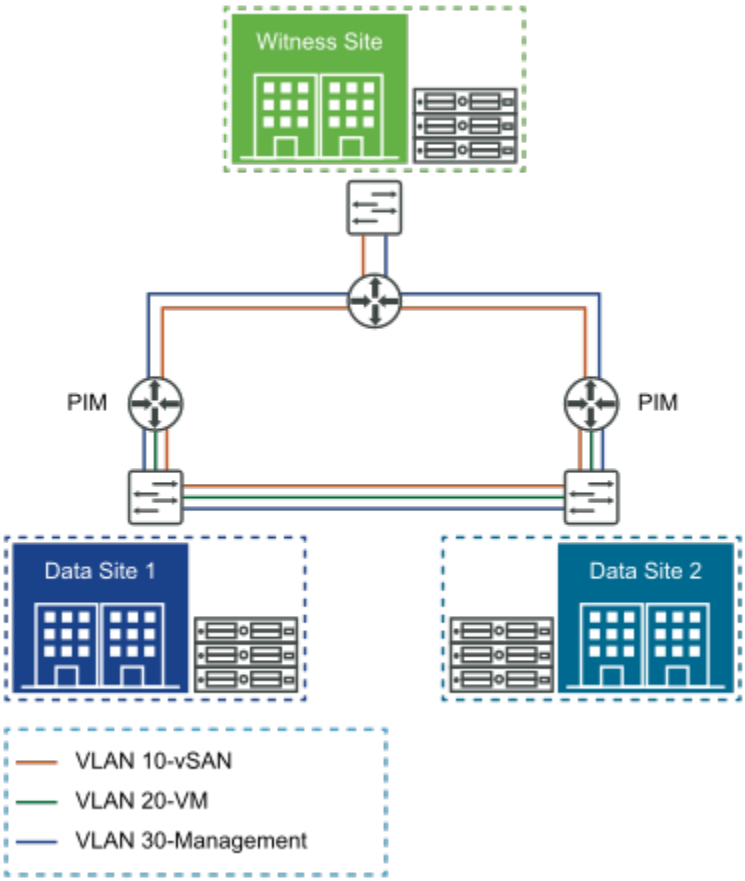
계층 3 Everywhere

이 vSAN 확장 클러스터 구성에서 데이터 사이트와 감시 호스트 간에 데이터 트래픽이 라우팅됩니다.

계층 3 Everywhere를 최대한 간단히 구현하기 위해 토폴로지에서 라우터 또는 라우팅 스위치를 사용합니다.

예를 들어 멀티캐스트 트래픽을 사용하는 vSAN 6.5 이하 환경을 고려하십시오. 이 경우 데이터 사이트 스위치에서 IGMP 스누핑을 구성하여 네트워크의 멀티캐스트 트래픽 양을 관리합니다. 감시 트래픽이 유니캐스트이기 때문에 감시 호스트에서는 이것이 필요하지 않습니다. 데이터 사이트 간에 멀티캐스트 트래픽이 라우팅되므로 멀티캐스트 라우팅을 허용하도록 PIM을 구성합니다.

vSAN 6.6 이상에서는 라우팅된 모든 트래픽이 유니캐스트이기 때문에 IGMP 스누핑 및 PIM이 필요하지 않습니다.



vSAN 확장된 클러스터에서 감시 트래픽 분리

vSAN은 확장된 클러스터에서 감시 트래픽을 구분하도록 지원합니다.

vSAN 6.5 이상 릴리스에서는 2노드 구성의 vSAN 트래픽에서 감시 트래픽을 분리할 수 있습니다. 즉, 10Gb 스위치 없이도 2개 vSAN 호스트를 직접 연결할 수 있습니다.

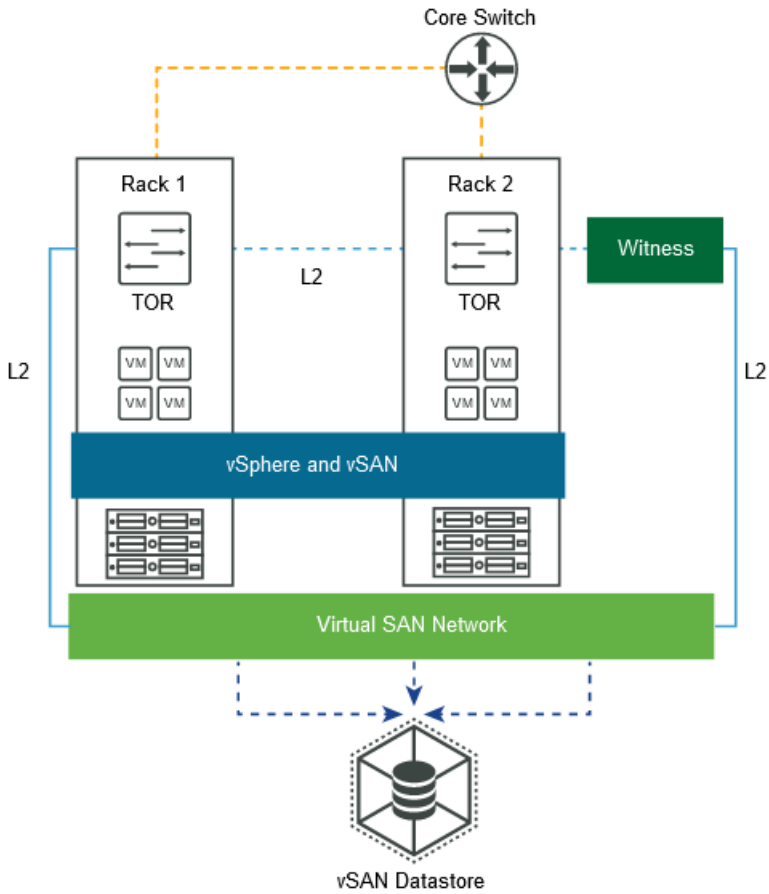
이 감시 트래픽 분리는 vSAN 6.6의 2노드 배포에서만 지원됩니다. vSAN 확장된 클러스터에서 감시 트래픽을 분리하는 것은 vSAN 6.7 이상에서 지원됩니다.

vSAN 확장된 클러스터를 사용하여 랙 인식 달성

vSAN 확장된 클러스터를 사용할 경우 vSAN은 단일 사이트에서 랙 인식을 제공합니다.

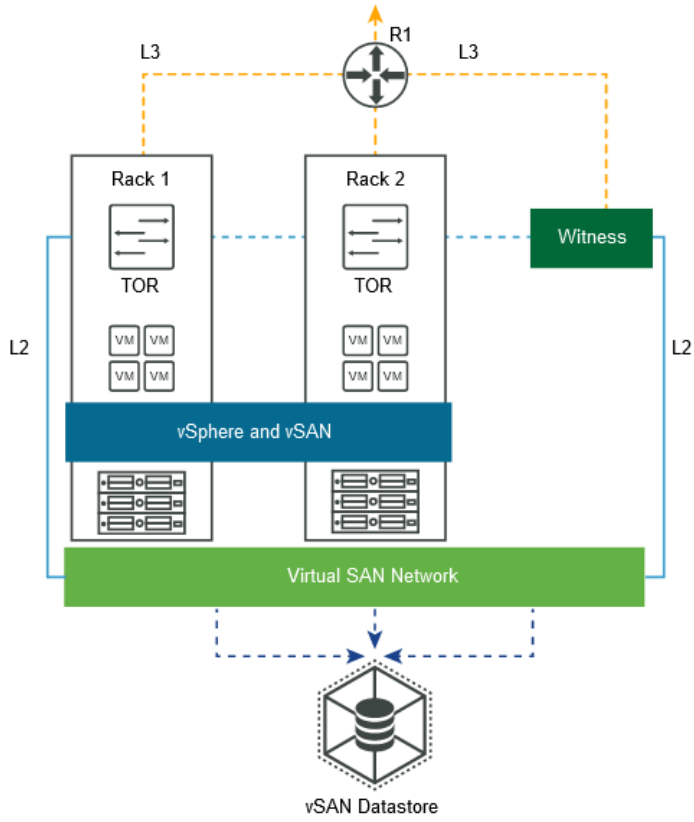
vSAN 호스트 랙이 2개 있는 경우 완전한 랙 실패가 발생한 후에도 vSAN 클러스터를 계속 실행할 수 있습니다. 이 경우, 남은 랙 및 원격 감시 호스트에서 VM 워크로드의 가용성을 제공합니다.

참고 이 구성을 지원하려면 vSAN 호스트의 2개 랙 내에 감시 호스트를 배치하지 마십시오.



이 예에서 랙 1이 실패하면 랙 2와 감시 호스트가 VM 가용성을 제공합니다. 이 구성은 vSAN 6.6 이전 환경으로, 네트워크에 멀티캐스트가 구성되어 있어야 합니다. 감시 호스트는 vSAN 네트워크에 있어야 합니다. 감시 트래픽은 유니캐스트입니다. vSAN 6.6 이상에서는 모든 트래픽이 유니캐스트입니다.

이 토폴로지는 L3를 통해서도 지원됩니다. 각 vSAN VMkernel 포트를 서로 다른 서브넷 또는 VLAN에 배치하고 각 랙에 대해 별도의 서브넷 또는 VLAN을 사용합니다.



이 토폴로지는 vSAN 확장된 클러스터를 사용하여 랙 인식(장애 도메인)을 실현하기 위해 두 개의 랙이 있는 배포를 지원합니다. 이 솔루션은 클러스터 외부에 있는 감시 호스트를 사용합니다.

2노드 vSAN 배포

vSAN에서는 2노드 배포를 지원합니다. 2노드 vSAN 배포는 적은 수의 워크로드를 실행하지만 고가용성을 필요로 하는 ROBO(원격 사무실/지사)에서 사용됩니다.

vSAN 2노드 배포는 지점에서 원격으로 찾을 수 있는 세 번째 감시 호스트를 사용합니다. 일반적으로 감시는 vCenter Server와 같은 관리 구성 요소와 함께 지점에서 유지 관리됩니다.

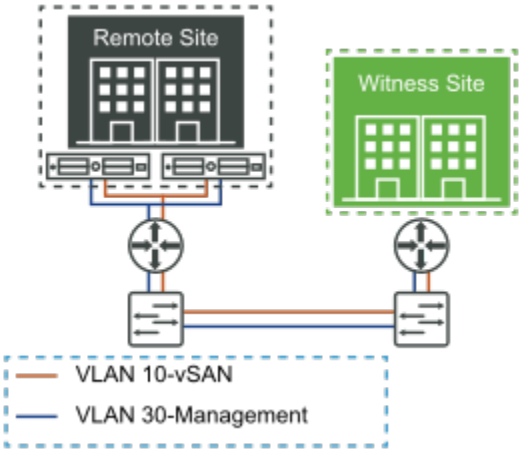
vSAN 6.5 이전의 2노드 vSAN 배포

2노드 배포를 지원하는 6.5 이전의 vSAN 릴리스에는 원격 사이트에 물리적 스위치가 필요합니다.

