개념
Element Software

NetApp
November 18, 2025

목차

개념

Element 소프트웨어와 관련된 기본 개념을 알아보세요.

- "제품 개요"
- SolidFire 아키텍처 개요
- 노드
- 클러스터
- "보안"
- 계정 및 권한
- "볼륨"
- 데이터 보호
- 성능 및 서비스 품질

제품 개요

SolidFire 올플래시 스토리지 시스템은 단일 스토리지 리소스 풀로 결합된 개별 하드웨어 구성 요소(드라이브 및 노드)로 구성됩니다. 이 통합 클러스터는 외부 클라이언트가 사용할 수 있는 단일 스토리지 시스템으로 제공되며 NetApp Element 소프트웨어로 관리됩니다.

Element 인터페이스, API 또는 기타 관리 도구를 사용하면 SolidFire 클러스터 스토리지 용량과 성능을 모니터링하고, 멀티 테넌트 인프라 전반의 스토리지 활동을 관리할 수 있습니다.

SolidFire 기능

Solidfire 시스템은 다음과 같은 기능을 제공합니다.

- 대규모 프라이빗 클라우드 인프라를 위한 고성능 스토리지를 제공합니다.
- 변화하는 스토리지 요구 사항을 충족할 수 있는 유연한 확장성을 제공합니다.
- API 기반 스토리지 관리 Element 소프트웨어 인터페이스를 사용합니다.
- 서비스 품질 정책을 사용하여 성능을 보장합니다.
- 클러스터의 모든 노드에 걸쳐 자동 부하 분산이 포함됩니다.
- 노드가 추가되거나 제거되면 클러스터를 자동으로 재조정합니다.

SolidFire 배포

NetApp 에서 제공하고 NetApp Element 소프트웨어와 통합된 스토리지 노드를 사용합니다.

"SolidFire 올플래시 스토리지 아키텍처 개요"

더 많은 정보를 찾아보세요

- "vCenter Server용 NetApp Element 플러그인"

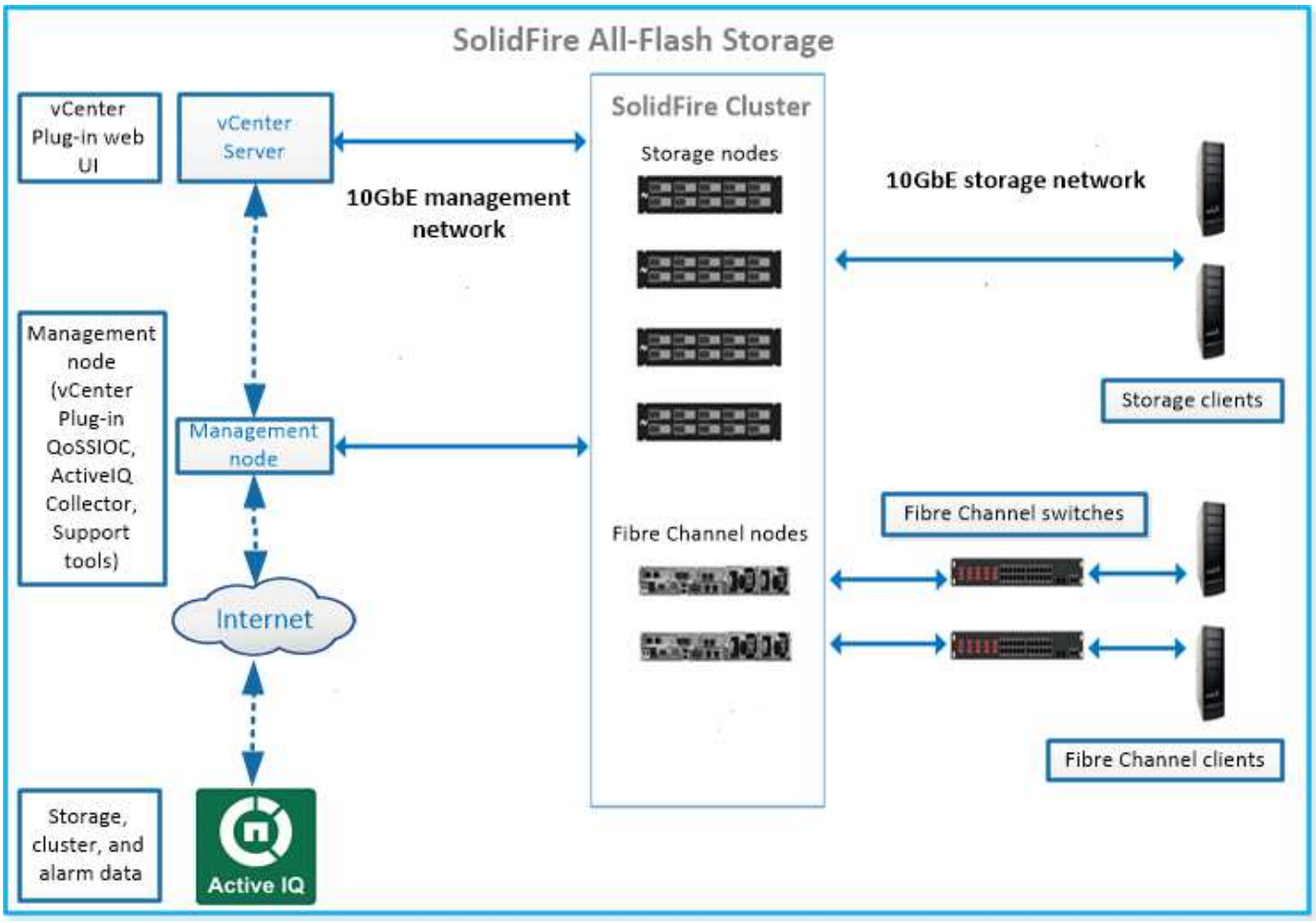
아키텍처 및 구성 요소

SolidFire 아키텍처에 대해 알아보세요

SolidFire 올플래시 스토리지 시스템은 드라이브와 노드라는 개별 하드웨어 구성 요소로 이루어져 있으며, 이러한 구성 요소는 스토리지 리소스 풀로 결합되고 각 노드에서 NetApp Element 소프트웨어가 독립적으로 실행됩니다. 이 단일 스토리지 시스템은 Element 소프트웨어 UI, API 및 기타 관리 도구를 사용하여 단일 엔터티로 관리됩니다.

SolidFire 스토리지 시스템에는 다음과 같은 하드웨어 구성 요소가 포함됩니다.

- 클러스터: 노드의 집합인 SolidFire 스토리지 시스템의 허브입니다.
- 노드: 클러스터로 그룹화된 하드웨어 구성 요소입니다. 노드에는 두 가지 유형이 있습니다.
  - 드라이브 컬렉션을 포함하는 서버인 스토리지 노드
  - FC 클라이언트에 연결하는 데 사용하는 FC(Fibre Channel) 노드
- 드라이브: 클러스터의 데이터를 저장하기 위해 스토리지 노드에서 사용됩니다. 저장 노드에는 두 가지 유형의 드라이브가 포함됩니다.
  - 볼륨 메타데이터 드라이브는 클러스터 내의 볼륨 및 기타 객체를 정의하는 정보를 저장합니다.
  - 블록 드라이브는 볼륨의 데이터 블록을 저장합니다.



Element 웹 UI 및 기타 호환 도구를 사용하여 시스템을 관리, 모니터링 및 업데이트할 수 있습니다.

- "SolidFire 소프트웨어 인터페이스"
- "SolidFire Active IQ"
- "Element 소프트웨어 관리 노드"
- "관리 서비스"

일반 URL

SolidFire 올플래시 스토리지 시스템에서 일반적으로 사용되는 URL은 다음과 같습니다.

URL	설명
`https://[storage cluster MVIP address]`	NetApp Element 소프트웨어 UI에 액세스합니다.
`https://activeiq.solidfire.com`	데이터를 모니터링하고 성능 병목 현상이나 잠재적인 시스템 문제에 대한 알림을 받습니다.
`https://[management node IP address]`	NetApp Hybrid Cloud Control에 액세스하여 스토리지 설치를 업그레이드하고 관리 서비스를 업데이트하세요.
`https://[IP address]:442`	노드별 UI에서 네트워크 및 클러스터 설정에 액세스하고 시스템 테스트와 유틸리티를 활용합니다."자세히 알아보세요."

URL	설명
`https://[management node IP address]/mnode`	관리 노드에서 관리 서비스 REST API 및 기타 기능을 사용합니다."자세히 알아보세요."
`https://[management node IP address]:9443`	vSphere Web Client에서 vCenter 플러그인 패키지를 등록합니다."자세히 알아보세요."

더 많은 정보를 찾아보세요

- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

SolidFire 소프트웨어 인터페이스

다양한 NetApp Element 소프트웨어 인터페이스와 통합 유틸리티를 사용하여 SolidFire 스토리지 시스템을 관리할 수 있습니다.

