



ONTAP이 포함된 vSphere Metro 스토리지 클러스터 Enterprise applications

NetApp
May 09, 2024

목차

ONTAP이 포함된 vSphere Metro 스토리지 클러스터	1
ONTAP이 포함된 vSphere Metro 스토리지 클러스터	1
VMware vSphere 솔루션 개요	3
vMSC 설계 및 구현 지침	8
계획되거나 계획되지 않은 이벤트에 대한 복원력	18
MCC가 있는 vMSC에 대한 실패 시나리오	18

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.

vSphere 환경을 위한 무중단 가용성 솔루션

ONTAP 아키텍처는 데이터 저장소에 SAN(FCP, iSCSI 및 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(주문형 컨트롤러 페일오버 또는 CFOD), 하드웨어 이중화 및 지리적 분리를 통해 높은 수준의 가용성을 달성합니다. SyncMirror는 데이터를 두 플렉스에 기록하여 MetroCluster 구성의 두 부분에 걸쳐 동기식으로 데이터를 미러링합니다. 로컬 플렉스(로컬 셸프에 있음)가 데이터를 능동적으로 제공하고 원격 플렉스(원격 셸프에 있음)는 일반적으로 데이터를 제공하지 않음. 컨트롤러, 스토리지, 케이블, 스위치(패브릭 MetroCluster와 함께 사용), 어댑터와 같은 모든 MetroCluster 구성요소에 대해 하드웨어 이중화가 적용됩니다.

NetApp SnapMirror 액티브 동기화는 FCP 및 iSCSI SAN 프로토콜을 통해 데이터 저장소의 세부적 보호 기능을 제공하므로 우선순위가 높은 워크로드만 선택적으로 보호할 수 있습니다. Active-Standby 솔루션인 NetApp MetroCluster과 달리 로컬 및 원격 사이트에 대한 액티브-액티브 액세스를 제공합니다. 현재 활성 동기화는 한 쪽이 다른 쪽보다 선호되는 비대칭 솔루션으로, 더 나은 성능을 제공합니다. 이 기능은 ESXi 호스트에 선호하는 컨트롤러를 자동으로 알려주는 ALUA(Asymmetric Logical Unit Access) 기능을 사용하여 달성할 수 있습니다. 하지만 NetApp는 액티브 동기화가 곧 완벽한 대칭 액세스를 활성화할 것이라고 발표했습니다.

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 참조하십시오 ["VMware vSphere Metro Storage Cluster 권장 사례"](#).

vSphere Metro Storage Cluster란 무엇입니까?

vMSC(vSphere Metro Storage Cluster)는 VM(가상 머신) 및 컨테이너를 장애로부터 보호하는 인증 구성입니다. 이는 확장 스토리지 개념을 랙, 건물, 캠퍼스 또는 도시와 같은 여러 장애 도메인에 분산되는 ESXi 호스트 클러스터와 함께 사용하여 달성할 수 있습니다. NetApp MetroCluster 및 SnapMirror Active sync 스토리지 기술은 호스트 클러스터에 각각 RPO=0 또는 RPO=0 정도의 보호를 제공하는 데 사용됩니다. vMSC 구성은 완전한 물리적 또는 논리적 "사이트"에 장애가 발생하더라도 데이터를 항상 사용할 수 있도록 설계되었습니다. vMSC 구성에 포함된 스토리지 디바이스는 vMSC 인증 프로세스를 성공적으로 완료한 후 인증을 받아야 합니다. 지원되는 모든 저장 장치는 에서 찾을 수 있습니다 ["VMware 스토리지 호환성 가이드 를 참조하십시오"](#).

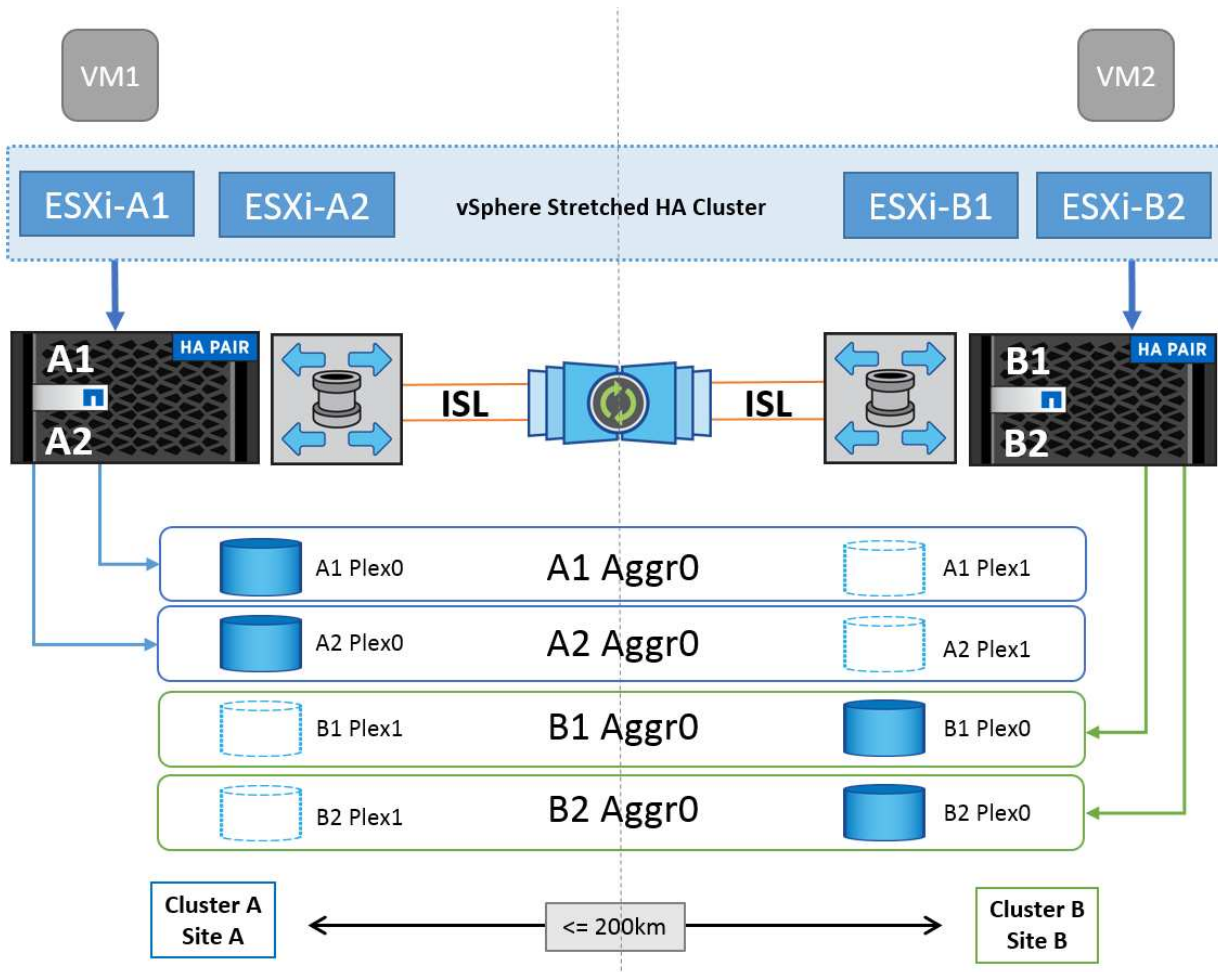
vSphere Metro Storage Cluster의 설계 지침에 대한 자세한 내용은 다음 설명서를 참조하십시오.

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

자연 시간 고려 사항에 따라 NetApp MetroCluster는 vSphere와 함께 사용할 수 있도록 두 가지 구성으로 구축할 수 있습니다.

- MetroCluster를 확장합니다
- Fabric MetroCluster의 약어입니다

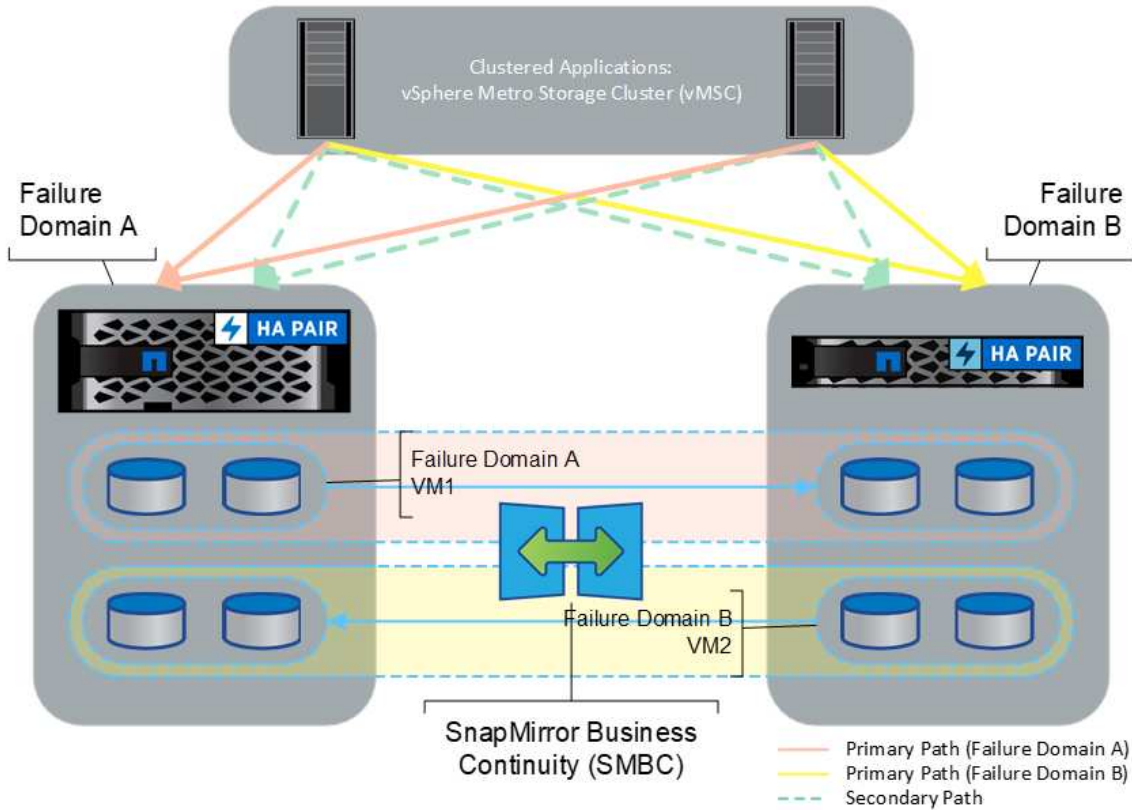
다음은 확장 MetroCluster의 상위 수준 토폴로지 다이어그램을 보여 줍니다.



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

SnapMirror Active Sync는 두 가지 방법으로 배포할 수도 있습니다.

- 비대칭
- 대칭(ONTAP 9.14.1의 비공개 미리보기)



을 참조하십시오 ["NetApp 문서"](#) SnapMirror 액티브 동기화에 대한 특정 설계 및 구축 정보를 제공합니다.