초기에 2노드 vSAN을 원격 사이트에서 사용하려면 물리적 10Gb 스위치가 필요했습니다. 이 원격 사이트의 서버만 vSAN 호스트라면 이 방법은 효율적이지 못한 솔루션일 것입니다.

이 배포에서는 10Gb 스위치를 사용하는 다른 디바이스가 없으면 IGMP 스누핑을 고려하지 않아도 됩니다. 원격 사이트의 다른 디바이스가 10Gb 스위치를 공유하는 경우 IGMP 스누핑을 사용하여 과도하고 불필요한 멀티캐스트 트래픽을 방지할 수 있습니다.

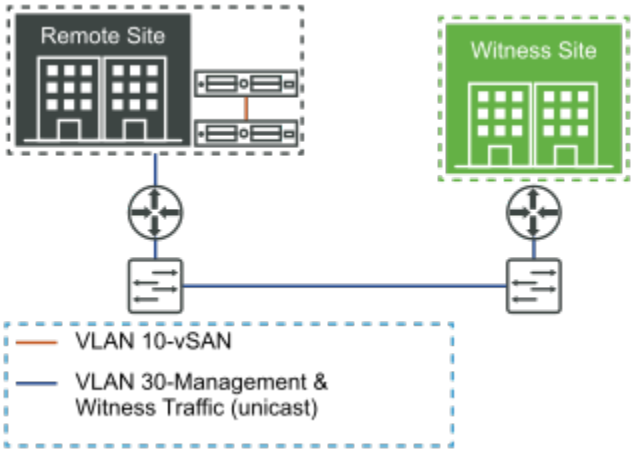
라우팅된 트래픽만 감시 트래픽(유니캐스트)이므로 PIM은 필요하지 않습니다.



vSAN 6.5 이상에 대한 2노드 배포

vSAN 6.5 이상에서는 2노드 배포를 지원합니다.

vSAN 버전 6.5 이상에서는 이러한 2노드 vSAN 구현이 훨씬 더 간단합니다. vSAN 6.5 이상에서는 데이터 사이트의 2개 호스트를 직접 연결할 수 있습니다.

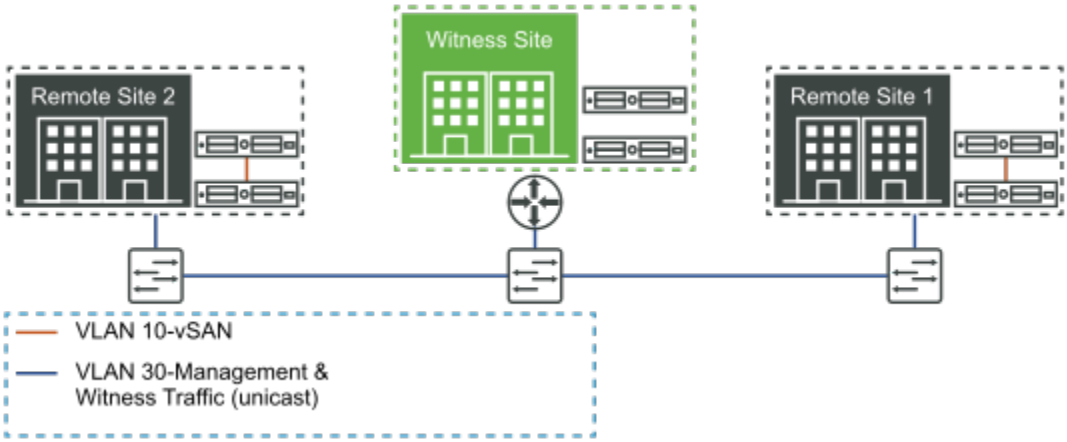


이 기능을 사용하도록 설정하면 감시 트래픽이 vSAN 데이터 트래픽과 완전히 구분됩니다. vSAN 데이터 트래픽은 직접 연결의 두 노드 간에 흐를 수 있지만 감시 트래픽은 관리 네트워크를 통해 감시 사이트로 라우팅될 수 있습니다.

감시 장치는 지점에서 원격으로 위치할 수 있습니다. 예를 들어, 감시 기능은 관리 인프라(vCenter Server, vROps, Log Insight 등)와 함께 기본 데이터 센터에서 다시 실행할 수 있습니다. 감시 기능이 지점에서 원격으로 상주할 수 있는 또 다른 지원 위치는 vCloud Air입니다.

이 구성에서는 원격 사이트에 스위치가 없습니다. 따라서 vSAN 연속 네트워크에서 멀티캐스트 트래픽에 대한 지원을 구성할 필요가 없습니다. 감시 트래픽이 유니캐스트이기 때문에 관리 네트워크에서 멀티캐스트를 고려할 필요가 없습니다.

vSAN 6.6 이상에서는 모두 유니캐스트를 사용하므로 멀티캐스트 고려 사항이 없습니다. 각각에 고유한 감시 기능이 있기만 하면 다중 원격 사무실/지점 2노드 배포도 지원됩니다.



2노드 vSAN 배포에 대한 일반적인 고려 사항

2노드 vSAN 배포는 다른 토폴로지에 대한 지원을 제공합니다. 이 섹션에서는 일반적인 구성에 대해 설명합니다.

2노드 구성에 대한 자세한 내용 및 네트워크 외부의 자세한 배포 고려 사항에 대해서는 vSAN 코어 설명서를 참조하십시오.

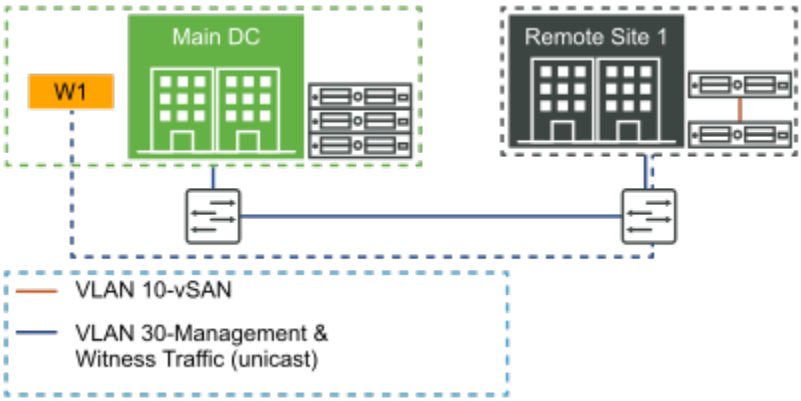
다른 두 노드 vSAN 클러스터에서 감시 실행

vSAN은 다른 2노드 클러스터에서 감시 기능을 실행하도록 지원하지 않습니다.

다른 표준 vSAN 배포에서 실행 중인 감시 기능

vSAN은 다른 표준 vSAN 배포에서 감시 기능을 실행하도록 지원합니다.

이 구성은 지원됩니다. 원격 사이트 2노드 vSAN에 장애가 발생해도 기본 데이터 센터의 표준 vSAN 환경의 가용성에는 영향을 주지 않습니다.



데이터 사이트에서 감시 호스트로의 네트워크 구성

데이터 사이트의 호스트 인터페이스는 vSAN 네트워크를 통해 감시 호스트와 통신합니다. 사용할 수 있는 구성 옵션이 다릅니다.

이 항목에서는 이러한 구성을 구현하는 방법을 설명합니다. 또한 vSAN 네트워크를 통해 서로 통신하는 데이터 사이트의 호스트에 있는 인터페이스가 감시 호스트와 통신하는 방법을 설명합니다.

옵션 1: 고정 경로를 사용하여 L3를 통해 연결된 물리적 ESXi 감시

데이터 사이트는 확장된 L2 네트워크를 통해 연결될 수 있습니다. 이 옵션을 데이터 사이트의 관리 네트워크, vSAN 네트워크, vMotion 네트워크 및 가상 시스템 네트워크에도 사용합니다.

이 네트워크 인프라의 물리적 네트워크 라우터는 데이터 사이트(사이트 1 및 사이트 2)의 호스트에서 감시 사이트(사이트 3)의 호스트로 트래픽을 자동으로 전송하지 않습니다. vSAN 확장된 클러스터를 성공적으로 구성하려면 클러스터의 모든 호스트가 통신해야 합니다. 이 환경에 vSAN 확장된 클러스터를 배포할 수 있습니다.

솔루션은 ESXi 호스트에 구성된 "고정 경로" 를 사용하여 사이트 1 및 사이트 2의 vSAN 트래픽이 사이트 3의 감시 호스트에 도달될 수 있도록 하는 것입니다. 데이터 사이트에 있는 ESXi 호스트의 경우, 해당 네트워크에 대해 지정된 게이트웨이를 통해 사이트 3의 감시 호스트로 트래픽을 리디렉션하는 고정 경로를 vSAN 인터페이스에 추가합니다. 감시 호스트의 경우 vSAN 인터페이스에는 데이터 사이트의 호스트로 향하는 vSAN 트래픽을 리디렉션하는 고정 경로를 추가해야 합니다. 다음 명령을 사용하여 vSAN 확장된 클러스터의 각 ESXi 호스트에 고정 경로를 추가합니다. **`esxcli network ip route ipv4 add -g`** "<gateway>" **`-n`** "<network>"

참고 vCenter Server는 데이터 사이트와 감시 사이트 모두에서 ESXi 호스트를 관리할 수 있어야 합니다. 감시 호스트에서 vCenter Server로 직접 연결하는 동안에는 관리 네트워크와 관련된 추가적인 문제가 발생하지 않습니다.

vMotion 네트워크 또는 VM 네트워크를 구성하거나, vSAN 확장된 클러스터의 컨텍스트에서 이러한 네트워크에 대한 고정 경로를 추가할 필요가 없습니다. 가상 시스템은 vSAN 감시 호스트에 마이그레이션하거나 배포되지 않습니다. 감시 개체만 유지 보수하려고 하며, 이 작업에 대해 이러한 네트워크 중 하나가 필요하지 않습니다.

옵션 2: 고정 경로를 사용하여 L3를 통해 연결된 가상 ESXi 감시 장치

감시 호스트는 vSAN 클러스터의 일부가 아닌 물리적 ESXi 호스트에 배포되는 가상 시스템이므로 물리적 ESXi 호스트에는 최소한 하나의 VM 네트워크가 미리 구성되어 있어야 합니다. 이 VM 네트워크는 관리 네트워크와 데이터 사이트의 ESXi 호스트에서 공유하는 vSAN 네트워크 둘 다에 연결되어야 합니다.