옵션

- NetApp Element 소프트웨어 사용자 인터페이스
- NetApp Element 소프트웨어 API
- vCenter Server용 NetApp Element 플러그인
- NetApp 하이브리드 클라우드 제어
- 관리 노드 UI
- 추가 통합 유틸리티 및 도구

NetApp Element 소프트웨어 사용자 인터페이스

Element 스토리지를 설정하고, 클러스터 용량과 성능을 모니터링하고, 멀티 테넌트 인프라 전반에서 스토리지 활동을 관리할 수 있습니다. Element는 SolidFire 클러스터의 핵심인 스토리지 운영 체제입니다. Element 소프트웨어는 클러스터의 모든 노드에서 독립적으로 실행되며, 클러스터 노드가 외부 클라이언트에 단일 스토리지 시스템으로 제공되는 리소스를 결합할 수 있도록 합니다. Element 소프트웨어는 시스템 전체의 모든 클러스터 조정, 규모 및 관리를 담당합니다. 소프트웨어 인터페이스는 Element API를 기반으로 구축되었습니다.

"Element 소프트웨어로 스토리지 관리"

NetApp Element 소프트웨어 API

객체, 메서드, 루틴 세트를 사용하여 Element 저장소를 관리할 수 있습니다. Element API는 HTTPS를 통한 JSON-RPC 프로토콜을 기반으로 합니다. API 로그를 활성화하면 Element UI에서 API 작업을 모니터링할 수 있습니다. 이를 통해 시스템에 발행된 메서드를 볼 수 있습니다. 요청과 응답을 모두 활성화하면 발행된 메서드에 시스템이 어떻게 응답하는지 확인할 수 있습니다.

"Element API로 저장소 관리"

vCenter Server용 NetApp Element 플러그인

VMware vSphere 내의 Element UI에 대한 대체 인터페이스를 사용하여 Element 소프트웨어를 실행하는 스토리지

클러스터를 구성하고 관리할 수 있습니다.

"vCenter Server용 NetApp Element 플러그인"

NetApp 하이브리드 클라우드 제어

NetApp Hybrid Cloud Control 인터페이스를 사용하여 Element 스토리지 및 관리 서비스를 업그레이드하고 스토리지 자산을 관리할 수 있습니다.

"NetApp Hybrid Cloud Control을 사용하여 스토리지를 관리하고 모니터링하세요"

관리 노드 UI

관리 노드에는 두 개의 UI가 포함되어 있습니다. REST 기반 서비스를 관리하는 UI와 네트워크 및 클러스터 설정, 운영 체제 테스트 및 유틸리티를 관리하는 노드별 UI입니다. REST API UI에서 관리 노드의 서비스 기반 시스템 기능을 제어하는 서비스 관련 API 메뉴에 액세스할 수 있습니다.

추가 통합 유틸리티 및 도구

일반적으로 NetApp Element, NetApp Element API 및 vCenter Server용 NetApp Element 플러그인을 사용하여 스토리지를 관리하지만 추가 통합 유틸리티와 도구를 사용하여 스토리지에 액세스할 수 있습니다.

요소 CLI

"요소 CLI"Element API를 사용하지 않고도 명령줄 인터페이스를 사용하여 SolidFire 스토리지 시스템을 제어할 수 있습니다.

Element PowerShell 도구

"Element PowerShell 도구"Element API를 사용하여 SolidFire 스토리지 시스템을 관리하는 Microsoft Windows PowerShell 함수 모음을 사용할 수 있습니다.

Element SDK

"Element SDK"다음 도구를 사용하여 SolidFire 클러스터를 관리할 수 있습니다.

- Element Java SDK: 프로그래머가 Element API를 Java 프로그래밍 언어와 통합할 수 있도록 합니다.
- Element .NET SDK: 프로그래머가 Element API를 .NET 프로그래밍 플랫폼과 통합할 수 있도록 합니다.
- Element Python SDK: 프로그래머가 Element API를 Python 프로그래밍 언어와 통합할 수 있도록 합니다.

SolidFire Postman API 테스트 모음

프로그래머가 컬렉션을 사용할 수 있도록 합니다."우편 집배원" Element API 호출을 테스트하는 함수입니다.

SolidFire 스토리지 복제 어댑터

"SolidFire 스토리지 복제 어댑터"복제된 SolidFire 스토리지 클러스터와 통신하고 지원되는 워크플로를 실행하기 위해 VMware Site Recovery Manager(SRM)와 통합됩니다.

SolidFire vRO

"SolidFire vRO"VMware vRealize Orchestrator를 사용하여 SolidFire 스토리지 시스템을 관리하기 위한 Element API를 사용하는 편리한 방법을 제공합니다.

SolidFire VSS 공급자

"SolidFire VSS 공급자"VSS 섀도 복사본을 Element 스냅샷 및 복제본과 통합합니다.

더 많은 정보를 찾아보세요

- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

SolidFire Active IQ

"SolidFire Active IQ"클러스터 전체 데이터의 지속적으로 업데이트된 과거 보기를 제공하는 웹 기반 도구입니다. 특정 이벤트, 임계값 또는 메트릭에 대한 알림을 설정할 수 있습니다. SolidFire Active IQ 사용하면 시스템 성능과 용량을 모니터링하고 클러스터 상태에 대한 정보를 얻을 수 있습니다.

SolidFire Active IQ 에서 시스템에 대한 다음 정보를 찾을 수 있습니다.

- 노드 수 및 노드 상태: 정상, 오프라인 또는 오류
- CPU, 메모리 사용량 및 노드 제한의 그래픽 표현
- 스토리지 노드에서 실행되는 NetApp Element 소프트웨어의 일련 번호, 섀시 내 슬롯 위치, 모델 및 버전과 같은 노드에 대한 세부 정보
- 가상 머신에 대한 CPU 및 스토리지 관련 정보

SolidFire Active IQ 에 대해 알아보려면 다음을 참조하세요. "SolidFire Active IQ 설명서" .

더 많은 정보를 원하시면

- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"
- **NetApp** 지원 사이트 › **Active IQ** 도구

Element 소프트웨어 관리 노드

그만큼"관리 노드(mNode)" 하나 이상의 Element 소프트웨어 기반 스토리지 클러스터와 병렬로 실행되는 가상 머신입니다. 모니터링 및 원격 측정을 포함한 시스템 서비스를 업그레이드하고 제공하고, 클러스터 자산 및 설정을 관리하고, 시스템 테스트 및 유틸리티를 실행하고, 문제 해결을 위해 NetApp 지원 액세스를 활성화하는 데 사용됩니다.

관리 노드는 스토리지 클러스터와 상호 작용하여 관리 작업을 수행하지만 스토리지 클러스터의 멤버는 아닙니다. 관리 노드는 API 호출을 통해 클러스터에 대한 정보를 주기적으로 수집하고 원격 모니터링을 위해 이 정보를 Active IQ 에 보고합니다(활성화된 경우). 관리 노드는 클러스터 노드의 소프트웨어 업그레이드를 조정하는 역할도 담당합니다.

Element 11.3 릴리스부터 관리 노드는 마이크로서비스 호스트 역할을 하므로 주요 릴리스 외에도 선택한 소프트웨어 서비스를 더 빠르게 업데이트할 수 있습니다. 이러한 마이크로서비스 또는"관리 서비스" 서비스 번들로 자주 업데이트됩니다.

SolidFire 올플래시 스토리지 관리 서비스

Element 11.3 릴리스부터 *관리 서비스*는 다음에서 호스팅됩니다."관리 노드" 이를 통해 주요 릴리스 외에도 선택한 소프트웨어 서비스를 더 빠르게 업데이트할 수 있습니다.

관리 서비스는 SolidFire 올플래시 스토리지에 대한 중앙 집중식 관리 기능과 확장된 관리 기능을 제공합니다. 이러한 서비스에는 다음이 포함됩니다."NetApp 하이브리드 클라우드 제어" , Active IQ 시스템 원격 측정, 로깅 및 서비스 업데이트, 그리고 vCenter용 Element 플러그인을 위한 QoSSIOC 서비스입니다.

자세히 알아보세요"관리 서비스 릴리스" .

노드

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

NetApp Element 소프트웨어는 클러스터에 대한 다양한 노드 역할을 정의합니다. 노드 역할의 유형은 다음과 같습니다.

- 관리 노드
- 저장 노드
- 파이버 채널 노드

노드 상태클러스터 연관성에 따라 다릅니다.

