

VMware vSAN 관리

VMware vSphere 6.5

VMware vSAN 6.6.1

VMware 웹 사이트 (<https://docs.vmware.com/kr/>) 에서 최신 기술 문서를 확인할 수 있습니다.
또한 VMware 웹 사이트에서 최신 제품 업데이트를 제공합니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

Copyright © 2017 VMware, Inc. 판권 소유. [저작권 및 상표 정보](#).

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

목차

| | |
|-------------------------------------|-----------|
| VMware vSAN 정보 | 7 |
| vSAN 을 위한 vSphere Client HTML5 | 7 |
| 1 vSAN 소개 | 9 |
| vSAN 개념 | 9 |
| vSAN 용어 및 정의 | 11 |
| vSAN 및 기존 스토리지 | 14 |
| vSAN 클러스터 구축 | 14 |
| 다른 VMware 소프트웨어와 통합 | 15 |
| vSAN 의 제한 사항 | 15 |
| 2 vSAN 을 사용하도록 설정하기 위한 요구 사항 | 17 |
| vSAN 에 대한 하드웨어 요구 사항 | 17 |
| vSAN 에 대한 클러스터 요구 사항 | 18 |
| vSAN 에 대한 소프트웨어 요구 사항 | 18 |
| vSAN 에 대한 네트워킹 요구 사항 | 19 |
| 라이선스 요구 사항 | 19 |
| 3 vSAN 클러스터 설계 및 크기 조정 | 21 |
| vSAN 스토리지 구성 요소 설계 및 크기 조정 | 21 |
| vSAN 호스트 설계 및 크기 조정 | 27 |
| vSAN 클러스터에 대한 설계 고려 사항 | 28 |
| vSAN 네트워크 설계 | 29 |
| vSAN 네트워킹 모범 사례 | 31 |
| vSAN 장애 도메인 설계 및 크기 조정 | 32 |
| 부팅 디바이스 및 vSAN 사용 | 32 |
| vSAN 클러스터의 영구 로깅 | 33 |
| 4 vSAN 에 대해 신규 또는 기존 클러스터 준비 | 35 |
| 스토리지 디바이스의 호환성 선택 또는 확인 | 35 |
| 스토리지 준비 | 36 |
| vSAN 에 대한 메모리 제공 | 39 |
| vSAN 에 대한 호스트 준비 | 40 |
| vSAN 및 vCenter Server 호환성 | 40 |
| 스토리지 컨트롤러 준비 | 40 |
| vSAN 네트워크 구성 | 41 |
| vSAN 라이선스에 대한 고려 사항 | 42 |
| 5 vSAN 클러스터 생성 | 43 |
| vSAN 클러스터의 특성 | 43 |
| vSAN 클러스터를 생성하기 전 | 44 |

| | | |
|-----------|---|------------|
| | vSAN 사용 | 45 |
| | vSAN 구성 지원 및 업데이트 사용 | 54 |
| 6 | 확장된 클러스터를 통해 2개의 사이트에 걸쳐 데이터스토어 확장 | 59 |
| | 확장된 클러스터 소개 | 59 |
| | 확장된 클러스터 설계 고려 사항 | 61 |
| | 확장된 클러스터 사용의 모범 사례 | 62 |
| | 확장된 클러스터에 대한 네트워크 설계 | 62 |
| | vSAN 확장된 클러스터 구성 | 63 |
| | 기본 장애 도메인 변경 | 64 |
| | 감시 호스트 변경 | 64 |
| | vSAN 감시 장치 배포 | 64 |
| | 감시 트래픽에 대한 네트워크 인터페이스 구성 | 65 |
| | 확장된 클러스터를 표준 vSAN 클러스터로 변환 | 67 |
| 7 | vSAN 클러스터에서 공간 효율성 향상 | 69 |
| | vSAN 공간 효율성 소개 | 69 |
| | 중복 제거 및 압축 사용 | 69 |
| | RAID 5 또는 RAID 6 이레이저 코딩 사용 | 73 |
| | RAID 5 또는 RAID 6 설계 고려 사항 | 74 |
| 8 | vSAN 클러스터에서 암호화 사용 | 75 |
| | vSAN 암호화 작동 방식 | 75 |
| | vSAN 암호화에 대한 설계 고려 사항 | 76 |
| | KMS 클러스터 설정 | 76 |
| | 새 vSAN 클러스터에서 암호화 사용 | 81 |
| | 새 암호화 키 생성 | 81 |
| | 기존 vSAN 클러스터에서 vSAN 암호화 사용 | 82 |
| | vSAN 암호화 및 코어 덤프 | 83 |
| 9 | vSAN 클러스터 업그레이드 | 87 |
| | vSAN 을 업그레이드하기 전 | 88 |
| | vCenter Server 업그레이드 | 89 |
| | ESXi 호스트 업그레이드 | 89 |
| | vSAN 디스크 형식 정보 | 91 |
| | vSAN 클러스터 업그레이드 확인 | 95 |
| | RVC 업그레이드 명령 옵션 사용 | 96 |
| | vSphere Update Manager에 대한 vSAN 빌드 권장 사항 | 96 |
| 10 | vSAN 클러스터에서 디바이스 관리 | 99 |
| | 디스크 그룹 및 디바이스 관리 | 99 |
| | 개별 디바이스 사용 | 101 |
| 11 | vSAN 클러스터 확장 및 관리 | 107 |
| | vSAN 클러스터 확장 | 107 |
| | 유지 보수 모드 사용 | 111 |
| | vSAN 클러스터에서 장애 도메인 관리 | 113 |
| | vSAN iSCSI 대상 서비스 사용 | 117 |

하이브리드 vSAN 클러스터를 플래시 전용 클러스터로 마이그레이션 120
 vSAN 클러스터 전원 끄기 121

12 vSAN 정책 사용 123

vSAN 정책 정보 123
 vSAN 스토리지 제공자 보기 126
 vSAN 기본 스토리지 정책 정보 126
 vSAN 데이터스토어에 기본 스토리지 정책 할당 128
 vSAN 에 대한 가상 시스템 스토리지 정책 정의 128

13 vSAN 모니터링 131

vSAN 클러스터 모니터링 131
 vSAN 용량 모니터링 132
 vSAN 클러스터에서 가상 디바이스 모니터링 133
 vSAN 클러스터 다시 동기화 정보 133
 vSAN 데이터스토어에 참여하는 디바이스 모니터링 135
 vSAN 상태 모니터링 135
 vSAN 성능 모니터링 138
 vSAN 클러스터 재조정 정보 142
 vSAN 기본 경보 사용 144
 경보 생성에 VMkernel 관찰 사용 145

14 vSAN 장애 처리 및 문제 해결 147

vSAN 에 Esxcli 명령 사용 147
 ESXi 호스트에 대한 vSAN 구성이 실패할 수 있음 150
 비준수 가상 시스템 개체가 즉시 준수 상태가 되지 않음 150
 vSAN 클러스터 구성 문제 151
 vSAN 에서 장애 처리 151
 vSAN 클러스터 종료 164

색인 165

VMware vSAN 정보

VMware vSAN 관리에서는 VMware vSphere® 환경에서 VMware vSAN 클러스터를 구성, 관리 및 모니터링하는 방법을 설명합니다. 또한 VMware vSAN 관리에서는 vSAN 클러스터에서 스토리지 용량 디바이스의 역할을 하는 로컬 물리적 스토리지 리소스를 구성하고, vSAN 데이터스토어에 배포된 가상 시스템의 스토리지 정책을 정의하고, vSAN 클러스터에서 장애를 관리하는 방법을 설명합니다.

대상 사용자

이 정보는 가상화 기술, 일상적인 데이터 센터 작업 및 vSAN 개념에 익숙한 숙련된 가상화 관리자용으로 작성되었습니다.

vSAN 을 위한 vSphere Client HTML5

vSphere Client

vSphere Client는 vSphere Web Client와 함께 vCenter Server에 동봉되어 제공되는 새 HTML5 기반 클라이언트입니다. 새 vSphere Client는 vSphere Web Client와 동일한 여러 인터페이스 용어, 토폴로지 및 워크플로를 사용합니다. 하지만 vSphere Client는 vSAN을 지원하지 않습니다. vSAN 사용자는 vSphere Web Client를 해당 용도에 계속해서 사용해야 합니다.

참고 vSphere Web Client의 기능 일부는 vSphere 6.5 릴리스의 vSphere Client에 구현되지 않았습니다. 지원되지 않는 기능의 최신 목록을 보려면 vSphere Client의 기능 업데이트 가이드 (<http://www.vmware.com/info?id=1413>)를 참조하십시오.

vSAN 소개

VMware vSAN은 기본적으로 ESXi 하이퍼바이저의 일부로 실행되는 소프트웨어의 분산 계층입니다. vSAN은 호스트 클러스터의 로컬 또는 직접 연결 용량 디바이스를 집계하여 vSAN 클러스터의 모든 호스트에서 공유되는 단일 스토리지 풀을 생성합니다.

vSAN은 HA, vMotion 및 DRS와 같이 공유 스토리지가 필요한 VMware 기능을 지원하는 동시에 외부 공유 스토리지의 필요성을 없애고 스토리지 구성 및 가상 시스템 프로비저닝 작업을 간소화합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN 개념,”](#) (9 페이지)
- [“vSAN 용어 및 정의,”](#) (11 페이지)
- [“vSAN 및 기존 스토리지,”](#) (14 페이지)
- [“vSAN 클러스터 구축,”](#) (14 페이지)
- [“다른 VMware 소프트웨어와 통합,”](#) (15 페이지)
- [“vSAN의 제한 사항,”](#) (15 페이지)

vSAN 개념

VMware vSAN은 소프트웨어 정의 방식을 사용하여 가상 시스템을 위한 공유 스토리지를 생성합니다. VMware vSAN은 ESXi 호스트의 로컬 물리적 스토리지 리소스를 가상화한 후, 서비스 품질 요구 사항에 따라 분할하여 가상 시스템 및 애플리케이션에 할당할 수 있는 스토리지 풀로 변환합니다. vSAN은 ESXi 하이퍼바이저에 직접 구현됩니다.

vSAN은 하이브리드 또는 플래시 전용 클러스터로 작동하도록 구성할 수 있습니다. 하이브리드 클러스터에서는 플래시 디바이스를 캐시 계층에 사용하고 자기 디스크를 스토리지 용량 계층에 사용합니다. 플래시 전용 클러스터에서는 플래시 디바이스가 캐시 및 용량 모두에 사용됩니다.

vSAN은 기존 호스트 클러스터에 활성화하거나 새 클러스터를 생성할 때 활성화할 수 있습니다. vSAN은 모든 로컬 용량 디바이스를 vSAN 클러스터 내의 모든 호스트가 공유하는 단일 데이터스토어로 집계합니다. 클러스터에 용량 디바이스 또는 용량 디바이스가 포함된 호스트를 추가하여 데이터스토어를 확장할 수 있습니다. vSAN은 클러스터의 모든 ESXi 호스트가 비슷하거나 동일한 스토리지 구성을 포함하여 클러스터 멤버 전체에서 비슷하거나 동일한 구성을 공유할 때 가장 잘 작동합니다. 이 일관된 구성은 클러스터의 모든 디바이스 및 호스트 간에 가상 시스템 스토리지 구성 요소의 균형을 유지합니다. 로컬 디바이스가 없는 호스트도 vSAN 데이터스토어에 참여하고 해당 가상 시스템을 실행할 수 있습니다.

호스트가 vSAN 데이터스토어에 해당 로컬 스토리지 디바이스를 제공하는 경우, 호스트는 하나 이상의 플래시 캐시용 디바이스와 하나 이상의 용량용 디바이스를 제공해야 합니다. 용량 디바이스는 데이터 디스크라고도 합니다.

제공하는 호스트의 디바이스는 하나 이상의 디스크 그룹을 형성합니다. 각 디스크 그룹에는 플래시 캐시 디바이스 하나와 영구 스토리지를 위한 하나 또는 여러 개의 용량 디바이스가 포함됩니다. 각 호스트는 여러 디스크 그룹을 사용하도록 구성할 수 있습니다.

vSAN 클러스터의 설계 및 크기 조정에 대한 모범 사례, 용량 고려 사항 및 일반 권장 사항은 VMware vSAN 설계 및 크기 조정 가이드를 참조하십시오.

vSAN의 특성

이 항목에서는 vSAN, 클러스터 및 데이터스토어에 적용되는 특성을 요약합니다.

vSAN은 환경에 수많은 이점을 제공합니다.

표 1-1. vSAN 기능

| 지원되는 기능 | 설명 |
|-----------------------------|---|
| 공유 스토리지 지원 | vSAN은 공유 스토리지가 필요한 VMware 기능(예: HA, vMotion 및 DRS)을 지원합니다. 예를 들어 호스트가 오버로드 되는 경우 DRS는 가상 시스템을 클러스터의 다른 호스트로 마이그레이션할 수 있습니다. |
| JBOD(Just a Bunch Of Disks) | vSAN은 블레이드 서버 환경에서 사용하기 위한 JBOD를 지원합니다. 클러스터에 블레이드 서버가 포함된 경우 블레이드 서버에 연결된 JBOD 스토리지를 사용하여 데이터스토어 용량을 확장할 수 있습니다. |
| 온디스크 형식 | vSAN 6.6은 vSAN 클러스터당 고도로 확장 가능한 스냅샷 및 복제 관리 지원을 제공하는 온디스크 가상 파일 형식 5.0을 지원합니다. vSAN 클러스터당 지원되는 가상 시스템 스냅샷 및 복제수에 대한 자세한 내용은 구성 최대값 설명서를 참조하십시오. |
| 플래시 전용 및 하이브리드 구성 | vSAN은 플래시 전용 또는 하이브리드 클러스터에 대해 구성할 수 있습니다. |
| 장애 도메인 | vSAN은 vSAN 클러스터가 데이터 센터의 여러 랙 또는 블레이드 서버 세시에 걸쳐 배포된 경우 랙 또는 세시 장애로부터 호스트를 보호하기 위한 장애 도메인의 구성을 지원합니다. |
| 확장된 클러스터 | vSAN은 2개의 지리적 위치에 걸쳐 있는 확장된 클러스터를 지원합니다. |
| vSAN Health Service | vSAN Health Service에는 클러스터 구성 요소 문제의 원인을 모니터링하고 문제를 해결 및 진단하며 잠재적인 위험을 식별하기 위한 미리 구성된 상태 점검 테스트가 포함됩니다. |
| vSAN 성능 서비스 | vSAN 성능 서비스에는 IOPS, 처리량, 지연 시간 및 정체를 모니터링하는 데 사용되는 통계 차트가 포함됩니다. vSAN 클러스터, 호스트, 디스크 그룹, 디스크 및 VM의 성능을 모니터링할 수 있습니다. |
| vSphere 스토리지 기능과 통합 | vSAN은 기존에 VMFS 및 NFS 스토리지와 함께 사용된 vSphere 데이터 관리 기능과 통합됩니다. 이러한 기능에는 스냅샷, 연결된 복제, vSphere Replication 및 vSphere APIs for Data Protection이 있습니다. |
| 가상 시스템 스토리지 정책 | vSAN은 VM 스토리지 정책과 함께 작동하여 VM 중심의 스토리지 관리 방식을 지원합니다. 배포 중에 가상 시스템에 스토리지 정책을 할당하지 않으면 vSAN 기본 스토리지 정책이 VM에 자동으로 할당됩니다. |
| 빠른 프로비저닝 | vSAN을 사용하면 가상 시스템 생성 및 배포 작업 도중 vCenter Server®에서 스토리지를 빠르게 프로비저닝할 수 있습니다. |

vSAN 용어 및 정의

vSAN에는 이해하고 있어야 하는 몇 가지 중요한 용어와 정의가 포함되어 있습니다.

vSAN을 시작하기 전에 주요 vSAN 용어 및 정의를 검토합니다.

디스크 그룹

디스크 그룹은 호스트의 물리적 스토리지 용량 단위이며 vSAN 클러스터에 성능과 용량을 제공하는 물리적 디바이스 그룹입니다. vSAN 클러스터에 로컬 디바이스를 제공하는 각 ESXi 호스트에서 디바이스는 디스크 그룹으로 구성됩니다.

각 디스크 그룹에는 하나의 플래시 캐시 디바이스와 하나 또는 여러 개의 용량 디바이스가 있어야 합니다. 캐시에 사용되는 디바이스는 디스크 그룹 간에 공유할 수 없으며 다른 용도로 사용할 수 없습니다. 단일 캐시 디바이스를 단일 디스크 그룹 전용으로 사용해야 합니다. 하이브리드 클러스터에서는 플래시 디바이스를 캐시 계층에 사용하고 자기 디스크를 스토리지 용량 계층에 사용합니다. 플래시 전용 클러스터에서는 캐시 및 용량 모두에 플래시 디바이스가 사용됩니다. 디스크 그룹 생성 및 관리에 대한 자세한 내용은 [10장, “vSAN 클러스터에서 디바이스 관리,”](#) (99 페이지) 항목을 참조하십시오.

사용 용량

사용 용량은 특정 시점에 하나 이상의 가상 시스템에서 사용하는 물리적 용량입니다. VMDK의 사용 크기, 보호 복제본 등을 비롯한 여러 요소가 사용 용량을 결정합니다. 캐시 크기 조정을 위해 계산하는 경우 보호 복제본에 사용되는 용량은 고려하지 마십시오.

개체 기반 스토리지

vSAN은 데이터를 개체라는 유연한 데이터 컨테이너의 형태로 저장하고 관리합니다. 개체는 해당 데이터 및 메타데이터가 클러스터 전체에 분산되어 있는 논리적 불륨입니다. 예를 들어 모든 스냅샷과 마찬가지로 모든 VMDK는 개체입니다. vSAN 데이터스토어에서 가상 시스템을 프로비저닝하는 경우 vSAN은 각 가상 디스크에 대해 여러 구성 요소로 이루어진 일련의 개체를 생성하고 가상 시스템의 모든 메타데이터 파일을 저장하는 컨테이너 개체인 VM 홈 네임스페이스도 생성합니다. vSAN은 할당된 가상 시스템 스토리지 정책을 기반으로 각 개체를 개별적으로 프로비저닝하고 관리합니다. 여기에는 각 개체에 대해 RAID 구성을 생성하는 것도 포함될 수 있습니다.

vSAN은 가상 디스크에 대한 개체를 생성하고 클러스터에 개체를 분산하는 방법을 결정할 때 다음과 같은 요소를 고려합니다.

- vSAN은 지정된 가상 시스템 스토리지 정책 설정에 따라 가상 디스크 요구 사항이 적용되는지 확인합니다.
- vSAN은 프로비저닝 시 올바른 클러스터 리소스가 사용되는지 확인합니다. 예를 들어 vSAN은 보호 정책을 기반으로 생성할 복제본 수를 결정합니다. 성능 정책은 각 복제본에 대해 할당된 Flash Read Cache의 양, 각 복제본에 대해 생성할 스트라이프의 수 그리고 이것을 배치할 클러스터 내의 위치를 결정합니다.
- vSAN은 가상 디스크의 정책 규정 준수 상태를 지속적으로 모니터링하고 보고합니다. 비준수 정책 상태가 발견되면 기본적인 문제를 반드시 해결해야 합니다.

참고 필요한 경우 VM 스토리지 정책 설정을 편집할 수 있습니다. 스토리지 정책 설정 변경은 가상 시스템 액세스에 영향을 미치지 않습니다. vSAN은 재구성에 사용되는 스토리지 및 네트워크 리소스를 적극적으로 조절하여 개체 재구성이 일반적인 워크로드에 미치는 영향을 최소화합니다. VM 스토리지 정책 설정을 변경하는 경우 vSAN이 개체 재생성 프로세스와 이후의 다시 동기화를 시작할 수 있습니다. [“vSAN 클러스터 다시 동기화 정보,”](#) (133 페이지)를 참조하십시오.

- vSAN은 미리 및 감시와 같은 필수 보호 구성 요소가 별도의 호스트 또는 장애 도메인에 배치되었는지 확인합니다. 예를 들어 vSAN은 장애 시 구성 요소를 재구축하기 위해 가상 시스템 개체의 보호 구성 요소가 2개의 서로 다른 호스트에 배치되거나 장애 도메인에 배치되어야 한다는 배치 규칙을 충족하는 ESXi 호스트를 찾습니다.

vSAN 데이터스토어

클러스터에서 vSAN을 사용하도록 설정하면 단일 vSAN 데이터스토어가 생성됩니다. 이 데이터스토어는 가상 볼륨, VMFS 및 NFS를 포함하여 사용할 수 있는 데이터스토어 목록에 또 다른 데이터스토어 유형으로 나타납니다. 단일 vSAN 데이터스토어는 각 가상 시스템 또는 각 가상 디스크에 대해 서로 다른 서비스 수준을 제공할 수 있습니다. vCenter Server®에서 vSAN 데이터스토어의 스토리지 특성은 기능 집합으로 나타납니다. 가상 시스템의 스토리지 정책을 정의할 때 이러한 기능을 참조할 수 있습니다. vSAN은 나중에 가상 시스템을 배포할 때 이 정책을 사용하여 각 가상 시스템의 요구 사항에 따라 최적의 방식으로 가상 시스템을 배치합니다. 스토리지 정책 사용에 대한 일반적인 내용은 vSphere Storage 설명서를 참조하십시오.

vSAN 데이터스토어에는 고려해야 할 특정 특성이 있습니다.

- vSAN은 클러스터에 스토리지를 제공하는지 여부에 관계없이 클러스터의 모든 호스트가 액세스할 수 있는 단일 vSAN 데이터스토어를 제공합니다. 각 호스트는 가상 볼륨, VMFS 또는 NFS를 포함한 다른 데이터스토어를 마운트할 수도 있습니다.
- Storage vMotion을 사용하여 vSAN 데이터스토어, NFS 데이터스토어 및 VMFS 데이터스토어 간에 가상 시스템을 이동할 수 있습니다.
- 용량에 사용되는 자기 디스크와 플래시 디바이스만 데이터스토어 용량으로 제공할 수 있습니다. 플래시 캐시에 사용되는 디바이스는 데이터스토어의 일부로 포함되지 않습니다.

개체 및 구성 요소

각 개체는 VM 스토리지 정책에서 사용 중인 기능을 통해 결정되는 일련의 구성 요소로 이루어져 있습니다. 예를 들어 허용할 수 있는 장애의 기본 수준이 1로 설정된 경우 vSAN은 감시 및 복제본과 같은 보호 구성 요소가 vSAN 클러스터에 있는 별도의 호스트에 배치되도록 합니다. 여기서 각 복제본은 개체 구성 요소입니다. 또한 동일한 정책에서 개체당 디스크 스트라이프의 수가 2개 이상으로 구성된 경우 vSAN은 여러 용량 디바이스에 걸쳐 개체를 스트라이핑하며, 각 스트라이프는 지정된 개체의 구성 요소로 간주됩니다. 필요한 경우 vSAN은 큰 개체를 여러 구성 요소로 나눌 수도 있습니다.

vSAN 데이터스토어에는 다음과 같은 개체 유형이 포함되어 있습니다.

| | |
|--------------------|--|
| VM 홈 네임스페이스 | .vmx, 로그 파일, vmdk, 스냅샷 델타 설명 파일과 같은 모든 가상 시스템 구성 파일이 저장되어 있는 가상 시스템 홈 디렉토리입니다. |
| VMDK | 가상 시스템의 하드 디스크 드라이브 내용을 저장하는 가상 시스템 디스크 또는 .vmdk 파일입니다. |
| VM 스왑 개체 | 가상 시스템 전원을 켜를 때 생성됩니다. |
| 스냅샷 델타 VMDK | 가상 시스템 스냅샷이 작성될 때 생성됩니다. |
| 메모리 개체 | 가상 시스템을 생성하거나 일시 중단할 때 스냅샷 메모리 옵션이 선택되면 생성됩니다. |

가상 시스템 규정 준수 상태: 준수 및 비준수

하나 이상의 가상 시스템 개체가 할당된 스토리지 정책 요구 사항을 충족하지 못하는 경우 해당 가상 시스템은 비준수 상태로 간주됩니다. 예를 들어 미리 복사본 중 하나에 액세스할 수 없는 경우 비준수 상태가 될 수 있습니다. 가상 시스템이 스토리지 정책에 정의된 요구 사항을 준수하면 해당 가상 시스템은 준수 상태입니다. 가상 디스크 페이지의 물리적 디스크 배치 탭에서 가상 시스템 개체 준수 상태를 확인할 수 있습니다. vSAN 클러스터 문제 해결에 대한 자세한 내용은 “vSAN에서 장애 처리,” (151 페이지) 항목을 참조하십시오.

구성 요소 상태: 성능 저하됨 및 없음 상태

vSAN은 구성 요소의 다음 장애 상태를 확인합니다.

- 성능 저하됨. vSAN에서 영구적인 구성 요소 장애를 감지하고 장애가 발생한 구성 요소가 원래 작동 상태로 복구될 수 없다고 판단할 경우 구성 요소는 성능 저하됨 상태가 됩니다. 이 경우 vSAN은 성능 저하됨 상태의 구성 요소를 즉시 재구축하기 시작합니다. 이 상태는 장애가 발생한 디바이스에 구성 요소가 있을 때 발생할 수 있습니다.
- 없음. vSAN에서 구성 요소 및 해당 모든 데이터가 복구되어 vSAN을 원래 상태로 되돌릴 수 있는 일시적인 구성 요소 장애를 감지하는 경우 구성 요소는 없음 상태가 됩니다. 이 상태는 호스트를 다시 시작하거나 vSAN 호스트에서 디바이스를 분리할 때 발생할 수 있습니다. vSAN은 60분을 대기한 후 없음 상태의 구성 요소를 재구축하기 시작합니다.

개체 상태: 정상 및 비정상

클러스터의 장애 수와 유형에 따라 개체는 다음 상태 중 하나일 수 있습니다.

- 정상. 하나 이상의 전체 RAID 1 미러를 사용할 수 있거나 필요한 최소 수의 데이터 세그먼트를 사용할 수 있으면 개체가 정상인 것으로 간주됩니다.
- 비정상. 전체 미러를 사용할 수 없거나 필요한 최소 수의 데이터 세그먼트를 RAID 5 또는 RAID 6 개체에 사용할 수 없으면 개체가 비정상인 것으로 간주됩니다. 개체 투표의 50% 미만이 사용 가능한 경우 해당 개체는 비정상입니다. 클러스터에서 장애가 여러 번 일어나면 개체가 비정상으로 될 수 있습니다. 개체의 작동 상태가 비정상으로 판단되면 연결된 VM의 가용성에도 영향을 줍니다.

감시

감시는 메타데이터만 포함하고 실제 애플리케이션 데이터는 포함하지 않는 구성 요소입니다. 이것은 잠재적 장애 후 아직 사용 가능한 데이터스토어 구성 요소의 가용성에 대해 결정을 내려야 할 때 타이브레이크 역할을 합니다. 감시는 온디스크 형식 1.0 사용 시 vSAN 데이터스토어에서 약 2MB의 메타데이터 공간을 사용하고 온디스크 형식 버전 2.0 이상 사용 시 4MB를 사용합니다.

vSAN 6.0 이상에서는 비대칭 투표 시스템을 사용하여 쿼럼을 유지 관리하며 각 구성 요소는 개체의 가용성을 결정하기 위해 두 개 이상의 표를 가질 수 있습니다. VM의 스토리지 개체를 구성하는 투표 중 항상 액세스할 수 있는 투표가 50%를 넘어야만 개체가 사용 가능한 것으로 간주됩니다. 모든 호스트에서 액세스할 수 있는 투표가 50% 이하인 경우에는 vSAN 데이터스토어에서 해당 개체에 더 이상 액세스할 수 없습니다. 액세스할 수 없는 개체는 연결된 VM의 가용성에 영향을 줄 수 있습니다.

SPBM(스토리지 정책 기반 관리)

vSAN을 사용할 경우 성능, 가용성 등의 가상 시스템 스토리지 요구 사항을 정책의 형태로 정의할 수 있습니다. vSAN은 vSAN 데이터스토어에 배포된 가상 시스템에 하나 이상의 가상 시스템 스토리지 정책이 할당되도록 합니다. 가상 시스템의 스토리지 요구 사항을 알고 있는 경우 스토리지 정책을 정의하고 가상 시스템에 정책을 할당할 수 있습니다. 가상 시스템을 배포할 때 스토리지 정책을 적용하지 않으면 vSAN은 허용할 수 있는 장애의 기본 수준이 1로 구성된 기본 vSAN 정책, 각 개체를 위한 단일 디스크 스트라이프 및 썬 프로비저닝된 가상 디스크를 자동으로 할당합니다. 최상의 결과를 얻으려면 정책의 요구 사항이 기본 스토리지 정책에 정의된 것과 같더라도 사용자 고유의 가상 시스템 스토리지 정책을 정의하십시오. vSAN 스토리지 정책 사용에 대한 자세한 내용은 12장, “vSAN 정책 사용,” (123 페이지) 항목을 참조하십시오.

RVC(Ruby vSphere Console)

RVC(Ruby vSphere Console)는 vSAN 클러스터 관리 및 문제 해결에 사용되는 명령줄 인터페이스를 제공합니다. RVC는 esxcli가 제공하는 호스트 중심의 보기 대신 클러스터 전체의 보기를 제공합니다. RVC는 vCenter Server Appliance 및 Windows용 vCenter Server와 함께 제공되기 때문에 별도로 설치하지 않아도 됩니다. RVC 명령에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.

vSphere PowerCLI

VMware vSphere PowerCLI는 구성 및 관리 작업을 자동화하는 데 도움이 되는 vSAN에 대한 명령 줄 스크립팅 지원을 추가합니다. vSphere PowerCLI는 vSphere API에 대한 Windows PowerShell 인터페이스를 제공합니다. PowerCLI에는 vSAN 구성 요소 관리를 위한 cmdlet이 포함되어 있습니다. vSphere PowerCLI 사용에 관한 자세한 내용은 vSphere PowerCLI 설명서를 참조하십시오.

vSAN Observer

VMware vSAN Observer는 RVC에서 실행되는 웹 기반 도구로 vSAN 클러스터에 대한 심층적인 성능 분석과 모니터링에 사용됩니다. vSAN Observer를 사용하여 용량 계층의 성능 통계, 물리적 디스크 그룹에 대한 통계 정보, CPU의 현재 로드, vSAN 메모리 풀의 사용량, vSAN 클러스터 전반의 물리적 및 메모리 내 개체 분포를 보십시오.

RVC 및 vSAN Observer의 구성, 시작 및 사용에 대한 자세한 내용은 vSAN 문제 해결 참조 설명서를 참조하십시오.

vSAN 및 기존 스토리지

vSAN이 기존 스토리지 어레이와 많은 특성을 공유하지만 vSAN의 전체적인 동작 및 기능은 다릅니다. 예를 들어 vSAN은 ESXi 호스트만 관리하고 사용할 수 있으며 단일 vSAN 인스턴스는 하나의 클러스터만 지원할 수 있습니다.

또한 vSAN과 기존 스토리지는 다음과 같은 주요 방식에서 다릅니다.

- vSAN은 FC(Fibre Channel)나 SAN(Storage Area Network) 등과 같이 가상 시스템 파일을 원격으로 저장하기 위한 외부 네트워크 스토리지를 필요로 하지 않습니다.
- 스토리지 관리자는 기존 스토리지를 사용하여 다른 스토리지 시스템에 스토리지 공간을 사전 할당합니다. vSAN은 자동으로 ESXi 호스트의 로컬 물리적 스토리지 리소스를 단일 스토리지 풀로 전환합니다. 이러한 풀은 해당 서비스 품질 요구 사항에 따라 나뉘고 가상 시스템 및 애플리케이션에 할당될 수 있습니다.
- iSCSI 대상 서비스는 LUN을 사용하여 원격 호스트의 이니시에이터가 블록 수준 데이터를 vSAN 클러스터의 스토리지 디바이스로 전송할 수 있도록 하지만 vSAN에는 LUN 또는 NFS 공유에 기반한 전통적인 스토리지 볼륨 개념이 없습니다.
- FCP와 같은 일부 표준 스토리지 프로토콜은 vSAN에 적용되지 않습니다.
- vSAN은 vSphere와 고도로 통합되었습니다. 기존 스토리지와 비교하여 vSAN에 대한 전용 플러그인이나 스토리지 콘솔이 필요하지 않습니다. vSphere Web Client를 사용하여 vSAN을 배포하고 관리하고 모니터링할 수 있습니다.
- 전담 스토리지 관리자는 vSAN을 관리하지 않아도 됩니다. 대신 vSphere 관리자는 vSAN 환경을 관리할 수 있습니다.
- vSAN 사용을 통해 새 VM을 배포할 때 VM 스토리지 정책이 자동으로 할당됩니다. 스토리지 정책은 필요에 따라 동적으로 변경될 수 있습니다.

vSAN 클러스터 구축

vSAN을 고려하는 경우 vSAN 클러스터 배포를 위한 2개 이상의 구성 솔루션 중에서 선택할 수 있습니다.

사용자의 요구 사항에 따라 다음과 같은 방식 중 하나로 vSAN을 배포할 수 있습니다.

vSAN Ready 노드

vSAN Ready 노드는 Cisco, Dell, Fujitsu, IBM 및 Supermicro와 같은 VMware 파트너가 제공하는 vSAN 소프트웨어의 사전 구성된 솔루션입니다. 이 솔루션에는 서버 OEM 및 VMware에서 권장하는 vSAN 배포를 위한 테스트를 완료했으며 인증된 하드웨어 폼 팩터의 검증된 서버 구성이 포함되어 있습니다. 특정 파트너를 위한 vSAN Ready 노드 솔루션에 대한 자세한 내용은 VMware 파트너 웹 사이트를 참조하십시오.

사용자 정의 vSAN 클러스터

<http://www.vmware.com/resources/compatibility/search.php>의 vSAN 호환성 가이드 (VCG) 웹 사이트에 나열되어 있는 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러와 같은 개별 소프트웨어 및 하드웨어 구성 요소를 선택하여 vSAN 클러스터를 구축할 수 있습니다. 인증되었으며 VCG 웹 사이트에 나열되어 있는 서버, 스토리지 I/O 컨트롤러, 용량 및 플래시 캐시 디바이스, 메모리, CPU당 확보해야 하는 코어 수 등을 선택할 수 있습니다. vSAN에서 지원되는 소프트웨어 및 하드웨어 구성 요소, 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러를 선택하기 전에 VCG 웹 사이트에서 호환성 정보를 검토합니다. vSAN 클러스터를 설계할 때 VCG 웹 사이트에 나열되어 있는 디바이스, 펌웨어 및 드라이버만 사용합니다. VCG에 나열되어 있지 않은 소프트웨어 및 하드웨어 버전을 사용할 경우 클러스터 장애나 예기치 않은 데이터 손실이 발생할 수 있습니다. vSAN 클러스터 설계에 대한 자세한 내용은 **3장, “vSAN 클러스터 설계 및 크기 조정,”** (21 페이지) 항목을 참조하십시오.

다른 VMware 소프트웨어와 통합

vSAN은 가동 및 실행한 후 나머지 VMware 소프트웨어 스택과 통합됩니다. vSphere vMotion, 스냅샷, 복제, DRS(Distributed Resource Scheduler), vSphere High Availability, vCenter Site Recovery Manager 등의 vSphere 구성 요소 및 기능을 사용하여 기존 스토리지로 수행 가능한 대부분의 작업을 수행할 수 있습니다.

vSphere HA와 통합

동일한 클러스터에서 vSphere HA 및 vSAN을 사용하도록 설정할 수 있습니다. 기존 데이터스토어와 마찬가지로 vSphere HA는 vSAN 데이터스토어의 가상 시스템에 대해 동일한 수준의 보호를 제공합니다. 이 보호 수준은 vSphere HA 및 vSAN이 상호 작용할 때 특정 제한 사항을 적용합니다. vSphere HA 및 vSAN 통합에 대한 특정 고려 사항은 **“vSAN 및 vSphere HA 사용,”** (52 페이지)의 내용을 참조하십시오.

VMware Horizon View와 통합

vSAN을 VMware Horizon View와 통합할 수 있습니다. 통합할 경우 vSAN은 가상 데스크톱 환경에 다음과 같은 이점을 제공합니다.

- 자동 캐시가 포함된 고성능 스토리지
- 자동 업데이트 적용을 위한 스토리지 정책 기반 관리

vSAN과 VMware Horizon을 통합하는 방법에 대한 자세한 내용은 VMware Horizon with View 설명서를 참조하십시오. vSAN용 VMware Horizon View 설계 및 크기 조정에 대한 자세한 내용은 Horizon View에 대한 설계 및 크기 조정 가이드를 참조하십시오.

vSAN의 제한 사항

이 항목에서는 vSAN의 제한 사항에 대해 설명합니다.

vSAN으로 작업할 때는 다음 제한 사항을 고려합니다.

- vSAN은 호스트가 여러 vSAN 클러스터에 참여하는 것을 지원하지 않습니다. 그러나 vSAN 호스트는 클러스터 간에 공유되는 다른 외부 스토리지 리소스에 액세스할 수 있습니다.

- vSAN은 vSphere DPM 및 Storage I/O Control을 지원하지 않습니다.
- vSAN은 SCSI 예약을 지원하지 않습니다.
- vSAN은 RDM, VMFS, 진단 파티션 및 기타 디바이스 액세스 기능을 지원하지 않습니다.

vSAN 을 사용하도록 설정하기 위한 요구 사항

2

vSAN을 활성화하기 전에 사용 환경이 모든 요구 사항을 충족하는지 확인해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “vSAN에 대한 하드웨어 요구 사항,” (17 페이지)
- “vSAN에 대한 클러스터 요구 사항,” (18 페이지)
- “vSAN에 대한 소프트웨어 요구 사항,” (18 페이지)
- “vSAN에 대한 네트워킹 요구 사항,” (19 페이지)
- “라이선스 요구 사항,” (19 페이지)

vSAN 에 대한 하드웨어 요구 사항

조직의 ESXi 호스트가 vSAN 하드웨어 요구 사항을 충족하는지 확인합니다.

스토리지 디바이스 요구 사항

vSAN 구성의 모든 용량 디바이스, 드라이버 및 펌웨어 버전은 인증되어야 하며 VMware 호환성 가이드의 vSAN 섹션에 나열되어 있어야 합니다.

표 2-1. vSAN 호스트에 대한 스토리지 디바이스 요구 사항

| 스토리지 구성 요소 | 요구 사항 |
|-----------------|---|
| 캐시 | <ul style="list-style-type: none">■ 하나의 SAS 또는 SATA SSD(Solid State Disk) 또는 PCIe 플래시 디바이스.■ 허용할 수 있는 장애의 기본 수준을 계산하기 전에 각 디스크 그룹에 있는 플래시 캐시 디바이스의 크기를 확인합니다. 플래시 캐시 디바이스가 용량 디바이스에서 사용할 것으로 예상되는 스토리지(미러와 같은 복제본은 제외)의 10% 이상을 제공 하는지 확인합니다.■ vSphere Flash Read Cache는 vSAN 캐시에 대해 예약된 플래시 디바이스를 사용하면 안 됩니다.■ 캐시 플래시 디바이스는 VMFS 또는 다른 파일 시스템으로 포맷되면 안 됩니다. |
| 가상 시스템 데이터 스토리지 | <ul style="list-style-type: none">■ 하이브리드 그룹 구성의 경우 SAS, NL-SAS 또는 SATA 자기 디스크를 하나 이상 사용할 수 있는지 확인합니다.■ 플래시 전용 디스크 그룹 구성의 경우 SAS, SATA SSD(Solid State Disk) 또는 PCIe 플래시 디바이스가 하나 이상 있는지 확인합니다. |
| 스토리지 컨트롤러 | SAS 또는 SATA HBA(호스트 버스 어댑터) 하나 또는 패스스루 모드나 RAID 0 모드인 RAID 컨트롤러 하나 |

메모리

vSAN의 메모리 요구 사항은 ESXi 하이퍼바이저에서 관리해야 하는 디스크 그룹 및 디바이스 수에 따라 다릅니다. 각 호스트에는 최대 디스크 그룹 수(5개)와 디스크 그룹당 최대 용량 디바이스 수(7개)를 수용하기 위해 최소 32GB의 메모리가 포함되어 있어야 합니다.

플래시 부팅 디바이스

설치 중에 ESXi 설치 관리자가 부팅 디바이스에 코어 덤프 파티션을 생성합니다. 코어 덤프 파티션의 기본 크기는 대부분의 설치 요구 사항을 충족합니다.

- ESXi 호스트의 메모리가 512GB 이하인 경우에는 USB, SD 또는 SATADOM 디바이스에서 호스트를 부팅할 수 있습니다. USB 디바이스나 SD 카드에서 vSAN 호스트를 부팅하는 경우에는 부팅 디바이스의 크기가 4GB 이상이어야 합니다.
- ESXi 호스트의 메모리가 512GB를 초과하는 경우 SATADOM 또는 디스크 디바이스에서 호스트를 부팅해야 합니다. SATADOM 디바이스에서 vSAN 호스트를 부팅하는 경우 SLC(단일 수준 셀) 디바이스를 사용해야 합니다. 부팅 디바이스의 크기가 16GB 이상이어야 합니다.

참고 vSAN 6.5 이상에서는 vSAN 클러스터에 있는 ESXi 호스트의 기존 코어 덤프 파티션의 크기를 조정할 수 있기 때문에 USB/SD 디바이스에서 부팅할 수 있습니다. 자세한 내용은 <http://kb.vmware.com/kb/2147881>에서 VMware 기술 자료 문서를 참조하십시오.

ESXi 6.0 이상 호스트를 USB 디바이스나 SD 카드에서 부팅하면 vSAN 추적 로그가 RAMDisk에 기록됩니다. 이러한 로그는 종료 또는 시스템 충돌(패닉) 시 영구 미디어에 자동으로 오프로드됩니다. 이는 USB 스틱 또는 SD 카드에서 ESXi를 부팅하는 경우에 vSAN 추적 정보를 처리하기 위해 지원되는 유일한 방법입니다. 전원 장애가 발생한 경우에는 vSAN 추적 로그가 유지되지 않습니다.

ESXi 6.0 이상 호스트를 SATADOM 디바이스에서 부팅하면 vSAN 추적 로그가 SATADOM 디바이스에 직접 기록됩니다. 따라서 SATADOM 디바이스가 이 가이드에 요약되어 있는 규격을 충족하는 것이 매우 중요합니다.

vSAN 에 대한 클러스터 요구 사항

호스트 클러스터가 vSAN을 사용하도록 설정하기 위한 요구 사항을 충족하는지 확인합니다.

- vSAN 구성의 모든 용량 디바이스, 드라이버 및 펌웨어 버전은 인증되어야 하며 VMware 호환성 가이드의 vSAN 섹션에 나열되어 있어야 합니다.
- vSAN 클러스터에는 용량을 클러스터에 제공하는 호스트가 3개 이상 포함되어야 합니다. 3개 호스트 클러스터에 대한 고려 사항에 대한 자세한 내용은 “vSAN 클러스터에 대한 설계 고려 사항,” (28 페이지) 항목을 참조하십시오.
- vSAN 클러스터에 있는 호스트는 다른 클러스터에 참여하면 안 됩니다.

vSAN 에 대한 소프트웨어 요구 사항

환경의 vSphere 구성 요소가 vSAN 사용을 위한 소프트웨어 버전 요구 사항을 충족하는지 확인합니다.

vSAN 기능 집합 전체를 사용하려면 vSAN 클러스터에 참여하는 ESXi 호스트의 버전이 6.5 이상이어야 합니다. vSAN을 이전 버전에서 업그레이드할 때 기존 온디스크 형식 버전을 유지할 수 있지만 이 경우 여러 가지 새 기능을 사용할 수 없습니다. vSAN 6.6 이상 소프트웨어는 모든 온디스크 형식을 지원합니다.

vSAN 에 대한 네트워킹 요구 사항

ESXi호스트의 네트워크 인프라 및 네트워킹 구성이 vSAN의 최소 네트워킹 요구 사항을 충족하는지 확인합니다.

표 2-2. vSAN 에 대한 네트워킹 요구 사항

| 네트워킹 구성 요소 | 요구 사항 |
|----------------|--|
| 호스트 대역폭 | <p>각 호스트에는 vSAN 전용의 최소 대역폭이 있어야 합니다.</p> <ul style="list-style-type: none"> ■ 하이브리드 구성의 경우 전용 1Gbps ■ 플래시 전용 구성의 경우 전용 또는 공유된 10Gbps <p>vSAN에서의 네트워킹 고려 사항에 대한 자세한 내용은 “vSAN 네트워킹 설계,” (29 페이지)의 내용을 참조하십시오.</p> |
| 호스트 간 연결 | <p>용량에 기여하는지 여부에 관계없이 vSAN 클러스터의 각 호스트에는 vSAN 트래픽을 위한 VMkernel 네트워크 어댑터가 있어야 합니다. “vSAN에 대한 VMkernel 네트워크 설정,” (45 페이지)를 참조하십시오.</p> |
| 호스트 네트워크 | <p>vSAN 클러스터의 모든 호스트는 vSAN 계층 2 또는 계층 3 네트워크에 연결되어야 합니다.</p> |
| IPv4 및 IPv6 지원 | <p>vSAN 네트워크는 IPv4와 IPv6을 모두 지원합니다.</p> |

라이선스 요구 사항

유효한 vSAN 라이선스가 있는지 확인합니다.

운영 환경에서 vSAN을 사용하려면 vSAN 클러스터에 할당하는 특수 라이선스가 필요합니다.

클러스터에 표준 vSAN 라이선스를 할당하거나 고급 기능이 포함된 라이선스를 할당할 수 있습니다. 고급 기능에는 RAID 5/6 삭제 코딩 및 중복 제거와 압축이 포함됩니다. IOPS 제한 및 확장된 클러스터에는 Enterprise 라이선스가 필요합니다. 라이선스 할당에 대한 자세한 내용은 [“vSAN 클러스터에 대한 라이선스 설정 구성,”](#) (50 페이지) 항목을 참조하십시오.

라이선스의 용량은 클러스터의 총 CPU 수 이상이어야 합니다.

vSAN 클러스터 설계 및 크기 조정

최고의 성능과 사용을 위해서는 vSphere 환경에 vSAN을 배포하기 전에 호스트 및 해당 스토리지 디바이스의 기능과 구성을 계획합니다. vSAN 클러스터 내의 특정 호스트 및 네트워킹 구성을 신중하게 고려합니다.

VMware vSAN 관리설명서에서는 vSAN 클러스터 설계 및 크기 조정에 대한 요점을 살펴봅니다. vSAN 클러스터 설계 및 크기 조정에 대한 자세한 지침은 VMware vSAN 설계 및 크기 조정 가이드 항목을 참조하십시오.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN 스토리지 구성 요소 설계 및 크기 조정,”](#) (21 페이지)
- [“vSAN 호스트 설계 및 크기 조정,”](#) (27 페이지)
- [“vSAN 클러스터에 대한 설계 고려 사항,”](#) (28 페이지)
- [“vSAN 네트워크 설계,”](#) (29 페이지)
- [“vSAN 네트워킹 모범 사례,”](#) (31 페이지)
- [“vSAN 장애 도메인 설계 및 크기 조정,”](#) (32 페이지)
- [“부팅 디바이스 및 vSAN 사용,”](#) (32 페이지)
- [“vSAN 클러스터의 영구 로깅,”](#) (33 페이지)

vSAN 스토리지 구성 요소 설계 및 크기 조정

예상되는 사용량을 기반으로 용량 및 캐시를 계획합니다. 가용성 및 내구성에 대한 요구 사항을 고려하십시오.

- [vSAN에서 용량 계획](#) (22 페이지)
클러스터의 VM(가상 시스템) 파일을 수용하고 장애 및 유지 보수 작업을 처리하도록 vSAN 데이터스토어의 용량 크기를 조정할 수 있습니다.
- [vSAN의 플래시 캐시 디바이스에 대한 설계 고려 사항](#) (24 페이지)
높은 성능과 필요한 스토리지 공간을 제공하고 향후 증가를 수용할 수 있도록 vSAN 캐시 및 플래시 전용 용량에 대한 플래시 디바이스의 구성을 계획합니다.
- [vSAN에서 플래시 용량 디바이스에 대한 설계 고려 사항](#) (25 페이지)
높은 성능과 필요한 스토리지 공간을 제공하고 향후 증가를 수용할 수 있도록 vSAN 플래시 전용 구성에 대한 플래시 용량 디바이스의 구성을 계획합니다.
- [vSAN의 자기 디스크에 대한 설계 고려 사항](#) (26 페이지)
하이브리드 구성의 용량에 대한 자기 디스크의 크기와 수는 스토리지 공간과 성능에 대한 요구 사항에 따라 결정합니다.

- **vSAN의 스토리지 컨트롤러에 대한 설계 고려 사항**(27 페이지)

성능 및 가용성에 대한 요구 사항을 가장 충족하는 vSAN 클러스터의 호스트에 있는 스토리지 컨트롤러를 포함합니다.

vSAN 에서 용량 계획

클러스터의 VM(가상 시스템) 파일을 수용하고 장애 및 유지 보수 작업을 처리하도록 vSAN 데이터스토어의 용량 크기를 조정할 수 있습니다.

원시 용량

vSAN 데이터스토어의 원시 용량을 확인하려면 클러스터에 있는 디스크 그룹의 총 개수를 해당 디스크 그룹에 있는 용량 디바이스의 크기와 곱한 후 vSAN 온디스크 형식에 필요한 오버헤드를 뺍니다.

허용할 수 있는 장애의 기본 수준

가상 시스템의 개수와 해당 VMDK 파일의 크기가 포함되지 않은 vSAN 데이터스토어의 용량을 계획할 때는 클러스터에 대한 가상 시스템 스토리지 정책의 **허용할 수 있는 장애의 기본 수준** 및 **장애 허용 방법** 특성을 고려해야 합니다.

허용할 수 있는 장애의 기본 수준은 vSAN의 스토리지 용량을 계획하고 크기를 조정할 때 중요한 역할을 합니다. 가상 시스템의 가용성 요구 사항을 기반으로, 설정의 사용량이 가상 시스템과 그 개별 디바이스의 사용량과 비교할 때 두 배 이상이 될 수 있습니다.

예를 들어 **장애 허용 방법**을 **RAID-1(미러링) - 성능**으로 설정하고 **PFTT(허용할 수 있는 장애의 기본 수준)**를 1로 설정하면 가상 시스템이 원시 용량의 약 50%를 사용할 수 있습니다. PFTT를 2로 설정하면 약 33%의 용량을 사용할 수 있습니다. PFTT를 3으로 설정하면 약 25%의 용량을 사용할 수 있습니다.

하지만 **장애 허용 방법**을 **RAID-5/6(이레이저 코딩) - 용량**으로 설정하고 PFTT를 1로 설정하면 가상 시스템이 원시 용량의 약 75%를 사용할 수 있습니다. PFTT를 2로 설정하면 약 67%의 용량을 사용할 수 있습니다. RAID 5/6에 대한 자세한 내용은 **“RAID 5 또는 RAID 6 이레이저 코딩 사용,”** (73 페이지)을 참조하십시오.

vSAN 스토리지 정책의 특성에 대한 자세한 내용은 **12장, “vSAN 정책 사용,”** (123 페이지)의 내용을 참조하십시오.

필요한 용량 계산

RAID 1 미러링을 사용하는 클러스터의 가상 시스템에 필요한 용량을 다음의 기준에 따라 계획하십시오.

- 1 vSAN 클러스터의 가상 시스템이 사용할 것으로 예상되는 스토리지 공간을 계산합니다.

$\text{expected overall consumption} = \text{number of VMs in the cluster} * \text{expected percentage of consumption per VMDK}$

- 2 클러스터의 가상 시스템에 대한 스토리지 정책에 구성되어 있는 **허용할 수 있는 장애의 기본 수준** 특성을 고려합니다. 이 특성은 클러스터의 호스트에 있는 VMDK 파일의 복제본 수에 직접적인 영향을 줍니다.

$\text{datastore capacity} = \text{expected overall consumption} * (\text{PFTT} + 1)$

- 3 vSAN 온디스크 형식의 오버헤드 요구 사항을 예측합니다.

- 온디스크 형식 버전 3.0 이상에서는 추가적인 오버헤드를 추가하며, 일반적으로 이 오버헤드는 디바이스당 용량의 1-2%를 초과하지 않습니다. 소프트웨어 체크섬을 사용하도록 설정된 중복 제거 및 압축 기능을 사용하려면 디바이스당 용량의 6.2% 정도에 해당하는 추가적인 오버헤드가 필요합니다.

- 온디스크 형식 버전 2.0에서는 추가적인 오버헤드를 추가하며, 일반적으로 이 오버헤드는 디바이스당 용량의 1-2%를 초과하지 않습니다.

- 온디스크 형식 버전 1.0에서는 용량 디바이스당 약 1GB의 추가적인 오버헤드를 추가합니다.

용량 크기 조정 지침

- vSAN이 스토리지 로드를 재조정하지 않도록 최소 30%의 사용되지 않은 공간을 유지합니다. vSAN은 단일 용량 디바이스의 사용량이 80% 이상이 될 때마다 클러스터 전반의 구성 요소를 재조정합니다. 재조정 작업은 애플리케이션의 성능에 영향을 줄 수 있습니다. 이러한 문제를 피하려면 스토리지 사용량을 70% 미만으로 유지합니다.
- 용량 디바이스, 디스크 그룹 및 호스트의 잠재적 장애 또는 교체를 처리하기 위한 추가 용량을 계획합니다. 용량 디바이스에 연결할 수 없는 경우 vSAN은 클러스터의 다른 디바이스에서 구성 요소를 복구합니다. 플래시 캐시 디바이스가 제거되거나 장애가 발생한 경우 vSAN은 전체 디스크 그룹의 구성 요소를 복구합니다.
- 호스트 장애 발생 후 또는 호스트가 유지 보수 모드로 전환되는 경우 vSAN이 구성 요소를 복구할 수 있도록 추가 용량을 예약합니다. 예를 들어 남은 사용 가능 용량으로 호스트 장애 발생 후 또는 유지 보수 동안 구성 요소를 재구축할 수 있도록 충분한 용량으로 호스트를 프로비저닝합니다. 용량이 중요한 이유는 호스트가 네 개 이상 있는 경우, 실패한 구성 요소를 재구축하기 위한 여유 용량이 충분해야 하기 때문입니다. 호스트에 장애가 발생하면 다른 장애를 허용할 수 있도록 다른 호스트에 있는 사용 가능한 스토리지에서 재구축이 수행됩니다. 하지만 호스트가 3개인 클러스터의 경우 **허용할 수 있는 장애의 기본 수준이 1로 설정되어 있으면 vSAN이 재구축 작업을 수행하지 않습니다.** 그 이유는 호스트 하나에서 장애가 발생했을 때 클러스터에 남아 있는 호스트가 2개뿐이기 때문입니다. 장애 후 재구축을 허용하려면 호스트가 3개 이상 있어야 합니다.
- vSAN VM 스토리지 정책의 변경을 위해 충분한 임시 스토리지 공간을 제공합니다. VM 스토리지 정책을 동적으로 변경할 때 vSAN에서 개체를 구성하는 복제본의 레이아웃을 생성할 수 있습니다. vSAN에서 해당 복제본을 인스턴스화하고 원래 복제본과 동기화하는 경우 클러스터는 일시적으로 추가 공간을 제공해야 합니다.
- 소프트웨어 체크섬 또는 중복 제거와 압축 같은 고급 기능을 사용할 계획이라면 작동 오버헤드를 처리할 추가적인 용량을 예약해야 합니다.

가상 시스템 개체에 대한 고려 사항

vSAN 데이터스토어의 스토리지 용량을 계획할 때 VM 홈 네임스페이스 개체, 스냅샷 및 스왑 파일을 위해 데이터스토어에 필요한 공간을 고려합니다.

- VM 홈 네임스페이스. 가상 시스템의 홈 네임스페이스 개체에 명시적으로 스토리지 정책을 할당할 수 있습니다. vSAN은 용량 및 캐시 스토리지가 불필요하게 할당되지 않도록 정책의 **허용할 수 있는 장애의 기본 수준 및 강제 프로비저닝** 설정만 VM 홈 네임스페이스에 적용합니다. **허용할 수 있는 장애의 기본 수준이 0보다 큰 VM 홈 네임스페이스에 할당된 스토리지 정책의 요구 사항을 충족하도록 스토리지 공간을 계획합니다.**
- 스냅샷입니다. 델타 디바이스는 기본 VMDK 파일의 정책을 상속합니다. 스냅샷의 예상 크기와 수 그리고 vSAN 스토리지 정책의 설정에 따라 추가 공간을 계획합니다.
필요한 공간이 서로 다를 수 있습니다. 그 크기는 가상 시스템에서 데이터를 변경하는 빈도와 스냅샷을 가상 시스템에 연결하는 시간에 따라 달라집니다.
- 스왑 파일. vSAN은 가상 시스템의 스왑 파일에 대해 개별 스토리지 정책을 사용합니다. 정책에서는 단일 장애를 허용하고, 스트라이핑 및 읽기 캐시 예약을 정의하지 않으며, 강제 프로비저닝을 사용합니다.

vSAN 의 플래시 캐시 디바이스에 대한 설계 고려 사항

높은 성능과 필요한 스토리지 공간을 제공하고 향후 증가를 수용할 수 있도록 vSAN 캐시 및 플래시 전용 용량에 대한 플래시 디바이스의 구성을 계획합니다.

PCIe 또는 SSD 플래시 디바이스 중에서 선택

vSAN 스토리지의 성능, 용량, 쓰기 내구성 및 비용에 대한 요구 사항에 따라 PCIe 또는 SSD 플래시 디바이스를 선택합니다.

- 호환성. PCIe 또는 SSD 디바이스의 모델이 VMware 호환성 가이드의 vSAN 섹션에 나열되어 있어야 합니다.
- 성능. PCIe 디바이스는 일반적으로 SSD 디바이스보다 빠른 성능을 가지고 있습니다.
- 용량. PCIe 디바이스에 사용할 수 있는 최대 용량은 일반적으로 VMware 호환성 가이드의 vSAN 에 대한 SSD 디바이스에 현재 나열되어 있는 최대 용량보다 큼니다.
- 쓰기 내구성. PCIe 또는 SSD 디바이스의 쓰기 내구성은 용량 또는 플래시 전용 구성의 캐시에 대한 요구 사항 및 하이브리드 구성의 캐시에 대한 요구 사항을 충족해야 합니다.

플래시 전용 및 하이브리드 구성의 쓰기 내구성 요구 사항에 대한 자세한 내용은 VMware vSAN 설계 및 크기 조정 가이드를 참조하십시오. PCIe 및 SSD 디바이스의 쓰기 내구성 등급에 대한 자세한 내용은 VMware 호환성 가이드의 vSAN 섹션을 참조하십시오.

- 비용. PCIe 디바이스는 일반적으로 SSD 디바이스보다 비용이 높습니다.

플래시 디바이스를 vSAN 캐시로

이러한 고려 사항을 기반으로 쓰기 내구성, 성능 및 잠재적 증가를 수용할 수 있도록 vSAN에 대한 플래시 캐시의 구성을 설계합니다.

표 3-1. vSAN 캐시 크기 조정

| 스토리지 구성 | 고려 사항 |
|-------------------|--|
| 플래시 전용 및 하이브리드 구성 | <ul style="list-style-type: none"> ■ 플래시 캐시 디바이스는 가상 시스템에서 사용할 것으로 예상되는 스토리지(미러와 같은 복제는 제외)의 10% 이상을 제공해야 합니다. <p>VM 스토리지 정책의 허용할 수 있는 장애의 기본 수준 특성은 캐시 크기에 영향을 주지 않습니다.</p> <ul style="list-style-type: none"> ■ 보다 높은 캐시 대 용량 비율은 이후 용량 증가를 용이하게 합니다. 크기가 초과된 캐시를 사용하면 캐시 크기를 늘리지 않고도 기존 디스크 그룹에 더 많은 용량을 쉽게 추가할 수 있습니다. ■ 플래시 캐시 디바이스는 쓰기 내구성이 높아야 합니다. ■ 해당 작업이 전체 디스크 그룹에 영향을 미치기 때문에 플래시 캐시 디바이스의 수명이 종료될 때 플래시 캐시 디바이스를 교체하는 것이 용량 디바이스를 교체하는 것보다 복잡합니다. ■ 캐시의 크기를 늘리기 위해 더 많은 플래시 디바이스를 추가하는 경우 더 많은 디스크 그룹을 생성해야 합니다. 플래시 캐시 디바이스와 디스크 그룹 간의 비율은 항상 1:1입니다. <p>디스크 그룹을 여러 개 구성하면 다음과 같은 이점이 있습니다.</p> <ul style="list-style-type: none"> ■ 단일 캐시 디바이스가 실패하는 경우 영향을 받는 용량 디바이스의 수가 적어지기 때문에 실패 위험이 줄어듭니다. ■ 보다 적은 플래시 캐시 디바이스가 포함된 여러 디스크 그룹을 배포하는 경우 잠재적으로 성능이 향상됩니다. <p>그러나 여러 디스크 그룹을 구성하는 경우 호스트의 메모리 사용이 증가합니다.</p> |
| 플래시 전용 구성 | <p>플래시 전용 구성에서는 vSAN이 쓰기 캐시 용도로만 캐시 계층을 사용합니다. 쓰기 캐시는 매우 높은 쓰기 작업을 처리할 수 있어야 합니다. 이러한 접근 방식은 보다 비용이 낮고 쓰기 내구성이 낮을 수 있는 용량 플래시의 수명을 연장합니다.</p> |
| 하이브리드 구성 | <p>성능상의 이유로 읽기 캐시 예약이 활성화된 VM 스토리지 정책에 구성된 경우 vSAN 클러스터의 호스트에는 실패 후 재구축 또는 유지 보수 작업 동안 예약을 충족하기에 충분한 캐시가 있어야 합니다.</p> <p>사용 가능한 읽기 캐시가 예약을 충족하기에 충분하지 않은 경우 재구축 또는 유지 보수 작업이 실패합니다. 특정 워크로드에 대한 알려진 특정 성능 요구 사항을 충족해야 하는 경우에만 읽기 캐시 예약을 사용합니다.</p> <p>스냅샷의 사용은 캐시 리소스를 사용합니다. 여러 스냅샷을 사용하려는 경우 일반적인 10%의 캐시 대 사용되는 용량 비율보다 많은 캐시를 전용으로 할당하는 것을 고려합니다.</p> |

vSAN 에서 플래시 용량 디바이스에 대한 설계 고려 사항

높은 성능과 필요한 스토리지 공간을 제공하고 향후 증가를 수용할 수 있도록 vSAN 플래시 전용 구성에 대한 플래시 용량 디바이스의 구성을 계획합니다.

PCIe 또는 SSD 플래시 디바이스 중에서 선택

vSAN 스토리지의 성능, 용량, 쓰기 내구성 및 비용에 대한 요구 사항에 따라 PCIe 또는 SSD 플래시 디바이스를 선택합니다.

- 호환성. PCIe 또는 SSD 디바이스의 모델이 VMware 호환성 가이드의 vSAN 섹션에 나열되어 있어야 합니다.
- 성능. PCIe 디바이스는 일반적으로 SSD 디바이스보다 빠른 성능을 가지고 있습니다.
- 용량. PCIe 디바이스에 사용할 수 있는 최대 용량은 일반적으로 VMware 호환성 가이드의 vSAN에 대한 SSD 디바이스에 현재 나열되어 있는 최대 용량보다 큼니다.

- 쓰기 내구성. PCIe 또는 SSD 디바이스의 쓰기 내구성은 용량 또는 플래시 전용 구성의 캐시에 대한 요구 사항 및 하이브리드 구성의 캐시에 대한 요구 사항을 충족해야 합니다.
플래시 전용 및 하이브리드 구성의 쓰기 내구성 요구 사항에 대한 자세한 내용은 VMware vSAN 설계 및 크기 조정 가이드를 참조하십시오. PCIe 및 SSD 디바이스의 쓰기 내구성 등급에 대한 자세한 내용은 VMware 호환성 가이드의 vSAN 섹션을 참조하십시오.
- 비용. PCIe 디바이스는 일반적으로 SSD 디바이스보다 비용이 높습니다.

