개념
HCI

NetApp
October 11, 2024

목차

개념

NetApp HCI 제품 개요

NetApp HCI는 스토리지, 컴퓨팅, 네트워킹, 하이퍼바이저를 결합하고 퍼블릭 클라우드와 프라이빗 클라우드를 포괄하는 기능을 더해 주는 엔터프라이즈급 하이브리드 클라우드 인프라 설계입니다.

NetApp의 분리확장형 하이브리드 클라우드 인프라를 사용하면 컴퓨팅과 스토리지를 독립적으로 확장하여 성능이 보장된 워크로드에 적응할 수 있습니다.

- 하이브리드 멀티 클라우드 요구사항을 충족합니다
- 컴퓨팅과 스토리지를 독립적으로 확장합니다
- 하이브리드 멀티 클라우드에서 데이터 서비스 오케스트레이션을 간소화합니다

NetApp HCI의 구성 요소

다음은 NetApp HCI 환경의 다양한 구성 요소에 대한 개요입니다.

- NetApp HCI는 스토리지 및 컴퓨팅 리소스를 모두 제공합니다. NetApp HCI를 배포하려면 * NetApp Deployment Engine * 마법사를 사용합니다. 구축이 성공적으로 완료되면 컴퓨팅 노드가 ESXi 호스트로 표시되고 VMware vSphere Web Client에서 이를 관리할 수 있습니다.
- * 관리 서비스 * 또는 마이크로서비스는 Active IQ Collector, vCenter 플러그인용 QoSSIOC 및 mNode 서비스를 포함하며 서비스 번들로 자주 업데이트됩니다. Element 11.3 릴리스 현재 * 관리 서비스 * 는 관리 노드에서 호스팅되므로 주요 릴리스 이외의 특정 소프트웨어 서비스를 더 빠르게 업데이트할 수 있습니다. mNode * (관리 노드 *)는 하나 이상의 Element 소프트웨어 기반 스토리지 클러스터와 병렬로 실행되는 가상 머신입니다. 이 툴을 사용하면 모니터링 및 원격 측정을 포함하여 시스템 서비스를 업그레이드 및 제공하고, 클러스터 자산 및 설정을 관리하고, 시스템 테스트 및 유틸리티를 실행하고, 문제 해결을 위해 NetApp Support 액세스를 지원할 수 있습니다.

  에 대해 자세히 "관리 서비스 릴리스"알아보십시오.

- * NetApp 하이브리드 클라우드 제어 * 를 사용하여 NetApp HCI를 관리할 수 있습니다. NetApp SolidFire Active IQ를 사용하여 관리 서비스를 업그레이드하고, 시스템을 확장하고, 로그를 수집하고, 설치를 모니터링할 수 있습니다. NetApp Hybrid Cloud Control에 로그인하려면 관리 노드의 IP 주소로 이동합니다.
- vCenter Server * 용 * NetApp Element 플러그인은 vSphere UI(사용자 인터페이스)와 통합된 웹 기반 툴입니다. 이 플러그인은 VMware vSphere를 위한 확장 가능하고 사용자 친화적인 인터페이스로 * NetApp Element 소프트웨어 * 를 실행하는 스토리지 클러스터를 관리하고 모니터링할 수 있습니다. 이 플러그인은 Element UI 대신 사용할 수 있습니다. 플러그인 사용자 인터페이스를 사용하여 클러스터를 검색 및 구성하고, 클러스터 용량의 스토리지를 관리, 모니터링 및 할당하여 데이터 저장소 및 가상 데이터 저장소(가상 볼륨용)를 구성할 수 있습니다. 클러스터는 호스트 및 관리자에게 가상 IP 주소로 표시되는 단일 로컬 그룹으로 네트워크에 표시됩니다. 또한 다양한 작업을 수행하는 동안 발생할 수 있는 이벤트에 대한 오류 및 경고 메시지를 포함하여 실시간 보고를 통해 클러스터 활동을 모니터링할 수 있습니다.

  에 대해 자세히 "vCenter Server용 NetApp Element 플러그인"알아보십시오.

- 기본적으로 NetApp HCI는 성능 및 경고 통계를 * NetApp SolidFire Active IQ * 서비스로 보냅니다. 일반 지원 계약의 일부로서, NetApp Support는 이 데이터를 모니터링하고 성능 병목 현상 또는 잠재적인 시스템 문제를 경고합니다. 기존 SolidFire Active IQ 계정이 있더라도 NetApp Support 계정을 생성해야 하므로 서비스를 활용할 수 있습니다.

에 대해 자세히 "NetApp SolidFire Active IQ를 참조하십시오"알아보십시오.

NetApp HCI URL

NetApp HCI에서 사용하는 일반적인 URL은 다음과 같습니다.

URL	설명
`https://[IPv4 address of Bond1G interface on a storage node]`	NetApp 배포 엔진 마법사에 액세스하여 NetApp HCI를 설치 및 구성합니다. "자세한 정보."
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </code>	NetApp 하이브리드 클라우드 제어에 액세스하여 NetApp HCI 설치를 업그레이드, 확장, 모니터링하고 관리 서비스를 업데이트합니다. "자세한 정보."
`https://[IP address]:442`	노드별 UI에서 네트워크 및 클러스터 설정에 액세스하고 시스템 테스트 및 유틸리티를 활용합니다. "자세한 정보."
`https://<ManagementNodeIP>:9443`	vSphere Web Client에 vCenter 플러그인 패키지를 등록합니다.
`https://activeiq.solidfire.com`	데이터를 모니터링하고 성능 병목 현상 또는 잠재적인 시스템 문제에 대한 경고를 받습니다.
`https://<ManagementNodeIP>/mnode`	관리 노드의 REST API UI를 사용하여 관리 서비스를 수동으로 업데이트합니다.
`https://[storage cluster MVIP address]`	NetApp Element 소프트웨어 UI에 액세스합니다.

자세한 내용을 확인하십시오

- "vCenter Server용 NetApp Element 플러그인"
- "NetApp HCI 리소스 페이지를 참조하십시오"

사용자 계정

시스템의 스토리지 리소스에 액세스하려면 사용자 계정을 설정해야 합니다.

사용자 계정 관리

사용자 계정은 NetApp Element 소프트웨어 기반 네트워크에서 스토리지 리소스에 대한 액세스를 제어하는 데 사용됩니다. 볼륨을 생성하기 전에 최소 하나의 사용자 계정이 필요합니다.

볼륨을 생성하면 계정에 할당됩니다. 가상 볼륨을 생성한 경우 해당 계정은 스토리지 컨테이너입니다.

다음은 몇 가지 추가 고려 사항입니다.

- 이 계정에는 할당된 볼륨에 액세스하는 데 필요한 CHAP 인증이 포함되어 있습니다.
- 계정에는 최대 2000개의 볼륨이 할당될 수 있지만 볼륨은 하나의 계정에만 속할 수 있습니다.
- 사용자 계정은 NetApp Element 관리 확장 지점에서 관리할 수 있습니다.

NetApp 하이브리드 클라우드 제어를 사용하면 다음과 같은 유형의 고객을 생성하고 관리할 수 있습니다.

- 스토리지 클러스터에 대한 관리자 사용자 계정입니다
- 권한 있는 사용자 계정
- 생성된 스토리지 클러스터에만 해당하는 볼륨 계정입니다.

스토리지 클러스터 관리자 계정

NetApp Element 소프트웨어를 실행하는 스토리지 클러스터에 있을 수 있는 관리자 계정에는 두 가지 유형이 있습니다.

- * 기본 클러스터 관리자 계정 *: 이 관리자 계정은 클러스터를 생성할 때 생성됩니다. 이 계정은 클러스터에 대한 최고 수준의 액세스 권한을 가진 기본 관리 계정입니다. 이 계정은 Linux 시스템의 루트 사용자와 유사합니다. 이 관리자 계정의 암호를 변경할 수 있습니다.
- * 클러스터 관리자 계정 *: 클러스터 관리자 계정에 제한된 범위의 관리 액세스 권한을 부여하여 클러스터 내에서 특정 작업을 수행할 수 있습니다. 각 클러스터 관리자 계정에 할당된 자격 증명은 스토리지 시스템 내에서 API 및 Element UI 요청을 인증하는 데 사용됩니다.

