VMware

Enterprise applications

NetApp
January 02, 2026

목차

VMware

ONTAP 기반의 VMware vSphere

ONTAP 기반의 VMware vSphere

ONTAP은 2002년에 최신 데이터 센터에 구현된 후로 VMware vSphere 및 최근에는 Cloud Foundation 환경을 위한 최고의 스토리지 솔루션으로 활동했습니다. 관리를 단순화하고 비용을 절감하는 혁신적인 기능을 지속적으로 도입하고 있습니다.

이 문서에서는 vSphere용 ONTAP 솔루션에 대해 소개하고 구축을 간소화하고 위험을 완화하며 관리를 단순화하는 최신 제품 정보와 Best Practice를 중점적으로 설명합니다.

이 문서는 이전에 게시된 기술 보고서_TR-4597: VMware vSphere for ONTAP _ 을(를) 대체합니다

모범 사례는 가이드 및 호환성 목록 등의 다른 문서를 보완합니다. 이러한 전문 분야는 연구소 테스트와 NetApp 엔지니어 및 고객의 광범위한 현장 경험을 기반으로 합니다. 모든 환경에서 작동하는 유일한 지원 방법은 아니지만 일반적으로 대부분의 고객 요구를 충족하는 가장 간단한 솔루션입니다.

이 문서는 vSphere 7.0 이상에서 실행되는 최신 릴리즈의 ONTAP(9.x)에 포함된 기능을 중점적으로 다룹니다. "상호운용성 매트릭스 툴(IMT)"특정 릴리스와 관련된 자세한 내용은 및 "VMware 호환성 가이드 를 참조하십시오" 를 참조하십시오.

ONTAP for VMware vSphere를 선택해야 하는 이유

고객은 SAN과 NAS 스토리지 솔루션 모두에 ONTAP for vSphere를 자신 있게 선택합니다. 최신 All SAN Arrays에 적용된 새로운 간소화된 분산 스토리지 아키텍처는 기존 ONTAP 시스템의 대부분 통합 및 기능 세트를 그대로 유지하면서 SAN 스토리지 관리자에게 익숙한 간소화된 환경을 제공합니다. ONTAP 시스템은 뛰어난 스냅샷 보호 기능과 견고한 관리 도구를 제공합니다. ONTAP 전용 스토리지에 기능을 오프로드함으로써 호스트 리소스를 극대화하고, 비용을 절감하며, 최적의 성능을 유지합니다. 또한 Storage vMotion을 사용하여 VMFS, NFS 또는 vVols 에서 작업 부하를 쉽게 마이그레이션할 수 있습니다.

ONTAP for vSphere를 사용할 때의 이점

수많은 고객들이 vSphere용 스토리지 솔루션으로 ONTAP을 선택한 이유가 있습니다. 예를 들어 SAN 및 NAS 프로토콜을 모두 지원하는 유니파이드 스토리지 시스템, 공간 효율적인 스냅샷을 사용하는 강력한 데이터 보호 기능, 애플리케이션 데이터를 관리하는 데 도움이 되는 다양한 툴이 있습니다. 하이퍼바이저와 별도로 스토리지 시스템을 사용하면 다양한 기능을 오프로드하고 vSphere 호스트 시스템에 대한 투자를 극대화할 수 있습니다. 이렇게 하면 호스트 리소스가 애플리케이션 워크로드에 집중되도록 할 뿐 아니라 스토리지 작업에서 애플리케이션에 미치는 랜덤 성능 영향을 방지할 수 있습니다.

ONTAP vSphere와 함께 사용하면 호스트 하드웨어와 VMware 소프트웨어 비용을 줄일 수 있는 훌륭한 조합입니다. 일관된 고성능을 유지하며 더 낮은 비용으로 데이터를 보호할 수도 있습니다. 가상화된 워크로드는 이동성이 있으므로 Storage vMotion을 사용하여 동일한 스토리지 시스템에서 VMFS, NFS 또는 vVols 데이터 저장소로 VM을 이동하는 다양한 접근 방식을 살펴볼 수 있습니다.

오늘날 고객이 중요하게 여기는 주요 요소는 다음과 같습니다.

- 통합 스토리지. ONTAP 실행하는 시스템은 여러 가지 중요한 면에서 통합되어 있습니다. 원래 이 접근 방식은 NAS와 SAN 프로토콜을 모두 의미했으며 ONTAP NAS의 원래 강점과 함께 SAN을 위한 선도적 플랫폼으로 계속 자리매김하고 있습니다. vSphere 환경에서 이 접근 방식은 가상 서버 인프라(VSI)와 함께 가상 데스크톱 인프라(VDI)를 위한 통합 시스템을 의미할 수도 있습니다. ONTAP 실행하는 시스템은 일반적으로 기존 엔터프라이즈 어레이보다 VSI 비용이 저렴하면서도 동일한 시스템에서 VDI를 처리할 수 있는 고급 스토리지 효율성 기능을 갖추고 있습니다. ONTAP SSD부터 SATA까지 다양한 저장 매체를 통합하고 이를 클라우드로 쉽게 확장할 수 있습니다. 성능을 위해 하나의 저장 운영 체제를 구입하고, 보관을 위해 또 다른 저장 운영 체제를 구입하고, 클라우드를 위해 또 다른 저장 운영 체제를 구입할 필요가 없습니다. ONTAP 이 모든 것을 하나로 연결합니다.

- * 모든 SAN 어레이(ASA). * 최신 ONTAP ASA 시스템(A1K, A90, A70, A50, A30 및 A20부터 시작)은 새로운 스토리지 아키텍처에 구축되어, 기존의 애그리게이트 및 볼륨 관리에 대한 ONTAP 스토리지 패러다임을 제거합니다. 파일 시스템 공유가 없기 때문에 볼륨이 필요하지 않습니다! HA 쌍에 연결된 모든 스토리지는 LUN 및 NVMe 네임스페이스를 "스토리지 유닛"(SUS)으로 프로비저닝하는 공통 SAZ(Storage Availability Zone)로 처리됩니다. 최신 ASA 시스템은 관리가 용이하고 SAN 스토리지 관리자에게 익숙한 경험을 제공하도록 설계되었습니다. 이 새로운 아키텍처는 스토리지 리소스를 간편하게 관리할 수 있고 SAN 스토리지 관리자에게 간소화된 환경을 제공하므로 vSphere 환경에 이상적입니다. 또한, ASA 아키텍처는 최신 NVMe-oF(NVMe over Fabrics) 기술을 지원하여 vSphere 워크로드에 훨씬 뛰어난 성능과 확장성을 제공합니다.

- * 스냅샷 기술. * ONTAP는 데이터 보호를 위한 스냅샷 기술을 최초로 제공한 기업이며 업계에서 가장 진보된 제품이라고 할 수 있습니다. 공간 효율적인 데이터 보호 방식이 VMware VAAI(vSphere APIs for Array Integration)를 지원하도록 확장되었습니다. 이러한 통합을 통해 백업 및 복원 작업에 ONTAP의 스냅샷 기능을 활용할 수 있으므로 프로덕션 환경에 미치는 영향이 줄어듭니다. 또한 스냅샷을 사용하여 VM을 빠르게 복구할 수 있으므로 데이터 복구에 필요한 시간과 노력을 줄일 수 있습니다. 또한 ONTAP의 스냅샷 기술은 VMware의 VLSR(Live Site Recovery Manager) 솔루션과 통합되어 가상화 환경에 포괄적인 데이터 보호 전략을 제공합니다.

- 가상 볼륨 및 스토리지 정책 기반 관리. NetApp vSphere Virtual Volumes(vVols) 개발에 있어 VMware와 초기 설계 파트너였으며, vVols 및 VMware vSphere APIs for Storage Awareness(VASA)에 대한 아키텍처 입력과 초기 지원을 제공했습니다. 이 접근 방식은 VMFS에 세분화된 VM 스토리지 관리를 제공할 뿐만 아니라 스토리지 정책 기반 관리를 통해 스토리지 프로비저닝을 자동화하는 기능도 지원합니다. 이러한 접근 방식을 통해 스토리지 설계자는 VM 관리자가 쉽게 사용할 수 있는 다양한 기능을 갖춘 스토리지 풀을 설계할 수 있습니다. ONTAP 단일 클러스터에서 수십만 개의 vVols 지원하여 vVol 규모 측면에서 스토리지 업계를 선도하는 반면, 엔터프라이즈 어레이 및 소규모 플래시 어레이 공급업체는 어레이당 수천 개의 vVols 지원합니다. NetApp 향후 기능을 통해 세분화된 VM 관리의 발전도 주도하고 있습니다.

- 저장 효율성. NetApp 프로덕션 워크로드에 대한 중복 제거 기능을 최초로 제공했지만, 이 혁신은 이 분야에서 처음이거나 마지막은 아니었습니다. 이는 성능에 영향을 미치지 않는 공간 효율적인 데이터 보호 메커니즘인 스냅샷과 FlexClone 기술로 시작되었으며, 이를 통해 프로덕션 및 백업용으로 VM의 읽기/쓰기 복사본을 즉시 만들 수 있었습니다. NetApp 값비싼 SSD에서 최대한 많은 저장 공간을 확보하기 위해 중복 제거, 압축, 제로 블록 중복 제거를 포함한 인라인 기능을 제공했습니다. ONTAP 또한 압축을 사용하여 더 작은 I/O 작업과 파일을 디스크 블록으로 묶는 기능을 추가했습니다. 이러한 기능을 결합한 결과, 고객은 일반적으로 VSI의 경우 최대 5:1, VDI의 경우 최대 30:1의 비용 절감 효과를 얻었습니다. 최신 세대 ONTAP 시스템에는 하드웨어 가속 압축 및 중복 제거 기능도 포함되어 있어 스토리지 효율성을 더욱 향상시키고 비용을 절감할 수 있습니다. 이 방법을 사용하면 더 적은 공간에 더 많은 데이터를 저장할 수 있어 전반적인 저장 비용이 줄어들고 성능이 향상됩니다. NetApp 자사의 스토리지 효율성 기능에 매우 자신감을 갖고 있어 다음 링크를 제공합니다: https://www.netapp.com/pdf.html?item=/media/79014-ng-937-Efficiency-Guarantee-Customer-Flyer.pdf [효율성 보장^].

- 다중 테넌시. ONTAP 오랫동안 멀티테넌시 분야를 선도해 왔으며, 단일 클러스터에서 여러 개의 스토리지 가상 머신(SVM)을 생성할 수 있도록 지원합니다. 이러한 접근 방식을 사용하면 작업 부하를 분리하고 다양한 테넌트에 다양한 수준의 서비스를 제공할 수 있으므로 서비스 제공업체와 대기업에 이상적입니다. 최신 세대의 ONTAP 시스템에는 테넌트 용량 관리에 대한 지원도 포함되어 있습니다. 이 기능을 사용하면 각 테넌트에 대한 용량 제한을 설정하여 단일 테넌트가 사용 가능한 모든 리소스를 소비하지 못하도록 할 수 있습니다. 이러한 접근 방식은 모든 세입자가 기대하는 수준의 서비스를 받을 수 있도록 보장하는 동시에 세입자 간에 높은 수준의 보안과 격리를 제공하는 데 도움이 됩니다. 또한 ONTAP의 멀티테넌시 기능은 VMware의 vSphere 플랫폼과 통합되어 가상화된 환경을 쉽게 관리하고 모니터링할 수 있습니다. "VMware vSphere용 ONTAP 툴" 그리고 "데이터 인프라 인사이트" .

- 하이브리드 클라우드. 온프레미스 프라이빗 클라우드, 퍼블릭 클라우드 인프라 또는 두 가지 장점을 결합한

하이브리드 클라우드에 사용하든 ONTAP 솔루션은 데이터 패브릭을 구축하여 데이터 관리를 간소화하고 최적화하는 데 도움이 됩니다. 고성능 올플래시 시스템부터 시작한 다음, 데이터 보호 및 클라우드 컴퓨팅을 위해 디스크나 클라우드 스토리지 시스템과 결합하세요. Azure, AWS, IBM 또는 Google Cloud 중에서 선택하여 비용을 최적화하고 종속성을 피하세요. 필요에 따라 OpenStack 및 컨테이너 기술에 대한 고급 지원을 활용하세요. NetApp 또한 ONTAP 위한 클라우드 기반 백업(SnapMirror Cloud, Cloud Backup Service, Cloud Sync)과 스토리지 계층화 및 보관 도구(FabricPool)를 제공하여 운영 비용을 줄이고 클라우드의 광범위한 도달 범위를 활용하는 데 도움을 줍니다.

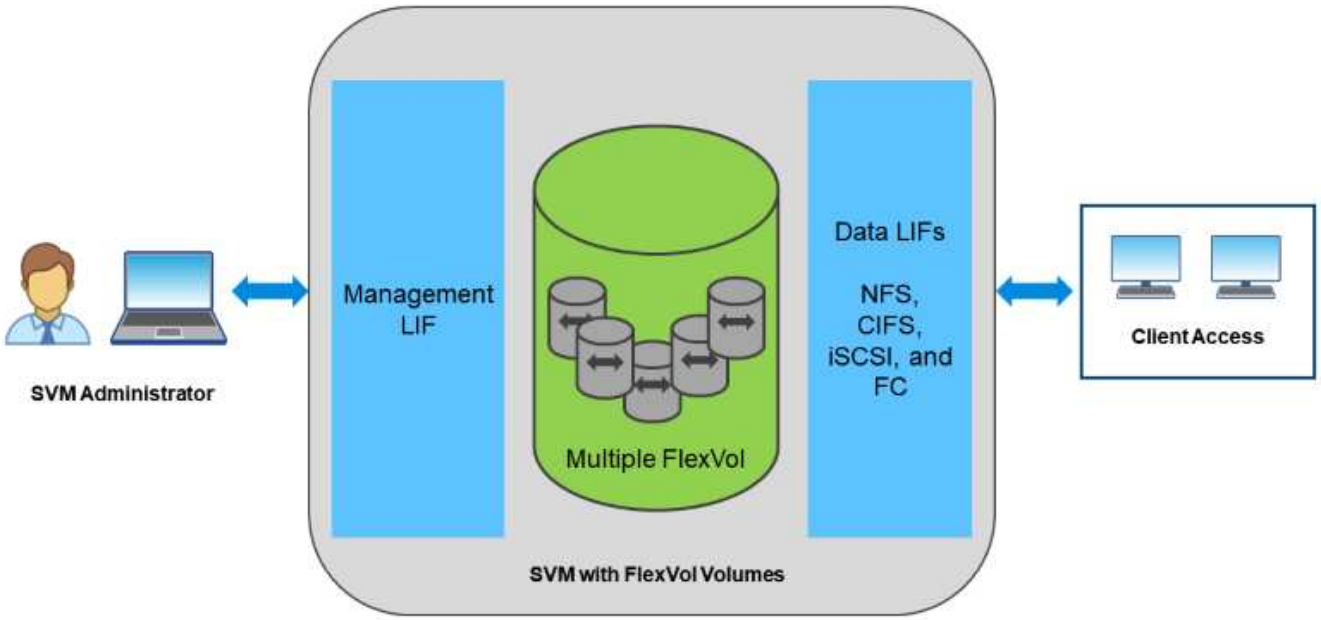
- * 그 이상. * NetApp AFF A-Series 어레이의 탁월한 성능을 활용하여 가상화 인프라를 가속하고 비용을 관리하십시오. 스케일아웃 ONTAP 클러스터를 사용하면 유지보수, 업그레이드, 스토리지 시스템 전체 교체 등 운영 중단 없이 완벽하게 수행할 수 있습니다. 추가 비용 없이 NetApp 암호화 기능으로 유휴 데이터를 보호합니다. 세분화된 서비스 품질 기능을 통해 성능이 비즈니스 서비스 수준을 충족하는지 확인합니다. 모두 업계 최고의 엔터프라이즈 데이터 관리 소프트웨어인 ONTAP에 포함된 광범위한 기능에 속합니다.

유니파이드 스토리지

ONTAP는 간소화된 소프트웨어 정의 접근 방식으로 스토리지를 통합하여 안전하고 효율적인 관리, 향상된 성능 및 원활한 확장성을 제공합니다. 이 접근 방식은 데이터 보호를 개선하고 클라우드 리소스를 효과적으로 사용할 수 있도록 합니다.

원래 이러한 통합 접근 방식은 단일 스토리지 시스템에서 NAS 및 SAN 프로토콜을 모두 지원한다고 언급했으며, ONTAP은 NAS에서 원래의 강점과 함께 SAN을 위한 최고의 플랫폼이 되었습니다. 이제 ONTAP는 S3 오브젝트 프로토콜 지원도 제공합니다. S3는 데이터 저장소에 사용되지 않지만 게스트 내 애플리케이션에 사용할 수 있습니다. ONTAP에서 S3 프로토콜 지원에 대한 자세한 내용은 를 "S3 구성 개요"참조하십시오. 유니파이드 스토리지라는 용어는 단일 인터페이스에서 모든 스토리지 리소스를 관리하는 기능을 포함하여 스토리지 관리에 대한 통합된 접근 방식을 의미하도록 개선되었습니다. 여기에는 사내 및 클라우드 스토리지 리소스, 최신 ASA(All SAN 어레이) 시스템, 단일 인터페이스에서 여러 스토리지 시스템을 관리할 수 있는 기능이 포함됩니다.

스토리지 가상 머신(SVM)은 ONTAP에서 안전한 멀티 테넌시(Multi-tenancy)의 장치입니다. ONTAP를 실행하는 시스템에 대한 클라이언트 액세스를 허용하는 논리적 구성입니다. SVM은 논리 인터페이스(LIF)를 통해 여러 데이터 액세스 프로토콜을 통해 데이터를 동시에 제공할 수 있습니다. SVM은 CIFS 및 NFS와 같은 NAS 프로토콜을 통해 파일 레벨 데이터 액세스를 지원하고, iSCSI, FC/FCoE, NVMe와 같은 SAN 프로토콜을 통해 블록 레벨 데이터 액세스를 제공합니다. SVM은 S3뿐만 아니라 SAN과 NAS 클라이언트에 데이터를 동시에 독립적으로 제공할 수 있습니다.



vSphere 환경에서 이 접근 방식은 가상 데스크톱 인프라(VDI)와 가상 서버 인프라(VSI)의 통합 시스템을 의미할 수도 있습니다. ONTAP를 실행하는 시스템은 일반적으로 VSI 비용이 기존 엔터프라이즈 어레이보다 저렴하지만 동일한 시스템에서 VDI를 처리할 수 있는 고급 스토리지 효율성 기능이 있습니다. 또한 ONTAP는 SSD에서 SATA에 이르는 다양한 스토리지 미디어를 통합하여 손쉽게 클라우드로 확장할 수 있습니다. 성능 향상을 위해 플래시 어레이 1개, 아카이브를 위한 SATA 어레이, 클라우드를 위한 별도의 시스템을 구입할 필요가 없습니다. ONTAP는 이러한 모든 것을 하나로 묶습니다.

- 참고: * SVM, 유니파이드 스토리지 및 클라이언트 액세스에 대한 자세한 내용은 를 참조하십시오 "스토리지 가상화" ONTAP 9 문서 센터

ONTAP용 가상화 툴

NetApp는 기존 ONTAP 및 ASA 시스템과 호환되는 여러 가지 독립 실행형 소프트웨어 툴을 제공하여 vSphere를 통합하여 가상화 환경을 효과적으로 관리합니다.

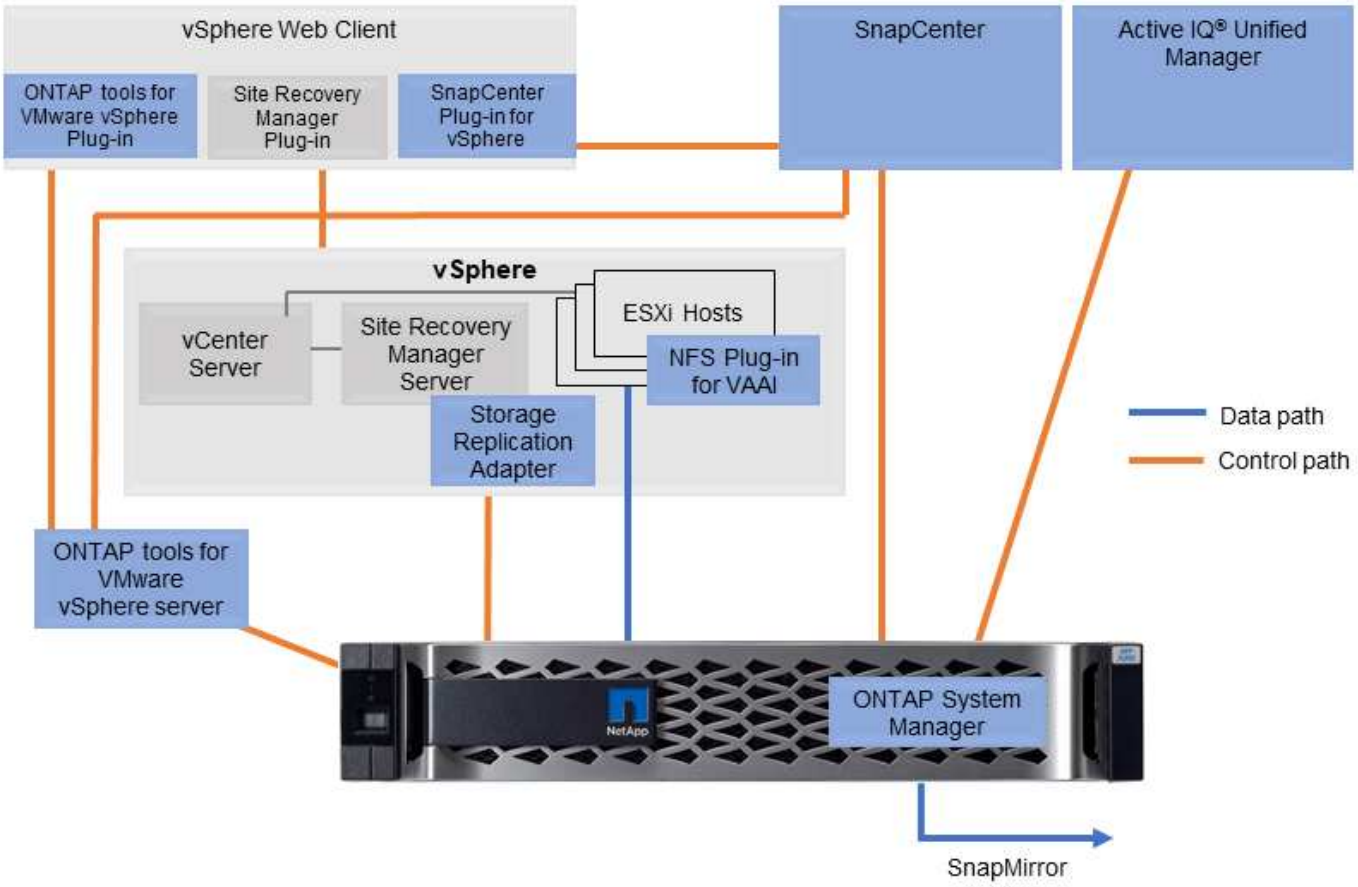
다음 도구는 추가 비용 없이 ONTAP One 라이센스에 포함되어 있습니다. 그림 1을 참조하여 vSphere 환경에서 이러한 툴이 함께 작동하는 방식을 보여 줍니다.

VMware vSphere용 ONTAP 툴

"VMware vSphere용 ONTAP 툴" 는 ONTAP 스토리지를 vSphere와 함께 사용하기 위한 툴 세트입니다. 이전에 VSC(Virtual Storage Console)라고도 하는 vCenter 플러그인을 사용하면 SAN 또는 NAS를 사용하든지 스토리지 관리 및 효율성 기능을 단순화하고, 가용성을 향상하고, 스토리지 비용과 운영 오버헤드를 줄일 수 있습니다. Best Practice를 사용하여 데이터 저장소를 프로비저닝하고 NFS 및 블록 스토리지 환경에 대한 ESXi 호스트 설정을 최적화합니다. 이러한 모든 이점을 위해 NetApp은 ONTAP를 실행하는 시스템에서 vSphere를 사용할 때 이러한 ONTAP 툴을 모범 사례로 사용할 것을 권장합니다. 여기에는 서버 어플라이언스, vCenter용 UI 확장, VASA Provider 및 Storage Replication Adapter가 포함됩니다. ONTAP 툴의 거의 모든 기능을 대부분의 최신 자동화 툴에서 사용 가능한 단순한 REST API를 사용하여 자동화할 수 있습니다.

- * vCenter UI 확장. * ONTAP 툴 UI 확장은 호스트 및 스토리지를 관리하기 위한 사용하기 쉬운 상황에 맞는 메뉴, 정보 포틀릿 및 기본 알림 기능을 vCenter UI에 직접 내장하여 워크플로우를 간소화함으로써 운영 팀과 vCenter 관리자의 작업을 간소화합니다.
- * VASA Provider for ONTAP. * VASA Provider for ONTAP는 VMware VASA(vStorage APIs for Storage Awareness) 프레임워크를 지원합니다. 이 제품은 구축 편의성을 위해 VMware vSphere용 ONTAP 툴의 일부로 단일 가상 어플라이언스로 제공됩니다. VASA Provider는 vCenter Server를 ONTAP와 연결하여 VM 스토리지를 프로비저닝하고 모니터링할 수 있도록 지원합니다. 이를 통해 VVol(VMware Virtual Volumes) 지원, 스토리지 기능 프로필 관리, 개별 VM VVol 성능, 용량 모니터링 및 프로파일 규정 준수에 대한 경보를 수행할 수 있습니다.
- 스토리지 복제 어댑터. SRA는 SnapMirror 사용하여 어레이 기반 복제를 통해 운영 사이트와 재해 복구 사이트 간의 데이터 복제를 관리하기 위해 VMware Live Site Recovery(VLSR)/Site Recovery Manager(SRM)와 함께 사용됩니다. 재해 발생 시 장애 조치 작업을 자동화하고, DR 복제본을 중단 없이 테스트하여 DR 솔루션에 대한 확신을 확보하는 데 도움이 될 수 있습니다.

다음 그림에서는 vSphere용 ONTAP 툴을 보여 줍니다.



VMware vSphere용 SnapCenter 플러그인

그만큼 "VMware vSphere용 SnapCenter 플러그인" vCenter Server용 플러그인으로, 가상 머신(VM)과 데이터스토어의 백업과 복원을 관리할 수 있습니다. 여러 ONTAP 시스템에서 VM과 데이터 저장소의 백업, 복원 및 복제를 관리하기 위한 단일 인터페이스를 제공합니다. SnapCenter SnapMirror 사용하여 보조 사이트로의 복제와 복구를 지원합니다. 최신 버전에서는 SnapMirror to cloud(S3), Tamperproof 스냅샷, SnapLock, SnapMirror Active Sync도 지원합니다. VMware vSphere용 SnapCenter 플러그인은 SnapCenter 애플리케이션 플러그인과 통합되어 애플리케이션과 일관된 백업을 제공할 수 있습니다.

VMware VAAI용 NFS 플러그인

는 "VMware VAAI용 NetApp NFS 플러그인" ONTAP의 NFS 데이터 저장소와 함께 VAAI 기능을 사용할 수 있는 ESXi 호스트용 플러그인입니다. 클론 작업을 위한 복제 오프로드, 일반 가상 디스크 파일에 대한 공간 예약 및 스냅샷 오프로드를 지원합니다. 복사 작업을 스토리지로 오프로드하는 것이 반드시 완료되기만은 않습니다. 그러나 이 작업은 네트워크 대역폭 요구 사항을 줄이고 CPU 주기, 버퍼 및 큐와 같은 호스트 리소스를 오프로드합니다. VMware vSphere용 ONTAP 툴을 사용하여 ESXi 호스트 또는 지원되는 경우 VLCM(vSphere Lifecycle Manager)에 플러그인을 설치할 수 있습니다.

프리미엄 소프트웨어 옵션

NetApp 에서 제공하는 프리미엄 소프트웨어 제품은 다음과 같습니다. 이러한 기능은 ONTAP One 라이선스에 포함되지 않으므로 별도로 구매해야 합니다.

- "NetApp Disaster Recovery (DR)"VMware vSphere용. 이는 VMware 환경에 대한 재해 복구 및 백업을 제공하는 클라우드 기반 서비스입니다. SnapCenter 와 함께 사용하거나 사용하지 않고도 사용할 수 있으며, SAN 또는 NAS를 사용하여 온프레미스 간 DR을 지원하고, 지원되는 경우 NFS를 사용하여 온프레미스와 클라우드 간 DR을 지원합니다.
- "데이터 인프라 인사이트(DII)". 이는 VMware 환경에 대한 모니터링과 분석을 제공하는 클라우드 기반 서비스입니다. 이 제품은 이기종 스토리지 환경의 다른 스토리지 공급업체는 물론, 여러 스위치 공급업체와 다른 하이퍼바이저를 지원합니다. DII는 VMware 환경의 성능, 용량 및 상태에 대한 완벽한 종단 간 통찰력을 제공합니다.

VVol(Virtual Volumes) 및 SPBM(Storage Policy Based Management)

2012년에 처음 발표한 NetApp는 엔터프라이즈 스토리지 시스템과 함께 SPBM(스토리지 정책 기반 관리)의 토대인 VASA(VMware vSphere APIs for Storage Awareness)를 개발하는 VMware의 초기 설계 파트너였습니다. 이 접근 방식은 VMFS 및 NFS 스토리지에 제한된 VM 세부 스토리지 관리를 제공했습니다.

기술 설계 파트너인 NetApp은 아키텍처에 대한 의견을 제공했으며 2015년에 VVOL을 지원한다고 발표했습니다. 이 새로운 기술은 이제 SPBM을 통해 VM 세분화 및 진정한 스토리지 네이티브 스토리지 프로비저닝을 자동화할 수 있게 되었습니다.

VVol(가상 볼륨)

VVOL은 VM 세부 스토리지 관리를 가능하게 하는 혁신적인 스토리지 아키텍처로, VM별(VM 메타데이터 포함)뿐만 아니라 VMDK를 기반으로 스토리지를 관리할 수 있도록 지원합니다. VVOL은 VMware Cloud Foundation(VCF)의 기반을 형성하는 SDDC(소프트웨어 정의 데이터 센터) 전략의 핵심 구성요소로서, 가상화 환경을 위한 더욱 효율적이고 확장 가능한 스토리지 아키텍처를 제공합니다.

VVOL을 통해 VM에서는 각 VM 스토리지 오브젝트가 NetApp ONTAP에서 고유한 엔터티이므로 VM 단위로 스토리지를 사용할 수 있습니다. 볼륨 관리가 더 이상 필요하지 않은 ASA R2 시스템에서는 각 VM 스토리지 객체가 스토리지의 고유한 SU(스토리지 유닛)이며 독립적으로 제어할 수 있습니다. 따라서 개별 VM 또는 VMDK(즉, 개별 SUS)에 적용할 수 있는 스토리지 정책을 생성하여 성능, 가용성, 데이터 보호와 같은 스토리지 서비스를 세부적으로 제어할 수 있습니다.

SPBM(스토리지 정책 기반 관리)

SPBM은 가상화 환경에서 사용 가능한 스토리지 서비스와 정책을 통해 프로비저닝된 스토리지 요소 간의 추상화 계층 역할을 하는 프레임워크를 제공합니다. 이러한 접근 방식을 통해 스토리지 설계자는 다양한 기능의 스토리지 풀을 설계할 수 있습니다. 이러한 풀은 VM 관리자가 쉽게 사용할 수 있습니다. 그런 다음 관리자는 가상 머신 워크로드 요구

사항을 프로비저닝된 스토리지 풀에 일치시킬 수 있습니다. 이 접근 방식은 스토리지 관리를 단순화하고 스토리지 리소스를 더욱 효율적으로 사용할 수 있도록 합니다.

SPBM은 VVol의 핵심 구성 요소로서 스토리지 서비스 관리를 위한 정책 기반 프레임워크를 제공합니다. vSphere 관리자는 공급업체의 VASA Provider(VP)가 노출한 규칙과 기능을 사용하여 정책을 생성합니다. 성능, 가용성, 데이터 보호 등 다양한 스토리지 서비스에 대한 정책을 생성할 수 있습니다. 정책을 개별 VM 또는 VMDK에 할당하여 스토리지 서비스를 세부적으로 제어할 수 있습니다.

NetApp ONTAP 및 VVOL

NetApp ONTAP은 VVOL 확장 스토리지 산업을 선도하여 단일 클러스터에서 수십만 개의 VVOL을 지원합니다 *. 반면, 엔터프라이즈 어레이 및 소규모 플래시 어레이 공급업체는 어레이당 수천 개의 VVOL을 지원합니다. ONTAP는 VMware vSphere 환경을 위한 확장성과 효율성이 우수한 스토리지 솔루션을 제공하여 데이터 중복제거, 압축, 씬 프로비저닝, 데이터 보호 등 다양한 스토리지 서비스를 통해 VVOL을 지원합니다. SPBM을 사용하면 VMware vSphere 환경과의 원활한 통합이 가능합니다.

앞서 VM 관리자가 용량을 스토리지 풀로 사용할 수 있다고 언급했습니다. 이 작업은 vSphere에서 논리적 데이터 저장소로 표시되는 스토리지 컨테이너를 사용하여 수행됩니다.

스토리지 컨테이너는 스토리지 관리자가 생성하며 VM 관리자가 사용할 수 있는 스토리지 리소스를 그룹화하는 데 사용됩니다. 스토리지 컨테이너는 사용 중인 ONTAP 시스템의 유형에 따라 다르게 생성할 수 있습니다. 기존 ONTAP 9 클러스터의 경우 컨테이너에는 하나 이상의 백업 FlexVol 볼륨이 할당되어 함께 스토리지 풀을 구성합니다. ASA R2 시스템에서는 전체 클러스터가 스토리지 풀입니다.

> VMware vSphere 가상 볼륨, SPBM 및 ONTAP에 대한 자세한 내용은 을 참조하십시오 "TR-4400: ONTAP를 포함한 VMware vSphere 가상 볼륨".

- 플랫폼 및 프로토콜에 따라 다릅니다

데이터 저장소 및 프로토콜

vSphere 데이터 저장소 및 프로토콜 기능 개요

VMware vSphere를 ONTAP를 실행하는 시스템의 데이터 저장소에 연결하는 데 사용되는 6가지 프로토콜이 다음과 같습니다.

- FCP
- NVMe/FC
- NVMe/TCP
- iSCSI
- NFS v3
- NFS v4.1

FCP, NVMe/FC, NVMe/TCP 및 iSCSI는 vSphere VMFS(가상 머신 파일 시스템)를 사용하여 ONTAP FlexVol volume에 포함된 ONTAP LUN 또는 NVMe 네임스페이스 내에 VM을 저장하는 블록 프로토콜입니다. NFS는 VMFS 없이 VM을 데이터 저장소(단순한 ONTAP 볼륨)에 배치하는 파일 프로토콜입니다. SMB(CIFS), iSCSI, NVMe/TCP 또는 NFS를 게스트 OS에서 ONTAP로 직접 사용할 수도 있습니다.

다음 표에서는 ONTAP에서 vSphere가 지원하는 기존 데이터 저장소 기능을 보여 줍니다. 이 정보는 VVOL 데이터 저장소에 적용되지 않지만 일반적으로 지원되는 ONTAP 릴리즈를 사용하는 vSphere 6.x 이상 릴리즈에 적용됩니다.

특정 vSphere 릴리즈에 대한 을 참조하여 특정 제한을 확인할 수도 "VMware Configuration Maximums 툴"있습니다.

기능/특징	FC	iSCSI	NVMe - oF	NFS 를 참조하십시오
형식	VMFS 또는 RDM(Raw Device Mapping)	VMFS 또는 RDM	VMFS를 참조하십시오	해당 없음
최대 데이터 저장소 또는 LUN 수	호스트당 LUN 1024개	서버당 LUN 1024개	서버당 256개의 Names입니다	호스트당 256개의 NFS 연결(nconnect 및 세션 트렁킹에 의해 영향을 받음) 기본 NFS. MaxVolumes는 8입니다. VMware vSphere용 ONTAP 툴을 사용하여 256으로 늘리십시오.
최대 데이터 저장소 크기입니다	64TB	64TB	64TB	FlexGroup 볼륨에서 300TB FlexVol 볼륨 이상
최대 데이터 저장소 파일 크기입니다	62TB	62TB	62TB	ONTAP 9.12.1P2 이상이 설치된 62TB
LUN 또는 파일 시스템당 최적의 큐 크기	64-256	64-256	자동 협상	NFS.MaxQueueDepth in 을 참조하십시오 "권장되는 ESXi 호스트 및 기타 ONTAP 설정".

다음 표에는 지원되는 VMware 스토리지 관련 기능이 나와 있습니다.

용량/기능	FC	iSCSI	NVMe - oF	NFS 를 참조하십시오
마이그레이션	예	예	예	예
마이그레이션	예	예	예	예
VMware HA입니다	예	예	예	예
SDRS(Storage Distributed Resource Scheduler)	예	예	예	예
VADP(VMware vStorage APIs for Data Protection) 지원 백업 소프트웨어	예	예	예	예
VM 내의 MSCS(Microsoft Cluster Service) 또는 장애 조치 클러스터링	예	예(1	예(1	지원되지 않습니다
내결함성	예	예	예	예

용량/기능	FC	iSCSI	NVMe - oF	NFS 를 참조하십시오
Live Site Recovery/Site Recovery Manager(라이브 사이트 복구/사이트 복구 관리자)	예	예	없음 2	V3만 해당
씬 프로비저닝된 VM(가상 디스크)	예	예	예	예 VAAI를 사용하지 않는 경우 NFS에서 모든 VM에 대해 이 설정이 기본값입니다.
VMware 기본 다중 경로	예	예	예	NFS v4.1 세션 트렁킹에는 ONTAP 9.14.1 이상이 필요합니다

다음 표에는 지원되는 ONTAP 스토리지 관리 기능이 나와 있습니다.

기능/특징	FC	iSCSI	NVMe - oF	NFS 를 참조하십시오
데이터 중복제거	어레이에 대한 비용 절감	어레이에 대한 비용 절감	어레이에 대한 비용 절감	데이터 저장소의 절감 효과
씬 프로비저닝	데이터 저장소 또는 RDM	데이터 저장소 또는 RDM	데이터 저장소	데이터 저장소
데이터 저장소 크기를 조정합니다	성장만 하십시오	성장만 하십시오	성장만 하십시오	확장, 자동 확장 및 축소
Windows, Linux 애플리케이션용 SnapCenter 플러그인(게스트)	예	예	예	예
VMware vSphere용 ONTAP 툴을 사용하여 모니터링 및 호스트 구성	예	예	예	예
VMware vSphere용 ONTAP 툴을 사용하여 프로비저닝	예	예	예	예

다음 표에는 지원되는 백업 기능이 나와 있습니다.

기능/특징	FC	iSCSI	NVMe - oF	NFS 를 참조하십시오
ONTAP 스냅샷	예	예	예	예
SRM은 복제된 백업에서 지원됩니다	예	예	없음 2	V3만 해당

기능/특징	FC	iSCSI	NVMe - oF	NFS 를 참조하십시오
volume SnapMirror를 선택합니다	예	예	예	예
VMDK 이미지 액세스	SnapCenter 및 VADP 지원 백업 소프트웨어	SnapCenter 및 VADP 지원 백업 소프트웨어	SnapCenter 및 VADP 지원 백업 소프트웨어	SnapCenter 및 VADP 지원 백업 소프트웨어, vSphere Client 및 vSphere Web Client 데이터 저장소 브라우저
VMDK 파일 레벨 액세스	SnapCenter 및 VADP 지원 백업 소프트웨어, Windows만 해당	SnapCenter 및 VADP 지원 백업 소프트웨어, Windows만 해당	SnapCenter 및 VADP 지원 백업 소프트웨어, Windows만 해당	SnapCenter 및 VADP 지원 백업 소프트웨어 및 타사 애플리케이션
NDMP 세분성	데이터 저장소	데이터 저장소	데이터 저장소	데이터 저장소 또는 VM

NetApp는 VMFS 데이터 저장소에서 멀티라이터가 활성화된 VMDK 대신 Microsoft 클러스터에 게스트 내 iSCSI를 사용할 것을 권장합니다. 이 접근 방식은 Microsoft와 VMware에서 완벽하게 지원하고, ONTAP(SnapMirror-ONTAP 시스템 사내 또는 클라우드)를 통해 뛰어난 유연성을 제공하고, 구성과 자동화가 쉬우며, SnapCenter을 통해 보호할 수 있습니다. vSphere 7에 새로운 클러스터 VMDK 옵션이 추가되었습니다. 이는 멀티라이터 지원 VMDK와 다릅니다. 이 VMDK를 지원하는 VMFS 6 데이터 저장소가 필요합니다. 기타 제한 사항이 적용됩니다. 구성 지침은 VMware "Windows Server 장애 조치 클러스터링에 대한 설치"설명서를 참조하십시오.

NVMe-oF 및 NFS v4.1을 사용하는 데이터 저장소에는 vSphere 복제가 필요합니다. NFS v4.1에 대한 어레이 기반 복제는 현재 SRM에서 지원되지 않습니다. NVMe-oF를 사용한 어레이 기반 복제는 현재 VMware SRA(vSphere Storage Replication Adapter)용 ONTAP 툴에서 지원되지 않습니다.

스토리지 프로토콜 선택

ONTAP를 실행하는 시스템은 모든 주요 스토리지 프로토콜을 지원하므로 고객은 기존 및 계획된 네트워킹 인프라 및 직원 기술에 따라 환경에 가장 적합한 시스템을 선택할 수 있습니다. 역사적으로 NetApp 테스트는 일반적으로 유사한 회선 속도와 연결 수로 실행되는 프로토콜 간에는 거의 차이가 없는 것으로 나타났습니다. 그러나 NVMe-oF(NVMe/TCP 및 NVMe/FC)는 IOPS에서 상당한 향상, 지연 시간 감소, 스토리지 IO에 의한 호스트 CPU 사용량 최대 50% 이상 감소 효과를 입증했습니다. 또 다른 한편으로는, NFS는 특히 많은 수의 VM에 대해 최고의 유연성과 관리 편의성을 제공합니다. 이러한 모든 프로토콜을 VMware vSphere용 ONTAP 툴과 함께 사용 및 관리할 수 있으며, 이는 데이터 저장소를 간편하게 생성하고 관리할 수 있는 인터페이스를 제공합니다.

프로토콜 선택을 고려할 때 다음과 같은 요소가 유용할 수 있습니다.

- * 현재 운영 환경. * IT 팀은 일반적으로 이더넷 IP 인프라 관리에 능숙하지만 FC SAN 패브릭 관리에 능숙하지 않습니다. 그러나 스토리지 트래픽용으로 설계되지 않은 범용 IP 네트워크를 사용하는 것은 잘 작동하지 않을 수 있습니다. 현재 보유하고 있는 네트워킹 인프라, 계획된 개선 사항, 이를 관리할 직원의 기술 및 가용성을 고려하십시오.
- * 손쉬운 설정 * FC 패브릭의 초기 구성(추가 스위치 및 케이블 연결, 조닝, HBA 및 펌웨어의 상호 운용성 검증) 외에도 블록 프로토콜은 LUN 생성 및 매핑과 게스트 OS의 검색 및 포맷이 필요합니다. NFS 볼륨을 생성 및 내보낸 후에는 ESXi 호스트에 의해 마운트되며 사용할 수 있습니다. NFS에는 특별한 하드웨어 검증 또는 관리 펌웨어가 없습니다.
- * 관리 용이성. * SAN 프로토콜을 사용할 경우 더 많은 공간이 필요할 경우 LUN 확장, 새 크기 검색, 파일 시스템 확장 등 여러 단계가 필요합니다. LUN을 확장할 수 있지만 LUN 크기를 줄이는 것은 불가능합니다. NFS를

사용하면 위나 아래로 쉽게 사이징할 수 있으며, 이러한 크기 조정은 스토리지 시스템에서 자동화할 수 있습니다. SAN은 게스트 OS 할당 해제/TRIM/UNMAP 명령을 통해 공간 재확보를 제공하므로 삭제된 파일의 공간이 스토리지로 반환될 수 있습니다. NFS 데이터 저장소에서는 이러한 유형의 공간 재확보가 어렵지 않습니다.

- * 스토리지 공간 투명성. * 씬 프로비저닝이 즉시 절약 효과를 반환하므로 NFS 환경에서는 일반적으로 스토리지 사용률을 쉽게 확인할 수 있습니다. 마찬가지로, 같은 데이터 저장소 또는 다른 스토리지 시스템 볼륨에 있는 다른 VM에 대해서도 중복 제거 및 클론 생성 절약 효과를 즉시 사용할 수 있습니다. 일반적으로 VM 밀도는 NFS 데이터 저장소에서 더 높으며, 관리할 데이터 저장소 수를 줄여 데이터 중복 제거 비용을 절감할 수 있습니다.

데이터 저장소 레이아웃

ONTAP 스토리지 시스템은 VM 및 가상 디스크용 데이터 저장소를 유연하게 생성할 수 있습니다. ONTAP 툴을 사용하여 vSphere용 데이터 저장소를 프로비저닝할 때는 많은 ONTAP 모범 사례가 적용되지만(섹션 참조"권장되는 ESXi 호스트 및 기타 ONTAP 설정"), 다음은 고려해야 할 몇 가지 추가 지침입니다.

- ONTAP NFS 데이터 저장소를 사용하여 vSphere를 구축하면 관리가 용이한 고성능 구축이 가능하기 때문에 블록 기반 스토리지 프로토콜로는 얻을 수 없는 VM-데이터 저장소 비율을 제공할 수 있습니다. 이 아키텍처를 사용하면 데이터 저장소 밀도가 10배 증가하여 데이터 저장소 수가 서로 관련지어 줄어들 수 있습니다. 데이터 저장소가 클수록 스토리지 효율성에도 도움이 되고 운영상의 이점을 제공할 수 있지만, 하드웨어 리소스의 성능을 극대화하려면 노드당 4개 이상의 데이터 저장소(FlexVol 볼륨)를 사용하여 단일 ONTAP 컨트롤러에 VM을 저장하는 것이 좋습니다. 이 방법을 사용하면 복구 정책이 서로 다른 데이터 저장소를 설정할 수도 있습니다. 비즈니스 요구 사항에 따라 다른 사람보다 더 자주 백업하거나 복제할 수 있는 경우도 있습니다. FlexGroup 볼륨은 설계상 확장되므로 성능을 위해 여러 데이터 저장소가 필요하지 않습니다.
- * NetApp는 대부분의 NFS 데이터 저장소에 FlexVol 볼륨을 사용할 것을 권장합니다 *. ONTAP 9.8부터 FlexGroup 볼륨은 데이터 저장소로도 사용할 수 있으며, 일반적으로 특정 활용 사례에 권장됩니다. qtree와 같은 다른 ONTAP 스토리지 컨테이너는 현재 VMware vSphere용 ONTAP 툴 또는 VMware vSphere용 NetApp SnapCenter 플러그인에서 지원되지 않으므로 일반적으로 권장되지 않습니다.
- FlexVol 볼륨 데이터 저장소의 적절한 크기는 약 4TB에서 8TB입니다. 이 크기는 성능, 관리 용이성 및 데이터 보호 측면에서 우수한 균형 점입니다. 작게 시작하고(예: 4TB) 필요에 따라 데이터 저장소를 최대 300TB까지 확장할 수 있습니다. 작은 데이터 저장소가 백업이나 재해 발생 후 복구 속도가 빨라지므로 클러스터 간에 빠르게 이동할 수 있습니다. ONTAP 자동 크기 조정을 사용하면 사용된 공간이 변경될 때 볼륨을 자동으로 확대 및 축소할 수 있습니다. VMware vSphere 데이터 저장소 프로비저닝 마법사용 ONTAP 툴은 새 데이터 저장소에 대해 기본적으로 자동 크기 조정을 사용합니다. System Manager 또는 명령줄을 사용하여 확장 및 축소 임계값과 최대 및 최소 크기를 추가로 사용자 지정할 수 있습니다.
- 또는 FC, iSCSI, NVMe/FC 또는 NVMe/TCP에서 액세스하는 LUN 또는 NVMe 네임스페이스(새 ASA 시스템의 스토리지 유닛)로 VMFS 데이터 저장소를 구성할 수 있습니다. VMFS를 사용하면 클러스터의 모든 ESX Server에서 데이터 저장소를 동시에 액세스할 수 있습니다. VMFS 데이터 저장소의 크기는 최대 64TB이고 최대 32개의 2TB LUN(VMFS 3) 또는 단일 64TB LUN(VMFS 5)으로 구성될 수 있습니다. ONTAP의 최대 LUN 크기는 AFF, ASA 및 FAS 시스템에서 128TB입니다. NetApp에서는 익스텐트를 사용하는 대신 항상 각 데이터 저장소에 하나의 큰 LUN을 사용할 것을 권장합니다. NFS와 마찬가지로 단일 ONTAP 컨트롤러에서 성능을 극대화하기 위해 여러 데이터 저장소(볼륨 또는 스토리지 유닛)를 사용하는 것을 고려해 보십시오.
- 기존 게스트 운영 체제(OS)는 최고의 성능과 스토리지 효율성을 위해 스토리지 시스템과 조율해야 했습니다. 그러나 Red Hat과 같은 Microsoft 및 Linux 배포업체에서 제공하는 최신 공급업체 지원 OS는 더 이상 가상 환경에서 파일 시스템 파티션을 기본 스토리지 시스템의 블록과 일치시킬 필요가 없습니다. 정렬이 필요할 수도 있는 이전 OS를 사용 중인 경우 NetApp 지원 Knowledgebase에서 "VM 정렬"을 사용하는 문서를 검색하거나 NetApp 세일즈 또는 파트너 담당자에게 TR-3747 복사본을 요청하십시오.
- 게스트 OS 내에서 조각 모음 유틸리티를 사용하지 마십시오. 이 유틸리티는 성능 이점을 제공하지 않으며 스토리지 효율성 및 스냅샷 공간 사용에 영향을 줍니다. 또한 게스트 OS에서 가상 데스크톱에 대한 검색 인덱싱을 해제하는 것도 고려하십시오.
- ONTAP은 혁신적인 스토리지 효율성 기능으로 업계에서 최고의 가용성을 제공하므로 사용 가능한 디스크 공간을 최대한 활용할 수 있습니다. AFF 시스템은 기본 인라인 중복제거 및 압축을 사용해 이 효율성을 더욱 높여줍니다.

데이터는 애그리게이트 내 모든 볼륨에서 중복 제거되므로, 더 이상 단일 데이터 저장소 내에서 유사한 운영 체제 및 유사한 애플리케이션을 그룹화할 필요가 없으며 절약 효과를 극대화할 수 있습니다.

- 경우에 따라 데이터 저장소가 필요하지 않을 수도 있습니다. 게스트가 관리하는 NFS, SMB, NVMe/TCP 또는 iSCSI 파일 시스템과 같은 게스트 소유 파일 시스템을 고려하십시오. 구체적인 애플리케이션 지침은 해당 애플리케이션에 대한 NetApp 기술 보고서를 참조하십시오. 예를 들어, 에는 "ONTAP 기반의 Oracle 데이터베이스 "가상화에 대한 섹션과 자세한 정보가 있습니다.
- 1등급 디스크(또는 개선된 가상 디스크)는 vSphere 6.5 이상을 사용하는 VM과 독립적으로 vCenter 관리 디스크를 사용할 수 있습니다. 주로 API에서 관리되지만, VVOL은 특히 OpenStack 또는 Kubernetes 툴로 관리할 때 유용합니다. ONTAP 및 VMware vSphere용 ONTAP 툴을 통해 지원됩니다.

데이터 저장소 및 **VM** 마이그레이션

다른 스토리지 시스템의 기존 데이터 저장소에서 ONTAP로 VM을 마이그레이션할 때 다음 몇 가지 사항을 염두에 두어야 합니다.

- Storage vMotion을 사용하여 대량의 가상 머신을 ONTAP로 이동합니다. 이 접근 방식은 실행 중인 VM에 중단 없이 적용할 수 있을 뿐만 아니라 인라인 중복제거 및 압축과 같은 ONTAP 스토리지 효율성 기능을 사용하여 마이그레이션 시 데이터를 처리할 수 있습니다. vCenter 기능을 사용하여 인벤토리 목록에서 여러 VM을 선택한 다음 적절한 시간에 마이그레이션을 예약합니다(작업을 클릭하는 동안 Ctrl 키 사용).
- 적절한 대상 데이터 저장소로 마이그레이션을 신중하게 계획할 수 있지만, 대개 대량으로 마이그레이션한 다음 필요에 따라 나중에 구성하는 것이 더 간단합니다. 서로 다른 스냅샷 일정과 같은 특정 데이터 보호 요구 사항이 있는 경우 이 방법을 사용하여 다른 데이터 저장소로 마이그레이션할 수 있습니다. 또한 VM이 NetApp 클러스터에 배치되면 Storage vMotion에서 VAAI 오프로드를 사용하여 호스트 기반 복사본 없이 클러스터의 데이터 저장소 간에 VM을 이동할 수 있습니다. NFS는 전원이 켜진 VM의 Storage vMotion을 오프로드하지 않지만 VMFS는 오프로드합니다.
- 보다 신중한 마이그레이션이 필요한 가상 머신에는 연결된 스토리지를 사용하는 데이터베이스와 애플리케이션이 포함됩니다. 일반적으로 마이그레이션 관리에 애플리케이션 툴을 사용하는 것을 고려합니다. Oracle의 경우 RMAN 또는 ASM과 같은 Oracle 툴을 사용하여 데이터베이스 파일을 마이그레이션할 수 있습니다. 자세한 내용은 을 "Oracle 데이터베이스를 ONTAP 스토리지 시스템으로 마이그레이션" 참조하십시오. 마찬가지로 SQL Server의 경우 SQL Server Management Studio 또는 SnapManager for SQL Server 또는 SnapCenter와 같은 NetApp 툴을 사용하는 것이 좋습니다.

VMware vSphere용 **ONTAP** 툴

ONTAP를 실행하는 시스템과 함께 vSphere를 사용할 때 가장 중요한 모범 사례는 VMware vSphere 플러그인(이전의 가상 스토리지 콘솔)용 ONTAP 툴을 설치하고 사용하는 것입니다. 이 vCenter 플러그인은 SAN 또는 NAS, ASA, AFF, FAS 또는 ONTAP Select(VMware 또는 KVM VM에서 실행되는 소프트웨어 정의 버전 ONTAP)에서 스토리지 관리를 간소화하고 가용성을 개선하며 스토리지 비용과 운영 오버헤드를 줄여줍니다. 데이터 저장소를 프로비저닝하는 모범 사례를 사용하고 다중 경로 및 HBA 시간 초과를 위해 ESXi 호스트 설정을 최적화합니다(부록 B에 설명되어 있음). vCenter 플러그인이기 때문에 vCenter 서버에 접속하는 모든 vSphere 웹 클라이언트에서 사용할 수 있습니다.

이 플러그인은 vSphere 환경에서 다른 ONTAP 툴을 사용하는 데에도 도움이 됩니다. VMware VAAI용 NFS 플러그인을 설치하면 VM 클론 생성 작업, 일반 가상 디스크 파일에 대한 공간 예약 및 ONTAP 스냅샷 오프로드를 위해 ONTAP로 복사 오프로드를 수행할 수 있습니다.

이미지 기반 vSphere 클러스터에서는 ONTAP 툴을 사용하여 설치할 때 규정 준수 범위를 벗어나지 않도록 이미지에 NFS 플러그인을 추가할 수 있습니다.

또한, ONTAP 툴은 VASA Provider for ONTAP의 다양한 기능을 위한 관리 인터페이스로, VVOL을 통해 스토리지 정책 기반 관리를 지원합니다.

일반적으로 * NetApp는 vCenter 내에서 ONTAP Tools for VMware vSphere 인터페이스를 사용하여 기존 데이터 저장소와 VVol 데이터 저장소를 프로비저닝하여 모범 사례를 준수할 것을 권장합니다.

일반 네트워킹

ONTAP를 실행하는 시스템에서 vSphere를 사용할 때 네트워크 설정을 구성하는 것은 다른 네트워크 구성과 매우 간단하며 비슷합니다. 다음은 고려해야 할 몇 가지 사항입니다.

- 스토리지 네트워크 트래픽을 다른 네트워크와 분리합니다. 전용 VLAN 또는 스토리지에 개별 스위치를 사용하면 별도의 네트워크를 구축할 수 있습니다. 스토리지 네트워크가 업링크와 같은 물리적 경로를 공유하는 경우 충분한 대역폭을 확보하기 위해 QoS 또는 추가 업링크 포트가 필요할 수 있습니다. 호스트를 스토리지에 직접 연결하지 말고, 스위치를 사용하여 중복 경로를 확보하고 VMware HA가 개입 없이 작동할 수 있도록 하십시오. 을 참조하십시오 "직접 연결 네트워킹" 자세한 내용은 를 참조하십시오.
- 원하는 경우 점보 프레임을 사용할 수 있으며 네트워크에서 지원됩니다(특히 iSCSI 사용 시). 사용하는 경우 스토리지와 ESXi 호스트 간 경로에서 모든 네트워크 디바이스, VLAN 등에 동일하게 구성되었는지 확인합니다. 그렇지 않으면 성능 또는 연결 문제가 나타날 수 있습니다. MTU는 ESXi 가상 스위치, VMkernel 포트 및 각 ONTAP 노드의 물리적 포트 또는 인터페이스 그룹에서도 동일하게 설정되어야 합니다.
- NetApp은 ONTAP 클러스터 내 클러스터 인터커넥트 포트에서 네트워크 흐름 제어를 사용하지 않도록 설정하는 것만 권장합니다. NetApp은 데이터 트래픽에 사용되는 나머지 네트워크 포트에 대한 모범 사례를 위해 다른 권장사항을 제공하지 않습니다. 필요에 따라 활성화하거나 비활성화해야 합니다. 흐름 제어에 대한 자세한 내용은 을 "TR-4182 를 참조하십시오" 참조하십시오.
- ESXi 및 ONTAP 스토리지 어레이가 이더넷 스토리지 네트워크에 연결된 경우 * NetApp는 이러한 시스템이 RSTP(고속 스패닝 트리 프로토콜) 에지 포트로 연결되는 이더넷 포트를 구성하거나 Cisco 포트패스트 기능을 사용하여 구성할 것을 권장합니다. *NetApp는 Cisco 포트패스트 기능을 사용하고 ESXi 서버 또는 ONTAP 스토리지 어레이에 대해 802.1Q VLAN 트렁킹이 활성화된 환경에서 스패닝 트리 포트패스트 트렁크 기능을 활성화할 것을 권장합니다.
- * NetApp는 링크 집계를 위한 다음과 같은 모범 사례를 권장합니다.
  - Cisco vPC(Virtual PortChannel)와 같은 다중 섀시 링크 통합 그룹 접근 방식을 사용하여 두 개의 별도 스위치 섀시에 있는 포트의 링크 집계를 지원하는 스위치를 사용합니다.
  - LACP가 구성된 dvSwitch 5.1 이상을 사용하지 않는 한 ESXi에 연결된 스위치 포트에 대해 LACP를 사용하지 않도록 설정합니다.
  - LACP를 사용하여 포트 또는 IP 해시가 있는 동적 멀티모드 인터페이스 그룹이 있는 ONTAP 스토리지 시스템용 링크 애그리게이트를 생성합니다. 을 참조하십시오 "네트워크 관리" 추가 지침을 참조하십시오.
  - 정적 링크 통합(예: EtherChannel) 및 표준 vSwitch를 사용하거나 vSphere Distributed Switches를 사용하여 LACP 기반 링크 집계를 사용하는 경우 ESXi에서 IP 해시 팀 구성 정책을 사용하십시오. Link Aggregation을 사용하지 않는 경우 대신 "원래 가상 포트 ID를 기반으로 하는 Route"를 사용합니다.

SAN(FC, FCoE, NVMe/FC, iSCSI), RDM

vSphere에서 블록 스토리지 디바이스를 사용하는 방법에는 네 가지가 있습니다.

- VMFS 데이터 저장소 사용
- RDM(Raw Device Mapping) 사용
- VM 게스트 OS의 소프트웨어 이니시에이터가 액세스하고 제어하는 iSCSI 연결 LUN 또는 NVMe/TCP 연결 네임스페이스입니다
- VVOL 데이터 저장소 역할을 합니다

VMFS는 공유 스토리지 풀인 데이터 저장소를 제공하는 고성능 클러스터 파일 시스템입니다. VMFS 데이터 저장소는 FC, iSCSI, FCoE 또는 NVMe/FC 또는 NVMe/TCP 프로토콜을 사용하여 액세스하는 NVMe 네임스페이스를 사용하여 구성할 수 있습니다. VMFS를 사용하면 클러스터의 모든 ESX Server에서 스토리지를 동시에 액세스할 수 있습니다. 최대 LUN 크기는 일반적으로 ONTAP 9.12.1P2(ASA 시스템의 경우 이전 버전)부터 128TB이므로 단일 LUN을 사용하여 최대 크기의 VMFS 5 또는 6 데이터 저장소를 생성할 수 있습니다.

익스텐트는 여러 LUN을 "연결"하여 하나의 더 큰 데이터 저장소를 만들 수 있는 vSphere 스토리지 개념입니다. 원하는 데이터 저장소 크기에 도달하기 위해 익스텐트를 사용해서는 안 됩니다. VMFS 데이터 저장소의 경우 단일 LUN이 Best Practice입니다.

vSphere는 스토리지 디바이스에 대한 다중 경로를 기본적으로 지원합니다. vSphere는 지원되는 스토리지 시스템에 대한 스토리지 디바이스 유형을 감지하고 사용 중인 스토리지 시스템의 기능, 사용된 프로토콜의 재생성 또는 ASA, AFF, FAS 또는 소프트웨어 정의 ONTAP를 사용하는 경우 다중 경로 스택을 자동으로 구성합니다.

vSphere와 ONTAP는 모두 ALUA(Asymmetric Logical Unit Access)를 지원하여 파이버 채널 및 iSCSI에 대한 액티브/최적화 및 액티브/최적화되지 않은 경로를 설정하고 NVMe/FC 및 NVMe/TCP를 사용하는 NVMe 네임스페이스를 위한 ANA(Asymmetric Namespace Access)를 설정합니다. ONTAP에서 ALUA 또는 ANA에 최적화된 경로는 액세스 중인 LUN 또는 네임스페이스를 호스팅하는 노드에서 타겟 포트를 사용하여 직접 데이터 경로를 따릅니다. ALUA/ANA는 vSphere와 ONTAP 모두에서 기본적으로 사용하도록 설정됩니다. vSphere의 다중 경로 소프트웨어는 ONTAP 클러스터를 ALUA 또는 ANA로 인식하며 라운드 로빈 로드 밸런싱 정책을 통해 적절한 기본 플러그인을 사용합니다.

NetApp의 ASA 시스템에서는 LUN과 네임스페이스가 대칭 경로를 통해 ESXi 호스트에 제공됩니다. 즉, 모든 경로가 활성 및 최적화됩니다. vSphere의 다중 경로 소프트웨어는 ASA 시스템을 대칭으로 인식하며 라운드 로빈 로드 밸런싱 정책을 통해 적절한 기본 플러그인을 사용합니다.

최적화된 경로 다중화 설정은 을 "권장되는 ESXi 호스트 및 기타 ONTAP 설정"참조하십시오.

ESXi는 LUN, 네임스페이스 또는 경로를 제한 범위를 벗어나는 것으로 보지 않습니다. 대규모 ONTAP 클러스터에서는 LUN 제한보다 먼저 경로 제한에 도달할 수 있습니다. 이 제한을 해결하기 위해 ONTAP은 릴리즈 8.3 이상에서 선택적 LUN 맵(SLM)을 지원합니다.

ESXi에서 지원되는 최신 제한은 를 "VMware Configuration Maximums 툴"참조하십시오.

SLM은 특정 LUN에 경로를 알리는 노드를 제한합니다. NetApp 모범 사례에서는 SVM당 노드당 최소 2개의 LIF를 구축하고 SLM을 사용하여 LUN과 그 HA 파트너를 호스팅하는 노드에 보급된 경로를 제한하는 것이 좋습니다. 다른 경로가 존재하지만 기본적으로 알려지지 않습니다. SLM 내에서 ADD 및 REMOVE 노드 인수로 보급된 경로를 수정할 수 있습니다. 8.3 이전에 생성된 LUN은 모든 경로를 보급하므로 호스팅 HA 쌍에 대한 경로를 보급하기 위해서만 수정되어야 합니다. SLM에 대한 자세한 내용은 의 섹션 5.9 "TR-4080 을 참조하십시오"를 참조하십시오. 이전 portset 방법을 사용하여 LUN에 사용 가능한 경로를 더 줄일 수도 있습니다. Portsets는 igroup의 이니시에이터가 LUN을 볼 수 있는 가시적인 경로의 수를 줄여 줍니다.

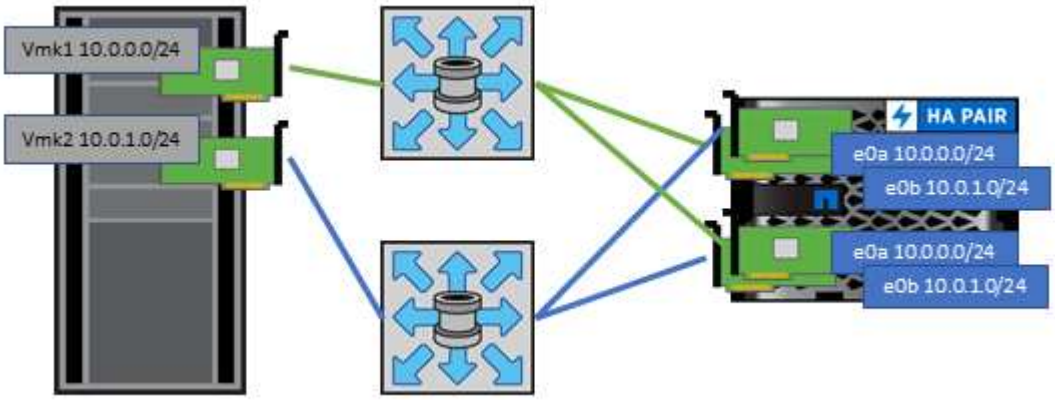
- SLM은 기본적으로 활성화되어 있습니다. 포트 세트를 사용하지 않는 경우 추가 구성이 필요하지 않습니다.
- Data ONTAP 8.3 이전에 생성된 LUN의 경우, 명령을 실행하여 LUN 보고 노드를 제거하고 LUN 소유 노드 및 해당 HA 파트너에 대한 LUN 액세스를 제한하여 SLM을 수동으로 `lun mapping remove-reporting-nodes` 적용합니다.

SCSI 기반 블록 프로토콜(iSCSI, FC 및 FCoE)은 LUN ID와 일련 번호 및 고유 이름을 사용하여 LUN에 액세스합니다. FC 및 FCoE는 WWNs 및 WWPN을 사용하며 iSCSI는 IQN(iSCSI Qualified Name)을 사용하여 포트 세트 및 SLM으로 필터링된 igroup에 대한 LUN 기반 경로를 설정합니다. NVMe 기반 블록 프로토콜은 자동으로 생성된 네임스페이스 ID를 사용하는 네임스페이스를 NVMe 서브시스템에 할당하고 해당 서브시스템을 호스트의 NVMe

Qualified Name(NQN)에 매핑하여 관리됩니다. FC 또는 TCP와 관계없이 NVMe 네임스페이스는 WWPN 또는 WWNN이 아니라 NQN을 사용하여 매핑됩니다. 그런 다음 호스트는 매핑된 하위 시스템에 대한 소프트웨어 정의 컨트롤러를 만들어 해당 네임스페이스를 액세스합니다. ONTAP 내부 LUN 및 네임스페이스 경로는 블록 프로토콜에서는 의미가 없으며 프로토콜에서는 제공되지 않습니다. 따라서 LUN만 포함된 볼륨은 내부적으로 마운트할 필요가 없으며, 데이터 저장소에 사용되는 LUN이 포함된 볼륨에는 접합 경로가 필요하지 않습니다.

기타 모범 사례:

- "권장되는 ESXi 호스트 및 기타 ONTAP 설정"VMware와 공동으로 NetApp에서 권장하는 설정을 확인합니다.
- 가용성과 이동성을 극대화하기 위해 ONTAP 클러스터의 각 노드에서 논리 인터페이스(LIF)를 생성해야 합니다. ONTAP SAN 모범 사례는 노드당 물리적 포트 2개와 LIF를 각 패브릭에 대해 하나씩 사용하는 것입니다. ALUA는 경로를 구문 분석하고 활성 최적화(직접) 경로와 최적화되지 않은 활성 경로를 식별하는 데 사용됩니다. ALUA는 FC, FCoE 및 iSCSI에 사용됩니다.
- iSCSI 네트워크의 경우 여러 가상 스위치가 있을 때 NIC 티밍을 사용하여 서로 다른 네트워크 서브넷에 있는 여러 VMkernel 네트워크 인터페이스를 사용합니다. 또한 여러 물리적 스위치에 연결된 여러 물리적 NIC를 사용하여 HA를 제공하고 처리량을 늘릴 수 있습니다. 다음 그림은 다중 경로 연결의 예입니다. ONTAP에서 둘 이상의 스위치에 연결된 2개 이상의 링크를 사용하여 페일오버에 단일 모드 인터페이스 그룹을 구성하거나 LACP 또는 다중 모드 인터페이스 그룹과 함께 다른 Link-Aggregation 기술을 사용하여 HA와 링크 집계의 이점을 제공합니다.
- 대상 인증을 위해 ESXi에서 CHAP(Challenge-Handshake Authentication Protocol)를 사용하는 경우 CLI를 사용하여 ONTAP에서도 구성해야 합니다 (`vserver iscsi security create`) 또는 System Manager를 사용할 경우(스토리지 > SVM > SVM 설정 > 프로토콜 > iSCSI에서 이니시에이터 보안 편집).
- VMware vSphere용 ONTAP 툴을 사용하여 LUN 및 igroup을 생성하고 관리합니다. 이 플러그인은 서버의 WWPN을 자동으로 확인하여 적절한 igroup을 생성합니다. 또한 모범 사례에 따라 LUN을 구성하고 올바른 igroup에 매핑합니다.
- RDM은 관리하기가 더 어려울 수 있고 앞에서 설명한 대로 제한된 경로를 사용할 수도 있으므로 주의해서 사용합니다. ONTAP LUN은 둘 다 지원합니다 "물리적 및 가상 호환성 모드" RDM
- vSphere 7.0에서 NVMe/FC를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오 "ONTAP NVMe/FC 호스트 구성 가이드" 및 "TR-4684를 참조하십시오"다음 그림에서는 vSphere 호스트에서 ONTAP LUN으로의 다중 경로 연결을 보여 줍니다.



NFS 를 참조하십시오

ONTAP은 특히 엔터프라이즈급 스케일아웃 NAS 어레이입니다. ONTAP를 사용하면 VMware vSphere가 여러 ESXi 호스트에서 NFS 연결 데이터 저장소에 동시에 액세스할 수 있으므로 VMFS 파일 시스템에 적용되는 제한을 훨씬 초과합니다. vSphere와 함께 NFS를 사용하면 섹션에서 언급한 것처럼 사용 편의성 및 스토리지 효율성 가시성의 이점을 얻을 수 "데이터

저장소"있습니다.

vSphere와 함께 ONTAP NFS를 사용할 때는 다음과 같은 Best Practice를 따르는 것이 좋습니다.

- VMware vSphere용 ONTAP 툴 사용(가장 중요한 모범 사례):
  - VMware vSphere용 ONTAP 툴을 사용하면 엑스포트 정책의 관리를 자동으로 간소화할 수 있으므로 데이터 저장소를 프로비저닝할 수 있습니다.
  - 플러그인을 사용하여 VMware 클러스터용 데이터 저장소를 생성할 때 단일 ESX Server가 아닌 클러스터를 선택합니다. 이 옵션을 선택하면 데이터 저장소가 클러스터의 모든 호스트에 자동으로 마운트됩니다.
  - 플러그인 마운트 기능을 사용하여 기존 데이터 저장소를 새 서버에 적용합니다.
  - VMware vSphere용 ONTAP 툴을 사용하지 않는 경우 모든 서버 또는 추가 액세스 제어가 필요한 각 서버 클러스터에 대해 단일 엑스포트 정책을 사용하십시오.
- ONTAP 클러스터의 각 노드에서 각 SVM에 대해 단일 논리 인터페이스(LIF)를 사용합니다. 데이터 저장소당 LIF의 과거 권장사항은 더 이상 필요하지 않습니다. 직접 액세스(LIF 및 동일한 노드의 데이터 저장소)가 가장 좋지만 성능 영향이 일반적으로 최소(마이크로초)이기 때문에 간접 액세스에 대해 걱정하지 마십시오.
- FPolicy를 사용하는 경우 VM 전원이 켜질 때마다 vSphere에서 잠금을 위해 .lck 파일을 사용하므로 .lck 파일을 제외해야 합니다.
- 현재 지원되는 모든 VMware vSphere 버전은 NFS v3 및 v4.1을 모두 사용할 수 있습니다. nconnect에 대한 공식 지원이 NFS v3용 vSphere 8.0 업데이트 2와 NFS v4.1용 업데이트 3에 추가되었습니다. NFS v4.1의 경우 vSphere는 세션 트렁킹, Kerberos 인증 및 무결성을 통한 Kerberos 인증을 계속 지원합니다. 세션 트렁킹에는 ONTAP 9.14.1 이상 버전이 필요합니다. nconnect 기능에 대한 자세한 내용과 에서 성능을 향상시키는 방법에 대해 알아볼 수 있습니다"NFSv3 nconnect 기능: NetApp 및 VMware".