참고 감시 호스트는 전용 호스트일 필요가 없습니다. 감시를 동시에 호스팅하는 여러 다른 VM 워크로드에 사용될 수 있습니다.

다른 옵션은 기본 물리적 ESXi 호스트에 두 개의 미리 구성된 VM 네트워크(관리 네트워크용 1개, vSAN 네트워크용 1개)를 사용하는 것입니다. 이 물리적 ESXi 호스트에 가상 ESXi 감시가 배포된 경우 네트워크를 적절히 연결하고 구성해야 합니다.

가상 ESXi 감시 호스트를 배포한 후에는 고정 경로를 구성합니다. 데이터 사이트가 확장된 L2 네트워크를 통해 연결된다고 가정합니다. 이 옵션을 데이터 사이트의 관리 네트워크, vSAN 네트워크, vMotion 네트워크 및 가상 시스템 네트워크에도 사용합니다. vSAN 트래픽은 데이터 사이트(사이트 1 및 사이트 2)의 호스트에서 기본 게이트웨이를 통해 감시 사이트(사이트 3)의 호스트로 라우팅되지 않습니다. vSAN 확장된 클러스터를 성공적으로 구성하려면 클러스터의 모든 호스트에 사이트 1 및 사이트 2의 vSAN 트래픽이 사이트 3의 감시 호스트에 도달할 수 있도록 하는 고정 경로가 필요합니다. **`esxcli network ip route`** 명령을 사용하여 각 ESXi 호스트에 고정 경로를 추가합니다.

복합 경계 조건 배포

일반적이지 않은 복합 경계 조건 구성에 vSAN을 배포할 수 있습니다.

이러한 일반적이지 않은 토폴로지에는 특별한 고려 사항이 필요합니다.

3개의 위치, vSAN 확장된 클러스터 없음, 분산 감시 호스트

확장된 클러스터 구성을 배포하는 대신, 여러 방, 건물 또는 사이트 간에 vSAN을 배포할 수 있습니다.

이 구성은 지원됩니다. 한 가지 요구 사항은 사이트 간 지연 시간을 동일한 데이터 센터의 정상적인 vSAN 배포에 대해 예상되는 지연 시간과 동일한 수준으로 유지해야 한다는 것입니다. 지연 시간은 모든 호스트에서 **1ms 미만**이어야 합니다. 지연 시간이 이 값보다 클 경우 5ms의 지연 시간을 허용하는 vSAN 확장된 클러스터를 고려하십시오. vSAN 6.5 이하 버전에서는 멀티캐스트에 대한 추가 고려 사항을 해결해야 합니다.

최상의 결과를 얻으려면 이러한 토폴로지의 모든 사이트에서 일관된 구성을 유지해야 합니다. VM의 가용성을 유지하려면 각 방, 건물 또는 사이트의 호스트가 동일한 장애 도메인에 배치되는 방식으로 장애 도메인을 구성합니다. 호스트 A는 호스트 B와 통신할 수 없지만 호스트 B는 호스트 A와 통신할 수 있는 클러스터의 비대칭 파티셔닝을 방지합니다.

2노드를 1+1+W 확장된 클러스터로 배포

2노드 구성을 vSAN 확장된 클러스터 구성으로 배포하여 각 호스트를 다른 방, 건물 또는 사이트에 배치할 수 있습니다.

각 사이트의 호스트 수를 늘리려고 하면 라이센싱 관련 오류와 함께 실패합니다. 2개 호스트보다 크고 전용 감시 장치/호스트 기능(N+N+감시(N>1))을 사용하는 클러스터의 경우 구성을 vSAN 확장된 클러스터로 간주합니다.

vSAN 네트워크 문제 해결

12

vSAN을 사용하면 잘못 구성된 vSAN 네트워크에서 발생하는 다양한 유형의 문제를 검토하고 해결할 수 있습니다.

vSAN 작업은 네트워크 구성, 안정성 및 성능에 따라 달라집니다. 많은 지원 요청이 잘못된 네트워크 구성이 있거나 네트워크가 예상되는 성능을 나타내지 않을 때 발생합니다.

vSAN 상태 서비스를 사용하여 네트워크 문제를 해결하십시오. 네트워크 상태 점검은 상태 점검 결과에 따라 적절한 기술 자료 문서로 안내할 수 있습니다. 기술 자료 문서에서는 네트워크 문제를 해결하기 위한 지침을 제공합니다.

네트워크 상태 점검

상태 서비스에는 네트워킹 상태 점검을 위한 범주가 포함되어 있습니다.

각 상태 점검에는 **AskVMware** 링크가 있습니다. 상태 점검이 실패하면 **AskVMware**를 클릭하고 관련 VMware 기술 자료 문서에서 자세한 정보와 문제를 쉽게 해결하는 방법에 대한 지침을 참조하십시오.

다음 네트워킹 상태 검사는 vSAN 환경에 대한 유용한 정보를 제공합니다.

- vSAN**: 기본(유니캐스트) 연결 확인**. 이 검사는 vSAN 네트워크에 있는 각 ESXi 호스트를 다른 ESXi 호스트에서 ping하여 vSAN 클러스터의 모든 ESXi 호스트 간에 IP 연결이 존재하는지 확인합니다.
- **vMotion: 기본(유니캐스트) 연결 확인**. 이 검사는 vMotion이 구성된 vSAN 클러스터의 모든 ESXi 호스트 간에 IP 연결이 존재하는지 확인합니다. vMotion 네트워크의 각 ESXi 호스트는 다른 모든 ESXi 호스트를 ping합니다.
- **모든 호스트에 구성된 vSAN vmknic가 있음**. 이 검사는 vSAN 클러스터의 각 ESXi 호스트에 vSAN 트래픽용으로 구성된 VMkernel NIC가 있는지 확인합니다.
- 모든 호스트에 일치하는 멀티캐스트 설정이 있음. 이 검사는 각 호스트에 올바르게 구성된 멀티캐스트 주소가 있는지 확인합니다.
- **모든 호스트에 일치하는 서브넷이 있음**. 이 검사는 모든 vSAN VMkernel NIC가 동일한 IP 서브넷에 있도록 vSAN 클러스터의 모든 ESXi 호스트가 구성되었는지 테스트합니다.
- **호스트가 VC에서 연결이 끊김**. 이 검사는 vCenter Server에서 vSAN 클러스터의 모든 ESXi 호스트에 대한 활성 연결이 있는지 확인합니다.

- **연결 문제가 있는 호스트**. 이 검사는 vCenter Server가 호스트를 연결된 것으로 표시되지만 vCenter에서 호스트로의 API 호출이 실패하는 상황을 나타냅니다. 호스트와 vCenter Server 간의 연결 문제를 중점적으로 나타낼 수 있습니다.
- **네트워크 지연 시간**. 이 검사는 vSAN 호스트의 네트워크 지연 시간 검사를 수행합니다. 임계값이 5ms를 초과하면 주의가 표시됩니다.
- **vMotion: MTU 확인(큰 패킷 크기를 사용하는 ping)**. 이 검사는 기본 vMotion ping 연결 검사를 보완합니다. 네트워크 성능을 향상하기 위해 최대 전송 단위 크기가 증가합니다. 잘못 구성된 MTU가 네트워크 구성 문제로 나타나지 않을 수 있지만 성능 문제를 유발할 수도 있습니다.
- **vSAN 클러스터 파티션**. 이 상태 점검은 클러스터를 검사하여 존재하는 파티션의 수를 확인합니다. vSAN 클러스터에 파티션이 둘 이상 있으면 오류가 표시됩니다.
- **다른 확인을 기반으로 하는 멀티캐스트 평가**. 이 상태 점검은 모든 네트워크 상태 점검에서 데이터를 집계합니다. 이 검사에 실패하면 멀티캐스트가 네트워크 파티션의 근본 원인일 가능성이 큽니다.

네트워크 확인 명령

vSAN 네트워크가 구성된 경우 다음 명령을 사용하여 해당 상태를 검사합니다. vSAN에 사용되는 VMkernel 어댑터(vmknic) 및 포함된 특성을 확인할 수 있습니다.

ESXCLI 및 RVC 명령을 사용하여 네트워크가 완전히 작동하는지 확인하고 vSAN과 관련된 네트워크 문제를 해결합니다.

vSAN 네트워크에 사용되는 vmknic가 모든 호스트에서 올바르고 균일하게 구성되었는지 확인하고, 멀티캐스트가 작동하는지 확인하고, vSAN 클러스터에 참여하는 호스트가 서로 성공적으로 통신할 수 있는지 확인합니다.

esxcli vsan network list

이 명령을 사용하여 vSAN 네트워크에서 사용하는 VMkernel 인터페이스를 식별할 수 있습니다.

아래 출력에서는 vSAN 네트워크가 vmk2를 사용하고 있음을 보여 줍니다. 이 명령은 vSAN이 클러스터에서 꺼져 있고 호스트가 더는 vSAN에 참여하지 않는 경우에도 계속 작동합니다.

에이전트 그룹 멀티캐스트 및 마스터 그룹 멀티캐스트도 확인하는 데 중요합니다.

```
[root@esxi-dell-m:~] esxcli vsan network list
Interface
   VmkNic Name: vmk1
   IP Protocol: IP
   Interface UUID: 32efc758-9ca0-57b9-c7e3-246e962c24d0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
```

```
    Multicast TTL: 5
    Traffic Type: vsan
```

이러한 사항은 vSAN 트래픽에 사용되는 VMkernel 인터페이스와 같은 유용한 정보를 제공합니다. 이 경우에는 **vmk1**입니다. 그러나 멀티캐스트 주소도 함께 표시됩니다. 이 정보는 클러스터를 유니캐스트 모드로 실행하는 경우에도 표시될 수 있습니다. 그룹 멀티캐스트 주소 및 포트가 있습니다. 포트 23451은 기본에서 1초마다 전송되는 하트비트에 사용되며 클러스터의 다른 모든 호스트에 표시됩니다. 포트 12345는 기본과 백업 간의 CMMDS 업데이트에 사용됩니다.

esxcli network ip interface list

이 명령을 사용하면 vSwitch 또는 분산 스위치와 같은 항목을 확인할 수 있습니다.