플래시 디바이스를 vSAN 용량으로

플래시 전용 구성에서는 vSAN이 읽기 작업에 캐시를 사용하지 않으며 VM 스토리지 정책의 읽기 캐시 예약 설정을 적용하지 않습니다. 캐시에 대해서는, 쓰기 내구성이 높지만 더 비싼 플래시를 소량만 사용할 수 있습니다. 용량에 대해서는, 상대적으로 저렴하고 쓰기 내구성은 낮은 플래시를 사용할 수 있습니다.

다음 지침에 따라 플래시 용량 디바이스의 구성을 계획하십시오.

- vSAN의 성능 향상을 위해서는 작은 플래시 용량 디바이스로 구성된 더 많은 수의 디스크 그룹을 사용합니다.
- 균형 잡힌 성능과 예측 가능한 동작을 위해서는 동일한 유형과 모델의 플래시 용량 디바이스를 사용하십시오.

vSAN 의 자기 디스크에 대한 설계 고려 사항

하이브리드 구성의 용량에 대한 자기 디스크의 크기와 수는 스토리지 공간과 성능에 대한 요구 사항에 따라 결정합니다.

SAS, NL-SAS 및 SATA 자기 디스크

vSAN 스토리지의 비용과 성능 및 용량에 대한 요구 사항에 따라 SAS, NL-SAS 또는 SATA 자기 디바이스를 사용합니다.

- 호환성. 자기 디스크의 모델은 인증되어야 하며 VMware 호환성 가이드의 vSAN 섹션에 나열되어 있어야 합니다.
- 성능. SAS 및 NL-SAS 디바이스는 SATA 디스크보다 성능이 빠릅니다.
- 용량. vSAN용 SAS, NL-SAS 및 SATA 자기 디스크의 용량은 VMware 호환성 가이드의 vSAN 섹션에서 확인할 수 있습니다. 소량의 큰 디바이스보다는 대량의 작은 디바이스를 사용하는 것을 고려하십시오.
- 비용. SAS 및 NL-SAS 디바이스는 SATA 디스크보다 고가입니다.

용량 및 비용 절감이 성능보다 높은 우선 순위를 가지는 환경에서는 SAS 및 NL-SAS 디바이스 대신 SATA 디바이스를 사용하는 것이 적합합니다.

자기 디스크를 vSAN 용량으로

아래 지침에 따라 자기 디스크 구성을 계획하십시오.

- vSAN의 성능 향상을 위해서는 작은 용량의 자기 디스크 여러 개를 사용합니다.
캐시와 용량 간의 데이터 전송을 위한 적절한 집계 성능을 제공하는 충분한 자기 디스크가 있어야 합니다. 더 작은 디바이스를 사용하는 것이 더 적은 수의 큰 디바이스를 사용하는 것보다 성능이 높습니다. 여러 개의 자기 디스크 스핀들을 사용하면 디스테이징 프로세스의 속도를 높일 수 있습니다.
가상 시스템이 여러 개 포함된 환경에서 데이터를 읽기 캐시에서 사용할 수 없어서 vSAN이 이 데이터를 자기 디스크에서 읽을 경우, 자기 디스크의 수가 읽기 작업에 중요합니다. 적은 수의 가상 시스템이 포함된 환경에서는 활성 VM 스토리지 정책의 개체당 디스크 스트라이프 수가 1보다 크면 디스크 수가 읽기 작업에 영향을 줍니다.

- 균형 잡힌 성능과 예측 가능한 동작을 위해 vSAN 데이터스토어에 동일한 유형과 모델의 자기 디스크를 사용합니다.
- 정의된 스토리지 정책의 **허용할 수 있는 장애의 기본 수준 및 개체당 디스크 스트라이프 수** 특성 값을 충족하기에 충분한 수의 자기 디스크를 지정하십시오. vSAN의 VM 스토리지 정책에 대한 자세한 내용은 12장, “vSAN 정책 사용,” (123 페이지)의 내용을 참조하십시오.

vSAN 의 스토리지 컨트롤러에 대한 설계 고려 사항

성능 및 가용성에 대한 요구 사항을 가장 충족하는 vSAN 클러스터의 호스트에 있는 스토리지 컨트롤러를 포함합니다.

- VMware 호환성 가이드에 나열되어 있는 스토리지 컨트롤러 모델, 드라이버 및 펌웨어 버전을 사용합니다. VMware 호환성 가이드에서 vSAN을 검색합니다.
- 가능한 경우 성능을 향상하고 잠재적인 컨트롤러 장애를 디스크 그룹의 하위 집합으로만 분리하기 위해 여러 스토리지 컨트롤러를 사용합니다.
- VMware 호환성 가이드에서 대기열 크기가 가장 큰 스토리지 컨트롤러를 사용합니다. 대기열 크기가 큰 컨트롤러를 사용하면 성능이 향상됩니다. vSAN이 장애 후 구성 요소를 재구축하거나 호스트가 유지 보수 모드로 전환되는 경우를 예로 들 수 있습니다.
- 최고의 vSAN 성능을 위해 패스스루 모드의 스토리지 컨트롤러를 사용합니다. RAID 0 모드의 스토리지 컨트롤러는 패스스루 모드의 스토리지 컨트롤러에 비해 더 많은 구성 및 유지 보수 작업을 필요로 합니다.

vSAN 호스트 설계 및 크기 조정

최고의 성능과 가용성을 제공하도록 vSAN 클러스터의 호스트 구성을 계획합니다.

메모리 및 CPU

다음 고려 사항을 기반으로 vSAN 클러스터 호스트의 메모리 및 CPU 크기를 조정합니다.

표 3-2. vSAN 호스트의 메모리 및 CPU 크기 조정

| 계산 리소스 | 고려 사항 |
|--------|---|
| 메모리 | <ul style="list-style-type: none"> ■ 가상 시스템당 메모리 ■ 예상 가상 시스템 수에 기반한 호스트당 메모리 ■ 호스트당 5개의 디스크 그룹, 디스크 그룹당 7개의 용량 디바이스가 포함된 vSAN의 완전한 작동을 위한 최소 32GB의 메모리 <p>메모리가 512GB 이하인 호스트는 USB, SD 또는 SATADOM 디바이스에서 부팅할 수 있습니다. 호스트의 메모리가 512GB보다 큰 경우에는 SATADOM 또는 디스크 디바이스에서 호스트를 부팅합니다.</p> |
| CPU | <ul style="list-style-type: none"> ■ 호스트당 소켓 ■ 소켓당 코어 ■ 예상 가상 시스템 수에 기반한 vCPU 수 ■ vCPU 및 코어 간 비율 ■ vSAN에 대한 10% CPU 오버헤드 |

호스트 네트워킹

성능을 높이기 위해 vSAN 트래픽에 더 많은 대역폭을 제공합니다.

- 1GbE 어댑터가 포함된 호스트를 사용하려는 경우에는 어댑터를 vSAN 전용으로 사용합니다. 플래시 전용 구성의 경우 10-GbE 어댑터를 전용으로 사용하거나 공유하는 호스트를 계획합니다.

- 10-GbE 어댑터를 사용하려는 경우 하이브리드 및 플래시 전용 구성 모두에 대해 어댑터를 다른 트래픽 유형과 공유할 수 있습니다.
- 10GbE 어댑터를 다른 트래픽 유형과 공유하는 경우 Network I/O Control과 VLAN을 사용하여 트래픽을 분리하려면 vSAN 트래픽에 대해 vSphere Distributed Switch를 사용합니다.
- 이중화를 위해 vSAN 트래픽에 대한 물리적 어댑터 팀을 생성합니다.

여러 디스크 그룹

플래시 캐시 또는 스토리지 컨트롤러가 응답을 중지하는 경우 전체 디스크 그룹에 장애가 발생할 수 있습니다. 결과적으로, vSAN은 장애가 발생한 디스크 그룹의 모든 구성 요소를 클러스터의 다른 위치에 있는 디스크 그룹에서 재구축합니다.

각각의 디스크 그룹이 적은 용량을 제공하는 여러 디스크 그룹을 사용하면 다음과 같은 장점과 단점이 있습니다.

- 장점
 - 데이터스토어가 더 많은 집계 캐시를 포함하고 I/O 작업이 더 빨라지기 때문에 성능이 향상됩니다.
 - 장애 위험이 여러 디스크 그룹 사이에 확산됩니다.
 - 디스크 그룹에 장애가 발생하는 경우 vSAN은 더 적은 구성 요소를 재구축하기 때문에 성능이 향상됩니다.
- 단점
 - 캐시 디바이스가 두 개 이상 필요하기 때문에 비용이 증가합니다.
 - 더 많은 디스크 그룹을 처리하기 위해 더 많은 메모리가 필요합니다.
 - 단일 장애 지점의 위험을 줄이기 위해 스토리지 컨트롤러가 여러 개 필요합니다.

드라이브 베이

간편한 유지 보수를 위해 드라이브 베이와 PCIe 슬롯이 서버 본체의 전면에 위치한 호스트를 고려합니다.

블레이드 서버 및 외부 스토리지

블레이드 서버는 제한된 수의 디스크 슬롯을 가지기 때문에 보통 vSAN 데이터스토어에서 블레이드 서버의 용량이 확장되지 않습니다. 블레이드 서버의 계획된 용량을 확장하려면 외부 스토리지 엔클로저를 사용합니다. 지원되는 외부 스토리지 엔클로저 모델에 대한 자세한 내용은 VMware 호환성 가이드 항목을 참조하십시오.

디바이스 핫 플러그 및 스왑

호스트의 자기 디스크 및 플래시 용량 디바이스에 대한 손쉬운 핫 플러그 또는 교체를 위해 스토리지 컨트롤러 패스스루 모드 지원을 고려합니다. 컨트롤러가 RAID 0 모드에서 작동하는 경우 추가적인 단계를 수행해야만 호스트가 새 드라이브를 검색할 수 있습니다.

vSAN 클러스터에 대한 설계 고려 사항

소비 증가에 대한 최상의 가용성 및 허용성을 위한 호스트 및 관리 노드의 구성을 설계합니다.

허용되는 장애에 대한 vSAN 클러스터 크기 조정

호스트 장애를 처리하기 위해 VM 스토리지 정책에 PFTT(허용할 수 있는 장애의 기본 수준) 특성을 구성합니다. 클러스터에 필요한 호스트 수를 계산하는 공식은 $2 * PFTT + 1$ 입니다. 클러스터가 허용하는 장애 수를 더 많게 구성할수록 더 많은 용량 호스트가 필요합니다.

클러스터 호스트가 랙 서버에 연결된 경우에는 호스트를 장애 도메인에 구성하여 장애 관리 기능을 개선할 수 있습니다. “vSAN 장애 도메인 설계 및 크기 조정,” (32 페이지)를 참조하십시오.

호스트가 2개 또는 3개인 클러스터 구성의 제한 사항

호스트가 2개 또는 3개인 구성에서는 허용할 수 있는 장애의 기본 수준을 1로 설정하여 하나의 호스트 장애만 허용할 수 있습니다. vSAN은 가상 시스템 데이터의 필수 복제본 2개를 각각 별도의 호스트에 저장합니다. 감시 개체는 세 번째 호스트에 있습니다. 클러스터의 적은 호스트 수로 인해 다음과 같은 제한 사항이 있습니다.

- 호스트에 장애가 발생할 경우 vSAN은 다른 장애로부터 보호하기 위해 데이터를 다른 호스트에 재구성할 수 없습니다.
- 호스트가 유지 보수 모드로 전환되어야 하는 경우 vSAN은 제거된 데이터를 다시 보호할 수 없습니다. 호스트가 유지 보수 모드 상태에 있는 동안 데이터는 잠재적 장애에 노출됩니다.

데이터 액세스 지원 보장 데이터 제거 옵션만 사용할 수 있습니다. 이 경우에는 데이터를 제거하는 데 사용할 수 있는 여유 호스트가 클러스터에 없기 때문에 **모든 데이터 제거** 옵션을 사용할 수 없습니다.

그 결과 다른 장애가 발생할 경우 액세스할 수 없게 되므로 가상 시스템이 위험하게 됩니다.

균형 및 불균형 클러스터 구성

vSAN은 구성이 일관된 호스트에서 최적으로 작동합니다.

구성이 서로 다른 호스트를 사용하면 vSAN 클러스터에서 다음과 같은 단점이 있습니다.

- vSAN이 동일한 수의 구성 요소를 각 호스트에 저장하지 않으므로 스토리지 성능의 예측 가능성이 줄어듭니다.
- 다른 유지 보수 절차.
- 더 적거나 다른 유형의 캐시 디바이스가 있는 클러스터의 호스트에 대한 성능이 저하됨.

vSAN 에 vCenter Server 배포

vSAN 데이터스토어에 vCenter Server를 배포하는 경우 vSAN 클러스터에서 문제가 발생하면 문제 해결에 vCenter Server를 사용하지 못할 수 있습니다.

vSAN 네트워크 설계

vSAN 클러스터에서 가용성, 보안 및 대역폭을 보장할 수 있는 네트워킹 기능을 고려합니다.

vSAN 네트워크 구성에 대한 자세한 내용은 VMware vSAN 설계 및 크기 조정 가이드 및 vSAN 네트워크 설계 가이드 항목을 참조하십시오.

네트워킹 페일오버 및 로드 밸런싱

vSAN은 네트워크 이중화를 위해서만 백업 가상 스위치에서 구성된 팀 구성 및 페일오버 정책을 사용합니다. vSAN은 로드 밸런싱을 위해 NIC 팀 구성을 사용하지 않습니다.

가용성을 위해 NIC 팀을 구성하려면 다음과 같은 페일오버 구성을 고려하십시오.

| 팀 구성 알고리즘 | 팀의 어댑터 페일오버 구성 |
|------------------------|--|
| 원래 가상 포트를 기반으로 라우팅 | 능동/수동 |
| IP 해시 기준 라우팅 | 능동/능동, 표준 스위치를 위한 정적 EtherChannel 및 Distributed Switch를 위한 LACP 포트 채널 사용 |
| 물리적 네트워크 어댑터 로드 기준 라우팅 | 능동/능동 |

vSAN은 IP-해시 로드 밸런싱을 지원하지만 모든 구성에서 성능 향상을 보장할 수 없습니다. vSAN이 많은 소비자 중 하나인 경우 IP 해시를 통해 이점을 얻을 수 있습니다. 이 경우 IP 해시는 로드 밸런싱을 수행합니다. vSAN이 유일한 소비자인 경우 향상이 눈에 띄지 않을 수 있습니다. 이 동작은 특히 1-GbE 환경에 적용됩니다. 예를 들어 vSAN에 IP 해시를 사용하는 4개의 1GbE 물리적 어댑터를 사용하는 경우 1Gbps 이상을 사용하지 못할 수 있습니다. 이 동작은 VMware에서 지원하는 모든 NIC 팀 구성 정책에도 적용됩니다.

vSAN 네트워크에서 유니캐스트 사용

vSAN 6.6 이상 릴리스에서는 vSAN 클러스터를 지원하는 물리적 스위치에 멀티캐스트가 필요하지 않습니다. vSAN을 위한 단순한 유니캐스트 네트워크를 설계할 수 있습니다. vSAN의 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. vSAN 클러스터에서 멀티캐스트 사용에 대한 자세한 내용은 VMware vSAN 관리의 이전 버전을 참조하십시오.

참고 예약 없이 DHCP의 IP 주소를 사용하는 vSAN 6.6 클러스터에 vCenter Server를 배포하는 구성은 지원되지 않습니다. 할당된 IP 주소는 VMkernel 포트의 MAC 주소에 바인딩되기 때문에 예약과 함께 DHCP를 사용할 수 있습니다.

Network I/O Control을 사용하여 vSAN 에 대한 대역폭 할당

vSAN 트래픽에서 다른 시스템 트래픽 유형(예: vSphere vMotion 트래픽, vSphere HA 트래픽, 가상 시스템 트래픽 등)과 공유되는 10GbE 물리적 네트워크 어댑터를 사용하는 경우 vSphere Distributed Switch에서 vSphere Network I/O Control을 사용하여 vSAN에 필요한 대역폭 양을 보장할 수 있습니다.

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

- 예약을 설정하면 Network I/O Control이 물리적 어댑터에서 vSAN에 대해 최소 대역폭을 사용할 수 있도록 보장합니다.
- 공유를 설정하면 vSAN에 할당된 물리적 어댑터가 포화 상태가 되는 경우 특정 대역폭이 vSAN에 사용되고 재구축 및 동기화 작업 중 vSAN이 물리적 어댑터의 전체 용량을 사용하지 못하도록 합니다. 예를 들어 팀에서 다른 물리적 어댑터가 실패하고 포트 그룹의 모든 트래픽이 팀의 다른 어댑터로 전송되면 물리적 어댑터가 포화 상태가 될 수 있습니다.

예를 들어 vSAN, vSphere vMotion 및 가상 시스템에 대한 트래픽을 처리하는 10GbE 물리적 어댑터에서 특정 대역폭 및 공유를 구성할 수 있습니다.

표 3-3. vSAN 을 처리하는 물리적 어댑터에 대한 Network I/O Control 구성 예

| 트래픽 유형 | 예약, Gbps | 공유 |
|-----------------|----------|-----|
| vSAN | 1 | 100 |
| vSphere vMotion | 0.5 | 70 |
| 가상 시스템 | 0.5 | 30 |

10GbE 어댑터가 포화 상태가 되면 Network I/O Control에서 물리적 어댑터의 vSAN에 5Gbps를 할당합니다.

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

vSAN 트래픽 표시

우선 순위 태그 지정은 연결된 네트워크 디바이스에 vSAN 트래픽이 더 높은 QoS(서비스 품질) 요구를 가지고 있음을 나타내기 위한 메커니즘입니다. vSAN 트래픽을 특정 등급에 할당하고 이에 따라 vSphere Distributed Switch의 트래픽 필터링 및 표시 정책을 사용하여 0(낮은 우선 순위)에서 7(높은 우선 순위) 사이의 CoS(서비스 등급) 값으로 트래픽을 표시할 수 있습니다.

VLAN에서 vSAN 트래픽 세분화

보안 및 성능 향상을 위해, 특히 여러 트래픽 유형 간에 백업 물리적 어댑터의 용량을 공유하는 경우 VLAN에서 vSAN 트래픽을 분리하는 것을 고려합니다.

점보 프레임

CPU 성능 향상을 위해 vSAN에서 점보 프레임을 사용하려는 경우 클러스터의 모든 네트워크 디바이스 및 호스트에서 점보 프레임을 사용하도록 설정했는지 확인합니다.

기본적으로 TSO(TCP 세분화 오프로드) 및 LRO(대규모 수신 오프로드) 기능은 ESXi에서 사용하도록 설정됩니다. 점보 프레임을 통한 성능 개선이 네트워크의 모든 노드에서 점보 프레임을 사용하도록 설정하는 데 드는 비용을 상쇄할 정도로 충분한지 검토해야 합니다.

vSAN 네트워킹에 대한 정적 경로 생성

vSAN 환경에서 정적 경로를 생성해야 할 수 있습니다.

vSphere가 기본 게이트웨이 하나만 사용하는 일반적인 구성에서는 라우팅된 모든 트래픽이 이 게이트웨이를 통해 대상에 도달하려고 합니다.

하지만 특정 vSAN 배포에 정적 라우팅이 필요한 경우도 있습니다. 예를 들어 감시 호스트가 다른 네트워크에 있는 배포 또는 데이터 사이트와 감시 호스트가 서로 다른 사이트에 있는 확장된 클러스터 배포가 여기에 해당됩니다.

ESXi 호스트에 정적 라우팅을 구성하려면 `esxcli` 명령을 사용하십시오.

```
esxcli network ip route ipv4 add -n remote-network -g gateway-to-use
```

`remote-network`는 호스트가 액세스해야 하는 원격 네트워크이며 `gateway-to-use`는 트래픽이 원격 네트워크로 전송될 때 사용할 인터페이스입니다.

자세한 내용은 “[확장된 클러스터에 대한 네트워크 설계](#),” (62 페이지)를 참조하십시오.

vSAN 네트워킹 모범 사례

성능과 처리량을 향상하기 위한 vSAN에 대한 네트워킹 모범 사례를 고려합니다.

- 하이브리드 구성의 경우 최소 1-GbE 물리적 네트워크 어댑터를 전용으로 할당합니다. 최상의 네트워킹 성능을 위해 전용 또는 공유 10GbE 물리적 어댑터에 vSAN 트래픽을 배치합니다.
- 플래시 전용 구성의 경우 전용 또는 공유 10-GbE 물리적 네트워크 어댑터를 사용합니다.
- 하나의 추가 물리적 NIC를 페일오버 NIC로 프로비저닝합니다.
- 공유 10GbE 네트워크 어댑터를 사용하는 경우 Distributed Switch에 vSAN 트래픽을 배치하고 vSAN에 대한 대역폭을 보장하도록 Network I/O Control을 구성합니다.

vSAN 장애 도메인 설계 및 크기 조정

vSAN 장애 도메인 기능은 이중화 구성 요소를 분리된 컴퓨팅 랙의 여러 서버로 분산시키도록 vSAN에 지시합니다. 이 방법을 통해 정전이나 연결 끊김과 같은 랙 수준 장애로부터 환경을 보호할 수 있습니다.

장애 도메인 구성체

vSAN에는 각각 하나 이상의 호스트로 구성된 장애 도메인이 2개 이상 필요합니다. 장애 도메인 정의는 개별 컴퓨팅 랙 인클로저와 같은 잠재적 장애 영역을 나타낼 수 있는 물리적 하드웨어 구성체를 인식해야 합니다.

가능한 경우 최소 네 개의 장애 도메인을 사용하십시오. 장애 도메인이 3개인 경우에는 일부 데이터 제거 모드가 지원되지 않고 vSAN이 장애 후에 데이터를 다시 보호할 수 없습니다. 이 경우에는 장애 도메인 세 개만으로는 제공할 수 없는 재구축용 용량을 가진 추가적인 장애 도메인이 필요합니다.

장애 도메인을 사용하도록 설정한 경우, vSAN은 개별 호스트가 아니라 장애 도메인에 활성 가상 시스템 스토리지 정책을 적용합니다.

가상 시스템에 할당할 스토리지 정책의 PFTT(허용할 수 있는 장애의 기본 수준) 특성에 기반하여 클러스터의 장애 도메인 수를 계산합니다.

number of fault domains = 2 * PFTT + 1

호스트가 장애 도메인의 멤버가 아닌 경우 vSAN은 해당 호스트를 독립형 장애 도메인으로 해석합니다.

여러 호스트의 장애에 대해 장애 도메인 사용

각각 두 개의 호스트가 있는 서버 랙 네 개가 포함된 클러스터를 예로 들어보겠습니다. **허용할 수 있는 장애의 기본 수준**을 1로 설정하고, 장애 도메인을 사용하도록 설정하지 않은 경우 vSAN은 개체 복제본 2개를 호스트와 함께 동일한 랙 인클로저에 저장할 수 있습니다. 이러한 방식으로 랙 수준 장애 발생 시 애플리케이션이 데이터 손실의 위험에 노출될 수 있습니다. 함께 장애가 발생할 가능성이 있는 호스트를 별도의 장애 도메인으로 구성하면 vSAN은 각 보호 구성 요소(복제본 및 감시)를 별도의 장애 도메인에 배치합니다.

호스트와 용량을 추가하는 경우 기존 장애 도메인 구성을 사용하거나 장애 도메인을 정의할 수 있습니다.

장애 도메인을 사용하는 경우에 스토리지 로드와 Fault Tolerance의 균형을 유지하려면 다음 지침을 고려하십시오.

- 스토리지 정책에 구성된 **허용할 수 있는 장애의 기본 수준**을 충족하기에 충분한 장애 도메인을 제공하십시오.
 - 장애 도메인을 세 개 이상 정의하십시오. 최상의 보호를 위해서는 최소 네 개의 도메인을 정의하십시오.
- 각 장애 도메인에 동일한 수의 호스트를 할당하십시오.
- 구성이 동일한 호스트를 사용하십시오.
- 가능한 경우 여유 용량이 있는 장애 도메인 하나를 장애 후 데이터 재구축 전용으로 지정하십시오.

부팅 디바이스 및 vSAN 사용

플래시 디바이스에서 vSAN 클러스터의 일부인 ESXi 설치를 시작하려면 몇 가지 제약이 따릅니다.

USB/SD 디바이스에서 vSAN 호스트를 부팅하는 경우에는 4GB 이상의 고품질 USB 또는 SD 플래시 드라이브를 사용해야 합니다.

SATADOM 디바이스에서 vSAN 호스트를 부팅하는 경우 SLC(단일 수준 셀) 디바이스를 사용해야 합니다. 부팅 디바이스의 크기가 16GB 이상이어야 합니다.

설치 중에 ESXi 설치 관리자가 부팅 디바이스에 코어 덤프 파티션을 생성합니다. 코어 덤프 파티션의 기본 크기는 대부분의 설치 요구 사항을 충족합니다.

ESXi 호스트의 메모리가 512GB 이하인 경우에는 USB, SD 또는 SATADOM 디바이스에서 호스트를 부팅할 수 있습니다. ESXi 호스트의 메모리가 512GB를 초과하는 경우 SATADOM 또는 디스크 디바이스에서 호스트를 부팅해야 합니다.

참고 vSAN 6.5 이상에서는 vSAN 클러스터에 있는 ESXi 호스트의 기존 코어 덤프 파티션 크기를 조정할 수 있으며, 호스트를 USB/SD 디바이스에서 부팅할 수 있습니다. 자세한 내용은 <http://kb.vmware.com/kb/2147881>에서 VMware 기술 자료 문서를 참조하십시오.

디스크에서 부팅하는 호스트에는 로컬 VMFS가 있습니다. VM을 실행하는 VMFS가 포함된 디스크가 있는 경우에는 vSAN에 사용하지 않을 ESXi 부팅용 디스크를 구분해야 합니다. 이 경우에는 별도의 컨트롤러가 필요합니다.

vSAN 의 로그 정보 및 부팅 디바이스

USB 또는 SD 디바이스에서 ESXi를 부팅하면 호스트 재부팅 시 로그 정보와 스택 추적이 손실됩니다. 그 이유는 스크래치 파티션이 RAM 드라이브에 있기 때문입니다. 로그, 스택 추적 및 메모리 덤프에는 영구 스토리지를 사용하십시오.

로그 정보를 vSAN 데이터스토어에 저장하면 안 됩니다. vSAN 클러스터의 장애가 로그 정보의 액세스 지원에 영향을 미칠 수 있기 때문에 이 구성은 지원되지 않습니다.

영구 로그 스토리지에 대해 다음 옵션을 고려하십시오.

- vSAN에 사용되지 않으며 VMFS 또는 NFS로 포맷된 스토리지 디바이스를 사용합니다.
- 호스트에서 ESXi Dump Collector 및 vSphere Syslog Collector가 메모리 덤프 및 시스템 로그를 vCenter Server로 보내도록 구성하십시오.

영구 위치가 있는 스크래치 파티션을 설정하는 방법에 대해서는 vSphere 설치 및 설정 설명서를 참조하십시오.

vSAN 클러스터의 영구 로깅

vSAN 클러스터의 호스트에서 영구적 로그를 위한 스토리지를 제공합니다.

ESXi를 USB 또는 SD 디바이스에 설치하고 vSAN에 로컬 스토리지를 할당하면 영구 로깅을 저장할 충분한 로컬 스토리지 또는 데이터스토어 공간이 남지 않을 수 있습니다.

로그 정보의 손실을 방지하려면 ESXi 메모리 덤프 및 시스템 로그를 네트워크 서버로 리디렉션하도록 ESXi Dump Collector 및 vSphere Syslog Collector를 구성하십시오. vSphere 설치 및 설정 설명서를 참조하십시오.

vSAN 에 대해 신규 또는 기존 클러스터 준비

4

클러스터에서 vSAN을 사용하도록 설정하고 가상 시스템 스토리지로 사용하기 전에 vSAN의 올바른 작동에 필요한 인프라를 제공해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “스토리지 디바이스의 호환성 선택 또는 확인,” (35 페이지)
- “스토리지 준비,” (36 페이지)
- “vSAN에 대한 메모리 제공,” (39 페이지)
- “vSAN에 대한 호스트 준비,” (40 페이지)
- “vSAN 및 vCenter Server 호환성,” (40 페이지)
- “스토리지 컨트롤러 준비,” (40 페이지)
- “vSAN 네트워크 구성,” (41 페이지)
- “vSAN 라이선스에 대한 고려 사항,” (42 페이지)

스토리지 디바이스의 호환성 선택 또는 확인

vSAN을 배포하기 전 중요 단계는 VMware 호환성 가이드 항목을 참조하여 스토리지 디바이스, 드라이버 및 펌웨어가 vSAN과 호환되는지 확인하는 것입니다.

vSAN 호환성을 위한 여러 옵션 중에서 선택할 수 있습니다.

- OEM 벤더와 VMware가 vSAN 호환성을 검증한 물리적 서버인 vSAN Ready 노트 서버를 사용합니다.
- 검증된 디바이스 모델에서 개별 구성 요소를 선택하여 노트를 구성합니다.

VMware 호환성 가이드 섹션

확인을 위한 구성 요소 유형

| | |
|------|--|
| 시스템 | ESXi를 실행하는 물리적 서버. |
| vSAN | <ul style="list-style-type: none">■ 하이브리드 구성을 위한 자기 디스크 SAS 또는 SATA 모델.■ VMware 호환성 가이드에 나열되어 있는 플래시 디바이스 모델. PCIe 플래시 디바이스의 특정 모델은 vSAN과 함께 사용할 수도 있습니다. 쓰기 내구성과 성능 등급도 고려합니다.■ 페스스루를 지원하는 스토리지 컨트롤러 모델. <p>각 스토리지 디바이스가 개별 RAID 0 그룹으로 표시되는 경우 vSAN은 RAID 0 모드에 대해 구성된 스토리지 컨트롤러와 함께 사용할 수 있습니다.</p> |

스토리지 준비

vSAN과 vSAN 데이터스토어를 사용하는 가상 워크로드에 충분한 디스크 공간을 제공합니다.

스토리지 디바이스 준비

vSAN에 대한 요구 사항에 따라 플래시 디바이스 및 자기 디스크를 사용합니다.

예상되는 가상 시스템 사용량 및 가상 시스템 스토리지 정책의 **허용할 수 있는 장애의 기본 수준**을 수용할 수 있는 용량이 클러스터에 있는지 확인합니다.

스토리지 디바이스가 다음 요구 사항을 충족해야 vSAN이 해당 디바이스를 할당할 수 있습니다.

- 스토리지 디바이스가 ESXi 호스트에 로컬입니다. vSAN은 원격 디바이스를 할당할 수 없습니다.
- 스토리지 디바이스에 기존 파티션 정보가 없습니다.
- 동일한 호스트에 플래시 전용 디스크 그룹과 하이브리드 디스크 그룹이 모두 있을 수 없습니다.

디스크 그룹에 사용할 디바이스 준비

각 디스크 그룹은 하나의 플래시 캐싱 디바이스와 하나 이상의 자기 디스크 또는 하나의 플래시 용량 디바이스를 제공합니다. 플래시 캐싱 디바이스의 용량은 보호 복사본을 제외하고 용량 디바이스의 예상 스토리지 사용량의 10퍼센트 이상이어야 합니다.

vSAN을 사용하려면 3개 이상의 호스트로 구성된 클러스터에 스토리지를 제공하는 하나 이상의 디스크 그룹이 호스트에 있어야 합니다. 최고의 vSAN 성능을 위해서는 구성이 동일한 호스트를 사용합니다.

원시 용량 및 사용 가능 용량

가상 시스템이 특정 사례를 처리하기 위한 용량보다 큰 원시 스토리지 용량을 제공하십시오.

- 플래시 캐싱 디바이스의 크기를 용량으로 포함하지 마십시오. 이러한 디바이스는 스토리지를 제공하지 않으며 스토리지에 대한 플래시 디바이스를 추가한 경우 이외에는 캐시로 사용됩니다.
- 가상 시스템 스토리지 정책의 **PFTT(허용할 수 있는 장애의 기본 수준)** 값을 처리하기에 충분한 공간을 제공하십시오. PFTT가 0보다 크면 디바이스 공간이 확장됩니다. PFTT를 1로 설정하면 공간이 두 배가 됩니다. PFTT를 2로 설정하면 공간이 세 배가 되며, 이 같은 방식으로 증가합니다.
- 통합된 vSAN 데이터스토어 개체가 아니라 개별 호스트의 공간을 확인하여 vSAN 데이터스토어에 운영을 위한 충분한 공간이 있는지 확인합니다. 예를 들어 호스트를 제거할 때 데이터스토어의 사용 가능한 공간 모두가 현재 제거하고 있는 호스트에 있어서 클러스터가 다른 호스트로의 제거를 수용하지 못할 수 있습니다.
- 씬 프로비저닝된 스토리지가 포함된 워크로드가 대량의 스토리지를 사용하기 시작할 경우 데이터스토어의 용량 부족을 방지하기 위해 충분한 공간을 제공하십시오.
- 물리적 스토리지가 vSAN 클러스터에서 호스트의 다시 보호 및 유지 보수 모드를 수용할 수 있는지 확인합니다.
- 사용 가능한 스토리지 공간에 대한 vSAN 오버헤드를 고려합니다.
 - 온디스크 형식 버전 1.0에서는 용량 디바이스당 약 1GB의 추가적인 오버헤드를 추가합니다.
 - 온디스크 형식 버전 2.0에서는 일반적으로 디바이스당 용량의 1-2%를 초과하지 않는 추가적인 오버헤드를 추가합니다.
 - 온디스크 형식 버전 3.0 이상에서는 일반적으로 디바이스당 용량의 1-2%를 초과하지 않는 추가적인 오버헤드를 추가합니다. 소프트웨어 체크섬을 사용하도록 설정된 중복 제거 및 압축 기능을 사용하려면 디바이스당 용량의 6.2% 정도에 해당하는 추가적인 오버헤드가 필요합니다.

vSAN 데이터스토어의 용량 계획에 대한 자세한 내용은 VMware vSAN 설계 및 크기 조정 가이드 항목을 참조하십시오.

용량에 대한 vSAN 정책의 영향

가상 시스템에 대한 vSAN 스토리지 정책은 몇 가지 방식으로 용량 디바이스에 영향을 미칩니다.

표 4-1. vSAN VM 정책 및 원시 용량

| 정책 영향의 측면 | 설명 |
|------------------------------|---|
| 정책 변경 | <ul style="list-style-type: none"> ■ PFTT(허용할 수 있는 장애의 기본 수준)은 가상 시스템에 제공해야 하는 물리적 스토리지 공간에 영향을 미칩니다. PFTT를 크게 설정할수록 가용성이 향상되지만 더 많은 공간을 제공해야 합니다. <p>PFTT를 1로 설정하면 가상 시스템의 VMDK 파일 복제본 두 개가 적용됩니다. PFTT를 1로 설정하면 50GB인 VMDK 파일의 경우 여러 호스트에 100GB의 공간이 필요합니다. PFTT를 2로 변경하면 클러스터의 호스트 전체에 세 개의 VMDK 복제본을 지원할 수 있는 공간, 즉 150GB의 공간이 있어야 합니다.</p> <ul style="list-style-type: none"> ■ 개체당 디스크 스트라이프 수의 변경과 같은 일부 정책 변경의 경우에는 임시 리소스가 필요합니다. vSAN은 변경의 영향을 받는 개체를 재생성합니다. 특정 시간 동안 물리적 스토리지는 이전 개체 및 새 개체를 수용해야 합니다. |
| 다시 보호 또는 유지 보수 모드에 사용 가능한 공간 | 호스트를 유지 보수 모드로 전환하거나 가상 시스템을 복제하는 경우 vSAN 데이터스토어가 충분한 공간을 사용할 수 있음을 나타내더라도 데이터스토어가 가상 시스템 개체를 제거하지 못할 수 있습니다. 이러한 공간 부족은 사용 가능한 공간이 유지 보수 모드로 전환 중인 호스트에 있는 경우 발생할 수 있습니다. |

ESXCLI를 사용하여 플래시 디바이스를 용량으로 표시

esxcli를 사용하여 수동으로 각 호스트의 플래시 디바이스를 용량 디바이스로 표시할 수 있습니다.

필수 조건

vSAN 6.5 이상을 사용 중인지 확인합니다.

프로시저

- 1 용량으로 표시할 플래시 디바이스의 이름을 알아보려면 각 호스트에서 다음 명령을 실행합니다.
 - a ESXi Shell에서 esxcli storage core device list 명령을 실행합니다.
 - b 명령 출력의 맨 위에서 디바이스 이름을 찾고 해당 이름을 기록합니다.
 이 명령에는 다음 옵션이 해당됩니다.

표 4-2. 명령 옵션

| 옵션 | 설명 |
|---------------|---|
| -d --disk=str | 용량 디바이스로 태그 지정할 디바이스의 이름입니다. 예를 들어 mpx.vmhba1:C0:T4:L0입니다. |
| -t --tag=str | 추가하거나 제거할 태그를 지정합니다. 예를 들어 capacityFlash 태그는 용량을 위한 플래시 디바이스를 표시하는 데 사용됩니다. |

이 명령은 ESXi에서 식별된 모든 디바이스 정보를 나열합니다.

- 2 출력에서 디바이스에 대한 Is SSD 특성이 true인지 확인합니다.
- 3 플래시 디바이스를 용량으로 태그 지정하려면 esxcli vsan storage tag add -d <device name> -t capacityFlash 명령을 실행합니다.

예를 들어 esxcli vsan storage tag add -t capacityFlash -d mpx.vmhba1:C0:T4:L0 명령을 사용합니다. 여기서 mpx.vmhba1:C0:T4:L0는 디바이스 이름입니다.

4 플래시 디바이스가 용량으로 표시되었는지 확인합니다.

- a 출력에서 디바이스에 대한 IsCapacityFlash 특성이 1으로 설정되었는지 확인합니다.

예: 명령 출력

vdq -q -d <device name> 명령을 실행하여 IsCapacityFlash 특성을 확인할 수 있습니다. 예를 들어 vdq -q -d mpx.vmhba1:C0:T4:L0 명령을 실행하면 다음과 같은 출력이 반환됩니다.

```
W{
  "Name"      : "mpx.vmhba1:C0:T4:L0",
  "VSANUID"   : "",
  "State"     : "Eligible for use by VSAN",
  "ChecksumSupport": "0",
  "Reason"    : "None",
  "IsSSD"     : "1",
  "IsCapacityFlash": "1",
  "IsPDL"     : "0",
  W},
```

ESXCLI를 사용하여 용량으로 사용되는 플래시 디바이스의 태그 해제

용량 디바이스로 사용되는 플래시 디바이스의 태그를 해제하여 캐싱에 사용 가능하도록 만들 수 있습니다.

프로시저

- 1 용량으로 표시된 플래시 디바이스의 태그를 해제하려면 esxcli vsan storage tag remove -d <device name> -t capacityFlash 명령을 실행하십시오. 예를 들어 esxcli vsan storage tag remove -t capacityFlash -d mpx.vmhba1:C0:T4:L0 명령을 사용합니다. 여기서 mpx.vmhba1:C0:T4:L0는 디바이스 이름입니다.
- 2 플래시 디바이스가 태그 해제되었는지 확인합니다.
 - a 출력에서 디바이스에 대한 IsCapacityFlash 특성이 0으로 설정되었는지 확인합니다.

예: 명령 출력

vdq -q -d <device name> 명령을 실행하여 IsCapacityFlash 특성을 확인할 수 있습니다. 예를 들어 vdq -q -d mpx.vmhba1:C0:T4:L0 명령을 실행하면 다음과 같은 출력이 반환됩니다.

```
[
  W{
    "Name"      : "mpx.vmhba1:C0:T4:L0",
    "VSANUID"   : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "None",
    "IsSSD"     : "1",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
    W},
```

RVC를 사용하여 플래시 디바이스를 용량으로 표시

`vsan.host_claim_disks_differently` RVC 명령을 실행하여 스토리지 디바이스를 플래시, 용량 플래시 또는 자기 디스크(HDD)로 표시합니다.

RVC 도구를 사용하여 플래시 디바이스를 개별적으로 또는 디바이스 모델을 지정하여 일괄적으로 용량 디바이스로 태그 지정할 수 있습니다. 플래시 디바이스를 용량 디바이스로 태그 지정하려는 경우 해당 디바이스를 플래시 전용 디스크 그룹에 포함할 수 있습니다.

참고 `vsan.host_claim_disks_differently` 명령은 디바이스를 태그 지정하기 전에 디바이스 유형을 확인하지 않습니다. 이 명령은 이미 사용 중인 자기 디스크와 디바이스를 포함하여 `capacity_flash` 명령 옵션을 사용하여 추가하는 모든 디바이스를 태그 지정합니다. 태그 지정하기 전에 디바이스 상태를 확인합니다.

vSAN 관리를 위한 RVC 명령에 대한 자세한 내용은 RVC 명령 참조 가이드 항목을 참조하십시오.

필수 조건

- vSAN 버전 6.5 이상을 사용 중인지 확인합니다.
- vCenter Server Appliance에서 SSH가 사용하도록 설정되어 있는지 확인합니다.

프로시저

- 1 vCenter Server Appliance에 대한 SSH 연결을 엽니다.
- 2 관리자 권한이 있는 로컬 계정을 사용하여 장치에 로그인합니다.
- 3 다음 명령을 실행하여 RVC를 시작합니다.

```
rvc local_user_name@target_vCenter_Server
```

예를 들어 동일한 vCenter Server Appliance를 사용하여 용량을 위한 플래시 디바이스를 사용자 루트로 표시하려면 다음 명령을 실행합니다.

```
rvc root@localhost
```

- 4 사용자 이름에 대한 암호를 입력합니다.
- 5 vSphere 인프라의 `vcenter_server/data_center/computers/cluster/hosts` 디렉토리로 이동합니다.
- 6 `vsan.host_claim_disks_differently` 명령을 `--claim-type capacity_flash --model model_name` 옵션과 함께 실행하여 클러스터의 모든 호스트에서 동일한 모델의 모든 플래시 디바이스를 용량으로 표시합니다.

```
vsan.host_claim_disks_differently --claim-type capacity_flash --model model_name *
```

후속 작업

클러스터에서 vSAN을 사용하도록 설정하고 용량 디바이스를 할당합니다.

vSAN 에 대한 메모리 제공

vSAN에 매핑하려고 하는 디스크 그룹 및 디바이스의 최대 수에 해당하는 메모리를 사용하여 호스트를 프로비저닝해야 합니다.

디바이스 및 디스크 그룹의 최대 수를 충족하려면 시스템 운영을 위한 32GB의 메모리를 가진 호스트를 프로비저닝해야 합니다. 최대 디바이스 구성에 대해서는 vSphere 구성 최대값 설명서를 참조하십시오.

vSAN 에 대한 호스트 준비

vSAN을 사용하도록 설정하기 위한 준비의 일부로 클러스터의 호스트 구성에 대한 요구 사항 및 권장 사항을 검토합니다.

- 호스트의 스토리지 디바이스와 해당 디바이스에 대한 드라이버 및 펌웨어 버전이 VMware 호환성 가이드의 vSAN 섹션에 나열되어 있는지 확인합니다.
- 3개 이상의 호스트가 vSAN 데이터스토어에 스토리지를 제공하는지 확인합니다.
- 장애 시 유지 보수 및 업데이트 적용 작업의 경우 클러스터에 4개 이상의 호스트를 추가합니다.
- 클러스터에서 최상의 스토리지 균형을 위한 일관된 구성을 가진 호스트를 지정합니다.
- 스토리지를 제공하는 호스트에 대한 스토리지 구성 요소의 불균형 배포를 방지하기 위해 계산 리소스만 가진 호스트를 클러스터에 추가하지 마십시오. 많은 스토리지 공간을 요구하며 계산 전용 호스트에서 실행되는 가상 시스템은 개별 용량 호스트에 많은 구성 요소를 저장할 수 있습니다. 따라서 클러스터의 스토리지 성능이 낮을 수 있습니다.
- 전원 절약을 위해 호스트에 대한 적극적 CPU 전원 관리 정책을 구성하지 마십시오. CPU 속도 지연 시간에 민감한 특정 애플리케이션의 성능은 매우 낮을 수 있습니다. CPU 전원 관리 정책에 대한 자세한 내용은 vSphere 리소스 관리 설명서를 참조하십시오.
- 클러스터에 블레이드 서버가 포함되어 있는 경우 블레이드 서버에 연결되어 있으며 VMware 호환성 가이드의 vSAN 섹션에 나열되어 있는 외부 스토리지 인클로저를 통해 데이터스토어의 용량을 확장하는 것을 고려합니다.
- 하이브리드 또는 플래시 전용 디스크 구성에 배치하는 워크로드의 구성을 고려합니다.
 - 높은 수준의 예측 가능한 성능이 필요한 경우 플래시 전용 디스크 그룹의 클러스터를 제공합니다.
 - 성능과 비용 간의 균형이 필요한 경우 하이브리드 디스크 그룹의 클러스터를 제공합니다.

vSAN 및 vCenter Server 호환성

vCenter Server 및 ESXi의 vSAN 지원 차이로 인한 잠재적 장애를 방지하려면 vCenter Server의 버전과 ESXi의 버전을 동기화합니다.

vCenter Server 및 ESXi의 vSAN 구성 요소 간의 최상의 통합을 위해 두 vSphere 구성 요소의 최신 버전을 배포합니다. vSphere 설치 및 설정 및 vSphere 업그레이드 설명서를 참조하십시오.

스토리지 컨트롤러 준비

vSAN의 요구 사항에 따라 호스트에 스토리지 컨트롤러를 구성합니다.

vSAN 호스트의 스토리지 컨트롤러가 모드, 드라이버 및 펌웨어 버전, 대기열 크기, 캐시 및 고급 기능에 대한 특정 요구 사항을 충족하는지 확인합니다.

표 4-3. vSAN 에 대한 스토리지 컨트롤러 구성 검사

| 스토리지 컨트롤러 기능 | 스토리지 컨트롤러 요구 사항 |
|---------------|---|
| 필수 모드 | <ul style="list-style-type: none"> VMware 호환성 가이드에서 필요한 컨트롤러 모드인 패스스루 또는 RAID 0에 대한 vSAN 요구 사항을 검토합니다. 패스스루 모드와 RAID 0 모드가 모두 지원되는 경우 RAID 0 대신 패스스루 모드를 구성합니다. RAID 0은 디스크 교체에 대한 복잡성을 초래합니다. |
| RAID 모드 | <ul style="list-style-type: none"> RAID 0의 경우 물리적 디스크 디바이스당 하나의 RAID 볼륨을 생성합니다. VMware 호환성 가이드에 나열되어 있는 모드 이외의 RAID 모드를 사용하도록 설정하지 마십시오. 컨트롤러 스페닝을 사용하도록 설정하지 마십시오. |
| 드라이버 및 펌웨어 버전 | <ul style="list-style-type: none"> VMware 호환성 가이드에 따라 컨트롤러에 대해 최신 드라이버 및 펌웨어 버전을 사용합니다. 기본 제공 컨트롤러 드라이버를 사용하는 경우 해당 드라이버가 vSAN에 대해 인증되었는지 확인합니다. <p>OEM ESXi 릴리스에는 인증되지 않았으며 VMware 호환성 가이드에 나열되어 있지 않은 드라이버가 포함되어 있을 수 있습니다.</p> |
| 대기열 크기 | 컨트롤러의 대기열 크기가 256 이상인지 확인합니다. 큰 대기열 크기는 향상된 성능을 제공합니다. |
| 캐시 | 스토리지 컨트롤러 캐시를 사용하지 않도록 설정하거나 캐시를 사용하지 않도록 설정하는 것이 불가능한 경우 100% 읽기로 설정합니다. |
| 고급 기능 | HP SSD Smart Path와 같은 고급 기능을 사용하지 않도록 설정합니다. |

vSAN 네트워크 구성

클러스터 및 ESXi 호스트에서 vSAN을 사용하도록 설정하기 전에 vSAN 통신에 필요한 네트워크를 구성해야 합니다.

vSAN은 클러스터에 참여하는 ESXi 호스트 간의 데이터 교환을 수반하는 분산 스토리지 솔루션을 제공합니다. vSAN을 설치하기 위해 네트워크를 준비할 때는 특정한 구성 작업을 수행해야 합니다.

네트워크 설계 지침에 대한 자세한 내용은 “vSAN 네트워크 설계,” (29 페이지)를 참조하십시오.

호스트를 동일한 서브넷에 배치

최상의 네트워킹 성능을 위해서는 호스트를 동일한 서브넷에서 연결해야 합니다. vSAN 6.0 이상에서는 필요한 경우 동일한 계층 3 네트워크에 있는 호스트를 연결할 수도 있습니다.

물리적 어댑터에서 전용 네트워크 대역폭 지정

vSAN에 대해 1Gbps 이상의 대역폭을 할당합니다. 다음 구성 옵션 중 하나를 사용할 수 있습니다.

- 1GbE 물리적 어댑터를 하이브리드 호스트 구성 전용으로 지정합니다.
- 플래시 전용 구성에 전용 또는 공유 10GbE 물리적 어댑터를 사용합니다.
- 가능한 경우 하이브리드 구성에 전용 또는 공유 10GbE 물리적 어댑터를 사용합니다.
- 다른 시스템 트래픽을 처리하는 10GbE 물리적 어댑터에서 vSAN 트래픽을 경로 지정하고 Distributed Switch에서 vSphere Network I/O Control을 사용하여 vSAN을 위한 대역폭을 예약합니다.

가상 스위치에서 포트 그룹 구성

가상 스위치에서 vSAN용 포트 그룹을 구성합니다.

- vSAN용 물리적 어댑터를 활성 업링크로 포트 그룹에 할당합니다.
네트워크 가용성을 위해 NIC 팀을 사용하는 경우 스위치에 대한 물리적 어댑터의 연결에 기반하여 팀 구성 알고리즘을 선택합니다.
- 원하는 경우 가상 스위치에서 태그 지정을 사용하도록 설정하여 vSAN 트래픽을 VLAN에 할당합니다.

호스트의 방화벽을 vSAN 에 대해 검사

vSAN은 클러스터의 각 호스트에서 특정 포트를 통해 메시지를 전송합니다. 호스트 방화벽이 이러한 포트에서 트래픽을 허용하는지 확인하십시오.

표 4-4. vSAN 호스트의 포트

| vSAN 서비스 | 트래픽 방향 | 통신 노드 | 전송 프로토콜 | 포트 |
|-------------------------|---------|--------------------------|---------|-----------------|
| vSAN 밴더 제 공자(vsanvp) | 수신 및 송신 | vCenter Server 및 ESXi | TCP | 8080 |
| vSAN 클러스 터링 서비스 | | ESXi | UDP | 12345, 23451 |
| vSAN 전송 | | ESXi | TCP | 2233 |
| 유니캐스트 에이 전트 | | ESXi | UDP | 12321 |

vSAN 라이선스에 대한 고려 사항

vSAN에 대한 클러스터를 준비하는 경우 vSAN 라이선스의 요구 사항을 검토합니다.

- 클러스터의 전체 호스트 구성 제어를 위한 유효한 라이선스를 얻었는지 확인합니다. 라이선스는 평가 목적으로 사용하는 라이선스와 달라야 합니다.
vSAN의 라이선스 또는 평가 기간이 만료된 후 계속해서 vSAN 리소스의 현재 구성을 사용할 수 있습니다. 그러나 용량을 디스크 그룹에 추가하거나 디스크 그룹을 생성할 수 없습니다.
- 클러스터가 플래시 전용 디스크 그룹으로 구성된 경우 라이선스에서 플래시 전용 기능을 사용할 수 있는지 확인합니다.
- vSAN 클러스터에서 중복 제거와 압축 또는 확장된 클러스터 같은 고급 기능을 사용하는 경우 라이선스에서 해당 기능을 사용할 수 있는지 확인합니다.
- 호스트를 클러스터에 추가하거나 클러스터에서 제거할 때 클러스터 전체에서 vSAN 라이선스의 CPU 용량을 고려합니다.

vSAN 라이선스에는 CPU당 용량이 있습니다. vSAN 라이선스를 클러스터에 할당하는 경우 사용되는 라이선스 용량은 클러스터에 참여하는 호스트의 총 CPU 수와 같습니다.

vSAN 클러스터 생성

클러스터를 생성할 때 vSAN을 활성화하거나, 기존 클러스터에서 vSAN을 사용하도록 설정할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN 클러스터의 특성,”](#) (43 페이지)
- [“vSAN 클러스터를 생성하기 전,”](#) (44 페이지)
- [“vSAN 사용,”](#) (45 페이지)
- [“vSAN 구성 지원 및 업데이트 사용,”](#) (54 페이지)

vSAN 클러스터의 특성

vSAN 환경에서 작업하기 전에 vSAN 클러스터의 특성에 대해 알아두어야 합니다.

vSAN 클러스터에는 다음과 같은 특성이 포함됩니다.

- 각 vCenter Server 인스턴스에 대해 여러 개의 vSAN 클러스터를 사용할 수 있습니다. 하나의 vCenter Server를 사용하여 2개 이상의 vSAN 클러스터를 관리할 수 있습니다.
- vSAN은 플래시 캐시 및 용량 디바이스를 포함하여 모든 디바이스를 사용하며 디바이스를 다른 기능과 공유하지 않습니다.
- vSAN 클러스터에는 용량 디바이스가 있거나 없는 호스트가 포함될 수 있습니다. 최소 요구 사항은 용량 디바이스가 있는 호스트를 세 개 포함하는 것입니다. 최상의 결과를 위해서는 동일하게 구성된 호스트가 포함된 vSAN 클러스터를 생성합니다.
- 호스트가 용량을 제공하는 경우 해당 호스트에는 최소 하나의 플래시 캐시 디바이스와 하나의 용량 디바이스가 있어야 합니다.
- 하이브리드 클러스터에서는 자기 디스크가 용량에 사용되며 플래시 디바이스는 읽기 및 쓰기 캐시에 사용됩니다. vSAN은 사용 가능한 모든 캐시의 70%를 읽기 캐시에 할당하고 사용 가능한 캐시의 30%를 쓰기 버퍼에 할당합니다. 이 구성에서는 플래시 디바이스가 읽기 캐시 및 쓰기 버퍼의 역할을 합니다.
- 플래시 전용 클러스터에서는 하나의 지정된 플래시 디바이스가 쓰기 캐시로 사용되고 추가적인 플래시 디바이스가 용량에 사용됩니다. 플래시 전용 클러스터에서는 모든 읽기 요청이 플래시 풀 용량으로부터 직접 수신됩니다.
- 로컬 또는 직접 연결된 용량 디바이스만 vSAN 클러스터에 참여할 수 있습니다. vSAN은 클러스터에 연결된 SAN이나 NAS 등의 다른 외부 스토리지를 사용할 수 없습니다.

vSAN 클러스터의 설계 및 크기 조정에 대한 모범 사례는 [3장, “vSAN 클러스터 설계 및 크기 조정,”](#) (21 페이지) 항목을 참조하십시오.

vSAN 클러스터를 생성하기 전

이 항목에서는 vSAN 클러스터를 생성하기 위한 소프트웨어 및 하드웨어 요구 사항의 검사 목록을 제공합니다. 이 검사 목록을 사용하여 클러스터가 지침 및 기본 요구 사항을 충족하는지도 확인할 수 있습니다.

vSAN 클러스터에 대한 요구 사항

시작하기 전에 VMware 호환성 가이드 웹 사이트 (<http://www.vmware.com/resources/compatibility/search.php>)에서 하드웨어 디바이스의 특정 모델과 드라이버 및 펌웨어의 특정 버전을 확인하십시오. 다음 표에서는 vSAN이 지원하는 주요 소프트웨어 및 하드웨어 요구 사항을 나열합니다.



주의 인증되지 않은 소프트웨어 및 하드웨어 구성 요소, 드라이버, 컨트롤러 및 펌웨어를 사용하면 예기치 않은 데이터 손실 및 성능 문제가 발생할 수 있습니다.

표 5-1. vSAN 클러스터 요구 사항

| 요구 사항 | 설명 |
|--------------------------|--|
| ESXi 호스트 | <ul style="list-style-type: none"> 호스트에서 최신 버전의 ESXi를 사용하고 있는지 확인합니다. 지원되는 스토리지 구성이 적용된 ESXi 호스트를 3개 이상 vSAN 클러스터에 할당할 수 있는지 확인합니다. 최상의 결과를 위해서는 4개 이상의 호스트로 vSAN 클러스터를 구성합니다. |
| 메모리 | <ul style="list-style-type: none"> 각 호스트에 최소 8GB의 메모리가 있는지 확인합니다. 더 큰 규모의 구성과 향상된 성능을 위해서는 클러스터에 최소 32GB의 메모리가 있어야 합니다. “vSAN 호스트 설계 및 크기 조정,” (27 페이지)를 참조하십시오. |
| 스토리지 I/O 컨트롤러, 드라이버, 펌웨어 | <ul style="list-style-type: none"> 스토리지 I/O 컨트롤러, 드라이버 및 펌웨어 버전이 인증되고 VCG 웹 사이트 (http://www.vmware.com/resources/compatibility/search.php)에 나열되어 있는지 확인합니다. 컨트롤러가 패스트루 또는 RAID 0 모드에 대해 구성되었는지 확인합니다. 컨트롤러 캐시 및 고급 기능이 비활성화되어 있는지 확인합니다. 캐시를 비활성화할 수 없는 경우 읽기 캐시를 100퍼센트로 설정해야 합니다. 대기열 깊이가 높은 컨트롤러를 사용하고 있는지 확인합니다. 대기열 깊이가 256 미만인 컨트롤러를 사용하면 유지 보수 및 장애 시 가상 시스템의 성능에 큰 영향을 미칠 수 있습니다. |
| 캐시 및 용량 | <ul style="list-style-type: none"> 클러스터에 스토리지를 제공하는 vSAN 호스트에 최소 하나의 캐시 디바이스와 하나의 용량 디바이스가 있는지 확인합니다. vSAN은 vSAN 클러스터에 있는 호스트의 로컬 캐시 디바이스 및 용량 디바이스에 단독으로 액세스할 수 있어야 합니다. VFFS(Virtual Flash File System), VMFS 파티션 또는 ESXi 부팅 파티션 같은 다른 용도와 이러한 디바이스를 공유할 수 없습니다. 최상의 결과를 위해서는 동일하게 구성된 호스트를 사용하여 vSAN 클러스터를 생성합니다. |
| 네트워크 연결 | <ul style="list-style-type: none"> 각 호스트가 최소 하나의 네트워크 어댑터로 구성되어 있는지 확인합니다. 하이브리드 구성의 경우 vSAN 호스트에 최소 1GbE의 전용 대역폭이 있는지 확인합니다. 플래시 전용 구성의 경우 vSAN 호스트에 최소 10GbE의 대역폭이 있는지 확인합니다. <p>vSAN 네트워크 설계에 대한 모범 사례 및 고려 사항에 대해서는 “vSAN 네트워크 설계,” (29 페이지) 및 “vSAN에 대한 네트워킹 요구 사항,” (19 페이지)을 참조하십시오.</p> |

표 5-1. vSAN 클러스터 요구 사항 (계속)

| 요구 사항 | 설명 |
|---------------------------|--|
| vSAN 및 vCenter Server 호환성 | 최신 버전의 vCenter Server를 사용하고 있는지 확인합니다. |
| 라이선스 키 | <ul style="list-style-type: none"> ■ 유효한 vSAN 라이선스 키가 있는지 확인합니다. ■ 플래시 전용 기능을 사용하려면 라이선스가 해당 기능을 지원해야 합니다. ■ 확장된 클러스터 또는 중복 제거와 압축 같은 고급 기능을 사용하려면 라이선스가 이러한 기능을 지원해야 합니다. ■ 사용하려는 라이선스 용량이 vSAN 클러스터에 참여하는 호스트의 총 CPU 수와 같은지 확인합니다. 클러스터에 용량을 제공하는 호스트에만 라이선스 용량을 제공해서는 안 됩니다. vSAN 라이선싱에 대한 자세한 내용은 vCenter Server 및 호스트 관리 설명서를 참조하십시오. |

vSAN 클러스터 요구 사항에 대한 자세한 내용은 2장, “vSAN을 사용하도록 설정하기 위한 요구 사항,” (17 페이지)을 참조하십시오.

vSAN 클러스터 설계 및 크기 조정에 대한 자세한 내용은 VMware vSAN 설계 및 크기 조정 가이드를 참조하십시오.

vSAN 사용

vSAN을 사용하려면 호스트 클러스터를 생성하고 해당 클러스터에서 vSAN을 사용하도록 설정해야 합니다.

vSAN 클러스터에는 용량이 있는 호스트와 용량이 없는 호스트가 포함될 수 있습니다. vSAN 클러스터를 생성할 때는 다음 지침을 따릅니다.

- vSAN 클러스터에는 최소 3개의 ESXi 호스트가 포함되어야 합니다. vSAN 클러스터에서 호스트 및 디바이스 장애를 허용하려면 vSAN 클러스터에 가입된 3개 이상의 호스트가 클러스터에 용량을 제공해야 합니다. 최상의 결과를 얻으려면 클러스터에 용량을 제공하는 4개 이상의 호스트를 추가하는 것을 고려합니다.
- ESXi 5.5 업데이트 1 이상 호스트만 vSAN 클러스터에 가입될 수 있습니다.
- vSAN 클러스터에 있는 모든 호스트는 온디스크 형식이 동일해야 합니다.
- 호스트를 한 vSAN 클러스터에서 다른 클러스터로 이동하기 전에 대상 클러스터에서 vSAN이 사용되도록 설정되었는지 확인합니다.
- vSAN 데이터스토어에 액세스할 수 있으려면 ESXi 호스트가 vSAN 클러스터의 멤버여야 합니다.

vSAN을 사용하도록 설정한 후 vSAN 스토리지 제공자가 vCenter Server에 자동으로 등록되고 vSAN 데이터스토어가 생성됩니다. 스토리지 제공자에 대한 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.

vSAN 에 대한 VMkernel 네트워크 설정

vSAN 클러스터에서 데이터 교환을 사용하도록 설정하려면 각 ESXi 호스트에 vSAN 트래픽에 대한 VMkernel 네트워크 어댑터를 제공해야 합니다.

프로시저

- 1 vSphere Web Client에서 호스트로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 **네트워킹**에서 **VMkernel 어댑터**를 선택합니다.
- 4 **호스트 네트워킹 추가** 아이콘(🌐)을 클릭하여 [네트워킹 추가] 마법사를 엽니다.
- 5 연결 유형 선택 페이지에서 **VMkernel 네트워크 어댑터**를 선택한 후 **다음**을 클릭합니다.
- 6 대상 스위칭 디바이스를 구성합니다.

- 7 포트 속성 페이지에서 **vSAN 트래픽**을 선택합니다.
- 8 VMkernel 어댑터 구성을 완료합니다.
- 9 완료 준비 페이지에서 VMkernel 어댑터의 상태에 vSAN이 사용되도록 설정되었는지 확인한 후 **마침**을 클릭합니다.

vSAN 네트워크가 호스트에 대해 사용되도록 설정되었습니다.

후속 작업

이제 호스트 클러스터에서 vSAN을 사용하도록 설정할 수 있습니다.

vSAN 클러스터 생성

클러스터를 생성할 때 vSAN을 사용하도록 설정할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **새 클러스터**를 선택합니다.
- 2 **이름** 텍스트 상자에 클러스터의 이름을 입력합니다.
이 이름은 vSphere Web Client 탐색기에 나타납니다.
- 3 vSAN **설정** 확인란을 선택하고 **확인**을 클릭합니다.
클러스터가 인벤토리에 나타납니다.
- 4 vSAN 클러스터에 호스트를 추가합니다. **“vSAN 클러스터에 호스트 추가,”** (108 페이지)를 참조하십시오.

vSAN 클러스터에는 용량 디바이스가 있거나 없는 호스트가 포함될 수 있습니다. 최상의 결과를 얻으려면 용량이 있는 호스트를 추가하십시오.

vSAN을 사용하도록 설정하면 vSAN 데이터스토어가 생성되고 vSAN 스토리지 제공자가 등록됩니다. vSAN 스토리지 제공자는 데이터스토어의 스토리지 기능을 vCenter Server로 전달하는 기본 제공 소프트웨어 구성 요소입니다.