관리 노드

관리 노드는 모니터링 및 원격 측정을 포함한 시스템 서비스를 업그레이드하고 제공하고, 클러스터 자산 및 설정을 관리하고, 시스템 테스트 및 유틸리티를 실행하고, 문제 해결을 위해 NetApp 지원 액세스를 활성화하는 데 사용되는 가상 머신입니다."자세히 알아보기"

저장 노드

SolidFire 스토리지 노드는 Bond10G 네트워크 인터페이스를 통해 서로 통신하는 드라이브 컬렉션을 포함하는 서버입니다. 노드의 드라이브에는 데이터 저장 및 관리를 위한 블록 및 메타데이터 공간이 포함되어 있습니다. 각 노드에는 NetApp Element 소프트웨어의 팩토리 이미지가 포함되어 있습니다.

저장 노드는 다음과 같은 특징을 가지고 있습니다.

- 각 노드에는 고유한 이름이 있습니다. 관리자가 노드 이름을 지정하지 않으면 기본값은 SF-XXXX입니다. 여기서 XXXX는 시스템에서 생성한 4개의 무작위 문자입니다.
- 각 노드에는 자체 고성능 비휘발성 랜덤 액세스 메모리(NVRAM) 쓰기 캐시가 있어 전반적인 시스템 성능을 향상시키고 쓰기 지연 시간을 줄입니다.
- 각 노드는 두 개의 네트워크(저장 및 관리)에 연결되며, 각 네트워크는 중복성과 성능을 위해 두 개의 독립적인 링크를 갖습니다. 각 노드에는 각 네트워크의 IP 주소가 필요합니다.

- 새로운 스토리지 노드로 클러스터를 만들거나 기존 클러스터에 스토리지 노드를 추가하여 스토리지 용량과 성능을 높일 수 있습니다.
- 서비스를 중단하지 않고 언제든지 클러스터에 노드를 추가하거나 제거할 수 있습니다.

파이버 채널 노드

SolidFire 파이버 채널 노드는 파이버 채널 스위치에 대한 연결을 제공하며, 이를 파이버 채널 클라이언트에 연결할 수 있습니다. 파이버 채널 노드는 파이버 채널과 iSCSI 프로토콜 간의 프로토콜 변환기 역할을 합니다. 이를 통해 새 SolidFire 클러스터나 기존 SolidFire 클러스터에 파이버 채널 연결을 추가할 수 있습니다.

파이버 채널 노드는 다음과 같은 특징을 가지고 있습니다.

- 파이버 채널 스위치는 패브릭의 상태를 관리하여 최적화된 상호 연결을 제공합니다.
- 두 포트 간의 트래픽은 스위치를 통해서만 흐르며, 다른 포트로는 전송되지 않습니다.
- 포트 하나에 오류가 발생해도 다른 포트의 작동에는 영향을 미치지 않습니다.
- 패브릭 내에서 여러 쌍의 포트가 동시에 통신할 수 있습니다.

노드 작동 상태

노드는 구성 수준에 따라 여러 상태 중 하나일 수 있습니다.

- 사용 가능

  노드에 연관된 클러스터 이름이 없으며 아직 클러스터의 일부가 아닙니다.

- 보류 중

  노드가 구성되었으며 지정된 클러스터에 추가할 수 있습니다.

  노드에 접근하려면 인증이 필요하지 않습니다.

- 보류 중 활성

  시스템은 노드에 호환되는 Element 소프트웨어를 설치하는 중입니다. 완료되면 노드는 활성 상태로 전환됩니다.

- 활동적인

  노드가 클러스터에 참여하고 있습니다.

  노드를 수정하려면 인증이 필요합니다.

각 상태에서 일부 필드는 읽기 전용입니다.

더 많은 정보를 찾아보세요

- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

클러스터

클러스터는 SolidFire 스토리지 시스템의 허브이며 여러 노드로 구성됩니다. SolidFire 스토리지 효율성을 실현하려면 클러스터에 최소 4개의 노드가 있어야 합니다. 클러스터는 네트워크에 단일 논리적 그룹으로 나타나며 블록 스토리지로 액세스할 수 있습니다.

새로운 클러스터를 생성하면 클러스터의 통신 소유자로 노드가 초기화되고 클러스터의 각 노드에 대한 네트워크 통신이 설정됩니다. 이 프로세스는 새로운 클러스터마다 한 번씩만 수행됩니다. Element UI나 API를 사용하여 클러스터를 만들 수 있습니다.

추가 노드를 추가하여 클러스터를 확장할 수 있습니다. 새로운 노드를 추가하면 서비스가 중단되지 않으며 클러스터는 자동으로 새 노드의 성능과 용량을 사용합니다.

관리자와 호스트는 가상 IP 주소를 사용하여 클러스터에 액세스할 수 있습니다. 클러스터의 모든 노드는 가상 IP 주소를 호스팅할 수 있습니다. 관리 가상 IP(MVIP)는 1GbE 연결을 통해 클러스터 관리를 가능하게 하고, 스토리지 가상 IP(SVIP)는 10GbE 연결을 통해 호스트가 스토리지에 액세스할 수 있도록 합니다. 이러한 가상 IP 주소를 사용하면 SolidFire 클러스터의 크기나 구성에 관계없이 일관된 연결이 가능합니다. 가상 IP 주소를 호스팅하는 노드에 장애가 발생하면 클러스터의 다른 노드가 가상 IP 주소를 호스팅하기 시작합니다.

> Element 버전 11.0부터 노드는 관리 네트워크에 IPv4, IPv6 또는 두 주소 모두를 사용하여 구성할 수 있습니다. 이는 IPv6를 지원하지 않는 관리 노드 11.3 이상을 제외하고 저장 노드와 관리 노드 모두에 적용됩니다. 클러스터를 생성할 때 MVIP에는 단일 IPv4 또는 IPv6 주소만 사용할 수 있으며 모든 노드에서 해당 주소 유형을 구성해야 합니다.

클러스터에 대한 추가 정보

- 권한 있는 스토리지 클러스터
- [삼분법]
- 좌초 용량
- 스토리지 효율성
- 스토리지 클러스터 쿼럼

권한 있는 스토리지 클러스터

권한 있는 스토리지 클러스터는 NetApp Hybrid Cloud Control이 사용자를 인증하는 데 사용하는 스토리지 클러스터입니다.

관리 노드에 스토리지 클러스터가 하나만 있는 경우 해당 클러스터가 권한 클러스터입니다. 관리 노드에 두 개 이상의 스토리지 클러스터가 있는 경우 해당 클러스터 중 하나가 권한 있는 클러스터로 지정되고 해당 클러스터의 사용자만 NetApp Hybrid Cloud Control에 로그인할 수 있습니다. 어떤 클러스터가 권위 있는 클러스터인지 알아내려면 다음을 사용할 수 있습니다. `GET /mnode/about` API. 응답에서 IP 주소는 `token_url` 필드는 권한 있는 스토리지 클러스터의 관리 가상 IP 주소(MVIP)입니다. 권한이 있는 클러스터에 없는 사용자로 NetApp Hybrid Cloud Control에 로그인을 시도하면 로그인 시도가 실패합니다.

NetApp Hybrid Cloud Control 기능 중 다수는 여러 스토리지 클러스터에서 작동하도록 설계되었지만 인증 및 권한 부여에는 제한이 있습니다. 인증 및 권한 부여와 관련된 제한은 권한이 있는 클러스터의 사용자가 다른 스토리지 클러스터의 사용자가 아니더라도 NetApp Hybrid Cloud Control에 연결된 다른 클러스터에서 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. 사용자를 관리할 수 있습니다."Element 소프트웨어 사용자 인터페이스" .

보다"스토리지 클러스터 자산을 생성하고 관리합니다." 관리 노드 스토리지 클러스터 자산 작업에 대한 자세한 내용은 다음을 참조하세요.

삼분법

NetApp SolidFire 스토리지 클러스터에서 스토리지 노드 유형을 혼합하는 경우 단일 스토리지 노드는 전체 스토리지 클러스터 용량의 33% 이상을 포함할 수 없습니다.

좌초 용량

새로 추가된 노드가 전체 클러스터 용량의 50% 이상을 차지하는 경우, 해당 노드의 일부 용량은 사용할 수 없게 됩니다("고착"). 이는 용량 규칙을 준수하기 위한 조치입니다. 더 많은 저장 용량이 추가될 때까지 이는 그대로 유지됩니다. 용량 규칙을 위반하는 매우 큰 노드가 추가되면 이전에 고립되었던 노드는 더 이상 고립되지 않지만 새로 추가된 노드는 고립됩니다. 이런 일이 발생하지 않도록 용량은 항상 쌍으로 추가해야 합니다. 노드가 고립되면 적절한 클러스터 오류가 발생합니다.

스토리지 효율성

Netapp SolidFire 스토리지 클러스터는 중복 제거, 압축 및 씬 프로비저닝을 활용하여 볼륨을 저장하는 데 필요한 물리적 스토리지 양을 줄입니다.