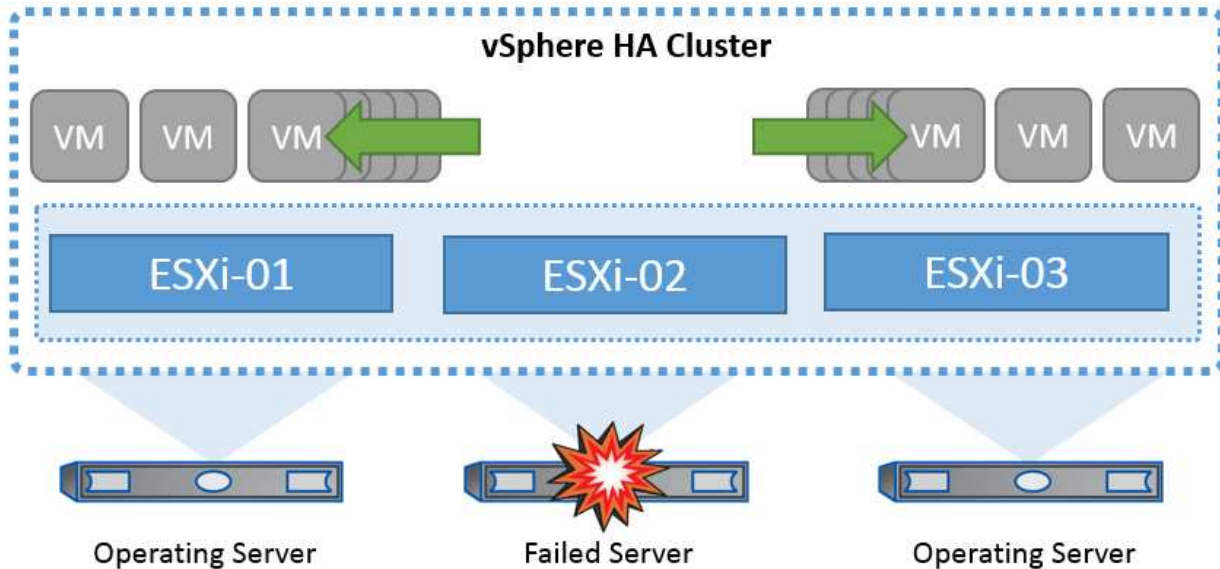
VMware vSphere 솔루션 개요

VCSA(vCenter Server Appliance)는 관리자가 ESXi 클러스터를 효과적으로 운영할 수 있도록 지원하는 강력한 중앙 집중식 관리 시스템이자 vSphere용 단일 창입니다. VM 프로비저닝, vMotion 작업, HA(고가용성), DRS(Distributed Resource Scheduler), Tanzu Kubernetes Grid 등의 주요 기능을 지원합니다. VMware 클라우드 환경에서 필수적인 구성 요소이며 서비스 가용성을 고려하여 설계해야 합니다.

vSphere 고가용성

VMware의 클러스터 기술은 ESXi 서버를 가상 시스템용 공유 리소스 풀로 그룹화하고 vSphere HA(High Availability)를 제공합니다. vSphere HA는 가상 머신에서 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 시작합니다. vSphere HA를 사용하면 계획된 다운타임을 줄이고, 예기치 않은 다운타임을 방지하며, 운영 중단으로부터 신속하게 복구할 수 있습니다.

vSphere HA 클러스터 장애가 발생한 서버에서 VM을 복구합니다.



VMware vSphere는 NetApp MetroCluster 또는 SnapMirror 활성화 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 생성되면 클러스터의 모든 호스트가 선택에 참여하며 호스트 중 하나가 마스터가 됩니다. 각 슬레이브는 네트워크 하트비트를 마스터로 수행하고, 마스터는 모든 슬레이브 호스트에서 네트워크 하트비트를 수행합니다. vSphere HA 클러스터의 마스터 호스트는 슬레이브 호스트의 장애를 감지합니다.

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 검사 안정성을 향상시킬 수 있습니다.

모범 사례

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 HA의 설정으로, vSphere HA 클러스터의 호스트에서 관리 네트워크 연결이 끊어지지만 계속 실행되는 경우 가상 시스템에서 트리거되는 작업을 결정합니다. 이 설정에는 "사용 안 함", "VM 종료 및 다시 시작", "VM 전원 끄기 및 다시 시작"이라는 세 가지 옵션이 있습니다.

"시스템 종료"는 "전원 끄기"보다 낮습니다. 이는 디스크에 대한 가장 최근의 변경 사항을 플러시하거나 트랜잭션을 커밋하지 않습니다. 가상 시스템이 300초 내에 종료되지 않으면 전원이 꺼집니다. 대기 시간을 변경하려면 고급 옵션인 DAS.isolationshutdowntimeout을 사용합니다.

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.

모범 사례

NetApp에서는 "호스트 격리 응답"을 사용 안 함으로 설정하는 것이 좋습니다.

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 저장소 장치가 영구적으로 실패하거나 관리자가 제거되어 반환되지 않을 때 발생하는 상태입니다. NetApp 스토리지 배열은 ESXi에 SCSI 감지 코드를 발행하여 디바이스가 영구적으로 손실되었음을 알립니다. vSphere HA의 Failure Conditions and VM Response 섹션에서 PDL 조건이 감지된 후 응답을 구성할 수 있습니다.

모범 사례

NetApp은 "PDL을 사용한 데이터 저장소 응답"을 " * VM 전원을 끄고 다시 시작 * "으로 설정할 것을 권장합니다. 이 상태가 감지되면 vSphere HA 클러스터 내의 정상 호스트에서 VM이 즉시 재시작됩니다.

모든 경로 다운(APD)

APD는 스토리지 디바이스가 호스트에 액세스할 수 없고 스토리지에 대한 경로를 사용할 수 없는 경우에 발생하는 상태입니다. ESXi는 이 문제가 디바이스의 일시적인 문제로 간주하여 다시 사용할 수 있게 될 것으로 예상하고 있습니다.

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).

모범 사례

NetApp은 “APD를 사용한 데이터 저장소에 대한 응답”을 “* VM 전원을 끄고 다시 시작(보수적)*”으로 구성할 것을 권장합니다.

보존적 은 HA가 VM을 다시 시작할 수 있는 가능성을 나타냅니다. 보존으로 설정하면 다른 호스트가 다시 시작할 수 있다는 것을 알고 있는 경우에만 HA가 APD의 영향을 받는 VM을 다시 시작합니다. 공격적인 경우 HA는 다른 호스트의 상태를 모르는 경우에도 VM을 다시 시작합니다. 따라서 해당 데이터 저장소에 액세스할 수 있는 호스트가 없는 경우 VM이 다시 시작되지 않을 수 있습니다.

APD 상태가 해결되고 제한 시간이 경과하기 전에 스토리지에 대한 액세스가 복구되는 경우, 사용자가 명시적으로 가상 머신을 구성하지 않으면 HA가 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.

모범 사례

NetApp에서는 APD 시간 초과 후 APD 복구에 대한 응답을 사용 안 함으로 구성하는 것이 좋습니다.

NetApp MetroCluster용 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. 사이트 간 트래픽을 방지하기 위해 NetApp에서는 VM의 논리적 분리를 관리하기 위해 DRS 선호도 규칙을 구성하는 것이 좋습니다. 따라서 전체 사이트 장애가 발생하지 않는 한 HA 및 DRS는 로컬 호스트만 사용합니다.

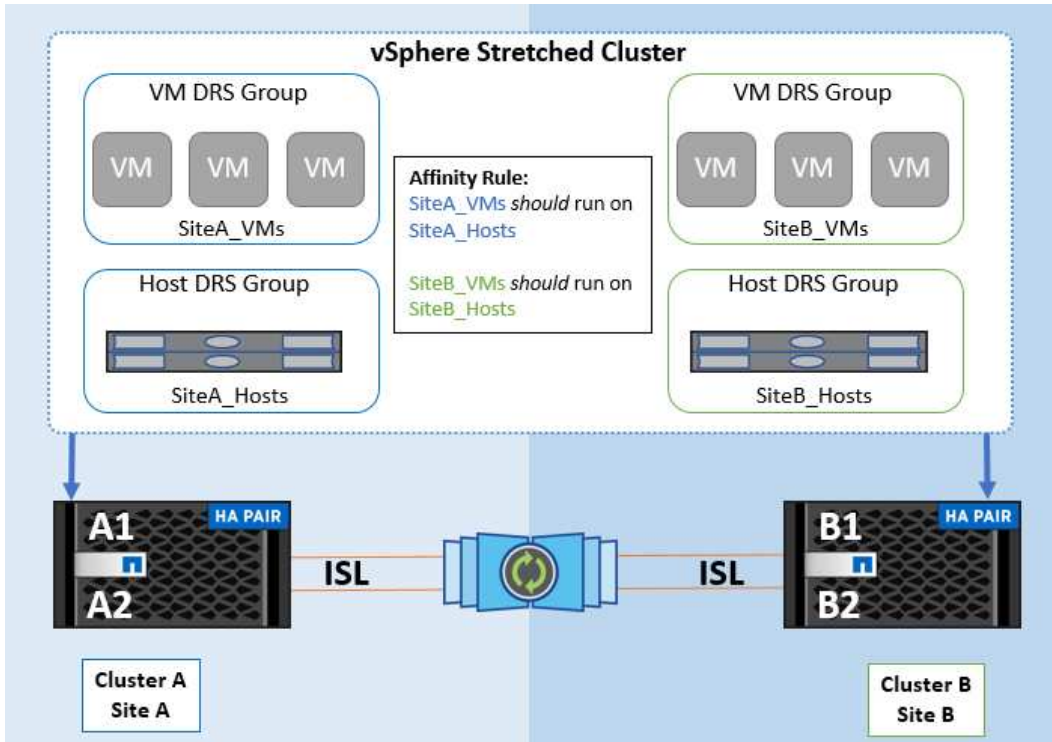
클러스터에 대한 DRS 선호도 규칙을 생성하는 경우 vSphere가 가상 머신 페일오버 중에 해당 규칙을 적용하는 방법을 지정할 수 있습니다.

vSphere HA 페일오버 동작을 지정할 수 있는 두 가지 규칙 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 장애 발생 시 vSphere HA로 인해 위반되므로 "Must" 규칙 대신 "Must" 규칙을 적용하는 것이 좋습니다. "필수" 규칙을 사용하면 서비스가 중단될 수 있습니다.

서비스의 가용성은 항상 성과보다 우선해야 합니다. 전체 데이터 센터에 장애가 발생할 경우 "필수" 규칙은 VM 호스트 선호도 그룹에서 호스트를 선택해야 하며, 데이터 센터를 사용할 수 없으면 가상 시스템이 다시 시작되지 않습니다.

NetApp MetroCluster를 사용한 VMware Storage DRS 구축

VMware Storage DRS 기능을 사용하면 데이터 저장소를 단일 유닛으로 통합할 수 있으며 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.