후속 작업

vSAN 데이터스토어가 생성되었는지 확인합니다. **“vSAN 데이터스토어 보기,”** (51 페이지)를 참조하십시오.

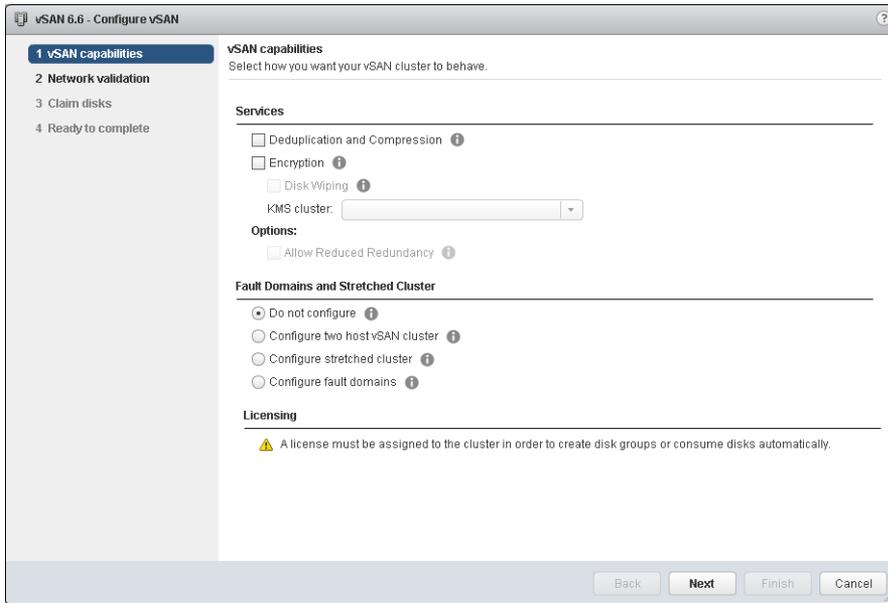
vSAN 스토리지 제공자가 등록되었는지 확인합니다. **“vSAN 스토리지 제공자 보기,”** (126 페이지)를 참조하십시오.

스토리지 디바이스를 할당하거나 디스크 그룹을 생성합니다. 10장, **“vSAN 클러스터에서 디바이스 관리,”** (99 페이지)를 참조하십시오.

vSAN 클러스터를 구성합니다. **“vSAN에 대한 클러스터 구성,”** (47 페이지)를 참조하십시오.

vSAN 에 대한 클러스터 구성

[vSAN 구성] 마법사를 사용하여 vSAN 클러스터의 기본 구성을 완료할 수 있습니다.



필수 조건

[vSAN 구성] 마법사를 사용하여 기본 구성을 완료하려면 먼저 클러스터를 생성하고 클러스터에 호스트를 추가해야 합니다.

프로시저

- 1 vSphere Web Client에서 기존 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택하고 **구성** 버튼을 클릭합니다.
- 4 **vSAN 기능**을 선택합니다.
 - a (선택 사항) 클러스터에서 중복 제거 및 압축을 사용하려면 **중복 제거 및 압축** 확인란을 선택합니다.
감소된 이중화 허용 확인란을 선택하면 3개 호스트로 구성되고 **허용할 수 있는 장애의 기본 수준**이 1로 설정된 클러스터와 같이 리소스가 제한된 vSAN 클러스터에 대해 중복 제거 및 압축을 사용하도록 설정할 수 있습니다. 감소된 이중화를 허용하면 디스크를 다시 포맷하는 작업 중에 데이터가 위험할 수 있습니다.
 - b (선택 사항) 저장된 데이터 암호화를 사용하려면 **암호화** 확인란을 선택한 후 KMS를 선택합니다.

- c 클러스터에 대해 Fault Tolerance 모드를 선택합니다.

| 옵션 | 설명 |
|---------------------|---|
| 구성 안 함 | 단일 사이트 vSAN 클러스터에 사용되는 기본 설정입니다. |
| 2개 호스트 vSAN 클러스터 구성 | 원격 사무실에 호스트 두 개와 본사 사무실에 감시 호스트 1개가 있는 클러스터에 대해 Fault Tolerance를 제공합니다. 허용할 수 있는 장애의 기본 수준 정책을 1로 설정합니다. |
| 확장된 클러스터 구성 | 각각 짝수 개의 호스트와 스토리지 디바이스가 포함된 활성 사이트 두 개 및 감시 호스트 1개가 있는 세 번째 사이트를 지원합니다. |
| 장애 도메인 구성 | 함께 장애가 발생할 수 있는 vSAN 호스트를 그룹화하는 데 사용할 수 있는 장애 도메인을 지원합니다. 각 장애 도메인에 호스트를 하나 이상 할당합니다. |

- d **감소된 이중화 허용** 확인란을 선택하면 리소스가 제한된 vSAN 클러스터에서 암호화 또는 중복 제거와 압축을 사용하도록 설정할 수 있습니다. 예를 들어, 호스트가 3개인 클러스터에 **허용할 수 있는 장애의 기본 수준**이 1로 설정된 경우입니다. 감소된 이중화를 허용하면 디스크를 다시 포맷하는 작업 중에 데이터가 위협할 수 있습니다.

5 다음을 클릭합니다.

6 네트워크 검증 페이지에서 vSAN VMkernel 어댑터의 설정을 확인하고 다음을 클릭합니다.

7 디스크 할당 페이지에서 클러스터에 사용할 디스크를 선택하고 다음을 클릭합니다.

스토리지에 기여하는 각 호스트에 대해 캐시 계층용 플래시 디바이스 하나와 용량 계층용 디바이스 하나 이상을 선택합니다.

8 마법사를 따라 Fault Tolerance 모드에 기반하여 클러스터 구성을 완료합니다.

a **2개 호스트 vSAN 클러스터 구성**을 선택한 경우, 클러스터의 감시 호스트를 선택하고 감시 호스트의 디스크를 할당합니다.

b **확장된 클러스터 구성**을 선택한 경우, 클러스터의 장애 도메인을 정의하고, 감시 호스트를 선택하고, 해당 감시 호스트의 디스크를 할당합니다.

c **장애 도메인 구성**을 선택한 경우, 클러스터의 장애 도메인을 정의합니다.

장애 도메인에 대한 자세한 내용은 [“vSAN 클러스터에서 장애 도메인 관리,”](#) (113 페이지)를 참조하십시오.

확장된 클러스터에 대한 자세한 내용은 6장, [“확장된 클러스터를 통해 2개의 사이트에 걸쳐 데이터 스토어 확장,”](#) (59 페이지)을 참조하십시오.

9 완료 준비 페이지에서 구성을 검토하고 마침을 클릭합니다.

vSAN 설정 편집

vSAN 클러스터의 설정을 편집하여 디스크 할당 방식을 변경하고 데이터 중복과 압축을 사용하도록 설정할 수 있습니다.

기존 vSAN 클러스터의 설정을 편집하여 중복 제거와 압축을 사용하도록 설정하거나 암호화를 사용하도록 설정할 수 있습니다. 중복 제거와 압축을 사용하도록 설정하거나 암호화를 사용하도록 설정하면 클러스터의 온디스크 형식이 최신 버전으로 자동 업그레이드됩니다.

프로시저

- 1 vSphere Web Client에서 vSAN 호스트 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택합니다.
- 4 [vSAN 커집] 창에서 **편집** 버튼을 클릭합니다.

- 5 (선택 사항) 클러스터에서 중복 제거와 압축을 사용하도록 설정하려면 중복 제거와 압축 확인란을 선택합니다.
vSAN이 온디스크 형식을 자동으로 업그레이드하고, 이로 인해 클러스터에 있는 모든 디스크 그룹에 대해 롤링 다시 포맷이 수행됩니다.
- 6 (선택 사항) 클러스터에서 암호화를 사용하도록 설정하려면 암호화 확인란을 선택합니다.
vSAN이 온디스크 형식을 자동으로 업그레이드하고, 이로 인해 클러스터에 있는 모든 디스크 그룹에 대해 롤링 다시 포맷이 수행됩니다.
- 7 **확인**을 클릭합니다.

기존 클러스터에서 vSAN 사용

클러스터 속성을 편집하여 기존 클러스터에 대해 vSAN을 사용하도록 설정할 수 있습니다.

클러스터에서 vSAN을 사용하도록 설정한 후 vSAN 지원 클러스터에서 비vSAN 클러스터로 vSAN 호스트를 이동할 수 없습니다.

필수 조건

환경이 모든 요구 사항을 충족하는지 확인합니다. [2장, “vSAN을 사용하도록 설정하기 위한 요구 사항,”](#) (17 페이지)를 참조하십시오.

프로시저

- 1 vSphere Web Client에서 기존 호스트 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택하고 **편집**을 클릭하여 클러스터 설정을 편집합니다.
- 4 클러스터에서 중복 제거와 압축을 사용하도록 설정하려면 중복 제거 및 압축 확인란을 선택합니다.
vSAN이 온디스크 형식을 자동으로 업그레이드하고, 이로 인해 클러스터에 있는 모든 디스크 그룹에 대해 롤링 다시 포맷이 수행됩니다.
- 5 (선택 사항) 클러스터에서 암호화를 사용하도록 설정하려면 암호화 확인란을 선택합니다.
vSAN이 온디스크 형식을 자동으로 업그레이드하고, 이로 인해 클러스터에 있는 모든 디스크 그룹에 대해 롤링 다시 포맷이 수행됩니다.
- 6 **확인**을 클릭합니다.

후속 작업

스토리지 디바이스를 할당하거나 디스크 그룹을 생성합니다. [10장, “vSAN 클러스터에서 디바이스 관리,”](#) (99 페이지)를 참조하십시오.

vSAN 사용 안 함

호스트 클러스터에 대해 vSAN을 해제할 수 있습니다.

vSAN 클러스터를 사용하지 않도록 설정하면 공유 vSAN 데이터스토어에 있는 모든 가상 시스템에 액세스할 수 없게 됩니다. vSAN이 사용되지 않도록 설정되어 있는 동안 가상 시스템을 사용하려면 vSAN 데이터스토어에서 다른 데이터스토어로 가상 시스템을 마이그레이션한 후에 vSAN 클러스터를 사용하지 않도록 설정해야 합니다.

필수 조건

호스트가 유지 보수 모드에 있는지 확인합니다.

프로시저

- 1 vSphere Web Client에서 호스트 클러스터로 이동합니다.

- 2 구성 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택하고 **편집**을 클릭하여 vSAN 설정을 편집합니다.
- 4 vSAN **설정** 확인란을 선택 취소합니다.

vSAN 클러스터에 대한 라이선스 설정 구성

평가 기간이 만료되거나 현재 할당된 라이선스가 만료되기 전에 vSAN 클러스터에 라이선스를 할당해야 합니다.

vSAN 라이선스를 업그레이드, 결합 또는 분할하는 경우에는 vSAN 클러스터에 새 라이선스를 할당해야 합니다. vSAN 라이선스를 클러스터에 할당하는 경우 사용되는 라이선스 용량은 클러스터에 참여하는 호스트의 총 CPU 수와 같습니다. vSAN 클러스터의 라이선스 사용은 클러스터에서 호스트를 추가하거나 제거할 때마다 다시 계산하여 업데이트됩니다. 라이선스 관리와 라이선싱 용어 및 정의에 대해서는 vCenter Server 및 호스트 관리 설명서를 참조하십시오.

클러스터에 vSAN을 사용하도록 설정할 경우 vSAN을 평가 모드에서 사용하여 해당 기능을 살펴볼 수 있습니다. 평가 기간은 vSAN을 사용하도록 설정할 때 시작되며 60일 후에 만료됩니다. vSAN을 사용하려면 평가 기간이 만료되기 전에 클러스터에 라이선스를 부여해야 합니다. vSphere 라이선스와 마찬가지로 vSAN 라이선스에도 CPU당 용량이 있습니다. 플래시 전용 구성과 확장된 클러스터 같은 일부 고급 기능을 사용하려면 해당 기능을 지원하는 라이선스가 필요합니다.

필수 조건

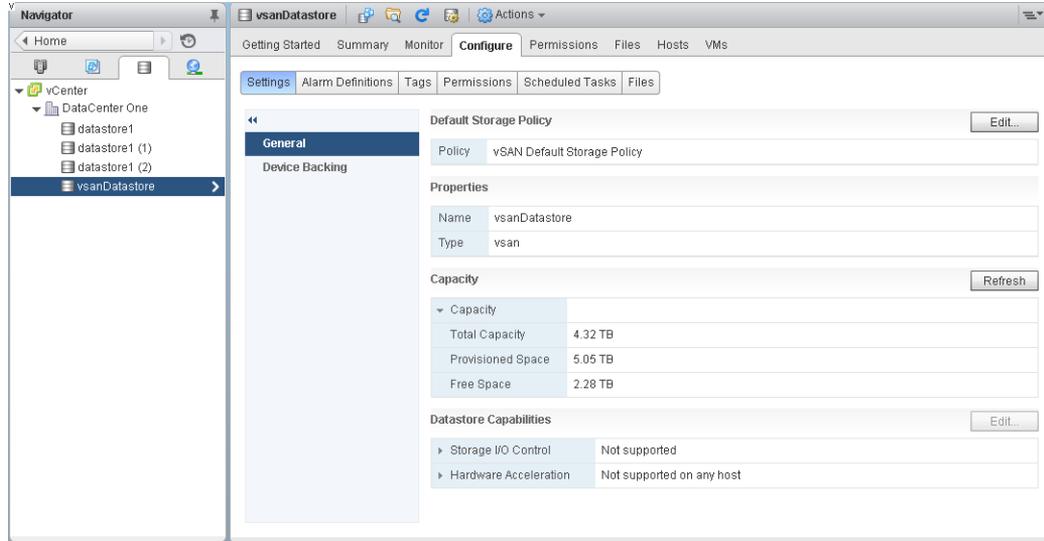
- vSAN 라이선스를 보고 관리하려면 vSphere Web Client가 실행되는 vCenter Server 시스템에 대한 **글로벌.라이선스** 권한이 있어야 합니다.

프로시저

- 1 vSphere Web Client에서, vSAN을 사용하도록 설정한 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 **구성**에서 **라이선싱**을 선택하고 **라이선스 할당**을 클릭합니다.
- 4 라이선싱 옵션을 선택합니다.
 - 기존 라이선스를 선택하고 **확인**을 클릭합니다.
 - vSAN 라이선스를 생성합니다.
 - a **새 라이선스 생성 (+)** 아이콘을 클릭합니다.
 - b [새 라이선스] 대화상자에서 vSAN 라이선스 키를 입력하거나 복사하여 붙여넣고 **다음**을 클릭합니다.
 - c 라이선스 이름 편집 페이지에서 새 라이선스의 이름을 적절히 변경하고 **다음**을 클릭합니다.
 - d **마침**을 클릭합니다.
 - e 라이선스 할당 대화상자에서 새로 생성된 라이선스를 선택하고 **확인**을 클릭합니다.

vSAN 데이터스토어 보기

vSAN을 사용하도록 설정하면 단일 데이터스토어가 생성됩니다. vSAN 데이터스토어의 용량을 검토할 수 있습니다.



필수 조건

vSAN을 활성화하고 디스크 그룹을 구성합니다.

프로시저

- 1 vSphere Web Client에서 스토리지로 이동합니다.
- 2 vSAN 데이터스토어를 선택합니다.
- 3 **구성** 탭을 클릭합니다.
- 4 vSAN 데이터스토어 용량을 검토합니다.

vSAN 데이터스토어의 크기는 ESXi 호스트당 용량 디바이스의 수와 클러스터에 있는 ESXi 호스트의 수에 따라 다릅니다. 예를 들어 호스트에 용량 디바이스를 위한 7개의 2TB가 있고 클러스터에 8개의 호스트가 포함되어 있는 경우 대략적인 스토리지 용량은 $7 \times 2\text{TB} \times 8 = 112\text{TB}$ 입니다. 플래시 전용 구성을 사용할 경우 플래시 디바이스가 용량에 사용됩니다. 하이브리드 구성의 경우 자기 디스크가 용량에 사용됩니다.

일부 용량은 메타데이터에 할당됩니다.

- 온디스크 형식 버전 1.0에서는 용량 디바이스당 약 1GB를 추가합니다.
- 온디스크 형식 버전 2.0에서는 용량 오버헤드를 추가하며, 일반적으로 디바이스당 용량의 1-2%를 초과하지 않습니다.
- 온디스크 형식 버전 3.0 이상에서는 용량 오버헤드를 추가하며, 일반적으로 디바이스당 용량의 1-2%를 초과하지 않습니다. 소프트웨어 체크섬을 사용하도록 설정된 중복 제거 및 압축 기능을 사용하려면 디바이스당 용량의 6.2% 정도에 해당하는 추가적인 오버헤드가 필요합니다.

후속 작업

vSAN 데이터스토어의 스토리지 기능을 사용하여 가상 시스템에 대한 스토리지 정책을 생성합니다. 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.

vSAN 및 vSphere HA 사용

동일한 클러스터에서 vSphere HA 및 vSAN을 사용하도록 설정할 수 있습니다. 기존 데이터스토어와 마찬가지로 vSphere HA는 vSAN 데이터스토어의 가상 시스템에 대해 동일한 수준의 보호를 제공합니다. 이 보호 수준은 vSphere HA와 vSAN이 상호 작용할 때 특정 제한 사항을 적용합니다.

ESXi 호스트 요구 사항

다음 조건을 충족해야만 vSAN을 vSphere HA 클러스터와 함께 사용할 수 있습니다.

- 클러스터의 ESXi 호스트가 모두 버전 5.5 업데이트 1 이상이어야 합니다.
- 클러스터에 3개 이상의 ESXi 호스트가 있어야 합니다. 최상의 결과를 위해서는 4개 이상의 호스트로 vSAN 클러스터를 구성합니다.

네트워킹 차이점

vSAN은 자체 논리적 네트워크를 사용합니다. vSAN 및 vSphere HA가 동일한 클러스터에 대해 사용되도록 설정된 경우 HA 에이전트 간 트래픽은 관리 네트워크가 아니라 이 스토리지 네트워크를 통해 전송됩니다. vSphere HA는 vSAN이 사용되지 않도록 설정된 경우에만 관리 네트워크를 사용합니다. vCenter Server는 호스트에서 vSphere HA가 구성된 경우 적절한 네트워크를 선택합니다.

참고 클러스터에서 vSAN 을 사용하도록 설정하기 전에 먼저 vSphere HA 를 사용하지 않도록 설정해야 합니다. 그런 후 vSphere HA를 다시 사용하도록 설정할 수 있습니다.

모든 네트워크 파티션에서 가상 시스템에 부분적으로만 액세스할 수 있는 경우, 모든 파티션에서 가상 시스템 전원을 켜거나 완전히 액세스할 수 없습니다. 예를 들어 클러스터를 P1 및 P2로 분할한 경우 P1 파티션은 VM 네임스페이스 개체에 액세스할 수 있지만 P2는 액세스할 수 없습니다. P2 파티션은 VMDK에 액세스할 수 있지만 P1은 액세스할 수 없습니다. 이러한 경우 가상 시스템의 전원을 켤 수 없고 모든 파티션에서 완전히 액세스할 수 없습니다.

다음 표에서는 vSAN을 사용할 때와 사용하지 않을 때 vSphere HA 네트워킹의 차이점을 보여 줍니다.

표 5-2. vSphere HA 네트워킹 차이점

| | vSAN 사용 | vSAN 사용 안 함 |
|------------------------|---|--------------------------------------|
| vSphere HA에서 사용하는 네트워크 | vSAN 스토리지 네트워크 | 관리 네트워크 |
| 하트비트 데이터스토어 | vSAN 데이터스토어가 아닌, 둘 이상의 호스트에 마운트된 모든 데이터스토어 | 둘 이상의 호스트에 마운트된 모든 데이터스토어 |
| 호스트가 분리된 것으로 선언됨 | 분리 주소를 ping할 수 없고 vSAN 스토리지 네트워크에 액세스할 수 없음 | 분리 주소를 ping할 수 없고 관리 네트워크에 액세스할 수 없음 |

vSAN 네트워크 구성을 변경하는 경우 vSphere HA 에이전트는 자동으로 새 네트워크 설정을 가져오지 않습니다. vSAN 네트워크를 변경하려면 vSphere Web Client를 사용하여 vSphere HA 클러스터에 대한 호스트 모니터링을 다시 사용하도록 설정해야 합니다.

- 1 vSphere HA 클러스터에 대한 호스트 모니터링을 사용하지 않도록 설정합니다.
- 2 vSAN 네트워크를 변경합니다.
- 3 클러스터의 모든 호스트를 마우스 오른쪽 버튼으로 클릭하고 **HA 재구성**을 선택합니다.
- 4 vSphere HA 클러스터에 대한 호스트 모니터링을 다시 사용하도록 설정합니다.

용량 예약 설정

승인 제어 정책으로 vSphere HA 클러스터에 대한 용량을 예약하는 경우 이 설정은 vSAN 규칙 집합의 해당 **허용할 수 있는 장애의 기본 수준** 정책 설정에 따라 조정되어야 하며 vSphere HA 승인 제어 설정으로 예약된 용량보다 적으면 안 됩니다. 예를 들어 vSAN 규칙 집합이 두 번의 장애만 허용할 경우 vSphere HA 승인 제어 정책은 한두 번의 호스트 장애에만 해당하는 용량을 예약해야 합니다. 8개의 호스트로 구성된 클러스터에 대해 예약된 클러스터 리소스 비율 정책을 사용하는 경우 25%가 넘는 클러스터 리소스를 예약할 수 없습니다. 동일한 클러스터에서 **허용할 수 있는 장애의 기본 수준** 정책을 사용하는 경우 호스트를 2개보다 많이 설정하면 안 됩니다. vSphere HA가 더 적은 용량을 예약하는 경우 예기치 않은 페일오버 작업이 발생할 수 있습니다. 너무 많은 용량을 예약하면 가상 시스템 전원 켜기 및 클러스터 간 vSphere vMotion 마이그레이션이 크게 제약될 수 있습니다. 예약된 클러스터 리소스 비율 정책에 대한 자세한 내용은 vSphere 가용성 설명서를 참조하십시오.

여러 호스트에서 장애가 발생한 경우 vSAN 및 vSphere HA의 동작

vSAN 클러스터에서 오류가 발생하여 가상 시스템 개체의 페일오버 쿼럼이 손실된 경우 클러스터 쿼럼이 복원되어도 vSphere HA가 가상 시스템을 다시 시작하지 못할 수 있습니다. vSphere HA는 클러스터 쿼럼이 있고 가상 시스템 개체의 최신 사본에 액세스할 수 있는 경우에만 다시 시작하도록 보장합니다. 최신 사본은 마지막으로 기록한 사본입니다.

vSAN 가상 시스템이 호스트 장애를 한 번 허용하도록 프로비저닝된 경우를 예로 들어 보겠습니다. 가상 시스템은 호스트가 세 개(H1, H2, H3) 포함된 vSAN 클러스터에서 실행됩니다. 세 호스트에서 모두 장애가 차례로 발생하고 H3 호스트에서 장애가 마지막으로 발생합니다.

H1과 H2가 복구되면 클러스터에는 호스트 장애가 한 번 허용되는 쿼럼이 포함됩니다. 이 쿼럼에도 불구하고, 가상 시스템 개체의 최신 사본은 마지막으로 장애가 발생한 호스트(H3)에 포함되어 있고 H3 호스트에는 아직 액세스할 수 없기 때문에 vSphere HA는 가상 시스템을 다시 시작하지 못합니다.

이 예에서는 세 호스트가 모두 동시에 복구되거나, 두 호스트 쿼럼에 H3이 포함되어 있어야 합니다. 이 두 조건이 모두 충족되지 않을 경우 HA는 H3 호스트가 온라인 상태로 돌아온 후에야 가상 시스템을 다시 시작합니다.

vCenter Server Appliance와 함께 vSAN 배포

vCenter Server Appliance를 배포할 때 vSAN 클러스터를 생성하여 해당 클러스터에서 장치를 호스팅할 수 있습니다.

vCenter Server Appliance는 미리 구성된 Linux 가상 시스템으로, Linux 시스템에서 VMware vCenter Server를 실행하기 위해 사용됩니다. 이 기능을 사용하면 vCenter Server를 사용하지 않고도 vSAN 클러스터를 새로운 ESXi 호스트에 구성할 수 있습니다.

vCenter Server Appliance 설치 관리자를 사용하여 vCenter Server Appliance를 배포할 때 단일 호스트 vSAN 클러스터를 생성한 후 이 클러스터에서 vCenter Server Appliance를 호스팅할 수 있습니다. 배포의 1단계 중에 데이터스토어를 선택할 때 **대상 호스트가 포함된 새 vSAN 클러스터에 설치**를 클릭합니다. 설치 관리자 마법사의 단계에 따라 배포를 완료합니다.

vCenter Server Appliance 설치 관리자는 호스트에서 할당된 디스크와 함께 단일 호스트 vSAN 클러스터를 생성합니다. vCenter Server Appliance가 vSAN 클러스터에 배포됩니다.

배포를 완료한 후에는 vCenter Server Appliance를 사용하여 단일 호스트 vSAN 클러스터를 관리할 수 있습니다. vSAN 클러스터의 구성을 완료해야 합니다.

Platform Services Controller와 vCenter Server를 동일한 vSAN 클러스터에 배포하거나 별개의 클러스터에 배포할 수 있습니다.

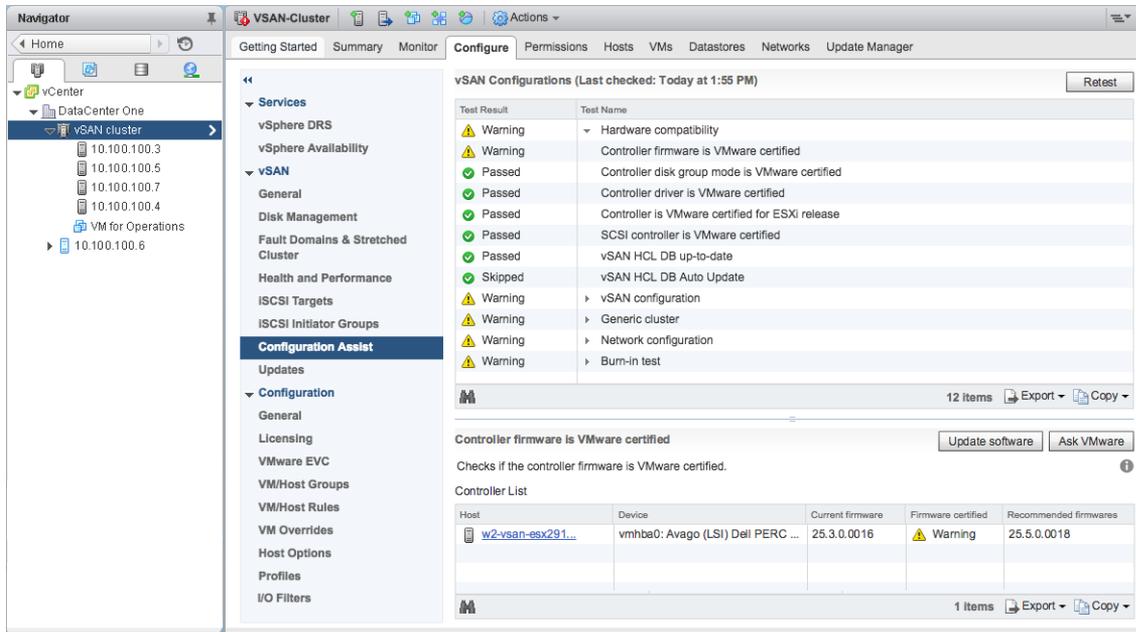
- Platform Services Controller와 vCenter Server를 동일한 vSAN 클러스터에 배포할 수 있습니다. PSC와 vCenter Server를 동일한 단일 호스트 vSAN 데이터스토어에 배포합니다. 배포를 완료하면 Platform Services Controller와 vCenter Server 둘 모두 동일한 클러스터에서 실행됩니다.

- Platform Services Controller와 vCenter Server를 서로 다른 vSAN 클러스터에 배포할 수 있습니다. Platform Services Controller와 vCenter Server를 서로 다른 단일 호스트 vSAN 클러스터에 배포합니다. 배포를 완료한 후에는 각 vSAN 클러스터의 구성을 개별적으로 완료해야 합니다.

vSAN 구성 지원 및 업데이트 사용

구성 지원을 사용하면 vSAN 클러스터의 구성을 확인하고 문제를 해결할 수 있습니다.

vSAN 구성 지원을 사용하면 클러스터 구성 요소의 구성을 확인하고, 문제를 진단 및 해결할 수 있습니다. 구성 점검 대상에는 하드웨어 호환성, 네트워크 및 vSAN 구성 옵션이 포함됩니다.



구성 지원 점검은 범주로 분류되며 각 범주에는 개별 구성 점검이 포함됩니다.

표 5-3. 구성 지원 범주

| 구성 범주 | 설명 |
|----------|--|
| 하드웨어 호환성 | vSAN 클러스터의 하드웨어 구성 요소가 지원되는 하드웨어, 소프트웨어 및 드라이버를 사용하는지 확인합니다. |
| vSAN 구성 | vSAN 구성 옵션을 확인합니다. |
| 일반 클러스터 | 기본 클러스터 구성 옵션을 확인합니다. |
| 네트워크 구성 | vSAN 네트워크 구성을 확인합니다. |
| 변인 테스트 | 변인 테스트 작업을 확인합니다. |

스토리지 컨트롤러 펌웨어 또는 드라이버가 VMware 호환성 가이드에 나열된 요구 사항을 충족하지 않을 경우에는 [업데이트] 페이지를 사용하여 컨트롤러를 업데이트할 수 있습니다.

vSAN 구성 점검

vSAN 클러스터의 구성 상태를 보고, 클러스터의 작업에 영향을 주는 문제를 해결할 수 있습니다.

프로시저

- vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 구성 탭을 클릭합니다.

- 3 **vSAN**에서 **구성 지원**을 클릭하고 vSAN 구성 범주를 검토합니다.
[테스트 결과] 옆에 주의 아이콘이 표시되면 해당 범주를 확장하여 개별 구성 점검의 결과를 검토합니다.
- 4 개별 구성 점검을 선택하고 페이지 맨 아래에서 세부 정보를 검토합니다.
VMware에 문의 버튼을 클릭하면 점검에 대해 설명하고 문제 해결 방법에 대한 정보를 제공하는 기술 자료 문서를 열 수 있습니다.
일부 구성 점검에는 구성을 완료하는 데 도움을 줄 수 있는 추가적인 버튼이 제공됩니다.

vSAN 에 대한 Distributed Switch 구성

[vSAN용 새 Distributed Switch 구성] 마법사를 사용하면 vSAN 트래픽을 지원할 vSphere Distributed Switch를 구성할 수 있습니다.

vSAN 트래픽을 지원할 vSphere Distributed Switch가 클러스터에 구성되어 있지 않으면 [구성 지원] 페이지에서 **네트워크 구성 > vSAN에 vDS 사용**에 대해 주의가 생성됩니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN 아래에서 **구성 지원**을 선택하고 **네트워크 구성** 범주를 클릭하여 확장합니다.
- 4 **vSAN용 vDS 사용**을 클릭합니다. 페이지 하단에서 **vDS 생성**을 클릭합니다.
- 5 [이름 및 유형]에 새 Distributed Switch의 이름을 입력하고, 새 스위치를 생성할지 아니면 기존 표준 스위치를 마이그레이션할지 선택합니다.
- 6 새 Distributed Switch로 마이그레이션할 사용되지 않은 어댑터를 선택하고 **다음**을 클릭합니다.
- 7 (선택 사항) [인프라 VM 마이그레이션]에서 기존 표준 스위치에 대해 마이그레이션 중에 인프라 VM으로 처리할 VM을 선택하고 **다음**을 클릭합니다.
새 Distributed Switch를 생성하는 경우에는 이 단계가 필요하지 않습니다.
- 8 [완료 준비]에서 구성을 검토하고 **마침**을 클릭합니다.

vSAN 에 대한 VMkernel 네트워크 어댑터 생성

[vSAN용 새 VMkernel 네트워크 어댑터] 마법사를 사용하여 vSAN 트래픽을 지원할 vmknic를 구성할 수 있습니다.

vSAN 트래픽을 지원할 vmknic가 클러스터의 ESXi 호스트에 구성되어 있지 않으면 [구성 지원] 페이지에서 **네트워크 구성 > 모든 호스트에 구성된 vSAN vmknic가 있음**에 대해 주의가 생성됩니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN 아래에서 **구성 지원**을 선택하고 **네트워크 구성** 범주를 클릭하여 확장합니다.
- 4 **모든 호스트에 구성된 vSAN vmknic가 있음**을 클릭합니다. 페이지 하단에서 **VMkernel 네트워크 어댑터 생성**을 클릭합니다.
- 5 [호스트 선택]에서 vSAN용 vmknic가 구성되어 있지 않은 각 호스트의 확인란을 선택하고 **다음**을 클릭합니다.
vSAN vmknic가 없는 호스트가 [구성 지원] 페이지에 나열됩니다.

- 6 [위치 및 서비스]에서 Distributed Switch를 선택하고 **vSAN 트래픽** 확인란을 선택합니다. **다음**을 클릭합니다.
- 7 [vSAN 어댑터 설정]에서 포트 그룹, IP 설정 및 구성을 선택하고 **다음**을 클릭합니다.
- 8 [완료 준비]에서 구성을 검토하고 **마침**을 클릭합니다.

드라이버 및 펌웨어 업데이트를 위한 컨트롤러 관리 도구 설치

스토리지 컨트롤러 벤더는 vSAN이 컨트롤러 드라이버 및 펌웨어를 업데이트하는 데 사용할 수 있는 소프트웨어 관리 도구를 제공합니다. 이러한 관리 도구가 ESXi 호스트에 없으면 해당 도구를 다운로드할 수 있습니다.

업데이트 페이지에서는 일부 벤더의 특정 스토리지 컨트롤러 모델만 지원합니다.

필수 조건

- 구성 지원 페이지에서 하드웨어 호환성을 확인합니다.
- 소프트웨어를 업데이트하는 동안 VM을 계속 실행해야 하면 DRS를 사용하도록 설정해야 합니다.

프로시저

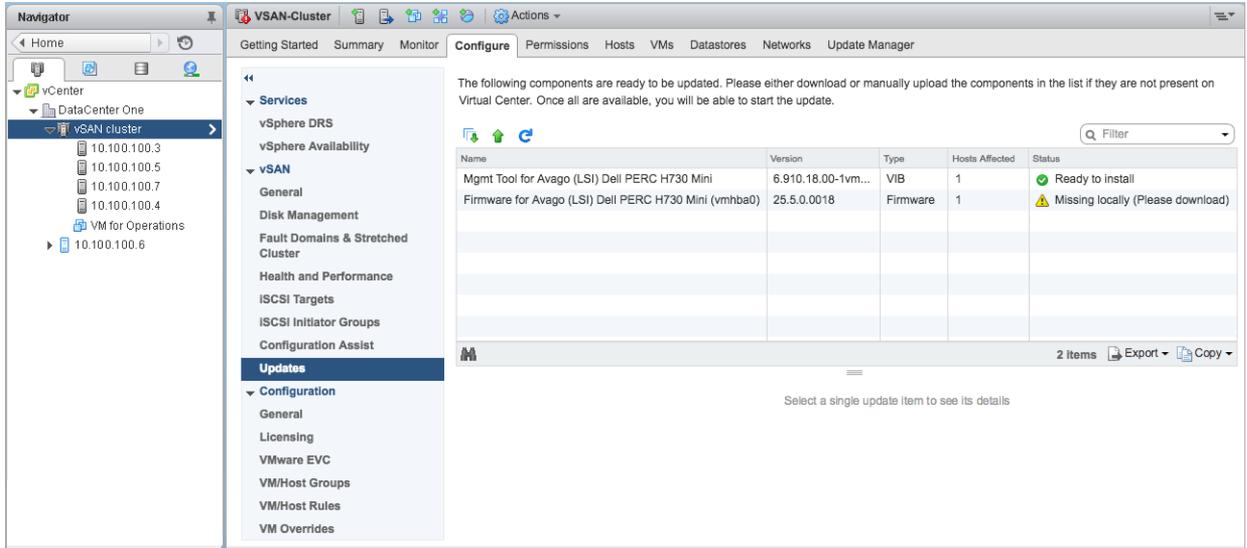
- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **업데이트**를 클릭한 후 누락되거나 설치 준비가 된 구성 요소를 검토합니다.
- 4 컨트롤러의 관리(Mgmt) 도구를 선택하고 **다운로드** 아이콘을 클릭합니다.
관리 도구가 인터넷에서 사용자의 vCenter Server에 다운로드됩니다.
- 5 클러스터의 ESXi 호스트에 관리 도구를 설치하려면 **모두 업데이트** 아이콘을 클릭합니다.
모든 호스트를 동시에 업데이트할지 롤링 업데이트를 사용할지 확인합니다.
- 6 **새로 고침** 아이콘을 클릭합니다.
업데이트가 필요한 컨트롤러 구성 요소가 [업데이트] 페이지에 표시됩니다.

후속 작업

스토리지 컨트롤러 관리 도구를 사용할 수 있으면 누락된 드라이버나 펌웨어 모두 [업데이트] 페이지에 나열됩니다. 이러한 누락된 구성 요소를 업데이트할 수 있습니다.

스토리지 컨트롤러 드라이버 및 펌웨어 업데이트

vSAN을 사용하여 스토리지 컨트롤러의 오래되거나 잘못된 드라이버와 펌웨어를 업데이트할 수 있습니다.



구성 지원은 VMware 호환성 가이드에 따라 스토리지 컨트롤러가 최신 드라이버 및 펌웨어 버전을 사용하는지 확인합니다. 컨트롤러 드라이버나 펌웨어가 요구 사항을 충족하지 못할 경우, [업데이트] 페이지를 사용하여 드라이버 및 펌웨어 업데이트를 수행하십시오.

필수 조건

스토리지 디바이스의 컨트롤러 관리 도구가 ESXi 호스트에 있어야 합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **업데이트**를 클릭한 후 누락되거나 설치 준비가 된 구성 요소를 검토합니다.
[업데이트] 페이지에는 누락된 펌웨어 및 드라이버 구성 요소가 나열됩니다.

참고 컨트롤러 관리(Mgmt) 도구를 사용할 수 없으면 관리 도구를 다운로드하고 설치하라는 메시지가 표시됩니다. 관리 도구를 사용할 수 있으면 누락된 드라이버나 펌웨어가 모두 나열됩니다.

- 4 업데이트할 구성 요소를 선택하고 **업데이트** 아이콘을 클릭하여 클러스터의 ESXi 호스트에서 구성 요소를 업데이트합니다. 또는 **모두 업데이트** 아이콘을 클릭하여 누락된 모든 구성 요소를 업데이트할 수 있습니다.

모든 호스트를 동시에 업데이트할지 롤링 업데이트를 사용할지 확인합니다.

참고 일부 관리 도구와 드라이버에 대해서는 업데이트 프로세스가 유지 보수 모드를 생략하고 설치 결과에 기반하여 재부팅을 수행합니다. 이러한 경우에는 **MM 필요** 및 **재부팅 필요** 필드가 비어 있습니다.

- 5 **새로 고침** 아이콘을 클릭합니다.
업데이트된 구성 요소가 화면에 더 이상 표시되지 않습니다.

확장된 클러스터를 통해 2개의 사이트에 걸쳐 데이터스토어 확장

6

2개의 지리적 위치(또는 사이트)에 걸쳐 있는 확장된 클러스터를 생성할 수 있습니다. 확장된 클러스터를 사용하면 2개의 사이트에 걸쳐 vSAN 데이터스토어를 확장하여 확장된 스토리지로 사용할 수 있습니다. 한 사이트에서 장애 또는 예약된 유지 보수가 발생하는 경우 확장된 클러스터가 계속해서 작동합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “확장된 클러스터 소개,” (59 페이지)
- “확장된 클러스터 설계 고려 사항,” (61 페이지)
- “확장된 클러스터 사용의 모범 사례,” (62 페이지)
- “확장된 클러스터에 대한 네트워크 설계,” (62 페이지)
- “vSAN 확장된 클러스터 구성,” (63 페이지)
- “기본 장애 도메인 변경,” (64 페이지)
- “감시 호스트 변경,” (64 페이지)
- “vSAN 감시 장치 배포,” (64 페이지)
- “감시 트래픽에 대한 네트워크 인터페이스 구성,” (65 페이지)
- “확장된 클러스터를 표준 vSAN 클러스터로 변환,” (67 페이지)

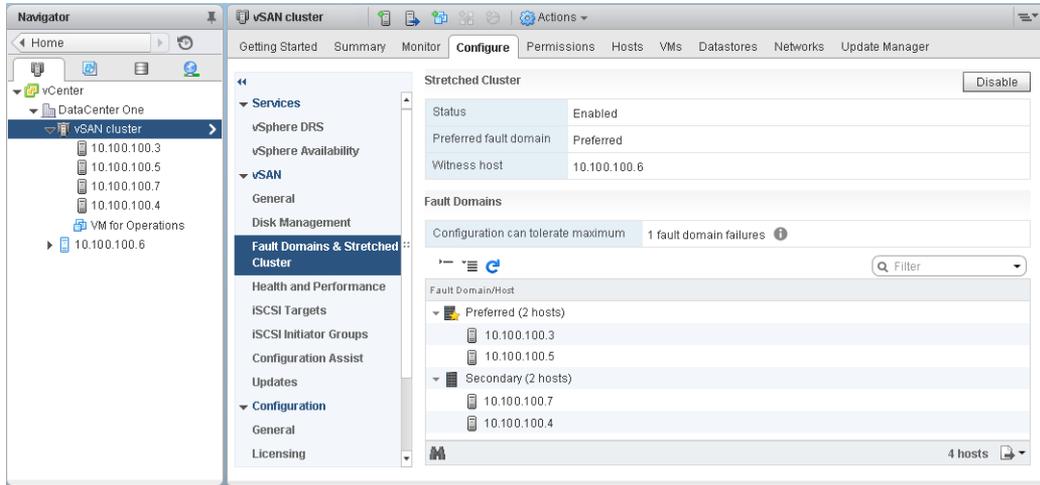
확장된 클러스터 소개

확장된 클러스터는 더 높은 수준의 가용성과 사이트 간 로드 밸런싱을 위해 vSAN 클러스터를 단일 사이트에서 2개의 사이트로 확장합니다. 확장된 클러스터는 대도시나 캠퍼스 환경과 같이 데이터 센터 사이의 거리가 제한된 환경에 주로 배포됩니다.

확장된 클러스터를 사용하면 한 사이트의 유지 보수 또는 손실이 클러스터의 전반적인 운영에 영향을 주지 않기 때문에 계획된 유지 보수를 관리하고 재해 시나리오를 방지할 수 있습니다. 확장된 클러스터 구성에서는 두 사이트 모두 활성 사이트입니다. 두 사이트 중 하나에서 장애가 발생하면 vSAN은 다른 사이트의 스토리지를 사용합니다. vSphere HA는 재시작해야 하는 모든 VM을 나머지 활성 사이트에서 재시작합니다.

사이트 하나를 기본 사이트로 지정해야 합니다. 다른 사이트는 보조 또는 비기본 사이트로 지정됩니다. 활성 사이트 두 개 사이에 네트워크 연결이 끊어지면 시스템에서 기본 사이트만 사용하기 때문에 기본 사이트로 지정된 사이트가 작동 상태로 남아 있습니다.

vSAN 확장된 클러스터는 데이터 가용성에 영향을 주지 않으면서 한 번에 하나의 연결 장애를 허용할 수 있습니다. 연결 장애는 두 사이트 사이 또는 사이트와 감시 호스트 사이의 네트워크 연결이 끊어지는 것입니다. 사이트 장애가 발생하거나 네트워크 연결이 끊어지면 vSAN은 정상적으로 작동 가능한 사이트로 자동 전환됩니다.



확장된 클러스터 사용에 대한 자세한 내용은 vSAN 확장된 클러스터 가이드를 참조하십시오.

감시 호스트

각 확장된 클러스터는 사이트 2개와 감시 호스트 1개로 구성됩니다. 감시 호스트는 세 번째 사이트에 있으며 가상 시스템 개체의 감시 구성 요소를 포함합니다. 감시 호스트는 메타데이터만 포함하며 스토리지 작업에는 참여하지 않습니다.

감시 호스트는 두 사이트 사이의 네트워크 연결이 끊어진 경우 데이터스토어 구성 요소의 가용성과 관련하여 결정을 내려야 할 때 타이브레이커 역할을 합니다. 이 경우 감시 호스트는 일반적으로 기본 사이트를 사용하여 vSAN 클러스터를 구성합니다. 그러나 기본 사이트가 보조 사이트 및 감시 호스트로부터 분리되면 감시 호스트는 보조 사이트를 사용하여 클러스터를 구성합니다. 기본 사이트가 다시 온라인 상태가 되면 양쪽 사이트가 모든 데이터의 최신 복사본을 보유할 수 있도록 데이터가 다시 동기화됩니다.

감시 호스트가 실패하면 해당하는 모든 개체는 비준수 상태가 되지만 완전하게 액세스 가능합니다.

감시 호스트의 특징은 다음과 같습니다.

- 감시 호스트는 느린 대역폭/높은 지연 시간 링크를 사용합니다.
- 감시 호스트는 VM을 실행할 수 없습니다.
- 단일 감시 호스트는 vSAN 확장된 클러스터를 하나만 지원할 수 있습니다.
- 감시 호스트에는 vSAN 트래픽을 사용하도록 설정한 VMkernel 어댑터가 하나 있어야 하며, 클러스터 내의 모든 호스트에 연결되어야 합니다. 감시 호스트는 관리에 VMkernel 어댑터 1개를 사용하고 vSAN 데이터 트래픽에 VMkernel 어댑터 1개를 사용합니다. 감시 호스트에는 vSAN 전용 VMkernel 어댑터가 1개만 있을 수 있습니다.
- 감시 호스트는 확장된 클러스터 전용의 독립형 호스트여야 하며, vCenter Server를 통해 인벤토리로 이동하거나 다른 클러스터에 추가할 수 없습니다.

감시 호스트는 물리적 호스트이거나 VM 내에서 실행되는 ESXi 호스트일 수 있습니다. VM 감시 호스트는 VM 실행 또는 저장 같은 다른 유형의 기능은 제공하지 않습니다. 물리적 서버 하나에 여러 개의 감시 호스트가 VM으로 실행될 수 있습니다. 패치 적용 및 기본적인 네트워킹과 모니터링 구성 측면에서 VM 감시 호스트는 일반적인 ESXi 호스트와 동일한 방식으로 작동합니다. vCenter Server를 사용하여 관리하고, esxcli 또는 vSphere Update Manager를 사용하여 업데이트할 수 있으며, ESXi 호스트와 상호 작용하는 표준 도구를 사용하여 모니터링할 수 있습니다.

감시 가상 장치를 확장된 클러스터의 감시 호스트로 사용할 수 있습니다. 감시 가상 장치는 VM에 포함된 ESXi 호스트이며 OVF 또는 OVA로 패키징됩니다. 장치는 배포의 크기에 따라 여러 가지 옵션으로 사용할 수 있습니다.

확장된 클러스터 및 장애 도메인 비교

확장된 클러스터는 두 개의 지리적 위치에 있는 데이터 센터 간에 이중화 및 장애 보호 기능을 제공합니다. 장애 도메인은 같은 사이트 내의 랙 수준 장애에 대한 보호 기능을 제공합니다. 확장된 클러스터에 있는 각 사이트는 별도의 장애 도메인에 위치합니다.

확장된 클러스터에는 세 개의 장애 도메인(기본 사이트, 보조 사이트 및 감시 호스트)이 필요합니다.

vSAN 6.6 이상 릴리스에서는 확장된 클러스터에서 가상 시스템 개체에 대해 추가적인 수준의 로컬 장애 보호 기능을 제공할 수 있습니다. 각 사이트에 호스트가 4개 이상 있는 확장된 클러스터를 구성할 때는 클러스터의 개체에 대해 다음과 같은 정책 규칙을 사용할 수 있습니다.

- **PFTT(허용할 수 있는 장애의 기본 수준).** 이 규칙은 두 사이트 전체에서 가상 시스템 개체가 허용할 수 있는 호스트 및 디바이스 장애 수를 정의합니다. 기본값은 1이고 최대값은 3입니다.
- **허용할 수 있는 장애의 보조 수준.** 단일 사이트 내에서 가상 시스템 개체가 허용할 수 있는 호스트 및 개체 장애 수를 정의합니다. 기본값은 0이고 최대값은 3입니다.
- **선호도.** 이 규칙은 **허용할 수 있는 장애의 기본 수준**이 0으로 설정된 경우에만 사용할 수 있습니다. 선호도 규칙은 [없음], [기본] 또는 [보조]로 설정할 수 있습니다. 이 규칙을 사용하면 가상 시스템 개체를 확장된 클러스터에 있는 선택된 사이트로 제한할 수 있습니다. 기본값은 [없음]입니다.

참고 확장된 클러스터에 대해 **허용할 수 있는 장애의 보조 수준**을 구성할 때는 **장애 허용 방법** 규칙이 **허용할 수 있는 장애의 보조 수준**에 적용됩니다. **PFTT(허용할 수 있는 장애의 기본 수준)**에 사용되는 장애 허용 방법의 기본값은 RAID 1입니다.

로컬 장애 보호 기능이 있는 확장된 클러스터에서는 사이트 하나를 사용할 수 없는 경우에도 클러스터가 누락되거나 연결이 끊어진 구성 요소를 사용 가능한 사이트에서 복원할 수 있습니다.

확장된 클러스터 설계 고려 사항

vSAN 확장된 클러스터를 사용하는 경우에는 다음과 같은 지침을 고려합니다.

- 확장된 클러스터의 DRS 설정을 구성합니다.
 - 클러스터에서 DRS를 사용하도록 설정해야 합니다. DRS를 반자동 모드로 설정하면 각 사이트에 마이그레이션할 VM을 제어할 수 있습니다.
 - 기본 사이트와 보조 사이트에 대해 하나씩 사용하도록 호스트 그룹 두 개를 생성합니다.
 - 기본 사이트와 보조 사이트에 대해 하나씩 사용하도록 VM을 저장할 VM 그룹 두 개를 생성합니다.
 - VM-호스트 그룹을 매핑하는 VM-호스트 선호도 규칙 두 개를 생성하고, 기본 사이트에 있는 VM과 호스트 및 보조 사이트에 있는 VM과 호스트를 지정합니다.
 - 클러스터에서 VM 초기 배치를 수행하기 위한 VM-호스트 선호도 규칙을 구성합니다.
- 확장된 클러스터의 HA 설정을 구성합니다.
 - 클러스터에서 HA를 사용하도록 설정해야 합니다.
 - HA 규칙 설정은 페일오버 중에 VM-호스트 선호도 규칙을 따라야 합니다.
 - HA 데이터스토어 하트비트를 사용하지 않도록 설정합니다.
- 확장된 클러스터에는 온디스크 형식 2.0 이상이 필요합니다. 필요한 경우, 확장된 클러스터를 구성하기 전에 온디스크 형식을 업그레이드하십시오. [“vSphere Web Client를 사용하여 vSAN 디스크 형식 업그레이드,”](#) (93 페이지)를 참조하십시오.
- 확장된 클러스터에서 **허용할 수 있는 장애의 기본 수준**을 1로 설정합니다.
- vSAN 확장된 클러스터는 SMP-FT(Symmetric Multiprocessing Fault Tolerance)를 지원하지 않습니다.

- 호스트가 연결이 끊어지거나 응답하지 않을 경우 감시 호스트를 추가하거나 제거할 수 없습니다. 이와 같은 제한은 vSAN이 재구성 작업을 시작하기 전에 모든 호스트로부터 충분한 정보를 수집할 수 있도록 보장합니다.
- `esxcli`를 사용하여 호스트를 추가하거나 제거하는 기능은 확장된 클러스터에서 지원되지 않습니다.

확장된 클러스터 사용의 모범 사례

vSAN 확장된 클러스터를 사용할 경우 적절한 성능을 보장하려면 다음의 권장 사항을 따르십시오.

- 확장된 클러스터의 사이트(장애 도메인) 중 하나에 액세스할 수 없는 경우, 다른 두 사이트가 포함된 하위 클러스터에 새 VM을 프로비저닝할 수 있습니다. 이러한 새 VM은 명시적으로 강제 프로비저닝되며 분할된 사이트가 클러스터에 다시 가입될 때까지 비준수 상태로 유지됩니다. 이 명시적인 강제 프로비저닝은 사이트 세 개 중 두 개를 사용할 수 있을 때만 수행됩니다. 여기서 사이트는 데이터 사이트 또는 감시 호스트를 의미합니다.
- 정전 또는 네트워크 연결 끊김 때문에 전체 사이트가 오프라인 상태가 될 경우에는 지체 없이 사이트를 즉시 재시작합니다. vSAN 호스트를 하나씩 다시 시작하는 대신 모든 호스트가 10분 이내에 거의 동시에 온라인 상태가 되도록 해야 합니다. 이 프로세스를 따르면 사이트 간에 대량의 데이터를 동기화하는 것을 방지할 수 있습니다.
- 영구적으로 사용할 수 없는 호스트가 있는 경우, 재구성 작업을 수행하기 전에 해당 호스트를 클러스터에서 제거합니다.
- 여러 개의 확장된 클러스터를 지원하기 위해 VM 감시 호스트를 복제하려면 복제 전에 해당 VM을 감시 호스트로 구성하지 않습니다. 먼저 OVF에서 VM을 배포한 다음 VM을 복제하고, 각 복제본을 서로 다른 클러스터의 감시 호스트로 구성합니다. 또는 OVF에서 VM을 필요한 수만큼 배포한 후 각 VM을 서로 다른 클러스터의 감시 호스트로 구성합니다.

확장된 클러스터에 대한 네트워크 설계

확장된 클러스터의 3개 사이트 모두는 관리 네트워크와 vSAN 네트워크를 통해 통신합니다. 2개 데이터 사이트의 VM은 공통 가상 시스템 네트워크를 통해 통신합니다.

vSAN 확장된 클러스터는 특정 기본 네트워킹 요구 사항을 충족해야 합니다.

- 관리 네트워크에는 계층 2 확장된 네트워크 또는 계층 3 네트워크를 사용하여 3개 사이트 모두에 대한 연결이 필요합니다.
- vSAN 네트워크에는 3개 사이트 모두에 대한 연결이 필요합니다. 2개의 데이터 사이트 간에는 계층 2 확장된 네트워크를 사용하고 데이터 사이트와 감시 호스트 간에는 계층 3 네트워크를 사용하는 것이 좋습니다.
- VM 네트워크에는 데이터 사이트 간 연결이 필요하지만 감시 호스트와의 연결은 필요하지 않습니다. 데이터 사이트 간에는 계층 2 확장된 네트워크를 사용하는 것이 좋습니다. 실패가 발생하는 경우 원격 사이트에서 작업하기 위한 새 IP 주소가 VM에 필요하지 않습니다.
- vMotion 네트워크에는 데이터 사이트 간 연결이 필요하지만 감시 호스트와의 연결은 필요하지 않습니다. VMware는 데이터 사이트 간에 계층 2 확장된 네트워크 또는 계층 3 확장된 네트워크를 사용하도록 지원합니다.

ESXi 호스트에서 정적 라우팅 사용

ESXi 호스트에서 단일 기본 게이트웨이를 사용하는 경우 각 ESXi 호스트에 단일 기본 게이트웨이가 있는 기본 TCP/IP 스택이 포함되어야 합니다. 기본 라우팅은 일반적으로 관리 네트워크 TCP/IP 스택과 연결됩니다.

관리 네트워크 및 vSAN 네트워크가 서로 분리될 수 있습니다. 예를 들어 관리 네트워크는 물리적 NIC 0의 `vmk0`을 사용하는 반면 vSAN 네트워크는 물리적 NIC 1의 `vmk2`를 사용할 수 있습니다(2개의 구분된 TCP/IP 스택에 대한 개별 네트워크 어댑터). 이 구성은 vSAN 네트워크에 기본 게이트웨이가 없음을 의미합니다.

vSAN 네트워크가 계층 2 브로드캐스트 도메인(예: 172.10.0.0)에 있는 2개의 데이터 사이트에 걸쳐 확장되었고 감시 호스트가 다른 브로드캐스트 도메인(예: 172.30.0.0)에 있다고 가정합니다. 데이터 사이트의 VMkernel 어댑터가 감시 호스트의 vSAN 네트워크에 연결을 시도하는 경우 ESXi 호스트의 기본 게이트웨이가 관리 네트워크와 연결되어 있고 관리 네트워크에서 vSAN 네트워크로의 경로가 없으므로 연결이 실패합니다.

정적 라우팅을 사용하여 이 문제를 해결할 수 있습니다. 특정 네트워크에 연결하기 위해 따로 경로를 나타내는 새 라우팅 항목을 정의합니다. 확장된 클러스터의 vSAN 네트워크의 경우 정적 경로를 추가하여 모든 호스트에 걸쳐 올바르게 통신할 수 있습니다.

예를 들어 각 데이터 사이트의 호스트에 정적 라우팅을 추가하여 172.30.0.0 감시 네트워크 연결 요청이 172.10.0.0 인터페이스를 통해 라우팅되도록 할 수 있습니다. 또한 감시 호스트에 정적 라우팅을 추가하여 데이터 사이트에 대한 172.10.0.0 네트워크 연결 요청이 172.30.0.0 인터페이스를 통해 라우팅되도록 할 수 있습니다.

참고 정적 라우팅을 사용하는 경우 새 ESXi 호스트가 클러스터에서 통신할 수 있도록 하려면 사이트에 해당 호스트에 대한 정적 라우팅을 수동으로 추가해야 합니다. 감시 호스트를 교체하는 경우 정적 라우팅 구성을 업데이트해야 합니다.

esxcli network ip route 명령을 사용하여 정적 라우팅을 추가합니다.

vSAN 확장된 클러스터 구성

2개의 지리적 위치 또는 사이트에 걸쳐 확장되는 vSAN 클러스터를 구성합니다.

필수 조건

- 기본 사이트와 보조 사이트에 호스트가 하나씩 있고 감시 역할을 할 호스트 하나를 포함하여 호스트가 세 개 이상 있는지 확인합니다.
- 확장된 클러스터의 감시 호스트로 사용될 호스트 하나를 구성했는지 확인합니다. 감시 호스트가 vSAN 클러스터의 일부가 아니고 vSAN 데이터 트래픽에 대한 VMkernel 어댑터가 하나만 구성되었는지 확인합니다.
- 감시 호스트가 비어 있고 구성 요소를 포함하지 않는지 확인합니다. 기존 vSAN 호스트를 감시 호스트로 구성하려면 먼저 호스트에서 모든 데이터를 제거하고 디스크 그룹을 삭제합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 확장된 클러스터 **구성** 버튼을 클릭하여 확장된 클러스터 구성 마법사를 엽니다.
- 5 보조 사이트에 할당할 장애 도메인을 선택하고 >>를 클릭합니다.
기본 장애 도메인 아래에 나열된 호스트는 기본 사이트에 있습니다.
- 6 **다음**을 클릭합니다.
- 7 vSAN 확장된 클러스터의 멤버가 아닌 감시 호스트를 선택하고 **다음**을 클릭합니다.
- 8 감시 호스트에 스토리지 디바이스를 할당하고 **다음**을 클릭합니다.
감시 호스트에 스토리지 디바이스를 할당합니다. 캐시 계층용 플래시 디바이스 하나와 용량 계층용 디바이스 하나 이상을 선택합니다.
- 9 완료 준비 페이지에서 구성을 검토하고 **마침**을 클릭합니다.

기본 장애 도메인 변경

보조 사이트를 기본 사이트로 구성할 수 있습니다. 그러면 현재의 기본 사이트가 보조 사이트가 됩니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 보조 장애 도메인을 선택하고 **장애 도메인을 확장된 클러스터의 기본 장애 도메인으로 표시** 아이콘 (🏠)을 클릭합니다.
- 5 **예**를 클릭하여 확인합니다.
선택한 장애 도메인이 기본 장애 도메인으로 표시됩니다.

감시 호스트 변경

vSAN 확장된 클러스터의 감시 호스트를 변경할 수 있습니다.

vSAN 확장된 클러스터의 감시 호스트로 사용되는 ESXi 호스트를 변경합니다.

필수 조건

감시 호스트가 사용 중이 아닌지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 **감시 호스트 변경** 버튼을 클릭합니다.
- 5 감시 호스트로 사용할 새 호스트를 선택하고 **다음**을 클릭합니다.
- 6 새 감시 호스트에 디스크를 할당하고 **다음**을 클릭합니다.
- 7 [완료 준비] 페이지에서 구성을 검토하고 **마침**을 클릭합니다.

vSAN 감시 장치 배포

확장된 클러스터와 같은 특정 vSAN 구성에는 감시 호스트가 필요합니다. 전용 물리적 ESXi 호스트를 감시 호스트로 사용하는 대신 vSAN 감시 장치를 배포할 수 있습니다. 장치는 ESXi를 실행하는 미리 구성된 가상 시스템이며 OVA 파일로 분산됩니다.

범용 ESXi 호스트와 달리 감시 장치는 가상 시스템을 실행하지 않습니다. 유일한 용도는 vSAN 감시로 사용하는 것입니다.

vSAN 감시 장치를 배포 및 구성하는 워크플로에 이 프로세스가 포함됩니다.

- 1 VMware 웹 사이트에서 장치를 다운로드합니다.
- 2 vSAN 호스트 또는 클러스터에 장치를 배포합니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서에서 "OVF 템플릿 배포"를 참조하십시오.
- 3 감시 장치에서 vSAN 네트워크를 구성합니다.
- 4 감시 장치에서 관리 네트워크를 구성합니다.

- 5 장치를 감시 ESXi 호스트로 vCenter Server에 추가합니다. 호스트에서 vSAN VMkernel 인터페이스를 구성해야 합니다.

감시 장치에서 vSAN 네트워크 설정

vSAN 감시 장치에는 미리 구성된 네트워크 어댑터 2개가 포함됩니다. 장치가 vSAN 네트워크에 연결할 수 있으려면 두 번째 어댑터의 구성을 변경해야 합니다.

프로시저

- 1 vSphere Web Client에서 감시 호스트가 포함된 가상 장치로 이동합니다.
- 2 장치를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 두 번째 네트워크 어댑터를 확장합니다.
- 4 드롭다운 메뉴에서 vSAN 포트 그룹을 선택하고 **확인**을 클릭합니다.

관리 네트워크 구성

네트워크에서 연결할 수 있도록 감시 장치를 구성합니다.

기본적으로 장치는 네트워크에 DHCP 서버가 포함된 경우 자동으로 네트워킹 매개 변수를 가져옵니다. 그렇지 않은 경우 적절한 설정을 구성해야 합니다.

프로시저

- 1 감시 장치의 전원을 켜고 콘솔을 엽니다.
장치가 ESXi 호스트이므로 DCUI(직접 콘솔 사용자 인터페이스)가 표시됩니다.
- 2 F2를 눌러 [네트워크 어댑터] 페이지로 이동합니다.
- 3 [네트워크 어댑터] 페이지에서 전송을 위한 vmnic가 하나 이상 선택되었는지 확인합니다.
- 4 관리 네트워크에 대한 IPv4 매개 변수를 구성합니다.
 - a [IPv4 구성] 섹션으로 이동하여 기본 DHCP 설정을 정적으로 변경합니다.
 - b 다음 설정을 입력합니다.
 - IP 주소
 - 서브넷 마스크
 - 기본 게이트웨이
- 5 DNS 매개 변수를 구성합니다.
 - 기본 DNS 서버
 - 대체 DNS 서버
 - 호스트 이름

감시 트래픽에 대한 네트워크 인터페이스 구성

vSAN 데이터 트래픽에는 낮은 지연 시간과 높은 대역폭 링크가 필요합니다. 감시 트래픽은 높은 지연 시간, 낮은 대역폭 및 라우팅 가능 링크를 사용할 수 있습니다. 데이터 트래픽을 감시 트래픽과 분리하기 위해 vSAN 감시 트래픽에 대한 전용 VMkernel 네트워크 어댑터를 구성할 수 있습니다.

