VMware vSAN 관리

업데이트 3

VMware vSphere 7.0
VMware vSAN 7.0

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

https://docs.vmware.com/kr/

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화:+82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

목차

VMware vSAN 관리 정보

"VMware vSAN 관리" 에서는 VMware vSphere® 환경에서 vSAN 클러스터를 구성하고 관리하는 방법을 설명합니다. 또한 "VMware vSAN 관리" 에서는 vSAN 클러스터에서 스토리지 용량 디바이스 역할을 하는 로컬의 물리적 스토리지 리소스를 관리하는 방법과 vSAN 데이터스토어에 배포된 가상 시스템의 스토리지 정책을 정의하는 방법을 설명합니다.

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

대상 사용자

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

vSAN에 대한 자세한 내용 및 vSAN 클러스터를 생성하는 방법은 "vSAN 계획 및 배포 가이드" 를 참조하십시오.

vSAN 클러스터를 모니터링하고 문제를 해결하는 방법에 대한 자세한 내용은 "vSAN 모니터링 및 문제 해결 가이드" 참조하십시오.

업데이트된 정보

1

이 문서는 제품의 각 릴리스에 따라 또는 필요할 때 업데이트됩니다.

이 표에서는 "VMware vSAN 관리" 의 업데이트 기록을 보여 줍니다.

개정	설명
2023년 6월 12일	■ 감시 호스트가 데이터 호스트보다 먼저 업그레이드됨을 나타내도록 확장된 클러스터 및 2 호스트 클러스터를 업그레이드하기 위한 지침이 업데이트되었습니다. vSAN을 업그레이드하기 전. ■ 추가적인 부분적 업데이트.
2021년 11월 8일	■ 파일 서비스 구성에서 vSAN 파일 서비스를 구성하기 위한 사전 요구 사항이 업데이트되었습니다. ■ vSAN 디스크 형식 정보에서 디스크 업그레이드에 대한 정보가 추가되었습니다. ■ vSphere with Tanzu 환경인 경우 "VMware Cloud Foundation 운영 가이드" 를 참조하여 구성 요소를 종료하거나 시작하십시오. vSAN 클러스터 수동 종료 및 다시 시작을 업데이트했습니다.
2021년 4월 16일	■ 제한 사항 및 고려 사항에서 vSAN 파일 서비스 제한 사항 및 고려 사항이 업데이트되었습니다. ■ 파일 서비스 구성에서 AD 지원 제한 사항이 업데이트되었습니다. ■ **My VMware** 포털의 브랜드가 **VMware Customer Connect**로 변경되었습니다. 이 이름 변경을 반영하기 위해 vSphere Lifecycle Manager에 대한 vSAN 빌드 권장 사항 항목이 업데이트되었습니다.
2020년 11월 12일	■ HCI 메시와 원격 데이터스토어 공유 에서 HCI 메시 설계 고려 사항이 업데이트되었습니다. ■ ESXi 호스트 업그레이드에서 ESXi 업그레이드 정보가 업데이트되었습니다.
2020년 10월 06일	최초 릴리스.

vSAN 소개

2

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.

vSAN 클러스터 구성 및 관리

3

vSphere Client, esxcli 명령 및 기타 도구를 사용하여 vSAN 클러스터를 구성하고 관리할 수 있습니다.

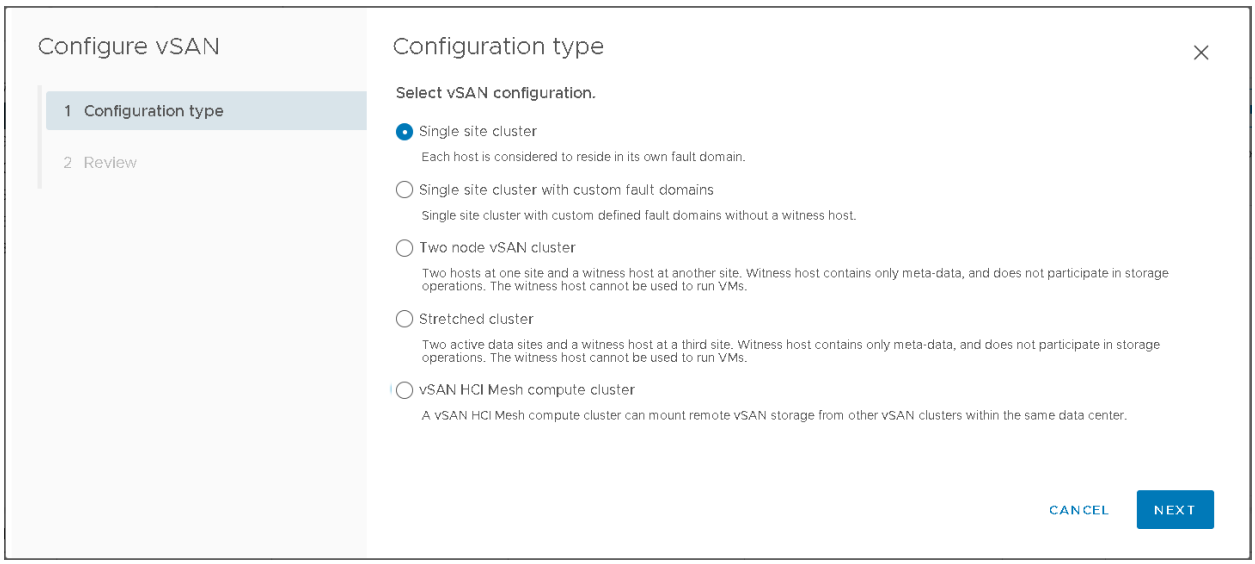
본 장은 다음 항목을 포함합니다.

vSphere Client를 사용하여 vSAN에 클러스터 구성

HTML5 기반 vSphere Client를 사용하여 vSAN 클러스터를 구성할 수 있습니다.

참고 Quickstart를 사용하면 vSAN 클러스터를 신속하게 생성하고 구성할 수 있습니다. 자세한 내용은 "vSAN 계획 및 배포" 의 "Quickstart를 사용하여 vSAN 클러스터 구성 및 확장"을 참조하십시오.

참고 vSAN HCI 메시 계산 클러스터에는 제한된 구성 옵션이 있습니다.



사전 요구 사항

환경이 모든 요구 사항을 충족하는지 확인합니다. "vSAN 계획 및 배포" 에서 "vSAN 사용을 위한 요구 사항"을 참조하십시오.

vSAN을 사용하도록 설정하고 구성하기 전에 클러스터를 생성하고 클러스터에 호스트를 추가합니다.

절차

1 기존 호스트 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **서비스**를 선택합니다.

4 **vSAN 구성**을 클릭하여 [vSAN 구성] 마법사를 엽니다.

5 구성할 클러스터의 vSAN 유형을 선택하고 **다음**을 클릭합니다.

- 단일 사이트 클러스터. 자세한 내용은 "vSAN 계획 및 배포" 의 "vSAN 배포 옵션"을 참조하십시오.
- 사용자 지정 장애 도메인이 있는 단일 사이트 클러스터.
- 2개 노드 vSAN 클러스터.
- 확장된 클러스터.
- vSAN HCI 메시 계산 클러스터. 자세한 내용은 "VMware vSAN 관리" 에서 "HCI 메시와 원격 데이터스토어 공유"를 참조하십시오.

6 사용할 vSAN 서비스를 구성하고 **다음**을 클릭합니다.

중복 제거 및 압축, 미사용 데이터 암호화 및 전송 중 데이터 암호화를 포함하는 데이터 관리 기능을 구성합니다. 자세한 내용은 vSAN 설정 편집을 참조하십시오.

7 vSAN 클러스터에 디스크를 할당하고 **다음**을 클릭합니다.

각 호스트에는 캐시 계층에 하나 이상의 플래시 디바이스와 용량 계층에 하나 이상의 디바이스가 있어야 합니다. 자세한 내용은 "VMware vSAN 관리" 의 "디스크 그룹 및 디바이스 관리"를 참조하십시오.

8 구성을 검토하고 **마침**을 클릭합니다.

결과

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

다음에 수행할 작업

디스크를 할당하거나 디스크 그룹을 생성합니다. "VMware vSAN 관리" 의 "디스크 그룹 및 디바이스 관리"를 참조하십시오.

vSAN 데이터스토어가 생성되었는지 확인합니다.

vSAN 스토리지 제공자가 등록되었는지 확인합니다.

기존 클러스터에서 vSAN 사용

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

사전 요구 사항

환경이 모든 요구 사항을 충족하는지 확인합니다. "vSAN 계획 및 배포" 에서 "vSAN 사용을 위한 요구 사항"을 참조하십시오.

참고 vSAN HCI 메시 계산 클러스터에는 제한된 구성 옵션이 있습니다.

절차

1 기존 호스트 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **서비스**를 선택합니다.

4 **vSAN 구성**을 클릭합니다.

5 구성할 클러스터의 vSAN 유형을 선택하고 **다음**을 클릭합니다.

- 단일 사이트 클러스터.
- 사용자 지정 장애 도메인이 있는 단일 사이트 클러스터.
- 2개 노드 vSAN 클러스터.
- 확장된 클러스터.

- vSAN HCI 메시 계산 클러스터. 자세한 내용은 "VMware vSAN 관리" 에서 "HCI 메시와 원격 데이터스토어 공유"를 참조하십시오.

6 사용할 vSAN 서비스를 구성하고 **다음**을 클릭합니다.

- vSAN 성능 서비스를 구성합니다. 자세한 내용은 "vSAN 모니터링 및 문제 해결" 의 "vSAN 성능 모니터링"을 참조하십시오.
- 파일 서비스를 사용하도록 설정합니다. 자세한 내용은 "VMware vSAN 관리" 의 "vSAN 파일 서비스"를 참조하십시오.
- vSAN 네트워크 옵션을 구성합니다. 자세한 내용은 "vSAN 계획 및 배포" 의 "vSAN 네트워크 디자인"을 참조하십시오.
- vSAN 기록 상태 서비스를 구성합니다.
- iSCSI 대상 서비스를 구성합니다. 자세한 내용은 "VMware vSAN 관리" 의 "vSAN iSCSI 대상 서비스 사용"을 참조하십시오.
- 중복 제거 및 압축, 미사용 데이터 암호화 및 전송 중 데이터 암호화를 포함하는 데이터 관리 옵션을 구성합니다.
- 용량 예약 및 경고를 구성합니다. 자세한 내용은 "vSAN 모니터링 및 문제 해결" 의 "예약된 용량 정보"를 참조하십시오.
- 고급 옵션을 구성합니다.
  - 개체 복구 타이머
  - 확장된 클러스터에 대한 사이트 읽기 위치
  - 씬 스왑 프로비저닝
  - 최대 64개 호스트에 대한 대규모 클러스터 지원
  - 자동 재조정

7 vSAN 클러스터에 디스크를 할당하고 **다음**을 클릭합니다.

각 호스트에는 캐시 계층에 하나 이상의 플래시 디바이스와 용량 계층에 하나 이상의 디바이스가 있어야 합니다. 자세한 내용은 "VMware vSAN 관리" 의 "디스크 그룹 및 디바이스 관리"를 참조하십시오.

8 구성을 검토하고 **완료**를 클릭합니다.

vSAN 끄기

호스트 클러스터에 대해 vSAN을 해제할 수 있습니다.

vSAN 클러스터를 끄면 vSAN 데이터스토어에 있는 모든 가상 시스템 및 데이터 서비스에 액세스할 수 없게 됩니다. vSAN Direct를 통해 vSAN 클러스터에서 스토리지를 사용하면 상태 점검, 공간 보고 및 성능 모니터링과 같은 vSAN Direct 모니터링 서비스도 사용할 수 없습니다. vSAN이 꺼진 동안 가상 시스템을 사용하려면 vSAN 데이터스토어에서 다른 데이터스토어로 가상 시스템을 마이그레이션한 후에 vSAN 클러스터를 꺼야 합니다.

사전 요구 사항

호스트가 유지 보수 모드에 있는지 확인합니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **서비스**를 선택합니다.

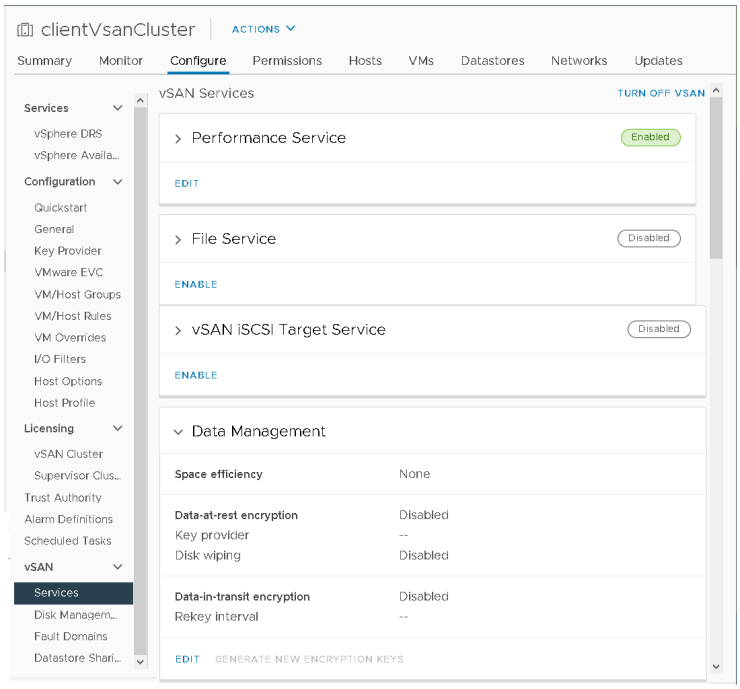
4 **vSAN 해제**를 클릭합니다.

5 [vSAN 해제] 대화상자에서 선택 항목을 확인합니다.

vSAN 설정 편집

vSAN 클러스터의 설정을 편집하여 데이터 관리 기능을 구성하고 클러스터가 제공하는 서비스를 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.



절차

1 vSAN 호스트 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

a vSAN에서 **서비스**를 선택합니다.

b 구성하려는 서비스에 대한 **편집** 또는 **사용** 버튼을 클릭합니다.

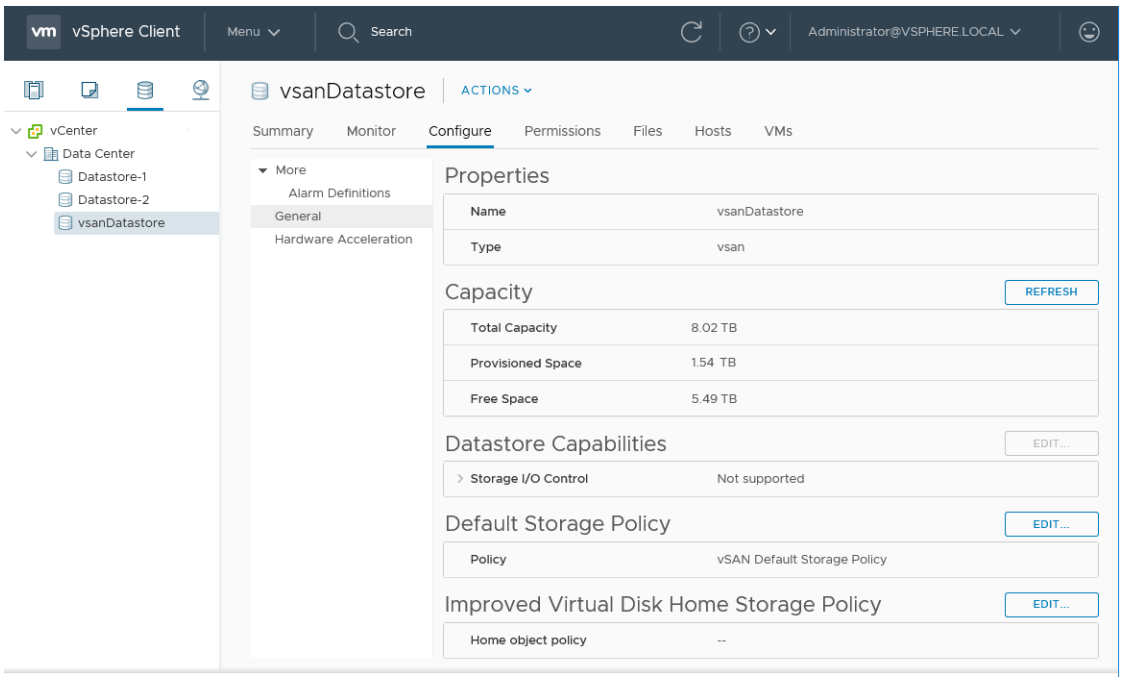
- vSAN 성능 서비스를 구성합니다. 자세한 내용은 "vSAN 모니터링 및 문제 해결" 에서 vSAN 성능 모니터링을 참조하십시오.
- 파일 서비스를 사용하도록 설정합니다. 자세한 내용은 "VMware vSAN 관리" 의 "vSAN 파일 서비스"를 참조하십시오.
- vSAN 네트워크 옵션을 구성합니다. 자세한 내용은 "vSAN 계획 및 배포" 의 "vSAN 네트워크 구성"을 참조하십시오.
- vSAN 기록 상태 서비스를 구성합니다.
- iSCSI 대상 서비스를 구성합니다. 자세한 내용은 "VMware vSAN 관리" 의 "vSAN iSCSI 대상 서비스 사용"을 참조하십시오.
- 중복 제거 및 압축, 미사용 데이터 암호화 및 전송 중 데이터 암호화를 포함하는 데이터 관리 옵션을 구성합니다.
- 용량 예약 및 경고를 구성합니다. 자세한 내용은 "vSAN 모니터링 및 문제 해결" 의 "예약된 용량 정보"를 참조하십시오.
- 고급 옵션을 구성합니다.
  - 개체 복구 타이머
  - 확장된 클러스터에 대한 사이트 읽기 위치
  - 씬 스왑 프로비저닝
  - 최대 64개 호스트에 대한 대규모 클러스터 지원
  - 자동 재조정

c 해당 요구 사항에 맞게 설정을 수정합니다.

3 **적용**을 클릭하여 선택을 확인합니다.

vSAN 데이터스토어 보기

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



사전 요구 사항

vSAN을 활성화하고 디스크 그룹을 구성합니다.

절차

1 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 x 2TB x 8 = 112TB입니다. 플래시 전용 구성을 사용할 경우 플래시 디바이스가 용량에 사용됩니다. 하이브리드 구성의 경우 자화 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.

다음에 수행할 작업

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

vSAN 데이터스토어에 파일 또는 폴더 업로드

vmdk 파일을 vSAN 데이터스토어에 업로드할 수 있습니다. vSAN 데이터스토어에 폴더를 업로드할 수도 있습니다. 데이터스토어에 대한 자세한 내용은 "vSphere 스토리지" 를 참조하십시오.

vSAN 데이터스토어에 vmdk 파일을 업로드할 때는 다음 사항을 고려해야 합니다.

- 스트림에 최적화된 vmdk 파일만 vSAN 데이터스토어에 업로드할 수 있습니다. VMware 스트림 최적화 파일 형식은 스트리밍을 위해 압축된 모놀리식 스파스 형식입니다. 스트림에 최적화된 형식이 아닌 vmdk 파일을 업로드하려면 업로드하기 전에 vmware-vdiskmanager 명령줄 유틸리티를 사용하여 스트림에 최적화된 형식으로 변환합니다. 자세한 내용은 "가상 디스크 관리자 사용자 가이드" 를 참조하십시오.
- vmdk 파일을 vSAN 데이터스토어에 업로드하면 vmdk 파일이 해당 데이터스토어의 기본 정책을 상속합니다. vmdk는 vmdk가 다운로드된 VM의 정책을 상속하지 않습니다. vSAN은 vsanDatastore 기본 정책 (RAID -1)을 적용하여 개체를 생성합니다. 데이터스토어의 기본 정책은 변경할 수 있습니다. vSAN 데이터스토어의 기본 스토리지 정책 변경 의 내용을 참조하십시오.
- vmdk 파일을 VM 홈 폴더에 업로드해야 합니다.

절차

1 vSAN 데이터스토어로 이동합니다.

2 **파일** 탭을 클릭합니다.

옵션	설명
파일 업로드	a 대상 폴더를 선택하고 **파일 업로드**를 클릭합니다. VMware 스트림 최적화 형식으로만 vmdk 파일을 업로드할 수 있다는 메시지가 표시됩니다. vmdk 파일을 다른 형식으로 업로드하려고 하면 내부 서버 오류 메시지가 표시됩니다. b **업로드**를 클릭합니다. c 로컬 컴퓨터에서 업로드할 항목을 찾고 **열기**를 클릭합니다.
폴더 업로드	a 대상 폴더를 선택하고 **폴더 업로드**를 클릭합니다. VMware 스트림 최적화 형식으로만 vmdk 파일을 업로드할 수 있다는 메시지가 표시됩니다. b **업로드**를 클릭합니다. c 로컬 컴퓨터에서 업로드할 항목을 찾고 **열기**를 클릭합니다.

vSAN 데이터스토어에서 파일 또는 폴더 다운로드

vSAN 데이터스토어에서 파일과 폴더를 다운로드할 수 있습니다. 데이터스토어에 대한 자세한 내용은 "vSphere 스토리지" 를 참조하십시오.

vmdk 파일은 파일 이름이 `<vmdkName>_stream.vmdk`인 스트림 최적화 파일로 다운로드됩니다. VMware 스트림 최적화 파일 형식은 스트리밍을 위해 압축된 모놀리식 스파스 형식입니다.

vmware-vdiskmanager 명령줄 유틸리티를 사용하여 VMware 스트림 최적화 vmdk 파일을 다른 vmdk 파일 형식으로 변환할 수 있습니다. 자세한 내용은 "가상 디스크 관리자 사용자 가이드" 를 참조하십시오.

절차

1 vSAN 데이터스토어로 이동합니다.

2 **파일** 탭을 클릭한 다음, **다운로드**를 클릭합니다.

vmdk 파일이 파일 확장명이 `.stream.vmdk`인 VMware 스트림 최적화 형식으로 vSAN 데이터스토어에서 다운로드되었다고 알려주는 메시지가 표시됩니다.

3 **다운로드**를 클릭합니다.

4 다운로드할 항목을 찾아서 **다운로드**를 클릭합니다.

vSAN 정책 사용

4

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.

본 장은 다음 항목을 포함합니다.

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 보급하는 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 **허용되는 장애**가 1로 설정되며, 개체당 하나의 디스크 스트라이프 및 씬 프로비저닝된 가상 디스크가 있습니다.

VM 스왑 개체와 VM 스냅샷 메모리 개체는 VM에 할당된 스토리지 정책을 준수하지 않습니다. 이러한 개체는 **허용되는 장애**가 1로 설정되어 구성됩니다. 이러한 개체의 가용성은 **허용되는 장애** 값이 다르게 지정된 정책이 할당된 개체의 가용성과 다를 수 있습니다.

표 4-1. 스토리지 정책 규칙

기능	설명
FTT(허용되는 장애)	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. 장애 도메인이 구성된 경우에는 용량을 제공하는 호스트가 있는 장애 도메인이 2n+1개 필요합니다. 장애 도메인에 속하지 않는 호스트는 자체 단일 호스트 장애 도메인으로 간주됩니다. 성능 또는 용량에 최적화된 데이터 복제 방법을 선택할 수 있습니다. RAID-1(미러링)은 개체 구성 요소를 배치하는 데 더 많은 디스크 공간을 사용하지만 더 나은 개체 액세스 성능을 제공합니다. RAID-5/6(이레이저 코딩)은 디스크 공간을 더 적게 사용하지만 성능이 저하됩니다. **참고** vSAN을 통해 가상 시스템 개체의 단일 미러 복사본을 보호하지 않으려는 경우 **데이터 이중화 없음**을 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. **데이터 이중화 없음**을 설정하면 데이터가 보호되지 않으며 vSAN 클러스터에서 디바이스 장애가 발생하면 데이터가 손실될 수 있습니다. **참고** 스토리지 정책을 생성할 때 **FTT** 값을 지정하지 않으면 vSAN이 VM 개체의 단일 미러 복사본을 생성합니다. 그러면 단일 장애를 허용할 수 있습니다. 하지만 여러 구성 요소 장애가 발생할 경우에는 데이터가 위험할 수 있습니다.
사이트 재해 허용	확장된 클러스터에서 이 규칙은 **FTT**가 정의된 장애 수에 도달하면 개체가 허용하는 추가 호스트 장애 수를 정의합니다. 없음 - 표준 클러스터가 기본값입니다. 확장된 클러스터의 경우 호스트 선호도를 위해 기본 사이트 또는 보조 사이트에 데이터를 보관하도록 선택할 수 있습니다. 호스트 미러링 - 2노드 클러스터는 FTT로 정의된 장애 수에 도달한 후 개체가 허용할 수 있는 추가 장애 수를 정의합니다. vSAN은 디스크 그룹 수준에서 개체 미러링을 수행합니다. 이 규칙을 사용하려면 각 데이터 호스트에 3개 이상의 디스크 그룹이 있어야 합니다. 사이트 미러링 - 확장된 클러스터는 FTT로 정의된 장애 수에 도달한 후 개체가 허용할 수 있는 추가 호스트 장애 수를 정의합니다.
개체당 디스크 스트라이프 수	가상 시스템 개체의 각 복제본이 스트라이핑되는 용량 디바이스의 최소 수입니다. 값이 1보다 크면 성능이 더 향상되겠지만 시스템 리소스도 더 많이 소모됩니다. 기본값은 1이고 최대값은 12입니다. 기본 스트라이핑 값을 변경하지 마십시오. 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.

표 4-1. 스토리지 정책 규칙 (계속)

기능	설명
Flash Read Cache 예약	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. 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. 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. 기본값은 0%이고, 최대값은 100%입니다. **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. 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.
강제 프로비저닝	이 옵션을 **예**로 설정하면 데이터스토어가 스토리지 정책에 지정된 **허용되는 장애**, **개체당 디스크 스트라이프 수** 및 **Flash Read Cache 예약** 정책을 충족하지 않더라도 개체가 프로비저닝됩니다. 이 매개 변수는 부트스트래핑 시나리오에 사용하거나 더 이상 표준 프로비저닝을 수행할 수 없는 운영 중단 시에 사용할 수 있습니다. 기본값인 **아니요**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. 다음 옵션을 사용할 수 있습니다. ■ 씬 프로비저닝(기본값) ■ 25% 예약 ■ 50% 예약 ■ 75% 예약 ■ 씩 프로비저닝

표 4-1. 스토리지 정책 규칙 (계속)

기능	설명
개체 체크섬 사용 안 함	이 옵션을 **아니요**로 설정하면 개체가 체크섬 정보를 계산하여 해당 데이터의 무결성을 보장합니다. 이 옵션을 **예**로 설정하면 개체가 체크섬 정보를 계산하지 않습니다. vSAN은 종단 간 체크섬을 사용하여 파일의 각 복사본이 소스 파일과 정확히 동일한지 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 **아니요**이며, 이는 체크섬이 사용되도록 설정되었다는 의미입니다.
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 "VMware vSAN 관리" 에서 "vSAN 클러스터 설계 및 크기 조정"을 참조하십시오.

vSAN에서 정책 변경을 관리하는 방법

vSAN 6.7 Update 3 이상에서는 클러스터 전체에서 사용되는 임시 공간의 양을 줄이기 위해 정책 변경 사항을 관리합니다. vSAN이 정책 변경에 대해 개체를 재구성하면 일시적인 용량이 생성됩니다.