이 명령을 사용하여 연결된 vSwitch 또는 분산 스위치와 환경에서 점보 프레임이 구성된 경우 유용할 수 있는 MTU 크기를 확인합니다. 이 경우 MTU는 기본값인 1500을 유지합니다.

```
[root@esxi-dell-m:~] esxcli network ip interface list
vmk0
   Name: vmk0
   <<truncated>>
vmk1
   Name: vmk1
   MAC Address: 00:50:56:69:96:f0
   Enabled: true
   Portset: DvsPortset-0
   Portgroup: N/A
   Netstack Instance: defaultTcpipStack
   VDS Name: vDS
   VDS UUID: 50 1e 5b ad e3 b4 af 25-18 f3 1c 4c fa 98 3d bb
   VDS Port: 16
   VDS Connection: 1123658315
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 9000
   TSO MSS: 65535
   Port ID: 50331814
```

최대 전송 단위 크기는 9000으로 표시되므로 이 VMkernel 포트는 약 9,000의 MTU가 필요한 점보 프레임용으로 구성된 것입니다. VMware는 점보 프레임 사용에 대한 권장 사항을 제공하지 않습니다. 그러나 점보 프레임은 vSAN에서 사용하도록 지원됩니다.

esxcli network ip interface ipv4 get –i vmk2

이 명령은 vSAN VMkernel 인터페이스의 IP 주소 및 넷마스크와 같은 정보를 표시합니다.

이 정보를 사용하여 관리자는 명령줄에서 사용할 수 있는 다른 명령을 사용하여 vSAN 네트워크가 올바르게 작동하는지 확인할 수 있습니다.

```
[root@esxi-dell-m:~] esxcli network ip interface ipv4 get -i vmk1
Name  IPv4 Address  IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway  DHCP DNS
----  ------------  -------------  --------------  ------------  -------  --------
vmk1  172.40.0.9   255.255.255.0   172.40.0.255   STATIC         0.0.0.0 false
```

vmkping

`vmkping` 명령은 네트워크의 다른 모든 ESXi 호스트가 ping 요청에 응답하는지 확인합니다.

```
~ # vmkping -I vmk2 172.32.0.3 -s 1472 -d
 PING 172.32.0.3 (172.32.0.3): 56 data bytes
 64 bytes from 172.32.0.3: icmp_seq=0 ttl=64 time=0.186 ms
 64 bytes from 172.32.0.3: icmp_seq=1 ttl=64 time=2.690 ms
 64 bytes from 172.32.0.3: icmp_seq=2 ttl=64 time=0.139 ms

 --- 172.32.0.3 ping statistics ---
 3 packets transmitted, 3 packets received, 0% packet loss
 round-trip min/avg/max = 0.139/1.005/2.690 ms
```

멀티캐스트 기능을 확인하지는 않지만 네트워크 문제가 있는 rogue ESXi 호스트를 식별하는 데 도움이 될 수 있습니다. 또한 응답 시간을 검토하여 vSAN 네트워크에 비정상적인 지연 시간이 발생하는지 확인할 수 있습니다.

점보 프레임이 구성된 경우 점보 프레임 MTU 크기가 잘못되어도 이 명령은 문제를 보고하지 않습니다. 기본적으로 이 명령은 MTU 크기 1500을 사용합니다. 점보 프레임이 전체적으로 작업을 성공적으로 수행하는지 확인해야 하는 경우 다음과 같이 더 큰 패킷 크기(-s) 옵션으로 vmkping을 사용합니다.

```
 ~ # vmkping -I vmk2 172.32.0.3 -s 8972 -d
 PING 172.32.0.3 (172.32.0.3): 8972 data bytes
 9008 bytes from 172.32.0.3: icmp_seq=0 ttl=64 time=0.554 ms
 9008 bytes from 172.32.0.3: icmp_seq=1 ttl=64 time=0.638 ms
 9008 bytes from 172.32.0.3: icmp_seq=2 ttl=64 time=0.533 ms

 --- 172.32.0.3 ping statistics ---
 3 packets transmitted, 3 packets received, 0% packet loss
 round-trip min/avg/max = 0.533/0.575/0.638 ms
 ~ #
```

패킷을 조각화 없이 전송할 수 있는지를 테스트하려면 vmkping 명령에 -d를 추가하는 것을 고려하십시오.

esxcli network ip neighbor list

이 명령은 모든 vSAN 호스트가 동일한 네트워크 세그먼트에 있는지 확인하는 데 도움이 됩니다.

이 구성에는 4개 호스트 클러스터가 있으며, 이 명령은 IP 주소와 해당 vmknic(vSAN이 이 클러스터의 모든 호스트에서 vmk1을 사용하도록 구성됨)를 포함하는 다른 3개 호스트에 대한 ARP(Address Resolution Protocol) 항목을 반환합니다.

```
[root@esxi-dell-m:~] esxcli network ip neighbor list -i vmk1
Neighbor     Mac Address        Vmknic   Expiry  State  Type
-----------  -----------------  ------  -------  -----  -------
172.40.0.12  00:50:56:61:ce:22  vmk1    164 sec         Unknown
172.40.0.10  00:50:56:67:1d:b2  vmk1    338 sec         Unknown
172.40.0.11  00:50:56:6c:fe:c5  vmk1    162 sec         Unknown
[root@esxi-dell-m:~]
```

esxcli network diag ping

이 명령은 네트워크의 중복 여부와 라운드 트립 시간을 확인합니다.

다양한 호스트 간 vSAN 네트워크 연결에 대한 자세한 정보를 확인할 수 있도록 ESXCLI에서는 강력한 네트워크 진단 명령을 제공합니다. 다음은 이러한 출력의 예입니다. 여기서 vmk1에 VMkernel 인터페이스가 있고 네트워크에 있는 다른 호스트의 원격 vSAN 네트워크 IP가 172.40.0.10입니다.

```
[root@esxi-dell-m:~] esxcli network diag ping -I vmk1 -H 172.40.0.10
   Trace:
         Received Bytes: 64
         Host: 172.40.0.10
         ICMP Seq: 0
         TTL: 64
         Round-trip Time: 1864 us
         Dup: false
         Detail:

         Received Bytes: 64
         Host: 172.40.0.10
         ICMP Seq: 1
         TTL: 64
         Round-trip Time: 1834 us
         Dup: false
         Detail:

         Received Bytes: 64
         Host: 172.40.0.10
         ICMP Seq: 2
         TTL: 64
         Round-trip Time: 1824 us
         Dup: false
         Detail:
   Summary:
         Host Addr: 172.40.0.10
         Transmitted: 3
         Recieved: 3
         Duplicated: 0
         Packet Lost: 0
         Round-trip Min: 1824 us
```

```
          Round-trip Avg: 1840 us
          Round-trip Max: 1864 us
[root@esxi-dell-m:~]
```

vsan.lldpnetmap

이 RVC 명령은 업링크 포트 정보를 표시합니다.

환경에서 LLDP(Link Layer Discovery Protocol)가 사용하도록 설정된 Cisco 이외 스위치가 있는 경우 업링크 <-> 스위치 <-> 스위치 포트 정보를 표시하기 위한 RVC 명령이 있습니다. RVC에 대한 자세한 내용은 RVC 명령 가이드를 참조하십시오.

이 가이드는 vSAN 클러스터가 여러 스위치에 걸쳐 있을 때 스위치에 연결된 호스트를 확인하는 데 유용합니다. 클러스터에 있는 호스트의 하위 집합만 영향을 받는 경우 특정 스위치로 문제를 분리하는 것이 도움될 수 있습니다.

```
> vsan.lldpnetmap 02013-08-15 19:34:18 -0700: This operation will take 30-60
seconds ...+---------------+---------------------------+| Host          | LLDP
info                 |+---------------+---------------------------+| 10.143.188.54 | w2r13-
vsan-x650-2: vmnic7 ||               | w2r13-vsan-x650-1: vmnic5 |+---------------
+---------------------------+
```

이 명령은 LLDP를 지원하는 스위치에서만 사용할 수 있습니다. 이 명령을 구성하려면 스위치에 로그온하고 다음을 실행합니다.

```
switch# config t
Switch(Config)# feature lldp
```

LLDP가 사용하도록 설정되었는지 확인하려면 다음을 수행합니다.

```
switch(config)#do show running-config lldp
```

참고 LLDP는 기본적으로 보내기 및 받기 모드 둘 다에서 작동합니다. 물리적 스위치 정보가 검색되지 않는 경우 vDS 속성의 설정을 확인합니다. 기본적으로 vDS는 CDP(Cisco Discovery Protocol)로 설정된 검색 프로토콜을 사용하여 생성됩니다. 이 문제를 해결하려면 검색 프로토콜을 LLDP로 설정하고 vDS에서 작업을 **both**로 설정합니다.

멀티캐스트 통신 확인

멀티캐스트 구성은 초기 vSAN 배포 문제를 유발할 수 있습니다.

멀티캐스트가 vSAN 환경에서 올바르게 작동하는지 확인하는 가장 간단한 방법 중 하나는 `tcpdump-uw` 명령을 사용하는 것입니다. 이 명령은 ESXi 호스트의 명령줄에서 사용할 수 있습니다.

이 `tcpdump-uw` 명령은 기본에서 멀티캐스트 패킷(포트 및 IP 정보)을 올바르게 전송하는지와 클러스터의 다른 모든 호스트가 해당 패킷을 수신하는지를 표시합니다.

기본에서 이 명령은 멀티캐스트 주소로 전송되는 패킷을 표시합니다. 다른 모든 호스트에서는 기본에서 멀티캐스트 주소까지 동일한 패킷이 표시됩니다. 그렇지 않으면 멀티캐스트가 올바르게 작동하지 않는 것입니다. 클러스터의 모든 호스트에서 여기에 표시된 `tcpdump-uw` 명령을 실행하면 기본의 하트비트가 표시됩니다. 이 경우 기본은 IP 주소 172.32.0.2에 있습니다. 자세한 정보 표시를 위한 **-v** 옵션은 선택 사항입니다.