- 압축

  압축은 데이터 블록을 압축 그룹으로 결합하여 볼륨에 필요한 물리적 저장 공간의 양을 줄입니다. 각 압축 그룹은 단일 블록으로 저장됩니다.

- 중복 제거

  중복 제거는 중복된 데이터 블록을 삭제하여 볼륨에 필요한 물리적 저장 공간의 양을 줄입니다.

- 씬 프로비저닝

  씬 프로비저닝 볼륨 또는 LUN은 저장소가 사전에 예약되지 않은 볼륨입니다. 대신, 저장소는 필요에 따라 동적으로 할당됩니다. 볼륨 또는 LUN의 데이터가 삭제되면 여유 공간이 스토리지 시스템으로 다시 해제됩니다.

스토리지 클러스터 쿼럼

Element 소프트웨어는 선택된 노드에서 스토리지 클러스터를 생성하고, 이를 통해 클러스터 구성의 복제된 데이터베이스를 유지 관리합니다. 클러스터 복원력을 위한 쿼럼을 유지하려면 클러스터 앙상블에 참여해야 하며 최소 3개의 노드가 필요합니다.

보안

SolidFire 올플래시 스토리지 시스템을 사용하면 데이터는 업계 표준 보안 프로토콜로 보호됩니다.

휴면 암호화(하드웨어)

저장 노드의 모든 드라이브는 드라이브 수준에서 AES 256비트 암호화를 활용하여 암호화할 수 있습니다. 각 드라이브에는 고유한 암호화 키가 있으며, 이 키는 드라이브가 처음 초기화될 때 생성됩니다. 암호화 기능을 활성화하면 클러스터 전체 암호가 생성되고 암호 일부가 클러스터의 모든 노드에 배포됩니다. 어떤 단일 노드도 전체 비밀번호를 저장하지 않습니다. 이 비밀번호는 드라이브에 대한 모든 액세스를 비밀번호로 보호하는 데 사용됩니다. 비밀번호는 드라이브 잠금을 해제하는 데 필요하며, 드라이브의 전원을 끄거나 드라이브가 잠겨 있지 않는 한 필요하지 않습니다.

"휴면 상태의 하드웨어 암호화 기능 활성화"클러스터의 성능이나 효율성에 영향을 미치지 않습니다. Element API 또는 Element UI를 사용하여 암호화가 활성화된 드라이브나 노드를 클러스터 구성에서 제거하면 해당 드라이브에서 저장 데이터 암호화가 비활성화됩니다. 드라이브를 제거한 후에는 다음을 사용하여 드라이브를 안전하게 지울 수 있습니다. `SecureEraseDrives` API 방식. 물리적 드라이브나 노드가 강제로 제거된 경우에도 데이터는 클러스터 전체 암호와 드라이브의 개별 암호화 키로 보호됩니다.

휴면 암호화(소프트웨어)

저장 중 암호화의 또 다른 유형인 소프트웨어 저장 중 암호화를 사용하면 스토리지 클러스터의 SSD에 기록된 모든 데이터를 암호화할 수 있습니다. "활성화 시" 소프트웨어에서 자동으로 작성된 모든 데이터를 암호화하고, 읽은 모든 데이터를 복호화합니다. 휴면 상태의 소프트웨어 암호화는 하드웨어에서 SED(자체 암호화 드라이브) 구현을 반영하여 SED가 없는 경우에도 데이터 보안을 제공합니다.

SolidFire 올플래시 스토리지 클러스터의 경우, 클러스터 생성 중에 소프트웨어 암호화를 활성화해야 하며 클러스터가 생성된 후에는 비활성화할 수 없습니다.

소프트웨어 기반 암호화와 하드웨어 기반 암호화는 독립적으로 또는 서로 결합하여 사용할 수 있습니다.

외부 키 관리

Element 소프트웨어를 구성하여 타사 KMIP 호환 키 관리 서비스(KMS)를 사용하여 스토리지 클러스터 암호화 키를 관리할 수 있습니다. 이 기능을 활성화하면 스토리지 클러스터의 클러스터 전체 드라이브 액세스 암호 암호화 키가 사용자가 지정한 KMS에서 관리됩니다.

Element는 다음과 같은 키 관리 서비스를 사용할 수 있습니다.

- Gemalto SafeNet KeySecure
- 세이프넷 AT 키시큐어
- 하이트러스트 키컨트롤
- Vormetric 데이터 보안 관리자
- IBM 보안 키 라이프사이클 관리자

외부 키 관리 구성에 대한 자세한 내용은 다음을 참조하세요."외부 키 관리 시작하기" 선적 서류 비치.

다중 요소 인증

다중 요소 인증(MFA)을 사용하면 사용자가 로그인할 때 NetApp Element 웹 UI 또는 스토리지 노드 UI에서 인증을 받기 위해 여러 유형의 증거를 제시하도록 요구할 수 있습니다. 기존 사용자 관리 시스템 및 ID 공급자와 통합하여 Element를 구성하여 로그인에 대해 다중 요소 인증만 허용할 수 있습니다. Element를 기존 SAML 2.0 ID 공급자와 통합하도록 구성하면 비밀번호와 문자 메시지, 비밀번호와 이메일 메시지 또는 기타 방법과 같은 여러 인증 체계를 적용할 수 있습니다.

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

MFA를 구성하려면 다음을 참조하세요. "다중 요소 인증을 활성화합니다" 선적 서류 비치.

HTTPS 및 저장 데이터 암호화를 위한 FIPS 140-2

NetApp SolidFire 스토리지 클러스터는 암호화 모듈에 대한 FIPS(연방 정보 처리 표준) 140-2 요구 사항을 준수하는 암호화를 지원합니다. SolidFire 클러스터에서 HTTPS 통신과 드라이브 암호화 모두에 대해 FIPS 140-2 규정 준수를 활성화할 수 있습니다.

클러스터에서 FIPS 140-2 운영 모드를 활성화하면 클러스터에서 NetApp 암호화 보안 모듈(NCSM)이 활성화되고 HTTPS를 통해 NetApp Element UI 및 API에 대한 모든 통신에 FIPS 140-2 레벨 1 인증 암호화가 활용됩니다. 당신은 사용합니다 `EnableFeature` Element API를 사용하여 `fips` FIPS 140-2 HTTPS 암호화를 활성화하는 매개변수입니다. FIPS 호환 하드웨어가 있는 스토리지 클러스터에서는 다음을 사용하여 저장 중인 데이터에 대한 FIPS 드라이브 암호화를 활성화할 수도 있습니다. `EnableFeature` Element API를 사용하여 `FipsDrives` 매개변수.

FIPS 140-2 암호화를 위한 새 스토리지 클러스터 준비에 대한 자세한 내용은 다음을 참조하세요."FIPS 드라이브를 지원하는 클러스터 만들기" .

기존의 준비된 클러스터에서 FIPS 140-2를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하세요."EnableFeature 요소 API" .

더 많은 정보를 원하시면

- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

계정 및 권한

시스템의 저장 리소스를 관리하고 액세스를 제공하려면 시스템 리소스에 대한 계정을 설정해야 합니다.

Element 저장소를 사용하면 다음 유형의 계정을 만들고 관리할 수 있습니다.

- 스토리지 클러스터의 관리자 사용자 계정
- 저장소 볼륨 액세스를 위한 사용자 계정
- NetApp Hybrid Cloud Control에 대한 권한 있는 클러스터 사용자 계정

스토리지 클러스터 관리자 계정

NetApp Element 소프트웨어를 실행하는 스토리지 클러스터에는 두 가지 유형의 관리자 계정이 있을 수 있습니다.

- 기본 클러스터 관리자 계정: 이 관리자 계정은 클러스터가 생성될 때 생성됩니다. 이 계정은 클러스터에 대한 가장 높은 수준의 액세스 권한을 가진 기본 관리 계정입니다. 이 계정은 Linux 시스템의 루트 사용자와 유사합니다. 이 관리자 계정의 비밀번호를 변경할 수 있습니다.
- 클러스터 관리자 계정: 클러스터 관리자 계정에 클러스터 내에서 특정 작업을 수행하기 위한 제한된 범위의 관리 액세스 권한을 부여할 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(비 LDAP) 클러스터 관리자 계정이 필요합니다. 아직 클러스터에 속하지 않은 노드에 액세스하는 데는 계정 자격 증명이 필요하지 않습니다.

당신은 할 수 있습니다"클러스터 관리자 계정 관리" 클러스터 관리자 계정을 생성, 삭제, 편집하고, 클러스터 관리자 비밀번호를 변경하고, LDAP 설정을 구성하여 사용자의 시스템 액세스를 관리합니다.

사용자 계정

사용자 계정은 NetApp Element 소프트웨어 기반 네트워크의 스토리지 리소스에 대한 액세스를 제어하는 데 사용됩니다. 볼륨을 생성하려면 최소한 하나의 사용자 계정이 필요합니다.