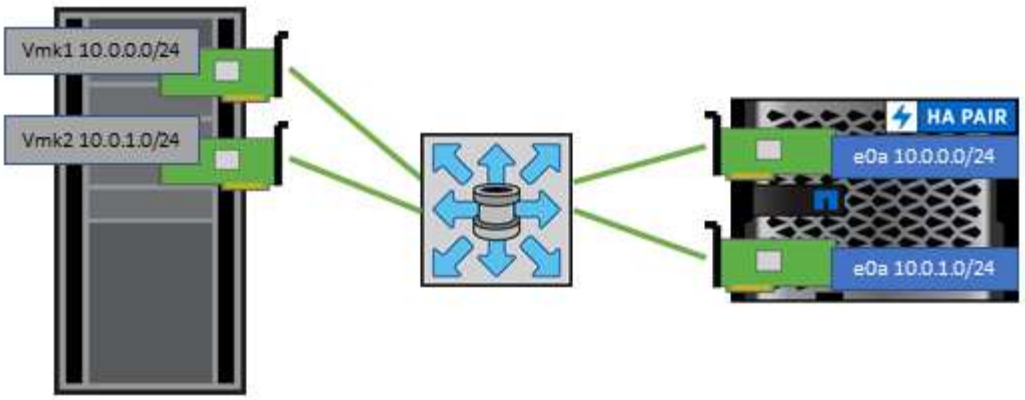
  

  - vSphere 8에서 nconnect의 최대값은 4이고 기본값은 1입니다. vSphere의 최대 값 제한은 고급 설정을 통해 호스트별로 높일 수 있지만 일반적으로 필요하지 않습니다.
  - 단일 TCP 연결이 제공할 수 있는 것보다 더 높은 성능이 필요한 환경에는 4가 권장됩니다.
  - ESXi의 NFS 연결은 256개로 제한되며, 각 nconnect 연결은 이 합계에 대해 계산됩니다. 예를 들어 nconnect=4인 데이터 저장소 2개는 총 8개의 연결로 계산됩니다.
  - 운영 환경에 대규모 변경을 구현하기 전에 nconnect가 환경에 미치는 성능 영향을 테스트하는 것이 중요합니다.
- NFSv3과 NFSv4.1은 서로 다른 잠금 메커니즘을 사용한다는 점을 유의해야 합니다. NFSv3은 클라이언트 측 잠금을 사용하는 반면 NFSv4.1은 서버 측 잠금을 사용합니다. 두 프로토콜을 통해 ONTAP 볼륨을 내보낼 수 있지만 ESXi는 하나의 프로토콜을 통해서만 데이터 저장소를 마운트할 수 있습니다. 그러나 다른 ESXi 호스트가 다른 버전을 통해 동일한 데이터 저장소를 마운트할 수 없다는 의미는 아닙니다. 문제를 방지하려면 마운트할 때 사용할 프로토콜 버전을 지정하고 모든 호스트가 동일한 버전과 동일한 잠금 스타일을 사용하도록 해야 합니다. 여러 호스트에 NFS 버전을 혼합하여 사용하지 않는 것이 중요합니다. 가능한 경우 호스트 프로필을 사용하여 준수 여부를 확인합니다.
  - NFSv3과 NFSv4.1 간에는 자동 데이터 저장소가 변환되지 않으므로 새로운 NFSv4.1 데이터 저장소를 생성하고 Storage vMotion을 사용하여 VM을 새 데이터 저장소로 마이그레이션합니다.
  - 지원에 필요한 특정 ESXi 패치 수준은 의 NFS v4.1 Interoperability 표 참고 사항을 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.
- 에 나와 있는 것처럼 "설정"Kubernetes용 vSphere CSI를 사용하지 않는 경우 에 따라 newSyncInterval을 설정해야 합니다 "VMware KB 386364"
- NFS 내보내기 정책 규칙은 vSphere 호스트의 액세스를 제어하는 데 사용됩니다. 여러 볼륨(데이터 저장소)에

하나의 정책을 사용할 수 있습니다. NFS에서 ESXi는 sys(UNIX) 보안 스타일을 사용하며 VM을 실행하려면 루트 마운트 옵션이 필요합니다. ONTAP에서 이 옵션을 수퍼 유저라고 하며, 수퍼유저 옵션을 사용할 때 익명 사용자 ID를 지정할 필요가 없습니다. 의 값이 다른 엑스포트 정책 규칙으로 `-anon -allow-suid` 인해 ONTAP 툴에서 SVM 검색 문제가 발생할 수 있습니다. IP 주소는 데이터 저장소를 마운트하는 vmkernel 포트 주소의 공백이 없는 쉼표로 구분된 목록이어야 합니다. 다음은 샘플 정책 규칙입니다.

  - 액세스 프로토콜: NFS(NFS3 및 nfs4 모두 포함)
  - 클라이언트 일치 호스트 이름, IP 주소, 넷그룹 또는 도메인 목록: 192.168.42.21,192.168.42.22
  - RO 액세스 규칙: 모두
  - RW 액세스 규칙: 모두
  - 익명 사용자가 매핑되는 사용자 ID: 65534
  - 고급 사용자 보안 유형: 모두
  - SetAttr:true에서 setuid 비트를 지정합니다
  - 디바이스 생성 허용: true

- VMware VAAI용 NetApp NFS 플러그인을 사용하는 경우 내보내기 정책 규칙이 생성되거나 수정될 때 프로토콜을 설정해야 `nfs` 합니다. VAAI 복사본 오프로드가 작동하려면 NFSv4 프로토콜이 필요하며, 프로토콜을 에 NFSv3 및 NFSv4 버전이 자동으로 포함되도록 지정해야 `nfs` 합니다. 데이터 저장소 유형이 NFS v3으로 생성된 경우에도 필요합니다.
- NFS 데이터 저장소 볼륨은 SVM의 루트 볼륨에서 접합되므로 ESXi에서 루트 볼륨에 액세스하여 데이터 저장소 볼륨을 탐색하고 마운트해야 합니다. 루트 볼륨 및 데이터 저장소 볼륨의 교차점이 중첩된 다른 볼륨에 대한 내보내기 정책에는 읽기 전용 액세스를 부여하는 ESXi 서버에 대한 규칙 또는 규칙이 포함되어야 합니다. 다음은 VAAI 플러그인을 사용하는 루트 볼륨에 대한 샘플 정책입니다.
  - 액세스 프로토콜: NFS
  - 클라이언트 일치 사양: 192.168.42.21,192.168.42.22
  - ro 액세스 규칙: sys
  - RW 액세스 규칙: 사용 안 함(루트 볼륨에 대한 최상의 보안)
  - 익명 UID
  - 슈퍼유저:sys(VAAI를 사용하는 루트 볼륨에도 필요)
- ONTAP는 접합을 사용하여 트리에서 볼륨을 정렬하는 유연한 볼륨 네임스페이스 구조를 제공하지만, 이 접근 방식에는 vSphere의 가치가 없습니다. 스토리지의 네임스페이스 계층에 관계없이 데이터 저장소의 루트에 각 VM에 대한 디렉토리를 생성합니다. 따라서 가장 좋은 방법은 SVM의 루트 볼륨에서 vSphere의 볼륨에 대한 접합 경로를 마운트하는 것입니다. 이것이 바로 VMware vSphere용 ONTAP 툴이 데이터 저장소를 프로비저닝하는 방법입니다. 중첩된 연결 경로가 없다는 것은 루트 볼륨 이외의 볼륨에 종속되지 않으며 볼륨을 오프라인으로 전환하거나 의도적으로 파괴하더라도 다른 볼륨에 대한 경로에 영향을 주지 않는다는 것을 의미합니다.
- NFS 데이터 저장소의 NTFS 파티션에 4K 블록 크기가 적합합니다. 다음 그림에서는 vSphere 호스트에서 ONTAP NFS 데이터 저장소로의 접속을 보여 줍니다.



다음 표에는 NFS 버전 및 지원되는 기능이 나와 있습니다.

vSphere 기능	**NFSv3**	**NFSv4.1**
vMotion 및 Storage vMotion입니다	예	예
고가용성	예	예
내결함성	예	예
DRS	예	예
호스트 프로파일	예	예
Storage DRS를 참조하십시오	예	아니요
스토리지 I/O 제어	예	아니요
SRM	예	아니요
가상 볼륨	예	아니요
하드웨어 가속(VAAI)	예	예
Kerberos 인증	아니요	예(AES, krb5i를 지원하도록 vSphere 6.5 이상에서 향상)
다중 경로 지원	아니요	예(ONTAP 9.14.1)

FlexGroup 볼륨

ONTAP 및 FlexGroup 볼륨을 VMware vSphere와 함께 사용하면 전체 ONTAP 클러스터의 모든 성능을 활용하는, 간단하고 확장 가능한 데이터 저장소를 만들 수 있습니다.

ONTAP 9.8은 VMware vSphere 9.8-9.13용 ONTAP 툴 및 VMware 4.4 이상 릴리즈용 SnapCenter 플러그인과 함께 vSphere에서 FlexGroup 볼륨 지원 데이터 저장소에 대한 지원이 추가되었습니다. FlexGroup 볼륨은 대규모 데이터 저장소 생성을 단순화하고 ONTAP 클러스터에 필요한 분산 구성 볼륨을 자동으로 생성하여 ONTAP 시스템의 성능을 극대화합니다.

전체 ONTAP 클러스터의 성능을 지원하는 확장 가능한 단일 vSphere 데이터 저장소가 필요하거나 클론 캐시를 지속적으로 워밍업하여 FlexGroup 클론 복제 메커니즘의 이점을 누릴 수 있는 매우 큰 클론 복제 워크로드가 있는 경우 vSphere와 함께 FlexGroup 볼륨을 사용하십시오.

복사본 오프로드

ONTAP 9.8에는 vSphere 워크로드를 사용한 광범위한 시스템 테스트 외에도 FlexGroup 데이터 저장소에 대한 새로운 복제 오프로드 메커니즘이 추가되었습니다. 이 새로운 시스템은 향상된 복제 엔진을 사용하여 백그라운드에서 구성 요소 간에 파일을 복제하면서 소스와 대상에 모두 액세스할 수 있도록 합니다. 그런 다음 이 구성 로컬 캐시를 사용하여 필요 시 VM 클론을 빠르게 인스턴스화합니다.

FlexGroup 최적화 복사본 오프로드를 활성화하려면 을 참조하십시오 "VAAI 복사 오프로드를 허용하도록 ONTAP FlexGroup 볼륨을 구성하는 방법"

VAAI 클로닝을 사용하지만 캐시를 따뜻하게 유지할 만큼 클론을 생성하지 않으면 클론이 호스트 기반 복제본보다 빠를 수 있습니다. 이 경우 필요에 맞게 캐시 시간 제한을 조정할 수 있습니다.

다음 시나리오를 고려해 보십시오.

- 8개 구성 요소로 구성된 새 FlexGroup를 만들었습니다
- 새 FlexGroup에 대한 캐시 시간 초과는 160분으로 설정됩니다

이 시나리오에서는 처음 8개의 클론이 로컬 파일 클론이 아닌 전체 복제본이 됩니다. 160초 시간 초과가 만료되기 전에 해당 VM을 추가로 클로닝할 경우 각 구성 요소 내의 파일 클론 엔진을 라운드 로빈 방식으로 사용하여 구성 볼륨에 거의 즉각적으로 생성되는 복사본을 생성합니다.

볼륨이 수신하는 모든 새 클론 작업은 시간 초과를 재설정합니다. 예제 FlexGroup의 구성 볼륨이 시간 초과 전에 클론 요청을 수신하지 못하면 해당 특정 VM의 캐시가 지워지고 볼륨을 다시 채워야 합니다. 또한 원본 클론의 소스가 변경된 경우(예: 템플릿을 업데이트함) 충돌을 방지하기 위해 각 구성요소의 로컬 캐시가 무효화됩니다. 앞서 설명한 대로 캐시는 튜닝 가능하며 운영 환경의 요구 사항에 맞게 설정할 수 있습니다.

VAAI에서 FlexGroup 볼륨을 사용하는 방법에 대한 자세한 내용은 다음 KB 문서를 참조하십시오. "VAAI: FlexGroup 볼륨에서 캐싱은 어떻게 작동합니까?"

FlexGroup 캐시를 최대한 활용할 수 없지만 신속한 볼륨 간 클로닝이 필요한 환경에서는 VVOL을 사용하는 것이 좋습니다. VVOL을 통한 교차 볼륨 클로닝은 기존 데이터 저장소를 사용하는 것보다 훨씬 빠르며 캐시에 의존하지 않습니다.

QoS 설정

ONTAP System Manager 또는 클러스터 쉘을 사용하여 FlexGroup 레벨에서 QoS를 구성할 수는 있지만, VM 인식 또는 vCenter 통합을 제공하지 않습니다.

QoS(최대/최소 IOPS)는 vCenter UI에서 개별 VM 또는 해당 시점의 데이터 저장소에 있는 모든 VM에 설정하거나 ONTAP 툴을 사용하여 REST API를 통해 설정할 수 있습니다. 모든 VM에서 QoS를 설정하면 별도의 VM별 설정이 대체됩니다. 설정은 향후 새 VM이나 마이그레이션된 VM으로 확장되지 않습니다. 새 VM에 QoS를 설정하거나 데이터 저장소의 모든 VM에 QoS를 다시 적용하십시오.

VMware vSphere는 NFS 데이터 저장소의 모든 입출력을 호스트당 단일 대기열로 처리하며, 한 VM의 QoS 임계치 조절은 해당 호스트의 동일한 데이터 저장소에 있는 다른 VM의 성능에 영향을 미칠 수 있습니다. 이는 다른 데이터 저장소로 마이그레이션할 경우 QoS 정책 설정을 유지할 수 있고 임계치 조절 시 다른 VM의 입출력에 영향을 주지 않는 VVOL과 다릅니다.

메트릭

ONTAP 9.8에는 FlexGroup 파일에 대한 새로운 파일 기반 성능 메트릭(IOPS, 처리량, 지연 시간)도 추가되었으며, 이러한 메트릭은 VMware vSphere 대시보드 및 VM 보고서용 ONTAP 툴에서 확인할 수 있습니다. VMware vSphere

플러그인용 ONTAP 툴을 사용하면 최대 및/또는 최소 IOPS의 조합을 사용하여 서비스 품질(QoS) 규칙을 설정할 수도 있습니다. 데이터 저장소의 모든 VM에 대해 또는 특정 VM에 대해 개별적으로 설정할 수 있습니다.

모범 사례

- ONTAP 툴을 사용하여 FlexGroup 데이터 저장소를 생성하여 FlexGroup를 최적으로 생성하고 vSphere 환경에 맞게 엑스포트 정책을 구성할 수 있습니다. 그러나 ONTAP 툴을 사용하여 FlexGroup 볼륨을 생성한 후에는 vSphere 클러스터의 모든 노드에서 단일 IP 주소를 사용하여 데이터 저장소를 마운트하는 것을 확인할 수 있습니다. 이로 인해 네트워크 포트에 병목 현상이 발생할 수 있습니다. 이 문제를 방지하려면 데이터 저장소를 마운트 해제한 다음 SVM의 LIF 간 로드 밸런싱을 수행하는 라운드 로빈 DNS 이름을 사용하여 표준 vSphere 데이터 저장소 마법사를 사용하여 데이터 저장소를 다시 마운트합니다. 다시 마운트하면 ONTAP 툴이 다시 데이터 저장소를 관리할 수 있습니다. ONTAP 도구를 사용할 수 없는 경우 FlexGroup 기본값을 사용하고 의 지침에 따라 내보내기 정책을 만듭니다 "데이터 저장소 및 프로토콜 - NFS".
- FlexGroup 데이터 저장소를 사이징할 때 FlexGroup는 더 큰 네임스페이스를 생성하는 여러 개의 작은 FlexVol 볼륨으로 구성되어 있습니다. 따라서 데이터 저장소의 크기를 최대 VMDK 파일 크기의 8배(기본 8개 구성 요소로 가정) 이상이어야 하고 사용되지 않은 여유 공간은 10-20%가 되도록 하여 유연하게 재조정할 수 있습니다. 예를 들어 환경에 6TB VMDK가 있는 경우 FlexGroup 데이터 저장소의 크기를 52.8TB(6x8 + 10%) 이하로 조정하십시오.
- VMware와 NetApp는 ONTAP 9.14.1부터 NFSv4.1 세션 트렁킹을 지원합니다. 구체적인 버전에 대한 자세한 내용은 NetApp NFS 4.1 상호 운용성 매트릭스 툴(IMT) 참고 사항을 참조하십시오. NFSv3은 볼륨에 대한 여러 물리적 경로를 지원하지 않지만, vSphere 8.0U2부터 nconnect는 지원합니다. nconnect에 대한 자세한 내용은 을 "NFSv3 nConnect 기능을 지원하는 NetApp 및 VMware"참조하십시오.
- 복제 오프로드에 VMware VAAI용 NFS 플러그인을 사용하십시오. 앞에서 설명한 것처럼 FlexGroup 데이터 저장소 내에서 클론 생성이 향상되지만 FlexVol 및/또는 FlexGroup 볼륨 간에 VM을 복사할 때 ONTAP는 ESXi 호스트 복사본에 비해 상당한 성능 이점을 제공하지 않습니다. 따라서 VAAI 또는 FlexGroup 볼륨을 사용하기로 결정할 때 클론 복제 워크로드를 고려하십시오. 구성 볼륨의 수를 수정하는 것이 FlexGroup 기반 클로닝을 최적화하는 한 가지 방법입니다. AS는 앞서 언급한 캐시 시간 초과를 튜닝합니다.
- VMware vSphere 9.8-9.13용 ONTAP 툴을 사용하면 ONTAP 메트릭(대시보드 및 VM 보고서)을 사용하여 FlexGroup VM의 성능을 모니터링하고 개별 VM의 QoS를 관리할 수 있습니다. 이러한 메트릭은 현재 ONTAP 명령 또는 API를 통해 사용할 수 없습니다.
- VMware vSphere 릴리즈 4.4 이상용 SnapCenter 플러그인은 운영 스토리지 시스템의 FlexGroup 데이터 저장소에 있는 VM의 백업 및 복구를 지원합니다. SCV 4.6은 FlexGroup 기반 데이터 저장소에 대한 SnapMirror 지원을 추가합니다. 스토리지 기반 스냅샷 및 복제를 사용하는 것이 데이터를 보호하는 가장 효율적인 방법입니다.

네트워크 구성

ONTAP를 실행하는 시스템에서 vSphere를 사용할 때 네트워크 설정을 구성하는 것은 다른 네트워크 구성과 매우 간단하며 비슷합니다.

다음은 고려해야 할 몇 가지 사항입니다.

- 스토리지 네트워크 트래픽을 다른 네트워크와 분리합니다. 전용 VLAN 또는 스토리지에 개별 스위치를 사용하면 별도의 네트워크를 구축할 수 있습니다. 스토리지 네트워크가 업링크와 같은 물리적 경로를 공유하는 경우 충분한 대역폭을 확보하기 위해 QoS 또는 추가 업링크 포트가 필요할 수 있습니다. 솔루션 가이드에서 특별히 요구하지 않는 한 호스트를 스토리지에 직접 연결하지 마십시오. 스위치를 사용하여 중복 경로를 확보하고 VMware HA가 개입 없이 작동할 수 있습니다.
- 네트워크에서 지원하는 경우 점보 프레임을 사용해야 합니다. 사용하는 경우 스토리지와 ESXi 호스트 간 경로에서 모든 네트워크 디바이스, VLAN 등에 동일하게 구성되었는지 확인합니다. 그렇지 않으면 성능 또는 연결 문제가 나타날 수 있습니다. MTU는 ESXi 가상 스위치, VMkernel 포트 및 각 ONTAP 노드의 물리적 포트 또는 인터페이스 그룹에서도 동일하게 설정되어야 합니다.

- NetApp은 ONTAP 클러스터 내 클러스터 인터커넥트 포트에서 네트워크 흐름 제어를 사용하지 않도록 설정하는 것만 권장합니다. NetApp는 데이터 트래픽에 사용되는 나머지 네트워크 포트의 흐름 제어와 관련된 모범 사례에 대한 다른 권장 사항은 없습니다. 필요에 따라 활성화 또는 비활성화해야 합니다. 흐름 제어에 대한 자세한 내용은 을 "TR-4182 를 참조하십시오" 참조하십시오.
- ESXi 및 ONTAP 스토리지 어레이가 이더넷 스토리지 네트워크에 연결되어 있는 경우, 이러한 시스템이 RSTP(Rapid Spanning Tree Protocol) 에지 포트로 연결되거나 Cisco PortFast 기능을 사용하여 연결되는 이더넷 포트를 구성하는 것이 좋습니다. Cisco PortFast 기능을 사용하고 ESXi 서버 또는 ONTAP 스토리지 어레이에 802.1Q VLAN 트렁킹을 사용하는 환경에서는 스패닝 트리 포트패스트 트렁크 기능을 활성화하는 것이 좋습니다.
- Link Aggregation에 대해 다음 모범 사례를 따르는 것이 좋습니다.
  - Cisco vPC(Virtual PortChannel)와 같은 다중 섀시 링크 통합 그룹 접근 방식을 사용하여 두 개의 별도 스위치 섀시에 있는 포트의 링크 집계를 지원하는 스위치를 사용합니다.
  - LACP가 구성된 dvSwitch 5.1 이상을 사용하지 않는 한 ESXi에 연결된 스위치 포트에 대해 LACP를 사용하지 않도록 설정합니다.
  - LACP를 사용하여 IP 해시를 사용하는 동적 멀티모드 인터페이스 그룹을 통해 ONTAP 스토리지 시스템에 대한 링크 애그리게이트를 생성합니다.
  - ESXi에서 IP 해시 팀 구성 정책을 사용합니다.

다음 표에는 네트워크 구성 항목에 대한 요약과 설정이 적용되는 위치가 나와 있습니다.

항목	**ESXi**	스위치	노드	**SVM**
IP 주소입니다	VMkernel	아니요**	아니요**	예
Link Aggregation	가상 스위치	예	예	아니요 *
VLAN	VMkernel 및 VM 포트 그룹	예	예	아니요 *
흐름 제어	NIC	예	예	아니요 *
스패닝 트리	아니요	예	아니요	아니요
MTU(점보 프레임의 경우)	가상 스위치 및 VMkernel 포트(9000)	예(최대로 설정)	예(9000)	아니요 *
페일오버 그룹	아니요	아니요	예(생성)	예(선택)

- SVM LIF는 VLAN, MTU 및 기타 설정이 있는 포트, 인터페이스 그룹 또는 VLAN 인터페이스에 연결됩니다. 하지만 SVM 레벨에서 설정을 관리하지 않습니다.
  - 이러한 디바이스에는 자체 관리 IP 주소가 있지만 이러한 주소는 ESXi 스토리지 네트워킹의 맥락에서 사용되지 않습니다.

SAN(FC, NVMe/FC, iSCSI, NVMe/TCP), RDM

ONTAP은 기존 iSCSI 및 파이버 채널 프로토콜(FCP)을 사용하는 VMware vSphere용 엔터프라이즈급 블록 스토리지와 매우 효율적이고 성능이 우수한 차세대 블록 프로토콜, NVMe-oF(NVMe over Fabrics)를 제공하며 NVMe/FC 및 NVMe/TCP를 모두 지원합니다.

vSphere 및 ONTAP를 사용하여 VM 스토리지에 블록 프로토콜을 구현하는 Best Practice는 를 참조하십시오 "데이터 저장소 및 프로토콜 - SAN"

NFS 를 참조하십시오

vSphere를 사용하면 엔터프라이즈급 NFS 스토리지를 사용하여 ESXi 클러스터의 모든 노드에 대한 데이터 저장소에 대한 동시 액세스를 제공할 수 있습니다. 섹션에서 언급한 것처럼 "데이터 저장소"vSphere와 함께 NFS를 사용할 경우 사용 편의성 및 스토리지 효율성 가시성의 이점을 얻을 수 있습니다.

권장되는 모범 사례는 를 참조하십시오 "데이터 저장소 및 프로토콜 - NFS"

직접 연결 네트워킹

스토리지 관리자는 구성에서 네트워크 스위치를 제거하여 인프라를 단순화하기를 원할 수도 있습니다. 일부 시나리오에서는 이 기능이 지원될 수 있습니다. 하지만 몇 가지 제한 사항과 주의사항이 있습니다.

iSCSI 및 NVMe/TCP

iSCSI 또는 NVMe/TCP를 사용하는 호스트는 스토리지 시스템에 직접 연결하여 정상적으로 작동할 수 있습니다. 그 이유는 경로 지정입니다. 두 개의 서로 다른 스토리지 컨트롤러에 직접 연결되므로 데이터 흐름을 위한 두 개의 독립적 경로가 됩니다. 경로, 포트 또는 컨트롤러가 손실되어도 다른 경로가 사용되지 않습니다.

NFS 를 참조하십시오

직접 연결 NFS 스토리지를 사용할 수 있지만 중대한 제한 사항이 있는 경우 스크립팅의 상당한 노력 없이는 페일오버가 수행되지 않으며 고객의 책임입니다.

직접 연결 NFS 스토리지에서 무중단 페일오버가 복잡해지는 이유는 로컬 OS에서 발생하는 라우팅입니다. 예를 들어, 호스트의 IP 주소가 192.168.1.1/24이고 IP 주소가 192.168.1.50/24인 ONTAP 컨트롤러에 직접 연결되어 있다고 가정합니다. 장애 조치 중에 192.168.1.50 주소는 다른 컨트롤러로 장애 조치될 수 있으며 호스트에서 사용할 수 있지만 호스트는 어떻게 그 존재를 감지합니까? 원래 192.168.1.1 주소는 더 이상 운영 체제에 연결되지 않는 호스트 NIC에 계속 존재합니다. 192.168.1.50으로 향하는 트래픽은 작동하지 않는 네트워크 포트로 계속 전송됩니다.

두 번째 OS NIC를 19로 구성할 수 있습니다 2.168.1.2 및 은 192.168.1.50을 통해 실패한 주소와 통신할 수 있지만, 로컬 라우팅 테이블은 기본적으로 192.168.1.0/24 서브넷과 통신하는 데 하나의 * 및 하나의 * 주소만 사용합니다. sysadmin은 실패한 네트워크 연결을 감지하고 로컬 라우팅 테이블을 변경하거나 인터페이스를 가동 및 중지시키는 스크립팅 프레임워크를 생성할 수 있습니다. 정확한 절차는 사용 중인 운영 체제에 따라 다릅니다.

실제로 NetApp 고객은 직접 연결 NFS를 가지고 있지만 일반적으로 페일오버 중에 IO가 일시 중지되는 워크로드에만 해당됩니다. 하드 마운트를 사용하는 경우 이러한 일시 중지 중에는 입출력 오류가 발생하지 않아야 합니다. 호스트의 NIC 간에 IP 주소를 이동하기 위해 페일백이나 수동 작업으로 인해 서비스가 복구될 때까지 입출력이 중지되어야 합니다.

FC 직접 연결

호스트를 FC 프로토콜을 사용하여 ONTAP 스토리지 시스템에 직접 연결할 수는 없습니다. NPIV를 사용하기 때문입니다. FC 네트워크에 대한 ONTAP FC 포트를 식별하는 WWN은 NPIV라는 가상화 유형을 사용합니다. ONTAP 시스템에 연결된 모든 디바이스가 NPIV WWN을 인식할 수 있어야 합니다. 현재 NPIV 타겟을 지원할 수 있는 호스트에 설치할 수 있는 HBA를 제공하는 HBA 공급업체는 없습니다.

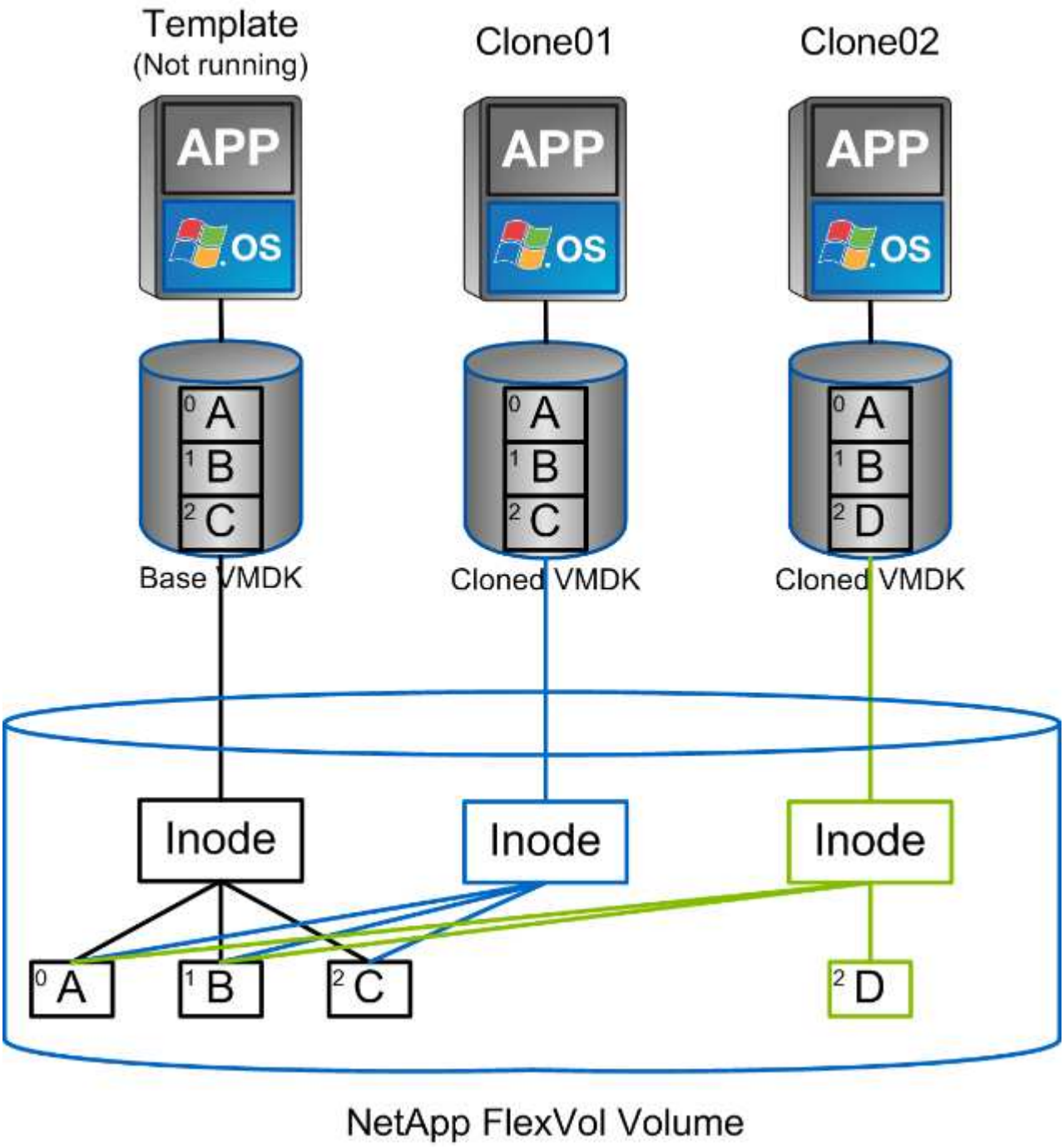
VM 및 데이터 저장소 클론 생성

스토리지 객체를 클론 복제하면 추가 VM 프로비저닝, 백업/복구 작업 등과 같은 추가 사용을 위한 복사본을 빠르게 생성할 수 있습니다.

vSphere에서 VM, 가상 디스크, VVOL 또는 데이터 저장소를 복제할 수 있습니다. 복제된 개체는 대개 자동화된 프로세스를 통해 추가로 사용자 지정할 수 있습니다. vSphere는 전체 복제본 클론과 연결된 클론을 모두 지원하며, 이 클론에서는 원래 객체와 별도로 변경 사항을 추적합니다.

연결된 클론은 공간을 절약하는 데 좋지만 vSphere에서 VM에 대해 처리하는 I/O 양을 늘려 해당 VM 및 호스트의 성능에 영향을 줄 수 있습니다. 따라서 NetApp 고객은 스토리지 시스템 기반 복제본을 사용하여 두 가지 이점을 모두 최대한 활용할 수 있습니다. 즉, 효율적인 스토리지 사용과 향상된 성능을 모두 활용할 수 있습니다.

다음 그림은 ONTAP 클론을 보여 줍니다.



클론 복제는 일반적으로 VM, VVOL 또는 데이터 저장소 수준에서 여러 메커니즘을 통해 ONTAP을 실행하는 시스템으로 오프로드할 수 있습니다. 여기에는 다음이 포함됩니다.

- NetApp VASA(vSphere APIs for Storage Awareness) 공급자를 사용하여 VVOL을 이동합니다. ONTAP 클론은 vCenter에서 관리하는 VVol 스냅샷을 지원하는 데 사용되며 이 스냅샷은 I/O 효과가 최소화되어 생성 및 삭제가 가능합니다. vCenter를 사용하여 VM을 복제할 수도 있으며, 단일 데이터 저장소/볼륨 내에서 또는 데이터 저장소/볼륨 간에 ONTAP로 오프로드됩니다.
- VAAI(vSphere API – Array Integration)를 사용한 vSphere 클론 생성 및 마이그레이션 VM 클론 복제 작업은 SAN 및 NAS 환경 모두에서 ONTAP로 오프로드할 수 있습니다(NetApp는 NFS용 VAAI를 지원하기 위해 ESXi 플러그인을 제공합니다). vSphere는 NAS 데이터 저장소의 콜드(전원이 꺼진) VM에서만 작업을 오프로드하고 핫 VM(클론 복제 및 스토리지 vMotion)에서의 작업도 SAN용으로 오프로드됩니다. ONTAP는 소스 및 대상을 기반으로 가장 효율적인 접근 방식을 사용합니다. 이 기능은 에서도 "옴니사 호라이즌 뷰" 사용됩니다.
- SRA(VMware Live Site Recovery/Site Recovery Manager와 함께 사용) 이 경우 클론은 DR 복제본의 복구를 중단 없이 테스트하는 데 사용됩니다.
- SnapCenter와 같은 NetApp 툴을 사용한 백업 및 복구 VM 클론은 백업 작업을 확인하고 개별 파일을 복구할 수 있도록 VM 백업을 마운트하는 데 사용됩니다.

ONTAP 오프로드 클론 복제는 VMware, NetApp 및 타사 툴에서 호출할 수 있습니다. ONTAP로 오프로드되는 클론에는 여러 가지 이점이 있습니다. 대부분의 경우 오브젝트 변경에만 스토리지가 필요한 공간 효율적이며, 데이터를 읽고 쓰는 데는 추가 성능 영향이 없으며, 고속 캐시에서 블록을 공유하여 성능을 향상할 수도 있습니다. 또한 CPU 사이클과 네트워크 I/O를 ESXi 서버에서 오프로드합니다. 라이센스를 통해 ONTAP One 라이센스에 포함된 FlexClone 라이센스를 사용하면 FlexVol volume을 사용하는 기존 데이터 저장소 내에서 복사 오프로드를 빠르고 효율적으로 수행할 수 있지만, FlexVol 볼륨 간 복사본은 속도가 느려질 수 있습니다. VM 템플릿을 클론의 소스로 유지 관리하는 경우 빠르고 공간 효율적인 클론을 위해 데이터 저장소 볼륨(폴더 또는 콘텐츠 라이브러리를 사용하여 구성) 내에 배치하는 것이 좋습니다.

ONTAP 내에서 직접 볼륨 또는 LUN을 복제하여 데이터 저장소를 복제할 수도 있습니다. NFS 데이터 저장소를 사용하면 FlexClone 기술을 통해 전체 볼륨을 클론 복제할 수 있으며, ONTAP에서 클론을 내보내고 ESXi에서 다른 데이터 저장소로 마운트할 수 있습니다. VMFS 데이터 저장소의 경우 ONTAP는 LUN 내에 하나 이상의 LUN을 포함하여 볼륨 또는 전체 볼륨 내에서 LUN을 클론 복제할 수 있습니다. VMFS를 포함하는 LUN은 ESXi 이니시에이터 그룹(igroup)에 매핑한 다음 ESXi에 의해 재서명하여 일반 데이터 저장소로 마운트하고 사용해야 합니다. 일부 임시 사용 사례에서는 재서명 없이 클론 생성된 VMFS를 마운트할 수 있습니다. 데이터 저장소의 클론을 생성한 후에는 해당 데이터 저장소 내의 VM을 개별적으로 클론 복제된 VM처럼 등록, 재구성 및 사용자 지정할 수 있습니다.

경우에 따라 라이센스가 부여된 추가 기능을 사용하여 백업용 SnapRestore 또는 FlexClone과 같은 복제를 향상시킬 수 있습니다. 이러한 라이센스는 라이센스 번들에 추가 비용 없이 포함되는 경우가 많습니다. VVOL 클론 복제 작업에는 FlexClone 라이센스가 필요하며, 하이퍼바이저에서 ONTAP로 오프로드되는 VVOL의 관리형 스냅샷을 지원하기 위해서는 FlexClone 라이센스가 필요합니다. FlexClone 라이센스는 데이터 저장소/볼륨 내에서 사용할 때 특정 VAAI 기반 클론을 개선할 수도 있습니다. 블록 복사본 대신 즉각적이고 공간 효율적인 복사본을 생성합니다. 또한 SRA에서는 DR 복제본의 복구를 테스트할 때, 클론 작업을 위한 SnapCenter 및 개별 파일을 복원할 백업 복사본을 찾아볼 때 사용됩니다.

데이터 보호

ONTAP for vSphere를 사용하면 VM(가상 머신)을 백업하고 신속하게 복구할 수 있습니다. 이 기능은 VMware vSphere용 SnapCenter 플러그인을 통해 vCenter 내에서 쉽게 관리할 수 있습니다. ONTAP로 VM을 복구하는 가장 빠르고 간단한 방법을 제공하는 SnapCenter를 사용하여 타사 백업 솔루션을 강화함으로써 ONTAP의 스냅샷 기술을 활용합니다. SnapCenter는 ONTAP One 라이센스를 보유한 고객에게 무료로 제공되며, 다른 라이센스 번들도 이용할 수 있습니다.

또한 VMware용 SnapCenter 플러그인은 다음과 통합될 수 있습니다. "가상 머신을 위한 NetApp Backup and Recovery"대부분의 ONTAP 시스템에 효과적인 3-2-1 백업 솔루션을 제공합니다. 프리미엄 서비스(추가 백업 저장소를

위한 개체 저장소 등)를 사용하여 가상 머신에 백업 및 복구를 사용하는 경우 일부 요금이 적용될 수 있습니다. 이 섹션에서는 VM과 데이터 저장소를 보호하는 데 사용할 수 있는 다양한 옵션을 간략하게 설명합니다.

NetApp ONTAP 볼륨 스냅샷

스냅샷을 사용하여 성능에 영향을 주지 않고 VM 또는 데이터 저장소를 신속하게 복사한 다음, SnapMirror를 사용하여 보조 시스템으로 전송하여 장기적인 오프 사이트 데이터 보호를 실현합니다. 이러한 접근 방식은 변경된 정보만 저장하여 스토리지 공간과 네트워크 대역폭을 최소화합니다.

스냅샷은 ONTAP의 핵심 기능으로, 데이터의 시점 복사본을 생성할 수 있습니다. 이러한 솔루션은 공간 효율적이며 신속하게 생성할 수 있으므로 VM 및 데이터 저장소를 보호하는 데 이상적입니다. 스냅샷은 백업, 복구 및 테스트를 포함한 다양한 용도로 사용할 수 있습니다. 이러한 스냅샷은 VMware(정합성 보장) 스냅샷과는 다르며 장기간 보호에 적합합니다. VMware의 vCenter 관리 스냅샷은 성능 및 기타 효과로 인해 단기간 사용하는 경우에만 권장됩니다. "스냅샷 제한 사항"자세한 내용은 을 참조하십시오.

스냅샷은 볼륨 레벨에서 생성되며 해당 볼륨 내의 모든 VM 및 데이터 저장소를 보호하는 데 사용될 수 있습니다. 즉, 해당 데이터 저장소 내의 모든 VM을 포함하는 전체 데이터 저장소의 스냅샷을 생성할 수 있습니다.

NFS 데이터 저장소의 경우 .snapshots 디렉토리를 탐색하여 스냅샷에서 VM 파일을 쉽게 볼 수 있습니다. 따라서 특정 백업 솔루션을 사용하지 않고도 스냅샷에서 파일을 빠르게 액세스하고 복구할 수 있습니다.

VMFS 데이터 저장소의 경우 원하는 스냅샷을 기반으로 데이터 저장소의 FlexClone을 생성할 수 있습니다. 이를 통해 스냅샷을 기반으로 새 데이터 저장소를 생성할 수 있으며, 이 데이터 저장소는 테스트 또는 개발 목적으로 사용할 수 있습니다. FlexClone는 스냅샷이 생성된 후 변경된 내용에만 공간을 사용하므로 데이터 저장소의 복제본을 공간 효율적으로 생성할 수 있습니다. FlexClone이 생성되면 일반 데이터 저장소처럼 LUN 또는 네임스페이스를 ESXi 호스트에 매핑할 수 있습니다. 이를 통해 특정 VM 파일을 복원할 수 있을 뿐만 아니라 프로덕션 환경의 성능에 영향을 주지 않고 프로덕션 데이터를 기반으로 테스트 또는 개발 환경을 빠르게 만들 수 있습니다.

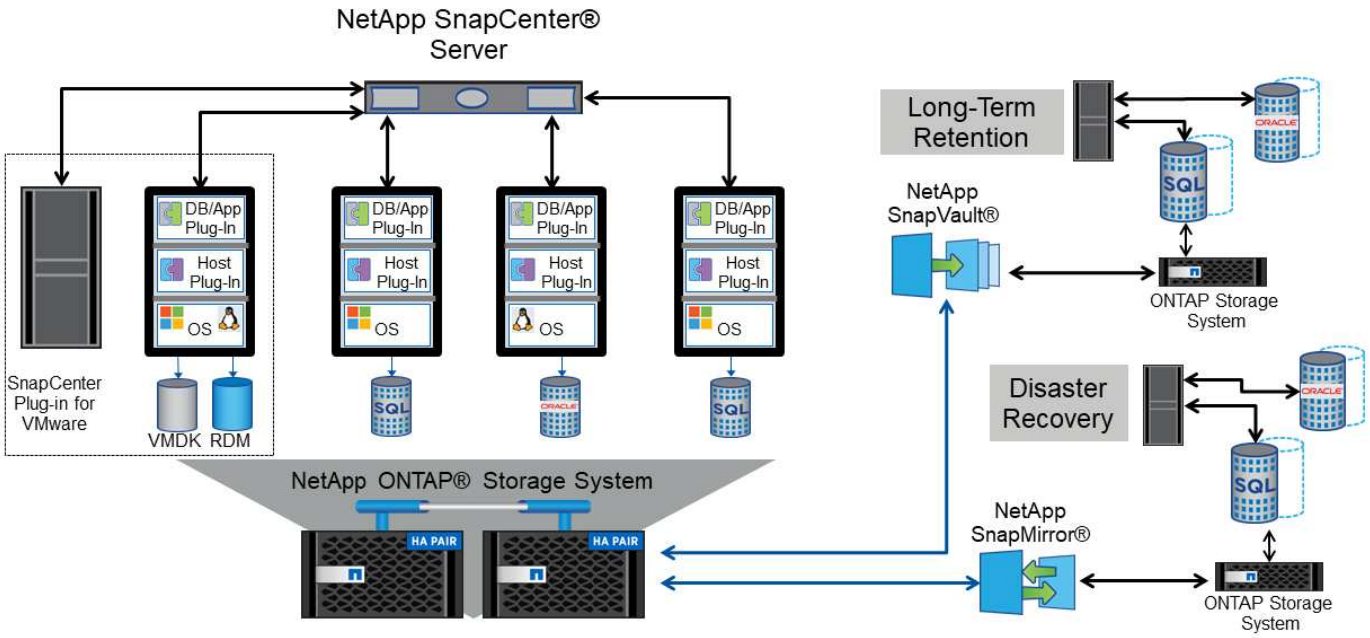
스냅샷에 대한 자세한 내용은 ONTAP 설명서를 참조하십시오. 다음 링크에서 추가 정보를 확인할 수 있습니다. "ONTAP 로컬 스냅샷 복사본" "ONTAP SnapMirror 복제 워크플로"

VMware vSphere용 **SnapCenter** 플러그인

SnapCenter를 사용하면 여러 작업에 적용할 수 있는 백업 정책을 생성할 수 있습니다. 이러한 정책은 스케줄, 보존, 복제 및 기타 기능을 정의할 수 있습니다. 또한 VM 정합성 보장 스냅샷의 선택적인 선택을 계속 허용하므로 VMware 스냅샷을 생성하기 전에 하이퍼바이저의 입출력 중지 기능을 활용할 수 있습니다. 그러나 VMware 스냅샷의 성능 때문에 게스트 파일 시스템을 중지해야 하는 경우가 아니면 일반적으로 이러한 스냅샷을 사용하지 않는 것이 좋습니다. 대신 일반적인 보호를 위해 스냅샷을 사용하고 SnapCenter 애플리케이션 플러그인 같은 애플리케이션 툴을 사용하여 SQL Server 또는 Oracle과 같은 트랜잭션 데이터를 보호하십시오.

이러한 플러그인은 물리적 환경과 가상 환경 모두에서 데이터베이스를 보호하는 확장된 기능을 제공합니다. vSphere를 사용하면 RDM LUN, VVol 또는 NVMe/TCP 네임스페이스와 게스트 OS에 직접 연결된 iSCSI LUN 또는 VMFS 또는 NFS 데이터 저장소의 VMDK 파일에 데이터가 저장되는 SQL Server 또는 Oracle 데이터베이스를 보호할 수 있습니다. 플러그인을 사용하면 다양한 유형의 데이터베이스 백업을 지정하고 온라인 또는 오프라인 백업을 지원하며 로그 파일과 함께 데이터베이스 파일을 보호할 수 있습니다. 플러그인은 백업 및 복구 외에도 개발 또는 테스트 목적으로 데이터베이스의 클론 복제를 지원합니다.

다음 그림은 SnapCenter 구축의 예를 보여 줍니다.



사이징 정보는 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인용 사이징 가이드"

VMware Live Site Recovery가 포함된 **VMware vSphere**용 **ONTAP** 툴

OT4VS(VMware vSphere)용 ONTAP 툴은 VMware vSphere와 NetApp ONTAP 간의 원활한 통합을 지원하는 무료 플러그인입니다. vSphere Web Client에서 직접 ONTAP 스토리지를 관리할 수 있으므로 스토리지 용량 할당, 복제 관리, 성능 모니터링 등의 작업을 보다 쉽게 수행할 수 있습니다.

향상된 재해 복구 기능을 사용하려면 VMware vSphere용 ONTAP 툴의 일부인 NetApp SRA for ONTAP를 VMware 라이브 사이트 복구(이전의 사이트 복구 관리자)와 함께 사용하는 것이 좋습니다. 이 툴은 SnapMirror을 사용하는 재해 복구 사이트에 데이터 저장소를 복제할 뿐만 아니라 복제된 데이터 저장소를 클론 복제하여 DR 환경에서 무중단 테스트를 지원합니다. 또한 내장된 자동화 기능 덕분에 운영 중단 해결 후 재해 복구 및 운영 재보호가 간소화됩니다.

NetApp Disaster Recovery

재해 복구(DR)는 재해 발생 시 데이터와 애플리케이션을 보호하기 위한 포괄적인 솔루션을 제공하는 클라우드 기반 서비스입니다. 여기에는 자동 장애 조치 및 장애 복구, 여러 시점 복구 지점, 애플리케이션 일관성 재해 복구, 온프레미스 및 클라우드 기반 ONTAP 시스템 모두에 대한 지원 등 다양한 기능이 제공됩니다. NetApp Disaster Recovery ONTAP과 VMware vSphere 환경과 원활하게 작동하도록 설계되어 재해 복구를 위한 통합 솔루션을 제공합니다.

NetApp MetroCluster 및 **SnapMirror** 액티브 동기화가 포함된 **vMSC(vSphere Metro Storage Cluster**

마지막으로, 최고 수준의 데이터 보호를 위해 NetApp MetroCluster를 사용하는 VMware vMSC(vSphere Metro Storage Cluster) 구성을 고려해 보십시오. vMSC는 동기식 복제를 사용하는 VMware 인증 NetApp 지원 솔루션으로, 고가용성 클러스터에서와 동일한 이점을 제공하지만 사이트 재해로부터 보호하기 위해 별도의 사이트에 분산됩니다. ASA 및 AFF, MetroCluster with AFF를 통한 NetApp SnapMirror 액티브 동기화는 동기식 복제를 위한 비용 효율적인 구성을 제공하며 단일 스토리지 구성 요소 장애로부터의 투명한 복구는 물론, SnapMirror 활성 동기화의 경우 투명한 복구 또는 MetroCluster로 사이트 재해 발생 시 단일 명령 복구에 대해 자세히 설명합니다. vMSC는 에 자세히 설명되어 있습니다. "TR-4128"

서비스 품질(QoS)

처리량 제한은 서비스 수준을 제어하고, 알 수 없는 워크로드를 관리하거나, 구축 전에 애플리케이션을 테스트하여 운영 중인 다른 워크로드에 영향을 미치지 않도록 하는 데 유용합니다. 이러한 워크로드는 식별된 후 대규모 워크로드를 제한하는 데 사용할 수도 있습니다.

ONTAP QoS 정책 지원

ONTAP을 실행하는 시스템에서는 스토리지 QoS 기능을 사용하여 파일, LUN, 볼륨, 전체 SVM과 같은 서로 다른 스토리지 오브젝트의 초당 I/O(IOPS) 및/또는 처리량을 제한할 수 있습니다.

ONTAP 9.2의 SAN 오브젝트 및 ONTAP 9.3의 NAS 오브젝트에 대해 일관된 성능을 제공하기 위해 IOPS를 기반으로 하는 최소 서비스 레벨도 지원됩니다.

개체에 대한 QoS 최대 처리량 제한은 Mbps 및/또는 IOPS로 설정할 수 있습니다. 둘 다 사용되는 경우 첫 번째 제한에 도달한 값은 ONTAP에 의해 적용됩니다. 워크로드에는 여러 개체가 포함될 수 있으며 QoS 정책을 하나 이상의 워크로드에 적용할 수 있습니다. 정책이 여러 워크로드에 적용될 경우 워크로드는 정책의 총 한도를 공유합니다. 중첩된 개체는 지원되지 않습니다(예: 볼륨 내의 파일은 각각 고유한 정책을 가질 수 없음). QoS 최소값을 IOPS에서만 설정할 수 있습니다.

현재 ONTAP QoS 정책을 관리하고 객체에 적용하는 데 사용할 수 있는 툴은 다음과 같습니다.

- ONTAP CLI를 참조하십시오
- ONTAP 시스템 관리자
- OnCommand Workflow Automation
- Active IQ Unified Manager
- ONTAP를 위한 NetApp PowerShell Toolkit
- VMware vSphere VASA Provider용 ONTAP 툴

VMFS 및 RDM을 포함하여 LUN에 QoS 정책을 할당하려면 ONTAP vSphere용 ONTAP 툴 홈 페이지의 스토리지 시스템 메뉴에서 SVM(SVM으로 표시됨), LUN 경로 및 일련 번호를 확인할 수 있습니다. 스토리지 시스템(SVM)을 선택한 다음 관련 오브젝트 > SAN을 선택합니다. ONTAP 툴 중 하나를 사용하여 QoS를 지정할 때 이 접근 방식을 사용합니다.

을 참조하십시오 "성능 모니터링 및 관리 개요" 를 참조하십시오.

비 **VVOL NFS** 데이터 저장소입니다

ONTAP QoS 정책을 전체 데이터 저장소 또는 이 데이터 저장소 내의 개별 VMDK 파일에 적용할 수 있습니다. 그러나 기존(비 VVol) NFS 데이터 저장소에 있는 모든 VM은 해당 호스트에서 공통 I/O 대기열을 공유한다는 점을 이해하는 것이 중요합니다. VM이 ONTAP QoS 정책에 의해 스로틀되는 경우 실제로 해당 데이터 저장소의 모든 입출력이 해당 호스트에 대해 스로틀되는 것처럼 보입니다.

- 예: *
- 호스트 ESXi-01에 의해 기존 NFS 데이터 저장소로 마운트된 볼륨에 대해 vm1.vmdk에 QoS 제한을 구성합니다.
- 동일한 호스트(ESXi-01)가 VM2.vmdk를 사용하고 있으며 동일한 볼륨에 있습니다.
- vm1.vmdk가 스로틀되면 vm1.vmdk와 동일한 IO 큐를 공유하기 때문에 VM2.vmdk도 스로틀된 것처럼 보입니다.

VVOL에는 적용되지 않습니다.

vSphere 6.5부터는 SPBM(Storage Policy-Based Management)과 SIOC(Storage I/O Control) v2를 활용하여 VVol이 아닌 데이터 저장소에 대한 파일 세분화 제한을 관리할 수 있습니다.

SIOC 및 SPBM 정책을 사용한 성능 관리에 대한 자세한 내용은 다음 링크를 참조하십시오.

"SPBM 호스트 기반 규칙: SIOC v2"
"vSphere를 사용하여 스토리지 입출력 리소스 관리"

NFS에서 VMDK에 QoS 정책을 할당하려면 다음 지침을 따르십시오.

- 정책을 에 적용해야 합니다 `vmname-flat.vmdk` 여기에는 가 아닌 실제 가상 디스크 이미지가 포함됩니다 `vmname.vmdk` (가상 디스크 설명자 파일) 또는 `vmname.vmx` (VM 설명자 파일).
- 가상 스왑 파일과 같은 다른 VM 파일에 정책을 적용하지 마십시오 (`vmname.vswp`)를 클릭합니다.
- vSphere Web Client를 사용하여 파일 경로(Datastore > Files)를 찾을 때는 의 정보가 결합되어 있다는 점을 유념하십시오 - `flat.vmdk` 및 . `vmdk` 의 이름을 가진 파일 하나가 표시됩니다 . `vmdk` 그러나 의 크기는 - `flat.vmdk`. 추가 `-flat` 파일 이름에 올바른 경로를 입력합니다.

FlexGroup 데이터 저장소는 VMware vSphere 9.8 이상용 ONTAP 툴을 사용할 때 향상된 QoS 기능을 제공합니다. 데이터 저장소 또는 특정 VM의 모든 VM에 대해 QoS를 쉽게 설정할 수 있습니다. 자세한 내용은 이 보고서의 FlexGroup 섹션을 참조하십시오. 앞에서 언급한 기존 NFS 데이터 저장소 방식의 QoS 제한 사항은 여전히 적용됩니다.

VMFS 데이터 저장소

ONTAP LUN을 사용하면 ONTAP에서 VMFS 파일 시스템을 인식하지 못하기 때문에 LUN 또는 개별 LUN이 포함된 FlexVol 볼륨에는 QoS 정책을 적용할 수 있지만 개별 VMDK 파일은 적용할 수 없습니다.

VVOL 데이터 저장소

스토리지 정책 기반 관리 및 VVol을 사용하면 다른 VM 또는 VMDK에 영향을 주지 않고 개별 VM 또는 VMDK에 대해 최소 및/또는 최대 QoS를 쉽게 설정할 수 있습니다.

VVOL 컨테이너에 대한 스토리지 기능 프로필을 생성할 때 성능 기능에서 최대 및/또는 최소 IOPS 값을 지정한 다음 이 SCP를 VM의 스토리지 정책에 참조합니다. VM을 생성하거나 기존 VM에 정책을 적용할 때 이 정책을 사용합니다.

VVOL에는 ONTAP를 위한 VASA 공급자 역할을 하는 VMware vSphere용 ONTAP 툴을 사용해야 합니다. VVOL 모범 사례는 를 "ONTAP을 사용한 VVOL(VMware vSphere 가상 볼륨"참조하십시오.

ONTAP QoS 및 **VMware SIOC**

ONTAP QoS 및 VMware vSphere 스토리지 SIOC(I/O Control)는 vSphere 및 스토리지 관리자가 함께 사용하여 ONTAP를 실행하는 시스템에서 호스팅되는 vSphere VM의 성능을 관리할 수 있는 보완 기술입니다. 다음 표에 나와 있는 것처럼 각 툴마다 고유한 강점이 있습니다. VMware vCenter와 ONTAP의 범위가 서로 다르기 때문에 한 시스템에서 일부 객체를 보고 관리할 수 있으며 다른 객체는 볼 수 없습니다.

속성	**ONTAP QoS**를 참조하십시오	**VMware SIOC**
활성화 시	정책이 항상 활성화되어 있습니다	경합이 있을 때 활성(데이터 저장소 지연 시간이 임계값을 초과함)

속성	**ONTAP QoS**를 참조하십시오	**VMware SIOC**
단위 유형	IOPS, MBps	IOPS, 공유
vCenter 또는 애플리케이션 범위	다양한 vCenter 환경, 기타 하이퍼바이저 및 애플리케이션	단일 vCenter Server
VM에서 QoS를 설정하시겠습니까?	VMDK는 NFS에만 해당합니다	NFS 또는 VMFS의 VMDK입니다
LUN(RDM)에 QoS를 설정하시겠습니까?	예	아니요
LUN(VMFS)에서 QoS를 설정하시겠습니까?	예	예(데이터 저장소 제한 가능)
볼륨에 QoS를 설정하시겠습니까(NFS 데이터 저장소)?	예	예(데이터 저장소 제한 가능)
SVM(테넌트)에서 QoS를 설정하시겠습니까?	예	아니요
정책 기반 접근 방식?	예. 정책의 모든 워크로드에서 공유하거나 정책의 각 워크로드에 전체적으로 적용할 수 있습니다.	예, vSphere 6.5 이상에서 가능합니다.
라이센스가 필요합니다	ONTAP에 포함되어 있습니다	엔터프라이즈급 플러스

VMware 스토리지 분산 리소스 스케줄러입니다

VMware SDRS(Storage Distributed Resource Scheduler)는 현재 입출력 지연 시간 및 공간 사용량을 기반으로 스토리지에 VM을 배치하는 vSphere 기능입니다. 그런 다음 데이터 저장소 클러스터(Pod라고도 함)의 데이터 저장소 간에 VM 또는 VMDK를 중단 없이 이동하여 VM 또는 VMDK를 데이터 저장소 클러스터에 배치할 최상의 데이터 저장소를 선택합니다. 데이터 저장소 클러스터는 vSphere 관리자의 관점에서 단일 사용 단위로 집계되는 유사한 데이터 저장소의 모음입니다.

VMware vSphere용 ONTAP 툴과 함께 SDRS를 사용하는 경우 먼저 플러그인을 사용하여 데이터 저장소를 생성하고 vCenter를 사용하여 데이터 저장소 클러스터를 생성한 다음 데이터 저장소를 데이터 저장소에 추가해야 합니다. 데이터 저장소 클러스터가 생성된 후 세부 정보 페이지의 프로비저닝 마법사에서 추가 데이터 저장소를 데이터 저장소 클러스터에 직접 추가할 수 있습니다.

SDRS에 대한 기타 ONTAP 모범 사례는 다음과 같습니다.

- 클러스터의 모든 데이터 저장소는 동일한 유형의 스토리지(예: SAS, SATA 또는 SSD)를 사용하고 모든 VMFS 또는 NFS 데이터 저장소이며 복제 및 보호 설정이 동일해야 합니다.
- 기본(수동) 모드에서 SDRS 사용을 고려하십시오. 이 접근 방식을 통해 권장 사항을 검토하고 적용 여부를 결정할 수 있습니다. VMDK 마이그레이션의 영향을 숙지하십시오.
  - SDRS에서 VMDK를 데이터 저장소 간에 이동할 경우 ONTAP 클론 생성 또는 중복 제거를 통한 공간 절약이 손실됩니다. 중복제거를 재실행하여 이러한 절약 효과를 다시 실현할 수 있습니다.
  - SDRS가 VMDK를 이동한 후 NetApp는 소스 데이터 저장소에서 스냅샷을 다시 생성하는 것이 좋습니다. 그렇지 않으면 공간이 이동된 VM에 의해 잠기기 때문입니다.
  - 동일한 애그리게이트에서 데이터 저장소 간에 VMDK를 이동하는 것은 효과가 거의 없으며 SDRS는 애그리게이트를 공유할 수 있는 다른 워크로드를 파악할 수 없습니다.

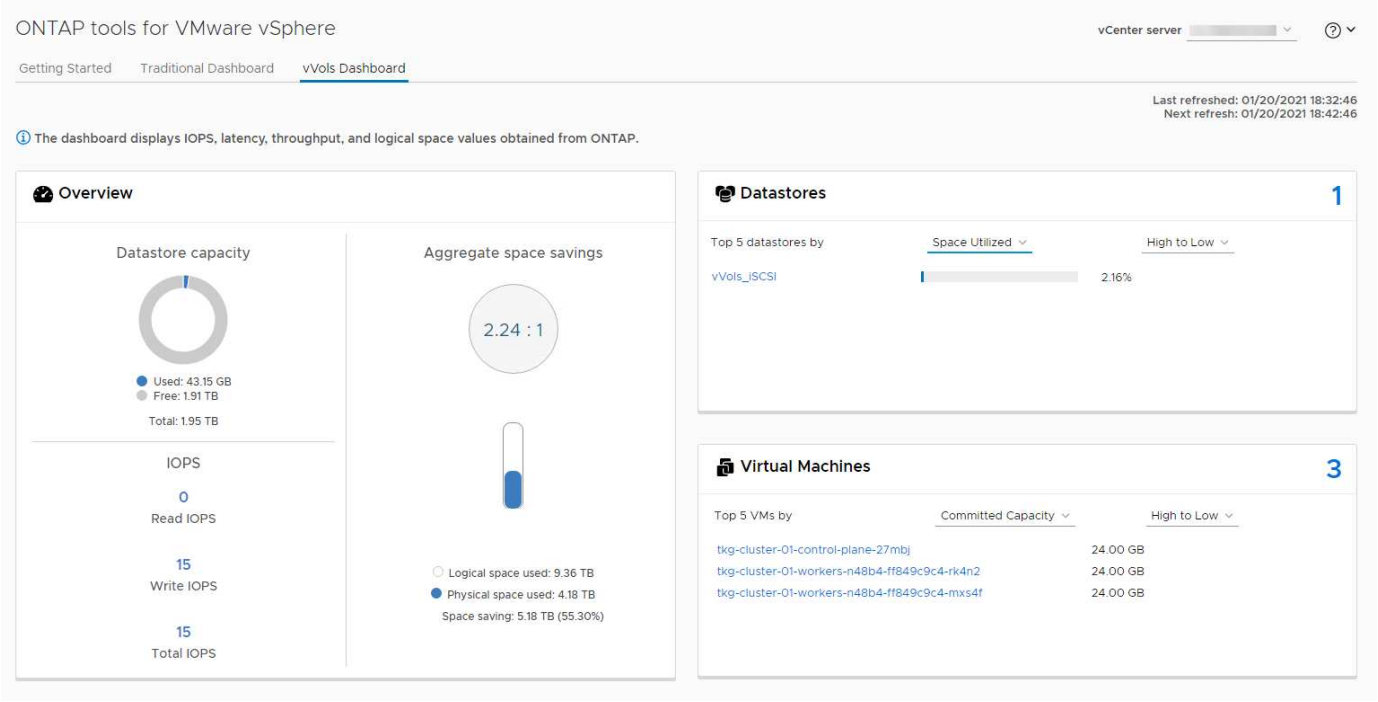
스토리지 정책 기반 관리 및 **VVOL**

VMware VASA(vSphere APIs for Storage Awareness)를 사용하면 스토리지 관리자가 잘 정의된 기능을 사용하여 데이터 저장소를 쉽게 구성하고 VM 관리자는 상호 작용하지 않고도 VM을 프로비저닝할 때 이러한 데이터 저장소를 사용할 수 있습니다. 가상화 스토리지 운영을 간소화하고 사소한 작업을 많이 피하는 방법을 알아보려면 이 접근 방식을 살펴보시기 바랍니다.

VASA를 사용하기 전에는 VM 관리자가 VM 스토리지 정책을 정의할 수 있었지만, 스토리지 관리자와 협력하여 적절한 데이터 저장소를 식별해야 했습니다. 이러한 데이터 저장소는 보통 설명서 또는 명명 규칙을 사용합니다. 스토리지 관리자는 VASA를 통해 성능, 계층화, 암호화, 복제를 비롯한 다양한 스토리지 기능을 정의할 수 있습니다. 볼륨 또는 볼륨 세트에 대한 기능 세트를 SCP(Storage Capability Profile)라고 합니다.

SCP는 VM의 데이터 VVol에 대한 최소 및/또는 최대 QoS를 지원합니다. 최소 QoS는 AFF 시스템에서만 지원됩니다. VMware vSphere용 ONTAP 툴에는 ONTAP 시스템에서 VVOL을 위한 VM 레벨의 세분화된 성능과 논리적 용량을 보여주는 대시보드가 포함되어 있습니다.

다음 그림은 VMware vSphere 9.8 VVol 대시보드를 위한 ONTAP 툴을 보여 줍니다.



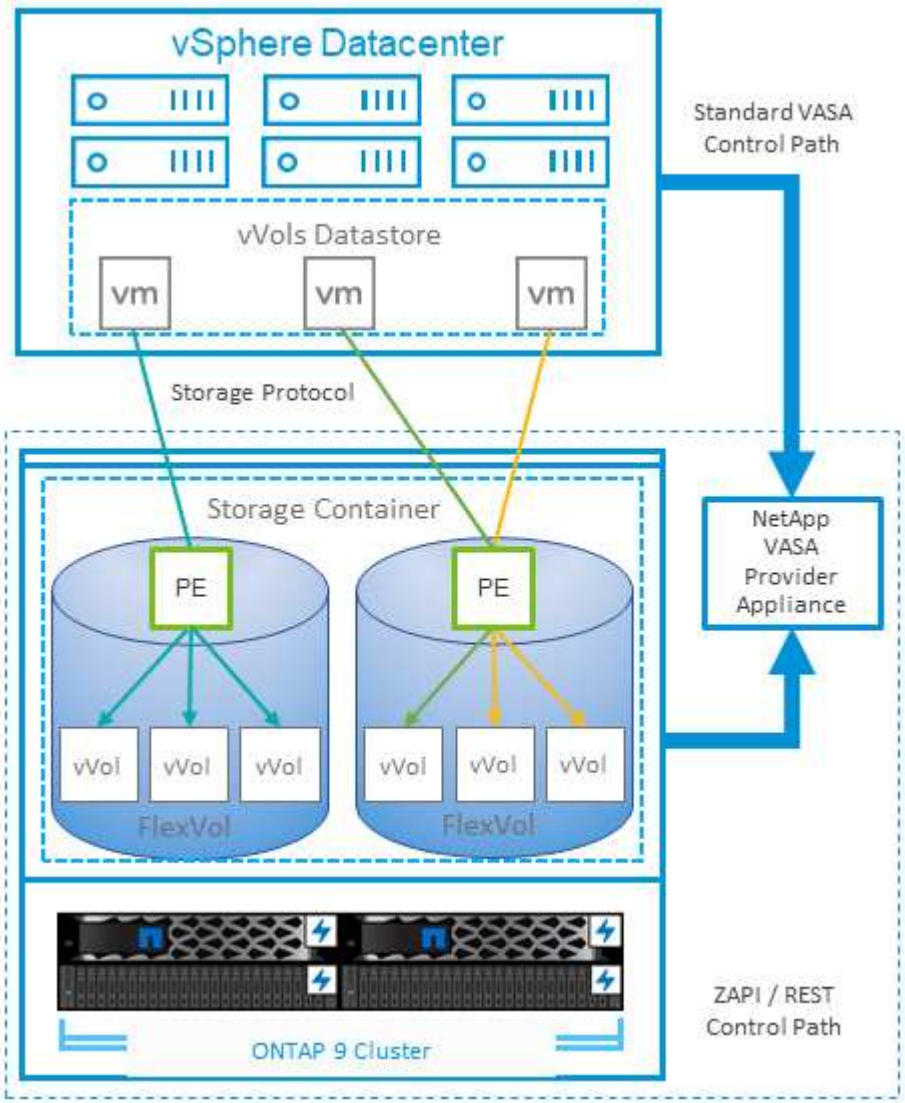
스토리지 용량 프로필을 정의한 후에는 요구 사항을 식별하는 스토리지 정책을 사용하여 VM을 프로비저닝하는 데 사용할 수 있습니다. VM 스토리지 정책과 데이터 저장소 스토리지 용량 프로파일 간의 매핑을 통해 vCenter에서 선택할 수 있는 호환 데이터 저장소 목록을 표시할 수 있습니다. 이러한 접근 방식을 스토리지 정책 기반 관리라고 합니다.

VASA는 스토리지를 쿼리하고 스토리지 기능 집합을 vCenter에 반환하는 기술을 제공합니다. VASA 공급업체 공급자는 스토리지 시스템 API 및 구성 요소 및 vCenter에서 인식할 수 있는 VMware API 간의 변환을 제공합니다. NetApp의 VASA Provider for ONTAP는 VMware vSphere 어플라이언스 VM을 위한 ONTAP 툴의 일부로 제공됩니다. 또한, vCenter 플러그인은 VVOL 데이터 저장소를 프로비저닝 및 관리하기 위한 인터페이스를 제공하며 SCP(스토리지 기능 프로필)를 정의합니다.

ONTAP는 VMFS 및 NFS VVOL 데이터 저장소를 모두 지원합니다. SAN 데이터 저장소와 VVOL을 함께 사용하면 VM 수준 정밀도와 같은 NFS의 몇 가지 이점이 있습니다. 다음은 고려해야 할 몇 가지 모범 사례이며 에서 추가 정보를 찾을 수 있습니다 "TR-4400 을 참조하십시오":

- VVOL 데이터 저장소는 여러 클러스터 노드의 여러 FlexVol 볼륨으로 구성될 수 있습니다. 가장 간단한 방법은 볼륨에 기능이 다른 경우에도 단일 데이터 저장소를 사용하는 것입니다. SPBM은 호환 볼륨이 VM에 사용되는지 확인합니다. 하지만 모든 볼륨은 단일 ONTAP SVM에 속하고 단일 프로토콜을 사용하여 액세스해야 합니다. 각 프로토콜당 하나의 LIF로 충분합니다. 스토리지 기능이 릴리즈별로 다를 수 있으므로 단일 VVOL 데이터 저장소 내에서 여러 ONTAP 릴리즈를 사용하는 것은 피하십시오.
- VMware vSphere용 ONTAP 툴을 사용하여 VVOL 데이터 저장소를 만들고 관리합니다. 데이터 저장소와 해당 프로필을 관리하는 것 외에도 필요한 경우 데이터 저장소에 액세스하기 위한 프로토콜 엔드포인트가 자동으로 생성됩니다. LUN을 사용하는 경우 LUN PES는 LUN ID 300 이상을 사용하여 매핑됩니다. ESXi 호스트 고급 시스템 설정을 확인합니다 `Disk.MaxLUN` 300보다 높은 LUN ID 번호를 허용합니다(기본값: 1,024). 이 단계를 수행하려면 vCenter에서 ESXi 호스트를 선택한 다음 구성 탭을 선택하고 을 찾습니다 `Disk.MaxLUN` 고급 시스템 설정 목록에서 선택합니다.
- VMware vSphere를 위한 VASA Provider, vCenter Server(어플라이언스 또는 Windows 기반) 또는 ONTAP 툴을 VVOL 데이터 저장소에 설치하거나 마이그레이션하지 마십시오. 상호 의존하기 때문에 정전이 발생하거나 기타 데이터 센터가 중단될 경우 이를 관리할 수 없습니다.
- VASA Provider VM을 정기적으로 백업합니다. VASA Provider가 포함된 기존 데이터 저장소의 시간별 스냅샷을 적어도 생성합니다. VASA Provider 보호 및 복구에 대한 자세한 내용은 다음을 참조하십시오 "KB 문서를 참조하십시오".

다음 그림은 VVol 구성 요소를 보여줍니다.



클라우드 마이그레이션 및 백업

ONTAP의 또 다른 강점은 하이브리드 클라우드를 광범위하게 지원하여 사내 프라이빗 클라우드의 시스템을 퍼블릭 클라우드 기능과 병합하는 것입니다. 다음은 vSphere와 함께 사용할 수 있는 몇 가지 NetApp 클라우드 솔루션입니다.

- **1**차 제공**.** Amazon FSx for NetApp ONTAP, Google Cloud NetApp Volumes 및 Azure NetApp Files 주요 퍼블릭 클라우드 환경에서 고성능의 다중 프로토콜 관리형 스토리지 서비스를 제공합니다. 이러한 스토리지는 VMware Cloud on AWS(VMC on AWS), Azure VMware Solution(AVS), Google Cloud VMware Engine(GCVE)에서 게스트 운영 체제(GOS) 및 컴퓨팅 인스턴스의 데이터 저장소 또는 스토리지로 직접 사용할 수 있습니다.
- 클라우드 서비스**.** 퍼블릭 클라우드 스토리지를 사용하여 온프레미스 시스템의 데이터를 보호하려면 NetApp Backup and Recovery 또는 SnapMirror Cloud를 사용하세요. NetApp Copy and Sync NAS와 개체 저장소에서 데이터를 마이그레이션하고 동기화하는 데 도움이 됩니다. NetApp Disaster Recovery 클라우드 재해 복구, 온프레미스 재해 복구, 온프레미스 간 재해 복구를 위한 강력하고 유능한 재해 복구 솔루션의 기반으로 NetApp 기술을 활용하는 비용 효과적이고 효율적인 솔루션을 제공합니다.
- * FabricPool. * FabricPool는 ONTAP 데이터를 빠르고 쉽게 계층화할 수 있도록 지원합니다. 콜드 블록은 퍼블릭 클라우드 또는 프라이빗 StorageGRID 오브젝트 저장소의 오브젝트 저장소로 마이그레이션할 수 있으며, ONTAP 데이터에 다시 액세스할 때 자동으로 호출됩니다. 또는 SnapVault에서 이미 관리하는 데이터를 보호하기 위해 개체 계층을 세 번째 수준으로 사용할 수도 있습니다. 이 접근 방식을 통해 다음을 수행할 수 있습니다 "VM의 스냅샷을 더 많이 저장합니다" 주요 및/또는 보조 ONTAP 스토리지 시스템
- * ONTAP Select. * NetApp 소프트웨어 정의 스토리지를 사용하여 프라이빗 클라우드를 인터넷으로 원격 시설 및 사무소로 확장할 수 있습니다. ONTAP Select를 사용하여 블록 및 파일 서비스와 엔터프라이즈 데이터 센터에서 사용하는 vSphere 데이터 관리 기능을 지원할 수 있습니다.