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast -v
tcpdump-uw: listening on vmk2, link-type EN10MB (Ethernet), capture size 96 bytes
11:04:21.800575 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 34917, offset 0,
flags [none], proto UDP (17), length 228)
  172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:04:22.252369 IP truncated-ip - 234 bytes missing! (tos 0x0, ttl 5, id 15011, offset 0,
flags [none], proto UDP (17), length 316)
  172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:04:22.262099 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 3359, offset 0,
flags [none], proto UDP (17), length 228)
  172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
11:04:22.324496 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 20914, offset 0,
flags [none], proto UDP (17), length 228)
  172.32.0.5.60460 > 224.1.2.3.12345: UDP, length 200
11:04:22.800782 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 35010, offset 0,
flags [none], proto UDP (17), length 228)
  172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:04:23.252390 IP truncated-ip - 234 bytes missing! (tos 0x0, ttl 5, id 15083, offset 0,
flags [none], proto UDP (17), length 316)
  172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:04:23.262141 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 3442, offset 0,
flags [none], proto UDP (17), length 228)
  172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
```

이 출력은 약간 혼동을 가져올 수 있지만, 여기에 표시된 출력은 클러스터의 4개 호스트가 기본에서 하트비트를 가져오는 것을 의미합니다. 이 **tcpdump-uw** 명령은 하트비트를 수신하는지 확인하기 위해 모든 호스트에서 실행해야 합니다. 이 명령은 기본이 하트비트를 전송하고 있고 클러스터의 다른 모든 호스트가 이를 수신 중인지 확인합니다. 그럴 경우 멀티캐스트가 작동 중인 것입니다.

일부 vSAN 호스트가 기본에서 1초 하트비트를 선택할 수 없는 경우 네트워크 관리자는 해당 스위치의 멀티캐스트 구성을 확인해야 합니다.

truncated-ip - 146바이트 누락을 방지하기 위해서입니다! 메시지가 표시되지 않도록 하려면 동일한 명령에 **-s0** 옵션을 사용하여 패킷 잘림을 방지하십시오.

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast -v -s0
tcpdump-uw: listening on vmk2, link-type EN10MB (Ethernet), capture size 65535 bytes
11:18:29.823622 IP (tos 0x0, ttl 5, id 56621, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:18:30.251078 IP (tos 0x0, ttl 5, id 52095, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
11:18:30.267177 IP (tos 0x0, ttl 5, id 8228, offset 0, flags [none], proto UDP (17), length
316)
    172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
```

```
11:18:30.336480 IP (tos 0x0, ttl 5, id 28606, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.5.60460 > 224.1.2.3.12345: UDP, length 200
11:18:30.823669 IP (tos 0x0, ttl 5, id 56679, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
```

tcpdump 명령은 IGMP(Internet Group Management Protocol) 멤버 자격과 관련되어 있습니다. 호스트(및 네트워크 디바이스)는 IGMP를 사용하여 멀티캐스트 그룹 멤버 자격을 설정합니다.

vSAN 클러스터의 각 ESXi 호스트는 일반 IGMP 멤버 자격 보고서(가입)를 전송합니다.

tcpdump 명령은 호스트의 IGMP 멤버 보고서를 표시합니다.

```
[root@esxi-dell-m:~] tcpdump-uw -i vmk1 igmp
tcpdump-uw: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmk1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:49:23.134458 IP 172.40.0.9 > igmp.mcast.net: igmp v3 report, 1 group record(s)
15:50:22.994461 IP 172.40.0.9 > igmp.mcast.net: igmp v3 report, 1 group record(s)
```

ESXi 호스트가 정기적으로 멤버 자격을 업데이트하고 있음을 나타내는 IGMP v3 보고서가 출력에 표시됩니다. 네트워크 관리자는 vSAN ESXi 호스트가 IGMP를 올바르게 수행하는지 의심스러운 경우 클러스터의 각 ESXi 호스트에서 이 명령을 실행하고 이 추적을 표시하여 확인할 수 있습니다.

멀티캐스트 통신이 있는 경우 IGMP v3를 사용합니다.

실제로 다음 명령을 사용하여 멀티캐스트 및 IGMP 트래픽을 동시에 확인할 수 있습니다.

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast or igmp -v -s0
```

일반적인 문제는 vSAN 클러스터가 여러 물리적 스위치에 걸쳐 구성되어 있고 멀티캐스트가 한 스위치에서 사용하도록 설정되어 있지만 스위치 전체에서 사용하도록 설정되어 있지 않다는 것입니다. 이 경우 클러스터는 한 파티션에 두 개의 ESXi 호스트를 포함하며, 다른 ESXi 호스트(다른 스위치에 연결됨)는 이 클러스터에 가입할 수 없습니다. 대신 다른 파티션에 고유한 vSAN 클러스터를 형성합니다. 앞에서 살펴본 `vsan.lldpnetmap` 명령은 네트워크 구성을 확인하고 어떤 호스트가 어떤 스위치에 연결되어 있는지 파악하는 데 도움이 될 수 있습니다.

vSAN 클러스터가 구성되는 동안 멀티캐스트가 문제가 될 수 있다는 사실을 보여주는 지표가 제공됩니다.

서브넷, VLAN, MTU에 대한 검사 목록을 따르고 클러스터의 각 호스트가 클러스터의 다른 모든 호스트를 `vmkping`할 수 있다고 가정합니다.

클러스터가 생성될 때 멀티캐스트 문제가 있는 경우 각 ESXi 호스트가 스스로 기본이 되고 고유한 vSAN 클러스터를 구성하게 되는 것이 일반적인 증상입니다. 이러한 증상이 있더라도 각 호스트에 고유한 네트워크 파티션 ID가 있는 경우 호스트 간에 멀티캐스트가 없는 것을 암시합니다.

그러나 ESXi 호스트의 하위 집합이 클러스터를 형성하고 다른 하위 집합은 다른 클러스터를 형성하며, 각각에 고유한 기본, 백업 및 에이전트 호스트까지 있는 고유한 파티션을 포함할 경우 여러 스위치가 아닌 해당 스위치에서 멀티캐스트가 사용하도록 설정됩니다. vSAN은 자체 클러스터 파티션을 형성하는 첫 번째 물리적 스위치의 호스트와 각각이 고유한 기본을 보유하는 고유한 클러스터 파티션을 형성하는 두 번째 물리적 스위치의 호스트를 보여줍니다. 클러스터의 호스트가 연결하는 스위치를 확인할 수 있고 클러스터의 호스트가 동일한 스위치에 연결된 경우 이것에 문제가 될 수 있습니다.

vSAN 네트워크 성능 확인

ESXi 호스트 간에 충분한 대역폭이 있는지 확인합니다. 이 도구는 vSAN 네트워크가 최적의 성능으로 작동되는지 여부를 테스트하는 데 도움이 될 수 있습니다.

vSAN 네트워크의 성능을 확인하려면 `iperf` 도구를 사용하여 최대 TCP 대역폭과 지연 시간을 측정할 수 있습니다. 이 도구는 `/usr/lib/vmware/vsan/bin/iperf.copy`.에 있습니다. 다양한 옵션을 확인하려면 `--help`를 사용하여 실행합니다. 이 도구를 사용하여 vSAN 클러스터에 참여하는 ESXi 호스트 간의 네트워크 대역폭과 지연 시간을 확인합니다.

VMware KB 2001003은 설정 및 테스트에 도움이 될 수 있습니다.

이 도구는 vSAN 클러스터에 권한을 부여한 경우에 가장 유용합니다. 클러스터가 이미 운영 환경에서 작동될 때 vSAN 네트워크에서 **iperf** 테스트를 실행하면 클러스터에서 실행되는 가상 시스템의 성능에 영향을 줄 수 있습니다.

vSAN 네트워크 제한 확인

`vsan.check.limits` 명령은 어떠한 vSAN 임계값도 위반되지 않음을 확인합니다.

```
> ls
0 /
1 vcsa-04.rainpole.com/
> cd 1
/vcsa-04.rainpole.com> ls
0 Datacenter (datacenter)
/vcsa-04.rainpole.com> cd 0
/vcsa-04.rainpole.com/Datacenter> ls
0 storage/
1 computers [host]/
2 networks [network]/
3 datastores [datastore]/
4 vms [vm]/
/vcsa-04.rainpole.com/Datacenter> cd 1
/vcsa-04.rainpole.com/Datacenter/computers> ls
0 Cluster (cluster): cpu 155 GHz, memory 400 GB
1 esxi-dell-e.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
2 esxi-dell-f.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
3 esxi-dell-g.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
4 esxi-dell-h.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
/vcsa-04.rainpole.com/Datacenter/computers> vsan.check_limits 0
2017-03-14 16:09:32 +0000: Querying limit stats from all hosts ...
```