볼륨을 생성하면 볼륨이 계정에 할당됩니다. 가상 볼륨을 생성한 경우 해당 계정이 스토리지 컨테이너입니다.

다음은 몇 가지 추가 고려 사항입니다.

- 계정에는 할당된 볼륨에 액세스하는 데 필요한 CHAP 인증이 포함되어 있습니다.
- 한 계정에는 최대 2000개의 볼륨을 할당할 수 있지만, 볼륨은 한 계정에만 속할 수 있습니다.
- 사용자 계정은 NetApp Element Management 확장 지점에서 관리할 수 있습니다.

권한 있는 클러스터 사용자 계정

권한 있는 클러스터 사용자 계정은 NetApp Hybrid Cloud Control 노드 및 클러스터 인스턴스와 연결된 모든 스토리지 자산에 대해 인증할 수 있습니다. 이 계정을 사용하면 모든 클러스터에서 볼륨, 계정, 액세스 그룹 등을 관리할 수 있습니다.

권한이 있는 사용자 계정은 NetApp Hybrid Cloud Control의 오른쪽 상단 메뉴인 사용자 관리 옵션에서 관리됩니다.

그만큼"권한 있는 스토리지 클러스터" NetApp Hybrid Cloud Control이 사용자를 인증하는 데 사용하는 스토리지 클러스터입니다.

권한 있는 스토리지 클러스터에서 생성된 모든 사용자는 NetApp Hybrid Cloud Control에 로그인할 수 있습니다. 다른 스토리지 클러스터에서 생성된 사용자는 Hybrid Cloud Control에 로그인할 수 없습니다.

- 관리 노드에 스토리지 클러스터가 하나만 있는 경우 해당 클러스터가 권한 클러스터입니다.
- 관리 노드에 두 개 이상의 스토리지 클러스터가 있는 경우 해당 클러스터 중 하나가 권한 있는 클러스터로 지정되고 해당 클러스터의 사용자만 NetApp Hybrid Cloud Control에 로그인할 수 있습니다.

많은 NetApp Hybrid Cloud Control 기능이 여러 스토리지 클러스터에서 작동하지만 인증 및 권한 부여에는 불가피한 제한이 있습니다. 인증 및 권한 부여와 관련된 제한은 권한이 있는 클러스터의 사용자가 다른 스토리지 클러스터의 사용자가 아니더라도 NetApp Hybrid Cloud Control에 연결된 다른 클러스터에서 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 Hybrid Cloud Control에서 사용자를 관리할 수 있습니다.

볼륨 계정

볼륨별 계정은 해당 계정이 생성된 스토리지 클러스터에만 적용됩니다. 이러한 계정을 사용하면 네트워크 전반의 특정 볼륨에 대한 권한을 설정할 수 있지만 해당 볼륨 외부에는 아무런 영향도 미치지 않습니다.

볼륨 계정은 NetApp Hybrid Cloud Control Volumes 테이블 내에서 관리됩니다.

스토리지

볼륨

NetApp Element 스토리지 시스템은 볼륨을 사용하여 스토리지를 프로비저닝합니다. 볼륨은 iSCSI 또는 파이버 채널 클라이언트가 네트워크를 통해 액세스하는 블록 장치입니다.

Element 저장소를 사용하면 사용자 계정에 대한 볼륨을 생성, 보기, 편집, 삭제, 복제, 백업 또는 복원할 수 있습니다. 클러스터의 각 볼륨을 관리하고 볼륨 액세스 그룹에 볼륨을 추가하거나 제거할 수도 있습니다.

영구 볼륨

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

설치 및 업그레이드 스크립트에는 영구 볼륨을 활성화하는 옵션이 포함되어 있습니다."새로운 관리 노드 배포" . 영구 볼륨은 Element 소프트웨어 기반 스토리지 클러스터의 볼륨으로, VM의 수명을 넘어서도 유지되는 호스트 관리 노드 VM에 대한 관리 노드 구성 정보가 들어 있습니다. 관리 노드가 손실되면 대체 관리 노드 VM이 손실된 VM에 다시 연결하여 구성 데이터를 복구할 수 있습니다.

설치 또는 업그레이드 중에 영구 볼륨 기능을 활성화하면 자동으로 여러 볼륨이 생성됩니다. 이러한 볼륨은 모든 Element 소프트웨어 기반 볼륨과 마찬가지로 사용자의 선호도와 설치에 따라 Element 소프트웨어 웹 UI, vCenter Server용 NetApp Element 플러그인 또는 API를 사용하여 볼 수 있습니다. 복구에 사용할 수 있는 최신 구성 데이터를 유지하려면 영구 볼륨을 관리 노드에 iSCSI로 연결하여 실행해야 합니다.

> 관리 서비스와 연관된 영구 볼륨은 설치 또는 업그레이드 중에 생성되어 새 계정에 할당됩니다. 영구 볼륨을 사용하는 경우 볼륨이나 연결된 계정을 수정하거나 삭제하지 마십시오.

가상 볼륨(vVols)

vSphere Virtual Volumes는 vSphere의 스토리지 관리 대부분을 스토리지 시스템에서 VMware vCenter로 옮기는 VMware용 스토리지 패러다임입니다. 가상 볼륨(vVols)을 사용하면 개별 가상 머신의 요구 사항에 따라 스토리지를 할당할 수 있습니다.

바인딩

NetApp Element 클러스터는 최적의 프로토콜 엔드포인트를 선택하고, ESXi 호스트와 가상 볼륨을 프로토콜 엔드포인트와 연결하는 바인딩을 생성하고, 해당 바인딩을 ESXi 호스트로 반환합니다. 바인딩된 후 ESXi 호스트는 바인딩된 가상 볼륨에 대해 I/O 작업을 수행할 수 있습니다.

프로토콜 엔드포인트

VMware ESXi 호스트는 프로토콜 엔드포인트라고 하는 논리적 I/O 프록시를 사용하여 가상 볼륨과 통신합니다. ESXi 호스트는 가상 볼륨을 프로토콜 엔드포인트에 바인딩하여 I/O 작업을 수행합니다. 호스트의 가상 머신이 I/O 작업을 수행하면 연관된 프로토콜 엔드포인트는 페어링된 가상 볼륨으로 I/O를 전달합니다.

NetApp Element 클러스터의 프로토콜 엔드포인트는 SCSI 관리 논리 단위로 작동합니다. 각 프로토콜 엔드포인트는

클러스터에 의해 자동으로 생성됩니다. 클러스터의 각 노드에 대해 해당 프로토콜 엔드포인트가 생성됩니다. 예를 들어, 4노드 클러스터에는 4개의 프로토콜 엔드포인트가 있습니다.

iSCSI는 NetApp Element 소프트웨어에서 지원되는 유일한 프로토콜입니다. 파이버 채널 프로토콜은 지원되지 않습니다. 프로토콜 엔드포인트는 사용자가 삭제하거나 수정할 수 없으며, 계정과 연결되지 않고, 볼륨 액세스 그룹에 추가할 수 없습니다.

저장 용기

스토리지 컨테이너는 NetApp Element 계정에 매핑되는 논리적 구조이며 보고 및 리소스 할당에 사용됩니다. 가상 볼륨에 스토리지 시스템이 제공할 수 있는 원시 스토리지 용량이나 집계 스토리지 기능을 풀링합니다. vSphere에서 생성된 VVol 데이터스토어는 개별 스토리지 컨테이너에 매핑됩니다. 기본적으로 단일 스토리지 컨테이너에는 NetApp Element 클러스터의 모든 사용 가능한 리소스가 포함됩니다. 다중 테넌시에 대한 보다 세부적인 거버넌스가 필요한 경우 여러 개의 스토리지 컨테이너를 생성할 수 있습니다.

저장 컨테이너는 기존 계정처럼 기능하며 가상 볼륨과 기존 볼륨을 모두 포함할 수 있습니다. 클러스터당 최대 4개의 저장 컨테이너가 지원됩니다. VVols 기능을 사용하려면 최소 하나의 저장 컨테이너가 필요합니다. VVol을 생성하는 동안 vCenter에서 스토리지 컨테이너를 검색할 수 있습니다.

VASA 제공업체

NetApp Element 클러스터의 vVol 기능을 vSphere에 알리려면 vSphere 관리자가 NetApp Element VASA 공급자를 vCenter에 등록해야 합니다. VASA 공급자는 vSphere와 Element 클러스터 간의 대역 외 제어 경로입니다. vSphere를 대신하여 Element 클러스터에서 VM 생성, vSphere에서 VM 사용 가능, vSphere에 스토리지 용량 광고 등의 요청을 실행하는 역할을 담당합니다.