모범 사례

NetApp은 스토리지 사이트 선호도와 관련하여 데이터 저장소 클러스터를 생성하는 것이 좋습니다. 즉, 사이트 A에 대한 사이트 선호도를 갖는 데이터 저장소와 사이트 B에 대한 사이트 선호도를 갖는 데이터 저장소를 함께 사용하면 안 됩니다.

Storage vMotion을 사용하여 가상 머신을 새로 프로비저닝하거나 마이그레이션할 때마다 NetApp은 해당 가상 머신과 관련된 모든 VMware DRS 규칙을 수동으로 업데이트하는 것이 좋습니다. 그러면 호스트와 데이터 저장소에 대한

사이트 레벨에서 가상 머신 선호도가 확인되므로 네트워크 및 스토리지 오버헤드가 줄어듭니다.

vMSC 설계 및 구현 지침

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

NetApp 스토리지 구성

NetApp MetroCluster에 대한 설정 지침(MCC 구성이라고 함)은 에서 확인할 수 있습니다 "[MetroCluster 문서](#)". SnapMirror 활성 동기화에 대한 지침은 에서도 확인할 수 있습니다 "[SnapMirror 비즈니스 연속성 개요](#)".

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 않는 경우 SnapMirror 액티브 동기화를 사용하여 서로 다른 장애 도메인에 있는 여러 ONTAP 클러스터에서 데이터 저장소에 대한 세분화된 보호와 액티브-액티브 액세스를 제공할 수 있습니다. SnapMirror 액티브 동기화에서는 정합성 보장 그룹을 사용하여 하나 이상의 데이터 저장소 간에 쓰기 순서 일관성을 보장하고 애플리케이션 및 데이터 저장소 요구 사항에 따라 여러 정합성 보장 그룹을 생성할 수 있습니다. 일관성 그룹은 여러 데이터 저장소 간에 데이터를 동기화해야 하는 애플리케이션에 특히 유용합니다. 또한 SnapMirror 활성 동기화는 RDM(Raw Device Mappings) 및 게스트 내 iSCSI 초기자가 있는 게스트 연결 스토리지를 지원합니다. 일관성 그룹에 대한 자세한 내용은 에서 확인할 수 있습니다 "[일관성 그룹 개요](#)".

SnapMirror 액티브 동기화를 사용하여 vMSC 구성을 관리하는 것은 MetroCluster와 비교하여 몇 가지 차이가 있습니다. 첫째, SAN 전용 구성이며 SnapMirror 활성 동기화로 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.

VMware vSphere HA

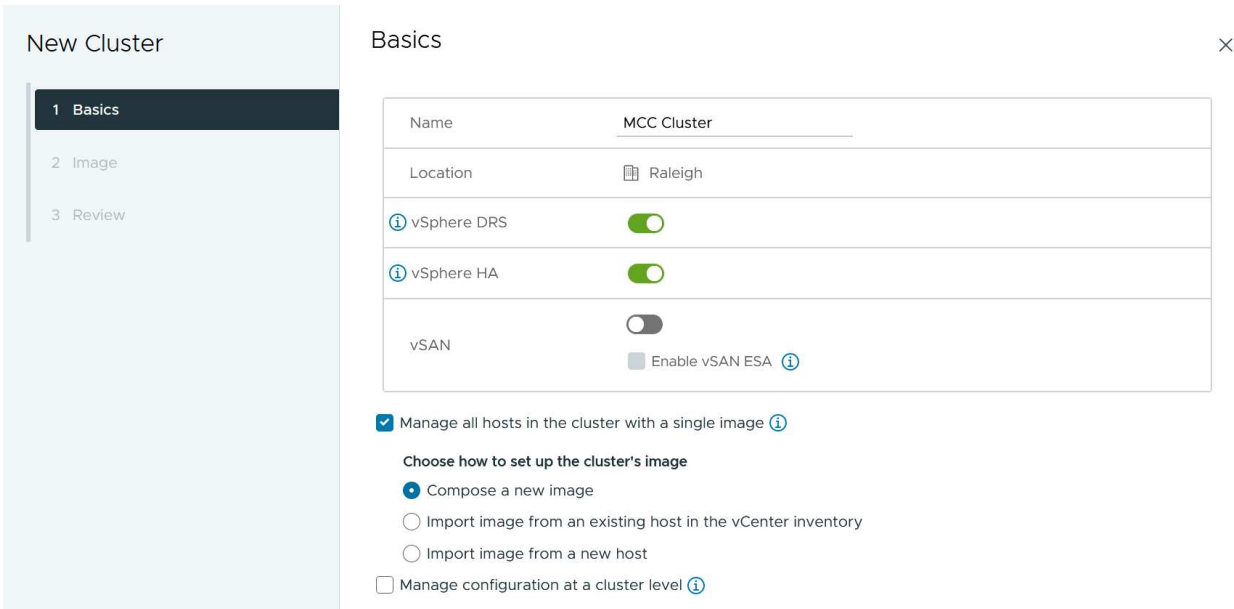
vSphere HA 클러스터를 생성합니다

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.

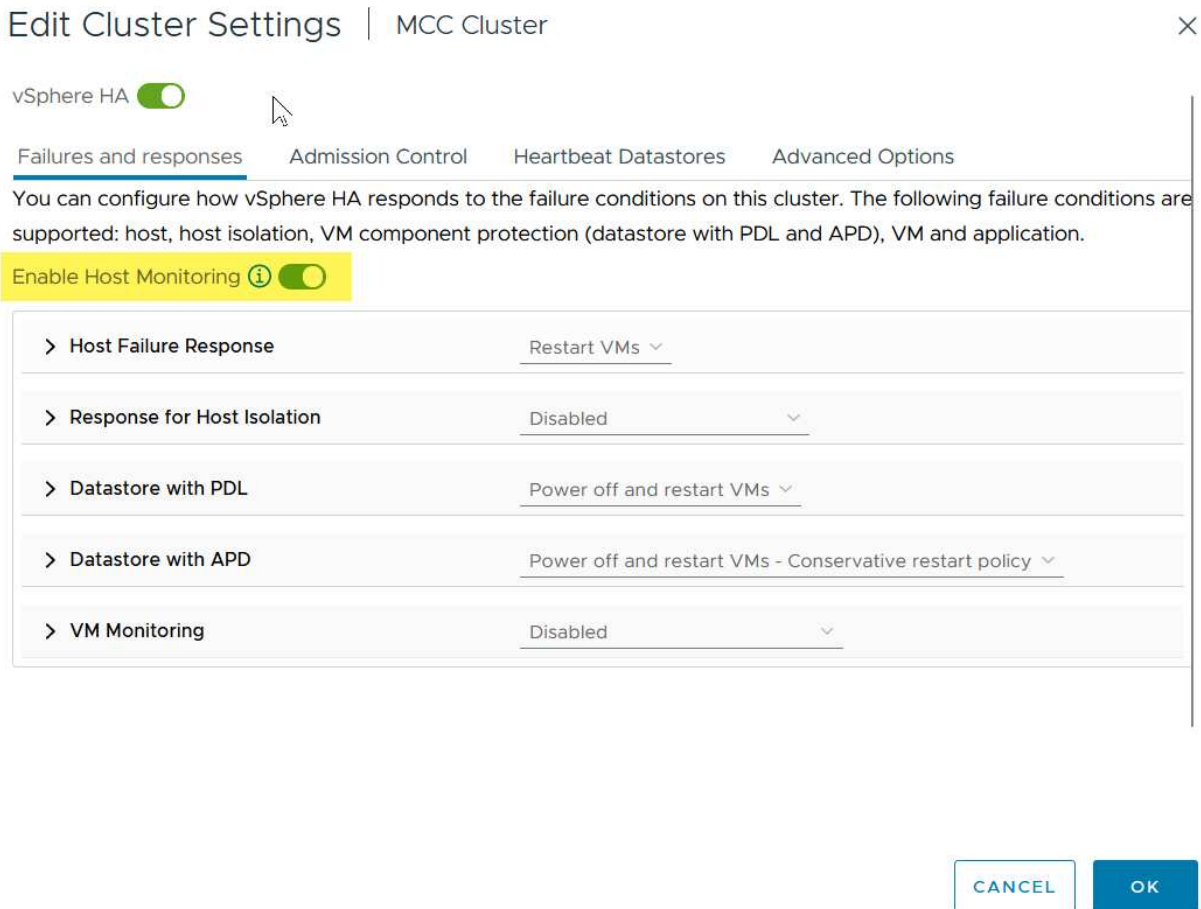
- 참고: * 이 문서의 어떤 내용도 대체되지 않습니다 "[VMware vSphere Metro Storage Cluster 권장 사례](#)"

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.

> Response for Host Isolation Disabled ▼

> Datastore with PDL Power off and restart VMs ▼

> Datastore with APD Power off and restart VMs - Conservative restart policy ▼

▼ VM Monitoring

Enable heartbeat monitoring

VM monitoring resets individual VMs if their VMware tools heartbeats are not received within a set time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.

Disabled

VM Monitoring Only

VM and Application Monitoring

Turns on application heartbeats. When heartbeats are not received within a set time, the VM is reset.

CANCEL
OK

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

vSphere HA

Failures and responses | **Admission Control** | Heartbeat Datastores | Advanced Options

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

Host failures cluster tolerates:
 Maximum is one less than number of hosts in cluster.

Define host failover capacity by: **Cluster resource Percentage**

Override calculated failover capacity.

Reserved failover CPU capacity: % CPU

Reserved failover Memory capacity: % Memory

Reserve Persistent Memory failover capacity ⓘ

Override calculated Persistent Memory failover capacity ⓘ

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

vSphere DRS

Automation | Additional Options | Power Management | Advanced Options

Automation Level: **Manual**

DRS generates both power-on placement recommendations, and migration recommendations for virtual machines. Recommendations need to be manually applied or ignored.

Migration Threshold ⓘ

Conservative (Less Frequent vMotions) **Aggressive (More Frequent vMotions)**

(3) DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads. (Default)

Predictive DRS ⓘ Enable

Virtual Machine Automation ⓘ Enable

1. VM 구성 요소 보호를 활성화합니다. 을 참조하십시오 "docs.vmware.com".
2. MCC가 있는 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.

vSphere HA









Failures and responses Admission Control **Heartbeat Datastores** Advanced Options

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 4 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

- Automatically select datastores accessible from the hosts
- Use datastores only from the specified list
- Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

	Name ↑	Datastore Cluster	Hosts Mounting Datastore
<input checked="" type="checkbox"/>	 d11	N/A	2
<input checked="" type="checkbox"/>	 d12	N/A	2
<input checked="" type="checkbox"/>	 d21	N/A	2
<input checked="" type="checkbox"/>	 d22	N/A	2
<input type="checkbox"/>	 d31	N/A	2
<input type="checkbox"/>	 d32	N/A	2
<input type="checkbox"/>	 d41	N/A	2
<input type="checkbox"/>	 d42	N/A	2

11 items

CANCEL OK

고급 옵션 구성

- 호스트 장애 감지 *

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.

