Element 소프트웨어를 사용하여 스토리지 관리

Element Software

NetApp
January 15, 2024

목차

Element 소프트웨어를 사용하여 스토리지 관리

Element 소프트웨어를 사용하여 SolidFire 스토리지를 설정하고, 클러스터 용량 및 성능을 모니터링하고, 멀티 테넌트(multi-tenant) 인프라 전반에서 스토리지 활동을 관리합니다.

요소는 SolidFire 클러스터의 중심에 있는 스토리지 운영 체제입니다. Element 소프트웨어는 클러스터의 모든 노드에서 독립적으로 실행되며 클러스터 노드가 리소스를 결합하여 단일 스토리지 시스템으로 외부 클라이언트에 제공할 수 있도록 합니다. Element 소프트웨어는 시스템 전체의 모든 클러스터 조정, 확장 및 관리를 책임집니다.

소프트웨어 인터페이스는 Element API를 기반으로 구축됩니다.

- "Element 소프트웨어 사용자 인터페이스에 액세스합니다"
- "구축 후 SolidFire 시스템 옵션을 구성합니다"
- "스토리지 시스템 구성 요소 업그레이드"
- "Element 소프트웨어 UI에서 기본 옵션을 사용합니다"
- "계정 관리"
- "시스템 관리"
- "볼륨 및 가상 볼륨 관리"
- "데이터 보호"
- "시스템 문제를 해결합니다"

자세한 내용을 확인하십시오

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

Element 소프트웨어 사용자 인터페이스에 액세스합니다

기본 클러스터 노드의 관리 가상 IP(MVIP) 주소를 사용하여 Element UI에 액세스할 수 있습니다.

브라우저에서 팝업 차단기와 NoScript 설정이 비활성화되어 있는지 확인해야 합니다.

클러스터 생성 중 구성에 따라 IPv4 또는 IPv6 주소 지정을 사용하여 UI에 액세스할 수 있습니다.

1. 다음 중 하나를 선택합니다.
   - IPv6: https://[IPv6 MVIP 주소 입력] 예:

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

   - IPv4: https://[IPv4 MVIP 주소 입력] 예:

```
https://10.123.456.789/
```

2. DNS의 경우 호스트 이름을 입력합니다.
3. 인증 인증서 메시지를 클릭합니다.

자세한 내용을 확인하십시오

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

구축 후 SolidFire 시스템 옵션을 구성합니다

SolidFire 시스템을 설정한 후 몇 가지 선택적 작업을 수행할 수 있습니다.

시스템에서 자격 증명을 변경하는 경우 다른 구성 요소에 미치는 영향을 알고 싶을 수 있습니다.

또한 다중 요소 인증, 외부 키 관리 및 FIPS(Federal Information Processing Standards) 보안에 대한 설정을 구성할 수 있습니다. 필요한 경우 암호 업데이트도 고려해야 합니다.