VASA 공급자는 Element 소프트웨어의 클러스터 마스터의 일부로 실행됩니다. 클러스터 마스터는 필요에 따라 클러스터의 모든 노드로 장애 조치를 수행하는 고가용성 서비스입니다. 클러스터 마스터가 장애 조치되면 VASA 공급자도 함께 이동하여 VASA 공급자의 고가용성을 보장합니다. 모든 프로비저닝 및 스토리지 관리 작업은 Element 클러스터에서 필요한 모든 변경 사항을 처리하는 VASA 공급자를 사용합니다.

Element 12.5 및 이전 버전의 경우 단일 vCenter 인스턴스에 두 개 이상의 NetApp Element VASA 공급자를 등록하지 마세요. 두 번째 NetApp Element VASA 공급자가 추가되면 모든 VVOL 데이터 저장소에 액세스할 수 없게 됩니다.

vCenter에 VASA 공급자를 이미 등록한 경우 업그레이드 패치로 최대 10개의 vCenter에 대한 VASA 지원을 사용할 수 있습니다. 설치하려면 VASA39 매니페스트의 지침을 따르고 .tar.gz 파일을 다운로드하세요."NetApp 소프트웨어 다운로드" 대지. NetApp Element VASA 공급자는 NetApp 인증서를 사용합니다. 이 패치를 사용하면 인증서가 vCenter에서 수정되지 않고 사용되어 VASA 및 VVols 사용을 위한 여러 vCenter를 지원합니다. 인증서를 수정하지 마세요. VASA에서는 사용자 정의 SSL 인증서를 지원하지 않습니다.

더 많은 정보를 찾아보세요

- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

볼륨 액세스 그룹

볼륨 액세스 그룹을 만들고 사용하면 볼륨 세트에 대한 액세스를 제어할 수 있습니다. 볼륨 세트와 초기자 세트를 볼륨 액세스 그룹과 연결하면 액세스 그룹은 해당 초기자에게 해당 볼륨

세트에 대한 액세스 권한을 부여합니다.

NetApp SolidFire 스토리지의 볼륨 액세스 그룹을 사용하면 iSCSI 이니시에이터 IQN 또는 파이버 채널 WWPN이 볼륨 컬렉션에 액세스할 수 있습니다. 액세스 그룹에 추가하는 각 IQN은 CHAP 인증을 사용하지 않고도 그룹의 각 볼륨에 액세스할 수 있습니다. 액세스 그룹에 WWPN을 추가하면 액세스 그룹의 볼륨에 대한 파이버 채널 네트워크 액세스가 가능해집니다.

볼륨 액세스 그룹에는 다음과 같은 제한이 있습니다.

- 볼륨 액세스 그룹당 최대 128개의 이니시에이터.
- 볼륨당 최대 64개의 액세스 그룹.
- 액세스 그룹은 최대 2000개의 볼륨으로 구성될 수 있습니다.
- IQN 또는 WWPN은 하나의 볼륨 액세스 그룹에만 속할 수 있습니다.
- 파이버 채널 클러스터의 경우 단일 볼륨은 최대 4개의 액세스 그룹에 속할 수 있습니다.

개시자

이니시에이터는 외부 클라이언트가 클러스터의 볼륨에 액세스할 수 있도록 하여 클라이언트와 볼륨 간 통신의 진입점 역할을 합니다. 계정 기반이 아닌 CHAP 기반으로 스토리지 볼륨에 액세스하려면 이니시에이터를 사용할 수 있습니다. 볼륨 액세스 그룹에 단일 이니시에이터를 추가하면 볼륨 액세스 그룹 구성원이 인증 없이도 그룹에 추가된 모든 스토리지 볼륨에 액세스할 수 있습니다. 개시자는 하나의 액세스 그룹에만 속할 수 있습니다.

데이터 보호

데이터 보호 기능에는 원격 복제, 볼륨 스냅샷, 볼륨 복제, 보호 도메인, 이중 나선 기술을 통한 고가용성 등이 포함됩니다.

요소 저장 데이터 보호에는 다음과 같은 개념이 포함됩니다.

- 원격 복제 유형
- 데이터 보호를 위한 볼륨 스냅샷
- 볼륨 클론
- Element 저장소에 대한 백업 및 복원 프로세스 개요
- 보호 도메인
- 사용자 정의 보호 도메인
- Double Helix 고가용성

원격 복제 유형

데이터의 원격 복제는 다음과 같은 형태를 취할 수 있습니다.

- 클러스터 간 동기 및 비동기 복제
- 스냅샷 전용 복제

- SnapMirror 사용한 Element와 ONTAP 클러스터 간 복제

자세한 내용은 다음을 참조하세요. "TR-4741: NetApp Element 소프트웨어 원격 복제" .

클러스터 간 동기 및 비동기 복제

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

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

동기 복제

동기 복제는 소스 클러스터에서 대상 클러스터로 데이터를 지속적으로 복제하며 지연 시간, 패킷 손실, 지터, 대역폭의 영향을 받습니다.

동기 복제는 다음과 같은 상황에 적합합니다.

- 짧은 거리에 걸쳐 여러 시스템 복제
- 출처와 지리적으로 가까운 재해 복구 사이트
- 시간에 민감한 애플리케이션 및 데이터베이스 보호
- 기본 사이트가 다운되었을 때 보조 사이트가 기본 사이트 역할을 해야 하는 비즈니스 연속성 애플리케이션

비동기 복제

비동기 복제는 대상 클러스터의 확인을 기다리지 않고 소스 클러스터에서 대상 클러스터로 데이터를 지속적으로 복제합니다. 비동기 복제 중에 쓰기는 소스 클러스터에서 커밋된 후 클라이언트(애플리케이션)에 확인됩니다.

비동기 복제는 다음과 같은 상황에 적합합니다.

- 재해 복구 사이트가 소스와 멀리 떨어져 있으며, 애플리케이션이 네트워크로 인해 발생하는 지연을 허용하지 않습니다.
- 소스 클러스터와 대상 클러스터를 연결하는 네트워크에는 대역폭 제한이 있습니다.

스냅샷 전용 복제

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

스냅샷 복제 빈도를 설정할 수 있습니다.

스냅샷 복제는 비동기 또는 동기 복제에 영향을 미치지 않습니다.

SnapMirror 사용한 **Element**와 **ONTAP** 클러스터 간 복제

NetApp SnapMirror 기술을 사용하면 NetApp Element 소프트웨어를 사용하여 촬영한 스냅샷을 재해 복구 목적으로 ONTAP 에 복제할 수 있습니다. SnapMirror 관계에서 Element는 한 엔드포인트이고 ONTAP 다른 엔드포인트입니다.

SnapMirror 는 재해 복구를 용이하게 하는 NetApp 스냅샷 복제 기술로, 지리적으로 멀리 떨어진 사이트의 기본

스토리지에서 보조 스토리지로 장애 조치를 수행하도록 설계되었습니다. SnapMirror 기술은 기본 사이트에 장애가 발생하더라도 보조 저장소에 작업 데이터의 복제본 또는 미러를 생성하여 이를 통해 데이터를 계속 제공할 수 있습니다. 데이터는 볼륨 수준에서 미러링됩니다.

기본 저장소의 소스 볼륨과 보조 저장소의 대상 볼륨 간의 관계를 데이터 보호 관계라고 합니다. 클러스터는 볼륨이 상주하는 엔드포인트라고 하며 복제된 데이터가 포함된 볼륨은 피어링되어야 합니다. 피어 관계를 통해 클러스터와 볼륨이 안전하게 데이터를 교환할 수 있습니다.

SnapMirror NetApp ONTAP 컨트롤러에서 기본적으로 실행되며 NetApp HCI 및 SolidFire 클러스터에서 실행되는 Element에 통합되어 있습니다. SnapMirror 제어하는 논리는 ONTAP 소프트웨어에 있습니다. 따라서 모든 SnapMirror 관계에는 조정 작업을 수행하기 위해 최소한 하나의 ONTAP 시스템이 포함되어야 합니다. 사용자는 주로 Element UI를 통해 Element와 ONTAP 클러스터 간의 관계를 관리합니다. 하지만 일부 관리 작업은 NetApp ONTAP System Manager에 있습니다. 사용자는 ONTAP 과 Element에서 모두 사용 가능한 CLI와 API를 통해 SnapMirror 관리할 수도 있습니다.

보다 "TR-4651: NetApp SolidFire SnapMirror 아키텍처 및 구성" (로그인 필요)

Element 소프트웨어를 사용하여 클러스터 수준에서 SnapMirror 기능을 수동으로 활성화해야 합니다. SnapMirror 기능은 기본적으로 비활성화되어 있으며, 새로 설치하거나 업그레이드해도 자동으로 활성화되지 않습니다.

SnapMirror 활성화한 후 Element 소프트웨어의 데이터 보호 탭에서 SnapMirror 관계를 만들 수 있습니다.

NetApp Element 소프트웨어 10.1 이상은 ONTAP 시스템에서 스냅샷을 복사하고 복원하는 SnapMirror 기능을 지원합니다.