```
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-m.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-n.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-o.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-p.rainpole.com (may take a
moment) ...
2017-03-14 16:09:39 +0000: Done fetching vSAN disk infos
+--------------------------+--------------------
+-------------------------------------------------------------------+
| Host                     | RDT                |
Disks                                                        |
+--------------------------+--------------------
+-------------------------------------------------------------------+
| esxi-dell-m.rainpole.com | Assocs: 1309/45000 | Components:
485/9000                                             |
|                          | Sockets: 89/10000  | naa.500a075113019b33: 0% Components:
0/0                      |
|                          | Clients: 136       | naa.500a075113019b37: 40% Components:
81/47661                 |
|                          | Owners: 138        |
t10.ATA_____Micron_P420m2DMTFDGAR1T4MAX_____ 0% Components: 0/0 |
|                          |                    | naa.500a075113019b41: 37% Components:
80/47661                 |
|                          |                    | naa.500a07511301a1eb: 38% Components:
81/47661                 |
|                          |                    | naa.500a075113019b39: 39% Components:
79/47661                 |
|                          |                    | naa.500a07511301a1ec: 41% Components:
79/47661                 |
<<truncated>>
```

네트워크 관점에서 보면 중요한 RDT 연결(Assocs) 및 소켓 수입니다. vSAN 6.0 이상에서는 호스트마다 45,000개의 연결이 있습니다. RDT 연결은 vSAN 내에서 피어 투 피어 네트워크 상태를 추적하는 데 사용됩니다. vSAN은 RDT 연결이 부족하지 않도록 크기가 조정됩니다. 또한 vSAN은 사용할 수 있는 TCP 소켓 수를 제한하며, TCP 소켓 할당이 부족하지 않도록 크기가 조정됩니다. 호스트당 10,000개 소켓으로 제한됩니다.

vSAN **client**는 vSAN 클러스터의 개체 액세스를 나타냅니다. 클라이언트는 일반적으로 호스트에서 실행되는 가상 시스템을 나타냅니다. 클라이언트와 개체가 동일한 호스트에 있지 않을 수 있습니다. 명확하게 정의된 제한은 없지만 이 메트릭은 클라이언트가 여러 호스트에서 밸런스를 유지하는 방법을 이해하는 데 도움을 줍니다.

주어진 vSAN 개체에는 하나의 vSAN **소유자**만 있으며, 이 소유자는 일반적으로 이 개체에 액세스하는 vSAN 클라이언트와 함께 배치됩니다. vSAN 소유자는 vSAN 개체에 대한 모든 액세스를 조정하고 미러링 및 스트라이핑과 같은 기능을 구현합니다. 명확하게 정의된 제한은 없지만 이 메트릭은 소유자가 여러 호스트에서 밸런스를 유지하는 방법을 이해하는 데 도움을 주기 위해 한번 더 표시됩니다.

vSAN 네트워크에서 멀티캐스트 사용 13

멀티캐스트는 IP 네트워크를 통해 대상 그룹에 정보 패킷을 전송하는 네트워크 통신 기술입니다.

vSAN 버전 6.6의 이전 릴리스는 IP 멀티캐스트를 지원하며, IP 멀티캐스트 통신을 검색 프로토콜로 사용하여 vSAN 클러스터에 가입하려는 노드를 식별합니다. vSAN 버전 6.6의 이전 릴리스는 클러스터 그룹을 가입 및 탈퇴하는 동안 및 다른 클러스터 간 통신 작업을 수행하는 동안 IP 멀티캐스트 통신에 의존합니다. vSAN 트래픽 서비스를 전송하기 위해 IP 네트워크 세그먼트에서 IP 멀티캐스트를 사용하도록 설정하고 구성해야 합니다.

IP 멀티캐스트 주소를 MG(멀티캐스트 그룹)라고 합니다. IP 멀티캐스트는 그룹 전송 형태로 여러 수신자에게 소스 패킷을 전송합니다. IP 멀티캐스트는 호스트, 클라이언트 및 네트워크 디바이스가 멀티캐스트 기반 통신에 참여하기 위해 사용하는 통신 프로토콜에 의존합니다. IGMP(Internet Group Management Protocol) 및 PIM(프로토콜 독립 멀티캐스트)와 같은 통신 프로토콜은 IP 멀티캐스트 통신을 사용하기 위한 기본 구성 요소 및 종속성입니다.

vSAN 클러스터를 생성하는 동안 각 vSAN 클러스터에 기본 멀티캐스트 주소가 할당됩니다. vSAN 트래픽 서비스는 기본 멀티캐스트 주소 설정을 각 호스트에 자동으로 할당합니다. 이 멀티캐스트 주소는 프레임을 기본 멀티캐스트 그룹과 멀티캐스트 그룹 에이전트로 보냅니다.

여러 vSAN 클러스터가 동일한 계층 2 네트워크에 있는 경우 추가 vSAN 클러스터 내에서 기본 멀티캐스트 주소를 변경하는 것이 좋습니다. 이로 인해 여러 클러스터가 모든 멀티캐스트 스트림을 수신하지는 못합니다. 기본 vSAN 멀티캐스트 주소 변경에 대한 자세한 내용은 VMware KB 2075451을 참조하십시오.

다음으로 아래 항목을 읽으십시오.

- Internet Group Management Protocol
- 프로토콜 독립 멀티캐스트

Internet Group Management Protocol

IGMP(Internet Group Management Protocol)를 사용하여 계층 2 도메인 내의 IP 멀티캐스트 그룹 멤버 자격에 수신자를 추가할 수 있습니다.

IGMP를 사용하면 수신자는 가입하려는 멀티캐스트 그룹으로 요청을 보낼 수 있습니다. 멀티캐스트 그룹의 멤버가 되면 라우터는 수신자가 스위치 포트에 연결된 계층 3 세그먼트의 멀티캐스트 그룹으로 트래픽을 전달할 수 있습니다.

IGMP 스누핑을 사용하여 멀티캐스트 그룹에 참여하는 물리적 스위치 포트를 vSAN VMkernel 포트 업링크로만 제한할 수 있습니다. IGMP 스누핑은 IGMP 스누핑 쿼리 발송기를 사용하여 구성됩니다. IGMP 스누핑을 지원하기 위해 IGMP 스누핑 쿼리 발송기를 구성해야 하는지 여부는 스위치 벤더에 따라 다릅니다. IGMP 스누핑 구성에 대해서는 해당 스위치 벤더에 문의하십시오.

vSAN은 IGMP 버전 2와 IGMP 버전 3을 모두 지원합니다. 계층 3 네트워크 세그먼트에서 vSAN 배포를 수행하는 경우 동일한 계층 3 네트워크 세그먼트에 연결되어 있거나 액세스할 수 있는 라우터 또는 스위치와 같은 계층 3 지원 디바이스를 구성할 수 있습니다.

vSAN 네트워크의 모든 VMkernel 포트는 IGMP를 사용하는 멀티캐스트 그룹을 구독하여 모든 네트워크 포트의 멀티캐스트 서비스 장애를 방지합니다.

참고 이 클러스터에 있는 모든 호스트의 vSAN 포트로 확장할 수 있는 비라우팅 또는 트렁킹 VLAN에 vSAN이 있을 때 IGMP 스누핑을 비활성화할 수 있습니다.

프로토콜 독립 멀티캐스트

PIM(프로토콜 독립 멀티캐스트)은 계층 3 멀티캐스트 라우팅 프로토콜로 구성됩니다.

IP 멀티캐스트 트래픽이 멀티캐스트 그룹 소스에서 서로 다른 계층 3 세그먼트에 있는 수신자에 도달하기 위한 다양한 통신 기법을 제공합니다. 이전 vSAN 버전 6.6 클러스터의 경우 PIM을 사용하여 멀티캐스트 트래픽이 여러 다른 서브넷 간에 전송되도록 설정해야 합니다. PIM 구현에 대해서는 네트워크 벤더에 문의하십시오.

vSAN 파일 서비스에 대한 네트워킹 고려 사항

14

vSAN 파일 서비스는 파일 공유를 제공하기 위해 vSAN 위에 있는 레이어입니다. 현재 SMB, NFSv3 및 NFSv4.1 파일 공유를 지원합니다.

다음은 vSAN 파일 서비스에 대한 네트워크 고려 사항입니다.