지원되는 확장된 클러스터 구성에서 데이터 트래픽을 감시 트래픽과 분리할 수 있습니다. vSAN 데이터 트래픽에 사용된 VMkernel 어댑터 및 감시 트래픽에 사용된 VMkernel 어댑터는 동일한 물리적 스위치에 연결되어야 합니다.

2개 호스트 vSAN 확장된 클러스터에서 vSAN 데이터 트래픽을 전송하기 위해 직접 네트워크 교차 연결에 대한 지원을 추가할 수 있습니다. 감시 트래픽에 대한 별도의 네트워크 연결을 구성할 수 있습니다. 클러스터의 각 데이터 호스트에서 관리 VMkernel 네트워크 어댑터를 구성하여 감시 트래픽도 전송합니다. 감시 호스트에서 감시 트래픽 유형을 구성하지 마십시오.

필수 조건

- 감시 트래픽 연결에 대한 데이터 사이트에 최소 100MBps의 대역폭과 200ms RTT 미만의 지연 시간이 있는지 확인합니다.
- vSAN 트래픽이 10GBps 속도의 직접 이더넷 케이블 연결을 통해 전송될 수 있는지 확인합니다.
- 데이터 트래픽 및 감시 트래픽이 동일한 IP 버전을 사용하는지 확인합니다.

프로시저

- 1 ESXi 호스트에 대한 SSH 연결을 엽니다.
- 2 `esxcli network ip interface list` 명령을 사용하여 관리 트래픽에 사용되는 VMkernel 네트워크 어댑터를 확인합니다.

예:

```
esxcli network ip interface list
vmk0
  Name: vmk0
  MAC Address: e4:11:5b:11:8c:16
  Enabled: true
  Portset: vSwitch0
  Portgroup: Management Network
  Netstack Instance: defaultTcpipStack
  VDS Name: N/A
  VDS UUID: N/A
  VDS Port: N/A
  VDS Connection: -1
  Opaque Network ID: N/A
  Opaque Network Type: N/A
  External ID: N/A
  MTU: 1500
  TSO MSS: 65535
  Port ID: 33554437
```

```
vmk1
  Name: vmk1
  MAC Address: 00:50:56:6a:3a:74
  Enabled: true
  Portset: vSwitch1
  Portgroup: vsandata
  Netstack Instance: defaultTcpipStack
  VDS Name: N/A
  VDS UUID: N/A
  VDS Port: N/A
  VDS Connection: -1
  Opaque Network ID: N/A
  Opaque Network Type: N/A
```

External ID: N/A
 MTU: 9000
 TSO MSS: 65535
 Port ID: 50331660

참고 이전 버전과 호환되도록 멀티캐스트 정보가 포함됩니다. vSAN 6.6 이상 릴리스에는 멀티캐스트가 필요하지 않습니다.

- 3 esxcli vsan network ip add 명령을 사용하여 감시 트래픽을 지원하기 위한 관리 VMkernel 네트워크 어댑터를 구성합니다.

```
esxcli vsan network ip add -i vmkx -T=witness
```

- 4 esxcli vsan network list 명령을 사용하여 새 네트워크 구성을 확인합니다.

예:

```
esxcli vsan network list
Interface
  VmKNic Name: vmk0
  IP Protocol: IP
  Interface UUID: 8cf3ec57-c9ea-148b-56e1-a0369f56dcc0
  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: witness
```

```
Interface
  VmKNic Name: vmk1
  IP Protocol: IP
  Interface UUID: 6df3ec57-4fb6-5722-da3d-a0369f56dcc0
  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
```

vSphere Web Client에서 관리 VMkernel 네트워크 인터페이스가 vSAN 트래픽에 대해 선택되지 않았습니다. vSphere Web Client에서 인터페이스를 다시 사용하도록 설정하지 마십시오.

확장된 클러스터를 표준 vSAN 클러스터로 변환

확장된 클러스터를 해제하고 표준 vSAN 클러스터로 변환할 수 있습니다.

확장된 클러스터를 사용하지 않도록 설정하는 경우 감시 호스트가 제거되지만 장애 도메인 구성은 유지됩니다. 감시 호스트를 사용할 수 없으므로 가상 시스템에 대한 모든 감시 구성 요소가 누락됩니다. VM의 전체 가용성을 확보하려면 클러스터 개체를 즉시 복구하십시오.

프로시저

- 1 vSphere Web Client에서 vSAN 확장된 클러스터로 이동합니다.
- 2 확장된 클러스터를 사용하지 않도록 설정합니다.
 - a 구성 탭을 클릭합니다.
 - b vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
 - c 확장된 클러스터 **구성** 버튼을 클릭합니다.
확장된 클러스터 구성 마법사가 표시됩니다.
 - d **사용 안 함**을 클릭한 다음 **예**를 클릭하여 확인합니다.
- 3 장애 도메인 구성을 제거합니다.
 - a 장애 도메인을 선택하고 **선택한 장애 도메인 제거** 아이콘(✖)을 클릭합니다. **예**를 클릭하여 확인합니다.
 - b 다른 장애 도메인을 선택하고 **선택한 장애 도메인 제거** 아이콘(✖)을 클릭합니다. **예**를 클릭하여 확인합니다.
- 4 클러스터의 개체를 복구합니다.
 - a **모니터** 탭을 클릭하고 **vSAN**을 선택합니다.
 - b vSAN에서 **상태**를 클릭하고 **vSAN 개체 상태**를 클릭합니다.
 - c **즉시 개체 복구**를 클릭합니다.
vSAN이 클러스터 내 감시 구성 요소를 다시 생성합니다.

vSAN 클러스터에서 공간 효율성 향상

공간 효율성 기술을 사용하면 데이터를 저장하는 데 필요한 공간의 양을 줄일 수 있습니다. 이러한 기술은 요구 사항을 충족하는 데 필요한 총 스토리지 공간을 줄입니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN 공간 효율성 소개,”](#) (69 페이지)
- [“중복 제거 및 압축 사용,”](#) (69 페이지)
- [“RAID 5 또는 RAID 6 이레이저 코딩 사용,”](#) (73 페이지)
- [“RAID 5 또는 RAID 6 설계 고려 사항,”](#) (74 페이지)

vSAN 공간 효율성 소개

공간 효율성 기술을 사용하면 데이터를 저장하는 데 필요한 공간의 양을 줄일 수 있습니다. 이러한 기술은 요구 사항을 충족하는 데 필요한 총 스토리지 용량을 줄입니다.

vSAN 클러스터에 중복 제거와 압축을 사용하도록 설정하면 중복 데이터를 제거하고 데이터 저장에 필요한 공간의 양을 줄일 수 있습니다.

RAID 5 또는 RAID 6 이레이저 코딩을 사용하도록 VM에 **장애 허용 방법** 정책 특성을 설정할 수 있습니다. 이레이저 코딩은 기본 RAID 1 미러링에 비해 스토리지 공간을 적게 사용하면서 데이터를 보호할 수 있습니다.

중복 제거와 압축 및 RAID 5 또는 RAID 6 이레이저 코딩을 사용하면 스토리지 공간을 더 많이 절감할 수 있습니다. RAID 5 또는 RAID 6은 RAID 1에 비해 확연하게 공간 절약 효과를 제공하며, 중복 제거와 압축은 추가적인 공간 절약 효과를 제공합니다.

중복 제거 및 압축 사용

vSAN은 블록 수준 중복 제거와 압축을 수행하여 스토리지 공간을 절약할 수 있습니다. vSAN 플래시 전용 클러스터에서 중복 제거와 압축을 사용하도록 설정하면 각 디스크 그룹 내의 중복 데이터가 줄어듭니다.

중복 제거는 중복 데이터 블록을 제거하는 반면 압축은 각 데이터 블록 내에서 추가적인 중복 데이터를 제거합니다. 이 두 가지 기술은 데이터 저장에 필요한 공간의 양을 줄이는 데 함께 기여합니다. vSAN은 캐시 계층에서 용량 계층으로 데이터를 이동할 때 중복 제거와 압축을 차례로 적용합니다.

중복 제거와 압축을 클러스터 전체의 설정으로 사용할 수 있지만 이러한 기능은 디스크 그룹 단위로 적용됩니다. vSAN 클러스터에서 중복 제거와 압축을 사용하도록 설정하면 특정 디스크 그룹 내의 중복 데이터가 단일 복사본으로 줄어듭니다.

중복 제거와 압축은 새 vSAN 플래시 전용 클러스터를 생성하거나, 기존 vSAN 플래시 전용 클러스터를 편집할 때 사용하도록 설정할 수 있습니다. vSAN 클러스터 생성 및 편집에 대한 자세한 내용은 [“vSAN 사용,”](#) (45 페이지) 항목을 참조하십시오.

중복 제거와 압축을 사용하거나 사용하지 않도록 설정할 경우 vSAN은 모든 호스트에 있는 모든 디스크 그룹에 대해 롤링 다시 포맷을 수행합니다. vSAN 데이터스토어에 저장된 데이터에 따라 이 프로세스를 수행하는 데 상당한 시간이 소요될 수 있습니다. 따라서 이러한 작업은 자주 수행하지 않는 것이 좋습니다. 중복 제거와 압축을 사용하지 않도록 설정하려면 데이터를 저장하는 데 사용할 수 있는 물리적 용량이 충분히 있는지를 먼저 확인해야 합니다.

참고 VM 암호화는 호스트의 데이터를 스토리지에 쓰기 전에 암호화하므로 암호화된 VM에는 중복 제거와 압축이 효과적이지 않을 수 있습니다. VM 암호화를 사용할 경우 스토리지의 균형을 고려하십시오.

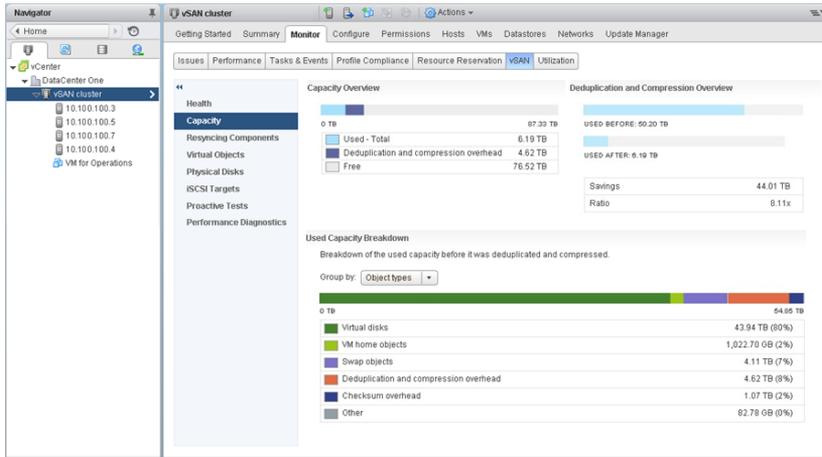
중복 제거와 압축을 사용하는 클러스터의 디스크 관리 방법

중복 제거와 압축을 사용하도록 설정된 클러스터를 관리하는 경우 다음과 같은 지침을 고려하십시오.

- 디스크 그룹에 디스크를 추가하여 늘리지 마십시오. 중복 제거 및 압축 효율성을 높이려면 새 디스크 그룹을 추가하는 방법으로 클러스터 스토리지 용량을 늘리십시오.
- 디스크 그룹을 수동으로 추가하는 경우, 모든 용량 디스크를 동시에 추가하십시오.
- 단일 디스크를 디스크 그룹에서 제거할 수 없습니다. 수정해야 할 사항이 있으면 디스크 그룹 전체를 제거해야 합니다.
- 단일 디스크 장애 때문에 디스크 그룹 전체에서 장애가 발생할 수 있습니다.

중복 제거와 압축을 통한 공간 절약 확인

중복 제거와 압축을 통해 줄어드는 스토리지 양은 저장되는 데이터의 유형, 중복 블록의 개수 등 여러 요인에 따라 달라집니다. 디스크 그룹의 크기가 클수록 중복 제거 비율이 높은 경향이 있습니다. vSAN 용량 모니터에서 중복 제거 및 압축 개요를 확인하여 중복 제거와 압축의 결과를 확인할 수 있습니다.



중복 제거 및 압축 개요는 vSphere Web Client에서 vSAN 용량을 모니터링할 때 볼 수 있습니다. 중복 제거 및 압축 개요에는 중복 제거 및 압축의 결과에 대한 정보가 표시됩니다. 이전 사용 공간은 중복 제거와 압축을 적용하기 전에 필요했던 논리적 공간을 나타내고 이후 사용 공간은 중복 제거와 압축을 적용한 후에 사용된 물리적 공간을 나타냅니다. 이후 사용 공간에는 절약된 공간의 양에 대한 개요와 중복 제거 및 압축 비율도 표시됩니다.

중복 제거 및 압축 비율은 중복 제거와 압축을 적용한 후에 필요한 물리적(이후 사용) 공간을 기준으로 중복 제거와 압축을 적용하기 전에 데이터를 저장하는 데 필요한 논리적(이전 사용) 공간을 기반으로 합니다. 구체적으로 이 비율은 이전 사용 공간을 이후 사용 공간으로 나눈 값입니다. 예를 들어 이전 사용 공간이 3GB이고 물리적인 이후 사용 공간이 1GB인 경우 중복 제거와 압축 비율은 3x입니다.

vSAN 클러스터에서 중복 제거와 압축을 사용하도록 설정하면 디스크 공간이 회수되고 다시 할당되면서 용량 업데이트가 용량 모니터에 반영되는 데 몇 분 정도 소요될 수 있습니다.

중복 제거와 압축의 설계 고려 사항

vSAN 클러스터에 중복 제거와 압축을 구성하는 경우 다음과 같은 지침을 고려합니다.

- 중복 제거와 압축은 플래시 전용 디스크 그룹에서만 사용할 수 있습니다.
- 중복 제거와 압축을 지원하려면 온디스크 형식 버전 3.0 이상이 필요합니다.
- 클러스터에서 중복 제거와 압축을 사용하도록 설정하려면 유효한 라이선스를 가지고 있어야 합니다.
- 수동 스토리지 할당 방법을 설정한 경우에만 중복 제거와 압축을 사용하도록 설정할 수 있습니다. 스토리지 할당 방법은 중복 제거와 압축을 사용하도록 설정한 이후에 자동 스토리지 할당 방법으로 변경할 수 있습니다.
- vSAN 클러스터에서 중복 제거와 압축을 사용하도록 설정하면 모든 디스크 그룹이 중복 제거와 압축을 통한 데이터 감소에 참여합니다.
- vSAN은 각 디스크 그룹 내에서 중복 데이터 블록을 제거할 수 있지만 디스크 그룹 사이의 중복 데이터 블록은 제거할 수 없습니다.
- 중복 제거와 압축을 위한 용량 오버헤드는 총 원시 용량의 약 5%입니다.
- 정책의 개체 공간 예약은 0% 또는 100% 중 하나여야 합니다. 100% 개체 공간 예약을 가진 정책은 항상 적용되지만 중복 제거 및 압축의 효율이 떨어질 수 있습니다.

새 vSAN 클러스터에서 중복 제거와 압축 사용

새 vSAN 플래시 전용 클러스터를 구성할 때 중복 제거와 압축을 사용하도록 설정할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 기존 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택하고 **vSAN 구성** 버튼을 클릭합니다.
- 4 클러스터에서 중복 제거와 압축을 구성합니다.
 - a **vSAN 기능** 페이지에서 중복 제거와 압축의 **사용** 확인란을 선택합니다.
 - b (선택 사항) VM에 대해 감소된 이중화를 사용하도록 설정합니다.
 “vSAN 클러스터에 대한 VM 이중화 감소,” (72 페이지)를 참조하십시오.
- 5 **디스크 할당** 페이지에서 vSAN 클러스터에 대해 할당할 디스크를 지정합니다.
 - a 용량으로 사용할 플래시 디바이스를 선택하고 **용량 계층에 대해 할당** 아이콘()을 클릭합니다.
 - b 캐시로 사용할 플래시 디바이스를 선택하고 **캐시 계층에 대해 할당** 아이콘()을 클릭합니다.
- 6 클러스터 구성을 완료합니다.

기존 vSAN 클러스터에서 중복 제거와 압축 사용

기존 vSAN 클러스터에서 구성 매개 변수를 편집하여 중복 제거와 압축을 사용하도록 설정할 수 있습니다.

필수 조건

vSAN 클러스터를 생성합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 호스트 클러스터로 이동합니다.

- 2 구성 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택합니다.
- 4 [vSAN 켜짐] 창에서 **편집** 버튼을 클릭합니다.
- 5 중복 제거와 압축을 구성합니다.
 - a 중복 제거와 압축을 **사용**으로 설정합니다.
 - b (선택 사항) VM에 대해 감소된 이중화를 사용하도록 설정합니다.
 “vSAN 클러스터에 대한 VM 이중화 감소,” (72 페이지)를 참조하십시오.
 - c **확인**을 클릭하여 구성 변경 내용을 저장합니다.

중복 제거와 압축을 사용하도록 설정하는 동안 vSAN이 클러스터의 각 디스크 그룹에서 디스크 형식을 변경합니다. 이 변경을 수행하기 위해 vSAN이 디스크 그룹에서 데이터를 제거하고 디스크 그룹을 제거한 다음 중복 제거와 압축을 지원하는 새 형식으로 재생성합니다.

사용 설정 작업에는 가상 시스템 마이그레이션 또는 DRS가 필요하지 않습니다. 이 작업에 필요한 시간은 클러스터의 호스트 수와 데이터 양에 따라 다릅니다. **작업 및 이벤트** 탭에서 진행률을 모니터링할 수 있습니다.

중복 제거와 압축 사용하지 않도록 설정

vSAN 클러스터에서 중복 제거와 압축을 사용하지 않도록 설정할 수 있습니다.

vSAN 클러스터에서 중복 제거와 압축이 사용되지 않도록 설정된 경우 중복 제거 비율에 따라 클러스터의 사용된 용량 크기가 확장될 수 있습니다. 중복 제거와 압축을 사용하지 않도록 설정하기 전에 클러스터에 확장된 데이터 크기를 처리할 충분한 용량이 있는지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 호스트 클러스터로 이동합니다.
- 2 구성 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택합니다.
- 4 [vSAN 켜짐] 창에서 **편집** 버튼을 클릭합니다.
- 5 중복 제거와 압축을 사용하지 않도록 설정합니다.
 - a 디스크 할당 모드를 **수동**으로 설정합니다.
 - b 중복 제거와 압축을 **사용 안 함**으로 설정합니다.
 - c **확인**을 클릭하여 구성 변경 내용을 저장합니다.

중복 제거와 압축을 사용하지 않도록 설정하는 동안 vSAN이 클러스터의 각 디스크 그룹에서 디스크 형식을 변경합니다. 또한 디스크 그룹에서 데이터를 제거하고 디스크 그룹을 제거한 다음 중복 제거와 압축을 지원하지 않는 형식으로 다시 생성합니다.

이 작업에 필요한 시간은 클러스터의 호스트 수와 데이터 양에 따라 다릅니다. **작업 및 이벤트** 탭에서 진행률을 모니터링할 수 있습니다.

vSAN 클러스터에 대한 VM 이중화 감소

중복 제거와 압축을 사용하도록 설정하면 특정 경우에 가상 시스템에 대한 보호 수준을 낮춰야 할 수 있습니다.

중복 제거와 압축을 사용하도록 설정하려면 디스크 그룹에 대한 형식 변경이 필요합니다. 이 변경을 수행하기 위해 vSAN이 디스크 그룹에서 데이터를 제거하고 디스크 그룹을 제거한 다음 중복 제거와 압축을 지원하는 새 형식으로 재생성합니다.

특정 환경에서 vSAN 클러스터에 디스크 그룹을 완전히 제거하기에 충분한 리소스가 없을 수 있습니다. 이러한 배포의 예에는 전체 보호를 유지하면서 복제 또는 감시를 제거하기 위한 리소스가 없는 노드 3개로 구성된 클러스터가 포함됩니다. 또는 RAID-5 개체가 이미 배포된 노드 4개로 구성된 클러스터도 포함됩니다. 후자의 경우 RAID-5 개체에 최소 4개의 노드가 필요하므로 RAID-5 스트라이프의 일부를 이동할 공간이 없습니다.

이러한 경우에도 중복 제거와 압축을 사용하도록 설정하고 [감소된 이중화 허용] 옵션을 사용할 수 있습니다. 이 옵션은 VM이 실행되도록 유지해 주지만 해당 VM은 VM 스토리지 정책에 정의된 전체 장애 수준을 허용하지 못할 수 있습니다. 결과적으로 중복 제거와 압축에 대한 형식을 변경하는 동안 일시적으로 가상 시스템에 데이터 손실 위험이 발생할 수 있습니다. vSAN은 형식 변환 완료 후 전체 규정 준수 및 이중화를 복원합니다.

중복 제거와 압축이 사용되도록 설정된 경우 디스크 추가 또는 제거

중복 제거와 압축이 사용되도록 설정된 vSAN 클러스터에 디스크를 추가하는 경우 특정 고려 사항이 적용됩니다.

- 중복 제거와 압축이 사용되도록 설정된 디스크 그룹에 용량 디스크를 추가할 수 있습니다. 그러나 중복 제거와 압축 효율성을 높이려면 용량 디스크를 추가하는 대신 새 디스크 그룹을 생성하여 클러스터 스토리지 용량을 늘리십시오.
- 캐시 계층에서 디스크를 제거하는 경우 전체 디스크 그룹이 제거됩니다. 중복 제거와 압축이 사용되도록 설정된 경우 캐시 계층 디스크를 제거하면 데이터 제거가 트리거됩니다.
- 중복 제거와 압축은 디스크 그룹 수준에서 구현됩니다. 중복 제거와 압축이 사용되도록 설정된 클러스터에서 용량 디스크를 제거할 수 없습니다. 전체 디스크 그룹을 제거해야 합니다.
- 용량 디스크가 실패하는 경우 전체 디스크 그룹이 사용할 수 없게 됩니다. 이 문제를 해결하려면 실패하는 구성 요소를 즉시 식별하고 교체하십시오. 실패한 디스크 그룹을 제거할 경우 [데이터 마이그레이션 없음] 옵션을 사용하십시오.

RAID 5 또는 RAID 6 이레이저 코딩 사용

RAID 5 또는 RAID 6 이레이저 코딩을 사용하면 데이터 손실을 방지하고 스토리지 효율성을 높일 수 있습니다. 이레이저 코딩은 스토리지 용량은 더 적게 사용하면서 미러링(RAID 1)과 동일한 수준의 데이터 보호 기능을 제공할 수 있습니다.

RAID 5 또는 RAID 6 이레이저 코딩을 사용할 경우 vSAN은 데이터스토어에서 최대 2개의 용량 디바이스 장애를 허용할 수 있습니다. 장애 도메인이 4개 이상 있는 플래시 전용 클러스터에는 RAID 5를 구성할 수 있습니다. 장애 도메인이 6개 이상 있는 플래시 전용 클러스터에는 RAID 5 또는 RAID 6을 구성할 수 있습니다.

RAID 5 또는 RAID 6 이레이저 코딩은 데이터를 보호하는 데 RAID 1 미러링보다 추가 용량을 더 적게 사용합니다. 예를 들어 허용할 수 있는 장애의 기본 수준 값을 1로 설정하여 VM을 보호하는 경우 RAID 1을 사용하면 가상 디스크 크기의 두 배가 필요하지만 RAID 5를 사용하면 가상 디스크 크기의 1.33배가 필요합니다. 다음 표에는 RAID 1과 RAID 5 또는 RAID 6에 대한 일반적인 비교 정보가 나와 있습니다.

표 7-1. RAID 수준별로 데이터를 저장하고 보호하는 데 필요한 용량

| RAID 구성 | 허용할 수 있는 장애의 기본 수준 | 데이터 크기 | 필요 용량 |
|---------------------------------------|--------------------|--------|-------|
| RAID 1(미러링) | 1 | 100GB | 200GB |
| RAID 5 또는 RAID 6(이레이저 코딩) 및 장애 도메인 4개 | 1 | 100GB | 133GB |

표 7-1. RAID 수준별로 데이터를 저장하고 보호하는 데 필요한 용량 (계속)

| RAID 구성 | 허용할 수 있는 장애의 기본 수준 | 데이터 크기 | 필요 용량 |
|---------------------------------------|--------------------|--------|-------|
| RAID 1(미러링) | 2 | 100GB | 300GB |
| RAID 5 또는 RAID 6(이레이저 코딩) 및 장애 도메인 6개 | 2 | 100GB | 150GB |

RAID 5 또는 RAID 6 이레이저 코딩은 가상 시스템 구성 요소에 적용할 수 있는 정책 특성입니다. RAID 5를 사용하려면 **장애 허용 방법을 RAID-5/6(이레이저 코딩) - 용량**으로 설정하고 **허용할 수 있는 장애의 기본 수준**을 1로 설정합니다. RAID 6을 사용하려면 **장애 허용 방법을 RAID-5/6(이레이저 코딩) - 용량**으로 설정하고 **허용할 수 있는 장애의 기본 수준**을 2로 설정합니다. RAID 5 또는 RAID 6 이레이저 코딩을 사용할 경우 **허용할 수 있는 장애의 기본 수준** 값을 3으로 설정할 수 없습니다.

RAID 1을 설정하려면 **장애 허용 방법을 RAID-1(미러링) - 성능**으로 설정합니다. RAID 1 미러링을 사용하면 스토리지 디바이스에 대한 I/O 작업 수가 적기 때문에 성능이 더 뛰어납니다. 예를 들어 RAID 1을 사용할 경우 클러스터 다시 동기화를 더 짧은 시간 안에 완료할 수 있습니다.

정책 구성에 대한 자세한 내용은 [12장, “vSAN 정책 사용,”](#) (123 페이지)을 참조하십시오.

RAID 5 또는 RAID 6 설계 고려 사항

vSAN 클러스터에 RAID 5 또는 RAID 6 이레이저 코딩을 구성하는 경우 다음과 같은 지침을 고려합니다.

- RAID 5 또는 RAID 6 이레이저 코딩은 플래시 전용 디스크 그룹에만 사용할 수 있습니다.
- RAID 5 또는 RAID 6을 지원하려면 온디스크 형식 버전 3.0 이상이 필요합니다.
- 클러스터에서 RAID 5/6을 사용하려면 유효한 라이선스를 가지고 있어야 합니다.
- 확장된 클러스터에는 RAID 5/6이 지원되지 않습니다.
- vSAN 클러스터에 중복 제거와 압축을 사용하도록 설정하면 공간을 추가적으로 절약할 수 있습니다.

vSAN 클러스터에서 암호화 사용

저장된 데이터 암호화를 사용하여 vSAN 클러스터의 데이터를 보호할 수 있습니다.

vSAN은 저장된 데이터 암호화를 수행할 수 있습니다. 데이터는 중복 제거 같은 다른 모든 처리가 수행된 이후에 암호화됩니다. 저장된 데이터 암호화 기능은 디바이스가 클러스터에서 제거될 경우에 스토리지 디바이스의 데이터를 보호합니다.

vSAN 클러스터에서 암호화를 사용하려면 준비 작업이 필요합니다. 환경 설정이 완료된 후에 vSAN 클러스터에서 암호화를 사용하도록 설정할 수 있습니다.

vSAN 암호화를 위해서는 외부 KMS(키 관리 서버), vCenter Server 시스템 및 ESXi 호스트가 필요합니다. vCenter Server가 외부 KMS에 암호화 키를 요청합니다. KMS는 키를 생성 및 저장하고, vCenter Server는 KMS로부터 키 ID를 가져와 ESXi 호스트에 배포합니다.

vCenter Server는 KMS 키를 저장하지 않지만 키 ID 목록을 보관합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN 암호화 작동 방식,”](#) (75 페이지)
- [“vSAN 암호화에 대한 설계 고려 사항,”](#) (76 페이지)
- [“KMS 클러스터 설정,”](#) (76 페이지)
- [“새 vSAN 클러스터에서 암호화 사용,”](#) (81 페이지)
- [“새 암호화 키 생성,”](#) (81 페이지)
- [“기존 vSAN 클러스터에서 vSAN 암호화 사용,”](#) (82 페이지)
- [“vSAN 암호화 및 코어 덤프,”](#) (83 페이지)

vSAN 암호화 작동 방식

암호화를 사용하도록 설정하는 경우 vSAN은 vSAN 데이터스토어의 모든 항목을 암호화합니다. 모든 파일이 암호화되기 때문에 모든 가상 시스템과 해당 데이터가 보호됩니다. 암호화 및 암호 해독 작업은 암호화 권한을 가진 관리자만 수행할 수 있습니다.

vSAN은 암호화 키를 다음과 같이 사용합니다.

- vCenter Server가 AES-256 KEK(키 암호화 키)를 KMS에 요청합니다. vCenter Server는 키 자체가 아니라 KEK의 ID만 저장합니다.
- ESXi 호스트는 업계 표준 AES-256 XTS 모드를 사용하여 디스크 데이터를 암호화합니다. 각 디스크에는 임의로 생성된 서로 다른 DEK(데이터 암호화 키)가 있습니다.
- 각 ESXi 호스트는 KEK를 사용하여 해당 DEK를 암호화하고, 암호화된 DEK를 디스크에 저장합니다. 호스트는 KEK를 디스크에 저장하지 않습니다. 재부팅 시 호스트는 해당하는 ID를 사용하여 KMS에 KEK를 요청합니다. 이렇게 하면 호스트가 필요에 따라 DEK를 암호 해독할 수 있습니다.

- 호스트 키는 데이터가 아니라 코어 덤프를 암호화하는 데 사용됩니다. 동일한 클러스터의 모든 호스트는 동일한 호스트 키를 사용합니다. 지원 번들을 수집할 때 임의 키가 생성되어 코어 덤프를 다시 암호화합니다. 임의 키를 암호화하는 경우 암호를 사용하십시오.

재부팅 시 호스트는 KEK를 받기 전에는 해당 디스크 그룹을 마운트하지 않습니다. 이 프로세스가 완료되는 데 몇 분 또는 그 이상이 소요될 수 있습니다. vSAN Health Service의 **물리적 디스크 > 소프트웨어 상태**에서 디스크 그룹의 상태를 모니터링할 수 있습니다.

vSAN 암호화에 대한 설계 고려 사항

vSAN 암호화를 사용하는 경우에 다음과 같은 지침을 고려합니다.

- 암호화하려는 동일한 vSAN 데이터스토어에 KMS 서버를 배포하지 마십시오.
- 암호화에는 많은 CPU가 사용됩니다. AES-NI는 암호화 성능을 크게 개선합니다. BIOS에서 AES-NI를 사용하도록 설정하십시오.
- 확장된 클러스터의 감시 호스트는 vSAN 암호화에 참여하지 않습니다. 감시 호스트에는 메타데이터만 저장됩니다.
- 코어 덤프에 대한 정책을 설정합니다. 코어 덤프는 키 등 중요한 정보를 포함할 수 있기 때문에 암호화됩니다. 코어 덤프를 암호 해독할 때는 해당 중요 정보를 주의해서 처리해야 합니다. ESXi 코어 덤프에는 ESXi 호스트 및 호스트에 있는 데이터의 키가 포함될 수 있습니다.
 - `vm-support` 번들을 수집할 때 항상 암호를 사용합니다. vSphere Web Client에서 지원 번들을 생성할 때 암호를 지정하거나 `vm-support` 명령을 사용하여 암호를 지정할 수 있습니다.
암호는 암호에 기반한 키를 사용하기 위해 내부 키를 사용하는 코어 덤프를 이중 암호화합니다. 나중에 지원 번들에 포함되었을 수도 있는 암호화된 코어 덤프의 암호를 해독하는 데 이 암호를 사용할 수 있습니다. 암호화되지 않은 코어 덤프 또는 로그는 영향을 받지 않습니다.
 - `vm-support` 번들을 생성하는 동안 지정하는 암호는 vSphere 구성 요소에 유지되지 않습니다. 지원 번들용 암호를 추적하는 것은 사용자의 책임입니다.

KMS 클러스터 설정

KMS(키 관리 서버) 클러스터는 vSAN 데이터스토어를 암호화하는 데 사용할 수 있는 키를 제공합니다.

vSAN 데이터스토어를 암호화하려면 먼저 암호화를 지원하도록 KMS 클러스터를 설정해야 합니다. 그러기 위해서는 KMS를 vCenter Server에 추가하고 KMS와의 신뢰 관계를 설정해야 합니다.

vCenter Server는 KMS 클러스터에서 암호화 키를 프로비저닝합니다.

KMS는 KMIP(Key Management Interoperability Protocol) 1.1 표준을 지원해야 합니다.

vCenter Server 에 KMS 추가

vSphere Web Client에서 vCenter Server 시스템에 KMS(키 관리 서버)를 추가할 수 있습니다.

첫 번째 KMS 인스턴스를 추가하면 vCenter Server에서 KMS 클러스터를 생성합니다. 둘 이상의 vCenter Server에 KMS 클러스터를 구성할 때는 동일한 KMS 클러스터 이름을 사용해야 합니다.

참고 암호화할 예정인 vSAN 클러스터에는 KMS 서버를 배포하지 마십시오. 장애가 발생할 경우 vSAN 클러스터에 있는 호스트가 KMS와 통신해야 하기 때문입니다.

- KMS를 추가할 때 이 클러스터를 기본값으로 설정하라는 메시지가 표시됩니다. 나중에 기본 클러스터를 명시적으로 변경할 수 있습니다.
- vCenter Server에서 첫 번째 클러스터를 생성한 후에는 동일한 벤더의 KMS 인스턴스를 클러스터에 추가할 수 있습니다.
- KMS 인스턴스 하나만으로 클러스터를 설정해도 됩니다.

- 환경에서 여러 벤더의 KMS 솔루션을 지원하는 경우 여러 KMS 클러스터를 추가할 수 있습니다.

필수 조건

- 키 서버가 vSphere 호환성 매트릭스에 있고 KMIP 1.1을 준수하는지 확인합니다.
- 필요한 권한이 있는지 확인합니다(**Cryptographer.ManageKeyServers**).
- IPv6 주소만 사용하여 KMS에 연결하는 것은 지원되지 않습니다.
- 사용자 이름이나 암호가 필요한 프록시 서버를 통해 KMS에 연결하는 것은 지원되지 않습니다.

프로시저

- 1 vSphere Web Client를 사용하여 vCenter Server 시스템에 로그인합니다.
- 2 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.
- 3 구성을 클릭하고 **키 관리 서버**를 클릭합니다.
- 4 **KMS 추가**를 클릭하고 마법사에서 KMS 정보를 지정한 후 **확인**을 클릭합니다.

| 옵션 | 값 |
|----------|--|
| KMS 클러스터 | 새 클러스터를 생성하려면 새 클러스터 생성 을 선택합니다. 기존 클러스터가 있는 경우 해당 클러스터를 선택할 수 있습니다. |
| 클러스터 이름 | KMS 클러스터의 이름입니다. vCenter Server 인스턴스를 사용할 수 없는 경우 이 이름을 사용하여 KMS에 연결할 수 있습니다. |
| 서버 별칭 | KMS의 별칭입니다. vCenter Server 인스턴스를 사용할 수 없는 경우 별칭을 사용하여 KMS에 연결할 수 있습니다. |
| 서버 주소 | KMS의 IP 주소 또는 FQDN입니다. |
| 서버 포트 | vCenter Server에서 KMS에 연결하는 포트입니다. |
| 프록시 주소 | KMS에 연결하는 데 사용할 선택적 프록시 주소입니다. |
| 프록시 포트 | KMS에 연결하는 데 사용할 선택적 프록시 포트입니다. |
| 사용자 이름 | 일부 KMS 벤더에서는 사용자가 사용자 이름과 암호를 지정하여 서로 다른 사용자 또는 그룹이 사용하는 암호화 키를 분리할 수 있도록 합니다. KMS에서 이 기능을 지원하고 이 기능을 사용할 계획인 경우에만 사용자 이름을 지정하십시오. |
| 암호 | 일부 KMS 벤더에서는 사용자가 사용자 이름과 암호를 지정하여 서로 다른 사용자 또는 그룹이 사용하는 암호화 키를 분리할 수 있도록 합니다. KMS에서 이 기능을 지원하고 이 기능을 사용할 계획인 경우에만 암호를 지정하십시오. |

인증서 교환을 통한 신뢰할 수 있는 연결 설정

vCenter Server 시스템에 KMS를 추가한 후 신뢰할 수 있는 연결을 설정할 수 있습니다. 정확한 프로세스는 KMS가 수락하는 인증서와 회사 정책에 따라 달라집니다.

필수 조건

KMS 클러스터를 추가합니다.

프로시저

- 1 vSphere Web Client에 로그인하고 vCenter Server 시스템을 선택합니다.
- 2 구성을 클릭하고 **키 관리 서버**를 선택합니다.
- 3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.
- 4 **KMS와 신뢰 설정**을 클릭합니다.

- 5 서버에 적합한 옵션을 선택하고 단계를 완료합니다.

| 옵션 | 자세한 내용은 |
|----------------|---|
| 루트 CA 인증서 | “루트 CA 인증서 옵션을 사용하여 신뢰할 수 있는 연결 설정,” (78 페이지). |
| 인증서 | “인증서 옵션을 사용하여 신뢰할 수 있는 연결 설정,” (78 페이지). |
| 새 인증서 서명 요청 | “새 인증서 서명 요청 옵션을 사용하여 신뢰할 수 있는 연결 설정,” (79 페이지). |
| 인증서 및 개인 키 업로드 | “인증서 및 개인 키 업로드 옵션을 사용하여 신뢰할 수 있는 연결 설정,” (79 페이지). |

루트 CA 인증서 옵션을 사용하여 신뢰할 수 있는 연결 설정

SafeNet과 같은 일부 KMS 벤더의 경우 루트 CA 인증서를 KMS에 업로드해야 합니다. 그러면 루트 CA가 서명한 모든 인증서를 이 KMS에서 신뢰하게 됩니다.

vSphere 가상 시스템 암호화에 사용되는 루트 CA 인증서는 자체 서명된 인증서로, vCenter Server 시스템의 VECS(VMware Endpoint Certificate Store) 내 별도의 저장소에 저장됩니다.

참고 기존 인증서를 교체하려는 경우에만 루트 CA 인증서를 생성합니다. 루트 CA 인증서를 생성하면 해당 루트 CA에서 서명한 다른 인증서가 무효화됩니다. 이 워크플로의 일부로 새 루트 CA 인증서를 생성할 수 있습니다.

프로시저

- 1 vSphere Web Client에 로그인하고 vCenter Server 시스템을 선택합니다.
- 2 구성을 클릭하고 **키 관리 서버**를 선택합니다.
- 3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.
- 4 **루트 CA 인증서**를 선택하고 **확인**을 클릭합니다.

[루트 CA 인증서 다운로드] 대화상자가 vCenter Server에서 암호화에 사용하는 루트 인증서로 채워집니다. 이 인증서는 VECS에 저장됩니다.

- 5 인증서를 클립보드에 복사하거나 인증서를 파일로 다운로드합니다.
- 6 KMS 벤더의 지침을 따라 인증서를 해당 시스템에 업로드합니다.

참고 SafeNet과 같은 일부 KMS 벤더의 경우 업로드된 루트 인증서를 사용하기 위해 해당 KMS 벤더에서 KMS를 재시작해야 합니다.

후속 작업

인증서 교체를 완료합니다. “**신뢰 설정 완료**,” (80 페이지)를 참조하십시오.

인증서 옵션을 사용하여 신뢰할 수 있는 연결 설정

Vormetric과 같은 일부 KMS 벤더의 경우 vCenter Server 인증서를 KMS에 업로드해야 합니다. 업로드 후에 KMS는 이 인증서를 사용하여 시스템에서 들어오는 트래픽을 수락합니다.

vCenter Server에서는 인증서를 생성하여 KMS와의 연결을 보호합니다. 인증서는 vCenter Server 시스템의 VECS(VMware Endpoint Certificate Store) 내 별도 키 저장소에 저장됩니다.

프로시저

- 1 vSphere Web Client에 로그인하고 vCenter Server 시스템을 선택합니다.
- 2 구성을 클릭하고 **키 관리 서버**를 선택합니다.
- 3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

4 인증서를 선택하고 **확인**을 클릭합니다.

vCenter Server에서 암호화에 사용하는 루트 인증서가 [인증서 다운로드] 대화상자에 채워집니다. 이 저장소는 VECS에 저장됩니다.

참고 기존 인증서를 교체하려는 경우가 아니라면 새 인증서를 생성하지 마십시오.

5 인증서를 클립보드에 복사하거나 파일로 다운로드합니다.

6 KMS 벤더의 지침을 따라 인증서를 KMS에 업로드합니다.

후속 작업

신뢰 관계를 완료합니다. “[신뢰 설정 완료](#),” (80 페이지)를 참조하십시오.

새 인증서 서명 요청 옵션을 사용하여 신뢰할 수 있는 연결 설정

Thales와 같은 일부 KMS 벤더의 경우 vCenter Server에서 CSR(인증서 서명 요청)을 생성하고 해당 CSR을 KMS에 보내야 합니다. KMS에서는 CSR에 서명하고 서명된 인증서를 반환합니다. 서명된 인증서를 vCenter Server에 업로드할 수 있습니다.

새 인증서 서명 요청 옵션을 사용하는 프로세스는 2단계로 이루어집니다. 먼저 CSR을 생성하고 KMS 벤더에 보냅니다. 그런 다음 KMS 벤더에서 받은 서명된 인증서를 vCenter Server에 업로드합니다.

프로시저

1 vSphere Web Client에 로그인하고 vCenter Server 시스템을 선택합니다.

2 구성을 클릭하고 키 관리 서버를 선택합니다.

3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

4 새 인증서 서명 요청을 선택하고 **확인**을 클릭합니다.

5 대화 상자에서 텍스트 상자의 전체 인증서를 클립보드에 복사하거나 파일로 다운로드하고 **확인**을 클릭합니다.

명시적으로 CSR을 생성하려는 경우에만 대화 상자에서 **새 CSR 생성** 버튼을 사용합니다. 이 옵션을 사용하면 이전 CSR 기반의 서명된 인증서가 모두 무효화됩니다.

6 KMS 벤더의 지침을 따라 CSR을 제출합니다.

7 KMS 벤더로부터 서명된 인증서를 받으면 키 관리 서버를 다시 클릭하고 새 인증서 서명 요청을 다시 선택합니다.

8 서명된 인증서를 하단 텍스트 상자에 붙여 넣거나 파일 업로드를 클릭하고 파일을 업로드한 후 **확인**을 클릭합니다.

후속 작업

신뢰 관계를 완료합니다. “[신뢰 설정 완료](#),” (80 페이지)를 참조하십시오.

인증서 및 개인 키 업로드 옵션을 사용하여 신뢰할 수 있는 연결 설정

HyTrust와 같은 일부 KMS 벤더의 경우 사용자가 KMS 서버 인증서를 업로드하고 개인 키를 vCenter Server 시스템에 업로드해야 합니다.

일부 KMS 벤더는 연결용 인증서와 개인 키를 생성하여 제공합니다. 파일을 업로드한 후에 KMS는 vCenter Server 인스턴스를 신뢰합니다.

필수 조건

- KMS 벤더에서 인증서와 개인 키를 요청합니다. 파일은 PEM 형식의 X509 파일입니다.

프로시저

1 vSphere Web Client에 로그인하고 vCenter Server 시스템을 선택합니다.

- 2 구성을 클릭하고 **키 관리 서버**를 선택합니다.
- 3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.
- 4 **인증서 및 개인 키 업로드**를 선택하고 **확인**을 클릭합니다.
- 5 KMS 벤더에서 받은 인증서를 상단 텍스트 상자에 붙여 넣거나 **파일 업로드**를 클릭하여 인증서 파일을 업로드합니다.
- 6 키 파일을 하단 텍스트 상자에 붙여 넣거나 **파일 업로드**를 클릭하여 키 파일을 업로드합니다.
- 7 **확인**을 클릭합니다.

후속 작업

신뢰 관계를 완료합니다. “[신뢰 설정 완료](#),” (80 페이지)를 참조하십시오.

기본 KMS 클러스터 설정

첫 번째 클러스터를 기본 클러스터로 사용하지 않거나, 여러 클러스터를 사용하는 환경에서 기본 클러스터를 제거한 경우 기본 KMS 클러스터를 설정해야 합니다.

필수 조건

키 관리 서버 탭의 [연결 상태]에 [정상] 및 녹색 확인 표시가 있는지 확인하는 것이 모범 사례입니다.

프로시저

- 1 vSphere Web Client에 로그인하고 vCenter Server 시스템을 선택합니다.
- 2 구성 탭을 클릭하고 **더 보기** 아래에서 **키 관리 서버**를 클릭합니다.
- 3 클러스터를 선택하고 **KMS 클러스터를 기본으로 설정**을 클릭합니다.
서버를 선택하지 마십시오. 기본으로 설정하는 메뉴는 클러스터에 대해서만 사용할 수 있습니다.
- 4 **예**를 클릭합니다.
클러스터 이름 옆에 default라는 단어가 표시됩니다.

신뢰 설정 완료

서버 추가 대화상자에 KMS를 신뢰하라는 메시지가 표시된 경우가 아니면 인증서 교환이 완료된 이후에 신뢰를 명시적으로 설정해야 합니다.

KMS를 신뢰하거나, KMS 인증서를 업로드하는 방법으로 신뢰 설정을 완료, 즉 vCenter Server가 KMS를 신뢰하도록 설정할 수 있습니다. 다음 두 가지 옵션 중에서 선택할 수 있습니다.

- **KMS 인증서 새로 고침** 옵션을 사용하여 인증서를 명시적으로 신뢰합니다.
- **KMS 인증서 업로드** 옵션을 사용하여 KMS 리프 인증서 또는 KMS CA 인증서를 vCenter Server에 업로드합니다.

참고 루트 CA 인증서 또는 중간 CA 인증서를 업로드하면 vCenter Server는 해당 CA에서 서명한 모든 인증서를 신뢰합니다. 보안을 강화하려면 KMS 벤더가 제어하는 리프 인증서나 중간 CA 인증서를 업로드해야 합니다.

프로시저

- 1 vSphere Web Client에 로그인하고 vCenter Server 시스템을 선택합니다.
- 2 구성을 클릭하고 **키 관리 서버**를 선택합니다.
- 3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

- 4 신뢰 관계를 설정하려면 KMS 인증서를 새로 고치거나 업로드합니다.

| 옵션 | 작업 |
|---------------|---|
| KMS 인증서 새로 고침 | a 모든 작업을 클릭하고 KMS 인증서 새로 고침 을 선택합니다. b 표시되는 대화상자에서 신뢰 를 클릭합니다. |
| KMS 인증서 업로드 | a 모든 작업을 클릭하고 KMS 인증서 업로드 를 선택합니다. b 표시되는 대화상자에서 파일 업로드 를 클릭하고 인증서 파일을 업로드한 후 확인 을 클릭합니다. |

새 vSAN 클러스터에서 암호화 사용

새 vSAN 클러스터를 구성할 때 암호화를 사용하도록 설정할 수 있습니다.

필수 조건

- 필요한 권한:
 - Host.Inventory.EditCluster
 - Cryptographer.ManageEncryptionPolicy
 - Cryptographer.ManageKMS
 - Cryptographer.ManageKeys
- KMS 클러스터가 설정되고 vCenter Server와 KMS 사이에 신뢰할 수 있는 연결이 설정되어 있어야 합니다.

프로시저

- 1 vSphere Web Client에서 기존 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택하고 **vSAN 구성** 버튼을 클릭합니다.
- 4 **vSAN 기능** 페이지에서 **암호화** 확인란을 선택하고 KMS 클러스터를 선택합니다.

참고 암호화하는 동안 스토리지 디바이스의 기존 데이터를 지우려는 경우가 아니면 **사용하기 전에 디스크 지우기** 확인란을 선택 취소했는지 확인합니다.

- 5 **디스크 할당** 페이지에서 vSAN 클러스터에 대해 할당할 디스크를 지정합니다.
 - a 용량으로 사용할 플래시 디바이스를 선택하고 **용량 계층에 대해 할당** 아이콘()을 클릭합니다.
 - b 캐시로 사용할 플래시 디바이스를 선택하고 **캐시 계층에 대해 할당** 아이콘()을 클릭합니다.
- 6 클러스터 구성을 완료합니다.

vSAN 클러스터에서 저장된 데이터 암호화 기능이 사용되도록 설정됩니다. vSAN은 vSAN 데이터스토어에 추가된 모든 데이터를 암호화합니다.

새 암호화 키 생성

키가 만료되거나 손상된 경우에 새 암호화 키를 생성할 수 있습니다.

vSAN 클러스터의 새 암호화 키를 생성할 때 다음과 같은 옵션을 사용할 수 있습니다.

- 새 KEK를 생성하면 vSAN 클러스터의 모든 호스트가 KMS로부터 새 KEK를 받습니다. 각 호스트의 DEK는 새 KEK를 사용하여 다시 암호화됩니다.
- 새 키를 사용하여 모든 데이터를 다시 암호화하도록 선택하면 새 KEK와 새 DEK가 생성됩니다. 데이터를 다시 암호화하려면 롤링 디스크 다시 포맷을 수행해야 합니다.

필수 조건

- 필요한 권한:
 - **Host.Inventory.EditCluster**
 - **Cryptographer.ManageKeys**
- KMS 클러스터가 설정되고 vCenter Server와 KMS 사이에 신뢰할 수 있는 연결이 설정되어 있어야 합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 호스트 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택합니다.
- 4 [vSAN 켜짐] 창에서 **새 암호화 키 생성** 버튼을 클릭합니다.
- 5 새 KEK를 생성하려면 **확인**을 클릭합니다. 새 KEK를 사용하여 DEK가 다시 암호화됩니다.
 - 새 KEK와 새 DEK를 생성하고 vSAN 클러스터의 모든 데이터를 다시 암호화하려면 **새 키를 사용하여 스토리지의 모든 데이터도 다시 암호화** 확인란을 선택합니다.
 - vSAN 클러스터에 제한된 리소스가 있으면 **감소된 이중화 허용** 확인란을 선택합니다. 감소된 이중화를 허용하면 디스크를 다시 포맷하는 작업 중에 데이터가 위협할 수 있습니다.

기존 vSAN 클러스터에서 vSAN 암호화 사용

기존 vSAN 클러스터의 구성 매개 변수를 편집하여 암호화를 사용하도록 설정할 수 있습니다.

필수 조건

- 필요한 권한:
 - **Host.Inventory.EditCluster**
 - **Cryptographer.ManageEncryptionPolicy**
 - **Cryptographer.ManageKMS**
 - **Cryptographer.ManageKeys**
- KMS 클러스터가 설정되고 vCenter Server와 KMS 사이에 신뢰할 수 있는 연결이 설정되어 있어야 합니다.
- 클러스터의 디스크 할당 모드를 수동 모드로 설정해야 합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 호스트 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **일반**을 선택합니다.
- 4 [vSAN 켜짐] 창에서 **편집** 버튼을 클릭합니다.
- 5 [vSAN 설정 편집] 대화상자에서 **암호화** 확인란을 선택하고 KMS 클러스터를 선택합니다.
- 6 (선택 사항) 클러스터의 스토리지 디바이스에 중요한 데이터가 포함된 경우, **사용하기 전에 디스크 지우기** 확인란을 선택합니다.

이 설정은 암호화하는 동안 스토리지 디바이스의 기존 데이터를 지우도록 vSAN에 지시합니다.
- 7 **확인**을 클릭합니다.

vSAN이 vSAN 데이터스토어의 모든 데이터를 암호화할 때 모든 디스크 그룹의 롤링 다시 포맷이 수행됩니다.

vSAN 암호화 및 코어 덤프

vSAN 클러스터에서 암호화를 사용하는 경우 ESXi 호스트에 오류가 발생하면 고객 데이터를 보호하기 위해 결과 코어 덤프가 암호화됩니다. vm-support 패키지에 포함되어 있는 코어 덤프도 함께 암호화됩니다.

참고 코어 덤프에는 중요한 정보가 포함될 수 있습니다. 코어 덤프를 처리할 때는 조직의 데이터 보호 및 개인 정보 보호 정책을 따르십시오.

ESXi 호스트의 코어 덤프

ESXi 호스트가 충돌하면 암호화된 코어 덤프가 생성되고 호스트가 재부팅됩니다. 코어 덤프는 ESXi 키 캐시에 있는 호스트 키를 사용하여 암호화됩니다. 다음으로 수행할 수 있는 작업은 여러 가지 요소에 따라 달라집니다.

- 대부분의 경우 vCenter Server는 KMS에서 호스트의 키를 검색하고, 재부팅 후 ESXi 호스트에 키를 푸시합니다. 작업이 성공하면 vm-support 패키지를 생성하고 코어 덤프를 암호 해독하거나 다시 암호화할 수 있습니다.
- vCenter Server가 ESXi 호스트에 연결할 수 없는 경우, KMS에서 키를 검색할 수 있습니다.
- 호스트에서 사용자 지정 키를 사용했고 이 키가 vCenter Server에서 호스트에 푸시한 키와 다르다면 코어 덤프를 조작할 수 없습니다. 사용자 지정 키를 사용하지 않도록 하십시오.

코어 덤프 및 vm-support 패키지

심각한 오류로 인해 VMware 기술 지원에 문의할 경우 지원 담당자는 대개 vm-support 패키지를 생성하도록 요청합니다. 이 패키지에는 로그 파일과 코어 덤프를 비롯한 기타 정보가 포함되어 있습니다. 지원 담당자가 로그 파일과 기타 정보를 확인하고도 문제를 해결할 수 없는 경우 관련 정보를 사용할 수 있도록 코어 덤프의 암호를 해독할 수 있습니다. 조직의 보안 및 개인 정보 보호 정책을 따라 호스트 키와 같은 중요한 정보를 보호하십시오.

vCenter Server 시스템의 코어 덤프

vCenter Server 시스템의 코어 덤프는 암호화되지 않습니다. vCenter Server에는 이미 잠재적으로 중요한 정보가 포함되어 있습니다. 최소한 vCenter Server가 실행되는 Windows 시스템 또는 vCenter Server Appliance는 보호되도록 해야 합니다. vCenter Server 시스템에 대한 코어 덤프를 해제하는 것을 고려할 수도 있습니다. 로그 파일의 기타 정보를 통해 문제를 파악할 수도 있습니다.

암호화된 vSAN 클러스터의 ESXi 호스트에 대해 vm-support 패키지 수집

vSAN 클러스터에서 암호화가 사용되도록 설정되면 vm-support 패키지의 모든 코어 덤프가 암호화됩니다. vSphere Web Client에서 패키지를 수집할 수 있으며, 나중에 코어 덤프를 암호 해독하려는 경우에는 암호를 지정할 수 있습니다.

vm-support 패키지에는 로그 파일, 코어 덤프 파일 등이 포함되어 있습니다.

필수 조건

vSAN 클러스터에 대해 암호화가 사용되도록 설정되었음을 지원 담당자에게 알립니다. 관련 정보를 추출하기 위해 코어 덤프를 암호 해독하도록 지원 담당자가 요청할 수 있습니다.

참고 코어 덤프에는 중요한 정보가 포함될 수 있습니다. 조직의 보안 및 개인 정보 보호 정책을 따라 호스트 키와 같은 중요한 정보를 보호하십시오.

프로시저

- 1 vSphere Web Client를 사용하여 vCenter Server에 로그인합니다.
- 2 **호스트 및 클러스터**를 클릭하고 ESXi 호스트를 마우스 오른쪽 버튼으로 클릭합니다.
- 3 **시스템 로그 내보내기**를 선택합니다.
- 4 대화상자에서 **암호화된 코어 덤프에 대한 암호**를 선택하고 암호를 지정한 후 확인합니다.
- 5 다른 옵션의 경우 기본값을 그대로 사용하거나 VMware 기술 지원에서 요청한 대로 변경한 후 **마침**을 클릭합니다.
- 6 파일의 위치를 지정합니다.
- 7 지원 담당자가 vm-support 패키지의 코어 덤프를 암호 해독하라고 요청한 경우, 임의의 ESXi 호스트에 로그인하여 다음 단계를 수행합니다.
 - a ESXi에 로그인하여 vm-support 패키지가 있는 디렉토리에 연결합니다.
파일 이름은 **esx.date_and_time.tgz**와 같은 패킷입니다.
 - b 패키지, 압축 해제된 패키지 및 다시 압축된 패키지를 저장할 수 있을 정도로 디렉토리의 공간이 충분한지 확인합니다. 공간이 부족한 경우 다른 디렉토리로 패키지를 이동합니다.
 - c 패키지를 로컬 디렉토리에 추출합니다.

```
vm-support -x *.tgz .
```


추출 후 생성되는 파일 계층에는 ESXi 호스트의 코어 덤프 파일이 /var/core에 포함될 수 있으며, 가상 시스템의 코어 덤프 파일이 여러 개 포함될 수 있습니다.
 - d 암호화된 각 코어 덤프 파일을 개별적으로 암호 해독합니다.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file --password encryptedZdump decryptedZdump
```


vm-support-incident-key-file은 디렉토리의 최상위 수준에 있는 인시던트 키 파일입니다.
encryptedZdump는 암호화된 코어 덤프 파일의 이름입니다.
decryptedZdump는 명령을 통해 생성되는 파일의 이름입니다. 이름을 encryptedZdump 이름과 비슷하게 지정합니다.
 - e vm-support 패키지를 생성할 때 지정한 암호를 제공합니다.
 - f 암호화된 코어 덤프를 제거하고, 패키지를 다시 압축합니다.