을 참조하십시오 ["core.vmware.com"](https://core.vmware.com) 자세한 내용은 .

vSphere HA

Failures and responses Admission Control Heartbeat Datastores **Advanced Options**

You can set advanced options that affect the behavior of your vSphere HA cluster.

+ Add ✕ Delete

Option	Value
das.IgnoreRedundantNetWarning	true
das.Isolationaddress0	10.61.99.100
das.Isolationaddress1	10.61.99.110
das.heartbeatDsPerHost	4

4 items

CANCEL OK

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. 하지만 MCC 또는 SnapMirror 액티브 동기화로 해당 데이터를 보호할 필요는 없습니다.

을 참조하십시오 "core.vmware.com" 자세한 내용은 .

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 VMHost Rules에서는 SiteA_VMs가 SiteA_hosts의 호스트에서 실행되어야 한다고 설명합니다.

모범 사례

- 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.

- 참고: * 가상 머신이 VM-호스트 선호도 규칙을 위반할 때 트리거되는 이벤트 기반 알람을 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"](#) 문서화:

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.

Create VM/Host Rule | Cluster-01 ×

Name	sitea_affinity	<input checked="" type="checkbox"/> Enable rule.
Type	Virtual Machines to Hosts ▼	

Virtual machines that are members of the Cluster VM Group sitea_vms should run on host group sitea_hosts.

VM Group:

sitea_vms	▼
Should run on hosts in group	▼

Host Group:

sitea_hosts	▼
-------------	---

CANCEL
OK

NetApp MetroCluster용 VMware vSphere Storage DRS

데이터 저장소 클러스터를 생성합니다

각 사이트에 대해 데이터 저장소 클러스터를 구성하려면 다음 단계를 완료합니다.

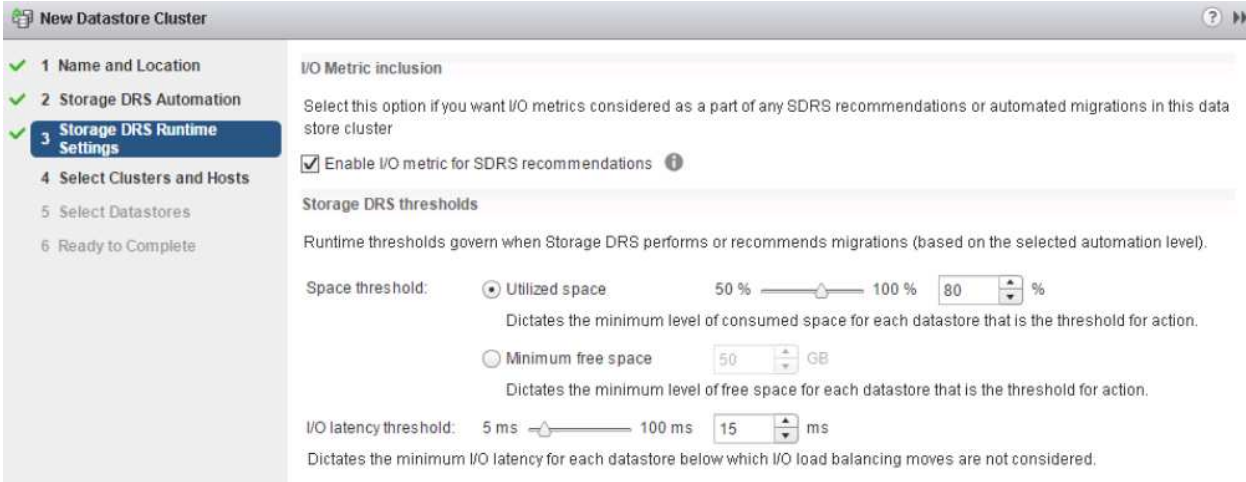
1. vSphere Web Client를 사용하여 Storage 아래에 HA 클러스터가 있는 데이터 센터로 이동합니다.
2. 데이터 센터 개체를 마우스 오른쪽 버튼으로 클릭하고 스토리지 > 새 데이터 저장소 클러스터 를 선택합니다.
3. Turn on Storage DRS 옵션을 선택하고 Next를 클릭합니다.
4. 모든 옵션을 자동화 안 함(수동 모드)으로 설정하고 다음을 클릭합니다.

모범 사례

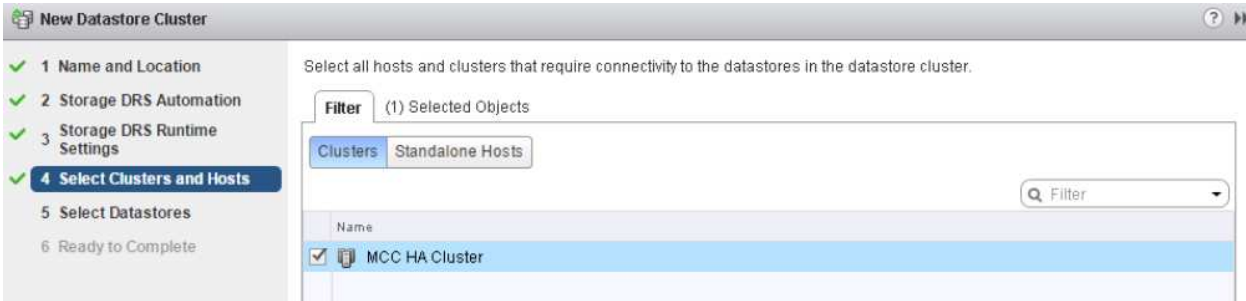
- NetApp는 관리자가 마이그레이션이 필요한 시기를 결정하고 제어할 수 있도록 Storage DRS를 수동 모드로 구성하는 것이 좋습니다.

▼ Storage DRS automation	
Cluster automation level	<input checked="" type="radio"/> No Automation (Manual Mode) vCenter Server will make migration recommendations for virtual machine storage, but will not perform automatic migrations.
	<input type="radio"/> Fully Automated Files will be migrated automatically to optimize resource usage.

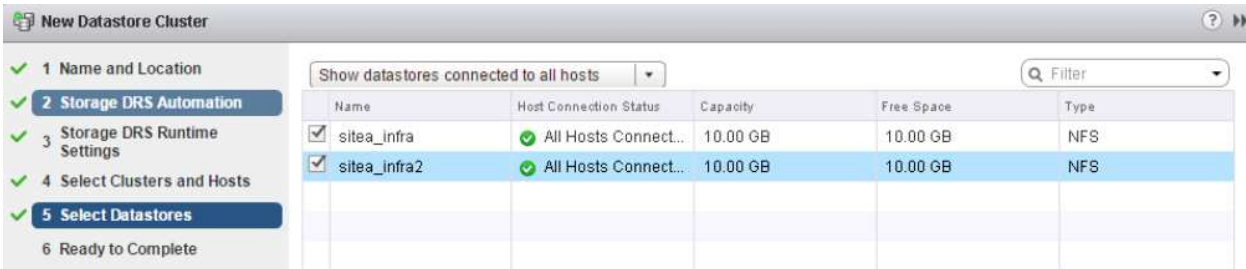
1. Enable I/O Metric for SDRS Recommendations 확인란이 선택되어 있는지 확인합니다. 메트릭 설정을 기본값으로 유지할 수 있습니다.



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, Docker 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. 반환은 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 중 MetroCluster 구성의 NAS(Network Attached Storage 논리 인터페이스)는 자동으로 페일오버됩니다. 그러나 SAN LIF(Storage Area Network LIF)는 페일오버되지 않으며 LUN(논리 유닛 번호)에 대한 직접 경로를 계속 사용합니다.

HA 테이크오버 및 반환에 대한 자세한 내용은 ["HA 쌍 관리 개요"](#)를 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 NetApp 중재자가 필요합니다.

MCC가 있는 vMSC에 대한 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, 프론트엔드 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.

- 참고: * 이 시나리오에서는 MetroCluster 동작에 변화가 없으며 모든 데이터 저장소는 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 타이밍은 Active-Active 또는 Active-Standby 중 하나로 구성할 수 있습니다.

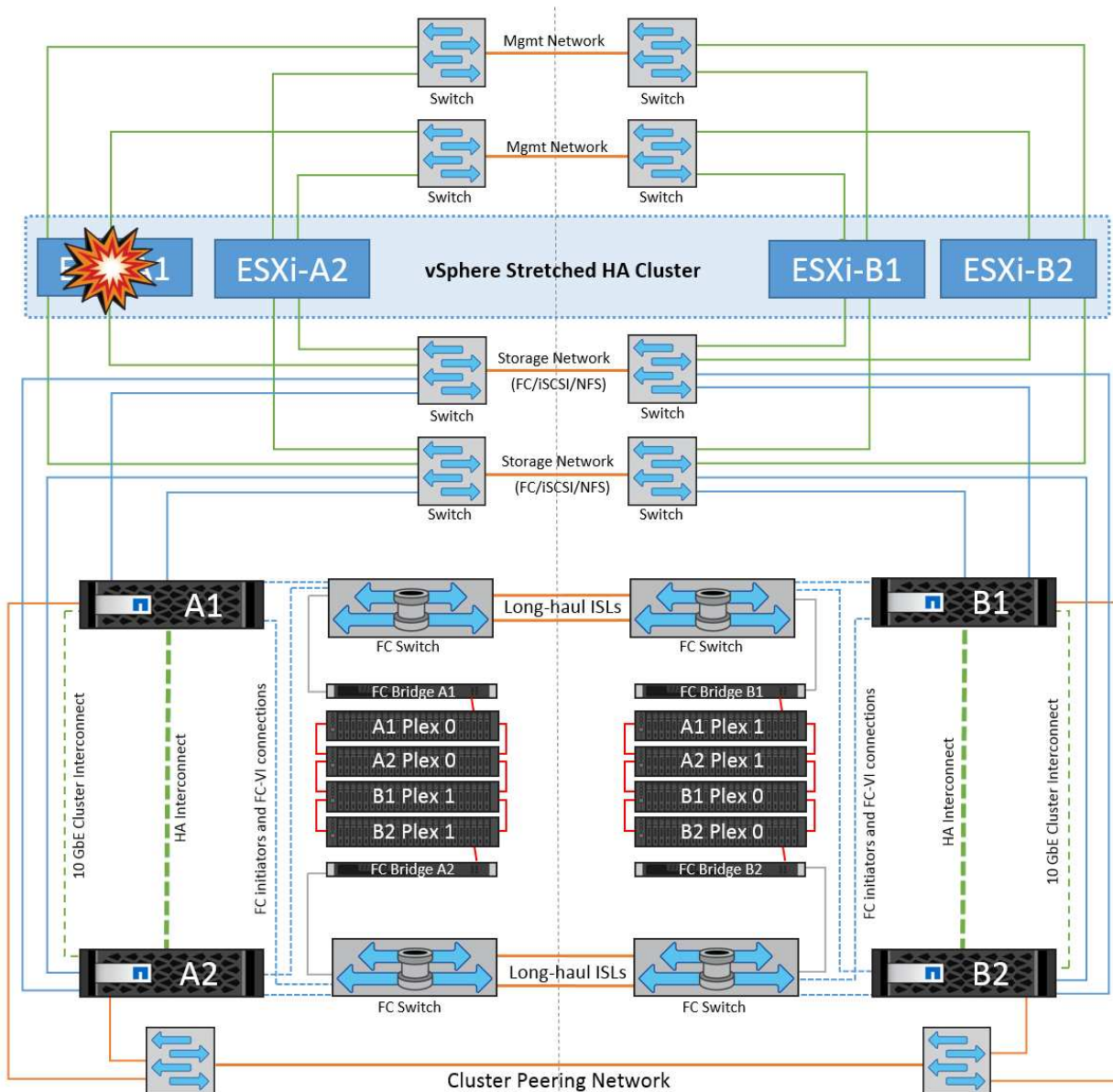
또한 iSCSI LUN의 경우 vmkernel 인터페이스를 iSCSI 네트워크 어댑터에 바인딩하여 다중 경로를 구성해야 합니다. 자세한 내용은 vSphere 스토리지 설명서를 참조하십시오.