> 노드별 UI를 통해 클러스터의 활성 노드에 액세스하려면 로컬(LDAP가 아닌) 클러스터 관리자 계정이 필요합니다. 아직 클러스터에 속하지 않은 노드에 액세스하려면 계정 자격 증명이 필요하지 않습니다.

클러스터 관리자 계정을 생성, 삭제 및 편집하고, 클러스터 관리자 암호를 변경하고, 사용자에 대한 시스템 액세스를 관리하도록 LDAP 설정을 구성하여 클러스터 관리자 계정을 관리할 수 있습니다.

자세한 내용은 를 "SolidFire 및 Element 문서 센터"참조하십시오.

권한 있는 사용자 계정

권한 있는 사용자 계정은 노드 및 클러스터의 NetApp 하이브리드 클라우드 제어 인스턴스와 연결된 스토리지 자산에 대해 인증할 수 있습니다. 이 계정을 사용하면 모든 클러스터에서 볼륨, 계정, 액세스 그룹 등을 관리할 수 있습니다.

권한 있는 사용자 계정은 NetApp 하이브리드 클라우드 제어의 오른쪽 상단 메뉴 사용자 관리 옵션에서 관리합니다.

"권한 있는 스토리지 클러스터"는 NetApp 하이브리드 클라우드 제어가 사용자 인증에 사용하는 스토리지 클러스터입니다.

신뢰할 수 있는 스토리지 클러스터에서 생성된 모든 사용자는 NetApp 하이브리드 클라우드 제어에 로그인할 수 있습니다. 다른 스토리지 클러스터에서 생성한 사용자는 하이브리드 클라우드 제어에 _cannot_logon 할 수 없습니다.

- 관리 노드에 스토리지 클러스터가 하나만 있는 경우 신뢰할 수 있는 클러스터입니다.
- 관리 노드에 둘 이상의 스토리지 클러스터가 있는 경우 이러한 클러스터 중 하나가 권한 있는 클러스터로 할당되고 해당 클러스터의 사용자만 NetApp 하이브리드 클라우드 제어에 로그인할 수 있습니다.

많은 NetApp 하이브리드 클라우드 제어 기능이 여러 스토리지 클러스터에서 작동되지만, 인증과 권한 부여는 필수 제한 사항이 됩니다. 인증 및 권한 부여에 대한 제한 사항은 권한 있는 클러스터의 사용자가 다른 스토리지 클러스터에 있는

사용자가 아니더라도 NetApp 하이브리드 클라우드 제어에 연결된 다른 클러스터에 대해 작업을 실행할 수 있다는 것입니다. 여러 스토리지 클러스터를 관리하기 전에 권한 있는 클러스터에 정의된 사용자가 동일한 권한을 가진 다른 모든 스토리지 클러스터에 정의되어 있는지 확인해야 합니다. NetApp 하이브리드 클라우드 제어에서 사용자를 관리할 수 있습니다.

볼륨 계정

볼륨별 계정은 생성된 스토리지 클러스터에만 적용됩니다. 이러한 계정을 사용하면 네트워크 전체의 특정 볼륨에 대한 사용 권한을 설정할 수 있지만 이러한 볼륨 외부에는 영향을 미치지 않습니다.

볼륨 계정은 NetApp Hybrid Cloud Control Volumes 표 내에서 관리됩니다.

자세한 내용을 확인하십시오

- "사용자 계정을 관리합니다"
- "클러스터에 대해 알아보십시오"
- "NetApp HCI 리소스 페이지를 참조하십시오"
- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 문서 센터"

데이터 보호

NetApp HCI 데이터 보호 용어에는 다양한 유형의 원격 복제, 볼륨 스냅샷, 볼륨 클론 복제, 보호 도메인, 이중 Helix 기술을 통한 고가용성 등이 포함됩니다.

NetApp HCI 데이터 보호에는 다음과 같은 개념이 포함되어 있습니다.

- 원격 복제 유형입니다
- 데이터 보호를 위한 볼륨 스냅샷입니다
- 볼륨 클론
- SolidFire 스토리지에 대한 백업 및 복원 프로세스 개요
- 보호 도메인
- 이중 Helix 고가용성

원격 복제 유형입니다

데이터의 원격 복제에는 다음과 같은 형태가 있습니다.

- 클러스터 간 동기식 및 비동기식 복제
- 스냅샷 전용 복제
- SnapMirror를 사용하여 Element와 ONTAP 클러스터 간 복제

을 "TR-4741: NetApp Element 소프트웨어 원격 복제"참조하십시오.

클러스터 간 동기식 및 비동기식 복제

NetApp Element 소프트웨어를 실행하는 클러스터의 경우 실시간 복제를 통해 볼륨 데이터의 원격 복사본을 신속하게 생성할 수 있습니다.

스토리지 클러스터를 최대 4개의 다른 스토리지 클러스터와 페어링할 수 있습니다. 장애 조치 및 장애 복구 시나리오를 위해 클러스터 쌍의 클러스터 중 하나에서 볼륨 데이터를 동기 또는 비동기식으로 복제할 수 있습니다.

동기식 복제

동기식 복제는 소스 클러스터에서 타겟 클러스터로 지속적으로 데이터를 복제하며 지연 시간, 패킷 손실, 지터 및 대역폭에 의해 영향을 받습니다.

동기식 복제는 다음과 같은 상황에 적합합니다.

- 짧은 거리에서 여러 시스템을 복제합니다
- 소스에 지리적으로 로컬 재해 복구 사이트입니다
- 시간에 민감한 애플리케이션 및 데이터베이스 보호
- 운영 사이트가 다운된 경우 2차 사이트가 운영 사이트 역할을 해야 하는 비즈니스 연속성 애플리케이션

비동기식 복제

비동기식 복제는 타겟 클러스터의 승인을 기다리지 않고 소스 클러스터에서 타겟 클러스터로 지속적으로 데이터를 복제합니다. 비동기식 복제 중에는 소스 클러스터에서 커밋된 후 클라이언트(애플리케이션)에 쓰기가 확인됩니다.

비동기식 복제는 다음과 같은 상황에 적합합니다.

- 재해 복구 사이트가 소스에서 멀리 떨어져 있고 애플리케이션이 네트워크에 의해 발생하는 지연 시간을 허용하지 않습니다.
- 소스 및 타겟 클러스터를 연결하는 네트워크에는 대역폭 제한이 있습니다.

스냅샷 전용 복제

스냅샷 전용 데이터 보호는 특정 시점의 변경된 데이터를 원격 클러스터로 복제합니다. 소스 클러스터에서 생성된 스냅샷만 복제됩니다. 소스 볼륨의 활성 쓰기는 그렇지 않습니다.

스냅샷 복제 빈도를 설정할 수 있습니다.

스냅샷 복제는 비동기식 또는 동기식 복제에 영향을 주지 않습니다.

SnapMirror를 사용하여 **Element**와 **ONTAP** 클러스터 간 복제

NetApp SnapMirror 기술을 사용하면 NetApp Element 소프트웨어를 사용하여 촬영한 스냅샷을 재해 복구를 위해 ONTAP로 복제할 수 있습니다. SnapMirror 관계에서 Element는 하나의 엔드포인트이고 ONTAP는 다른 엔드포인트입니다.

SnapMirror는 지리적으로 원격 사이트의 운영 스토리지에서 2차 스토리지로 페일오버할 수 있도록 설계된 재해 복구를 촉진하는 NetApp Snapshot ™ 복제 기술입니다. SnapMirror 기술은 1차 사이트에서 장애가 발생하더라도 데이터를 계속 제공할 수 있는 2차 스토리지에서 작업 데이터의 복제본 또는 미러를 생성합니다. 데이터가 볼륨 레벨에서 미러링됩니다.

운영 스토리지의 소스 볼륨과 2차 스토리지의 타겟 볼륨 간의 관계를 데이터 보호 관계라고 합니다. 클러스터는 볼륨이 상주하는 엔드포인트라고 하며 복제된 데이터가 포함된 볼륨을 살펴봐야 합니다. 피어 관계를 사용하면 클러스터와 볼륨이 데이터를 안전하게 교환할 수 있습니다.