VM 기반 애플리케이션을 설계할 때 미래의 클라우드 모빌리티를 고려하세요. 예를 들어, 애플리케이션과 데이터 파일을 함께 배치하는 대신 데이터에 대해 별도의 LUN이나 NFS 내보내기를 사용합니다. 이를 통해 VM과 데이터를 별도로 클라우드 서비스로 마이그레이션할 수 있습니다.

자세한 보안 항목에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- "ONTAP Select 설명서"
- "백업 및 복구 문서"
- "재해 복구 문서"
- "NetApp ONTAP용 Amazon FSx"
- "AWS 기반 VMware 클라우드"
- "Azure NetApp Files 무엇인가요?"
- "Azure VMware 솔루션"
- "Google Cloud VMware 엔진"
- "Google Cloud NetApp 볼륨이란?"

vSphere 데이터 암호화

오늘날, 암호화를 통해 유휴 데이터를 보호해야 하는 요구가 증가하고 있습니다. 처음에는 금융 및 의료 정보에 초점을 맞추었지만 파일, 데이터베이스 또는 기타 데이터 유형에 관계없이 모든

정보를 보호하는 데 대한 관심이 높아지고 있습니다.

ONTAP을 실행하는 시스템의 유휴 데이터를 쉽게 보호할 수 있습니다. NSE(NetApp 스토리지 암호화)는 ONTAP와 함께 SED(자체 암호화 드라이브)를 사용하여 SAN 및 NAS 데이터를 보호합니다. NetApp은 또한 디스크 드라이브에서 볼륨을 암호화하는 단순한 소프트웨어 기반 접근 방식으로 NetApp 볼륨 암호화 및 NetApp 애그리게이트 Encryption도 제공합니다. 이 소프트웨어 암호화는 특수 디스크 드라이브나 외부 키 관리자가 필요하지 않으며 ONTAP 고객이 추가 비용 없이 사용할 수 있습니다. 클라이언트나 애플리케이션의 중단 없이 업그레이드하고 사용할 수 있으며, Onboard Key Manager를 비롯한 FIPS 140-2 레벨 1 표준에 따라 검증됩니다.

VMware vSphere에서 실행되는 가상화된 애플리케이션의 데이터를 보호하기 위한 몇 가지 접근 방식이 있습니다. 한 가지 방법은 게스트 OS 수준에서 VM 내부의 소프트웨어로 데이터를 보호하는 것입니다. vSphere 6.5와 같은 최신 하이퍼바이저는 VM 수준에서 암호화를 지원하는 또 다른 대안으로, 그러나 NetApp 소프트웨어 암호화는 간단하고 쉬우며 다음과 같은 이점을 제공합니다.

- * 가상 서버 CPU에 영향을 미치지 않습니다. * 일부 가상 서버 환경에서는 애플리케이션에 사용할 수 있는 모든 CPU 사이클이 필요하지만 하이퍼바이저 레벨 암호화를 위해서는 최대 5배의 CPU 리소스가 필요하다는 결과가 있습니다. 암호화 소프트웨어가 암호화 워크로드를 오프로드하는 인텔의 AES-NI 명령 집합을 지원하더라도(NetApp 소프트웨어 암호화처럼), 이전 서버와 호환되지 않는 새로운 CPU가 필요하기 때문에 이 접근 방식은 적합하지 않을 수 있습니다.
- * Onboard Key Manager 포함. * NetApp 소프트웨어 암호화에는 추가 비용 없이 온보드 키 관리자가 포함되어 있으므로 구입 및 사용이 복잡한 고가용성 키 관리 서버 없이도 쉽게 시작할 수 있습니다.
- * 스토리지 효율성에 영향을 미치지 않습니다. * 데이터 중복 제거 및 압축과 같은 스토리지 효율성 기술이 현재 널리 사용되고 있으며 플래시 디스크 미디어를 비용 효율적으로 사용하는 데 핵심적인 역할을 합니다. 그러나 암호화된 데이터는 일반적으로 중복제거되거나 압축할 수 없습니다. NetApp 하드웨어 및 스토리지 암호화는 다른 접근법과는 달리 낮은 수준에서 작동하며 업계 최고의 NetApp 스토리지 효율성 기능을 충분히 활용할 수 있도록 합니다.
- * 데이터스토어의 세분화된 암호화. * NetApp Volume Encryption을 사용하면 각 볼륨에 고유한 AES 256비트 키를 사용할 수 있습니다. 변경해야 하는 경우 단일 명령을 사용하여 변경할 수 있습니다. 이 접근 방식은 테넌트가 여러 개이거나 서로 다른 부서 또는 애플리케이션에 대해 독립적인 암호화를 증명해야 하는 경우에 유용합니다. 이 암호화는 개별 VM을 관리하는 것보다 훨씬 쉬운 데이터 저장소 수준에서 관리됩니다.

소프트웨어 암호화를 간단하게 시작할 수 있습니다. 라이센스를 설치한 후 암호를 지정하여 Onboard Key Manager를 구성한 다음 새 볼륨을 생성하거나 스토리지 측 볼륨 이동을 수행하여 암호화를 설정합니다. NetApp은 향후 VMware 툴 릴리즈에서 암호화 기능에 대한 통합 지원을 추가하기 위해 노력하고 있습니다.

자세한 보안 항목에 대한 자세한 내용은 다음 리소스를 참조하십시오.

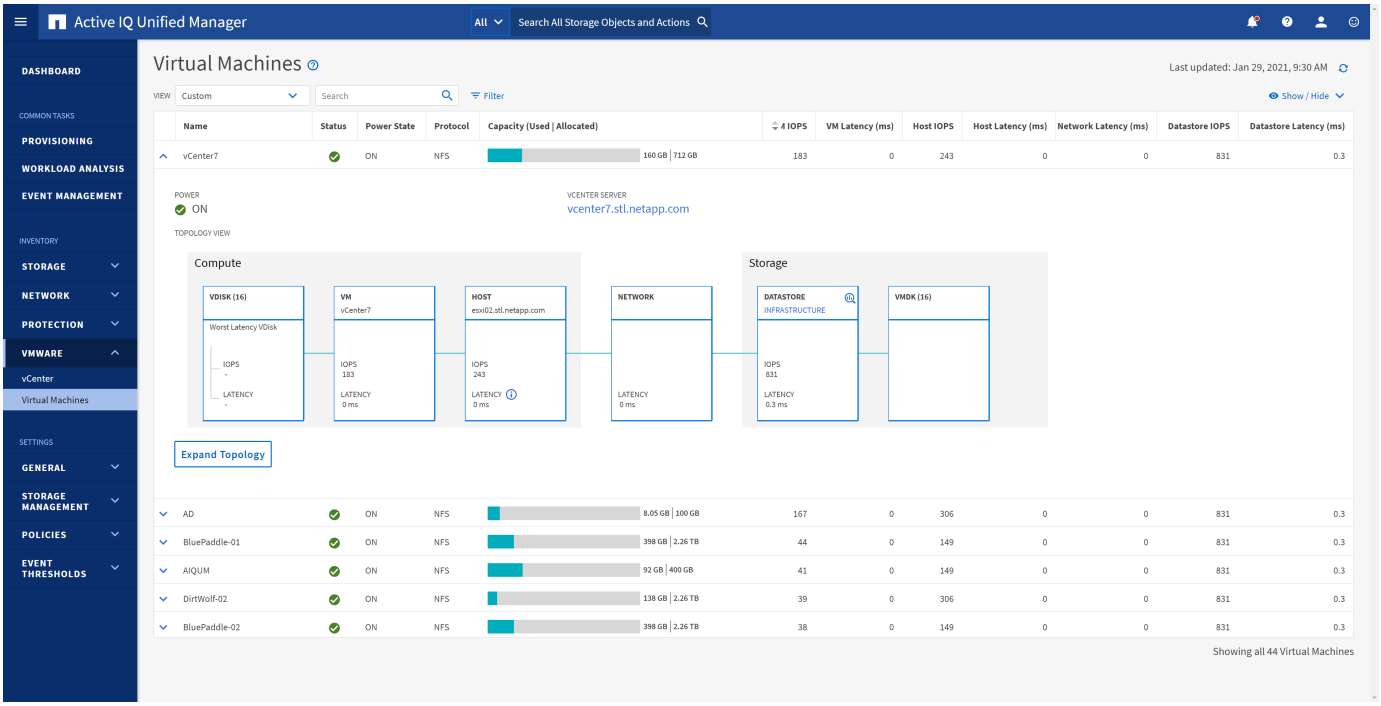
- "보안 기술 보고서"
- "보안 강화 가이드"
- "ONTAP 보안 및 데이터 암호화 제품 설명서"

Active IQ Unified Manager

Active IQ Unified Manager는 가상 인프라의 VM에 대한 가시성을 제공하고 가상 환경에서 스토리지 및 성능 문제를 모니터링하고 문제를 해결할 수 있도록 지원합니다.

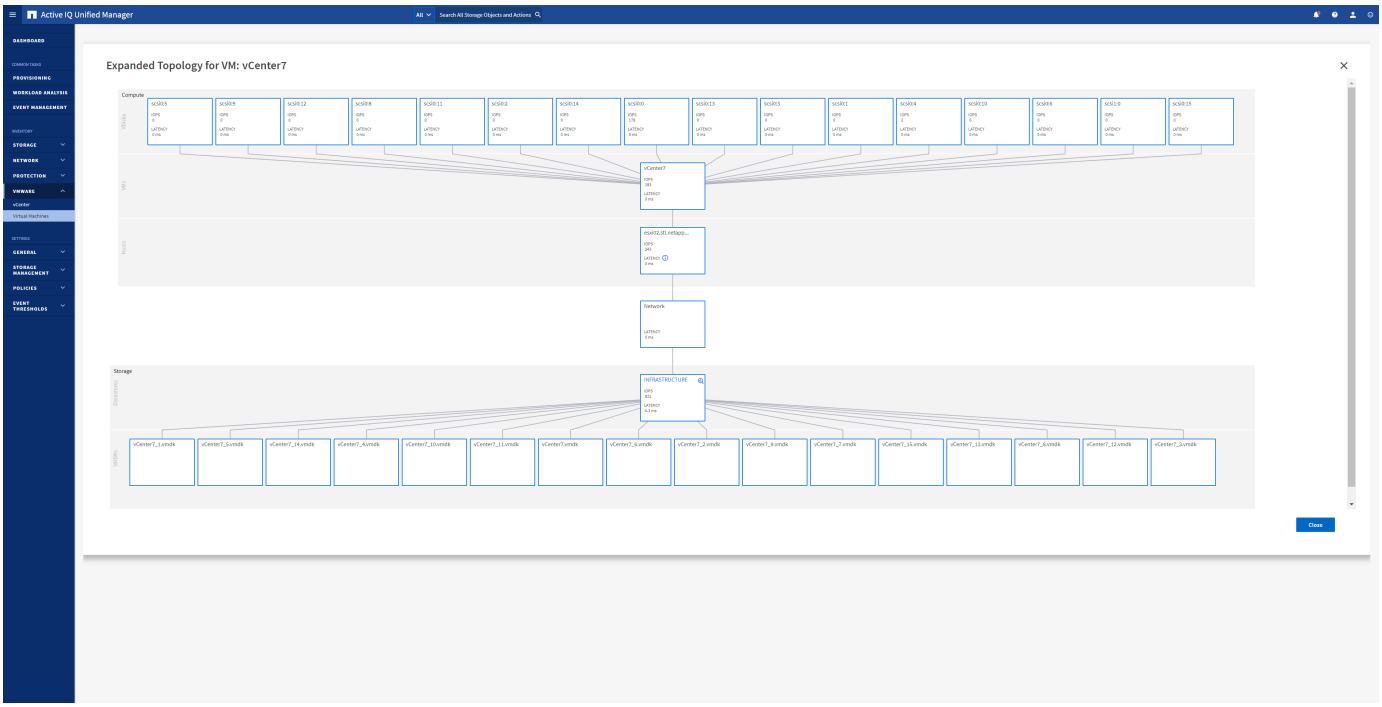
ONTAP 기반의 일반적인 가상 인프라 구축에는 컴퓨팅, 네트워크 및 스토리지 계층 전체에 분산된 다양한 구성 요소가 있습니다. VM 애플리케이션의 성능 지연은 각 계층의 다양한 구성 요소에 의해 발생하는 지연 시간의 조합으로 인해 발생할 수 있습니다.

다음 스크린샷은 Active IQ Unified Manager 가상 머신 보기를 보여 줍니다.



Unified Manager는 가상 환경의 기본 하위 시스템을 토폴로지 뷰에서 제공하므로 컴퓨팅 노드, 네트워크 또는 스토리지에서 지연 시간 문제가 발생했는지 여부를 확인할 수 있습니다. 또한 개선 단계를 수행하고 기본 문제를 해결하는 데 성능 지연이 발생하는 특정 개체를 중점적으로 보여 줍니다.

다음 스크린샷은 AIQUM 확장 토폴로지를 보여줍니다.



스토리지 정책 기반 관리 및 **VVOL**

VMware VASA(vSphere APIs for Storage Awareness)를 사용하면 스토리지 관리자가 잘

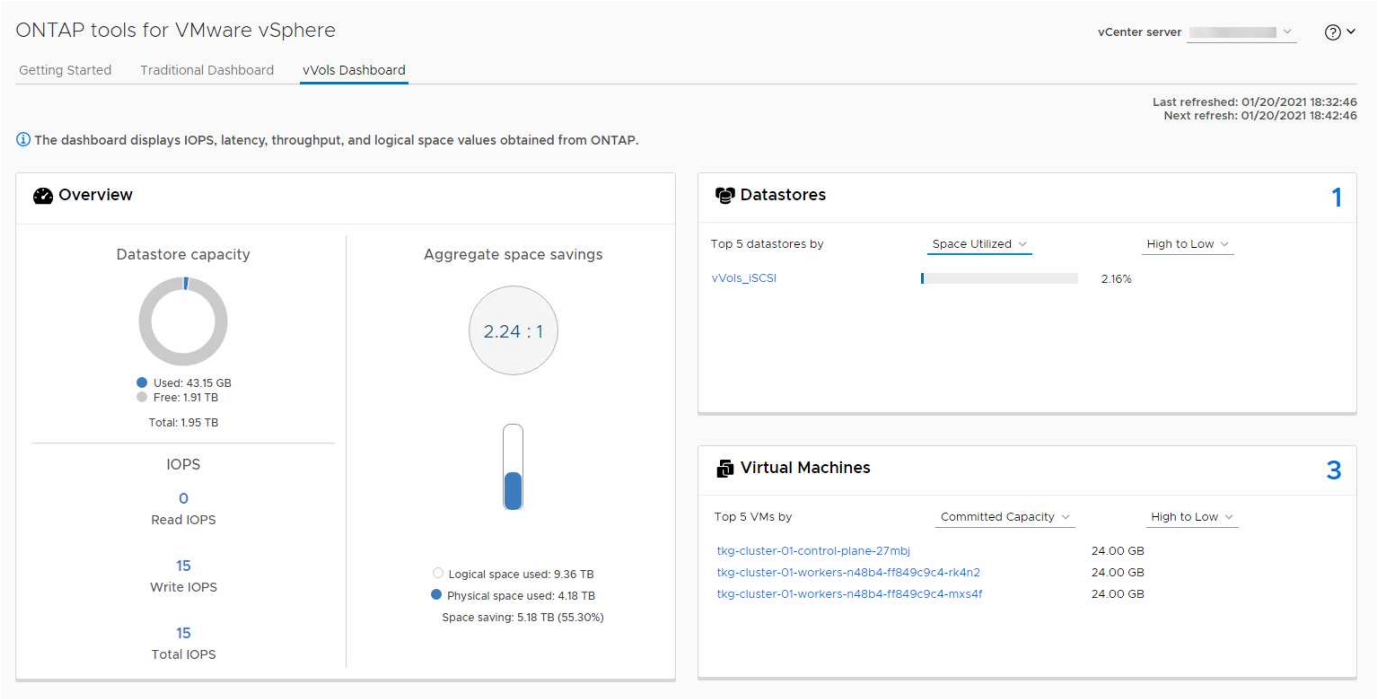
정의된 기능을 사용하여 데이터 저장소를 쉽게 구성하고 VM 관리자는 상호 작용하지 않고도 VM을 프로비저닝할 때 이러한 데이터 저장소를 사용할 수 있습니다.

가상화 스토리지 운영을 간소화하고 사소한 작업을 많이 피하는 방법을 알아보려면 이 접근 방식을 살펴보시기 바랍니다.

VASA를 사용하기 전에는 VM 관리자가 VM 스토리지 정책을 정의할 수 있었지만, 스토리지 관리자와 협력하여 적절한 데이터 저장소를 식별해야 했습니다. 이러한 데이터 저장소는 보통 설명서 또는 명명 규칙을 사용합니다. 스토리지 관리자는 VASA를 통해 성능, 계층화, 암호화, 복제를 비롯한 다양한 스토리지 기능을 정의할 수 있습니다. 볼륨 또는 볼륨 세트에 대한 기능 세트를 SCP(Storage Capability Profile)라고 합니다.

SCP는 VM의 데이터 VVol에 대한 최소 및/또는 최대 QoS를 지원합니다. 최소 QoS는 AFF 시스템에서만 지원됩니다. VMware vSphere용 ONTAP 툴에는 ONTAP 시스템에서 VVOL을 위한 VM 레벨의 세분화된 성능과 논리적 용량을 보여주는 대시보드가 포함되어 있습니다.

다음 그림은 VMware vSphere 9.8 VVol 대시보드를 위한 ONTAP 툴을 보여 줍니다.



스토리지 용량 프로필을 정의한 후에는 요구 사항을 식별하는 스토리지 정책을 사용하여 VM을 프로비저닝하는 데 사용할 수 있습니다. VM 스토리지 정책과 데이터 저장소 스토리지 용량 프로파일 간의 매핑을 통해 vCenter에서 선택할 수 있는 호환 데이터 저장소 목록을 표시할 수 있습니다. 이러한 접근 방식을 스토리지 정책 기반 관리라고 합니다.

VASA는 스토리지를 쿼리하고 스토리지 기능 집합을 vCenter에 반환하는 기술을 제공합니다. VASA 공급업체 공급자는 스토리지 시스템 API 및 구성 요소 및 vCenter에서 인식할 수 있는 VMware API 간의 변환을 제공합니다. NetApp의 VASA Provider for ONTAP는 VMware vSphere 어플라이언스 VM을 위한 ONTAP 툴의 일부로 제공됩니다. 또한, vCenter 플러그인은 VVOL 데이터 저장소를 프로비저닝 및 관리하기 위한 인터페이스를 제공하며 SCP(스토리지 기능 프로필)를 정의합니다.

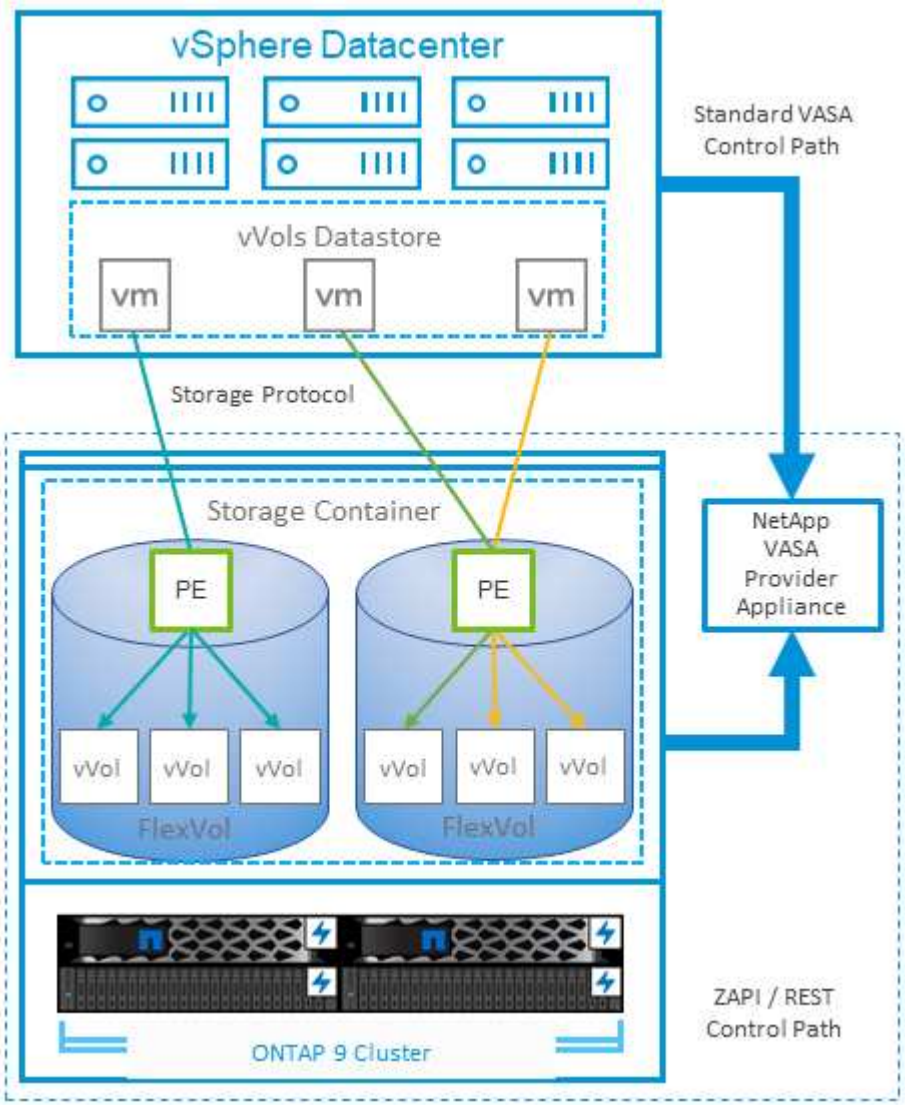
ONTAP는 VMFS 및 NFS VVOL 데이터 저장소를 모두 지원합니다. SAN 데이터 저장소와 VVOL을 함께 사용하면 VM 수준 정밀도와 같은 NFS의 몇 가지 이점이 있습니다. 다음은 고려해야 할 몇 가지 모범 사례이며 에서 추가 정보를 찾을 수 있습니다 "TR-4400 을 참조하십시오":

- VVOL 데이터 저장소는 여러 클러스터 노드의 여러 FlexVol 볼륨으로 구성될 수 있습니다. 가장 간단한 방법은

볼륨에 기능이 다른 경우에도 단일 데이터 저장소를 사용하는 것입니다. SPBM은 호환 볼륨이 VM에 사용되는지 확인합니다. 하지만 모든 볼륨은 단일 ONTAP SVM에 속하고 단일 프로토콜을 사용하여 액세스해야 합니다. 각 프로토콜당 하나의 LIF로 충분합니다. 스토리지 기능이 릴리즈별로 다를 수 있으므로 단일 VVOL 데이터 저장소 내에서 여러 ONTAP 릴리즈를 사용하는 것은 피하십시오.

- VMware vSphere용 ONTAP 툴을 사용하여 VVOL 데이터 저장소를 만들고 관리합니다. 데이터 저장소와 해당 프로필을 관리하는 것 외에도 필요한 경우 데이터 저장소에 액세스하기 위한 프로토콜 엔드포인트가 자동으로 생성됩니다. LUN을 사용하는 경우 LUN PES는 LUN ID 300 이상을 사용하여 매핑됩니다. ESXi 호스트 고급 시스템 설정을 확인합니다 `Disk.MaxLUN` 300보다 높은 LUN ID 번호를 허용합니다(기본값: 1,024). 이 단계를 수행하려면 vCenter에서 ESXi 호스트를 선택한 다음 구성 탭을 선택하고 을 찾습니다 `Disk.MaxLUN` 고급 시스템 설정 목록에서 선택합니다.
- VMware vSphere를 위한 VASA Provider, vCenter Server(어플라이언스 또는 Windows 기반) 또는 ONTAP 툴을 VVOL 데이터 저장소에 설치하거나 마이그레이션하지 마십시오. 상호 의존하기 때문에 정전이 발생하거나 기타 데이터 센터가 중단될 경우 이를 관리할 수 없습니다.
- VASA Provider VM을 정기적으로 백업합니다. VASA Provider가 포함된 기존 데이터 저장소의 시간별 스냅샷을 적어도 생성합니다. VASA Provider 보호 및 복구에 대한 자세한 내용은 다음을 참조하십시오 "KB 문서를 참조하십시오".

다음 그림은 VVol 구성 요소를 보여줍니다.



VMware 스토리지 분산 리소스 스케줄러입니다

VMware SDRS(Storage Distributed Resource Scheduler)는 현재 입출력 지연 시간과 공간 사용량을 기준으로 VM을 데이터 저장소 클러스터에 자동으로 배치하는 vSphere 기능입니다.

그런 다음 데이터 저장소 클러스터(Pod라고도 함)의 데이터 저장소 간에 VM 또는 VMDK를 중단 없이 이동하여 VM 또는 VMDK를 데이터 저장소 클러스터에 배치할 최상의 데이터 저장소를 선택합니다. 데이터 저장소 클러스터는 vSphere 관리자의 관점에서 단일 사용 단위로 집계되는 유사한 데이터 저장소의 모음입니다.

VMware vSphere용 ONTAP 툴과 함께 SDRS를 사용하는 경우 먼저 플러그인을 사용하여 데이터 저장소를 생성하고 vCenter를 사용하여 데이터 저장소 클러스터를 생성한 다음 데이터 저장소를 데이터 저장소에 추가해야 합니다. 데이터 저장소 클러스터가 생성된 후 세부 정보 페이지의 프로비저닝 마법사에서 추가 데이터 저장소를 데이터 저장소 클러스터에 직접 추가할 수 있습니다.

SDRS에 대한 기타 ONTAP 모범 사례는 다음과 같습니다.

- 특별한 요구 사항이 없는 경우 SDRS를 사용하지 마십시오.
  - ONTAP를 사용할 때는 SDRS가 필요하지 않습니다. SDRS는 중복 제거 및 압축과 같은 ONTAP 스토리지 효율성 기능에 대해 알지 못하므로 고객의 환경에 적합하지 않은 의사 결정을 내릴 수 있습니다.
  - SDRS는 ONTAP QoS 정책을 인식하지 못하므로 성능에 적합하지 않은 의사 결정을 내릴 수 있습니다.
  - SDRS는 ONTAP 스냅샷 복사본에 대해 알지 못하므로 스냅샷이 기하급수적으로 증가할 수 있는 결정을 내릴 수 있습니다. 예를 들어 VM을 다른 데이터 저장소로 이동하면 새 데이터 저장소에 새 파일이 생성되며, 이로 인해 스냅샷이 커지게 됩니다. 특히 대용량 디스크 또는 많은 스냅샷이 있는 VM의 경우 이러한 현상이 더욱 두드러집니다. 그런 다음 VM을 원래 데이터 저장소로 다시 이동하면 원래 데이터 저장소의 스냅샷이 더욱 커집니다.

SDRS를 사용하는 경우 다음 모범 사례를 고려하십시오.

- 클러스터의 모든 데이터 저장소는 동일한 유형의 스토리지(예: SAS, SATA 또는 SSD)를 사용하고 모든 VMFS 또는 NFS 데이터 저장소이며 복제 및 보호 설정이 동일해야 합니다.
- 기본(수동) 모드에서 SDRS 사용을 고려하십시오. 이 접근 방식을 통해 권장 사항을 검토하고 적용 여부를 결정할 수 있습니다. VMDK 마이그레이션의 영향을 숙지하십시오.
  - SDRS가 데이터 저장소 간에 VMDK를 이동할 경우 대상에서 중복제거 또는 압축의 정도에 따라 ONTAP 클론 복제 또는 중복제거를 통해 절약되는 공간이 감소할 수 있습니다.
  - SDRS가 VMDK를 이동한 후 NetApp는 소스 데이터 저장소에서 스냅샷을 다시 생성하는 것이 좋습니다. 그렇지 않으면 공간이 이동된 VM에 의해 잠기기 때문입니다.
  - 동일한 애그리게이트에서 데이터 저장소 간에 VMDK를 이동하는 것은 효과가 거의 없으며 SDRS는 애그리게이트를 공유할 수 있는 다른 워크로드를 파악할 수 없습니다.

SDRS에 대한 자세한 내용은 VMware 설명서를 참조하십시오 "스토리지 DRS FAQ".

권장되는 ESXi 호스트 및 기타 ONTAP 설정

NetApp은 NFS 및 블록 프로토콜 모두에 최적의 ESXi 호스트 설정 세트를 개발했습니다. NetApp 및 VMware 내부 테스트 기반의 ONTAP에서 올바른 동작을 수행할 수 있도록 다중 경로 및 HBA 시간 초과 설정에 대해서도 구체적인 지침이 제공됩니다.

이러한 값은 VMware vSphere용 ONTAP 툴을 사용하여 쉽게 설정할 수 있습니다. ONTAP 툴 개요 페이지에서 아래로

스크롤하여 ESXi 호스트 규정 준수 포틀릿에서 권장 설정 적용을 클릭합니다.

다음은 현재 지원되는 모든 ONTAP 버전에 대해 권장되는 호스트 설정입니다.

* 호스트 설정 *	* **NetApp** 권장 가치 *	* 재부팅 필요 *
* ESXi 고급 구성 *		
VMFS3. HardwareAcceleratedLocking	기본값 유지(1)	아니요
VMFS3.EnableBlockDelete 를 참조하십시오	기본값 유지(0), 필요한 경우 변경할 수 있습니다. 자세한 내용은 을 참조하십시오 "VMFS5 가상 머신에 대한 공간 재확보"	아니요
VMFS3.EnableVMFS6매핑 해제	기본값 유지(1) 자세한 내용은 을 참조하십시오 "VMware vSphere API: 어레이 통합(VAAI)"	아니요
* NFS 설정 *		
newSyncInterval	Kubernetes용 vSphere CSI를 사용하지 않는 경우 를 설정합니다 "VMware KB 386364"	아니요
NET.TcpipHeapSize	vSphere 6.0 이상, 32로 설정. 다른 모든 NFS 구성은 30으로 설정합니다	예
net.TcpipHeapMax	대부분의 vSphere 6.X 릴리즈에서는 512MB로 설정합니다. 6.5U3, 6.7U3 및 7.0 이상에서는 기본값(1024MB)으로 설정합니다.	예
NFS.MaxVolumes	vSphere 6.0 이상, 256으로 설정 기타 모든 NFS 구성은 64로 설정되었습니다.	아니요
NFS41.최대 볼륨	vSphere 6.0 이상, 256으로 설정	아니요
NFS.MaxQueueDepth[1]	vSphere 6.0 이상으로, 128로 설정합니다	예
NFS.HeartbeatMaxFailures 를 참조하십시오	모든 NFS 구성에 대해 10으로 설정합니다	아니요
NFS.HeartbeatFrequency 를 선택합니다	모든 NFS 구성에 대해 12로 설정합니다	아니요
NFS.HeartbeatTimeout	모든 NFS 구성에 대해 5로 설정합니다.	아니요
SunRPC.MaxConnPerIP입니다	vSphere 7.0~8.0은 128로 설정되었습니다. 이 설정은 ESXi 8.0 이후 릴리스에서는 무시됩니다.	아니요
* FC/FCoE 설정 *		

* 호스트 설정 *	* **NetApp** 권장 가치 *	* 재부팅 필요 *
경로 선택 정책	ALUA를 사용하는 FC 경로를 사용할 때 RR(라운드 로빈)으로 설정합니다. 다른 모든 설정에 대해 고정으로 설정합니다. 이 값을 RR로 설정하면 모든 활성/최적화 경로에서 로드 밸런싱을 제공하는 데 도움이 됩니다. 고정 값은 이전 비 ALUA 구성에 대한 값이며 프록시 I/O를 방지하는 데 도움이 됩니다 다시 말해, 7-Mode에서 Data ONTAP를 실행하는 환경에서 I/O가 고가용성(HA) 쌍의 다른 노드로 이동하는 것을 돕니다	아니요
Disk.QFullSampleSize 를 참조하십시오	모든 설정에 대해 32로 설정합니다. 이 값을 설정하면 I/O 오류가 방지됩니다.	아니요
Disk.QFullThreshold를 참조하십시오	모든 설정에 대해 8로 설정합니다. 이 값을 설정하면 I/O 오류가 방지됩니다.	아니요
Emulex FC HBA 시간 초과	기본값을 사용합니다.	아니요
QLogic FC HBA 시간 초과	기본값을 사용합니다.	아니요
iSCSI 설정 *		
경로 선택 정책	모든 iSCSI 경로에 대해 RR(라운드 로빈)으로 설정합니다. 이 값을 RR로 설정하면 모든 활성/최적화 경로에서 로드 밸런싱을 제공하는 데 도움이 됩니다.	아니요
Disk.QFullSampleSize 를 참조하십시오	모든 설정에 대해 32로 설정합니다. 이 값을 설정하면 I/O 오류가 방지됩니다	아니요
Disk.QFullThreshold를 참조하십시오	모든 설정에 대해 8로 설정합니다. 이 값을 설정하면 I/O 오류가 방지됩니다.	아니요

NFS 고급 구성 옵션 MaxQueueDepth는 VMware vSphere ESXi 7.0.1 및 VMware vSphere ESXi 7.0.2를 사용할 때 의도한 대로 작동하지 않을 수 있습니다. 자세한 내용은 을 "VMware KB 86331"참조하십시오.

ONTAP 툴은 ONTAP FlexVol 볼륨 및 LUN을 생성할 때 특정 기본 설정도 지정합니다.

* ONTAP 도구 *	* 기본 설정 *
스냅숏 예비 공간(-percent-snapshot-space)	0
분할 예약(-fractional-reserve)	0
액세스 시간 업데이트(-atime-update)	거짓

최소 미리 읽기(-min-readahead)	거짓
예약된 스냅샷	없음
스토리지 효율성	활성화됨
볼륨 보장	없음(씬 프로비저닝됨)
볼륨 자동 크기 조정	grow_shrink
LUN 공간 예약	사용 안 함
LUN 공간 할당	활성화됨

성능을 위한 다중 경로 설정

현재 사용 가능한 ONTAP 툴에 의해 구성되지 않은 상태에서 NetApp에서는 다음과 같은 구성 옵션을 제안합니다.

- 고성능 환경에서 ASA 가 아닌 시스템을 사용하거나 단일 LUN 데이터 저장소로 성능을 테스트하는 경우 라운드 로빈(VMW_PSP_RR) 경로 선택 정책(PSP)의 부하 분산 설정을 기본 IOPS 설정인 1000에서 값 1로 변경하는 것을 고려하세요. 보다"VMware KB 2069356" 자세한 내용은.
- vSphere 6.7 업데이트 1에서 VMware는 라운드 로빈 PSP에 대한 새로운 지연 부하 분산 메커니즘을 도입했습니다. 이제 NVMe 네임스페이스와 함께 HPP(고성능 플러그인)를 사용하고 vSphere 8.0u2 이상, iSCSI 및 FCP 연결 LUN을 사용하는 경우에도 대기 시간 옵션을 사용할 수 있습니다. 새로운 옵션은 I/O에 대한 최적의 경로를 선택할 때 I/O 대역폭과 경로 지연 시간을 고려합니다. NetApp 경로 연결이 동등하지 않은 환경(예: 한 경로에 다른 경로보다 많은 네트워크 홉이 있는 경우)이나 NetApp ASA 시스템을 사용하는 경우에서 대기 시간 옵션을 사용할 것을 권장합니다. 보다 "지연 라운드 로빈의 기본 매개 변수를 변경합니다" 자세한 내용은.

추가 문서

vSphere 7이 포함된 FCP 및 iSCSI의 경우 자세한 "ONTAP와 함께 VMware vSphere 7.x를 사용합니다"내용은 vSphere 8이 설치된 FCP 및 iSCSI에서 찾을 "ONTAP와 함께 VMware vSphere 8.x를 사용합니다"수 있습니다. 자세한 내용은 vSphere 7이 설치된 NVMe-oF 를 "NVMe-oF의 경우 자세한 내용은 ONTAP를 사용하는 ESXi 7.x용 NVMe-oF 호스트 구성 을 참조하십시오"참조하십시오. 자세한 내용은 vSphere 8이 설치된 NVMe-oF 를 참조하십시오 "NVMe-oF의 경우 자세한 내용은 ONTAP를 사용하는 ESXi 8.x용 NVMe-oF 호스트 구성 을 참조하십시오"

ONTAP 툴을 이용한 VVOL(가상 볼륨) 10

개요

ONTAP는 20년 이상 VMware vSphere 환경을 위한 업계 최고의 스토리지 솔루션으로, 비용을 절감하는 동시에 관리를 간소화하는 혁신적인 기능을 지속적으로 추가하고 있습니다.

본 문서에서는 구축 간소화 및 오류 감소를 위한 모범 사례와 함께 최신 제품 정보 및 사용 사례를 비롯하여 VMware VVOL(vSphere Virtual Volumes)의 ONTAP 기능에 대해 다룹니다.

> ⓘ 이 문서는 이전에 게시된 기술 보고서_TR-4400: VMware VVol(vSphere 가상 볼륨)을 ONTAP _ 로 대체합니다

모범 사례는 가이드 및 호환성 목록 등의 다른 문서를 보완합니다. 이러한 전문 분야는 연구소 테스트와 NetApp 엔지니어 및 고객의 광범위한 현장 경험을 기반으로 합니다. 이러한 방법은 효과가 있거나 지원되는 유일한 방법이 아닐 수 있지만, 일반적으로 대부분의 고객의 요구를 충족하는 가장 간단한 솔루션입니다.

이 문서는 vSphere 8.0 업데이트 3, ONTAP 툴 10.4 릴리즈 및 새로운 NetApp ASA 시스템에서 발견되는 새로운 VVOL 기능을 포함하도록 업데이트되었습니다.

VVol(가상 볼륨) 개요

NetApp은 VMware와 협력하여 2012년에 vSphere 5용 VASA(vSphere APIs for Storage Awareness)를 지원하기 시작했습니다. 이 초기 VASA Provider는 프로비저닝 시 데이터 저장소를 필터링하고 나중에 정책 준수 여부를 확인하는 데 사용할 수 있는 프로파일의 스토리지 용량 정의를 허용합니다. 시간이 지나면서 프로비저닝 시 더 많은 자동화를 가능하게 하는 새로운 기능을 추가하고 개별 스토리지 오브젝트를 가상 머신 파일 및 가상 디스크에 사용하는 가상 볼륨 또는 VVol을 추가하였습니다. 이러한 오브젝트는 LUN, 파일일 수 있으며 이제 vSphere 8-NVMe 네임스페이스(ONTAP 툴 9.13P2에서 사용)와 함께 사용할 수 있습니다. NetApp은 2015년에 vSphere 6에 릴리즈된 VVOL의 참조 파트너로 VMware와 긴밀하게 협력했으며, vSphere 8에서 NVMe over Fabrics를 사용하는 VVOL의 설계 파트너로 다시 활동했습니다. NetApp은 ONTAP의 최신 기능을 활용하기 위해 VVOL을 지속적으로 개선합니다.

다음과 같은 몇 가지 구성 요소를 알고 있어야 합니다.

VASA 공급자

이 소프트웨어 구성 요소는 VMware vSphere와 스토리지 시스템 간의 통신을 처리합니다. ONTAP의 경우 VASA Provider는 VMware vSphere용 ONTAP 툴(짧은 경우 ONTAP 툴)이라는 어플라이언스에서 실행됩니다. ONTAP 툴에는 vCenter 플러그인, VMware Site Recovery Manager용 SRA(스토리지 복제 어댑터), 자체 자동화 구축을 위한 REST API 서버도 포함되어 있습니다. vCenter에 ONTAP 툴이 구성 및 등록되면 vCenter UI 내에서 직접 또는 REST API 자동화를 통해 거의 모든 스토리지 요구 사항을 관리할 수 있으므로 더 이상 ONTAP 시스템과 직접 상호 작용할 필요가 없습니다.

프로토콜 엔드포인트**(PE)**

프로토콜 엔드포인트는 ESXi 호스트와 VVol 데이터 저장소 간의 I/O용 프록시입니다. ONTAP VASA Provider는 이러한 프로토콜을 자동으로 생성합니다. 즉, VVols 데이터 저장소의 FlexVol 볼륨당 프로토콜 엔드포인트 LUN(4MB 크기) 1개 또는 데이터 저장소에서 FlexVol 볼륨을 호스팅하는 스토리지 노드의 NFS 인터페이스(LIF)당 NFS 마운트 지점 1개 중 하나입니다. ESXi 호스트는 개별 VVol LUN 및 가상 디스크 파일이 아니라 이러한 프로토콜 엔드포인트를 직접 마운트합니다. 필요한 인터페이스 그룹 또는 내보내기 정책과 함께 VASA Provider가 프로토콜 엔드포인트를 자동으로 생성, 마운트, 마운트 해제 및 삭제할 때 이를 관리할 필요가 없습니다.

VPE(가상 프로토콜 엔드포인트)

vSphere 8의 새로운 기능으로, VVOL과 NVMe-oF(NVMe over Fabrics)를 사용하면 프로토콜 엔드포인트 개념이 ONTAP에서 더 이상 의미가 없습니다. 그 대신 첫 번째 VM의 전원이 켜지자마자 각 ANA 그룹의 ESXi 호스트에 의해 가상 PE가 자동으로 인스턴스화됩니다. ONTAP는 데이터 저장소에서 사용하는 각 FlexVol 볼륨에 대해 ANA 그룹을 자동으로 생성합니다.

VVOL을 위한 NVMe-oF를 사용할 경우 추가적인 이점은 VASA Provider에 필요한 바인딩 요청이 없다는 것입니다. 대신 ESXi 호스트는 VPE를 기반으로 내부적으로 VVol 바인딩 기능을 처리합니다. 따라서 VVOL 바인딩 스톰이 서비스에 영향을 줄 수 있는 기회가 줄어듭니다.

자세한 내용은 을 참조하십시오 "NVMe 및 가상 볼륨" 켜짐 "VMware.com"

가상 볼륨 데이터 저장소

가상 볼륨 데이터 저장소는 VASA 공급자가 생성하고 유지 관리하는 vVols 컨테이너의 논리적 데이터 저장소 표현입니다. 컨테이너는 VASA 공급자가 관리하는 스토리지 시스템에서 제공되는 스토리지 용량 풀을 나타냅니다. ONTAP 도구는 여러 FlexVol 볼륨(백업 볼륨이라고 함)을 단일 vVols 데이터스토어에 할당하는 것을 지원하며, 이러한 vVols 데이터스토어는 ONTAP 클러스터의 여러 노드에 걸쳐 있을 수 있으므로 기능이 다른 플래시 및 하이브리드

시스템을 결합할 수 있습니다. 관리자는 프로비저닝 마법사 또는 REST API를 사용하여 새 FlexVol 볼륨을 생성하거나, 사용 가능한 경우 미리 생성된 FlexVol 볼륨을 백업 스토리지로 선택할 수 있습니다.

VVol(가상 볼륨)

vVols 는 vVols 데이터 저장소에 저장된 실제 가상 머신 파일 및 디스크입니다. vVol(단수)이라는 용어는 특정 파일, LUN 또는 네임스페이스 하나를 지칭합니다. ONTAP 데이터 저장소가 사용하는 프로토콜에 따라 NVMe 네임스페이스, LUN 또는 파일을 생성합니다. vVols 에는 여러 가지 유형이 있습니다. 가장 일반적인 유형으로는 Config(VMFS가 사용되는 유일한 유형으로, VM의 VMX 파일과 같은 메타데이터 파일을 포함함), Data(가상 디스크 또는 VMDK), Swap(VM이 시작될 때 생성됨)이 있습니다. VMware VM 암호화로 보호되는 vVols 기타 유형입니다. VMware VM 암호화는 ONTAP 볼륨 또는 집계 암호화와 혼동해서는 안 됩니다.

정책 기반 관리

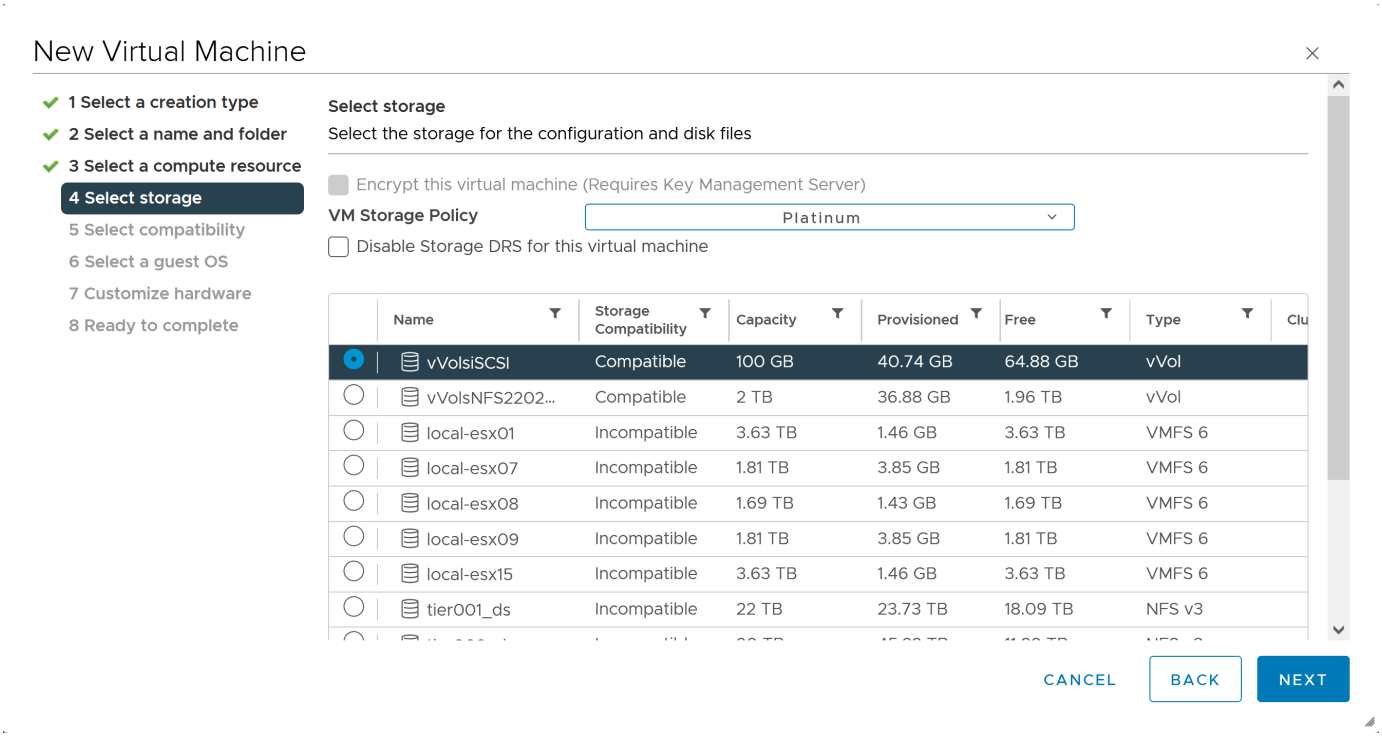
VMware vSphere APIs for Storage Awareness(VASA)를 사용하면 VM 관리자가 스토리지 팀과 상호 작용하지 않고도 VM을 프로비저닝하는 데 필요한 모든 스토리지 기능을 쉽게 사용할 수 있습니다. VASA 이전에는 VM 관리자가 VM 스토리지 정책을 정의할 수 있었지만, 스토리지 관리자와 협력하여 문서나 명명 규칙을 활용해 적절한 데이터 저장소를 식별해야 했습니다. VASA를 사용하면 적절한 권한을 가진 vCenter 관리자가 vCenter 사용자가 VM을 프로비저닝하는 데 사용할 수 있는 스토리지 기능 범위를 정의할 수 있습니다. VM 스토리지 정책과 데이터스토어 기능 간의 매핑을 통해 vCenter는 선택할 수 있는 호환 데이터스토어 목록을 표시할 뿐만 아니라 VCF(이전의 Aria 및 vRealize) 자동화 또는 VMware vSphere Kubernetes Service(VKS)와 같은 다른 기술에서 할당된 정책에서 스토리지를 자동으로 선택할 수 있도록 합니다. 이러한 접근 방식을 스토리지 정책 기반 관리라고 합니다. VASA 공급자 규칙 및 VM 스토리지 정책은 기존 데이터스토어와 함께 사용할 수도 있지만, 여기서는 vVols 데이터스토어에 초점을 맞추겠습니다.

VM 스토리지 정책

VM 스토리지 정책은 vCenter의 정책 및 프로필 아래에 생성됩니다. VVOL의 경우 NetApp VVOL 스토리지 유형 공급자에서 규칙을 사용하여 규칙 집합을 생성합니다. 이제 ONTAP 툴 10.X는 VM 스토리지 정책 자체에 스토리지 속성을 직접 지정할 수 있으므로 ONTAP 툴 9.X보다 더 간단한 접근 방식을 제공합니다.

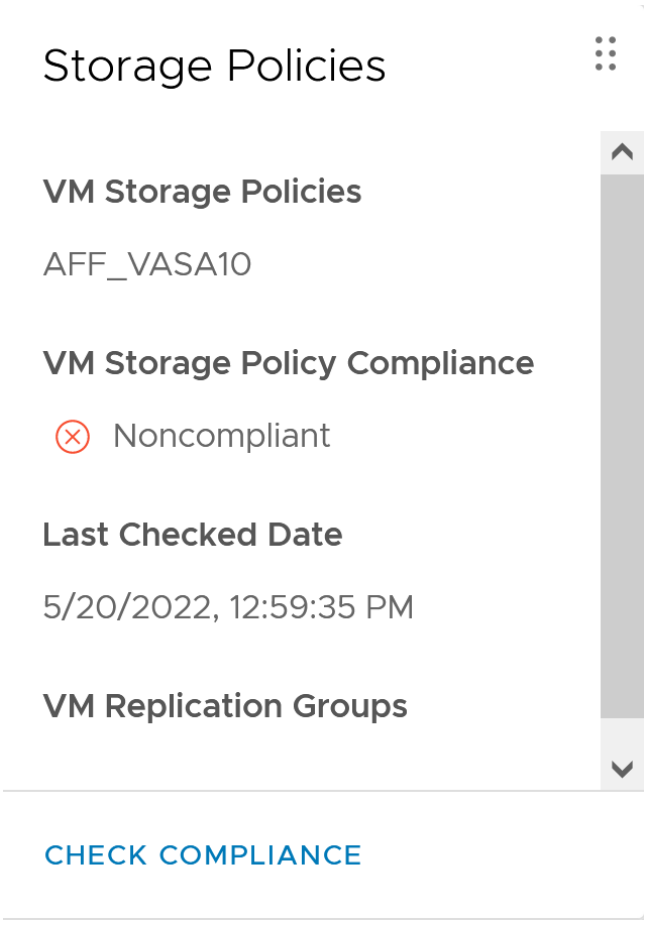
위에서 언급한 것처럼 정책을 사용하면 VM 또는 VMDK 프로비저닝 작업을 간소화할 수 있습니다. 적절한 정책을 선택하기만 하면 VASA Provider는 해당 정책을 지원하는 VVol 데이터 저장소를 표시하고 VVOL을 호환되는 개별 FlexVol volume에 배치합니다.

스토리지 정책을 사용하여 VM 구축



VM이 프로비저닝되면 VASA 공급자는 지속적으로 규정 준수 여부를 확인하고 백업 볼륨이 더 이상 정책을 준수하지 않을 경우 vCenter에서 알람을 통해 VM 관리자에게 알립니다.

VM 스토리지 정책 준수



NetApp VVOL 지원

ONTAP 2012년 최초 출시 이후 VASA 사양을 지원해 왔습니다. 다른 NetApp 스토리지 시스템에서도 VASA를 지원할 수 있지만, 이 문서에서는 현재 지원되는 ONTAP 9 릴리스에 중점을 둡니다.

ONTAP

AFF, ASA 및 FAS 시스템의 ONTAP 9 외에도 NetApp ONTAP Select 의 VMware 워크로드, AWS의 VMware Cloud를 사용하는 Amazon FSx for NetApp , Azure VMware Solution을 사용하는 Azure NetApp Files , Google Cloud NetApp Volumes , Equinix의 NetApp Private Storage를 지원하지만 특정 기능은 서비스 공급자 및 사용 가능한 네트워크 연결에 따라 달라질 수 있습니다.

이 문서가 발행될 당시 하이퍼스케일러 환경은 기존 NFS v3 데이터스토어로만 제한되었습니다. 따라서 vVols 온프레미스 ONTAP 시스템 또는 전 세계 NetApp 파트너 및 서비스 제공업체가 호스팅하는 시스템과 같이 온프레미스 시스템의 모든 기능을 제공하는 클라우드 연결 시스템에서만 사용할 수 있습니다.

_ ONTAP에 대한 자세한 내용은 을(를) 참조하십시오 "ONTAP 제품 설명서"_

_ ONTAP 및 VMware vSphere Best Practice에 대한 자세한 내용은 를 참조하십시오 "TR-4597 을 참조하십시오"_

ONTAP와 함께 VVOL을 사용할 때의 이점

VMware는 2015년 VASA 2.0에서 vVols 지원을 도입하면서 이를 "외부 스토리지(SAN/NAS)를 위한 새로운 운영 모델을 제공하는 통합 및 관리 프레임워크"라고 설명했습니다. 이 운영 모델은 ONTAP 스토리지와 함께 여러 가지 이점을 제공합니다.

정책 기반 관리

섹션 1.2에서 설명한 바와 같이 정책 기반 관리를 통해 미리 정의된 정책을 사용하여 VM을 프로비저닝하고 관리할 수 있습니다. 이는 IT 운영에 여러 가지 방식으로 도움이 될 수 있습니다.

- 속도를 높이세요. ONTAP 도구를 사용하면 vCenter 관리자가 스토리지 프로비저닝 작업을 위해 스토리지 팀에 티켓을 발행해야 하는 요구 사항이 사라집니다. 하지만 vCenter와 ONTAP 시스템의 ONTAP 도구 RBAC 역할은 원하는 경우 특정 기능에 대한 액세스를 제한함으로써 독립적인 팀(예: 스토리지 팀) 또는 동일 팀 내의 독립적인 활동을 허용합니다.
- * 보다 현명한 프로비저닝. * 스토리지 시스템 기능은 VASA API를 통해 노출되므로 VM 관리자가 스토리지 시스템 관리 방법을 이해하지 않고도 프로비저닝 워크플로우를 통해 고급 기능을 활용할 수 있습니다.
- 신속한 프로비저닝 * 다양한 스토리지 기능을 단일 데이터 저장소에서 지원하고 VM 정책에 따라 VM에 적합한 대로 자동으로 선택할 수 있습니다.
- * 실수를 피하십시오. * 스토리지 및 VM 정책은 미리 개발되고 VM을 프로비저닝할 때마다 스토리지를 사용자 지정할 필요 없이 필요에 따라 적용됩니다. 정의된 정책에서 스토리지 기능이 떨어지면 규정 준수 알람이 발생합니다. 앞서 언급한 것처럼, ICP는 초기 프로비저닝을 예측 가능하고 반복 가능하게 만드는 동시에, ICP를 기반으로 하는 VM 스토리지 정책을 수립하여 정확한 배치를 보장합니다.
- * 향상된 용량 관리 * VASA 및 ONTAP 툴을 사용하면 필요한 경우 스토리지 용량을 개별 애그리게이트 레벨까지 확인하고, 용량이 부족해지기 시작할 때 여러 계층의 알림을 제공할 수 있습니다.

최신 SAN에서 VM 세부 관리

파이버 채널과 iSCSI를 사용하는 SAN 스토리지 시스템은 VMware에서 ESX용으로 처음 지원되었지만, 스토리지 시스템에서 개별 VM 파일과 디스크를 관리하는 기능은 부족했습니다. 대신 LUN이 프로비저닝되고 VMFS가 개별 파일을 관리합니다. 이로 인해 스토리지 시스템이 개별 VM 스토리지 성능, 클론 생성 및 보호를 직접 관리하기

어렵습니다. vVols NFS 스토리지를 사용하는 고객이 이미 누리고 있는 스토리지 세분성을 ONTAP 의 강력하고 고성능 SAN 기능과 결합하여 제공합니다.

이제 vSphere 8과 ONTAP tools for VMware vSphere 기존 SCSI 기반 프로토콜용 vVols 에서 사용되던 것과 동일한 세부 제어 기능을 NVMe over Fabric을 사용하는 최신 파이버 채널 SAN에서도 사용할 수 있어 확장성 측면에서 더욱 뛰어난 성능을 제공합니다. vSphere 8.0 업데이트 1을 사용하면 하이퍼바이저 스토리지 스택에서 I/O 변환 없이 vVols 사용하여 완벽한 엔드투엔드 NVMe 솔루션을 배포할 수 있습니다.

스토리지 오프로드 기능

VAAI는 스토리지로 오프로드되는 다양한 작업을 제공하지만, VASA 공급자가 해결하는 몇 가지 부족한 부분이 있습니다. SAN VAAI는 VMware에서 관리하는 스냅샷을 스토리지 시스템으로 오프로드할 수 없습니다. NFS VAAI는 VM에서 관리하는 스냅샷을 오프로드할 수 있지만, 스토리지 네이티브 스냅샷을 사용하는 VM에는 몇 가지 제한 사항이 있습니다. vVols 가상 머신 디스크에 개별 LUN, 네임스페이스 또는 파일을 사용하므로 ONTAP 파일이나 LUN을 신속하고 효율적으로 복제하여 델타 파일이 더 이상 필요하지 않은 VM 단위의 스냅샷을 생성할 수 있습니다. NFS VAAI는 전원이 켜진 상태의 Storage vMotion 마이그레이션을 위한 클론 작업 오프로딩도 지원하지 않습니다. 기존 NFS 데이터스토어를 사용하는 VAAI를 사용할 경우 마이그레이션 오프로딩을 허용하려면 VM의 전원을 꺼야 합니다. ONTAP 도구의 VASA Provider를 사용하면 핫 마이그레이션 및 콜드 마이그레이션을 위한 스토리지 효율적인 클론을 거의 즉시 생성할 수 있으며, vVols 의 볼륨 간 마이그레이션을 위한 거의 즉각적인 복사도 지원합니다. 이러한 상당한 스토리지 효율성 이점 덕분에 vVols 워크로드를 최대한 활용할 수 있습니다. "효율성 보장" 프로그램. 마찬가지로, VAAI를 사용한 볼륨 간 복제가 요구 사항을 충족하지 못하는 경우 vVols 의 향상된 복사 환경 덕분에 비즈니스 문제를 해결할 수 있을 것입니다.

VVOL의 일반적인 사용 사례

이러한 이점 외에도 VVOL 스토리지의 일반적인 사용 사례도 있습니다.

- * VM의 온디맨드 프로비저닝 *
  - 프라이빗 클라우드 또는 서비스 공급자 IaaS
  - Aria(이전의 vRealize) 제품군, OpenStack 등을 통해 자동화 및 오케스트레이션 기능을 활용할 수 있습니다.
- * 일등석 디스크(FCD) *
  - VMware vSphere Kubernetes Service(VKS) 영구 볼륨.
  - 독립적인 VMDK 수명주기 관리를 통해 Amazon EBS와 유사한 서비스를 제공합니다.
- * 임시 VM의 온디맨드 프로비저닝 *
  - 테스트/개발 연구소
  - 교육 환경

VVOL의 일반적인 이점

위와 같은 사용 사례에서 VVOL을 최대한 활용했을 때 VVOL은 다음과 같은 구체적인 개선을 제공합니다.

- 클론은 단일 볼륨 내에서 또는 ONTAP 클러스터의 여러 볼륨에 걸쳐 빠르게 생성되므로 기존 VAAI 지원 클론에 비해 이점이 있습니다. 또한 저장 효율도 뛰어납니다. 볼륨 내의 클론은 ONTAP 파일 클론을 사용하는데, 이는 FlexClone 볼륨과 유사하며 소스 vVol 파일/LUN/네임스페이스의 변경 사항만 저장합니다. 따라서 프로덕션 또는 기타 애플리케이션 용도로 장기간 사용할 VM을 신속하게 생성하고 최소한의 공간만 차지하며 VM 수준 보호(VMware vSphere용 NetApp SnapCenter 플러그인, VMware 관리형 스냅샷 또는 VADP 백업 사용) 및 성능 관리(ONTAP QoS 사용)의 이점을 누릴 수 있습니다. VASA를 사용하면 복제가 완료되기 전에 대상 위치에서 복제본에 대한 액세스를 허용할 수 있으므로, VAAI보다 vVols 사용한 크로스 볼륨 복제가 훨씬 빠릅니다. 데이터 블록은 백그라운드 프로세스로 복사되어 대상 vVol을 채웁니다. 이는 기존 LUN에 대해 ONTAP 무중단 LUN

이동이 작동하는 방식과 유사합니다.

- VVol은 vSphere CSI와 함께 TKG를 사용할 때 이상적인 스토리지 기술로서 vCenter 관리자가 관리하는 개별 스토리지 클래스 및 용량을 제공합니다.
- Amazon EBS와 유사한 서비스는 FCD를 통해 제공될 수 있습니다. 이름에서 알 수 있듯이 FCD VMDK는 vSphere에서 핵심적인 역할을 하며, 연결된 VM과 별도로 독립적으로 관리할 수 있는 수명 주기를 가지고 있기 때문입니다.

체크리스트

성공적인 배포를 위해 이 설치 체크리스트를 사용하십시오(10.3 이상 업데이트).

1 초기 계획

- 설치를 시작하기 전에 에서 배포가 인증되었는지 확인해야 "상호 운용성 매트릭스 툴(IMT)" 합니다.
- 환경에 필요한 ONTAP 툴 구성의 크기 및 유형을 결정합니다. 자세한 내용은 을 "VMware vSphere용 ONTAP 툴을 구축하기 위한 구성 제한" 참조하십시오.
- 멀티테넌트 SVM을 사용할 것인지 또는 전체 클러스터 액세스를 허용할 것인지 결정합니다. 멀티테넌트 SVM을 사용하는 경우 사용할 각 SVM에 SVM 관리 LIF가 있어야 합니다. ONTAP 툴을 통해 포트 443을 통해 이 LIF에 연결할 수 있어야 합니다.
- 스토리지 접속에 FC(Fibre Channel)를 사용할 것인지 결정합니다. 그럴 경우 ESXi 호스트와 SVM의 FC LIF 간 연결을 설정하려면 FC 스위치에서 연결해야 "조닝 구성" 합니다.
- VMware SRM(사이트 복구 관리자)에 대해 ONTAP 툴 SRA(스토리지 복제 어댑터)를 사용할지, VLSR(라이브 사이트 복구)을 사용할지 결정합니다. 이 경우 SRM/VLSR 서버 관리 인터페이스에 액세스하여 SRA를 설치해야 합니다.
- ONTAP 도구로 관리되는 SnapMirror 복제(SnapMirror 활성 동기화 포함, 이에 국한되지 않음)를 사용하는 경우 ONTAP 관리자가 "ONTAP에서 인터클러스터 SVM 피어 관계를 생성합니다" ONTAP 도구를 SnapMirror와 함께 사용할 수 있도록 해야 "ONTAP에서 클러스터 피어 관계를 생성합니다" 합니다.
- "다운로드" ONTAP는 OVA를, 필요한 경우 SRA tar.gz 파일을 사용합니다.

2 IP 주소 및 DNS 레코드를 프로비저닝합니다

- 네트워크 팀에 다음 IP 정보를 요청합니다. 처음 3개의 IP 주소가 필요합니다. 노드 2와 노드 3은 스케일아웃 HA(고가용성) 구축에 사용됩니다. DNS 호스트 레코드가 필요하며 모든 노드 이름과 모든 주소가 동일한 VLAN 및 서브넷에 있어야 합니다.
- ONTAP 도구 응용 프로그램 주소 ____. \\. \\. _
- 내부 서비스 주소 ___. _____. ___\. _
- 1노드의 DNS 호스트 이름 ______
- 노드 1의 IP 주소 ____. \\. \\. _
- 서브넷 마스크_____. _____. ___\. _
- 기본 게이트웨이 ___. _____. ___\. _
- DNS 서버 1_____. ___\. \\. __
- DNS 서버 2_____. ___\. \\. __

- DNS 검색 도메인 ___
- 노드 2의 DNS 호스트 이름(선택 사항) _____
- 노드 2의 IP 주소(선택 사항)____. \\. \\. __
- 노드 3의 DNS 호스트 이름(선택 사항) _____
- 노드 3의 IP 주소(선택 사항)____. \\. \\. __
- 위의 모든 IP 주소에 대한 DNS 레코드를 만듭니다.

3 네트워크 방화벽 구성

- 네트워크 방화벽에서 위의 IP 주소에 필요한 포트를 엽니다. 최신 업데이트는 을 "포트 요구 사항" 참조하십시오.

4 바로 스토리지죠

- 공유 스토리지 디바이스의 데이터 저장소가 필요합니다. 또는 VAAI를 사용하여 템플릿을 빠르게 복제할 수 있도록 노드 1과 동일한 데이터 저장소에 있는 컨텐츠 라이브러리를 사용할 수 있습니다.
- 컨텐츠 라이브러리(HA에만 필요) _____
- 노드 1 데이터 저장소 ____
- 노드 2 데이터 저장소(선택 사항이지만 HA의 경우 권장됨) ________
- 노드 3 데이터 저장소(선택 사항이지만 HA의 경우 권장됨) ___

5 **OVA**를 배포합니다

- 이 단계를 완료하는 데 최대 45분이 소요될 수 있습니다
- "OVA를 배포합니다" vSphere Client 사용
- OVA 배포의 3단계에서 "이 가상 시스템의 하드웨어 사용자 지정" 옵션을 선택하고 10단계에서 다음을 설정합니다.
- "CPU 핫 추가 활성화"
- "메모리 핫 플러그"

6 **ONTAP** 툴에 **vCenter** 추가

- "vCenter Server 인스턴스를 추가합니다" ONTAP 도구 관리자

7 **ONTAP** 툴에 스토리지 백엔드를 추가합니다

- "ONTAP 사용자 역할 및 권한을 구성합니다" admin을 사용하지 않는 경우 포함된 JSON 파일 사용
- vCenter에서 ONTAP 클러스터 자격 증명을 사용하는 대신 스토리지 멀티테넌시를 사용하여 vCenter에 특정 SVM을 할당하려는 경우 다음 단계를 따르세요.
- "온보드 클러스터" ONTAP Tools Manager에서 vCenter에 연결합니다.
- "온보드 SVM" ONTAP 툴 vCenter UI

- vCenter 내에서 멀티테넌트 SVM을 사용하지 않는 경우:
- "온보드 클러스터" ONTAP 툴에 직접 있음 vCenter UI 또는 이 경우 VVOL을 활용하지 않을 때 SVM을 직접 추가할 수 있습니다.

8 어플라이언스 서비스 구성(선택 사항)

- VVOL을 사용하려면 먼저 해야 "어플라이언스 설정을 편집하고 VASA 서비스를 설정합니다" 합니다. 동시에 다음 두 항목을 검토합니다.
- 프로덕션 환경에서 VVol을 사용할 계획이라면 "고가용성 지원" 위의 두 개의 선택적 IP 주소를 사용하십시오.
- VMware 사이트 복구 관리자 또는 라이브 사이트 복구용 ONTAP 툴 SRA(스토리지 복제 어댑터)를 사용하려는 경우 "SRA 서비스를 활성화합니다"

9 인증서(옵션)

- VMware에서는 여러 vCenter에서 VVol을 사용하는 경우 CA 서명 인증서가 필요합니다.
- VASA 서비스_____
- 관리 서비스_____

10 기타 배포 후 작업

- HA 구축 환경에서 VM에 대한 반유사성 규칙을 생성합니다.
- HA를 사용하는 경우 Storage vMotion 노드 2와 3을 서로 다른 데이터 저장소로 사용합니다(선택 사항이지만 권장).
- "인증서 관리를 사용합니다" ONTAP 도구 관리자에서 모든 필수 CA 서명 인증서를 설치합니다.
- 기존 데이터 저장소를 보호하기 위해 SRM/VLSR에 대해 SRA를 설정한 경우 "VMware Live Site Recovery 어플라이언스에 SRA를 구성합니다"
- 네이티브 백업을 구성합니다. "제로급 RPO".
- 다른 저장 매체에 대한 정기 백업을 구성합니다.

ONTAP에서 VVOL 사용

NetApp와 함께 VVOL을 사용하려면 먼저 VMware vSphere용 ONTAP 툴이 있습니다. 이 툴은 NetApp의 ONTAP 9 시스템을 위한 VASA(vSphere API for Storage Awareness) 공급자 인터페이스로 사용됩니다.

또한 ONTAP 툴에는 vCenter UI 확장, REST API 서비스, VMware Site Recovery Manager/Live Site Recovery용 스토리지 복제 어댑터, 모니터링 및 호스트 구성 툴, VMware 환경을 보다 효율적으로 관리하는 데 도움이 되는 보고서 모음이 포함되어 있습니다.

제품 및 문서

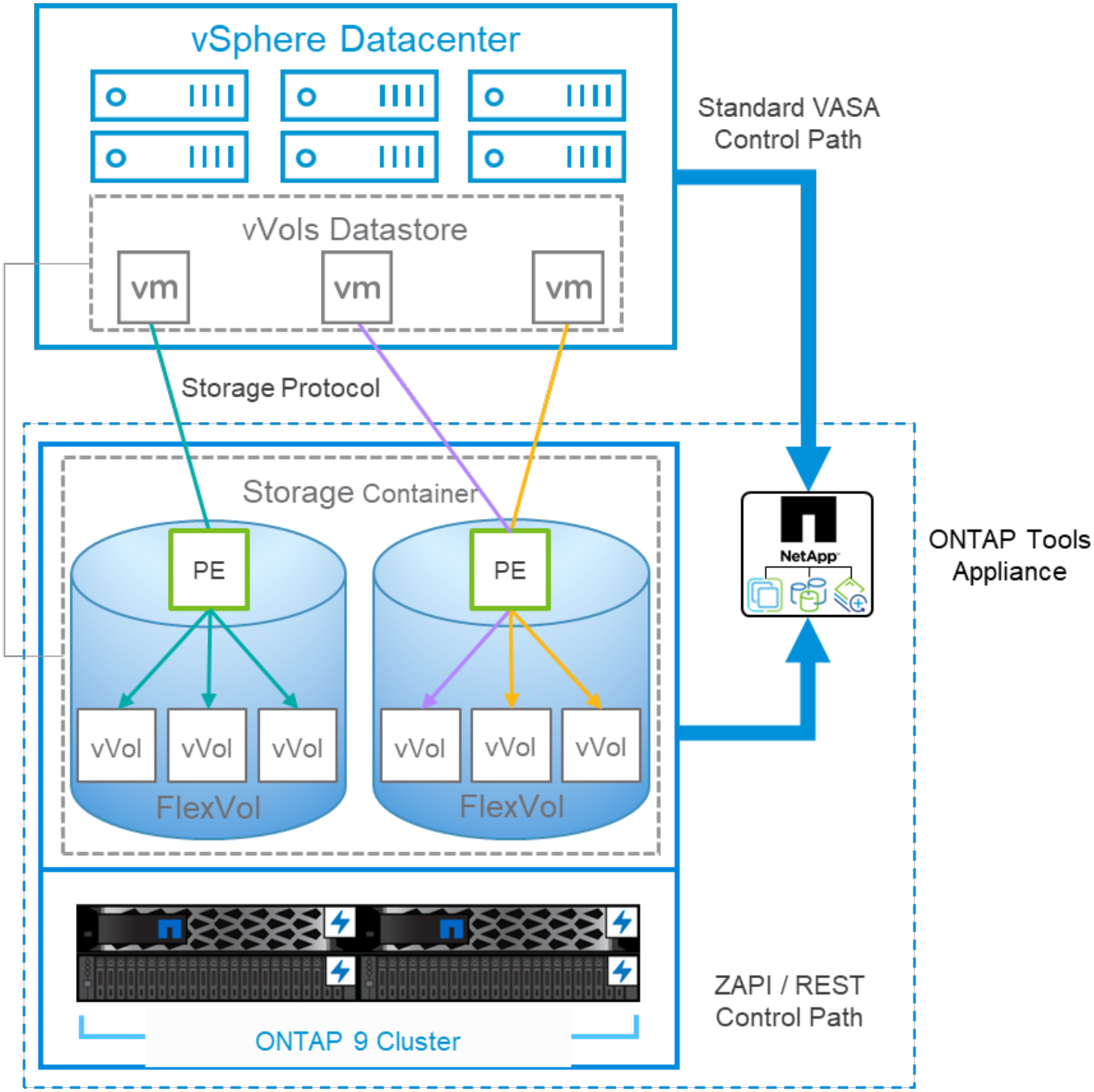
ONTAP One 라이센스에는 ONTAP 시스템에서 VVOL을 사용하는 데 필요한 모든 라이센스가 포함되어 있습니다. VASA 공급자 역할을 하는 무료 ONTAP 툴 OVA가 추가로 필요합니다. VVOL 환경에서 VASA Provider 소프트웨어는 어레이 기능을 정책 기반 특성으로 변환하며, VASA API를 통해 활용될 수 있습니다. 따라서 vSphere 관리자가 기능이

백그라운드에서 어떻게 관리되는지 알 필요가 없습니다. 따라서 정책에 따라 할당된 스토리지 용량을 동적으로 사용할 수 있으므로 기존 데이터 저장소를 수동으로 생성하고 개별 스토리지 사용율을 관리할 필요가 없습니다. 간단히 말해, VVOL은 엔터프라이즈 스토리지 관리에 수반되는 복잡성을 모두 해소하고 vSphere 관리자에서 추상화하므로 가상화 레이어에 집중할 수 있습니다.

VMware Cloud Foundation과 vSAN을 사용하는 고객의 경우 모든 관리 또는 워크로드 도메인에 VVOL을 보조 스토리지로 추가할 수 있습니다. VVOL은 공통 스토리지 정책 기반 관리 프레임워크를 통해 vSAN과 원활하게 통합됩니다.