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



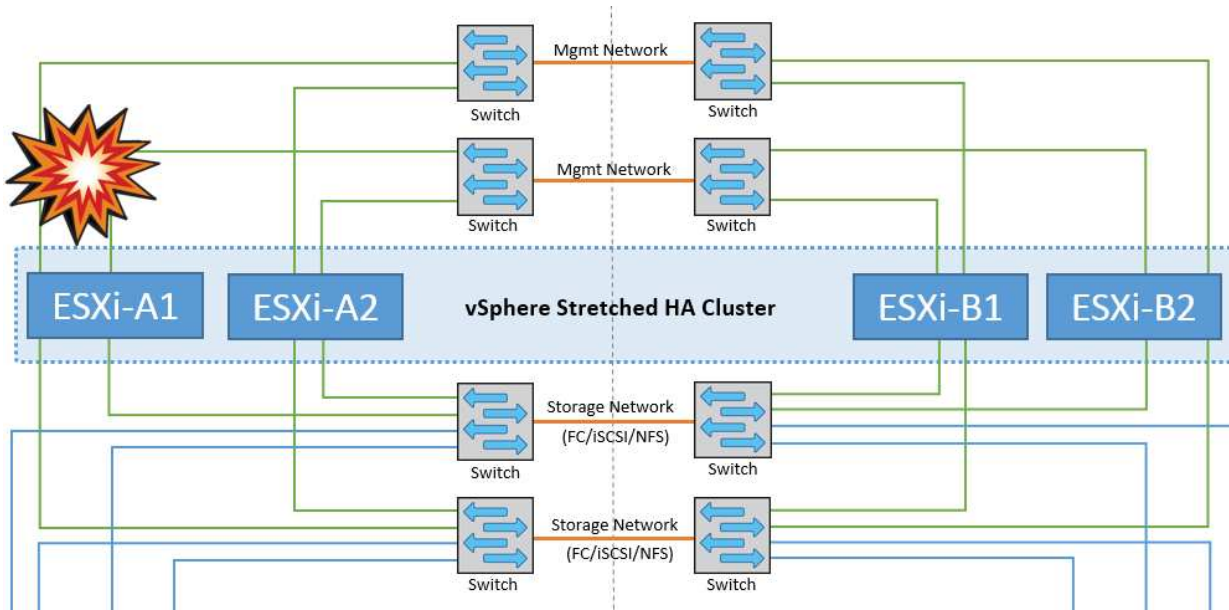
이 시나리오에서는 ESXi 호스트 장애가 있는 경우 VMware HA 클러스터의 마스터 노드가 더 이상 네트워크 하트비트를 수신하지 않기 때문에 호스트 장애를 감지합니다. 호스트가 실제로 다운되었는지 아니면 네트워크 파티션만 발생하는지 확인하기 위해 마스터 노드는 데이터 저장소 하트비트를 모니터링하고, 이 하트비트가 없는 경우 장애가 발생한 호스트의 관리 IP 주소를 ping하여 최종 점검을 수행합니다. 이러한 검사가 모두 음수이면 마스터 노드가 이 호스트에 장애가 발생한 호스트를 선언하고 장애가 발생한 이 호스트에서 실행 중이던 모든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

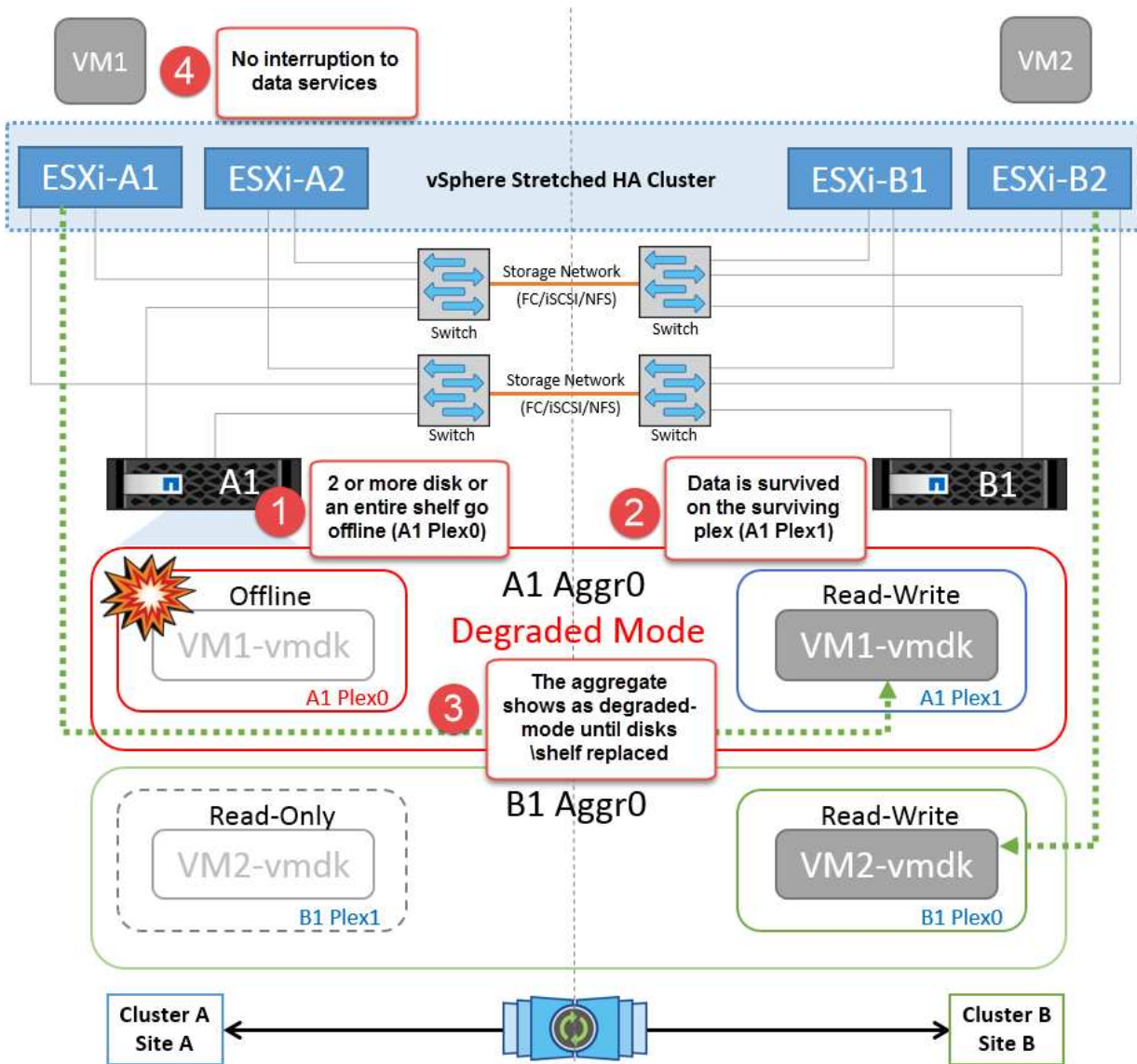


이 시나리오에서는 ESXi 호스트의 관리 네트워크가 다운된 경우 HA 클러스터의 마스터 노드가 하트비트를 수신하지 않으므로 이 호스트가 네트워크에서 격리됩니다. 마스터 노드가 데이터 저장소 하트비트를 모니터링하기 시작합니다. 호스트가 있는 경우 마스터 노드에 의해 격리된 것으로 선언됩니다. 구성된 격리 응답에 따라 호스트는 전원을 끄거나, 가상 시스템을 종료하거나, 가상 시스템의 전원을 계속 켜도록 선택할 수 있습니다. 격리 응답의 기본 간격은 30 초입니다.

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

디스크 셀프 오류입니다

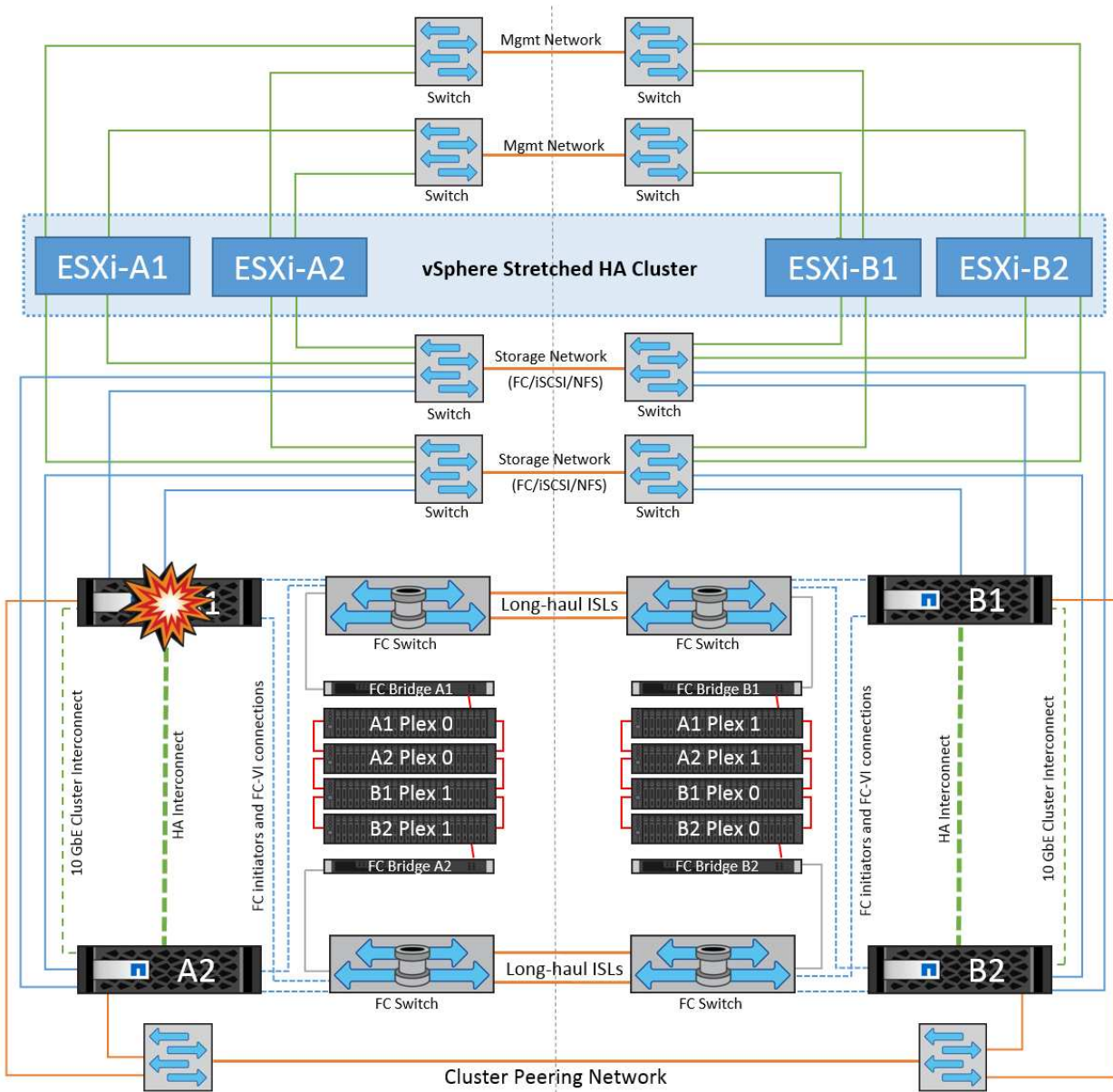
이 시나리오에서는 두 개 이상의 디스크에서 장애가 발생하거나 전체 쉘프에 장애가 발생합니다. 작동하는 플렉스에서 데이터 서비스를 중단하지 않고 데이터를 제공합니다. 디스크 장애가 로컬 또는 원격 플렉스에 영향을 줄 수 있습니다. 하나의 플렉스만 활성 상태이므로 애그리게이트가 성능 저하 모드로 표시됩니다. 장애가 발생한 디스크를 교체하면 영향을 받는 애그리게이트가 자동으로 다시 동기화되어 데이터를 재구축합니다. 다시 동기화하면 애그리게이트가 정상 미러링된 모드로 자동으로 돌아갑니다. 단일 RAID 그룹 내에서 두 개 이상의 디스크에 장애가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