정책을 수정하면 변경 사항이 수락되지만 즉시 적용되지는 않습니다. vSAN은 고정된 양의 일시적인 공간을 유지하기 위해 정책 변경 요청을 일괄 처리하고 비동기식으로 수행합니다.

5노드 클러스터에서 RAID5 정책을 RAID6으로 변경하는 것과 같은 용량과 관련이 없는 이유로 인한 정책 변경은 즉시 거부됩니다.

vSAN 용량 모니터에서 일시적인 용량 사용량을 볼 수 있습니다. 개체에 대한 정책 변경 상태를 확인하려면 vSAN Health Service를 사용하여 vSAN 개체 상태를 확인합니다.

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.

vSAN 6.7 이상 릴리스에서는 다음 URL을 사용하여 vCenter Server에서 관리하는 모든 vSAN 클러스터에 대해 하나의 vSAN 스토리지 제공자만 등록합니다.

```
https://<VC fqdn>:<VC https port>/vsanHealth/vsanvp/version.xml
```

스토리지 제공자가 등록되었는지 확인합니다.

절차

1 vCenter Server로 이동합니다.

2 **구성** 탭을 클릭하고 **스토리지 제공자**를 클릭합니다.

결과

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 취소하려면 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 기능이 포함되며 이는 일반적으로 vSAN 데이터스토어에 배포된 가상 시스템의 배치에 사용됩니다.

표 4-2. vSAN 기본 스토리지 정책 규격

규격	설정
허용되는 장애	1
개체당 디스크 스트라이프 수	1

표 4-2. 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 씬 프로비저닝됩니다.
강제 프로비저닝	아니요

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. 때에 따라 클러스터를 수직 확장할 때 기본 스토리지 정책을 수정하여 VMware Cloud on AWS에 대한 서비스 수준 계약의 요구 사항을 준수해야 합니다.

사용자 정의 스토리지 정책을 데이터스토어에 할당하면 vSAN은 사용자 정의 정책에 대한 설정을 지정된 데이터스토어에 적용합니다. 언제든지, 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 할당하지 않으면 vSAN 기본 스토리지 정책이 모든 가상 시스템 개체에 할당됩니다. **VM 스토리지 정책** 텍스트 상자는 [스토리지 선택] 페이지에서 **데이터스토어 기본값**으로 설정됩니다. 스토리지 정책 사용에 대한 자세한 내용은 "vSphere 스토리지" 설명서를 참조하십시오.

  참고 VM 스왑 및 VM 메모리 개체에는 **강제 프로비저닝**이 **예**로 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. 일반적으로 기본 스토리지 정책의 설정은 편집하지 않습니다.
- 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 데이터스토어의 기본 스토리지 정책 변경

선택한 vSAN 데이터스토어의 기본 스토리지 정책을 변경할 수 있습니다.

사전 요구 사항

vSAN 데이터스토어에 기본 정책으로 할당할 VM 스토리지 정책이 vSAN 클러스터의 가상 시스템에 대한 요구 사항을 충족하는지 확인합니다.

절차

1. vSAN 데이터스토어로 이동합니다.
2. **구성**을 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 목록에서 선택할 수 있습니다.
4. 정책을 선택하고 **확인**을 클릭합니다.

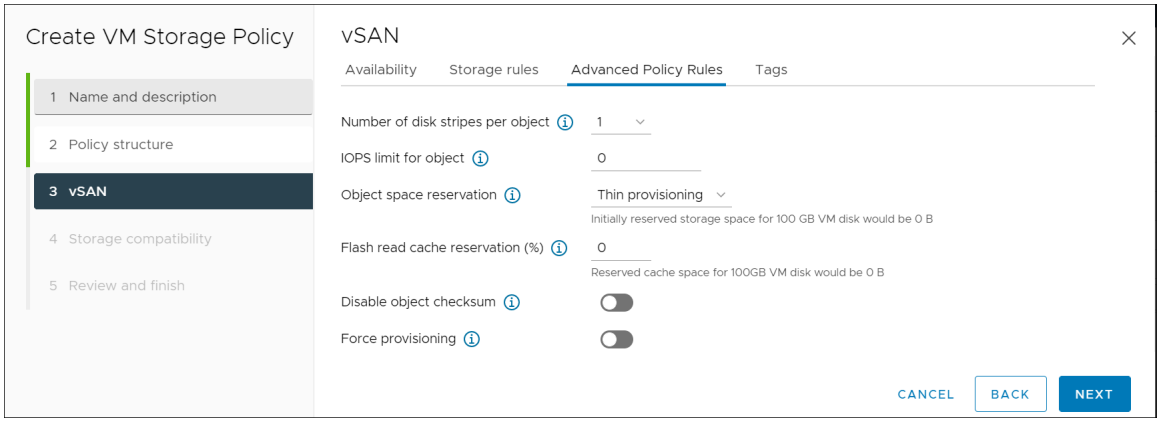
   데이터스토어의 스토리지 정책을 명시적으로 지정하지 않고 새 가상 시스템을 프로비저닝하면 스토리지 정책이 기본 정책으로 적용됩니다.

다음에 수행할 작업

가상 시스템에 대한 새 스토리지 정책을 정의할 수 있습니다. vSphere Client를 사용하여 vSAN에 대한 스토리지 정책 정의를 참조하십시오.

vSphere Client를 사용하여 vSAN에 대한 스토리지 정책 정의

VM 및 해당 가상 디스크의 스토리기 요구 사항을 정의하는 스토리지 정책을 생성할 수 있습니다. 이 정책에서는 vSAN 데이터스토어가 지원하는 스토리지 용량을 참조합니다.



사전 요구 사항

- vSAN 스토리지 제공자를 사용할 수 있는지 확인합니다. vSAN 스토리지 제공자 보기를 참조하십시오.
- 필요한 권한: **Profile-driven storage.Profile-driven storage view** 및 **Profile-driven storage.Profile-driven storage update**

절차

1. **정책 및 프로파일**로 이동한 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 이름과 설명을 입력하고 **다음**을 클릭합니다.
5. [정책 구조] 페이지에서 ["vSAN" 스토리지에 대한 규칙 사용]을 선택하고 **다음**을 클릭합니다.

6 vSAN 페이지에서 정책 규칙 집합을 정의하고 **다음**을 클릭합니다.

a [가용성] 탭에서 **사이트 재해 허용** 및 **허용되는 장애**를 정의합니다.

가용성 옵션은 [허용되는 장애], [데이터 인접성] 및 [장애 허용 방법]에 대한 규칙을 정의합니다.

- **사이트 재해 허용**은 가상 시스템 개체에 사용되는 사이트 장애 허용의 유형을 정의합니다.
- **허용되는 장애**는 가상 시스템 개체가 허용할 수 있는 호스트 및 디바이스 장애 수 및 데이터 복제 방법을 정의합니다.

예를 들어 **이중 사이트 미러링** 및 **2개의 장애 - RAID-6(삭제 코딩)**을 선택하면 vSAN에서 다음과 같은 정책 규칙이 구성됩니다.

- 허용되는 장애: 1
- 허용할 수 있는 장애의 보조 수준: 2
- 데이터 인접성: 없음
- 장애 허용 방법: RAID-5/6(이레이저 코딩) - 용량

b [스토리지 규칙] 탭에서 원격 데이터스토어 구분을 위해 HCI 메시와 함께 사용할 수 있는 암호화, 공간 효율성 및 스토리지 계층 규칙을 정의합니다.

- **암호화 서비스**: 이 정책을 사용하여 배포하는 가상 시스템용 암호화 규칙을 정의합니다. 다음 옵션 중 하나를 선택할 수 있습니다.
  - **미사용 데이터 암호화**: 가상 시스템에서 암호화를 사용하도록 설정됩니다.
  - **암호화 없음**: 가상 시스템에서 암호화가 사용하도록 설정되지 않았습니다.
  - **기본 설정 없음**: 가상 시스템은 [미사용 데이터 암호화] 및 [암호화 없음] 옵션 둘 다와 호환됩니다.
- **공간 효율성**: 이 정책을 사용하여 배포하는 가상 시스템의 공간 절약 규칙을 정의합니다. 다음 옵션 중 하나를 선택할 수 있습니다.
  - **중복 제거 및 압축**: 가상 시스템에서 중복 제거와 압축을 둘 다 사용할 수 있습니다. 중복 제거 및 압축은 플래시 전용 디스크 그룹에서만 사용할 수 있습니다. 자세한 내용은 중복 제거와 압축의 설계 고려 사항의 내용을 참조하십시오.
  - **압축 전용**: 가상 시스템에서 압축만 사용할 수 있습니다. 압축은 플래시 전용 디스크 그룹에서만 사용할 수 있습니다. 자세한 내용은 중복 제거와 압축의 설계 고려 사항의 내용을 참조하십시오.
  - **공간 효율성 없음**: 가상 시스템에서 공간 효율성 기능을 사용하지 않도록 설정됩니다. 이 옵션을 선택하면 공간 효율성 옵션이 켜져 있지 않은 데이터스토어가 필요합니다.
  - **기본 설정 없음**: 가상 시스템은 모든 옵션과 호환됩니다.
- **스토리지 계층**: 이 정책을 사용하여 배포하는 가상 시스템에 대해 스토리지 계층을 지정합니다. 다음 옵션 중 하나를 선택할 수 있습니다. **기본 설정 없음** 옵션을 선택하면 가상 시스템은 하이브리드 환경과 플래시 전용 환경 둘 다와 호환됩니다.
  - **플래시 전용**

- **하이브리드**
- **기본 설정 없음**

c [고급 정책 규칙] 탭에서 개체 및 IOPS 제한당 디스크 스트라이프 수와 같은 고급 정책 규칙을 정의합니다.

d [태그] 탭에서 **태그 규칙 추가**를 클릭하고 태그 규칙에 대한 옵션을 정의합니다.

제공하는 값은 vSAN 데이터스토어의 스토리지 기능에서 보급되는 값 범위 내에 있어야 합니다.

7 [스토리지 호환성] 페이지의 **호환** 및 **비호환** 탭에 있는 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.

8 [검토 및 완료] 페이지에서 정책 설정을 검토하고 **마침**을 클릭합니다.

결과

새 정책이 목록에 추가됩니다.

다음에 수행할 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 클러스터 확장 및 관리

5

vSAN 클러스터를 설정한 후 호스트와 용량 디바이스를 추가하고 호스트와 디바이스를 제거하고 장애 시나리오를 관리할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vSAN 클러스터 확장
- HCI 메시와 원격 데이터스토어 공유
- 유지 보수 모드 사용
- vSAN 클러스터에서 장애 도메인 관리
- vSAN iSCSI 대상 서비스 사용
- vSAN 파일 서비스
- 하이브리드 vSAN 클러스터를 플래시 전용 클러스터로 마이그레이션
- vSAN 클러스터 종료 및 다시 시작

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 추가를 참조하십시오. 디바이스를 추가하거나 용량이 포함된 호스트를 추가하는 경우 vSAN은 새롭게 추가된 디바이스에 자동으로 데이터를 배포합니다. "vSAN 모니터링 및 문제 해결" 에서 "자동 재조정 구성"을 참조하십시오.
- 호스트 프로파일을 사용하여 기존 ESXi 호스트를 vSAN 클러스터로 이동합니다. 호스트 프로파일을 사용하여 호스트 구성를 참조하십시오. 새 클러스터 멤버는 스토리지를 추가하고 용량을 계산합니다. 새로 추가된 호스트의 로컬 용량 디바이스에서 일부 디스크 그룹을 수동으로 생성해야 합니다. vSAN 호스트에서 디스크 그룹 생성를 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 추가를 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 디스크 그룹을 추가하여 클러스터의 스토리지 용량을 확장합니다. 새 디스크 그룹을 생성하려면 캐시를 위한 플래시 디바이스가 필요합니다. 디스크 그룹의 디바이스 추가에 대한 자세한 내용은 디스크 그룹에 디바이스 추가 항목을 참조하십시오. 캐시를 늘리지 않고 용량 디바이스를 추가하는 경우 캐시 대 용량 비율이 지원되지 않는 수준으로 줄어들 수 있습니다. 자세한 내용은 "vSAN 계획 및 배포" 를 참조하십시오.
- 하나 이상의 캐시 디바이스(플래시)와 하나 이상의 용량 디바이스(플래시 또는 자기 디스크)를 기존 스토리지 I/O 컨트롤러나 새 호스트에 추가하여 클러스터 성능을 향상시킵니다. 또는 디스크 그룹이 포함된 호스트를 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 클러스터에 존재할 수 있지만 효율적인 작동을 위해서는 구성이 일관된 호스트를 추가해야 합니다. 최상의 결과 얻으려면 캐시 및 용량 디바이스가 있는 호스트를 추가하여 클러스터 용량을 확장하십시오. 디스크 그룹에 동일하거나 유사한 디바이스를 사용하는 것이 가장 좋지만 vSAN HCL에 나열된 디바이스는 모두 지원됩니다. 호스트 및 디스크 그룹 전체에 용량을 균등하게 분산해 보십시오. 디바이스를 디스크 그룹에 추가하는 방법에 대한 자세한 내용은 디스크 그룹에 디바이스 추가 항목을 참조하십시오.

클러스터 용량을 확장한 후 수동 재조정을 수행하여 클러스터 전체에 리소스를 균등하게 분산합니다. 자세한 내용은 "vSAN 모니터링 및 문제 해결" 을 참조하십시오.

Quickstart를 사용하여 vSAN 클러스터에 호스트 추가

Quickstart를 통해 vSAN 클러스터를 구성한 경우 Quickstart 워크플로를 사용하여 호스트 및 스토리지 디바이스를 클러스터에 추가할 수 있습니다.

vSAN 클러스터에 새 호스트를 추가하는 경우 클러스터 구성 마법사를 사용하여 호스트 구성을 완료할 수 있습니다. Quickstart에 대한 자세한 내용은 "vSAN 계획 및 배포" 에서 "Quickstart를 사용하여 vSAN 클러스터 구성 및 확장"을 참조하십시오.

참고 호스트에서 vCenter Server를 실행하는 경우 Quickstart 워크플로를 사용하여 호스트를 클러스터에 추가할 때 호스트를 유지 보수 모드로 설정할 수 없습니다. 동일한 호스트가 Platform Services Controller를 실행 중일 수도 있습니다. 호스트에서 다른 모든 VM의 전원을 꺼야 합니다.

사전 요구 사항

- vSAN 클러스터에 대해 Quickstart 워크플로를 사용할 수 있어야 합니다.
- Quickstart 워크플로 외부에서 Quickstart 워크플로를 통해 수행된 네트워크 구성이 수정되지 않았습니다.

절차

1. vSphere Client에서 클러스터로 이동합니다.
2. [구성] 탭을 클릭하고 **구성 > Quickstart**를 선택합니다.
3. [호스트 추가] 카드에서 **시작**을 클릭하여 호스트 추가 마법사를 엽니다.
   a. [호스트 추가] 페이지에서 새 호스트에 대한 정보를 입력하거나 [기존 호스트]를 클릭하고 인벤토리에 나열된 호스트 중에서 선택합니다.
   b. [호스트 요약] 페이지에서 호스트 설정을 확인합니다.
   c. [완료 준비] 페이지에서 **마침**을 클릭합니다.
4. 클러스터 구성 카드에서 **시작**을 클릭하여 클러스터 구성 마법사를 엽니다.
   a. [Distributed Switch 구성] 페이지에서 새 호스트에 대한 네트워킹 설정을 입력합니다.
   b. (선택 사항) [디스크 할당] 페이지에서 각각의 새 호스트에서 디스크를 선택합니다.
   c. (선택 사항) [장애 도메인 생성] 페이지에서 새 호스트를 해당 장애 도메인으로 이동합니다.

      장애 도메인에 대한 자세한 내용은 vSAN 클러스터에서 장애 도메인 관리를 참조하십시오.
   d. [완료 준비] 페이지에서 클러스터 설정을 확인하고 **마침**을 클릭합니다.

vSAN 클러스터에 호스트 추가

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

사전 요구 사항

- 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.

절차

1. vSAN 클러스터로 이동합니다.

2 클러스터를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가**를 선택합니다. [호스트 추가] 마법사가 나타납니다.

옵션	설명
새 호스트	a 호스트 이름이나 IP 주소를 입력합니다. b 호스트에 연결된 사용자 이름과 암호를 입력합니다.
기존 호스트	a 이전에 vCenter Server에 추가한 호스트를 선택합니다.

3 **다음**을 클릭합니다.

4 요약 정보를 확인한 후 **다음**을 클릭합니다.

5 설정을 검토하고 **완료**를 클릭합니다.

호스트가 클러스터에 추가됩니다.

다음에 수행할 작업

vSAN 디스크 균형 상태 점검이 녹색인지 확인합니다.

vSAN 클러스터 구성 및 문제 해결에 대한 자세한 내용은 "vSAN 모니터링 및 문제 해결" 에서 "vSAN 클러스터 구성 문제"를 참조하십시오.

호스트 프로파일을 사용하여 호스트 구성

vSAN 클러스터에 여러 호스트가 있는 경우 기존 vSAN 호스트의 프로파일을 사용하여 vSAN 클러스터의 나머지 호스트를 구성할 수 있습니다.

호스트 프로파일에는 스토리지 구성, 네트워크 구성 또는 호스트의 다른 특징과 같은 정보가 포함되어 있습니다. 호스트가 많이 있는(예: 8, 16, 32 또는 64개의 호스트) 클러스터를 생성하려면 호스트 프로파일 기능을 사용합니다. 호스트 프로파일을 사용하면 vSAN 클러스터에 한 번에 둘 이상의 호스트를 추가할 수 있습니다.

사전 요구 사항

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

절차

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 **다음**을 클릭합니다.

e **마침**을 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 **분리**를 클릭합니다.

d 나열된 호스트 및 클러스터를 모두 프로파일에서 분리하려면 **모두 분리**를 클릭합니다.

e **다음**을 클릭합니다.

f **마침**을 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 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 규정 준수 오류를 해결하려면 호스트에 업데이트를 적용합니다.

a **모니터** 탭을 선택하고 **규정 준수**를 클릭합니다.

b 업데이트를 적용할 하나 이상의 호스트를 마우스 오른쪽 버튼으로 클릭하고 **모든 vCenter 작업 > 호스트 프로파일 > 업데이트 적용**을 선택합니다.

호스트를 사용자 지정하여 호스트 프로파일 정책의 사용자 입력 매개 변수를 업데이트하거나 변경할 수 있습니다.

c **다음**을 클릭합니다.

d 호스트 프로파일 업데이트를 적용하는 데 필요한 작업을 검토하고 **마침**을 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.

HCI 메시와 원격 데이터스토어 공유

vSAN 클러스터는 데이터스토어를 다른 vSAN 클러스터와 공유할 수 있습니다. 로컬 클러스터에서 실행되는 VM을 원격 데이터스토어의 스토리지 공간을 사용하여 프로비저닝할 수 있습니다.

[데이터스토어 공유] 보기를 사용하여 로컬 vSAN 클러스터에 마운트된 원격 데이터스토어를 모니터링하고 관리합니다. 각 클라이언트 vSAN 클러스터는 vCenter Server에서 관리하는 동일한 데이터 센터에 있는 서버 vSAN 클러스터에서 원격 데이터스토어를 마운트할 수 있습니다. 호환되는 각 vSAN 클러스터는 서버 역할을 할 수 있으며 다른 vSAN 클러스터가 로컬 데이터스토어를 마운트할 수 있도록 허용할 수도 있습니다.

HCI 메시를 사용한 원격 데이터스토어 마운트는 클러스터 전체 구성입니다. 원격 데이터스토어를 vSAN 클러스터에 마운트할 수 있으며, 이 경우 클러스터의 모든 호스트에 마운트됩니다.

새 가상 시스템을 프로비저닝할 때 클라이언트 클러스터에 마운트된 원격 데이터스토어를 선택할 수 있습니다. 데이터스토어에 대해 구성된 호환되는 스토리지 정책을 할당합니다.

가상 개체의 용량, 성능, 상태 및 배치에 대한 모니터링 보기에는 원격 개체 및 데이터스토어의 상태가 표시됩니다.

HCI 메시 vSAN에는 다음과 같은 설계 고려 사항이 있습니다.

- 클러스터는 동일한 vCenter Server에서 관리되며 동일한 데이터 센터 내에 배치되어야 합니다.
- 클러스터에서 7.0 업데이트 1 이상이 실행되고 있어야 합니다.
- vSAN 클러스터는 최대 10개의 클라이언트 vSAN 클러스터에 로컬 데이터스토어를 제공할 수 있습니다.
- 클라이언트 클러스터는 하나 이상의 vSAN 서버 클러스터에서 최대 5개의 원격 데이터스토어를 마운트할 수 있습니다.

- 단일 원격 데이터스토어는 vSAN 서버 클러스터에 있는 최대 128개의 vSAN 호스트로 마운트할 수 있습니다.
- VM을 구성하는 모든 개체는 동일한 데이터스토어에 상주해야 합니다.
- vSphere HA가 HCI 메시에서 작동하려면 APD의 데이터스토어에 대해 "전원 끄기 및 VM 다시 시작" 고장 대응을 구성합니다.
- 클러스터의 일부가 아닌 클라이언트 호스트는 지원되지 않습니다. 단일 호스트 컴퓨팅 전용 클러스터를 구성할 수 있지만 또 다른 호스트를 클러스터에 추가하지 않으면 vSphere HA가 작동하지 않습니다.

다음 기능은 HCI 메시에서 지원되지 않습니다.

- vSAN 전송 중 데이터 암호화
- vSAN 확장된 클러스터
- vSAN 2노드 클러스터

다음 구성은 HCI 메시에서 지원되지 않습니다.

- vSAN 파일 공유, iSCSI 볼륨 또는 CNS 영구 볼륨의 원격 프로비저닝. 로컬 vSAN 데이터스토어에 프로비저닝할 수 있지만 원격 vSAN 데이터스토어에서는 프로비저닝할 수 없습니다.
- 여러 vSAN VMkernel 포트를 사용하는 에어갭 vSAN 네트워크 또는 클러스터
- RDMA를 통한 vSAN 통신

HCI 메시 계산 전용 클라이언트

vSAN 7.0 Update 2 이상에서는 vSAN 이외의 클러스터를 HCI 메시 클라이언트로 구성할 수 있습니다. HCI 메시 계산 전용 클라이언트 클러스터의 호스트에는 로컬 스토리지가 필요하지 않습니다. 이러한 호스트는 동일한 데이터 센터에 있는 vSAN 클러스터에서 원격 데이터스토어를 마운트할 수 있습니다.

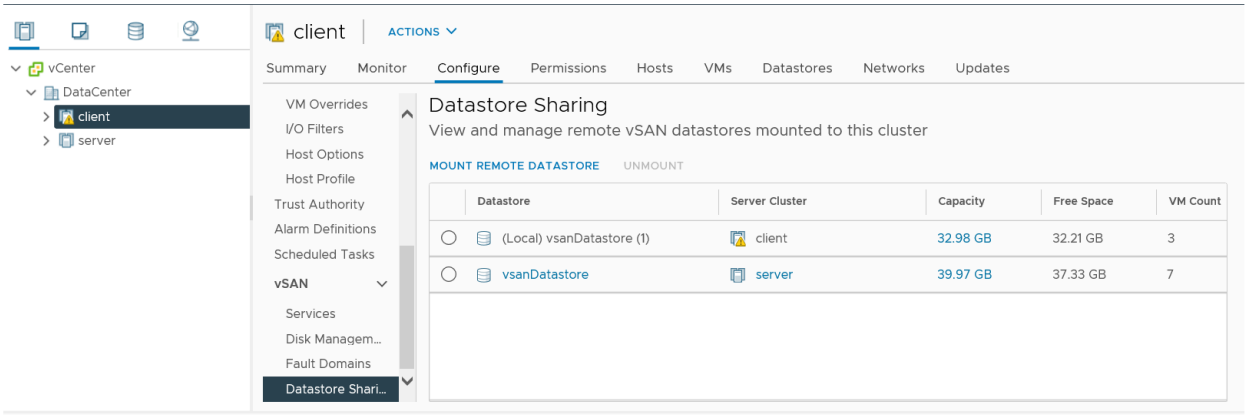
HCI 메시 계산 전용 클러스터에는 다음과 같은 설계 고려 사항이 있습니다.

- vSAN 네트워킹을 클라이언트 호스트에 구성해야 합니다.
- vSAN 계산 전용 호스트에는 디스크 그룹이 있을 수 없습니다.
- 계산 전용 클러스터에서는 vSAN 데이터 관리 기능을 구성할 수 없습니다.

vSAN에 대해 vSphere 클러스터를 구성할 경우 HCI 메시 계산 클러스터로 지정할 수 있습니다. 원격 데이터스토어를 마운트하고 원격 vSAN 데이터스토어의 용량, 상태 및 성능을 모니터링할 수 있습니다.

원격 데이터스토어 보기

[데이터스토어 공유] 페이지를 사용하여 로컬 vSAN 클러스터에 마운트된 원격 데이터스토어와 로컬 데이터스토어를 공유하는 클라이언트 클러스터를 볼 수 있습니다.



절차

1 로컬 vSAN 클러스터로 이동합니다.

2 [구성] 탭을 클릭합니다.

3 vSAN에서 **데이터스토어 공유**를 클릭합니다.

결과

이 보기에는 로컬 클러스터에 마운트된 각 데이터스토어에 대한 정보가 표시됩니다.

- 데이터스토어를 호스팅하는 서버 클러스터
- 데이터스토어의 용량
- 사용 가능한 공간
- 데이터스토어를 사용하는 VM의 수(로컬 클러스터에서는 계산 리소스를 사용하지만 서버 클러스터에서는 스토리지 리소스를 사용하는 VM의 수)
- 데이터스토어를 마운트한 클라이언트 클러스터.

다음에 수행할 작업

이 페이지에서 원격 데이터스토어를 마운트 또는 마운트 해제할 수 있습니다.

원격 데이터스토어 마운트

동일한 vCenter Server에서 관리하는 다른 vSAN 클러스터에서 하나 이상의 데이터스토어를 마운트할 수 있습니다.

절차

1 로컬 vSAN 클러스터로 이동합니다.

2 [구성] 탭을 클릭합니다.