SnapMirror는 기본적으로 NetApp ONTAP 컨트롤러에서 실행되며 NetApp HCI 및 SolidFire 클러스터에서 실행되는 Element에 통합되어 있습니다. SnapMirror를 제어하는 로직은 ONTAP 소프트웨어에 상주하므로, 모든 SnapMirror 관계는 조정 작업을 수행하기 위해 적어도 하나의 ONTAP 시스템을 포함해야 합니다. 사용자는 기본적으로 Element UI를 통해 Element와 ONTAP 클러스터 간의 관계를 관리합니다. 그러나 일부 관리 작업은 NetApp ONTAP System Manager에 상주합니다. 사용자는 ONTAP와 Element에서 모두 사용할 수 있는 CLI 및 API를 통해 SnapMirror를 관리할 수도 있습니다.

를 참조하십시오 "TR-4651: NetApp SolidFire SnapMirror 아키텍처 및 구성"(로그인 필요).

Element 소프트웨어를 사용하여 클러스터 레벨에서 SnapMirror 기능을 수동으로 활성화해야 합니다. SnapMirror 기능은 기본적으로 비활성화되어 있으며, 새로운 설치 또는 업그레이드의 일부로 자동 활성화되지 않습니다.

SnapMirror를 사용하도록 설정한 후 Element 소프트웨어의 데이터 보호 탭에서 SnapMirror 관계를 생성할 수 있습니다.

데이터 보호를 위한 볼륨 스냅샷입니다

볼륨 스냅샷은 나중에 볼륨을 특정 시간으로 복원하는 데 사용할 수 있는 볼륨의 시점 복제본입니다.

스냅숏은 볼륨 클론과 비슷하지만 스냅숏은 볼륨 메타데이터의 복제본이므로 마운트하거나 쓸 수 없습니다. 볼륨 스냅샷을 생성하면 시스템 리소스 및 공간도 소량만 차지하기 때문에 클론 생성보다 스냅샷 생성 속도가 빨라집니다.

스냅샷을 원격 클러스터에 복제하고 이를 볼륨의 백업 복사본으로 사용할 수 있습니다. 이렇게 하면 복제된 스냅샷을 사용하여 볼륨을 특정 시점으로 롤백할 수 있으며 복제된 스냅샷으로부터 볼륨의 클론을 생성할 수도 있습니다.

SolidFire 클러스터에서 외부 오브젝트 저장소 또는 다른 SolidFire 클러스터로 스냅샷을 백업할 수 있습니다. 외부 개체 저장소에 스냅샷을 백업할 때 읽기/쓰기 작업을 허용하는 개체 저장소에 대한 연결이 있어야 합니다.

데이터 보호를 위해 개별 볼륨의 스냅샷 또는 여러 개의 스냅샷을 생성할 수 있습니다.

볼륨 클론

단일 볼륨 또는 여러 볼륨의 클론은 데이터의 시점 복사본입니다. 볼륨을 클론하면 시스템에서 볼륨의 스냅샷을 생성한 다음 스냅샷이 참조하는 데이터의 복제본을 생성합니다.

비동기식 프로세스이며, 프로세스에 필요한 시간은 클론 생성 중인 볼륨의 크기와 현재 클러스터 로드에 따라 다릅니다.

클러스터는 한 번에 볼륨당 최대 2개의 클론 요청을 실행하고 한 번에 최대 8개의 활성 볼륨 클론 작업을 지원합니다. 이러한 제한을 초과하는 요청은 나중에 처리할 수 있도록 대기열에 추가됩니다.

SolidFire 스토리지에 대한 백업 및 복원 프로세스 개요

Amazon S3 또는 OpenStack Swift와 호환되는 2차 오브젝트 저장소뿐만 아니라 다른 SolidFire 스토리지에 볼륨을 백업 및 복원할 수 있습니다.

볼륨을 다음 항목에 백업할 수 있습니다.

- SolidFire 스토리지 클러스터입니다

- Amazon S3 오브젝트 저장소
- OpenStack Swift 오브젝트 저장소

OpenStack Swift 또는 Amazon S3에서 볼륨을 복원할 때 원래 백업 프로세스에서 매니페스트 정보가 필요합니다. SolidFire 스토리지 시스템에서 백업한 볼륨을 복원하는 경우 매니페스트 정보가 필요하지 않습니다.

보호 도메인

보호 도메인은 데이터 가용성을 유지하면서 일부 또는 전부에 장애가 발생할 수 있도록 그룹화된 노드 또는 노드 세트입니다. 보호 도메인을 사용하면 스토리지 클러스터가 섀시(섀시 선호도) 또는 전체 도메인(섀시 그룹)의 손실로부터 자동으로 치유됩니다.

보호 도메인 레이아웃은 각 노드를 특정 보호 도메인에 할당합니다.

보호 도메인 수준이라는 두 가지 보호 도메인 레이아웃이 지원됩니다.

- 노드 레벨에서 각 노드는 고유한 보호 도메인에 있습니다.
- 섀시 레벨에서는 섀시를 공유하는 노드만 동일한 보호 도메인에 있습니다.
  - 섀시 레벨 레이아웃은 노드가 클러스터에 추가될 때 하드웨어에서 자동으로 결정됩니다.
  - 각 노드가 별도의 섀시에 있는 클러스터에서는 이 두 레벨이 기능적으로 동일합니다.

vCenter Server용 NetApp Element 플러그인을 사용하여 수동으로 수행할 수 "보호 도메인 모니터링을 활성화합니다" 있습니다. 노드 또는 섀시 도메인에 따라 보호 도메인 임계값을 선택할 수 있습니다.

새 클러스터를 생성할 때 공유 섀시에 있는 스토리지 노드를 사용하는 경우 보호 도메인 기능을 사용하여 섀시 레벨 장애 보호를 설계할 수 있습니다.

각 노드가 1개 및 1개의 사용자 지정 보호 도메인과 연결되는 사용자 지정 보호 도메인 레이아웃을 정의할 수 있습니다. 기본적으로 각 노드는 동일한 기본 사용자 지정 보호 도메인에 할당됩니다.

을 "SolidFire 및 Element 12.2 문서 센터"참조하십시오.

이중 **Helix** 고가용성

이중 Helix 데이터 보호는 시스템 내 모든 드라이브에 두 개 이상의 중복 데이터 복사본을 배포하는 복제 방법입니다. “RAID-less” 접근 방식을 통해 시스템은 스토리지 시스템의 모든 레벨에서 동시에 여러 건의 장애를 흡수하고 신속하게 복구할 수 있습니다.

자세한 내용을 확인하십시오

- "NetApp HCI 리소스 페이지를 참조하십시오"
- "vCenter Server용 NetApp Element 플러그인"

클러스터

클러스터는 집합적인 방식으로 작동하는 노드 그룹으로, 스토리지 또는 컴퓨팅 리소스를 제공합니다. NetApp HCI 1.8부터는 스토리지 클러스터에 두 개의 노드를 포함할 수 있습니다. 스토리지 클러스터는 네트워크에 단일 논리 그룹으로 표시되며, 그런 다음 블록 스토리지로

액세스할 수 있습니다.

NetApp HCI의 스토리지 계층은 NetApp Element 소프트웨어에 의해 제공되며 관리 계층은 vCenter Server용 NetApp Element 플러그인에서 제공됩니다. 스토리지 노드는 Bond10G 네트워크 인터페이스를 통해 서로 통신하는 드라이브 모음이 포함된 서버입니다. 각 스토리지 노드는 2개의 네트워크, 즉 스토리지와 관리에 연결되며 각 네트워크에는 중복성과 성능을 위한 2개의 독립적인 링크가 있습니다. 각 노드에는 각 네트워크의 IP 주소가 필요합니다. 새 스토리지 노드로 클러스터를 생성하거나 기존 클러스터에 스토리지 노드를 추가하여 스토리지 용량과 성능을 높일 수 있습니다.

권한 있는 스토리지 클러스터

신뢰할 수 있는 스토리지 클러스터는 NetApp 하이브리드 클라우드 제어에서 사용자를 인증하는 데 사용하는 스토리지 클러스터입니다.

관리 노드에 스토리지 클러스터가 하나만 있는 경우 신뢰할 수 있는 클러스터입니다. 관리 노드에 둘 이상의 스토리지 클러스터가 있는 경우 이러한 클러스터 중 하나가 권한 있는 클러스터로 할당되고 해당 클러스터의 사용자만 NetApp 하이브리드 클라우드 제어에 로그인할 수 있습니다. API를 사용하면 어떤 클러스터가 신뢰할 수 있는 클러스터인지 확인할 수 `GET /mnode/about` 있습니다. 응답에서 필드의 IP 주소는 `token_url` 권한 있는 스토리지 클러스터의 관리 가상 IP 주소(MVIP)입니다. NetApp 하이브리드 클라우드 제어에 권한 있는 클러스터에 없는 사용자로 로그인하려고 하면 로그인 시도가 실패합니다.