참고: 이 기간 동안 가상 머신 I/O 작업에는 아무런 영향이 없지만 ISL 링크를 통해 원격 디스크 셸프에서 데이터에 액세스하므로 성능이 저하됩니다.

단일 스토리지 컨트롤러 장애

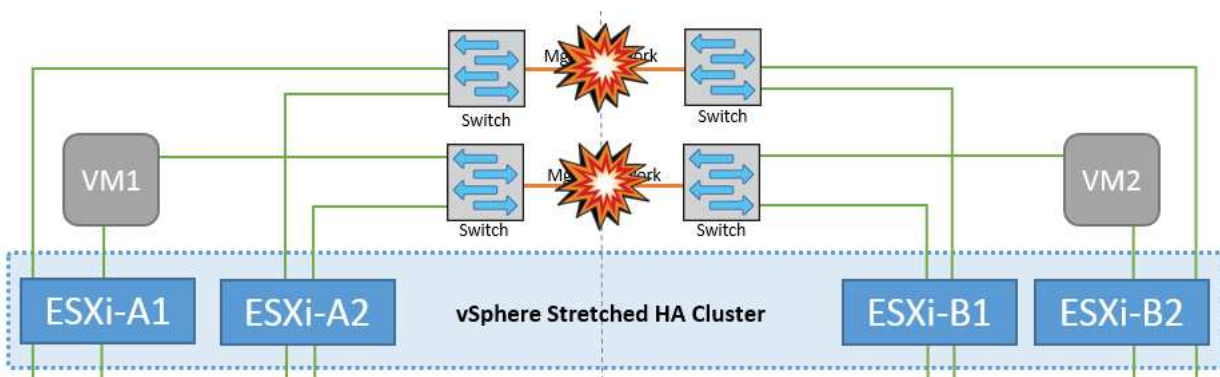
이 시나리오에서는 두 스토리지 컨트롤러 중 하나가 한 사이트에서 장애가 발생합니다. 각 사이트에 HA 쌍이 있으므로 한 노드에 장애가 발생하면 운영에 영향을 미치지 않고 다른 노드에 대한 페일오버가 자동으로 트리거됩니다. 예를 들어 노드 A1에 장애가 발생하면 해당 스토리지 및 워크로드가 자동으로 노드 A2로 전송됩니다. 모든 플렉스를 사용할 수 있으므로 가상 머신은 영향을 받지 않습니다. 두 번째 사이트 노드(B1 및 B2)는 영향을 받지 않습니다. 또한 클러스터의 마스터 노드가 네트워크 하트비트를 계속 수신하므로 vSphere HA는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

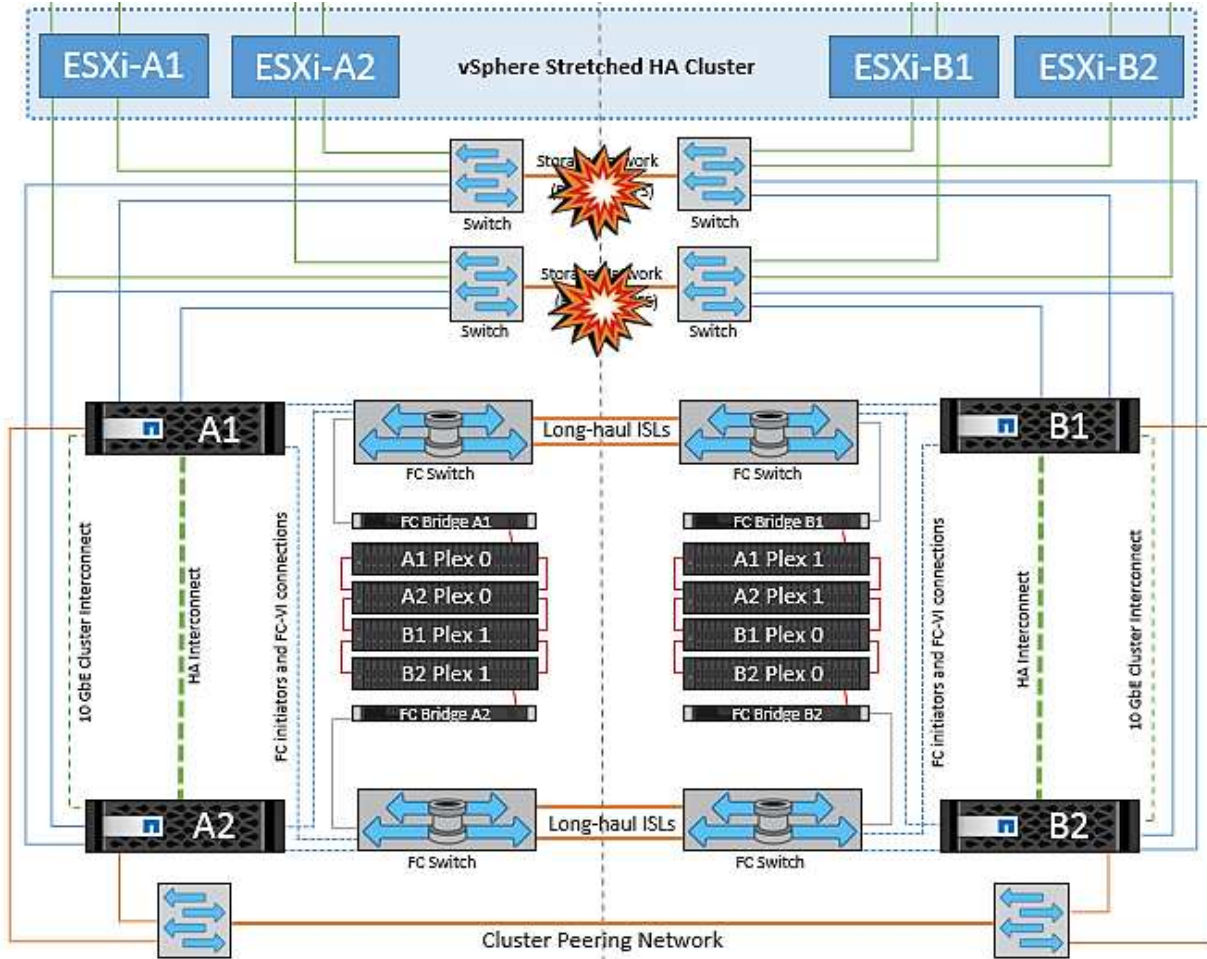
관리 네트워크에서 스위치 간 링크 오류



이 시나리오에서 프론트엔드 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.

- 참고: * 이 기간 동안 가상 머신은 계속 실행되고 있으며 이 시나리오에서는 MetroCluster 동작에 변화가 없습니다. 모든 데이터 저장소는 해당 사이트에서 그대로 유지됩니다.