```
vm-support --reconstruct
```
- 8 기밀 정보가 포함된 모든 파일을 제거합니다.

암호화된 코어 덤프 암호 해독 또는 다시 암호화

crypto-util CLI를 사용하여 ESXi 호스트에서 암호화된 코어 덤프를 암호 해독하고 다시 암호화할 수 있습니다.

vm-support 패키지에 있는 코어 덤프를 직접 암호 해독하고 검사할 수 있습니다. 코어 덤프에는 중요한 정보가 포함될 수 있습니다. 조직의 보안 및 개인 정보 보호 정책을 따라 호스트 키와 같은 중요한 정보를 보호하십시오.

코어 덤프를 다시 암호화하는 기능 및 crypto-util의 다른 기능에 대한 자세한 내용은 명령줄 도움말을 참조하십시오.

참고 crypto-util은 고급 사용자를 위한 기능입니다.

필수 조건

코어 덤프를 생성한 ESXi 호스트에서 코어 덤프를 암호화하는 데 사용된 ESXi 호스트 키를 사용할 수 있어야 합니다.

프로시저

- 1 코어 덤프가 생성된 ESXi 호스트에 직접 로그인합니다.

ESXi 호스트가 잠금 모드에 있거나 SSH 액세스가 사용되지 않도록 설정되어 있는 경우에는 먼저 액세스가 가능하도록 설정해야 할 수 있습니다.

- 2 코어 덤프가 암호화되었는지 여부를 확인합니다.

| 옵션 | 설명 |
|------------|---|
| 코어 덤프 모니터링 | <code>crypto-util envelope describe vmmcores.ve</code> |
| zdump 파일 | <code>crypto-util envelope describe --offset 4096 <i>zdumpFile</i></code> |

- 3 코어 덤프 유형에 따라 코어 덤프를 암호 해독합니다.

| 옵션 | 설명 |
|------------|---|
| 코어 덤프 모니터링 | <code>crypto-util envelope extract vmmcores.ve vmmcores</code> |
| zdump 파일 | <code>crypto-util envelope extract --offset 4096 <i>zdumpEncrypted</i> <i>zdumpUnencrypted</i></code> |

vSAN 클러스터 업그레이드

vSAN 업그레이드는 여기에서 설명하는 순서대로 업그레이드 절차를 수행해야 하는 다단계 프로세스입니다.

업그레이드를 시도하기 전에 원활하고 중단 없는 업그레이드를 위해 전체 업그레이드 프로세스를 확실하게 이해해야 합니다. 일반 vSphere 업그레이드 절차에 익숙하지 않은 경우에는 먼저 vSphere 업그레이드 설명서를 살펴보아야 합니다.

참고 여기에서 설명하는 업그레이드 작업 순서를 따르지 않으면 데이터 손실 및 클러스터 장애가 발생할 수 있습니다.

vSAN 클러스터 업그레이드는 다음과 같은 작업 순서로 진행됩니다.

- 1 vCenter Server를 업그레이드합니다. 자세한 내용은 vSphere 업그레이드 설명서를 참조하십시오.
- 2 ESXi 호스트를 업그레이드합니다. [“ESXi 호스트 업그레이드,”](#) (89 페이지)를 참조하십시오. 업그레이드를 위해 ESXi 호스트를 준비 및 마이그레이션하는 방법에 대해서는 vSphere 업그레이드 설명서를 참조하십시오.
- 3 vSAN 디스크 형식을 업그레이드합니다. 디스크 형식 업그레이드는 선택 사항이지만 최상의 결과를 얻으려면 최신 버전을 사용하도록 개체를 업그레이드하십시오. 온디스크 형식을 사용하면 환경에서 vSAN의 전체 기능 세트를 활용할 수 있습니다. [“RVC를 사용하여 vSAN 디스크 형식 업그레이드,”](#) (94 페이지)를 참조하십시오.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN을 업그레이드하기 전,”](#) (88 페이지)
- [“vCenter Server 업그레이드,”](#) (89 페이지)
- [“ESXi 호스트 업그레이드,”](#) (89 페이지)
- [“vSAN 디스크 형식 정보,”](#) (91 페이지)
- [“vSAN 클러스터 업그레이드 확인,”](#) (95 페이지)
- [“RVC 업그레이드 명령 옵션 사용,”](#) (96 페이지)
- [“vSphere Update Manager에 대한 vSAN 빌드 권장 사항,”](#) (96 페이지)

vSAN 을 업그레이드하기 전

오류 보호를 위해 업그레이드를 계획하고 설계합니다. vSAN 업그레이드를 시도하기 전에 해당 환경이 vSphere 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인합니다.

업그레이드 사전 요구 사항

전반적인 업그레이드 프로세스를 지연시킬 수 있는 측면을 고려합니다. 지침과 모범 사례는 vSphere 업그레이드 설명서를 참조하십시오.

클러스터를 vSAN 6.6으로 업그레이드하기 전에 주요 요구 사항을 검토합니다.

표 9-1. 업그레이드 사전 요구 사항

| 업그레이드 전제 조건 | 설명 |
|--|--|
| 소프트웨어, 하드웨어, 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러 | 사용하려는 소프트웨어 및 하드웨어 구성 요소, 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러가 vSAN 6.6 이상에서 지원되는지 그리고 이러한 항목이 VMware 호환성 가이드 웹 사이트 (http://www.vmware.com/resources/compatibility/search.php)에 나열되어 있는지 확인합니다. |
| vSAN 버전 | 최신 버전의 vSAN을 사용하고 있는지 확인합니다. 현재 베타 버전을 실행 중인 경우 vSAN을 6.6으로 업그레이드하려고 하면 업그레이드가 실패합니다. 베타 버전에서 업그레이드하는 경우 vSAN을 새로 배포해야 합니다. |
| 디스크 공간 | 소프트웨어 버전 업그레이드를 완료할 수 있는 충분한 공간이 있는지 확인합니다. vCenter Server 설치에 필요한 디스크 스토리지 양은 vCenter Server 구성에 따라 다릅니다. vSphere 업그레이드에 필요한 디스크 공간에 대한 지침은 vSphere 업그레이드 설명서를 참조하십시오. |
| vSAN 디스크 형식 | 디스크 형식을 업그레이드하는 데 사용할 수 있는 용량이 충분한지 확인합니다. 사용 가능한 공간이 가장 큰 디스크 그룹의 사용 용량만큼 높고, 사용 가능한 공간이 변환될 디스크 그룹 외의 디스크 그룹에 있는 경우에는 데이터 마이그레이션 옵션으로 감소된 이중화 허용 을 선택해야 합니다. 예를 들어 클러스터의 가장 큰 디스크 그룹에 10TB의 물리적 용량이 있고 단 5TB만 사용되고 있는 경우 마이그레이션되고 있는 디스크 그룹을 제외한 클러스터의 다른 곳에서 5TB의 추가 여유 용량이 필요합니다. vSAN 디스크 형식을 업그레이드할 때 호스트가 유지 보수 모드에 있지는 않은지 확인합니다. vSAN 클러스터의 멤버 호스트가 유지 보수 모드로 전환되면 멤버 호스트가 더 이상 클러스터에 스토리지를 제공하지 않고 호스트의 용량을 데이터에 사용할 수 없기 때문에 클러스터 용량이 자동으로 줄어듭니다. 다양한 제거 모드에 대한 자세한 내용은 "vSAN 클러스터의 멤버를 유지 보수 모드로 전환," (112 페이지) 항목을 참조하십시오. |
| vSAN 호스트 | vSAN 호스트를 유지 보수 모드로 설정했고 데이터 액세스 지원 보장 또는 모든 데이터 제거 옵션을 선택했는지 확인합니다. vSphere Update Manager를 사용하여 업그레이드 프로세스를 자동화하고 테스트할 수 있습니다. 하지만 vSphere Update Manager를 사용하여 vSAN을 업그레이드하는 경우에는 기본 제거 모드가 데이터 액세스 지원 보장 입니다. 데이터 액세스 지원 보장 모드를 사용하면 데이터가 완전하게 보호되지 않으며, vSAN을 업그레이드하는 동안 장애가 발생할 경우 예기치 않은 데이터 손실이 발생할 수 있습니다. 하지만 데이터 액세스 지원 보장 모드의 경우 모든 데이터를 클러스터의 다른 호스트로 이동할 필요가 없기 때문에 모든 데이터 제거 모드보다 속도가 더 빠릅니다. 다양한 제거 모드에 대한 자세한 내용은 "vSAN 클러스터의 멤버를 유지 보수 모드로 전환," (112 페이지) 항목을 참조하십시오. |
| 가상 시스템 | 가상 시스템을 백업했는지 확인합니다. |

권장 사항

vSAN에서 사용하도록 ESXi 호스트를 배포할 때 다음 권장 사항을 고려합니다.

- ESXi 호스트의 메모리 용량이 512GB 이하로 구성되어 있으면 SATADOM, SD, USB 또는 하드 디스크 디바이스를 설치 미디어로 사용합니다.
- ESXi 호스트의 메모리 용량이 512GB보다 크게 구성되어 있으면 별도의 자기 디스크나 플래시 디바이스를 설치 디바이스로 사용합니다. 별도의 디바이스를 사용 중인 경우에는 vSAN에서 해당 디바이스를 할당하지 않는지 확인합니다.
- SATADOM 디바이스에서 vSAN 호스트를 부팅하는 경우 SLC(단일 수준 셀) 디바이스를 사용하여 하며 부팅 디바이스의 크기가 16GB 이상이어야 합니다.

vSAN 6.5 이상에서는 vSAN 클러스터의 ESXi 호스트에 대한 부팅 크기 요구 사항을 조정할 수 있습니다. 자세한 내용은 <http://kb.vmware.com/kb/2147881>에서 VMware 기술 자료 문서를 참조하십시오.

2개 호스트 클러스터 또는 확장된 클러스터의 감시 호스트 업그레이드

2개 호스트 클러스터 또는 확장된 클러스터의 감시 호스트는 vSAN 클러스터 외부에 있지만 동일한 vCenter Server에 의해 관리됩니다. vSAN 데이터 호스트를 업그레이드할 때와 동일한 프로세스를 사용하여 감시 호스트를 업그레이드할 수 있습니다.

모든 데이터 호스트가 업그레이드되고 유지 보수 모드가 종료되기 전까지 감시 호스트를 업그레이드하지 마십시오.

vSphere Update Manager를 사용하여 호스트를 동시에 업그레이드하면 감시 호스트가 데이터 호스트 중 하나와 동시에 업그레이드될 수 있습니다. 업그레이드 문제를 방지하려면 감시 호스트를 데이터 호스트와 동시에 업그레이드하지 않도록 vSphere Update Manager를 구성하십시오.

vCenter Server 업그레이드

vSAN 업그레이드 중 가장 먼저 수행해야 할 작업은 vCenter Server 및 ESXi 호스트 업그레이드를 포함하는 일반 vSphere 업그레이드입니다.

VMware는 64비트 시스템에서 vCenter Server 4.x, vCenter Server 5.0.x, vCenter Server 5.1.x 및 vCenter Server 5.5를 vCenter Server 6.0 이상으로 인플레이스 업그레이드할 수 있도록 지원합니다. vCenter Server 업그레이드에는 데이터베이스 스키마 업그레이드와 vCenter Server 업그레이드가 포함됩니다. vCenter Server에 인플레이스 업그레이드를 수행하지 않고 업그레이드에 다른 시스템을 사용할 수 있습니다. 자세한 지침 및 다양한 업그레이드 옵션은 vSphere 업그레이드 설명서를 참조하십시오.

ESXi 호스트 업그레이드

vCenter Server를 업그레이드한 후 vSAN 클러스터 업그레이드의 다음 작업은 ESXi 호스트를 최신 버전으로 업그레이드하는 것입니다.

vSAN 클러스터에 호스트가 여러 개 있고 vSphere Update Manager를 사용하여 호스트를 업그레이드하는 경우 기본 제거 모드는 **데이터 액세스 지원 보장**입니다. 이 모드를 사용하는 경우에는 vSAN 업그레이드 중 장애가 발생하면 데이터가 위협해집니다. 제거 모드 사용에 대한 자세한 내용은 **“vSAN 클러스터의 멤버를 유지 보수 모드로 전환,”** (112 페이지) 항목을 참조하십시오.

vSphere Update Manager 사용에 대한 자세한 내용은 설명서 웹 사이트 (https://www.vmware.com/support/pubs/vum_pubs.html)를 참조하십시오.

ESXi 호스트의 업그레이드를 시도하기 전에 vSphere 업그레이드 설명서에서 설명하는 모범 사례를 검토하십시오. VMware는 몇 가지 ESXi 업그레이드 옵션을 제공합니다. 업그레이드할 호스트의 유형에 가장 적합한 업그레이드 옵션을 선택하십시오. 여러 업그레이드 옵션에 대한 자세한 내용은 vSphere 업그레이드 설명서를 참조하십시오.

필수 조건

- ESXi 호스트를 업그레이드하는 데 충분한 디스크 공간이 있는지 확인합니다. 디스크 공간 요구 사항에 대한 지침은 vSphere 업그레이드 설명서를 참조하십시오.
- 최신 버전의 ESXi를 사용하고 있는지 확인합니다. 최신 ESXi 설치 관리자는 VMware 제품 다운로드 웹 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 다운로드할 수 있습니다.
- 최신 버전의 vCenter Server를 사용하고 있는지 확인합니다.
- 네트워크 구성, 스토리지 I/O 컨트롤러, 스토리지 디바이스 및 백업 소프트웨어의 호환성을 확인합니다.
- 가상 시스템을 백업했는지 확인합니다.
- 업그레이드 동안 가상 시스템 다운타임을 생기지 않도록 DRS(Distributed Resource Scheduler)를 사용합니다. 호스트가 유지 보수 모드로 전환될 때 DRS가 가상 시스템을 마이그레이션하는 데 도움이 되도록 각 가상 시스템의 자동화 수준이 **완전 자동화됨** 모드로 설정되어 있는지 확인합니다. 또는 모든 가상 시스템의 전원을 끄거나 수동 마이그레이션을 수행할 수도 있습니다.

프로시저

- 1 업그레이드할 호스트를 유지 보수 모드로 전환합니다.

vSAN 클러스터의 ESXi 5.5 이상 호스트에서 업그레이드 경로를 시작해야 합니다.

- a vSphere Web Client 탐색기에서 호스트를 마우스 오른쪽 버튼으로 클릭하고 **유지 보수 모드 > 유지 보수 모드 설정**을 선택합니다.
- b 요구 사항에 따라 **데이터 액세스 지원 보장** 또는 **모든 데이터 제거** 제거 모드를 선택하고 호스트가 유지 보수 모드로 전환될 때까지 기다립니다.

vSphere Update Manager를 사용하여 호스트를 업그레이드하는 경우나 호스트가 3개인 클러스터를 사용 중인 경우에 사용할 수 있는 기본 제거 모드는 **데이터 액세스 지원 보장**입니다. 이 모드는 **모든 데이터 제거** 모드보다 빠릅니다. 하지만 **데이터 액세스 지원 보장** 모드는 데이터를 완벽하게 보호하지 않습니다. 장애 도중 데이터가 위협해질 수 있으며 다운타임 및 예기치 않은 데이터 손실이 발생할 수 있습니다.

- 2 소프트웨어를 ESXi 호스트의 데이터스토어에 업로드하고 데이터스토어 내 디렉토리에서 파일을 사용할 수 있는지 확인합니다. 예를 들어 소프트웨어를 /vmfs/volumes/<datastore>/VMware-ESXi-6.0.0-1921158-depot.zip로 업로드할 수 있습니다.
- 3 esxcli 명령 `install -d /vmfs/volumes/53b536fd-34123144-8531-00505682e44d/depot/VMware-ESXi-6.0.0-1921158-depot.zip --no-sig-check`를 실행합니다. 이 명령은 esxcli 소프트웨어 VIB를 사용하여 실행하십시오.

ESXi 호스트가 설치되면 다음 메시지가 표시됩니다.

업데이트가 성공적으로 완료되었지만 변경 내용을 적용하려면 시스템을 재부팅해야 합니다.

- 4 vSphere Web Client에서 ESXi를 수동으로 다시 시작해야 합니다.
 - a vSphere Web Client 인벤토리에서 ESXi 호스트로 이동합니다.
 - b 호스트를 마우스 오른쪽 버튼으로 클릭하고 **전원 > 재부팅**을 선택한 후 **예**를 클릭하여 확인한 다음 호스트가 다시 시작될 때까지 기다립니다.
 - c 호스트를 마우스 오른쪽 버튼으로 클릭하고 **연결 > 연결 끊기**를 선택한 다음 **연결 > 연결**을 선택하여 호스트에 다시 연결합니다.

클러스터의 나머지 호스트를 업그레이드하려면 각 호스트에 대해 이 절차를 반복합니다.

vSAN 클러스터에 여러 호스트가 있는 경우에는 vSphere Update Manager를 사용하여 나머지 호스트를 업그레이드할 수 있습니다.

5 유지 보수 모드를 종료합니다.

후속 작업

- (선택 사항) vSAN 디스크 형식을 업그레이드합니다. [“RVC를 사용하여 vSAN 디스크 형식 업그레이드,”](#) (94 페이지)를 참조하십시오.
- 호스트 라이선스를 확인합니다. 대개의 경우 호스트 라이선스를 다시 적용해야 합니다. vSphere Web Client 및 vCenter Server를 사용하여 호스트 라이선스를 적용할 수 있습니다. 호스트 라이선스 적용에 대한 자세한 내용은 vCenter Server 및 호스트 관리 설명서를 참조하십시오.
- (선택 사항) vSphere Web Client 또는 vSphere Update Manager를 사용하여 호스트에서 가상 시스템을 업그레이드합니다.

vSAN 디스크 형식 정보

디스크 형식 업그레이드는 선택 사항입니다. 이전 디스크 형식 버전을 사용하는 경우에도 vSAN 클러스터가 원활하게 실행됩니다.

최상의 결과를 얻으려면 최신 온디스크 형식을 사용하도록 개체를 업그레이드하십시오. 최신 온디스크 형식은 vSAN의 전체 기능 세트를 제공합니다.

디스크 그룹은 한 번에 하나씩 업그레이드되기 때문에 디스크 그룹의 크기에 따라 디스크 형식 업그레이드에 시간이 많이 소요될 수 있습니다. 각 디스크 그룹 업그레이드 과정에서는 각 디바이스에서 모든 데이터가 제거되고 해당 디스크 그룹이 vSAN 클러스터에서 제거됩니다. 그런 다음 디스크 그룹이 새로운 온디스크 형식으로 vSAN에 다시 추가됩니다.

참고 온디스크 형식을 업그레이드한 후에는 호스트에서 소프트웨어를 롤백하거나 클러스터에 특정 이전 호스트를 추가할 수 없습니다.

온디스크 형식의 업그레이드를 시작하면 vSAN은 [구성 요소 다시 동기화] 페이지에서 사용자가 모니터링할 수 있는 몇 가지 작업을 수행합니다. 다음 표에는 디스크 형식을 업그레이드하는 동안 수행되는 각 프로세스가 요약되어 있습니다.

표 9-2. 업그레이드 프로세스

| 완료율 | 설명 |
|---------|---|
| 0%~5% | 클러스터 검사. 업그레이드를 위해 클러스터 구성 요소를 검사하고 준비합니다. 이 프로세스는 몇 분 정도 소요됩니다. vSAN이 업그레이드가 완료되는 것을 방지할 수 있는 미결 문제가 없음을 확인합니다. <ul style="list-style-type: none"> ■ 모든 호스트가 연결되었습니다. ■ 모든 호스트가 올바른 소프트웨어 버전을 사용합니다. ■ 모든 디스크가 정상 상태입니다. ■ 모든 개체가 액세스 가능합니다. |
| 5%~10% | 디스크 그룹 업그레이드. vSAN이 데이터 마이그레이션 없이 초기 디스크 업그레이드를 수행합니다. 이 프로세스는 몇 분 정도 소요됩니다. |
| 10%~15% | 개체 다시 정렬. vSAN이 모든 개체의 레이아웃을 수정하여 올바르게 정렬합니다. 이 프로세스는 스냅샷이 많지 않은 소규모 시스템의 경우 몇 분 정도 소요될 수 있습니다. 스냅샷, 조각화된 쓰기 및 정렬되지 않은 개체가 많은 대규모 시스템의 경우에는 이 프로세스가 몇 시간에서 며칠까지 소요될 수 있습니다. |

표 9-2. 업그레이드 프로세스 (계속)

| 완료율 | 설명 |
|------------|--|
| 15% - 95% | 디스크 그룹 제거 및 다시 포맷. 각 디스크 그룹이 클러스터에서 제거되고, 다시 포맷된 후 클러스터에 다시 추가됩니다. 이 프로세스에 소요되는 시간은 할당된 메가바이트 및 시스템 로드와 따라 다릅니다. I/O 용량에 도달하거나 거의 도달한 시스템에서는 전송 속도가 저하됩니다. |
| 95% - 100% | 최종 개체 버전 업그레이드. 새로운 온디스크 형식으로서의 개체 변환과 다시 동기화가 완료됩니다. 이 프로세스에 소요되는 시간은 사용된 공간의 양 및 감소된 이중화 허용 옵션을 선택했는지 여부에 따라 다릅니다. |

업그레이드를 수행하는 동안 vSphere Web Client에서 [구성 요소 다시 동기화] 페이지로 이동하여 업그레이드 프로세스를 모니터링할 수 있습니다. **“vSAN 클러스터의 다시 동기화 작업 모니터링,”** (134 페이지)를 참조하십시오. RVC `vsan.upgrade_status <cluster>` 명령을 사용하여 업그레이드를 모니터링할 수도 있습니다. 선택 사항인 `-r <seconds>` 플래그를 사용하면 Ctrl+C를 누를 때까지 업그레이드 상태를 주기적으로 새로 고칠 수 있습니다. 새로 고침 사이의 최소 간격은 60초입니다.

디바이스 제거 및 업그레이드와 같은 기타 업그레이드 작업을 vSphere Web Client 상태 표시줄의 최근 태스크 창에서 모니터링할 수 있습니다.

디스크 형식을 업그레이드할 때 다음 고려 사항이 적용됩니다.

- 호스트가 3개인 클러스터를 업그레이드할 때 전체 제거를 수행하려는 경우, **허용할 수 있는 장애의 기본 수준**이 0보다 큰 개체에 대해서는 제거가 실패합니다. 호스트가 3개인 클러스터는 전체 제거되는 디스크 그룹을 호스트 두 개의 리소스만 사용하여 다시 보호할 수 없습니다. 예를 들어 **허용할 수 있는 장애의 기본 수준**이 1로 설정된 경우, vSAN에는 보호 구성 요소 3개(미러 2개와 감시 1개)가 필요하며, 각 보호 구성 요소는 개별 호스트에 배치됩니다.

호스트가 3개인 클러스터에 대해서는 **데이터 액세스 지원 보장** 제거 모드를 선택해야 합니다. 이 모드에서는 하드웨어 장애가 발생하는 경우 데이터가 손실될 수 있습니다.

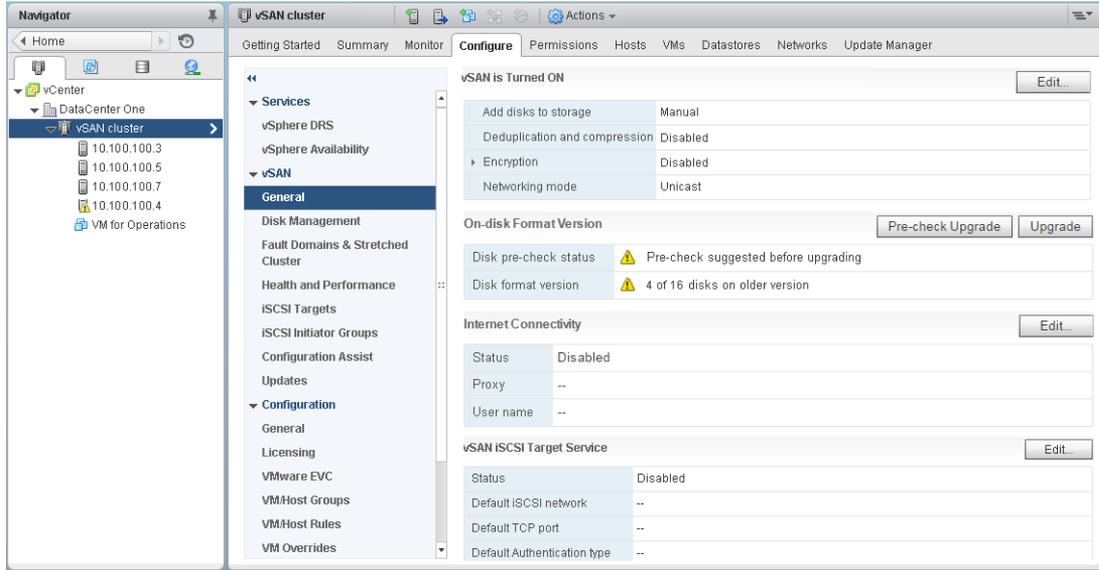
또한 사용 가능한 공간이 충분한지 확인해야 합니다. 공간은 가장 큰 디스크 그룹의 논리적 사용 용량과 동일해야 하며, 이 용량은 마이그레이션 중인 디스크 그룹이 아닌 다른 디스크 그룹에 있어야 합니다.

- 호스트가 3개인 클러스터를 업그레이드하거나 리소스가 제한된 클러스터를 업그레이드하는 경우에는 가상 시스템이 감소된 이중화 모드에서 작동하도록 허용합니다. `vsan.ondisk_upgrade --allow-reduced-redundancy` 옵션과 함께 RVC 명령을 실행합니다.
- `--allow-reduced-redundancy` 명령 옵션을 사용하면 특정 가상 시스템이 마이그레이션 중에 장애를 허용하지 못할 수 있습니다. 이와 같은 장애 허용 수준 감소도 데이터 손실을 유발할 수 있습니다. vSAN은 업그레이드 완료 후 전체 규정 준수 및 이중화를 복원합니다. 업그레이드 중에는 가상 시스템의 규정 준수 상태 및 해당 이중화가 일시적으로 비준수 상태가 됩니다. 업그레이드를 완료하고 재구축 작업을 모두 마치고 나면 가상 시스템이 준수 상태가 됩니다.
- 업그레이드가 진행 중일 때는 호스트를 제거하거나 연결을 끊지 않아야 하며 호스트를 유지 보수 모드로 두면 안 됩니다. 이로 인해 업그레이드가 실패할 수 있습니다.

RVC 명령 및 명령 옵션에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.

vSphere Web Client 를 사용하여 vSAN 디스크 형식 업그레이드

vSAN 호스트 업그레이드를 마친 후에는 디스크 형식 업그레이드를 수행할 수 있습니다.



참고 기존 vSAN 클러스터에서 암호화 또는 중복 제거와 압축을 사용하도록 설정하면 온디스크 형식이 최신 버전으로 자동 업그레이드됩니다. 따라서 이 절차는 필요하지 않습니다. 디스크 그룹 다시 포맷을 두 번 수행하는 것을 방지할 수 있습니다. “vSAN 설정 편집,” (48 페이지)를 참조하십시오.

필수 조건

- 업데이트된 버전의 vCenter Server를 사용 중인지 확인합니다.
- 최신 버전의 ESXi 호스트를 사용하고 있는지 확인합니다.
- 디스크가 정상 상태인지 확인합니다. vSphere Web Client의 [디스크 관리] 페이지로 이동하여 개체 상태를 확인합니다.
- 사용하려는 하드웨어와 소프트웨어가 인증되었으며 VMware 호환성 가이드 웹 사이트 (<http://www.vmware.com/resources/compatibility/search.php>)에 나열되어 있는지 확인합니다.
- 디스크 형식 업그레이드를 수행할 사용 가능한 공간이 충분한지 확인합니다. RVC 명령 `vsan.whatif_host_failures`를 실행하여, 업그레이드를 완료할 용량이 충분한지 또는 업그레이드 중에 장애가 발생했을 때 구성 요소 재구축을 수행할 용량이 충분한지 확인합니다.
- 호스트가 유지 보수 모드로 설정되지 않았는지 확인합니다. 디스크 형식을 업그레이드할 때는 호스트를 유지 보수 모드로 전환하지 않아야 합니다. vSAN 클러스터의 멤버 호스트가 유지 보수 모드로 전환되면 해당 멤버 호스트가 더 이상 클러스터에 용량을 제공하지 않으므로 클러스터의 사용 가능한 리소스 용량이 줄어듭니다. 따라서 클러스터 업그레이드가 실패할 수 있습니다.
- 현재 vSAN 클러스터에서 진행 중인 구성 요소 재구축 작업이 없는지 확인합니다. “vSAN 클러스터의 다시 동기화 작업 모니터링,” (134 페이지)를 참조하십시오.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 구성 탭을 클릭합니다.
- 3 vSAN에서 일반을 선택합니다.

- 4 (선택 사항) 온디스크 형식 버전에서 **업그레이드 사전 점검**을 클릭합니다.

업그레이드 사전 점검에서 클러스터를 분석하여 성공적인 업그레이드를 방해할 수 있는 문제를 찾아냅니다. 점검되는 일부 항목은 호스트 상태, 디스크 상태, 네트워크 상태 및 개체 상태입니다. **디스크 사전 검사 상태** 텍스트 상자에 업그레이드 문제가 표시됩니다.

- 5 온디스크 형식 버전에서 **업그레이드**를 클릭합니다.

- 6 [업그레이드] 대화상자에서 **예**를 클릭하여 온디스크 형식 업그레이드를 수행합니다.

vSAN이 클러스터에 있는 각 디스크 그룹에 대해 롤링 재부팅을 수행합니다. 클러스터에 있는 스토리지 디바이스의 디스크 형식 버전이 [온디스크 형식 버전] 옆에 표시됩니다. 오래된 버전이 있는 디스크 옆에는 새 형식을 사용하는 디바이스의 개수가 표시됩니다. 업그레이드가 완료되면 오래된 버전이 있는 디스크가 0이 됩니다.

업그레이드 중에 장애가 발생하면 vSphere Web Client의 [구성 요소 다시 동기화] 페이지를 확인할 수 있습니다. 다시 동기화가 모두 완료될 때까지 기다렸다가 업그레이드를 다시 실행합니다. 상태 서비스를 사용하여 클러스터 상태를 확인할 수도 있습니다. 상태 점검을 통해 확인된 모든 문제를 해결한 후 업그레이드를 다시 실행할 수 있습니다.

RVC를 사용하여 vSAN 디스크 형식 업그레이드

vSAN 호스트의 업그레이드를 마친 후에는 RVC(Ruby vSphere Console)를 사용하여 디스크 형식 업그레이드를 계속할 수 있습니다.

필수 조건

- 업데이트된 버전의 vCenter Server를 사용 중인지 확인합니다.
- vSAN 클러스터에서 실행되고 있는 ESXi 호스트의 버전이 6.5 이상인지 확인합니다.
- vSphere Web Client의 [디스크 관리] 페이지에서 디스크가 정상 상태인지 확인합니다. `vsan.disk_stats` RVC 명령을 실행하여 디스크 상태를 확인할 수도 있습니다.
- 사용하려는 하드웨어와 소프트웨어가 인증되었으며 VMware 호환성 가이드 웹 사이트 (<http://www.vmware.com/resources/compatibility/search.php>)에 나열되어 있는지 확인합니다.
- 디스크 형식 업그레이드를 수행할 사용 가능한 공간이 충분한지 확인합니다. RVC `vsan.whatif_host_failures` 명령을 실행하여, 업그레이드를 완료할 용량이 충분한지 또는 업그레이드 중에 장애가 발생했을 때 구성 요소 재구축을 수행할 용량이 충분한지 확인합니다.
- RVC를 액세스하기 위해 PuTTY 또는 이와 유사한 SSH 클라이언트가 설치되어 있는지 확인합니다.

RVC 도구 다운로드 및 RVC 명령 사용에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.

- 호스트가 유지 보수 모드로 설정되지 않았는지 확인합니다. 온디스크 형식을 업그레이드할 때는 호스트를 유지 보수 모드로 전환하지 않아야 합니다. vSAN 클러스터의 멤버 호스트가 유지 보수 모드로 전환되면 해당 멤버 호스트가 더 이상 클러스터에 용량을 제공하지 않기 때문에 클러스터에서 사용할 수 있는 리소스 용량이 줄어들고 클러스터 업그레이드가 실패할 수 있습니다.
- RVC `vsan.resync_dashboard` 명령을 실행하여, 현재 vSAN 클러스터에서 진행 중인 구성 요소 재구축 작업이 없는지 확인합니다.

프로시저

- 1 RVC를 사용하여 vCenter Server에 로그인합니다.

- vsan.disks_stats /< vCenter IP address or hostname>/<data center name>/computers/<cluster name> 명령을 실행하여 디스크 상태를 봅니다.

예: vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster

vSAN 클러스터에 있는 모든 디바이스 이름과 호스트 이름이 나열되고 현재 디스크 형식과 상태도 표시됩니다. 디스크 관리 페이지의 **상태** 열에서 디바이스의 현재 상태를 확인할 수도 있습니다. 예를 들어 장애가 발생한 디바이스가 있는 디스크 그룹 또는 호스트의 **상태** 열에는 디바이스 상태가 비정상적으로 나타납니다.

- vsan.ondisk_upgrade <path to vsan cluster> 명령을 실행합니다.

예: vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster

- RVC에서 진행 상황을 모니터링합니다.

RVC가 한 번에 하나의 디스크 그룹을 업그레이드합니다.

디스크 형식 업그레이드가 완료되면 다음 메시지가 나타납니다.

디스크 형식 업그레이드 단계 완료

n개의 v1 개체를 업그레이드해야 합니다. 개체 업그레이드 진행률: n개 업그레이드됨, 0개 남음

완료된 개체 업그레이드: n개 업그레이드됨

VSAN 업그레이드 완료

- vsan.obj_status_report 명령을 실행하여 개체 버전이 새 온디스크 형식으로 업그레이드되었는지 확인합니다.

vSAN 디스크 형식 업그레이드 확인

디스크 형식 업그레이드를 완료한 후 vSAN 클러스터가 새로운 온디스크 형식을 사용하고 있는지 확인해야 합니다.

프로시저

- vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 구성** 탭을 클릭합니다.
- vSAN에서 **디스크 관리**를 클릭합니다.

[디스크 형식 버전] 열에 현재 디스크 형식 버전이 나타납니다. 예를 들어 디스크 형식 2.0을 사용 중인 경우 [디스크 형식 버전] 열에 버전 2로 나타납니다. 온디스크 형식 3.0의 경우 디스크 형식 버전이 버전 3으로 나타납니다.

vSAN 클러스터 업그레이드 확인

vSAN 클러스터 업그레이드는 최신 버전의 vSphere를 사용 중이며 vSAN을 사용할 수 있음을 확인할 때까지 완료되지 않습니다.

프로시저

- vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 구성** 탭을 클릭하고 vSAN이 나열되는지 확인합니다.
 - ◆ ESXi 호스트로 이동한 후 **요약 > 구성**을 선택하고, ESXi 호스트의 최신 버전을 현재 사용 중인 지 확인할 수 있습니다.

RVC 업그레이드 명령 옵션 사용

vsan.ondisk_upgrade 명령은 vSAN 클러스터 업그레이드를 제어하고 관리하는 데 사용할 수 있는 여러 명령 옵션을 제공합니다. 예를 들어, 사용 가능한 공간이 적은 경우에 업그레이드를 수행할 때 감소된 이중화를 허용할 수 있습니다.

vsan.ondisk_upgrade --help 명령을 실행하면 RVC 명령 옵션 목록을 표시할 수 있습니다.

vsan.ondisk_upgrade 명령과 함께 사용하는 명령 옵션은 다음과 같습니다.

표 9-3. 업그레이드 명령 옵션

| 옵션 | 설명 |
|--------------------------------|--|
| --hosts_and_clusters | 클러스터 또는 클러스터의 계산 리소스에서 모든 호스트 시스템으로의 경로를 지정하는 데 사용됩니다. |
| --ignore-objects, -i | vSAN 개체 업그레이드를 건너뛰는 데 사용됩니다. 이 명령 옵션을 사용하여 개체 버전 업그레이드를 제거할 수도 있습니다. 이 명령 옵션을 사용하면 개체가 현재의 온디스크 형식 버전을 계속 사용합니다. |
| --allow-reduced-redundancy, -a | 디스크 업그레이드 도중 하나의 디스크 그룹과 동일한 사용 가능한 공간이 있어야 하는 요구 사항을 제거하는 데 사용됩니다. 이 옵션을 사용하면 가상 시스템이 업그레이드 도중 감소된 이중화 모드에서 작동합니다. 즉, 특정 가상 시스템이 일시적으로 장애를 허용하지 못할 수 있으며 이로 인해 데이터 손실이 발생할 수 있음을 의미합니다. vSAN은 업그레이드 완료 후 전체 규정 준수 및 이중화를 복원합니다. |
| --force, -f | 모든 확인 질문을 강제 진행하고 자동으로 답변할 수 있도록 합니다. |
| --help, -h | 도움말 옵션을 표시하는 데 사용됩니다. |

RVC 명령 사용에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.

vSphere Update Manager에 대한 vSAN 빌드 권장 사항

vSAN은 vSphere Update Manager와 함께 사용하기 위한 시스템 기준선 및 기준선 그룹을 생성합니다. 이러한 권장 기준선을 사용하여 vSAN 클러스터의 호스트에 대한 소프트웨어, 패치 및 확장을 업데이트할 수 있습니다.

vSAN 6.6.1 이상은 vSAN 클러스터에 대한 자동화된 빌드 권장 사항을 생성합니다. vSAN은 VMware 호환성 가이드 및 vSAN 릴리스 카탈로그의 정보와 설치된 ESXi 릴리스에 대한 정보를 결합합니다. 이러한 권장 업데이트는 지원되는 상태로 해당 하드웨어를 유지하기 위해 사용 가능한 최상의 릴리스를 제공합니다.

vSAN 시스템 기준선

vSAN 빌드 권장 사항은 Update Manager에 대한 vSAN 시스템 기준선을 통해 제공됩니다. 해당 시스템 기준선은 vSAN에서 관리합니다. 이러한 기준선은 읽기 전용이며 사용자 지정할 수 없습니다.

vSAN은 각 vSAN 클러스터에 대해 하나의 기준선 그룹을 생성합니다. vSAN 시스템 기준선은 [기준선 및 그룹] 탭의 기준선 창에 나열되어 있습니다. 사용자는 고유한 기준선을 생성하고 업데이트 적용을 수행할 수 있습니다.

Update Manager는 자동으로 각 vSAN 클러스터를 검색하여 기준선 그룹에 대한 규정 준수를 확인합니다. 클러스터를 업그레이드하려면 Update Manager를 통해 수동으로 시스템 기준선 업데이트 적용을 수행해야 합니다. 단일 호스트 또는 전체 클러스터에서 vSAN 시스템 기준선 업데이트 적용을 수행할 수 있습니다.

vSAN 릴리스 카탈로그

vSAN 릴리스 카탈로그는 사용 가능한 릴리스, 릴리스에 대한 우선 순위 및 각 릴리스에 필요한 중요 패치 등에 대한 정보를 유지 관리합니다. vSAN 릴리스 카탈로그는 VMware Cloud에서 호스팅됩니다.

vSAN에서 릴리스 카탈로그에 액세스하려면 인터넷 연결이 필요합니다. vSAN에서 릴리스 카탈로그에 액세스하기 위해 CEIP(고객 환경 향상 프로그램)에 등록할 필요가 없습니다.

vSAN 빌드 권장 사항 사용

Update Manager는 VMware 호환성 가이드에 있는 하드웨어 호환성 목록(HCL)의 정보와 비교하여, 설치된 ESXi 릴리스를 확인합니다. 현재 vSAN 릴리스 카탈로그에 기반하여 각 vSAN 클러스터에 대한 올바른 업그레이드 경로를 결정합니다. 또한 vSAN은 권장 릴리스에 필요한 드라이버 및 패치 업데이트를 시스템 기준선에 포함시킵니다.

vSAN 빌드 권장 사항은 각 vSAN 클러스터가 현재 하드웨어 호환성 상태 또는 그보다 개선된 상태를 유지하도록 보장합니다. vSAN 클러스터의 하드웨어가 HCL에 포함되지 않은 경우, vSAN은 최신 릴리스로 업그레이드를 권장합니다. 최신 릴리스가 현재 상태보다 나쁘지 않기 때문입니다.

다음 예제는 vSAN 빌드 권장 사항을 뒷받침하는 논리에 대해 설명합니다.

- 예제 1** vSAN 클러스터가 6.0 업데이트 2를 실행 중이고, 해당 하드웨어는 6.0 업데이트 2 HCL에 포함되어 있습니다. HCL에는 해당 하드웨어가 릴리스 6.0 업데이트 3까지 지원되지만, 6.5 이상에 대해서는 지원되지 않는 것으로 나와 있습니다. vSAN은 해당 릴리스에 필요한 중요 패치를 포함하여 6.0 업데이트 3으로 업그레이드를 권장합니다.
- 예제 2** vSAN 클러스터가 6.0 업데이트 2를 실행 중이고, 해당 하드웨어는 6.0 업데이트 2 HCL에 포함되어 있습니다. 또한 HCL에서 해당 하드웨어는 릴리스 6.5 업데이트 1에 대해 지원됩니다. vSAN은 릴리스 6.5 업데이트 1로 업그레이드를 권장합니다.
- 예제 3** vSAN 클러스터가 6.0 업데이트 2를 실행 중이고, 해당 하드웨어는 이 릴리스의 HCL에 없습니다. vSAN은 6.5 업데이트 1의 HCL에 이 하드웨어가 나와 있지 않더라도 6.5 업데이트 1로 업그레이드를 권장합니다. vSAN은 새로운 상태가 현재 상태보다 나쁘지 않기 때문에 업그레이드를 권장합니다.

권장 엔진은 주기적으로(매일 한 번) 또는 다음과 같은 이벤트 발생 시 실행됩니다.

- 클러스터 멤버 자격이 변경됩니다. 예를 들어 호스트를 추가 또는 제거하는 경우입니다.
- vSAN 관리 서비스가 다시 시작됩니다.
- 사용자가 vSphere Client 또는 RVC를 통해 My VMware(my.vmware.com)에 로그인합니다.
- VMware 호환성 가이드 또는 vSAN 릴리스 카탈로그가 업데이트되었습니다.

vSAN 빌드 권장 사항 상태 점검은 vSAN 클러스터에 대해 권장되는 현재 빌드를 표시합니다. 또한 기능 관련 문제에 대한 경고를 표시할 수 있습니다.

시스템 요구 사항

Update Manager는 Windows vCenter Server에서 수동으로 설치해야 합니다.

vSAN에서 릴리스 메타데이터를 업데이트하고, VMware 호환성 가이드를 확인하고, My VMware에서 ISO 이미지를 다운로드하려면 인터넷 액세스가 필요합니다.

vSAN에는 업그레이드용 ISO 이미지 다운로드를 위해 유효한 My VMware(my.vmware.com) 자격 증명이 필요합니다. 6.0 업데이트 1 이전 버전이 실행되는 호스트의 경우 RVC를 사용하여 My VMware 자격 증명을 입력해야 합니다. 이후 버전의 소프트웨어가 실행되는 호스트의 경우 ESX 빌드 권장 사항 상태 점검에서 로그인할 수 있습니다.

RVC에서 My VMware 자격 증명을 입력하려면 다음 명령을 실행합니다. `vsan.login_iso_depot -u <username> -p <password>`

vSAN 클러스터에서 디바이스 관리

vSAN 클러스터에서는 다양한 디바이스 관리 작업을 수행할 수 있습니다. 예를 들면 하이브리드 또는 플래시 전용 디스크 그룹을 생성하고, vSAN에서 용량 및 캐시용 디바이스를 할당하도록 설정하고, 디바이스의 LED 표시기를 사용 또는 사용하지 않도록 설정하고, 디바이스를 플래시로 표시하고, 원격 디바이스를 로컬 디바이스로 표시하는 등의 작업을 수행할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “디스크 그룹 및 디바이스 관리,” (99 페이지)
- “개별 디바이스 사용,” (101 페이지)

디스크 그룹 및 디바이스 관리

클러스터에서 vSAN을 사용하도록 설정할 경우, 디바이스를 그룹으로 구성하기 위한 디스크 할당 모드를 선택합니다.

vSAN 6.6 이상 릴리스에서는 모든 시나리오에서 디스크를 할당하는 데 동일한 워크플로를 사용합니다. 이 워크플로는 사용 가능한 모든 디스크를 모델과 크기 또는 호스트별로 그룹화합니다. 캐시에 사용할 디바이스와 용량에 사용할 디바이스를 선택해야 합니다.

호스트에서 디스크 그룹 생성

디스크 그룹을 생성하는 경우 vSAN 데이터스토어에 사용될 각 호스트와 각 디바이스를 수동으로 지정해야 합니다. 또한 캐시 및 용량 디바이스를 디스크 그룹으로 구성해야 합니다.

디스크 그룹을 생성하려면 디스크 그룹을 정의하고 디스크 그룹에 포함될 디바이스를 개별적으로 선택합니다. 각 디스크 그룹에는 하나의 플래시 캐시 디바이스와 하나 이상의 용량 디바이스가 포함됩니다.

디스크 그룹을 생성할 때는 플래시 캐시 대 사용 용량의 비율을 고려하십시오. 비율은 클러스터의 워크로드와 요구 사항에 따라 달라지지만 사용되는 용량 비율에(미러와 같은 복제 제외) 플래시 캐시를 10% 이상 사용하는 것이 좋습니다.

vSAN 클러스터에는 처음에 0바이트가 사용된 단일 vSAN 데이터스토어가 포함되어 있습니다.

각 호스트에서 디스크 그룹을 생성하고 캐시 및 용량 디바이스를 추가하면 데이터스토어의 크기가 해당 디바이스에 의해 추가된 물리적 용량에 따라 증가됩니다. vSAN은 클러스터에 추가된 호스트에서 사용 가능한 로컬 빈 용량을 사용하여 하나의 분산된 vSAN 데이터스토어를 생성합니다.

클러스터에 플래시 캐시 디바이스가 여러 개 필요한 경우, 디스크 그룹당 최대 한 개의 플래시 캐시 디바이스가 허용되므로 여러 디스크 그룹을 수동으로 생성해야 합니다.

참고 vSAN 클러스터에 새 ESXi 호스트를 추가하면 해당 호스트의 로컬 스토리지가 vSAN 데이터스토어에 자동으로 추가되지 않습니다. 새 ESXi 호스트의 새 스토리지를 사용하려면 디스크 그룹을 생성하고 디스크 그룹에 디바이스를 추가해야 합니다.

vSAN 클러스터에 대한 디스크 할당

호스트에서 여러 디바이스를 선택하면 vSAN이 기본 디스크 그룹을 생성합니다.

호스트에 용량을 추가하거나 용량이 있는 새 호스트를 vSAN 클러스터에 추가하면 새 디바이스를 선택하여 vSAN 데이터스토어의 용량을 늘릴 수 있습니다. 플래시 전용 클러스터에서는 용량으로 사용할 플래시 디바이스를 표시할 수 있습니다.

vSAN이 디바이스를 할당한 후 vSAN 공유 데이터스토어를 생성합니다. 데이터스토어의 전체 크기는 클러스터에 있는 모든 호스트의 디스크 그룹 내 모든 용량 디바이스의 용량을 반영합니다. 일부 용량 오버헤드는 메타데이터에 사용됩니다.

vSAN 호스트에서 디스크 그룹 생성

특정 캐시 디바이스와 특정 용량 디바이스를 수동으로 결합하여 특정 호스트의 디스크 그룹을 정의할 수 있습니다.

이 방법에서는 디바이스를 수동으로 선택하여 호스트에 대한 디스크 그룹을 생성합니다. 캐시 디바이스 하나와 용량 디바이스 하나 이상을 디스크 그룹에 추가합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 호스트를 선택하고 **새 디스크 그룹 생성** 아이콘()을 클릭합니다.
 - 캐시로 사용할 플래시 디바이스를 선택합니다.
 - 생성하려는 디스크 그룹 유형에 따라 **용량 유형** 드롭다운 메뉴에서 사용할 용량 디스크 유형을 선택합니다. 예를 들어 하이브리드 디스크 그룹을 생성하려면 HDD를 선택하고, 플래시 전용 디스크 그룹을 생성하려면 플래시를 선택합니다.
 - ◆ 용량으로 사용할 디바이스를 선택합니다.
- 5 **확인**을 클릭합니다.

새 디스크 그룹이 목록에 나타납니다.

vSAN 클러스터에 대한 스토리지 디바이스 할당

캐시 및 용량 디바이스 그룹을 선택하면 vSAN이 이들 디바이스를 기본 디스크 그룹으로 구성합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.

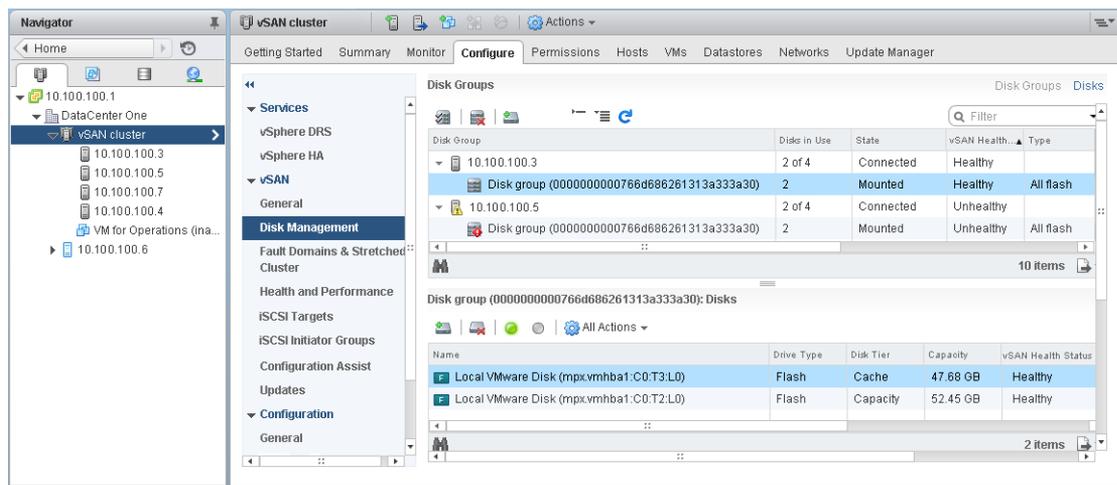
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 **디스크 할당** 아이콘()을 클릭합니다.
- 5 디스크 그룹에 추가할 디바이스를 선택합니다.
 - 하이브리드 디스크 그룹에 스토리지를 제공하는 각 호스트는 플래시 캐시 디바이스 하나와 용량 디바이스 하나 이상을 제공해야 합니다. 디스크 그룹당 하나의 플래시 캐시 디바이스만 추가할 수 있습니다.
 - 캐시로 사용할 플래시 디바이스를 선택하고 **캐시 계층에 대해 할당** 아이콘()을 클릭합니다.
 - 용량으로 사용할 HDD 디바이스를 선택하고 **용량 계층에 대해 할당** 아이콘()을 클릭합니다.
 - **확인**을 클릭합니다.
 - 플래시 전용 디스크 그룹의 경우, 용량 및 캐시 모두에 대해 플래시 디바이스를 선택합니다.
 - 캐시로 사용할 플래시 디바이스를 선택하고 **캐시 계층에 대해 할당** 아이콘()을 클릭합니다.
 - 용량으로 사용할 플래시 디바이스를 선택하고 **용량 계층에 대해 할당** 아이콘()을 클릭합니다.
 - **확인**을 클릭합니다.

플래시 전용 디스크 그룹에 추가된 각 디바이스의 역할을 확인하려면 [디스크 관리] 페이지의 아래쪽에 있는 [디스크 역할] 열로 이동하십시오. 이 열에는 디바이스 목록 및 디스크 그룹에서 해당 디바이스의 용도가 나열됩니다.

vSAN은 선택된 디바이스를 할당하고 vSAN 데이터스토어를 지원하는 기본 디스크 그룹으로 구성합니다.

개별 디바이스 사용

vSAN 클러스터에서는 디스크 그룹에 디바이스를 추가하고, 디스크 그룹에서 디바이스를 제거하고, 로케이터 LED를 사용 또는 사용 안 함으로 설정하고 디바이스를 표시하는 등 다양한 디바이스 관리 작업을 수행할 수 있습니다.



The screenshot shows the vSAN Disk Management interface. The left sidebar displays the vSAN cluster configuration, including services like vSphere DRS and vSAN. The main area shows a list of Disk Groups with columns for Disk Group, Disks in Use, State, vSAN Health, and Type. Below this, a detailed view of a specific Disk Group shows a table of disks with columns for Name, Drive Type, Disk Tier, Capacity, and vSAN Health Status.

| Disk Group | Disks in Use | State | vSAN Health | Type |
|---|--------------|-----------|-------------|-----------|
| 10.100.100.3 | 2 of 4 | Connected | Healthy | |
| Disk group (0000000000766d686261313a333a30) | 2 | Mounted | Healthy | All flash |
| 10.100.100.5 | 2 of 4 | Connected | Unhealthy | |
| Disk group (0000000000766d686261313a333a30) | 2 | Mounted | Unhealthy | All flash |

| Name | Drive Type | Disk Tier | Capacity | vSAN Health Status |
|---|------------|-----------|----------|--------------------|
| Local VMware Disk (mpx.vmhba1.C0:T3:L0) | Flash | Cache | 47.68 GB | Healthy |
| Local VMware Disk (mpx.vmhba1.C0:T2:L0) | Flash | Capacity | 52.45 GB | Healthy |

디스크 그룹에 디바이스 추가

수동 모드에서 디스크를 할당하도록 vSAN을 구성하는 경우에는 기존 디스크 그룹에 추가적인 로컬 디바이스를 추가할 수 있습니다.

디바이스는 SSD 또는 자기 디스크 같이 디스크 그룹에 있는 기존 디바이스와 같은 유형이어야 합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 디스크 그룹을 선택하고 **선택한 디스크 그룹에 디스크 추가** 아이콘()을 클릭합니다.
- 5 추가할 디바이스를 선택하고 **확인**을 클릭합니다.

남은 데이터나 파티션 정보가 포함된 사용했던 디바이스를 추가하는 경우 장치를 먼저 정리해야 합니다. 디바이스의 파티션 정보 제거에 대한 자세한 내용은 “[디바이스에서 파티션 제거](#),” (106 페이지)를 참조하십시오. `host_wipe_vsan_disks` RVC 명령을 실행하여 디바이스를 포맷할 수도 있습니다. RVC 명령에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.

vSAN 에서 디스크 그룹 또는 디바이스 제거

전체 디스크 그룹을 제거하거나 디스크 그룹에서 선택한 디바이스를 제거할 수 있습니다.

보호되지 않는 디바이스를 제거할 경우 vSAN 데이터스토어와 해당 데이터스토어의 가상 시스템이 중단될 수 있으므로 디바이스나 디스크 그룹을 제거하지 마십시오.

일반적으로 디바이스를 업그레이드하거나 장애가 발생한 디바이스를 교체하는 경우, 또는 캐시 디바이스를 제거해야 하는 경우에 vSAN에서 디스크 그룹이나 디바이스를 삭제합니다. 기타 vSphere 스토리지 기능은 vSAN 클러스터에서 제거하는 모든 플래시 기반 디바이스를 사용할 수 있습니다.

디스크 그룹을 영구적으로 삭제하면 디스크 멤버 자격과 함께 디바이스에 저장된 데이터가 삭제됩니다.

참고 디스크 그룹에서 하나의 플래시 캐시 디바이스나 모든 용량 디바이스를 제거하면 전체 디스크 그룹이 제거됩니다.

디바이스나 디스크 그룹에서 데이터를 제거하면 가상 시스템 스토리지 정책의 일시적인 규정 비준수가 발생할 수 있습니다.

필수 조건

- 디바이스 또는 디스크 그룹을 삭제할 경우 **모든 데이터 제거** 옵션 또는 **데이터 액세스 지원 보장을** 선택하여 vSAN 호스트를 유지 보수 모드로 전환할 수 있습니다. 드롭다운 메뉴에서 **데이터 이동 안 함**을 선택하는 경우, 제거 중 장애가 발생하면 데이터가 위협할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.

- 4 디스크 그룹 또는 선택한 디바이스를 제거합니다.

| 옵션 | 설명 |
|-------------|--|
| 디스크 그룹 제거 | <p>a [디스크 그룹]에서 제거할 디스크 그룹을 선택하고 디스크 그룹 제거 아이콘()을 클릭합니다</p> <p>b 데이터 제거 모드를 선택합니다.</p> |
| 선택한 디바이스 제거 | <p>a 디스크 그룹에서 제거하려는 디바이스가 포함된 디스크 그룹을 선택합니다.</p> <p>b 디스크에서 제거할 디바이스를 선택하고 선택한 디스크를 디스크 그룹에서 제거 아이콘()을 클릭합니다.</p> <p>c 데이터 제거 모드를 선택합니다.</p> |

제거된 데이터를 동일한 호스트의 다른 디스크나 디스크 그룹으로 이동할 수 있습니다.

- 5 예를 클릭하여 확인합니다.

데이터가 선택한 디바이스 또는 디스크 그룹에서 제거되고 vSAN에서 더 이상 사용할 수 없습니다.

로케이터 LED 사용

로케이터 LED를 사용하면 스토리지 디바이스의 위치를 식별할 수 있습니다.

vSAN은 장애가 발생한 디바이스를 쉽게 식별할 수 있도록 해당 디바이스의 로케이터 LED를 점등할 수 있습니다. 이 기능은 다중 핫 플러그 및 호스트 스왑 시나리오를 사용 중일 때 특히 유용합니다.

RAID 0 모드의 컨트롤러에서는 컨트롤러가 로케이터 LED를 인식하도록 하기 위한 추가 단계가 필요하기 때문에 패스스루 모드의 I/O 스토리지 컨트롤러를 사용하는 것을 고려해야 합니다.

RAID 0 모드의 스토리지 컨트롤러 구성에 대한 자세한 내용은 벤더 설명서를 참조하십시오.

로케이터 LED 사용 또는 사용 안 함

vSAN 스토리지 디바이스에서 로케이터 LED를 사용 또는 사용 안 함으로 설정할 수 있습니다. 로케이터 LED를 사용하도록 설정하면 특정 스토리지 디바이스의 위치를 식별할 수 있습니다.

vSAN 디바이스에 대한 시각적 경고가 더 이상 필요하지 않은 경우에는 선택된 디바이스의 로케이터 LED를 사용하지 않도록 설정할 수 있습니다.

필수 조건

- 이 기능을 사용할 수 있도록 해주는 스토리지 I/O 컨트롤러용 지원 드라이버를 설치했는지 확인합니다. VMware에서 인증한 드라이버에 대한 자세한 내용은 VMware 호환성 가이드 (<http://www.vmware.com/resources/compatibility/search.php>)를 참조하십시오.
- 일부 경우 스토리지 I/O 컨트롤러에서 로케이터 LED 기능을 구성하기 위해 타사 유틸리티를 사용해야 할 수 있습니다. 예를 들어 HP를 사용하는 경우, HP SSA CLI가 설치되었는지 확인해야 합니다.

타사 VIB 설치에 대한 자세한 내용은 vSphere 업그레이드 설명서를 참조하십시오.

프로시저

- vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 구성** 탭을 클릭합니다.
- vSAN에서 **디스크 관리**를 클릭합니다.
- 디바이스 목록을 보려면 호스트를 선택합니다.

- 5 페이지 맨 아래의 목록에서 스토리지 디바이스를 하나 이상 선택하고, 선택된 디바이스의 로케이터 LED를 사용하거나 사용하지 않도록 설정합니다.

| 옵션 | 작업 |
|--------------------------|--|
| 선택한 디스크의 로케이터 LED 켜기 아이콘 | 선택한 스토리지 디바이스의 로케이터 LED를 사용하도록 설정합니다. 관리 탭에서 스토리지 > 스토리지 디바이스 를 클릭하여 로케이터 LED를 사용하도록 설정할 수 있습니다. |
| 선택한 디스크의 로케이터 LED 끄기 아이콘 | 선택한 스토리지 디바이스의 로케이터 LED를 사용하지 않도록 설정합니다. 관리 탭에서 스토리지 > 스토리지 디바이스 를 클릭하여 로케이터 LED를 사용하지 않도록 설정할 수 있습니다. |

디바이스를 플래시로 표시

ESXi 호스트가 플래시 디바이스를 플래시로 자동 식별하지 못하는 경우에는 해당 디바이스를 수동으로 로컬 플래시 디바이스로 표시할 수 있습니다.

패스트루 모드가 아니라 RAID 0 모드에 대해 사용되도록 설정된 경우에도 이런 상황이 발생할 수 있습니다. 디바이스가 로컬 플래시로 인식되지 않는 경우에는 vSAN에 대해 제공되는 디바이스 목록에서 제외되며 vSAN 클러스터에서 사용할 수 없습니다. 이러한 디바이스를 로컬 플래시로 표시하면 vSAN에서 사용할 수 있게 됩니다.

필수 조건

- 디바이스가 호스트에 로컬인지 확인합니다.
- 디바이스가 사용 중이 아닌지 확인합니다.
- 디바이스에 액세스하는 가상 시스템의 전원이 꺼져 있고 데이터스토어가 마운트 해제되었는지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 호스트를 선택하여 사용 가능한 디바이스를 봅니다.
- 5 페이지 맨 아래의 **표시** 드롭다운 메뉴에서 **사용 중 아님**을 선택합니다.
- 6 목록에서 플래시 디바이스를 하나 이상 선택하고 **선택한 디스크를 플래시 디스크로 표시** 아이콘()을 클릭합니다.
- 7 **예**를 클릭하여 변경 내용을 저장합니다.
선택한 디바이스의 드라이브 유형이 플래시로 표시됩니다.

디바이스를 HDD로 표시

ESXi 호스트가 로컬 자기 디스크를 HDD 디바이스로 자동 식별하지 못하는 경우에는 수동으로 해당 디스크를 HDD 디바이스로 표시할 수 있습니다.

자기 디스크를 플래시 디바이스로 표시한 경우, 자기 디스크로 표시하여 디바이스의 디스크 유형을 변경할 수 있습니다.

필수 조건

- 자기 디스크가 호스트에 대해 로컬인지 확인합니다.
- 자기 디스크가 사용 중이 아니며 비어 있는지 확인합니다.
- 디바이스에 액세스하는 가상 시스템의 전원이 꺼졌는지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 호스트를 선택하여 사용 가능한 자기 디스크 목록을 봅니다.
- 5 페이지 맨 아래의 **표시** 드롭다운 메뉴에서 **사용 중 아님**을 선택합니다.
- 6 목록에서 자기 디스크를 하나 이상 선택하고 **선택한 디스크를 HDD 디스크로 표시** 아이콘()을 클릭합니다.
- 7 **예**를 클릭하여 저장합니다.
선택한 자기 디스크의 드라이브 유형이 HDD로 표시됩니다.

디바이스를 로컬로 표시

호스트가 외부 SAS 인클로저를 사용하는 경우 vSAN은 특정 디바이스를 원격으로 인식하여 이를 자동으로 로컬로 할당하지 못할 수 있습니다.

그러한 경우 디바이스를 로컬로 표시할 수 있습니다.

필수 조건

스토리지 디바이스가 공유되지 않았는지 확인합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터를 찾습니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 디바이스 목록을 보려면 호스트를 선택합니다.
- 5 페이지 맨 아래의 **표시** 드롭다운 메뉴에서 **사용 중 아님**을 선택합니다.
- 6 디바이스 목록에서 로컬로 표시할 원격 디바이스를 하나 이상 선택하고 **선택한 디스크를 호스트의 로컬로 표시** 아이콘을 클릭합니다.
- 7 **예**를 클릭하여 변경 내용을 저장합니다.

디바이스를 원격으로 표시

외부 SAS 컨트롤러를 사용하는 호스트는 디바이스를 공유할 수 있습니다. vSAN이 디스크 그룹을 생성할 때 공유 디바이스를 할당하지 않도록 수동으로 이러한 공유 디바이스를 원격으로 표시할 수 있습니다.

vSAN에서는 공유 디바이스를 디스크 그룹에 추가할 수 없습니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터를 찾습니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 디바이스 목록을 보려면 호스트를 선택합니다.
- 5 페이지 맨 아래의 **표시** 드롭다운 메뉴에서 **사용 중 아님**을 선택합니다.
- 6 원격으로 표시할 하나 이상의 디바이스를 선택하고 **선택한 디스크를 호스트의 원격으로 표시** 아이콘을 클릭합니다.

- 7 **예**를 클릭하여 확인합니다.

용량 디바이스 추가

기존 vSAN 디스크 그룹에 용량 디바이스를 추가할 수 있습니다.

공유 디바이스는 디스크 그룹에 추가할 수 없습니다.

필수 조건

디바이스가 포맷되고 사용 중이 아닌지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 디스크 그룹을 선택합니다.
- 5 페이지 맨 아래에서 **선택한 디스크 그룹에 디스크 추가** 아이콘()을 클릭합니다.
- 6 디스크 그룹에 추가할 용량 디바이스를 선택합니다.
- 7 **확인**을 클릭합니다.
디바이스가 디스크 그룹에 추가됩니다.

디바이스에서 파티션 제거

vSAN이 디바이스를 할당하여 사용할 수 있도록 디바이스에서 파티션 정보를 제거할 수 있습니다.

남은 데이터나 파티션 정보가 포함된 디바이스를 추가한 경우, vSAN에서 해당 디바이스를 할당하여 사용할 수 있으려면 먼저 기존의 모든 파티션 정보를 디바이스에서 제거해야 합니다. 디스크 그룹에는 깨끗한 디바이스를 추가하는 것이 좋습니다.

사용자가 디바이스에서 파티션 정보를 제거하면 vSAN은 디스크 포맷 정보가 포함된 기본 파티션과 논리적 파티션을 디바이스에서 삭제합니다.

필수 조건

ESXi에서 디바이스를 부팅 디스크, VMFS 데이터스토어 또는 vSAN으로 사용하고 있지 않은지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **디스크 관리**를 클릭합니다.
- 4 사용 가능한 디바이스 목록을 볼 호스트를 선택합니다.
- 5 페이지 맨 아래의 **표시** 드롭다운 메뉴에서 **부적격**을 선택합니다.
- 6 목록에서 디바이스를 선택하고 **선택한 디스크의 파티션 지우기** 아이콘()을 클릭합니다.
- 7 **확인**을 클릭하여 확인합니다.
이제 디바이스가 깨끗한 상태이며 그 어떤 파티션 정보도 포함되어 있지 않습니다.

vSAN 클러스터 확장 및 관리

vSAN 클러스터를 설정한 후 vSphere Web Client를 사용하여 호스트와 용량 디바이스를 추가하고 호스트와 디바이스를 제거하고 장애 시나리오를 관리할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “vSAN 클러스터 확장,” (107 페이지)
- “유지 보수 모드 사용,” (111 페이지)
- “vSAN 클러스터에서 장애 도메인 관리,” (113 페이지)
- “vSAN iSCSI 대상 서비스 사용,” (117 페이지)
- “하이브리드 vSAN 클러스터를 플래시 전용 클러스터로 마이그레이션,” (120 페이지)
- “vSAN 클러스터 전원 끄기,” (121 페이지)

vSAN 클러스터 확장

호스트를 추가하거나 기존 호스트에 디바이스를 추가하여 진행 중인 작업을 하나도 중단하지 않고 기존 vSAN 클러스터를 확장할 수 있습니다.

다음 방법 중 하나를 사용하여 vSAN 클러스터를 확장합니다.

- 지원되는 캐시 및 용량 디바이스를 사용하여 구성된 클러스터에 새로운 ESXi 호스트를 추가합니다. “vSAN 클러스터에 호스트 추가,” (108 페이지)를 참조하십시오. 디바이스를 추가하거나 용량이 포함된 호스트를 추가하는 경우 vSAN은 새롭게 추가된 디바이스에 자동으로 데이터를 배포하지 않습니다. vSAN에서 최근에 추가된 디바이스에 데이터를 배포하도록 설정하려는 경우 RVC(Ruby vSphere Console)를 사용하여 수동으로 클러스터를 재조정해야 합니다. “수동 재조정,” (143 페이지)를 참조하십시오.
- 호스트 프로파일을 사용하여 기존 ESXi 호스트를 vSAN 클러스터로 이동합니다. “호스트 프로파일을 사용하여 호스트 구성,” (109 페이지)를 참조하십시오. 새 클러스터 멤버는 스토리지를 추가하고 용량을 계산합니다. 새로 추가된 호스트의 로컬 용량 디바이스에서 일부 디스크 그룹을 수동으로 생성해야 합니다. “vSAN 호스트에서 디스크 그룹 생성,” (100 페이지)를 참조하십시오.

사용하려는 하드웨어 구성 요소, 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러가 인증되고 VMware 호환성 가이드(<http://www.vmware.com/resources/compatibility/search.php>)에 나열되어 있는지 확인합니다. 용량 디바이스를 추가할 때는 vSAN이 디바이스를 인식하고 할당할 수 있도록 해당 디바이스가 포맷되지 않고 분할되지 않은 상태인지 확인해야 합니다.

- 클러스터 멤버인 ESXi 호스트에 새 용량 디바이스를 추가합니다. 호스트의 디스크 그룹에 디바이스를 수동으로 추가해야 합니다. “디스크 그룹에 디바이스 추가,” (102 페이지)를 참조하십시오.

vSAN 클러스터 용량 및 성능 확장

vSAN 클러스터의 스토리지 용량이 부족하거나 클러스터의 성능 저하가 나타나는 경우 용량 및 성능을 위해 클러스터를 확장할 수 있습니다.

- 스토리지 디바이스를 기존 디스크 그룹에 추가하거나 새 디스크 그룹을 생성하여 클러스터의 스토리지 용량을 확장합니다. 새 디스크 그룹을 생성하려면 캐시를 위한 플래시 디바이스가 필요합니다. 디스크 그룹의 디바이스 추가에 대한 자세한 내용은 “디스크 그룹에 디바이스 추가,” (102 페이지) 항목을 참조하십시오. 캐시를 늘리지 않고 용량 디바이스를 추가하는 경우 캐시 대 용량 비율이 지원되지 않는 수준으로 줄어들 수 있습니다. “vSAN의 플래시 캐시 디바이스에 대한 설계 고려 사항,” (24 페이지)를 참조하십시오.
- 하나 이상의 캐시 디바이스(플래시)와 용량 디바이스(플래시 또는 자기 디스크) 하나를 기존 스토리지 I/O 컨트롤러나 새 서버 호스트에 추가하여 클러스터 성능을 향상합니다. 추가적인 디스크 그룹이 포함된 서버를 하나 이상 추가할 수 있습니다. 이 경우 vSAN이 vSAN 클러스터에서 사전 재조정을 완료하면 성능 측면에서 동일한 효과가 있습니다.

클러스터 내 다른 호스트의 용량을 사용하는 계산 전용 호스트도 vSAN 환경에서 사용할 수 있지만 원활한 운영을 위해서는 구성이 일관된 호스트를 추가해야 합니다.

최상의 결과를 얻으려면 캐시 디바이스와 용량 디바이스 둘 모두가 구성된 호스트를 추가합니다. 디스크 그룹의 디바이스 추가에 대한 자세한 내용은 “디스크 그룹에 디바이스 추가,” (102 페이지) 항목을 참조하십시오.

vSAN 클러스터에 호스트 추가

진행 중인 작업을 중단하지 않고 실행 중인 vSAN 클러스터에 ESXi 호스트를 추가할 수 있습니다. 그러면 호스트의 리소스가 클러스터에 연결됩니다.

필수 조건

- 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러를 포함한 리소스가 VMware 호환성 가이드 (<http://www.vmware.com/resources/compatibility/search.php>)에 나열되어 있는지 확인합니다.
- 클러스터에서 구성 요소 및 개체가 디바이스 전체에 균등하게 배포되도록 동일하게 구성된 호스트를 vSAN 클러스터에 생성하는 것이 좋습니다. 하지만 특히 유지 보수 도중이거나 과도한 가상 시스템 배포로 vSAN 데이터스토어 용량이 오버 커밋된 경우에는 클러스터의 균형이 균일하지 않은 상황이 발생할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 클러스터를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가**를 선택합니다.
- 3 호스트 이름 또는 IP 주소를 입력하고 **다음**을 클릭합니다.
- 4 호스트에 연결된 사용자 이름과 암호를 입력하고 **다음**을 클릭합니다.
- 5 요약 정보를 확인한 후 **다음**을 클릭합니다.
- 6 라이선스 키를 할당하고 **다음**을 클릭합니다.
- 7 (선택 사항) 원격 사용자가 호스트에 직접 로그인하지 못하도록 하려면 잠금 모드를 설정합니다. 나중에 호스트 설정의 보안 프로파일을 편집하여 이 옵션을 구성할 수 있습니다.

- 8 호스트의 가상 시스템과 리소스 풀에서 수행할 작업을 선택합니다.
 - **클러스터의 루트 리소스 풀에 이 호스트의 모든 가상 시스템을 추가합니다.**
vCenter Server는 호스트의 기존 리소스 풀을 모두 제거합니다. 호스트의 계층에 있는 가상 시스템은 모두 루트에 연결됩니다. 공유 할당은 리소스 풀과 관련이 있으므로 가상 시스템의 공유를 변경해야 할 수 있습니다. 이러한 변경을 수행하면 리소스 풀 계층이 삭제됩니다.
 - **이 호스트의 가상 시스템 및 리소스 풀을 위한 리소스 풀을 생성합니다.**
vCenter Server가 클러스터의 직속 하위 리소스 풀이 되는 최상위 리소스 풀을 생성하고 호스트의 모든 하위 항목을 이 새 리소스 풀에 추가합니다. 새로 생성된 최상위 리소스 풀의 이름을 입력할 수 있습니다. 기본값은 <host_name>에서 이식됩니다.
- 9 설정을 검토하고 **완료**를 클릭합니다.
호스트가 클러스터에 추가됩니다.

호스트 프로파일을 사용하여 호스트 구성

vSAN 클러스터에 여러 호스트가 있는 경우 기존 vSAN 호스트의 프로파일을 재사용하고 vSAN 클러스터의 나머지 호스트에 해당 프로파일 설정을 적용할 수 있습니다.

호스트 프로파일에는 스토리지 구성, 네트워크 구성 또는 호스트의 다른 특징과 같은 정보가 포함되어 있습니다. 일반적으로 8개, 16개, 32개 또는 64개 호스트와 같이 대량의 호스트가 포함된 클러스터를 생성하려는 경우 호스트 프로파일 기능을 사용하여 한 번에 2개 이상의 호스트를 vSAN 클러스터에 추가할 수 있습니다.

필수 조건

- 호스트가 유지 보수 모드에 있는지 확인합니다.
- 하드웨어 구성 요소, 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러가 <http://www.vmware.com/resources/compatibility/search.php>의 VMware 호환성 가이드에 나열되어 있는지 확인합니다.

프로시저

- 1 호스트 프로파일을 만들 수 있습니다.
 - a 호스트 프로파일 보기로 이동합니다.
 - b **호스트에서 프로파일 추출** 아이콘(+)을 클릭합니다.
 - c 참조 호스트로 사용할 호스트를 선택하고 **다음**을 클릭합니다.
선택한 호스트는 반드시 활성 호스트여야 합니다.
 - d 새 프로파일의 이름 및 설명을 입력하고 **다음**을 클릭합니다.
 - e 새 호스트 프로파일에 대한 요약 정보를 검토하고 **마침**을 클릭합니다.
새로운 프로파일이 호스트 프로파일 목록에 나타납니다.
- 2 호스트를 원하는 호스트 프로파일에 연결합니다.
 - a [호스트 프로파일] 보기의 [프로파일] 목록에서 vSAN 호스트에 적용할 호스트 프로파일을 선택합니다.
 - b **호스트 프로파일에 호스트 및 클러스터 연결/분리** 아이콘(🔗)을 클릭합니다.
 - c 확장된 목록에서 호스트를 선택하고 **연결**을 클릭하여 해당 호스트를 프로파일에 연결합니다.
호스트가 연결된 엔터티 목록에 추가됩니다.

- d 다음을 클릭합니다.
 - e 마침을 클릭하여 프로파일에 대한 호스트 연결을 완료합니다.
- 3 호스트 프로파일에서 참조된 vSAN 호스트를 분리합니다.
- 호스트 프로파일이 클러스터에 연결되면 클러스터에 포함된 호스트도 해당 호스트 프로파일에 연결됩니다. 하지만 클러스터에서 호스트 프로파일이 분리되어도 호스트 또는 클러스터 내 호스트와 해당 호스트 프로파일에 포함된 호스트 간의 연결은 손상되지 않고 그대로 유지됩니다.
- a 호스트 프로파일 보기의 프로파일 목록에서 호스트 또는 클러스터에서 분리할 호스트 프로파일을 선택합니다.
 - b 호스트 프로파일에 호스트 및 클러스터 연결/분리 아이콘()을 클릭합니다.
 - c 확장된 목록에서 호스트 또는 클러스터를 선택하고 분리를 클릭합니다.
 - d 나열된 호스트 및 클러스터를 모두 프로파일에서 분리하려면 모두 분리를 클릭합니다.
 - e 다음을 클릭합니다.
 - f 마침을 클릭하여 호스트 프로파일에서의 호스트 분리를 완료합니다.
- 4 연결된 호스트 프로파일에 대하여 vSAN 호스트가 규정을 준수하는지 확인하고 해당 호스트에 호스트 프로파일에서 지정된 것과 다른 구성 매개 변수가 있는지 파악합니다.
- a 호스트 프로파일로 이동합니다.

개체 탭에는 모든 호스트 프로파일, 각 호스트 프로파일에 연결된 호스트 수 및 마지막 규정 준수 검사의 요약된 결과가 나열됩니다.
 - b 호스트 프로파일 규정 준수 여부 검사 아이콘()을 클릭합니다.

규정 준수에 실패한 호스트와 호스트 프로파일 간에 다른 매개 변수에 대한 자세한 정보를 보려면 모니터 탭을 클릭하고 [규정 준수] 보기를 선택합니다. 해당 개체 계층을 확장하고 규정 비준수 호스트를 선택합니다. 다른 매개 변수가 규정 준수 창의 해당 계층 아래에 표시됩니다.

규정 준수에 실패할 경우 업데이트 적용 작업을 사용하여 호스트 프로파일 설정을 호스트에 적용합니다. 이 작업을 수행하면 모든 호스트 프로파일 관리 매개 변수가 호스트에 연결된 호스트 프로파일에 포함되어 있는 값으로 변경됩니다.
 - c 규정 준수에 실패한 호스트와 호스트 프로파일 간에 다른 매개 변수에 대한 자세한 정보를 보려면 모니터 탭을 클릭하고 [규정 준수] 보기를 선택합니다.
 - d 해당 개체 계층을 확장하고 규정 준수에 실패한 호스트를 선택합니다.

다른 매개 변수가 규정 준수 창의 해당 계층 아래에 표시됩니다.
- 5 호스트에 업데이트를 적용하여 호스트에 있는 규정 준수 오류를 수정합니다.
- a 모니터 탭을 선택하고 규정 준수를 클릭합니다.
 - b 업데이트를 적용할 하나 이상의 호스트를 마우스 오른쪽 버튼으로 클릭하고 모든 vCenter 작업 > 호스트 프로파일 > 업데이트 적용을 선택합니다.

호스트를 사용자 지정하여 호스트 프로파일 정책의 사용자 입력 매개 변수를 업데이트하거나 변경할 수 있습니다.
 - c 다음을 클릭합니다.
 - d 호스트 프로파일 업데이트를 적용하는 데 필요한 작업을 검토하고 마침을 클릭합니다.
- 이 호스트는 vSAN 클러스터의 일부이며 이 호스트의 리소스는 vSAN 클러스터에서 액세스할 수 있습니다. 또한 이 호스트는 vSAN 클러스터에 있는 기존의 모든 vSAN 스토리지 I/O 정책에 액세스할 수 있습니다.

유지 보수 모드 사용

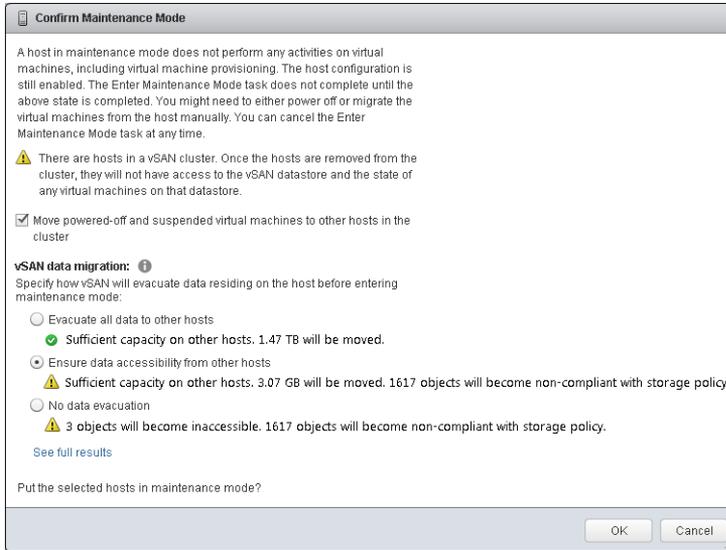
vSAN 클러스터의 멤버인 호스트를 종료, 재부팅 또는 연결 해제하기 전에 호스트를 유지 보수 모드로 전환해야 합니다.

유지 보수 모드를 사용할 경우 다음 지침을 고려하십시오.

- ESXi 호스트를 유지 보수 모드로 전환할 때는 **다른 호스트에서의 데이터 액세스 보장** 또는 **모든 데이터를 다른 호스트로 이동**과 같은 데이터 제거 모드를 선택해야 합니다.
- vSAN 클러스터의 멤버 호스트가 유지 보수 모드로 전환되면 해당 멤버 호스트가 더 이상 클러스터에 스토리지를 제공하지 않으므로 클러스터 용량이 자동으로 줄어듭니다.
- 가상 시스템의 계산 리소스가 유지 보수 모드로 전환 중인 호스트에 없을 수 있으며 가상 시스템을 위한 스토리지 리소스가 클러스터 내의 임의의 위치에 있을 수 있습니다.
- **데이터 액세스 지원 보장** 모드는 가상 시스템 실행에 꼭 필요한 구성 요소만 호스트에서 마이그레이션하기 때문에 **데이터 액세스 지원 보장** 모드가 **모든 데이터 제거** 모드보다 빠릅니다. 이 모드에서 장애가 발생할 경우 가상 시스템의 가용성이 영향을 받습니다. **데이터 액세스 지원 보장** 모드를 선택하면 장애 발생 시 데이터가 다시 보호되지 않으며 예기치 않은 데이터 손실이 발생할 수 있습니다.
- **모든 데이터 제거** 모드를 선택하는 경우, 리소스를 사용할 수 있고 **허용할 수 있는 장애의 기본 수준**이 1 이상으로 설정되어 있으면 장애 시 데이터가 자동으로 다시 보호됩니다. 이 모드에서는 호스트의 모든 구성 요소가 마이그레이션되고 호스트에 있는 데이터의 양에 따라 마이그레이션이 더 오래 걸릴 수 있습니다. **모든 데이터 제거** 모드를 사용할 경우 가상 시스템은 계획된 유지 보수 중에도 장애를 허용할 수 있습니다.
- 호스트가 3개인 클러스터를 사용하는 경우에는 서버를 유지 보수 모드로 전환할 때 **모든 데이터 제거**를 선택할 수 없습니다. 가용성을 극대화하려면 호스트가 4개 이상인 클러스터를 설계하는 것을 고려해야 합니다.

호스트를 유지 보수 모드로 전환하기 전에 다음을 확인해야 합니다.

- **모든 데이터 제거** 모드를 사용하는 경우에는 **허용할 수 있는 장애의 기본 수준** 정책 요구 사항을 충족하기에 충분한 호스트와 용량이 클러스터에 있는지 확인해야 합니다.
- 나머지 호스트에 플래시 읽기 캐시 예약을 처리하기에 충분한 플래시 용량이 있는지 확인합니다. `vsan.whatif_host_failures RVC` 명령을 실행하여 호스트당 현재 용량 사용을 분석할 수 있습니다. 이 정보를 통해 단일 호스트 장애가 클러스터의 공간 부족을 일으킬 수 있는지 여부와 클러스터 용량, 캐시 예약 및 클러스터 구성 요소에 영향을 미칠 수 있는지 여부를 판단할 수 있습니다. RVC 명령에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.
- 선택한 경우 나머지 호스트에 스트라이프 너비 정책 요구 사항을 처리하기 위한 충분한 용량 디바이스가 있는지 확인합니다.
- 유지 보수 모드로 전환되는 호스트에서 마이그레이션해야 하는 데이터 양을 처리하기 위한 충분한 사용 가능 용량이 나머지 호스트에 있는지 확인합니다.



[유지 보수 모드 확인] 대화상자에는 유지 보수 작업을 안내하는 정보가 제공됩니다. 각 데이터 제거 옵션의 효과를 볼 수 있습니다.

- 작업을 수행하는 데 사용할 수 있는 용량이 충분히 있는지 여부
- 이동할 데이터의 양
- 비준수 상태로 전환될 개체의 수
- 액세스할 수 없는 상태가 될 개체의 수

vSAN 클러스터의 멤버를 유지 보수 모드로 전환

vSAN 클러스터의 멤버인 호스트를 종료, 재부팅 또는 연결 해제하기 전에 해당 호스트를 유지 보수 모드로 전환해야 합니다. 호스트를 유지 보수 모드로 전환할 때는 **다른 호스트에서의 데이터 액세스 보장** 또는 **모든 데이터를 다른 호스트로 이동**과 같은 데이터 제거 모드를 선택해야 합니다.

vSAN 클러스터의 멤버 호스트가 유지 보수 모드로 전환되면 해당 멤버 호스트가 더 이상 클러스터에 용량을 제공하지 않으므로 클러스터 용량이 자동으로 줄어듭니다.

필수 조건

선택한 옵션에 필요한 기능이 환경에 있는지 확인합니다.

프로시저

- 1 호스트를 마우스 오른쪽 버튼으로 클릭하고 **유지 보수 모드 > 유지 보수 모드 설정**을 선택합니다.

2 제거 모드를 선택하고 **확인**을 클릭합니다.

| 옵션 | 설명 |
|-----------------------------|--|
| 다른 호스트에서의 데이터 액세스 보장 | <p>기본 옵션입니다. 호스트의 전원을 끄거나 호스트를 클러스터에서 제거할 때 vSAN은 이 호스트에 있는 모든 액세스 가능 가상 시스템이 액세스 가능한 상태를 계속 유지하도록 합니다. 업그레이드 설치와 같이 호스트를 클러스터에서 일시적으로 제외하고 나중에 클러스터에 다시 포함하려는 경우 이 옵션을 선택합니다. 호스트를 클러스터에서 영구적으로 제거하려는 경우에는 이 옵션이 적합하지 않습니다.</p> <p>일반적으로 일부 데이터만 제거해야 합니다. 그러나 가상 시스템은 제거 중 VM 스토리지 정책을 더 이상 완전하게 준수하지 않을 수 있습니다. 즉, 모든 해당 복제본에 액세스할 수 없을 수 있습니다. 호스트가 유지 보수 모드에 있고 허용할 수 있는 장애의 기본 수준이 1로 설정되어 있는 상태에서 장애가 발생할 경우 클러스터에서 데이터 손실이 발생할 수 있습니다.</p> <p>참고 이는 3개의 장애 도메인으로 구성된 vSAN 클러스터 또는 3개 호스트 클러스터를 사용 중인 경우 사용할 수 있는 유일한 제거 모드입니다.</p> |
| 모든 데이터를 다른 호스트로 이동 | <p>vSAN이 모든 데이터를 클러스터의 다른 호스트로 전송하고 영향을 받는 구성 요소에 대한 가용성 준수 상태를 유지하거나 수정하고 클러스터에 충분한 리소스가 있는 경우 데이터를 보호합니다. 호스트를 영구적으로 마이그레이션하려는 경우에 이 옵션을 선택합니다. 클러스터의 마지막 호스트에서 데이터를 전송하는 경우 가상 시스템을 다른 데이터스토어로 마이그레이션한 후 호스트를 유지 보수 모드로 설정해야 합니다.</p> <p>이 제거 모드를 선택하면 가장 많은 양의 데이터가 전송되므로 시간과 리소스가 가장 많이 소모됩니다. 호스트가 유지 보수로 전환되면 모든 가상 시스템이 해당 스토리지 구성 요소에 액세스할 수 있고 할당된 스토리지 정책을 계속해서 준수할 수 있도록 선택한 호스트의 로컬 스토리지에 있는 모든 구성 요소가 클러스터의 어느 곳으로 마이그레이션됩니다.</p> <p>참고 호스트에 데이터가 있는 가상 시스템 개체에 액세스할 수 없으며 해당 개체가 완전히 제거되지 않은 경우에는 호스트를 유지 보수 모드로 전환할 수 없습니다.</p> |
| 데이터 이동 안 함 | <p>vSAN이 이 호스트에서 데이터를 전혀 제거하지 않습니다. 호스트의 전원을 끄거나 호스트를 클러스터에서 제거하면 일부 가상 시스템에 액세스하지 못하게 될 수도 있습니다.</p> |

장애 도메인이 3개인 클러스터는 **모든 데이터 제거** 모드를 사용할 수 없고 장애 후 데이터를 다시 보호할 수 없는 등 호스트가 3개인 클러스터와 동일한 제한 사항을 가지고 있습니다.

후속 작업

클러스터의 데이터 마이그레이션 진행률을 추적할 수 있습니다. [“vSAN 클러스터의 다시 동기화 작업 모니터링,”](#) (134 페이지)를 참조하십시오.

vSAN 클러스터에서 장애 도메인 관리

vSAN 클러스터가 데이터 센터에서 여러 랙 또는 블레이드 서버 새시에 걸쳐 있고 호스트를 랙 또는 새시 장애로부터 보호하려는 경우 장애 도메인을 생성하고 각 장애 도메인에 호스트를 하나 이상 추가할 수 있습니다.

장애 도메인은 데이터 센터 내의 물리적 위치에 따라 그룹화된 하나 이상의 vSAN 호스트로 구성되어 있습니다. 장애 도메인을 구성하는 경우 vSAN은 전체 물리적 랙의 장애뿐만 아니라 단일 호스트, 용량 디바이스, 네트워크 링크 또는 장애 도메인 전용 네트워크 스위치의 장애도 허용할 수 있습니다.

클러스터의 **허용할 수 있는 장애의 기본 수준** 정책은 가상 시스템이 허용하도록 프로비저닝된 장애 수에 따라 다릅니다. 예를 들어 특정 가상 시스템이 **허용할 수 있는 장애의 기본 수준**이 1로 설정되어 구성되어 있고((PFTT = 1)) 여러 장애 도메인을 사용하는 경우, vSAN은 전체 랙의 장애를 포함하여 장애 도메인에서 모든 종류의 단일 장애 및 모든 구성 요소의 단일 장애를 허용할 수 있습니다.

랙에서 장애 도메인을 구성하고 새로운 가상 시스템을 프로비저닝하는 경우 vSAN은 복제본 및 감시와 같은 보호 개체가 서로 다른 장애 도메인에 배치되도록 합니다. 예를 들어 가상 시스템의 스토리지 정책에 **허용할 수 있는 장애의 기본 수준**이 N으로 설정된 경우((PFTT = n)), vSAN은 클러스터에 최소 $2 \times n + 1$ 개의 장애 도메인을 필요로 합니다. 이 정책을 사용하여 장애 도메인이 포함된 클러스터에서 가상 시스템을 프로비저닝하는 경우 연관된 가상 시스템 개체의 복사본은 별도의 랙에 저장됩니다.

최소 3개의 장애 도메인이 필요합니다. 최상의 결과를 얻으려면 클러스터에서 4개 이상의 장애 도메인을 구성하십시오. 장애 도메인 3개가 포함된 클러스터는 장애 후 데이터를 다시 보호할 수 없고 **전체 데이터 마이그레이션** 모드를 사용할 수 없는 등 호스트가 3개인 클러스터와 동일한 제한 사항을 가지고 있습니다. 장애 도메인 설계 및 크기 조정에 대한 자세한 내용은 **“vSAN 장애 도메인 설계 및 크기 조정,”** (32 페이지) 항목을 참조하십시오.

16개의 호스트가 포함된 vSAN 클러스터가 있는 시나리오를 고려합니다. 호스트는 4개의 랙에 걸쳐 있습니다. 즉, 랙 하나에 4개의 호스트가 있습니다. 전체 랙 장애를 허용하려면 각 랙에 대해 장애 도메인을 생성해야 합니다. 이러한 용량을 가진 클러스터는 1로 설정된 **허용할 수 있는 장애의 기본 수준**을 허용하도록 구성할 수 있습니다. **허용할 수 있는 장애의 기본 수준**이 2로 설정된 가상 시스템을 허용하도록 클러스터를 구성하려면 클러스터에 장애 도메인 5개를 구성해야 합니다.

랙에 장애가 발생하면 클러스터에서 랙의 CPU 및 메모리를 비롯한 모든 리소스를 사용할 수 없게 됩니다. 잠재적인 랙 장애의 영향을 줄이려면 장애 도메인을 더 작은 크기로 구성해야 합니다. 이렇게 하면 랙 장애가 발생한 후에도 클러스터에서 사용할 수 있는 총 리소스 양이 증가합니다.

장애 도메인을 사용할 때 다음 모범 사례를 따르십시오.

- vSAN 클러스터에 장애 도메인을 3개 이상 구성합니다. 최상의 결과를 얻으려면 장애 도메인을 4개 이상 구성하십시오.
- 어느 장애 도메인에도 포함되지 않은 호스트는 고유한 단일 호스트 장애 도메인으로 간주됩니다.
- 모든 vSAN 호스트를 장애 도메인에 할당할 필요는 없습니다. vSAN 환경을 보호하기 위해 장애 도메인을 사용하기로 결정한 경우 동일한 크기의 장애 도메인 생성을 고려합니다.
- 다른 클러스터로 이동하는 경우 vSAN 호스트는 해당하는 장애 도메인 할당을 유지합니다.
- 장애 도메인을 설계할 때 일정한 호스트 수로 장애 도메인을 구성하는 것이 좋습니다.

장애 도메인 설계에 대한 지침은 **“vSAN 장애 도메인 설계 및 크기 조정,”** (32 페이지) 항목을 참조하십시오.

- 호스트를 원하는 수만큼 장애 도메인에 추가할 수 있습니다. 각 장애 도메인은 호스트를 하나 이상 포함해야 합니다.

vSAN 클러스터에서 새 장애 도메인 생성

랙 장애 시에도 원활한 가상 시스템 개체의 실행을 위해 호스트를 여러 장애 도메인으로 그룹화할 수 있습니다.

장애 도메인이 포함된 클러스터에서 가상 시스템을 프로비저닝하면 vSAN은 가상 시스템 개체의 감시 및 복제본과 같은 보호 구성 요소를 여러 장애 도메인으로 분산합니다. 그 결과 vSAN 환경은 단일 호스트, 스토리지 디스크 또는 네트워크 장애 이외에도 랙 전체의 장애도 허용할 수 있게 됩니다.

필수 조건

- 고유한 장애 도메인 이름을 선택합니다. vSAN은 클러스터에서 중복되는 장애 도메인 이름을 지원하지 않습니다.
- ESXi 호스트의 버전을 확인합니다. 6.0 이상의 호스트만 장애 도메인에 포함할 수 있습니다.
- vSAN 호스트가 온라인 상태인지 확인합니다. 하드웨어 구성 문제로 인해 사용할 수 없거나 오프라인 상태인 호스트는 장애 도메인에 할당할 수 없습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.

- 2 구성 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 새 **장애 도메인 생성** 아이콘(+)을 클릭합니다.
- 5 장애 도메인 이름을 입력합니다.
- 6 표시 드롭다운 메뉴에서 **장애 도메인에 속하지 않은 호스트**를 선택하여 장애 도메인에 할당되지 않은 호스트 목록을 보거나, **모든 호스트 표시**를 선택하여 클러스터에 있는 모든 호스트를 봅니다.
- 7 장애 도메인에 추가할 호스트를 하나 이상 선택합니다.
장애 도메인은 비워 둘 수 없습니다. 장애 도메인에 포함할 호스트를 하나 이상 선택해야 합니다.
- 8 **확인**을 클릭합니다.
선택한 호스트가 장애 도메인에 나타납니다.

선택한 장애 도메인으로 호스트 이동