차세대 ONTAP 툴 10 릴리스 제품군은 ESXi의 간단한 OVA 형식 어플라이언스를 통해 배포 가능한 확장 가능하고 컨테이너화된 마이크로서비스 기반 아키텍처로 이전 기능을 현대화합니다. ONTAP 도구 10 은 세 가지 이전 어플라이언스 및 제품의 모든 기능을 한 번의 구축으로 결합합니다. VVOL 관리를 위해 직관적인 vCenter UI 확장 또는 ONTAP 툴용 REST API를 VASA Provider를 사용합니다. SRA 구성 요소는 기존 데이터 저장소용입니다. VMware Site Recovery Manager는 VVol에 SRA를 사용하지 않습니다.

ONTAP 툴**:** 통합 시스템에서 **iSCSI** 또는 **FCP**를 사용하는 경우 **VASA Provider** 아키텍처를 사용합니다



제품 설치

새로 설치하려면 가상 어플라이언스를 vSphere 환경에 구축하십시오. 배포되면 관리자 UI에 로그인하거나 REST API를 사용하여 배포, 온보드 vCenter(vCenter에 플러그인 등록), 온보드 스토리지 시스템 및 vCenter에 스토리지 시스템을 연결하여 확장 또는 축소할 수 있습니다. ONTAP Tools Manager UI에서 스토리지 시스템을 온보딩, 그리고 클러스터와 vCenter를 연결하는 것은 전용 SVM과 함께 보안 멀티테넌시를 사용하려는 경우에만 필요합니다. 그렇지 않을 경우 ONTAP 툴 vCenter UI 확장에서 또는 REST API를 사용하여 원하는 스토리지 클러스터를 온보드하면 됩니다.

이 문서의 또는 "VMware vSphere용 ONTAP 툴 설명서" 을 "VVOL 스토리지 구축"참조하십시오.

Best Practice는 상호 의존성 충돌을 방지하기 위해 ONTAP 툴과 vCenter 어플라이언스를 기존 NFS 또는 VMFS 데이터 저장소에 저장하는 것입니다. VVol 작업 중에는 vCenter와 ONTAP 툴이 모두 서로 통신해야 하므로 ONTAP 툴 어플라이언스나 VCSA(vCenter Server 어플라이언스)를 관리하고 있는 VVol 스토리지로 설치하거나 이동하지 마십시오. 이 경우 vCenter 또는 ONTAP 툴 어플라이언스를 재부팅하면 제어 플레인 액세스가 중단되고 어플라이언스를 부팅하지 못할 수 있습니다.

ONTAP 도구의 전체 업그레이드는 NetApp 지원 사이트(로그인 필요)에서 다운로드할 수 있는 업그레이드 ISO 파일을 사용하여 "VMware vSphere 10용 ONTAP 툴 - 다운로드" 지원됩니다. 가이드 지침에 따라 "VMware vSphere 10.x용 ONTAP 툴을 10.3로 업그레이드하십시오" 어플라이언스를 업그레이드합니다. ONTAP 도구 9.13에서 10.3으로 나란히 업그레이드할 수도 있습니다. 해당 주제에 대한 자세한 내용은 을 "VMware vSphere 9.x용 ONTAP 툴에서 10.3로 마이그레이션합니다" 참조하십시오.

가상 어플라이언스 사이징 및 구성 제한에 대한 자세한 내용은 을 참조하십시오 "VMware vSphere용 ONTAP 툴을 구축하기 위한 구성 제한"

제품 설명서

다음 문서는 ONTAP 도구를 배포하는 데 도움이 됩니다.

"VMware vSphere용 ONTAP 툴 설명서"

시작하십시오

- "릴리스 정보"
- "VMware vSphere용 ONTAP 툴 개요"
- "ONTAP 툴 구축"
- "ONTAP 툴을 업그레이드합니다"

ONTAP 도구를 사용합니다

- "데이터 저장소를 프로비저닝합니다"
- "역할 기반 액세스 제어를 구성합니다"
- "고가용성을 구성합니다"
- "ESXi 호스트 설정을 수정합니다"

데이터 저장소 보호 및 관리

- "ONTAP 툴 및 SnapMirror 액티브 동기화를 사용하여 vMSC(vSphere Metro Storage Cluster)를 구성합니다"
- "가상 시스템 보호" SRM을 사용합니다
- "클러스터, 데이터 저장소 및 가상 머신 모니터링"

VASA 공급자 대시보드

VASA Provider에는 개별 VVol VM에 대한 성능 및 용량 정보가 포함된 대시보드가 포함되어 있습니다. 이 정보는 지연 시간, IOPS, 처리량 등을 비롯하여 VVOL 파일과 LUN에 대한 ONTAP에서 직접 제공됩니다. 이 기능은 현재 지원되는 모든 ONTAP 9 버전을 사용할 때 기본적으로 사용됩니다. 초기 구성 후 데이터가 대시보드를 채우는 데 최대 30분이 소요될 수 있습니다.

기타 모범 사례

vSphere에서 ONTAP VVOL을 사용하는 것은 간단하며 게시된 vSphere 방법을 따릅니다(사용 중인 ESXi 버전에 대한 VMware 설명서의 vSphere 스토리지 아래에서 가상 볼륨 작업 참조). 다음은 ONTAP와 관련하여 고려해야 할 몇 가지 추가 사례입니다.

- 제한 *

일반적으로 ONTAP는 VMware에 정의된 VVol 제한을 지원합니다(게시된 참조 "최대 구성"). LUN, 네임스페이스 및 파일의 수와 크기에 대한 업데이트된 제한은 항상 에서 "NetApp Hardware Universe를 참조하십시오" 확인하십시오.

- VMware vSphere의 UI 확장 또는 REST API용 ONTAP 툴을 사용하여 VVOL 데이터 저장소 * * 및 프로토콜 엔드포인트 프로비저닝 *

일반 vSphere 인터페이스를 통해 VVOL 데이터 저장소를 생성할 수도 있지만, ONTAP 툴을 사용하면 필요에 따라 프로토콜 엔드포인트를 자동으로 생성하고 ONTAP 모범 사례를 사용하여 FlexVol 볼륨(ASA R2에서는 필요하지 않음)을 생성할 수 있습니다. 호스트/클러스터/데이터 센터를 마우스 오른쪽 버튼으로 클릭한 다음 _ONTAP tools_and_provision datastore_를 선택합니다. 마법사에서 원하는 VVOL 옵션을 선택하기만 하면 됩니다.

- ONTAP 툴 어플라이언스 또는 VCSA(vCenter Server Appliance)를 관리하는 VVol 데이터 저장소에 저장하지 마십시오. *

이 경우 어플라이언스를 재부팅해야 하는 경우 "닭고기와 달걀"이 발생할 수 있습니다. 재부팅하는 동안 자신의 VVol을 다시 찾을 수 없기 때문입니다. 다른 ONTAP 툴과 vCenter 구축을 통해 관리되는 VVol 데이터 저장소에 저장할 수 있습니다.

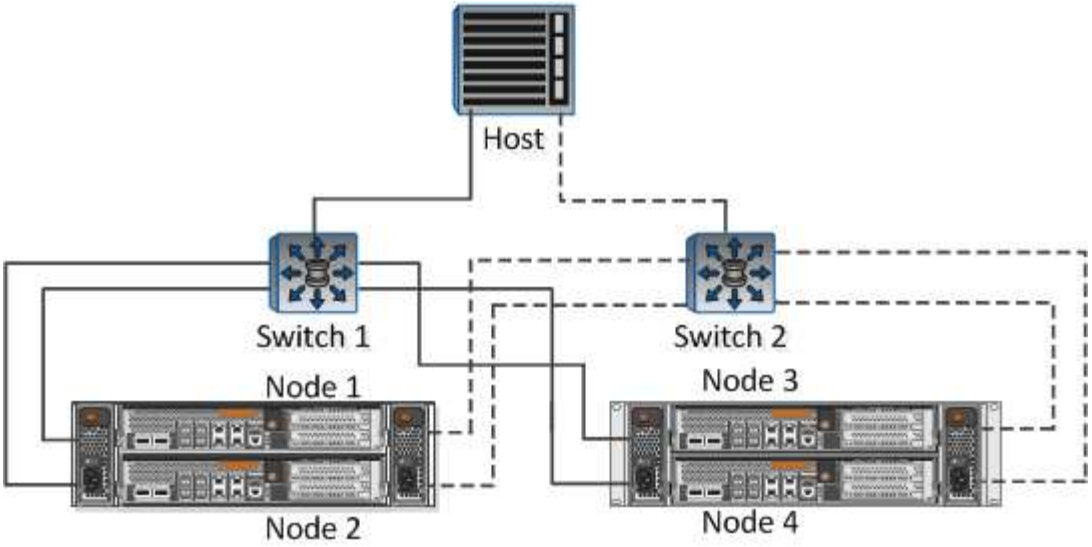
- 다양한 ONTAP 릴리즈에서 VVOL을 운영하는 것을 방지합니다. *

VASA Provider의 다양한 릴리즈에서 QoS, 특성 등과 같은 지원되는 스토리지 기능이 변경되었으며, 일부는 ONTAP 릴리즈에 따라 달라집니다. ONTAP 클러스터에서 다른 릴리즈를 사용하거나 서로 다른 릴리즈를 가진 클러스터 간에 VVOL을 이동하면 예기치 않은 동작 또는 규정 준수 경보가 발생할 수 있습니다.

- VVOL에 FCP를 사용하기 전에 파이버 채널 패브릭을 존재해 주십시오. *

ONTAP 툴 VASA Provider는 관리되는 ESXi 호스트의 검색된 이니시에이터를 기반으로 ONTAP에서 FCP 및 iSCSI igroup과 NVMe 서브시스템을 관리합니다. 그러나 조닝을 관리하기 위해 파이버 채널 스위치와 통합되지 않습니다. 조닝은 Best Practice에 따라 수행해야 프로비저닝이 수행될 수 있습니다. 다음은 4개의 ONTAP 시스템에 대한 단일 이니시에이터 조닝의 예입니다.

단일 이니시에이터 조닝:



자세한 모범 사례는 다음 문서를 참조하십시오.

"_TR-4080 최신 SAN ONTAP 9_에 대한 모범 사례"

"_TR-4684 NVMe-oF_로 최신 SAN 구현 및 구성"

- 필요에 따라 FlexVol 볼륨을 지원할 계획을 세우십시오. *

비 ASA R2 시스템의 경우 여러 백업 볼륨을 VVol 데이터 저장소에 추가하여 ONTAP 클러스터 전체에 워크로드를 분산하거나, 다른 정책 옵션을 지원하거나, 허용된 LUN 또는 파일 수를 늘리는 것이 좋습니다. 하지만 최대 스토리지 효율성이 필요한 경우에는 모든 백업 볼륨을 단일 Aggregate에 배치하십시오. 또는 최대 클론 복제 성능이 필요한 경우 단일 FlexVol 볼륨을 사용하고 템플릿 또는 콘텐츠 라이브러리를 동일한 볼륨에 유지하는 것을 고려해 보십시오. VASA Provider는 마이그레이션, 클론 생성 및 스냅샷을 비롯한 다양한 VVOL 스토리지 작업을 ONTAP로 오프로드합니다. 단일 FlexVol 볼륨 내에서 이 작업을 수행할 경우 공간 효율적인 파일 클론이 사용되며 거의 즉시 사용할 수 있습니다. FlexVol 볼륨 전체에 걸쳐 복사본을 빠르게 생성하여 인라인 중복제거 및 압축을 사용할 수 있지만, 백그라운드 작업이 백그라운드 중복제거 및 압축을 사용하는 볼륨에서 실행될 때까지 최대 스토리지 효율성이 복구되지 않을 수 있습니다. 소스 및 타겟에 따라 일부 효율성이 저하될 수 있습니다.

ASA R2 시스템에서는 볼륨 또는 애그리게이트의 개념이 사용자로부터 추상화됨에 따라 이러한 복잡성이 제거됩니다. 동적 배치가 자동으로 처리되고 프로토콜 엔드포인트가 필요에 따라 생성됩니다. 추가 스케일이 필요한 경우 추가 프로토콜 엔드포인트를 즉시 자동으로 생성할 수 있습니다.

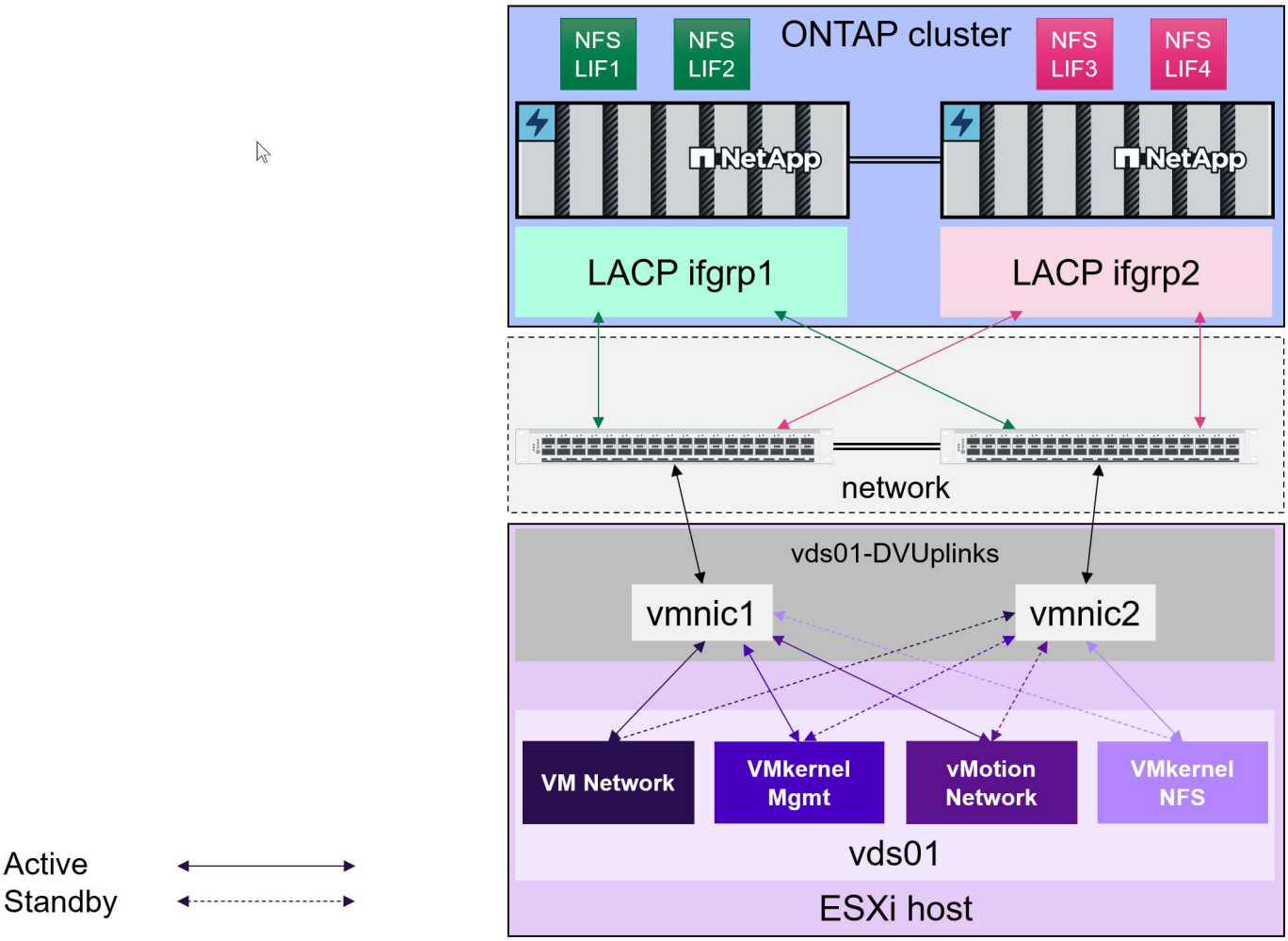
- 최대 IOPS를 사용하여 알 수 없는 VM을 제어하거나 VM을 테스트하는 것을 고려해 보십시오. *

VASA Provider 7.1에서 처음 사용할 수 있는 Max IOPS를 사용하면 알 수 없는 워크로드를 위해 IOPS를 특정 VVOL으로 제한하여 다른 중요한 워크로드에 미치는 영향을 방지할 수 있습니다. 성능 관리에 대한 자세한 내용은 표 4를 참조하십시오.

- 충분한 데이터 LIF가 있는지 확인하십시오. * 을 "VVOL 스토리지 구축"참조하십시오.
- 모든 프로토콜 모범 사례를 따르십시오. *

선택한 프로토콜에 관련된 NetApp 및 VMware의 기타 모범 사례 가이드를 참조하십시오. 일반적으로 이미 언급한 것 이외의 다른 변경 사항은 없습니다.

- NFS v3을 통한 VVol을 사용한 네트워크 구성의 예 *



AFF, ASA, ASA R2 및 FAS 시스템에 VVOL을 구축합니다

가상 시스템에 사용할 VVol 스토리지를 생성하는 모범 사례를 따르십시오.

VVOL 데이터 저장소를 프로비저닝하는 데는 몇 가지 단계가 필요합니다. NetApp의 ASA R2 시스템은 VMware 워크로드를 위해 설계되었으며 기존의 ONTAP 시스템과 다른 사용자 환경을 제공합니다. ASA R2 시스템을 사용할 경우 ONTAP 툴 버전 10.3 이상을 사용하면 새로운 스토리지 아키텍처에 최적화된 UI 확장 및 REST API 지원을 설정하고 포함하기 위한 단계를 줄일 수 있습니다.

ONTAP 툴을 사용하여 VVOL 데이터 저장소 생성 준비

이미 ONTAP 툴을 사용하여 기존 VMFS 또는 기존 NFS 기반 스토리지를 관리, 자동화 및 보고하는 경우 구축 프로세스의 처음 두 단계를 건너뛸 수 있습니다. ONTAP 도구 배포 및 구성에 대해서는 이 전체 내용을 참조할 수도 "체크리스트"있습니다.

1. 스토리지 가상 머신(SVM)과 해당 프로토콜 구성을 생성합니다. 참고로, ASA r2 시스템에는 일반적으로 데이터 서비스를 위한 단일 SVM이 이미 탑재되어 있으므로 이 과정이 필요하지 않을 수 있습니다. NVMe/FC(ONTAP 도구 9.13에서만 사용 가능), NFSv3, NFSv4.1, iSCSI, FCP 또는 이러한 옵션의 조합 중에서 선택할 수 있습니다. NVMe/TCP 및 NVMe/FC는 ONTAP 도구 10.3 이상 버전에서 기존 VMFS 데이터스토어에도 사용할 수 있습니다. ONTAP 시스템 관리자 마법사 또는 클러스터 셸 명령줄을 사용할 수 있습니다.
   - "SVM에 로컬 계층(애그리게이트)을 할당합니다" 모든 비 ASA R2 시스템의 경우.
   - 각 스위치/패브릭 연결마다 노드당 하나 이상의 LIF가 있어야 합니다. 모범 사례로서, FCP, iSCSI 또는 NVMe

기반 프로토콜에 대해 노드당 두 개 이상의 를 생성합니다. LIF는 NFS 기반 VVol에는 노드당 하나의 LIF로 충분하지만 이 LIF는 LACP ifgroup으로 보호해야 합니다. "LIF 개요 구성"자세한 내용은 및 "물리적 포트를 결합하여 인터페이스 그룹을 생성합니다" 을 참조하십시오.

- 테넌트 vCenter에 SVM 범위 자격 증명을 사용하려면 SVM당 최소 하나의 관리 LIF가 필요합니다.
- SnapMirror를 사용할 계획이라면 소스와 대상을 "ONTAP 클러스터 및 SVM이 피어링됩니다"확인하십시오.
- ASA r2 시스템이 아닌 경우 이 시점에 볼륨을 생성할 수 있지만, ONTAP 도구의 데이터스토어 프로비저닝 마법사를 사용하여 볼륨을 생성하는 것이 가장 좋습니다. 이 규칙의 유일한 예외는 VMware Site Recovery Manager 및 ONTAP 도구 9.13과 함께 vVols 복제를 사용하려는 경우입니다. 기존에 SnapMirror 관계가 설정된 FlexVol 볼륨을 사용하면 설정이 더 간편합니다. vVols 에 사용할 볼륨에는 QoS를 활성화하지 않도록 주의하십시오. QoS는 SPBM 및 ONTAP 도구에서 관리하도록 되어 있습니다.

2. "VMware vSphere용 ONTAP 툴을 구축합니다" NetApp 지원 사이트에서 다운로드한 OVA 사용
   - ONTAP Tools 10.0 이상 버전은 어플라이언스당 여러 vCenter 서버를 지원하므로 더 이상 vCenter마다 ONTAP Tools 어플라이언스를 하나씩 배포할 필요가 없습니다.
     - 여러 vCenter를 단일 ONTAP 도구 인스턴스에 연결하려면 CA에서 서명한 인증서를 생성하고 설치해야 합니다. 참조하다 "인증서를 관리합니다" 단계별로.
   - 10.3 버전부터 ONTAP 도구는 대부분의 vVols 이외의 워크로드에 적합한 단일 노드 소형 어플라이언스로 배포됩니다.

- 권장되는 최적의 방법은 다음과 같습니다. "스케일아웃 ONTAP 툴" 10.3 버전 이상에서는 모든 프로덕션 워크로드에 대해 3노드 고가용성(HA) 구성을 지원합니다. 실험실이나 테스트 목적으로는 단일 노드 배포를 사용할 수 있습니다.
- 프로덕션 환경에서 vVols 사용할 때 권장되는 최적의 방법은 단일 장애 지점을 제거하는 것입니다. ONTAP 도구 VM이 동일한 호스트에서 함께 실행되는 것을 방지하기 위해 안티 어피니티 규칙을 생성합니다. 초기 배포 후에는 스토리지 vMotion을 사용하여 ONTAP 도구 VM을 다른 데이터스토어에 배치하는 것이 좋습니다. 더 자세히 알아보세요 "vSphere DRS 없이 선호도 규칙 사용" 또는 "VM-VM 선호도 규칙을 생성합니다". 또한 빈번한 백업 일정을 예약해야 합니다. "내장된 구성 백업 유틸리티를 사용합니다".

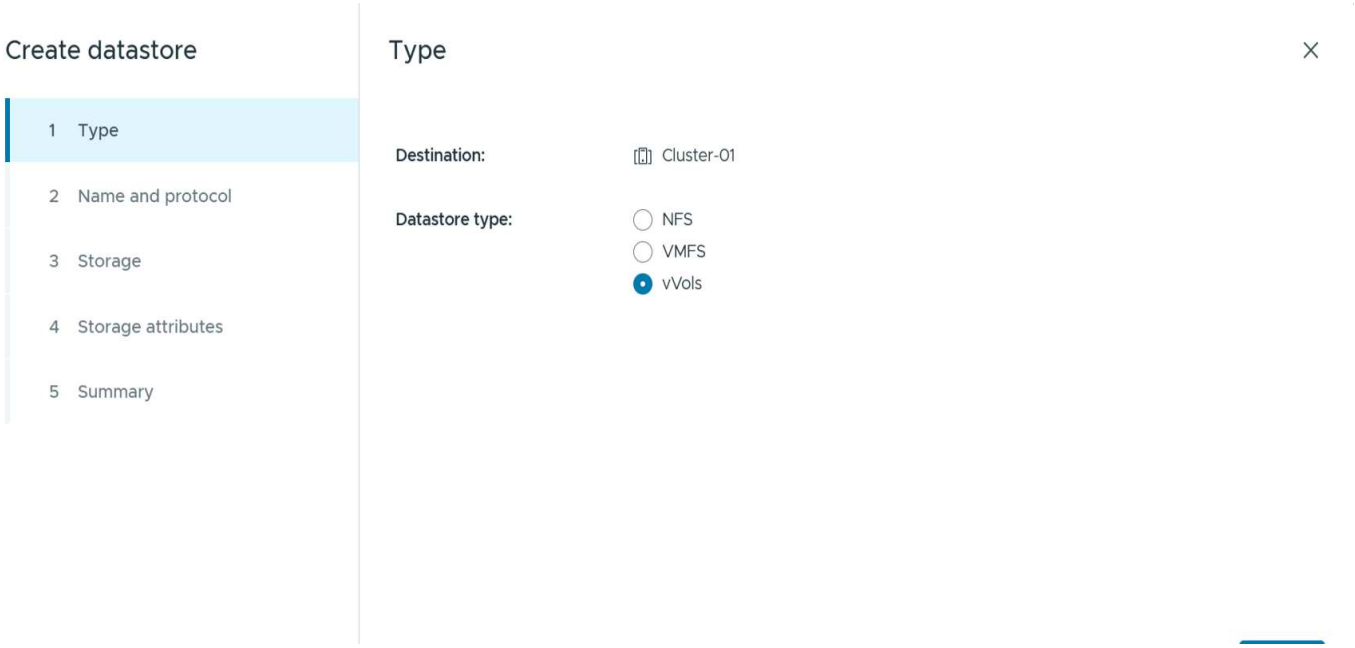
1. 사용자 환경에 맞게 ONTAP 도구 10.3 구성
   - "vCenter Server 인스턴스를 추가합니다" ONTAP 도구 관리자 UI에서
   - ONTAP 도구 10.3은 보안 멀티 테넌시를 지원합니다. 보안 멀티 테넌시가 필요하지 않은 경우 "ONTAP 클러스터를 추가합니다" vCenter에서 ONTAP tools 메뉴로 이동하여 _Storage backends_를 클릭하고 _add_버튼을 클릭하면 됩니다.
   - 특정 SVM(Storage Virtual Machine)을 특정 vCenter에 위임하려는 보안 멀티테넌트 환경에서 다음을 수행해야 합니다.
     - ONTAP tools manager UI에 로그인합니다
     - "스토리지 클러스터를 온보딩합니다"
     - "스토리지 백엔드를 vCenter Server 인스턴스에 연결합니다"
     - vCenter 관리자에게 특정 SVM 자격 증명을 제공하면, 관리자는 vCenter의 ONTAP 도구 스토리지 백엔드 메뉴에 해당 SVM을 스토리지 백엔드로 추가합니다.

- 스토리지 계정에 대한 RBAC 역할을 생성하는 것이 모범 사례입니다.
- ONTAP 도구에는 ONTAP 도구 스토리지 계정에 필요한 역할 권한이 포함된 JSON 파일이 있습니다. JSON 파일을 ONTAP 시스템 관리자에 업로드하면 RBAC 역할 및 사용자 생성을 간소화할 수 있습니다.
- ONTAP RBAC 역할에 대한 자세한 내용은 에서확인할 수 있습니다 "ONTAP 사용자 역할 및 권한을 구성합니다".

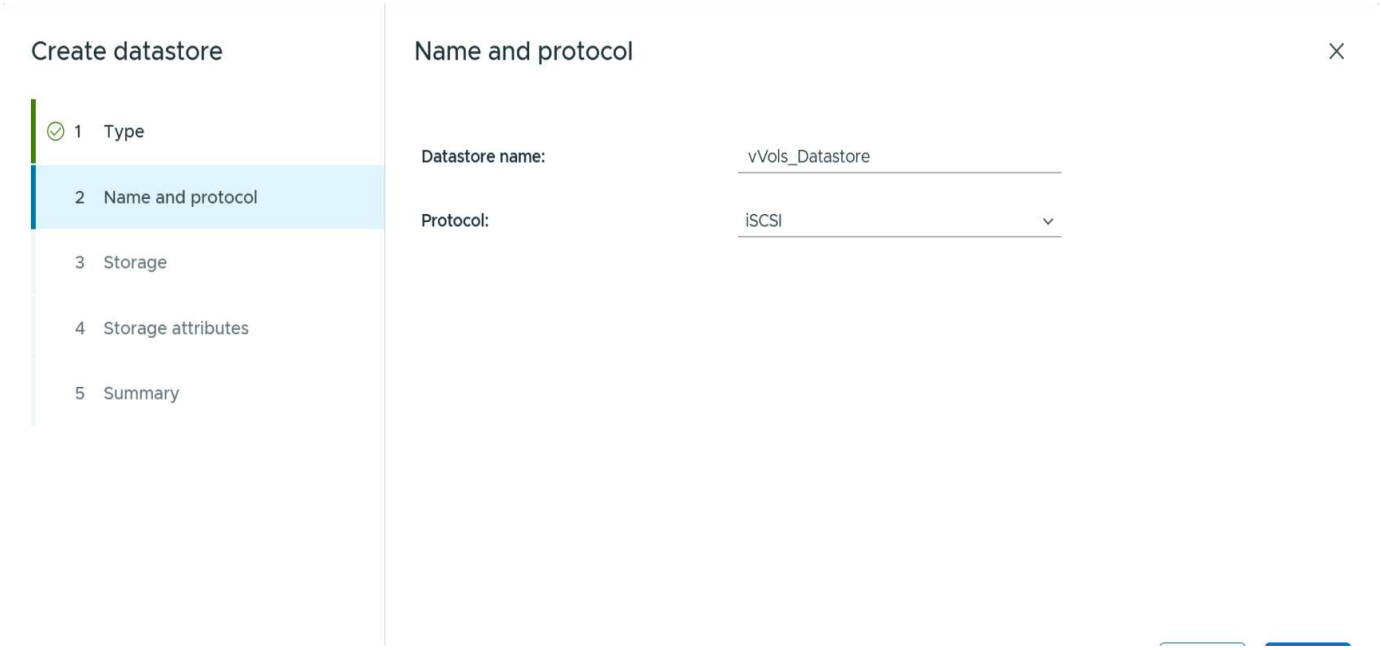
클러스터 전체를 ONTAP 도구 관리자 UI에 등록해야 하는 이유는 vVols 에 사용되는 많은 API가 클러스터 수준에서만 사용 가능하기 때문입니다.

ONTAP 툴을 사용하여 **VVOL** 데이터 저장소를 생성합니다

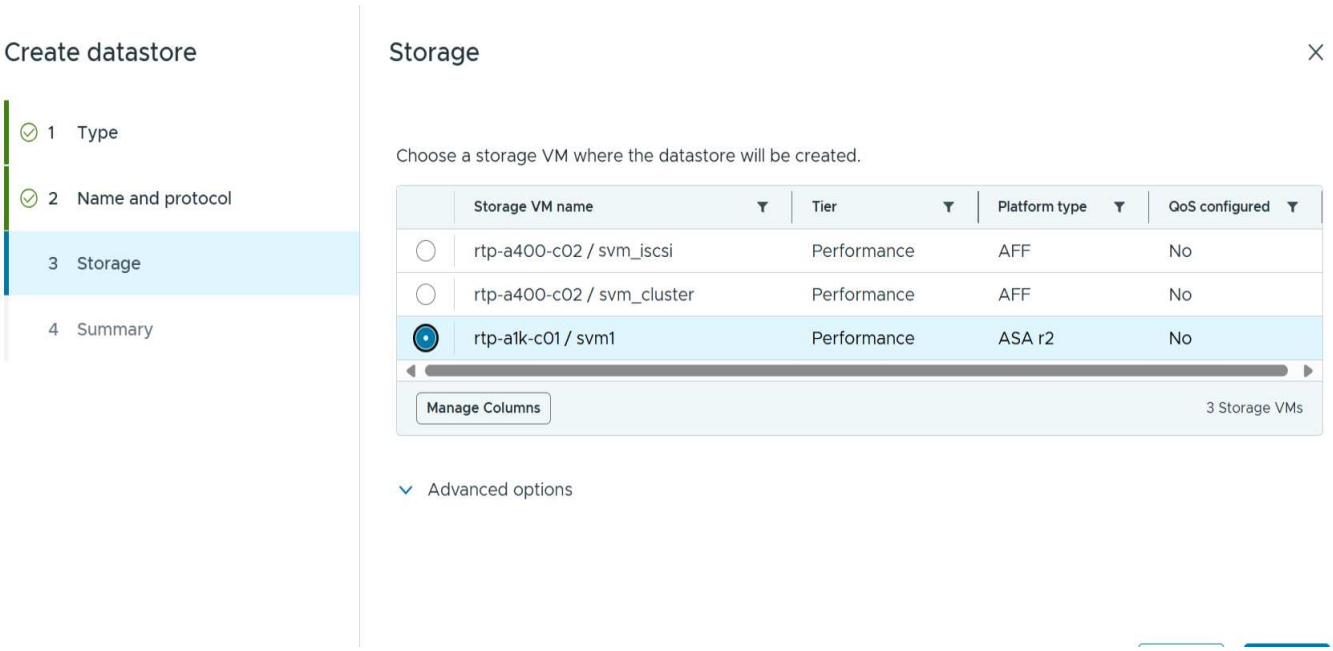
VVOL 데이터 저장소를 생성할 호스트, 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭한 다음 *ONTAP tools*>_Provision Datastore_를 선택합니다.



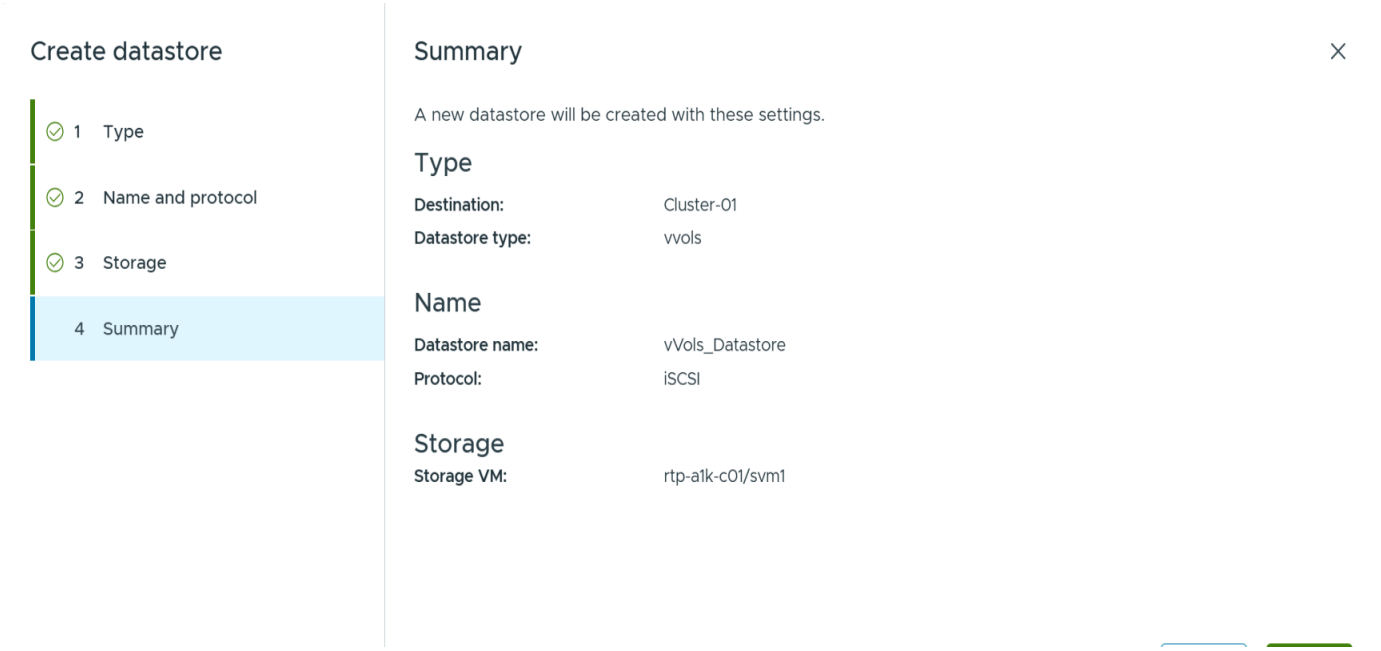
- VVol을 선택하고 의미 있는 이름을 입력한 다음 원하는 프로토콜을 선택합니다. 데이터 저장소에 대한 설명도 제공할 수 있습니다.
  - ONTAP 도구 10.3(ASA R2 포함).



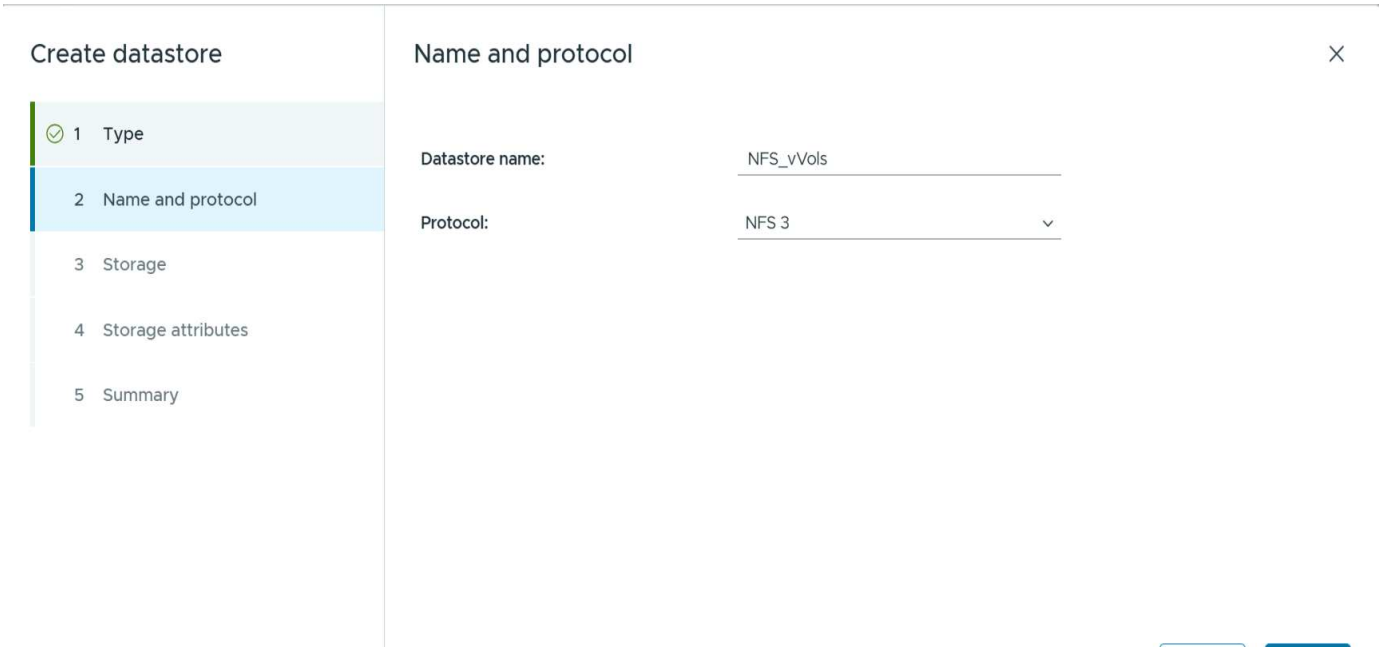
- ASA R2 시스템 SVM을 선택하고 _NEXT_를 클릭합니다.



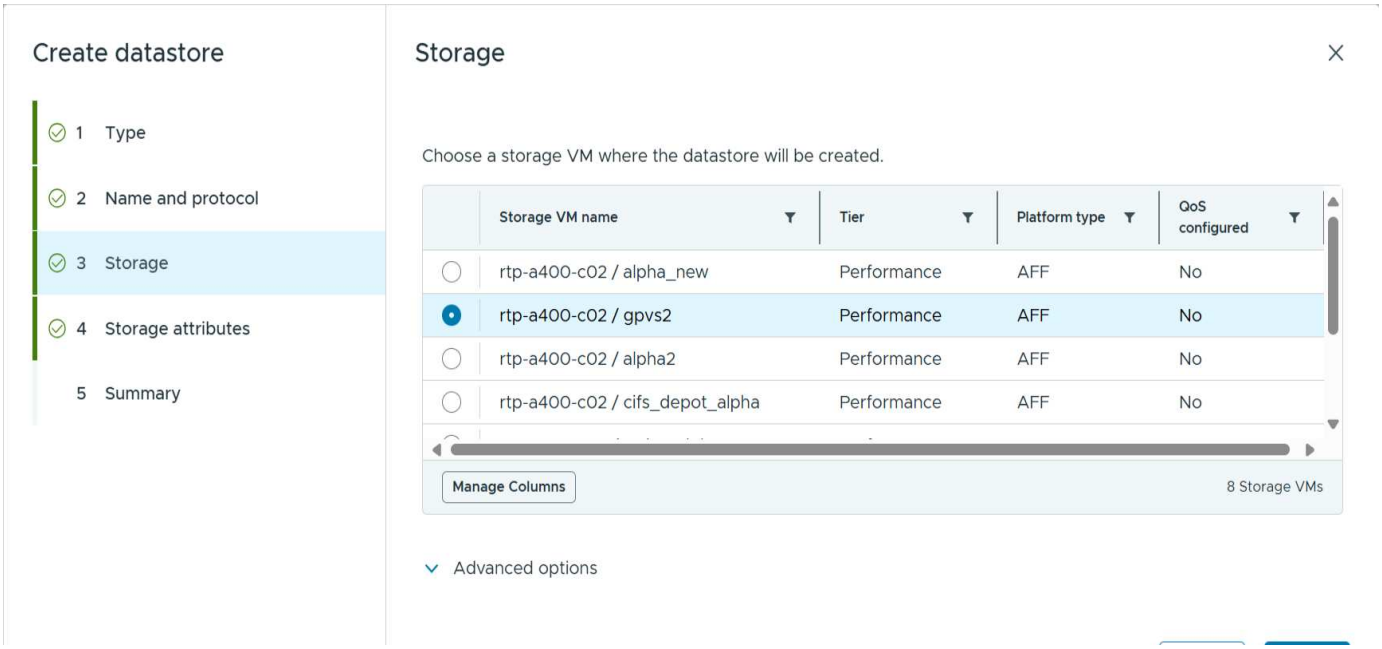
- 마침 을 클릭합니다



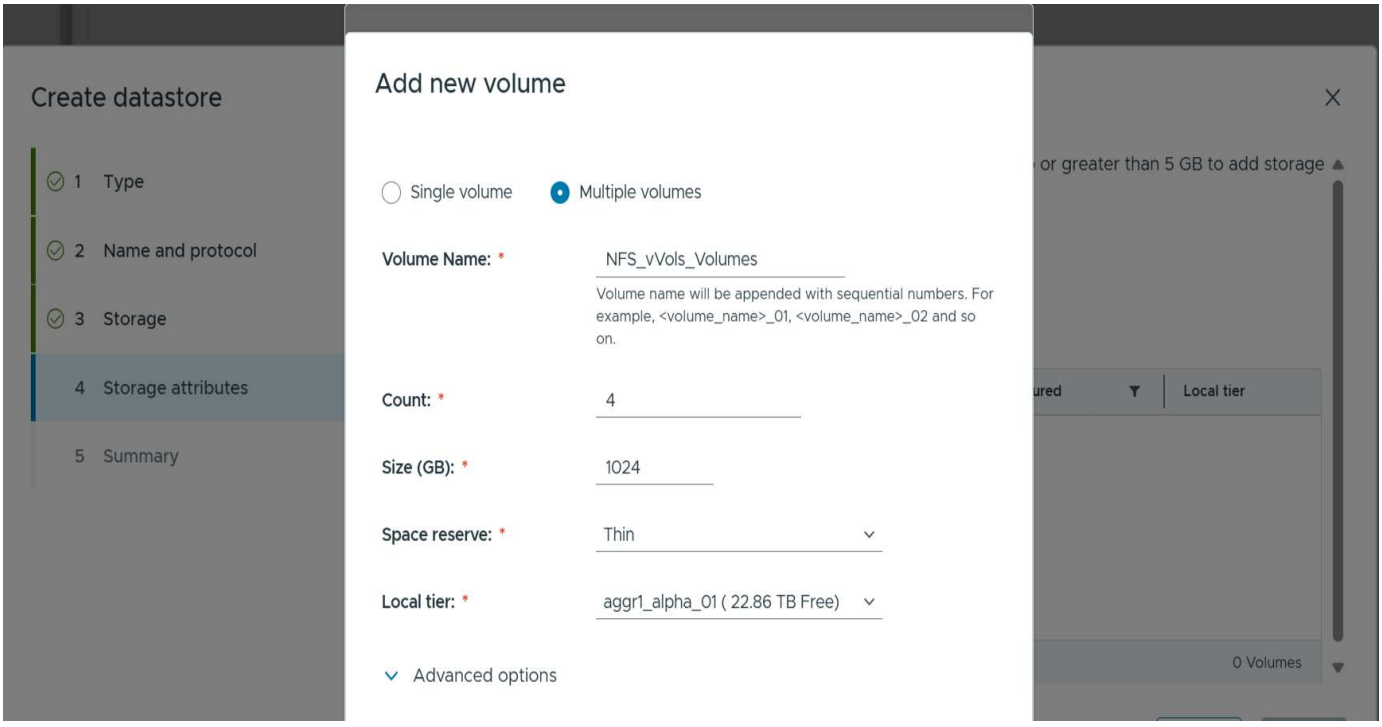
- 정말 간단합니다!
  - ONTAP 도구 10.3은 ONTAP FAS, AFF 및 ASA r2 이전 버전과 함께 사용할 ASA 있습니다.
- 프로토콜을 선택합니다

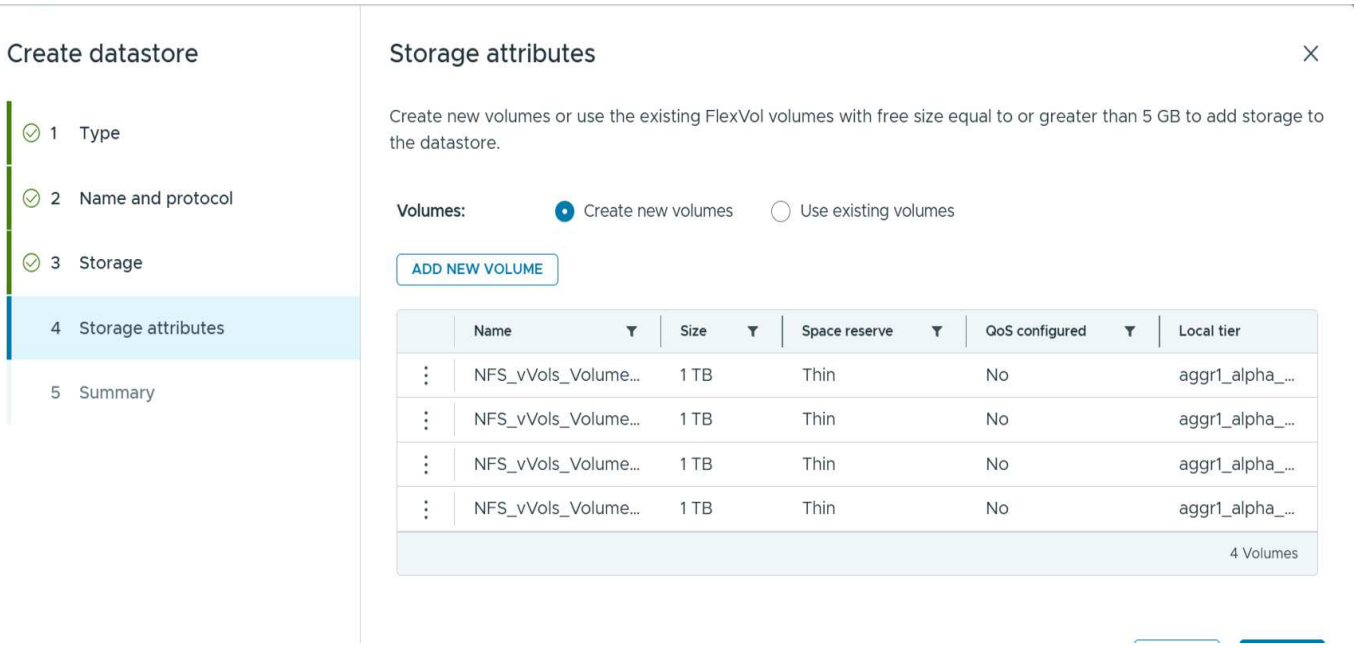


- SVM을 선택하고 _NEXT_를 클릭합니다.

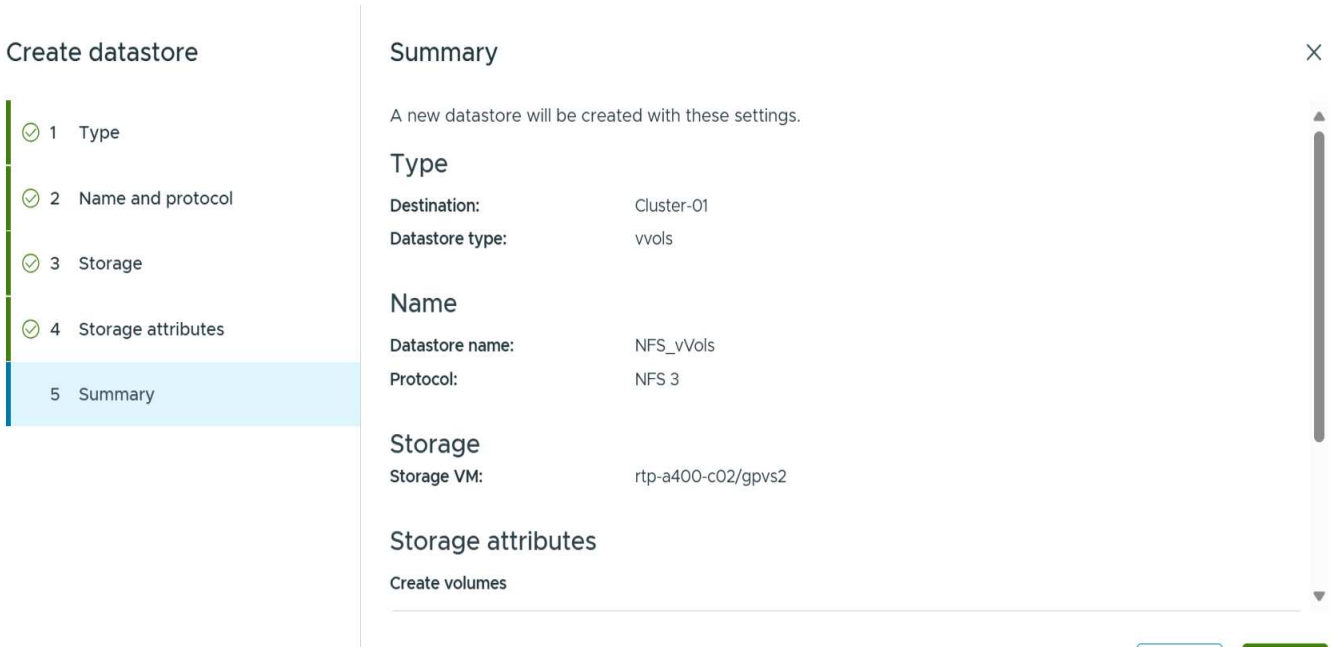


- '새 볼륨 추가' 또는 '기존 볼륨 사용'을 클릭하고 속성을 지정하세요. 참고로 ONTAP 도구 10.3에서는 여러 볼륨을 동시에 생성하도록 요청할 수 있습니다. ONTAP 클러스터 전체에 걸쳐 용량 균형을 맞추기 위해 여러 볼륨을 수동으로 추가할 수도 있습니다. _다음_을 클릭하세요

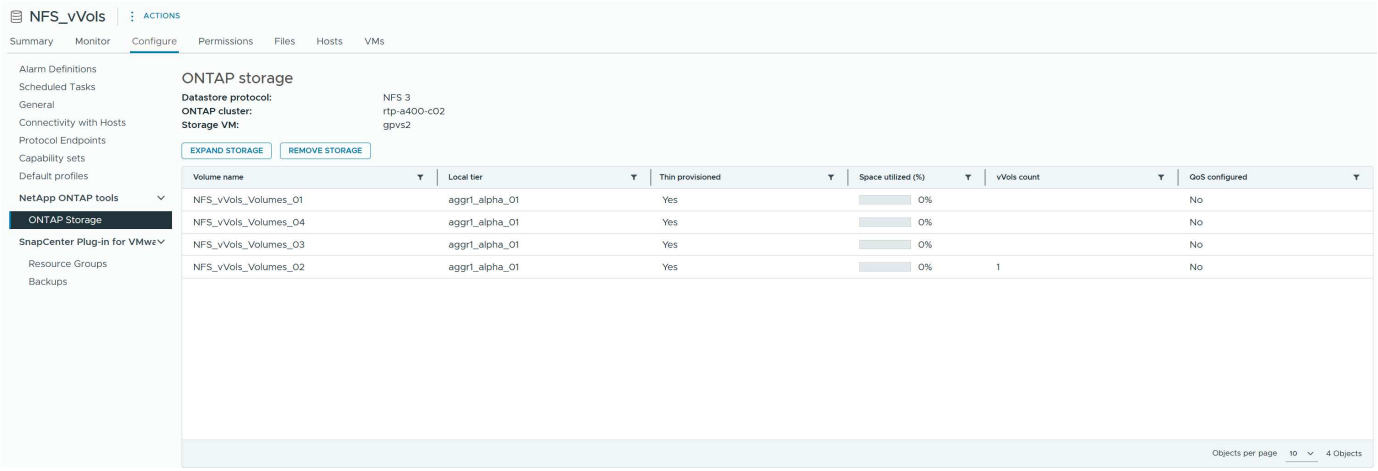




- 마침 을 클릭합니다



- 데이터 저장소에 대한 구성 탭의 ONTAP tools 메뉴에서 할당된 볼륨을 볼 수 있습니다.



- 이제 vCenter UI의 _Policies 및 Profiles_메뉴에서 VM 스토리지 정책을 생성할 수 있습니다.

기존 데이터 저장소에서 **VVOL**으로 **VM** 마이그레이션

기존 데이터 저장소에서 VVOL 데이터 저장소로 VM을 마이그레이션하는 작업은 기존 데이터 저장소 간에 VM을 이동하는 것처럼 간단합니다. VM을 선택한 다음 작업 목록에서 마이그레이션 을 선택하고 마이그레이션 유형 _change storage only_를 선택합니다. 메시지가 표시되면 VVol 데이터 저장소와 일치하는 VM 저장소 정책을 선택합니다. SAN VMFS에서 VVol로의 마이그레이션을 위해 vSphere 6.0 이상을 사용하여 마이그레이션 복사 작업을 오프로드할 수 있지만 NAS VMDK에서 VVol로 마이그레이션할 수는 없습니다.

정책을 사용하여 **VM** 관리

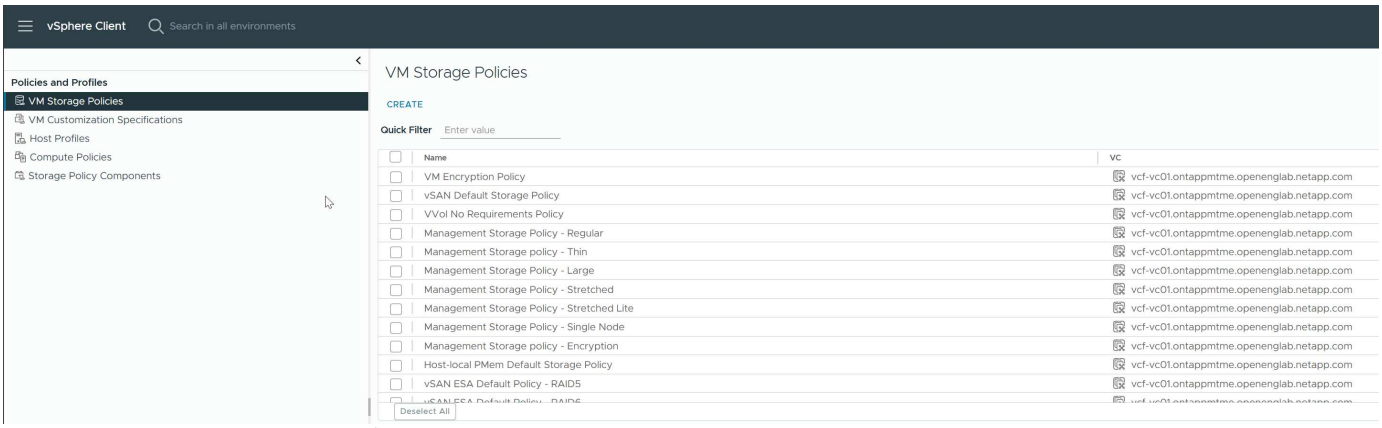
정책 기반 관리를 통해 스토리지 프로비저닝을 자동화하려면 원하는 스토리지 기능에 매핑되는 VM 스토리지 정책을 생성해야 합니다.

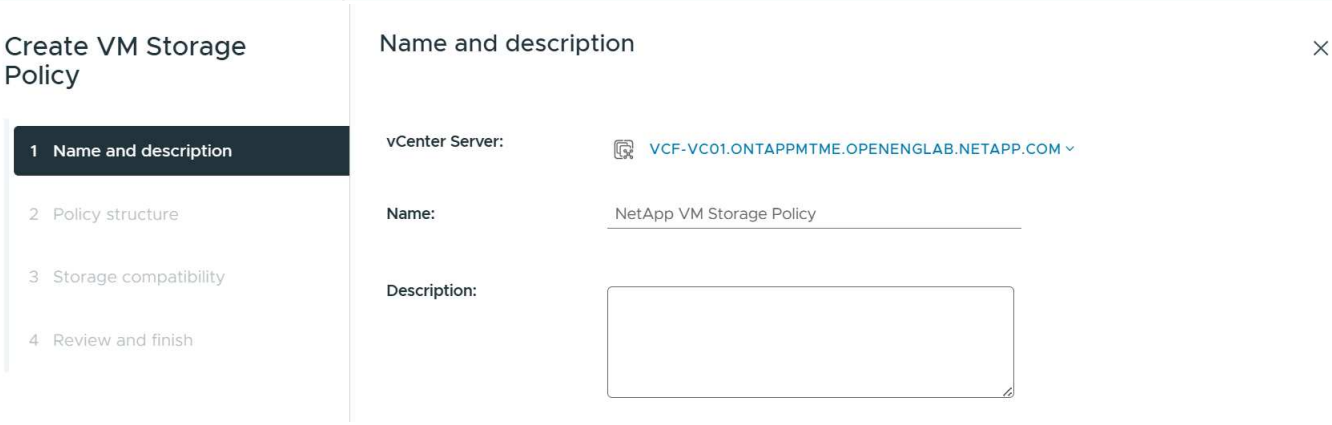
ONTAP 도구 10.0 이상에서는 더 이상 이전 버전과 같은 저장소 기능 프로파일을 사용하지 않습니다. 대신 스토리지 기능은 VM 스토리지 정책 자체에서 직접 정의됩니다.

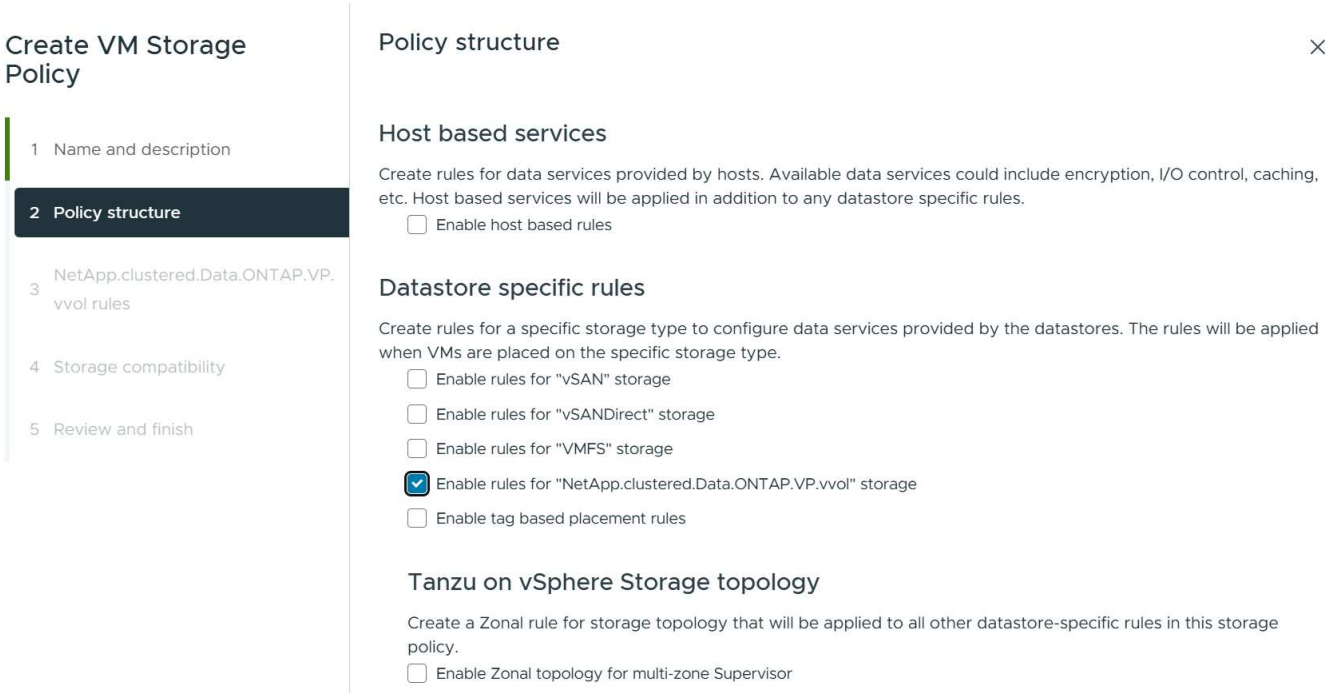
VM 스토리지 정책을 생성하는 중입니다

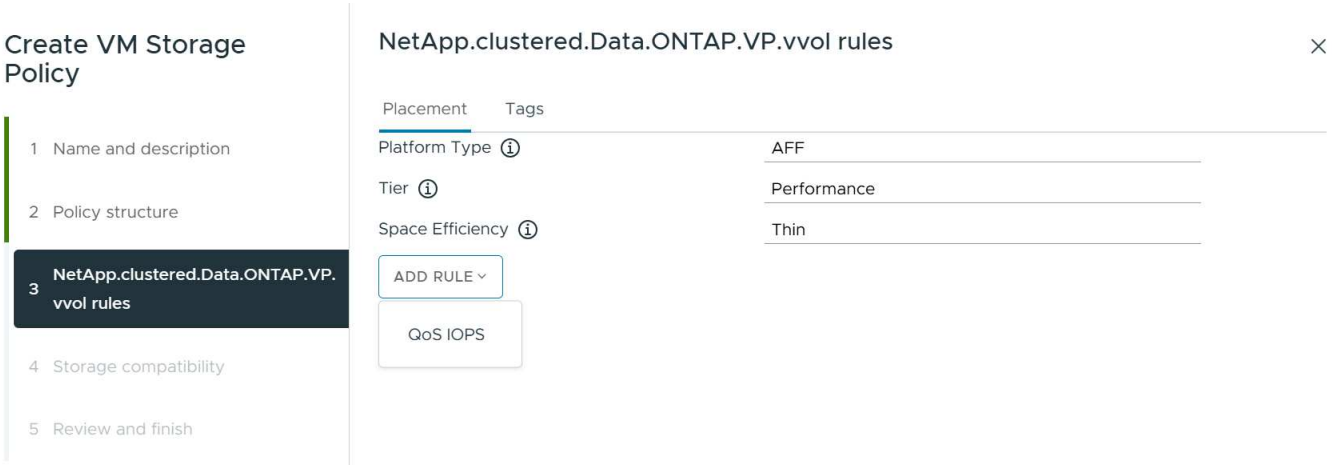
vSphere에서 VM 스토리지 정책은 스토리지 I/O 제어 또는 vSphere 암호화와 같은 선택적 기능을 관리하는 데 사용됩니다. 또한 vVols 과 함께 사용하여 VM에 특정 스토리지 기능을 적용하는 데에도 사용됩니다. "NetApp.clustered.Data. ONTAP .VP.vvol" 스토리지 유형을 사용하십시오. ONTAP 도구 VASA Provider를 사용한 예시는 다음 링크를 참조하세요: vmware-vvols-ontap.html#Best Practices[NFS v3를 통한 vVols 네트워크 구성 예시]. " NetApp.clustered.Data. ONTAP.VP.VASA10" 스토리지에 대한 규칙은 vVols 기반이 아닌 데이터스토어와 함께 사용해야 합니다.

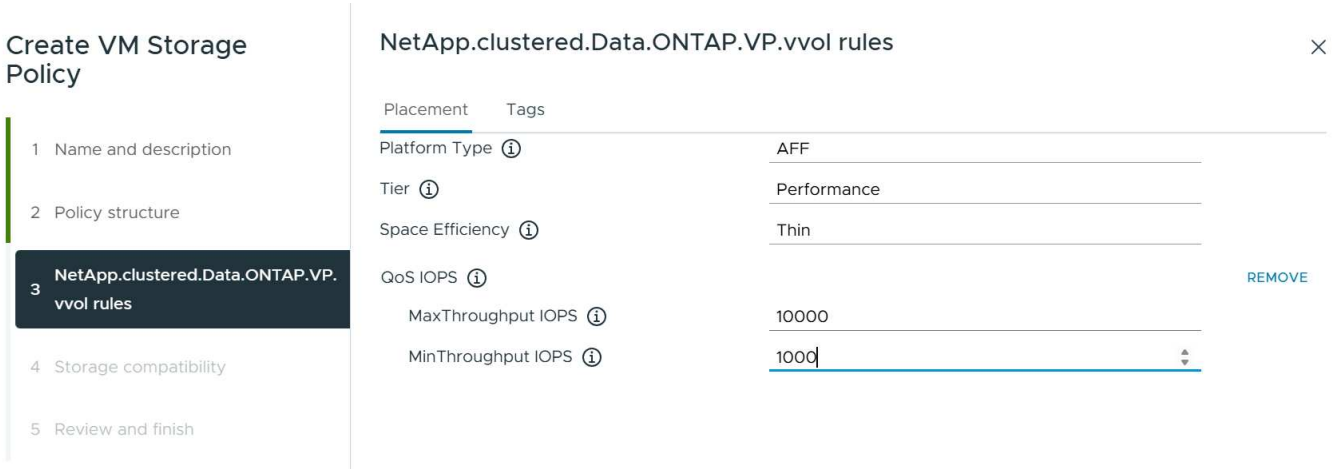
스토리지 정책이 생성되면 새 VM을 프로비저닝할 때 사용할 수 있습니다.

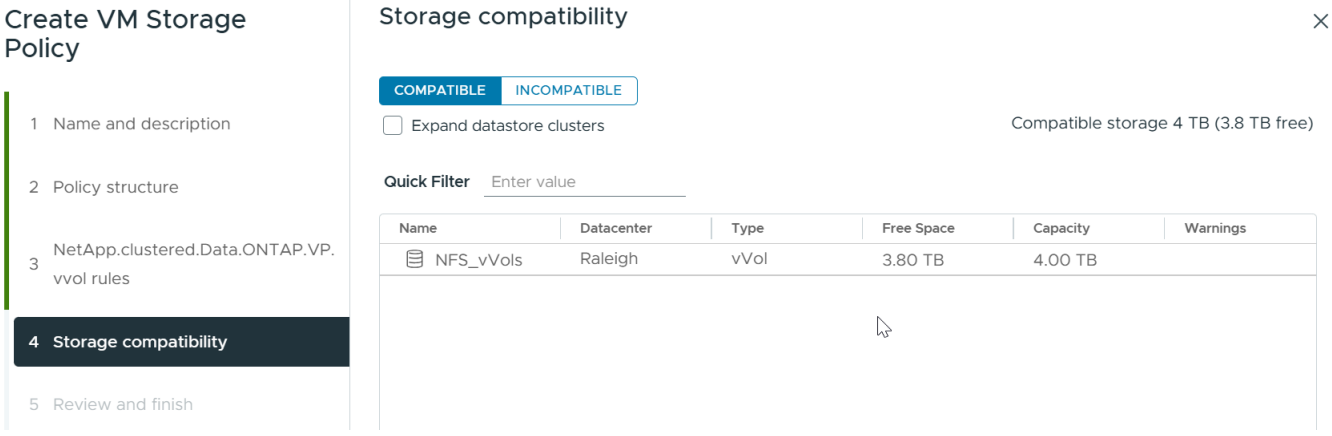

vSphere Client
Search in all environments
Policies and Profiles
VM Storage Policies
VM Customization Specifications
Host Profiles
Compute Policies
Storage Policy Components
VM Storage Policies
CREATE
Quick Filter
Enter value
Name
VC
VM Encryption Policy
vSAN Default Storage Policy
VVol No Requirements Policy
Management Storage Policy - Regular
Management Storage policy - Thin
Management Storage Policy - Large
Management Storage Policy - Stretched
Management Storage Policy - Stretched Lite
Management Storage Policy - Single Node
Management Storage policy - Encryption
Host-local PMem Default Storage Policy
vSAN ESA Default Policy - RAID5
vcf-vc01.ontappmtme.openenglab.netapp.com
Deselect All

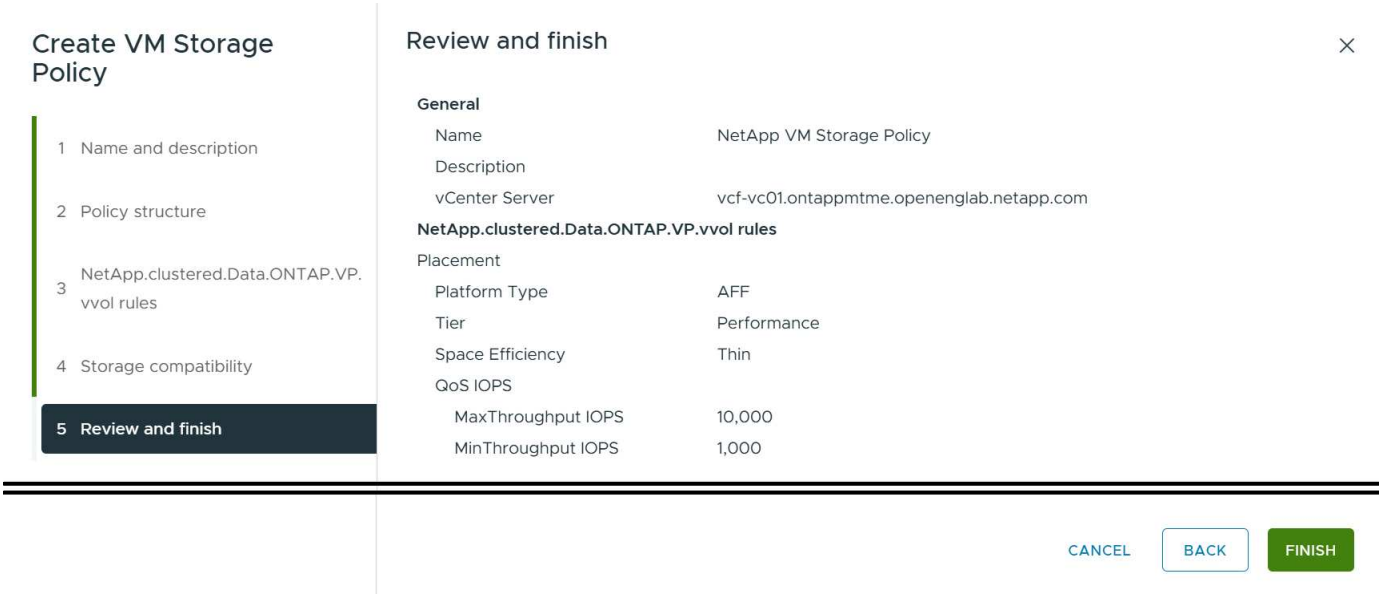

Create VM Storage Policy
1 Name and description
2 Policy structure
3 Storage compatibility
4 Review and finish
Name and description
vCenter Server:
VCF-VC01.ONTAPPMTME.OPENENGLAB.NETAPP.COM
Name:
NetApp VM Storage Policy
Description:


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Policy structure
Host based services
Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.
Enable host based rules
Datastore specific rules
Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.
Enable rules for "vSAN" storage
Enable rules for "vSANDirect" storage
Enable rules for "VMFS" storage
Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
Enable tag based placement rules
Tanzu on vSphere Storage topology
Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.
Enable Zonal topology for multi-zone Supervisor


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
ADD RULE
QoS IOPS


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
QoS IOPS
REMOVE
MaxThroughput IOPS
10000
MinThroughput IOPS
1000


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Storage compatibility
COMPATIBLE
INCOMPATIBLE
Expand datastore clusters
Compatible storage 4 TB (3.8 TB free)
Quick Filter
Enter value
Name
Datacenter
Type
Free Space
Capacity
Warnings
NFS_vVols
Raleigh
vVol
3.80 TB
4.00 TB



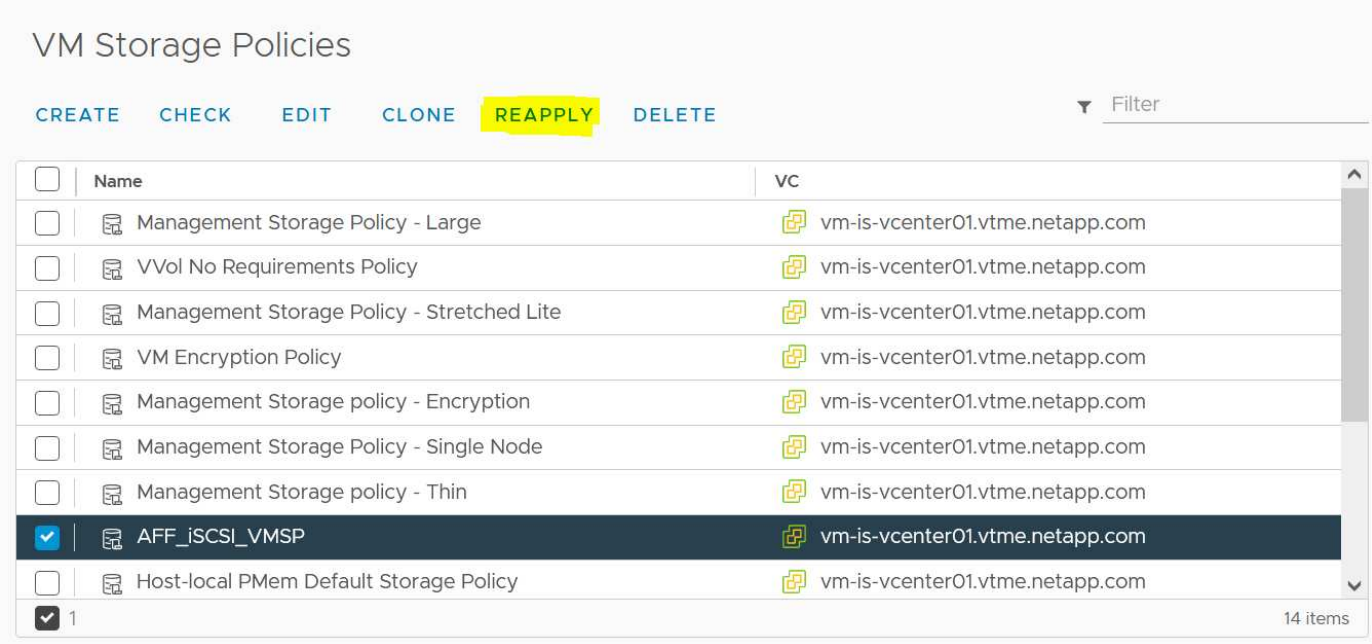
ONTAP 툴을 사용한 성능 관리

ONTAP 툴은 자체적인 밸런스 배치 알고리즘을 사용하여 새로운 VVOL을 유니파이드 또는 기존 ASA 시스템이 있는 최고의 FlexVol volume에 배치하거나, ASA R2 시스템이 포함된 SAZ(Storage Availability Zone)를 VVOL 데이터 저장소 내에 배치합니다. 배치는 백업 스토리지와 VM 스토리지 정책을 일치시키는 것을 기반으로 합니다. 이렇게 하면 데이터 저장소 및 백업 스토리지가 지정된 성능 요구 사항을 충족할 수 있습니다.