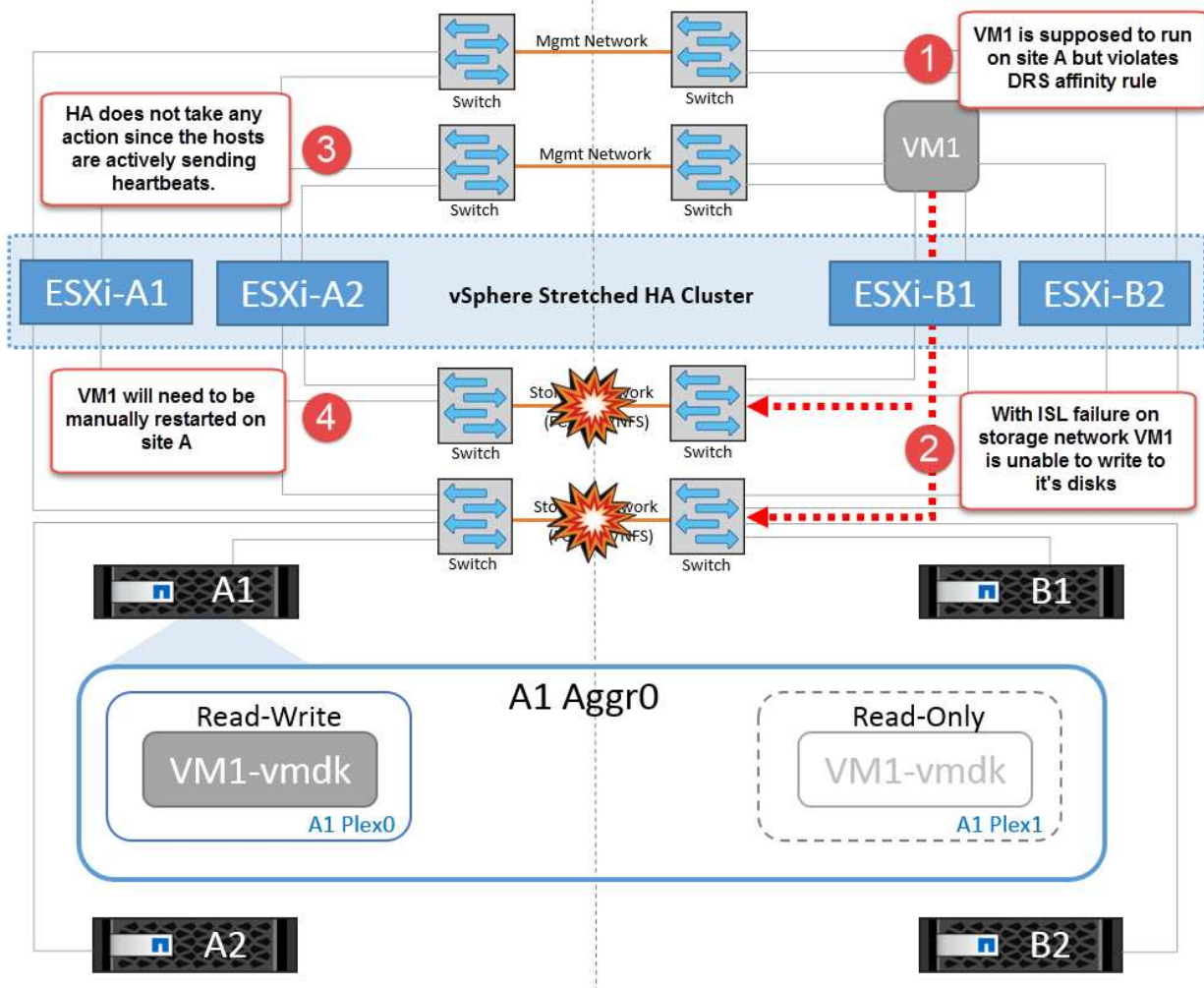
스토리지 네트워크에서 스위치 간 링크 오류



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.

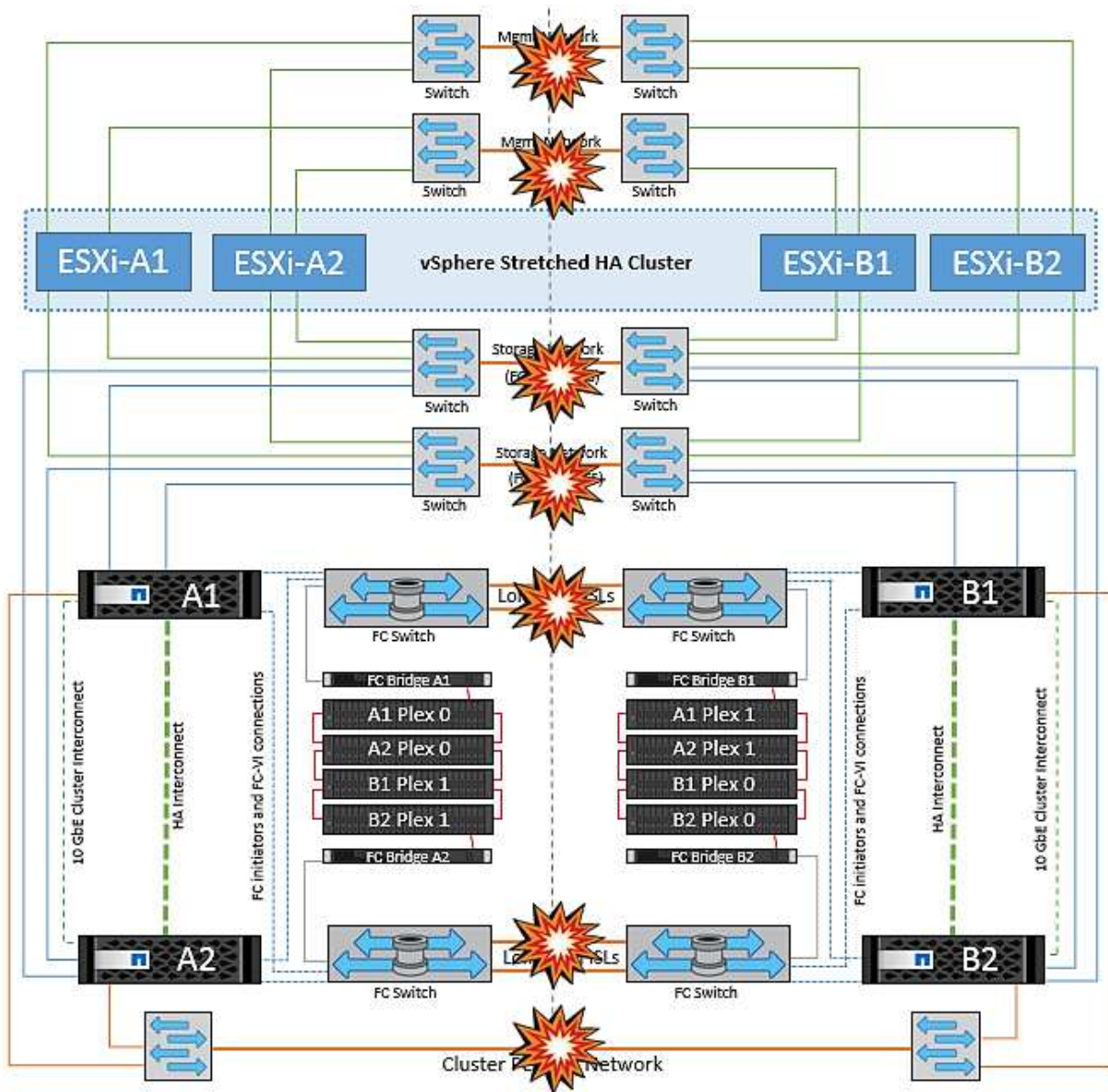
어떤 이유로 선호도 규칙을 위반하는 경우(예: 디스크가 로컬 클러스터 A 노드에 있는 사이트 A에서 실행되어야 하는 VM1이 사이트 B의 호스트에서 실행), 가상 머신의 디스크는 ISL 링크를 통해 원격으로 액세스됩니다. ISL 링크 장애로 인해 사이트 B에서 실행되는 VM1은 스토리지 볼륨에 대한 경로가 다운되고 특정 가상 시스템이 다운되기 때문에 해당 디스크에 쓸 수 없습니다. 이러한 경우 VMware HA는 호스트가 심박동을 능동적으로 전송하기 때문에 아무 작업도 수행하지 않습니다. 이러한 가상 머신의 전원을 수동으로 끄고 해당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



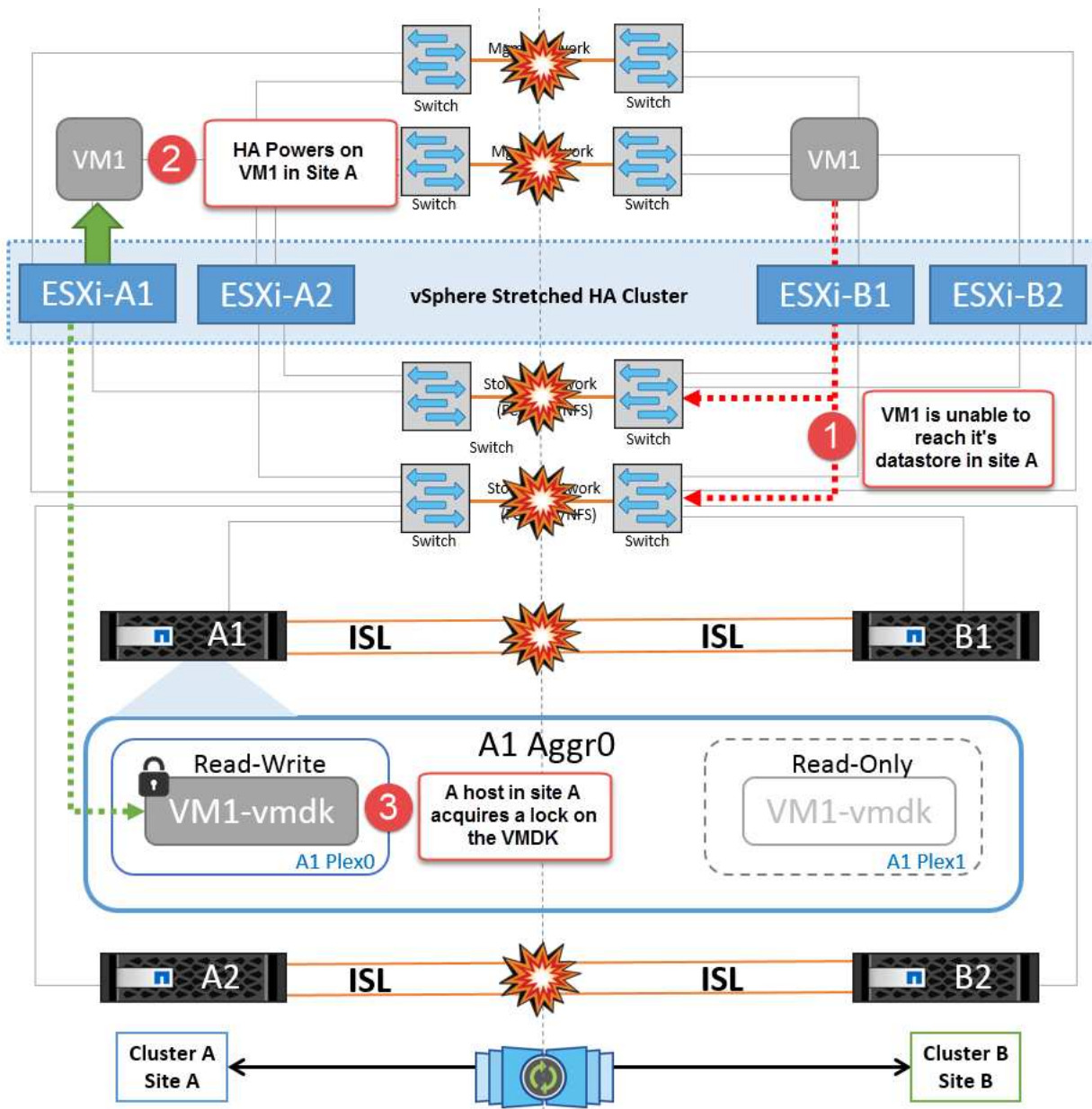
모든 인터스위치 오류 또는 전체 데이터 센터 파티션

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 다시 시작하려고 시도합니다. 스토리지 ISL 장애로 인해 사이트 B의 데이터 저장소에 액세스할 수 없기 때문에 결국 실패합니다. 비슷한 상황이 사이트 B에서 반복됩니다