- vSAN 파일 서비스 네트워크에서 고정 IP 주소를 파일 서버 IP로 할당해야 합니다. 각 IP는 vSAN 파일 공유에 대한 액세스 지점입니다.
  - 최상의 성능을 위해 IP 주소 수는 vSAN 클러스터의 호스트 수와 같아야 합니다.
  - 모든 고정 IP 주소는 동일한 서브넷에 있어야 합니다.
  - 모든 고정 IP 주소에는 DNS 서버에서 정방향 조회 및 역방향 조회 영역의 일부여야 하는 해당 FQDN이 있습니다.
- 네트워크를 vSAN 파일 서비스 네트워크로 준비해야 합니다.
  - 표준 스위치 기반 네트워크를 사용하는 경우 무차별 모드 및 구축된 전송이 vSAN 파일 서비스 사용 설정 프로세스의 일부로 사용되도록 설정됩니다.
  - DVS 기반 네트워크를 사용하는 경우 vSAN 파일 서비스는 DVS 버전 6.6.0 이상에서 지원됩니다. DVS에서 vSAN 파일 서비스에 대한 전용 포트 그룹을 생성합니다. MacLearning 및 위조 전송은 제공된 DVS 포트 그룹에 vSAN 파일 서비스 사용 설정 프로세스의 일부로 사용하도록 설정됩니다.

    참고 NSX 기반 네트워크를 사용하는 경우 NSX 관리 콘솔에서 제공된 네트워크 엔티티에 대해 MacLearning을 사용하도록 설정되어 있는지 확인하고 모든 호스트 및 파일 서비스 노드가 원하는 NSX-T 네트워크에 연결되어 있는지 확인합니다.
- Kerberos 보안을 사용한 SMB 공유 및 NFS 공유의 경우 AD 도메인 및 조직 구성단위에 대한 정보를 제공해야 합니다(선택 사항). 또한 개체를 생성하고 삭제할 수 있는 충분한 권한이 있는 사용자 계정이 필요합니다.
- 파일 서버가 AD 서버 및 DNS 서버에 액세스할 수 있는지 확인합니다. 파일 서버는 AD 서비스에 필요한 모든 포트에 액세스할 수 있어야 합니다.

다음은 vSAN 파일 서비스에서 네트워크 연결에 사용하는 포트입니다. 이러한 포트가 방화벽에 의해 차단되지 않는지 확인합니다.

서비스	포트 번호	엔티티	연결 요구 사항
SMB(서버 메시지 블록)	TCP 포트 445	파일 서버	파일 서버에 대한 외부 네트워크
로컬 파일 시스템 사용자에 대한 할당량(RQUOTA)	TCP 포트 875	파일 서버	파일 서버에 대한 외부 네트워크
네트워크 파일 시스템(NFS)	TCP 및 UDP 포트 2049	파일 서버	파일 서버에 대한 외부 네트워크. NFSv3은 TCP 및 UDP 포트를 모두 사용할 수 있지만 NFSv4.1은 TCP만 사용합니다.
NFS 마운트	TCP 및 UDP 포트 20048	파일 서버	파일 서버에 대한 외부 네트워크
NSM(네트워크 상태 모니터) 서버 데몬	TCP 및 UDP 포트 27689	파일 서버	파일 서버에 대한 외부 네트워크. 내부 및 외부 통신이 모두 허용되어야 합니다.
NLM(네트워크 잠금 관리자)	TCP 및 UDP 포트 32803	파일 서버	파일 서버에 대한 외부 네트워크. 파일 서버에서 클라이언트로의 연결을 시작할 수 있습니다. 방화벽에서 인바운드 및 아웃바운드 연결을 허용해야 합니다. 기본 포트는 UDP입니다.
Sun 원격 프로시저 호출(sunrpc)	TCP 및 UDP 포트 111	파일 서버	파일 서버에 대한 외부 네트워크
LDAP	TCP 포트 389	AD(Active Directory) 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로
LDAP에서 글로벌 카탈로그로	TCP 포트 3268	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로
Kerberos	TCP 포트 88	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로
Kerberos 암호 변경	TCP 포트 464	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로
DNS(도메인 이름 서버)	TCP 및 UDP 포트 53	DNS 서버	파일 서버에서 DNS 서버로
VDFS(vSAN 분산 파일 시스템) 서버	TCP 포트 1564	ESXi 호스트	vSAN 네트워크 내부
원격 프로시저 호출	TCP 포트 135	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로

서비스	포트 번호	엔티티	연결 요구 사항
NetBIOS 세션 서비스	TCP 포트 139	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로
DNS	UDP 포트 53	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로
LDAP, DC 로케이터 및 네트워크 로그온	UDP 포트 389	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로
임의로 할당된 높은 TCP 포트	TCP 49152 - 65535	AD 서버(AD 도메인이 구성된 경우)	파일 서버에서 AD 서버로

vSAN의 iSCSI에 대한 네트워킹 고려 사항

15

vSAN iSCSI 대상 서비스를 통해 vSAN 클러스터 외부에 있는 호스트와 물리적 워크로드가 vSAN 데이터스토어에 액세스할 수 있습니다. 이 기능은 원격 호스트에 있는 iSCSI 이니시에이터가 블록 수준 데이터를 vSAN 클러스터의 스토리지 디바이스에 있는 iSCSI 대상으로 전송할 수 있도록 합니다.

vSAN의 iSCSI 대상은 다른 vSAN 개체와 유사한 SPBM(스토리지 정책 기반 관리)을 사용하여 관리됩니다. iSCSI LUN의 경우 이 공간은 중복 제거 및 압축을 통해 공간을 절약하고 암호화를 통해 보안을 제공합니다. 보안 강화를 위해 vSAN iSCSI 대상 서비스는 CHAP(Challenge Handshake Authentication Protocol) 및 상호 CHAP 인증을 사용합니다.

vSAN은 고유 IQN(iSCSI 정규화된 이름)으로 각 iSCSI 대상을 식별합니다. iSCSI 대상은 IQN을 사용하여 원격 iSCSI 이니시에이터에 제공되므로 이니시에이터는 대상의 LUN에 액세스할 수 있습니다. vSAN iSCSI 대상 서비스를 사용하여 iSCSI 이니시에이터 그룹을 생성할 수 있습니다. iSCSI 이니시에이터 그룹은 그룹 구성원인 이니시에이터에만 액세스하도록 제한합니다.

다음으로 아래 항목을 읽으십시오.

- vSAN iSCSI 네트워크의 특성

vSAN iSCSI 네트워크의 특성

다음은 vSAN iSCSI 네트워크의 특성입니다.

- iSCSI 라우팅 - iSCSI 이니시에이터는 L3 네트워크를 통해 vSAN iSCSI 대상에 대해 라우팅된 연결을 만들 수 있습니다.
- IPv4 및 IPv6 - vSAN iSCSI 네트워크는 IPv4와 IPv6을 모두 지원합니다.
- IP 보안 - vSAN iSCSI 네트워크의 IPSec은 보안을 강화합니다.

  참고 ESXi 호스트는 IPv6만 사용하는 IPsec을 지원합니다.

- 점보 프레임 - 점보 프레임은 vSAN iSCSI 네트워크에서 지원됩니다.
- NIC 팀 구성 - 모든 NIC 팀 구성이 vSAN iSCSI 네트워크에서 지원됩니다.
- MCS(세션당 다중 연결) - vSAN iSCSI 구현은 MCS를 지원하지 않습니다.

Standard에서 Distributed vSwitch로 마이그레이션

16

vSphere Standard Switch에서 vSphere Distributed Switch로 마이그레이션하고 Network I/O Control을 사용할 수 있습니다. 이렇게 하면 vSAN 트래픽에 QoS(서비스 품질) 우선 순위를 지정할 수 있습니다.

경고 필요하지 않더라도 ESXi 호스트에 대한 액세스 권한이 있는 것이 좋습니다. 문제가 발생하면 ESXi 호스트의 콘솔에 액세스할 수 있습니다.

기존 vSwitch 설정을 기록해 둡니다. 특히 소스의 로드 밸런싱 및 NIC 팀 구성 설정을 기록해 둡니다. 대상 구성이 소스와 일치하는지 확인합니다.

분산 스위치 생성

분산 스위치를 생성하고 이름을 지정합니다.

1 vSphere Client 호스트 및 클러스터 보기에서 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 메뉴 **새 Distributed Switch**를 선택합니다.

2 이름을 입력합니다.

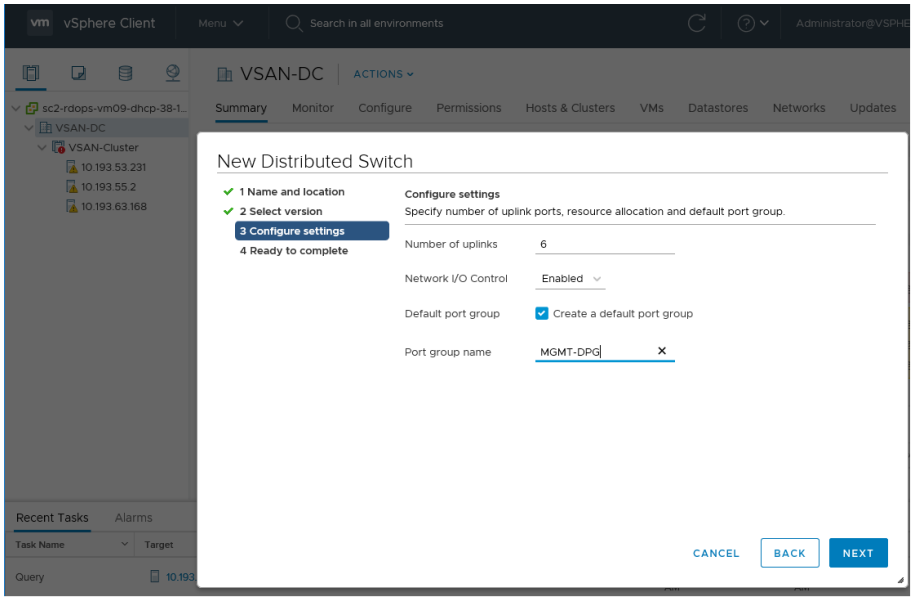
3 vSphere Distributed Switch의 버전을 선택합니다. 이 예에서는 마이그레이션에 버전 6.6.0이 사용됩니다.

4 설정을 추가합니다. 현재 네트워킹에 사용 중인 업링크 수를 확인합니다. 이 예에서는 관리, vMotion, 가상 시스템 각각에 대해 1개씩, vSAN(LAG 구성)에 대해 3개가 있으므로 전체 업링크 수는 6개입니다. 업링크 수로 6을 입력합니다. 사용자 환경이 다를 수 있지만 나중에 편집할 수 있습니다.

   지금 기본 포트 그룹을 생성할 수 있지만, 추가 포트 그룹이 필요합니다.

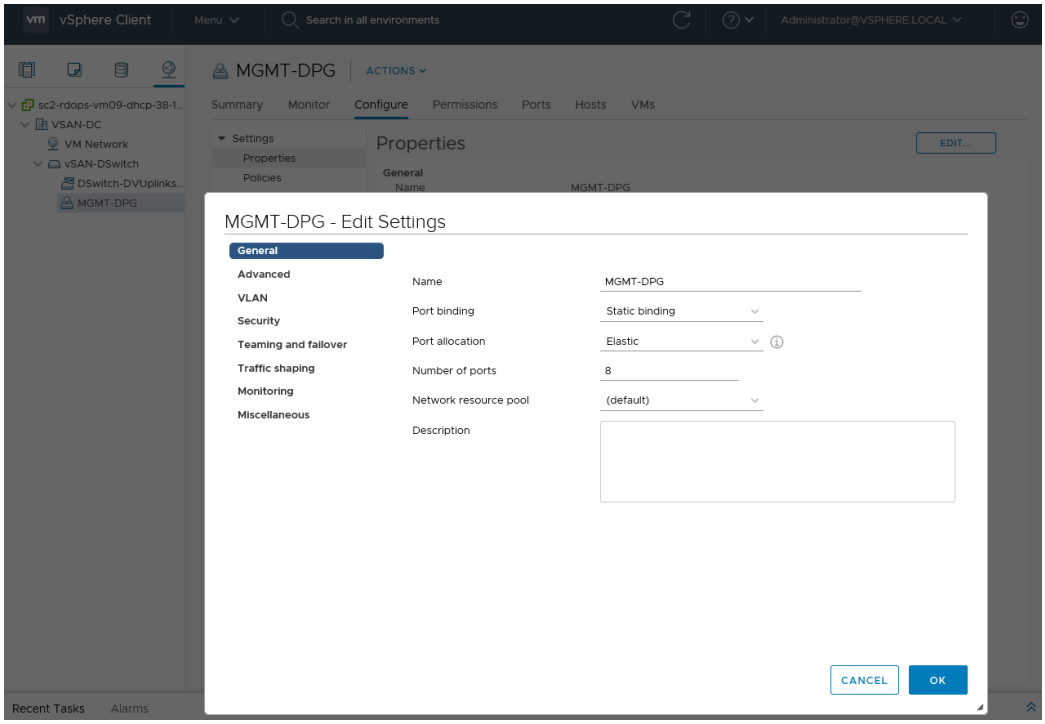
5 분산 스위치의 구성을 마칩니다.

다음 단계는 추가 포트 그룹을 구성하고 생성하는 것입니다.