3 vSAN에서 **데이터스토어 공유**를 클릭합니다.

4 **원격 데이터스토어 마운트**를 클릭합니다.

5 데이터스토어를 선택하고 **다음**을 클릭합니다.

6 데이터스토어 호환성을 확인하고 **완료**를 클릭합니다.

결과

원격 데이터스토어가 로컬 vSAN 클러스터에 마운트됩니다.

다음에 수행할 작업

VM을 프로비저닝할 때 원격 데이터스토어를 스토리지 리소스로 선택할 수 있습니다. 원격 데이터스토어에서 지원되는 스토리지 정책을 할당합니다.

원격 데이터스토어 마운트 해제

vSAN 클러스터에서 원격 데이터스토어를 마운트 해제할 수 있습니다.

로컬 클러스터에 원격 vSAN 데이터스토어를 사용하는 가상 시스템이 없는 경우 로컬 vSAN 클러스터에서 데이터스토어를 마운트 해제할 수 있습니다.

절차

1 로컬 vSAN 클러스터로 이동합니다.

2 [구성] 탭을 클릭합니다.

3 vSAN에서 **데이터스토어 공유**를 클릭합니다.

4 원격 데이터스토어를 선택하고 **마운트 해제**를 클릭합니다.

5 **마운트 해제**를 클릭하여 확인합니다.

결과

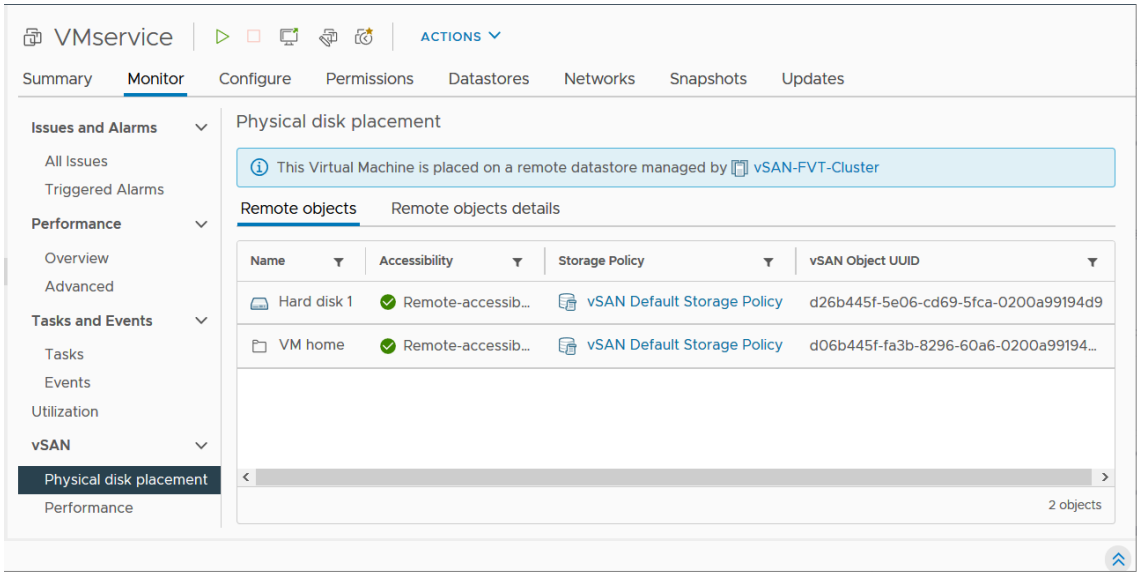
선택한 데이터스토어가 로컬 클러스터에서 마운트 해제됩니다.

HCI 메시 모니터링

vSphere Client를 사용하여 HCI 메시 작업의 상태를 모니터링할 수 있습니다.

vSAN 용량 모니터는 원격 데이터스토어가 클러스터에 마운트된 경우 이를 알려줍니다. 원격 데이터스토어를 선택하여 해당 용량 정보를 볼 수 있습니다.

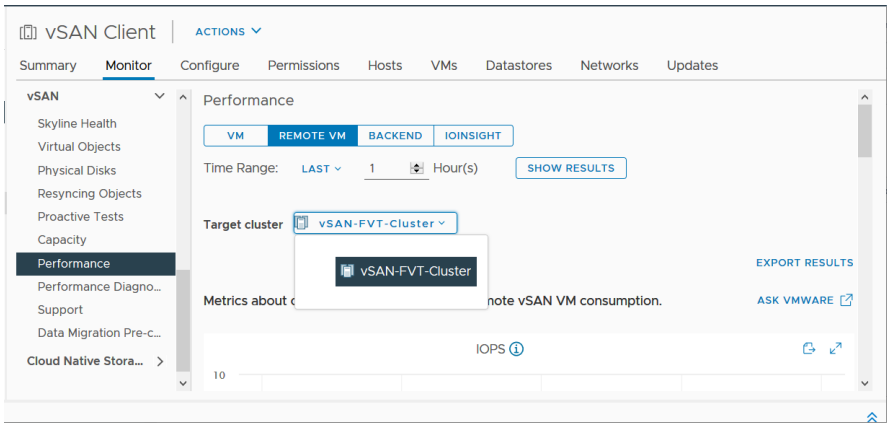
가상 개체 보기에는 가상 개체가 있는 데이터스토어가 표시됩니다. 원격 데이터스토어에 있는 VM의 물리적 디스크 배치 보기에는 원격 위치에 대한 정보가 표시됩니다.



vSAN 상태 점검은 HCI 함수의 상태를 보고합니다.

- [데이터] > [vSAN 개체 상태] 검사에서는 원격 개체의 접근성 정보를 표시합니다.
- [네트워크] > [서버] 클러스터 파티션 검사는 클라이언트 클러스터와 서버 클러스터의 호스트 간 네트워크 파티션에 대한 보고서를 확인합니다.
- [네트워크] > [지연 시간]은 클라이언트 클러스터 및 서버 클러스터에 있는 호스트 간의 지연 시간을 검사합니다.

vSAN 클러스터 성능 보기에는 원격 클러스터의 관점에서 클라이언트 클러스터의 VM 수준 성능을 표시하는 VM 성능 차트가 포함됩니다. 원격 데이터스토어를 선택하여 성능을 볼 수 있습니다.



원격 데이터스토어에서 사전 테스트를 실행하여 VM 생성 및 네트워크 성능을 확인할 수 있습니다. VM 생성 테스트는 원격 데이터스토어에 VM을 생성합니다. 네트워크 성능 테스트는 클라이언트 클러스터의 모든 호스트와 서버 클러스터의 모든 호스트 간의 네트워크 성능을 확인합니다.

유지 보수 모드 사용

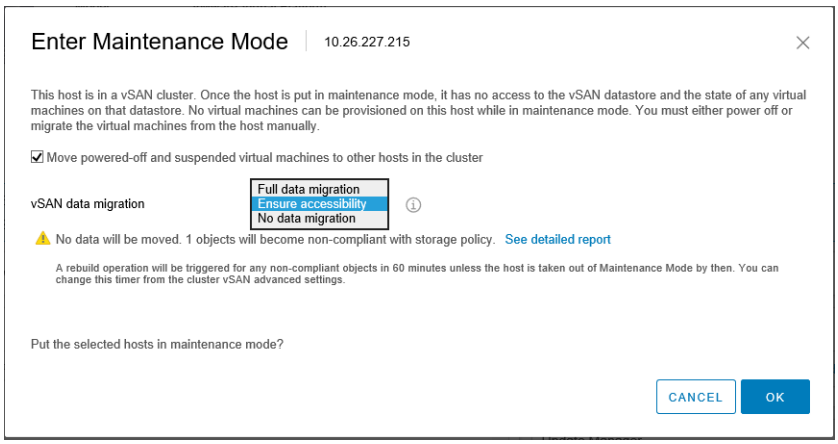
vSAN 클러스터의 멤버인 호스트를 종료, 재부팅 또는 연결 해제하기 전에 호스트를 유지 보수 모드로 전환해야 합니다.

유지 보수 모드를 사용할 경우 다음 지침을 고려하십시오.

- ESXi 호스트를 유지 보수 모드로 전환할 때는 **액세스 지원 보장** 또는 **전체 데이터 마이그레이션** 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.
- **액세스 지원 보장** 모드는 가상 시스템 실행에 꼭 필요한 구성 요소만 호스트에서 마이그레이션하기 때문에 **액세스 지원 보장** 모드가 **전체 데이터 마이그레이션** 모드보다 빠릅니다. 이 모드에서 장애가 발생할 경우 가상 시스템의 가용성이 영향을 받습니다. **액세스 지원 보장** 모드를 선택하면 장애 중에 데이터가 보호되지 않으며 예기치 않은 데이터 손실이 발생할 수 있습니다.
- **전체 데이터 마이그레이션** 모드를 선택하는 경우, 리소스를 사용할 수 있고 **허용되는 장애**가 1 이상으로 구성되었으면 자동으로 데이터가 장애로부터 다시 보호됩니다. 이 모드에서는 호스트의 모든 구성 요소가 마이그레이션되고 호스트에 있는 데이터의 양에 따라 마이그레이션이 더 오래 걸릴 수 있습니다. **전체 데이터 마이그레이션** 모드를 사용하는 경우 가상 시스템은 계획된 유지 보수 중에도 장애를 허용할 수 있습니다.
- 호스트가 3개인 클러스터를 사용하는 경우에는 **전체 데이터 마이그레이션**을 사용하여 서버를 유지 보수 모드로 전환할 수 없습니다. 가용성을 극대화하려면 호스트가 4개 이상인 클러스터를 설계하는 것을 고려해야 합니다.

호스트를 유지 보수 모드로 전환하기 전에 다음을 확인해야 합니다.

- **전체 데이터 마이그레이션** 모드를 사용하는 경우에는 **허용되는 장애** 정책 요구 사항을 충족하기에 충분한 호스트와 용량이 클러스터에 있는지 확인해야 합니다.
- 나머지 호스트에 Flash Read Cache 예약을 처리하기에 충분한 플래시 용량이 있는지 확인합니다. 호스트당 현재 용량 사용을 분석하고 단일 호스트 장애로 인해 클러스터의 공간이 부족해져서 클러스터 용량, 캐시 예약 및 클러스터 구성 요소에 영향을 줄지 여부를 분석하려면 다음 RVC 명령을 실행합니다. `vsan.whatif_host_failures` RVC 명령에 대한 자세한 내용은 "RVC 명령 참조 가이드" 를 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.



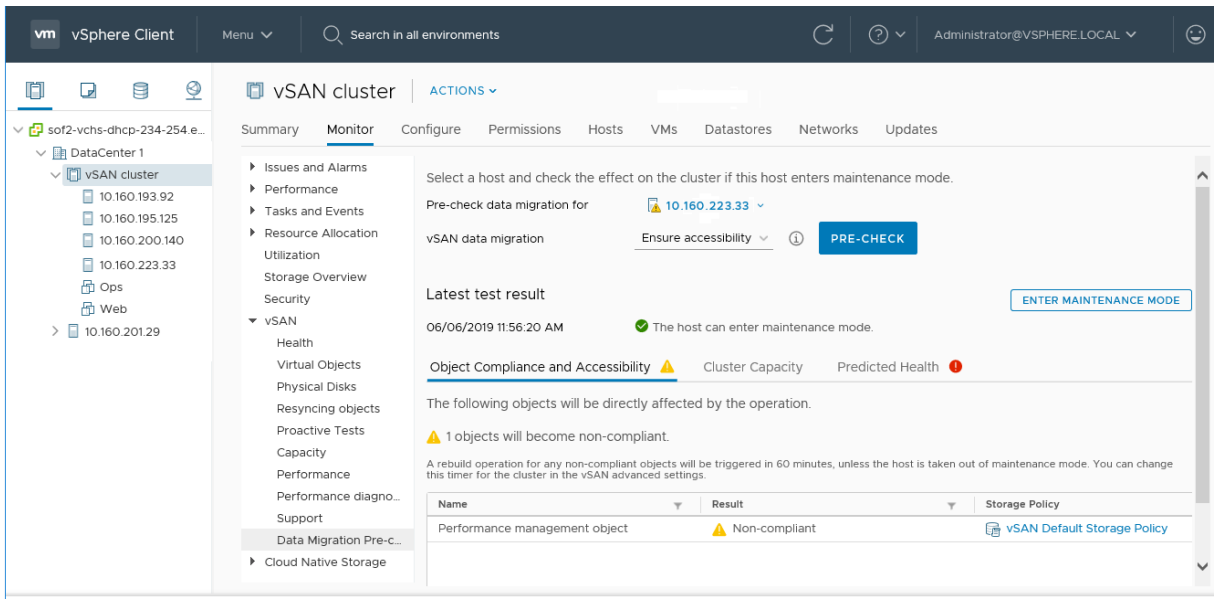
[유지 보수 모드 확인] 대화상자에는 유지 보수 작업을 안내하는 정보가 제공됩니다. 각 데이터 제거 옵션의 효과를 볼 수 있습니다.

- 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

호스트의 데이터 마이그레이션 기능 확인

데이터 마이그레이션 사전 검사를 사용하여 호스트를 유지 보수 모드로 전환하거나 클러스터에서 제거할 때 데이터 마이그레이션 옵션의 영향을 확인합니다.

vSAN 호스트를 유지 보수 모드로 전환하기 전에 데이터 마이그레이션 사전 검사를 실행합니다. 테스트 결과에는 클러스터 용량, 예측되는 상태 점검 및 규정을 준수하지 않는 개체에 미치는 영향을 확인하는 데 도움이 되는 정보가 제공됩니다. 작업이 성공하지 못하면 사전 검사는 필요한 리소스에 대한 정보를 제공합니다.



절차

1 vSAN 클러스터로 이동합니다.

2 [모니터] 탭을 클릭합니다.

3 vSAN에서 **데이터 마이그레이션 사전 검사**를 클릭합니다.

4 호스트, 데이터 마이그레이션 옵션을 선택하고 **사전 검사**를 클릭합니다.

vSAN에서 데이터 마이그레이션 사전 검사 테스트가 실행됩니다.

5 테스트 결과를 살펴봅니다.

사전 검사 결과에는 호스트가 유지 보수 모드를 안전하게 전환될 수 있는지 여부가 표시됩니다.

- [개체 규정 준수] 및 [액세스 지원] 탭에는 데이터 마이그레이션 후 문제가 있을 수 있는 개체가 표시됩니다.
- [클러스터 용량] 탭에는 작업을 수행하기 전과 후에 데이터 마이그레이션이 vSAN 클러스터에 미치는 영향이 표시됩니다.
- [예측되는 상태] 탭에는 데이터 마이그레이션의 영향을 받을 수 있는 상태 점검이 표시됩니다.

다음에 수행할 작업

사전 검사에서 호스트를 유지 보수 모드로 전환할 수 있다고 나타나면 **유지 보수 모드 설정**을 클릭하여 데이터를 마이그레이션하고 호스트를 유지 보수 모드로 전환합니다.

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 경우 **액세스 지원 보장** 또는 **전체 데이터 마이그레이션** 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.

이 호스트에서 제공하는 모든 vSAN iSCSI 대상은 클러스터의 다른 호스트로 전송되므로 iSCSI 이니시에이터가 새 대상 소유자로 리디렉션됩니다.

사전 요구 사항

선택한 옵션에 필요한 기능이 환경에 있는지 확인합니다.

절차

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

2 제거 모드를 선택하고 **확인**을 클릭합니다.

옵션	설명
액세스 지원 보장	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. 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 **허용되는 장애**가 1로 설정된 상태에서 장애가 발생하면 클러스터에 데이터 손실이 발생할 수 있습니다. **참고** 이는 3개의 장애 도메인으로 구성된 vSAN 클러스터 또는 3개 호스트 클러스터를 사용 중인 경우 사용할 수 있는 유일한 제거 모드입니다.
전체 데이터 마이그레이션	vSAN은 모든 데이터를 클러스터의 다른 호스트로 내보내고 현재 개체 규정 준수 상태를 유지합니다. 호스트를 영구적으로 마이그레이션하려는 경우에 이 옵션을 선택합니다. 클러스터의 마지막 호스트에서 데이터를 제거하는 경우 가상 시스템을 다른 데이터스토어로 마이그레이션한 후 호스트를 유지 보수 모드로 설정해야 합니다. 이 제거 모드를 선택하면 가장 많은 양의 데이터가 전송되므로 시간과 리소스가 가장 많이 소모됩니다. 선택한 호스트의 로컬 스토리지에 있는 모든 구성 요소가 클러스터의 다른 곳으로 마이그레이션됩니다. 호스트가 유지 보수 모드로 전환되면 모든 가상 시스템은 해당 스토리지 구성 요소에 액세스할 수 있고 할당된 스토리지 정책을 계속 준수합니다. **참고** 가용성이 저하된 상태의 개체가 있는 경우 이 모드는 이 규정 준수 상태를 유지하며 개체의 규정 준수를 보장하지 않습니다. 호스트에 데이터가 있는 가상 시스템 개체에 액세스할 수 없으며 해당 개체가 완전히 제거되지 않는 경우 호스트가 유지 보수 모드로 전환될 수 없습니다.
데이터 마이그레이션 없음	vSAN이 이 호스트에서 데이터를 전혀 제거하지 않습니다. 호스트의 전원을 끄거나 호스트를 클러스터에서 제거하면 일부 가상 시스템에 액세스하지 못하게 될 수도 있습니다.

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

또는 ESXCLI를 사용하여 호스트를 유지 보수 모드로 전환할 수 있습니다. 호스트를 이 모드로 전환하기 전에 호스트에서 실행되는 VM의 전원을 꺼야 합니다.

유지 보수 모드로 전환하려면 호스트에서 다음 명령을 실행합니다.

```
esxcli system maintenanceMode set --enable 1
```

호스트의 상태를 확인하려면 다음 명령을 실행합니다.

```
esxcli system maintenanceMode get
```

유지 보수 모드를 종료하려면 다음 명령을 실행합니다.

```
esxcli system maintenanceMode set --enable 0
```

다음에 수행할 작업

클러스터의 데이터 마이그레이션 진행률을 추적할 수 있습니다. 자세한 내용은 "vSAN 모니터링 및 문제 해결" 을 참조하십시오.

vSAN 클러스터에서 장애 도메인 관리

장애 도메인을 사용하면 vSAN 클러스터가 여러 랙 또는 블레이드 서버 섀시에 걸쳐 있는 경우 랙 또는 섀시 장애로부터 보호를 제공할 수 있습니다. 장애 도메인을 생성하고 각 장애 도메인에 하나 이상의 호스트를 추가할 수 있습니다.

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

클러스터의 **허용되는 장애** 정책은 가상 시스템이 허용하도록 프로비저닝된 장애 수에 따라 다릅니다. **허용되는 장애**가 1(`FTT=1`)로 설정된 가상 시스템을 구성하면 vSAN이 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 **허용되는 장애**가 N으로 설정되면(`(FTT=n)`), vSAN은 클러스터에 최소 `2*n+1`개의 장애 도메인이 필요합니다. 이 정책을 사용하여 장애 도메인이 포함된 클러스터에서 가상 시스템을 프로비저닝하는 경우 연관된 가상 시스템 개체의 복사본은 별도의 랙에 저장됩니다.

FTT를 1로 설정하려면 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 계획 및 배포" 에서 "vSAN 장애 도메인 설계 및 크기 조정"을 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 생성합니다. 이러한 용량의 클러스터는 **허용되는 장애**를 1로 설정하여 구성할 수 있습니다. **허용되는 장애**를 2로 설정하려면 클러스터에 5개의 장애 도메인을 구성합니다.

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 구성합니다. 장애 도메인 수를 늘리면 랙 장애 후 클러스터에서 사용할 수 있는 전체 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 지정할 때 각 장애 도메인에 일정한 수의 호스트를 배치합니다.

  장애 도메인 설계에 대한 지침은 "vSAN 계획 및 배포" 에서 "vSAN 장애 도메인 설계 및 크기 조정"을 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.

사전 요구 사항

- 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.

절차

1. vSAN 클러스터로 이동합니다.
2. **구성** 탭을 클릭합니다.
3. vSAN에서 **장애 도메인**을 클릭합니다.
4. 더하기 아이콘을 클릭합니다. [새 장애 도메인] 마법사가 열립니다.
5. 장애 도메인 이름을 입력합니다.
6. 장애 도메인에 추가할 호스트를 하나 이상 선택합니다.

   장애 도메인은 비워 둘 수 없습니다. 장애 도메인에 포함할 호스트를 하나 이상 선택해야 합니다.
7. **생성**을 클릭합니다.

   선택한 호스트가 장애 도메인에 나타납니다. 각 장애 도메인에는 사용된 용량과 예약된 용량 정보가 표시됩니다. 이를 통해 장애 도메인 전체의 용량 분포를 볼 수 있습니다.

선택한 장애 도메인으로 호스트 이동

호스트를 vSAN 클러스터의 선택한 장애 도메인으로 이동할 수 있습니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **장애 도메인**을 클릭합니다.

4 추가할 호스트를 클릭하여 기존 장애 도메인에 끌어다 놓습니다.

선택한 호스트가 장애 도메인에 나타납니다.

장애 도메인 외부로 호스트 이동

요구 사항에 따라 호스트를 장애 도메인 외부로 이동할 수 있습니다.

사전 요구 사항

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

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **장애 도메인**을 클릭합니다.

a 호스트를 클릭하여 장애 도메인에서 독립형 호스트 영역으로 끌어다 놓습니다.

b **이동**을 클릭하여 확인합니다.

결과

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

다음에 수행할 작업

호스트를 장애 도메인에 추가할 수 있습니다. 선택한 장애 도메인으로 호스트 이동를 참조하십시오.

장애 도메인 이름 변경

vSAN 클러스터에서 기존 장애 도메인의 이름을 변경할 수 있습니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **장애 도메인**을 클릭합니다.

   a 장애 도메인의 오른쪽에 있는 [작업] 아이콘을 클릭하고 **편집**을 선택합니다.

   b 새 장애 도메인 이름을 입력합니다.

4 **적용** 또는 **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.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **장애 도메인**을 클릭합니다.

4 장애 도메인의 오른쪽에 있는 [작업] 아이콘을 클릭하고 **삭제**를 선택합니다.

5 **삭제**를 클릭하여 확인합니다.

결과

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.

장애 도메인을 사용하여 추가 장애 허용

vSAN 클러스터의 장애 도메인은 복원력을 제공하며, 정책에 따라 장애가 발생하더라도 데이터를 사용할 수 있도록 합니다. FTT(허용되는 장애)를 1로 설정하면 개체는 장애를 허용할 수 있습니다. 그러나 클러스터에서 일시적인 장애가 발생한 후 영구적인 장애가 발생하면 데이터가 손실될 수 있습니다.

추가 장애 도메인은 개체에 대한 추가 FTT 없이도 지속성 구성 요소를 생성할 수 있는 기능을 vSAN에 제공합니다. vSAN은 계획된 장애 및 계획되지 않은 장애 동안 이 추가 구성 요소를 트리거합니다. 계획되지 않은 장애에는 네트워크 연결 끊기, 디스크 장애 및 호스트 장애가 포함됩니다. 계획된 장애에는 EMM(유지 보수 모드 시작)이 포함됩니다. 예를 들어, RAID 6 개체가 있는 6 호스트 클러스터는 호스트 장애가 발생하는 경우 지속성 구성 요소를 생성합니다.

vSAN은 구성 요소가 오프라인 상태가 되었다가 스토리지 정책에 지정된 FTT에 따라 예기치 않게 다시 온라인 상태로 전환될 경우 개체의 데이터 가용성을 보장합니다. 장애가 발생하면 장애가 있는 구성 요소의 쓰기가 지속성 구성 요소로 리디렉션됩니다. 구성 요소가 일시적인 장애로부터 복구된 후 다시 온라인 상태가 되면 지속성 구성 요소가 사라지고 구성 요소가 다시 동기화됩니다.

지속성 구성 요소가 없는 경우 클러스터에 두 번째 영구적 장애가 발생하고 미러 개체가 영향을 받는 경우 장애가 해결된 경우에도 개체 데이터가 영구적으로 손실됩니다.

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 6.7 이상은 WSFC(Windows Server 페일오버 클러스터링)를 지원하므로 WSFC 노드에서 vSAN iSCSI 대상에 액세스할 수 있습니다.

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 대상의 고가용성을 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.

vSAN iSCSI 대상 서비스 사용에 대한 자세한 내용은 iSCSI 대상 사용 가이드를 참조하십시오.

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. vSAN iSCSI 대상 서비스의 홈 개체에 대한 기본 정책으로 사용할 스토리지 정책을 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 구성원 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.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **서비스**를 클릭합니다.

2 [vSAN iSCSI 대상 서비스] 행에서 **사용**을 클릭합니다.

[vSAN iSCSI 대상 서비스 편집] 마법사가 열립니다.

3 vSAN iSCSI 대상 서비스 구성을 편집합니다.

이때 기본 네트워크, TCP 포트 및 인증 방법을 선택할 수 있습니다. 또한 vSAN 스토리지 정책을 선택할 수 있습니다.

4 **vSAN iSCSI 대상 서비스 사용** 슬라이더를 클릭하여 켠 후 **적용**을 클릭합니다.

결과

vSAN iSCSI 대상 서비스가 사용하도록 설정되었습니다.

다음에 수행할 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.

사전 요구 사항

iSCSI 대상 서비스가 사용하도록 설정되었는지 확인합니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

a vSAN에서 **iSCSI 대상 서비스**를 클릭합니다.

b [iSCSI 대상] 탭을 클릭합니다.

c **추가**를 클릭합니다. **새 iSCSI 대상** 대화상자가 표시됩니다. 대상 IQN 필드를 비워두면 IQN이 자동으로 생성됩니다.

d 대상 **별칭**을 입력합니다.

e **스토리지 정책**, **네트워크**, **TCP 포트** 및 **인증** 방법을 선택합니다.

f **I/O 소유자 위치**를 선택합니다. 이 기능은 클러스터를 확장된 클러스터로 vSAN 구성한 경우에만 사용할 수 있습니다. 이를 통해 대상에 대한 iSCSI 대상 서비스를 호스팅하기 위한 사이트 위치를 지정할 수 있습니다. 이렇게 하면 교차 사이트 iSCSI 트래픽을 방지하는 데 도움이 됩니다. 정책을 HFT>=1로 설정한 경우, 사이트 장애 발생 시 I/O 소유자 위치가 대체 사이트로 변경됩니다. 사이트 장애 복구 후 I/O 소유자 위치는 구성에 따라 자동으로 원래 I/O 소유자 위치로 다시 변경됩니다. 다음 옵션 중 하나를 선택하여 사이트 위치를 설정할 수 있습니다.

- **둘 중 하나**: 기본 사이트 또는 보조 사이트에서 iSCSI 대상 서비스를 호스팅합니다.
- **기본**: 기본 사이트에서 iSCSI 대상 서비스를 호스팅합니다.
- **보조**: 보조 사이트에서 iSCSI 대상 서비스를 호스팅합니다.