최소 및 최대 IOPS와 같은 성능 기능을 변경하려면 특정 구성에 주의를 기울여야 합니다.

- * 최소 및 최대 IOPS * 는 VM 정책에 지정할 수 있습니다.
  - 정책에서 IOPS를 변경해도 해당 VM 정책을 사용하는 VM에 다시 적용하기 전까지는 vVols 의 QoS가 변경되지 않습니다. 또는 원하는 IOPS로 새 정책을 생성하여 대상 VM에 적용할 수도 있습니다. 일반적으로는 서비스 계층별로 별도의 VM 스토리지 정책을 정의하고 VM에서 해당 정책을 변경하는 것이 좋습니다.
  - ASA, ASA r2, AFF 및 FAS 유형은 각각 다른 IOP 설정값을 가지고 있습니다. Min과 Max는 모든 플래시 시스템에서 사용할 수 있지만, AFF 지원하지 않는 시스템에서는 Max IOPs 설정만 사용할 수 있습니다.
- ONTAP 툴은 현재 지원되는 버전의 ONTAP로 개별 비공유 QoS 정책을 생성합니다. 따라서 각 개별 VMDK는 고유한 IOP 할당을 받게 됩니다.

VM 스토리지 정책을 다시 적용합니다



VVOL 보호

다음 섹션에서는 ONTAP 스토리지에서 VMware VVOL을 사용하기 위한 절차 및 모범 사례를 간략히 설명합니다.

VASA 공급자 고가용성

NetApp VASA Provider는 vCenter 플러그인 및 REST API 서버(이전의 VSC(Virtual Storage Console)) 및 스토리지 복제 어댑터와 함께 가상 어플라이언스의 일부로 실행됩니다. VASA Provider를 사용할 수 없는 경우 VVol을 사용하는 VM은 계속 실행됩니다. 그러나 새로운 VVOL 데이터 저장소를 생성할 수 없으며 VVol은 vSphere에서 생성하거나 바인딩할 수 없습니다. 즉, vCenter에서 VVOL의 생성을 요청할 수 없기 때문에 VVOL을 사용하는 VM의 전원을 켤 수 없습니다. 실행 중인 VM은 VVol을 새 호스트에 바인딩할 수 없으므로 vMotion을 사용하여 다른 호스트로 마이그레이션할 수 없습니다.

VASA Provider 7.1 이상은 새로운 기능을 지원하여 필요할 때 서비스를 사용할 수 있도록 합니다. VASA Provider 및 통합 데이터베이스 서비스를 모니터링하는 새로운 Watchdog 프로세스가 포함되어 있습니다. 오류가 감지되면 로그 파일을 업데이트한 다음 서비스를 자동으로 다시 시작합니다.

소프트웨어, 호스트 하드웨어 및 네트워크의 장애로부터 다른 미션 크리티컬 VM을 보호하는 데 사용되는 동일한 가용성 기능을 사용하여 vSphere 관리자가 추가 보호를 구성해야 합니다. 이러한 기능을 사용하기 위해 가상 어플라이언스에 추가 구성이 필요하지 않습니다. 표준 vSphere 방식을 사용하여 구성하기만 하면 됩니다. 이러한 기능은 테스트를 거쳤으며 NetApp에서 지원됩니다.

장애가 발생할 경우 호스트 클러스터의 다른 호스트에서 VM을 다시 시작하도록 vSphere High Availability를 손쉽게 구성할 수 있습니다. vSphere Fault Tolerance는 지속적으로 복제되고 어느 시점에서든 인계받을 수 있는 보조 VM을 생성하여 가용성을 높여 줍니다. 이러한 기능에 대한 추가 정보는 에서 확인할 수 있습니다 "VMware vSphere용 ONTAP 툴 설명서(ONTAP 툴에 대한 고가용성 구성)"및 VMware vSphere 설명서(ESXi 및 vCenter Server에서 vSphere 가용성 확인)

ONTAP 툴 VASA Provider는 FlexVol 볼륨 메타데이터 내에 VVol 정보가 저장된 관리되는 ONTAP 시스템에 VVOL 구성을 실시간으로 자동 백업합니다. 어떤 이유로든 ONTAP 도구 어플라이언스를 사용할 수 없게 되는 경우 새 도구를 쉽고 빠르게 배포하고 구성을 가져올 수 있습니다. VASA Provider 복구 단계에 대한 자세한 내용은 이 KB 문서를 참조하십시오.

"VASA Provider 재해 복구 - 해결 가이드를 수행하는 방법"

VVOL 복제

많은 ONTAP 고객은 NetApp SnapMirror를 사용하여 기존 데이터 저장소를 2차 스토리지 시스템으로 복제한 다음, 재해 발생 시 2차 시스템을 사용하여 개별 VM 또는 전체 사이트를 복구합니다. 대부분의 경우 고객은 VMware vSphere용 NetApp SnapCenter 플러그인과 같은 백업 소프트웨어 제품 또는 VMware의 사이트 복구 관리자(ONTAP 툴의 스토리지 복제 어댑터 포함)와 같은 재해 복구 솔루션과 같은 소프트웨어 툴을 사용하여 이를 관리합니다.

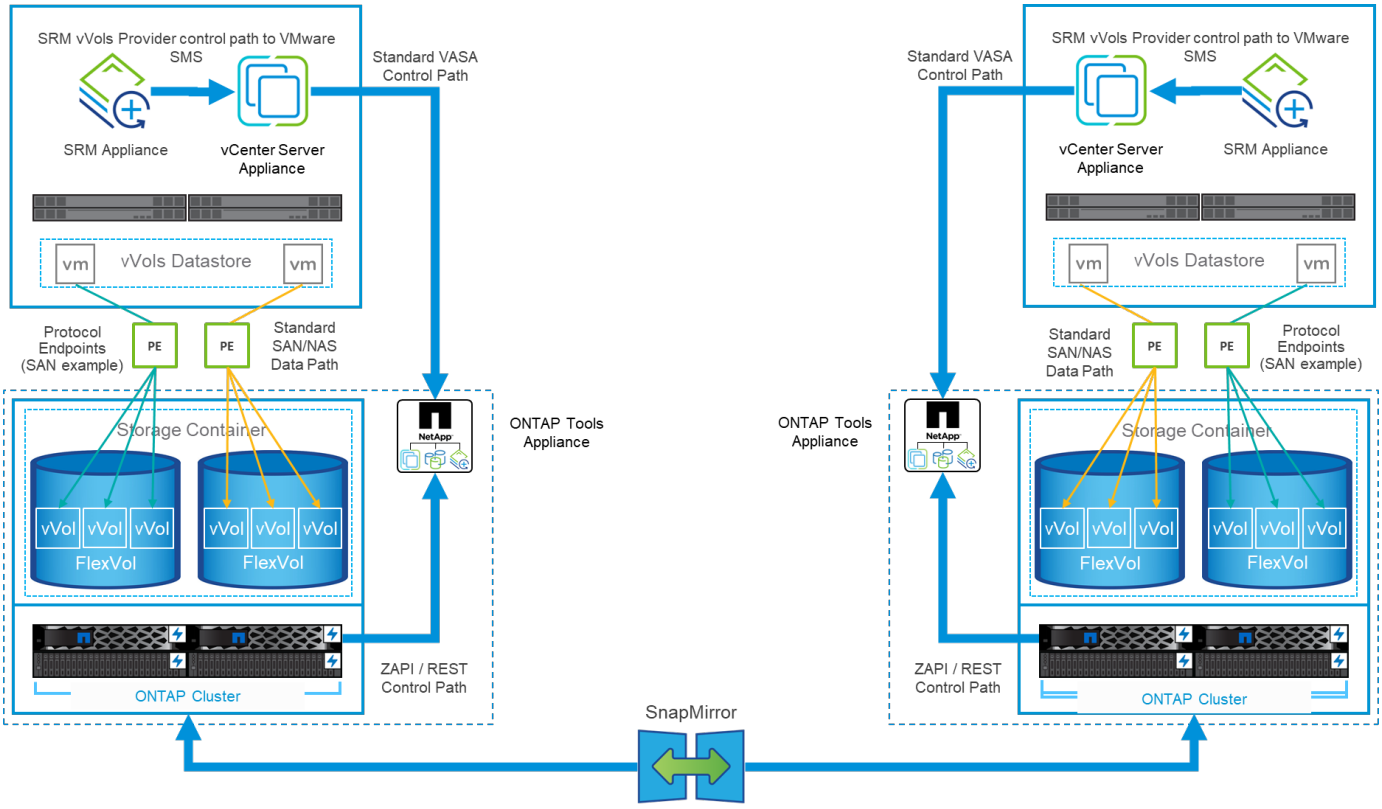
VVOL 복제를 관리하려면 소프트웨어 툴에 대한 이 요구사항이 더 중요합니다. 일부 측면은 기본 기능(예: VMware에서 관리하는 VVOL 스냅샷)을 통해 관리할 수 있지만(예: 빠르고 효율적인 파일 또는 LUN 클론을 사용하는 ONTAP로 오프로드됨) 복제 및 복구를 관리하려면 일반적으로 오케스트레이션이 필요합니다. VVOL에 대한 메타데이터는 ONTAP와 VASA Provider에 의해 보호되지만 보조 사이트에서 이를 사용하려면 추가 처리가 필요합니다.

ONTAP 툴 9.7.1 을 VMware SRM(Site Recovery Manager) 8.3 릴리스와 함께 사용하면 NetApp SnapMirror 기술을 활용하여 재해 복구 및 마이그레이션 워크플로우 오케스트레이션에 대한 지원이 추가되었습니다.

ONTAP 툴 9.7.1을 통한 SRM 지원의 초기 릴리즈에서는 FlexVol 볼륨을 미리 생성하고 SnapMirror 보호를 활성화한 후 VVol 데이터 저장소의 백업 볼륨으로 사용해야 했습니다. ONTAP 도구 9.10부터는 더 이상 이 프로세스가 필요하지 않습니다. 이제 기존의 백업 볼륨에 SnapMirror 보호를 추가하고 VM 스토리지 정책을 업데이트하여 SRM과 통합된 재해 복구 및 마이그레이션 오케스트레이션 및 자동화 기능을 통해 정책 기반 관리를 활용할 수 있습니다.

현재 VMware SRM은 NetApp에서 지원하는 VVOL을 위한 유일한 재해 복구 및 마이그레이션 자동화 솔루션이며, ONTAP 툴은 VVOL 복제를 활성화하기 전에 vCenter에 등록된 SRM 8.3 이상 서버의 존재를 ONTAP 툴 REST API를 활용하여 자체 서비스를 생성할 수 있지만

SRM을 사용한 **VVol** 복제



MetroCluster 지원

ONTAP 툴은 MetroCluster 전환을 트리거할 수 없지만, 동일한 vMSC(vSphere Metro Storage Cluster) 구성에서 VVOL을 지원하는 볼륨을 위한 NetApp MetroCluster 시스템은 지원합니다. MetroCluster 시스템의 전환은 일반적인 방식으로 처리됩니다.

NetApp SnapMirror 비즈니스 연속성(SM-BC)을 vMSC 구성의 기반으로 사용할 수도 있지만, 현재 VVOL에서 지원되지 않습니다.

NetApp MetroCluster에 대한 자세한 내용은 다음 가이드를 참조하십시오.

"_TR-4689 MetroCluster IP 솔루션 아키텍처 및 설계 _"

"_TR-4705 NetApp MetroCluster 솔루션 아키텍처 및 설계 _"

"*VMware KB 2031038 NetApp MetroCluster* 기반 VMware vSphere 지원"

VVOL 백업 개요

게스트 내 백업 에이전트 사용, 백업 프록시에 VM 데이터 파일 연결 또는 VMware VADP 같은 정의된 API 사용과 같은 VM을 보호하기 위한 몇 가지 방법이 있습니다. VVOL은 동일한 메커니즘을 사용하여 보호할 수 있으며 많은 NetApp 파트너가 VVOL을 포함한 VM 백업을 지원합니다.

앞서 언급했듯이 VMware vCenter 관리 스냅샷은 공간 효율적이고 빠른 ONTAP 파일/LUN 클론으로 오프로드됩니다. 이러한 스냅샷은 빠른 수동 백업에 사용할 수 있지만 vCenter에 의해 최대 32개의 스냅샷으로 제한됩니다. 필요에 따라 vCenter를 사용하여 스냅샷을 생성하고 되돌릴 수 있습니다.

SnapCenter SCV(VMware vSphere) 플러그인 4.6부터 ONTAP 도구 9.10 이상과 함께 사용할 경우 SnapMirror 및 SnapVault 복제를 지원하는 ONTAP FlexVol 볼륨 스냅샷을 활용하여 충돌 시에도 정합성이 보장되는 VVol 기반 VM 백업 및 복구를 지원합니다. 볼륨당 최대 1023개의 스냅샷이 지원됩니다. 또한 SCV는 미러 볼트 정책이 적용된 SnapMirror를 사용하여 보조 볼륨에 더 많은 스냅샷을 더 오래 보존할 수 있습니다.

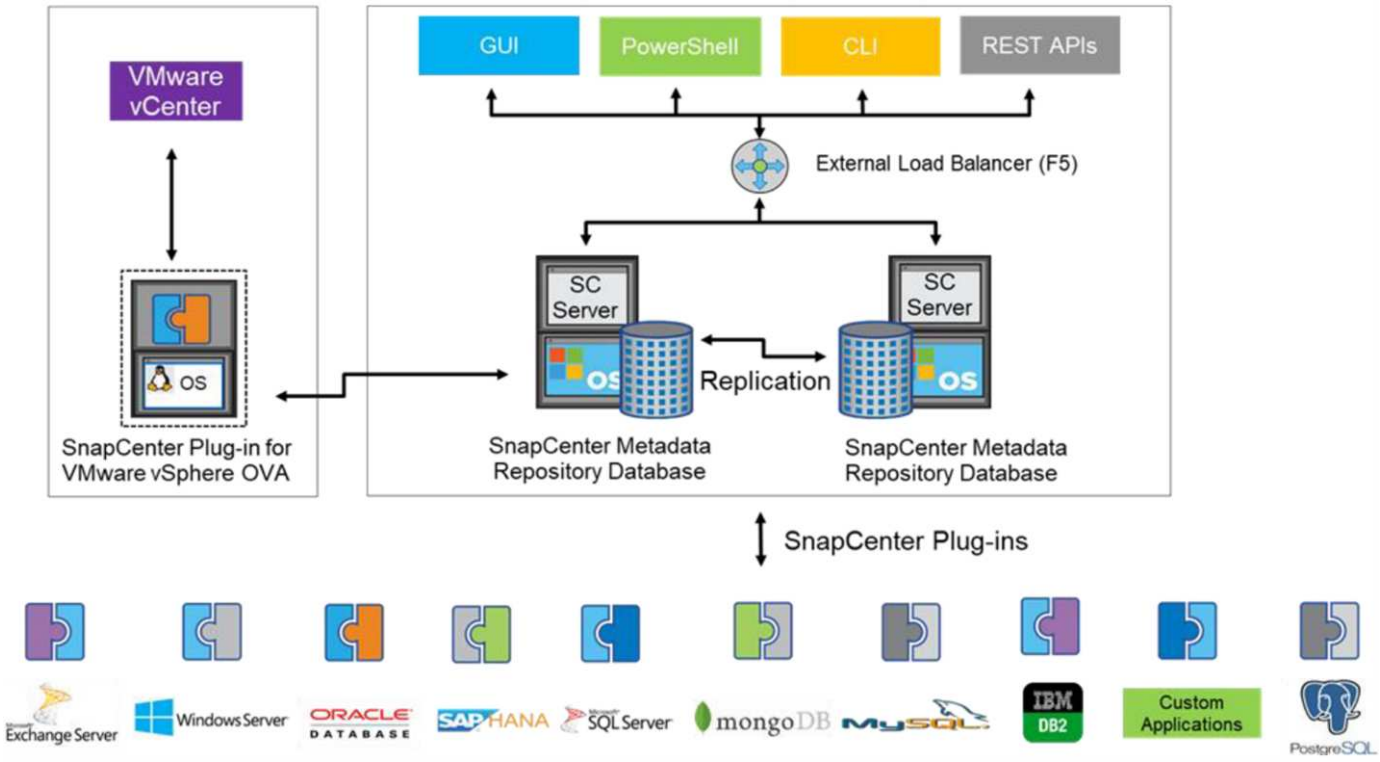
vSphere 8.0 지원은 격리된 로컬 플러그인 아키텍처를 사용하는 SCV 4.7에 도입되었습니다. 새로운 원격 플러그인 아키텍처로 완전히 전환된 SCV 4.8에 vSphere 8.0U1 지원이 추가되었습니다.

VMware vSphere용 SnapCenter 플러그인을 사용한 VVol 백업

이제 NetApp SnapCenter를 사용하여 태그 및/또는 폴더를 기반으로 VVol용 리소스 그룹을 생성하여 VVol 기반 VM에 대해 ONTAP의 FlexVol 기반 스냅샷을 자동으로 활용할 수 있습니다. 이를 통해 환경 내에서 VM이 동적으로 프로비저닝될 때 자동으로 VM을 보호하는 백업 및 복구 서비스를 정의할 수 있습니다.

VMware vSphere용 SnapCenter 플러그인은 vCenter 확장으로 등록된 독립 실행형 어플라이언스로 구축되며, vCenter UI 또는 REST API를 통해 관리되며 백업 및 복구 서비스 자동화를 지원합니다.

SnapCenter 아키텍처



다른 SnapCenter 플러그인은 이 작성 시점에 VVol을 지원하지 않으므로 이 문서의 독립 실행형 배포 모델에 대해 중점적으로 살펴보겠습니다.

SnapCenter는 ONTAP FlexVol 스냅샷을 사용하기 때문에 vSphere에 오버헤드가 발생하지 않으며, vCenter 관리 스냅샷을 사용하여 기존 VM에서 볼 수 있는 성능 패널도 없습니다. 또한 SCV의 기능은 REST API를 통해 노출되기 때문에 VMware Aria Automation, Ansible, Terraform 및 거의 표준 REST API를 사용할 수 있는 기타 자동화 툴과 같은 툴을 사용하여 자동화된 워크플로우를 쉽게 생성할 수 있습니다.

SnapCenter REST API에 대한 자세한 내용은 를 참조하십시오 "REST API 개요"

VMware vSphere REST API용 SnapCenter 플러그인에 대한 자세한 내용은 을 참조하십시오 "VMware vSphere REST API용 SnapCenter 플러그인"

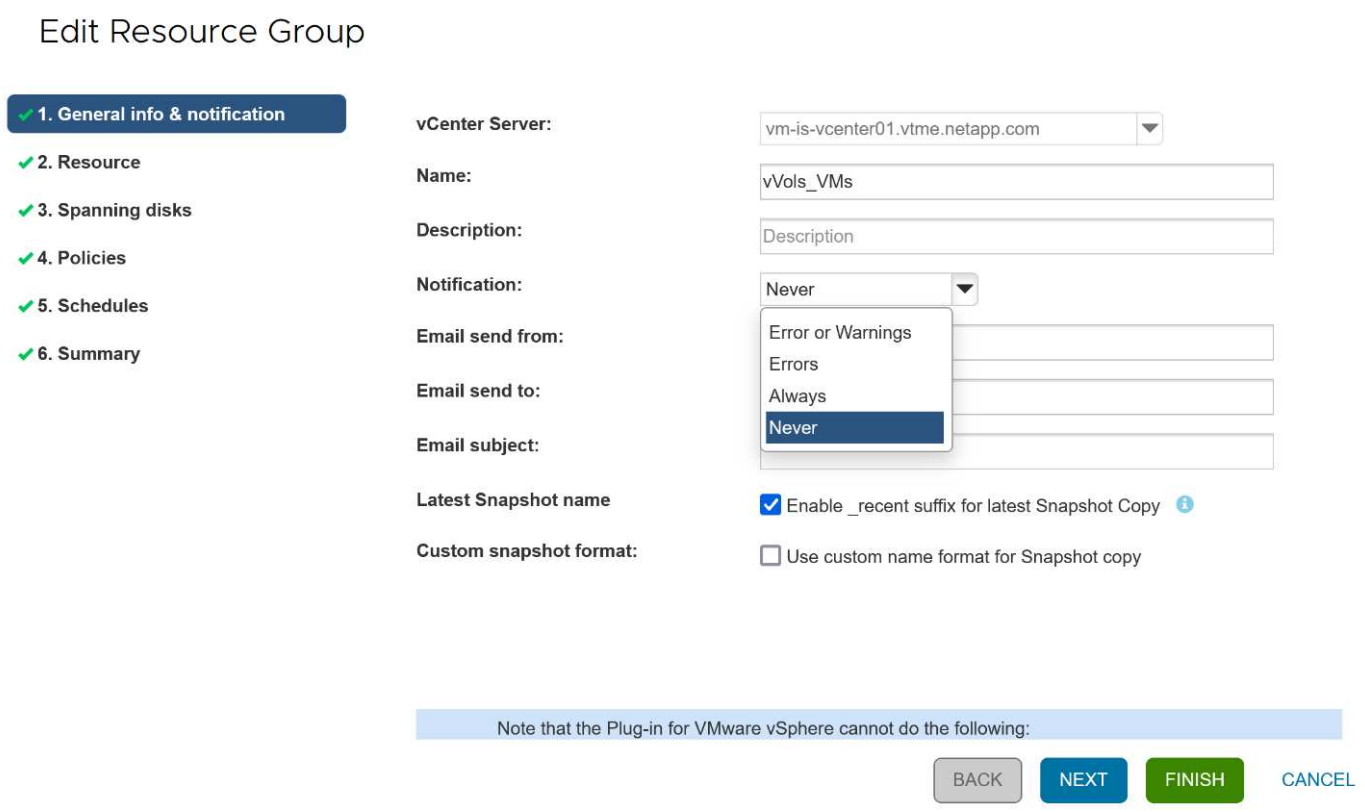
모범 사례

다음 모범 사례를 사용하면 SnapCenter 배포를 최대한 활용할 수 있습니다.

- SCV는 vCenter Server RBAC와 ONTAP RBAC를 모두 지원하며 플러그인이 등록될 때 자동으로 생성되는 사전 정의된 vCenter 역할을 포함합니다. 지원되는 RBAC 유형에 대해 자세히 알아볼 수 있습니다 "여기."
  - vCenter UI를 사용하여 설명된 사전 정의된 역할을 사용하여 최소 권한 계정 액세스를 할당합니다 "여기".
  - SnapCenter 서버와 함께 SCV를 사용하는 경우 _SnapCenterAdmin_role을 할당해야 합니다.
  - ONTAP RBAC는 SCV에서 사용되는 스토리지 시스템을 추가 및 관리하는 데 사용되는 사용자 계정을 의미합니다. ONTAP RBAC는 VVOL 기반 백업에 적용되지 않습니다. ONTAP RBAC 및 SCV에 대해 자세히 알아보십시오 "여기".

• SnapMirror를 사용하여 소스 볼륨의 전체 복제본을 사용하여 백업 데이터 세트를 두 번째 시스템으로 복제합니다. 앞서 언급했듯이 소스 볼륨 스냅샷 보존 설정과 관계없이 백업 데이터의 장기 보존을 위해 미러 볼트(mirror-vault) 정책을 사용할 수도 있습니다. 두 가지 메커니즘 모두 VVOL에서 지원됩니다.
• SCV에는 VVOL 기능을 위해 VMware vSphere용 ONTAP 툴도 필요하므로 항상 NetApp IMT(Interoperability Matrix Tool)에서 특정 버전 호환성을 확인하십시오
• VMware SRM에서 VVol 복제를 사용하는 경우 정책 RPO 및 백업 일정을 고려해야 합니다
• 조직에서 정의한 RPO(복구 시점 목표)를 충족하는 보존 설정으로 백업 정책 설계
• 백업이 실행될 때 상태를 알리도록 리소스 그룹의 알림 설정을 구성합니다(아래 그림 10 참조).

리소스 그룹 알림 옵션



이 문서를 사용하여 **SCV**를 시작하십시오

"VMware vSphere용 SnapCenter 플러그인에 대해 자세히 알아보십시오"

"VMware vSphere용 SnapCenter 플러그인 구축"

문제 해결

추가 정보와 함께 여러 문제 해결 리소스를 사용할 수 있습니다.

NetApp Support 사이트

NetApp 지원 사이트에는 NetApp 가상화 제품에 대한 다양한 Knowledgebase 문서 외에 해당 제품에 대한 간편한 랜딩 페이지도 "VMware vSphere용 ONTAP 툴" 있습니다. 이 포털은 NetApp 커뮤니티에서 기사, 다운로드, 기술 보고서 및 VMware Solutions 토론에 대한 링크를 제공합니다. 이 제품은 다음 위치에서 사용할 수 있습니다.

"_NetApp Support 사이트 _"

추가 솔루션 설명서는 여기에서 확인할 수 있습니다.

"_NetApp Broadcom의 VMware 가상화 솔루션 _"

제품 문제 해결

vCenter 플러그인, VASA 공급자, 스토리지 복제 어댑터 등과 같은 ONTAP 툴의 다양한 구성 요소는 NetApp 문서 저장소에 함께 정리되어 있습니다. 그러나 각 기술 문서는 별도의 하위 섹션을 가지고 있으며 특정 문제 해결 절차가 있을 수 있습니다. VASA Provider에서 발생할 수 있는 가장 일반적인 문제를 해결합니다.

VASA Provider UI 문제

때때로 vCenter vSphere Web Client에서 Serenity 구성 요소에 문제가 발생하여 VASA Provider for ONTAP 메뉴 항목이 표시되지 않는 경우가 있습니다. 구축 가이드 또는 이 기술 자료에서 VASA 공급자 등록 문제 해결 을 참조하십시오 "기사".

VVOL 데이터 저장소 프로비저닝이 실패합니다

VVOL 데이터 저장소를 생성할 때 vCenter 서비스가 시간 초과되는 경우가 있습니다. 이 문제를 해결하려면 VMware-SPS 서비스를 다시 시작한 다음 vCenter 메뉴(Storage > New Datastore)를 사용하여 VVol 데이터 저장소를 다시 마운트합니다. 관리 가이드의 vCenter Server 6.5와 함께 VVol 데이터 저장소 프로비저닝이 실패하는 경우 이에 대해 다룹니다.

Unified Appliance를 Mount ISO로 업그레이드하지 못했습니다

vCenter의 버그로 인해 Unified Appliance를 한 릴리즈에서 다음 릴리즈로 업그레이드하는 데 사용되는 ISO가 마운트되지 않을 수 있습니다. vCenter에서 ISO를 어플라이언스에 연결할 수 있는 경우 이 Knowledgebase의 프로세스를 따르십시오 "기사" 를 눌러 해결합니다.

ONTAP를 사용하는 VMware 사이트 복구 관리자

ONTAP를 사용한 VMware 라이브 사이트 복구

ONTAP 20년 전 ESX가 현대 데이터 센터에 도입된 이래로 VMware vSphere를 위한 선도적인 스토리지 솔루션이었으며, 최근에는 Cloud Foundation을 위한 솔루션도 출시되었습니다. NetApp SnapMirror Active Sync와 같은 기능과 함께 최신 세대의 ASA A 시리즈를 비롯한 혁신적인 시스템을 지속적으로 출시하고 있습니다. 이러한 발전으로 인해 관리가 간소화되고, 복원력이 향상되며, IT 인프라의 총 소유 비용(TCO)이 낮아집니다.

이 문서에서는 이전에 Site Recovery Manager(SRM)로 알려졌던 VMware Live Site Recovery(VLSR)용 ONTAP 솔루션을 소개합니다. VLSR은 VMware의 업계 선도적인 재해 복구(DR) 소프트웨어로, 배포를 간소화하고 위험을 줄이며 지속적인 관리를 단순화하는 최신 제품 정보와 모범 사례를 포함합니다.

이 문서는 이전에 게시된 기술 보고서 _TR-4900: ONTAP을 탑재한 VMware Site Recovery Manager_를 대체합니다.

모범 사례는 가이드 및 호환성 도구와 같은 다른 문서를 보완합니다. 이러한 전문 분야는 연구소 테스트와 NetApp 엔지니어 및 고객의 광범위한 현장 경험을 기반으로 합니다. 권장 모범 사례가 귀사의 환경에 적합하지 않은 경우도 있지만, 일반적으로 대부분의 고객 요구사항을 충족하는 가장 간단한 솔루션입니다.

이 문서에서는 VMware vSphere 10.4(NetApp SRA(Storage Replication Adapter) 및 VASA 공급자[VP] 포함)용 ONTAP 툴 및 VMware 라이브 사이트 복구 9용 ONTAP 9 최신 릴리즈의 기능에 대해 중점적으로 다룹니다.

VLSR 또는 **SRM**과 함께 **ONTAP**를 사용해야 하는 이유

ONTAP 기반의 NetApp 데이터 관리 플랫폼은 VLSR에 가장 널리 채택된 스토리지 솔루션 중 일부입니다. 그 이유는 많습니다. 업계를 선도하는 스토리지 효율성, 멀티테넌시, 서비스 품질 제어, 공간 효율적인 스냅샷을 통한 데이터 보호, SnapMirror 통한 복제 기능을 제공하는 안전하고 고성능의 통합 프로토콜(NAS 및 SAN 통합) 데이터 관리 플랫폼입니다. 모든 솔루션은 VMware 워크로드를 보호하기 위한 네이티브 하이브리드 멀티 클라우드 통합을 활용하며, 다양한 자동화 및 오케스트레이션 도구를 손쉽게 사용할 수 있습니다.

어레이 기반 복제에 SnapMirror 사용하면 ONTAP의 가장 검증되고 성숙한 기술 중 하나를 활용할 수 있습니다. SnapMirror 전체 VM이나 데이터 저장소가 아닌 변경된 파일 시스템 블록만 복사하여 안전하고 효율적인 데이터 전송이라는 이점을 제공합니다. 이러한 블록도 중복 제거, 압축, 압축과 같은 공간 절약의 이점을 활용합니다. 최신 ONTAP 시스템은 이제 버전에 독립적인 SnapMirror 사용하여 소스 및 대상 클러스터를 선택하는 데 유연성이 제공됩니다. SnapMirror 재해 복구에 사용할 수 있는 가장 강력한 도구 중 하나가 되었습니다.

기존 NFS, iSCSI 또는 파이버 채널 연결 데이터 저장소(현재 vVols 데이터 저장소 지원 포함)를 사용하는지 여부에 관계없이 VLSR은 재해 복구 또는 데이터 센터 마이그레이션 계획 및 오케스트레이션을 위해 ONTAP 기능의 장점을 최대한 활용하는 강력한 자체 솔루션을 제공합니다.

VLSR이 **ONTAP 9**를 활용하는 방법

VLSR은 세 가지 주요 구성 요소가 포함된 가상 어플라이언스인 ONTAP for VMware vSphere와 통합하여 ONTAP 시스템의 고급 데이터 관리 기술을 활용합니다.

- 이전에 VSC(가상 스토리지 콘솔)로 알려진 ONTAP 툴 vCenter 플러그인을 사용하면 SAN 또는 NAS에서 스토리지 관리 및 효율성 기능을 간소화하고, 가용성을 개선하고 스토리지 비용 및 운영 오버헤드를 줄일 수 있습니다. Best Practice를 사용하여 데이터 저장소를 프로비저닝하고 NFS 및 블록 스토리지 환경에 대한 ESXi 호스트 설정을 최적화합니다. 이러한 모든 이점을 위해 NetApp은 ONTAP를 실행하는 시스템에서 vSphere를 사용할 때 이 플러그인을 사용하는 것이 좋습니다.
- ONTAP 툴 VASA Provider는 VMware VASA(vStorage APIs for Storage Awareness) 프레임워크를 지원합니다. VASA Provider는 vCenter Server를 ONTAP와 연결하여 VM 스토리지를 프로비저닝하고 모니터링할 수 있도록 지원합니다. 이를 통해 VVol(VMware Virtual Volumes)은 VM 스토리지 정책과 개별 VM VVol 성능을 지원하고 관리할 수 있게 되었습니다. 또한 용량을 모니터링하고 프로파일 준수를 위한 알람을 제공합니다.
- SRA는 VLSR과 함께 사용되어 기존 VMFS 및 NFS 데이터 저장소의 프로덕션 및 재해 복구 사이트 간에 VM 데이터 복제를 관리하고 DR 복제본의 무중단 테스트를 수행합니다. 검색, 복구 및 재보호 작업을 자동화할 수 있습니다. 여기에는 Windows SRM 서버 및 VLSR 어플라이언스용 SRA 어댑터와 SRA 어댑터가 모두 포함됩니다.

vVols가 아닌 데이터 저장소를 보호하기 위해 VLSR 서버에 SRA 어댑터를 설치하고 구성한 후 재해 복구를 위해 vSphere 환경을 구성하는 작업을 시작할 수 있습니다.

SRA는 VLSR 서버에 대한 명령 및 제어 인터페이스를 제공하여 VMware 가상 머신(VM)이 포함된 ONTAP FlexVol 볼륨을 관리하고 이를 보호하는 SnapMirror 복제를 관리합니다.

VLSR은 NetApp의 독점 FlexClone 기술을 사용하여 DR 계획을 중단 없이 테스트하고 DR 사이트에서 보호된 데이터 저장소를 거의 즉시 복제할 수 있습니다. VLSR은 귀하의 조직과 고객이 실제 재해 발생 시 보호받을 수 있도록 안전하게 테스트할 수 있는 샌드박스를 만들어 재해 발생 시 장애 조치를 실행할 수 있는 조직의 능력에 대한 확신을 제공합니다.

실제 재해 또는 계획된 마이그레이션이 있는 경우 VLSR을 사용하면 최종 SnapMirror 업데이트(선택한 경우)를 통해 데이터 세트에 대한 최신 변경 사항을 보낼 수 있습니다. 그런 다음 미러를 해제하고 데이터 저장소를 DR 호스트에 마운트합니다. 이 시점에서 사전 계획된 전략에 따라 임의의 순서로 VM을 자동으로 켤 수 있습니다.

ONTAP 시스템을 사용하면 동일한 클러스터에서 SnapMirror 복제를 위해 SVM을 페어링할 수 있지만, 이 시나리오는 VLSR에서 테스트 및 인증되지 않았습니다. 따라서 VLSR을 사용할 때는 서로 다른 클러스터의 SVM만 사용하는 것이 좋습니다.

ONTAP 및 기타 사용 사례를 지원하는 **VLSR:** 하이브리드 클라우드 및 마이그레이션

VLSR 배포를 ONTAP 고급 데이터 관리 기능과 통합하면 로컬 스토리지 옵션과 비교했을 때 규모와 성능이 크게 향상됩니다. 하지만 그보다 더 중요한 것은 하이브리드 클라우드의 유연성입니다. 하이브리드 클라우드를 사용하면 FabricPool 사용하여 고성능 어레이에서 사용하지 않는 데이터 블록을 선호하는 하이퍼스케일러로 계층화하여 비용을 절감할 수 있습니다. 이는 NetApp StorageGRID 와 같은 온프레미스 S3 저장소가 될 수 있습니다. 소프트웨어 정의 ONTAP Select 또는 클라우드 기반 DR을 사용하여 에지 기반 시스템에 SnapMirror 사용할 수도 있습니다. "Equinix Metal의 NetApp 스토리지"또는 다른 호스팅 ONTAP 서비스.

그런 다음, FlexClone을 통해 스토리지 설치 공간이 거의 0에 가까운 클라우드 서비스 공급자의 데이터 센터 내에서 테스트 페일오버를 수행할 수 있습니다. 이제 조직을 보호하는 데 드는 비용이 그 어느 때보다 줄어듭니다.

또한 VLSR은 SnapMirror를 활용하여 VM을 하나의 데이터 센터에서 다른 데이터 센터로 효율적으로 전송하거나 자체 또는 NetApp 파트너 서비스 공급자의 수를 통해 동일한 데이터 센터 내에서 효율적으로 전송하여 계획된 마이그레이션을 실행하는 데 사용할 수 있습니다.

배포 모범 사례

다음 섹션에서는 ONTAP 및 VMware SRM의 구축 Best Practice를 간략히 설명합니다.

최신 버전의 **ONTAP** 도구 사용 **10**

ONTAP 도구 10은 다음을 포함하여 이전 버전에 비해 크게 향상된 기능을 제공합니다.

- 테스트 대체 작동 속도 8배 향상 *
- 2배 빠른 정리 및 재보호*
- 페일오버 속도 32% 향상 *
- 더 뛰어난 확장성
- 공유 사이트 레이아웃 기본 지원

*이러한 개선 사항은 내부 테스트를 기반으로 하며 사용자 환경에 따라 달라질 수 있습니다.

SMT를 위한 **SVM** 레이아웃 및 **Segmentation**

ONTAP를 사용하면 SVM(스토리지 가상 머신)이라는 개념을 통해 보안 멀티 테넌트 환경에서 엄격한 세분화를 제공할 수 있습니다. 한 SVM의 SVM 사용자는 다른 SVM에서 리소스를 액세스하거나 관리할 수 없습니다. 이렇게 하면 동일한 클러스터에서 고유한 SRM 워크플로우를 관리하는 여러 사업부에 대해 별도의 SVM을 생성하여 ONTAP 기술을

활용함으로써 전반적인 스토리지 효율성을 높일 수 있습니다.

보안 제어를 개선하면서 성능을 향상할 뿐만 아니라 SVM 범위 계정 및 SVM 관리 LIF를 사용하여 ONTAP를 관리하는 것을 고려해 보십시오. SRA는 물리적 리소스를 포함하여 전체 클러스터의 모든 리소스를 처리할 필요가 없으므로 SVM 범위 연결을 사용할 때 기본적으로 성능이 향상됩니다. 대신, 특정 SVM에 추상화된 논리적 자산만 이해해야 합니다.

ONTAP 9 시스템 관리 모범 사례

앞서 언급했듯이 클러스터 또는 SVM 범위의 자격 증명 및 관리 LIF를 사용하여 ONTAP 클러스터를 관리할 수 있습니다. 최적의 성능을 위해 VVOL을 사용하지 않을 때마다 SVM 범위 자격 증명 사용을 고려할 수 있습니다. 그러나 이렇게 하면 일부 요구 사항을 인식하고 일부 기능을 사용할 수 없게 됩니다.

- 기본 vsadmin SVM 계정에는 ONTAP 툴 작업을 수행하는 데 필요한 액세스 수준이 없습니다. 따라서 새 SVM 계정을 생성해야 합니다. "ONTAP 사용자 역할 및 권한을 구성합니다" 포함된 JSON 파일 사용 SVM 또는 클러스터 범위 어카운트에 사용할 수 있습니다.
- vCenter UI 플러그인, VASA Provider 및 SRA 서버는 모두 완전히 통합된 마이크로서비스이므로 vCenter UI for ONTAP 툴에 스토리지를 추가하는 것과 동일한 방식으로 SRM의 SRA 어댑터에 스토리지를 추가해야 합니다. 그렇지 않으면 SRA 서버는 SRA 어댑터를 통해 SRM에서 전송되는 요청을 인식하지 못할 수 있습니다.
- ONTAP Tools Manager에서 먼저 SVM 범위 자격 증명을 사용하여 vCenter에 연결하지 않는 한 NFS 경로 검사는 수행되지 않습니다. "온보드 클러스터" 물리적 위치가 SVM에서 논리적으로 추상화되기 때문입니다. 하지만 최신 ONTAP 시스템은 간접 경로를 사용할 때 눈에 띄는 성능 저하가 더 이상 발생하지 않으므로 이는 우려의 원인이 아닙니다.
- 스토리지 효율성으로 인한 애그리게이트 공간 절약은 보고되지 않을 수 있습니다.
- 지원되는 경우 로드 공유 미러를 업데이트할 수 없습니다.
- SVM 범위 자격 증명으로 관리되는 ONTAP 시스템에서는 EMS 로깅이 수행되지 않을 수 있습니다.

운영 모범 사례

다음 섹션에서는 VMware SRM 및 ONTAP 스토리지에 대한 운영 Best Practice를 간략히 설명합니다.

데이터 저장소 및 프로토콜

- 가능하면 항상 ONTAP 툴을 사용하여 데이터 저장소와 볼륨을 프로비저닝하십시오. 이렇게 하면 볼륨, 접합 경로, LUN, igroup, 엑스포트 정책이 및 기타 설정은 호환되는 방식으로 구성됩니다.
- SRM은 SRA를 통해 어레이 기반 복제를 사용할 때 ONTAP 9를 통해 iSCSI, 파이버 채널 및 NFS 버전 3을 지원합니다. SRM은 기존 데이터 저장소 또는 VVOL 데이터 저장소를 사용하는 NFS 버전 4.1에 대한 어레이 기반 복제를 지원하지 않습니다.
- 접속을 확인하려면 항상 대상 ONTAP 클러스터에서 DR 사이트의 새 테스트 데이터 저장소를 마운트하고 마운트 해제할 수 있는지 확인하십시오. 데이터 저장소 연결에 사용할 각 프로토콜을 테스트합니다. 모범 사례는 ONTAP 툴을 사용하여 테스트 데이터 저장소를 생성하는 것입니다. 이는 SRM의 지시에 따라 모든 데이터 저장소 자동화를 수행하기 때문입니다.
- SAN 프로토콜은 각 사이트에서 동종이어야 합니다. NFS와 SAN을 혼합할 수 있지만 SAN 프로토콜을 사이트 내에서 혼합하면 안 됩니다. 예를 들어, 사이트 A에는 FCP를, 사이트 B에는 iSCSI를 사용할 수 있습니다. 사이트 A에서는 FCP와 iSCSI를 모두 사용하면 안 됩니다
- 이전 가이드에서는 데이터 지역성에 LIF를 생성하는 것이 권장되었습니다. 다시 말해, 볼륨을 물리적으로 소유한 노드에 있는 LIF를 사용하여 데이터 저장소를 항상 마운트합니다. 이것이 모범 사례이기는 하지만, 최신 버전의

ONTAP 9에서는 더 이상 필요하지 않습니다. 가능한 한 언제든지, 클러스터 범위 자격 증명이 있을 경우 ONTAP 툴은 데이터를 로컬에 있는 LIF 간 로드 밸런싱을 계속 선택하지만 고가용성 또는 성능이 필요하지 않습니다.

- 자동 크기 조정이 필요한 비상 용량을 충분히 제공할 수 없는 경우 공간이 부족한 경우 가동 시간을 유지하기 위해 스냅샷을 자동으로 제거하도록 ONTAP 9를 구성할 수 있습니다. 이 기능의 기본 설정은 SnapMirror에 의해 생성된 스냅샷을 자동으로 삭제하지 않습니다. SnapMirror 스냅샷이 삭제된 경우 NetApp SRA는 영향을 받는 볼륨에 대해 복제를 역순으로 재동기화할 수 없습니다. ONTAP가 SnapMirror 스냅샷을 삭제하지 못하도록 하려면 스냅샷 자동 삭제 기능을 '시도'로 구성합니다.

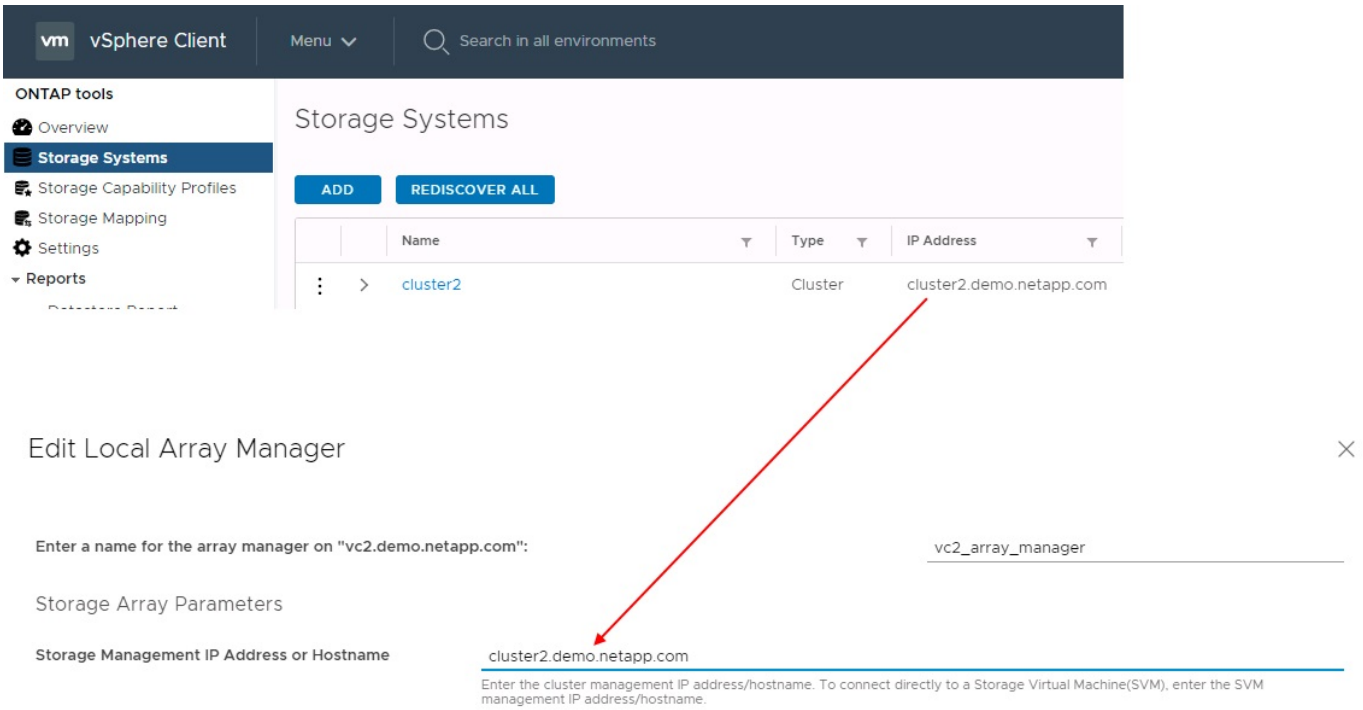
```
snap autodelete modify -volume -commitment try
```

- SAN 데이터 저장소가 포함된 볼륨 및 NFS 데이터 저장소에 대해 `grow_shrink` 볼륨 자동 크기 조정을 로 `grow` 설정해야 합니다. 이 주제에 대한 자세한 내용은 을 "크기를 자동으로 확대 및 축소하도록 볼륨을 구성합니다 "참조하십시오.
- SRM은 데이터 저장소 수를 최소화하여 복구 계획에서 보호 그룹을 최소화할 때 가장 잘 작동합니다. 따라서 RTO가 중요한 SRM 보호 환경에서 VM 밀도 최적화를 고려해야 합니다.
- DRS(Distributed Resource Scheduler)를 사용하여 보호 및 복구 ESXi 클러스터의 로드 균형을 조정합니다. 페일백을 계획하는 경우 재보호 를 실행하면 이전에 보호된 클러스터가 새 복구 클러스터가 됩니다. DRS는 양방향으로 진행되는 배치의 균형을 유지하는 데 도움이 됩니다.
- 가능하면 SRM에서 IP 사용자 지정을 사용하지 마십시오. 이렇게 하면 RTO가 증가할 수 있습니다.

스토리지 쌍 정보

각 스토리지 쌍에 대해 스토리지 관리자가 생성됩니다. SRM 및 ONTAP 툴을 사용하면 클러스터 자격 증명을 사용해도 SVM의 범위에서 각 어레이 페어링을 수행할 수 있습니다. 따라서 각 테넌트가 관리하기 위해 할당된 SVM에 따라 테넌트 간에 DR 워크플로우를 분할할 수 있습니다. 특정 클러스터에 대해 여러 어레이 관리자를 생성할 수 있으며 비대칭적일 수 있습니다. 서로 다른 ONTAP 9 클러스터 간에 팬아웃 또는 팬할 수 있습니다. 예를 들어, 클러스터 1의 SVM-A 및 SVM-B를 클러스터 2의 SVM-C, 클러스터 3의 SVM-D 또는 그 반대로 복제할 수 있습니다.

SRM에서 어레이 쌍을 구성할 때는 항상 ONTAP 툴에 추가한 것과 같은 방법으로 SRM에 어레이 쌍을 추가해야 합니다. 즉, 이들은 동일한 사용자 이름, 암호 및 관리 LIF를 사용해야 합니다. 이 요구 사항은 SRA가 어레이와 제대로 통신하도록 보장합니다. 다음 스크린샷은 ONTAP 툴에 클러스터가 표시되는 방식과 이를 어레이 관리자에 추가하는 방법을 보여 줍니다.



복제 그룹 정보

복제 그룹에는 함께 복구되는 가상 머신의 논리적 컬렉션이 포함됩니다. ONTAP SnapMirror 복제는 볼륨 레벨에서 수행되기 때문에 볼륨의 모든 VM이 동일한 복제 그룹에 속해 있습니다.

복제 그룹과 FlexVol 볼륨 간에 VM을 배포하는 방법은 여러 가지 요소를 고려해야 합니다. 동일한 볼륨에서 유사한 VM을 그룹화하면 집계 수준 중복 제거 기능이 없는 기존 ONTAP 시스템에서 스토리지 효율성이 향상될 수 있지만 그룹화하면 볼륨 크기가 증가하고 볼륨 I/O 동시성이 줄어듭니다. 최신 ONTAP 시스템에서는 동일한 애그리게이트의 FlexVol 볼륨에 VM을 분산하여 애그리게이트 레벨 중복제거를 활용하고 여러 볼륨에서 더 많은 I/O 병렬화를 수행하여 성능과 스토리지 효율성의 균형을 최적으로 유지할 수 있습니다. 아래에 설명된 보호 그룹에 여러 복제 그룹이 포함될 수 있으므로 볼륨에서 VM을 함께 복구할 수 있습니다. 이 레이아웃의 단점은 SnapMirror가 애그리게이트 중복제거 기능을 고려하지 않기 때문에 블록을 유선으로 여러 번 전송할 수 있다는 것입니다.

복제 그룹에 대한 마지막 고려 사항은 각 그룹이 기본적으로 논리적 정합성 보장 그룹이라는 점입니다(SRM 정합성 보장 그룹과 혼동하지 마십시오). 볼륨의 모든 VM이 동일한 스냅샷을 사용하여 함께 전송되기 때문입니다. 따라서 VM이 서로 일치해야 하는 경우 동일한 FlexVol에 VM을 저장하는 것이 좋습니다.

보호 그룹 정보

보호 그룹은 보호 사이트에서 함께 복구되는 그룹으로 VM 및 데이터 저장소를 정의합니다. 보호 사이트는 정상적인 정상 상태 작업 중에 보호 그룹에 구성된 VM이 존재하는 곳입니다. SRM이 보호 그룹에 대해 여러 스토리지 관리자를 표시할 수 있지만 보호 그룹은 여러 스토리지 관리자를 포괄할 수 없습니다. 따라서 서로 다른 SVM의 데이터 저장소에 VM 파일을 확장해서는 안 됩니다.

복구 계획에 대해 설명합니다

복구 계획은 동일한 프로세스에서 복구할 보호 그룹을 정의합니다. 동일한 복구 계획에서 여러 보호 그룹을 구성할 수 있습니다. 또한 복구 계획 실행을 위한 추가 옵션을 사용하기 위해 단일 보호 그룹을 여러 복구 계획에 포함할 수 있습니다.

복구 계획을 사용하면 SRM 관리자가 우선 순위 그룹에 VM을 1(가장 높음)에서 5(가장 낮음)까지 할당하고 3(중간)을

기본값으로 지정하여 복구 워크플로를 정의할 수 있습니다. 우선 순위 그룹 내에서 VM을 종속성에 맞게 구성할 수 있습니다.

예를 들어, 데이터베이스에 Microsoft SQL Server를 사용하는 계층 1 비즈니스 크리티컬 애플리케이션을 가질 수 있습니다. 따라서 우선 순위 그룹 1에 VM을 배치하기로 결정합니다. 우선 순위 그룹 1 내에서 서비스를 가져오기 위한 주문 계획을 시작합니다. Microsoft Windows 도메인 컨트롤러를 Microsoft SQL Server보다 먼저 부팅하고, 응용 프로그램 서버보다 먼저 온라인 상태여야 하는 경우가 있습니다. 이러한 모든 VM을 우선 순위 그룹에 추가한 다음 종속성이 지정된 우선 순위 그룹 내에서만 적용되기 때문에 종속성을 설정합니다.

NetApp은 애플리케이션 팀과 협력하여 페일오버 시나리오에 필요한 운영 순서를 파악하고 그에 따라 복구 계획을 수립하는 것이 좋습니다.

테스트 대체 작동

가장 좋은 방법은 보호된 VM 스토리지의 구성이 변경될 때마다 항상 테스트 대체 작동을 수행하는 것입니다. 이렇게 하면 재해 발생 시 Site Recovery Manager가 예상 RTO 목표 내에서 서비스를 복구할 수 있다는 것을 신뢰할 수 있습니다.

또한, 특히 VM 스토리지를 재구성한 후에는 게스트 내 애플리케이션 기능을 확인하는 것이 좋습니다.

테스트 복구 작업이 수행되면 VM에 대한 전용 테스트 버블 네트워크가 ESXi 호스트에 생성됩니다. 그러나 이 네트워크는 물리적 네트워크 어댑터에 자동으로 연결되지 않으므로 ESXi 호스트 간에 연결을 제공하지 않습니다. DR 테스트 중에 서로 다른 ESXi 호스트에서 실행 중인 VM 간의 통신을 허용하기 위해 DR 사이트의 ESXi 호스트 간에 물리적 전용 네트워크가 생성됩니다. 테스트 네트워크가 전용인지 확인하기 위해 테스트 버블 네트워크를 물리적으로 또는 VLAN 또는 VLAN 태깅을 사용하여 분리할 수 있습니다. VM이 복구될 때 실제 운영 시스템과 충돌할 수 있는 IP 주소를 사용하여 운영 네트워크에 배치할 수 없으므로 이 네트워크를 운영 네트워크와 분리해야 합니다. SRM에서 복구 계획을 생성할 때 생성된 테스트 네트워크를 테스트 중에 VM을 연결할 전용 네트워크로 선택할 수 있습니다.

테스트를 검증하고 더 이상 필요하지 않은 후에는 정리 작업을 수행합니다. 정리 작업을 실행하면 보호된 VM이 초기 상태로 돌아가고 복구 계획이 준비 상태로 재설정됩니다.

페일오버 고려 사항

이 가이드에 언급된 작업 순서 외에 사이트 장애 조치 시 몇 가지 다른 고려 사항이 있습니다.

사이트 간 네트워크 차이는 문제가 될 수 있습니다. 일부 환경에서는 운영 사이트와 DR 사이트 모두에서 동일한 네트워크 IP 주소를 사용할 수 있습니다. 이러한 기능을 확장 가상 LAN(VLAN) 또는 확장 네트워크 설정이라고 합니다. 다른 환경에서는 DR 사이트와 관련하여 운영 사이트에서 서로 다른 네트워크 IP 주소(예: VLAN)를 사용해야 할 수 있습니다.

VMware는 이 문제를 해결할 수 있는 여러 가지 방법을 제공합니다. VMware NSX-T Data Center와 같은 네트워크 가상화 기술은 운영 환경의 계층 2에서 계층 7까지 전체 네트워킹 스택을 추상화하여 보다 휴대성이 뛰어난 솔루션을 제공합니다. 에 대해 자세히 알아보십시오 "SRM의 NSX-T 옵션".

또한 SRM은 VM이 복구될 때 VM의 네트워크 구성을 변경할 수 있는 기능을 제공합니다. 이러한 재구성에는 IP 주소, 게이트웨이 주소 및 DNS 서버 설정과 같은 설정이 포함됩니다. 개별 VM이 복구될 때 개별 VM에 적용되는 다양한 네트워크 설정은 복구 계획에서 VM의 속성 설정에서 지정할 수 있습니다.

복구 계획에서 각 VM의 속성을 편집하지 않고도 여러 VM에 서로 다른 네트워크 설정을 적용하도록 SRM을 구성하려면 VMware에서 DR-IP-customizer라는 도구를 제공합니다. 이 유틸리티를 사용하는 방법은 을 참조하십시오 "VMware 설명서".

재보호

복구 후에는 복구 사이트가 새 운영 사이트가 됩니다. 복구 작업이 SnapMirror 복제를 중단했기 때문에 새 프로덕션 사이트는 이후의 재해로부터 보호되지 않습니다. 모범 사례는 복구 후 즉시 새 프로덕션 사이트를 다른 사이트로 보호하는 것입니다. 원래 운영 사이트가 작동 중인 경우 VMware 관리자는 원래 운영 사이트를 새 복구 사이트로 사용하여 새 운영 사이트를 보호할 수 있으므로 보호 방향을 효과적으로 바꿀 수 있습니다. 재보호는 비치명적인 오류에서만 사용할 수 있습니다. 따라서 원래 vCenter Server, ESXi Server, SRM Server 및 해당 데이터베이스를 최종적으로 복구할 수 있어야 합니다. 사용할 수 없는 경우 새 보호 그룹과 새 복구 계획을 생성해야 합니다.

장애 복구

장애 복구 작업은 기본적으로 이전과 다른 방식으로 장애 조치입니다. 모범 사례로서, 원래 사이트가 장애 복구를 시도하기 전에 허용 가능한 수준의 기능으로 복구되었는지 또는 다시 말해 원래 사이트로 장애 조치를 수행하는 것이 좋습니다. 원래 사이트가 여전히 손상된 경우 장애가 충분히 해결될 때까지 페일백을 지연해야 합니다.

또 다른 장애 복구 모범 사례는 재보호 완료 후 그리고 최종 장애 복구를 수행하기 전에 항상 테스트 장애 조치를 수행하는 것입니다. 이렇게 하면 원래 사이트에 있는 시스템이 작업을 완료할 수 있는지 확인합니다.

원래 사이트를 다시 보호합니다

장애 복구 후 다시 보호 기능을 실행하기 전에 모든 이해 관계자에게 서비스가 정상으로 돌아왔는지 확인해야 합니다.

페일백 후 재보호를 실행하면 기본적으로 환경이 원래 상태로 전환되며, 이때 SnapMirror 복제가 운영 사이트에서 복구 사이트로 다시 실행됩니다.

복제 토폴로지

ONTAP 9에서는 클러스터의 물리적 구성 요소가 클러스터 관리자에게 표시되지만 클러스터를 사용하는 애플리케이션과 호스트에는 직접 표시되지 않습니다. 물리적 구성 요소는 논리적 클러스터 리소스가 구성되는 공유 리소스 풀을 제공합니다. 애플리케이션과 호스트는 볼륨 및 LIF가 포함된 SVM을 통해서만 데이터에 액세스합니다.

각 NetApp SVM은 Site Recovery Manager에서 고유한 어레이로 처리됩니다. VLSR은 특정 어레이 간(또는 SVM 간) 복제 레이아웃을 지원합니다.

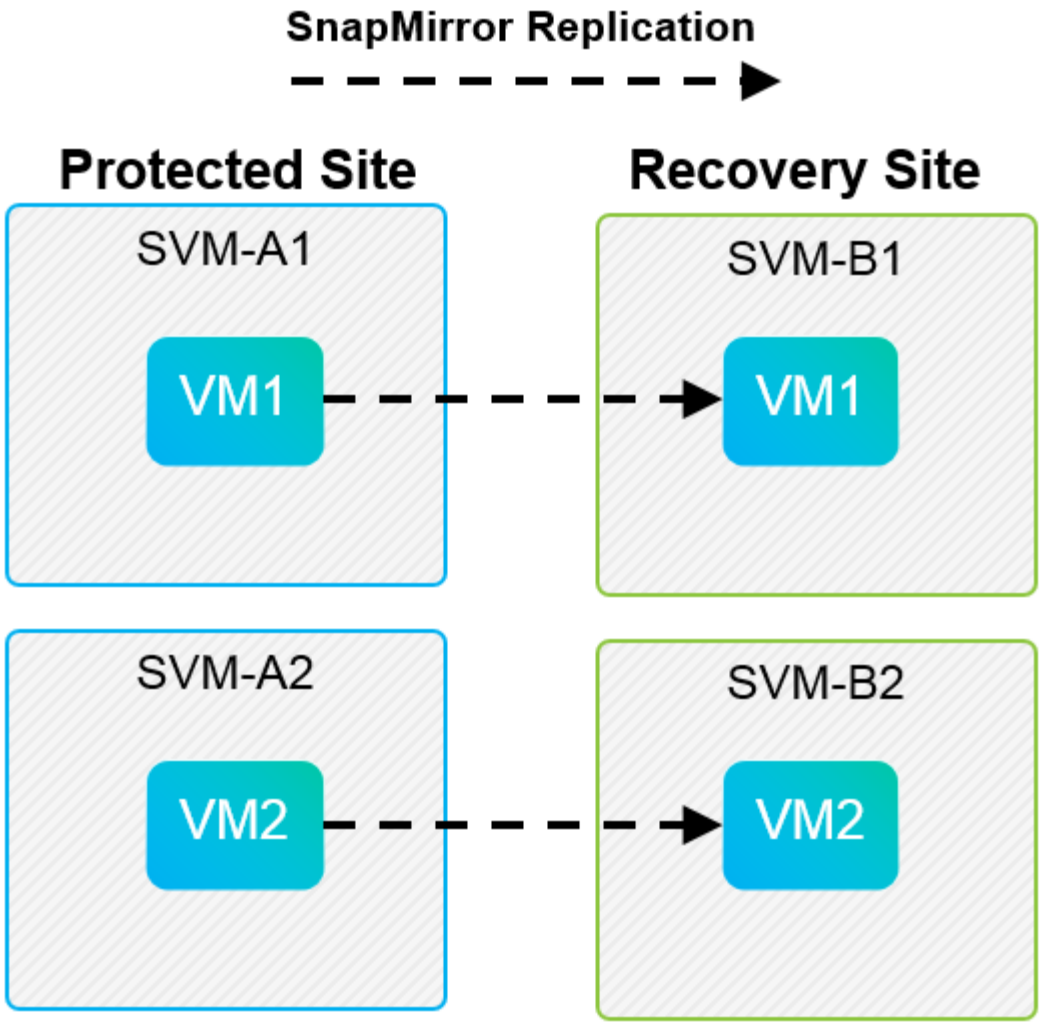
단일 VM은 VMDK(Virtual Machine Disk) 또는 RDM 같은 데이터를 소유할 수 없습니다. 이러한 데이터를 여러 VLSR 스토리지에서 소유할 수 없는 이유는 다음과 같습니다.

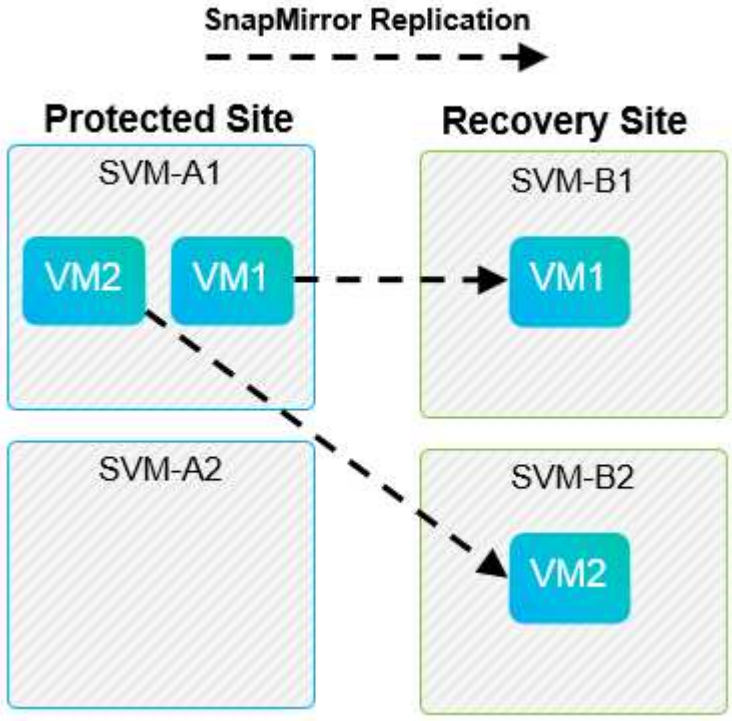
- VLSR에는 개별 물리적 컨트롤러가 아닌 SVM만 표시됩니다.
- SVM은 하나의 클러스터에서 여러 노드에 걸쳐 있는 LUN 및 볼륨을 제어할 수 있습니다.

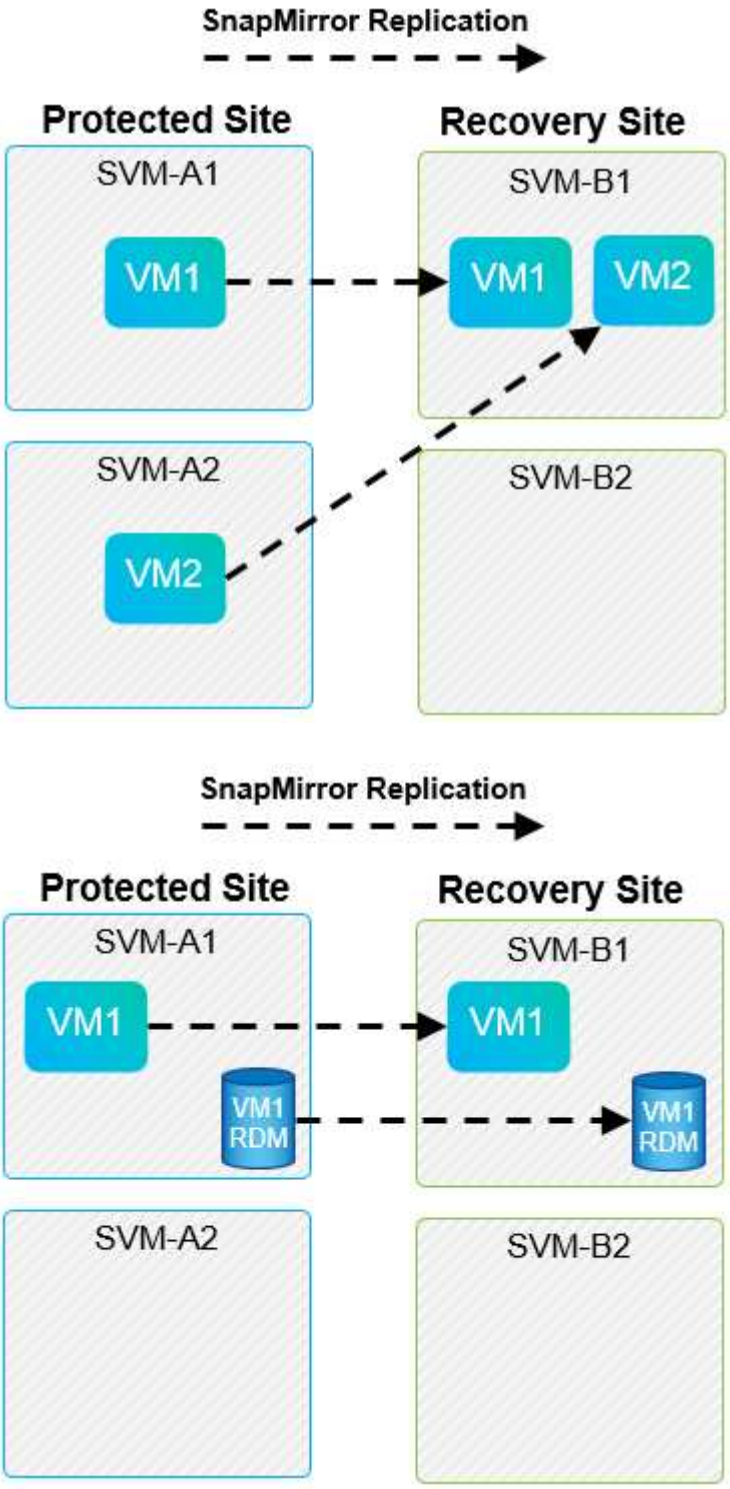
모범 사례
지원 가능성을 확인하려면 이 규칙을 염두에 두십시오. VLSR 및 NetApp SRA를 사용하여 VM을 보호하려면 VM의 모든 부분이 하나의 SVM에만 존재해야 합니다. 이 규칙은 보호 사이트와 복구 사이트 모두에 적용됩니다.

지원되는 **SnapMirror** 레이아웃

다음 그림은 VLSR 및 SRA에서 지원하는 SnapMirror 관계 레이아웃 시나리오를 보여 줍니다. 복제된 볼륨의 각 VM은 각 사이트의 한 VLSR 어레이(SVM)에만 데이터를 소유합니다.


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2



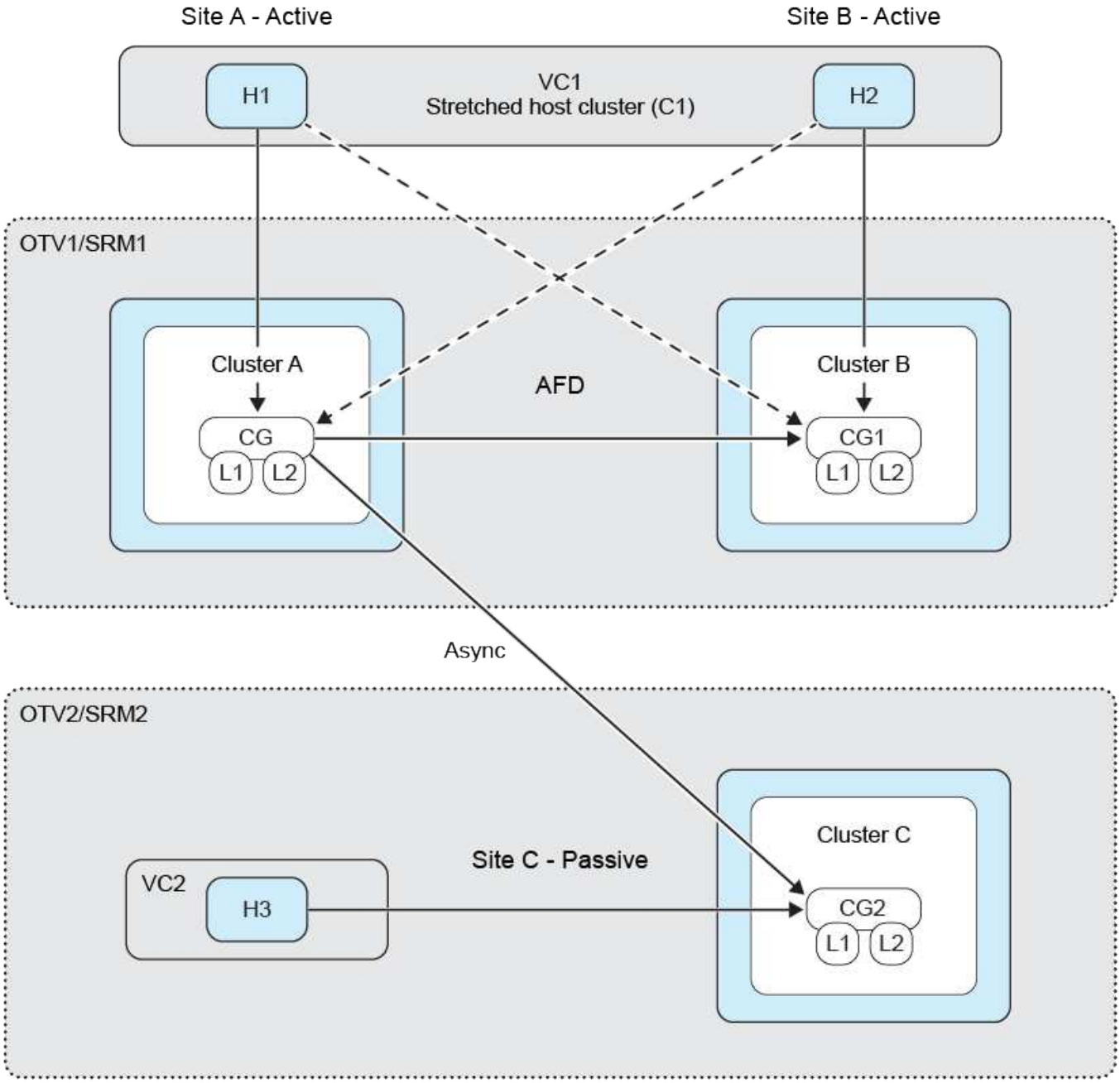
SnapMirror Active Sync를 통한 **VMFS** 지원

ONTAP 도구 10.3 이상에서는 SnapMirror Active Sync(SMas)를 사용하여 VMFS 데이터 저장소를 보호하는 기능도 지원합니다. 이를 통해 비교적 가까이 있는 두 데이터 센터(장애 도메인이라고 함) 간의 비즈니스 연속성을 위한 투명한 장애 조치가 가능해집니다. ONTAP 도구 SRA와 VLSR을 통해 SnapMirror 비동기를 사용하여 장거리 재해 복구를 조율할 수 있습니다.