많은 NetApp 하이브리드 클라우드 제어 기능은 여러 스토리지 클러스터에서 작동하도록 설계되었지만 인증과 권한 부여에는 제한이 있습니다. 인증 및 권한 부여에 대한 제한 사항은 권한 있는 클러스터의 사용자가 다른 스토리지 클러스터의 사용자가 아니더라도 NetApp 하이브리드 클라우드 제어에 연결된 다른 클러스터에 대한 작업을 실행할 수 있다는 것입니다. 여러 스토리지 클러스터를 관리하기 전에 권한 있는 클러스터에 정의된 사용자가 동일한 권한을 가진 다른 모든 스토리지 클러스터에 정의되어 있는지 확인해야 합니다.

NetApp 하이브리드 클라우드 제어로 사용자를 관리할 수 있습니다.

여러 스토리지 클러스터를 관리하기 전에 권한 있는 클러스터에 정의된 사용자가 동일한 권한을 가진 다른 모든 스토리지 클러스터에 정의되어 있는지 확인해야 합니다. Element 소프트웨어 사용자 인터페이스(Element 웹 UI)에서 수행할 수 "사용자 관리" 있습니다.

관리 노드 스토리지 클러스터 자산 작업에 대한 자세한 내용은 을 "스토리지 클러스터 자산을 생성하고 관리합니다 "참조하십시오.

고립된 용량

새로 추가된 노드가 전체 클러스터 용량의 50% 이상을 차지하는 경우 이 노드의 일부 용량을 사용할 수 없게 되어 용량 규칙을 준수합니다("고립됨"). 이는 스토리지 용량이 더 추가될 때까지 유지됩니다. 용량 규칙에 불복종하는 매우 큰 노드가 추가되면 이전에 고립된 노드는 더 이상 고립되지 않고 새로 추가된 노드는 고립됩니다. 이러한 상황이 발생하지 않도록 용량을 항상 쌍으로 추가해야 합니다. 노드가 고립되면 적절한 클러스터 장애가 throw됩니다.

2노드 스토리지 클러스터

NetApp HCI 1.8부터 스토리지 노드 2개로 스토리지 클러스터를 설정할 수 있습니다.

- 특정 유형의 노드를 사용하여 2노드 스토리지 클러스터를 구성할 수 있습니다. 을 "NetApp HCI 1.8 릴리스 정보 "참조하십시오.

> 2노드 클러스터의 스토리지 노드는 480GB 및 960GB 드라이브가 있는 노드로 제한되며 노드는 동일한 모델 유형이어야 합니다.

- 2노드 스토리지 클러스터는 대용량 및 고성능 요구사항에 종속되지 않는 워크로드를 가진 소규모 구축에 적합합니다.
- 2개의 스토리지 노드 외에도 2노드 스토리지 클러스터에는 2개의 NetApp HCI Witness Node * 가 포함됩니다.

  에 대해 자세히 알아보십시오 "증명선 노드."

- 2노드 스토리지 클러스터를 3노드 스토리지 클러스터로 확장할 수 있습니다. 3노드 클러스터는 스토리지 노드 장애를 자동으로 복구할 수 있는 기능을 제공하여 복원력을 향상합니다.
- 2노드 스토리지 클러스터는 기존의 4노드 스토리지 클러스터와 동일한 보안 기능을 제공합니다.
- 2노드 스토리지 클러스터는 4노드 스토리지 클러스터와 동일한 네트워크를 사용합니다. NetApp HCI 구축 중에 NetApp 구축 엔진 마법사를 사용하여 네트워크를 설정합니다.

스토리지 클러스터 쿼럼입니다

Element 소프트웨어는 선택한 노드에서 스토리지 클러스터를 생성하며, 이 노드는 클러스터 구성의 복제된 데이터베이스를 유지 관리합니다. 클러스터 복원력을 위해 쿼럼을 유지하려면 클러스터 앙상블에 최소한 3개의 노드가 필요합니다. 2노드 클러스터의 감시 노드는 유효한 앙상블 쿼럼을 형성하기에 충분한 스토리지 노드가 있는지 확인하는 데 사용됩니다. 앙상블 생성을 위해 스토리지 노드가 Witness Node 보다 선호됩니다. 2노드 스토리지 클러스터를 포함하는 최소 3노드 앙상블의 경우 2개의 스토리지 노드와 1개의 Witness 노드가 사용됩니다.

스토리지 노드 2개와 Witness 노드 1개가 있는 3노드 앙상블에서 스토리지 노드 1개가 오프라인이 되면 클러스터는 성능 저하 상태가 됩니다. 두 개의 Witness Node 중 한 개만 앙상블에서 활성화할 수 있습니다. 두 번째 Witness Node는 백업 역할을 수행하기 때문에 앙상블에 추가할 수 없습니다. 오프라인 스토리지 노드가 온라인 상태가 되거나 대체 노드가 클러스터에 연결될 때까지 클러스터는 성능 저하 상태를 유지합니다.

Witness Node에 장애가 발생하면 나머지 Witness Node가 앙상블에 가입하여 3노드 앙상블을 형성합니다. 장애가 발생한 Witness 노드를 교체하기 위해 새 Witness 노드를 구축할 수 있습니다.

2노드 스토리지 클러스터에서 자동 복구 및 장애 처리

기존 클러스터에 속한 노드에서 하드웨어 구성 요소에 장애가 발생하면 클러스터가 클러스터의 다른 사용 가능한 노드로 장애가 발생한 구성 요소에 있던 데이터를 재조정합니다. 2노드 스토리지 클러스터에서는 최소 3개의 물리적 스토리지 노드를 사용하여 자동으로 복구할 수 있어야 하므로 이 자동 복구 기능을 사용할 수 없습니다. 2노드 클러스터의 한 노드에 장애가 발생할 경우 2노드 클러스터에서 두 번째 데이터 복사본을 재생성할 필요가 없습니다. 나머지 활성 스토리지 노드의 블록 데이터에 대해 새 쓰기가 복제됩니다. 장애가 발생한 노드가 교체되고 클러스터에 추가되면 데이터가 두 물리적 스토리지 노드 간에 재조정됩니다.

3개 이상의 노드가 있는 스토리지 클러스터

2개의 스토리지 노드에서 3개의 스토리지 노드로 확장하면 노드 및 드라이브 장애가 발생할 경우 자동 복구가 가능하지만 추가 용량은 제공되지 않습니다. 를 사용하여 확장할 수 "NetApp 하이브리드 클라우드 제어 UI"있습니다. 2노드 클러스터에서 3노드 클러스터로 확장할 경우 용량이 고립될 수 있습니다(참조고립된 용량). UI 마법사는 설치 전에 고립된 용량에 대한 경고를 표시합니다. 스토리지 노드 장애 시 앙상블 쿼럼을 유지할 수 있는 단일 Witness Node를 사용할 수 있으며, 두 번째 Witness Node는 대기 상태로 유지됩니다. 3노드 스토리지 클러스터를 4노드 클러스터로 확장하면 용량과 성능이 향상됩니다. 4노드 클러스터에서는 Witness 노드가 더 이상 클러스터 쿼럼을 형성하지 않아도 됩니다. 최대 64개의 컴퓨팅 노드와 40개의 스토리지 노드로 확장할 수 있습니다.

자세한 내용을 확인하십시오

- "NetApp HCI 2노드 스토리지 클러스터 | TR-4823"
- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 설명서 센터"

노드

노드는 블록 스토리지 및 컴퓨팅 기능을 제공하기 위해 클러스터로 그룹화된 하드웨어 또는 가상 리소스입니다.

NetApp HCI 및 Element 소프트웨어는 클러스터에 대한 다양한 노드 역할을 정의합니다. 노드 역할의 네 가지 유형은 * 관리 노드 *, * 스토리지 노드 *, * 컴퓨팅 노드 * 및 * NetApp HCI Witness 노드 * 입니다.