호스트를 vSAN 클러스터의 선택한 장애 도메인으로 이동할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 구성 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 장애 도메인을 선택하고 **선택한 장애 도메인으로 호스트 이동** 아이콘()을 클릭합니다.
- 5 페이지 맨 아래의 표시 드롭다운 메뉴에서 **장애 도메인에 속하지 않은 호스트**를 선택하여 장애 도메인에 추가할 수 있는 호스트를 보거나, **모든 호스트 표시**를 선택하여 클러스터의 모든 호스트를 봅니다.
- 6 장애 도메인에 추가할 호스트를 선택합니다.
- 7 **확인**을 클릭합니다.
선택한 호스트가 장애 도메인에 나타납니다.

기존 장애 도메인으로 호스트 이동

호스트를 vSAN 클러스터의 기존 장애 도메인으로 이동할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 구성 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 호스트를 하나 이상 선택하고 **호스트를 장애 도메인으로 이동** 아이콘()을 클릭합니다.
- 5 장애 도메인을 선택하고 **확인**을 클릭합니다.
각 장애 도메인은 호스트를 하나 이상 포함해야 합니다. 이동하는 호스트가 소스 장애 도메인의 유일한 호스트인 경우 vSAN은 클러스터에서 빈 장애 도메인을 삭제합니다.

장애 도메인 외부로 호스트 이동

요구 사항에 따라 호스트를 장애 도메인 외부로 이동할 수 있습니다.

필수 조건

호스트가 온라인 상태인지 확인합니다. 장애 도메인에서 오프라인 상태이거나 사용할 수 없는 호스트는 이동할 수 없습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 이동할 호스트를 선택하고 **장애 도메인 외부로 호스트 이동** 아이콘()을 클릭합니다.
- 5 **예**를 클릭합니다.

선택한 호스트가 더 이상 장애 도메인의 일부가 아닙니다. 장애 도메인의 일부가 아닌 모든 호스트는 고유한 단일 호스트 장애 도메인에 있는 것으로 간주됩니다.

후속 작업

호스트를 장애 도메인에 추가할 수 있습니다. “[기존 장애 도메인으로 호스트 이동](#),” (115 페이지)를 참조하십시오.

장애 도메인 이름 변경

vSAN 클러스터에서 기존 장애 도메인의 이름을 변경할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 이름을 변경할 장애 도메인을 선택하고 **선택한 장애 도메인 이름 변경** 아이콘()을 클릭합니다.
- 5 새 장애 도메인 이름을 입력합니다.
- 6 **확인**을 클릭합니다.

새 이름이 장애 도메인 목록에 나타납니다.

선택한 장애 도메인 제거

장애 도메인이 더 이상 필요하지 않은 경우 vSAN 클러스터에서 제거할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **장애 도메인 및 확장된 클러스터**를 클릭합니다.
- 4 삭제할 장애 도메인을 선택하고 **선택한 장애 도메인 제거** 아이콘()을 클릭합니다.

5 예를 클릭합니다.

장애 도메인의 모든 호스트가 제거되고 선택된 장애 도메인이 vSAN 클러스터에서 삭제됩니다. 장애 도메인의 일부가 아닌 각 호스트는 고유한 단일 호스트 장애 도메인에 있는 것으로 간주됩니다.

vSAN iSCSI 대상 서비스 사용

iSCSI 대상 서비스를 사용하여 vSAN 클러스터 외부에 있는 호스트 및 물리적 워크로드가 vSAN 데이터스토어에 액세스할 수 있도록 합니다.

이 기능은 원격 호스트에 있는 iSCSI 이니시에이터가 블록 수준 데이터를 vSAN 클러스터의 스토리지 디바이스에 있는 iSCSI 대상으로 전송할 수 있도록 합니다.

vSAN iSCSI 대상 서비스를 구성한 후 원격 호스트에서 vSAN iSCSI 대상을 검색할 수 있습니다. vSAN iSCSI 대상을 검색하려면 vSAN 클러스터의 호스트 IP 주소와 iSCSI 대상의 TCP 포트를 사용합니다. vSAN iSCSI 대상의고가용성을 보장하기 위해 iSCSI 애플리케이션에 대한 MultiPath 지원을 구성합니다. 2개 이상의 호스트의 IP 주소를 사용하여 MultiPath를 구성할 수 있습니다.

참고 vSAN iSCSI 대상 서비스는 다른 vSphere, ESXi 클라이언트, 이니시에이터 및 타사 하이퍼바이저 또는 RDM(원시 디바이스 매핑)을 사용한 마이그레이션을 지원하지 않습니다.

vSAN iSCSI 대상 서비스는 다음 CHAP 인증 방법을 지원합니다.

| | |
|----------------|---|
| CHAP | CHAP 인증에서는 대상이 이니시에이터를 인증하지만 이니시에이터는 대상을 인증하지 않습니다. |
| 상호 CHAP | 상호 CHAP 인증에서는 추가 보안 수준을 사용하여 이니시에이터에서 대상을 인증할 수 있습니다. |

iSCSI 대상

스토리지 블록을 LUN(논리 단위 번호)으로 제공하는 하나 이상의 iSCSI 대상을 추가할 수 있습니다. vSAN은 고유 IQN(iSCSI 정규화된 이름)으로 각 iSCSI 대상을 식별합니다. IQN을 사용하여 이니시에이터가 대상의 LUN에 액세스할 수 있도록 원격 iSCSI 이니시에이터에 대한 iSCSI 대상을 나타낼 수 있습니다.

각 iSCSI 대상에는 하나 이상의 LUN이 포함됩니다. 각 LUN의 크기를 정의하고 각 LUN에 vSAN 스토리지 정책을 할당하고 vSAN 클러스터에서 iSCSI 대상 서비스를 사용하도록 설정합니다. 스토리지 정책을 vSAN iSCSI 대상 서비스의 홈 개체에 대한 기본 정책으로 사용하도록 구성할 수 있습니다.

iSCSI 이니시에이터 그룹

지정된 iSCSI 대상에 대한 액세스 권한이 있는 iSCSI 이니시에이터 그룹을 정의할 수 있습니다. iSCSI 이니시에이터 그룹은 그룹 구성원인 이니시에이터에만 액세스하도록 제한합니다. iSCSI 이니시에이터 또는 이니시에이터 그룹을 정의하지 않을 경우 모든 iSCSI 이니시에이터가 각 대상에 액세스할 수 있습니다.

고유 이름으로 각 iSCSI 이니시에이터 그룹을 식별합니다. 하나 이상의 iSCSI 이니시에이터를 그룹 멤버로 추가할 수 있습니다. 이니시에이터의 IQN을 구성된 이니시에이터 이름으로 사용합니다.

iSCSI 대상 서비스를 사용하도록 설정

iSCSI 대상 및 LUN을 생성하고 iSCSI 이니시에이터 그룹을 정의하려면 vSAN 클러스터에서 iSCSI 대상 서비스를 사용하도록 설정해야 합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다. vSAN에서 **일반**을 클릭합니다.

- 3 vSAN iSCSI 대상 서비스에 대한 **편집** 버튼을 클릭합니다.
- 4 **vSAN iSCSI 대상 서비스 사용** 확인란을 선택합니다. 이때 기본 네트워크, TCP 포트 및 인증 방법을 선택할 수 있습니다. 또한 vSAN 스토리지 정책을 선택할 수 있습니다.
- 5 **확인**을 클릭합니다.

후속 작업

iSCSI 대상 서비스가 사용하도록 설정된 후 iSCSI 대상 및 LUN을 생성하고 iSCSI 이니시에이터 그룹을 정의할 수 있습니다.

iSCSI 대상 생성

iSCSI 대상 및 연결된 LUN을 생성하고 편집할 수 있습니다.

필수 조건

iSCSI 대상 서비스가 사용하도록 설정되었는지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다. vSAN에서 **iSCSI 대상**을 클릭합니다.
- 3 [vSAN iSCSI 대상] 섹션에서 **새 iSCSI 대상 추가(+)** 아이콘을 클릭합니다.
새 iSCSI 대상 대화상자가 표시됩니다. 대상 IQN이 자동으로 생성됩니다.
- 4 대상 별칭을 입력합니다. 이 대상에 대한 네트워크, TCP 포트 및 인증 방법을 편집할 수도 있습니다.
- 5 (선택 사항) 대상에 대한 LUN을 정의하려면 **iSCSI 대상에 대한 첫 번째 LUN 추가** 확인란을 클릭하고 LUN의 크기를 입력합니다.
- 6 **확인**을 클릭합니다.

후속 작업

이 대상에 액세스할 수 있는 iSCSI 이니시에이터 목록을 정의합니다.

iSCSI 대상에 LUN 추가

iSCSI 대상에 하나 이상의 LUN을 추가하거나 기존 LUN을 편집할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다. vSAN에서 **iSCSI 대상**을 클릭합니다.
- 3 페이지의 [대상 세부 정보] 섹션에서 **LUN** 탭을 선택합니다.
- 4 **대상에 새 iSCSI LUN 추가(+)** 아이콘을 클릭합니다.
대상에 LUN 추가 대화상자가 표시됩니다.
- 5 LUN의 크기를 입력합니다.
iSCSI 대상 서비스에 대해 구성된 vSAN 스토리지 정책이 자동으로 할당됩니다. 각 LUN에 다른 정책을 할당할 수 있습니다.
- 6 **확인**을 클릭합니다.

iSCSI 이니시에이터 그룹 생성

iSCSI 이니시에이터 그룹을 생성하여 iSCSI 대상에 대한 액세스 제어를 제공할 수 있습니다. 이니시에이터 그룹의 구성원인 이니시에이터만 iSCSI 대상에 액세스할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다. vSAN에서 **iSCSI 이니시에이터 그룹**을 클릭합니다.
- 3 [vSAN iSCSI 이니시에이터 그룹] 섹션에서 **새 iSCSI 이니시에이터 그룹 추가(+)** 아이콘을 클릭합니다.
새 vSAN iSCSI 이니시에이터 그룹 대화상자가 표시됩니다.
- 4 iSCSI 이니시에이터 그룹 이름을 입력합니다.
- 5 (선택 사항) 이니시에이터 그룹에 구성원을 추가하려면 각 구성원의 IQN을 입력합니다.
다음 형식을 사용하여 구성원 IQN을 입력합니다.
iqn.YYYY-MM.domain:name
형식 설명:
 - YYYY = 연도(예: 2016)
 - MM = 월(예: 09)
 - domain = 이니시에이터가 위치하는 도메인
 - name = 구성원 이름(선택 사항)
- 6 **확인**을 클릭합니다.

후속 작업

iSCSI 이니시에이터 그룹에 구성원을 추가합니다.

iSCSI 이니시에이터 그룹에 대상 할당

iSCSI 이니시에이터 그룹에 iSCSI 대상을 할당할 수 있습니다. 이니시에이터 그룹의 구성원인 이니시에이터만 할당된 대상에 액세스할 수 있습니다.

필수 조건

기존 iSCSI 이니시에이터 그룹이 있는지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다. vSAN에서 **iSCSI 이니시에이터 그룹**을 클릭합니다.
- 3 [그룹 세부 정보] 섹션에서 **액세스 가능 대상** 탭을 선택합니다.
- 4 **iSCSI 이니시에이터 그룹에 액세스 가능한 새 대상 추가(+)** 아이콘을 클릭합니다.
이니시에이터 그룹에 대한 대상에 액세스 허용 대화상자가 표시됩니다.
- 5 **필터** 탭의 사용할 수 있는 대상 목록에서 대상을 선택합니다.
[선택한 개체] 탭에 현재 선택된 대상이 표시됩니다.
- 6 **확인**을 클릭합니다.

vSAN iSCSI 대상 서비스 모니터링

iSCSI 대상 서비스를 모니터링하여 iSCSI 대상 구성 요소의 물리적 배치를 보고 실패한 구성 요소를 확인할 수 있습니다. 또한 iSCSI 대상 서비스의 상태를 모니터링할 수 있습니다.

필수 조건

vSAN iSCSI 대상 서비스를 사용하도록 설정하고 대상 및 LUN을 생성했는지 확인합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터를 찾습니다.
- 2 **모니터**를 클릭하고 **vSAN**을 선택합니다.
- 3 **iSCSI 대상**을 클릭합니다.
페이지 위쪽에 iSCSI 대상 및 LUN이 나열됩니다.
- 4 대상 별칭을 클릭하여 해당 상태를 봅니다.
페이지의 아래쪽에 있는 [물리적 디스크 배치] 탭에 대상의 데이터 구성 요소가 있는 위치가 표시됩니다. [규정 준수 실패] 탭에 실패한 구성 요소가 표시됩니다.
- 5 LUN을 클릭하여 해당 상태를 봅니다.
페이지의 아래쪽에 있는 [물리적 디스크 배치] 탭에 대상의 데이터 구성 요소가 있는 위치가 표시됩니다. [규정 준수 실패] 탭에 실패한 구성 요소가 표시됩니다.

하이브리드 vSAN 클러스터를 플래시 전용 클러스터로 마이그레이션

하이브리드 vSAN 클러스터의 디스크 그룹을 플래시 전용 디스크 그룹으로 마이그레이션할 수 있습니다.

vSAN 하이브리드 클러스터는 용량 계층에 자기 디스크를 사용하고 캐시 계층에 플래시 디바이스를 사용합니다. 캐시 계층 및 용량 계층에 플래시 디바이스를 사용하도록 클러스터의 디스크 그룹 구성을 변경할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 클러스터의 각 호스트에 대한 하이브리드 디스크를 제거합니다.
 - a **구성** 탭을 클릭합니다.
 - b vSAN에서 **디스크 관리**를 클릭합니다.
 - c [디스크 그룹]에서 제거할 디스크 그룹을 선택하고 **디스크 그룹 제거** 아이콘()을 클릭합니다.
 - d 마이그레이션 모드로 **전체 데이터 마이그레이션**을 선택하고 **예**를 클릭합니다.
- 3 호스트에서 물리적 HDD 디스크를 제거합니다.
- 4 호스트에 플래시 디바이스를 추가합니다.
플래시 디바이스에 파티션이 없는지 확인합니다.
- 5 각 호스트에서 플래시 전용 디스크 그룹을 생성합니다.

vSAN 클러스터 전원 끄기

vSAN 클러스터의 전원을 끌 수 있습니다.

필수 조건

vSAN 클러스터에서 vCenter Server VM이 실행 중인 경우 VM을 첫 번째 호스트로 마이그레이션하거나 현재 VM이 실행되고 있는 호스트를 기록합니다.

프로시저

- 1 vSAN 클러스터에서 실행 중인 모든 가상 시스템의 전원을 끕니다.
vCenter Server 가상 시스템의 전원을 마지막에 꺼야 합니다.
- 2 클러스터를 구성하는 모든 ESXi 호스트를 유지 보수 모드로 전환합니다.
esxcli 명령을 실행하여 vSAN을 유지 보수 모드로 전환 상태로 설정합니다.
`esxcli system maintenanceMode set -e true -m noAction`
- 3 ESXi 호스트의 전원을 끕니다.

vSAN 정책 사용

vSAN을 사용할 경우 성능, 가용성 등의 가상 시스템 스토리지 요구 사항을 정책에 정의할 수 있습니다. vSAN은 vSAN 데이터스토어에 배포된 각 가상 시스템에 하나 이상의 스토리지 정책이 할당되도록 합니다.

스토리지 정책이 할당되면 가상 시스템이 생성될 때 스토리지 정책 요구 사항이 vSAN 계층에 푸시됩니다. 가상 디바이스는 성능 및 가용성 요구 사항을 충족하기 위해 vSAN 데이터스토어 전체에 분산됩니다.

vSAN은 스토리지 제공자를 사용하여 기본 스토리지에 대한 정보를 vCenter Server에 제공합니다. 이 정보를 통해 가상 시스템 배치에 대한 적절한 결정을 내리고 스토리지 환경을 모니터링할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN 정책 정보,”](#) (123 페이지)
- [“vSAN 스토리지 제공자 보기,”](#) (126 페이지)
- [“vSAN 기본 스토리지 정책 정보,”](#) (126 페이지)
- [“vSAN 데이터스토어에 기본 스토리지 정책 할당,”](#) (128 페이지)
- [“vSAN에 대한 가상 시스템 스토리지 정책 정의,”](#) (128 페이지)

vSAN 정책 정보

vSAN 스토리지 정책은 가상 시스템의 스토리지 요구 사항을 정의합니다. 이러한 정책은 필요한 서비스 수준을 보장하기 위해 가상 시스템 스토리지 개체가 데이터스토어 내에 프로비저닝되고 할당되는 방법을 결정합니다.

호스트 클러스터에서 vSAN을 사용하도록 설정하면 단일 vSAN 데이터스토어가 생성되고 기본 스토리지 정책이 데이터스토어에 할당됩니다.

가상 시스템의 스토리지 요구 사항을 알고 있는 경우 데이터스토어가 제공하는 기능을 참조하는 스토리지 정책을 생성할 수 있습니다. 서로 다른 유형 또는 등급의 요구 사항을 캡처하는 여러 개의 정책을 생성할 수 있습니다.

vSAN 데이터스토어에 배포된 각 가상 시스템에는 가상 시스템 스토리지 정책이 하나 이상 할당됩니다. 스토리지 정책은 가상 시스템을 생성하거나 편집할 때 할당할 수 있습니다.

참고 가상 시스템에 스토리지 정책을 할당하지 않으면 vSAN에서 기본 정책을 할당합니다. 기본 정책에는 **허용할 수 있는 장애의 기본 수준**이 1로 설정되며, 개체당 하나의 디스크 스트라이프 및 썬 프로비저닝된 가상 디스크가 있습니다.

VM 스왑 개체와 VM 스냅샷 메모리 개체는 VM에 할당된 스토리지 정책을 준수하지 않습니다. 이러한 개체는 **허용할 수 있는 장애의 기본 수준**이 1로 설정되어 구성됩니다. 이러한 개체의 가용성은 **허용할 수 있는 장애의 기본 수준** 값이 다르게 지정된 정책이 할당된 개체의 가용성과 다를 수 있습니다.

표 12-1. 스토리지 정책 특성

| 기능 | 설명 |
|---------------------|---|
| 개체당 디스크 스트라이프 수 | <p>가상 시스템 개체의 각 복제본이 스트라이프되는 용량 디바이스의 최소 수입니다. 값이 1보다 크면 성능이 더 향상되겠지만 시스템 리소스도 더 많이 소모됩니다.</p> <p>기본값은 1이고 최대값은 12입니다.</p> <p>기본 스트라이프 값을 변경하지 마십시오.</p> <p>하이브리드 환경에서는 디스크 스트라이프가 자기 디스크로 분산됩니다. 플래시 전용 구성의 경우 스트라이핑은 용량 계층을 구성하는 플래시 디바이스로 분산됩니다. vSAN 환경에 요청을 수용하기에 충분한 용량 디바이스가 있는지 확인합니다.</p> |
| Flash Read Cache 예약 | <p>가상 시스템 개체에 대해 읽기 캐시로 예약된 플래시 용량입니다. VMDK(가상 시스템 디스크) 개체의 논리적 크기에 대한 백분율로 지정됩니다. 예약된 플래시 용량은 다른 개체가 사용할 수 없습니다. 예약되지 않은 플래시는 모든 개체 간에 균등하게 공유됩니다. 이 옵션은 특정 성능 문제를 해결할 때만 사용하십시오.</p> <p>캐시 예약을 설정할 필요가 없습니다. 캐시 예약 설정은 항상 개체와 함께 포함되기 때문에 읽기 캐시 예약을 설정하면 가상 시스템 개체를 이동할 때 문제가 발생할 수 있습니다.</p> <p>Flash Read Cache 예약 스토리지 정책 특성은 하이브리드 구성에 대해서만 지원됩니다. 플래시 전용 클러스터에 사용할 VM 스토리지 정책을 정의할 때는 이 특성을 사용하면 안 됩니다.</p> <p>기본값은 0%이고, 최대값은 100%입니다.</p> <p>참고 기본적으로 vSAN은 요청 시 읽기 캐시를 스토리지 개체에 동적으로 할당합니다. 이 기능은 리소스를 가장 유연하고 최적으로 사용하는 방법입니다. 따라서 일반적으로 이 매개 변수의 기본값인 0을 변경할 필요가 없습니다.</p> <p>성능 문제를 해결하기 위해 이 값을 높일 때는 주의가 필요합니다. 여러 가상 시스템에서 캐시 예약을 과다 프로비저닝하면 과다 예약에 플래시 디바이스 공간이 낭비될 수 있습니다. 이 경우 지정된 시간에 해당 공간이 필요한 워크로드에 캐시 예약을 제공하지 못할 수 있습니다. 이와 같은 공간의 낭비 및 사용 불가능 문제는 성능 저하로 이어질 수 있습니다.</p> |
| 허용할 수 있는 장애의 기본 수준 | <p>가상 시스템 개체가 허용할 수 있는 호스트 및 디바이스 장애 수를 정의합니다. 허용되는 n개의 장애에 대해 기록된 각 데이터 부분(RAID 5 또는 RAID 6을 사용하는 경우 패리티 복사본 포함)은 n+1개의 위치에 저장됩니다.</p> <p>가상 시스템을 프로비저닝할 때 스토리지 정책을 선택하지 않은 경우 vSAN이 이 정책을 기본 가상 시스템 스토리지 정책으로 할당합니다.</p> <p>장애 도메인이 구성된 경우에는 용량을 제공하는 호스트가 있는 장애 도메인이 2n+1개 필요합니다. 장애 도메인의 일부가 아닌 호스트는 고유한 단일 호스트 장애 도메인으로 간주됩니다.</p> <p>기본값은 1입니다. 최대값은 3입니다.</p> <p>참고 vSAN이 가상 시스템 개체의 단일 미러 복사본을 보호하지 않도록 하려면 허용할 수 있는 장애의 기본 수준을 0으로 지정할 수 있습니다. 하지만 호스트가 유지 보수 모드에 들어갈 때 비정상적인 지연이 발생할 수 있습니다. 유지 보수 작업이 성공적으로 완료되려면 vSAN이 개체를 호스트에서 제거해야 하기 때문에 지연 시간이 발생합니다. 허용할 수 있는 장애의 기본 수준을 0으로 설정하면 데이터가 보호되지 않으며 vSAN 클러스터에서 디바이스 장애가 발생할 경우 데이터가 손실될 수 있습니다.</p> <p>참고 스토리지 정책을 생성할 때 허용할 수 있는 장애의 기본 수준 값을 지정하지 않으면 vSAN은 VM 개체의 단일 미러 복사본을 생성합니다. 그러면 Virtual SAN이 단일 장애를 허용할 수 있습니다. 하지만 여러 구성 요소 장애가 발생할 경우에는 데이터가 위험할 수 있습니다.</p> <p>확장된 클러스터에서 가상 시스템 개체가 허용할 수 있는 호스트 및 디바이스 장애 수를 정의합니다. 허용할 수 있는 장애의 기본 수준과 허용할 수 있는 장애의 보조 수준을 함께 사용하여 단일 사이트 내의 개체에 대해 로컬 장애 보호 기능을 제공할 수 있습니다.</p> |

표 12-1. 스토리지 정책 특성 (계속)

| 기능 | 설명 |
|--------------------|--|
| 허용할 수 있는 장애의 보조 수준 | 확장된 클러스터에서 이 규칙은 단일 사이트 내에서 가상 시스템 개체가 허용할 수 있는 호스트 및 개체 장애 수를 정의합니다. 기본값은 1입니다. 최대값은 3입니다. |
| 선호도 | 확장된 클러스터에서 이 규칙은 허용할 수 있는 장애의 기본 수준 이 0으로 설정된 경우에만 사용할 수 있습니다. 선호도 규칙은 없음 , 기본 또는 보조 로 설정할 수 있습니다. 이 규칙을 사용하면 가상 시스템 개체를 확장된 클러스터에 있는 선택된 사이트로 제한할 수 있습니다. 기본값은 [없음]입니다. |
| 장애 프로비저닝 | 이 옵션을 예 로 설정하면 스토리지 정책에 지정된 허용할 수 있는 장애의 기본 수준 , 개체당 디스크 스트라이프 수 및 Flash Read Cache 예약 정책이 데이터스토어에 의해 충족되지 않더라도 개체가 프로비저닝됩니다. 이 매개 변수는 부트스트래핑 시나리오에 사용하거나 더 이상 표준 프로비저닝을 수행할 수 없는 운영 중단 시에 사용할 수 있습니다. 기본값인 아니오 는 대부분의 운영 환경에 허용됩니다. vSAN은 정책 요구 사항이 충족되지 않을 경우 가상 시스템을 프로비저닝하지 못하지만 사용자 정의 스토리지 정책은 성공적으로 생성합니다. |
| 개체 공간 예약 | 예약되거나, 가상 시스템 배포 시 씩 프로비저닝되어야 하는 VMDK(가상 시스템 디스크) 개체의 논리적 크기 비율입니다. 기본값은 0%이고, 최대값은 100%입니다. |
| 개체 체크섬 사용 안 함 | 이 옵션을 아니오 로 설정하면 개체가 체크섬 정보를 계산하여 해당 데이터의 무결성을 보장합니다. 이 옵션을 예 로 설정하면 개체가 체크섬 정보를 계산하지 않습니다. vSAN은 중단 간 체크섬을 사용하여 파일의 각 복사본이 소스 파일과 정확히 동일인지 확인함으로써 데이터의 무결성을 보장합니다. 시스템에서 읽기/쓰기 작업 중에 데이터의 유효성을 확인하고, 오류가 감지되면 vSAN이 데이터를 복구하거나 오류를 보고합니다. 체크섬 불일치가 감지되면 vSAN이 잘못된 데이터를 올바른 데이터로 덮어써서 데이터를 자동으로 복구합니다. 체크섬 계산 및 오류 수정은 백그라운드 작업으로 수행됩니다. 클러스터에서 모든 개체의 기본 설정은 아니오 이며, 이는 체크섬이 사용되도록 설정되었다는 의미입니다. |
| 장애 허용 방법 | 데이터 복제 방법을 성능 또는 용량에 대해 최적화하는지 여부를 지정합니다. RAID-1(미러링) - 성능 을 선택하면 vSAN이 개체 구성 요소를 배치하는 데 더 많은 디스크 공간을 사용하지만 더 나은 개체 액세스 성능을 제공합니다. RAID-5/6(이레이저 코딩) - 용량 을 선택하면 vSAN이 디스크 공간을 더 적게 사용하지만 성능이 저하됩니다. 장애 도메인이 4개 이상 있는 클러스터에 RAID-5/6(이레이저 코딩) - 용량 특성을 적용하여 RAID 5를 사용하고 허용할 수 있는 장애의 기본 수준 을 1로 설정할 수 있습니다. 장애 도메인이 6개 이상 있는 클러스터에 RAID-5/6(이레이저 코딩) - 용량 특성을 적용하여 RAID 6을 사용하고 허용할 수 있는 장애의 기본 수준 을 2로 설정할 수 있습니다. 허용할 수 있는 장애의 보조 수준 이 구성되어 있는 확장된 클러스터에서 이 규칙은 허용할 수 있는 장애의 보조 수준 에만 적용됩니다. RAID 5 또는 RAID 6에 대한 자세한 내용은 "RAID 5 또는 RAID 6 이레이저 코딩 사용," (73 페이지)을 참조하십시오. |
| 개체에 대한 IOPS 제한 | VMDK 같은 개체의 IOPS 제한을 정의합니다. IOPS는 I/O 작업의 수로 계산되며, 가중 크기가 사용됩니다. 시스템에서 기본 기반 크기인 32KB를 사용하는 경우 64KB I/O는 I/O 작업 두 개를 나타냅니다. IOPS 계산 시 읽기 및 쓰기는 동일하게 고려되지만 캐시 적중률과 순차성은 고려되지 않습니다. 디스크의 IOPS가 제한을 초과하면 I/O 작업이 조절됩니다. 개체에 대한 IOPS 제한 을 0으로 설정하면 IOPS 제한이 적용되지 않습니다. vSAN은 작업의 처음 1초 동안 또는 비활성 상태가 일정한 기간 지속된 후에 개체에 대해 IOPS 제한의 두 배 속도까지 허용합니다. |

가상 시스템 스토리지 정책으로 작업할 때는 스토리지 용량이 vSAN 클러스터의 스토리지 용량 사용에 미치는 영향을 이해해야 합니다. 스토리지 정책의 설계 및 크기 조정 고려 사항에 대한 자세한 내용은 3 장, “vSAN 클러스터 설계 및 크기 조정,” (21 페이지)을 참조하십시오.

vSAN 스토리지 제공자 보기

vSAN을 사용하도록 설정하면 vSAN 클러스터의 각 호스트에 대한 스토리지 제공자를 자동으로 구성 및 등록합니다.

vSAN 스토리지 제공자는 데이터스토어 기능을 vCenter Server로 전달하는 기본 소프트웨어 구성 요소입니다. 스토리지 기능은 일반적으로 키-값 쌍으로 표시되며, 여기서 키는 데이터스토어가 제공하는 특정 속성입니다. 값은 가상 시스템 홈 네임스페이스 개체 또는 가상 디스크 같이 프로비저닝된 개체에 대해 데이터스토어가 제공할 수 있는 숫자 또는 범위입니다 또한 태그를 사용하여 사용자 정의 스토리지 기능을 생성한 후 생성한 사용자 정의 스토리지 기능을 가상 시스템에 대한 스토리지 정책을 정의할 때 참조할 수도 있습니다. 데이터스토어에서 태그를 적용하고 사용하는 방법에 대한 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.

vSAN 스토리지 제공자는 기본 스토리지 기능 집합을 vCenter Server에 보고합니다. 또한 vSAN 계층과 통신하여 가상 시스템의 스토리지 요구 사항을 보고합니다. 스토리지 제공자에 대한 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.

vSAN은 다음 URL을 사용하여 vSAN 클러스터의 각 호스트에 대해 별도의 스토리지 제공자를 등록합니다.

`http://host_ip:8080/version.xml`

여기서 `host_ip`는 호스트의 실제 IP입니다.

스토리지 제공자가 등록되었는지 확인합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vCenter Server를 찾습니다.
- 2 구성 탭을 클릭하고 **스토리지 제공자**를 클릭합니다.

vSAN의 스토리지 제공자가 목록에 나타납니다. 각 호스트에 스토리지 제공자가 있지만 스토리지 제공자 하나만 활성 상태입니다. 다른 호스트에 속해 있는 스토리지 제공자는 대기 상태입니다. 활성 스토리지 제공자를 현재 사용 중인 호스트에서 장애가 발생하면 다른 호스트의 스토리지 제공자가 활성 상태가 됩니다.

참고 vSAN에서 사용하는 스토리지 제공자를 수동으로 등록 취소할 수 없습니다. vSAN 스토리지 제공자를 제거하거나 등록 취소해야 하는 경우 vSAN 클러스터에서 해당 호스트를 제거한 다음 호스트를 다시 추가합니다. 하나 이상의 스토리지 제공자가 활성 상태여야 합니다.

vSAN 기본 스토리지 정책 정보

vSAN을 사용하려면 vSAN 데이터스토어에 배포된 가상 시스템에 최소 하나의 스토리지 정책을 할당해야 합니다. 가상 시스템을 프로비저닝할 때 스토리지 정책을 가상 시스템에 명시적으로 할당하지 않으면 vSAN 기본 스토리지 정책이 가상 시스템에 할당됩니다.

기본 정책에는 vSAN 규칙 집합과 일련의 기본 스토리지 기능 집합이 포함되며 이는 일반적으로 vSAN 데이터스토어에 배포된 가상 시스템의 배치에 사용됩니다.

표 12-2. vSAN 기본 스토리지 정책 규칙

| 규칙 | 설정 |
|--------------------|----|
| 허용할 수 있는 장애의 기본 수준 | 1 |
| 개체당 디스크 스트라이프 수 | 1 |

표 12-2. vSAN 기본 스토리지 정책 규격 (계속)

| 규격 | 설정 |
|---|---|
| Flash Read Cache 예약 또는 읽기 캐시에 사용되는 플래시 용량 | 0 |
| 개체 공간 예약 | 0 참고 개체 공간 예약이 0으로 설정되면 가상 디스크가 기본적으로 쉰 프로비저닝됩니다. |
| 강제 프로비저닝 | 아니오 |

vSphere Web Client에서 **VM 스토리지 정책 > vSAN 기본 스토리지 정책 > 관리 > 규칙 집합 1: VSAN**으로 이동하여 기본 가상 시스템 스토리지 정책의 구성 설정을 검토할 수 있습니다.

최상의 결과를 위해서는 정책의 요구 사항이 기본 스토리지 정책에 정의된 것과 동일하더라도 자체 VM 스토리지 정책을 만들어 사용하는 방법을 고려하십시오. 사용자 정의 VM 스토리지 정책 생성에 대한 자세한 내용은 **“vSAN에 대한 가상 시스템 스토리지 정책 정의,”** (128 페이지)를 참조하십시오.

사용자 정의 스토리지 정책을 데이터스토어에 기본 정책으로 할당하면, vSAN은 지정된 데이터스토어에서 기본 스토리지 정책에 대한 연결을 자동으로 제거하고 사용자 정의 정책에 대한 설정을 적용합니다. 연결이 해제되면, 하나의 가상 시스템 스토리지 정책만 vSAN 데이터스토어에 기본 정책으로 할당할 수 있습니다.

특성

vSAN 기본 스토리지 정책에는 다음의 특성이 적용됩니다.

- 가상 시스템을 프로비저닝할 때 다른 vSAN 정책을 선택하지 않을 경우, 즉 [스토리지 선택] 페이지에서 **VM 스토리지 정책** 필드를 **데이터스토어 기본값**으로 설정한 경우에는 vSAN 기본 스토리지 정책이 모든 가상 시스템 개체에 할당됩니다. 스토리지 정책 사용에 대한 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.

참고 VM 스왑 및 VM 메모리 개체에는 **강제 프로비저닝**이 예로 설정된 vSAN 기본 스토리지 정책이 사용됩니다.

- vSAN 기본 정책은 vSAN 데이터스토어에만 적용됩니다. NFS 또는 VMFS 데이터스토어와 같은 비vSAN 데이터스토어에는 기본 스토리지 정책을 적용할 수 없습니다.
- 기본 가상 시스템 스토리지 정책은 vCenter Server의 모든 vSAN 데이터스토어와 호환되므로 기본 정책으로 프로비저닝된 가상 시스템 개체를 vCenter Server의 모든 vSAN 데이터스토어로 이동할 수 있습니다.
- 기본 정책을 복제하여 사용자 정의 스토리지 정책을 생성하기 위한 템플릿으로 사용할 수 있습니다.
- StorageProfile.View 권한이 있으면 기본 정책을 편집할 수 있습니다. 적어도 하나의 호스트가 포함된 vSAN 지원 클러스터가 하나 이상 있어야 합니다. VMware는 기본 스토리지 정책의 설정을 편집하지 말 것을 강력하게 권장합니다.
- 기본 정책의 이름과 설명 또는 vSAN 스토리지 제공자 규격은 편집할 수 없습니다. 정책 규칙을 비롯한 다른 모든 매개 변수는 편집할 수 있습니다.
- 기본 정책은 삭제할 수 없습니다.
- 가상 시스템 프로비저닝 중에 할당하는 정책에 vSAN에 관련된 규칙이 포함되어 있지 않은 경우에는 기본 스토리지 정책이 할당됩니다.

vSAN 데이터스토어에 기본 스토리지 정책 할당

요구 사항에 일치하는 스토리지 정책을 재사용하려는 경우 사용자 정의 스토리지 정책을 데이터스토어의 기본 정책으로 할당할 수 있습니다.

필수 조건

vSAN 데이터스토어에 기본 정책으로 할당할 VM 스토리지 정책이 vSAN 클러스터의 가상 시스템에 대한 요구 사항을 충족하는지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 데이터스토어로 이동합니다.
- 2 구성 탭을 클릭합니다.
- 3 [일반]에서 기본 스토리지 정책 **편집** 버튼을 클릭하고 vSAN 데이터스토어의 기본 정책으로 할당할 스토리지 정책을 선택합니다.

vSAN 기본 스토리지 정책 및 vSAN 규칙 집합이 정의된 사용자 정의 스토리지 정책과 같이 vSAN 데이터스토어와 호환되는 스토리지 정책의 목록이 vSphere Web Client에 표시됩니다.

- 4 정책을 선택하고 **확인**을 클릭합니다.

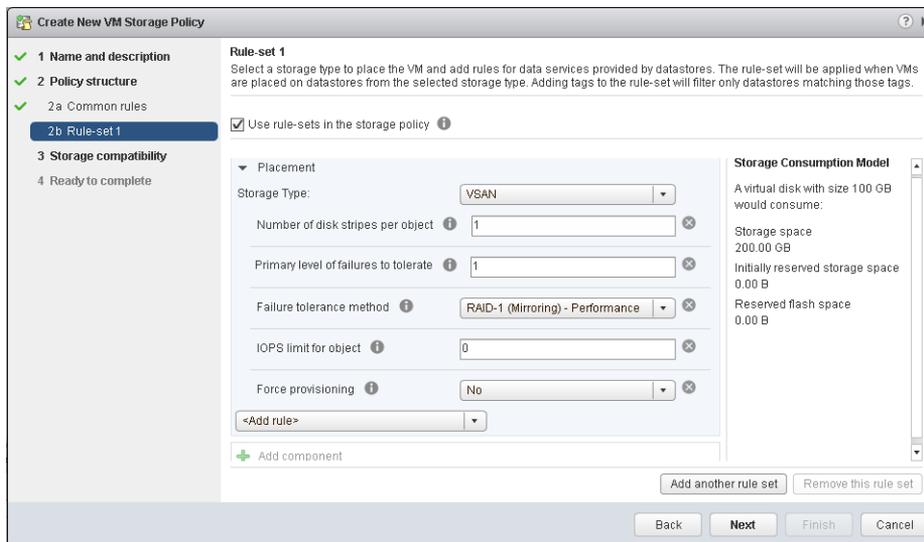
데이터스토어의 스토리지 정책을 명시적으로 지정하지 않고 새 가상 시스템을 프로비저닝하면 스토리지 정책이 기본 정책으로 적용됩니다.

후속 작업

가상 시스템에 대한 새 스토리지 정책을 정의할 수 있습니다. [“vSAN에 대한 가상 시스템 스토리지 정책 정의,”](#) (128 페이지)를 참조하십시오.

vSAN 에 대한 가상 시스템 스토리지 정책 정의

VM 및 해당 가상 디스크의 스토리지 요구 사항을 정의하는 스토리지 정책을 생성할 수 있습니다. 이 정책에서는 vSAN 데이터스토어가 지원하는 스토리지 용량을 참조합니다.



필수 조건

- vSAN 스토리지 제공자를 사용할 수 있는지 확인합니다. [“vSAN 스토리지 제공자 보기,”](#) (126 페이지)를 참조하십시오.

- 가상 시스템 스토리지 정책을 반드시 사용해야 합니다. 스토리지 정책에 대한 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.
- 필요한 권한: **Profile-driven storage.Profile-driven storage view** 및 **Profile-driven storage.Profile-driven storage update**

프로시저

- 1 vSphere Web Client 홈에서 **정책 및 프로파일**을 클릭한 다음 **VM 스토리지 정책**을 클릭합니다.
- 2 **새 VM 스토리지 정책 생성** 아이콘()을 클릭합니다.
- 3 [이름 및 설명] 페이지에서 vCenter Server를 선택합니다.
- 4 스토리지 정책의 이름 및 설명을 입력하고 **다음**을 클릭합니다.
- 5 [정책 구조] 페이지에서 **다음**을 클릭합니다.
- 6 **호스트에서 제공한 데이터 서비스에 대한 일반 규칙** 페이지에서 **다음**을 클릭합니다.
- 7 [규칙 집합 1] 페이지에서 첫 번째 규칙 집합을 정의합니다.
 - a **스토리지 정책의 규칙 집합 사용** 확인란을 선택합니다.
 - b **스토리지 유형** 드롭다운 메뉴에서 **VSAN**을 선택합니다.
vSAN 데이터스토어에 대한 규칙을 추가함에 따라 페이지가 확장됩니다.
 - c **규칙 추가** 드롭다운 메뉴에서 규칙을 선택합니다.
제공하는 값은 vSAN 데이터스토어의 스토리지 기능에서 보급되는 값 범위 내에 있어야 합니다.
스토리지 사용량 모델에서는 사용 가능한 가상 디스크 크기와 해당하는 캐시 및 용량 요구 사항 (스토리지 정책을 적용할 경우 가상 시스템에서 잠재적으로 소비할 수 있는 예약된 스토리지 공간 포함)을 검토할 수 있습니다.
 - d (선택 사항) 태그 기반 기능을 추가합니다.
- 8 (선택 사항) **다른 규칙 집합 추가** 버튼을 클릭하여 다른 규칙 집합을 추가합니다.
- 9 **다음**을 클릭합니다.
- 10 [스토리지 호환성] 페이지에서 이 정책과 일치하는 데이터스토어 목록을 검토하고 **다음**을 클릭합니다.
데이터스토어는 자격을 갖추기 위해 정책 내의 모든 규칙 집합을 충족하지 않아도 됩니다. 최소 하나의 규칙 집합과 이 집합 내의 모든 규칙만 충족하면 됩니다. vSAN 데이터스토어가 스토리지 정책에 설정된 요구 사항을 충족하며 호환 데이터스토어 목록에 나타나는지 확인합니다.
- 11 [완료 준비] 페이지에서 정책 세부 정보를 검토하고 **마침**을 클릭합니다.

새 정책이 목록에 추가됩니다.

후속 작업

이 정책을 가상 시스템 및 해당 가상 디스크에 할당합니다. vSAN은 정책에 지정된 요구 사항에 따라 가상 시스템 개체를 배치합니다. 가상 시스템 개체에 스토리지 정책을 적용하는 것에 관한 정보는 vSphere 스토리지 설명서를 참조하십시오.

vSAN 모니터링

vSphere Web Client에서 vSAN 환경을 모니터링할 수 있습니다.

vSAN 클러스터 및 vSAN 데이터스토어에 참여하는 호스트를 포함하여 vSAN 환경의 모든 개체를 모니터링할 수 있습니다. vSAN 클러스터에서 개체와 스토리지 리소스를 모니터링하는 방법에 대한 자세한 내용은 vSphere 모니터링 및 성능 설명서를 참조하십시오.

이 장에서는 다음 주제에 대해 설명합니다.

- “vSAN 클러스터 모니터링,” (131 페이지)
- “vSAN 용량 모니터링,” (132 페이지)
- “vSAN 클러스터에서 가상 디바이스 모니터링,” (133 페이지)
- “vSAN 클러스터 다시 동기화 정보,” (133 페이지)
- “vSAN 데이터스토어에 참여하는 디바이스 모니터링,” (135 페이지)
- “vSAN 상태 모니터링,” (135 페이지)
- “vSAN 성능 모니터링,” (138 페이지)
- “vSAN 클러스터 재조정 정보,” (142 페이지)
- “vSAN 기본 경고 사용,” (144 페이지)
- “경보 생성에 VMkernel 관찰 사용,” (145 페이지)

vSAN 클러스터 모니터링

vSAN 클러스터 및 이와 관련된 모든 개체를 모니터링할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 클릭하고 **vSAN**을 클릭합니다.
- 3 **물리적 디스크**를 선택하여 클러스터에 있는 모든 호스트, 캐시 디바이스 및 용량 디바이스를 검토합니다.

vSAN은 총 용량, 사용된 용량, 예약된 용량, 기능 상태, 물리적 위치 등과 같이 용량 디바이스에 대한 정보를 표시합니다. 물리적 위치는 vSAN 호스트에서 캐시, 용량 및 디바이스의 하드웨어 위치를 기반으로 합니다.
- 4 용량 디바이스를 선택하고 **가상 디스크**를 클릭하여 디바이스를 사용하는 가상 시스템을 검토합니다.

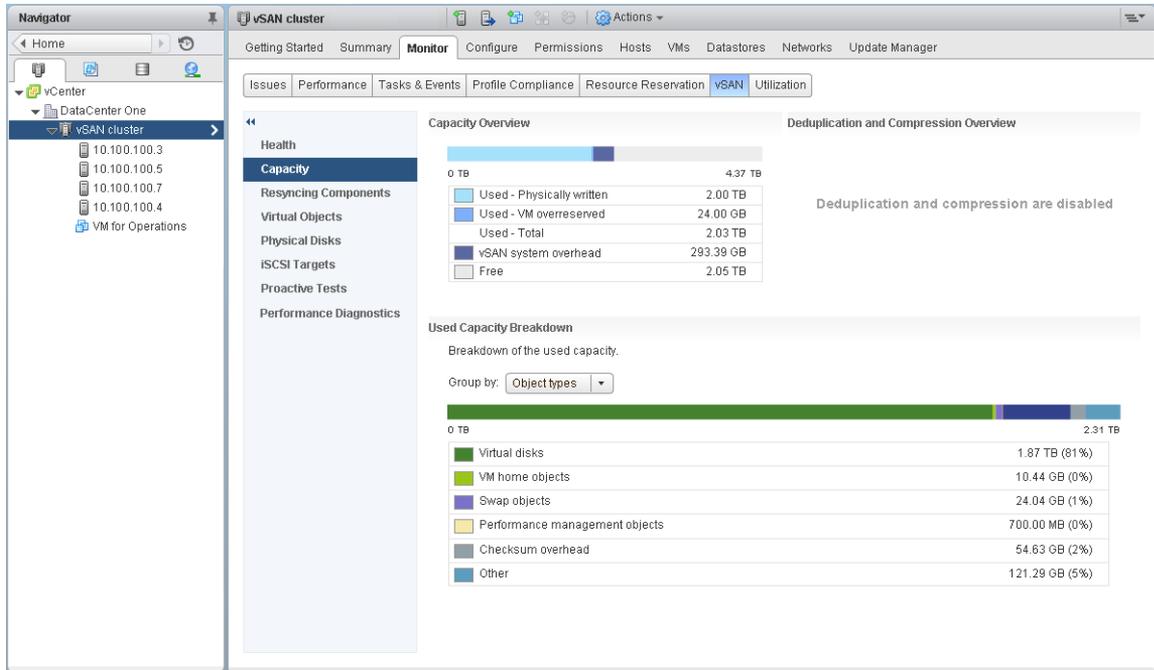
현재 상태 및 할당된 스토리지 정책과 호환되는지 여부를 포함하여 가상 시스템 개체의 여러 측면을 모니터링할 수 있습니다.

- 5 용량을 선택하여, 클러스터에 프로비저닝되어 사용된 용량의 양에 대한 정보를 검토하고, 개체 유형이나 데이터 유형별로 사용된 용량에 대한 분석을 검토합니다.
- 6 구성 탭을 선택하고 일반을 선택하여 vSAN 클러스터의 상태를 점검하고, 인터넷 연결을 확인하고, 클러스터에서 사용되는 온디스크 형식을 검토합니다.

vSAN 용량 모니터링

vSAN 데이터스토어의 용량, 중복 제거와 압축의 효율성 및 용량 사용량에 대한 분석 정보를 모니터링할 수 있습니다.

vSphere Web Client 클러스터 [요약] 탭에는 vSAN 용량에 대한 요약이 포함됩니다. 용량 모니터에서 더 세부적인 정보를 볼 수도 있습니다.



프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 모니터 탭을 클릭하고 vSAN을 클릭합니다.
- 3 vSAN 용량 정보를 보려면 용량을 선택합니다.

[용량 개요]에는 사용된 공간과 사용 가능한 공간을 포함하여 vSAN 데이터스토어의 스토리지 용량이 표시됩니다. [사용된 용량 분석]에는 서로 다른 개체 유형 또는 데이터 유형에 사용된 용량의 백분율이 표시됩니다. 데이터 유형을 선택하면 vSAN은 기본 VM 데이터, vSAN 오버헤드 및 임시 오버헤드에 사용된 용량의 백분율을 표시합니다. 개체 유형을 선택하면 vSAN은 다음과 같은 개체 유형에 사용된 용량의 백분율을 표시합니다.

- 가상 디스크
- VM 홈 개체
- 스왑 개체
- 성능 관리 개체
- .vmem 파일
- 체크섬 오버헤드

- 스냅샷 메모리
- 중복 제거 및 압축 오버헤드
- 중복 제거 엔진 사용 시의 공간 고려 사항
- iSCSI 홈 및 대상 개체와 iSCSI LUN
- 사용자가 생성한 파일, VM 템플릿 등의 기타 개체 유형

클러스터에서 중복 제거와 압축을 사용하도록 설정한 경우에는 해당 기능과 관련된 용량 정보가 [중복 제거 및 압축 개요]에 표시됩니다. 중복 제거와 압축을 사용하도록 설정하면 디스크 공간이 회수되고 다시 할당되면서 용량 업데이트가 용량 모니터에 반영되는 데 몇 분 정도 소요될 수 있습니다. 중복 제거와 압축에 대한 자세한 내용은 “중복 제거 및 압축 사용,” (69 페이지)을 참조하십시오.

vSAN 클러스터에서 가상 디바이스 모니터링

vSAN 클러스터에서 가상 디스크의 상태를 볼 수 있습니다.

하나 이상의 호스트가 vSAN 데이터스토어와 통신할 수 없으면 가상 디바이스에 대한 정보가 표시되지 않습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 클릭하고 **vSAN**을 클릭합니다.
- 3 **가상 디스크**를 선택하여 vSAN 클러스터에 있는 모든 호스트와 해당 가상 디스크 그리고 해당 구성 요소가 현재 사용 중인 호스트, 캐시 및 용량 디바이스를 봅니다.
- 4 가상 시스템 중 하나에서 **VM 홈** 폴더를 선택하고 **물리적 디스크 배치** 탭을 클릭하여 이름, 식별자, UUID 등의 디바이스 정보를 봅니다.

규정 준수 실패 탭을 클릭하면 가상 시스템의 규정 준수 상태를 확인할 수 있습니다.
- 5 가상 시스템 중 하나의 **하드 디스크**를 선택하고 **물리적 디스크 배치** 탭을 클릭하여 디바이스의 이름, 식별자 또는 UUID 같은 디바이스 정보, 각 가상 시스템에 사용되는 디바이스 수 및 호스트 간에 미러링되는 방법을 봅니다.

규정 준수 실패 탭을 클릭하면 가상 디바이스의 규정 준수 상태를 확인할 수 있습니다.
- 6 **규정 준수 실패** 탭을 클릭하면 가상 시스템의 규정 준수 상태를 확인할 수 있습니다.

vSAN 클러스터 다시 동기화 정보

vSAN 클러스터에서 다시 동기화되고 있는 가상 시스템 개체의 상태를 모니터링할 수 있습니다.

하드웨어 디바이스, 호스트 또는 네트워크에 장애가 발생하거나 호스트가 유지 보수 모드로 전환되는 경우 vSAN은 vSAN 클러스터에서 다시 동기화를 시작합니다. 그러나 vSAN은 다시 동기화 작업을 시작하기 전에 장애가 발생한 구성 요소가 다시 온라인 상태가 될 때까지 잠시 기다릴 수 있습니다.

다음 이벤트는 클러스터에서 다시 동기화를 트리거합니다.

- VM(가상 시스템) 스토리지 정책 편집. VM 스토리지 정책 설정을 변경하면 vSAN이 개체 재생성 및 개체의 이후 다시 동기화를 시작할 수 있습니다.

특정 정책 변경 내용은 vSAN이 다른 버전의 개체를 생성하고 이를 이전 버전과 동기화하도록 할 수 있습니다. 동기화가 완료되면 원래 개체는 삭제됩니다.

vSAN은 VM이 계속해서 실행되고 이 프로세스에 의해 중단되지 않도록 보장합니다. 이 프로세스에는 추가 임시 용량이 필요할 수 있습니다.
- 장애 후 호스트 다시 시작.

- 영구 또는 장기 장애로부터 호스트 복구. 기본적으로 호스트를 60분 이상 사용할 수 없는 경우 vSAN은 완전한 정책 규정 준수를 복구하기 위한 데이터 복사본을 생성합니다.
- 호스트를 유지 보수 모드로 전환하기 전에 전체 데이터 마이그레이션 모드를 사용하여 데이터 제거.
- 용량 디바이스의 사용률 임계값 초과. vSAN 클러스터에서 용량 디바이스 사용률이 80% 임계값 수준에 도달하거나 이 수준을 초과하면 다시 동기화가 트리거됩니다.

다시 동기화로 인한 지연 시간 때문에 VM이 응답하지 않을 때는 다시 동기화에 사용되는 IOPS를 조절할 수 있습니다.

vSAN 클러스터의 다시 동기화 작업 모니터링

다시 동기화되고 있는 개체의 상태를 평가하기 위해 현재 진행 중인 다시 동기화 작업을 모니터링할 수 있습니다.

필수 조건

vSAN 클러스터에 포함된 호스트가 ESXi 6.5 이상을 실행 중인지 확인합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 선택하고 **vSAN**을 클릭합니다.
- 3 **구성 요소 다시 동기화**를 선택하여 가상 시스템 개체의 다시 동기화 진행률과 다시 동기화가 완료되기 전까지 남은 바이트 수를 추적합니다.

현재 클러스터에서 동기화되고 있는 개체의 수, 예상되는 다시 동기화 완료 시간, 스토리지 개체가 할당된 스토리지 정책을 완전히 준수할 때까지 남은 시간 등에 대한 정보를 볼 수도 있습니다.

클러스터에 연결 문제가 있는 경우 [구성 요소 다시 동기화] 페이지의 데이터가 예상대로 새로 고쳐지지 않을 수 있으며 필드에 정확하지 않은 정보가 반영될 수 있습니다.

vSAN 클러스터의 다시 동기화 작업 조절

vSAN 클러스터의 디스크 그룹에 대해 다시 동기화를 수행하는 데 사용되는 IOPS 수를 줄일 수 있습니다. 다시 동기화 조절은 클러스터 차원의 설정이며 디스크 그룹 단위로 적용됩니다.

다시 동기화로 인한 지연 시간 때문에 VM이 응답하지 않을 때는 다시 동기화에 사용되는 IOPS 수를 조절할 수 있습니다. 다시 동기화 조절은 다시 동기화 때문에 클러스터에서 지연 시간이 계속 증가하는 경우나 호스트에서 다시 동기화 트래픽이 너무 높을 때만 고려하십시오.

다시 동기화를 조절하면 다시 동기화를 완료하는 데 필요한 시간이 증가할 수 있습니다. 비준수 VM의 다시 보호가 지연될 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 선택하고 **vSAN**을 클릭합니다.
- 3 **구성 요소 다시 동기화**를 선택하고 **다시 동기화 조절**을 클릭합니다.
- 4 (선택 사항) **호스트당 현재 다시 동기화 트래픽 표시**를 클릭하여 다시 동기화 작업을 봅니다.
- 5 **구성 요소 트래픽 다시 동기화에 대해 조절 사용** 확인란을 선택합니다.
- 6 다음과 같이 슬라이더를 이동하여 조절 정도를 설정합니다.
 - 다시 동기화에 허용되는 IOPS 양을 늘리려면 슬라이더를 오른쪽으로 이동합니다.

- 다시 동기화에 허용되는 IOPS 양을 줄이려면 슬라이더를 왼쪽으로 이동합니다.

시간을 두고 클러스터가 적응할 수 있도록 IOPS를 절반으로 줄이는 것이 일반적인 규칙입니다. 추가적인 조치가 필요한 경우 클러스터가 안정화될 때까지 IOPS를 다시 절반으로 조절합니다.

- 7 **확인**을 클릭합니다.

vSAN 데이터스토어에 참여하는 디바이스 모니터링

vSAN 데이터스토어를 백업하는 디바이스의 상태를 확인하여 디바이스에 문제가 있는지 확인할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 스토리지로 이동합니다.
- 2 vSAN 데이터스토어를 선택합니다.
- 3 **구성** 탭을 클릭합니다.
용량, 기능 및 기본 스토리지 정책을 포함하여 vSAN 데이터스토어에 대한 일반적인 정보를 볼 수 있습니다.
- 4 **디바이스 백업**을 클릭하고 디스크 그룹을 선택하여 페이지 맨 아래의 디스크 표에 로컬 디바이스를 표시합니다.
- 5 숨겨진 열을 표시하려면 열 머리글을 마우스 오른쪽 버튼으로 클릭하고 **열 표시/숨기기**를 선택합니다.
- 6 표시할 열을 선택하고 **확인**을 클릭합니다.
선택한 열이 디스크 표에 표시됩니다.

vSAN 상태 모니터링

vSAN 클러스터의 상태를 점검할 수 있습니다.

vSAN 상태 점검을 사용하면 클러스터 구성 요소의 상태를 모니터링하고, 문제를 진단하고, 문제를 해결할 수 있습니다. 상태 점검 대상에는 하드웨어 호환성, 네트워크 구성과 작업, 고급 vSAN 구성 옵션, 스토리지 디바이스 상태 및 가상 시스템 개체가 포함됩니다.

The screenshot displays the vSAN Health monitoring interface. The 'vSAN Health' section shows a table of test results. The 'Controller Driver' test is highlighted with a yellow warning icon. Below this, a 'Controller List' table shows details for four hosts, all with 'Warning' status for the Controller Driver.

| Host | Device | Driver in use | Driver health | Drivers on HCL |
|--------------|-----------------------|--------------------------|---------------|----------------|
| 10.100.100.3 | vmhba1: LSI Logic ... | mptspi (4.23.01.00-9vmw) | Warning | N/A |
| 10.100.100.5 | vmhba1: LSI Logic ... | mptspi (4.23.01.00-9vmw) | Warning | N/A |
| 10.100.100.7 | vmhba1: LSI Logic ... | mptspi (4.23.01.00-9vmw) | Warning | N/A |
| 10.100.100.4 | vmhba1: LSI Logic ... | mptspi (4.23.01.00-9vmw) | Warning | N/A |

vSAN 상태 점검은 범주로 분류되며, 각 범주에는 개별 상태 점검이 포함됩니다.

표 13-1. vSAN 상태 점검 범주

| 상태 점검 범주 | 설명 |
|-------------------|--|
| 하드웨어 호환성 | 클러스터 구성 요소가 지원되는 하드웨어, 소프트웨어 및 드라이버를 사용하는지 모니터링합니다. |
| 성능 서비스 | vSAN 성능 서비스의 상태를 모니터링합니다. |
| 네트워크 | vSAN 네트워크 상태를 모니터링합니다. |
| 물리적 디스크 | vSAN 클러스터에 포함된 물리적 디바이스의 상태를 모니터링합니다. |
| 데이터 | vSAN 데이터 상태를 모니터링합니다. |
| 클러스터 | vSAN 클러스터 상태를 모니터링합니다. |
| 제한 | vSAN 클러스터 제한을 모니터링합니다. |
| 온라인 상태 | vSAN 클러스터 상태를 모니터링하고, 고급 분석을 위해 VMware의 분석 백엔드 시스템에 보냅니다. 온라인 상태 점검 기능을 사용하려면 고객 환경 향상 프로그램에 참가해야 합니다. |
| vSAN iSCSI 대상 서비스 | 네트워크 구성 및 런타임 상태를 포함하여 iSCSI 대상 서비스를 모니터링합니다. |
| 암호화 | vSAN 암호화 상태를 모니터링합니다. |
| 확장된 클러스터 | 확장된 클러스터의 상태를 모니터링합니다(해당하는 경우). |

vSAN은 각 상태 점검을 주기적으로 다시 테스트하고 결과를 업데이트합니다. 상태 점검을 실행하고 결과를 즉시 업데이트하려면 **다시 테스트** 버튼을 클릭합니다.

고객 환경 향상 프로그램에 참여하면 상태 점검을 실행하고 고급 분석을 위해 데이터를 VMware에 보낼 수 있습니다. **온라인 상태 점검을 사용하여 다시 테스트** 버튼을 클릭합니다.

vSAN 상태 점검에 대한 자세한 내용은 VMware Virtual SAN 상태 점검 플러그인 가이드를 참조하십시오.

호스트에서 vSAN 상태 모니터링

ESXi 호스트 클라이언트는 단일 ESXi 호스트를 관리하기 위한 브라우저 기반의 인터페이스입니다. 이 호스트 클라이언트를 사용하면 vCenter Server를 사용할 수 없을 때 호스트를 관리할 수 있습니다. 호스트 클라이언트는 호스트 수준에서 vSAN을 관리하고 모니터링할 수 있는 탭을 제공합니다.

- **vSAN** 탭은 기본 vSAN 구성을 표시합니다.
- **호스트** 탭에는 vSAN 클러스터에 참여하는 호스트가 표시됩니다.
- **상태** 탭에는 호스트 수준의 상태 점검이 표시됩니다.

vSAN Health Service 구성

vSAN Health Service의 상태 점검 간격을 구성할 수 있습니다.

vSAN Health Service는 기본적으로 설정되어 있습니다. 정기 상태 점검을 해제 또는 설정하고 상태 점검 간격을 설정할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **상태 및 성능**을 선택합니다.

- 4 상태 서비스 **설정 편집** 버튼을 클릭합니다.
 - a 정기 상태 점검을 해제하려면 **정기 상태 점검 설정**을 선택 취소합니다.
상태 점검 사이의 시간 간격을 설정할 수도 있습니다.
 - b 정기 상태 점검을 설정하려면 **정기 상태 점검 설정**을 선택합니다.

vSAN 상태 점검

vSAN 상태 점검의 상태를 확인하여 vSAN 클러스터의 구성 및 운영을 확인할 수 있습니다.

필수 조건

상태 점검을 보려면 먼저 vSAN Health Service를 설정해야 합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 클릭하고 **vSAN**을 클릭합니다.
- 3 **상태**를 선택하여 vSAN 상태 점검 범주를 검토합니다.
[테스트 결과] 옆에 [주의] 또는 [실패]가 표시되는 경우 범주를 확장하여 개별 상태 점검의 결과를 검토하십시오.
- 4 개별 상태 점검을 선택하고 페이지 맨 아래에서 세부 정보를 확인합니다.
VMware에 문의 버튼을 클릭하면 상태 점검에 대해 설명하고 문제 해결 방법에 대한 정보를 제공하는 기술 자료 문서를 열 수 있습니다.

ESXi Host Client에서 vSAN 모니터링

ESXi 호스트 클라이언트를 통해 vSAN 상태와 기본 구성을 모니터링할 수 있습니다.

필수 조건

상태 점검을 보려면 먼저 vSAN Health Service를 설정해야 합니다.

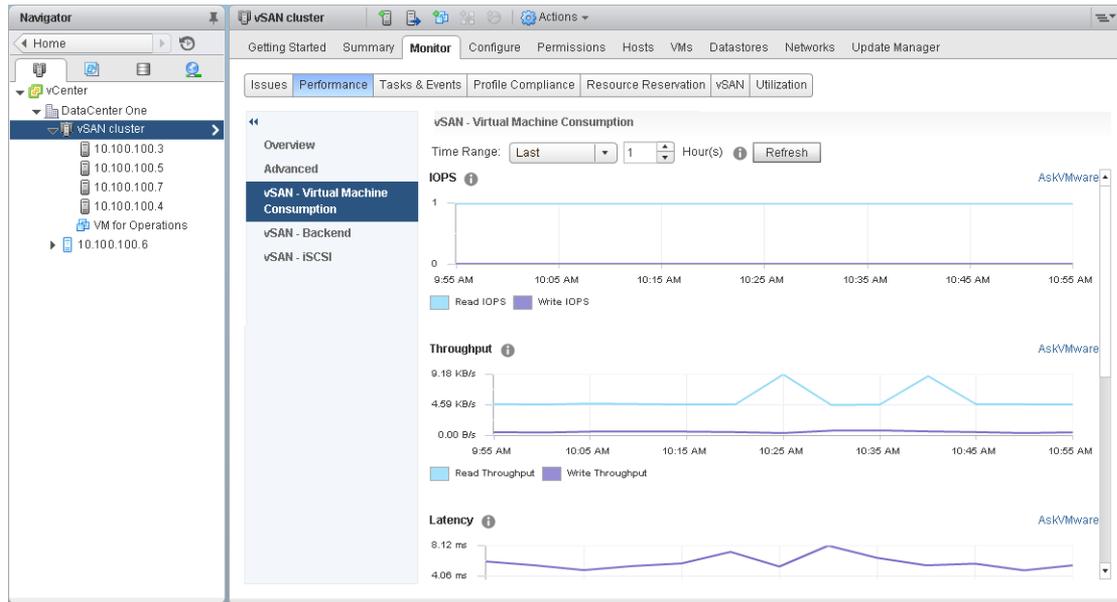
프로시저

- 1 브라우저를 열고 호스트의 IP 주소를 입력합니다.
호스트 클라이언트의 로그인 페이지로 브라우저가 리디렉션됩니다.
- 2 호스트의 사용자 이름과 암호를 입력하고 **로그인**을 클릭합니다.
- 3 호스트 클라이언트 탐색기에서 **스토리지**를 클릭합니다.
- 4 기본 페이지에서 vSAN 데이터스토어를 클릭하여 탐색기에서 모니터링 링크를 표시합니다.
- 5 탭을 클릭하여 호스트의 vSAN 정보를 확인합니다.
 - a 기본 vSAN 구성을 표시하려면 **vSAN** 탭을 클릭합니다.
 - b vSAN 클러스터에 참여하는 호스트를 표시하려면 **호스트** 탭을 클릭합니다.
 - c 호스트 수준의 상태 점검을 표시하려면 **상태** 탭을 클릭합니다.
- 6 (선택 사항) **vSAN** 탭에서 **설정 편집**을 클릭하여 호스트 수준에서 구성 문제를 수정합니다. vSAN 클러스터의 구성과 일치하는 값을 선택합니다.
vSAN 클러스터의 구성과 일치하는 값을 선택하고 **저장**을 클릭합니다.

vSAN 성능 모니터링

vSAN 성능 서비스를 사용하면 vSAN 환경의 성능을 모니터링하고 잠재적인 문제를 조사할 수 있습니다.

성능 서비스는 성능 통계를 수집 및 분석하고 데이터를 그래픽 형식으로 표시합니다. 성능 차트를 사용하여 워크로드를 관리하고 문제의 근본 원인을 확인할 수 있습니다.



vSAN 성능 서비스를 설정하면 IOPS, 처리량 및 지연 시간을 포함하여 vSAN 성능 통계에 대한 개요가 클러스터 요약에 표시됩니다. 클러스터와 vSAN 클러스터 내 각 호스트, 디스크 그룹 및 디스크에 대해 세부적인 성능 통계를 볼 수 있습니다. 또한 가상 시스템과 가상 디스크에 대한 성능 차트도 볼 수 있습니다.

vSAN 성능 서비스 설정

vSAN 클러스터를 생성할 경우 성능 서비스는 사용되지 않도록 설정됩니다. vSAN 클러스터, 호스트, 디스크 및 VM의 성능을 모니터링하려면 vSAN 성능 서비스를 설정합니다.

성능 서비스를 설정하면 vSAN은 통계 데이터를 수집하기 위해 통계 데이터베이스 개체를 데이터스토어에 배치합니다. 통계 데이터베이스는 클러스터의 vSAN 데이터스토어에 있는 네임스페이스 개체입니다.

필수 조건

- vSAN 클러스터의 모든 호스트는 ESXi 6.5 이상을 실행해야 합니다.
- vSAN 성능 서비스를 사용하도록 설정하기 전에 클러스터가 제대로 구성되어 있고 해결되지 않은 상태 문제가 없는지 확인합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터로 이동합니다.
- 2 **구성** 탭을 클릭합니다.
- 3 vSAN에서 **상태 및 성능**을 선택합니다.
- 4 **편집**을 클릭하여 성능 서비스 설정을 편집합니다.

- 5 **vSAN 성능 서비스 설정** 확인란을 선택합니다.
이 확인란을 선택 취소하면 vSAN 성능 서비스를 해제할 수 있습니다.
- 6 통계 데이터베이스 개체에 대한 스토리지 정책을 선택하고 **확인**을 클릭합니다.

저장된 시간 범위 사용

성능 보기의 시간 범위 선택기에서 저장된 시간 범위를 선택할 수 있습니다.

사용자 지정된 이름을 사용하여 시간 범위를 수동으로 저장할 수 있습니다. 스토리지 성능 테스트를 실행하면 선택한 시간 범위가 자동으로 저장됩니다. 모든 성능 보기의 시간 범위를 저장할 수 있습니다.

필수 조건

- vSAN 성능 서비스를 설정해야 합니다.
- vSAN 클러스터의 모든 호스트는 ESXi 6.6 이상을 실행해야 합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 클릭하고 **성능**을 클릭합니다.
- 3 원하는 탭(예: **vSAN - 백엔드**)을 선택합니다. 시간 범위 드롭다운에서 **시간 범위 저장...**을 선택합니다.
- 4 선택한 시간 범위의 이름을 입력합니다.
- 5 **확인**을 클릭합니다.

vSAN 클러스터 성능 보기

vSAN 클러스터 성능 차트를 사용하면 클러스터의 워크로드를 모니터링하고 문제의 근본 원인을 확인할 수 있습니다.

성능 서비스를 설정하면 vSAN IOPS, 처리량 및 지연 시간을 포함하여 vSAN 성능 통계에 대한 개요가 클러스터 요약에 표시됩니다. 클러스터 수준에서는 가상 시스템 사용량과 vSAN 백엔드에 대한 세부적인 통계 차트를 볼 수 있습니다.

필수 조건

성능 차트를 보려면 먼저 vSAN 성능 서비스를 설정해야 합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 클릭하고 **성능**을 클릭합니다.
- 3 **vSAN - 가상 시스템 사용량**을 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 IOPS, 처리량, 지연 시간, 정체 및 미결 I/O를 포함하여, 클러스터에서 실행 중인 클라이언트에 대한 성능 차트를 표시합니다. 이러한 차트에 표시되는 통계는 클러스터 내의 호스트에서 집계됩니다.
- 4 **vSAN - 백엔드**를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 IOPS, 처리량, 지연 시간, 정체 및 미결 I/O를 포함하여, 클러스터 백엔드 작업에 대한 성능 차트를 표시합니다. 이러한 차트에 표시되는 통계는 클러스터 내의 호스트에서 집계됩니다.

- 5 **vSAN - iSCSI**를 선택하고 iSCSI 대상 또는 LUN을 선택합니다. 쿼리할 시간 범위를 선택합니다.

참고 iSCSI 성능 차트를 보려면 vSAN 클러스터의 모든 호스트가 ESXi 6.6 이상을 실행해야 합니다.

vSAN은 IOPS, 대역폭, 지연 시간 및 미결 I/O를 포함하여, iSCSI 대상 또는 LUN에 대한 성능 차트를 표시합니다.

vSAN 호스트 성능 보기

vSAN 호스트 성능 차트를 사용하면 호스트의 워크로드를 모니터링하고 문제의 근본 원인을 확인할 수 있습니다. vSAN 성능 차트는 호스트, 디스크 그룹 및 개별 스토리지 디바이스에 대해 볼 수 있습니다.

성능 서비스를 설정하면 각 호스트 및 해당 호스트에 연결된 디스크에 대한 성능 통계가 호스트 요약에 표시됩니다. 호스트 수준에서는 IOPS, 처리량, 지연 시간 및 정체를 포함하여 가상 시스템 사용량과 vSAN 백엔드에 대한 세부적인 통계 차트를 볼 수 있습니다. 로컬 클라이언트 캐시 읽기 IOPS 및 적중률을 볼 수 있는 추가 차트를 사용할 수 있습니다. 디스크 그룹 수준에서는 디스크 그룹에 대한 통계를 볼 수 있습니다. 디스크 수준에서는 개별 스토리지 디바이스에 대한 통계를 볼 수 있습니다.

필수 조건

성능 차트를 보려면 먼저 vSAN 성능 서비스를 설정해야 합니다.

물리적 어댑터, VMkernel 어댑터, VMkernel 어댑터 집계, iSCSI, vSAN - 백엔드 다시 동기화 I/O, 다시 동기화 IOPS, 다시 동기화 처리량, 디스크 그룹 다시 동기화 지연 시간 등의 성능 차트를 보려면 vSAN 클러스터 내의 호스트가 ESXi 6.6 이상을 실행 중이어야 합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터로 이동하여 호스트를 선택합니다.
- 2 **모니터** 탭을 클릭하고 **성능**을 클릭합니다.
- 3 **vSAN - 가상 시스템 사용량**을 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 IOPS, 처리량, 지연 시간, 정체 및 미결 I/O를 포함하여, 호스트에서 실행 중인 클라이언트에 대한 성능 차트를 표시합니다.
- 4 **vSAN - 백엔드**를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 IOPS, 처리량, 지연 시간, 정체, 미결 I/O 및 다시 동기화 I/O를 포함하여, 호스트 백엔드 작업에 대한 성능 차트를 표시합니다.
- 5 **vSAN - 디스크 그룹**을 선택하고 디스크 그룹을 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 프런트 엔드(게스트) IOPS, 처리량 및 지연 시간은 물론 오버헤드 IOPS와 지연 시간을 포함하여, 디스크 그룹에 대한 성능 차트를 표시합니다. 또한 읽기 캐시 적중률, 축출, 사용 가능한 쓰기 버퍼 비율, 용량과 사용량, 캐시 디스크 디스테이징 비율, 정체, 미결 I/O, 미결 I/O 크기, I/O 지연율, 지연된 I/O 평균 지연 시간, 내부 대기열 IOPS, 내부 대기열 처리량, 다시 동기화 IOPS, 다시 동기화 처리량 및 다시 동기화 지연 시간도 함께 표시됩니다.
- 6 **vSAN - 디스크**를 선택하고 디스크를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 물리적/펌웨어 계층 IOPS, 처리량 및 지연 시간을 포함하여, 디스크에 대한 성능 차트를 표시합니다.
- 7 **vSAN - 물리적 어댑터**를 선택하고 NIC를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 처리량, 초당 패킷 수 및 패킷 손실율을 포함하여, 물리적 NIC(pNIC)에 대한 성능 차트를 표시합니다.

- 8 **vSAN - VMkernel 어댑터**를 선택하고 vmk1 같은 VMkernel 어댑터를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 처리량, 초당 패킷 수 및 패킷 손실율을 포함하여, VMkernel 어댑터에 대한 성능 차트를 표시합니다.
- 9 **vSAN - VMkernel 어댑터 집계**를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 처리량, 초당 패킷 수 및 패킷 손실율을 포함하여, vSAN이 사용하는 네트워크 어댑터에서 처리한 모든 네트워크 I/O에 대한 성능 차트를 표시합니다.
- 10 **vSAN - iSCSI**를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 IOPS, 대역폭, 지연 시간 및 미결 I/O를 포함하여, 호스트에 있는 모든 iSCSI 서비스에 대한 성능 차트를 표시합니다.

vSAN VM 성능 보기

vSAN VM 성능 차트를 사용하여 가상 시스템 및 가상 디스크의 워크로드를 모니터링할 수 있습니다.

성능 서비스를 설정하면 가상 시스템 성능 및 가상 디스크 성능에 대한 세부적인 통계 차트를 볼 수 있습니다. 호스트 간 마이그레이션 중에는 VM 성능 통계를 수집할 수 없으므로 VM 성능 차트에서 몇 분 정도의 공백이 나타날 수 있습니다.

참고 가상 디스크의 경우 성능 서비스는 가상 SCSI 컨트롤러만 지원합니다. IDE 같은 다른 컨트롤러를 사용하는 가상 디스크는 지원되지 않습니다.

필수 조건

성능 차트를 보려면 먼저 vSAN 성능 서비스를 설정해야 합니다.

프로시저

- 1 vSphere Web Client 탐색기에서 vSAN 클러스터로 이동하여 VM을 선택합니다.
- 2 **모니터** 탭을 클릭하고 **성능**을 클릭합니다.
- 3 **vSAN - 가상 시스템 사용량**을 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 IOPS, 처리량 및 지연 시간을 포함하여, VM에 대한 성능 차트를 표시합니다.
- 4 **vSAN - 가상 디스크**를 선택합니다. 쿼리할 시간 범위를 선택합니다.
vSAN이 IOPS, 표준화된 IOPS 지연, 가상 SCSI IOPS, 가상 SCSI 처리량 및 가상 SCSI 지연 시간을 포함하여, 가상 디스크에 대한 성능 차트를 표시합니다.

vSAN 성능 진단 사용

vSAN 성능 진단을 사용하면 vSAN 클러스터의 성능을 향상하고 성능 문제를 해결할 수 있습니다.

vSAN 성능 진단 도구는 vSAN 성능 서비스에서 수집된 이전에 실행된 벤치마크를 분석합니다. 이 도구는 문제를 감지하고, 업데이트 적용 단계를 제안하고, 더 깊은 이해를 위한 지원 성능 그래프를 제공할 수 있습니다.

vSAN 성능 서비스는 vSAN 성능 진단을 분석하는 데 사용되는 데이터를 제공합니다. vSAN은 CEIP를 사용하여 VMware에 분석을 위한 데이터를 보냅니다.

참고 운영 vSAN 클러스터에서 일반 성능 평가에 vSAN 성능 진단을 사용하지 마십시오.

필수 조건

- vSAN 성능 서비스를 설정해야 합니다.
- vCenter Server에는 ISO 이미지 및 패치를 다운로드하기 위한 인터넷 액세스가 필요합니다.

- CEIP(고객 환경 향상 프로그램)에 참여해야 합니다.

프로시저

- 1 vSphere Web Client탐색기에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 클릭하고 **vSAN**을 클릭합니다.
- 3 **성능 진단**을 선택합니다.
- 4 드롭다운 메뉴에서 벤치마크 목표를 선택합니다.
최대 IOPS, 최대 처리량 또는 최소 지연 시간과 같이 달성할 성능 향상을 기반으로 목표를 선택할 수 있습니다.
- 5 쿼리할 시간 범위를 선택합니다.
기본 시간 범위는 가장 최근 1시간입니다. 최근 24시간을 포함하도록 시간 범위를 늘리거나 최근 90일 이내의 사용자 지정 시간 범위를 정의할 수 있습니다. HCIbench 도구를 사용하여 vSAN 클러스터에서 성능 벤치마크 테스트를 실행한 경우 해당 테스트의 시간 범위가 드롭다운 메뉴에 나타납니다.
- 6 **제출**을 클릭합니다.

제출을 클릭하면 vSAN이 성능 데이터를 vSphere 백엔드 분석 서버로 전송합니다. 데이터를 분석한 후 vSAN 성능 진단 도구는 선택한 목표에 대한 벤치마크 성능에 영향을 미쳤을 수 있는 문제 목록을 표시합니다.

클릭하여 각 문제를 확장하여 관련 항목 목록과 같은 각 문제에 대한 자세한 세부 정보를 볼 수 있습니다. **VMware에 문의** 링크를 클릭하여 문제를 해결하고 성능 목표를 달성하기 위한 권장 사항을 설명하는 기술 자료 문서를 표시할 수도 있습니다.

vSAN 클러스터 재조정 정보

클러스터 내 임의 용량 디바이스의 사용률이 80%에 도달하면 vSAN은 모든 용량 디바이스의 사용률이 임계값 이하가 될 때까지 클러스터를 자동으로 재조정합니다.

클러스터 재조정은 클러스터 간에 리소스를 고르게 분산하여 성능과 가용성을 일관되게 유지합니다.

클러스터 재조정을 시작할 수 있는 기타 작업은 다음과 같습니다.

- vSAN이 클러스터에서 하드웨어 장애를 감지하는 경우
- **모든 데이터 제거** 옵션과 함께 vSAN 호스트를 유지 보수 모드로 전환한 경우
- PFTT가 0으로 할당된 개체가 호스트에 있는 경우에 **데이터 액세스 지원 보장** 옵션과 함께 vSAN 호스트를 유지 보수 모드로 전환한 경우

참고 유지 보수 및 다시 보호를 위한 충분한 공간을 제공하고 vSAN 클러스터에서 자동 재조정 이벤트를 최소화하려면 항상 30%의 사용 가능 용량을 유지하는 것이 좋습니다.

RVC(Ruby vSphere Console)를 사용하여 vSAN 클러스터를 수동으로 재조정할 수 있습니다. "[수동 재조정](#)," (143 페이지)를 참조하십시오.

자동 재조정

기본적으로 vSAN은 용량 디바이스가 80% 활용률에 도달하면 자동으로 vSAN 클러스터를 재조정합니다. vSAN 호스트를 유지 보수 모드로 전환할 때도 재조정이 수행됩니다.

다음 RVC 명령을 실행하여 클러스터의 재조정 작업을 모니터링합니다.

- `vsan.check_limits`. 디스크 공간 활용도가 클러스터에서 조정되는지 확인합니다.

- `vsan.whatif_host_failures`. 호스트당 현재 용량 활용도를 분석하고 단일 호스트 장애가 다시 보호를 위한 클러스터의 공간 부족을 강제할 수 있는지 해석하고, 호스트 장애가 클러스터 용량, 캐시 예약 및 클러스터 구성 요소에 미치는 영향을 분석합니다.

명령 출력으로 표시된 물리적 용량 사용량은 vSAN 클러스터의 모든 디바이스의 평균 사용량입니다.

- `vsan.resync_dashboard`. 클러스터의 모든 재구축 작업을 모니터링합니다.

RVC 명령 옵션에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.

수동 재조정

클러스터 상태 점검 또는 RVC 명령을 사용하여 수동으로 재조정할 수 있습니다.

vSAN 디스크 균형 상태 점검이 실패할 경우에는 vSphere Web Client에서 수동 재조정을 시작할 수 있습니다. [클러스터 상태]에서 [vSAN 디스크 밸런싱 상태 점검]을 액세스하고 **디스크 재조정** 버튼을 클릭합니다.

다음 RVC 명령을 사용하여 클러스터를 수동으로 재조정할 수 있습니다.

- `vsan.check_limits`. vSAN 클러스터에 80% 임계값 제한에 도달하고 있는 용량 디바이스가 있는지 확인합니다.
- `vsan.proactive_rebalance [opts]<Path to ClusterComputeResource> --start`. 수동으로 재조정 작업을 시작합니다. 이 명령을 실행하는 경우 vSAN은 클러스터에서 구성 요소의 현재 배포를 검색하고 클러스터에서 구성 요소의 배포를 조정하기 시작합니다. 클러스터에서 재조정 작업을 실행하는 기간과 각 vSAN 호스트에 대해 시간당 데이터 이동량을 지정하려면 명령 옵션을 사용합니다. vSAN 클러스터의 재조정 작업 관리를 위한 명령 옵션에 대한 자세한 내용은 RVC 명령 참조 가이드를 참조하십시오.

클러스터 재조정은 상당한 I/O 작업을 생성하기 때문에 시간이 많이 소요될 수 있으며 가상 시스템의 성능에 영향을 미칠 수 있습니다.

참고 디스크를 수동으로 재조정하는 경우 이동할 데이터가 더 이상 없을 때까지 선택한 기간 동안 작업이 실행됩니다. 기본 기간은 24시간입니다. 이동 중인 데이터가 없으면 vSAN이 재조정 작업을 종료합니다.

프로비저닝된 공간이 특정 임계값에 도달할 때 알려 주는 경보를 구성할 수 있습니다. “[vSAN 이벤트에 대한 vCenter Server 경고 생성](#),” (146 페이지)를 참조하십시오.

vSAN 클러스터의 디스크 사용 균형

vSAN 클러스터가 불균형 상태가 되면 디스크 사용을 재조정할 수 있습니다.

vSAN 클러스터에서 용량 디바이스를 제거하고 새 용량 디바이스를 추가하면 vSAN 클러스터가 용량 활용률 관점에서 불균형 상태가 될 수 있습니다. vSAN 상태 모니터링에 불균형에 대한 주의가 표시되면 클러스터를 재조정할 수 있습니다.

필수 조건

재조정 작업은 클러스터에 지나친 영향을 주지 않도록 업무 시간을 피해서 수행합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭을 클릭하고 **vSAN**을 클릭합니다.
- 3 **상태**를 클릭합니다.
- 4 vSAN Health Service 테이블에서 **주의: vSAN 디스크 균형**을 선택합니다.
호스트의 디스크 균형을 검토할 수 있습니다.

5 클러스터를 재조정하려면 **디스크 재조정** 버튼을 클릭합니다.

이 작업은 과다 사용된 디스크에서 과소 사용된 디스크로 구성 요소를 이동합니다.

vSAN 기본 정보 사용

기본 vSAN 경보를 사용하여 클러스터, 호스트 및 기존 vSAN 라이선스를 모니터링할 수 있습니다.

기본 정보는 경보에 해당하는 이벤트가 활성화되거나 경보에 지정된 조건 중 하나 또는 전체가 충족되면 자동으로 트리거됩니다. 이러한 조건을 편집하거나 기본 경보를 삭제할 수 없습니다. 요구 사항에 맞게 경보를 구성하려면 vSAN에 대해 사용자 지정 경보를 생성합니다. [“vSAN 이벤트에 대한 vCenter Server 경고 생성,”](#) (146 페이지) 항목을 참조하십시오.

다음 표에는 기본 vSAN 경보가 나열되어 있습니다.

표 13-2. 기본 vSAN 경보

| vSAN 경보 | 설명 |
|--|---|
| 만료된 vSAN 시간 제한 라이선스 | vSAN 평가판 라이선스를 모니터링합니다. |
| 장애가 발생한 vSAN 호스트에서 VASA 벤더 제공자를 등록/등록 취소 | 장애가 발생한 vSAN 호스트에서 VASA 제공자를 등록하거나 등록 취소합니다. |
| 만료된 vSAN 라이선스 | 만료된 vSAN 라이선스를 모니터링합니다. |
| vSAN 호스트의 디스크에서 오류가 발생함 | vSAN 디바이스에서 오류를 모니터링합니다. |
| 그룹 테스트 '클러스터 상태'에 대한 vSAN Health Service 경보 | vSAN 클러스터 상태를 모니터링합니다. |
| 그룹 테스트 '데이터 상태'에 대한 vSAN Health Service 경보 | vSAN 클러스터 데이터 상태를 모니터링합니다. |
| 그룹 테스트 '제한 상태'에 대한 vSAN Health Service 경보 | vSAN 클러스터 제한을 모니터링합니다. |
| 그룹 테스트 '네트워크 상태'에 대한 vSAN Health Service 경보 | vSAN 네트워크 상태를 모니터링합니다. |
| 그룹 테스트 '물리적 디스크 상태'에 대한 vSAN Health Service 경보 | 클러스터에 포함된 물리적 디바이스의 상태를 모니터링합니다. |
| 그룹 테스트 'vSAN HCL 상태'에 대한 vSAN Health Service 경보 | 클러스터 구성 요소가 지원되는 하드웨어, 소프트웨어 및 드라이버를 사용하는지 모니터링합니다. |
| 그룹 테스트 '소프트웨어 상태'에 대한 vSAN Health Service 경보 | 클러스터에서 현재 사용 중인 소프트웨어의 상태를 모니터링합니다. |
| 그룹 테스트 '예기치 않은 vSAN 상태'에 대한 vSAN Health Service 경보 | 예기치 않은 클러스터 상태 문제를 모니터링합니다. |
| 그룹 테스트 'vSAN CLOMD 작동 여부'에 대한 vSAN Health Service 경보 | ESXi 호스트에서 실행되고 데이터 이동 및 제거를 담당하는 CLOMD(Cluster Level Object Manager Daemon)가 활성화 상태인지 여부를 모니터링합니다. |
| 그룹 테스트 'vSAN 클러스터 파티션'에 대한 vSAN Health Service 경보 | vSAN 클러스터 파티션을 모니터링합니다. |

경보 및 이벤트 모니터링과 기존 경보 설정의 편집에 대한 자세한 내용은 vSphere 모니터링 및 성능 설명서를 참조하십시오.

vSAN 기본 정보 보기

기본 vSAN 경보를 사용하면 클러스터와 호스트를 모니터링하고, 새로운 이벤트를 분석하고, 전반적인 클러스터 상태를 평가할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 구성을 클릭한 다음 **정보 정의**를 클릭합니다.
- 3 검색 상자에 **vSAN**을 검색 용어로 입력하여 vSAN에 해당하는 경보를 표시합니다.
vSAN Health Service 경보를 입력하여 vSAN Health Service 경보를 검색합니다.
기본 vSAN 경보가 표시됩니다.
- 4 정보 목록에서 각 경보를 클릭하여 정보 정의를 봅니다.

정보 생성에 VMkernel 관찰 사용

VOB(VMkernel 관찰)은 vSAN 클러스터에서 성능 및 네트워킹 문제를 모니터링하고 해결하기 위한 vSAN 경보를 설정하는 데 사용할 수 있는 시스템 이벤트입니다. vSAN에서 이러한 이벤트는 관찰로 알려져 있습니다.

vSAN 에 대한 VMware ESXi 관찰 ID

각 VOB 이벤트에는 ID(식별자)가 연결됩니다. vCenter Server에서 vSAN 경보를 생성하기 전에 경고를 생성할 vSAN 이벤트에 대한 적절한 VOB ID를 식별해야 합니다. VMware ESXi 관찰 로그 파일(vobd.log)에 경고를 생성할 수 있습니다. 예를 들어 클러스터의 모든 디바이스 장애에 대해 경고를 생성하려면 다음 VOB ID를 사용해야 합니다.

- esx.problem.vob.vsan.lsom.diskerror
- esx.problem.vob.vsan.pdl.offline

vSAN에 대한 VOB ID의 목록을 검토하려면 ESXi 호스트의 /var/log 디렉토리에 있는 vobd.log 파일을 엽니다. 로그 파일에는 vSAN 정보 생성에 사용할 수 있는 다음 VOB ID가 포함되어 있습니다.

표 13-3. vSAN 에 대한 VOB ID

| VOB ID | 설명 |
|--|---------------------------------|
| esx.audit.vsan.clustering.enabled | vSAN 클러스터링 서비스가 사용되도록 설정되었습니다. |
| esx.clear.vob.vsan.pdl.online | vSAN 디바이스가 온라인 상태로 전환되었습니다. |
| esx.clear.vsan.clustering.enabled | vSAN 클러스터링 서비스가 사용되도록 설정되었습니다. |
| esx.clear.vsan.vsan.network.availability | vSAN에 하나의 활성 네트워크 구성이 있습니다. |
| esx.clear.vsan.vsan.vmknics.ready | 이전에 보고된 vmknics가 유효한 IP를 받았습니다. |
| esx.problem.vob.vsan.lsom.componentthreshold | vSAN이 노드 구성 요소 수 제한에 거의 도달했습니다. |
| esx.problem.vob.vsan.lsom.diskerror | vSAN 디바이스가 영구적 오류 상태에 있습니다. |
| esx.problem.vob.vsan.lsom.diskerror | vSAN이 새 디스크 그룹을 생성하지 못했습니다. |
| esx.problem.vob.vsan.lsom.disklimit | vSAN이 디스크 그룹에 디바이스를 추가하지 못했습니다. |
| esx.problem.vob.vsan.lsom.diskunhealthy | vSAN 디스크가 비정상입니다. |
| esx.problem.vob.vsan.pdl.offline | vSAN 디바이스가 오프라인 상태입니다. |

표 13-3. vSAN 에 대한 VOB ID (계속)

| VOB ID | 설명 |
|---|--|
| esx.problem.vsan.clustering.disabled | vSAN 클러스터링 서비스가 사용되지 않도록 설정되었습니다. |
| esx.problem.vsan.lsom.congestionthreshold | vSAN 디바이스 메모리 또는 SSD 정체가 업데이트되었습니다. |
| esx.problem.vsan.net.not.ready | vmknic가 유효한 IP 주소 없이 vSAN 네트워크 구성에 추가되었습니다. vSAN 네트워크가 준비되지 않았을 때 이 상황이 발생합니다. |
| esx.problem.vsan.net.redundancy.lost | vSAN 네트워크 구성에 필요한 이중화가 없습니다. |
| esx.problem.vsan.no.network.connectivity | vSAN에 현재 사용 중인 기존 네트워킹 구성이 없습니다. |
| esx.problem.vsan.vmknic.not.ready | vmknic가 유효한 IP 주소 없이 vSAN 네트워크 구성에 추가되었습니다. |

vSAN 이벤트에 대한 vCenter Server 정보 생성

클러스터, 호스트, 데이터스토어, 네트워크 및 가상 시스템을 포함하여 선택한 vSAN 개체에 대한 이벤트를 모니터링하기 위한 경보를 생성할 수 있습니다.

필수 조건

필요한 권한 수준인 Alarms.Create Alarm 또는 Alarm.Modify Alarm을 가지고 있어야 합니다.

프로시저

- 인벤토리에서 모니터링할 vCenter Server 개체를 선택합니다.
- 구성 탭 > **경보 정의**를 클릭한 후 **+** 아이콘을 클릭합니다.
- 새 경보의 이름과 설명을 입력합니다.
- 모니터** 드롭다운 메뉴에서 경보를 구성할 개체를 선택합니다.
- 이 개체에서 발생하는 특정 이벤트(예: VM 전원 켜기)**를 클릭하고 **다음**을 클릭합니다.
- 트리거**를 클릭하여 경보를 트리거할 vSAN 이벤트를 추가합니다. 트리거 페이지에 표시되는 옵션은 모니터링하려는 작업의 유형에 따라 다릅니다.
- 추가** 아이콘(**+**)을 클릭합니다.
- 이벤트** 열을 클릭하고 드롭다운 메뉴에서 옵션을 선택합니다.
- 상태** 열을 클릭하고 드롭다운 메뉴에서 옵션을 선택합니다.
- (선택 사항) 경보가 트리거되려면 충족해야 하는 추가 조건을 구성합니다.
 - 추가** 아이콘을 클릭하여 인수를 추가합니다.
 - 인수** 열을 클릭하고 드롭다운 메뉴에서 옵션을 선택합니다.
 - 연산자** 열을 클릭하고 드롭다운 메뉴에서 옵션을 선택합니다.
 - 값** 열을 클릭하고 텍스트 필드에 값을 입력합니다.
둘 이상의 인수를 추가할 수 있습니다.
- 다음**을 클릭합니다.

경보 트리거를 선택하고 구성했습니다.

vSAN 장애 처리 및 문제 해결

vSAN 사용 시 문제가 발생하는 경우 문제 해결 항목을 참조할 수 있습니다. 이 항목은 문제를 파악하는데 도움이 되며 적용 가능한 해결 방법이 있을 경우 이를 제공합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vSAN에 Esxcli 명령 사용,”](#) (147 페이지)
- [“ESXi 호스트에 대한 vSAN 구성이 실패할 수 있음,”](#) (150 페이지)
- [“비준수 가상 시스템 개체가 즉시 준수 상태가 되지 않음,”](#) (150 페이지)
- [“vSAN 클러스터 구성 문제,”](#) (151 페이지)
- [“vSAN에서 장애 처리,”](#) (151 페이지)
- [“vSAN 클러스터 종료,”](#) (164 페이지)

vSAN 에 Esxcli 명령 사용

Esxcli 명령을 사용하여 vSAN에 대한 정보를 가져오고 vSAN 환경의 문제를 해결할 수 있습니다.

다음 명령을 사용할 수 있습니다.

| 명령 | 설명 |
|--------------------------|------------------------------------|
| esxcli vsan network list | vSAN 통신에 사용되는 VMkernel 어댑터를 확인합니다. |
| esxcli vsan storage list | vSAN에 의해 할당된 스토리지 디스크를 나열합니다. |
| esxcli vsan cluster get | vSAN 클러스터 정보를 가져옵니다. |
| esxcli vsan health | vSAN 클러스터 상태를 가져옵니다. |
| esxcli vsan debug | vSAN 클러스터 디버그 정보를 가져옵니다. |

esxcli vsan debug 명령을 사용하면, 특히 vCenter Server를 사용할 수 없는 경우에 vSAN 클러스터를 디버깅하고 문제를 해결하는 데 도움이 됩니다.

사용: esxcli vsan debug {cmd} [cmd options]

디버깅 명령:

| 명령 | 설명 |
|------------------------------|-------------------------|
| esxcli vsan debug disk | vSAN 물리적 디스크를 디버깅합니다. |
| esxcli vsan debug object | vSAN 개체를 디버깅합니다. |
| esxcli vsan debug resync | vSAN 다시 동기화 개체를 디버깅합니다. |
| esxcli vsan debug controller | vSAN 디스크 컨트롤러를 디버깅합니다. |

| 명령 | 설명 |
|-------------------------|--------------------|
| esxcli vsan debug limit | vSAN 제한을 디버깅합니다. |
| esxcli vsan debug vmdk | vSAN VMDK를 디버깅합니다. |

esxcli vsan debug 명령 예:

```
esxcli vsan debug disk summary get
Overall Health: green
Component Metadata Health: green
Memory Pools (heaps): green
Memory Pools (slabs): green
```

```
esxcli vsan debug disk list
UUID: 52e1d1fa-af0e-0c6c-f219-e5e1d224b469
Name: mpx.vmhba1:C0:T1:L0
SSD: False
Overall Health: green
Congestion Health:
    State: green
    Congestion Value: 0
    Congestion Area: none
In Cmnds: true
In Vsi: true
Metadata Health: green
Operational Health: green
Space Health:
    State: green
    Capacity: 107365793792 bytes
    Used: 1434451968 bytes
    Reserved: 150994944 bytes
```

```
esxcli vsan debug object health summary get
```

| Health Status | Number Of Objects |
|--|-------------------|
| reduced-availability-with-no-rebuild-delay-timer | 0 |
| reduced-availability-with-active-rebuild | 0 |
| inaccessible | 0 |
| data-move | 0 |
| healthy | 1 |
| nonavailability-related-incompliance | 0 |
| nonavailability-related-reconfig | 0 |
| reduced-availability-with-no-rebuild | 0 |

```
esxcli vsan debug object list
Object UUID: 47cbdc58-e01c-9e33-dada-020010d5dfa3
Version: 5
Health: healthy
Owner:
Policy:
    stripeWidth: 1
    CSN: 1
    spbmProfileName: vSAN Default Storage Policy
    spbmProfileId: aa6d5a82-1c88-45da-85d3-3d74b91a5bad
    forceProvisioning: 0
    cacheReservation: 0
    proportionalCapacity: [0, 100]
```

spbmProfileGenerationNumber: 0
 hostFailuresToTolerate: 1

Configuration:

RAID_1

Component: 47cbdc58-6928-333f-0c51-020010d5dfa3
 Component State: ACTIVE, Address Space(B): 273804165120 (255.00GB),
 Disk UUID: 52e95956-42cf-4d30-9cbe-763c616614d5, Disk Name: mpx.vmhba1..
 Votes: 1, Capacity Used(B): 373293056 (0.35GB),
 Physical Capacity Used(B): 369098752 (0.34GB), Host Name: sc-rdops..
 Component: 47cbdc58-eebf-363f-cf2b-020010d5dfa3
 Component State: ACTIVE, Address Space(B): 273804165120 (255.00GB),
 Disk UUID: 52d11301-1720-9901-eb0a-157d68b3e4fc, Disk Name: mpx.vmh..
 Votes: 1, Capacity Used(B): 373293056 (0.35GB),
 Physical Capacity Used(B): 369098752 (0.34GB), Host Name: sc-rdops-vm..
 Witness: 47cbdc58-21d2-383f-e45a-020010d5dfa3
 Component State: ACTIVE, Address Space(B): 0 (0.00GB),
 Disk UUID: 52bfd405-160b-96ba-cf42-09da8c2d7023, Disk Name: mpx.vmh..
 Votes: 1, Capacity Used(B): 12582912 (0.01GB),
 Physical Capacity Used(B): 4194304 (0.00GB), Host Name: sc-rdops-vm..

Type: vmnamespace

Path: /vmfs/volumes/vsan:52134fafd48ad6d6-bf03cb6af0f21b8d/New Virtual Machine
 Group UUID: 00000000-0000-0000-0000-000000000000
 Directory Name: New Virtual Machine

esxcli vsan debug controller list

Device Name: vmhba1
 Device Display Name: LSI Logic/Symbios Logic 53c1030 PCI-X Fusion-MPT Dual Ult..
 Used By VSAN: true
 PCI ID: 1000/0030/15ad/1976
 Driver Name: mptspi
 Driver Version: 4.23.01.00-10vmw
 Max Supported Queue Depth: 127

esxcli vsan debug limit get

Component Limit Health: green
 Max Components: 750
 Free Components: 748
 Disk Free Space Health: green
 Lowest Free Disk Space: 99 %
 Used Disk Space: 1807745024 bytes
 Used Disk Space (GB): 1.68 GB
 Total Disk Space: 107365793792 bytes
 Total Disk Space (GB): 99.99 GB
 Read Cache Free Reservation Health: green

```
Reserved Read Cache Size: 0 bytes
Reserved Read Cache Size (GB): 0.00 GB
Total Read Cache Size: 0 bytes
Total Read Cache Size (GB): 0.00 GB
```

```
esxcli vsan debug vmdk list
Object: 50cbdc58-506f-c4c2-0bde-020010d5dfa3
Health: healthy
Type: vdisk
Path: /vmfs/volumes/vsan:52134fafd48ad6d6-bf03cb6af0f21b8d/47cbdc58-e01c-9e33-
dada-020010d5dfa3/New Virtual Machine.vmdk
Directory Name: N/A
```