3 **확인**을 클릭합니다.

결과

iSCSI 대상이 생성되고 [vSAN iSCSI 대상] 섹션 아래에 IQN, I/O 소유자 호스트 등과 같은 정보와 함께 표시됩니다.

다음에 수행할 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.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

a vSAN에서 **iSCSI 대상 서비스**를 클릭합니다.

b [iSCSI 대상] 탭을 클릭하고 대상을 선택합니다.

c vSAN iSCSI LUN 섹션에서 **추가**를 클릭합니다. **대상에 LUN 추가** 대화상자가 표시됩니다.

d LUN의 크기를 입력합니다. iSCSI 대상 서비스에 대해 구성된 vSAN 스토리지 정책이 자동으로 할당됩니다. 각 LUN에 다른 정책을 할당할 수 있습니다.

3 **추가**를 클릭합니다.

iSCSI 대상에서 LUN 크기 조정

요구 사항에 따라 온라인 LUN의 크기를 늘릴 수 있습니다. LUN의 온라인 크기 조정은 클러스터의 모든 호스트가 vSAN 6.7 업데이트 3 이상으로 업그레이드된 경우에만 사용하도록 설정됩니다.

절차

1 vSphere Client에서 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **iSCSI 대상 서비스**를 클릭합니다.

4 **iSCSI 대상** 탭을 클릭하고 대상을 선택합니다.

5 [vSAN iSCSI LUN] 섹션에서 LUN을 선택하고 **편집**을 클릭합니다. [LUN 편집] 대화상자가 표시됩니다.

6 요구 사항에 따라 LUN의 크기를 늘립니다.

7 **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.

참고 액세스 제어를 위한 이니시에이터 그룹이 iSCSI 대상에 생성된 경우 이니시에이터 그룹 외부의 이니시에이터가 대상에 액세스할 수 없습니다. 이러한 이니시에이터의 기존 연결은 끊어지고 이니시에이터 그룹에 추가될 때까지 복구할 수 없습니다. 현재 이니시에이터 연결을 확인하고 그룹 생성 전에 모든 인증된 이니시에이터가 이니시에이터 그룹에 추가되었는지 확인해야 합니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

   a vSAN에서 **iSCSI 대상 서비스**를 클릭합니다.

   b [이니시에이터 그룹] 탭을 클릭하고 **추가**를 클릭합니다. **새 이니시에이터 그룹** 대화상자가 표시됩니다.

   c iSCSI 이니시에이터 그룹 이름을 입력합니다.

   d (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)

3 **확인** 또는 **생성**을 클릭합니다.

다음에 수행할 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.

사전 요구 사항

기존 iSCSI 이니시에이터 그룹이 있는지 확인합니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

   a vSAN에서 **iSCSI 대상 서비스**를 클릭합니다.

   b **이니시에이터 그룹** 탭을 선택합니다.

   c [액세스 가능한 대상] 섹션에서 **추가**를 클릭합니다. **액세스 가능한 대상 추가** 대화상자가 표시됩니다.

   d 사용 가능한 대상 목록에서 대상을 선택합니다.

3 **추가**를 클릭합니다.

iSCSI 대상 서비스를 사용하지 않도록 설정

vSAN iSCSI 대상 서비스를 사용하지 않도록 설정할 수 있습니다. vSAN iSCSI 대상 서비스를 사용하지 않도록 설정해도 LUN/대상이 삭제되지 않습니다. 공간을 회수하려면 vSAN iSCSI 대상 서비스를 사용하지 않도록 설정하기 전에 LUN/대상을 수동으로 삭제하십시오.

사전 요구 사항

iSCSI 대상 서비스를 사용하지 않도록 설정하면 iSCSI LUN에서 실행 중인 워크로드가 중지됩니다. 사용하지 않도록 설정하기 전에 iSCSI LUN에서 실행 중인 워크로드가 없는지 확인합니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **서비스**를 클릭합니다.

2 [vSAN iSCSI 대상 서비스] 행에서 **편집**을 클릭합니다.

   [vSAN iSCSI 대상 서비스 편집] 마법사가 열립니다.

3 **vSAN iSCSI 대상 서비스 사용** 슬라이더를 클릭하여 끈 후 **적용**을 클릭합니다.

결과

vSAN iSCSI 대상 서비스가 사용되지 않도록 설정되었습니다.

다음에 수행할 작업

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.

사전 요구 사항

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

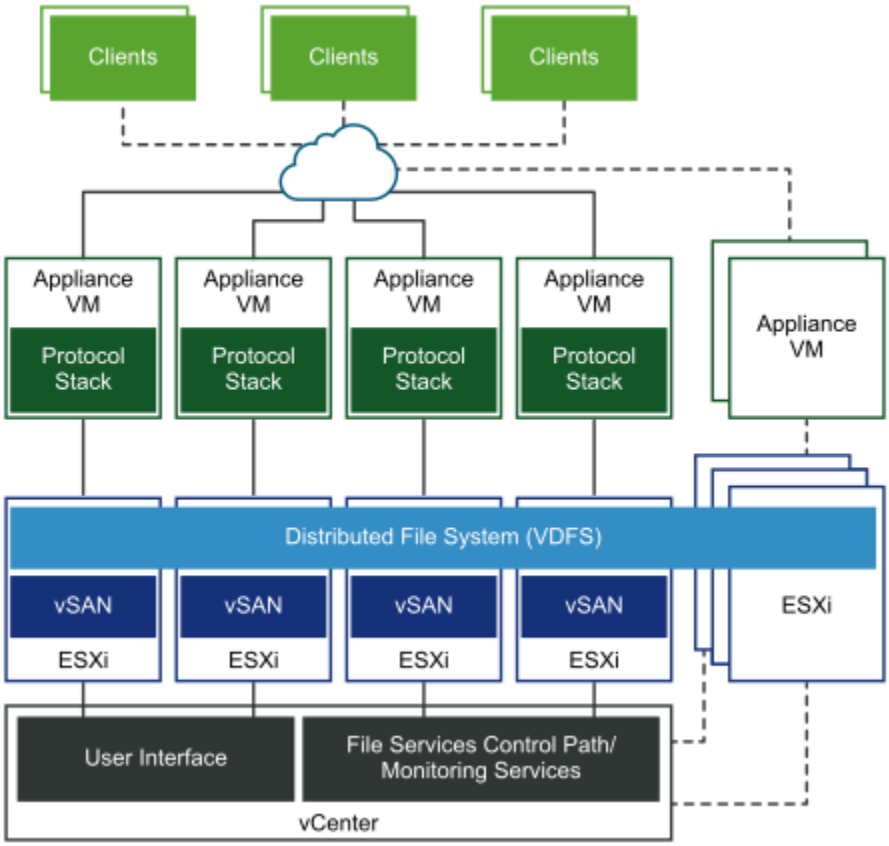
절차

1. vSAN 클러스터를 찾습니다.
2. **모니터**를 클릭하고 **가상 개체**를 선택합니다. iSCSI 대상이 페이지에 나열됩니다.
3. 대상을 선택하고 **배치 세부 정보 보기**를 클릭합니다. [물리적 배치]에 대상의 데이터 구성 요소 위치가 표시됩니다.
4. iSCSI 데이터 구성 요소에 연결된 호스트를 보려면 **호스트 배치별 그룹 구성 요소**를 클릭합니다.

vSAN 파일 서비스

vSAN 파일 서비스를 사용하여 클라이언트 워크스테이션이나 VM이 액세스할 수 있는 vSAN 데이터스토어에 파일 공유를 생성합니다. 파일 공유에 저장된 데이터는 액세스 권한이 있는 모든 디바이스에서 액세스할 수 있습니다.

vSAN 파일 서비스는 파일 공유를 제공하기 위해 vSAN 위에 있는 레이어입니다. 현재 SMB, NFSv3 및 NFSv4.1 파일 공유를 지원합니다. vSAN 파일 서비스는 vSAN 개체를 집계하여 기본 확장 파일 시스템을 제공하는 vDFS(분산 파일 시스템), 복원력 있는 파일 서버 끝점을 제공하는 스토리지 서비스 플랫폼 및 배포, 관리 및 모니터링을 위한 제어부로 구성됩니다. 파일 공유는 기존 vSAN 스토리지 정책 기반 관리에 공유별로 통합됩니다. vSAN 파일 서비스는 vSAN 클러스터에서 직접 파일 공유를 호스팅하는 기능을 제공합니다.



vSAN 파일 서비스를 구성하면 vSAN은 관리 목적으로 내부적으로 사용되는 클러스터를 위한 단일 VDFS 분산 파일 시스템을 생성합니다. FSVM(파일 서비스 VM)은 각 호스트에 배치됩니다. FSVM은 vSAN 데이터스토어에서 파일 공유를 관리합니다. 각 FSVM에는 NFS 및 SMB 서비스를 모두 제공하는 파일 서버가 포함되어 있습니다.

파일 서비스 워크플로를 사용하도록 설정하는 동안 고정 IP 주소 풀을 입력으로 제공해야 합니다. IP 주소 중 하나는 기본 IP 주소로 지정됩니다. 기본 IP 주소는 SMB 및 NFSv4.1 조회를 통해 파일 서비스 클러스터의 모든 공유에 액세스하는 데 사용할 수 있습니다. IP 풀에 제공된 모든 IP 주소에 대해 파일 서버가 시작됩니다. 파일 공유는 하나의 파일 서버에만 내보내집니다. 그러나 파일 공유는 모든 파일 서버에 균등하게 분산됩니다. 액세스 요청 관리에 도움이 되는 계산 리소스를 제공하려면 IP 주소 수가 vSAN 클러스터의 호스트 수와 같아야 합니다.

vSAN 파일 서비스는 확장된 클러스터 및 2노드 클러스터를 지원합니다. 2노드 클러스터에서는 동일한 위치 또는 사무실에 두 개의 데이터 노드 서버가 있고 원격 또는 공유 위치에 감시 호스트가 있어야 합니다.

CNS(클라우드 네이티브 스토리지) 파일 볼륨에 대한 자세한 내용은 "VMware vSphere Container Storage 플러그인" 설명서 및 "vSphere with Tanzu 구성 및 관리" 설명서를 참조하십시오.

제한 사항 및 고려 사항

vSAN 파일 서비스를 구성할 때 다음 사항을 고려하십시오.

- vSAN 7.0 U3를 사용하면 vSAN 클러스터가 유지 보수 모드로 전환될 때 파일 서비스 VM의 전원이 꺼지고 더 이상 삭제되지 않습니다.
- vSAN 7.0 Update 3는 2개 노드 구성 및 확장된 클러스터를 지원합니다.

- vSAN 7.0 Update 3는 64개 호스트 설정에서 64개 파일 서버를 지원합니다.
- vSAN 7.0 Update 3는 100개 파일 공유를 지원합니다.
- vSAN 7.0 Update 3 이전 릴리스에서 호스트가 유지 보수 모드로 전환되면 프로토콜 스택 컨테이너가 다른 FSVM으로 이동합니다. 유지 보수 모드로 전환된 호스트에 대한 FSVM이 삭제됩니다. 호스트가 유지 보수 모드를 종료하면 새 FSVM이 프로비저닝됩니다.

  vSAN 클러스터가 유지 보수 모드로 전환되면 파일 서비스 VM의 전원이 꺼진 후 삭제되고, 호스트가 유지 보수 모드를 종료하면 다시 생성됩니다.
- vSAN FSVM(파일 서비스 VM) Docker 내부 네트워크가 주의 또는 재구성 없이 고객 네트워크와 겹칠 수 있습니다.

  지정된 파일 서비스 네트워크가 Docker 내부 네트워크(172.17.0.0/16)와 겹치는 경우 알려진 충돌 문제가 발생합니다. 이로 인해 트래픽이 올바른 끝점으로 전송되지 못하는 라우팅 문제가 발생합니다.

  해결 방법으로 Docker 내부 네트워크(172.17.0.0/16)와 겹치지 않도록 다른 파일 서비스 네트워크를 지정하십시오.

파일 서비스 구성

파일 서비스를 구성하면 vSAN 데이터스토어에 파일 공유를 생성할 수 있습니다. 일반 vSAN 클러스터, vSAN 확장된 클러스터 또는 vSAN ROBO 클러스터에서 vSAN 파일 서비스를 사용하도록 설정할 수 있습니다.

사전 요구 사항

vSAN 파일 서비스를 사용하도록 설정하기 전에 다음이 구성되어 있는지 확인합니다.

vSAN 클러스터의 모든 ESXi 호스트에는 다음과 같은 최소 하드웨어 요구 사항이 있어야 합니다.

- 4코어 CPU
- 10GB 물리적 메모리

네트워크를 vSAN 파일 서비스 네트워크로 준비해야 합니다.

- 표준 스위치 기반 네트워크를 사용하는 경우 무차별 모드 및 구축된 전송이 vSAN 파일 서비스 사용 설정 프로세스의 일부로 사용되도록 설정됩니다.
- DVS 기반 네트워크를 사용하는 경우 vSAN 파일 서비스는 DVS 버전 6.6.0 이상에서 지원됩니다. DVS에서 vSAN 파일 서비스에 대한 전용 포트 그룹을 생성합니다. MacLearning 및 위조 전송은 제공된 DVS 포트 그룹에 vSAN 파일 서비스 사용 설정 프로세스의 일부로 사용하도록 설정됩니다.
- **중요** NSX 기반 네트워크를 사용하는 경우 NSX 관리 콘솔에서 제공된 네트워크 엔티티에 대해 MacLearning을 사용하도록 설정되어 있는지 확인하고 모든 호스트 및 파일 서비스 노드가 원하는 NSX-T 네트워크에 연결되어 있는지 확인합니다.

vSAN 파일 서비스 네트워크에서 고정 IP 주소를 파일 서버 IP로 할당합니다. 각 IP는 vSAN 파일 공유에 대한 단일 지점 액세스입니다.

- 최상의 성능을 위해 IP 주소 수는 vSAN 클러스터의 호스트 수와 같아야 합니다.

- 모든 고정 IP 주소는 동일한 서브넷에 있어야 합니다.
- 모든 고정 IP 주소에는 DNS 서버에서 정방향 조회 및 역방향 조회 영역의 일부여야 하는 해당 FQDN이 있습니다.

Kerberos 기반 SMB 파일 공유 또는 Kerberos 기반 NFS 파일 공유를 생성하려는 경우 다음이 필요합니다.

- Kerberos 보안을 사용하여 SMB 파일 공유 또는 NFS 파일 공유를 생성하기 위한 인증을 제공할 Microsoft AD(Active Directory) 도메인.
- (선택 사항) 모든 파일 서버 컴퓨터 개체를 생성하기 위한 Active Directory 조직 구성 단위.
- 컴퓨터 개체를 생성하고 삭제할 수 있는 충분한 권한이 있는 디렉토리 서비스의 도메인 사용자.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **서비스**를 클릭합니다.

2 [파일 서비스] 행에서 **사용**을 클릭합니다.

[파일 서비스 구성] 마법사가 열립니다.

3 [소개] 페이지에서 검사 목록을 검토하고 **다음**을 클릭합니다.

4 [파일 서비스 에이전트] 페이지에서 다음 옵션 중 하나를 선택하여 OVF 파일을 다운로드합니다.

옵션	설명
자동 방식	이 옵션을 사용하여 시스템에서 OVF를 검색하고 다운로드할 수 있습니다. **참고** ■ vCenter에서 다음 웹 사이트에 액세스하고 적절한 JSON 파일을 다운로드할 수 있도록 프록시 및 방화벽을 구성해야 합니다. https://download3.vmware.com/software/VSANOVF/FsOvfMapping.json vCenter DNS, IP 주소 및 프록시 설정 구성에 대한 자세한 내용은 "vCenter Server Appliance 구성" 을 참조하십시오. ■ OVF가 이미 다운로드되어 사용할 수 있는 경우 다음 옵션을 사용할 수 있습니다. ■ **현재 OVF 사용**: 이미 사용 가능한 OVF를 사용할 수 있습니다. ■ **최신 OVF 자동 로드**: 시스템에서 최신 OVF를 검색하고 다운로드할 수 있습니다.
수동 방식	이 옵션을 사용하여 로컬 시스템에서 이미 사용 가능한 OVF를 찾아보고 선택할 수 있습니다. **참고** 이 옵션을 선택하는 경우 다음 파일을 모두 업로드해야 합니다. ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf`

5 [도메인] 페이지에서 다음 정보를 입력하고 **다음**을 클릭합니다.

- **파일 서비스 도메인**: 도메인 이름은 최소 2자여야 합니다. 첫 번째 문자는 알파벳 또는 숫자여야 합니다. 나머지 문자에는 알파벳, 숫자, 밑줄(_), 마침표(.) 및 하이픈(-)을 사용할 수 있습니다.
- **DNS 서버**: 파일 서비스를 올바르게 구성하려면 올바른 DNS 서버를 입력해야 합니다.
- **DNS 접미사**: 파일 서비스에 사용되는 DNS 접미사를 제공합니다. 클라이언트가 이러한 파일 서버에 액세스할 수 있는 다른 모든 DNS 접미사도 포함되어야 합니다. 파일 서비스는 "app", "wiz", "com" 등과

같은 단일 레이블이 있는 DNS 도메인을 지원하지 않습니다. 파일 서비스에 지정된 도메인 이름은 thisdomain.registerdrootdnsname 형식이어야 합니다. DNS 이름과 접미사는 https://docs.microsoft.com/ko-kr/windows-server/identity/ad-ds/plan/selecting-the-forest-root-domain에 설명된 모범 사례를 따라야 합니다.

- **디렉토리 서비스**: 인증을 위해 Active Directory 도메인을 vSAN 파일 서비스로 구성합니다. Kerberos 인증을 사용하여 SMB 파일 공유 또는 NFSv4.1 파일 공유를 생성하려는 경우에는 AD 도메인을 vSAN 파일 서비스로 구성해야 합니다.

  다음 텍스트 상자에 적절한 값을 입력하여 Active Directory 도메인을 vSAN 파일 서비스로 구성합니다.

옵션	설명
AD 도메인	파일 서버가 가입된 정규화된 도메인 이름입니다.
조직 구성 단위(선택 사항)	vSAN 파일 서비스에서 생성한 컴퓨터 계정을 포함합니다. 복잡한 계층을 사용하는 조직에서 정방향 슬래시 표시로 계층 구조를 나타내어(예: organizational_unit/inner_organizational_unit) 지정된 컨테이너에 컴퓨터 계정을 생성합니다. **참고** 기본적으로 vSAN 파일 서비스는 컴퓨터 컨테이너에 컴퓨터 계정을 생성합니다.

옵션	설명
AD 사용자 이름	Active Directory 서비스를 연결하고 구성하는 데 사용되는 사용자 이름입니다. 이 사용자 이름은 도메인에서 Active Directory를 인증합니다. 도메인 사용자는 도메인 컨트롤러에서 인증받고 vSAN 파일 서비스 컴퓨터 계정, 관련 SPN 항목 및 DNS 항목(Microsoft DNS를 사용하는 경우)을 생성합니다. 모범 사례는 파일 서비스에 대한 전용 서비스 계정을 생성하는 것입니다. 컴퓨터 개체를 생성하고 삭제할 수 있는 다음과 같은 충분한 권한이 있는 디렉토리 서비스의 도메인 사용자. ■ (선택 사항) DNS 항목 추가/업데이트
암호	도메인에 있는 Active Directory의 사용자 이름에 대한 암호입니다. vSAN 파일 서비스는 암호를 사용하여 AD에서 인증을 받고 vSAN 파일 서비스 컴퓨터 계정을 생성합니다.

참고

- vSAN 파일 서비스는 다음을 지원하지 않습니다.
  - RODC(읽기 전용 도메인 컨트롤러)가 시스템 계정을 생성할 수 없기 때문에 도메인 가입을 위한 RODC를 지원하지 않습니다. 보안 모범 사례로 Active Directory 전용 조직 단위를 미리 생성해야 하며 여기에 언급된 사용자 이름이 이 조직을 제어해야 합니다.
  - 네임스페이스 분리.
  - OU(조직 구성 단위) 이름의 공백.
  - 다중 도메인 및 단일 Active Directory 포리스트 환경.
- Active Directory 사용자 이름에는 영어 문자만 지원됩니다.
- 단일 AD 도메인 구성만 지원됩니다. 그러나 파일 서버를 올바른 DNS 하위 도메인에 배치할 수 있습니다. 예를 들어, 이름이 `example.com`인 AD 도메인은 파일 서버 FQDN을 `name1.eng.example.com`으로 사용할 수 있습니다.
- 파일 서버에 대해 미리 생성된 컴퓨터 개체는 지원되지 않습니다. 여기에 제공된 사용자에게 조직 구성 단위에 대한 충분한 권한이 있는지 확인하십시오.
- Active Directory가 DNS 서버로도 사용되고 사용자에게 DNS 레코드를 업데이트할 수 있는 충분한 사용 권한이 있는 경우 vSAN 파일 서비스에서 파일 서버에 대한 DNS 레코드를 업데이트합니다. vSAN 파일 서비스에는 파일 서버에 대한 정방향 및 역방향 조회가 제대로 작동하는지 여부를 나타내는 상태 점검 기능이 있습니다. 그러나 DNS 서버로 사용되는 다른 독점 솔루션이 있는 경우 Vi 관리자는 이러한 DNS 레코드를 업데이트해야 합니다.

6 [네트워킹] 페이지에서 다음 정보를 입력하고 **다음**을 클릭합니다.

- 네트워크
- 프로토콜
- 서브넷 마스크

- 게이트웨이

7 [IP 풀] 페이지에서 IP 주소와 DNS 이름을 입력하고 **기본 IP**를 선택한 후 **다음**을 클릭합니다.

- **IP 주소**
- **DNS 이름**
- **선호도 사이트**: 이 옵션은 확장된 클러스터에서 vSAN 파일 서비스를 구성하는 경우에 사용할 수 있습니다. 이 옵션을 사용하면 **기본** 또는 **보조** 사이트의 파일 서버 배치를 구성할 수 있습니다. 이를 통해 사이트 간 트래픽 지연 시간을 줄일 수 있습니다. 기본값은 [사이트 선호도] 규칙이 파일 서버에 적용되지 않음을 나타내는 **둘 중 하나**입니다.

  참고 클러스터가 ROBO 클러스터인 경우 선호도 사이트 값이 **둘 중 하나**로 설정되어야 합니다.

  사이트 오류 이벤트에서 해당 사이트와 관련된 파일 서버가 다른 사이트로 페일오버됩니다. 파일 서버는 복구되면 선호되는 사이트로 페일백됩니다. 특정 사이트에서 더 많은 워크로드를 예상하는 경우 사이트 하나에 대해 더 많은 파일 서버를 구성합니다.

  참고 파일 서버에 SMB 파일 공유가 포함되어 있는 경우 사이트 장애가 복구된 경우에도 자동으로 페일백되지 않습니다.

IP 주소 및 DNS 이름을 구성하는 동안 다음 사항을 고려하십시오.

- 파일 서비스를 적절히 구성하려면 [IP 풀] 페이지에 입력하는 IP 주소가 고정 주소여야 하며 DNS 서버에 해당 IP 주소에 대한 레코드가 있어야 합니다. 최상의 성능을 위해 IP 주소 수는 vSAN 클러스터의 호스트 수와 같아야 합니다.
- 최대 32개의 IP 주소를 입력할 수 있습니다.
- 다음 옵션을 사용하여 IP 주소 및 DNS 서버 이름 텍스트 상자를 자동으로 채울 수 있습니다.

  자동 채우기: 이 옵션은 IP 주소 텍스트 상자에 첫 번째 IP 주소를 입력한 후에 표시됩니다. 첫 번째 행에 제공한 IP 주소의 서브넷 마스크 및 게이트웨이 주소를 기준으로 순차적 IP 주소로 나머지 필드를 자동으로 채우려면 [자동 채우기] 옵션을 클릭합니다. 자동으로 채워진 IP 주소를 편집할 수 있습니다.

  DNS 조회: [IP 주소] 텍스트 상자에 첫 번째 IP 주소를 입력한 후에 이 옵션이 표시됩니다. [DNS 조회] 옵션을 클릭하여 [IP 주소] 열의 IP 주소에 해당하는 FQDN을 자동으로 검색합니다.

  참고

  - FQDN에 대해 모든 유효한 규칙이 적용됩니다. 자세한 내용은 https://tools.ietf.org/html/rfc953 항목을 참조하십시오.
  - NetBIOS 이름이라고도 하는 FQDN의 첫 번째 부분은 15자를 초과할 수 없습니다.

  FQDN은 다음 조건에 따라 자동으로 검색됩니다.

  - [도메인] 페이지에서 올바른 DNS 서버를 입력해야 합니다.
  - IP 풀 페이지에 입력한 IP 주소는 고정 주소여야 하며 DNS 서버에는 해당 IP 주소에 대한 레코드가 있어야 합니다.

8 설정을 검토하고 **마침**을 클릭합니다.

결과

OVF가 다운로드되고 배포됩니다. 파일 서비스 도메인이 생성되고 vSAN 파일 서비스가 사용되도록 설정됩니다. 파일 서버는 vSAN 파일 서비스 구성 프로세스 중에 할당된 IP 주소로 시작됩니다.

- OVF가 다운로드되고 배포됩니다.
- 파일 서비스 도메인이 생성되고 vSAN 파일 서비스가 사용되도록 설정됩니다.
- 파일 서버는 vSAN 파일 서비스 구성 프로세스 중에 할당된 IP 주소로 시작됩니다.
- FSVM(파일 서비스 VM)은 각 호스트에 배치됩니다.

참고 FSVM은 vSAN 파일 서비스에서 관리합니다. FSVM에 대해서는 아무 작업도 수행하지 마십시오.

vSAN 파일 서비스 편집

vSAN 파일 서비스의 설정을 편집하고 다시 구성할 수 있습니다.

사전 요구 사항

- vSAN 7.0에서 7.0 업데이트 1로 업그레이드하는 경우 SMB 및 NFS Kerberos 파일 공유를 생성할 수 있습니다. 이렇게 하려면 Active Directory 도메인을 vSAN 파일 서비스로 구성해야 합니다.
- 활성 공유가 있는 경우 Active Directory 도메인을 변경하면 활성 공유에 대한 사용자 사용 권한이 중단될 수 있으므로 이러한 도메인 변경은 허용되지 않습니다.
- Active Directory 암호가 변경된 경우 Active Directory 구성 설정을 편집하고 새 암호를 제공할 수 있습니다.

참고 이 작업을 수행하면 파일 공유에 대한 진행 중 I/O에 사소한 중단이 발생할 수 있습니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **서비스**를 클릭합니다.

2 [파일 서비스] 행에서 **편집**을 클릭합니다.