자세한 내용을 확인하십시오

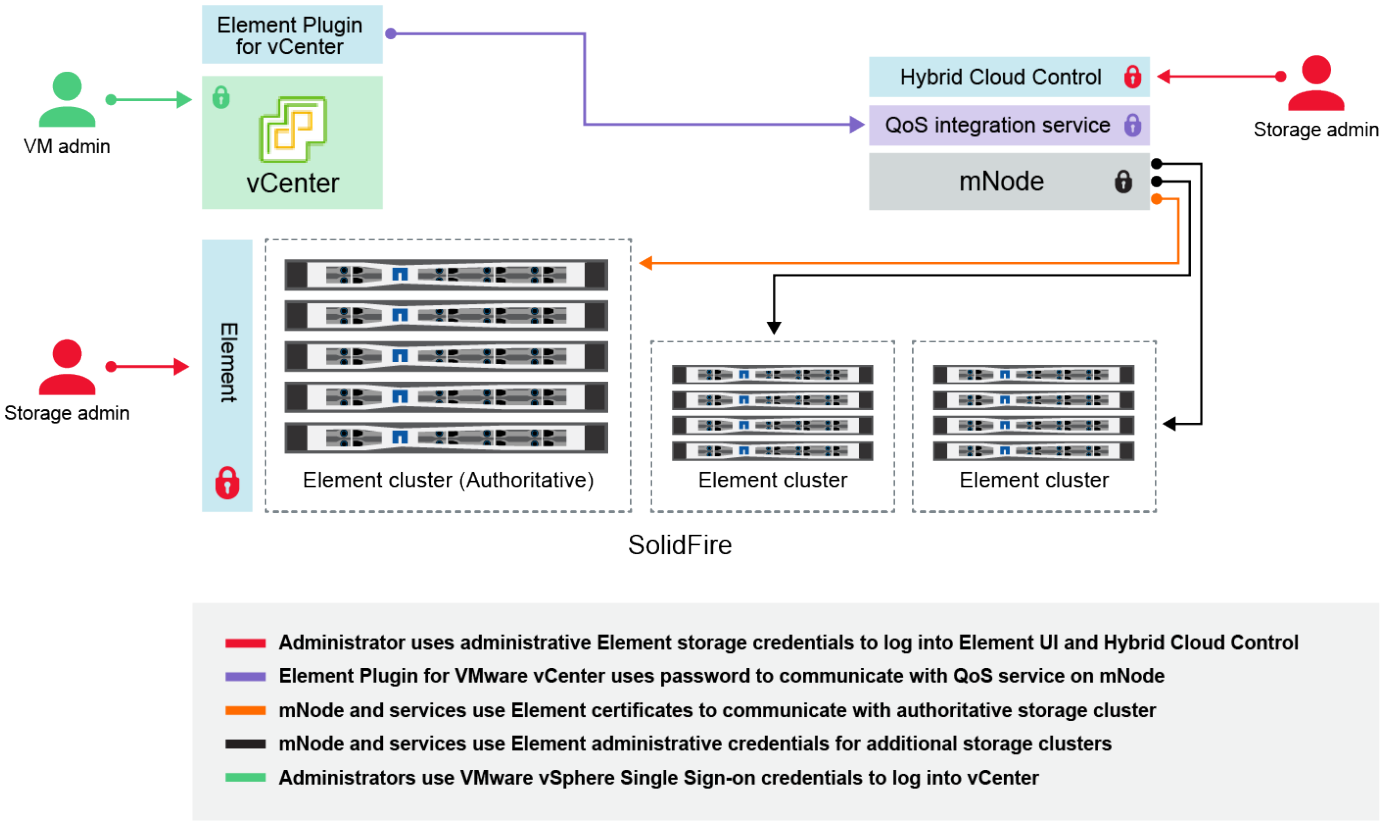
- "NetApp HCI 및 NetApp SolidFire에서 자격 증명을 변경합니다"
- "Element 소프트웨어 기본 SSL 인증서를 변경합니다"
- "노드의 IPMI 암호를 변경합니다"
- "다중 요소 인증을 사용합니다"
- "외부 키 관리를 시작합니다"
- "FIPS 드라이브를 지원하는 클러스터를 생성합니다"

NetApp HCI 및 NetApp SolidFire에서 자격 증명을 변경합니다

NetApp HCI 또는 NetApp SolidFire를 구축한 조직의 보안 정책에 따라 자격 증명 또는 암호를 변경하는 것이 일반적으로 보안 사례의 일부입니다. 암호를 변경하기 전에 배포의 다른 소프트웨어 구성 요소에 미치는 영향을 알고 있어야 합니다.

NetApp HCI 또는 NetApp SolidFire 구축의 구성 요소 중 하나에 대한 자격 증명을 변경하는 경우 다음 표에서는 다른 구성 요소에 미치는 영향에 대한 지침을 제공합니다.