"ONTAP SnapMirror Active Sync에 대해 알아보세요"

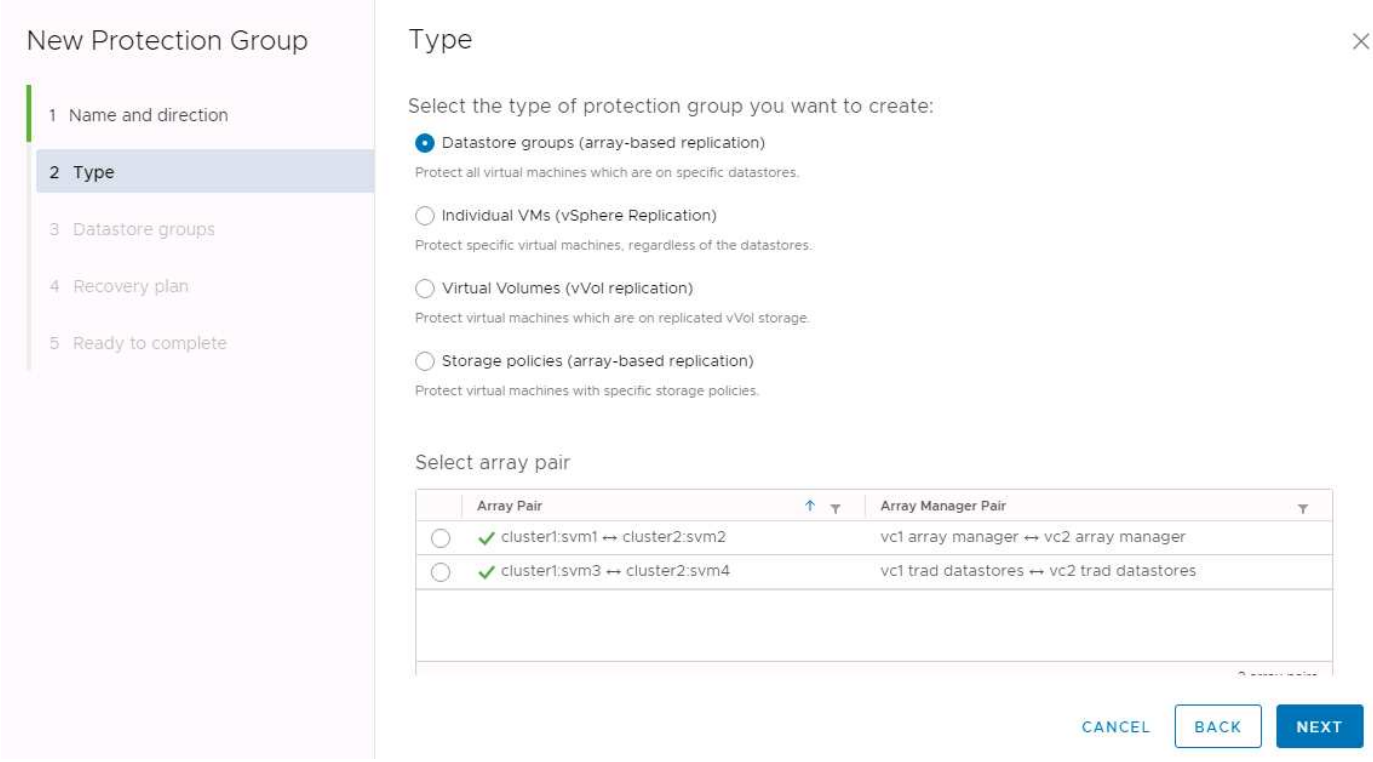
데이터 저장소는 일관성 그룹(CG)에 함께 수집되며, 모든 데이터 저장소의 VM은 모두 동일한 CG의 멤버로서 쓰기 순서 일관성을 유지합니다.

예를 들어 베를린과 함부르크의 사이트를 SMas로 보호하고, 세 번째 사이트 복제본을 비동기 SnapMirror 사용하고 VLSR로 보호하는 것이 있습니다. 또 다른 예로는 SMa를 사용하여 뉴욕과 뉴저지의 사이트를 보호하고, 세 번째 사이트는 시카고에 두는 것이 있습니다.



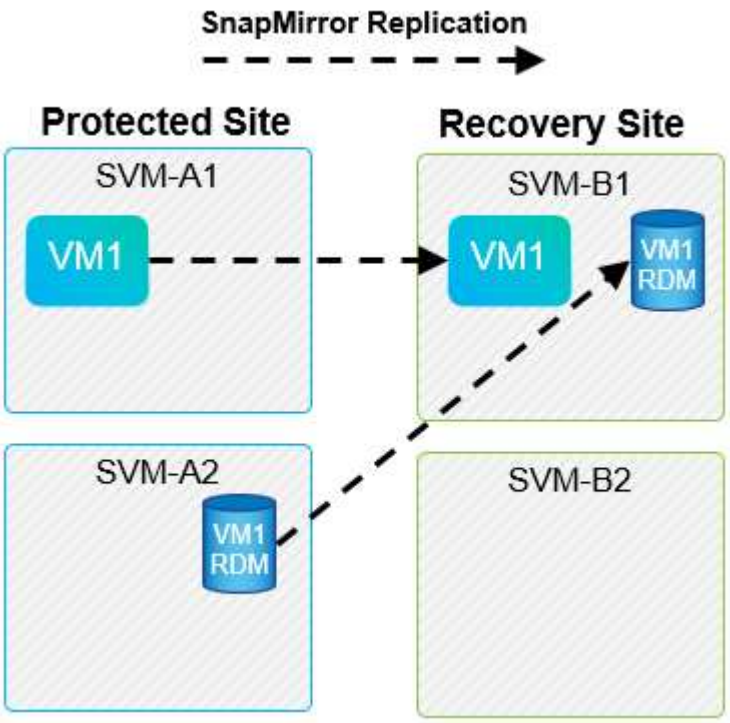
지원되는 **Array Manager** 레이아웃입니다

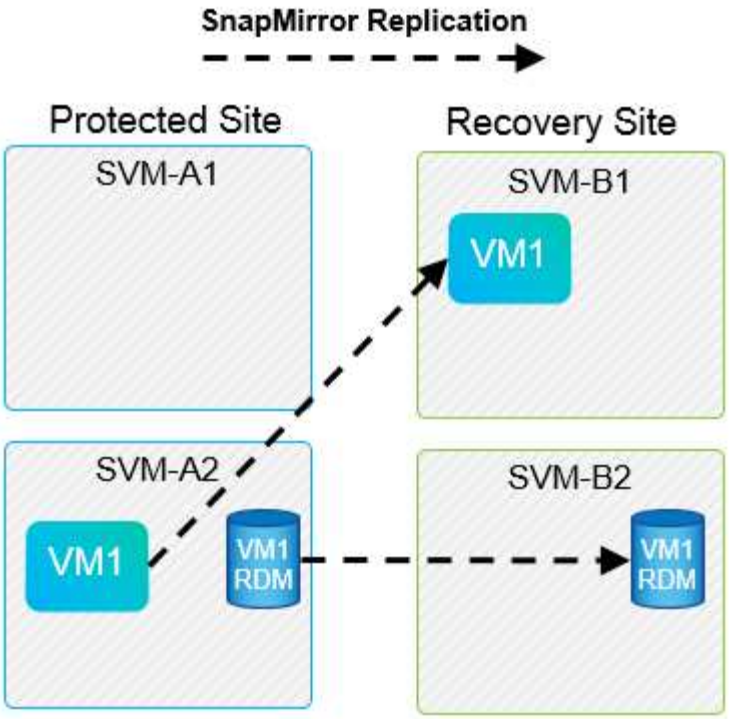
VLSR에서 ABR(스토리지 기반 복제)을 사용하면 다음 스크린샷과 같이 보호 그룹이 단일 스토리지 쌍으로 격리됩니다. 이 시나리오에서는 `SVM1` 및 가 `SVM2` `SVM4` 복구 사이트에서 피어링됩니다. `SVM3` 그러나 보호 그룹을 생성할 때는 두 스토리지 쌍 중 하나만 선택할 수 있습니다.



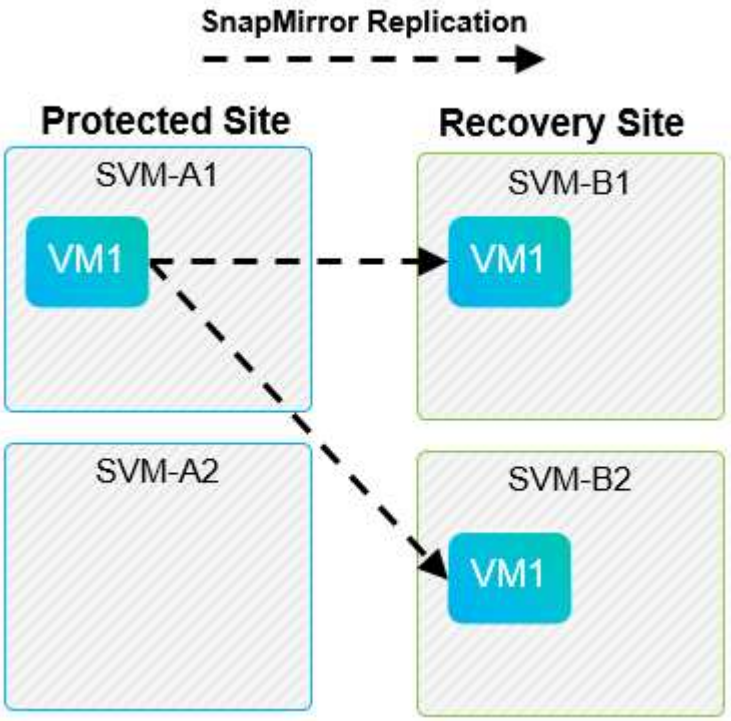
지원되지 않는 레이아웃입니다

지원되지 않는 구성에는 개별 VM이 소유하는 여러 SVM에 데이터(VMDK 또는 RDM)가 있습니다. 다음 그림에 표시된 예에서는 에서 `VM1` 두 개의 SVM에 데이터가 있기 때문에 VLSR을 사용하여 보호하도록 구성할 수 없습니다. `VM1`



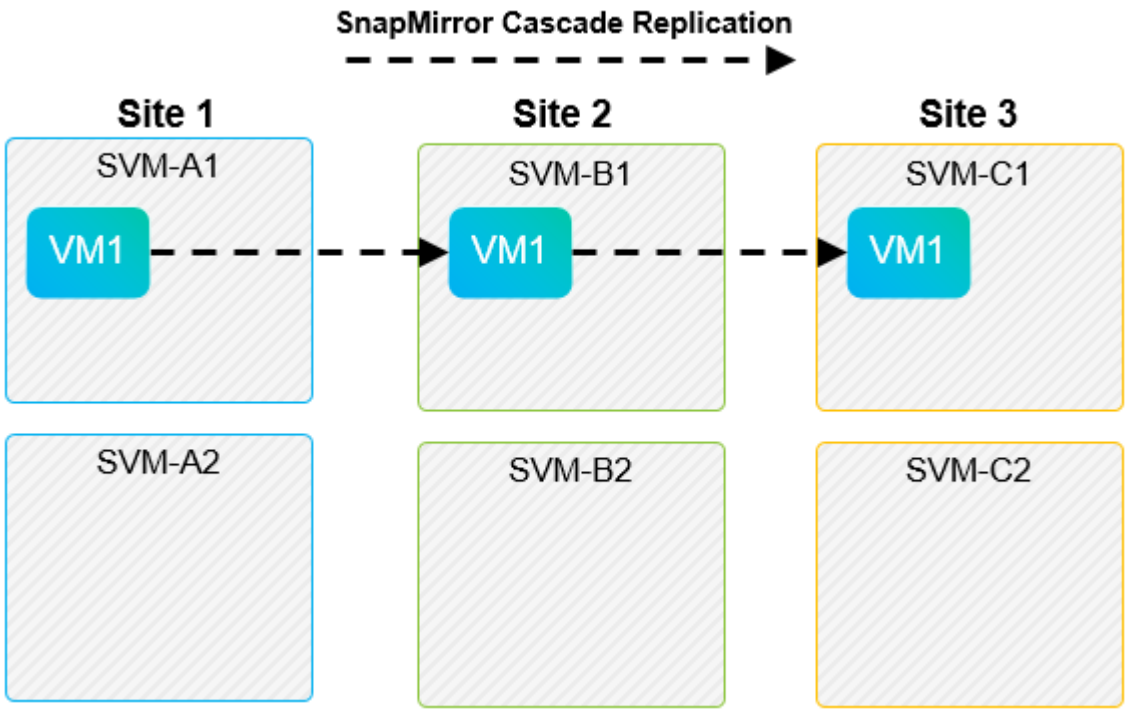


개별 NetApp 볼륨이 하나의 소스 SVM에서 동일한 SVM의 여러 대상 또는 서로 다른 SVM에 복제된 모든 복제 관계를 SnapMirror 팬아웃(fan-out)이라고 합니다. VLSR에서는 팬아웃이 지원되지 않습니다. 다음 그림에 표시된 예에서는 SnapMirror를 사용하여 서로 다른 두 위치에 복제되므로 VLSR에서 보호를 위해 을 `VM1` 구성할 수 없습니다.



SnapMirror 계단식 배열

VLSR은 소스 볼륨이 타겟 볼륨에 복제되고 해당 타겟 볼륨도 SnapMirror를 통해 다른 타겟 볼륨으로 복제되는 SnapMirror 관계의 다중 구간 기능을 지원하지 않습니다. 다음 그림에 표시된 시나리오에서는 사이트 간 장애 조치에 VLSR을 사용할 수 없습니다.



SnapMirror 및 **SnapVault**

NetApp SnapVault 소프트웨어를 사용하면 NetApp 스토리지 시스템 간에 엔터프라이즈 데이터를 디스크 기반으로 백업할 수 있습니다. SnapVault와 SnapMirror는 동일한 환경에 공존할 수 있지만 VLSR은 SnapMirror 관계의 페일오버만 지원합니다.

NetApp SRA는 를 지원합니다 `mirror-vault` 정책 유형.

SnapVault는 처음부터 ONTAP 8.2를 위해 재구축되었습니다. 이전 Data ONTAP 7-Mode 사용자에게도 유사한 점이 있긴 하지만, 이 버전의 SnapVault에서는 여러 가지 기능이 크게 향상되었습니다. 한 가지 중요한 발전은 SnapVault 전송 중에 운영 데이터의 스토리지 효율성을 유지할 수 있는 기능입니다.

중요한 아키텍처 변화는 ONTAP 9의 SnapVault가 7-Mode SnapVault와 마찬가지로 qtree 레벨이 아닌 볼륨 레벨에서 복제된다는 점입니다. 이 설정은 SnapVault 관계의 소스가 볼륨이어야 하며 해당 볼륨이 SnapVault 보조 시스템의 자체 볼륨으로 복제되어야 함을 의미합니다.

SnapVault가 사용되는 환경에서는 특히 이름이 지정된 스냅샷이 운영 스토리지 시스템에 생성됩니다. 구축된 구성에 따라 SnapVault 스케줄이나 NetApp Active IQ Unified Manager 같은 애플리케이션을 통해 운영 시스템에 명명된 스냅샷을 생성할 수 있습니다. 그런 다음 기본 시스템에서 생성된 명명된 스냅샷이 SnapMirror 대상에 복제되고 이 스냅샷에서 SnapVault 대상에 볼트가 됩니다.

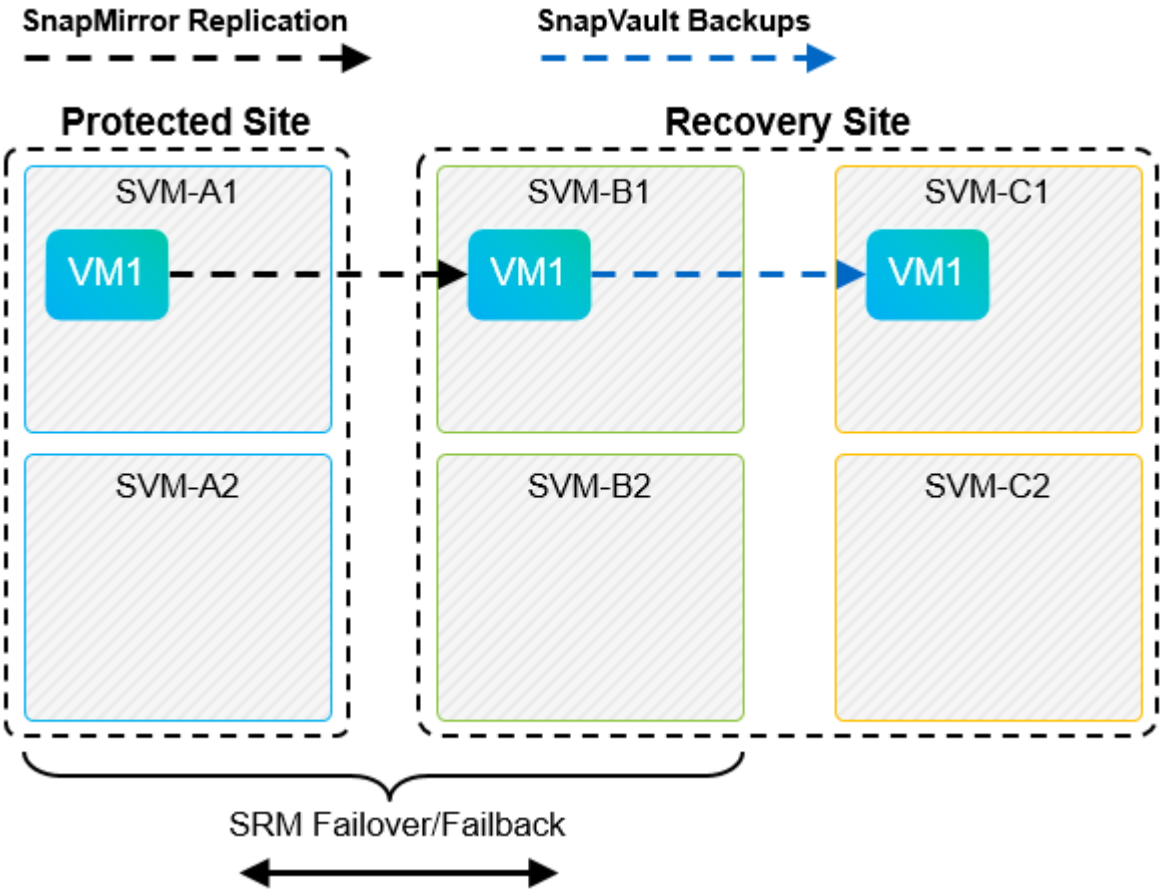
소스 볼륨은 DR 사이트의 SnapMirror 대상에 복제되는 계단식 구성으로 생성할 수 있으며, 이 구성에서는 볼륨을 SnapVault 타겟에 저장할 수 있습니다. 한 대상이 SnapMirror 대상이고 다른 대상이 SnapVault 대상인 팬아웃 관계에 소스 볼륨을 생성할 수도 있습니다. 그러나 VLSR 페일오버 또는 복제 반전이 발생할 경우 SnapMirror 대상 볼륨을 볼트의 소스로 사용하도록 SRA는 SnapVault 관계를 자동으로 재구성하지 않습니다.

ONTAP 9용 SnapMirror 및 SnapVault 에 대한 최신 정보는 다음을 참조하십시오. "ONTAP 9용 TR-4015 SnapMirror 구성 모범 사례 가이드."

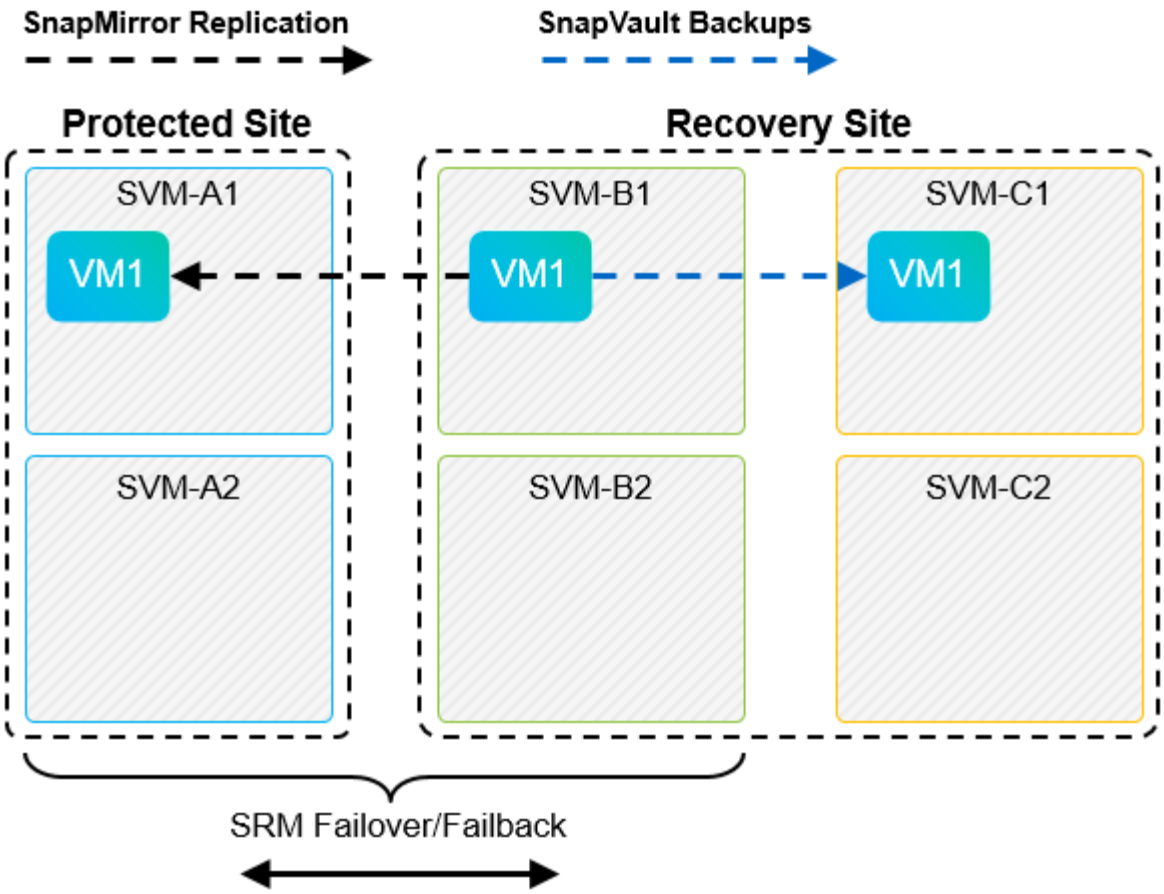
모범 사례
SnapVault 및 VLSR이 동일한 환경에서 사용되는 경우 SnapVault 백업이 일반적으로 DR 사이트의 SnapMirror 대상에서 수행되는 SnapMirror와 SnapVault 다중 구간 구성을 사용하는 것이 좋습니다. 재해가 발생할 경우 이 구성을 사용하면 운영 사이트에 액세스할 수 없습니다. 복구 사이트에서 SnapVault 대상을 유지하면 복구 사이트에서 운영 중인 동안 SnapVault 백업을 계속할 수 있도록 장애 조치 후 SnapVault 백업을 재구성할 수 있습니다.

VMware 환경에서 각 데이터 저장소에는 UUID(Universal Unique Identifier)가 있으며 각 VM에는 고유한 MOID(Managed Object ID)가 있습니다. 이러한 ID는 장애 조치 또는 장애 복구 중에 VLSR에 의해 유지되지 않습니다. 데이터 저장소 UUID 및 VM MOID는 VLSR에서 페일오버 중에 유지되지 않으므로 이러한 ID에 의존하는 모든 애플리케이션은 VLSR 페일오버 후에 재구성해야 합니다. 애플리케이션의 예로는 SnapVault 복제를 vSphere 환경과 조정하는 NetApp Active IQ Unified Manager가 있습니다.

다음 그림은 SnapVault 계단식으로 구성된 SnapMirror를 보여 줍니다. SnapVault 대상이 DR 사이트 또는 운영 사이트의 운영 중단으로 인해 영향을 받지 않는 3차 사이트에 있는 경우, 페일오버 후 백업을 계속할 수 있도록 환경을 재구성할 수 있습니다.



다음 그림에서는 VLSR을 사용하여 SnapMirror 복제를 기본 사이트로 되돌린 후의 구성을 보여 줍니다. 또한 SnapVault 백업이 현재 SnapMirror 소스에서 발생하도록 환경이 재구성되었습니다. 이 설정은 SnapMirror SnapVault 팬아웃 구성입니다.



vsrm이 페일백을 수행하고 SnapMirror 관계의 두 번째 반전을 수행한 후 운영 데이터가 운영 사이트에 다시 배치됩니다. 이 데이터는 SnapMirror 및 SnapVault 백업을 통해 DR 사이트로 페일오버 전의 방식과 동일하게 보호됩니다.

Site Recovery Manager 환경에서 **Qtree** 사용

qtree는 NAS에 대한 파일 시스템 할당량을 적용할 수 있는 특수 디렉토리입니다. ONTAP 9에서는 qtree를 생성할 수 있으며 qtree는 SnapMirror로 복제된 볼륨에 존재할 수 있습니다. 그러나 SnapMirror에서는 개별 qtree 또는 qtree 레벨 복제의 복제를 허용하지 않습니다. 모든 SnapMirror 복제는 볼륨 레벨에만 있습니다. 이러한 이유로 VLSR에서는 qtree를 사용하지 않는 것이 좋습니다.

FC 및 **iSCSI** 혼합 환경

지원되는 SAN 프로토콜(FC, FCoE 및 iSCSI)을 통해 ONTAP 9는 LUN 서비스를 제공합니다. 즉, LUN을 생성하여 연결된 호스트에 매핑할 수 있습니다. 클러스터는 여러 컨트롤러로 구성되며, 개별 LUN에 대한 다중 경로 I/O를 통해 관리되는 여러 논리적 경로가 있습니다. 호스트에서 ALUA(Asymmetric Logical Unit Access)가 사용되므로 LUN에 대한 최적화된 경로가 선택되고 데이터 전송을 위해 활성화됩니다. LUN에 대한 최적화된 경로(예: 포함된 볼륨이 이동됨)가 변경되면 ONTAP 9가 자동으로 해당 변경 사항을 인식하고 중단 없이 조정합니다. 최적화된 경로를 사용할 수 없게 되면 ONTAP는 무중단으로 다른 사용 가능한 경로로 전환할 수 있습니다.

VMware VLSR 및 NetApp SRA는 한 사이트에서 FC 프로토콜을 사용하고 다른 사이트에서는 iSCSI 프로토콜을 사용할 수 있도록 지원합니다. 하지만 동일한 ESXi 호스트 또는 동일한 클러스터의 다른 호스트에 FC 연결 데이터 저장소와 iSCSI 연결 데이터 저장소를 함께 사용할 수는 없습니다. VLSR 페일오버 또는 테스트 페일오버 중에 VLSR은 요청에 따라 ESXi 호스트의 모든 FC 및 iSCSI 이니시에이터를 포함하므로 VLSR에서는 이 구성이 지원되지 않습니다.

모범 사례
VLSR 및 SRA는 보호 사이트와 복구 사이트 간에 혼합 FC 및 iSCSI 프로토콜을 지원합니다. 그러나 각 사이트는 동일한 사이트에서 두 프로토콜을 모두 구성하지 않고 FC 또는 iSCSI 프로토콜을 하나만 사용하여 구성해야 합니다. FC와 iSCSI 프로토콜을 동일한 사이트에 모두 구성해야 하는 경우 일부 호스트는 iSCSI를 사용하고 다른 호스트는 FC를 사용하는 것이 좋습니다. 또한 이 경우에는 VM이 호스트 그룹 또는 다른 그룹으로 페일오버되도록 VLSR 리소스 매핑을 설정하는 것이 좋습니다.

VVol 복제를 사용할 때 VLSRM/SRM 문제 해결

ONTAP 도구 9.13P2를 사용할 때 SRA 및 기존 데이터 저장소와 함께 사용되는 VVol 복제를 사용할 때 VLSR과 SRM 내의 워크플로가 크게 달라집니다. 예를 들어, 어레이 관리자 개념은 없습니다. `discoverarrays`따라서 및 `discoverdevices` 명령은 표시되지 않습니다.

문제 해결 시 아래 나열된 새 워크플로를 이해하는 것이 좋습니다.

1. queryReplicationPeer: 두 오류 도메인 간의 복제 계약을 검색합니다.
2. queryFaultDomain: 오류 도메인 계층을 검색합니다.
3. queryReplicationGroup: 소스 또는 타겟 도메인에 있는 복제 그룹을 검색합니다.
4. SyncReplicationGroup: 소스와 대상 간의 데이터를 동기화합니다.
5. queryPointInTimeReplica: 타겟의 시점 복제본을 검색합니다.
6. testFailoverReplicationGroupStart: 테스트 대체 작동을 시작합니다.
7. testFailoverReplicationGroupStop: 테스트 대체 작동을 종료합니다.
8. PromoteReplicationGroup: 현재 테스트 중인 그룹을 프로덕션 환경으로 승격합니다.
9. prepareFailoverReplicationGroup: 재해 복구를 준비합니다.
10. failoverReplicationGroup: 재해 복구를 실행합니다.
11. reverseReplicateGroup: 역방향 복제를 시작합니다.
12. queryMatchingContainer: 지정된 정책으로 프로비저닝 요청을 충족할 수 있는 컨테이너(호스트 또는 복제 그룹과 함께)를 찾습니다.
13. queryResourceMetadata: VASA 공급자에서 모든 리소스의 메타데이터를 검색하며 리소스 사용률을 queryMatchingContainer 함수에 대한 응답으로 반환할 수 있습니다.

VVOL 복제 구성 시 가장 일반적인 오류는 SnapMirror 관계를 검색하지 못하는 것입니다. 이 문제는 볼륨 및 SnapMirror 관계가 ONTAP 도구 모음 외부에서 생성되기 때문에 발생합니다. 따라서 항상 SnapMirror 관계가 완전히 초기화되었는지, 그리고 복제된 VVol 데이터 저장소를 생성하기 전에 두 사이트의 ONTAP 도구에서 재검색을 실행하는 것이 좋습니다.

추가 정보

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- VMware vSphere 10.x용 ONTAP 툴 리소스
  "https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"
- VMware vSphere 9.x용 ONTAP 툴 리소스

"https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"

- TR-4597: ONTAP용 VMware vSphere
"https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- TR-4400: ONTAP를 포함한 VMware vSphere 가상 볼륨
"https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- ONTAP 9용 TR-4015 SnapMirror 구성 모범 사례 가이드
https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf
- VMware Live Site Recovery 설명서 "https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"

NetApp 지원 사이트의 를 "상호 운용성 매트릭스 툴(IMT)"통해 본 문서에 기술된 제품 및 기능 버전이 귀사의 환경에서 지원되는지 확인하십시오. NetApp IMT에는 NetApp이 지원하는 구성을 설계하는 데 사용할 수 있는 제품 구성요소 및 버전이 정의되어 있습니다. 구체적인 결과는 게시된 기술사양과 그에 따른 고객 설치 환경에 따라 달라집니다.

ONTAP이 포함된 vSphere Metro 스토리지 클러스터

ONTAP이 포함된 vSphere Metro 스토리지 클러스터

업계 최고 수준의 VMware vSphere 하이퍼바이저를 vMSC(vSphere Metro Storage Cluster)라고 하는 확장 클러스터로 구축할 수 있습니다.

vMSC 솔루션은 NetApp ® MetroCluster ™ 및 SnapMirror 액티브 동기화(이전의 SnapMirror Business Continuity 또는 SMBC) 모두에서 지원되며, 하나 이상의 장애가 발생한 도메인이 총 운영 중단을 겪을 경우 고급 비즈니스 연속성을 제공합니다. 다양한 실패 모드에 대한 복원력은 선택한 구성 옵션에 따라 다릅니다.

이 문서는 이전에 게시된 기술 보고서_TR-4128: NetApp MetroCluster_ 기반 vSphere를 대체합니다

vSphere 환경을 위한 무중단 가용성 솔루션

ONTAP 아키텍처는 데이터 저장소에 대한 SAN(FCP, iSCSI, NVMe-oF) 및 NAS(NFS v3 및 v4.1) 서비스를 제공하는 유연하고 확장 가능한 스토리지 플랫폼입니다. NetApp AFF, ASA 및 FAS 스토리지 시스템은 ONTAP 운영 체제를 사용하여 S3 및 SMB/CIFS와 같은 게스트 스토리지 액세스를 위한 추가 프로토콜을 제공합니다.

NetApp MetroCluster는 NetApp의 HA(컨트롤러 페일오버 또는 CFO) 기능을 사용하여 컨트롤러 장애로부터 보호합니다. 또한, 로컬 SyncMirror 기술, 재해 시 클러스터 페일오버(재해 또는 CFOD(Cluster Failover on Disaster), 하드웨어 이중화 및 지리적 분리를 통해 높은 수준의 가용성을 달성합니다. SyncMirror은 데이터를 두 플렉스에 기록하여 MetroCluster 구성의 두 부분에 걸쳐 동기식으로 데이터를 미러링합니다. 로컬 플렉스(로컬 쉘프에 있음)가 데이터를 능동적으로 제공하고 원격 플렉스(원격 쉘프에 있음)는 일반적으로 데이터를 제공하지 않음. 컨트롤러, 스토리지, 케이블, 스위치(패브릭 MetroCluster와 함께 사용), 어댑터와 같은 모든 MetroCluster 구성요소에 대해 하드웨어 이중화가 적용됩니다.

비 MetroCluster 시스템 및 ASA R2 시스템에서 사용 가능한 NetApp SnapMirror 액티브 동기화는 FCP 및 iSCSI SAN 프로토콜을 통해 데이터 저장소의 세부적인 보호 기능을 제공합니다. 전체 vMSC를 보호하거나 우선 순위가 높은 워크로드를 선택적으로 보호할 수 있습니다. Active-Standby 솔루션인 NetApp MetroCluster과 달리 로컬 및 원격 사이트에 대한 액티브-액티브 액세스를 제공합니다. ONTAP 9.15.1부터 SnapMirror 액티브 동기화는 대칭 액티브 /액티브 기능을 지원하여 양방향 동기식 복제를 통해 보호된 LUN의 두 복사본에서 읽기 및 쓰기 I/O 작업을 수행할 수 있으므로 두 LUN 복사본 모두 로컬에서 I/O 작업을 수행할 수 있습니다. ONTAP 9.15.1 이전의 SnapMirror 활성 동기화에서는 보조 사이트의 데이터가 LUN의 기본 복제본으로 프록시되는 비대칭 활성/활성 구성만 지원합니다.

두 사이트에 걸쳐 VMware HA/DRS 클러스터를 생성하기 위해 ESXi 호스트는 VCSA(vCenter Server Appliance)에 의해 사용되고 관리됩니다. vSphere 관리, vMotion ® 및 가상 머신 네트워크는 두 사이트 간에 중복 네트워크를 통해 연결됩니다. HA/DRS 클러스터를 관리하는 vCenter Server는 두 사이트의 ESXi 호스트에 연결할 수 있으며 vCenter HA를 사용하여 구성해야 합니다.

을 참조하십시오 "vSphere Client에서 클러스터를 생성하고 구성하는 방법" vCenter HA를 구성합니다.

또한 을 "VMware vSphere Metro Storage Cluster 권장 사례"참조하십시오.

vSphere Metro Storage Cluster란 무엇입니까**?**

vSphere Metro Storage Cluster(vMSC)는 가상 머신(VM)과 컨테이너를 장애로부터 보호하는 인증된 구성입니다. 이는 랙, 건물, 캠퍼스, 심지어 도시와 같은 다양한 장애 도메인에 분산된 ESXi 호스트 클러스터와 함께 확장 스토리지 개념을 사용하여 달성됩니다. NetApp MetroCluster 및 SnapMirror Active Sync 스토리지 기술은 호스트 클러스터에 RPO(복구 지점 목표)=0 보호를 제공하는 데 사용됩니다. vMSC 구성은 전체 물리적 또는 논리적 "사이트"에 장애가 발생하더라도 항상 데이터를 사용할 수 있도록 설계되었습니다. vMSC 구성의 일부인 저장 장치는 성공적인 vMSC 인증 프로세스를 거친 후 인증을 받아야 합니다. 지원되는 모든 저장 장치는 다음에서 찾을 수 있습니다. "VMware 스토리지 호환성 가이드 를 참조하십시오".

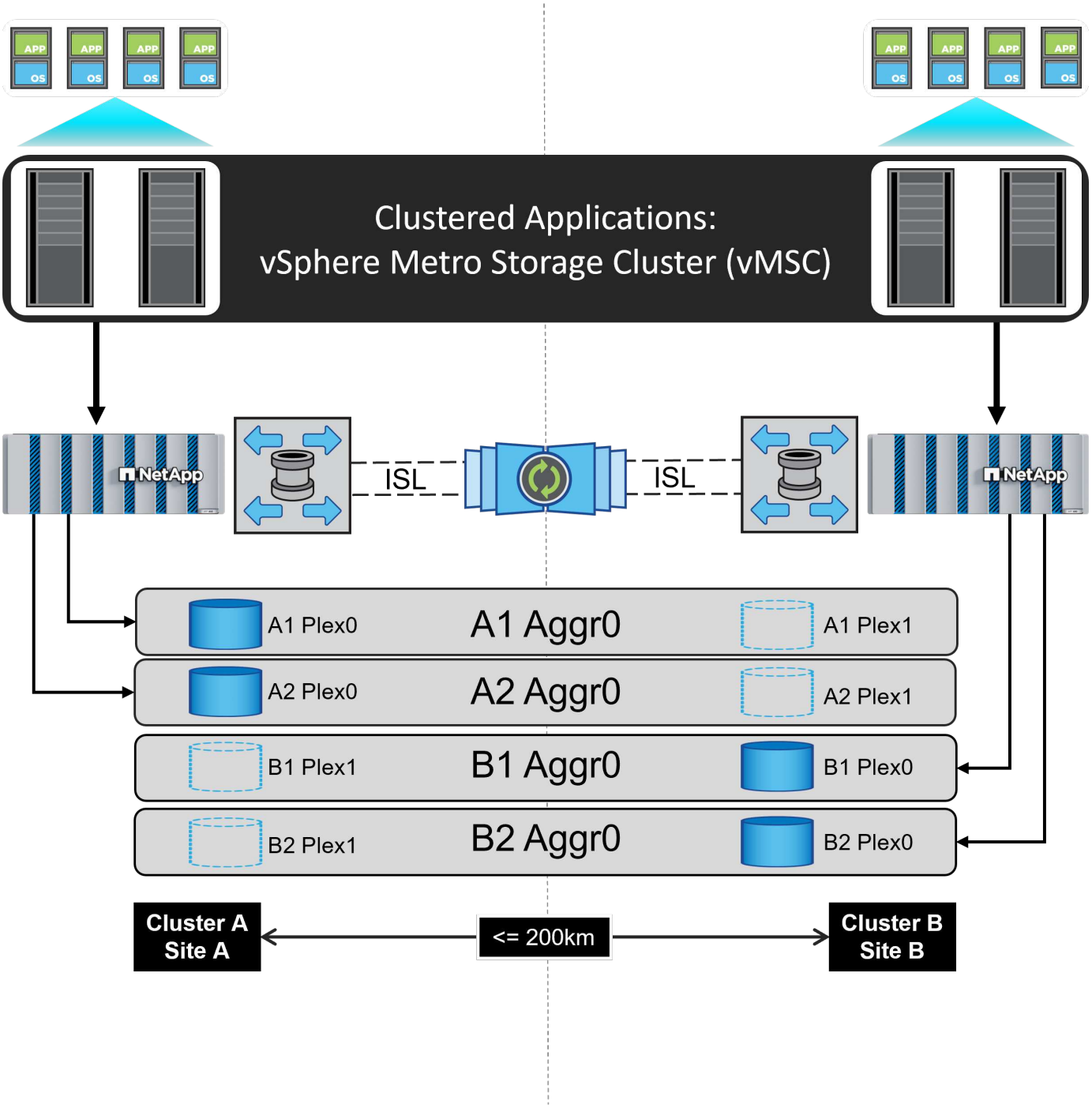
vSphere Metro Storage Cluster의 설계 지침에 대한 자세한 내용은 다음 설명서를 참조하십시오.

- "VMware vSphere는 NetApp MetroCluster를 지원합니다"
- "NetApp SnapMirror 비즈니스 연속성이 포함된 VMware vSphere 지원" (현재 SnapMirror Active Sync라고 함)

NetApp MetroCluster는 vSphere와 함께 사용할 수 있도록 두 가지 구성으로 구축할 수 있습니다.

- MetroCluster를 확장합니다
- Fabric MetroCluster의 약어입니다

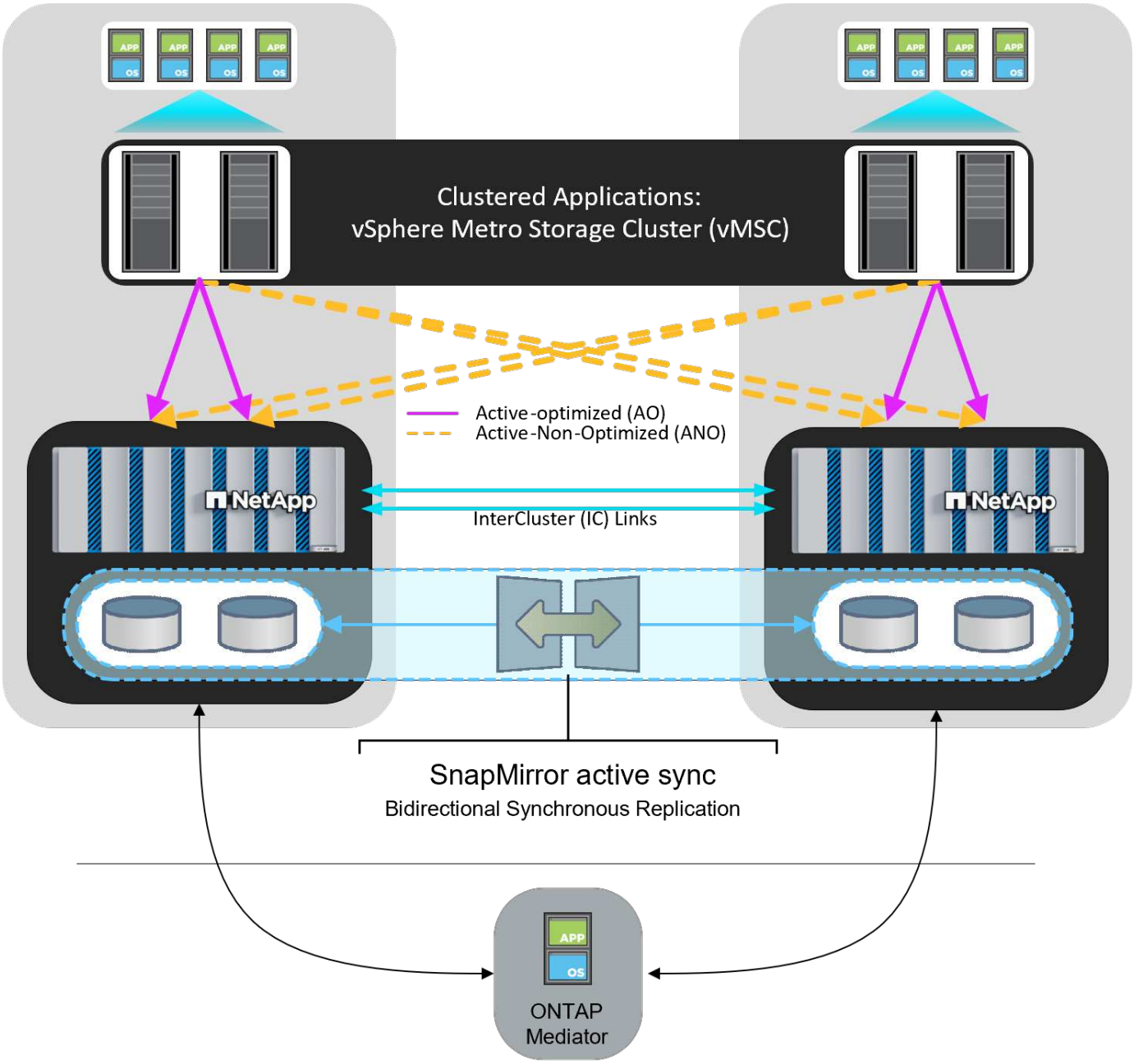
다음은 확장 MetroCluster의 상위 수준 토폴로지 다이어그램을 보여 줍니다.



을 참조하십시오 "MetroCluster 설명서" MetroCluster에 대한 구체적인 설계 및 구축 정보를 확인하십시오.

SnapMirror Active Sync는 두 가지 방법으로 배포할 수도 있습니다.

- 비대칭
- 대칭 액티브 동기화(ONTAP 9.15.1)



SnapMirror 액티브 동기화에 대한 구체적인 설계 및 구축 정보는 을 "NetApp 문서" 참조하십시오.

VMware vSphere 솔루션 개요

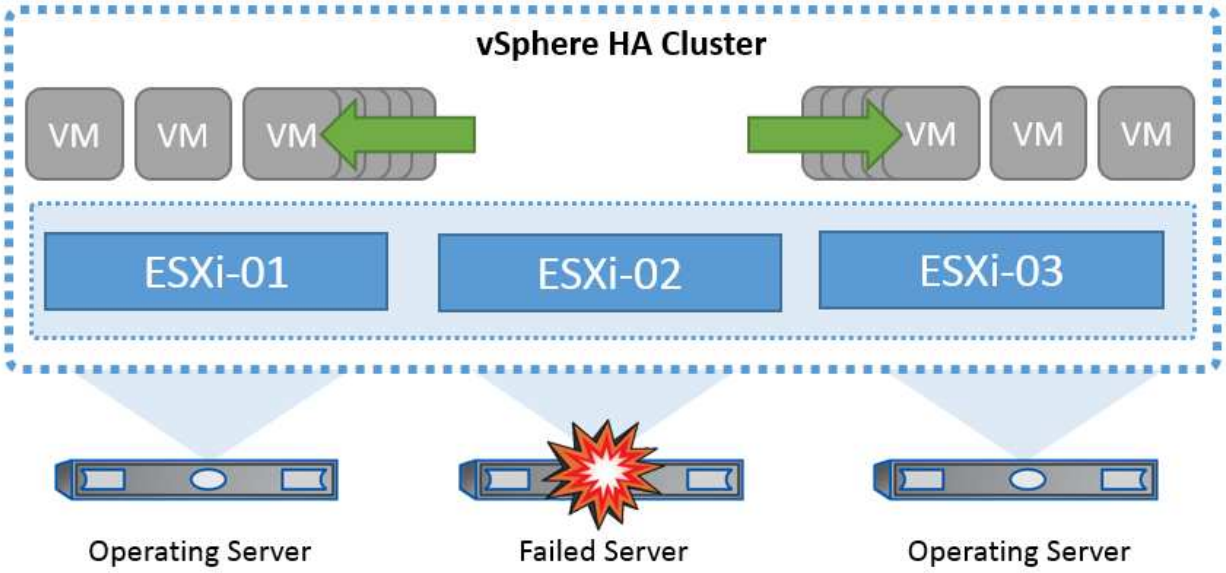
vCenter Server Appliance(VCSA)는 vSphere를 위한 강력한 중앙 집중식 관리 시스템이자 단일 통합 관리 콘솔로, 관리자가 ESXi 클러스터를 효과적으로 운영할 수 있도록 지원합니다. 이 솔루션은 VM 프로비저닝, vMotion 작업, 고가용성(HA), 분산 리소스 스케줄러(DRS), VMware vSphere Kubernetes Service(VKS) 등과 같은 주요 기능을 지원합니다. 이는 VMware 클라우드 환경의 필수 구성 요소이며 서비스 가용성을 염두에 두고 설계해야 합니다.

vSphere 고가용성

VMware의 클러스터 기술은 ESXi 서버를 가상 시스템의 공유 리소스 풀로 그룹화하고 vSphere HA(High Availability)를 제공합니다. vSphere HA는 가상 시스템에서 실행되는 애플리케이션에 사용하기 쉽고 고가용성을

제공합니다. 클러스터에서 HA 기능이 활성화된 경우 각 ESXi 서버는 다른 호스트와 통신을 유지하여 ESXi 호스트가 응답하지 않거나 격리될 경우 HA 클러스터는 클러스터의 남은 호스트 간에 해당 ESXi 호스트에서 실행 중이었던 가상 머신의 복구를 협상할 수 있습니다. 게스트 운영 체제에 장애가 발생할 경우 vSphere HA는 영향을 받는 가상 머신을 동일한 물리적 서버에서 다시 시작할 수 있습니다. vSphere HA를 사용하면 계획된 다운타임을 줄이고 예상치 못한 다운타임을 방지하며 운영 중단으로부터 신속하게 복구할 수 있습니다.

vSphere HA 클러스터에서 서버 장애 발생 시 가상 머신을 복구하는 방법.



VMware vSphere는 NetApp MetroCluster 또는 SnapMirror 활성 동기화에 대한 지식이 없으며 호스트 및 VM 그룹 선호도 구성에 따라 vSphere 클러스터의 모든 ESXi 호스트를 HA 클러스터 작업에 적합한 호스트로 간주한다는 점을 이해하는 것이 중요합니다.

호스트 장애 감지

HA 클러스터가 생성되는 즉시 클러스터의 모든 호스트가 마스터 선출에 참여하며, 그중 한 호스트가 마스터가 됩니다. 각 슬레이브는 마스터에게 네트워크 하트비트를 전송하고, 마스터는 모든 슬레이브 호스트에 네트워크 하트비트를 전송합니다. vSphere HA 클러스터의 마스터 호스트는 슬레이브 호스트의 장애를 감지하는 역할을 담당합니다.

감지된 장애 유형에 따라 호스트에서 실행 중인 가상 머신을 페일오버해야 할 수 있습니다.

vSphere HA 클러스터에서 세 가지 유형의 호스트 장애가 감지됩니다.

- 실패 - 호스트의 작동이 중지됩니다.
- 격리 - 호스트가 네트워크를 격리합니다.
- 파티션 - 호스트와 마스터 호스트의 네트워크 연결이 끊깁니다.

마스터 호스트는 클러스터의 슬레이브 호스트를 모니터링합니다. 이 통신은 네트워크 하트비트를 1초마다 교환하여 이루어집니다. 마스터 호스트가 슬레이브 호스트로부터 이러한 하트비트 수신을 중지하면 호스트가 실패했다고 선언하기 전에 호스트 활성 여부를 확인합니다. 마스터 호스트가 수행하는 활성 점검은 슬레이브 호스트가 데이터 저장소 중 하나와 하트비트를 교환하는지 여부를 확인하는 것입니다. 또한 마스터 호스트는 호스트가 관리 IP 주소로 전송된 ICMP 핑에 응답하여 호스트가 단순히 마스터 노드에서 격리되는지 아니면 네트워크에서 완전히 격리되는지 여부를 검사합니다. 기본 게이트웨이에 대해 ping을 수행하여 이 작업을 수행합니다. 하나 이상의 격리 주소를 수동으로 지정하여 격리 유효성 검사의 안정성을 향상시킬 수 있습니다.

NetApp에서는 최소 2개의 추가 격리 주소를 지정하고 각 주소는 사이트-로컬 주소를 지정하는 것이 좋습니다. 이렇게 하면 격리 검증의 신뢰성이 향상됩니다.

호스트 격리 응답

격리 응답은 vSphere HA 클러스터의 호스트가 관리 네트워크 연결이 끊어졌지만 계속 실행될 때 가상 머신에서 트리거되는 작업을 결정하는 vSphere HA 설정입니다. 이 설정에는 "사용 안 함", "VM 종료 후 재시작", "VM 전원 끄고 재시작"의 세 가지 옵션이 있습니다.

"종료"는 "전원 끄기"보다 낫습니다. "전원 끄기"는 최근 변경 사항을 디스크에 저장하거나 트랜잭션을 커밋하지 않기 때문입니다. 가상 머신이 300초 이내에 종료되지 않으면 전원이 꺼집니다. 대기 시간을 변경하려면 고급 옵션인 das.isolationshutdowntimeout을 사용하십시오.

HA는 격리 응답을 시작하기 전에 먼저 vSphere HA 마스터 에이전트가 VM 구성 파일이 포함된 데이터 저장소를 소유하는지 확인합니다. 그렇지 않으면 VM을 다시 시작할 마스터가 없기 때문에 호스트가 격리 응답을 트리거하지 않습니다. 호스트는 정기적으로 데이터 저장소 상태를 확인하여 마스터 역할을 가진 vSphere HA 에이전트에서 데이터 저장소를 요청하는지 확인합니다.

NetApp에서는 "호스트 격리 응답"을 사용 안 함으로 설정할 것을 권장합니다.

호스트가 vSphere HA 마스터 호스트에서 격리 또는 파티션되고 마스터가 하트비트 데이터 저장소 또는 Ping을 통해 통신할 수 없는 경우 브레인 분할 상태가 발생할 수 있습니다. 마스터가 격리된 호스트를 작동하지 않음을 선언하고 클러스터의 다른 호스트에서 VM을 다시 시작합니다. 가상 시스템의 두 인스턴스가 실행 중이기 때문에 브레인 분할 조건이 존재합니다. 그 중 하나만 가상 디스크를 읽거나 쓸 수 있습니다. 이제 VM 구성 요소 보호(VMCP)를 구성하여 브레인 분할 조건을 방지할 수 있습니다.

VM 구성 요소 보호**(VMCP)**

HA와 관련된 vSphere 6의 향상된 기능 중 하나는 VMCP입니다. VMCP는 블록(FC, iSCSI, FCoE) 및 파일 스토리지(NFS)에 대한 APD(All Path Down) 및 PDL(Permanent Device Loss) 조건에서 향상된 보호 기능을 제공합니다.

영구적 장치 손실**(PDL)**

PDL은 저장 장치가 영구적으로 고장 나거나 관리자에 의해 제거되어 다시 복구될 것으로 예상되지 않는 상태를 말합니다. NetApp 스토리지 어레이는 ESXi에 SCSI Sense 코드를 발행하여 장치가 영구적으로 연결 해제되었음을 알립니다. vSphere HA의 장애 조건 및 VM 응답 섹션에서 PDL 조건이 감지된 후 어떤 응답을 수행할지 구성할 수 있습니다.

NetApp "PDL이 있는 데이터스토어에 대한 응답"을 "**VM** 전원을 끄고 다시 시작"으로 설정하는 것을 권장합니다. 이 상태가 감지되면 vSphere HA 클러스터 내의 정상적인 호스트에서 VM이 즉시 다시 시작됩니다.

모든 경로 다운**(APD)**

APD는 호스트가 스토리지 장치에 액세스할 수 없게 되고 어레이에 대한 사용 가능한 경로가 없을 때 발생하는 상태입니다. ESXi는 이를 장치의 일시적인 문제로 간주하며, 곧 다시 사용 가능해질 것으로 예상합니다.

APD 조건이 감지되면 타이머가 시작됩니다. 140초 후에 APD 조건이 공식적으로 선언되고 장치가 APD 시간 초과로 표시됩니다. 140초가 지나면 HA는 VM 장애 조치 APD에 지정된 시간(분)을 계산하기 시작합니다. 지정된 시간이 경과하면 HA가 영향을 받는 가상 머신을 다시 시작합니다. 원하는 경우 다르게 응답하도록 VMCP를 구성할 수

있습니다(사용 안 함, 이벤트 발생 또는 VM 전원 끄기 및 재시작).

- NetApp에서는 "APD가 있는 데이터 저장소에 대한 응답"을 " * VM 전원을 끄고 다시 시작(보수적) * "으로 구성할 것을 권장합니다.
- 보수적이라는 것은 HA가 가상 머신을 재시작할 수 있을 가능성을 의미합니다. HA 설정을 '보수적'으로 하면, APD의 영향을 받는 VM은 다른 호스트에서 재시작할 수 있는 경우에만 재시작됩니다. 공격적 모드의 경우, HA는 다른 호스트의 상태를 알지 못하더라도 VM을 재시작하려고 시도합니다. 이로 인해 가상 머신이 위치한 데이터 저장소에 접근할 수 있는 호스트가 없는 경우 가상 머신이 재시작되지 않을 수 있습니다.
- APD 상태가 해결되고 시간 초과가 경과되기 전에 스토리지에 대한 액세스가 복구되는 경우, 사용자가 명시적으로 가상 머신을 구성하지 않는 한 HA는 가상 머신을 불필요하게 다시 시작하지 않습니다. 환경이 APD 조건으로부터 복구된 경우에도 응답이 필요한 경우 APD 시간 초과 후 APD 복구에 대한 응답을 VM 재설정 으로 구성해야 합니다.
- NetApp에서는 APD 시간 초과 후 APD 복구에 대한 응답을 사용 안 함으로 구성하는 것이 좋습니다.

NetApp SnapMirror Active Sync용 VMware DRS 구현

VMware DRS는 클러스터의 호스트 리소스를 집계하는 기능으로, 주로 가상 인프라스트럭처의 클러스터 내에서 로드 밸런싱을 수행하는 데 사용됩니다. VMware DRS는 주로 클러스터에서 로드 밸런싱을 수행하기 위한 CPU 및 메모리 리소스를 계산합니다. vSphere는 늘어난 클러스터링을 인식하지 못하므로 로드 밸런싱 시 두 사이트의 모든 호스트를 고려합니다.

NetApp MetroCluster용 VMware DRS 구현

```
 To avoid cross-site traffic, NetApp recommends configuring DRS affinity
rules to manage a logical separation of VMs. This will ensure that, unless
there is a complete site failure, HA and DRS will only use local hosts.
```

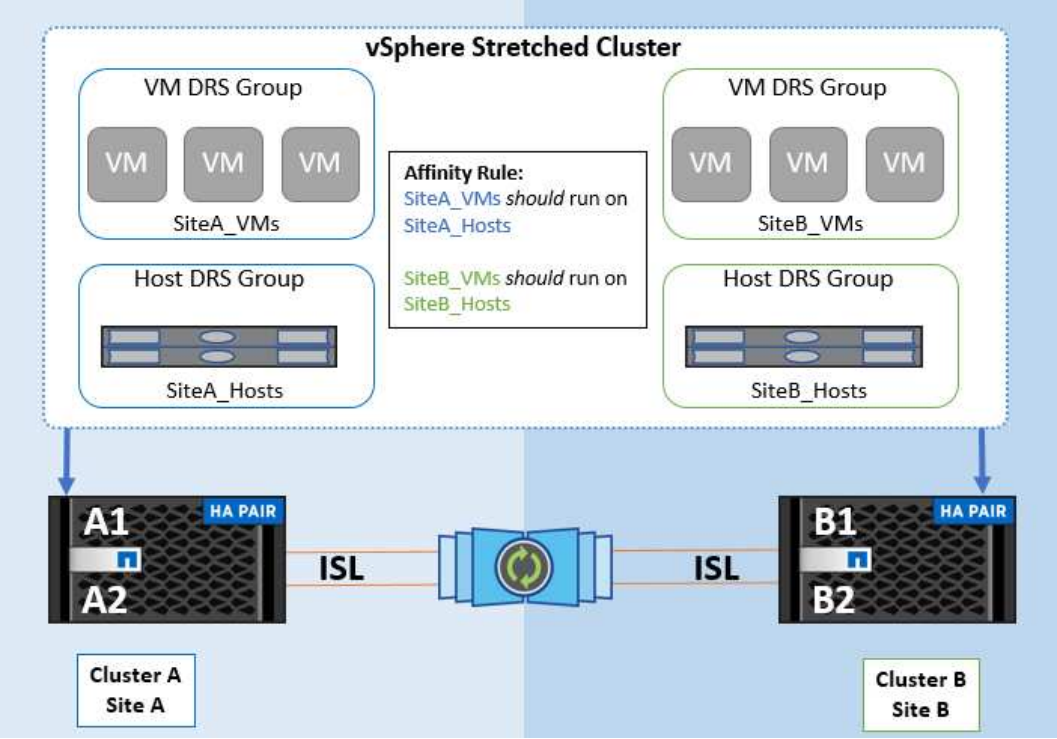
클러스터에 대한 DRS 선호도 규칙을 생성하는 경우 vSphere가 가상 머신 페일오버 중에 해당 규칙을 적용하는 방법을 지정할 수 있습니다.

vSphere HA 페일오버 동작에 대해 지정할 수 있는 규칙에는 두 가지 유형이 있습니다.

- VM 반유사성 규칙은 페일오버 작업 중에 지정된 가상 머신이 서로 떨어져 있도록 합니다.
- VM 호스트 선호도 규칙은 페일오버 작업 중에 특정 호스트 또는 정의된 호스트 그룹의 구성원에 지정된 가상 머신을 배치합니다.

VMware DRS의 VM 호스트 선호도 규칙을 사용하면 사이트 A와 사이트 B 간에 논리적 구분을 통해 VM이 지정된 데이터 저장소에 대한 운영 읽기/쓰기 컨트롤러로 구성된 스토리지와 동일한 사이트의 호스트에서 실행되도록 할 수 있습니다. 또한 VM 호스트 선호도 규칙을 통해 가상 머신이 스토리지에 로컬을 유지할 수 있으며, 이 경우 사이트 간에 네트워크 장애가 발생할 경우 가상 머신 연결을 확인할 수 있습니다.

다음은 VM 호스트 그룹 및 선호도 규칙의 예입니다.



모범 사례

NetApp은 장애가 발생할 경우 vSphere HA에 의해 위반되므로 "필수" 규칙 대신 "필수" 규칙을 구현하는 것이 좋습니다. "필수" 규칙을 사용하면 서비스가 중단될 수 있습니다.

서비스 제공 가능성은 항상 성능보다 우선시되어야 합니다. 데이터 센터 전체에 장애가 발생하는 시나리오에서 "필수" 규칙은 VM 호스트 선호도 그룹에서 호스트를 선택해야 하며, 데이터 센터를 사용할 수 없는 경우 가상 머신은 다시 시작되지 않습니다.

NetApp MetroCluster를 사용한 VMware Storage DRS 구축

VMware Storage DRS 기능을 사용하면 단일 유닛으로 데이터 저장소를 통합할 수 있으며 SIOC(스토리지 입출력 제어) 임계값을 초과할 경우 가상 머신 디스크의 균형을 조정할 수 있습니다.

Storage DRS가 활성화된 DRS 클러스터에서는 스토리지 입출력 제어가 기본적으로 설정됩니다. 스토리지 I/O 제어를 통해 관리자는 I/O 정체 기간 동안 가상 시스템에 할당되는 스토리지 I/O 양을 제어할 수 있으므로 더 중요한 가상 시스템이 I/O 리소스 할당에 덜 중요한 가상 시스템보다 우선 순위를 가질 수 있습니다.

Storage DRS는 Storage vMotion을 사용하여 가상 머신을 데이터 저장소 클러스터 내의 다른 데이터 저장소로 마이그레이션합니다. NetApp MetroCluster 환경에서는 해당 사이트의 데이터 저장소 내에서 가상 머신 마이그레이션을 제어해야 합니다. 예를 들어, 사이트 A의 호스트에서 실행되는 가상 머신 A는 사이트 A의 SVM 데이터 저장소 내에서 마이그레이션하는 것이 이상적입니다 가상 디스크 읽기/쓰기가 사이트 간 링크를 통해 사이트 B에서 이루어지므로 가상 머신이 계속 작동하지만 성능이 저하됩니다.

- ONTAP 스토리지를 사용할 경우 Storage DRS를 비활성화하는 것이 좋습니다.
- Storage DRS는 일반적으로 ONTAP 스토리지 시스템에서 사용할 필요가 없거나 권장되지 않습니다.
- ONTAP는 Storage DRS의 영향을 받을 수 있는 데이터 중복 제거, 압축 및 컴팩션과 같은 자체 스토리지 효율성 기능을 제공합니다.
- ONTAP 스냅샷을 사용하는 경우 스토리지 vMotion을 수행하면 스냅샷에 있는 VM 복사본이 그대로 남아 있게 되어 스토리지 사용량이 증가할 수 있으며, VM 및 ONTAP 스냅샷을 추적하는 NetApp SnapCenter 와 같은 백업 애플리케이션에 영향을 줄 수 있습니다.

vMSC 설계 및 구현 지침

이 문서에서는 ONTAP 스토리지 시스템을 지원하는 vMSC에 대한 설계 및 구현 지침을 개략적으로 설명합니다.

NetApp 스토리지 구성

NetApp MetroCluster 설치 지침은 에서 "MetroCluster 문서"확인할 수 있습니다. SMAS(SnapMirror Active Sync)에 대한 지침은 에서도 확인할 수 "SnapMirror 비즈니스 연속성 개요" 있습니다.

MetroCluster를 구성한 후에는 기존 ONTAP 환경을 관리하는 것과 같습니다. CLI(Command Line Interface), System Manager, Ansible과 같은 다양한 툴을 사용하여 SVM(스토리지 가상 머신)을 설정할 수 있습니다. SVM을 구성한 후 정상 작업에 사용할 클러스터에 논리 인터페이스(LIF), 볼륨 및 논리 유닛 번호(LUN)를 생성합니다. 이러한 오브젝트는 클러스터 피어링 네트워크를 사용하여 다른 클러스터로 자동으로 복제됩니다.

MetroCluster를 사용하지 않거나 ASA R2 시스템과 같이 MetroCluster에서 지원되지 않는 ONTAP 시스템이 있는 경우, 서로 다른 장애 도메인에 있는 여러 ONTAP 클러스터에서 데이터 저장소 세부 보호 및 Active-Active 액세스를 제공하는 SnapMirror Active Sync를 사용할 수 있습니다. SMAS는 CG(정합성 보장 그룹)를 사용하여 하나 이상의 데이터 저장소 간에 쓰기 순서 일관성을 보장하고 애플리케이션 및 데이터 저장소 요구 사항에 따라 여러 CG를 생성할 수 있습니다. 일관성 그룹은 여러 데이터 저장소 간에 데이터를 동기화해야 하는 애플리케이션에 특히 유용합니다. 예를 들어, 데이터 저장소 간에 분산된 게스트 LVM을 예로 들 수 있습니다. SMAS는 RDM(Raw Device Mappings) 및 게스트 내 iSCSI 초기자가 있는 게스트 연결 스토리지도 지원합니다. 일관성 그룹에 대한 자세한 내용은 에서 "일관성 그룹 개요"확인할 수 있습니다.

SnapMirror 액티브 동기화를 사용하여 vMSC 구성을 관리하는 것은 MetroCluster와 비교하여 몇 가지 차이가 있습니다. 첫째, SMAS는 SAN 전용 구성이므로 SnapMirror 활성 동기화를 사용하여 NFS 데이터 저장소를 보호할 수 없습니다. 둘째, 두 장애가 발생한 도메인 모두에서 복제된 데이터 저장소를 액세스할 수 있도록 LUN의 두 복제본을 ESXi 호스트에 매핑해야 합니다. 셋째, SnapMirror 활성 동기화를 사용하여 보호할 데이터 저장소에 대해 하나 이상의 정합성 보장 그룹을 생성해야 합니다. 마지막으로 생성한 일관성 그룹에 대한 SnapMirror 정책을 생성해야 합니다. 이 모든 작업은 ONTAP 도구 vCenter 플러그인의 "클러스터 보호" 마법사를 사용하거나 ONTAP CLI 또는 System Manager를 수동으로 사용하여 쉽게 수행할 수 있습니다.

ONTAP 도구 SnapMirror Active Sync용 vCenter 플러그인 사용

ONTAP tools vCenter 플러그인을 사용하면 vMSC에 대한 SnapMirror 활성 동기화를 간단하고 직관적으로 구성할 수 있습니다. ONTAP 도구 vCenter 플러그인을 사용하여 두 ONTAP 클러스터 간에 SnapMirror 활성 동기화 관계를 생성하고 관리할 수 있습니다. 이 플러그인은 이러한 관계를 효율적으로 설정하고 관리하기 위해 사용하기 쉬운 인터페이스를 제공합니다. ONTAP 툴 vCenter 플러그인에 대한 자세한 내용은 에서확인하거나 바로 로 이동할 "호스트 클러스터 보호를 사용하여 보호합니다" 수 "VMware vSphere용 ONTAP 툴" 있습니다.

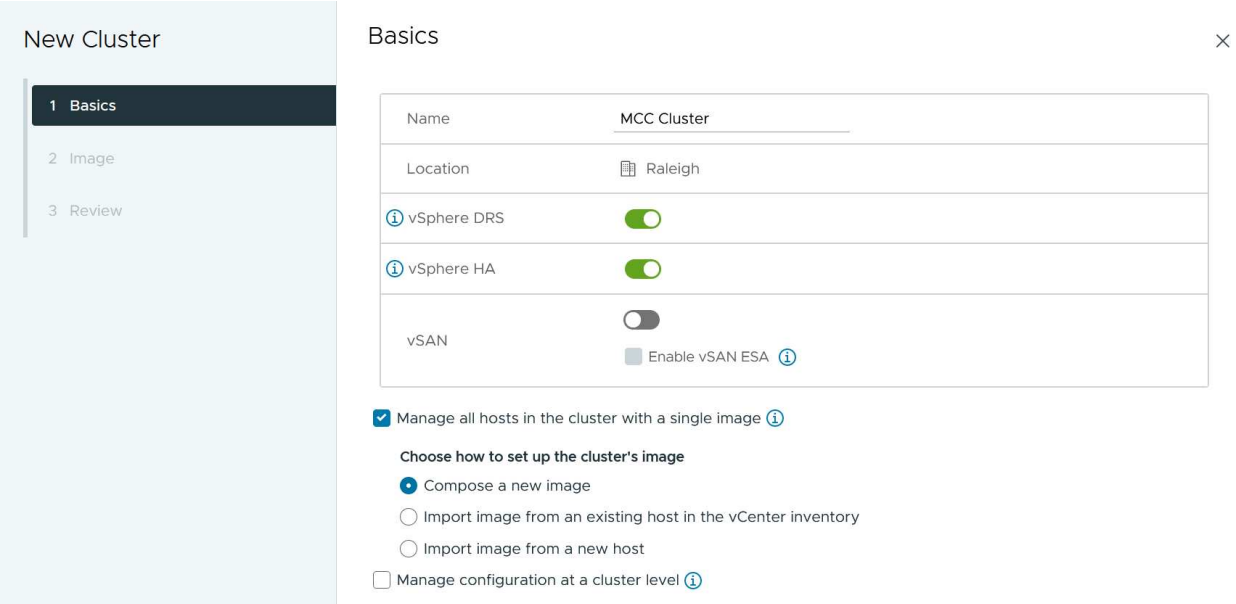
vSphere HA 클러스터를 생성합니다

vSphere HA 클러스터 생성은 에서 자세히 설명하는 다단계 프로세스입니다 "docs.vmware.com 에서 vSphere Client에서 클러스터를 생성하고 구성하는 방법". 즉, 먼저 빈 클러스터를 생성한 다음 vCenter를 사용하여 호스트를 추가하고 클러스터의 vSphere HA 및 기타 설정을 지정해야 합니다.

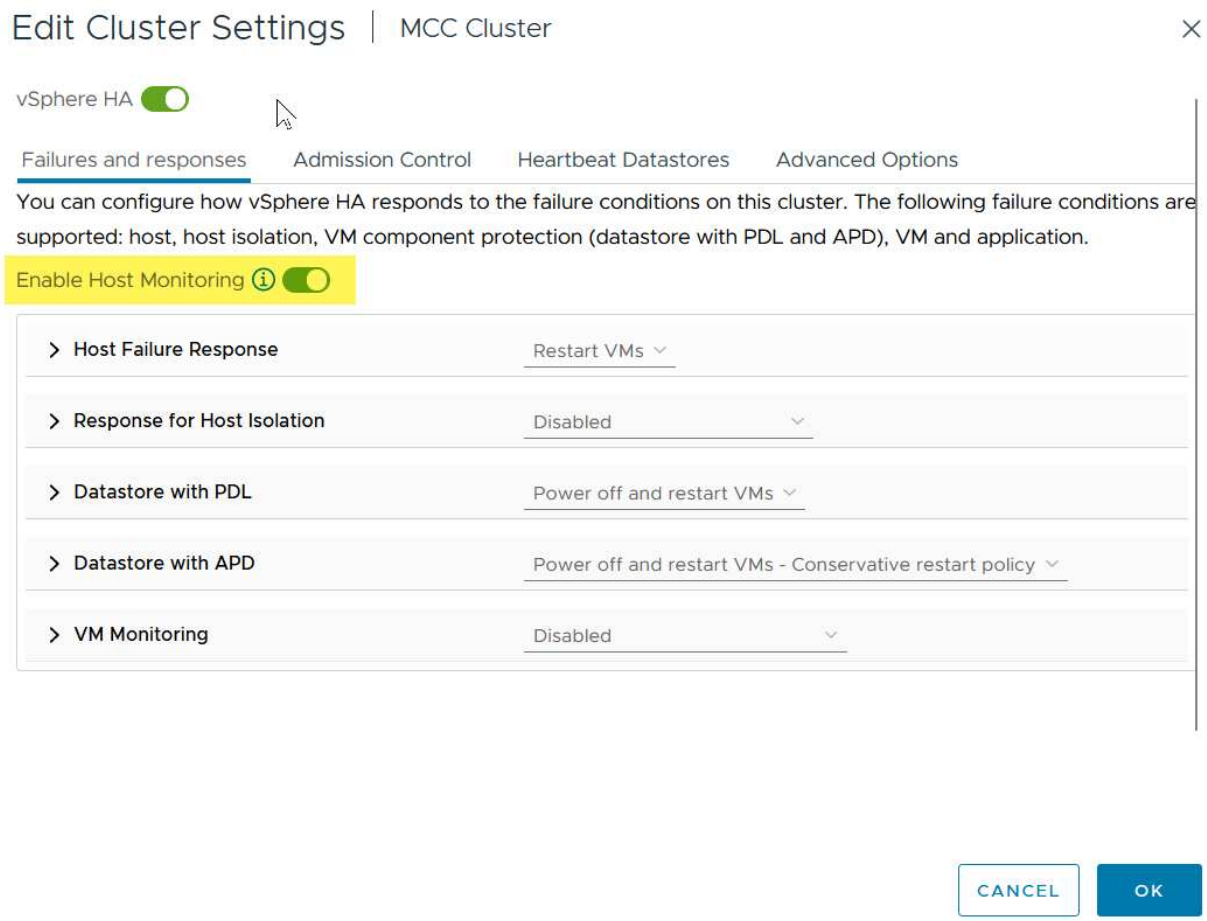
> 이 문서의 어떤 내용도 대체되지 "VMware vSphere Metro Storage Cluster 권장 사례"않습니다. 이 콘텐츠는 쉽게 참조할 수 있도록 제공되며 공식 VMware 설명서를 대체할 수 없습니다.