관리 노드

관리 노드(mNode로 약칭)는 스토리지 클러스터와 상호 작용하여 관리 작업을 수행하지만 스토리지 클러스터의 구성원이 아닙니다. 관리 노드는 API 호출을 통해 클러스터에 대한 정보를 정기적으로 수집하고 이 정보를 Active IQ에 보고하여 원격 모니터링을 수행합니다(활성화된 경우). 관리 노드도 클러스터 노드의 소프트웨어 업그레이드를 조정합니다.

관리 노드는 하나 이상의 Element 소프트웨어 기반 스토리지 클러스터와 병렬로 실행되는 가상 머신(VM)입니다. 업그레이드 외에도 모니터링 및 원격 측정을 포함한 시스템 서비스를 제공하고, 클러스터 자산 및 설정을 관리하고, 시스템 테스트 및 유틸리티를 실행하고, 문제 해결을 위해 NetApp Support 액세스를 지원하는 데 사용됩니다. Element 11.3 릴리스 현재 관리 노드는 마이크로서비스 호스트로 작동하며, 주요 릴리스 이외의 특정 소프트웨어 서비스를 더 빠르게 업데이트할 수 있습니다. Active IQ Collector, vCenter 플러그인용 QoSSIOC, 관리 노드 서비스와 같은 이러한 마이크로서비스 또는 관리 서비스는 서비스 번들로 자주 업데이트됩니다.

스토리지 노드

NetApp HCI 스토리지 노드는 NetApp HCI 시스템에 대한 스토리지 리소스를 제공하는 하드웨어입니다. 노드의 드라이브에는 데이터 스토리지 및 데이터 관리를 위한 블록 및 메타데이터 공간이 포함되어 있습니다. 각 노드에는 NetApp Element 소프트웨어의 출하 시 이미지가 포함되어 있습니다. NetApp HCI 스토리지 노드는 NetApp Element 관리 확장 지점을 사용하여 관리할 수 있습니다.

컴퓨팅 노드

NetApp HCI 컴퓨팅 노드는 NetApp HCI 설치에서 가상화에 필요한 CPU, 메모리, 네트워킹 등의 컴퓨팅 리소스를 제공하는 하드웨어입니다. 각 서버에서 VMware ESXi를 실행하기 때문에 vSphere의 호스트 및 클러스터 메뉴 내의 플러그인 외부에서 NetApp HCI 컴퓨팅 노드 관리(호스트 추가 또는 제거)를 수행해야 합니다. 4노드 스토리지 클러스터인지 2노드 스토리지 클러스터인지에 관계없이 NetApp HCI 구축에서는 최소 컴퓨팅 노드 수가 2개입니다.

증명선 노드

NetApp HCI Witness Node는 Element 소프트웨어 기반 스토리지 클러스터와 병렬로 컴퓨팅 노드에서 실행되는 VM입니다. 감시 노드는 슬라이스 또는 블록 서비스를 호스팅하지 않습니다. Witness Node를 사용하면 스토리지 노드 장애 시 스토리지 클러스터를 사용할 수 있습니다. Witness 노드를 다른 스토리지 노드와 같은 방식으로 관리 및 업그레이드할 수 있습니다. 스토리지 클러스터는 최대 4개의 Witness 노드를 포함할 수 있습니다. 이들의 주된 목적은 유효한 앙상블 쿼럼을 형성하기에 충분한 클러스터 노드가 있는지 확인하는 것입니다.

- 모범 사례: * Witness Node VM을 구성하여 컴퓨팅 노드의 로컬 데이터 저장소(NDE에 의해 기본 설정)를 사용하고, SolidFire 스토리지 볼륨과 같은 공유 스토리지에서는 이를 구성하지 마십시오. VM이 자동으로 마이그레이션되지 않도록 하려면 Witness Node VM의 DRS(Distributed Resource Scheduler) 자동화 수준을 * Disabled * 로 설정합니다. 이렇게 하면 Witness Node가 동일한 컴퓨팅 노드에서 실행되고 HA(Non-High Availability) 쌍 구성이 발생하지 않습니다.

및 에 대해 자세히 "증인 노드 리소스 요구 사항""감시 노드 IP 주소 요구 사항"알아보십시오.

2노드 스토리지 클러스터에서는 Witness 노드 장애가 발생할 경우 이중화를 위해 최소 2개의 Witness 노드가 구축됩니다. NetApp HCI 설치 프로세스에서 Witness 노드를 설치하면 VMware vCenter에 VM 템플릿이 저장되며, Witness 노드가 실수로 제거, 손실 또는 손상된 경우 이를 다시 배포하는 데 사용할 수 있습니다. Witness Node를 호스팅하던 장애가 발생한 컴퓨팅 노드를 교체해야 하는 경우 이 템플릿을 사용하여 Witness Node를 재구축할 수도 있습니다. 자세한 내용은 2노드 및 3노드 스토리지 클러스터에 대한 * 재배포 Witness Node * 섹션을 "여기"참조하십시오.

자세한 내용을 확인하십시오

- "NetApp HCI 2노드 스토리지 클러스터 | TR-4823"
- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 설명서 센터"

스토리지

유지보수 모드

소프트웨어 업그레이드 또는 호스트 복구 같이 유지보수를 위해 스토리지 노드를 오프라인 상태로 전환해야 하는 경우, 해당 노드에 대한 유지보수 모드를 지원하여 스토리지 클러스터의 나머지 부분에 대한 I/O 영향을 최소화할 수 있습니다. 유지보수 모드는 어플라이언스 노드와 SolidFire 엔터프라이즈 SDS 노드 모두에서 사용할 수 있습니다.

노드가 정상 상태(차단 클러스터 장애가 없음)이고 스토리지 클러스터가 단일 노드 장애를 허용하지 않는 경우에만 스토리지 노드를 유지보수 모드로 전환할 수 있습니다. 정상 및 허용 노드에 대해 유지보수 모드를 활성화하면 노드가 즉시 전환되지 않고 다음 조건이 충족될 때까지 노드가 모니터링됩니다.

- 노드에서 호스팅되는 모든 볼륨이 페일오버되었습니다
- 노드가 더 이상 모든 볼륨의 운영 노드로 호스팅되지 않습니다
- 페일오버되는 모든 볼륨에 임시 대기 노드가 할당됩니다

이러한 기준이 충족되면 노드는 유지보수 모드로 전환됩니다. 5분 이내에 이러한 조건이 충족되지 않으면 노드가 유지보수 모드로 전환되지 않습니다.

스토리지 노드에 대해 유지보수 모드를 해제하면 다음 조건이 충족될 때까지 노드가 모니터링됩니다.

- 모든 데이터가 노드에 완전히 복제됩니다
- 모든 차단 클러스터 장애가 해결되었습니다

- 노드에서 호스팅되는 볼륨에 대한 모든 임시 대기 노드 할당이 활성화되지 않았습니다

이러한 기준이 충족되면 노드는 유지보수 모드에서 전환됩니다. 1시간 이내에 이러한 조건이 충족되지 않으면 노드가 유지보수 모드에서 전환되지 않습니다.

Element API를 사용하여 유지보수 모드로 작업할 때 유지보수 모드 작업의 상태를 확인할 수 있습니다.

- * 비활성화됨 *: 요청된 유지보수가 없습니다.
- **FailedToRecover**: 노드가 유지 관리에서 복구되지 못했습니다.
- * RecoveringFromMaintenance *: 노드가 유지 관리에서 복구 중입니다.
- * PreparingForMaintenance *: 노드가 유지 관리를 수행할 수 있도록 조치를 취하는 중입니다.
- **ReadyForMaintenance**: 노드를 유지 관리할 준비가 되었습니다.

자세한 내용을 확인하십시오

- "SolidFire 및 Element 문서 센터"

볼륨

스토리지는 NetApp Element 시스템에서 볼륨으로 프로비저닝됩니다. 볼륨은 iSCSI 또는 Fibre Channel 클라이언트를 사용하여 네트워크를 통해 액세스하는 블록 디바이스입니다.

vCenter Server용 NetApp Element 플러그인을 사용하면 사용자 계정의 볼륨을 백업 또는 복원합니다. 또한 클러스터의 각 볼륨을 관리하고 볼륨 액세스 그룹에서 볼륨을 추가 또는 제거할 수 있습니다.