[파일 서비스 구성] 마법사가 열립니다.

3 적절한 구성 변경을 수행합니다. vSAN 파일 서비스 구성을 다음과 같이 변경할 수 있습니다.

페이지	편집 가능한 필드
도메인	다음과 같은 도메인 관련 정보를 편집할 수 있습니다. ■ 파일 서비스 도메인 ■ DNS 서버 ■ DNS 접미사 ■ 디렉토리 서비스 **참고** 도메인 정보를 변경하면 시스템 중단이 발생할 수 있습니다. 모든 클라이언트가 새 URL을 사용하여 파일 공유에 다시 연결해야 할 수 있습니다.
네트워킹	다음과 같은 네트워킹 관련 정보를 편집할 수 있습니다. ■ 서브넷 마스크 ■ 게이트웨이
IP 풀	기본 IP 주소와 DNS 이름을 제외한 정적 IP 주소와 DNS 이름을 편집할 수 있습니다.

필요한 변경을 수행한 후 [검토] 페이지의 변경 내용을 검토하고 **완료**를 클릭합니다.

결과

변경 내용이 vSAN 파일 서비스 구성에 적용됩니다.

파일 공유 생성

vSAN 파일 서비스를 사용하도록 설정하면 vSAN 데이터스토어에 하나 이상의 파일 공유를 생성할 수 있습니다. vSAN 파일 서비스는 이러한 파일 공유를 ESXi의 데이터스토어로 사용하는 것을 지원하지 않습니다.

사전 요구 사항

Kerberos 보안을 사용하여 SMB 파일 공유 또는 NFSv 4.1 파일 공유를 생성하는 경우, vSAN 파일 서비스를 AD 도메인으로 구성했는지 확인합니다.

공유 이름 및 사용량에 대한 고려 사항

- ascii가 아닌 문자가 포함된 사용자 이름은 공유 데이터에 액세스하는 데 사용될 수 있습니다.
- 공유 이름은 80자를 넘을 수 없으며 영어 문자, 숫자 및 하이픈 문자를 포함할 수 있습니다. 모든 하이픈 문자의 앞과 뒤에는 숫자 또는 알파벳이 와야 합니다. 연속 하이픈은 허용되지 않습니다.
- SMB 유형 공유의 경우 파일 및 디렉토리에는 모든 유니코드 호환 문자열이 포함될 수 있습니다.
- 순수 NFSv4 유형 공유의 경우 파일 및 디렉토리에는 모든 UTF-8 호환 문자열이 포함될 수 있습니다.
- 순수 NFSv3 및 NFSv3+NFSv4 공유 파일 및 디렉토리에는 ASCII 호환 문자열만 포함될 수 있습니다.
- 이전 NFSv3에서 NFSv4만 있는 새 vSAN 파일 서비스 공유로 공유 데이터를 마이그레이션하려면 모든 파일 및 디렉토리 이름을 UTF-8 인코딩으로 변환해야 합니다. 동일한 결과를 달성하기 위한 타사 도구가 있습니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 공유**를 클릭합니다.

2 **추가**를 클릭합니다.

[파일 공유 생성] 마법사가 열립니다.

3 [일반] 페이지에서 다음 정보를 입력하고 **다음**을 클릭합니다.

- **이름**: 파일 공유의 이름을 입력합니다.
- **프로토콜**: 적절한 프로토콜을 선택합니다. vSAN 파일 서비스는 SMB 및 NFS 파일 시스템 프로토콜을 지원합니다.

  SMB 프로토콜을 선택하는 경우 **프로토콜 암호화** 옵션을 사용하여 암호화된 데이터만 허용하도록 SMB 파일 공유를 구성할 수도 있습니다.

  NFS 프로토콜을 선택하는 경우 **NFS 3**, **NFS 4** 또는 **NFS 3 및 NFS 4** 버전을 둘 다 지원하도록 파일 공유를 구성할 수 있습니다. **NFS 4** 버전을 선택하는 경우 **AUTH_SYS** 또는 **Kerberos** 보안을 설정할 수 있습니다.

  참고 NFS 프로토콜에 대한 SMB 프로토콜 및 Kerberos 보안은 vSAN 파일 서비스가 Active Directory로 구성된 경우에만 구성할 수 있습니다. 자세한 내용은 파일 서비스 구성의 내용을 참조하십시오.

- SMB 프로토콜을 사용하면 **액세스 기반 열거** 옵션을 사용하여 공유 클라이언트 사용자에게 액세스 권한이 없는 파일 및 폴더를 숨길 수 있습니다.
- **스토리지 정책**: 적절한 스토리지 정책을 선택합니다.
- **선호도 사이트**: 이 옵션은 확장된 클러스터에서 파일 공유를 생성하는 경우에 사용할 수 있습니다. 이 옵션은 선택한 사이트에 속하는 파일 서버에 파일 공유를 배치하는 데 도움이 됩니다. 파일 공유에 액세스하는 동안 낮은 지연 시간을 선호하는 경우 이 옵션을 사용합니다. 기본값은 파일 공유가 기본 설정 사이트 또는 보조 사이트에서 트래픽 양이 더 적은 사이트에 배치됨을 나타내는 **둘 중 하나**입니다.
- **스토리지 공간 할당량**: 다음 값을 설정할 수 있습니다.
  - **공유 주의 임계값**: 공유가 이 임계값에 도달하면 주의 메시지가 표시됩니다.
  - **하드 할당량 공유**: 공유가 이 임계값에 도달하면 새 블록 할당이 거부됩니다.
- **레이블**: 레이블은 파일 공유를 구성하는 데 도움이 되는 키-값 쌍입니다. 각 파일 공유에 레이블을 연결한 다음, 레이블을 기준으로 필터링할 수 있습니다. 레이블 키는 1~250자의 문자열입니다. 레이블 값은 문자열이며 레이블 값의 길이는 1k자 미만이어야 합니다. vSAN 파일 서비스는 공유당 최대 5개의 레이블을 지원합니다.

4 [네트워크 액세스 제어] 페이지는 파일 공유에 대한 액세스를 정의하는 옵션을 제공합니다. 네트워크 액세스 제어 옵션은 NFS 공유에만 사용할 수 있습니다. 다음 옵션 중 하나를 선택하고 **다음**을 클릭합니다.

- **권한 없음**: 모든 IP 주소에서 파일 공유에 액세스할 수 없게 하려면 이 옵션을 선택합니다.

- **모든 IP에서 액세스 허용**: 모든 IP 주소에서 파일 공유에 액세스할 수 있도록 하려면 이 옵션을 선택합니다.
- **네트워크 액세스 사용자 지정**: 특정 IP 주소에 대한 사용 권한을 정의하려면 이 옵션을 선택합니다. 이 옵션을 사용하면 특정 IP 주소가 파일 공유를 액세스할 수 있는지, 변경할 수 있는지, 읽을 수만 있는지를 지정할 수 있습니다. 각 IP 주소에 대해 **루트 스쿼시**를 사용하거나 사용하지 않도록 설정할 수도 있습니다. IP 주소는 다음 형식으로 입력할 수 있습니다.
  - 단일 IP 주소. 예: 123.23.23.123
  - IP 주소와 서브넷 마스크. 예: 123.23.23.0/8
  - 시작 IP 주소와 끝 IP 주소를 하이픈(-)으로 구분해서 지정한 범위. 예: 123.23.23.123-123.23.23.128
  - 모든 클라이언트를 의미하는 별표(*).

5 [검토] 페이지에서 설정을 검토하고 **마침**을 클릭합니다.

새 파일 공유가 vSAN 데이터스토어에 생성됩니다.

파일 공유 보기

vSAN 파일 공유 목록을 볼 수 있습니다.

vSAN 파일 공유 목록을 보려면 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

vSAN 파일 공유 목록이 나타납니다. 각 파일 공유에 대해 스토리지 정책, 하드 할당량, 할당량 대비 사용량, 실제 사용량 등의 정보를 볼 수 있습니다.

파일 공유 액세스

호스트 클라이언트에서 파일 공유에 액세스할 수 있습니다.

NFS 파일 공유 액세스

NFS 파일 시스템과 통신하는 운영 체제를 사용하여 호스트 클라이언트에서 [파일 공유]로 액세스할 수 있습니다. RHEL 기반 Linux 배포의 경우 NFS 4.1 지원은 커널 3.10.0-514 이상을 실행하는 RHEL 7.3 및 CentOS 7.3-1611에서 사용할 수 있습니다. Debian 기반 Linux 배포의 경우 Linux 커널 버전 4.0.0 이상에서 NFS 4.1 지원을 사용할 수 있습니다. NFSv4.1이 작동하려면 모든 NFS 클라이언트에 고유한 호스트 이름이 있어야 합니다. Linux mount 명령을 기본 IP와 함께 사용하여 vSAN 파일 공유를 클라이언트에 마운트할 수 있습니다. 예: `mount -t nfs4 -o minorversion=1,sec=sys <primary ip>:/vsanfs/<share name>`. NFSv3 지원은 RHEL 기반 및 Debian 기반 Linux 배포에 사용할 수 있습니다. Linux 마운트 명령을 사용하여 vSAN 파일 공유를 클라이언트에 마운트할 수 있습니다. 예: 마운트 `-t nfs vers=3 <nfsv3_access_point> <localmount_point>`.

예

호스트 클라이언트에서 NFS 파일 공유를 확인하기 위한 샘플 v41 명령:

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

NFS Kerberos 파일 공유 액세스

NFS Kerberos 공유에 액세스하는 Linux 클라이언트에는 유효한 Kerberos 티켓이 있어야 합니다.

호스트 클라이언트에서 NFS Kerberos 파일 공유를 확인하기 위한 샘플 v41 명령:

NFS Kerberos 공유는 다음 마운트 명령을 사용하여 마운트할 수 있습니다.

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=krb5/krb5i/krb5p <primary ip
address>:/vsanfs/TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

NFS Kerberos 공유의 소유권 변경

공유의 소유권을 변경하려면 AD 도메인 사용자 이름을 사용하여 로그인해야 합니다. 파일 서비스 구성에 제공된 AD 도메인 사용자 이름은 Kerberos 파일 공유에 대한 sudo 사용자 역할을 합니다.

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[fsadmin@ocalhost ~]# chown user1 /mnt/TestShare-0
[user1@localhost ~]# ls -l /mnt/TestShare-0
total 0
drwxr-xr-x. 1 user1 domain  users 0 Feb 19 18:35 bar
-rw-r--r--. 1 user1 domain users 0 Feb 19 18:35 foo
```

SMB 파일 공유 액세스

Windows 클라이언트에서 SMB 파일 공유에 액세스할 수 있습니다.

사전 요구 사항

Windows 클라이언트가 vSAN 파일 서비스로 구성된 Active Directory 도메인에 가입되어 있는지 확인합니다.

절차

1 다음 절차를 사용하여 SMB 파일 공유 경로를 복사합니다.

   a vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

      모든 vSAN 파일 공유 목록이 나타납니다.

   b Windows 클라이언트에서 액세스하려는 SMB 파일 공유를 선택합니다.

   c **경로 복사** > **SMB**를 클릭합니다.

      SMB 파일 공유 경로가 클립보드에 복사됩니다.

2 Windows 클라이언트에 일반 Active Directory 도메인 사용자로 로그인합니다.

3 복사한 경로를 사용하여 SMB 파일 공유에 액세스합니다.

파일 공유 편집

vSAN 파일 공유의 설정을 편집할 수 있습니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

   모든 vSAN 파일 공유 목록이 나타납니다.

2 수정하려는 파일 공유를 선택하고 **편집**을 클릭합니다.

3 [파일 공유 편집] 페이지에서 파일 공유 설정을 적절하게 변경하고 **마침**을 클릭합니다.

결과

파일 공유 설정이 업데이트됩니다.

참고 vSAN은 SMB와 NFS 간의 파일 공유 프로토콜 변경을 허용하지 않습니다.

SMB 파일 공유 관리

vSAN 파일 서비스는 vSAN 클러스터의 SMB 공유를 관리하기 위해 MMC(Microsoft Management Console)에 대한 공유 폴더 스냅인을 지원합니다.

MMC 도구를 사용하여 vSAN 파일 시스템 SMB 공유에 대해 다음 작업을 수행할 수 있습니다.

- ACL(Access Control List)을 관리합니다.
- 열린 파일을 닫습니다.
- 활성 세션을 봅니다.
- 열린 파일을 봅니다.
- 클라이언트 연결을 닫습니다.

절차

1 다음 절차를 사용하여 MMC 명령을 복사합니다.

   a vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

      모든 vSAN 파일 공유 목록이 나타납니다.

   b MMC 도구를 사용하여 Windows 클라이언트에서 관리하려는 SMB 파일 공유를 선택합니다.

   c **MMC 복사 명령**을 클릭합니다.

      MMC 명령이 클립보드에 복사됩니다.

2 Windows 클라이언트에 파일 서버 관리자로 로그인합니다. 파일 서비스를 사용하도록 설정할 때 사용자를 파일 서버 관리자로 구성할 수 있습니다. 파일 서비스 관리자는 파일 서버에 접근할 수 있는 모든 권한이 있습니다.

3 작업 표시줄의 [검색] 상자에 [실행]을 입력한 후 **실행**을 선택합니다.

4 [실행] 상자에서 복사한 MMC 명령을 실행하여 MMC 도구를 통해 SMB 공유를 액세스하고 관리합니다.

파일 공유 삭제

더 이상 필요하지 않을 때 파일 공유를 삭제할 수 있습니다. 파일 공유를 삭제하면 해당 파일 공유와 연결된 스냅샷도 모두 삭제됩니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

   모든 vSAN 파일 공유 목록이 나타납니다.

2 수정하려는 파일 공유를 선택하고 **삭제**를 클릭합니다.

3 [파일 공유 삭제] 대화상자에서 **삭제**를 클릭합니다.

vSAN 분산 파일 시스템 스냅샷

스냅샷은 데이터의 공간 효율적인 시간 기반 아카이브를 제공합니다. 파일을 실수로 삭제하는 경우 파일 또는 파일 집합에서 데이터를 검색하는 기능을 제공합니다. 파일 시스템 수준 스냅샷은 변경된 파일과 파일 변경 사항에 대한 정보를 제공합니다. 자동화된 파일 복구 서비스를 제공하며 기존 테이프 기반 백업 방법에 비해 더 효율적입니다. 스냅샷 자체가 전체 재해 복구 솔루션을 제공하지는 않지만 타사 백업 벤더에서 변경된 파일(증분 백업)을 다른 물리적 위치로 복사하는 데 사용할 수 있습니다.

vSAN 파일 서비스에는 vSAN 파일 공유의 특정 시점 이미지를 생성할 수 있는 기본 제공 기능이 있습니다. vSAN 파일 서비스를 사용하도록 설정하면 공유당 최대 32개의 스냅샷을 생성할 수 있습니다. vSAN 파일 공유 스냅샷은 특정 시점의 vSAN 파일 공유 이미지를 제공하는 파일 시스템 스냅샷입니다.

참고 vSAN 분산 파일 시스템 스냅샷은 버전 7.0 Update 2 이상에서 지원됩니다.

스냅샷 생성

vSAN 파일 서비스를 사용하도록 설정한 경우 vSAN 파일 공유의 특정 시점 이미지를 제공하는 하나 이상의 스냅샷을 생성할 수 있습니다. 파일 공유별로 최대 32개의 스냅샷을 생성할 수 있습니다.

사전 요구 사항

vSAN 파일 공유를 생성했어야 합니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

vSAN 파일 공유 목록이 나타납니다.

2 스냅샷을 생성하려는 파일 공유를 선택하고 **스냅샷** > **새 스냅샷**을 클릭합니다.

새 스냅샷 생성 대화상자가 나타납니다.

3 새 스냅샷 생성 대화상자에서 스냅샷의 이름을 입력하고 **생성**을 클릭합니다.

결과

선택한 파일 공유에 대한 특정 시점 스냅샷이 생성됩니다.

스냅샷 보기

스냅샷 생성 날짜 및 시간, 해당 크기와 같은 정보와 함께 스냅샷 목록을 볼 수 있습니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

vSAN 파일 공유 목록이 나타납니다.

2 파일 공유를 선택하고 **스냅샷**을 클릭합니다.

결과

해당 파일 공유의 스냅샷 목록이 표시됩니다. 스냅샷 생성 날짜 및 시간, 해당 크기와 같은 정보를 볼 수 있습니다.

스냅샷 삭제

스냅샷이 더 이상 필요하지 않을 때 삭제할 수 있습니다.

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **파일 서비스 공유**를 클릭합니다.

vSAN 파일 공유 목록이 나타납니다.

2 파일 공유를 선택하고 **스냅샷**을 클릭합니다.

선택한 파일 공유에 속하는 스냅샷 목록이 표시됩니다.

3 삭제할 스냅샷을 선택하고 **삭제**를 클릭합니다.

vSAN 파일 서비스 호스트의 워크로드 재조정

Skyline 상태는 vSAN 파일 서비스 인프라에 포함된 모든 호스트의 워크로드 균형 상태를 표시합니다.

호스트의 워크로드에 불균형이 있는 경우 워크로드를 재조정하여 수정할 수 있습니다.

사전 요구 사항

절차

1 vSAN 클러스터로 이동하고 **모니터링** > **vSAN** > **Skyline 상태**를 클릭합니다.

2 [Skyline 상태]에서 **파일 서비스** 를 확장한 다음, **인프라 상태**를 클릭합니다.

[인프라 상태] 탭에는 vSAN 파일 서비스 인프라에 속하는 모든 호스트의 목록이 표시됩니다. 각 호스트에 대해 워크로드 균형 상태가 표시됩니다. 호스트의 워크로드에 불균형이 있는 경우 **설명** 열에 경고가 표시됩니다.

3 **불균형 수정**을 클릭한 다음, **재조정**을 클릭하여 불균형을 수정합니다.

재조정 작업을 진행하기 전에 다음을 고려하십시오.

- 재조정하는 동안 불균형 워크로드를 사용하는 호스트의 컨테이너가 다른 호스트로 이동될 수 있습니다. 재조정 작업은 클러스터의 다른 호스트에도 영향을 줄 수 있습니다.
- 재조정 프로세스 중에 NFS 공유에서 실행되는 워크로드는 중단되지 않습니다. 그러나 이동된 컨테이너에 위치한 SMB 공유에 대한 I/O가 중단됩니다.

결과

호스트 워크로드가 조정되고 워크로드 균형 상태가 녹색으로 바뀝니다.

매핑 해제로 공간 회수

vSAN 6.7 Update 2 이상에서는 게스트가 vSAN 개체에서 생성한 VDFS(vSAN 분산 파일 시스템)의 삭제된 파일에 매핑된 스토리지 공간을 회수할 수 있도록 하는 UNMAP 명령을 지원합니다.

파일 및 스냅샷을 삭제하거나 제거하면 파일 시스템 내의 공간이 비워집니다. 사용 가능한 이 공간은 파일 시스템에서 해당 공간을 해제하거나 매핑 해제할 때까지 스토리지 디바이스에 매핑됩니다. vSAN은 사용 가능한 공간의 회수를 지원하며, 이를 매핑 해제 작업이라고도 합니다. 파일 공유 및 스냅샷을 삭제하고 파일 공유 및 스냅샷을 통합하는 것과 같은 방법으로 VDFS에서 스토리지 공간을 확보할 수 있습니다. 파일 또는 스냅샷을 삭제할 때 스토리지 공간을 매핑 해제할 수 있습니다.

매핑 해제 기능은 기본적으로 사용하지 않도록 설정됩니다. vSAN 클러스터에서 매핑 해제를 사용하도록 설정하려면 다음 RVC 명령을 사용합니다.

```
vsan.unmap_support –enable
```

vSAN 클러스터에서 매핑 해제를 사용하도록 설정하는 경우 모든 VM의 전원을 껐다 켜야 합니다. 매핑 해제 작업을 수행하려면 VM은 가상 하드웨어 버전 13 이상을 사용해야 합니다.

파일 서비스 업그레이드

파일 서비스를 업그레이드할 때 업그레이드는 롤링 방식으로 수행됩니다. 업그레이드하는 동안 업그레이드 중인 가상 시스템에서 실행 중인 파일 서버 컨테이너가 다른 가상 시스템으로 페일오버됩니다. 업그레이드하는 동안 파일 공유에 액세스할 수 있는 상태로 유지됩니다. 업그레이드하는 동안 파일 공유에 액세스하는 동안 중단이 발생할 수 있습니다.

사전 요구 사항

다음이 업그레이드되었는지 확인합니다.

- ESXi 호스트
- vCenter Server
- vSAN 디스크 형식

절차

1 vSAN 클러스터로 이동하고 **구성** > **vSAN** > **서비스**를 클릭합니다.

2 [vSAN 서비스]의 [파일 서비스] 행에서 **업그레이드 확인**을 클릭합니다.

3 [파일 서비스 업그레이드] 대화상자에서 다음 배포 옵션 중 하나를 선택하고 **업그레이드**를 클릭합니다.

옵션	작업
자동 방식	기본 옵션입니다. 이 옵션을 사용하여 시스템에서 OVF를 검색하고 다운로드할 수 있습니다. 업그레이드가 시작된 후에는 작업을 취소할 수 없습니다. **참고** vSAN에서 이 옵션을 사용하려면 인터넷에 연결해야 합니다.
수동 방식	이 옵션을 사용하여 로컬 시스템에서 이미 사용 가능한 OVF를 찾아보고 선택할 수 있습니다. 업그레이드가 시작된 후에는 작업을 취소할 수 없습니다. **참고** 이 옵션을 선택하면 다음 파일을 모두 업로드해야 합니다. ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf`

성능 모니터링

NFS 및 SMB 파일 공유의 성능을 모니터링할 수 있습니다.

사전 요구 사항

vSAN 성능 서비스가 사용하도록 설정되어 있는지 확인합니다. vSAN 성능 서비스를 처음 사용하는 경우 사용하도록 설정하라는 메시지가 표시됩니다. vSAN 성능 서비스에 대한 자세한 내용은 "vSAN 모니터링 및 문제 해결 가이드" 를 참조하십시오.

절차

1 vSAN 클러스터로 이동하고 **모니터링** > **vSAN** > **성능**을 클릭합니다.

2 **파일 공유** 탭을 클릭합니다.

3 다음 옵션 중 하나를 선택합니다.

옵션	작업
시간 범위	■ **마지막**을 선택하여 성능 보고서를 보려는 시간을 선택합니다. ■ **사용자 지정**을 선택하여 성능 보고서를 보려는 날짜 및 시간을 선택합니다. ■ 현재 설정을 시간 범위 목록에 옵션으로 추가하려면 **저장**을 선택합니다.
파일 공유	생성하려는 파일 공유를 선택하고 성능 보고서를 봅니다.

4 **결과 표시**를 클릭합니다.

결과

선택한 기간에 대한 vSAN 파일 서비스의 처리량, IOPS, 지연 시간 메트릭 처리량이 표시됩니다.

vSAN 성능 그래프에 대한 자세한 내용은 VMware 기술 자료 문서 https://kb.vmware.com/s/article/2144493을 참조하십시오.

용량 모니터링

기본 파일 공유 및 CNS 관리 파일 공유의 용량을 모니터링할 수 있습니다.

절차

1 vSAN 클러스터로 이동하고 **모니터링** > **vSAN** > **용량**을 클릭합니다.

2 **용량 사용량** 탭을 클릭합니다.

3 중복 제거 및 압축 전에 사용량 분석 섹션에서 **사용자 개체**를 확장합니다.

결과

파일 공유 용량 정보가 표시됩니다.

vSAN 용량 모니터링에 대한 자세한 내용은 "vSAN 모니터링 및 문제 해결 가이드" 를 참조하십시오.

상태 모니터링

vSAN 파일 서비스 및 파일 공유 개체 둘 다의 상태를 모니터링할 수 있습니다.

vSAN 파일 서비스 상태 보기

vSAN 파일 서비스 상태를 모니터링할 수 있습니다.

사전 요구 사항

vSAN 성능 서비스가 사용하도록 설정되어 있는지 확인합니다.

절차

1 vSAN 클러스터로 이동하고 **모니터링** > **vSAN**을 클릭합니다.

2 [Skyline 상태] 섹션에서 **파일 서비스**를 확장합니다.

3 다음 파일 서비스 상태 매개 변수를 클릭하여 상태를 확인합니다.

옵션	작업
인프라 상태	ESXi 호스트별로 파일 서비스 인프라 상태를 표시합니다. 자세한 내용을 보려면 **정보** 탭을 클릭합니다.
파일 서버 상태	파일 서버 상태를 표시합니다. 자세한 내용을 보려면 **정보** 탭을 클릭합니다.
공유 상태	파일 서비스 공유 상태를 표시합니다. 자세한 내용을 보려면 **정보** 탭을 클릭합니다.

파일 공유 개체 상태 모니터링

파일 공유 개체의 상태를 모니터링할 수 있습니다.

파일 공유 개체 상태를 보려면 vSAN 클러스터로 이동한 다음, **모니터링** > **vSAN** > **가상 개체**를 클릭합니다.

각 가상 시스템에 사용되는 디바이스의 이름, 식별자 또는 UUID, 호스트에서 미러링되는 방식 등에 대한 디바이스 정보가 [배치 세부 정보 보기] 섹션에 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.

절차

1 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 **...**를 클릭한 다음, **제거**를 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.

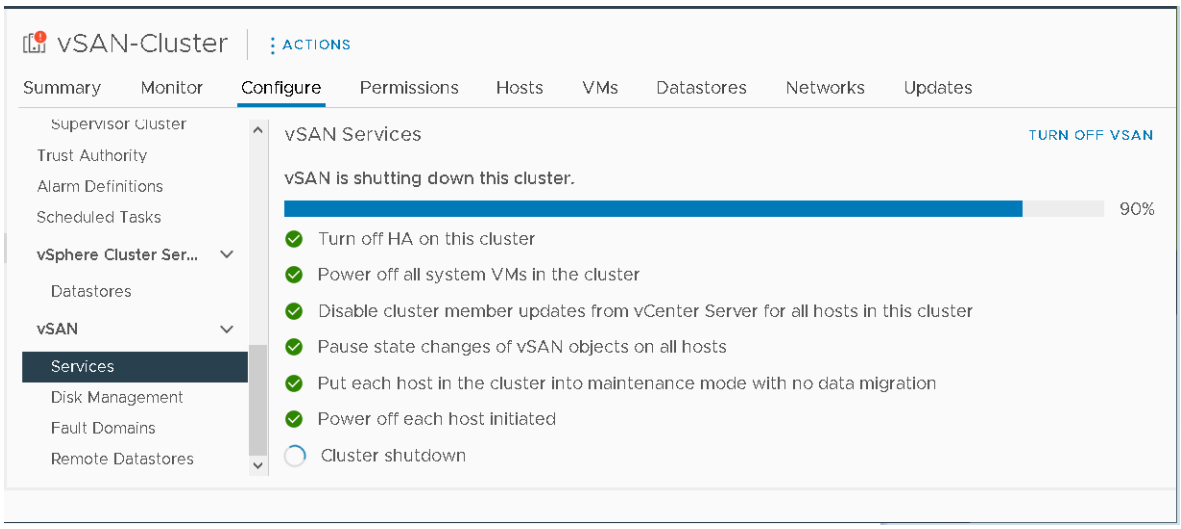
5 각 호스트에서 플래시 전용 디스크 그룹을 생성합니다.

vSAN 클러스터 종료 및 다시 시작

유지 보수 또는 문제 해결을 수행하기 위해 전체 vSAN 클러스터를 종료할 수 있습니다.

클러스터 종료 마법사를 사용하여 vSAN 클러스터를 종료합니다. 마법사는 필요한 단계를 수행하고 사용자 작업이 필요할 때 경고를 표시합니다. 필요하다면 클러스터를 수동으로 종료할 수도 있습니다.

참고 확장된 클러스터를 종료하면 감시 호스트가 활성 상태로 유지됩니다.



클러스터 종료 마법사를 사용하여 vSAN 클러스터 종료

클러스터 종료 마법사를 사용하여 유지 보수 또는 문제 해결을 위해 vSAN 클러스터를 정상적으로 종료합니다. 클러스터 종료 마법사는 vSAN 7.0 Update 3 이상 릴리스에서 사용할 수 있습니다.

참고 vSphere with Tanzu 환경이 있는 경우 구성 요소를 종료하거나 시작할 때 지정된 순서를 따라야 합니다. 자세한 내용은 "VMware Cloud Foundation 작업 가이드" 에서 "VMware Cloud Foundation 종료 및 시작"을 참조하십시오.

절차

1 vSAN 클러스터 종료를 준비합니다.

a vSAN 상태 서비스를 확인하여 클러스터가 정상인지 알아봅니다.

b vCenter Server VM, vCLS VM 및 파일 서비스 VM을 제외하고 vSAN 클러스터에 저장된 모든 VM(가상 시스템)의 전원을 끕니다. vCenter Server가 vSAN 클러스터에서 호스팅되는 경우 vCenter Server VM의 전원을 끄지 마십시오.

c HCI 메시 서버 클러스터라면 클러스터에 저장된 모든 클라이언트 VM의 전원을 끕니다. 클라이언트 클러스터의 vCenter Server VM이 이 클러스터에 저장되면 VM을 마이그레이션하거나 전원을 끕니다. 이 서버 클러스터가 종료되면 클라이언트에서 공유 데이터스토어에 액세스할 수 없습니다.

d 모든 재동기화 작업이 완료되었는지 확인합니다.

모니터 탭을 클릭하고 **vSAN** > **개체 다시 동기화**를 선택합니다.

참고 멤버 호스트가 잠금 모드에 있다면 호스트의 루트 계정을 보안 프로파일 예외 사용자 목록에 추가합니다. 자세한 내용은 "vSphere 보안" 의 "잠금 모드"를 참조하십시오.

2 vSphere Client에서 vSAN 클러스터를 마우스 오른쪽 버튼으로 클릭하고 **클러스터 종료** 메뉴를 선택합니다.

[vSAN 서비스] 페이지에서 **클러스터 종료**를 클릭할 수도 있습니다.

3 클러스터 종료 마법사에서 종료 사전 검사가 녹색 검사인지 확인합니다. 빨간색 느낌표가 있는 모든 문제를 해결합니다. **다음**을 클릭합니다.

vCenter Server Appliance가 vSAN 클러스터에 배포되면 종료 마법사에 vCenter Server 알림이 표시됩니다. 오케스트레이션 호스트의 IP 주소를 기록합니다(클러스터를 다시 시작하는 동안 필요한 경우). **다음**을 클릭합니다.

4 종료를 수행하는 이유를 입력하고 **종료**를 클릭합니다.

[vSAN 서비스] 페이지가 종료 프로세스에 대한 정보를 표시하도록 변경됩니다.

5 종료 프로세스를 모니터링합니다.

vSAN은 클러스터를 종료하고, 시스템 VM의 전원을 끄고, 호스트의 전원을 끄는 단계를 수행합니다.

vSAN 클러스터 다시 시작

유지 보수 또는 문제 해결을 위해 종료된 vSAN 클러스터를 다시 시작할 수 있습니다.

절차

1 클러스터 호스트의 전원을 켭니다.

vCenter Server가 vSAN 클러스터에서 호스팅되는 경우 vCenter Server를 다시 시작할 때까지 기다립니다.

2 vSphere Client에서 vSAN 클러스터를 마우스 오른쪽 버튼으로 클릭하고 **클러스터 다시 시작** 메뉴를 선택합니다.

[vSAN 서비스] 페이지에서 **클러스터 다시 시작**을 클릭할 수도 있습니다.

3 [클러스터 다시 시작] 대화상자에서 **다시 시작**을 클릭합니다.

[vSAN 서비스] 페이지가 변경되고 다시 시작 프로세스에 대한 정보가 표시됩니다.

4 클러스터가 다시 시작되면 vSAN 상태 서비스를 확인하고 미결 문제를 해결합니다.

vSAN 클러스터 수동 종료 및 다시 시작

유지 보수 또는 문제 해결을 수행하기 위해 전체 vSAN 클러스터를 수동으로 종료할 수 있습니다.

워크플로에 수동 종료가 필요한 경우가 아니면 클러스터 종료 마법사를 사용합니다. vSAN 클러스터를 수동으로 종료할 때 클러스터에서 vSAN을 사용하지 않도록 설정하지 마십시오.

참고 vSphere with Tanzu 환경이 있는 경우 구성 요소를 종료하거나 시작할 때 지정된 순서를 따라야 합니다. 자세한 내용은 "VMware Cloud Foundation 작업 가이드" 에서 "VMware Cloud Foundation 종료 및 시작"을 참조하십시오.

절차

1 vSAN 클러스터를 종료합니다.

a vSAN 상태 서비스를 확인하여 클러스터가 정상인지 알아봅니다.

b vCenter Server가 클러스터에서 호스팅되지 않으면 vSAN 클러스터에서 실행 중인 모든 VM(가상 시스템)의 전원을 끕니다. vCenter Server가 vSAN 클러스터에서 호스팅되는 경우 vCenter Server VM의 전원을 끄지 마십시오.

c **구성** 탭을 클릭하고 HA를 해제합니다. 그 결과 클러스터가 호스트 종료를 실패로 등록하지 않습니다.

vSphere 7.0 U1 이상에서는 vCLS 재처리 모드를 사용하도록 설정합니다. 자세한 내용은 https://kb.vmware.com/s/article/80472에서 VMware 기술 자료 문서를 참조하십시오.

d 모든 재동기화 작업이 완료되었는지 확인합니다.

모니터 탭을 클릭하고 **vSAN** > **개체 다시 동기화**를 선택합니다.

e vCenter Server가 vSAN 클러스터에서 호스팅되는 경우 vCenter Server VM의 전원을 끕니다.

vCenter Server VM을 실행하는 호스트를 기록해 둡니다. vCenter Server VM을 다시 시작해야 하는 호스트입니다.

f 클러스터의 ESXi 호스트에서 다음 명령을 실행하여 vCenter Server에서 클러스터 멤버 업데이트를 사용하지 않도록 설정합니다. 모든 호스트에서 다음 명령을 실행해야 합니다.