포트 그룹 생성

관리 네트워크에 대해 단일 기본 포트 그룹이 생성되었습니다. 이 포트 그룹을 편집하여 VLAN 및 NIC 팀 구성, 페일오버 설정과 같이 표준 vSwitch에 있는 관리 포트 그룹의 모든 특성을 지정합니다.



관리 포트 그룹을 구성합니다.

1 vSphere Client 네트워킹 보기에서 분산 포트 그룹을 선택하고 **편집**을 클릭합니다.

2 일부 포트 그룹의 경우 VLAN을 변경해야 합니다. VLAN 51은 관리 VLAN이므로 그에 따라 분산 포트 그룹에 태그를 지정합니다.

3 **확인**을 클릭합니다.

vMotion, 가상 시스템 네트워킹 및 vSAN 네트워킹에 대한 분산 포트 그룹을 생성합니다.

1 vSphere Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹** 메뉴를 선택합니다.

2 이 예에서는 vMotion 네트워크에 대한 포트 그룹을 생성합니다.

Distributed vSwitch에 모든 분산 포트 그룹을 생성합니다. 그런 다음, 업링크, VMkernel 네트워킹 및 가상 시스템 네트워킹을 Distributed vSwitch 및 연결된 분산 포트 그룹으로 마이그레이션합니다.

경고 단계별 방식으로 업링크 및 네트워크를 마이그레이션하여 신중하면서 원활하게 진행합니다.

관리 네트워크 마이그레이션

관리 네트워크(vmk0) 및 관련 업링크(vmnic0)를 Standard vSwitch에서 vDS(distributed vSwitch)로 마이그레이션합니다.

1 vDS에 호스트를 추가합니다.

   a vDS를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리** 메뉴를 선택합니다.

   b vDS에 호스트를 추가합니다. 녹색 추가 아이콘(+)을 클릭하고 클러스터의 모든 호스트를 추가합니다.

2 물리적 어댑터 및 VMkernel 어댑터를 구성합니다.

   a **물리적 어댑터 관리**를 클릭하여 물리적 어댑터 및 VMkernel 어댑터 vmnic0 및 vmk0를 vDS로 마이그레이션합니다.

   b 물리적 어댑터 vmnic0에 대해 vDS의 적절한 업링크를 선택합니다. 이 예에서는 Uplink1을 사용합니다. 해당 물리적 어댑터가 선택되고 업링크가 선택됩니다.

3 vmk0의 관리 네트워크를 Standard vSwitch에서 Distributed vSwitch로 마이그레이션합니다. 각 호스트에서 다음 단계를 수행합니다.

   a vmk0를 선택하고 **포트 그룹 할당**을 클릭합니다.

   b 관리 네트워크에 대해 이전에 생성된 분산 포트 그룹을 할당합니다.

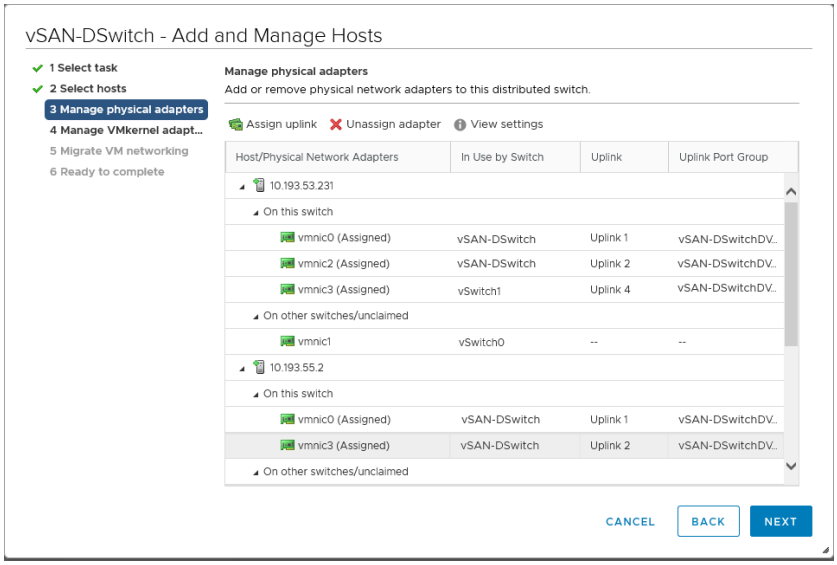
4 구성을 마칩니다.

   a 변경 내용을 검토하여 4개의 호스트, 4개의 업링크(각 호스트의 vmnic0) 및 4개의 VMkernel 어댑터(각 호스트의 vmk0)를 추가하는지 확인합니다.

   b **마침**을 클릭합니다.

각 호스트의 네트워킹 구성을 검토하는 경우 각 호스트에 하나의 업링크(vmnic0)와 vmk0 관리 포트가 있는 스위치 설정을 검토합니다.

다른 네트워크에 대해 이 프로세스를 반복합니다.



vMotion 마이그레이션

vMotion 네트워크를 마이그레이션하려면 관리 네트워크에 사용되는 것과 동일한 단계를 사용합니다.

시작하기 전에 vMotion 네트워크의 분산 포트 그룹에 Standard vSwitch의 포트 그룹과 동일한 특성이 있는지 확인합니다. 그런 다음, VMkernel 어댑터(vmk1)를 사용하여 vMotion에 사용되는 업링크(vmnic1)를 마이그레이션합니다.

vSAN 네트워크 마이그레이션

vSAN 네트워크에 대해 단일 업링크를 사용하는 경우에는 이전과 동일한 프로세스를 수행합니다. 그러나 둘 이상의 업링크를 사용하는 경우 추가 단계가 있습니다.

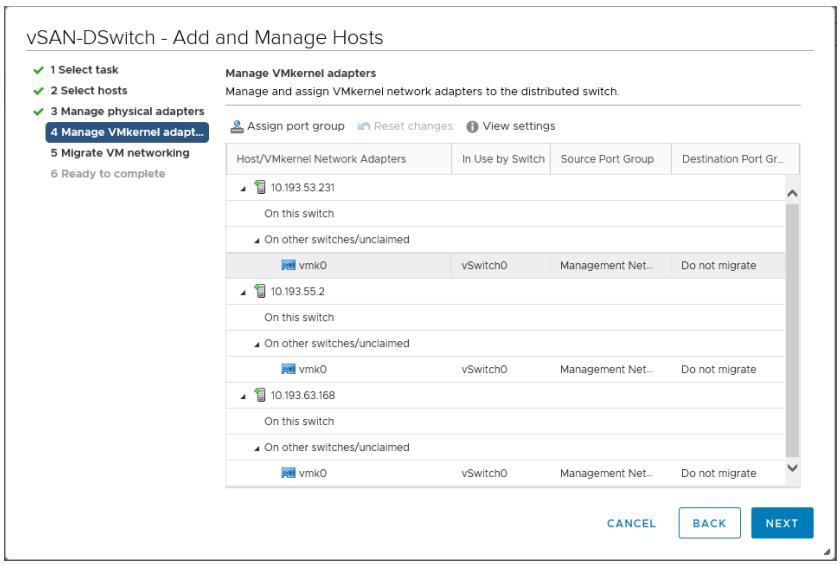
vSAN 네트워크가 LACP(링크 집계)를 사용하거나 다른 VMkernel 네트워크에 대한 다른 VLAN에 있는 경우 일부 업링크를 특정 VMkernel 어댑터에 대해 미사용 상태로 유지합니다.

예를 들어 VMkernel 어댑터 vmk2는 vSAN에 사용됩니다. 그러나 업링크 vmnic3, 4 및 5는 vSAN에 사용되며 LACP 구성에 있습니다. 따라서 vmk2의 경우 다른 모든 vmnic(0, 1 및 2)를 미사용 상태로 두어야 합니다. 마찬가지로 관리 어댑터(vmk0) 및 vMotion 어댑터(vmk0)의 경우 vSAN 업링크/vmnic를 미사용 상태로 둡니다.

분산 포트 그룹의 설정을 수정하고 경로 정책 및 페일오버 설정을 변경합니다. **물리적 네트워크 어댑터 관리** 페이지에서 다중 어댑터에 대한 단계를 수행합니다.

vSAN VMkernel 어댑터(vmk2)를 vSAN에 대한 분산 포트 그룹에 할당합니다.

참고 현재 vSAN 네트워크에 대한 업링크만 마이그레이션하는 경우에는 마이그레이션 이후까지 분산 포트 그룹 설정을 변경하지 못할 수 있습니다. 이 시간 동안 vSAN에 통신 문제가 있을 수 있습니다. 마이그레이션한 후에는 분산 포트 그룹 설정으로 이동하고 모든 정책을 변경한 후 업링크를 미사용 상태로 표시합니다. vSAN 네트워킹은 이 작업을 마치면 정상으로 돌아갑니다. vSAN 상태 서비스를 사용하여 모든 기능이 작동하는지 확인합니다.



VM 네트워크 마이그레이션

네트워크를 Standard vSwitch에서 Distributed vSwitch로 마이그레이션하는 데 필요한 마지막 작업은 VM 네트워크를 마이그레이션하는 것입니다.

호스트 네트워킹을 관리합니다.

1 vDS를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리** 메뉴를 선택합니다.

2 클러스터의 모든 호스트를 선택하여 모든 호스트에 대한 가상 시스템 네트워킹을 Distributed vSwitch로 마이그레이션합니다.

   업링크는 이동하지 마십시오. 하지만 호스트의 VM 네트워킹이 다른 업링크를 사용한 경우 업링크를 Standard vSwitch에서 마이그레이션합니다.

3 Standard vSwitch의 가상 시스템 네트워크에서 Distributed vSwitch의 가상 시스템 분산 포트 그룹으로 마이그레이션할 VM을 선택합니다. **포트 그룹 할당**을 클릭하고 분산 포트 그룹을 선택합니다.

4 변경 사항을 검토하고 **마침**을 클릭합니다. 이 예에서는 VM으로 이동합니다. 기존 Standard vSwitch 가상 시스템 네트워크를 사용하는 모든 템플릿은 가상 시스템으로 변환한 이후 편집해야 합니다. 가상 시스템에 대한 새 분산 포트 그룹을 네트워크로 선택해야 합니다. 이 단계는 마이그레이션 마법사를 통해 수행할 수 없습니다.

Standard vSwitch에 더는 업링크 또는 포트 그룹이 없으므로 제거해도 안전합니다.

이렇게 하면 vSphere Standard Switch에서 vSphere Distributed Switch로의 마이그레이션이 완료됩니다.

vSAN 네트워크에 대한 검사 목록 요약

17

검사 목록 요약을 사용하여 vSAN 네트워크 요구 사항을 확인합니다.

- 공유 10Gb NIC 또는 전용 1Gb NIC를 사용하고 있는지 확인합니다. 플래시 전용 클러스터에는 10Gb NIC가 필요합니다.
- 중복 NIC 팀 구성을 구성했는지 확인합니다.
- ESXi 호스트 NIC에서 흐름 제어가 사용하도록 설정되어 있는지 확인합니다.
- vSAN 네트워크 트래픽에 대한 VMkernel 포트가 각 호스트에 구성되어 있는지 확인합니다.
- 모든 인터페이스에서 동일한 VLAN, MTU 및 서브넷이 있는지 확인합니다.
- 모든 호스트 간에 성공적으로 **`vmkping`**을 성공적으로 실행할 수 있는지 확인합니다. 상태 서비스를 사용하여 확인합니다.
- 점보 프레임을 사용하는 경우 모든 호스트 간의 9000 패킷 크기를 사용하여 **`vmkping`**을 성공적으로 실행할 수 있는지 확인합니다. 상태 서비스를 사용하여 확인합니다.
- vSAN 버전이 v6.6 이전 버전인 경우 네트워크에서 멀티캐스트가 사용하도록 설정되어 있는지 확인하십시오.
- vSAN 버전이 v6.6 이전이고 다중 vSAN 클러스터가 동일한 네트워크에 있는 경우에는 고유한 멀티캐스트 주소를 사용하도록 멀티캐스트를 구성합니다.
- vSAN 버전이 v6.6 이전이고 여러 스위치에 걸쳐 있는 경우 멀티캐스트가 스위치 간에 구성되었는지 확인합니다.
- vSAN 버전이 v6.6 이전이고 라우팅된 경우에는 멀티캐스트 라우팅을 허용하도록 PIM이 구성되어 있는지 확인합니다.
- 물리적 스위치가 vSAN 요구 사항(멀티캐스트, 흐름 제어, 기능 상호 운용성)을 충족할 수 있는지 확인합니다.
- 과도하게 삭제된 패킷 또는 일시 중지 프레임과 같은 성능 문제가 네트워크에 없는지 확인합니다.
- 네트워크 제한이 허용되는 범위 내에 있는지 확인합니다.
- **`iperf`**를 사용하여 vSAN 네트워크 성능을 테스트하고 예상 결과와 일치하는지 확인합니다.