HA 클러스터를 구성하려면 다음 단계를 완료하십시오.

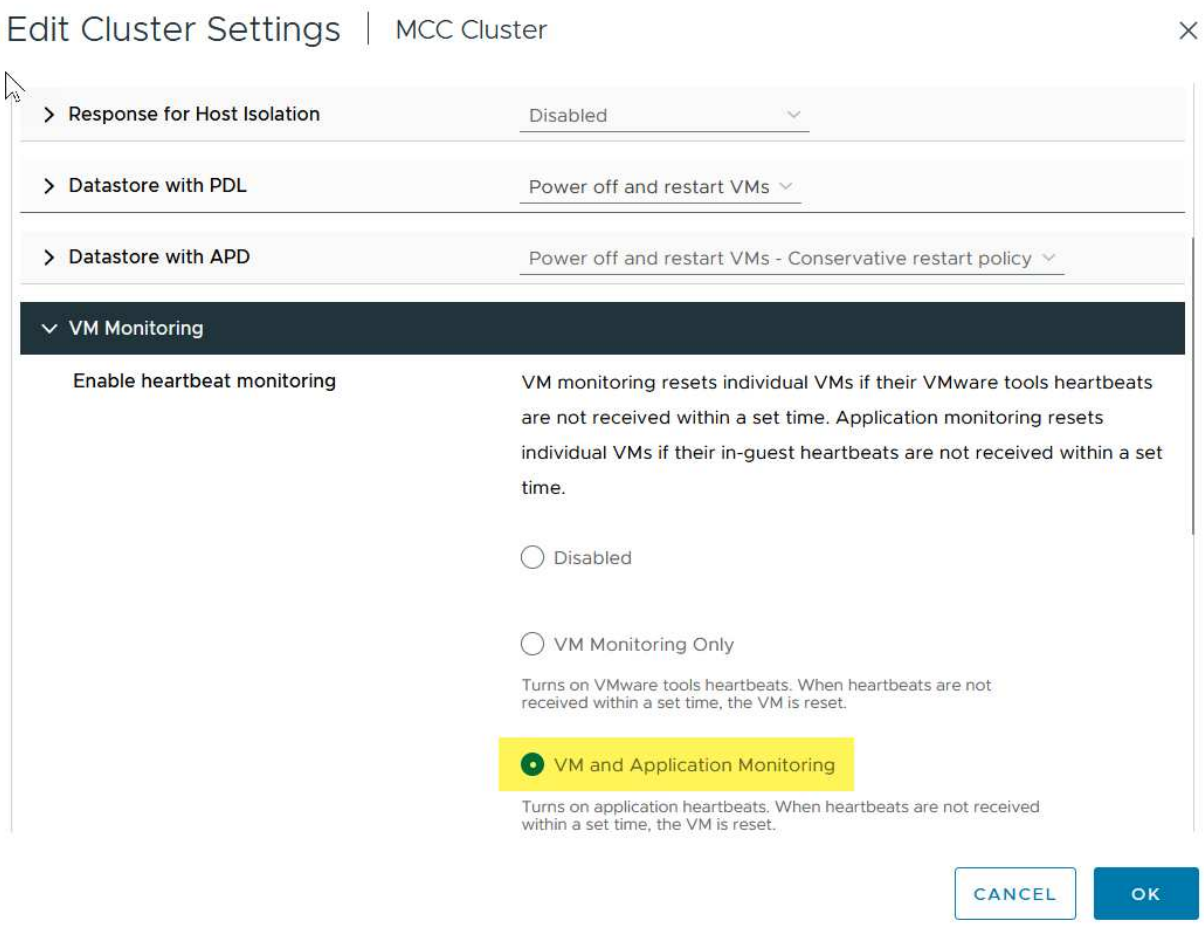
1. vCenter UI에 연결합니다.
2. 호스트 및 클러스터 에서 HA 클러스터를 생성할 데이터 센터를 찾습니다.
3. 데이터 센터 개체를 마우스 오른쪽 버튼으로 클릭하고 New Cluster를 선택합니다. 기본 사항에서 vSphere DRS 및 vSphere HA를 사용하도록 설정했는지 확인합니다. 마법사를 완료합니다.



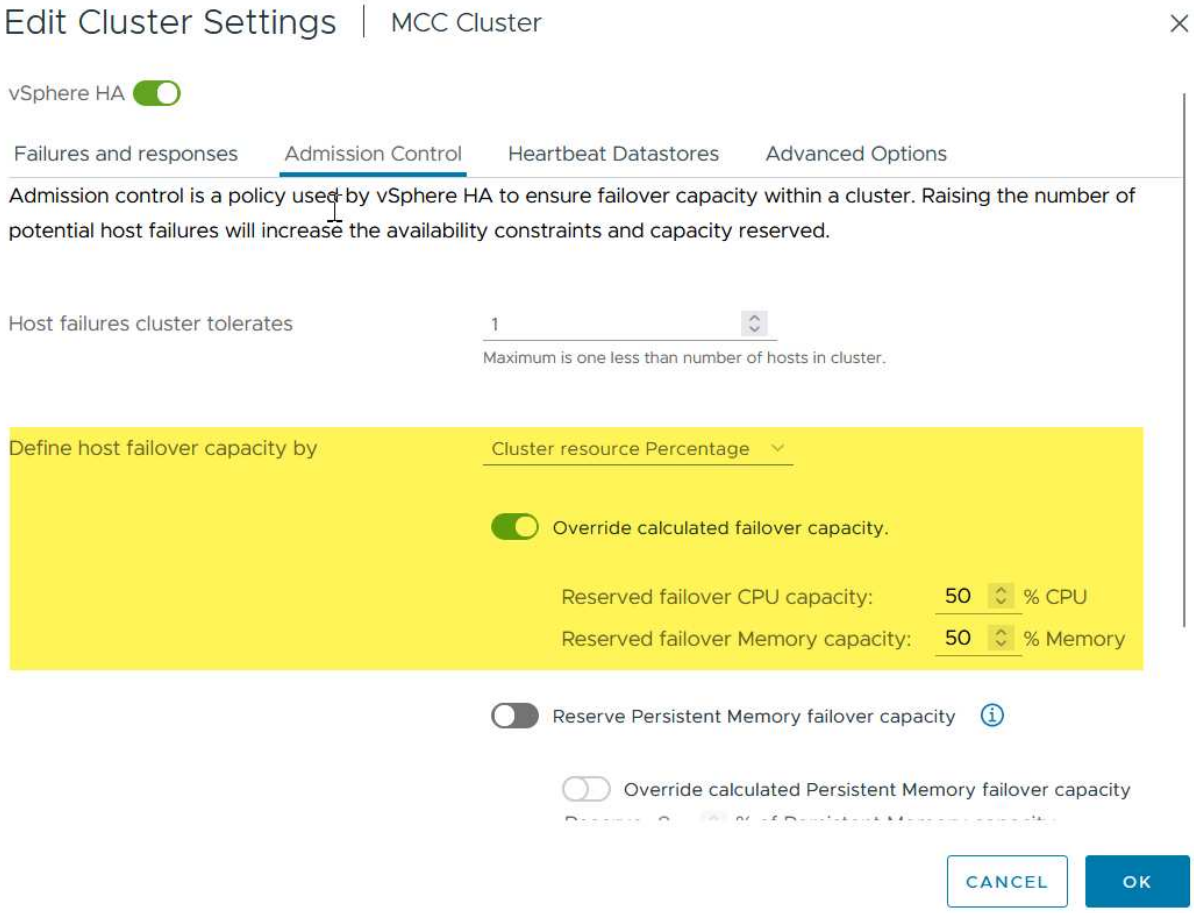
1. 클러스터를 선택하고 구성 탭으로 이동합니다. vSphere HA를 선택하고 Edit를 클릭합니다.
2. 호스트 모니터링 에서 호스트 모니터링 활성화 옵션을 선택합니다.



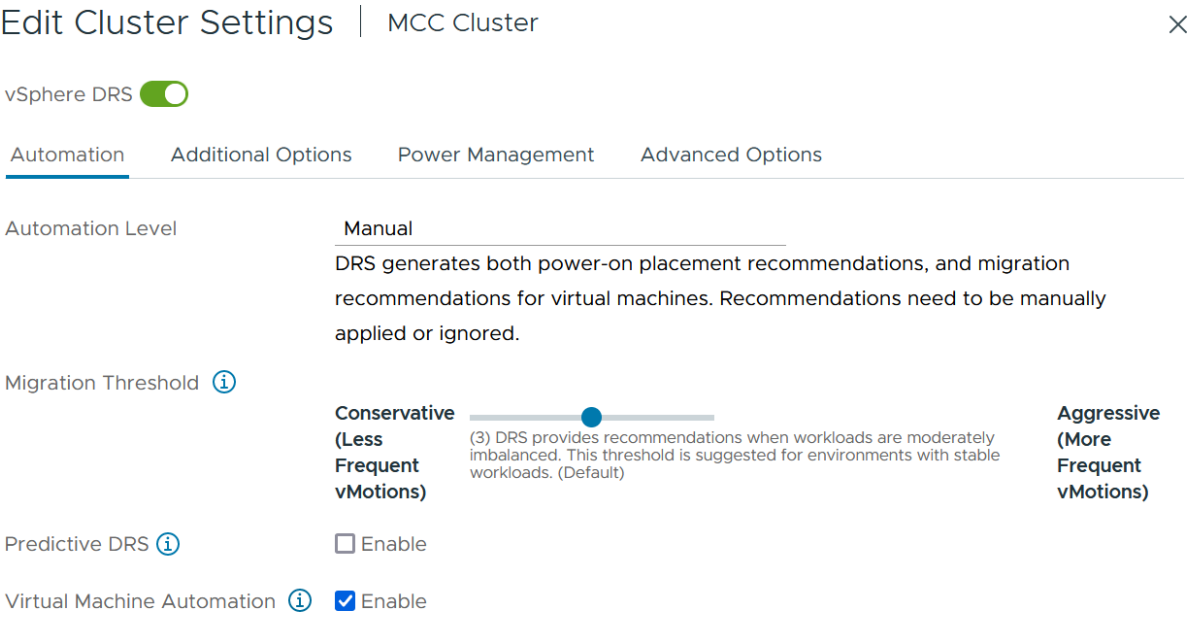
1. 오류 및 응답 탭에 있는 VM 모니터링에서 VM 모니터링만 옵션 또는 VM 및 애플리케이션 모니터링 옵션을 선택합니다.



1. Admission Control에서 HA 승인 제어 옵션을 cluster resource reserve로 설정하고 50% CPU/MEM을 사용합니다.



1. "확인"을 클릭합니다.
2. DRS를 선택하고 편집을 클릭합니다.
3. 응용 프로그램에서 요구하지 않는 한 자동화 수준을 수동으로 설정합니다.



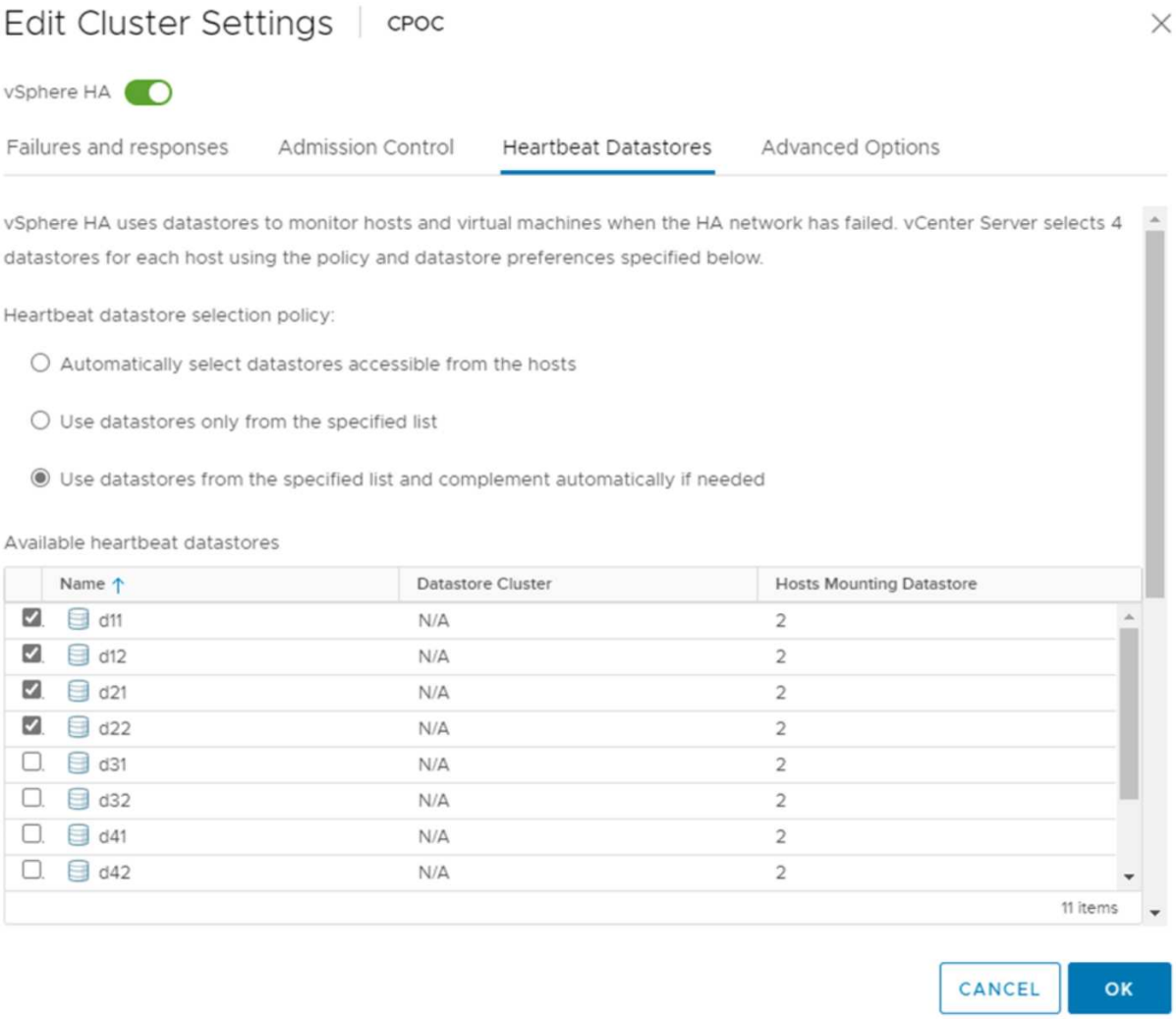
1. VM 구성 요소 보호를 활성화합니다. 을 참조하십시오 "docs.vmware.com".
2. MetroCluster를 사용하는 vMSC에는 다음과 같은 vSphere HA 설정이 추가로 권장됩니다.

실패	응답
호스트 오류입니다	VM을 다시 시작합니다
호스트 격리	사용 안 함
영구적 디바이스 손실(PDL)이 있는 데이터 저장소	VM의 전원을 끄고 다시 시작합니다
모든 경로가 다운된 데이터 저장소(APD)	VM의 전원을 끄고 다시 시작합니다
손님이 마음을 아프지 않습니다	VM을 재설정합니다
VM 다시 시작 정책	VM의 중요도에 따라 결정됩니다
호스트 격리에 대한 응답입니다	VM을 종료하고 다시 시작합니다
PDL이 있는 데이터 저장소에 대한 응답입니다	VM의 전원을 끄고 다시 시작합니다
APD가 있는 데이터 저장소에 대한 응답입니다	VM 전원 끄기 및 재시작(기본)
APD에 대한 VM 장애 조치 지연	3분
APD 시간 제한이 설정된 APD 복구에 대한 응답입니다	사용 안 함
VM 모니터링 민감도	사전 설정 높음

Heartbeating에 대한 데이터 저장소를 구성합니다

vSphere HA는 관리 네트워크에 장애가 발생한 경우 데이터 저장소를 사용하여 호스트와 가상 머신을 모니터링합니다. vCenter가 하트비트 데이터 저장소를 선택하는 방법을 구성할 수 있습니다. 하트비팅을 위해 데이터 저장소를 구성하려면 다음 단계를 수행하십시오.

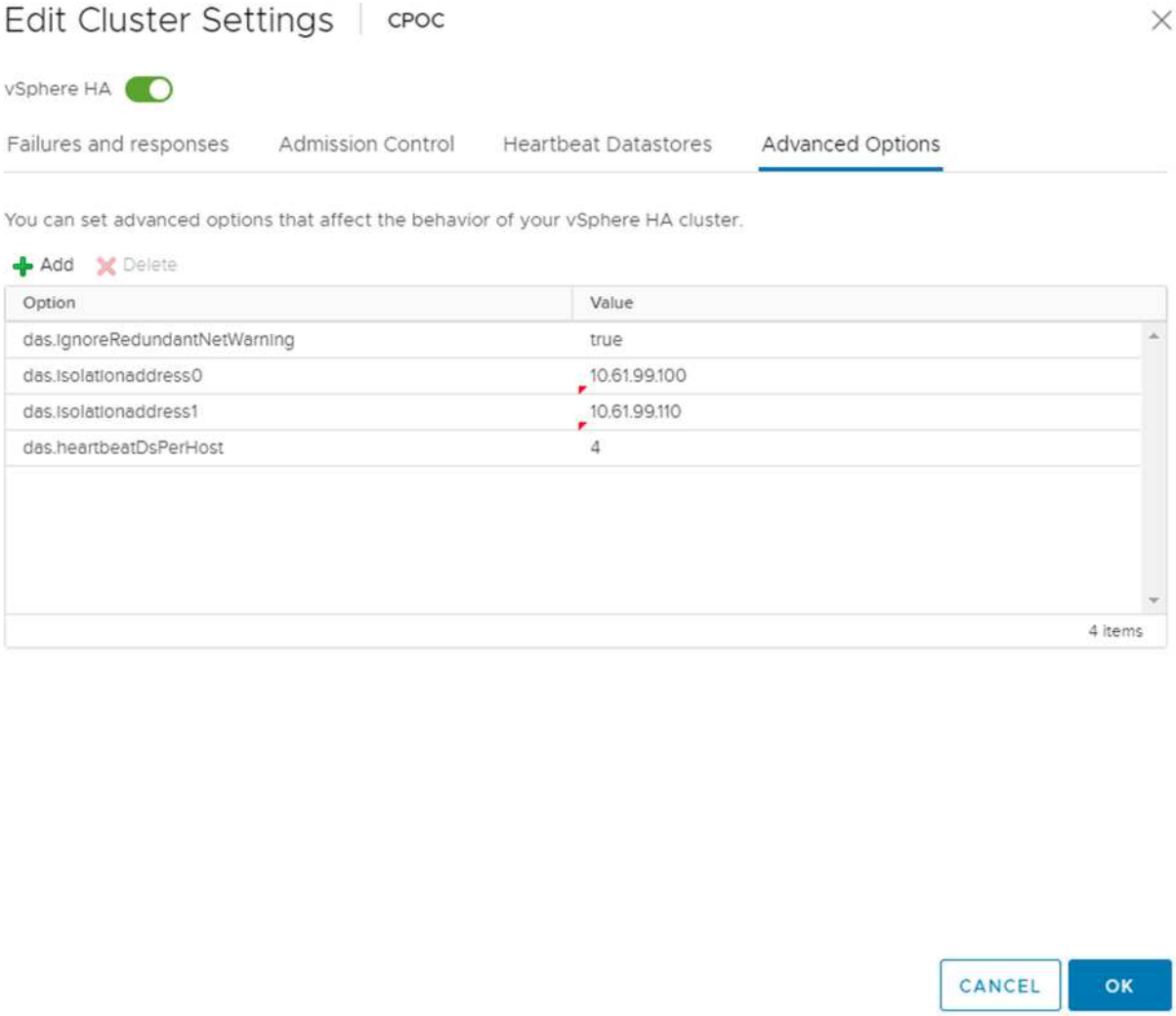
1. Datastore Heartbeating 섹션에서 Specified List 에서 Use datastores 를 선택하고 필요한 경우 자동으로 보완합니다.
2. vCenter가 두 사이트에서 사용할 데이터 저장소를 선택하고 OK를 누릅니다.



고급 옵션 구성

격리 이벤트는 HA 클러스터에 있는 호스트가 네트워크 또는 클러스터의 다른 호스트에 대한 연결이 끊어질 때 발생합니다. 기본적으로 vSphere HA는 관리 네트워크의 기본 게이트웨이를 기본 격리 주소로 사용합니다. 하지만 ping을 수행할 호스트에 대한 추가 격리 주소를 지정하여 격리 응답을 트리거할지 여부를 결정할 수 있습니다. 사이트당 하나씩 ping을 수행할 수 있는 두 개의 격리 IP를 추가합니다. 게이트웨이 IP를 사용하지 마십시오. 사용되는 vSphere HA 고급 설정은 DAS.isolationaddress입니다. 이러한 목적으로 ONTAP 또는 중재자 IP 주소를 사용할 수 있습니다.

자세한 내용은 을 "VMware vSphere Metro Storage Cluster 권장 사례" 참조하십시오. ._



das.heartbeatDsPerHost 라는 고급 설정을 추가하면 하트비트 데이터 저장소의 수가 증가할 수 있습니다. 사이트당 2개씩 4개의 하트비트 데이터 저장소(HB DSS)를 사용합니다. "목록에서 선택 하지만 칭찬" 옵션을 사용합니다. 한 사이트에 장애가 발생해도 두 개의 HB DSS가 필요하기 때문입니다. 그러나 이러한 파일은 MetroCluster 또는 SnapMirror 활성 동기화를 사용하여 보호할 필요가 없습니다.

자세한 내용은 을 "VMware vSphere Metro Storage Cluster 권장 사례" 참조하십시오. ._

NetApp MetroCluster용 VMware DRS Affinity

이 섹션에서는 MetroCluster 환경의 각 사이트\클러스터에 대해 VM 및 호스트용 DRS 그룹을 생성합니다. 그런 다음 VM 호스트 규칙을 구성하여 VM 호스트 선호도를 로컬 스토리지 리소스에 맞춥니다. 예를 들어 사이트 A VM은 VM 그룹 SiteA_VMs에 속하고 사이트 A 호스트는 호스트 그룹 SiteA_HOSTS에 속합니다. 다음으로 VM\Host Rules에서는 SiteA_VMs가 SiteA_hosts의 호스트에서 실행되어야 한다고 설명합니다.

- NetApp은 그룹*의 호스트에서 실행해야 함*이 아니라 그룹*의 호스트에서 실행되어야 함*을 사용할 것을 적극 권장합니다. 사이트 A 호스트에 장애가 발생할 경우 사이트 A의 VM을 vSphere HA를 통해 사이트 B의 호스트에서 다시 시작해야 하지만, 후자의 사양에서는 하드 규칙이기 때문에 HA가 사이트 B에서 VM을 다시 시작할 수 없습니다. 이전 사양은 소프트 규칙이며 HA가 발생할 경우 위반되므로 성능보다 가용성이 향상됩니다.
- 가상 시스템이 VM-호스트 선호도 규칙을 위반할 때 트리거되는 이벤트 기반 경보를 생성할 수 있습니다. vSphere Client에서 가상 머신에 대한 새 경고를 추가하고 이벤트 트리거로 "VM is behaving VM - Host Affinity Rule"을 선택합니다. 알람 생성 및 편집에 대한 자세한 내용은 "vSphere 모니터링 및 성능"설명서를 참조하십시오.

DRS 호스트 그룹을 생성합니다

사이트 A 및 사이트 B에만 해당하는 DRS 호스트 그룹을 생성하려면 다음 단계를 수행하십시오.

1. vSphere 웹 클라이언트에서 인벤토리에서 클러스터를 마우스 오른쪽 버튼으로 클릭하고 설정 을 선택합니다.
2. VM\호스트 그룹 을 클릭합니다.
3. 추가 를 클릭합니다.
4. 그룹의 이름을 입력합니다(예: SiteA_hosts).
5. 유형 메뉴에서 호스트 그룹 을 선택합니다.
6. Add를 클릭하고 사이트 A에서 원하는 호스트를 선택한 다음 OK를 클릭합니다.
7. 사이트 B에 대해 다른 호스트 그룹을 추가하려면 다음 단계를 반복합니다
8. 확인 을 클릭합니다.

DRS VM 그룹을 생성합니다

사이트 A 및 사이트 B에만 해당하는 DRS VM 그룹을 생성하려면 다음 단계를 수행하십시오.

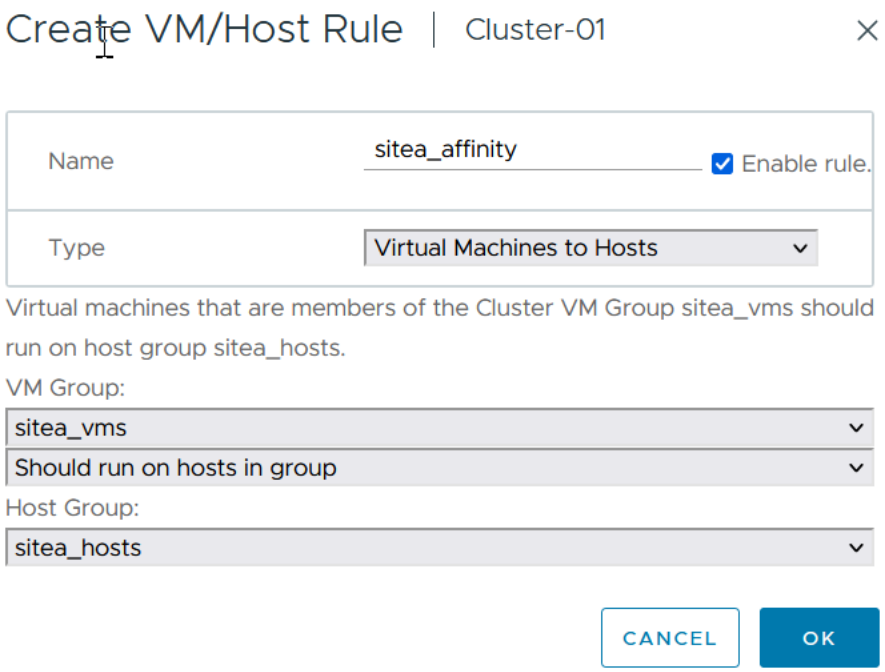
1. vSphere 웹 클라이언트에서 인벤토리에서 클러스터를 마우스 오른쪽 버튼으로 클릭하고 설정 을 선택합니다.
2. VM\호스트 그룹 을 클릭합니다.
3. 추가 를 클릭합니다.
4. 그룹의 이름을 입력합니다(예: SiteA_VMs).
5. 유형 메뉴에서 VM 그룹 을 선택합니다.
6. 추가 를 클릭하고 사이트 A에서 원하는 VM을 선택한 다음 확인 을 클릭합니다.
7. 사이트 B에 대해 다른 호스트 그룹을 추가하려면 다음 단계를 반복합니다
8. 확인 을 클릭합니다.

VM 호스트 규칙을 생성합니다

사이트 A 및 사이트 B에 고유한 DRS 선호도 규칙을 만들려면 다음 단계를 수행하십시오.

1. vSphere 웹 클라이언트에서 인벤토리에서 클러스터를 마우스 오른쪽 버튼으로 클릭하고 설정 을 선택합니다.
2. VM\호스트 규칙을 클릭합니다.
3. 추가 를 클릭합니다.

4. 규칙의 이름을 입력합니다(예: SiteA_affinity).
5. 규칙 사용 옵션이 선택되어 있는지 확인합니다.
6. 유형 메뉴에서 가상 머신을 호스트에 선택합니다.
7. VM 그룹(예: SiteA_VMS)을 선택합니다.
8. 호스트 그룹(예: SiteA_hosts)을 선택합니다.
9. 이 단계를 반복하여 사이트 B에 대해 다른 VM\호스트 규칙을 추가합니다
10. 확인 을 클릭합니다.



필요한 경우 데이터 저장소 클러스터를 생성합니다

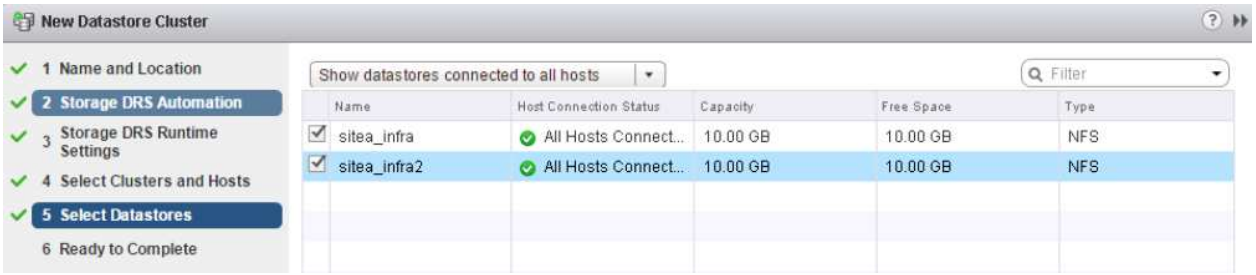
각 사이트에 대해 데이터 저장소 클러스터를 구성하려면 다음 단계를 완료합니다.

1. vSphere Web Client를 사용하여 Storage 아래에 HA 클러스터가 있는 데이터 센터로 이동합니다.
2. 데이터 센터 개체를 마우스 오른쪽 버튼으로 클릭하고 스토리지 > 새 데이터 저장소 클러스터 를 선택합니다.

- ONTAP 스토리지를 사용할 경우 Storage DRS를 비활성화하는 것이 좋습니다.
- Storage DRS는 일반적으로 ONTAP 스토리지 시스템에서 사용할 필요가 없거나 권장되지 않습니다.
- ONTAP는 Storage DRS의 영향을 받을 수 있는 데이터 중복 제거, 압축 및 컴팩션과 같은 자체 스토리지 효율성 기능을 제공합니다.
- ONTAP 스냅샷을 사용하는 경우 Storage vMotion은 스냅샷에서 VM의 복제본을 남겨 두므로 스토리지 활용도가 높아지며 VM 및 해당 ONTAP 스냅샷을 추적하는 NetApp SnapCenter와 같은 백업 애플리케이션에 영향을 미칠 수 있습니다.

1. HA 클러스터를 선택하고 Next를 클릭합니다.

1. 사이트 A에 속하는 데이터 저장소를 선택하고 Next를 클릭합니다.



1. 옵션을 검토하고 마침 을 클릭합니다.
2. 이 단계를 반복하여 사이트 B 데이터 저장소 클러스터를 생성하고 사이트 B의 데이터 저장소만 선택되어 있는지 확인합니다.

vCenter Server 가용성

vCenter Server Appliance(VCSA)는 vCenter HA로 보호되어야 합니다. vCenter HA를 사용하면 액티브-패시브 HA 쌍에 VCSA 두 개를 구축할 수 있습니다. 각 장애 도메인에 1개 에서 vCenter HA에 대한 자세한 내용을 확인할 수 있습니다 "docs.vmware.com".

계획되거나 계획되지 않은 이벤트에 대한 복원력

NetApp MetroCluster 및 SnapMirror 활성 동기화는 NetApp 하드웨어 및 ONTAP ® 소프트웨어의 고가용성 및 무중단 운영을 개선하는 강력한 툴입니다.

이러한 툴은 전체 스토리지 환경에 대해 사이트 전체를 보호하여 데이터를 항상 사용할 수 있도록 보장합니다. NetApp 기술을 사용하면 독립 실행형 서버, 고가용성 서버 클러스터, 컨테이너, 가상 서버 등 무엇을 사용하든 전력, 냉각 및 네트워크 연결이 끊어지고 스토리지 어레이 중단이나 운영 오류가 발생하여 전체 중단이 발생해도 스토리지 가용성을 원활하게 유지할 수 있습니다.

MetroCluster 및 SnapMirror 활성 동기화는 계획된 또는 계획되지 않은 이벤트가 발생할 경우 데이터 연속성을 위해 3가지 기본 방법을 제공합니다.

- 이중 구성 요소로 단일 구성 요소 장애로부터 보호
- 단일 컨트롤러에 영향을 주는 이벤트에 대한 로컬 HA 테이크오버
- 완벽한 사이트 보호 – 스토리지 및 클라이언트 액세스를 소스 클러스터에서 대상 클러스터로 이동하여 신속하게 서비스를 재개합니다

즉, 단일 구성 요소 장애 발생 시 작업을 계속 원활하게 수행하고 장애가 발생한 구성 요소를 교체하면 자동으로 중복 작업으로 되돌아갑니다.

단일 노드 클러스터(일반적으로 ONTAP Select 같은 소프트웨어 정의 버전)를 제외한 모든 ONTAP 클러스터에는 Takeover 및 Giveback이라는 HA 기능이 내장되어 있습니다. 클러스터의 각 컨트롤러가 다른 컨트롤러와 페어링되어 HA 쌍을 형성합니다. 이러한 페어를 통해 각 노드가 스토리지에 로컬로 접속됩니다.

Takeover는 한 노드가 다른 노드의 스토리지를 인수하여 데이터 서비스를 유지하는 자동화된 프로세스입니다. 반환 은 정상 작업을 복원하는 역 프로세스입니다. 하드웨어 유지 보수, ONTAP 업그레이드 수행 시 또는 계획되지 않은 노드 장애 또는 하드웨어 장애로 인해 테이크오버를 계획할 수 있습니다.

테이크오버 중에 MetroCluster 구성의 NAS LIF는 자동으로 페일오버됩니다. 그러나 SAN LIF는 페일오버되지 않으며 LUN(논리 유닛 번호)에 대한 직접 경로를 계속 사용합니다.

HA 테이크오버 및 반환에 대한 자세한 내용은 를 "HA 쌍 관리 개요"참조하십시오. 이 기능은 MetroCluster 또는 SnapMirror 활성 동기화에만 한정되지 않습니다.

MetroCluster를 통한 사이트 전환은 한 사이트가 오프라인일 때 또는 사이트 전체 유지 관리를 위한 계획된 활동으로 수행됩니다. 나머지 사이트에서는 오프라인 클러스터의 스토리지 리소스(디스크 및 애그리게이트)를 소유합니다. 그러면 장애가 발생한 사이트의 SVM이 온라인으로 전환되고 재해 사이트에서 다시 시작되므로 클라이언트 및 호스트 액세스를 위해 전체 ID를 유지할 수 있습니다.

SnapMirror 액티브 동기화를 사용할 때는 두 복사본이 동시에 활발하게 사용되므로 기존 호스트가 계속 작동합니다. 사이트 페일오버가 올바르게 수행되도록 하려면 ONTAP 중재자가 필요합니다.

MetroCluster가 있는 **vMSC**의 실패 시나리오

다음 섹션에서는 vMSC 및 NetApp MetroCluster 시스템의 다양한 장애 시나리오에서 예상되는 결과를 간략하게 설명합니다.

단일 스토리지 경로 오류

이 시나리오에서 HBA 포트, 네트워크 포트, 프런트엔드 데이터 스위치 포트 또는 FC 또는 이더넷 케이블과 같은 구성 요소에 장애가 발생하면 ESXi 호스트에서 스토리지 디바이스에 대한 특정 경로가 비활성 상태로 표시됩니다. HBA/네트워크/스위치 포트에서 복원력을 제공하여 스토리지 디바이스에 여러 경로를 구성한 경우 ESXi는 경로 전환을 수행하는 것이 가장 좋습니다. 이 기간 동안 스토리지 디바이스에 다중 경로를 제공하여 스토리지 가용성이 관리되기 때문에 가상 머신은 영향을 받지 않고 계속 실행됩니다.

> 이 시나리오에서는 MetroCluster 동작에 변화가 없으며 모든 데이터 저장소가 해당 사이트에서 그대로 유지됩니다.

모범 사례

NFS/iSCSI 볼륨이 사용되는 환경에서는 NetApp 표준 vSwitch의 NFS vmkernel 포트에 대해 두 개 이상의 네트워크 업링크를 구성하고 분산형 vSwitch에 대해 NFS vmkernel 인터페이스가 매핑된 포트 그룹에서 동일한 네트워크 업링크를 구성하는 것이 좋습니다. NIC 티밍은 Active-Active 또는 Active-Standby 중 하나로 구성할 수 있습니다.

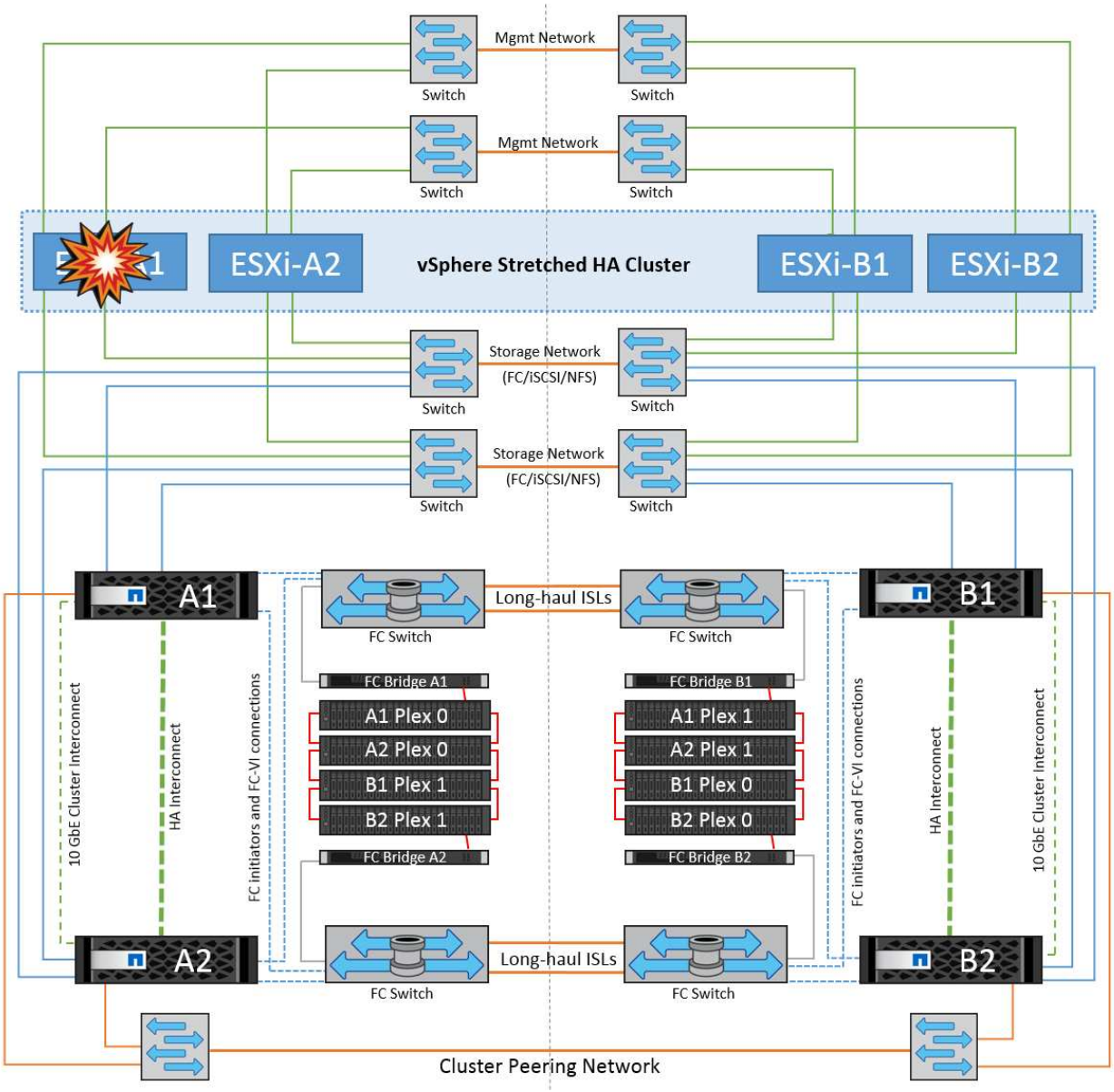
또한 iSCSI LUN의 경우 vmkernel 인터페이스를 iSCSI 네트워크 어댑터에 바인딩하여 다중 경로를 구성해야 합니다. 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.

모범 사례

Fibre Channel LUN이 사용되는 환경에서는 NetApp HBA/포트 레벨에서 복원력을 보장하는 HBA를 2개 이상 사용하는 것이 좋습니다. 또한 NetApp은 조닝을 구성하는 모범 사례로서 단일 이니시에이터에 단일 타겟 조닝으로 권장합니다.

모든 신규 및 기존 NetApp 스토리지 장치에 대한 정책을 설정하므로 VSC(가상 스토리지 콘솔)를 사용하여 다중 경로 정책을 설정해야 합니다.

단일 **ESXi** 호스트 장애



이 시나리오에서는 ESXi 호스트 장애가 있는 경우 VMware HA 클러스터의 마스터 노드가 더 이상 네트워크 하트비트를 수신하지 않기 때문에 호스트 장애를 감지합니다. 호스트가 실제로 다운되었는지 아니면 네트워크 파티션만 발생하는지 확인하기 위해 마스터 노드는 데이터 저장소 하트비트를 모니터링하고, 이 하트비트가 없는 경우 장애가 발생한 호스트의 관리 IP 주소를 ping하여 최종 점검을 수행합니다. 이러한 검사가 모두 음수이면 마스터 노드가 이

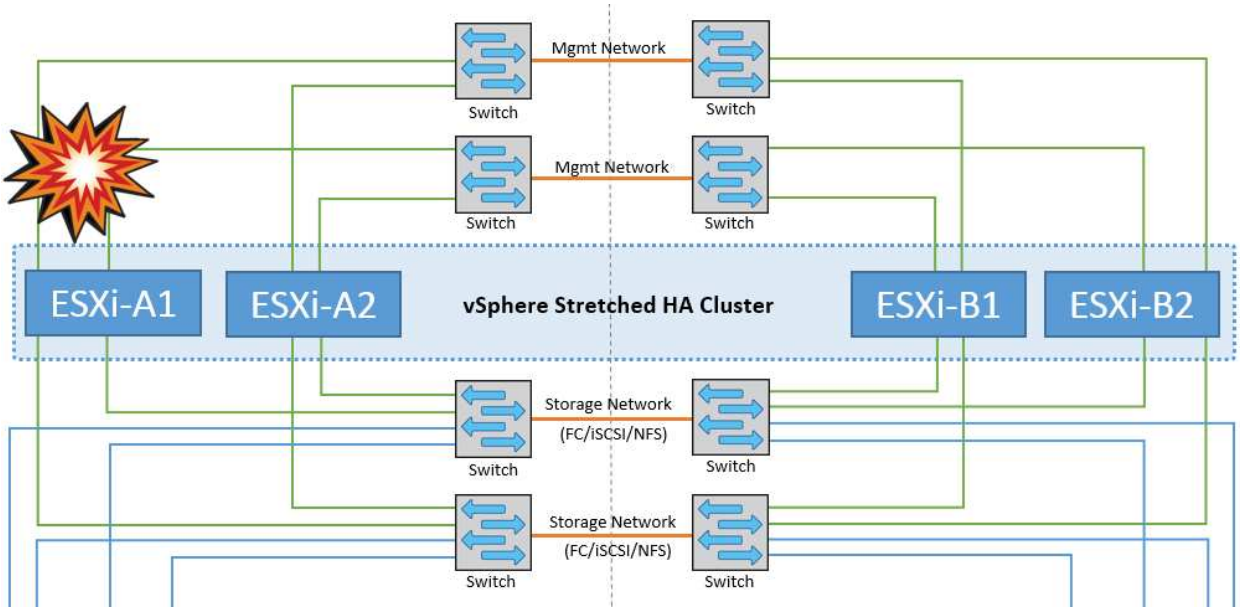
호스트에 장애가 발생한 호스트를 선언하고 장애가 발생한 이 호스트에서 실행 중이던 모든 가상 머신이 클러스터의 나머지 호스트에서 재부팅됩니다.

DRS VM 및 호스트 선호도 규칙이 구성된 경우(VM 그룹 SiteA_VM의 VM은 호스트 그룹 SiteA_hosts에서 호스트를 실행해야 함), HA 마스터는 먼저 사이트 A에서 사용 가능한 리소스를 확인합니다 사이트 A에 사용 가능한 호스트가 없는 경우 마스터가 사이트 B의 호스트에서 VM을 다시 시작하려고 시도합니다

로컬 사이트에 리소스 제한이 있는 경우 다른 사이트의 ESXi 호스트에서 가상 머신을 시작할 수 있습니다. 그러나 가상 머신을 로컬 사이트의 정상적인 ESXi 호스트로 다시 마이그레이션하여 규칙을 위반하는 경우 정의된 DRS VM 및 호스트 선호도 규칙이 수정됩니다. DRS가 수동으로 설정된 경우 NetApp는 DRS를 호출하고 권장 사항을 적용하여 가상 머신 배치를 수정하는 것이 좋습니다.

이 시나리오에서는 MetroCluster 동작에 변화가 없으며 모든 데이터 저장소가 해당 사이트에서 그대로 유지됩니다.

ESXi 호스트 격리

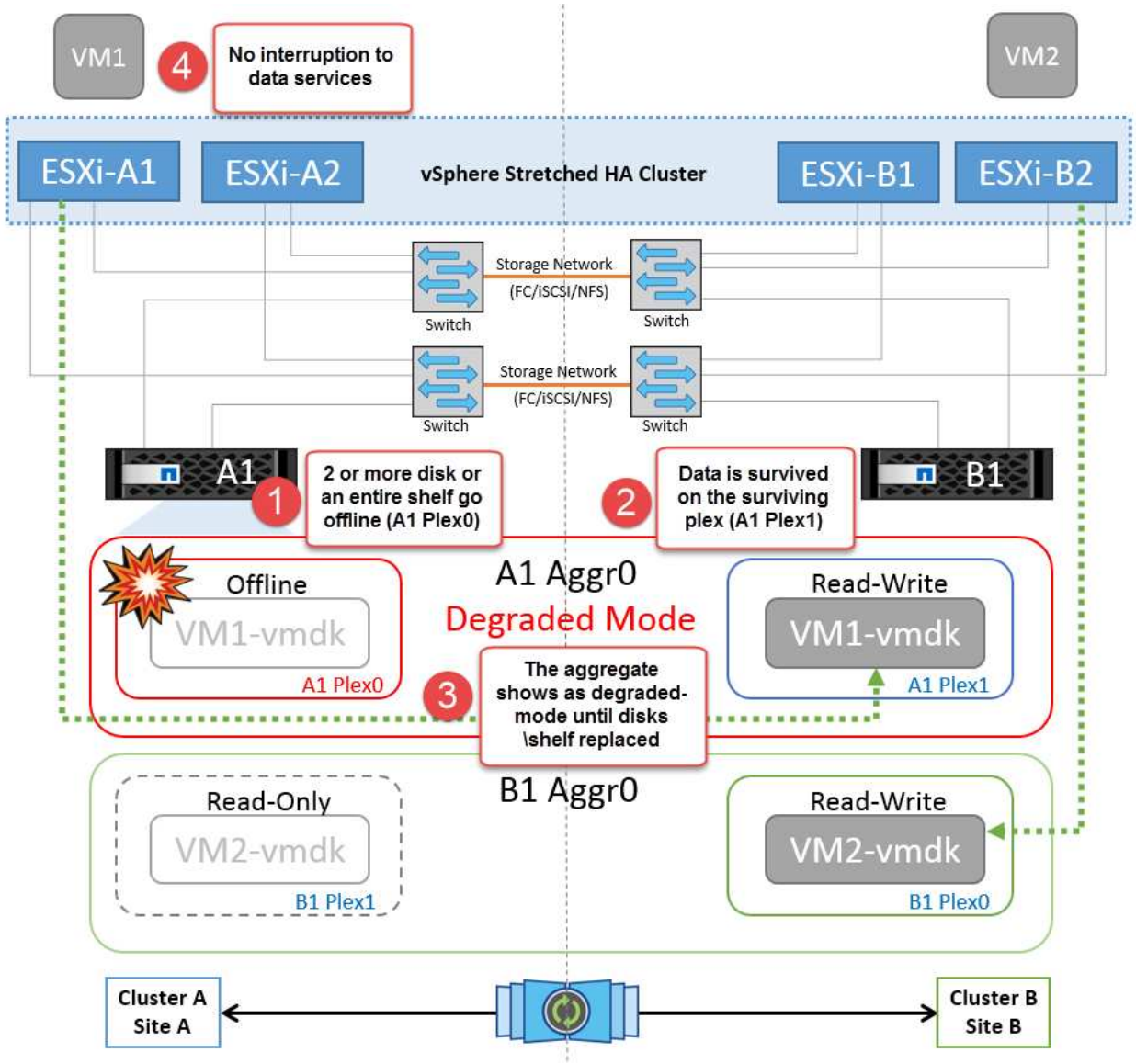


이 시나리오에서는 ESXi 호스트의 관리 네트워크가 다운된 경우 HA 클러스터의 마스터 노드가 하트비트를 수신하지 않으므로 이 호스트가 네트워크에서 격리됩니다. 마스터 노드가 데이터 저장소 하트비트를 모니터링하기 시작합니다. 호스트가 있는 경우 마스터 노드에 의해 격리된 것으로 선언됩니다. 구성된 격리 응답에 따라 호스트는 전원을 끄거나, 가상 시스템을 종료하거나, 가상 시스템의 전원을 계속 켜도록 선택할 수 있습니다. 격리 응답의 기본 간격은 30 초입니다.

이 시나리오에서는 MetroCluster 동작에 변화가 없으며 모든 데이터 저장소가 해당 사이트에서 그대로 유지됩니다.

디스크 쉘프 오류입니다

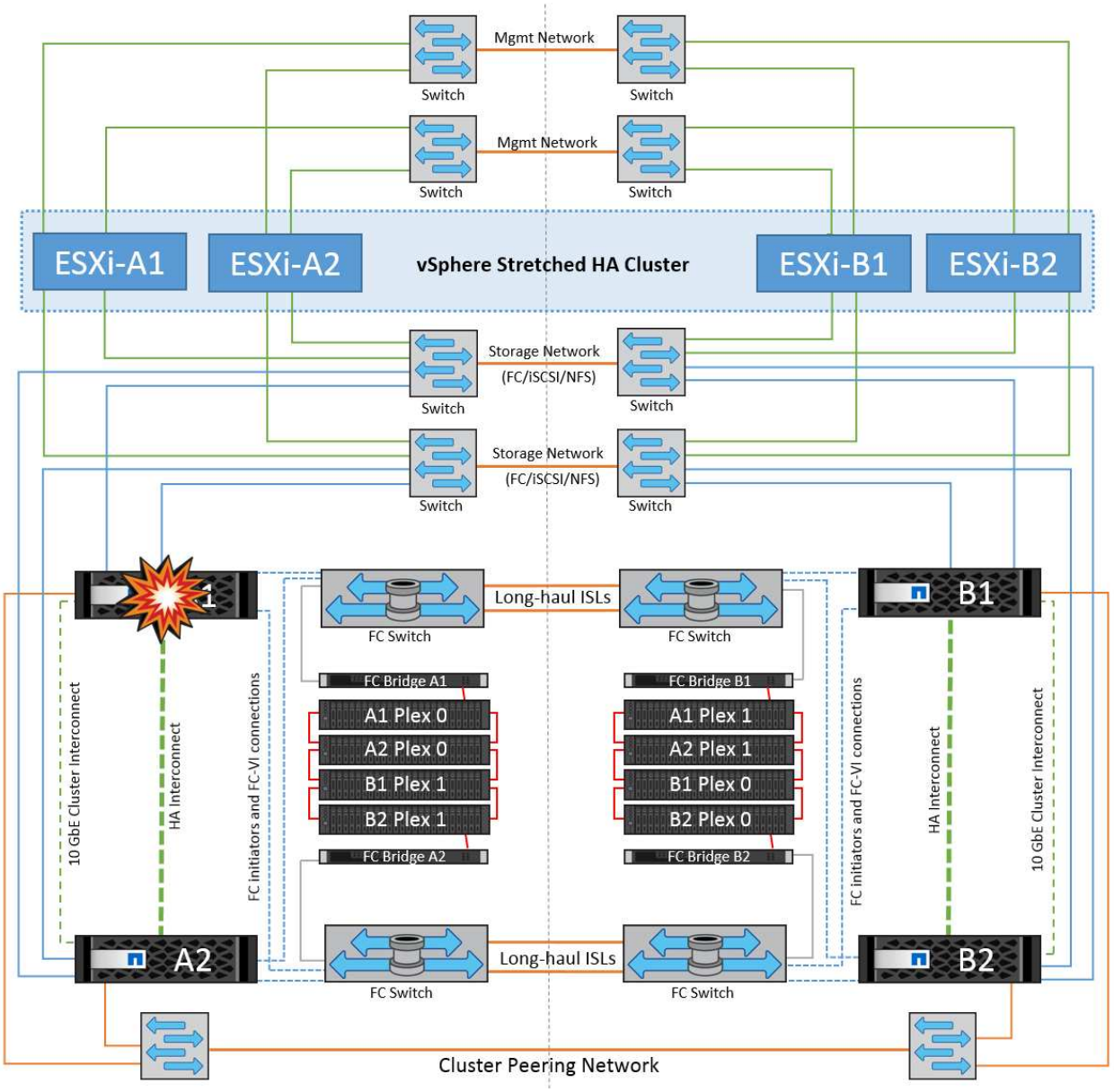
이 시나리오에서는 두 개 이상의 디스크에서 장애가 발생하거나 전체 쉘프에 장애가 발생합니다. 작동하는 플렉스에서 데이터 서비스를 중단하지 않고 데이터를 제공합니다. 디스크 장애가 로컬 또는 원격 플렉스에 영향을 줄 수 있습니다. 하나의 플렉스만 활성 상태이므로 애그리게이트가 성능 저하 모드로 표시됩니다. 장애가 발생한 디스크를 교체하면 영향을 받는 애그리게이트가 자동으로 다시 동기화되어 데이터를 재구축합니다. 다시 동기화하면 애그리게이트가 정상 미러링된 모드로 자동으로 돌아갑니다. 단일 RAID 그룹 내에서 두 개 이상의 디스크에 장애가 발생한 경우 플렉스를 재구축해야 합니다.



- [참고]
- 이 기간 동안에는 가상 머신 입출력 작업에 영향을 주지 않지만 ISL 링크를 통해 원격 디스크 셸프에서 데이터에 액세스하므로 성능이 저하됩니다.

단일 스토리지 컨트롤러 장애

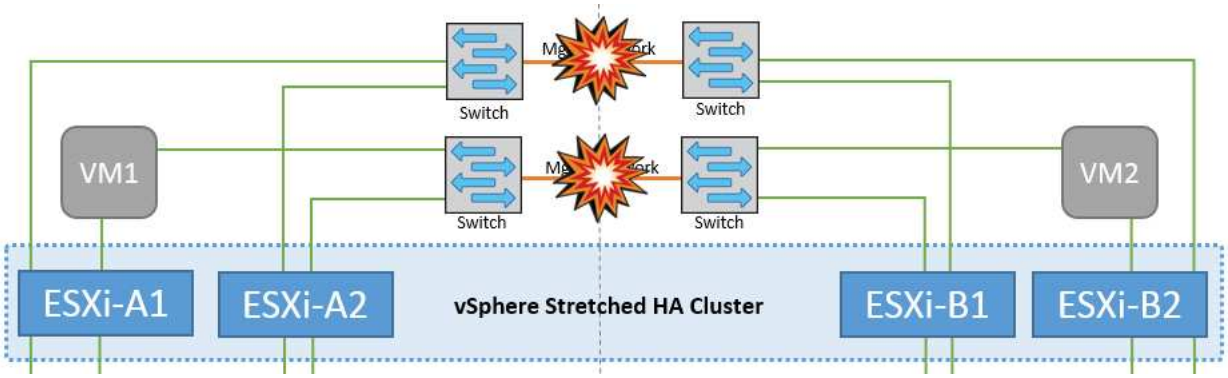
이 시나리오에서는 두 스토리지 컨트롤러 중 하나가 한 사이트에서 장애가 발생합니다. 각 사이트에 HA 쌍이 있으므로 한 노드에 장애가 발생하면 운영에 영향을 미치지 않고 다른 노드에 대한 페일오버가 자동으로 트리거됩니다. 예를 들어 노드 A1에 장애가 발생하면 해당 스토리지 및 워크로드가 자동으로 노드 A2로 전송됩니다. 모든 플렉스를 사용할 수 있으므로 가상 머신은 영향을 받지 않습니다. 두 번째 사이트 노드(B1 및 B2)는 영향을 받지 않습니다. 또한 클러스터의 마스터 노드가 네트워크 하트비트를 계속 수신하므로 vSphere HA는 아무 작업도 수행하지 않습니다.



장애 조치가 롤링 재해의 일부인 경우(노드 A1이 A2로 장애 조치), A2의 후속 장애 또는 사이트 A의 전체 장애가 발생한 경우 사이트 B에서 재해가 발생한 후 전환이 발생할 수 있습니다

인터스위치 링크 오류

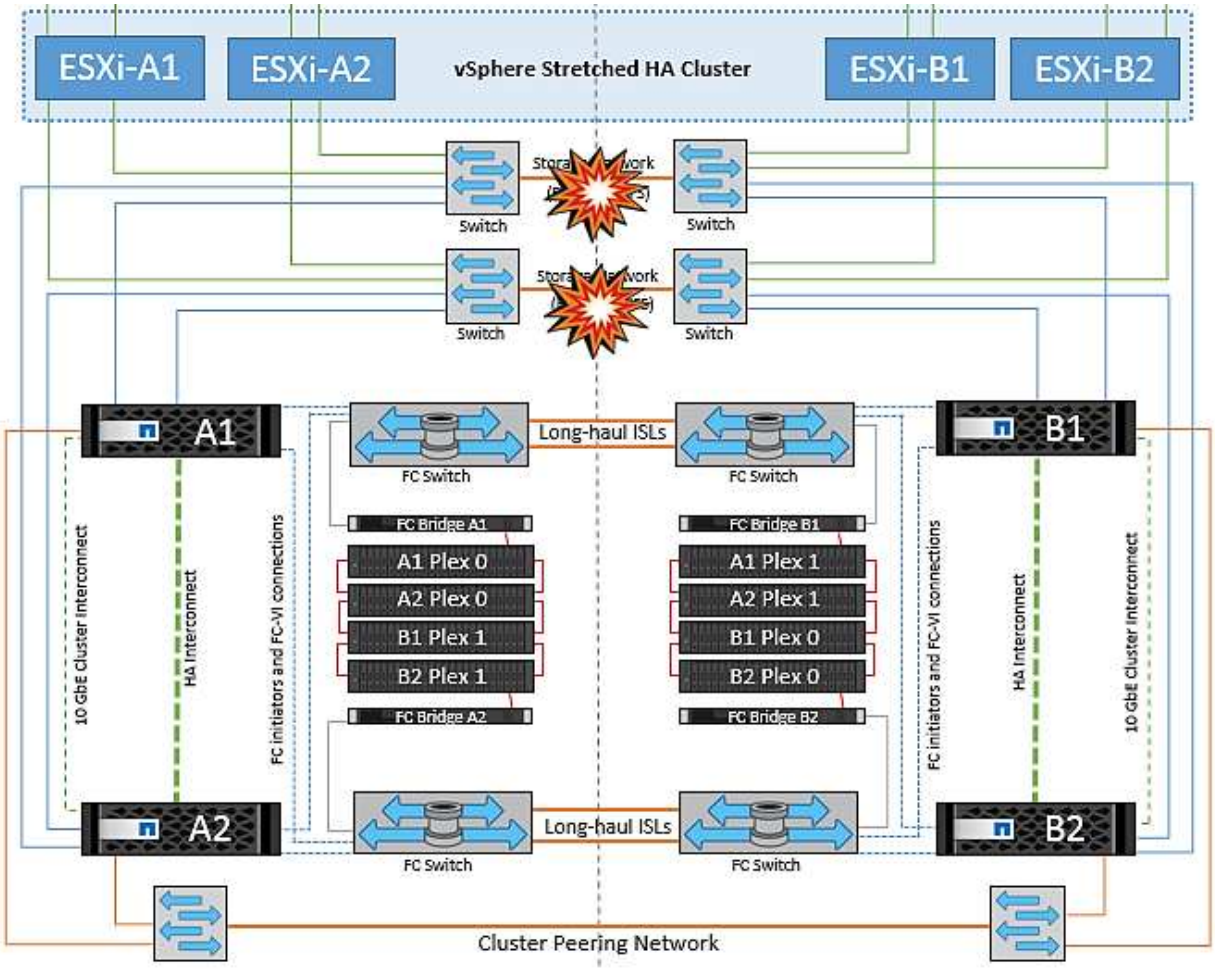
관리 네트워크에서 스위치 간 링크 오류



이 시나리오에서 프런트엔드 호스트 관리 네트워크의 ISL 링크에 장애가 발생하면 사이트 A의 ESXi 호스트가 사이트 B의 ESXi 호스트와 통신할 수 없습니다 특정 사이트의 ESXi 호스트는 네트워크 하트비트를 HA 클러스터의 마스터 노드로 보낼 수 없기 때문에 이로 인해 네트워크 파티션이 발생합니다. 따라서 파티션으로 인해 두 개의 네트워크 세그먼트가 있으며 각 세그먼트에는 특정 사이트 내의 호스트 장애로부터 VM을 보호하는 마스터 노드가 있습니다.

이 기간 동안 가상 머신은 실행 중인 상태로 유지되며 이 시나리오에서는 MetroCluster 동작이 변경되지 않습니다. 모든 데이터 저장소는 해당 사이트에서 그대로 유지됩니다.

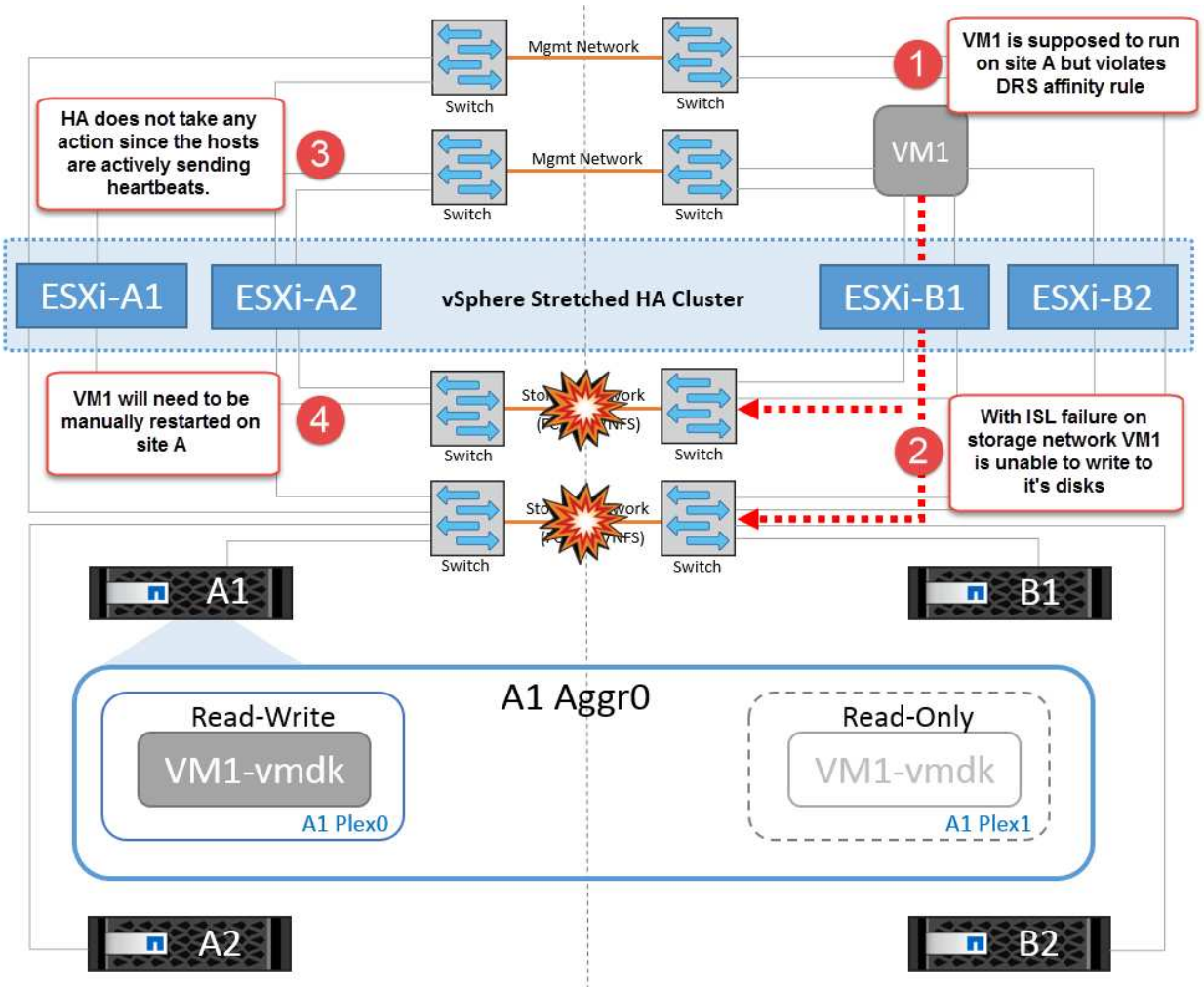
스토리지 네트워크에서 스위치 간 링크 오류



이 시나리오에서는 백엔드 스토리지 네트워크의 ISL 링크에 장애가 발생하면 사이트 A의 호스트가 사이트 B의 클러스터 B의 스토리지 볼륨 또는 LUN에 액세스할 수 없게 되며, 그 반대의 경우도 마찬가지입니다. VMware DRS 규칙은 호스트-스토리지 사이트 선호도를 통해 사이트 내에서 아무런 영향을 받지 않고 가상 시스템을 실행할 수 있도록 정의됩니다.

이 기간 동안 가상 머신은 해당 사이트에서 계속 실행되고 있으며 이 시나리오에서는 MetroCluster 동작이 변경되지 않습니다. 모든 데이터 저장소는 해당 사이트에서 그대로 유지됩니다.

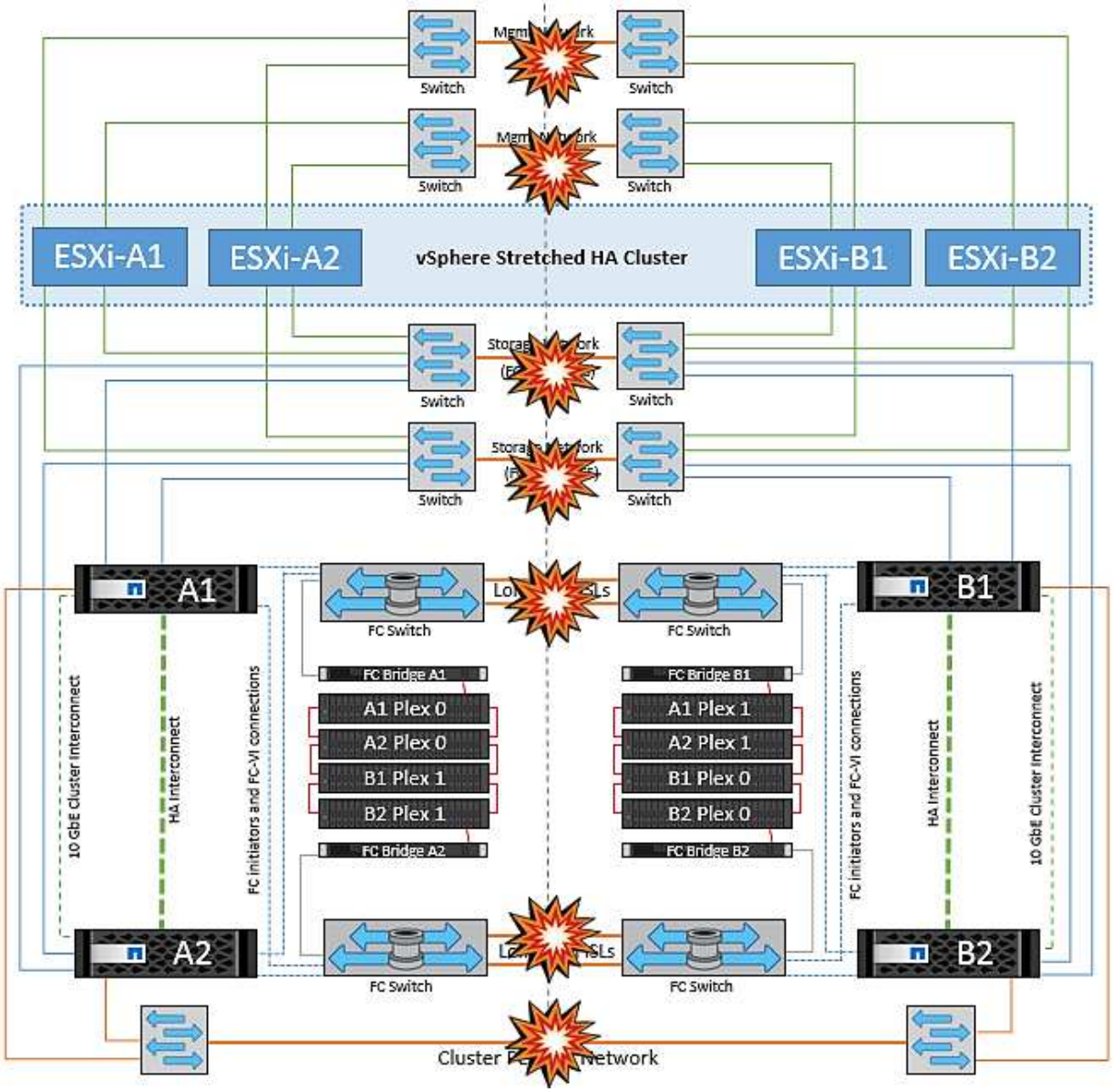
어떤 이유로 선호도 규칙을 위반하는 경우(예: 디스크가 로컬 클러스터 A 노드에 있는 사이트 A에서 실행되어야 하는 VM1이 사이트 B의 호스트에서 실행), 가상 머신의 디스크는 ISL 링크를 통해 원격으로 액세스됩니다. ISL 링크 장애로 인해 사이트 B에서 실행되는 VM1은 스토리지 볼륨에 대한 경로가 다운되고 특정 가상 시스템이 다운되기 때문에 해당 디스크에 쓸 수 없습니다. 이러한 경우 VMware HA는 호스트가 심박동을 능동적으로 전송하기 때문에 아무 작업도 수행하지 않습니다. 이러한 가상 머신의 전원을 수동으로 끄고 해당 사이트에서 전원을 켜야 합니다. 다음 그림에서는 DRS 선호도 규칙을 위반하는 VM을 보여 줍니다.



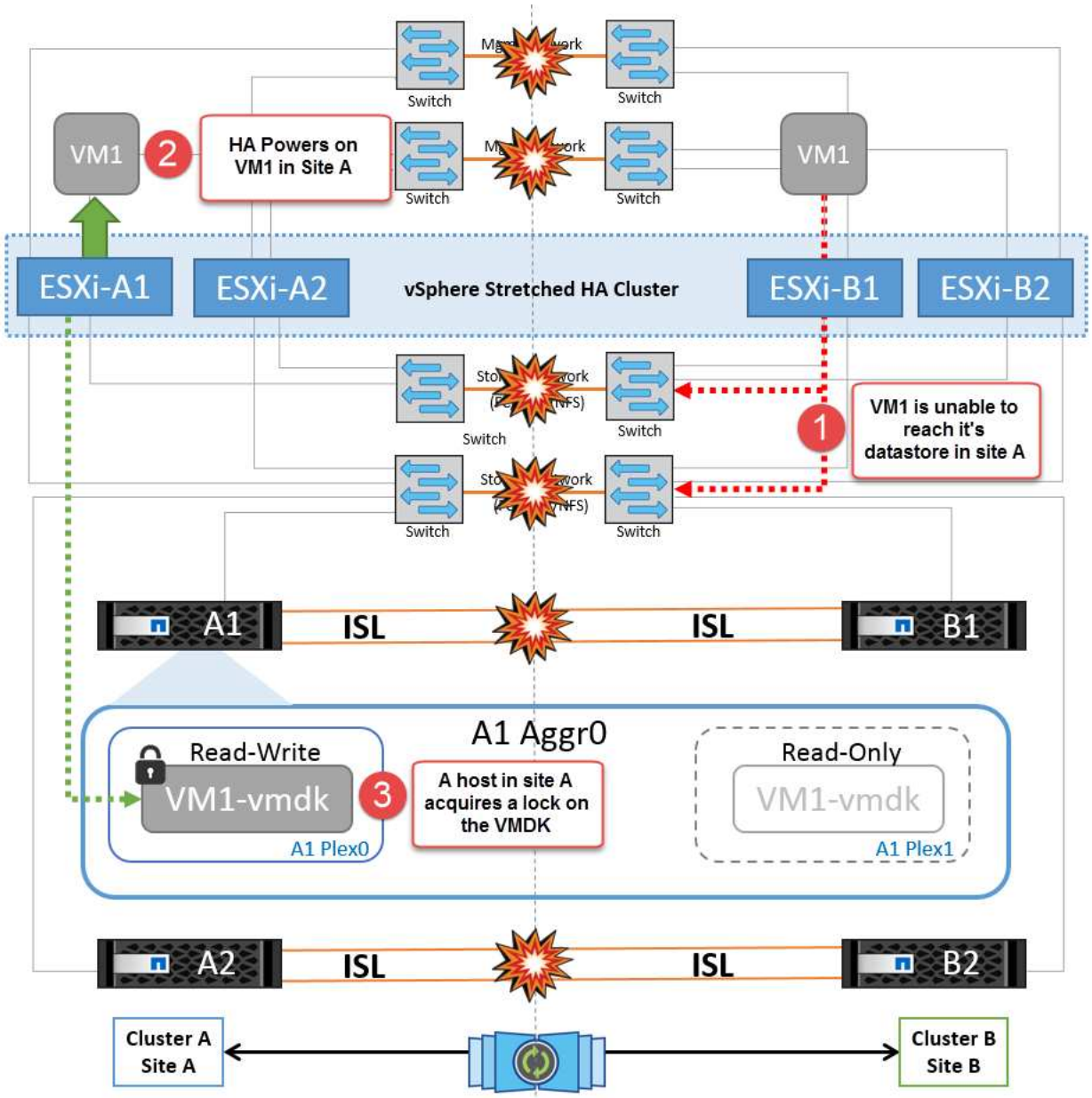
모든 인터스위치 오류 또는 전체 데이터 센터 파티션

이 시나리오에서는 사이트 간의 모든 ISL 링크가 다운되고 두 사이트가 서로 격리됩니다. 관리 네트워크 및 스토리지 네트워크에서 ISL 장애와 같은 이전 시나리오에서 설명한 것처럼 가상 머신은 완전한 ISL 장애에도 영향을 받지 않습니다.