```
esxcfg-advcfg -s 1 /VSAN/IgnoreClusterMemberListUpdates
```

g 감시 호스트 이외의 클러스터에 있는 호스트에 로그인합니다.

h 해당 호스트에서만 다음 명령을 실행합니다. 여러 호스트에서 이 명령을 동시에 실행하는 경우 경합 조건으로 인해 예기치 않은 결과가 발생할 수 있습니다.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py prepare
```

이 명령은 다음을 반환하고 출력합니다.

클러스터 준비가 완료되었습니다.

참고

- 명령이 성공적으로 완료된 후 클러스터가 완전히 분할됩니다.
- 오류가 발생하면 오류 메시지에 따라 문제를 해결하고 vCLS 재처리 모드를 다시 사용하도록 설정하십시오.
- 클러스터에 비정상 또는 연결이 끊긴 호스트가 있는 경우 해당 호스트를 제거하고 명령을 다시 시도하십시오.

i 모든 호스트를 **작업 없음**의 유지 보수 모드로 전환합니다. vCenter Server의 전원이 꺼져 있으면 다음 명령을 사용하여 ESXi 호스트를 **작업 없음**의 유지 보수 모드로 전환하십시오.

```
esxcli system maintenanceMode set -e true -m noAction
```

모든 호스트에서 이 단계를 수행합니다.

여러 호스트에서 **작업 없음**을 사용하고 여러 호스트를 재부팅하면서 데이터를 사용할 수 없게 되는 상황을 피하려면 VMware 기술 자료 문서(https://kb.vmware.com/s/article/60424)를 참조하십시오. 기본 제공 도구를 사용하여 클러스터의 모든 호스트를 동시에 재부팅하려면 VMware 기술 자료 문서(https://kb.vmware.com/s/article/70650)를 참조하십시오.

j 모든 호스트가 유지 보수 모드로 전환되면 필요한 모든 유지 보수 작업을 수행하고 호스트의 전원을 끕니다.

2 vSAN 클러스터를 다시 시작합니다.

a ESXi 호스트의 전원을 켭니다.

ESXi가 설치된 물리적 상자의 전원을 켭니다. ESXi 호스트가 시작되고 해당 VM을 찾은 후 정상적으로 작동합니다.

호스트가 다시 시작되지 않으면 수동으로 호스트를 복구하거나 잘못된 호스트를 vSAN 클러스터 외부로 이동해야 합니다.

b 전원을 켠 후 모든 호스트가 백업되면 모든 호스트의 유지 보수 모드를 종료합니다. vCenter Server의 전원이 꺼지면 ESXi 호스트에서 다음 명령을 사용하여 유지 보수 모드를 종료합니다.

```
esxcli system maintenanceMode set -e false
```

모든 호스트에서 이 단계를 수행합니다.

c 감시 호스트 이외의 클러스터에 있는 호스트 중 하나에 로그인합니다.

d 해당 호스트에서만 다음 명령을 실행합니다. 여러 호스트에서 이 명령을 동시에 실행하는 경우 경합 조건으로 인해 예기치 않은 결과가 발생할 수 있습니다.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

이 명령은 다음을 반환하고 출력합니다.

클러스터 재부팅/전원 켜기가 완료되었습니다.

e 각 호스트에서 다음 명령을 실행하여 클러스터에서 모든 호스트를 사용할 수 있는지 확인합니다.

```
esxcli vsan cluster get
```

f 클러스터의 ESXi 호스트에서 다음 명령을 실행하여 vCenter Server에서 클러스터 멤버 업데이트를 사용하도록 설정합니다. 모든 호스트에서 다음 명령을 실행해야 합니다.

```
esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

g 전원이 꺼진 경우 vCenter Server VM을 다시 시작합니다. vCenter Server VM의 전원이 켜지고 실행될 때까지 기다립니다. vCLS 재처리 모드를 사용하지 않도록 설정하려면 https://kb.vmware.com/s/article/80472에서 VMware 기술 지원 문서를 참조하십시오.

h 각 호스트에서 다음 명령을 실행하여 모든 호스트가 vSAN 클러스터에 참여하고 있는지를 다시 확인합니다.

```
esxcli vsan cluster get
```

i vCenter Server를 통해 나머지 VM을 다시 시작합니다.

j vSAN 상태 서비스를 확인하고 남아 있는 문제를 해결합니다.

k (선택 사항) vSAN 클러스터에서 vSphere 가용성을 사용하도록 설정한 경우 vSphere 가용성을 수동으로 다시 시작하여 `vSphere HA 마스터 에이전트를 찾을 수 없습니다.` 오류가 표시되지 않도록 해야 합니다.

vSphere 가용성을 수동으로 다시 시작하려면 vSAN 클러스터를 선택하고 다음으로 이동합니다.

1 **구성** > **서비스** > **vSphere 가용성** > **편집** > **vSphere HA 사용 안 함**

2 **구성** > **서비스** > **vSphere 가용성** > **편집** > **vSphere HA 사용**

3 클러스터에 비정상이거나 연결이 끊긴 호스트가 있는 경우 vSAN 클러스터에서 호스트를 복구하거나 제거합니다. vSAN 상태 서비스가 사용 가능한 모든 호스트를 녹색 상태로 표시한 후에만 위 명령을 다시 시도하십시오.

3노드 vSAN 클러스터가 있는 경우 단일 호스트 장애 상황에서는 `reboot_helper.py recover` 명령이 작동할 수 없습니다. 관리자는 다음을 수행합니다.

a 유니캐스트 에이전트 목록에서 실패 호스트 정보를 일시적으로 제거합니다.

b 다음 명령을 실행하여 호스트를 추가합니다.

```
reboot_helper.py recover
```

다음은 vSAN 클러스터에서 호스트를 제거 및 추가하는 명령입니다.

```
#esxcli vsan cluster unicastagent remove -a <IP Address> -t node -u <NodeUuid>
```