영구 볼륨

영구 볼륨을 사용하면 관리 노드 구성 데이터를 VM이 로컬로 저장되지 않고 지정된 스토리지 클러스터에 저장할 수 있으므로 관리 노드가 손실되거나 제거된 경우에도 데이터를 보존할 수 있습니다. 영구 볼륨은 선택 사항이지만 권장되는 관리 노드 구성입니다.

NetApp 배포 엔진을 사용하여 NetApp HCI용 관리 노드를 구축하는 경우 영구 볼륨이 자동으로 설정 및 구성됩니다.

새 관리 노드를 구축할 때 설치 및 업그레이드 스크립트에는 영구 볼륨을 사용하도록 설정하는 옵션이 포함되어 있습니다. 영구 볼륨은 VM 수명 기간 이후에도 지속된 호스트 관리 노드 VM에 대한 관리 노드 구성 정보가 포함된 Element 소프트웨어 기반 스토리지 클러스터의 볼륨입니다. 관리 노드가 손실된 경우 대체 관리 노드 VM이 손실된 VM에 다시 연결하여 구성 데이터를 복구할 수 있습니다.

설치 또는 업그레이드 중에 활성화된 영구 볼륨 기능은 할당된 클러스터의 이름에 NetApp-HCI 사전 할당 기능을 사용하여 여러 볼륨을 자동으로 생성합니다. 이러한 볼륨은 Element 소프트웨어 기반 볼륨과 마찬가지로 기본 설정 및 설치에 따라 Element 소프트웨어 웹 UI, vCenter Server용 NetApp Element 플러그인 또는 API를 사용하여 볼 수 있습니다. 복구에 사용할 수 있는 현재 구성 데이터를 유지하려면 관리 노드에 대한 iSCSI 연결을 통해 영구 볼륨이 가동되어 실행 중이어야 합니다.

설치 또는 업그레이드 중에 관리 서비스와 연결된 영구 볼륨이 생성되고 새 계정에 할당됩니다. 영구 볼륨을 사용하는 경우 볼륨이나 연결된 계정을 수정하거나 삭제하지 마십시오

자세한 내용을 확인하십시오

- "볼륨 관리"
- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 설명서 센터"

볼륨 액세스 그룹

볼륨 액세스 그룹은 사용자가 iSCSI 또는 파이버 채널 이니시에이터를 사용하여 액세스할 수 있는 볼륨의 모음입니다.

볼륨 액세스 그룹을 생성 및 사용하면 볼륨 세트에 대한 액세스를 제어할 수 있습니다. 볼륨 집합 및 이니시에이터 집합을 볼륨 액세스 그룹에 연결하면 액세스 그룹은 해당 이니시에이터 액세스 권한을 해당 볼륨 집합에 부여합니다.

볼륨 액세스 그룹은 다음과 같은 제한 사항이 있습니다.

- 볼륨 액세스 그룹당 최대 128개의 이니시에이터
- 볼륨당 최대 64개의 액세스 그룹
- 액세스 그룹은 최대 2000개의 볼륨으로 구성할 수 있습니다.
- IQN 또는 WWPN은 하나의 볼륨 액세스 그룹에만 속할 수 있습니다.

자세한 내용을 확인하십시오

- "볼륨 액세스 그룹을 관리합니다"
- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 설명서 센터"

이니시에이터

이니시에이터는 외부 클라이언트가 클러스터의 볼륨에 액세스할 수 있도록 하며, 클라이언트와 볼륨 간의 통신을 위한 진입점 역할을 합니다. 스토리지 볼륨에 대한 계정 기반 액세스 대신 CHAP 기반 액세스에 이니시에이터를 사용할 수 있습니다. 볼륨 액세스 그룹에 추가된 단일 이니시에이터는 볼륨 액세스 그룹 구성원이 인증을 요구하지 않고 그룹에 추가된 모든 스토리지 볼륨에 액세스할 수 있도록 합니다. 이니시에이터는 하나의 액세스 그룹에만 속할 수 있습니다.

자세한 내용을 확인하십시오

- "이니시에이터를 관리합니다"
- "볼륨 액세스 그룹"
- "볼륨 액세스 그룹을 관리합니다"
- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 설명서 센터"

NetApp HCI 라이센스

NetApp HCI를 사용하는 경우 사용 중인 항목에 따라 추가 라이센스가 필요할 수 있습니다.

NetApp HCI 및 VMware vSphere 라이센스

VMware vSphere 라이센스는 구성에 따라 다릅니다.

네트워킹 옵션	라이센싱
옵션 A: VLAN 태그 지정을 사용하는 컴퓨팅 노드용 케이블 2개(모든 컴퓨팅 노드)	VMware vSphere Enterprise Plus 라이센스가 필요한 vSphere Distributed Switch를 사용해야 합니다.
옵션 B: 태그가 지정된 VLAN을 사용하는 컴퓨팅 노드용 케이블 6개(H410C 2RU 4노드 컴퓨팅 노드)	이 구성에서는 vSphere Standard Switch가 기본값으로 사용됩니다. vSphere Distributed Switch를 선택적으로 사용하려면 VMware Enterprise Plus 라이센스가 필요합니다.
옵션 C: 네이티브 및 태그가 지정된 VLAN을 사용하는 컴퓨팅 노드용 케이블 6개(H410C, 2RU 4노드 컴퓨팅 노드)	이 구성에서는 vSphere Standard Switch가 기본값으로 사용됩니다. vSphere Distributed Switch를 선택적으로 사용하려면 VMware Enterprise Plus 라이센스가 필요합니다.

NetApp HCI 및 ONTAP Select 라이센스

구입한 NetApp HCI 시스템과 함께 사용하기 위해 ONTAP Select 버전을 제공받은 경우 다음과 같은 추가 제한 사항이 적용됩니다.

- NetApp HCI 시스템 판매와 함께 제공되는 ONTAP Select 라이센스는 NetApp HCI 컴퓨팅 노드와 함께 사용해서만 사용할 수 있습니다.
- 이러한 ONTAP Select 인스턴스의 스토리지는 NetApp HCI 스토리지 노드에만 상주해야 합니다.
- 타사 컴퓨팅 노드 또는 타사 스토리지 노드를 사용하는 것은 금지됩니다.

자세한 내용을 확인하십시오

- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 설명서 센터"

NetApp 하이브리드 클라우드 제어 구성 최대 한도

NetApp HCI에 포함된 NetApp 하이브리드 클라우드 제어기를 사용하면 컴퓨팅 라이프사이클과 스토리지 관리를 간소화할 수 있습니다. NetApp HCI 및 NetApp SolidFire 스토리지 클러스터의 스토리지 노드에 대한 Element 소프트웨어 업그레이드뿐만 아니라 NetApp HCI의 NetApp HCI 컴퓨팅 노드에 대한 펌웨어 업그레이드를 지원합니다. 이 기능은 NetApp HCI의 관리 노드에서 기본적으로 사용할 수 있습니다.

NetApp 하이브리드 클라우드 제어는 NetApp HCI 설치에서 NetApp이 제공한 하드웨어 및 소프트웨어 구성요소를 커뮤니케이션할 뿐만 아니라 VMware vCenter와 같은 고객 환경에서 타사 구성요소와 상호 작용합니다. NetApp에서는 NetApp 하이브리드 클라우드 컨트롤의 기능과 고객 환경에서 특정 규모까지 이러한 타사 구성 요소와의 상호 작용에 대해 설명합니다. NetApp 하이브리드 클라우드 제어를 최적의 상태로 유지하려면 최대 구성 범위 내에서 유지하는 것이 좋습니다.

이 테스트된 최대값을 초과하면 느린 사용자 인터페이스 및 API 응답 또는 기능을 사용할 수 없는 것과 같은 NetApp 하이브리드 클라우드 제어와 관련된 문제가 발생할 수 있습니다. 구성 최대값을 초과하여 구성된 환경에서 NetApp 하이브리드 클라우드 제어를 통해 제품 지원을 위해 NetApp에 문의할 경우, NetApp Support에서 구성 내용을 최대 문서로 변경할지 묻습니다.

구성 최대

NetApp 하이브리드 클라우드 제어는 최대 100개의 ESXi 호스트와 1,000개의 가상 머신을 지원하는 VMware vSphere 환경을 지원합니다(소규모 vCenter Server Appliance 구성과 유사).

NetApp HCI 보안

NetApp HCI를 사용하면 업계 표준 보안 프로토콜을 통해 데이터가 보호됩니다.