Element 10.1 이상을 실행하는 시스템에는 9.3 이상을 실행하는 ONTAP 시스템의 SnapMirror 와 직접 통신할 수 있는 코드가 포함되어 있습니다. Element API는 클러스터, 볼륨 및 스냅샷에서 SnapMirror 기능을 활성화하는 방법을 제공합니다. 또한 Element UI에는 Element 소프트웨어와 ONTAP 시스템 간의 SnapMirror 관계를 관리하는 기능이 포함되어 있습니다.

Element 10.3 및 ONTAP 9.4 시스템부터 제한된 기능으로 특정 사용 사례에서 ONTAP 생성된 볼륨을 Element 볼륨으로 복제할 수 있습니다.

자세한 내용은 다음을 참조하세요. "NetApp Element 소프트웨어와 ONTAP 간 복제(ONTAP CLI)".

데이터 보호를 위한 볼륨 스냅샷

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

스냅샷은 볼륨 복제본과 유사하지만, 볼륨 메타데이터의 복제본일 뿐이므로 마운트하거나 쓸 수 없습니다. 볼륨 스냅샷을 만드는 데는 시스템 리소스와 공간도 적게 사용되므로 복제보다 스냅샷을 만드는 속도가 더 빠릅니다.

스냅샷을 원격 클러스터에 복제하여 볼륨의 백업 사본으로 사용할 수 있습니다. 이를 통해 복제된 스냅샷을 사용하여 볼륨을 특정 시점으로 롤백할 수 있습니다. 또한 복제된 스냅샷에서 볼륨의 복제본을 생성할 수도 있습니다.

Element 클러스터의 스냅샷을 외부 개체 저장소나 다른 Element 클러스터로 백업할 수 있습니다. 스냅샷을 외부 개체 저장소에 백업하는 경우 읽기/쓰기 작업을 허용하는 개체 저장소에 대한 연결이 있어야 합니다.

개별 볼륨이나 여러 볼륨의 스냅샷을 찍어서 데이터를 보호할 수 있습니다.

볼륨 클론

단일 볼륨 또는 여러 볼륨의 복제본은 데이터의 특정 시점 복사본입니다. 볼륨을 복제하면 시스템은 볼륨의 스냅샷을 만든 다음 스냅샷에서 참조하는 데이터의 복사본을 만듭니다.

이는 비동기 프로세스이며, 프로세스에 필요한 시간은 복제하는 볼륨의 크기와 현재 클러스터 부하에 따라 달라집니다.

클러스터는 볼륨당 동시에 최대 2개의 실행 중인 복제 요청을 지원하고, 동시에 최대 8개의 활성 볼륨 복제 작업을 지원합니다. 이러한 제한을 초과하는 요청은 나중에 처리하기 위해 대기합니다.

Element 저장소에 대한 백업 및 복원 프로세스 개요

Amazon S3 또는 OpenStack Swift와 호환되는 보조 객체 저장소뿐만 아니라 다른 SolidFire 스토리지에도 볼륨을 백업하고 복원할 수 있습니다.

다음 위치에 볼륨을 백업할 수 있습니다.

- SolidFire 스토리지 클러스터
- Amazon S3 객체 저장소
- OpenStack Swift 객체 저장소

OpenStack Swift 또는 Amazon S3에서 볼륨을 복원하는 경우 원래 백업 프로세스의 매니페스트 정보가 필요합니다. SolidFire 스토리지 시스템에 백업된 볼륨을 복원하는 경우 매니페스트 정보가 필요하지 않습니다.

보호 도메인

보호 도메인은 일부 또는 전체가 실패하더라도 데이터 가용성을 유지할 수 있도록 그룹화된 노드 또는 노드 집합입니다. 보호 도메인을 사용하면 스토리지 클러스터가 섀시(섀시 친화성) 또는 전체 도메인(섀시 그룹) 손실로부터 자동으로 복구될 수 있습니다.

vCenter Server용 NetApp Element 플러그인의 NetApp Element 구성 확장 지점을 사용하여 보호 도메인 모니터링을 수동으로 활성화할 수 있습니다. 노드 또는 섀시 도메인을 기반으로 보호 도메인 임계값을 선택할 수 있습니다. Element API나 웹 UI를 사용하여 보호 도메인 모니터링을 활성화할 수도 있습니다.

보호 도메인 레이아웃은 각 노드를 특정 보호 도메인에 할당합니다.

보호 도메인 수준이라고 하는 두 가지 보호 도메인 레이아웃이 지원됩니다.

- 노드 수준에서 각 노드는 자체 보호 도메인에 있습니다.
- 섀시 수준에서는 섀시를 공유하는 노드만 동일한 보호 도메인에 있습니다.
  - 노드가 클러스터에 추가되면 섀시 수준 레이아웃이 하드웨어에서 자동으로 결정됩니다.
  - 각 노드가 별도의 섀시에 있는 클러스터에서는 이 두 수준이 기능적으로 동일합니다.

새 클러스터를 생성할 때 공유 섀시에 있는 스토리지 노드를 사용하는 경우 보호 도메인 기능을 사용하여 섀시 수준 장애 보호를 설계하는 것이 좋습니다.

사용자 정의 보호 도메인

사용자의 특정 섀시 및 노드 레이아웃에 맞는 사용자 정의 보호 도메인 레이아웃을 정의할 수 있으며, 각 노드는 단

하나의 사용자 정의 보호 도메인에만 연결됩니다. 기본적으로 각 노드는 동일한 기본 사용자 지정 보호 도메인에 할당됩니다.

사용자 지정 보호 도메인이 할당되지 않은 경우:

- 클러스터 작동에는 영향을 미치지 않습니다.
- 사용자 정의 수준은 관용적이지도 않고 회복력도 없습니다.

클러스터에 대한 사용자 지정 보호 도메인을 구성하는 경우 Element 웹 UI 대시보드에서 확인할 수 있는 세 가지 보호 수준이 있습니다.

- 보호되지 않음: 스토리지 클러스터가 사용자 지정 보호 도메인 중 하나의 장애로부터 보호되지 않습니다. 이 문제를 해결하려면 클러스터에 추가 저장 용량을 추가하거나 클러스터의 사용자 지정 보호 도메인을 재구성하여 클러스터를 잠재적인 데이터 손실로부터 보호하세요.
- 장애 허용: 스토리지 클러스터에는 사용자 지정 보호 도메인 중 하나에 장애가 발생한 후에도 데이터 손실을 방지할 수 있을 만큼 충분한 여유 용량이 있습니다.
- 장애 복구력: 스토리지 클러스터는 사용자 지정 보호 도메인 중 하나에 장애가 발생한 후에도 자체 복구를 수행할 수 있는 충분한 여유 용량을 확보합니다. 치료 과정이 완료되면 추가 도메인에 장애가 발생하더라도 클러스터는 데이터 손실로부터 보호됩니다.

두 개 이상의 사용자 정의 보호 도메인이 할당된 경우 각 하위 시스템은 중복된 보호 도메인을 별도의 사용자 정의 보호 도메인에 할당합니다. 이것이 가능하지 않으면 중복된 항목을 별도의 노드에 할당하게 됩니다. 각 하위 시스템(예: 빈, 슬라이스, 프로토콜 엔드포인트 공급자, 앙상블)은 이를 독립적으로 수행합니다.

Element UI를 사용하여 다음을 수행할 수 있습니다."사용자 정의 보호 도메인 구성" 또는 다음 API 메서드를 사용할 수 있습니다.

- "보호 도메인 레이아웃 가져오기"- 각 노드가 속한 섀시와 사용자 정의 보호 도메인을 표시합니다.
- "보호 도메인 레이아웃 설정"- 각 노드에 사용자 정의 보호 도메인을 할당할 수 있습니다.

Double Helix 고가용성

Double Helix 데이터 보호는 시스템 내의 모든 드라이브에 최소 두 개의 중복된 데이터 사본을 분산시키는 복제 방법입니다. "RAID-less" 방식을 사용하면 시스템이 스토리지 시스템의 모든 수준에서 동시에 발생하는 여러 가지 오류를 흡수하고 신속하게 복구할 수 있습니다.

성능 및 서비스 품질

SolidFire 스토리지 클러스터는 볼륨별로 QoS(서비스 품질) 매개변수를 제공할 수 있습니다. QoS를 정의하는 세 가지 구성 가능한 매개변수(최소 IOPS, 최대 IOPS, 버스트 IOPS)를 사용하여 초당 입력 및 출력(IOPS)으로 측정되는 클러스터 성능을 보장할 수 있습니다.

SolidFire Active IQ 에는 QoS 설정의 최적 구성 및 설정에 대한 조언을 제공하는 QoS 권장 사항 페이지가 있습니다.

서비스 품질 매개변수

IOPS 매개변수는 다음과 같은 방식으로 정의됩니다.