```
#esxcli vsan cluster unicastagent add -t node -u <NodeUuid> -U true -a <IP Address> -p
12321
```

vSAN 클러스터에서 디바이스 관리

6

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.

본 장은 다음 항목을 포함합니다.

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 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 달라집니다. 하이브리드 클러스터의 경우 플래시 캐시의 비율은 사용된 용량(미러와 같은 복제본은 제외)의 10퍼센트 이상으로 하는 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.

각 디스크 그룹에는 단일 플래시 캐시 디바이스가 포함됩니다. 여러 개의 디스크 그룹을 수동으로 생성하고 각 그룹에 대해 플래시 캐시 디바이스를 할당할 수 있습니다.

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 Direct를 위한 디스크 할당

vSAN Direct를 사용하여 상태 저장 서비스가 직접 경로를 통해 vSAN 이외의 원시 로컬 스토리지에 액세스할 수 있도록 합니다.

vSAN Direct에 대해 호스트-로컬 디바이스를 할당하고 vSAN을 사용하여 해당 디바이스를 관리하고 모니터링할 수 있습니다. 각 로컬 디바이스에서 vSAN Direct는 독립 VMFS 데이터스토어를 생성하고 상태 저장 애플리케이션에서 사용할 수 있도록 합니다.

각 로컬 vSAN Direct 데이터스토어는 vSAN-D 데이터스토어로 표시됩니다.

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.

참고 vSAN 데이터 지속성 플랫폼만 vSAN Direct 스토리지를 사용할 수 있습니다. vSAN 데이터 지속성 플랫폼은 소프트웨어 기술 파트너에게 VMware Infrastructure와 통합할 수 있도록 하는 프레임워크를 제공합니다. 각 파트너는 VMware 고객이 vSAN 데이터 지속성 플랫폼의 혜택을 받을 수 있도록 자체 플러그인을 개발해야 합니다. 이 플랫폼은 위에서 실행되는 파트너 솔루션이 작동할 때까지 작동하지 않습니다. 자세한 내용은 "vSphere(Tanzu 포함) 구성 및 관리" 를 참조하십시오.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

4 **사용되지 않는 디스크 할당**을 클릭합니다.

5 호스트별로 그룹화합니다.

6 할당할 디스크를 선택합니다.

- 캐시 계층에 사용할 플래시 디바이스를 선택합니다.
- 용량 계층에 사용할 디스크를 선택합니다.

7 **생성** 또는 **확인**을 클릭하여 선택 항목을 확인합니다.

결과

새 디스크 그룹이 목록에 나타납니다.

vSAN 클러스터에 대한 스토리지 디바이스 할당

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

이 방법에서는 디바이스를 선택하여 vSAN 클러스터에 대한 디스크 그룹을 생성합니다. 각 디스크 그룹에 대해 하나의 캐시 디바이스와 하나 이상의 용량 디바이스가 필요합니다.

참고 vSAN 데이터 지속성 플랫폼만 vSAN Direct 스토리지를 사용할 수 있습니다. vSAN 데이터 지속성 플랫폼은 소프트웨어 기술 파트너에게 VMware 인프라와 통합할 수 있도록 하는 프레임워크를 제공합니다. 각 파트너는 VMware 고객이 vSAN 데이터 지속성 플랫폼의 혜택을 얻을 수 있도록 하기 위해 자체 플러그인을 개발해야 합니다. 이 플랫폼은 위에서 실행되는 파트너 솔루션이 작동할 때까지 작동하지 않습니다. 자세한 내용은 "vSphere(Tanzu 포함) 구성 및 관리" 를 참조하십시오.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

4 **사용되지 않는 디스크 할당**을 클릭합니다.

5 디스크 그룹에 추가할 디바이스를 선택합니다.

- 하이브리드 디스크 그룹의 경우 스토리지를 제공하는 각 호스트가 하나의 플래시 캐시 디바이스와 하나 이상의 HDD 용량 디바이스를 제공해야 합니다. 디스크 그룹당 하나의 캐시 디바이스만 추가할 수 있습니다.
  - 캐시로 사용할 플래시 디바이스를 선택하고 **캐시 계층에 대해 할당**을 클릭합니다.
  - 용량으로 사용할 HDD 디바이스를 선택하고 **용량 계층에 대해 할당**을 클릭합니다.
  - **생성** 또는 **확인**을 클릭합니다.
- 플래시 전용 디스크 그룹의 경우 스토리지를 제공하는 각 호스트가 하나의 플래시 캐시 디바이스와 하나 이상의 플래시 용량 디바이스를 제공해야 합니다. 디스크 그룹당 하나의 캐시 디바이스만 추가할 수 있습니다.
  - 캐시로 사용할 플래시 디바이스를 선택하고 **캐시 계층에 대해 할당**을 클릭합니다.
  - 용량으로 사용할 플래시 디바이스를 선택하고 **용량 계층에 대해 할당**을 클릭합니다.
  - **생성** 또는 **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.

vSAN Direct를 위한 디스크 할당

로컬 스토리지 디바이스를 vSAN 데이터 지속성 플랫폼에서 사용하기 위해 vSAN Direct로서 할당할 수 있습니다.

참고 vSAN 데이터 지속성 플랫폼만 vSAN Direct 스토리지를 사용할 수 있습니다. vSAN 데이터 지속성 플랫폼은 소프트웨어 기술 파트너에게 VMware Infrastructure와 통합할 수 있도록 하는 프레임워크를 제공합니다. 각 파트너는 VMware 고객이 vSAN 데이터 지속성 플랫폼의 혜택을 받을 수 있도록 자체 플러그인을 개발해야 합니다. 이 플랫폼은 위에서 실행되는 파트너 솔루션이 작동할 때까지 작동하지 않습니다. 자세한 내용은 "vSphere(Tanzu 포함) 구성 및 관리" 를 참조하십시오.

절차

1 vSphere Client에서 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

4 **사용되지 않는 디스크 할당**을 클릭합니다.

5 [사용되지 않는 디스크 할당] 마법사에서 [vSAN Direct] 탭을 선택합니다.

6 할당할 디바이스를 선택하고 **vSAN Direct에 대한 할당** 확인란을 선택합니다.

   참고 vSAN 클러스터에 대해 할당된 디바이스는 [vSAN Direct] 탭에 나타나지 않습니다.

7 **생성**을 클릭합니다.

결과

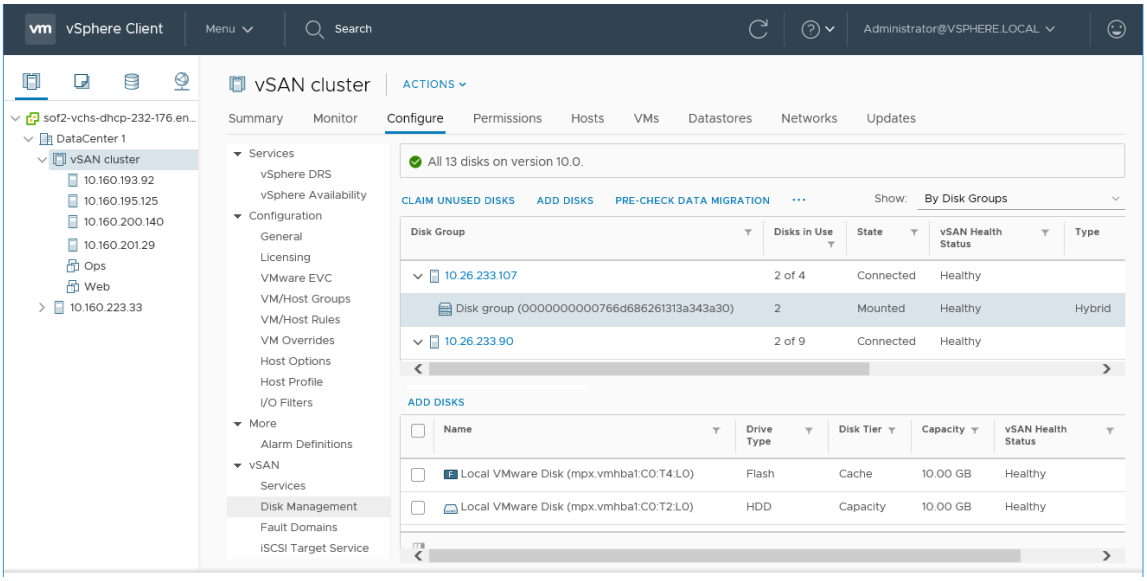
할당하는 각 디바이스에 대해 vSAN은 새 vSAN Direct 데이터스토어를 생성합니다.

다음에 수행할 작업

[데이터스토어] 탭을 클릭하여 클러스터의 vSAN Direct 데이터스토어를 표시할 수 있습니다.

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. vSAN Direct를 사용하여 할당된 디스크를 추가하거나 제거할 수도 있습니다.



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.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

4 디스크 그룹을 선택하고 **디스크 추가**를 클릭합니다.

5 추가할 디바이스를 선택하고 **추가**를 클릭합니다.

남은 데이터나 파티션 정보가 포함된 사용했던 디바이스를 추가하는 경우 장치를 먼저 정리해야 합니다. 디바이스의 파티션 정보 제거에 대한 자세한 내용은 디바이스에서 파티션 제거. `host_wipe_vsan_disks` RVC 명령을 실행하여 디바이스를 포맷할 수도 있습니다. RVC 명령에 대한 자세한 내용은 "RVC 명령 참조 가이드" 를 참조하십시오.

다음에 수행할 작업

vSAN 디스크 조정 상태 점검이 녹색인지 확인합니다. 디스크 조정 상태 점검에서 주의가 발생할 경우 작업량이 많지 않은 시간대에 수동 재조정 작업을 수행합니다. 자세한 내용은 "vSAN 모니터링 및 문제 해결" 에서 "수동 재조정"을 참조하십시오.

디스크 또는 디스크 그룹의 데이터 마이그레이션 기능 확인

데이터 마이그레이션 사전 검사를 사용하여 디스크 또는 디스크 그룹을 마우스 해제하거나 vSAN 클러스터에서 제거할 때 데이터 마이그레이션 옵션의 영향을 확인합니다.

vSAN 클러스터에서 디스크 또는 디스크 그룹을 마운트 해제하거나 제거하기 전에 데이터 마이그레이션 사전 검사를 실행합니다. 테스트 결과에는 클러스터 용량, 예측되는 상태 점검 및 규정을 준수하지 않는 개체에 미치는 영향을 확인하는 데 도움이 되는 정보가 제공됩니다. 작업이 성공하지 못하면 사전 검사는 필요한 리소스에 대한 정보를 제공합니다.

절차

1 vSAN 클러스터로 이동합니다.

2 [모니터] 탭을 클릭합니다.

3 vSAN에서 **데이터 마이그레이션 사전 검사**를 클릭합니다.

4 디스크 또는 디스크 그룹을 선택하고, 데이터 마이그레이션 옵션을 선택하고 **사전 검사**를 클릭합니다.

vSAN에서 데이터 마이그레이션 사전 검사 테스트가 실행됩니다.

5 테스트 결과를 살펴봅니다.

사전 검사 결과에는 디스크 또는 디스크 그룹을 안전하게 마운트 해제 혹은 제거 가능 여부가 표시됩니다.

- [개체 규정 준수] 및 [액세스 지원] 탭에는 데이터 마이그레이션 후 문제가 있을 수 있는 개체가 표시됩니다.
- [클러스터 용량] 탭에는 작업을 수행하기 전과 후에 데이터 마이그레이션이 vSAN 클러스터에 미치는 영향이 표시됩니다.
- [예측되는 상태] 탭에는 데이터 마이그레이션의 영향을 받을 수 있는 상태 점검이 표시됩니다.

다음에 수행할 작업

사전 검사 결과가 디바이스를 마운트 해제하거나 제거할 수 있다고 나오면 해당 옵션을 클릭하여 작업을 계속합니다.

vSAN에서 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 삭제하면 디스크 멤버 자격과 함께 디바이스에 저장된 데이터가 영구적으로 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.

사전 요구 사항

클러스터에서 제거하기 전에 디바이스 또는 디스크 그룹에 대한 데이터 마이그레이션 사전 검사를 실행합니다. 자세한 내용은 다음을 참조하십시오.

절차

1 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	a [디스크 그룹]에서 제거할 디스크 그룹을 선택하고 **...**를 클릭한 다음, **제거**를 클릭합니다. b 데이터 제거 모드를 선택합니다.
선택한 디바이스 제거	a 디스크 그룹에서 제거하려는 디바이스가 포함된 디스크 그룹을 선택합니다. b [디스크]에서 제거할 디바이스를 선택하고 **디스크 제거**를 클릭합니다. c 데이터 제거 모드를 선택합니다.

5 **예** 또는 **제거**를 클릭하여 확인합니다.

선택한 디바이스 또는 디스크 그룹에서 데이터가 제거됩니다.

디스크 그룹 다시 생성

vSAN 클러스터에서 디스크 그룹을 다시 생성하는 경우 디스크 그룹에서 기존 디스크가 제거되고 디스크 그룹이 삭제됩니다. vSAN은 동일한 디스크로 디스크 그룹을 다시 생성합니다.

vSAN 클러스터에서 디스크 그룹을 다시 생성하는 경우 vSAN에서 프로세스가 관리됩니다. vSAN은 디스크 그룹의 모든 디스크에서 데이터를 제거하고, 디스크 그룹을 제거한 다음, 동일한 디스크로 디스크 그룹을 생성합니다.

절차

1 vSphere Client에서 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

4 [디스크 그룹]에서 다시 생성할 디스크 그룹을 선택합니다.

5 **...**를 클릭한 다음 **다시 생성**을 클릭합니다.

[디스크 그룹 다시 생성] 대화 상자가 나타납니다.

6 데이터 마이그레이션 모드를 선택하고 **다시 생성**을 클릭합니다.

결과

디스크에 상주하는 모든 데이터 제거됩니다. 디스크 그룹이 클러스터에서 제거되고 다시 생성됩니다.

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.

사전 요구 사항

- 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.

절차

1. vSAN 클러스터로 이동합니다.
2. **구성** 탭을 클릭합니다.
3. vSAN에서 **디스크 관리**를 클릭합니다.
4. 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
LED 켜기	선택한 스토리지 디바이스의 로케이터 LED를 사용하도록 설정합니다. **관리** 탭에서 **스토리지 > 스토리지 디바이스**를 클릭하여 로케이터 LED를 사용하도록 설정할 수 있습니다.
LED 끄기	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.

플래시 디바이스는 패스스루 모드가 아닌 RAID 0 모드에 대해 사용되도록 설정된 경우 플래시로 인식되지 않을 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.

사전 요구 사항

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

절차

1 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 **플래시 디스크로 표시**를 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.

사전 요구 사항

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

절차

1. 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 **HDD 디스크로 표시**를 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.

사전 요구 사항

스토리지 디바이스가 공유되지 않았는지 확인합니다.

절차

1. vSAN 클러스터로 이동합니다.
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 **로컬 디스크로 표시**를 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.

절차

1 vSAN 클러스터로 이동합니다.

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 디바이스를 하나 이상 선택하고 **원격으로 표시**를 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.

사전 요구 사항

디바이스가 포맷되고 사용 중이 아닌지 확인합니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

4 디스크 그룹을 선택합니다.

5 페이지 맨 아래에서 **디스크 추가**를 클릭합니다.

6 디스크 그룹에 추가할 용량 디바이스를 선택합니다.

7 **확인** 또는 **추가**를 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.

사전 요구 사항

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

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

4 사용 가능한 디바이스 목록을 볼 호스트를 선택합니다.

5 **표시** 드롭다운 메뉴에서 **부적격**을 선택합니다.

6 목록에서 디바이스를 선택하고 **파티션 지우기**를 클릭합니다.

7 **확인**을 클릭하여 확인합니다.

이제 디바이스가 깨끗한 상태이며 그 어떤 파티션 정보도 포함되어 있지 않습니다.

vSAN 클러스터에서 공간 효율성 향상 7

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

본 장은 다음 항목을 포함합니다.

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 6.7 업데이트 1 이상은 삭제된 vSAN 개체에 매핑된 스토리지 공간을 회수할 수 있는 SCSI 매핑 해제 명령을 지원합니다.

vSAN 클러스터에 중복 제거와 압축을 사용하여 중복 데이터를 제거하고 데이터 저장에 필요한 공간의 양을 줄일 수 있습니다. 또는 압축 전용 vSAN을 사용하여 서버 성능을 손상하지 않으면서 스토리지 요구 사항을 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 각각 RAID 1에 비해 확연한 공간 절약 효과를 제공하며, 중복 제거와 압축은 추가적인 공간 절약 효과를 제공합니다.

SCSI 매핑 해제로 공간 회수

vSAN 6.7 업데이트 1 이상에서는 게스트가 vSAN 개체에서 생성한 파일 시스템의 삭제된 파일에 매핑된 스토리지 공간을 회수할 수 있도록 하는 SCSI UNMAP 명령을 지원합니다.

파일을 삭제하거나 제거하면 파일 시스템 내의 공간이 비워집니다. 사용 가능한 이 공간은 파일 시스템에서 해당 공간을 해제하거나 매핑 해제할 때까지 스토리지 디바이스에 매핑됩니다. vSAN은 사용 가능한 공간의 회수를 지원하며, 이를 매핑 해제 작업이라고도 합니다. VM 삭제 또는 마이그레이션, 스냅샷 통합 등을 수행하면 vSAN 데이터스토어의 스토리지 공간을 비울 수 있습니다.

스토리지 공간을 회수하면 호스트-플래시 I/O 처리량이 높아지고 플래시 내구성이 향상될 수 있습니다.

vSAN은 스토리지 공간을 회수하도록 게스트 운영 체제에서 직접 실행하는 SCSI UNMAP 명령도 지원합니다. vSAN은 오프라인 매핑 해제 및 인라인 매핑 해제를 지원합니다. Linux OS에서 오프라인 매핑 해제는 **`fstrim(8)`** 명령으로 수행되며 인라인 매핑 해제는 **`mount -o discard`** 명령이 사용될 때 수행됩니다. Windows OS에서는 NTFS가 기본적으로 인라인 매핑 해제를 수행합니다.

매핑 해제 기능은 기본적으로 사용하지 않도록 설정됩니다. vSAN 클러스터에서 매핑 해제를 사용하도록 설정하려면 다음 RVC 명령을 사용합니다. **`vsan.unmap_support -enable`**

vSAN 클러스터에서 매핑 해제를 사용하도록 설정하는 경우 모든 VM의 전원을 껐다 켜야 합니다. 매핑 해제 작업을 수행하려면 VM은 가상 하드웨어 버전 13 이상을 사용해야 합니다.

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. 온라인 트랜잭션 처리와 같이 중복 제거를 통해 혜택을 받지 못하는 워크로드에 대해서는 압축 전용 vSAN을 사용합니다.

중복 제거는 데이터를 캐시 계층에서 용량 계층으로 다시 쓸 때 인라인으로 발생합니다. 중복 제거 알고리즘은 고정된 블록 크기를 사용하며 각 디스크 그룹 내에 적용됩니다. 동일한 디스크 그룹 내 블록의 중복 복사본은 중복으로 제거됩니다.

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.

참고 압축 전용 vSAN은 디스크별로 적용됩니다.

중복 제거 및 압축은 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 계획 및 배포" 에서 "vSAN 사용"을 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. 이러한 작업은 자주 수행하지 마십시오. 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.

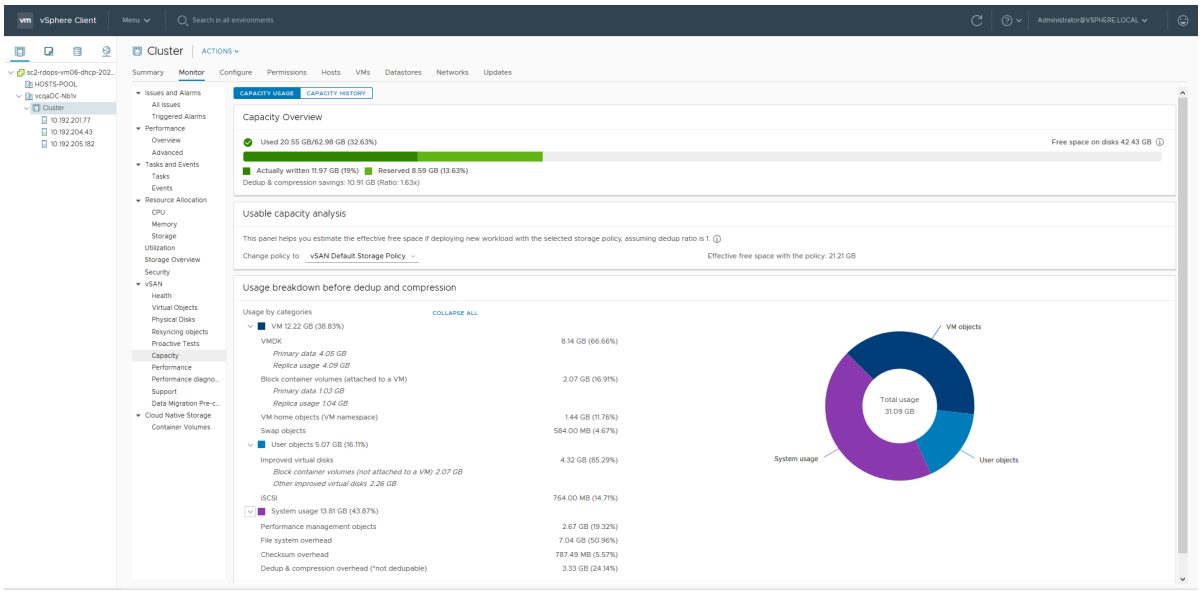
중복 제거와 압축을 사용하는 클러스터의 디스크 관리 방법

중복 제거와 압축을 사용하도록 설정된 클러스터를 관리하는 경우 다음과 같은 지침을 고려하십시오. 이러한 지침은 압축 전용 vSAN에는 적용되지 않습니다.

- 디스크 그룹에 디스크를 추가하여 늘리지 마십시오. 중복 제거 및 압축 효율성을 높이려면 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 전 사용량 분석]을 살펴보고 중복 제거와 압축 결과를 확인할 수 있습니다.



vSphere Client에서 vSAN 용량을 모니터링할 때 [중복 제거 및 압축 전 사용량 분석]을 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 라이센스를 가지고 있어야 합니다.
- 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.

절차

1. 새 플래시 전용 vSAN 클러스터로 이동합니다.
2. **구성** 탭을 클릭합니다.
3. vSAN에서 **서비스**를 선택합니다.
   a. [공간 효율성]을 클릭하여 편집합니다.
   b. 공간 효율성 옵션 중에서 중복 제거 및 압축 또는 압축 전용을 선택합니다.
   c. (선택 사항) **감소된 이중화 허용**을 선택합니다. 중복 제거와 압축이 사용되도록 설정되어 있는 동안에는 필요에 따라 vSAN이 VM의 보호 수준을 줄입니다. 자세한 내용은 vSAN 클러스터에 대한 VM 이중화 감소 항목을 참조하십시오.

4 클러스터 구성을 완료합니다.

기존 vSAN 클러스터에서 중복 제거와 압축 사용

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

사전 요구 사항

플래시 전용 vSAN 클러스터를 생성합니다.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **서비스**를 선택합니다.

   a [공간 효율성]을 편집하려면 클릭합니다.

   b 공간 효율성 옵션 중에서 중복 제거 및 압축 또는 압축 전용을 선택합니다.

   c (선택 사항) **감소된 이중화 허용**을 선택합니다. 중복 제거와 압축이 사용되도록 설정되어 있는 동안에는 필요에 따라 vSAN이 VM의 보호 수준을 줄입니다. 자세한 내용은 vSAN 클러스터에 대한 VM 이중화 감소 항목을 참조하십시오.

4 **적용**을 클릭하여 구성 변경 내용을 저장합니다.

결과

중복 제거와 압축을 사용하도록 설정하는 동안 vSAN이 클러스터의 각 디스크 그룹에서 온디스크 형식을 업데이트합니다. 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.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

   a vSAN에서 **서비스**를 선택합니다.

   b **편집**을 클릭합니다.

   c 중복 제거와 압축을 사용하지 않도록 설정합니다.

   d (선택 사항) **감소된 이중화 허용**을 선택합니다. vSAN은 중복 제거와 압축을 사용하지 않도록 설정하는 동안 필요에 따라 VM의 보호 수준을 낮춥니다. vSAN 클러스터에 대한 VM 이중화 감소를 참조하십시오.

3 **적용** 또는 **확인**을 클릭하여 구성 변경 내용을 저장합니다.

결과

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 사용하도록 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 사용하도록 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 **허용되는 장애** 값을 1로 설정하여 VM을 보호할 때 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	허용되는 장애	데이터 크기	필요 용량
RAID 1(미러링)	1	100GB	200GB
RAID 5 또는 RAID 6(이레이저 코딩) 및 장애 도메인 4개	1	100GB	133GB
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 방법**을 **RAID-5/6(이레이저 코딩) - 용량**으로 설정하고 **허용되는 장애**를 1로 설정합니다. RAID 6를 사용하려면 **장애 허용 방법**을 **RAID-5/6(이레이저 코딩) - 용량**으로 설정하고 **허용되는 장애**를 2로 설정합니다. RAID 5 또는 RAID 6 이레이저 코딩을 사용하면 **허용되는 장애** 값을 3으로 설정할 수 없습니다.

RAID 1을 설정하려면 **장애 허용 방법**을 **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.

참고 vSAN 확장된 클러스터에서 **RAID-5/6(이레이저 코딩) - 용량**의 **장애 허용 방법**은 **사이트 재해 허용**에만 적용됩니다.

정책 구성에 대한 자세한 내용은 장 4 vSAN 정책 사용을 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 라이이센스를 가지고 있어야 합니다.
- vSAN 클러스터에 중복 제거와 압축을 사용하도록 설정하면 공간을 추가적으로 절약할 수 있습니다.

vSAN 클러스터에서 암호화 사용

8

전송 중 데이터는 vSAN 클러스터에서 암호화하고 미사용 데이터는 vSAN 데이터스토어에 암호화할 수 있습니다.

vSAN은 vSAN 클러스터의 호스트 간에 전송 중인 데이터를 암호화할 수 있습니다. 전송 중 데이터 암호화는 vSAN 클러스터 주위로 데이터가 이동될 때 데이터를 보호합니다.

vSAN은 vSAN 데이터스토어에 있는 미사용 데이터를 암호화할 수 있습니다. 미사용 데이터 암호화 기능은 디바이스가 클러스터에서 제거되는 경우 스토리지 디바이스의 데이터를 보호합니다.

본 장은 다음 항목을 포함합니다.

- vSAN 전송 중 데이터 암호화
- vSAN 미사용 데이터 암호화

vSAN 전송 중 데이터 암호화

vSAN은 vSAN 클러스터의 호스트 간을 이동할 때 전송 중인 데이터를 암호화할 수 있습니다.

vSAN은 클러스터의 호스트 간에 전송 중인 데이터를 암호화할 수 있습니다. 전송 중 데이터 암호화를 사용하도록 설정하면 vSAN은 호스트 간의 모든 데이터 및 메타데이터 트래픽을 암호화합니다.

vSAN 전송 중 데이터 암호화는 다음과 같은 특성이 있습니다.

- vSAN은 전송 중인 데이터에 대해 AES-256비트 암호화를 사용합니다.
- vSAN 전송 중 데이터 암호화는 미사용 데이터 암호화와 관련이 없습니다. 각 항목을 개별적으로 사용하거나 사용하지 않도록 설정할 수 있습니다.
- 전달 보안은 vSAN 전송 중 데이터 암호화에 적용됩니다.
- 데이터 호스트와 감시 호스트 간의 트래픽이 암호화됩니다.
- VDFS 프록시와 VDFS 서버 간의 파일 서비스 데이터 트래픽이 암호화됩니다.
- vSAN 파일 서비스 호스트 간 연결이 암호화됩니다.

vSAN은 호스트 간에 동적으로 생성되고 공유되는 대칭 키를 사용합니다. 호스트는 연결을 설정할 때 암호화 키를 동적으로 생성하고 키를 사용하여 호스트 간의 모든 트래픽을 암호화합니다. 전송 중 데이터 암호화를 수행하는 데는 키 관리 서버가 필요하지 않습니다.

각 호스트는 클러스터에 가입할 때 인증되며 신뢰할 수 있는 호스트에 대한 연결만 허용됩니다. 호스트가 클러스터에서 제거되면 인증 인증서가 제거됩니다.

vSAN 전송 중 데이터 암호화는 클러스터 전체 설정입니다. 이 기능을 사용하도록 설정하면 모든 데이터 및 메타데이터 트래픽은 호스트 간에 전송될 때 암호화됩니다.

vSAN 클러스터에서 전송 중 데이터 암호화 사용

vSAN 클러스터의 구성 매개 변수를 편집하여 전송 중 데이터 암호화를 사용하도록 설정할 수 있습니다.

절차

1 기존 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **서비스**를 선택하고 전송 중 데이터 암호화 **편집** 버튼을 클릭합니다.

4 **전송 중 데이터 암호화**를 클릭하여 사용하도록 설정하고 키 재생성 간격을 선택합니다.

5 **적용**을 클릭합니다.

결과

vSAN 클러스터에서 전송 중 데이터 암호화 기능이 사용되도록 설정됩니다. vSAN은 클러스터의 모든 호스트 및 파일 서비스 호스트 간 연결을 통해 이동하는 모든 데이터를 암호화합니다.

vSAN 미사용 데이터 암호화

vSAN은 vSAN 데이터스토어에 있는 미사용 데이터를 암호화할 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 제거되는 경우 스토리지 디바이스의 데이터를 보호합니다.

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

미사용 데이터 암호화에는 외부 KMS(키 관리 서버) 또는 vSphere Native Key Provider가 필요합니다. vSphere 암호화에 대한 자세한 내용은 "vSphere 보안" 을 참조하십시오.

외부 KMS(키 관리 서버), vCenter Server 시스템 및 ESXi 호스트를 사용하여 vSAN 클러스터의 데이터를 암호화할 수 있습니다. 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.

미사용 데이터 암호화 작동 방식

미사용 데이터 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. 암호를 지정하여 임의의 키를 암호화할 수 있습니다.

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.

암호화 키 지속성

vSAN 7.0 Update 3 이상에서는 키 서버가 일시적으로 오프라인 상태이거나 사용할 수 없을 때도 미사용 데이터 암호화는 계속 작동합니다. 키 지속성을 사용하도록 설정하면 ESXi 호스트가 재부팅 후에도 암호화 키를 유지할 수 있습니다.

각 ESXi 호스트는 처음에 암호화 키를 가져와서 해당 키 캐시에 유지합니다. ESXi 호스트에 TPM(신뢰할 수 있는 플랫폼 모듈)이 있으면 재부팅 시 암호화 키가 TPM에 유지됩니다. 호스트는 암호화 키를 요청할 필요가 없습니다. 또한 키가 TPM에 유지되므로 키 서버를 사용할 수 없을 때도 암호화 작업은 계속할 수 있습니다.

다음 명령을 사용하여 클러스터 호스트에서 키 지속성을 사용하도록 설정합니다.