스토리지 노드의 유휴 데이터 암호화

NetApp HCI를 사용하면 스토리지 클러스터에 저장된 모든 데이터를 암호화할 수 있습니다.

스토리지 노드의 모든 드라이브에서 암호화 가능한 AES 256비트 암호화를 드라이브 레벨에서 사용합니다. 각 드라이브에는 드라이브가 처음 초기화될 때 생성되는 자체 암호화 키가 있습니다. 암호화 기능을 설정하면 스토리지 클러스터 전체의 암호가 생성되고 암호 청크가 클러스터의 모든 노드로 배포됩니다. 전체 암호를 저장하는 단일 노드는 없습니다. 그런 다음 암호를 사용하여 드라이브에 대한 모든 액세스를 암호로 보호합니다. 드라이브의 잠금을 해제하려면 암호가 필요합니다. 드라이브에서 모든 데이터를 암호화하므로 항상 데이터가 안전하게 보호됩니다.

저장된 데이터 암호화를 설정하면 스토리지 클러스터의 성능과 효율성이 영향을 받지 않습니다. 또한 Element API 또는 Element UI를 사용하여 스토리지 클러스터에서 암호화가 활성화된 드라이브 또는 노드를 제거하면 드라이브에서 저장된 암호화가 비활성화되고 드라이브는 안전하게 지워지고 이전에 해당 드라이브에 저장된 데이터가 보호됩니다. 드라이브를 제거한 후 API 방법으로 드라이브를 안전하게 지울 수 `SecureEraseDrives` 있습니다. 스토리지 클러스터에서 드라이브 또는 노드를 강제로 제거하면 데이터가 클러스터 전체 암호와 드라이브의 개별 암호화 키에 의해 보호됩니다.

저장 시 암호화 활성화 및 비활성화에 대한 자세한 내용은 SolidFire 및 요소 문서 센터 를 참조하십시오 "클러스터에 대한 암호화 설정 및 해제".

저장된 소프트웨어 암호화

저장 시 소프트웨어 암호화를 사용하면 스토리지 클러스터의 SSD에 기록된 모든 데이터를 암호화할 수 있습니다. SED(자체 암호화 드라이브)가 포함되지 않은 SolidFire 엔터프라이즈 SDS 노드에서 기본 암호화 계층을 제공합니다.

외부 키 관리

타사 KMIP 호환 키 관리 서비스(KMS)를 사용하여 스토리지 클러스터 암호화 키를 관리하도록 Element 소프트웨어를 구성할 수 있습니다. 이 기능을 활성화하면 스토리지 클러스터의 클러스터 전체 드라이브 액세스 암호 암호화 키가 사용자가 지정한 KMS에 의해 관리됩니다. 요소는 다음과 같은 주요 관리 서비스를 사용할 수 있습니다.

- Gemalto SafeNet KeySecure를 참조하십시오

- SafeNet AT KeySecure
- HyTrust 키컨트롤
- Vormetric Data Security Manager를 참조하십시오
- IBM Security Key Lifecycle Manager를 참조하십시오

외부 키 관리 구성에 대한 자세한 내용은 SolidFire 및 요소 문서 센터의 을 참조하십시오 "외부 키 관리 시작".

다중 요소 인증

다중 요소 인증(MFA)을 사용하면 사용자가 로그인할 때 NetApp Element 웹 UI 또는 스토리지 노드 UI를 사용하여 인증하기 위해 여러 유형의 증거를 제시하도록 할 수 있습니다. 기존 사용자 관리 시스템 및 ID 공급자와 통합되는 로그인에 대해 다중 요소 인증만 허용하도록 Element를 구성할 수 있습니다. 기존 SAML 2.0 ID 공급자와 통합되도록 Element를 구성할 수 있습니다. 이 공급자는 암호 및 텍스트 메시지, 암호 및 전자 메일 메시지 또는 기타 방법과 같은 여러 인증 체계를 적용할 수 있습니다.

다중 요소 인증을 ADFS(Microsoft Active Directory Federation Services) 및 Shibboleth와 같은 일반적인 SAML 2.0 호환 ID 공급자(IdP)와 페어링할 수 있습니다.

MFA를 구성하려면 SolidFire 및 요소 문서 센터의 를 "다중 요소 인증 활성화" 참조하십시오.

FIPS 140-2 - HTTPS 및 유휴 데이터 암호화를 지원합니다

NetApp SolidFire 스토리지 클러스터와 NetApp HCI 시스템은 암호화 모듈에 대한 FIPS(Federal Information Processing Standard) 140-2 요구사항을 준수하는 암호화를 지원합니다. SolidFire 또는 NetApp HCI 클러스터에서 FIPS 140-2 규정 준수를 활성화하여 HTTPS 통신과 드라이브 암호화를 모두 구현할 수 있습니다.

클러스터에서 FIPS 140-2 운영 모드를 활성화하면 클러스터는 NetApp CSM(Cryptographic Security Module)을 활성화하고 HTTPS를 통해 NetApp Element UI 및 API에 연결되는 모든 통신에 FIPS 140-2 Level 1 인증 암호화를 사용합니다. `EnableFeature`Element API를 매개 변수와 함께 `fips` 사용하여 FIPS 140-2 HTTPS 암호화를 활성화할 수 있습니다. FIPS 호환 하드웨어가 포함된 스토리지 클러스터에서 매개 변수가 포함된 Element API를 `FipsDrives` 사용하여 유휴 데이터에 대해 FIPS 드라이브 암호화를 활성화할 수도 `EnableFeature` 있습니다.

FIPS 140-2 암호화를 위한 새 스토리지 클러스터를 준비하는 방법에 대한 자세한 내용은 을 참조하십시오. "FIPS 드라이브를 지원하는 클러스터 생성"

기존 준비된 클러스터에서 FIPS 140-2를 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오. "EnableFeature 요소 API입니다"

성능 및 서비스 품질

SolidFire 스토리지 클러스터에는 볼륨 기준에 따라 서비스 품질(QoS) 매개 변수를 제공할 수 있는 기능이 있습니다. QoS를 정의하는 세 가지 구성 가능한 매개 변수(최소 IOPS, 최대 IOPS 및 버스트 IOPS)를 사용하여 초당 입력 및 출력(IOPS)으로 측정한 클러스터 성능을 보장할 수 있습니다.

SolidFire Active IQ에는 QoS 설정 및 최적의 구성에 대한 조언을 제공하는 QoS 권장 사항 페이지가 있습니다.

서비스 품질 매개 변수

IOPS 매개 변수는 다음과 같은 방법으로 정의됩니다.

- * 최소 IOPS * - 스토리지 클러스터가 볼륨에 제공하는 최소 유지 IOPS(초당 입출력) 수입니다. 볼륨에 대해 구성된 최소 IOPS는 볼륨의 보장된 성능 수준입니다. 성능이 이 수준 아래로 떨어지지 않습니다.
- * 최대 IOPS * - 스토리지 클러스터가 볼륨에 제공하는 최대 지속 IOPS 수입니다. 클러스터 IOPS 레벨이 매우 높을 경우 이 IOPS 성능 레벨이 초과하지 않습니다.
- * 버스트 IOPS * - 짧은 버스트 시나리오에서 허용되는 최대 IOPS 수입니다. 볼륨이 최대 IOPS 미만으로 실행 중인 경우 버스트 크레딧이 누적됩니다. 성능 수준이 매우 높고 최대 수준으로 푸시되면 볼륨에 대해 짧은 IOPS 버스트가 허용됩니다.

  Element 소프트웨어는 클러스터가 낮은 클러스터 IOPS 사용률로 실행 중일 때 버스트 IOPS를 사용합니다.

  단일 볼륨에서 버스트 IOPS를 적립하고 크레딧을 사용하여 설정된 "버스트 기간" 동안 최대 IOPS 수준까지 버스트 IOPS를 초과하여 버스트할 수 있습니다. 클러스터에 최대 60초 동안 연속 데이터 증가를 수용할 수 있는 용량이 있는 경우 볼륨이 폭발할 수 있습니다. 볼륨은 최대 IOPS 한도 미만으로 실행되는 초당 1초의 버스트 크레딧(최대 60초)을 누적합니다.

  버스트 IOPS는 두 가지 방법으로 제한됩니다.