```
esxcli vsan debug resync list
```

| Object | Component | Bytes Left To Resync | GB Left To Resync |
|------------------|-----------------------|----------------------|-------------------|
| 31cfdc58-e68d... | Component:23d1dc58... | 536870912 | 0.50 |
| 31cfdc58-e68d... | Component:23d1dc58... | 1073741824 | 1.00 |
| 31cfdc58-e68d... | Component:23d1dc58... | 1073741824 | 1.00 |

ESXi 호스트에 대한 vSAN 구성이 실패할 수 있음

경우에 따라 특정 호스트의 vSAN을 구성하지 못할 수 있습니다.

문제점

vSAN 클러스터에 가입하는 ESXi 호스트에 vSAN을 구성하지 못합니다.

원인

호스트가 하드웨어 요구 사항을 충족하지 않거나 다른 문제가 있을 경우 vSAN이 호스트를 구성하지 못할 수 있습니다. 예를 들어 호스트의 메모리가 부족하면 vSAN을 구성할 수 없습니다.

해결 방법

- 1 실패 원인이 되는 호스트를 유지 보수 모드로 전환합니다.
- 2 호스트를 vSAN 클러스터 외부로 이동합니다.
- 3 호스트에서 vSAN을 구성하지 못하도록 막는 문제를 해결합니다.
- 4 유지 보수 모드를 종료합니다.
- 5 호스트를 vSAN 클러스터로 다시 이동합니다.

비준수 가상 시스템 개체가 즉시 준수 상태가 되지 않음

규정 준수 검사 버튼을 사용할 때 vSAN 리소스를 사용할 수 있게 되어 가상 시스템 프로파일을 충족하는 경우에도 가상 시스템 개체의 상태가 비준수에서 준수로 변경되지 않습니다.

문제점

강제 프로비저닝을 사용하면 vSAN 클러스터에서 사용 가능한 리소스가 가상 시스템 프로파일에 지정된 정책을 충족할 수 없는 경우라도 가상 시스템 개체를 프로비저닝할 수 있습니다. 이때 개체는 생성되지만 비준수 상태로 유지됩니다.

호스트를 추가하는 경우와 같이 클러스터의 스토리지 리소스를 사용할 수 있게 되면 vSAN은 개체를 준수 상태로 전환해야 합니다. 하지만 리소스를 추가한 직후에 개체 상태가 준수로 변경되지는 않습니다.

원인

이는 vSAN이 시스템 오버로드를 방지하기 위해 재구성 속도를 조절하기 때문입니다. 준수 상태로 전환되는 데 걸리는 시간은 클러스터에 있는 개체 수, 클러스터의 I/O 로드 및 해당 개체의 크기에 따라 다릅니다. 대부분의 경우 적절한 시간 내에 준수 상태로 전환됩니다.

vSAN 클러스터 구성 문제

vSAN 구성을 변경한 후 vCenter Server는 vSAN 구성에 대한 유효성 검사를 수행합니다. 유효성 검사는 호스트 동기화 프로세스의 일부로도 수행됩니다. vCenter Server는 구성 문제가 감지될 경우 오류 메시지를 표시합니다.

문제점

오류 메시지가 vCenter Server가 vSAN 구성에 문제가 있음을 감지했음을 나타냅니다.

해결 방법

다음 방법을 사용하여 vSAN 구성 문제를 해결합니다.

표 14-1. vSAN 구성 오류 및 솔루션

| vSAN 구성 오류 | 솔루션 |
|--|---|
| VSAN 서비스를 사용하도록 설정된 호스트가 vCenter 클러스터에 없음 | 호스트를 vSAN 클러스터에 추가합니다. 1 호스트를 마우스 오른쪽 버튼으로 클릭하고 다음으로 이동 을 선택합니다. 2 vSAN 클러스터를 선택한 후 확인 을 클릭합니다. |
| 호스트가 VSAN 지원 클러스터에 있지만 VSAN 서비스를 사용하도록 설정되어 있지 않음 | vSAN 네트워크가 올바르게 구성되어 있고 호스트에서 사용하도록 설정되어 있는지 확인합니다. " vSAN 네트워크 구성 ," (41 페이지)를 참조하십시오. |
| VSAN 네트워크가 구성되어 있지 않음 | vSAN 네트워크를 구성합니다. " vSAN 네트워크 구성 ," (41 페이지)를 참조하십시오. |
| 호스트가 VSAN 지원 클러스터의 다른 모든 노드와 통신할 수는 없음 | 네트워크 분리로 인한 문제일 수 있습니다. " vSAN에 대한 네트워킹 요구 사항 ," (19 페이지) 설명서를 참조하십시오. |
| VSAN 서버에 참여하고 있지만 이 호스트의 vCenter 클러스터 멤버가 아닌 또 다른 호스트가 발견됨 | vSAN 클러스터 구성이 올바르고 모든 vSAN 호스트가 동일한 서브넷에 있는지 확인합니다. " vSAN 네트워크 설계 ," (29 페이지)를 참조하십시오. |

vSAN 에서 장애 처리

vSAN은 클러스터에서 스토리지 디바이스, 호스트 및 네트워크의 장애를 장애 심각도에 따라 처리합니다. vSAN 데이터스토어 및 네트워크의 성능을 관찰하여 vSAN에서 문제를 진단할 수 있습니다.

vSAN 에서 장애 처리

vSAN은 장애를 나타내고 데이터 보호를 위해 사용할 수 없는 데이터를 복구하기 위한 메커니즘을 구현합니다.

vSAN 구성 요소의 장애 상태

vSAN에서 장애가 발생한 구성 요소는 없음 또는 성능 저하될 상태일 수 있습니다. vSAN은 구성 요소 상태에 따라 가상 시스템 데이터 복구에 다른 접근 방식을 사용합니다.

vSAN은 구성 요소 장애 유형에 대한 경고도 제공합니다. "[경보 생성에 VMkernel 관찰 사용](#)," (145 페이지) 및 "[vSAN 기본 경고 사용](#)," (144 페이지) 항목을 참조하십시오.

vSAN은 구성 요소에 대한 다음과 같은 2개 유형의 장애 상태를 지원합니다.

표 14-2. vSAN 구성 요소의 장애 상태

| 구성 요소 장애 상태 | 설명 | 복구 | 원인 |
|-------------|---|---|---|
| 성능 저하됨 | vSAN에서 영구적인 구성 요소 장애를 감지하고 구성 요소가 작동 상태로 복구되지 않는다고 가정하는 경우 구성 요소는 성능 저하됨 상태가 됩니다. | vSAN은 즉시 관련 구성 요소를 재구축하기 시작합니다. | <ul style="list-style-type: none"> ■ 플래시 캐시 디바이스의 장애 ■ 자기 또는 플래시 용량 디바이스 장애 ■ 스토리지 컨트롤러 장애 |
| 없음 | vSAN이 구성 요소가 작동 상태를 복구 및 복원할 수 있는 일시적인 구성 요소 장애를 감지하는 경우 구성 요소가 없음 상태가 됩니다. | vSAN은 특정 시간 제한 내에 없음 구성 요소를 사용할 수 없으면 해당 구성 요소를 재구축하기 시작합니다. 기본적으로 vSAN은 60분 후 없음 구성 요소를 재구축하기 시작합니다. | <ul style="list-style-type: none"> ■ 네트워크 연결이 손실됨 ■ 물리적 네트워크 어댑터의 장애 ■ ESXi 호스트 장애 ■ 연결이 끊긴 플래시 캐시 디바이스 ■ 연결이 끊긴 자기 디스크 또는 플래시 용량 디바이스 |

구성 요소의 장애 상태 검토

vSphere Web Client를 사용하여 구성 요소가 없음 또는 성능 저하됨 장애 상태인지 검토합니다.

클러스터에서 장애가 발생할 경우 vSAN은 장애 심각도를 기반으로 개체에 대한 구성 요소를 없음 또는 성능 저하됨으로 표시합니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭에서 **vSAN**을 클릭하고 **가상 디스크**를 선택합니다.
클러스터의 가상 시스템의 홈 디렉토리 및 가상 디스크가 나타납니다.
- 3 가상 시스템 개체를 선택합니다.
- 4 **물리적 디스크 배치** 탭에서 선택한 개체에 대한 구성 요소의 구성 요소 상태 속성을 검토합니다.
vSAN 클러스터에서 장애가 발생한 경우 구성 요소 상태 속성은 없음 또는 성능 저하됨과 같습니다.

vSAN 에서 문제를 나타내는 개체 상태

가상 시스템 개체의 규정 준수 상태 및 작동 상태를 검토하여 클러스터의 장애가 가상 시스템에 어떻게 영향을 미치는지 판단합니다.

표 14-3. 개체 상태

| 개체 상태 유형 | 설명 |
|----------|---|
| 규정 준수 상태 | 가상 시스템 개체의 규정 준수 상태는 할당된 VM 스토리지 정책의 요구 사항을 충족하는지 여부를 나타냅니다. |
| 작동 상태 | <p>개체의 작동 상태는 정상 또는 비정상일 수 있습니다. 클러스터의 장애 유형 및 수를 나타냅니다.</p> <p>개체는 완전한 복제본을 사용할 수 있고 개체 투표의 50% 이상을 계속 사용할 수 있는 경우 정상입니다.</p> <p>개체는 전체 복제본을 사용할 수 없고 사용할 수 없는 개체 투표가 50% 미만인 경우 비정상입니다. 예를 들어 개체는 클러스터에 네트워크 장애가 발생하고 호스트가 분리되는 경우 비정상이 될 수 있습니다.</p> |

가상 시스템에 대한 장애의 전체적인 영향을 판단하려면 규정 준수 상태와 작동 상태를 검토합니다. 개체가 규정 비준수임에도 작동 상태가 정상으로 남아 있는 경우 가상 시스템은 계속해서 vSAN 데이터스토어를 사용할 수 있습니다. 작동 상태가 비정상인 경우 가상 시스템은 해당 데이터스토어를 사용할 수 없습니다.

vSAN 에서 개체의 상태 검토

vSphere Web Client를 사용하여 가상 시스템이 정상인지 검토합니다. 가상 시스템은 VM 개체의 복제본과 개체에 대한 투표의 50% 이상을 사용 가능한 경우 정상으로 간주됩니다.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 **모니터** 탭에서 **vSAN**을 클릭하고 **가상 디스크**를 선택합니다.
클러스터의 가상 시스템의 홈 디렉토리 및 가상 디스크가 나타납니다.
- 3 가상 시스템 개체의 경우 작동 상태 속성의 값을 검토합니다.
작동 상태가 비정상인 경우 vSphere Web Client는 대괄호 안에 비정상 상태에 대한 이유를 나타냅니다.

vSAN 에서 가상 시스템의 규정 준수 검사

vSphere Web Client를 사용하여 가상 시스템 개체가 할당된 VM 스토리지 정책을 준수하는지 검사합니다.

프로시저

- 1 가상 시스템의 규정 준수 상태를 검사합니다.
 - a vSphere Web Client 탐색기에서 가상 시스템을 찾습니다.
 - b **요약** 탭의 VM 스토리지 정책 아래에서 VM 스토리지 정책 규정 준수 속성의 값을 검사합니다.
- 2 가상 시스템의 개체의 규정 준수 상태를 검사합니다.
 - a vSphere Web Client에서 vSAN 클러스터로 이동합니다.
 - b **모니터** 탭에서 **vSAN**을 클릭하고 **가상 디스크**를 선택합니다.
 - c 가상 시스템 개체를 선택합니다.
 - d 개체에 대한 규정 준수 상태 속성의 값을 검사합니다. 규정 준수 상태가 준수가 아닌 경우 미준수의 원인을 파악합니다.
 - 개체의 작동 상태를 검사하여 개체 상태가 정상인지 확인합니다.
 - **규정 준수 실패** 탭에서 개체가 충족할 수 없는 VM 스토리지 정책 요구 사항을 검사합니다.
 - **물리적 디스크 배치** 탭에서 개체 구성 요소의 상태를 검사합니다.

vSAN 에서 장애 발생 시 가상 시스템의 액세스 지원

가상 시스템이 vSAN 스토리지를 사용하는 경우 vSAN 클러스터의 장애 유형에 따라 해당 스토리지 액세스 지원이 변경될 수 있습니다.

액세스 지원의 변경은 클러스터에서 가상 시스템 개체가 허용하는 정책보다 더 많은 장애가 발생하는 경우에 발생합니다.

vSAN 클러스터의 장애로 인해 가상 시스템 개체에 액세스하지 못하게 될 수 있습니다. 장애가 모든 복제본에 영향을 주어 개체의 전체 복제본을 사용할 수 없는 경우 또는 사용할 수 있는 개체 투표가 50% 미만인 경우에는 개체에 액세스할 수 없습니다.

액세스할 수 없는 개체의 유형에 따라 가상 시스템은 다음과 같은 방식으로 동작합니다.

표 14-4. 가상 시스템 개체의 액세스 불가능

| 개체 유형 | 가상 시스템 상태 | 가상 시스템 증상 |
|-------------|---|---|
| VM 홈 네임스페이스 | <ul style="list-style-type: none"> ■ 액세스할 수 없음 ■ vCenter Server 또는 ESXi 호스트가 가상 시스템의 .vmx 파일에 액세스할 수 없는 경우 연결이 끊어집니다. | 가상 시스템 프로세스가 충돌하고 가상 시스템의 전원이 꺼질 수 있습니다. |
| VMDK | 액세스할 수 없음 | 가상 시스템이 전원이 켜진 상태로 유지되지만 VMDK에 대한 I/O 작업이 실행되고 있지 않습니다. 특정 시간 제한이 지난 후 게스트 운영 체제는 해당 작업을 종료합니다. |

가상 시스템 액세스 불가능이 영구 상태가 아닙니다. 기본 문제가 해결되고 전체 복제본과 개체 투표의 50% 이상이 복원된 후 가상 시스템은 자동으로 다시 액세스할 수 있게 됩니다.

vSAN 클러스터에서 스토리지 디바이스 장애 발생

vSAN은 각 스토리지 디바이스의 성능을 모니터링하여 비정상 디바이스를 사전 예방적으로 분리합니다. 또한 스토리지 디바이스의 점진적 장애를 감지하고, 영향을 받은 호스트와 전체 vSAN 클러스터 내에 정체가 발생하기 전에 해당 디바이스를 분리합니다.

디스크에서 높은 지연 시간이나 정체가 지속적으로 발생할 경우 vSAN은 디바이스를 곧 비활성 상태가 될 디스크로 간주하고 해당 디스크로부터 데이터를 제거합니다. vSAN은 데이터를 제거하거나 재구축하여, 곧 비활성 상태가 될 디스크를 처리합니다. 클러스터에 리소스가 부족하거나 액세스할 수 없는 개체가 있지 않는 한 사용자 작업은 불필요합니다.

구성 요소 장애 상태 및 액세스 지원

자기 디스크나 플래시 용량 디바이스에 있는 vSAN 구성 요소는 없음으로 표시됩니다.

vSAN 의 동작

vSAN은 다음과 같은 방식으로 스토리지 디바이스 장애에 응답합니다.

| 매개 변수 | 동작 |
|---------|--|
| 경보 | 비정상 장치가 진단될 때마다 각 호스트에서 경보가 생성됩니다. 디스크가 비정상인 것으로 의심될 때마다 주의가 발생합니다. |
| 상태 점검 | 전체 디스크 상태 점검에서 곧 비활성 상태가 될 디스크에 대해 주의를 발생시킵니다. |
| 상태 | [디스크 관리] 페이지에서 곧 비활성 상태가 될 디스크의 상태가 비정상 으로 나열됩니다. vSAN에서 데이터 제거를 완료하면 상태가 DyingDiskEmpty 로 나열됩니다. |
| 데이터 재구축 | vSAN은 호스트와 용량 디바이스가 장애가 발생한 디바이스 또는 디스크 그룹의 개체에 대한 공간 및 배치 규칙에 대한 요구 사항을 충족할 수 있는지 검토합니다. 용량이 포함된 이러한 호스트를 사용할 수 있는 경우 구성 요소가 성능 저하됨으로 표시되기 때문에 vSAN은 즉시 복구 프로세스를 시작합니다. 사용 가능한 리소스가 있으면 vSAN이 데이터를 자동으로 다시 보호합니다. |

vSAN은 영구 오류가 있는 디스크를 감지하면 디스크를 마운트 해제했다가 마운트하여 제한된 횟수 동안 디스크 재활성화를 시도합니다.

vSAN 클러스터에서 용량 디바이스에 액세스할 수 없음

자기 디스크나 플래시 용량 디바이스에 장애가 발생할 경우, vSAN은 해당 디바이스에서 개체의 액세스 지원을 평가하고, **허용할 수 있는 장애의 기본 수준**이 1 이상으로 설정되고 다른 호스트에 사용 가능한 공간이 있으면 해당 호스트에 개체를 재구축합니다.

구성 요소 장애 상태 및 액세스 지원

자기 디스크나 플래시 용량 디바이스에 있는 vSAN 구성 요소는 저하됨 상태로 표시됩니다.

vSAN 의 동작

vSAN은 다음과 같은 방식으로 용량 디바이스 장애에 응답합니다.

| 매개 변수 | 동작 |
|--------------------|--|
| 허용할 수 있는 장애의 기본 수준 | VM 스토리지 정책의 허용할 수 있는 장애의 기본 수준 이 1보다 크거나 같으면 클러스터의 다른 ESXi 호스트에서 가상 시스템 개체에 계속해서 액세스할 수 있습니다. 리소스를 사용할 수 있는 경우 vSAN은 자동 다시 보호를 시작합니다. 허용할 수 있는 장애의 기본 수준 이 0으로 설정되어 있는 경우, 개체의 구성 요소 중 하나가 장애가 발생한 용량 디바이스에 있으면 가상 시스템 개체에 액세스할 수 없습니다. 백업에서 가상 시스템을 복원합니다. |
| 용량 디바이스 의 I/O 작업 | vSAN은 장애가 발생한 구성 요소 없이 개체를 계속해서 사용할 수 있는지 다시 평가할 때까지 5-7 초 동안 실행 중인 모든 I/O 작업을 중지합니다. vSAN이 개체를 사용할 수 있음을 판단하는 경우 실행 중인 모든 I/O 작업이 재개됩니다. |
| 데이터 재구축 | vSAN은 호스트와 용량 디바이스가 장애가 발생한 디바이스 또는 디스크 그룹의 개체에 대한 공간 및 배치 규칙에 대한 요구 사항을 충족할 수 있는지 검토합니다. 용량이 포함된 이러한 호스트를 사용할 수 있는 경우 구성 요소가 성능 저하됨으로 표시되기 때문에 vSAN은 즉시 복구 프로세스를 시작합니다. 리소스가 사용 가능하면 자동 다시 보호가 발생합니다. |

vSAN 클러스터에서 플래시 캐시 디바이스에 액세스할 수 없음

플래시 캐시 디바이스에 장애가 발생할 경우, vSAN은 캐시 디바이스가 포함된 디스크 그룹에서 개체의 액세스 지원을 평가한 후 **허용할 수 있는 장애의 기본 수준**이 1 이상으로 설정되어 있으면 가능한 경우 다른 호스트에 개체를 재구축합니다.

구성 요소 장애 상태 및 액세스 지원

디스크 그룹에 있는 캐시 디바이스와 용량 디바이스(예: 자기 디스크)가 성능 저하됨으로 표시됩니다. vSAN은 단일 플래시 캐시 디바이스의 장애를 전체 디스크 그룹의 장애로 해석합니다.

vSAN 의 동작

vSAN은 다음과 같은 방식으로 플래시 캐시 디바이스의 장애에 응답합니다.

| 매개 변수 | 동작 |
|--------------------|---|
| 허용할 수 있는 장애의 기본 수준 | VM 스토리지 정책의 허용할 수 있는 장애의 기본 수준 이 1보다 크거나 같으면 클러스터의 다른 ESXi 호스트에서 가상 시스템 개체에 계속해서 액세스할 수 있습니다. 리소스를 사용할 수 있는 경우 vSAN은 자동 다시 보호를 시작합니다. 허용할 수 있는 장애의 기본 수준 이 0으로 설정되어 있는 경우, 개체의 구성 요소 중 하나가 장애가 발생한 디스크 그룹에 있으면 가상 시스템 개체에 액세스할 수 없습니다. |
| 디스크 그룹에 대한 I/O 작업 | vSAN은 장애가 발생한 구성 요소 없이 개체를 계속해서 사용할 수 있는지 다시 평가할 때까지 5-7 초 동안 실행 중인 모든 I/O 작업을 중지합니다. vSAN이 개체를 사용할 수 있음을 판단하는 경우 실행 중인 모든 I/O 작업이 재개됩니다. |
| 데이터 재구축 | vSAN은 호스트와 용량 디바이스가 장애가 발생한 디바이스 또는 디스크 그룹의 개체에 대한 공간 및 배치 규칙에 대한 요구 사항을 충족할 수 있는지 검토합니다. 용량이 포함된 이러한 호스트를 사용할 수 있는 경우 구성 요소가 성능 저하됨으로 표시되기 때문에 vSAN은 즉시 복구 프로세스를 시작합니다. |

vSAN 클러스터에서 호스트가 응답하지 않음

호스트의 장애나 재부팅 때문에 호스트가 응답을 중지한 경우, vSAN이 클러스터의 다른 호스트에서 구성 요소를 재구축하기 전에 vSAN은 호스트의 복구를 기다립니다.

구성 요소 장애 상태 및 액세스 지원

호스트에 있는 vSAN 구성 요소가 없음으로 표시됩니다.

vSAN 의 동작

vSAN은 다음과 같은 방식으로 호스트 장애에 응답합니다.

| 매개 변수 | 동작 |
|--------------------|---|
| 허용할 수 있는 장애의 기본 수준 | VM 스토리지 정책의 허용할 수 있는 장애의 기본 수준 이 1보다 크거나 같으면 클러스터의 다른 ESXi 호스트에서 가상 시스템 개체에 계속해서 액세스할 수 있습니다. 리소스를 사용할 수 있는 경우 vSAN은 자동 다시 보호를 시작합니다. 허용할 수 있는 장애의 기본 수준 이 0으로 설정되어 있는 경우, 개체의 구성 요소가 장애가 발생한 호스트에 있으면 가상 시스템 개체에 액세스할 수 없습니다. |
| 호스트의 I/O 작업 | vSAN은 장애가 발생한 구성 요소 없이 개체를 계속해서 사용할 수 있는지 다시 평가할 때까지 5-7 초 동안 실행 중인 모든 I/O 작업을 중지합니다. vSAN이 개체를 사용할 수 있음을 판단하는 경우 실행 중인 모든 I/O 작업이 재개됩니다. |
| 데이터 재구축 | 호스트가 60분 이내에 클러스터에 재가입되지 않는 경우 vSAN은 클러스터의 다른 호스트 중 일부가 액세스할 수 없는 호스트의 개체에 대한 캐시, 공간 및 배치 규칙에 대한 요구 사항을 충족할 수 있는지 검토합니다. 이러한 호스트를 사용할 수 있는 경우 vSAN은 복구 프로세스를 시작합니다. 호스트가 60분 후 클러스터에 재가입되고 복구가 시작된 경우 vSAN은 복구를 계속하거나 복구를 중지하고 원래 구성 요소를 다시 동기화할지 평가합니다. |

vSAN 클러스터에서 네트워크 연결이 끊김

클러스터에서 호스트 간의 연결이 끊기면 vSAN은 연결이 복원되지 않을 경우 활성 파티션을 파악하고 분리된 파티션의 구성 요소를 활성 파티션에서 재구축합니다.

구성 요소 장애 상태 및 액세스 지원

vSAN은 개체 투표 중 50% 이상이 사용 가능한 파티션을 확인합니다. 격리된 호스트의 구성 요소는 없음으로 표시됩니다.

vSAN 의 동작

vSAN은 다음과 같은 방식으로 네트워크 장애에 응답합니다.

| 매개 변수 | 동작 |
|--------------------|--|
| 허용할 수 있는 장애의 기본 수준 | VM 스토리지 정책의 허용할 수 있는 장애의 기본 수준 이 1보다 크거나 같으면 클러스터의 다른 ESXi 호스트에서 가상 시스템 개체에 계속해서 액세스할 수 있습니다. 리소스를 사용할 수 있는 경우 vSAN은 자동 다시 보호를 시작합니다. 허용할 수 있는 장애의 기본 수준 이 0으로 설정되어 있는 경우, 개체의 구성 요소가 격리된 호스트에 있으면 가상 시스템 개체에 액세스할 수 없습니다. |
| 격리된 호스트의 I/O 작업 | vSAN은 장애가 발생한 구성 요소 없이 개체를 계속해서 사용할 수 있는지 다시 평가할 때까지 5-7 초 동안 실행 중인 모든 I/O 작업을 중지합니다. vSAN이 개체를 사용할 수 있음을 판단하는 경우 실행 중인 모든 I/O 작업이 재개됩니다. |
| 데이터 재구축 | 호스트가 60분 이내에 클러스터에 재가입되는 경우 vSAN은 호스트의 구성 요소를 동기화합니다. 호스트가 60분 이내에 클러스터에 재가입되지 않는 경우 vSAN은 클러스터의 다른 호스트 중 일부가 액세스할 수 없는 호스트의 개체에 대한 캐시, 공간 및 배치 규칙에 대한 요구 사항을 충족할 수 있는지 검토합니다. 이러한 호스트를 사용할 수 있는 경우 vSAN은 복구 프로세스를 시작합니다. 호스트가 60분 후 클러스터에 재가입되고 복구가 시작된 경우 vSAN은 복구를 계속하거나 복구를 중지하고 원래 구성 요소를 다시 동기화할지 평가합니다. |

vSAN 클러스터의 스토리지 컨트롤러 장애

스토리지 컨트롤러에 장애가 발생하는 경우 vSAN은 컨트롤러에 연결된 디스크 그룹에 있는 개체의 액세스 지원을 평가한 후 다른 호스트에 재구축합니다.

증상

호스트에 단일 스토리지 컨트롤러와 여러 디스크 그룹이 포함되어 있으며 모든 디스크 그룹의 모든 디바이스에 장애가 발생한 경우 공통 스토리지 컨트롤러의 장애가 근본 원인이라고 가정할 수 있습니다. VMkernel 로그 메시지를 검토하여 장애의 특성을 확인합니다.

구성 요소 장애 상태 및 액세스 지원

스토리지 컨트롤러에 장애가 발생하는 경우 컨트롤러에 연결된 모든 디스크 그룹의 플래시 캐시 디바이스 및 용량 디바이스의 구성 요소가 성능 저하됨으로 표시됩니다.

호스트에 여러 컨트롤러가 포함되어 있으며 개별 컨트롤러에 연결된 디바이스만 액세스할 수 없는 경우 이 컨트롤러에 장애가 발생했다고 가정할 수 있습니다.

vSAN 의 동작

vSAN은 다음과 같은 방식으로 스토리지 컨트롤러 장애에 응답합니다.

| 매개 변수 | 동작 |
|--------------------|---|
| 허용할 수 있는 장애의 기본 수준 | VM 스토리지 정책의 허용할 수 있는 장애의 기본 수준 이 1보다 크거나 같으면 클러스터의 다른 ESXi 호스트에서 가상 시스템 개체에 계속해서 액세스할 수 있습니다. 리소스를 사용할 수 있는 경우 vSAN은 자동 다시 보호를 시작합니다. 허용할 수 있는 장애의 기본 수준 이 0으로 설정되어 있는 경우, 개체의 구성 요소가 스토리지 컨트롤러에 연결된 디스크 그룹에 있으면 가상 시스템 개체에 액세스할 수 없습니다. |
| 데이터 재구축 | vSAN은 호스트와 용량 디바이스가 장애가 발생한 디바이스 또는 디스크 그룹의 개체에 대한 공간 및 배치 규칙에 대한 요구 사항을 충족할 수 있는지 검토합니다. 용량이 포함된 이러한 호스트를 사용할 수 있는 경우 구성 요소가 성능 저하됨으로 표시되기 때문에 vSAN은 즉시 복구 프로세스를 시작합니다. |

확장된 클러스터 사이트 장애 또는 네트워크 연결 손실

vSAN 확장된 클러스터는 사이트 간의 네트워크 연결 손실 또는 한 사이트의 일시적인 손실로 인해 발생하는 장애를 관리합니다.

확장된 클러스터 장애 처리

대부분의 경우 확장된 클러스터는 장애 동안 계속해서 작동하고 장애가 해결된 후 자동으로 복구합니다.

표 14-5. 확장된 클러스터가 장애를 처리하는 방식

| 장애 유형 | 동작 |
|-------------------------|--|
| 활성 사이트 간 네트워크 연결 손실 | 2개의 활성 사이트 간에 네트워크 연결이 실패하는 경우 감시 호스트 및 기본 사이트가 계속해서 스토리지 작업을 제공하고 데이터를 사용할 수 있도록 유지합니다. 네트워크 연결이 복구되는 경우 2개의 활성 사이트가 다시 동기화됩니다. |
| 보조 사이트 장애 또는 네트워크 연결 손실 | 보조 사이트가 오프라인으로 전환되거나 기본 사이트 및 감시 호스트에서 분리되는 경우 감시 호스트 및 기본 사이트가 계속해서 스토리지 작업을 제공하고 데이터를 사용할 수 있도록 유지합니다. 보조 사이트가 클러스터로 돌아오면 2개의 활성 사이트가 다시 동기화됩니다. |

표 14-5. 확장된 클러스터가 장애를 처리하는 방식 (계속)

| 장애 유형 | 동작 |
|-------------------------|---|
| 기본 사이트 장애 또는 네트워크 연결 손실 | 기본 사이트가 오프라인으로 전환되거나 보조 사이트 및 감시 호스트에서 분리되는 경우 보조 사이트가 감시 호스트에 연결되어 있으면 스토리지 작업을 계속합니다. 기본 사이트가 클러스터로 돌아오면 2개의 활성 사이트가 다시 동기화됩니다. |
| 감시 호스트 장애 또는 네트워크 연결 손실 | 감시 호스트가 오프라인으로 전환되거나 기본 사이트 또는 보조 사이트에서 분리되는 경우 개체가 비준수 상태가 되지만 데이터를 계속해서 사용할 수 있습니다. 현재 실행 중인 VM은 영향을 받지 않습니다. |

vSAN 문제 해결

가상 시스템의 성능과 액세스 지원을 검토하여 vSAN 클러스터의 문제를 진단합니다.

VMware 호환성 가이드 에 대한 드라이버, 펌웨어, 스토리지 I/O 컨트롤러 확인

vSAN Health Service를 사용하여 하드웨어 구성 요소, 드라이버 및 펌웨어가 vSAN과 호환되는지 확인합니다.

vSAN과 호환되지 않는 하드웨어 구성 요소, 드라이버 및 펌웨어를 사용할 경우 vSAN 클러스터와 해당 클러스터에서 실행 중인 가상 시스템의 작업에 문제가 발생할 수 있습니다.

하드웨어 호환성 상태 점검은 VMware 호환성 가이드를 기준으로 하드웨어를 확인합니다. vSAN Health Service 사용에 대한 자세한 내용은 “vSAN 상태 모니터링,” (135 페이지)의 내용을 참조하십시오.

vSAN 클러스터에서 성능 검사

가상 시스템, 호스트 및 vSAN 데이터스토어의 성능을 모니터링하여 잠재적 스토리지 문제를 식별합니다.

다음의 성능 지표를 주기적으로 모니터링하여 vSphere Web Client의 성능 차트를 사용하는 등의 방법으로 vSAN 스토리지에서 장애를 식별합니다.

- 데이터스토어. 집계 데이터스토어에서 I/O 작업의 비율.
- 가상 시스템. I/O 작업, 메모리 및 CPU 사용량, 네트워크 처리량 및 대역폭.

vSAN 성능 서비스를 사용하면 세부적인 성능 차트에 액세스할 수 있습니다. 성능 서비스 사용에 대한 자세한 내용은 “vSAN 성능 모니터링,” (138 페이지)을 참조하십시오. vSAN 클러스터에서의 성능 데이터 사용에 대한 자세한 내용은 vSAN 문제 해결 참조 설명서 항목을 참조하십시오.

vSAN 클러스터의 잘못된 네트워크 구성 상태

클러스터에서 vSAN을 사용하도록 설정한 후 잘못된 네트워크 구성이 감지되어 해당 데이터스토어가 올바르게 구성되지 않습니다.

문제점

클러스터에서 vSAN을 사용하도록 설정한 후 클러스터에 대한 요약 탭에 vSAN에 대한 네트워크 상태가 잘못된 구성이 감지됨으로 나타납니다.

원인

하나 이상의 클러스터 멤버는 다음과 같은 이유 중 하나로 인해 통신할 수 없습니다.

- 클러스터의 호스트에 vSAN에 대한 VMkernel 어댑터가 없습니다.
- 호스트가 네트워크에서 서로 간에 연결할 수 없습니다.

해결 방법

클러스터의 멤버를 동일한 네트워크에 가입시킵니다. [“vSAN 네트워크 구성,”](#) (41 페이지)를 참조하십시오.

가상 시스템이 vSAN 에서 비준수, 액세스할 수 없음 또는 링크가 끊어짐으로 표시됨

vSAN 데이터스토어에 데이터를 저장하는 가상 시스템의 상태가 vSAN 클러스터의 장애 때문에 비준수, 액세스할 수 없음 또는 링크가 끊어짐으로 표시됩니다.

문제점

vSAN 데이터스토어의 가상 시스템이 vSAN 클러스터의 장애를 나타내는 다음 상태 중 하나에 있습니다.

- 가상 시스템이 규정을 준수하지 않으며 해당 개체 중 일부의 규정 준수 상태가 비준수입니다. [“vSAN에서 가상 시스템의 규정 준수 검사,”](#) (153 페이지)를 참조하십시오.
- 가상 시스템 개체가 액세스할 수 없거나 링크가 끊어진 상태입니다. [“구성 요소의 장애 상태 검토,”](#) (152 페이지)를 참조하십시오.

개체 복제본을 다른 호스트에서 사용 가능한 경우 vSAN은 가상 시스템의 I/O 작업을 복제본으로 전달합니다.

원인

가상 시스템의 개체가 할당된 VM 스토리지 정책의 요구 사항을 더 이상 충족할 수 없는 경우 vSAN은 이를 비준수로 간주합니다. 예를 들어 호스트의 연결이 일시적으로 끊길 수 있습니다. [“vSAN에서 문제를 나타내는 개체 상태,”](#) (152 페이지)를 참조하십시오.

vSAN이 전체 복제본 또는 개체 투표의 50% 이상을 찾을 수 없는 경우, 가상 시스템은 액세스할 수 없는 상태가 됩니다. VM 홈 네임스페이스가 손상되어 .vmx 파일에 액세스할 수 없음을 vSAN이 감지하면, 가상 시스템은 링크가 끊긴 상태가 됩니다. [“vSAN에서 장애 발생 시 가상 시스템의 액세스 지원,”](#) (153 페이지)를 참조하십시오.

해결 방법

클러스터에 충분한 리소스가 포함되어 있으면 vSAN은 장애가 영구적인 경우 손상된 개체를 자동으로 복구합니다.

클러스터에 리소스가 부족하여 손상된 개체를 재구축할 수 없는 경우에는 클러스터의 공간을 확장하십시오. [“vSAN 클러스터 용량 및 성능 확장,”](#) (108 페이지) 및 [“vSAN 클러스터에 호스트 추가,”](#) (108 페이지) 항목을 참조하십시오.

vSAN 에서 가상 시스템을 생성하려고 하면 오류 발생

vSAN 클러스터에서 가상 시스템을 배포하려고 시도하면 작업이 실패하며 가상 시스템 파일을 생성할 수 없다는 오류가 표시됩니다.

문제점

가상 시스템을 생성하는 작업이 파일 생성 작업을 완료할 수 없음 오류와 함께 실패합니다.

원인

vSAN에서 가상 시스템을 배포하는 작업은 몇 가지 이유로 실패할 수 있습니다.

- vSAN이 가상 시스템 스토리지 정책과 가상 시스템 개체에 공간을 할당할 수 없습니다. 이러한 실패는 데이터스토어에 충분한 용량이 없을 때 일어날 수 있습니다. 예를 들어, 물리적 디스크와 호스트의 연결이 임시로 끊어졌기 때문일 수 있습니다.
- 가상 시스템에 아주 큰 가상 디스크가 포함되어 있으며 클러스터의 호스트가 VM 스토리지 정책의 배치 규칙에 따라 해당 가상 디스크에 스토리지를 제공할 수 없습니다.

예를 들어 VM 스토리지 정책의 **허용할 수 있는 장애의 기본 수준**이 1로 설정되어 있으면 vSAN은 가상 디스크의 복제본 2개를 클러스터 내의 서로 다른 호스트에 하나씩 저장해야 합니다. 데이터스토어는 클러스터에서 모든 호스트의 사용 가능한 공간을 집계한 후에 이 공간을 확보해야 합니다. 하지만 별도의 가상 디스크 복제본을 저장하는 데 필요한 공간이 충분한 호스트 두 개를 클러스터에서 찾을 수 없습니다.

클러스터에 새로운 가상 시스템을 프로비저닝할 수 있는 공간이 충분하더라도 vSAN은 새 복제본의 사용 가능한 공간을 확보하기 위해 호스트 또는 디스크 그룹 간에 구성 요소를 이동하지 않습니다.

해결 방법

- ◆ 클러스터에서 용량 디바이스의 상태를 확인합니다.
 - a vSphere Web Client에서 vSAN 클러스터로 이동합니다.
 - b **모니터** 탭에서 **vSAN**을 클릭하고 **물리적 디스크**를 선택합니다.
 - c 클러스터의 호스트에서 디바이스의 상태와 용량을 검사합니다.

호스트를 추가할 때의 확장된 클러스터 구성 오류

확장된 클러스터에 새 호스트를 추가하려면 먼저 모든 현재 호스트가 연결되어 있어야 합니다. 현재 호스트의 연결이 끊어진 경우에는 새 호스트의 구성이 완료되지 않습니다.

문제점

일부 호스트의 연결이 끊어져 있는 확장된 클러스터에 새 호스트를 추가하면 클러스터의 [요약] 탭에서 vSAN의 [구성 상태]가 호스트에 유니캐스트 에이전트가 설정되지 않았습니~~다~~.로 표시됩니다.

원인

새 호스트가 확장된 클러스터에 가입하면 vSAN은 클러스터의 모든 호스트에서 구성을 업데이트해야 합니다. 호스트 하나 이상이 vCenter Server에 연결되어 있지 않으면 업데이트가 실패합니다. 새 호스트는 클러스터에 가입할 수 있지만 해당 구성은 완료되지 않은 상태입니다.

해결 방법

모든 호스트가 vCenter Server에 연결되었는지 확인하고, [구성 상태] 메시지에 제공된 링크를 클릭하여 새 호스트의 구성을 업데이트합니다.

연결이 끊어진 호스트를 클러스터에 다시 가입할 수 없으면 연결이 끊어진 호스트를 클러스터에서 제거한 후 [구성 상태] 메시지에 제공된 링크를 클릭하여 새 호스트의 구성을 업데이트합니다.

RVC를 사용하여 호스트를 추가할 때의 확장된 클러스터 구성 오류

RVC 도구를 사용하여 확장된 클러스터에 새 호스트를 추가하는 경우 새 호스트의 구성이 완료되지 않습니다.

문제점

RVC 도구를 사용하여 확장된 클러스터에 새 호스트를 추가한 후 클러스터에 대한 [요약] 탭에 vSAN에 대한 구성 상태가 호스트에 유니캐스트 에이전트가 설정되지 않았습니~~다~~.로 나타납니다.

원인

새 호스트가 확장된 클러스터에 가입하면 vSAN은 클러스터의 모든 호스트에서 구성을 업데이트해야 합니다. RVC 도구를 사용하여 호스트를 추가하는 경우 업데이트가 발생하지 않습니다. 새 호스트는 클러스터에 가입할 수 있지만 해당 구성은 완료되지 않은 상태입니다.

해결 방법

모든 호스트가 vCenter Server에 연결되었는지 확인하고, [구성 상태] 메시지에 제공된 링크를 클릭하여 새 호스트의 구성을 업데이트합니다.

확장된 클러스터에서 감시 호스트를 추가하거나 제거할 수 없음

확장된 클러스터에서 감시 호스트를 추가하거나 제거하기 전에 모든 현재 호스트가 연결되어 있어야 합니다. 현재 호스트의 연결이 끊어진 경우에는 감시 호스트를 추가하거나 제거할 수 없습니다.

문제점

일부 호스트의 연결이 끊어진 확장된 클러스터에서 감시 호스트를 추가하거나 제거하는 경우 다음과 같은 오류 상태가 표시되며 작업이 실패합니다. 현재 상태에서 허용되지 않는 작업입니다. 클러스터의 일부 호스트가 Virtual Center에 연결되지 않았습니다.

원인

감시 호스트가 확장된 클러스터에 가입하거나 확장된 클러스터에서 탈퇴하면 vSAN은 클러스터의 모든 호스트에서 구성을 업데이트해야 합니다. vCenter Server에서 하나 이상의 호스트의 연결이 끊어진 경우 감시 호스트를 추가하거나 제거할 수 없습니다.

해결 방법

모든 호스트가 vCenter Server에 연결되어 있는지 확인하고 작업을 재시도합니다. 연결이 끊어진 호스트를 다시 가입할 수 없는 경우 클러스터에서 연결이 끊어진 호스트를 제거한 다음 감시 호스트를 추가하거나 제거할 수 있습니다.

디스크 그룹이 잠금 상태가 됨

암호화된 vSAN 클러스터에서 호스트와 KMS 사이의 통신이 끊어지면 호스트 재부팅 시 디스크 그룹이 잠금 상태가 될 수 있습니다.

문제점

호스트가 재부팅된 후 KMS로부터 KEK를 가져올 수 없으면 vSAN이 호스트의 디스크 그룹을 잠급니다. 이 경우 디스크는 마운트되지 않은 것처럼 동작합니다. 디스크의 개체도 액세스할 수 없는 상태가 됩니다.

vSphere Web Client의 [디스크 관리] 페이지에서 디스크 그룹의 상태를 볼 수 있습니다. 디스크가 잠금 상태임을 알리는 암호화 상태 점점 주의가 표시됩니다.

원인

암호화된 vSAN 클러스터의 호스트는 KEK를 디스크에 저장하지 않습니다. 호스트가 재부팅된 후 KMS로부터 KEK를 가져올 수 없으면 vSAN이 해당 호스트의 디스크 그룹을 잠급니다.

해결 방법

잠금 상태를 종료하려면 KMS와의 통신을 복원하고 신뢰 관계를 재설정해야 합니다.

기존 하드웨어 구성 요소 교체

특정 조건에서는 vSAN 클러스터의 하드웨어 구성 요소, 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러를 교체해야 합니다.

vSAN에서 장애가 발생하거나 클러스터를 업그레이드해야 하는 경우 하드웨어 디바이스를 교체해야 합니다.

호스트에서 플래시 캐시 디바이스 교체

플래시 캐시 디바이스에서 실패를 감지한 경우 또는 플래시 캐시 디바이스를 업그레이드해야 할 때 해당 디바이스를 교체해야 합니다. 호스트에서 플래시 디바이스를 물리적으로 분리하기 전에, vSAN에서 이 디바이스를 수동으로 제거해야 합니다.



주의 먼저 플래시 캐시 디바이스를 vSAN에서 제거하지 않고 서비스 해제한다면, vSAN은 예상보다 더 적은 양의 캐시를 사용하게 됩니다. 그 결과 클러스터 성능이 저하됩니다.

플래시 캐시 디바이스를 교체할 때, 디스크 그룹에 있는 가상 시스템에 액세스할 수 없게 되며 그룹에 있는 구성 요소는 저하된 상태로 표시됩니다. [“vSAN 클러스터에서 플래시 캐시 디바이스에 액세스할 수 없음.”](#) (155 페이지)를 참조하십시오.

필수 조건

- 호스트의 스토리지 컨트롤러가 패스스루 모드로 구성되었으며 핫 플러그 기능을 지원하는지 확인합니다.
 - 스토리지 컨트롤러가 RAID 0 모드로 구성된 경우 디바이스 추가 및 제거에 대한 자세한 내용은 벤더 설명서를 참조하십시오.
- 플래시 캐시 디바이스를 업그레이드할 경우 다음 요구 사항을 확인하십시오.
 - 플래시 캐시 디바이스를 업그레이드할 경우 클러스터에 플래시 디바이스와 연결된 디스크 그룹에서 데이터를 마이그레이션할 수 있는 공간이 충분히 있는지 확인해야 합니다.
 - 호스트를 유지 보수 모드에 설정합니다. [“vSAN 클러스터의 멤버를 유지 보수 모드로 전환.”](#) (112 페이지)를 참조하십시오.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 구성 탭의 vSAN 아래에서 **디스크 관리**를 클릭합니다.
- 3 교체할 디바이스가 포함된 디스크 그룹을 선택합니다.
- 4 플래시 캐시 디바이스를 선택하고 **디스크 그룹에서 선택된 디스크 제거**를 클릭합니다.

vSAN 클러스터에서 플래시 캐시 디바이스를 제거한 후에, 클러스터 세부 정보는 현재 클러스터 용량과 구성 설정을 반영합니다. vSAN은 디스크 그룹 멤버십을 삭제하고 파티션을 삭제하고 모든 디바이스에서 오래된 데이터를 제거합니다.

후속 작업

- 1 호스트에 새 디바이스를 추가합니다.
 - 호스트가 자동으로 디바이스를 감지합니다.
- 2 호스트가 디바이스를 감지할 수 없으면 디바이스 다시 검색을 수행합니다.

용량 디바이스 교체

장애를 감지하거나 업그레이드하는 경우 플래시 용량 디바이스 또는 자기 디스크를 교체해야 합니다. 호스트에서 디바이스를 물리적으로 제거하기 전에 vSAN에서 디바이스를 수동으로 삭제해야 합니다.

vSAN 클러스터에서 제거하지 않고 용량 디바이스를 분리하는 경우 디스크 그룹의 가상 시스템에 액세스할 수 없게 되고 그룹의 구성 요소가 없음으로 표시됩니다.

용량 디바이스에 장애가 발생하는 경우 가상 시스템에 액세스할 수 없게 되고 그룹의 구성 요소가 성능 저하됨으로 표시됩니다. [“vSAN 클러스터에서 용량 디바이스에 액세스할 수 없음.”](#) (155 페이지)를 참조하십시오.

필수 조건

- 호스트의 스토리지 컨트롤러가 패스스루 모드로 구성되었으며 핫 플러그 기능을 지원하는지 확인합니다.
스토리지 컨트롤러가 RAID 0 모드로 구성된 경우 디바이스 추가 및 제거에 대한 자세한 내용은 벤더 설명서를 참조하십시오.
- 용량 디바이스를 업그레이드하는 경우 다음과 같은 요구 사항을 확인합니다.
 - 클러스터에 용량 디바이스의 데이터를 마이그레이션하기에 충분한 공간이 포함되어 있는지 확인합니다.
 - 호스트를 유지 보수 모드에 설정합니다. “vSAN 클러스터의 멤버를 유지 보수 모드로 전환,” (112 페이지)를 참조하십시오.

프로시저

- 1 vSphere Web Client에서 vSAN 클러스터로 이동합니다.
- 2 구성 탭의 vSAN 아래에서 **디스크 관리**를 클릭합니다.
- 3 교체할 디바이스가 포함된 디스크 그룹을 선택합니다.
- 4 플래시 용량 디바이스 또는 자기 디스크를 선택하고 **디스크 그룹에서 선택한 디스크 제거**를 클릭합니다.

후속 작업

- 1 호스트에 새 디바이스를 추가합니다.
호스트가 자동으로 디바이스를 감지합니다.
- 2 호스트가 디바이스를 감지할 수 없으면 디바이스 다시 검색을 수행합니다.

ESXCLI 명령을 사용하여 호스트에서 디바이스 제거

장애가 발생한 스토리지 디바이스를 발견했거나 디바이스를 업그레이드하는 경우 ESXCLI 명령을 사용하여 해당 디바이스를 수동으로 호스트에서 제거할 수 있습니다.

플래시 캐시 디바이스를 제거하면 vSAN은 플래시 디바이스와 연결된 디스크 그룹과 해당 멤버 디바이스를 모두 삭제합니다.

필수 조건

호스트의 스토리지 컨트롤러가 패스스루 모드로 구성되었으며 핫 플러그 기능을 지원하는지 확인합니다.
스토리지 컨트롤러가 RAID 0 모드로 구성된 경우 디바이스 추가 및 제거에 대한 자세한 내용은 벤더 설명서를 참조하십시오.

프로시저

- 1 ESXi 호스트에 대한 SSH 연결을 엽니다.
- 2 장애가 발생한 디바이스의 디바이스 ID를 확인하려면 이 명령을 실행하고 출력에서 디바이스 ID를 확인합니다.

```
esxcli vsan storage list
```

- 3 vSAN에서 디바이스를 제거하려면 이 명령을 실행합니다.

```
esxcli vsan storage remove -d device_id
```

후속 작업

- 1 호스트에 새 디바이스를 추가합니다.
호스트가 자동으로 디바이스를 감지합니다.
- 2 호스트가 디바이스를 감지할 수 없으면 디바이스 다시 검색을 수행합니다.

vSAN 클러스터 종료

필요한 경우 전체 vSAN 클러스터를 종료할 수 있습니다.

vSAN 클러스터를 종료하려는 경우 수동으로 클러스터에서 vSAN을 사용하지 않도록 설정하지 않아도 됩니다.

프로시저

- 1 vSAN 클러스터에서 실행 중인 모든 VM(가상 시스템)의 전원을 끕니다.
- 2 ESXi 호스트를 유지 보수 모드로 전환합니다.
 - a 호스트를 마우스 오른쪽 버튼으로 클릭하고 **유지 보수 모드 시작**을 선택합니다.
 - b **데이터 마이그레이션 없음** 제거 모드를 선택하고 **확인**을 클릭합니다.
- 3 유지 보수 모드 확인 마법사에서 **전원이 꺼지고 일시 중단된 가상 시스템을 클러스터의 다른 호스트로 이동** 확인란의 선택을 취소합니다.
 이 확인란의 선택을 취소하는 경우 vSAN은 VM을 다른 호스트로 마이그레이션하지 않습니다. 전체 클러스터를 종료하고 모든 호스트를 유지 보수 모드로 전환하려는 경우 VM 스토리지 개체를 클러스터의 다른 호스트나 디바이스로 이동하거나 마이그레이션하지 않아도 됩니다.
- 4 유지 보수 모드로 전환된 후 호스트의 전원을 끕니다.
- 5 ESXi 호스트의 전원을 켭니다.
 - a ESXi가 설치된 물리적 시스템에서 전원 버튼을 눌러 전원 켜기 시퀀스를 시작합니다.
ESXi 호스트가 시작되고 해당 VM을 찾은 후 정상적으로 작동합니다.
호스트의 전원을 켜 후 vSAN 클러스터가 자동으로 재생성됩니다.

ESXi 호스트로 이동하고 **요약**을 클릭하는 경우 클러스터의 네트워크 상태가 잘못된 구성이 감지됨으로 표시될 수 있습니다.

네트워크 구성을 변경하지 않았으며 클러스터를 종료하기 전에 vSAN 클러스터가 예상대로 작동한 경우에는 이 상태 메시지를 무시할 수 있습니다. 이 메시지는 3개 이상의 호스트가 클러스터에 가입된 후 사라집니다.
- 6 호스트의 유지 보수 모드 설정을 해제합니다.
- 7 VM을 다시 시작합니다.

색인

C

crypto-util **84**

E

ESXCLI를 사용하여 용량 디바이스로 사용되는 플래시 디바이스의 태그 해제 **38**

esxcli를 사용하여 플래시 디바이스를 용량으로 표시 **37**

ESXi 호스트 업그레이드 **89**

H

Hytrust **79**

I

iSCSI 대상 **118**

iSCSI 대상 모니터링 **120**

iSCSI 대상 서비스 **117**

iSCSI 대상 서비스를 사용하도록 설정 **117**

iSCSI 이니시에이터 그룹 **119**

K

KMIP 서버

루트 CA **78**

vCenter Server에 추가 **80**

인증서 **77**

클러스터를 기본으로 설정 **80**

KMS **76**

KMS 서버, 새 인증서 서명 요청 옵션 **79**

L

LUN 정의 **118**

R

RAID 5 또는 RAID 6 설계 고려 사항 **74**

RAID 5/6 이레이저 코딩 **73**

RVC를 사용하여 확장된 클러스터에 새 호스트를 추가할 때의 구성 오류 **160**

V

vCenter Server, KMIP 서버 추가 **80**

vCenter Server Appliance **53**

vCenter Server 업그레이드 **89**

vDS **55**

VM 성능 모니터링 **141**

vmknix **55**

VMware 소프트웨어 스택 **15**

vSAN

및 vSphere HA **52**

부팅 디바이스 **32**

3호스트 클러스터 **28**

CPU 설계 **27**

vCenter Server 및 ESXi의 버전 **40**

VM 액세스 지원 **153**

VMware 호환성 가이드 **35, 158**

vSAN 네트워크 구성 **41**

vSAN 사용 전 **35**

가상 시스템 규정 준수 **159**

가상 시스템 생성 실패 **159**

가상 시스템 액세스 지원 **159**

개체 규정 준수 **152, 153**

개체 상태 **152, 153**

개체 액세스 지원 **153**

구성 요소 상태 **152**

구성 요소 장애 **151**

균형 및 불균형 구성 **28**

네트워크 **19**

네트워크 장애 **156**

네트워킹 **31**

네트워킹 설계 **29**

데이터스토어 **51**

디바이스 또는 디스크 그룹 제거 **102**

디바이스 준비 **36**

디바이스 할당 **99, 100**

디바이스의 호환성 확인 **35, 158**

디스크 그룹 생성 **99**

라이선스 요구 사항 **19, 42**

라이선싱 **50**

랙 인클로저 장애 **32**

메모리 설계 **27**

메모리 제공 **39**

모니터링 **131**

문제 해결 **147, 158**

및 esxcli 명령 **147**

설정 **45**

성능 **158**

소프트웨어 요구 사항 **18**

수동으로 디바이스 할당 **100**

스토리지 디바이스 **21**

스토리지 디바이스 바꾸기 **163**

스토리지 디바이스 준비 **36**

- 스토리지 정책 **123**
- 스토리지 제공자 **126**
- 스토리지 컨트롤러 **27**
- 스토리지 컨트롤러 장애 **157**
- 실패 **151**
- 여러 디스크 그룹 **27**
- 오류 메시지 **151**
- 요구 사항 **17**
- 용량 **22**
- 용량 디바이스 교체 **162**
- 용량 실패 **155, 163**
- 용량 업그레이드 **163**
- 용량 준비 **36**
- 용량을 위한 플래시 표시 **39**
- 장애 도메인 설계 **32**
- 장애 처리 **151**
- 정보 **9**
- 정의됨 **9**
- 캐시 장애 **155**
- 캐시 크기 조정 **24**
- 클러스터 리소스 준비 **35**
- 클러스터 사용 안 함 **49**
- 클러스터 설계 **28**
- 클러스터 요구 사항 **18**
- 클러스터 확장 **107**
- 플래시 디바이스를 캐시로 표시 **104**
- 플래시 설계 **24**
- 플래시 용량 **25**
- 플래시 캐시 실패 **162, 163**
- 플래시 캐시 업그레이드 **162, 163**
- 하드웨어 요구 사항 **17**
- 호스트 네트워킹 **27**
- 호스트 설계 **27**
- 호스트 장애 **156**
- 호스트 준비 **40**
- 호스트의 구성 실패 **150**
- 확장 및 관리 **107**
- vSAN 파티션 제거 **106**
- vSAN Health Service 경보 **144**
- vSAN Health Service 구성 **136**
- vSAN 개체
 - vSAN 개체, 상태 **153**
 - 규정 준수 **152, 153**
 - 상태 **152**
 - 액세스 지원 **153**
 - 작동 상태 **153**
- vSAN 경보 **144, 145**
- vSAN 경보 표시 **145**
- vSAN 구성 **54**
- vSAN 구성 요소
 - 상태 **152**
 - 장애 **152**
 - 장애 상태 **151**
- vSAN 기본 스토리지 정책 **126**
- vSAN 네트워크
 - IP 버전 지원 **19**
 - 대역폭 **19, 29**
 - 멀티캐스트 **19**
 - 멀티캐스트 고려 사항 **29**
 - 요구 사항 **19**
 - 장애 **156**
 - 정적 라우팅 **31**
 - 페일오버 및 로드 밸런싱 구성 **29**
 - 호스트 연결 **19**
- vSAN 데이터스토어, 디바이스 모니터링 **135**
- vSAN 데이터스토어에 기본 스토리지 정책 할당 **128**
- vSAN 데이터스토어에서 디바이스 모니터링 **135**
- vSAN 디스크 그룹, 디바이스 추가 **102**
- vSAN 디스크 그룹 사용 **99**
- vSAN 디스크 형식, 업그레이드 **93**
- vSAN 디스크 형식 업그레이드 **94**
- vSAN 디스크 형식 업그레이드 요구 사항 **91**
- vSAN 디스크 형식 업그레이드 확인 **95**
- vSAN 모니터링 **131**
- vSAN 및 기존 스토리지, vSAN과 비교 **14**
- vSAN 상태 점검 **137**
- vSAN 성능 **158**
- vSAN 성능 모니터링 **138**
- vSAN 성능 서비스 설정 **138**
- vSAN 스토리지 디바이스
 - ESXCLI를 사용하여 바꾸기 **163**
 - 설계 고려 사항 **21**
- vSAN 스토리지 컨트롤러
 - 설계 고려 사항 **27**
 - 장애 **157**
- vSAN 시작 **9**
- vSAN 업그레이드 vSAN 클러스터 **87**
- vSAN 업그레이드 사전 요구 사항 및 권장 사항 **88**
- vSAN 요구 사항
 - 네트워크 **19**
 - 라이선스 **19**
 - 소프트웨어 **18**
 - 클러스터 **18**
 - 하드웨어 **17**
- vSAN 용량
 - 고려 사항 **26**
 - 디바이스 교체 **162**
 - 자기 디스크 **26**
 - 장애 **155**
 - 크기 조정 **22**

- 플래시 디바이스 **25**
 - 플래시 표시 **39**
 - vSAN 용량 디바이스 추가 **106**
 - vSAN 용량 디스크 **106**
 - vSAN 용량 모니터링 **132**
 - vSAN 이벤트에 대한 vCenter Server 경보 생성 **146**
 - vSAN 자기 디스크, 설계 고려 사항 **26**
 - vSAN 장애
 - 구성 요소 상태 **151**
 - 문제 해결 **151**
 - 용량 **155**
 - 캐시 **155**
 - vSAN 장애 도메인, 설계 고려 사항 **32**
 - vSAN 장애 도메인을 기본 장애 도메인으로 표시 **64**
 - vSAN 정책 **123**
 - vSAN 캐시
 - 고려 사항 **24**
 - 장애 **155**
 - 플래시 디바이스 교체 **162**
 - vSAN 클러스터
 - 생성 **46**
 - 설계 **21**
 - 설계 고려 사항 **28**
 - 영구적 로깅 **33**
 - 요구 사항 **18**
 - 용량을 위한 플래시 표시 **39**
 - 재조정 **143**
 - 전원 끄기 **121**
 - 크기 조정 **21**
 - vSAN 클러스터 구성 **47**
 - vSAN 클러스터 구축 정보 **14**
 - vSAN 클러스터 사용 안 함 **49**
 - vSAN 클러스터 생성 **43, 46**
 - vSAN 클러스터 업그레이드 확인 **95**
 - vSAN 클러스터 요구 사항에 대한 검사 목록 **44**
 - vSAN 클러스터 종료 **164**
 - vSAN 클러스터 편집 **48**
 - vSAN 클러스터에 호스트 추가 **108**
 - vSAN 클러스터에서 가상 디스크의 상태 모니터링 **133**
 - vSAN 클러스터에서 장애 도메인 관리 **113**
 - vSAN 클러스터에서 장애 도메인 구성 **113**
 - vSAN 클러스터의 잘못된 네트워크 구성 상태 **158**
 - vSAN 클러스터의 재조정 작업 **142**
 - vSAN 클러스터의 클러스터 재조정 작업 **142**
 - vSAN 클러스터의 특성 **43**
 - vSAN 플래시
 - 고려 사항 **24, 25**
 - 용량을 위한 표시 **39**
 - vSAN 플래시 전용
 - 고려 사항 **25**
 - 용량 **25**
 - vSAN 하드웨어, 요구 사항 **17**
 - vSAN 호스트
 - 네트워킹 **27**
 - 여러 디스크 그룹 **27**
 - 장애 **156**
 - vSAN 호스트 모니터링 **131**
 - vSAN 호스트를 기존 장애 도메인으로 이동 **115**
 - vSAN 확장된 클러스터 **63**
 - vSAN, 네트워킹 **45**
 - vSAN, 사용 **49**
 - vSAN, 클러스터 설계 **21**
 - vsan.ondisk_upgrade 옵션 사용 **96**
 - vSAN에서 디바이스 또는 디스크 그룹 제거 **102**
 - vSAN을 업그레이드하기 전 **88**
 - vSAN의 제한 사항 **15**
 - vSAN의 특성, 특성 **10**
 - vSphere Update Manager **96**
- ㄱ**
- 가상 시스템
 - vSAN에서 생성 실패 **159**
 - vSAN의 규정 준수 **159**
 - vSAN의 액세스 불가능 **159**
 - 가상 시스템 개체, 비준수 **150**
 - 감시 장치
 - vSAN 네트워크 구성 **65**
 - 및 관리 네트워크 **65**
 - 감시 트래픽 **65**
 - 감시 호스트 **59**
 - 감시 호스트 교체 **64**
 - 개별 디바이스 사용 개별 디바이스 사용 **101**
 - 경보 생성을 위한 VMkernel 관찰 **145**
 - 곧 비활성 상태가 되는 디스크 **154**
 - 구성 지원 **54**
 - 기본 사이트 **59**
 - 기본 장애 도메인 **64**
 - 기존 하드웨어 구성 요소 교체 **161**
- ㄴ**
- 다른 VMware 소프트웨어와 통합 **15**
 - 다시 동기화 작업 **133**
 - 다시 동기화 작업 모니터링 **134**
 - 다시 동기화 조절 **134**
 - 대상 사용자 **7**
 - 대칭 키 **79**
 - 데이터스토어, vSAN **51**
 - 디바이스를 로컬로 표시 **105**
 - 디바이스를 원격으로 표시 **105**

디스크 그룹 잠금 상태 **161**
 디스크 그룹에 디바이스 추가 **102**
 디스크 형식 업그레이드 **95**
 디스크를 자기 디스크로 표시 **104**

ㄴ

로케이터 LED 사용 또는 사용 안 함 **103**
 로케이터 LED 정보 **103**
 루트 CA, KMIP 서버 **78**

ㄷ

메트로 클러스터 **59**

ㄹ

상태 서비스 경보 보기 **145**
 상태 점검 **135**
 새 온디스크 형식으로 업그레이드 **93**
 새 인증서 서명 요청 옵션, KMS 서버 **79**
 선택한 장애 도메인으로 호스트 이동 **115**
 성능 진단 **141**
 수동 재조정 **143**
 스토리지 정책, vSAN에 대해 정의 **128**
 스토리지 컨트롤러, vSAN 장애 **157**
 스토리지 효율성 **69**
 시간 범위 저장 **139**
 신뢰할 수 있는 연결 **78**

ㅇ

암호화 **75**
 암호화 사용 **81, 82**
 암호화 설계 **76**
 암호화를 위한 vm-support **83**
 압축
 기존 클러스터에서 사용하도록 설정 **71**
 사용 안 함 **72**
 설정 **71**
 업그레이드 RVC 명령 옵션 사용 **96**
 영구적 로깅 **33**
 용량 디바이스 추가 **106**
 용어집 **7**
 유지 보수 모드, vSAN **112**
 유지 보수 모드 사용 **111**
 이니시에이터 그룹에 iSCSI 대상 할당 **119**

ㅈ

자동 재조정 **142**
 장애 도메인 외부로 호스트 이동 **116**
 장애 도메인 이름 변경 **116**
 장애 도메인 제거 **116**
 장애 도메인에 vSAN 호스트 할당 **114**
 제거 모드 **112**
 주요 용어 vSAN 용어 및 정의 **11**

중복 제거
 기존 클러스터에서 사용하도록 설정 **71**
 사용 안 함 **72**
 설정 **71**
 중복 제거 설계 고려 사항 **71**
 중복 제거와 압축
 VM 이중화 감소 **72**
 디스크 제거 **73**
 클러스터에 디스크 추가 **73**

ㅊ

컨트롤러 관리 도구 **56**
 컨트롤러 준비 **40**
 컨트롤러 펌웨어 업데이트 **57**
 코어 덤프 및 vSAN 암호화 **83**
 클러스터 **14**
 클러스터 성능 모니터링 **139**
 클러스터 용량 및 성능 확장 **108**
 클러스터를 기본으로 설정 **80**
 키 서버, 인증서 교환 **77**
 키 재생성 암호화 **81**

ㅌ

플래시 전용 디스크 그룹, vSAN 디스크 그룹
 및 디바이스 **99**
 플래시 전용 클러스터, 마이그레이션 **120**

ㅎ

호스트 성능 모니터링 **140**
 호스트 클라이언트 **137**
 호스트 프로파일을 사용하여 vSAN 클러스터에
 호스트 추가 **109**
 호환성 가이드 **158**
 확장된 클러스터 **59**
 확장된 클러스터 구성 **63**
 확장된 클러스터 네트워크 설계 **62**
 확장된 클러스터 모범 사례 **62**
 확장된 클러스터 변환 **67**
 확장된 클러스터 설계 고려 사항 **61**
 확장된 클러스터 장애 **157**
 확장된 클러스터에 새 호스트를 추가할 때의 구
 성 오류 **160**
 확장된 클러스터에서 감시 호스트를 추가하거나
 제거할 수 없음 **161**