```
esxcli system settings encryption set --mode=TPM
```

```
esxcli system security keypersistence enable
```

암호화 키 지속성에 대한 자세한 내용은 "vSphere 보안" 의 "키 지속성 개요"를 참조하십시오.

vSphere Native Key Provider 사용

vSAN 7.0 Update 2는 vSphere Native Key Provider를 지원합니다. 작업 환경이 vSphere Native Key Provider에 맞게 설정된 경우 vSAN 클러스터에서 이 키 제공자를 사용하여 가상 시스템을 암호화할 수 있습니다. 자세한 내용은 "vSphere 보안" 에서 "vSphere Native Key Provider 구성 및 관리"를 참조하십시오.

vSphere Native Key Provider를 사용할 경우 외부 KMS(키 관리 서버)가 필요하지 않습니다. vCenter Server는 키 암호화 키를 생성하고 ESXi 호스트에 푸시합니다. 그러면 ESXi 호스트는 데이터 암호화 키를 생성합니다.

참고 vSphere Native Key Provider를 사용하는 경우 재구성 작업이 원활하게 실행되도록 네이티브 키 제공자를 백업해야 합니다.

vSphere Native Key Provider는 기존 키 서버 인프라와 함께 사용할 수 있습니다.

미사용 데이터 암호화에 대한 설계 고려 사항

미사용 데이터 암호화를 사용하는 경우에 다음과 같은 지침을 고려하십시오.

- 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 호스트는 고객 데이터, vSAN 개체의 크기 및 UUID, 구성 요소와 같은 메타데이터만 저장하지 않습니다.

  참고 감시 호스트가 다른 클러스터에서 실행 중인 장치라면 해당 호스트에 저장된 메타데이터를 암호화할 수 있습니다. 감시 호스트가 포함된 클러스터에서 미사용 데이터 암호화를 사용하도록 설정합니다.

- 코어 덤프에 대한 정책을 설정합니다. 코어 덤프는 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 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.

표준 키 제공자 설정

표준 키 제공자를 사용하여 vSAN 데이터스토어를 암호화하는 키를 배포합니다.

vSAN 데이터스토어를 암호화하려면 먼저 암호화를 지원하도록 표준 키 제공자를 설정해야 합니다. 그러기 위해서는 KMS를 vCenter Server에 추가하고 KMS와의 신뢰 관계를 설정해야 합니다. vCenter Server는 키 제공자에서 암호화 키를 프로비저닝합니다.

KMS는 KMIP(Key Management Interoperability Protocol) 1.1 표준을 지원해야 합니다. 자세한 내용은 "vSphere 호환성 Matrices" 를 참조하십시오.

vCenter Server에 KMS 추가

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

첫 번째 KMS 인스턴스를 추가하면 vCenter Server에서 표준 키 제공자를 생성합니다. 둘 이상의 vCenter Server에 키 제공자를 구성할 때는 동일한 키 제공자 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 키 제공자를 기본값으로 설정하라는 메시지가 표시됩니다. 나중에 기본 설정을 명시적으로 변경할 수 있습니다.
- vCenter Server에서 첫 번째 키 제공자를 만든 후에는 동일한 벤더의 KMS 인스턴스를 키 제공자에 추가하고 모든 KMS 인스턴스가 키를 서로 동기화하도록 구성할 수 있습니다. 해당 KMS 벤더가 제공하는 설명서의 방법을 따르십시오.
- KMS 인스턴스 하나만으로 키 제공자를 설정해도 됩니다.
- 환경에서 여러 벤더의 KMS 솔루션을 지원하는 경우 여러 키 제공자를 추가할 수 있습니다.

사전 요구 사항

- 키 관리 서버가 "vSphere 호환성 매트릭스" 에 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.

절차

1. vCenter Server에 로그인합니다.
2. 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.
3. **구성**을 클릭하고 보안에서 **키 제공자**를 클릭합니다.
4. **표준 키 제공자 추가**를 클릭하여 키 제공자 정보를 입력하고 **키 제공자 추가**를 클릭합니다.

   KMS 추가를 클릭하여 더 많은 키 관리 서버를 추가할 수 있습니다.
5. **신뢰**를 클릭합니다.

   vCenter Server는 키 제공자를 추가하고 상태를 연결됨으로 표시합니다.

인증서를 교환하여 표준 키 제공자 신뢰할 수 있는 연결 설정

표준 키 제공자를 vCenter Server 시스템에 추가한 후 신뢰할 수 있는 연결을 설정할 수 있습니다. 정확한 프로세스는 키 제공자가 수락하는 인증서와 회사 정책에 따라 달라집니다.

사전 요구 사항

표준 키 제공자를 추가합니다.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **키 관리 서버**를 선택합니다.

3 키 제공자를 선택합니다.

키 제공자에 대한 KMS가 표시됩니다.

4 KMS를 선택합니다.

5 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

6 서버에 적합한 옵션을 선택하고 단계를 수행합니다.

옵션	자세한 내용은
vCenter Server 루트 CA 인증서	루트 CA 인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.
vCenter Server 인증서	인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.
인증서 및 개인 키 업로드	인증서 및 개인 키 업로드 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.
새 인증서 서명 요청	새 인증서 서명 요청 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.

루트 CA 인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정

일부 KMS(키 관리 서버) 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.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **키 관리 서버**를 선택합니다.

3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

4 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

5 **vCenter 루트 CA 인증서**를 선택하고 **다음**을 클릭합니다.

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

6 인증서를 클립보드에 복사하거나 인증서를 파일로 다운로드합니다.

7 KMS 벤더의 지침을 따라 인증서를 해당 시스템에 업로드합니다.

참고 일부 KMS 벤더는 업로드한 루트 인증서를 사용하기 위해 해당 KMS 벤더에서 KMS를 재시작해야 합니다.

다음에 수행할 작업

인증서 교체를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료의 내용을 참조하십시오.

인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정

일부 KMS(키 관리 서버) 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.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **키 관리 서버**를 선택합니다.

3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

4 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

5 **vCenter 인증서** 를 선택하고 **다음**을 클릭합니다.

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

참고 기존 인증서를 교체하려는 경우가 아니라면 새 인증서를 생성하지 마십시오.

6 인증서를 클립보드에 복사하거나 파일로 다운로드합니다.

7 KMS 벤더의 지침을 따라 인증서를 KMS에 업로드합니다.

다음에 수행할 작업

신뢰 관계를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료의 내용을 참조하십시오.

새 인증서 서명 요청 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정

일부 KMS(키 관리 서버) 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.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **키 관리 서버**를 선택합니다.

3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

4 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

5 **새 CSR(인증서 서명 요청)**을 선택하고 **다음**을 클릭합니다.

6 대화상자에서 텍스트 상자의 전체 인증서를 클립보드에 복사하거나 파일로 다운로드합니다.

명시적으로 CSR을 생성하려는 경우에만 대화 상자에서 **새 CSR 생성** 버튼을 사용합니다.

7 KMS 벤더의 지침을 따라 CSR을 제출합니다.

8 KMS 벤더에서 서명된 인증서를 수신하는 경우 **키 제공자**를 다시 클릭하고 키 제공자를 선택하고 **신뢰 설정** 드롭다운 메뉴에서 **서명된 CSR 인증서 업로드**를 선택합니다.

9 서명된 인증서를 하단 텍스트 상자에 붙여넣거나 **파일 업로드**를 클릭하여 파일을 업로드한 후 **업로드**를 클릭합니다.

다음에 수행할 작업

신뢰 관계를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료를 참조하십시오.

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

일부 KMS(키 관리 서버) 벤더의 경우 사용자가 KMS 서버 인증서 및 개인 키를 vCenter Server 시스템에 업로드해야 합니다.

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

사전 요구 사항

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

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **키 관리 서버**를 선택합니다.

3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

4 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

5 **KMS 인증서 및 개인 키**를 선택하고 **다음**을 클릭합니다.

6 KMS 벤더에서 수신한 인증서를 상단 텍스트 상자에 붙여 넣거나 **파일 업로드**를 클릭하여 인증서 파일을 업로드합니다.

7 키 파일을 하단 텍스트 상자에 붙여 넣거나 **파일 업로드**를 클릭하여 키 파일을 업로드합니다.

8 **신뢰 설정**을 클릭합니다.

다음에 수행할 작업

신뢰 관계를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료의 내용을 참조하십시오.

기본 키 제공자 설정

첫 번째 키 제공자를 기본값으로 설정하지 않거나 환경에서 여러 키 제공자를 사용하여 기본 키 제공자를 제거하는 경우 기본 키 제공자를 설정해야 합니다.

사전 요구 사항

키 제공자 탭의 [연결 상태]에 [연결됨] 및 녹색 확인 표시가 있는지 확인하는 것이 모범 사례입니다.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **키 관리 서버**를 선택합니다.

3 키 제공자를 선택합니다.

4 **기본값으로 설정**을 클릭합니다.

[확인] 대화상자가 나타납니다.

5 **기본값으로 설정**을 클릭합니다.

키 제공자는 현재 기본값으로 표시됩니다.

표준 키 제공자에 대한 신뢰 설정 완료

KMS를 신뢰하도록 **표준 키 제공자 추가** 대화상자가 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 업로드** 옵션을 사용하여 인증서를 명시적으로 신뢰합니다.
- **vCenter가 KMS를 신뢰하도록 만들기** 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.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **키 관리 서버**를 선택합니다.

3 신뢰 연결을 설정할 KMS 인스턴스를 선택합니다.

4 KMS를 선택합니다.

5 **신뢰 설정** 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.

옵션	작업
vCenter가 KMS를 신뢰하도록 만들기	표시되는 대화상자에서 **신뢰**를 클릭합니다.
KMS 인증서 업로드	a 표시되는 대화상자에서 인증서에 붙여 넣거나 **파일 업로드**를 클릭하고 인증서 파일을 찾습니다. b **업로드**를 클릭합니다.

새 vSAN 클러스터에서 미사용 데이터 암호화 사용

새 vSAN 클러스터를 구성할 때 미사용 데이터 암호화를 사용하도록 설정할 수 있습니다.

사전 요구 사항

- 필요한 권한:
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageEncryptionPolicy**
  - **Cryptographer.ManageKMS**
  - **Cryptographer.ManageKeys**
- 표준 키 제공자를 구성하고 vCenter Server와 KMS 사이에 신뢰할 수 있는 연결이 설정되어 있어야 합니다.

절차

1 기존 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **서비스**를 선택하고 암호화 **편집** 버튼을 클릭합니다.

4 **vSAN 서비스** 대화 상자에서 **암호화**를 사용하도록 설정하고 KMS 클러스터 또는 키 제공자를 선택합니다.

참고 **잔여 데이터 지우기** 확인란을 사용하여 vSAN 암호화를 사용하도록 설정하기 전에 디바이스에서 잔여 데이터를 지웁니다. VM 데이터가 포함된 클러스터를 암호화할 때 스토리지 디바이스에서 기존 데이터를 초기화하지 않으려면 이 확인란을 선택 취소해야 합니다. 이렇게 하면 vSAN 암호화를 사용하도록 설정한 후 암호화되지 않은 데이터가 디바이스에 더 이상 존재하지 않게 됩니다. 스토리지 디바이스에 VM 데이터가 없는 새 설치에는 이 설정이 필요하지 않습니다.

5 클러스터 구성을 완료합니다.

결과

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

새로운 미사용 데이터 암호화 키 생성

키가 만료되거나 손상된 경우에 미사용 데이터에 대해 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 재 포맷이 필요합니다.

사전 요구 사항

- 필요한 권한:
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageKeys**
- 표준 키 제공자를 설정하고 vCenter Server와 KMS 사이에 신뢰할 수 있는 연결이 설정되어 있어야 합니다.

절차

1. vSAN 호스트 클러스터로 이동합니다.
2. **구성** 탭을 클릭합니다.
3. vSAN에서 **서비스**를 선택합니다.
4. **새 암호화 키 생성**을 클릭합니다.
5. 새 KEK를 생성하려면 **적용**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 위험할 수 있습니다.

기존 vSAN 클러스터에서 미사용 데이터 암호화 사용

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

사전 요구 사항

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

절차

1 vSAN 호스트 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **서비스**를 선택합니다.

4 암호화 **편집** 버튼을 클릭합니다.

5 vSAN 서비스 대화 상자에서 **암호화**를 사용하도록 설정하고 KMS 클러스터 또는 키 제공자를 선택합니다.

6 (선택 사항) 클러스터의 스토리지 디바이스에 중요 데이터가 포함된 경우, **잔여 데이터 지우기**를 선택합니다.

이 설정은 암호화하는 동안 스토리지 디바이스의 기존 데이터를 지우도록 vSAN에 지시합니다. 이 옵션을 선택하면 각 디스크를 처리하는 데 걸리는 시간이 늘어날 수 있으므로 디스크에 불필요한 데이터가 있는 경우가 아니면 선택하지 마십시오.

7 **적용**을 클릭합니다.

결과

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

vSAN 암호화 및 코어 덤프

vSAN 클러스터에서 미사용 데이터 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 다르면 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 보호되는지 확인합니다. vCenter Server 시스템에 대한 코어 덤프를 해제하는 것을 고려할 수도 있습니다. 로그 파일의 기타 정보를 통해 문제를 파악할 수도 있습니다.

암호화된 vSAN 데이터스토어의 ESXi 호스트에 대해 vm-support 패키지 수집

vSAN 클러스터에서 미사용 데이터 암호화가 사용되도록 설정되면 `vm-support` 패키지의 모든 코어 덤프가 암호화됩니다. 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.

사전 요구 사항

vSAN 데이터스토어에 대해 미사용 데이터 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.

절차

1. vSphere 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 패턴입니다.

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/core`에 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-file*은 디렉토리의 최상위 수준에 있는 인시던트 키 파일입니다.

*encryptedZdump*는 암호화된 코어 덤프 파일의 이름입니다.

*decryptedZdump*는 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-util`의 다른 기능에 대한 자세한 내용은 명령줄 도움말을 참조하십시오.

참고 `crypto-util`은 고급 사용자를 위한 기능입니다.

사전 요구 사항

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

절차

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	`crypto-util envelope describe vmmcores.ve`
zdump 파일	`crypto-util envelope describe --offset 4096 zdumpFile`

3 코어 덤프 유형에 따라 코어 덤프를 암호 해독합니다.

옵션	설명
코어 덤프 모니터링	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump 파일	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

vSAN 클러스터 업그레이드

9

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 업그레이드를 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 업그레이드를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- vSAN을 업그레이드하기 전
- vCenter Server 업그레이드
- ESXi 호스트 업그레이드
- vSAN 디스크 형식 정보
- vSAN 개체 형식 정보
- vSAN 클러스터 업그레이드 확인
- RVC 업그레이드 명령 옵션 사용
- vSphere Lifecycle Manager에 대한 vSAN 빌드 권장 사항

vSAN을 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 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	새 버전의 vSAN에서 사용하려는 소프트웨어 및 하드웨어 구성 요소, 드라이버, 펌웨어 및 스토리지 I/O 컨트롤러를 지원하는지 확인합니다. 지원되는 항목은 VMware 호환성 가이드 웹 사이트(http://www.vmware.com/resources/compatibility/search.php)에 나열되어 있습니다.
vSAN 버전	최신 버전의 vSAN를 사용하고 있는지 확인합니다. 베타 버전에서는 새 vSAN으로 업그레이드할 수 없습니다. 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. 가장 큰 디스크 그룹의 사용된 용량과 동일한 사용 가능한 공간이 없고 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 클러스터 용량이 자동으로 줄어듭니다. 멤버 호스트가 더 이상 클러스터에 스토리지를 제공하지 않고 호스트의 용량을 데이터에 사용할 수 없습니다. 다양한 제거 모드에 대한 자세한 내용은 "VMware vSAN 관리" 설명서를 참조하십시오.

표 9-1. 업그레이드 사전 요구 사항 (계속)

업그레이드 전제 조건	설명
vSAN 호스트	vSAN 호스트를 유지 보수 모드로 설정했고 **데이터 액세스 지원 보장** 또는 **모든 데이터 제거** 옵션을 선택했는지 확인합니다. 업그레이드 프로세스를 자동화하고 테스트하기 위해 vSphere Lifecycle Manager를 사용할 수 있습니다. 하지만 vSphere Lifecycle Manager를 사용하여 vSAN을 업그레이드하는 경우에는 기본 제거 모드가 **데이터 액세스 보장**입니다. **데이터 액세스 지원 보장** 모드를 사용하면 데이터가 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 "VMware vSAN 관리" 설명서를 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 자화 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 사용해야 하며 부팅 디바이스의 크기가 16GB 이상이어야 합니다.
- 하드웨어가 vSAN에 대한 요구 사항을 충족하도록 하려면 "vSAN 계획 및 배포" 를 참조하십시오.

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

2개 호스트 클러스터 또는 확장된 클러스터의 감시 호스트 업그레이드

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

데이터 호스트를 업그레이드하기 전에 감시 호스트를 업그레이드합니다.

vSphere Lifecycle 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 Lifecycle 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.

ESXi 7.0으로의 업그레이드에 대한 지원 세부 정보와 수준은 업그레이드되는 호스트와 사용하는 업그레이드 방법에 따라 달라집니다. 현재 ESXi 버전에서 업그레이드하려는 버전으로의 업그레이드 경로가 지원되는지 확인합니다. 자세한 내용은 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php에서 VMware 제품 상호 운용성 매트릭스를 참조하십시오.

vCenter Server에 인플레이스 업그레이드를 수행하지 않고 업그레이드에 다른 시스템을 사용할 수 있습니다. 자세한 지침 및 업그레이드 옵션은 "vCenter Server 업그레이드" 설명서를 참조하십시오.

ESXi 호스트 업그레이드

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

다음을 사용하여 vSAN 클러스터에서 ESXi 호스트를 업그레이드할 수 있습니다.

- vSphere Lifecycle Manager - 이미지 또는 기준선을 사용하여 vSphere Lifecycle Manager에서 vSAN 클러스터의 ESXi 호스트를 업그레이드할 수 있습니다. 기본 제거 모드는 **데이터 액세스 보장**입니다. 이 모드를 사용하고 vSAN을 업그레이드 하는 동안 오류가 발생하면 호스트 중 하나가 다시 온라인 상태가 될 때까지 데이터에 액세스할 수 없게 됩니다. 제거 및 유지 보수 모드 사용에 대한 자세한 내용은 유지 보수 모드 사용 항목을 참조하십시오. 업그레이드 및 업데이트에 대한 자세한 내용은 "호스트 및 클러스터 수명 주기" 설명서를 참조하십시오.
- Esxcli 명령 - 구성 요소, 기본 이미지 및 추가 기능을 새로운 소프트웨어 프로그램으로 사용하여 수동 업그레이드로 ESXi 7.0 호스트를 업데이트하거나 패치를 적용할 수 있습니다.

구성된 장애 도메인이 있는 vSAN 클러스터를 업그레이드하는 경우 vSphere Lifecycle Manager는 단일 장애 도메인 내에서 호스트를 업그레이드한 후 다음 호스트를 진행합니다. 이렇게 하면 클러스터의 모든 호스트에서 동일한 vSphere 버전이 실행됩니다. 확장 클러스터를 업그레이드하는 경우 vSphere Lifecycle Manager는 모든 호스트를 기본 사이트에서 업그레이드한 후 보조 사이트의 호스트의 업그레이드를 계속 진행합니다. 이렇게 하면 클러스터의 모든 호스트에서 동일한 vSphere 버전이 실행됩니다. 확장 클러스터 업그레이드에 대한 자세한 내용은 "호스트 및 클러스터 수명 주기 관리" 설명서를 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. 자세한 지침 및 업그레이드 옵션은 "VMware ESXi 업그레이드" 설명서를 참조하십시오.

다음에 수행할 작업

1 (선택 사항) vSAN 디스크 형식을 업그레이드합니다. RVC를 사용하여 vSAN 디스크 형식 업그레이드를 참조하십시오.

2 호스트 라이센스를 확인합니다. 대개의 경우 호스트 라이센스를 다시 적용해야 합니다. 호스트 라이센스 적용에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

3 (선택 사항) vSphere Client 또는 vSphere Lifecycle 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. ■ 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.

표 9-2. 업그레이드 프로세스 (계속)

완료율	설명
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.
15% - 95%	버전 3.0보다 낮은 vSAN 버전을 업그레이드할 때 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 로드에 따라 다릅니다. I/O 용량에 도달하거나 거의 도달한 시스템에서는 전송 속도가 저하됩니다.
95% - 100%	최종 개체 버전 업그레이드. 새로운 온디스크 형식으로의 개체 변환과 다시 동기화가 완료됩니다. 이 프로세스에 소요되는 시간은 사용된 공간의 양 및 **감소된 이중화 허용** 옵션을 선택했는지 여부에 따라 다릅니다.

업그레이드하는 동안 [구성 요소 다시 동기화] 페이지에서 업그레이드 프로세스를 모니터링할 수 있습니다. "vSAN 모니터링 및 문제 해결" 의 내용을 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 상태 표시줄의 [최근 작업] 창에서 모니터링할 수 있습니다.

디스크 형식을 업그레이드할 때 다음 고려 사항이 적용됩니다.

- 호스트가 3개인 클러스터를 업그레이드하고 전체 제거를 수행할 때 **허용되는 장애**가 0(제로)보다 큰 개체라면 제거할 수 없습니다. 호스트가 3개인 클러스터는 전체 제거되는 디스크 그룹을 호스트 두 개의 리소스만 사용하여 다시 보호할 수 없습니다. 예를 들어 **허용되는 장애**가 1로 설정되어 있다면 vSAN 보호 구성 요소가 3개(미러 2개와 감시 1개) 필요하고 각 보호 구성 요소는 개별 호스트에 배치됩니다.

  호스트가 3개인 클러스터에 대해서는 **데이터 액세스 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.

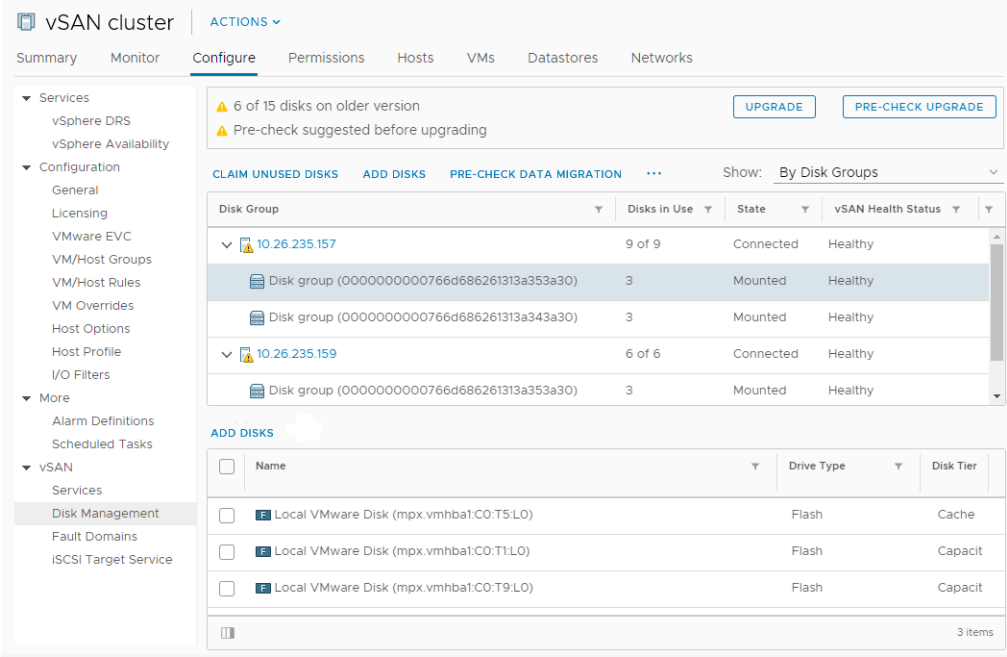
- `--allow-reduced-redundancy` 명령 옵션을 사용하면 특정 가상 시스템이 마이그레이션 중에 장애를 허용하지 못할 수 있습니다. 이와 같은 장애 허용 수준 감소도 데이터 손실을 유발할 수 있습니다. vSAN은 업그레이드 완료 후 전체 규정 준수 및 이중화를 복원합니다. 업그레이드 중에는 가상 시스템의 규정 준수 상태 및 해당 이중화가 일시적으로 비준수 상태가 됩니다. 업그레이드를 완료하고 재구축 작업을 모두 마치고 나면 가상 시스템이 준수 상태가 됩니다.

- 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 가이드" 를 참조하십시오.

vSphere Client를 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. vSAN 설정 편집를 참조하십시오.

사전 요구 사항

- 업데이트된 버전의 vCenter Server를 사용 중인지 확인합니다.
- 최신 버전의 ESXi 호스트를 사용하고 있는지 확인합니다.
- 디스크가 정상 상태인지 확인합니다. [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 않습니다. 클러스터 용량이 줄어들고 클러스터 업그레이드가 실패할 수 있습니다.

- 현재 vSAN 클러스터에서 진행 중인 구성 요소 재구축 작업이 없는지 확인합니다. vSAN 다시 동기화에 대한 자세한 내용은 "vSphere 모니터링 및 성능" 항목을 참조하십시오.

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 선택합니다.

4 (선택 사항) **업그레이드 사전 검사**를 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 **업그레이드**를 클릭합니다.

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

결과

vSAN은 온디스크 형식을 성공적으로 업그레이드합니다. 클러스터에 있는 스토리지 디바이스의 디스크 형식 버전이 [온디스크 형식 버전] 열에 표시됩니다.

업그레이드 중에 장애가 발생하면 [개체 다시 동기화] 페이지를 확인하면 됩니다. 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.

사전 요구 사항

- 업데이트된 버전의 vCenter Server를 사용 중인지 확인합니다.
- vSAN 클러스터에서 실행되고 있는 ESXi 호스트의 버전이 6.5 이상인지 확인합니다.
- [디스크 관리] 페이지에서 디스크의 상태가 정상인지 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 가이드" 의 내용을 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 않으므로 클러스터의 사용 가능한 리소스 용량이 줄어듭니다. 따라서 클러스터 업그레이드가 실패할 수 있습니다.
- RVC `vsan.resync_dashboard` 명령을 실행하여, 현재 vSAN 클러스터에서 진행 중인 구성 요소 재구축 작업이 없는지 확인합니다.

절차

1 RVC를 사용하여 vCenter Server에 로그인합니다.

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

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 비정상으로 나타납니다.

3 다음 RVC 명령을 실행합니다. `vsan.ondisk_upgrade <path to vsan cluster>`

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

4 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
```

5 다음 RVC 명령을 실행하여 개체 버전이 새 온디스크 형식으로 업그레이드되었는지 확인합니다. `vsan.obj_status_report`

vSAN 디스크 형식 업그레이드 확인

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

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭합니다.

3 vSAN에서 **디스크 관리**를 클릭합니다.

[디스크 형식 버전] 열에 현재 디스크 형식 버전이 나타납니다.

vSAN 개체 형식 정보

vSAN에서 vSAN 7.0 또는 이전 버전에서 생성된 개체에 대해 정책 변경 또는 기타 작업을 수행하기 위해 필요한 작업 공간은 클러스터의 가장 큰 개체에 사용되는 공간입니다. 이 작업은 일반적으로 계획하기 어렵기 때문에, 클러스터의 가장 큰 개체가 공간의 25% 이상을 소비하고, 정책 변경으로 인해 클러스터가 꽉 차지 않도록 공간의 5%가 예약될 가능성이 없다는 가정하에, 클러스터의 사용 가능한 공간을 30%로 유지하는 것이 좋습니다. vSAN 7.0U1 이상에서 8TB 미만의 개체에 대해 호스트당 255GB가 있고 8TB 이상의 개체에 대해 호스트당 765GB가 있는 경우 vSAN에서 개체에 대해 정책 변경을 수행하는 데 필요한 작업 공간을 허용하는 새 형식으로 모든 개체가 생성됩니다.

클러스터를 vSAN 7.0 또는 이전 릴리스에서 vSAN 7.0 U1 이상으로 업그레이드한 후에는 이전 릴리스에서 생성된 255GB보다 큰 개체를 새 vSAN 형식으로 다시 작성해야 합니다. 그래야 vSAN에서 새로운 여유 공간 요구 사항에 따라 개체에 대한 작업을 수행할 수 있습니다. 새 개체 형식으로 수정해야 하는 개체가 있는 경우 업그레이드 후에 새 개체 형식 상태 경고가 표시되고, 레이아웃 변경 작업을 시작하여 상태를 수정함으로써 이러한 개체를 수정할 수 있습니다. 상태 경고는 수정해야 하는 개체 수 및 다시 쓸 데이터 양 대한 정보를 제공합니다. 레이아웃 변경 작업이 진행되는 동안 클러스터 성능이 약 20% 저하될 수 있습니다. 다시 동기화 대시보드는 이 작업을 완료하는 데 소요되는 시간에 대해 좀 더 정확한 정보를 제공합니다.

vSAN 클러스터 업그레이드 확인

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

절차

1 vSAN 클러스터로 이동합니다.

2 **구성** 탭을 클릭하고 vSAN이 나열되는지 확인합니다.

- ESXi 호스트로 이동한 후 **요약** > **구성**을 선택하고, ESXi 호스트의 최신 버전을 현재 사용 중인지 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 사용합니다.
`--ignore-objects, -i`	vSAN 개체 업그레이드를 건너뛰는 데 사용합니다. 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 사용합니다. 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 사용합니다.

RVC 명령 사용에 대한 자세한 내용은 "RVC 명령 참조 가이드" 를 참조하십시오.

vSphere Lifecycle Manager에 대한 vSAN 빌드 권장 사항

vSAN은 vSphere Lifecycle Manager와 함께 사용할 수 있는 시스템 기준선 및 기준선 그룹을 생성합니다. vSphere 7.0의 vSphere Lifecycle Manager에는 이전 vSphere 릴리스에서 Update Manager가 제공하는 시스템 기준선이 포함되어 있습니다. 또한 ESXi 7.0 이상을 실행하는 호스트에 대한 새로운 이미지 관리 기능도 포함되어 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 6.7.1에서 vSAN 7.0으로의 시스템 기준선에는 디바이스 드라이버 및 펌웨어 업데이트도 포함될 수 있습니다. 이 업데이트는 클러스터에 권장되는 ESXi 소프트웨어를 지원합니다.

vSAN 6.7.3 이상에서는 현재 ESXi 릴리스에 대해서만 또는 지원되는 최신 ESXi 릴리스에 대한 빌드 권장 사항을 제공하도록 선택할 수 있습니다. 현재 릴리스에 대한 빌드 권장 사항에는 릴리스에 대한 모든 패치와 드라이버 업데이트가 포함됩니다.

vSAN 7.0 이상에서 vSAN 빌드 권장 사항에는 패치 업데이트 및 적용 가능한 드라이버 업데이트가 포함됩니다. vSAN 7.0 클러스터의 펌웨어를 업데이트하려면 vSphere Lifecycle Manager를 통해 이미지를 사용해야 합니다.

vSAN 시스템 기준선

vSAN 빌드 권장 사항은 vSphere Lifecycle 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.

vSAN 시스템 기준선에는 인증된 벤더가 제공하는 사용자 지정 ISO 이미지가 포함될 수 있습니다. vSAN 클러스터의 호스트에 OEM 관련 사용자 지정 ISO가 있는 경우에는 vSAN 권장 시스템 기준선에 동일한 벤더의 사용자 지정 ISO가 포함될 수 있습니다. vSphere Lifecycle Manager는 vSAN에서 지원되지 않는 사용자 지정 ISO에 대한 권장 사항을 생성할 수 없습니다. 호스트의 이미지 프로파일에 벤더 이름을 재정의하는 사용자 지정 소프트웨어 이미지를 실행 중인 경우, vSphere Lifecycle Manager가 시스템 기준선을 추천할 수 없습니다.

vSphere Lifecycle Manager는 자동으로 각 vSAN 클러스터를 검색하여 기준선 그룹에 대한 규정 준수를 확인합니다. 클러스터를 업그레이드하려면 vSphere Lifecycle 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.

인터넷에 연결되어 있지 않으면 vSAN 릴리스 카탈로그를 vCenter Server에 직접 업로드할 수 있습니다. vSphere Client에서 **구성 > vSAN > 업데이트**를 클릭하고 [릴리스 카탈로그] 섹션의 **파일에서 업로드**를 클릭합니다. 최신 vSAN 릴리스 카탈로그를 다운로드할 수 있습니다.

vSphere Lifecycle Manager를 사용하면 vSAN 클러스터에 권장되는 스토리지 컨트롤러 드라이버를 가져올 수 있습니다. 일부 스토리지 컨트롤러 벤더는 vSAN이 컨트롤러 드라이버를 업데이트하는 데 사용할 수 있는 소프트웨어 관리 도구를 제공합니다. 이러한 관리 도구가 ESXi 호스트에 없으면 해당 도구를 다운로드하면 됩니다.

vSAN 빌드 권장 사항 사용

vSphere Lifecycle Manager는 VMware 호환성 가이드에 있는 하드웨어 호환성 목록(HCL)의 정보를 기준으로, 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 포함합니다.

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 권장할 수 있습니다. 최신 릴리스가 현재 상태보다 나쁘지 않기 때문입니다.

참고 vSphere Lifecycle Manager는 vSAN 클러스터의 호스트에 대한 업데이트 적용 사전 확인을 수행할 때 vSAN Health Service를 사용합니다. vSAN 상태 서비스는 ESXi 6. 0 업데이트 1 또는 이전 버전을 실행하는 호스트에서는 사용할 수 없습니다. vSphere Lifecycle Manager가 ESXi 6.0 업데이트 1 또는 이전 버전을 실행하는 호스트를 업그레이드하면 vSAN 클러스터의 마지막 호스트 업그레이드가 실패할 수 있습니다. vSAN 상태 문제로 인해 업데이트 적용이 실패하더라도 업그레이드를 완료할 수 있습니다. vSAN 상태 서비스를 사용하여 호스트의 상태 문제를 해결한 다음 이 호스트를 유지 보수 모드에서 제거하여 업그레이드 워크플로를 완료합니다.

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 6.7 업데이트 2를 실행 중이고, 해당 하드웨어는 6.7 업데이트 2 HCL에 포함되어 있습니다. 또한 HCL에서 해당 하드웨어는 릴리스 7.0 업데이트 3에 대해 지원됩니다. vSAN은 릴리스 7.0 업데이트 3으로 업그레이드를 권장합니다.

예제 3

vSAN 클러스터가 6.7 업데이트 2를 실행 중이고, 해당 하드웨어는 이 릴리스의 HCL에 없습니다. vSAN은 7.0 업데이트 3의 HCL에 이 하드웨어가 나와 있지 않더라도 7.0 업데이트 3으로 업그레이드를 권장합니다. vSAN은 새로운 상태가 현재 상태보다 나쁘지 않기 때문에 업그레이드를 권장합니다.

예제 4

vSAN 클러스터가 6.7 업데이트 2를 실행 중이고, 해당 하드웨어는 6.7 업데이트 2 HCL에 포함되어 있습니다. 이 하드웨어는 릴리스 7.0 업데이트 3의 HCL에서도 지원되며 선택한 기준선 기본 설정은 패치 전용입니다. vSAN은 해당 릴리스에 필요한 중요 패치를 포함하여 7.0 업데이트 3으로 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.
- 사용자는 웹 브라우저나 RVC를 사용하여 VMware Customer Connect에 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

vSphere Lifecycle Manager는 vCenter Server 7.0 이상의 확장 서비스입니다.

vSAN에서 릴리스 메타데이터를 업데이트하고 VMware Customer Connect 호환성 가이드를 확인하고, VMware Customer Connect에서 ISO 이미지를 다운로드하려면 인터넷 액세스가 필요합니다.

VMware Customer Connect에서 업그레이드용 ISO 이미지를 다운로드하려면 vSAN에 유효한 자격 증명이 필요합니다. 6.0 업데이트 1 이전 버전이 실행되는 호스트의 경우 RVC를 사용하여 **VMware Customer Connect** 자격 증명을 입력해야 합니다. 이후 버전의 소프트웨어가 실행되는 호스트의 경우 ESX 빌드 권장 사항 상태 점검에서 로그인할 수 있습니다.

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