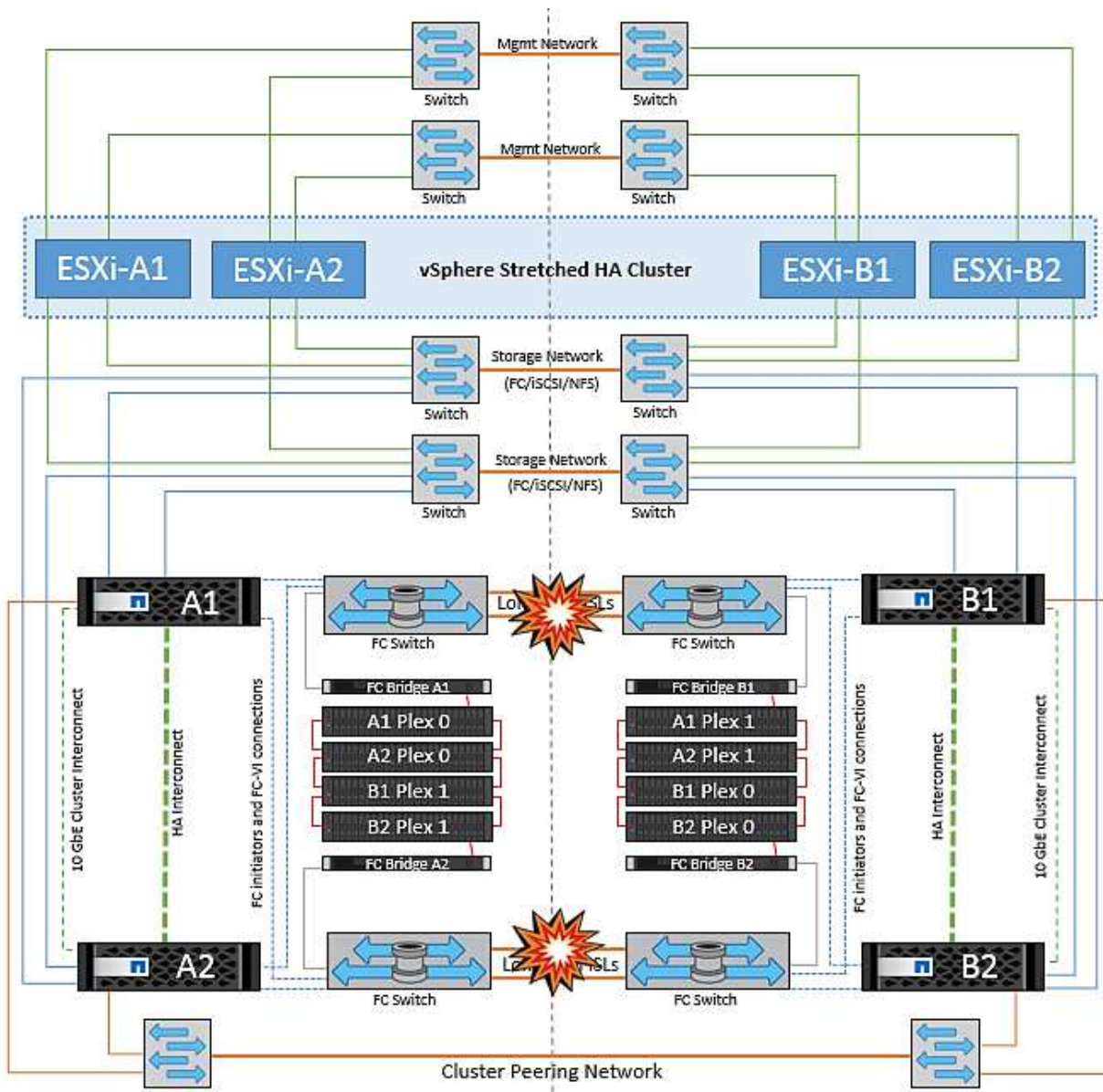
NetApp에서는 가상 시스템이 DRS 규칙을 위반했는지 여부를 확인하는 것이 좋습니다. 원격 사이트에서 실행되는 모든 가상 머신은 데이터 저장소에 액세스할 수 없으므로 작동이 중지되고 vSphere HA는 로컬 사이트에서 해당 가상 머신을 다시 시작합니다. ISL 링크가 다시 온라인 상태가 되면 동일한 MAC 주소로 실행되는 가상 시스템의 인스턴스가 두 개 있을 수 없으므로 원격 사이트에서 실행 중이던 가상 시스템이 종료됩니다.



NetApp MetroCluster의 두 Fabric에서 스위치 간 링크 장애가 발생했습니다

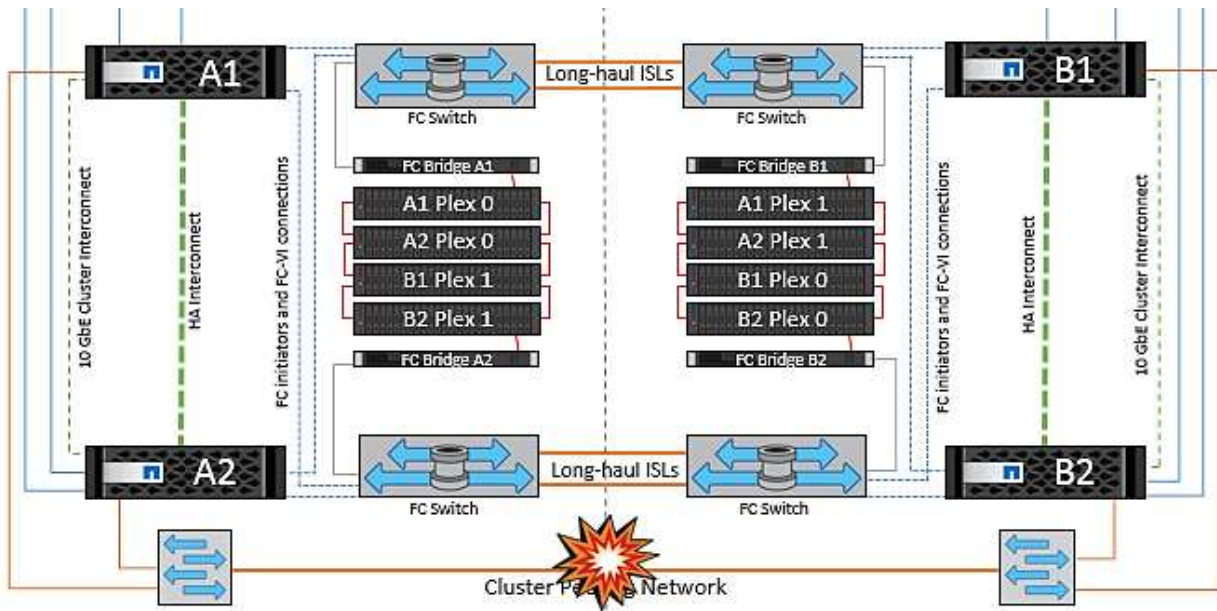
하나 이상의 ISL이 실패하는 경우 트래픽은 나머지 링크를 통해 계속됩니다. 두 Fabric의 모든 ISL에 장애가 발생하여 스토리지와 NVRAM 복제를 위해 사이트 간에 링크가 없는 경우, 각 컨트롤러는 계속해서 로컬 데이터를 제공합니다. ISL을 최소 한 개 이상 복구할 경우 모든 플렉스의 재동기화가 자동으로 수행됩니다.

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 링크를 복원하면 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.



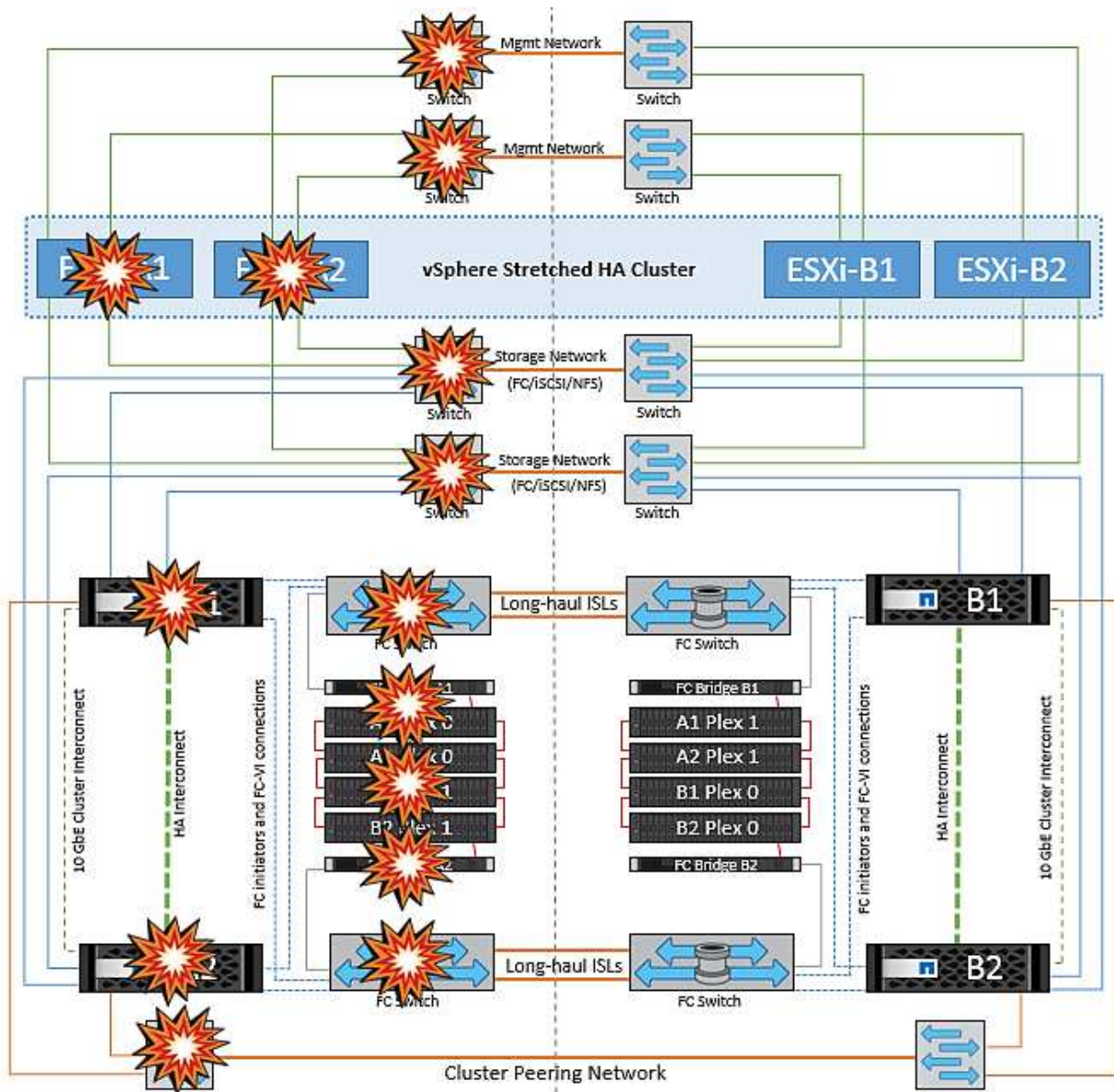
전체 사이트 오류입니다

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.

- 참고: * HA 마스터는 배치 관리자가 적합한 스토리지를 찾을 때까지 재시작 시도를 시작하지 않으므로 사이트 전체에 장애가 발생할 경우 전환이 수행된 후가 됩니다.

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.



저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.