- 최소 **IOPS** - 스토리지 클러스터가 볼륨에 제공하는 초당 지속적인 입력 및 출력(IOPS)의 최소 수입니다. 볼륨에 구성된 최소 IOPS는 볼륨에 대해 보장되는 성능 수준입니다. 이 수준 이하로는 성능이 떨어지지 않습니다.
- 최대 **IOPS** - 스토리지 클러스터가 볼륨에 제공하는 지속형 IOPS의 최대 수입니다. 클러스터 IOPS 수준이 매우 높은 경우, 이 수준의 IOPS 성능은 초과되지 않습니다.
- 버스트 **IOPS** - 짧은 버스트 시나리오에서 허용되는 최대 IOPS 수입니다. 볼륨이 최대 IOPS보다 낮게 실행되면 버스트 크레딧이 누적됩니다. 성능 수준이 매우 높아지고 최대 수준으로 끌어올려지면 볼륨에서 짧은 IOPS 버스트가 허용됩니다.

  Element 소프트웨어는 클러스터가 낮은 클러스터 IOPS 활용도 상태에서 실행될 때 Burst IOPS를 사용합니다.

  단일 볼륨은 버스트 IOPS를 축적하고 이 크레딧을 사용하여 설정된 "버스트 기간" 동안 최대 IOPS를 초과하여 버스트 IOPS 수준까지 버스트할 수 있습니다. 클러스터에 버스트를 수용할 수 있는 용량이 있는 경우 볼륨은 최대 60초 동안 버스트될 수 있습니다. 볼륨은 최대 IOPS 한도보다 낮은 속도로 실행되는 매 초마다 1초의 버스트 크레딧(최대 60초)을 누적합니다.

  버스트 IOPS는 두 가지 방법으로 제한됩니다.

  - 볼륨은 볼륨이 축적한 버스트 크레딧 수와 동일한 시간(초) 동안 최대 IOPS를 초과하여 버스트할 수 있습니다.
  - 볼륨이 최대 IOPS 설정을 초과하면 버스트 IOPS 설정에 의해 제한됩니다. 따라서 버스트 IOPS는 볼륨의 버스트 IOPS 설정을 초과하지 않습니다.
- 효과적인 최대 대역폭 - 최대 대역폭은 IOPS 수(QoS 곡선 기반)에 IO 크기를 곱하여 계산됩니다.

  예: QoS 매개변수를 최소 IOPS 100, 최대 IOPS 1000, 버스트 IOPS 1500으로 설정하면 성능 품질에 다음과 같은 효과가 있습니다.

  - 워크로드는 클러스터에서 IOPS에 대한 워크로드 경합 조건이 명확해질 때까지 최대 1000 IOPS에 도달하고 유지할 수 있습니다. 그런 다음 모든 볼륨의 IOPS가 지정된 QoS 범위 내에 있고 성능 경쟁이 완화될 때까지 IOPS를 점진적으로 줄입니다.
  - 모든 볼륨의 성능은 최소 IOPS 100에 근접합니다. 수준은 최소 IOPS 설정보다 낮아지지 않지만 작업 부하 경합이 완화되면 100 IOPS보다 높게 유지될 수 있습니다.
  - 성능은 1000 IOPS를 넘지 않으며, 일정 기간 동안 100 IOPS 미만이 되지 않습니다. 1500 IOPS(버스트 IOPS)의 성능은 허용되지만, 최대 IOPS 미만으로 실행하여 버스트 크레딧을 축적한 볼륨에만 해당되며 짧은 시간 동안만 허용됩니다. 버스트 수준은 지속되지 않습니다.

QoS 값 제한

QoS에 대한 가능한 최소값과 최대값은 다음과 같습니다.

매개변수	최소값	기본	**4 4KB**	**5 8KB**	**6 16KB**	**262KB**
최소 IOPS	50	50	15,000	9,375*	5556*	385*
최대 IOPS	100	15,000	20만**	125,000	74,074	5128
버스트 IOPS	100	15,000	20만**	125,000	74.074	5128

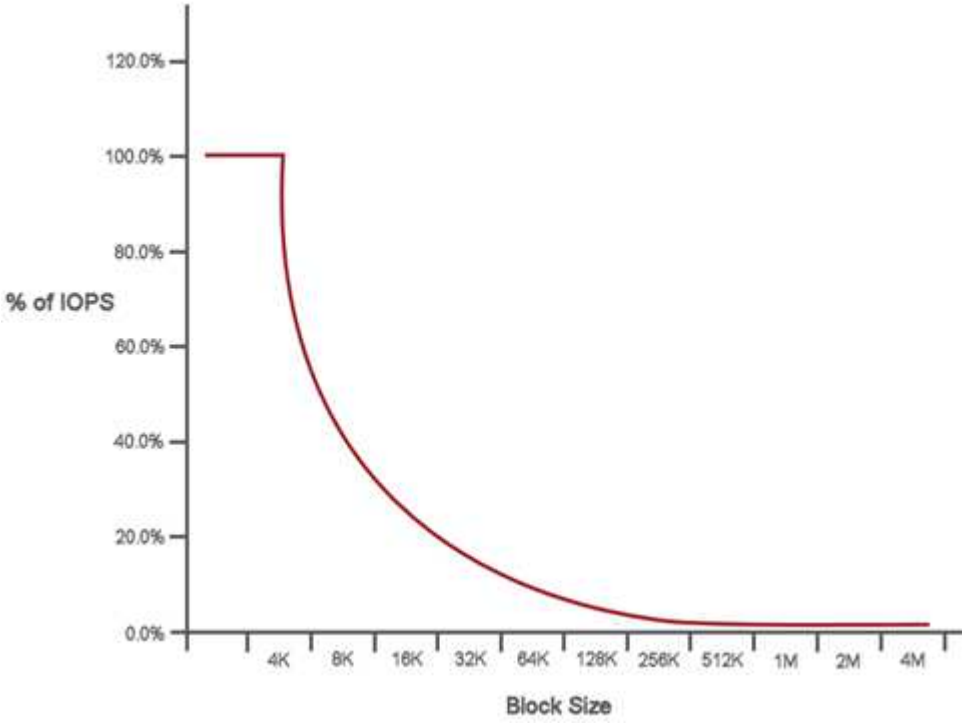
*이 추정치는 대략적인 수치입니다. **최대 IOPS와 버스트 IOPS는 최대 200,000까지 설정할 수 있습니다. 하지만 이 설정은 볼륨의 성능을 효과적으로 제한하지 않는 경우에만 허용됩니다. 볼륨의 실제 최대 성능은 클러스터 사용 및 노드별 성능에 따라 제한됩니다.

QoS 성능

QoS 성능 곡선은 블록 크기와 IOPS 비율 간의 관계를 보여줍니다.

블록 크기와 대역폭은 애플리케이션이 얻을 수 있는 IOPS 수에 직접적인 영향을 미칩니다. Element 소프트웨어는 수신한 블록 크기를 고려하여 블록 크기를 4k로 정규화합니다. 작업 부하에 따라 시스템이 블록 크기를 늘릴 수 있습니다. 블록 크기가 증가함에 따라 시스템은 더 큰 블록 크기를 처리하는 데 필요한 수준으로 대역폭을 늘립니다. 대역폭이 증가함에 따라 시스템이 달성할 수 있는 IOPS 수는 감소합니다.

QoS 성능 곡선은 블록 크기 증가와 IOPS 비율 감소 간의 관계를 보여줍니다.



예를 들어, 블록 크기가 4k이고 대역폭이 4000KBps인 경우 IOPS는 1000입니다. 블록 크기가 8k로 늘어나면 대역폭은 5000KBps로 늘어나고 IOPS는 625로 감소합니다. 시스템은 블록 크기를 고려하여 백업 및 하이퍼바이저 활동과 같이 더 높은 블록 크기를 사용하는 우선순위가 낮은 워크로드가 더 작은 블록 크기를 사용하는 우선순위가 높은 트래픽에 필요한 성능을 너무 많이 차지하지 않도록 보장합니다.

QoS 정책

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

QoS 정책은 데이터베이스, 애플리케이션 또는 인프라 서버가 재부팅이 거의 없고 저장소에 대한 지속적인 동일 액세스가 필요한 서비스 환경에 가장 적합합니다. 개별 볼륨 QoS는 매일 또는 하루에 여러 번 재부팅, 전원 켜기 또는 전원 끄기가 가능한 가상 데스크톱이나 특수 키오스크 유형 VM과 같이 사용량이 적은 VM에 가장 적합합니다.

QoS와 QoS 정책은 함께 사용해서는 안 됩니다. QoS 정책을 사용하는 경우 볼륨에서 사용자 지정 QoS를 사용하지 마세요. 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.

더 많은 정보를 찾아보세요

- "SolidFire 및 Element 소프트웨어 문서"