ESXi 호스트가 사이트 간에 분할된 후 vSphere HA 에이전트는 데이터 저장소 하트비트를 확인하고 각 사이트에서 로컬 ESXi 호스트는 데이터 저장소 하트비트를 해당 읽기/쓰기 볼륨/LUN으로 업데이트할 수 있습니다. 사이트 A의 호스트는 네트워크/데이터 저장소 하트비트가 없기 때문에 사이트 B의 다른 ESXi 호스트에 장애가 발생한 것으로 가정합니다. 사이트 A의 vSphere HA는 사이트 B의 가상 머신을 재시작합니다. 그러면 스토리지 ISL 장애로 인해 사이트 B의 데이터 저장소에 액세스할 수 없기 때문에 결국 실패합니다. 비슷한 상황이 사이트 B에서 반복됩니다



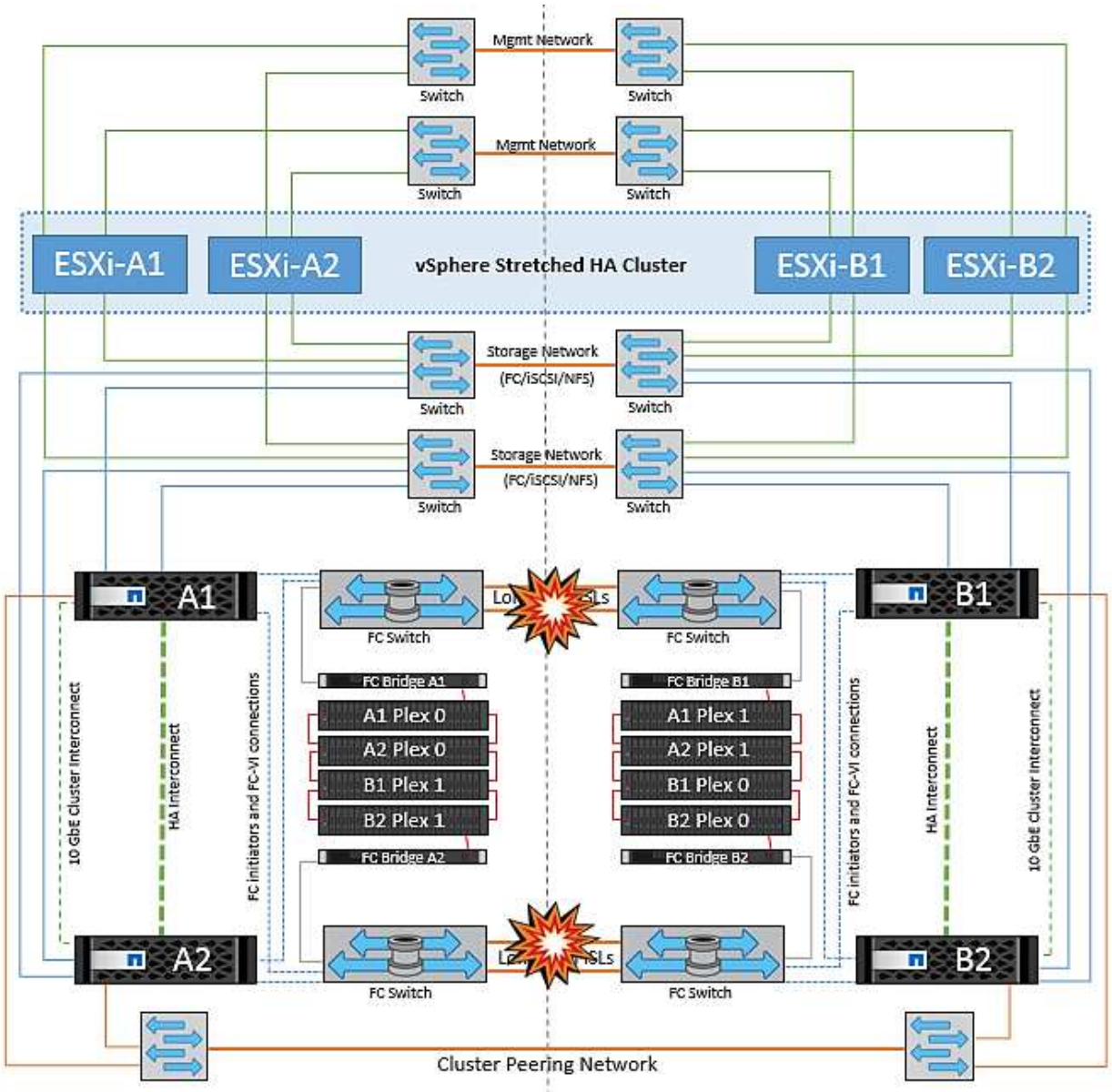
NetApp에서는 가상 시스템이 DRS 규칙을 위반했는지 여부를 확인하는 것이 좋습니다. 원격 사이트에서 실행되는 모든 가상 머신은 데이터 저장소에 액세스할 수 없으므로 작동이 중지되고 vSphere HA는 로컬 사이트에서 해당 가상 머신을 다시 시작합니다. ISL 링크가 다시 온라인 상태가 되면 동일한 MAC 주소로 실행되는 가상 시스템의 인스턴스가 두 개 있을 수 없으므로 원격 사이트에서 실행 중이던 가상 시스템이 종료됩니다.



NetApp MetroCluster의 두 **Fabric**에서 스위치 간 링크 장애가 발생했습니다

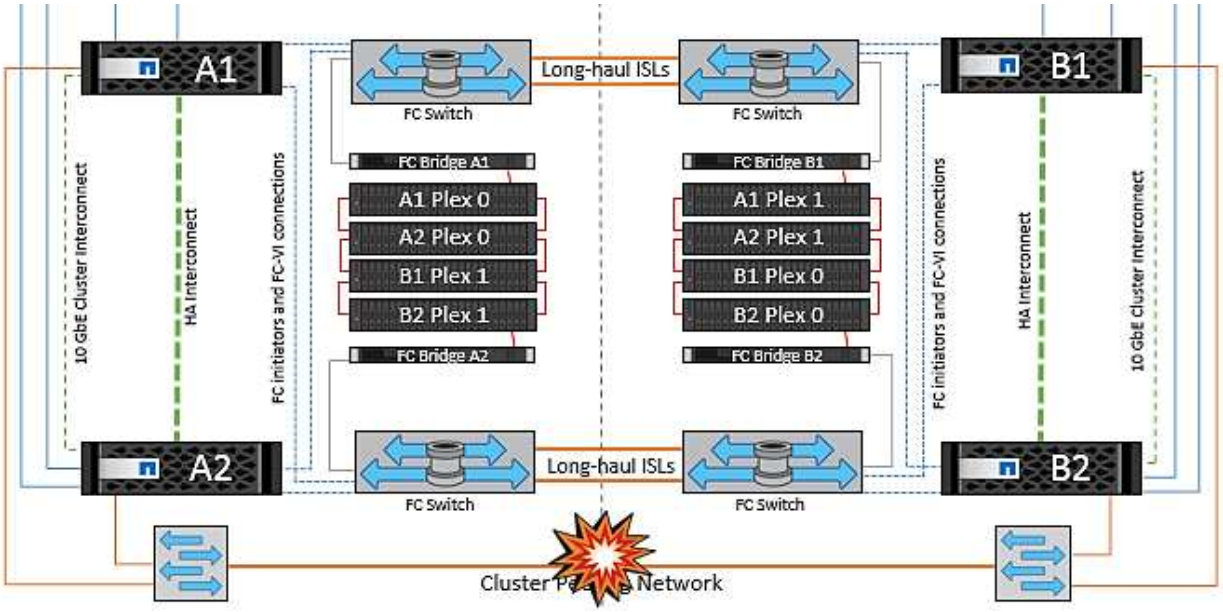
하나 이상의 ISL이 실패하는 경우 트래픽은 나머지 링크를 통해 계속됩니다. 두 Fabric의 모든 ISL에 장애가 발생하여 스토리지와 NVRAM 복제를 위해 사이트 간에 링크가 없는 경우, 각 컨트롤러는 계속해서 로컬 데이터를 제공합니다. 최소 하나의 ISL이 복구되면 모든 플렉스의 재동기화가 자동으로 수행됩니다.

모든 ISL이 다운된 후에 발생하는 모든 쓰기는 다른 사이트로 미러링되지 않습니다. 따라서 구성이 이 상태일 때 재해 발생 시 전환이 이루어지면 동기화되지 않은 데이터가 손실됩니다. 이 경우 전환 후 복구를 위해 수동 개입이 필요합니다. 장기간 사용할 수 있는 ISL이 없을 경우 관리자는 모든 데이터 서비스를 종료하여 재해 발생 시 전환이 필요할 경우 데이터 손실 위험을 피할 수 있습니다. 이 작업을 수행하는 것은 하나 이상의 ISL을 사용할 수 있게 되기 전에 전환이 필요한 재해의 가능성과 비교해야 합니다. 또는 다중 구간 시나리오에서 ISL이 실패하는 경우 관리자가 모든 링크에 장애가 발생하기 전에 사이트 중 하나로 계획된 전환을 트리거할 수 있습니다.



피어링된 클러스터 링크 장애

피어링된 클러스터 링크 장애 시나리오에서 패브릭 ISL은 여전히 활성 상태이므로 두 사이트에서 데이터 서비스(읽기 및 쓰기)가 두 플렉스에 계속 적용됩니다. 클러스터 구성 변경(예: 새 SVM 추가, 기존 SVM에서 볼륨 또는 LUN 프로비저닝)은 다른 사이트에 전파될 수 없습니다. 이러한 데이터는 로컬 CRS 메타데이터 볼륨에 보관되며 피어링된 클러스터 링크가 복구되면 자동으로 다른 클러스터로 전파됩니다. 피어링된 클러스터 링크를 복원하기 전에 강제 전환이 필요한 경우 전환 프로세스의 일부로 남아 있는 사이트에 있는 메타데이터 볼륨의 원격 복제 복사본에서 미결 클러스터 구성 변경 사항이 자동으로 재생됩니다.



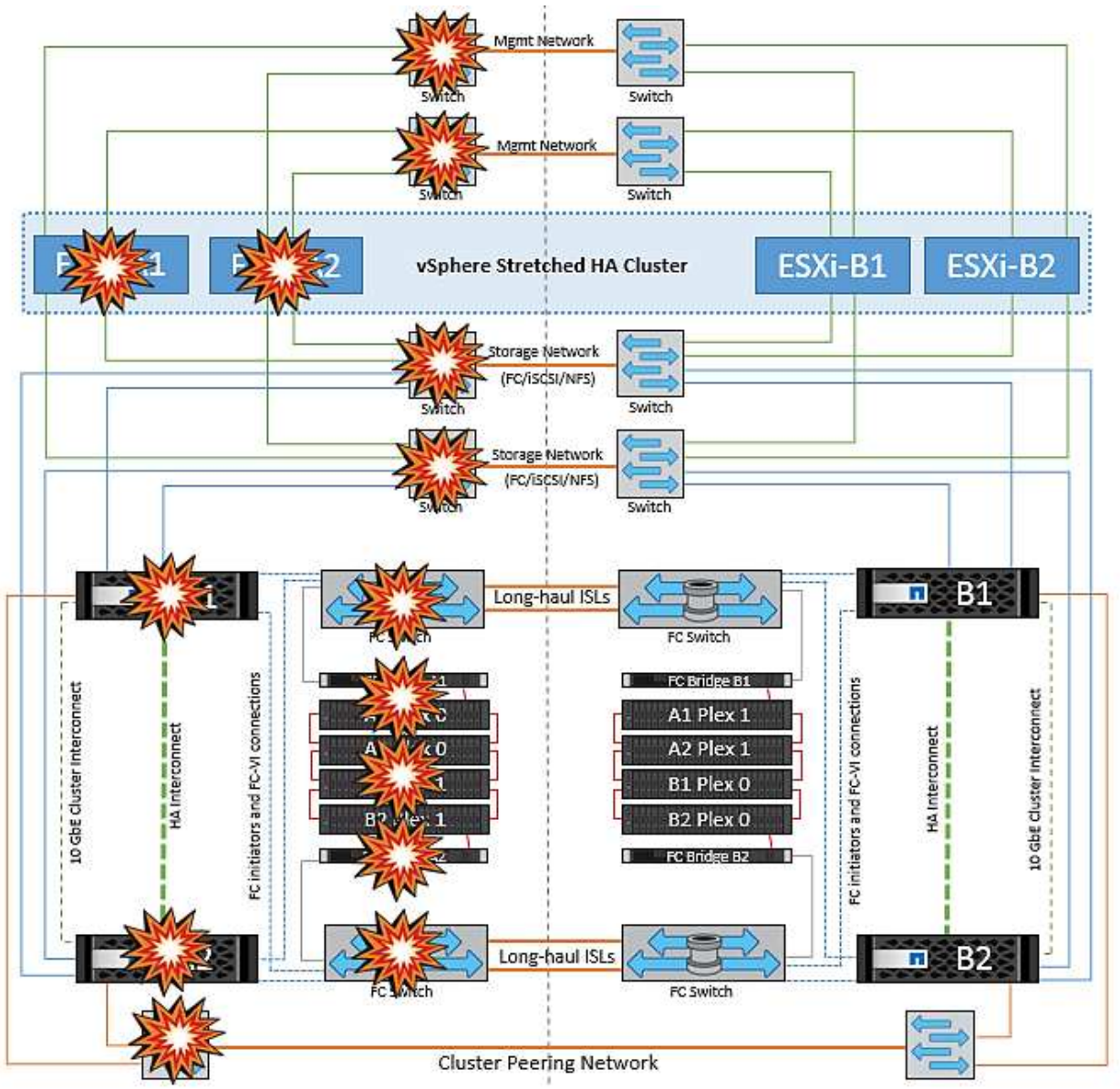
전체 사이트 오류입니다

전체 사이트 A 장애 시나리오에서 사이트 B에 있는 ESXi 호스트는 사이트 A의 ESXi 호스트에서 다운되었기 때문에 네트워크 하트비트를 가져오지 않습니다. 사이트 B의 HA 마스터는 데이터 저장소 하트비트가 없는지 확인하고, 사이트 A의 호스트가 실패하도록 선언한 다음 사이트 B의 가상 머신을 재시작합니다 이 기간 동안 스토리지 관리자는 스위치오버를 수행하여 장애가 발생한 사이트의 노드 서비스를 재개하고 사이트 B에 있는 사이트 A의 모든 스토리지 서비스를 복구합니다 사이트 B에서 사이트 A 볼륨 또는 LUN을 사용할 수 있게 되면 HA 마스터 에이전트가 사이트 B에서 사이트 A 가상 머신을 재시작합니다

vSphere HA 마스터 에이전트의 VM 재시작 시도(등록 및 전원 켜기 포함)가 실패하면 지연 후 재시작됩니다. 다시 시작 사이의 지연은 최대 30분까지 구성할 수 있습니다. vSphere HA는 최대 시도 횟수(기본적으로 6회 시도)에 대해 이러한 재시작을 시도합니다.

HA 마스터는 배치 관리자가 적합한 스토리지를 찾을 때까지 재시작 시도를 시작하지 않으므로, 전체 사이트 장애가 발생한 경우 전환이 수행된 후에 다시 시작합니다.

사이트 A가 페일오버된 경우 정상 사이트 B 노드 중 하나의 후속 장애 조치를 통해 정상적인 노드로 원활하게 처리할 수 있습니다. 이 경우 4개 노드의 작업은 현재 하나의 노드에서만 수행됩니다. 이 경우 복구는 로컬 노드로의 반환 수행으로 구성됩니다. 그런 다음 사이트 A가 복구되면 구성의 안정적 상태 작업을 복원하기 위한 스위치백 작업이 수행됩니다.



제품 보안

VMware vSphere용 ONTAP 툴

ONTAP Tools for VMware vSphere의 소프트웨어 엔지니어링에서는 다음과 같은 보안 개발 활동을 활용합니다.

- * 위협 모델링. * 위협 모델링의 목적은 소프트웨어 개발 수명 주기 초기에 피처, 부품 또는 제품의 보안 결함을 발견하기 위한 것입니다. 위협 모델은 응용 프로그램의 보안에 영향을 주는 모든 정보의 구조적 표현입니다. 본질적으로 보안 렌즈를 통해 응용 프로그램과 환경을 볼 수 있습니다.
- * DAST(Dynamic Application Security Testing). * 이 기술은 실행 중인 응용 프로그램의 취약한 상태를 감지하도록 설계되었습니다. DAST는 웹 활성화 애플리케이션의 노출된 HTTP 및 HTML 인터페이스를 테스트합니다.
- * 타사 코드 통화. * 오픈 소스 소프트웨어(OSS)를 통한 소프트웨어 개발의 일환으로 제품에 통합된 OSS와 관련된 보안 취약점을 해결해야 합니다. 이는 새로운 OSS 버전에 새로 발견된 취약점이 언제든지 보고될 수 있기 때문에 지속적인 노력입니다.

- * 취약성 검사. * 취약성 검사의 목적은 NetApp 제품이 고객에게 공개되기 전에 NetApp 제품의 알려진 공통 보안 취약점을 감지하는 것입니다.
- * 침투 테스트 * 침투 테스트는 시스템, 웹 응용 프로그램 또는 네트워크를 평가하여 공격자가 악용할 수 있는 보안 취약점을 찾는 프로세스입니다. NetApp의 침투 테스트(펜 테스트)는 승인되고 신뢰할 수 있는 타사 기업의 그룹에 의해 수행됩니다. 이러한 테스트 범위에는 정교한 악용 방법이나 도구를 사용하는 악의적인 침입자나 해커에 유사한 응용 프로그램 또는 소프트웨어에 대한 공격이 포함됩니다.

제품 보안 기능

VMware vSphere용 ONTAP 툴에는 각 릴리즈에 다음과 같은 보안 기능이 포함되어 있습니다.

- * 로그인 배너. * SSH는 기본적으로 비활성화되어 있으며 VM 콘솔에서 활성화된 경우 1회만 로그인할 수 있습니다. 사용자가 로그인 프롬프트에 사용자 이름을 입력하면 다음 로그인 배너가 표시됩니다.

  경고:* 이 시스템에 대한 무단 액세스는 금지되며 법률로 기소됩니다. 이 시스템에 액세스하면 무단 사용이 의심되는 경우 사용자의 조치를 모니터링할 수 있다는 데 동의하는 것입니다.

  사용자가 SSH 채널을 통한 로그인을 완료하면 다음 텍스트가 표시됩니다.

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * 역할 기반 액세스 제어(RBAC). * 두 가지 유형의 RBAC 컨트롤이 ONTAP 도구에 연결되어 있습니다.
  - 기본 vCenter Server 권한
  - vCenter 플러그인별 권한 자세한 내용은 을 참조하십시오 "이 링크".
- * 암호화된 통신 채널. * 모든 외부 통신은 TLS 버전 1.2를 사용하여 HTTPS를 통해 이루어집니다.
- * 최소 포트 노출. * 필요한 포트만 방화벽에서 열립니다.

  다음 표에서는 열려 있는 포트의 세부 정보를 설명합니다.

TCP v4/V6 포트 번호	방향	기능
8143	인바운드	REST API용 HTTPS 연결
8043을 참조하십시오	인바운드	HTTPS 연결
9060입니다	인바운드	HTTPS 연결 https 연결을 통한 SOAP에 사용됩니다 클라이언트가 ONTAP 도구 API 서버에 연결할 수 있도록 하려면 이 포트를 열어야 합니다.
22	인바운드	SSH(기본적으로 비활성화됨)

TCP v4/V6 포트 번호	방향	기능
9080입니다	인바운드	HTTPS 연결 - VP 및 SRA - 루프백에서만 내부 연결
9083	인바운드	HTTPS 연결 - VP 및 SRA https 연결을 통한 SOAP에 사용됩니다
1162	인바운드	VP SNMP 트랩 패킷입니다
1527년	내부 전용	Derby 데이터베이스 포트, 이 컴퓨터와 자체 사이에서만, 외부 연결은 허용되지 않음 — 내부 연결만
443	양방향	ONTAP 클러스터에 연결하는 데 사용됩니다

- * CA(인증 기관) 서명 인증서 지원. * VMware vSphere용 ONTAP 툴은 CA 서명 인증서를 지원합니다. 자세한 내용은 다음을 참조하십시오 "KB 문서를 참조하십시오" 를 참조하십시오.
- * 감사 로깅. * 지원 번들은 다운로드할 수 있으며 매우 자세히 설명되어 있습니다. ONTAP 도구는 모든 사용자 로그인 및 로그아웃 활동을 별도의 로그 파일에 기록합니다. VASA API 호출은 전용 VASA 감사 로그(로컬 CXF.log)에 기록됩니다.
- 암호 정책 * 다음 암호 정책을 따릅니다.
  - 암호는 로그 파일에 기록되지 않습니다.
  - 암호는 일반 텍스트로 전달되지 않습니다.
  - 암호는 설치 과정 중에 구성됩니다.
  - 암호 기록은 구성 가능한 매개 변수입니다.
  - 최소 암호 사용 기간은 24시간으로 설정됩니다.
  - 암호 필드에 대한 자동 완성 기능이 비활성화됩니다.
  - ONTAP 도구는 SHA256 해싱을 사용하여 저장된 모든 자격 증명 정보를 암호화합니다.

SnapCenter 플러그인 VMware vSphere

NetApp SnapCenter Plug-in for VMware vSphere 소프트웨어 엔지니어링은 다음과 같은 안전한 개발 활동을 사용합니다.

- * 위협 모델링. * 위협 모델링의 목적은 소프트웨어 개발 수명 주기 초기에 피처, 부품 또는 제품의 보안 결함을 발견하기 위한 것입니다. 위협 모델은 응용 프로그램의 보안에 영향을 주는 모든 정보의 구조적 표현입니다. 본질적으로 보안 렌즈를 통해 응용 프로그램과 환경을 볼 수 있습니다.
- * DAST(Dynamic Application Security Testing). * 실행 상태의 응용 프로그램에서 취약한 상태를 감지하도록 설계된 기술입니다. DAST는 웹 활성화 애플리케이션의 노출된 HTTP 및 HTML 인터페이스를 테스트합니다.
- * 타사 코드 통화. * 소프트웨어를 개발하고 오픈 소스 소프트웨어(OSS)를 사용하는 과정에서 제품에 통합된 OSS와 관련된 보안 취약점을 해결하는 것이 중요합니다. 이는 항상 OSS 구성 요소 버전에 새로 발견된 취약점이 보고될 수 있기 때문에 지속적으로 발생하는 것입니다.
- * 취약성 검사. * 취약성 검사의 목적은 NetApp 제품이 고객에게 공개되기 전에 NetApp 제품의 알려진 공통 보안 취약점을 감지하는 것입니다.

- * 침투 테스트 * 침투 테스트는 시스템, 웹 응용 프로그램 또는 네트워크를 평가하여 공격자가 악용할 수 있는 보안 취약점을 찾는 프로세스입니다. NetApp의 침투 테스트(펜 테스트)는 승인되고 신뢰할 수 있는 타사 기업의 그룹에 의해 수행됩니다. 이러한 테스트 범위에는 정교한 악용 방법이나 도구를 사용하는 악의적인 침입자나 해커 같은 응용 프로그램 또는 소프트웨어에 대한 공격이 포함됩니다.
- * 제품 보안 문제의 대응 활동 * 보안 취약성은 사내외에서 발견되며 적시에 해결되지 않을 경우 NetApp의 평판에 심각한 위험을 초래할 수 있습니다. 이 프로세스를 용이하게 하기 위해 PSIRT(Product Security Incident Response Team)는 취약점을 보고 및 추적합니다.

제품 보안 기능

VMware vSphere용 NetApp SnapCenter 플러그인에는 각 릴리즈마다 다음과 같은 보안 기능이 포함되어 있습니다.

- * 제한된 셸 액세스. * SSH는 기본적으로 비활성화되어 있으며, VM 콘솔에서 활성화된 경우에만 1회 로그인이 허용됩니다.
- 로그인 배너에 액세스 경고 * 로그인 프롬프트에 사용자 이름을 입력하면 다음 로그인 배너가 표시됩니다.

  경고:* 이 시스템에 대한 무단 액세스는 금지되며 법률로 기소됩니다. 이 시스템에 액세스하면 무단 사용이 의심되는 경우 사용자의 조치를 모니터링할 수 있다는 데 동의하는 것입니다.

  사용자가 SSH 채널을 통해 로그인을 완료하면 다음 출력이 표시됩니다.

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * 역할 기반 액세스 제어(RBAC). * 두 가지 유형의 RBAC 컨트롤이 ONTAP 도구에 연결되어 있습니다.
  - 기본 vCenter Server 권한
  - VMware vCenter 플러그인별 권한 자세한 내용은 을 참조하십시오 "역할 기반 액세스 제어(RBAC)".
- * 암호화된 통신 채널. * 모든 외부 통신은 TLS를 사용하여 HTTPS를 통해 이루어집니다.
- * 최소 포트 노출. * 필요한 포트만 방화벽에서 열립니다.

다음 표에는 열려 있는 포트 세부 정보가 나와 있습니다.

TCP v4/V6 포트 번호	기능
8144를 참조하십시오	REST API용 HTTPS 연결
8080	OVA GUI에 대한 HTTPS 연결
22	SSH(기본적으로 비활성화됨)
3306입니다	MySQL(내부 연결에만 해당, 외부 연결은 기본적으로 비활성화됨)
443	Nginx(데이터 보호 서비스)

- * CA(인증 기관) 서명 인증서 지원 * VMware vSphere용 SnapCenter 플러그인은 CA 서명 인증서의 기능을 지원합니다. 을 참조하십시오 "SSL 인증서를 생성 및/또는 VMware vSphere용 SnapCenter 플러그인(SCV)으로 가져오는 방법".
- * 암호 정책 * 다음 암호 정책이 적용됩니다.
  - 암호는 로그 파일에 기록되지 않습니다.
  - 암호는 일반 텍스트로 전달되지 않습니다.
  - 암호는 설치 과정 중에 구성됩니다.
  - 모든 자격 증명 정보는 SHA256 해싱을 사용하여 저장됩니다.
- 기본 운영 체제 이미지. 이 제품은 제한된 액세스 및 쉘 액세스가 비활성화된 OVA용 Debian Base OS와 함께 제공됩니다. 이렇게 하면 공격 발생 가능성이 줄어듭니다. 모든 SnapCenter 릴리스 기본 운영 체제는 보안 범위를 극대화하기 위해 최신 보안 패치로 업데이트됩니다.

NetApp은 VMware vSphere 어플라이언스인 SnapCenter 플러그인과 관련된 소프트웨어 기능 및 보안 패치를 개발한 다음 고객에게 번들 소프트웨어 플랫폼으로 배포합니다. 이러한 어플라이언스에는 특정 Linux 하위 운영 체제 종속성 및 NetApp의 독점 소프트웨어가 포함되어 있으므로 하위 운영 체제를 변경하지 않는 것이 좋습니다. 이 경우 NetApp 어플라이언스에 영향을 줄 가능성이 매우 높기 때문입니다. 이는 NetApp의 어플라이언스 지원 기능에 영향을 미칠 수 있습니다. 보안 관련 문제를 해결하기 위해 NetApp은 어플라이언스의 최신 코드 버전을 테스트하고 구축할 것을 권장합니다.

VMware vSphere용 ONTAP 툴에 대한 보안 강화 가이드

VMware vSphere 9.13용 ONTAP 툴에 대한 보안 강화 가이드

VMware vSphere용 ONTAP 툴에 대한 보안 강화 가이드에서는 가장 안전한 설정을 구성하기 위한 포괄적인 지침을 제공합니다.

이 가이드는 어플라이언스 자체의 애플리케이션과 게스트 OS 모두에 적용됩니다.

VMware vSphere 9.13 설치 패키지용 ONTAP 툴의 무결성 확인

고객은 두 가지 방법으로 ONTAP 도구 설치 패키지의 무결성을 확인할 수 있습니다.

1. 체크섬 확인
2. 서명을 확인하는 중입니다

체크섬은 OTV 설치 패키지의 다운로드 페이지에 제공됩니다. 사용자는 다운로드 페이지에 제공된 체크섬과 비교하여 다운로드한 패키지의 체크섬을 확인해야 합니다.

ONTAP 도구 OVA의 서명 확인

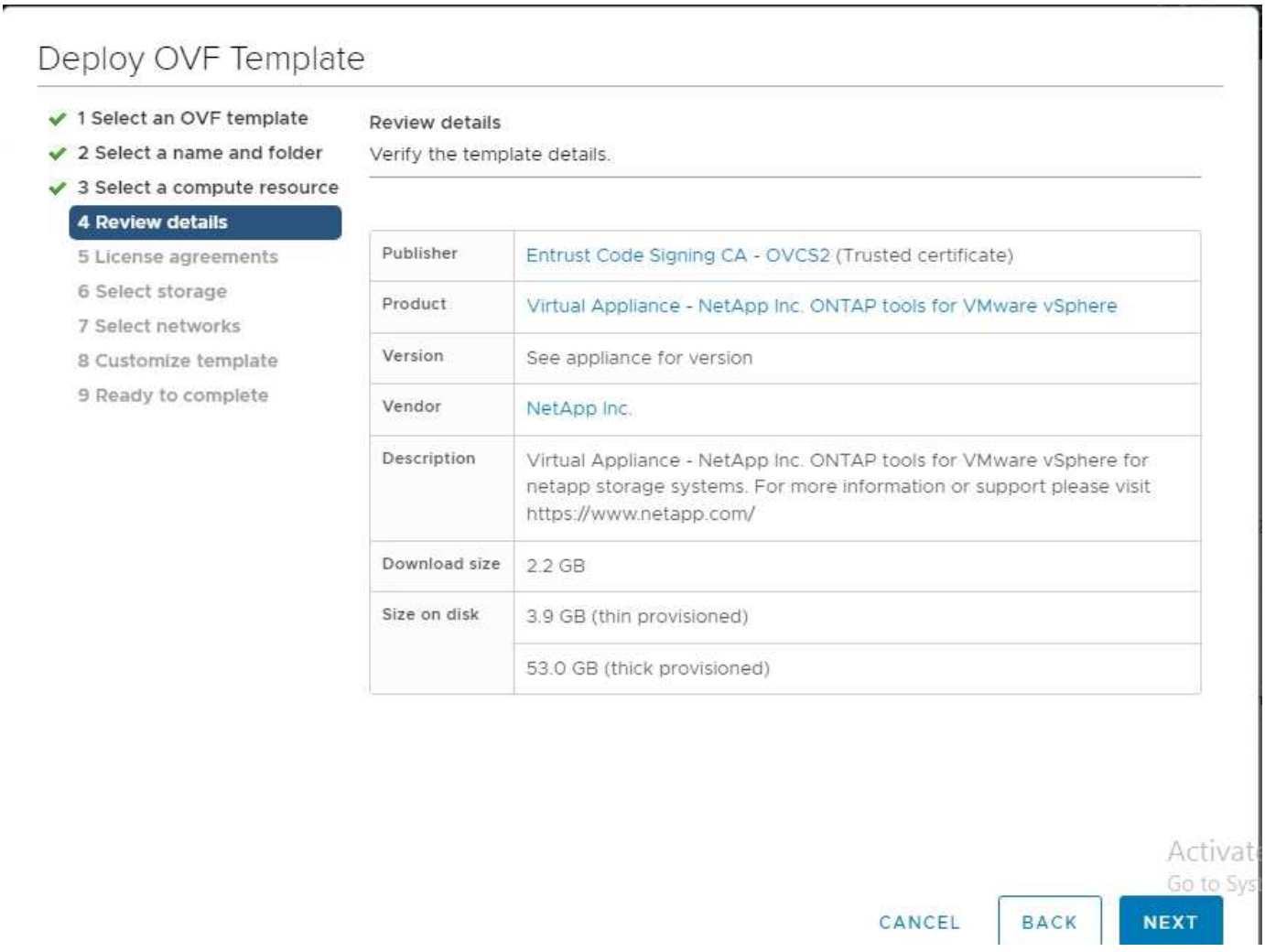
vApp 설치 패키지는 타볼 형태로 제공됩니다. 이 타볼에는 README 파일 및 OVA 패키지와 함께 가상 어플라이언스에 대한 중간 및 루트 인증서가 포함되어 있습니다. README 파일은 사용자에게 vApp OVA 패키지의 무결성을 확인하는 방법을 안내합니다.

또한 vCenter 버전 7.0U3E 이상에서 제공된 루트 및 중간 인증서를 업로드해야 합니다. 7.0.1 및 7.0.U3E 사이의 vCenter 버전의 경우 인증서 확인 기능은 VMware에서 지원되지 않습니다. 고객은 vCenter 버전 6.x에 대한 인증서를 업로드할 필요가 없습니다

신뢰할 수 있는 루트 인증서를 **vCenter**에 업로드하는 중입니다

1. VMware vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. administrator@vsphere.loca l 또는 vCenter Single Sign-On Administrators 그룹의 다른 구성원에 대한 사용자 이름과 암호를 지정합니다. 설치 중에 다른 도메인을 지정한 경우 administrator@mydomain으로 로그인합니다.
3. 인증서 관리 UI로 이동합니다. a. 홈 메뉴에서 관리를 선택합니다. b. 인증서에서 인증서 관리를 클릭합니다.
4. 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.
5. 신뢰할 수 있는 루트 인증서에서 추가를 클릭합니다.
6. 찾아보기 를 클릭하고 certificate.pem 파일(OTV_OVA_INTER_ROOT_CERT_CHAIN.pem)의 위치를 선택합니다.
7. 추가 를 클릭합니다. 인증서가 저장소에 추가됩니다.

을 참조하십시오 "인증서 저장소에 신뢰할 수 있는 루트 인증서를 추가합니다" 를 참조하십시오. OVA 파일을 사용하여 vApp을 구축하는 동안 vApp 패키지의 디지털 서명을 'Review details' 페이지에서 확인할 수 있습니다. 다운로드한 vApp 패키지가 정품이면 '게시자' 열에 '신뢰할 수 있는 인증서'가 표시됩니다(다음 스크린샷 참조).



ONTAP 도구 **ISO** 및 **SRA tar.gz** 서명 확인

NetApp는 OTV-iso 및 SRA.tgz용 제품 zip 파일과 함께 제품 다운로드 페이지의 고객과 코드 서명 인증서를 공유합니다.

코드 서명 인증서에서 사용자는 다음과 같이 공개 키를 추출할 수 있습니다.

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
```

그런 다음 공개 키를 사용하여 아래와 같이 `ISO` 및 `tgz` 제품 `zip`의 서명을 확인해야 합니다.

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file>
<binary-name>
```

예:

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

ONTAP 도구용 포트 및 프로토콜 9.13

이 슬라이드에는 VMware vSphere 서버용 ONTAP 툴과 관리 스토리지 시스템, 서버 및 기타 구성 요소 등의 기타 엔터티 간의 통신을 지원하는 데 필요한 포트와 프로토콜이 나와 있습니다.

OTV에 필요한 인바운드 및 아웃바운드 포트

아래 표에는 ONTAP 도구의 올바른 작동에 필요한 인바운드 및 아웃바운드 포트가 나열되어 있습니다. 표에 나와 있는 포트만 원격 컴퓨터에서 연결할 수 있도록 열려 있고 다른 모든 포트는 원격 컴퓨터에서 연결할 수 있도록 차단해야 합니다. 이렇게 하면 시스템의 보안 및 안전을 보장할 수 있습니다.

다음 표에서는 열려 있는 포트의 세부 정보를 설명합니다.

* TCP v4/v6 포트 # *	* 방향 *	* 기능 *
8143	인바운드	REST API용 HTTPS 연결
8043을 참조하십시오	인바운드	HTTPS 연결
9060입니다	인바운드	HTTPS 연결 HTTPS 연결을 통한 SOAP+에 사용됩니다 클라이언트가 ONTAP 도구 API 서버에 연결할 수 있도록 하려면 이 포트를 열어야 합니다.
22	인바운드	SSH(기본적으로 비활성화됨)
9080입니다	인바운드	HTTPS 연결 - VP 및 SRA - 루프백에서만 내부 연결
9083	인바운드	HTTPS 연결 - VP 및 SRA+ HTTPS 연결을 통한 SOAP에 사용됩니다

* TCP v4/v6 포트 # *	* 방향 *	* 기능 *
1162	인바운드	VP SNMP 트랩 패킷입니다
8443	인바운드	원격 플러그인
1527년	내부 전용	Derby 데이터베이스 포트, 이 컴퓨터와 자체 사이에서만 외부 연결이 허용되지 않음 - 내부 연결만 해당
8150입니다	내부 전용	로그 무결성 서비스가 포트에서 실행됩니다
443	양방향	ONTAP 클러스터에 연결하는 데 사용됩니다

Derby 데이터베이스에 대한 원격 액세스 제어

관리자는 다음 명령을 사용하여 derby 데이터베이스에 액세스할 수 있습니다. ONTAP 도구 로컬 VM 및 원격 서버를 통해 다음 단계에 따라 액세스할 수 있습니다.

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

*example: *

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                    |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                    |
SYS                 |SYSCHECKS                     |
SYS                 |SYSCOLPERMS                   |
SYS                 |SYSCOLUMNS                    |
SYS                 |SYSCONGLOMERATES              |
SYS                 |SYSCONSTRAINTS                |
SYS                 |SYSDEPENDS                    |
SYS                 |SYSFILES                      |
SYS                 |SYSFOREIGNKEYS                |
SYS                 |SYSKEYS                       |
SYS                 |SYSPERMS                      |
```

VMware vSphere 9.13 액세스 포인트용 ONTAP 툴(사용자)

VMware vSphere용 ONTAP 툴은 세 가지 유형의 사용자를 생성하고 사용합니다.

1. 시스템 사용자: 루트 사용자 계정입니다
2. 애플리케이션 사용자: 관리자 사용자, 유지보수 사용자 및 DB 사용자 계정
3. 지원 사용자: diag 사용자 계정입니다

1.시스템 사용자

시스템 (루트) 사용자는 기본 운영 체제 (데비안)에 ONTAP 도구 설치로 생성됩니다.

- 기본 시스템 사용자 "root"는 ONTAP 도구 설치로 데비안에 생성됩니다. 기본값은 비활성화되며 '이전' 콘솔을 통해

애드혹 방식으로 활성화할 수 있습니다.

응용 프로그램 사용자

응용 프로그램 사용자의 이름은 ONTAP 도구에서 로컬 사용자로 지정됩니다. ONTAP 도구 응용 프로그램에서 만든 사용자입니다. 아래 표에는 애플리케이션 사용자 유형이 나와 있습니다.

* 사용자 *	* 설명 *
관리자 사용자	ONTAP 도구를 설치하는 동안 생성되며 사용자가 ONTAP 도구를 배포하는 동안 자격 증명을 제공합니다. 사용자는 '이전' 콘솔에서 '암호'를 변경할 수 있습니다. 암호는 90일 후에 만료되며 사용자는 동일하게 변경해야 합니다.
유지보수 사용자	ONTAP 도구를 설치하는 동안 생성되며 사용자가 ONTAP 도구를 배포하는 동안 자격 증명을 제공합니다. 사용자는 '이전' 콘솔에서 '암호'를 변경할 수 있습니다. 이 사용자는 유지 관리 사용자이며 유지 관리 콘솔 작업을 실행하기 위해 생성됩니다.
데이터베이스 사용자	ONTAP 도구를 설치하는 동안 생성되며 사용자가 ONTAP 도구를 배포하는 동안 자격 증명을 제공합니다. 사용자는 '이전' 콘솔에서 '암호'를 변경할 수 있습니다. 암호는 90일 후에 만료되며 사용자는 동일하게 변경해야 합니다.

사용자 지원**(diag** 사용자**)**

ONTAP 도구를 설치하는 동안 지원 사용자가 생성됩니다. 이 사용자는 서버의 문제나 중단이 발생할 경우 ONTAP 도구에 액세스하고 로그를 수집하는 데 사용할 수 있습니다. 기본적으로 이 사용자는 비활성화되어 있지만 '이전' 콘솔을 통해 애드혹 방식으로 활성화할 수 있습니다. 이 사용자는 특정 시간이 지나면 자동으로 비활성화됩니다.

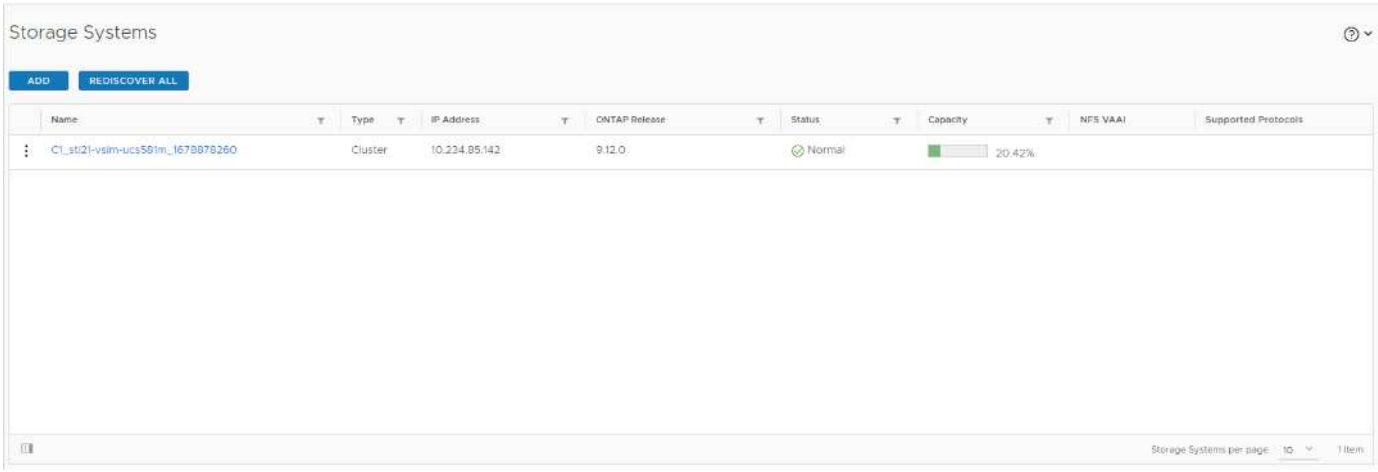
ONTAP 도구 **9.13** 상호 **TLS(**인증서 기반 인증**)**

ONTAP 버전 9.7 이상에서는 상호 TLS 통신을 지원합니다. VMware 및 vSphere 9.12용 ONTAP 툴부터 상호 TLS는 새로 추가된 클러스터와의 통신에 사용됩니다(ONTAP 버전에 따라 다름).

ONTAP

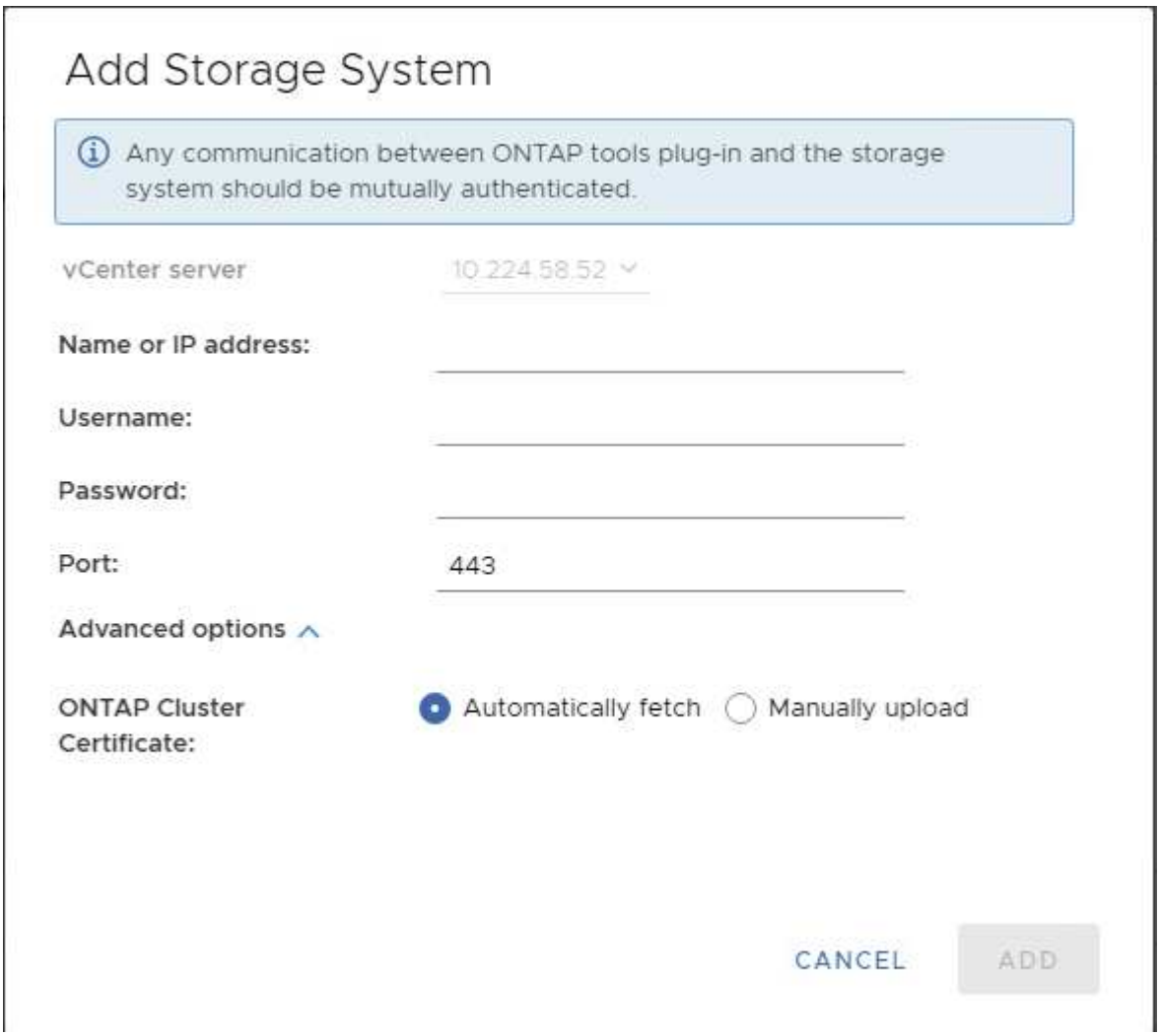
이전에 추가한 모든 스토리지 시스템에 대해 업그레이드 중에 추가된 모든 스토리지 시스템이 자동으로 신뢰되고 인증서 기반 인증 메커니즘이 구성됩니다.

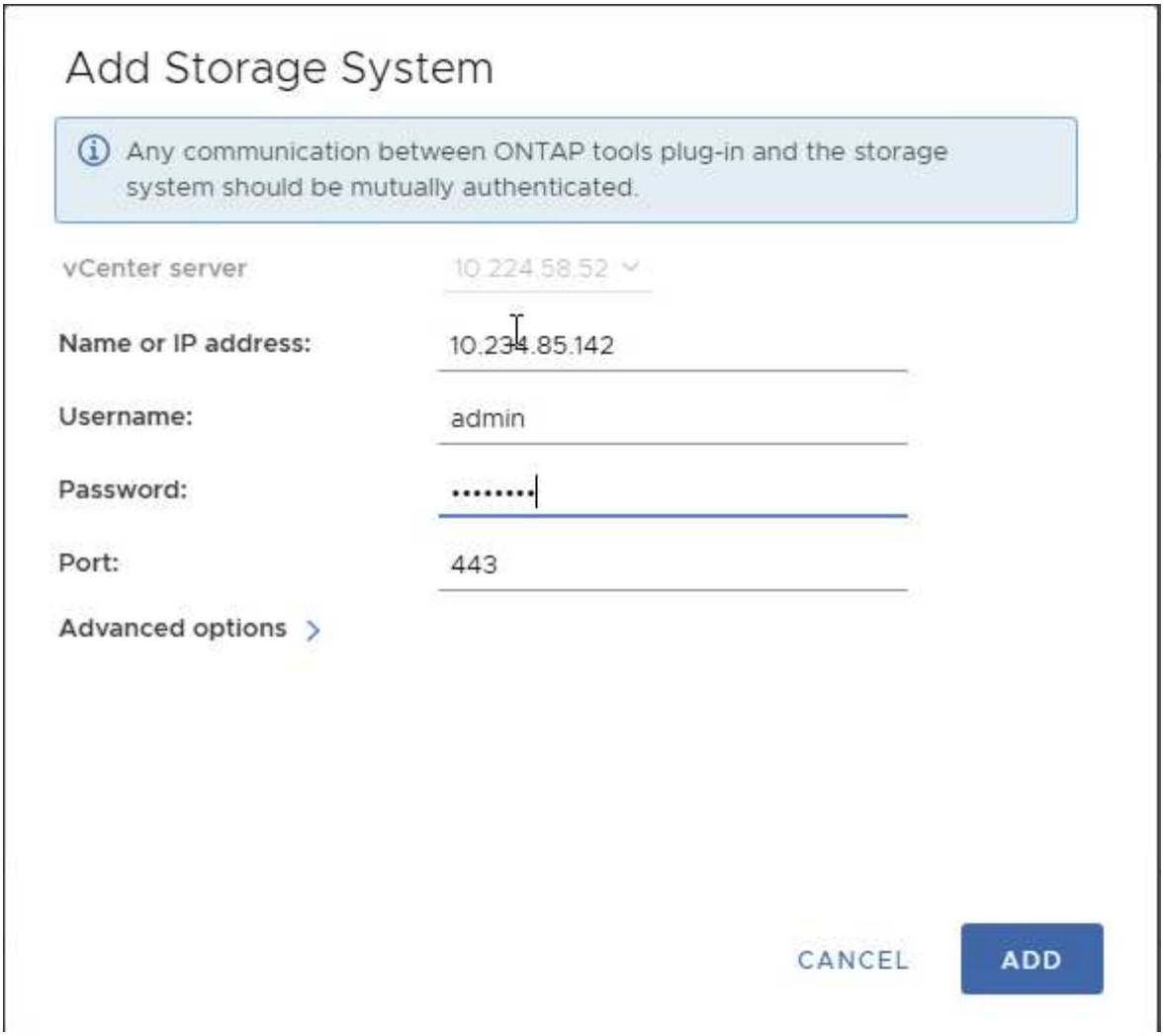
아래 스크린샷과 같이 클러스터 설정 페이지에는 각 클러스터에 대해 구성된 상호 TLS(인증서 기반 인증) 상태가 표시됩니다.

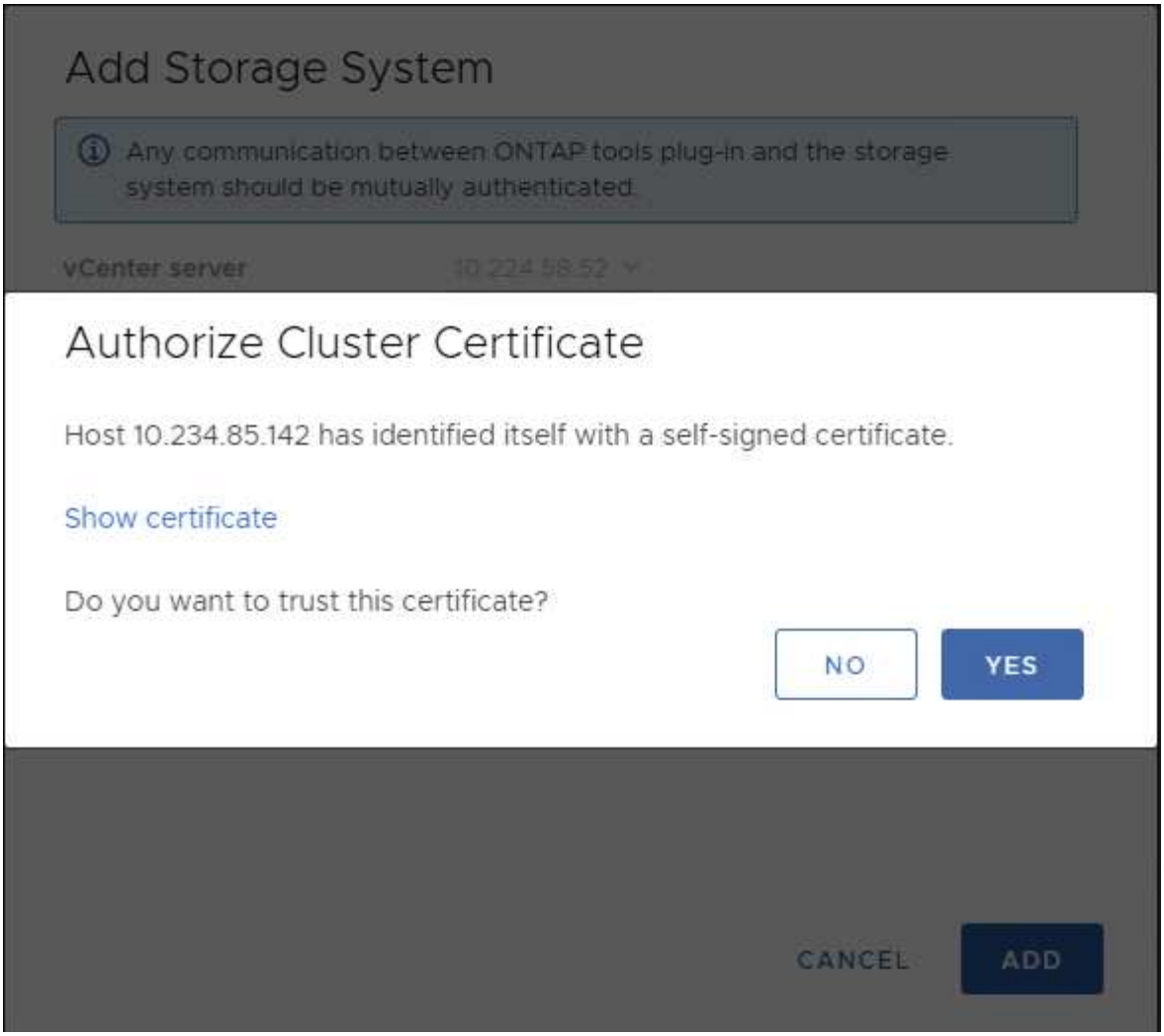


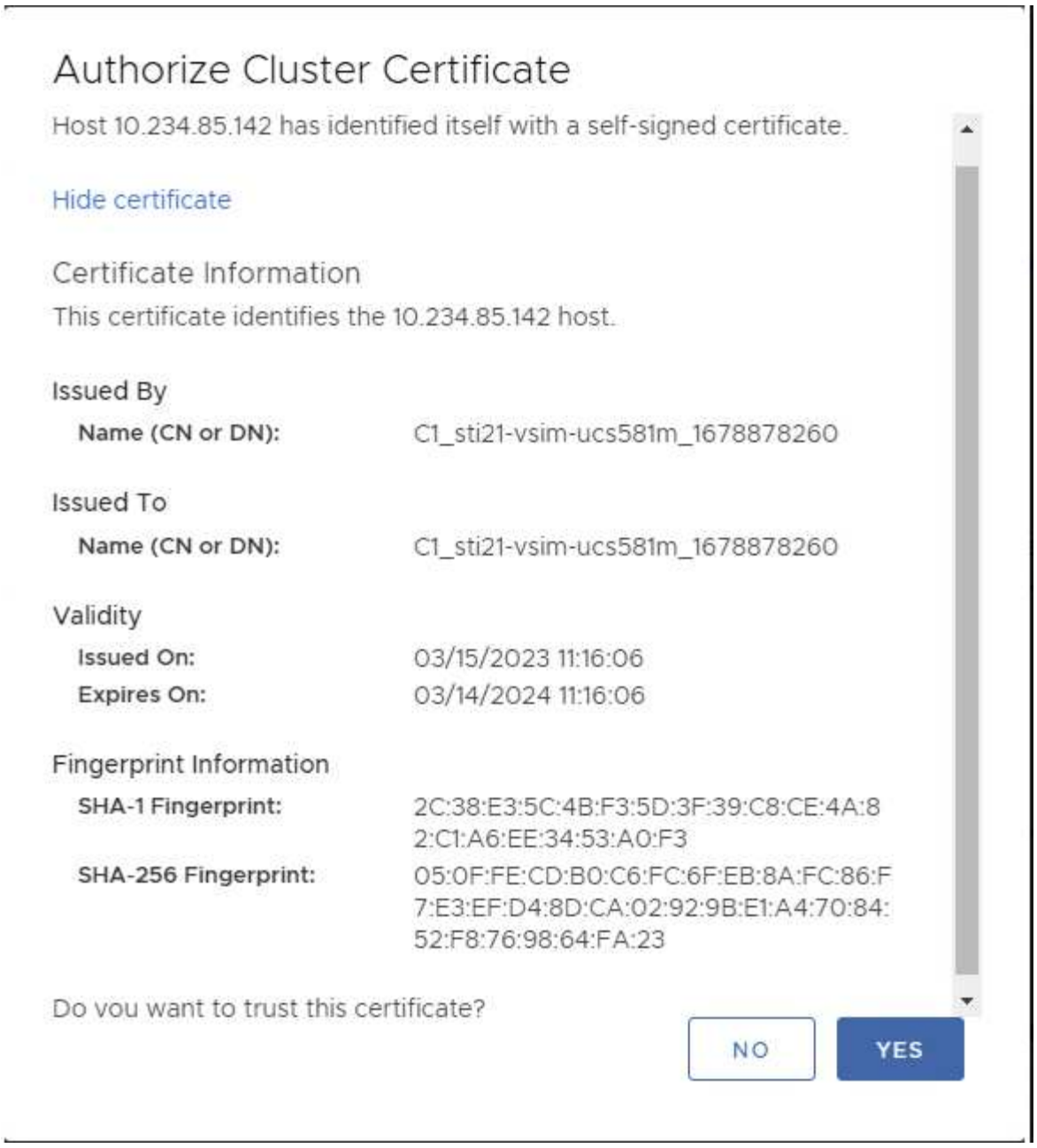
* 클러스터 추가 *

클러스터 추가 워크플로우 중에 추가되는 클러스터가 MTLS를 지원하는 경우 MTLS는 기본적으로 구성됩니다. 사용자는 이에 대해 구성을 수행할 필요가 없습니다. 아래 스크린샷은 클러스터 추가 중 사용자에게 표시되는 화면을 보여 줍니다.




Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

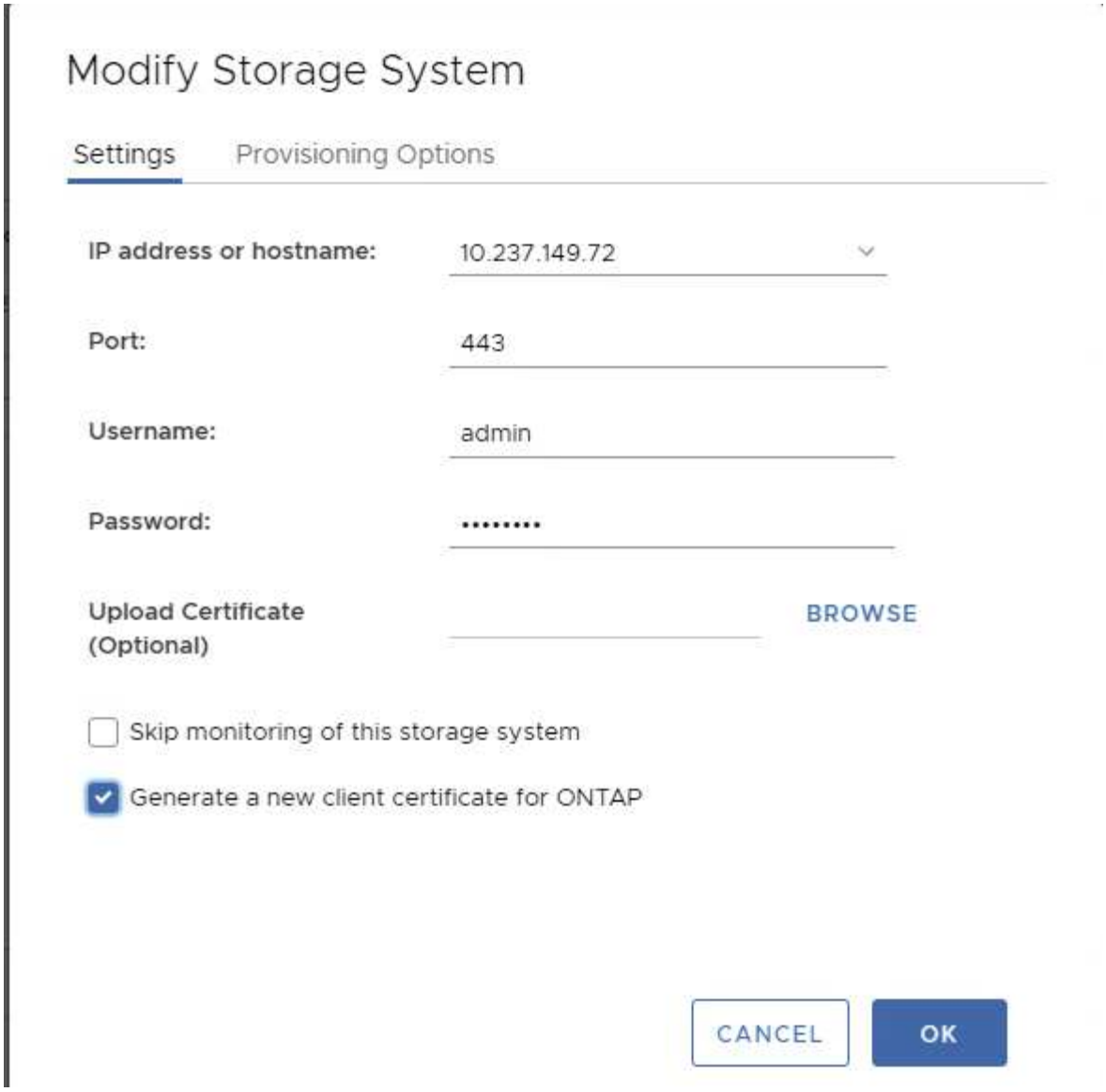

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

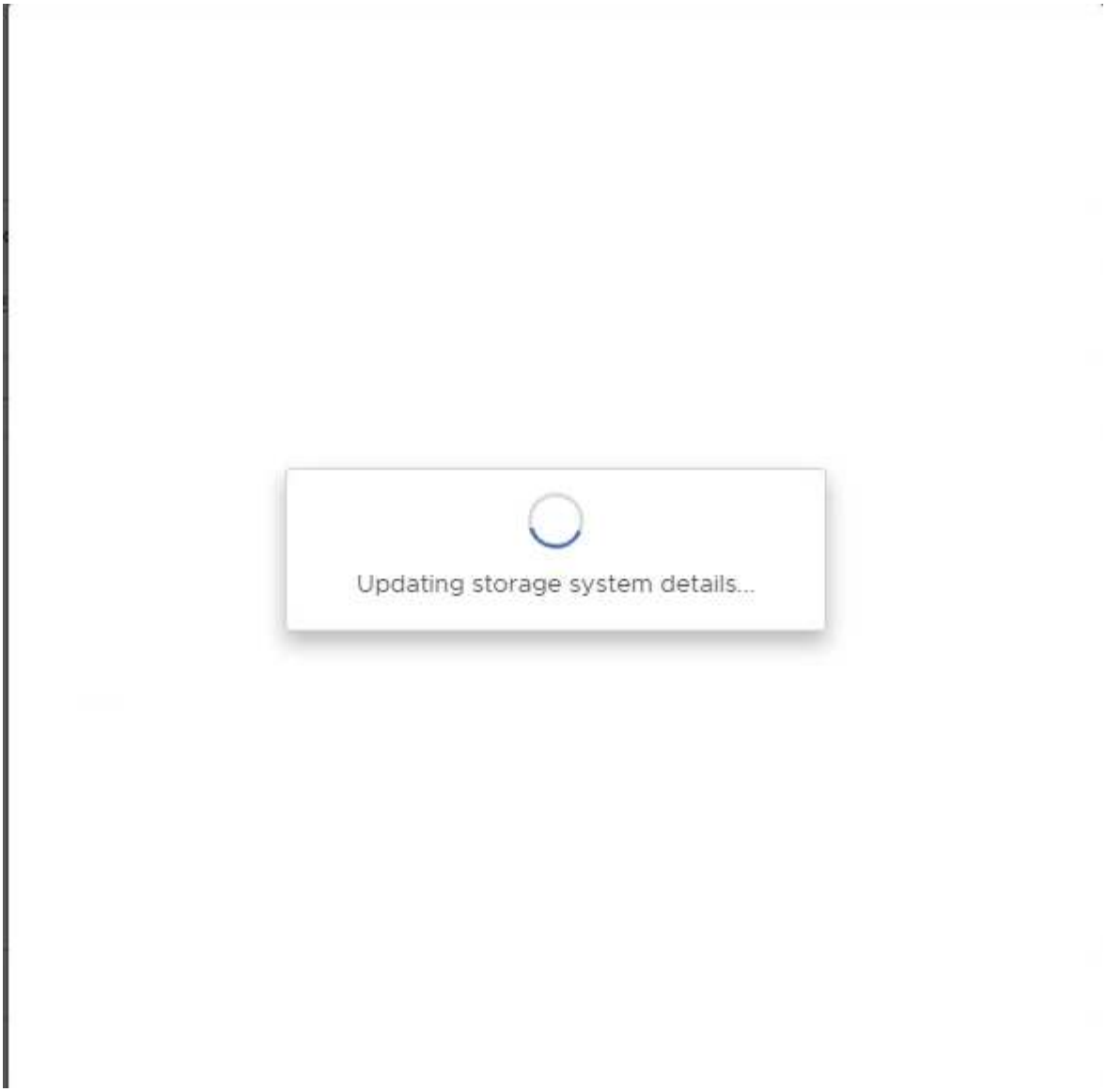


클러스터 편집

클러스터 편집 작업 중에 다음과 같은 두 가지 시나리오가 있습니다.

- ONTAP 인증서가 만료되면 사용자는 새 인증서를 얻고 업로드해야 합니다.
- OTV 인증서가 만료되면 사용자는 확인란을 선택하여 인증서를 다시 생성할 수 있습니다.
  - _ONTAP에 대한 새 클라이언트 인증서를 생성합니다


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK



ONTAP tools 9.13 HTTPS 인증서

기본적으로 ONTAP 도구는 웹 UI에 대한 HTTPS 액세스를 보호하기 위해 설치 중에 자동으로 만들어진 자체 서명 인증서를 사용합니다. ONTAP 도구는 다음과 같은 기능을 제공합니다.

1. HTTPS 인증서를 다시 생성합니다

ONTAP 도구를 설치하는 동안 HTTPS CA 인증서가 설치되고 인증서가 키 저장소에 저장됩니다. 사용자는 유지 관리 콘솔을 통해 HTTPS 인증서를 다시 생성할 수 있습니다.

위의 옵션은 _ '응용 프로그램 구성' → '인증서 다시 생성'._으로 이동하여 _maint_console에서 액세스할 수 있습니다

ONTAP TOOLS 9.13 로그인 배너

다음 로그인 배너는 사용자가 로그인 프롬프트에 사용자 이름을 입력하면 표시됩니다. SSH는 기본적으로 비활성화되어 있으며 VM 콘솔에서 설정한 경우에만 1회 로그인이 가능합니다.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

사용자가 SSH 채널을 통해 로그인을 완료하면 다음 텍스트가 표시됩니다.

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

ONTAP 도구 9.13에 대한 비활성 시간 초과

무단 액세스를 방지하기 위해 비활성 시간 제한이 설정되며, 이 시간 제한은 승인된 리소스를 사용하는 동안 특정 기간 동안 비활성 상태인 사용자를 자동으로 로그아웃시킵니다. 이렇게 하면 권한이 있는 사용자만 리소스에 액세스할 수 있으며 보안을 유지하는 데 도움이 됩니다.

- 기본적으로 vSphere Client 세션은 120분 동안 유휴 시간이 지나면 닫히므로 사용자가 다시 로그인하여 클라이언트 사용을 재개해야 합니다. webclient.properties 파일을 편집하여 시간 초과 값을 변경할 수 있습니다. vSphere Client의 시간 초과를 구성할 수 있습니다 "vSphere Client Timeout 값을 구성합니다"
- ONTAP 도구의 웹 CLI 세션 로그아웃 시간은 30분입니다.

사용자당 최대 동시 요청 수(네트워크 보안 보호/DOS 공격) VMware vSphere 9.13용 ONTAP 툴

기본적으로 사용자당 최대 동시 요청 수는 48개입니다. ONTAP 도구의 루트 사용자는 해당 환경의 요구 사항에 따라 이 값을 변경할 수 있습니다. 이 값은 서비스 거부(DOS) 공격에 대한 메커니즘을 제공하므로 매우 높은 값으로 설정하지 않아야 합니다.

사용자는 */opt/netapp/vscserver/etc/dosfilterParams.json* * 파일에서 최대 동시 세션 및 기타 지원되는 매개 변수의 수를 변경할 수 있습니다.

다음 매개 변수를 사용하여 필터를 구성할 수 있습니다.

- **delayms* * : 고려되기 전에 속도 제한을 초과하는 모든 요청에 주어진 지연 시간(밀리초)입니다. 요청을 거부하려면 -1을 지정합니다.
- **thromlems* * : 세마포에 대한 비동기 대기 시간.

- **maxRequests*: 이 요청을 실행할 수 있는 기간입니다.
- **ipWhitelist*: 속도 제한이 없는 쉼표로 구분된 IP 주소 목록입니다. (vCenter, ESXi 및 SRA IP일 수 있음)
- **maxRequestsPerSec*: 초당 연결의 최대 요청 수입니다.
- _dosfilterParams 파일의 기본값 _: *

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

ONTAP 도구 9.13에 대한 NTP(Network Time Protocol) 구성

경우에 따라 네트워크 시간 구성의 불일치로 인해 보안 문제가 발생할 수 있습니다. 이러한 문제를 방지하려면 네트워크 내의 모든 장치에 정확한 시간 설정이 있는지 확인하는 것이 중요합니다.

* 가상 어플라이언스 *

가상 어플라이언스의 유지 관리 콘솔에서 NTP 서버를 구성할 수 있습니다. 사용자는 시스템 구성⇒_새 NTP 서버 추가_옵션에서 NTP 서버 세부 정보를 추가할 수 있습니다

기본적으로 NTP에 대한 서비스는 ntpd입니다. 이 서비스는 레거시 서비스이며 일부 경우 가상 시스템에서 제대로 작동하지 않습니다.

* 데비안 *

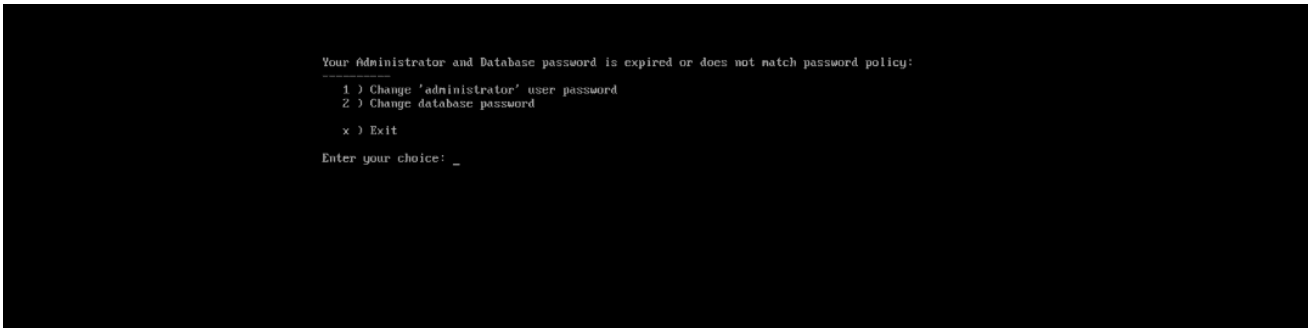
데비안에서 사용자는 /etc/ntp.conf 파일에 액세스하여 NTP 서버 세부 정보를 확인할 수 있습니다.

ONTAP 도구의 암호 정책 9.13

ONTAP 도구를 처음 배포하거나 버전 9.12 이상으로 업그레이드하는 사용자는 관리자와 데이터베이스 사용자 모두에 대해 강력한 암호 정책을 따라야 합니다. 배포 프로세스 중에 새 사용자에게 암호를 입력하라는 메시지가 표시됩니다. 버전 9.12 이상으로 업그레이드하는 Brownfield 사용자의 경우 유지 관리 콘솔에서 강력한 암호 정책을 따르는 옵션을 사용할 수 있습니다.

- 사용자가 유지 관리 콘솔에 로그인하면 복잡한 규칙 집합에 대해 암호가 확인되고, 따르지 않을 경우 사용자에게 동일한 암호를 재설정하라는 메시지가 표시됩니다.
- 암호 기본 유효 기간은 90일이며 75일 후에는 사용자가 암호 변경 알림을 받기 시작합니다.
- 모든 사이클에서 새 암호를 설정해야 합니다. 시스템에서는 마지막 암호를 새 암호로 사용하지 않습니다.
- 사용자가 유지 관리 콘솔에 로그인할 때마다 기본 메뉴를 로드하기 전에 아래 스크린샷과 같은 암호 정책을 확인합니다.

- 암호 정책 또는 ONTAP tools 9.11 또는 이전 버전에서 업그레이드 설정을 따르지 않는 경우. 그런 다음 사용자가 암호를 재설정하는 다음 화면을 볼 수 있습니다.



- 사용자가 약한 암호를 설정하려고 하거나 마지막 암호를 다시 입력하면 다음 오류가 표시됩니다.