  - 볼륨은 볼륨이 누적된 버스트 크레딧 수와 동일한 몇 초 동안 최대 IOPS 이상으로 급증할 수 있습니다.
  - 볼륨이 최대 IOPS 설정 이상으로 급증하면 버스트 IOPS 설정에 의해 제한됩니다. 따라서 버스트 IOPS는 볼륨에 대한 버스트 IOPS 설정을 초과하지 않는다.
- * 유효 최대 대역폭 * - 최대 대역폭은 IOPS 수(QoS 곡선 기준)에 IO 크기를 곱하여 계산합니다.

  예: 100분 IOPS, 1000 Max IOPS, 1500 Burst IOP의 QoS 매개 변수 설정은 성능 품질에 다음과 같은 영향을 미칩니다.

  - 클러스터에서 IOPS에 대한 워크로드 경합이 뚜렷해질 때까지 워크로드가 최대 1000 IOPS에 도달하고 이를 유지할 수 있습니다. 그런 다음 모든 볼륨의 IOPS가 지정된 QoS 범위 내에 있고 성능 경합이 완화될 때까지 IOPS가 점진적으로 감소합니다.
  - 모든 볼륨의 성능은 최소 IOPS 100으로 푸시됩니다. 레벨은 최소 IOPS 설정 아래로 떨어지지 않지만 워크로드 경합이 완화될 때 100 IOPS를 초과할 수 있습니다.
  - 성능이 1000 IOPS를 넘지 않거나 유지 기간 동안 100 IOPS를 넘지 않습니다. 1500 IOPS(버스트 IOPS)의 성능은 허용되지만, 최대 IOPS 미만으로 실행하여 버스트 크레딧을 계산한 볼륨에 대해서만 짧은 시간 동안만 허용됩니다. 버스트 레벨은 절대 지속되지 않습니다.

QoS 값 제한

다음은 QoS에 대해 가능한 최소 및 최대 값입니다.

매개 변수	최소 값	기본값	**4 4KB**	**5 8KB**	**6 16KB**	**262KB**
최소 IOPS	50	50	15,000	9,375 *	5556 *	385 *
최대 IOPS	100	15,000	200,000**	125,000	74,074)를 참조하십시오	5128을 참조하십시오
버스트 IOPS	100	15,000	200,000**	125,000	74.074를 참조하십시오	5128을 참조하십시오

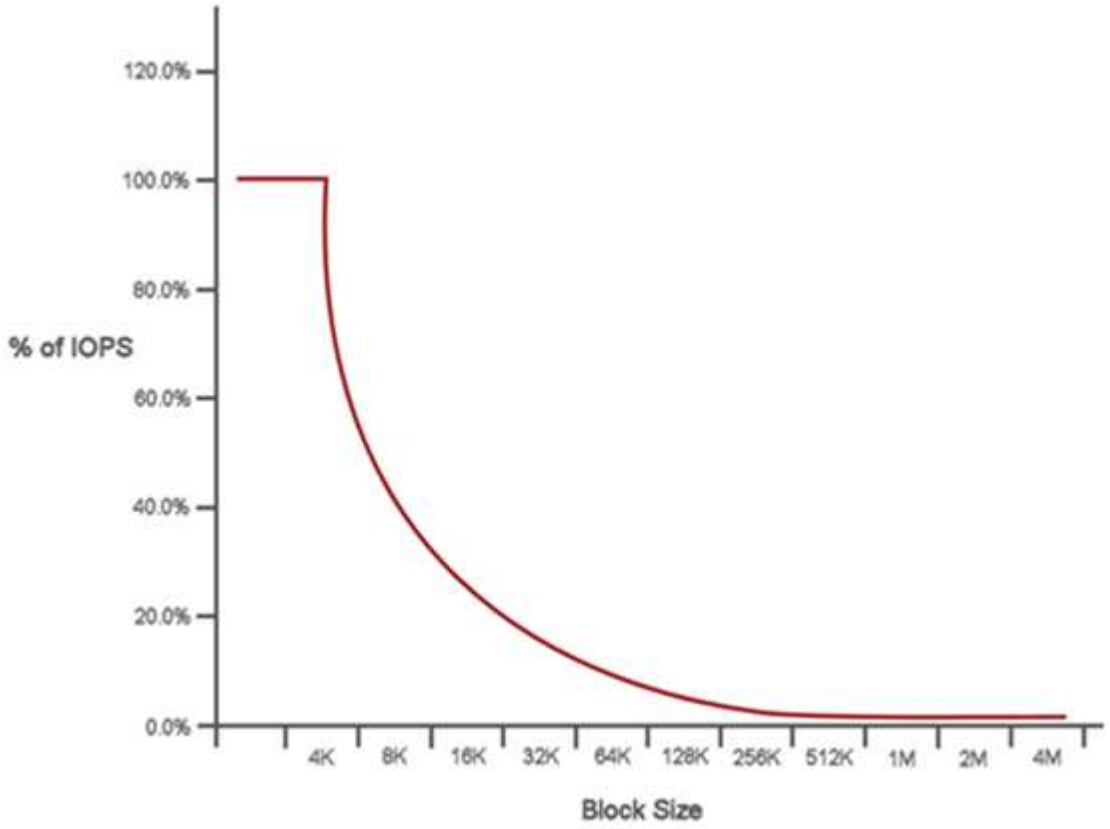
이러한 예측은 근사치입니다**.** * 최대 IOPS 및 버스트 IOPS는 200,000까지 설정할 수 있지만 이 설정은 볼륨의 성능을 효과적으로 해제할 수만 있습니다. 실제 볼륨 최대 성능은 클러스터 사용 및 노드당 성능에 의해 제한됩니다.

QoS 성능

QoS 성능 곡선은 블록 크기와 IOPS 백분율 간의 관계를 보여줍니다.

블록 크기 및 대역폭은 애플리케이션이 얻을 수 있는 IOPS 수에 직접적인 영향을 미칩니다. Element 소프트웨어는 블록 크기를 4K로 정규화하여 수신하는 블록 크기를 고려합니다. 워크로드에 따라 시스템에서 블록 크기를 늘릴 수 있습니다. 블록 크기가 증가함에 따라 시스템에서 더 큰 블록 크기를 처리하는 데 필요한 수준까지 대역폭을 높일 수 있습니다. 대역폭이 증가할수록 시스템에서 달성할 수 있는 IOPS가 감소합니다.

QoS 성능 곡선은 블록 크기 증가와 IOPS 백분율 간의 관계를 보여줍니다.



예를 들어, 블록 크기가 4K이고 대역폭이 4,000kbps인 경우 IOPS는 1000입니다. 블록 크기가 8K로 증가할 경우 대역폭이 5,000kbps로 증가하고 IOPS는 625로 감소합니다. 블록 크기를 고려하여 시스템은 백업 및 하이퍼바이저 작업과 같이 더 높은 블록 크기를 사용하는 낮은 우선 순위 워크로드가 더 작은 블록 크기를 사용하는 높은 우선 순위 트래픽에 필요한 성능을 너무 많이 사용하지 않도록 보장합니다.

QoS 정책

QoS 정책을 사용하면 여러 볼륨에 적용할 수 있는 표준화된 서비스 품질 설정을 생성하여 저장할 수 있습니다.

QoS 정책은 예를 들어, 거의 재부팅되지 않고 동일한 스토리지 액세스가 필요한 데이터베이스, 애플리케이션 또는 인프라 서버와 같은 서비스 환경에 가장 적합합니다. 개별 볼륨 QoS는 가상 데스크톱 또는 특수 키오스크 유형의 VM과 같이 매일 또는 하루에 여러 번 재부팅, 전원 켜기 또는 전원 끄기와 같은 경량 VM에 가장 적합합니다.

QoS 및 QoS 정책을 함께 사용해서는 안 됩니다. QoS 정책을 사용하는 경우 볼륨에 대해 사용자 지정 QoS를 사용하지 마십시오. 사용자 지정 QoS는 볼륨 QoS 설정에 대한 QoS 정책 값을 재정의하고 조정합니다.

QoS 정책을 사용하려면 선택한 클러스터가 Element 10.0 이상이어야 합니다. 그렇지 않으면 QoS 정책 기능을 사용할 수 없습니다.

자세한 내용을 확인하십시오

- "vCenter Server용 NetApp Element 플러그인"
- "NetApp HCI 리소스 페이지를 참조하십시오"