NetApp SolidFire 구성 요소 상호 작용
:



자격 증명 유형 및 아이콘	관리자별 사용	이 지침을 참조하십시오
요소 자격 증명	• 는 *:NetApp HCI 및 SolidFire에 적용됩니다 관리자는 다음 자격 증명을 사용하여 에 로그인합니다. • Element 스토리지 클러스터의 요소 사용자 인터페이스 • 관리 노드에서의 하이브리드 클라우드 제어(mnode) Hybrid Cloud Control은 여러 스토리지 클러스터를 관리할 때 mnode가 처음에 설정한 _authoritative cluster_로 알려진 스토리지 클러스터에 대한 관리자 자격 증명만 수락합니다. 나중에 하이브리드 클라우드 제어에 추가된 스토리지 클러스터의 경우 mnode는 관리자 자격 증명을 안전하게 저장합니다. 이후에 추가된 스토리지 클러스터에 대한 자격 증명이 변경된 경우 mnode API를 사용하여 mnode에서도 자격 증명을 업데이트해야 합니다.	• "스토리지 클러스터 관리자 암호를 업데이트합니다." • 를 사용하여 mnode의 스토리지 클러스터 관리자 자격 증명을 업데이트합니다 "modifyclusteradmin API를 사용합니다".

자격 증명 유형 및 아이콘	관리자별 사용	이 지침을 참조하십시오
vSphere SSO(Single Sign-On) 자격 증명	• 는 *:NetApp HCI에만 적용됩니다 관리자는 이러한 자격 증명을 사용하여 VMware vSphere Client에 로그인합니다. vCenter가 NetApp HCI 설치의 일부인 경우 자격 증명은 다음과 같이 NetApp 배포 엔진에서 구성됩니다. • username@vsphere.loca l 에 지정된 암호 및 를 입력합니다 • administrator@vsphere.loca l 을 입력합니다. 기존 vCenter를 사용하여 NetApp HCI를 구축하면 IT VMware 관리자가 vSphere Single Sign-On 자격 증명을 관리합니다.	"vCenter 및 ESXi 자격 증명을 업데이트합니다".
베이스보드 관리 컨트롤러(BMC) 자격 증명	• 는 *:NetApp HCI에만 적용됩니다 관리자는 이러한 자격 증명을 사용하여 NetApp HCI 배포에서 NetApp 컴퓨팅 노드의 BMC에 로그인합니다. BMC는 기본 하드웨어 모니터링 및 가상 콘솔 기능을 제공합니다. 각 NetApp 컴퓨팅 노드에 대한 BMC(*IPMI* 라고도 함) 자격 증명은 NetApp HCI 배포의 mnode에 안전하게 저장됩니다. NetApp 하이브리드 클라우드 제어에서는 서비스 계정 용량의 BMC 자격 증명을 사용하여 컴퓨팅 노드 펌웨어 업그레이드 중에 컴퓨팅 노드의 BMC와 통신합니다. BMC 자격 증명이 변경되면 해당 컴퓨팅 노드의 자격 증명이 mnode에서도 업데이트되어야 모든 하이브리드 클라우드 제어 기능을 유지할 수 있습니다.	• "NetApp HCI의 각 노드에 대해 IPMI를 구성합니다". • H410C, H610C 및 H615C 노드의 경우 "기본 IPMI 암호를 변경합니다". • H410S 및 H610S 노드의 경우 "기본 IPM 암호를 변경합니다". • "관리 노드에서 BMC 자격 증명을 변경합니다".
ESXi 자격 증명	• 는 *:NetApp HCI에만 적용됩니다 관리자는 SSH 또는 로컬 루트 계정이 있는 로컬 DCUI를 사용하여 ESXi 호스트에 로그인할 수 있습니다. NetApp HCI 배포에서는 사용자 이름이 '루트'이고 NetApp 배포 엔진에서 해당 컴퓨팅 노드를 처음 설치할 때 암호를 지정했습니다. 각 NetApp 컴퓨팅 노드의 ESXi 루트 자격 증명은 NetApp HCI 구축의 mnode에 안전하게 저장됩니다. NetApp 하이브리드 클라우드 제어에서는 서비스 계정 용량의 자격 증명을 사용하여 컴퓨팅 노드 펌웨어 업그레이드 및 상태 점검 중에 ESXi 호스트와 직접 통신합니다. VMware 관리자가 ESXi 루트 자격 증명을 변경하면 하이브리드 클라우드 제어 기능을 유지하려면 해당 컴퓨팅 노드의 자격 증명을 mnode에서 업데이트해야 합니다.	"vCenter 및 ESXi 호스트에 대한 자격 증명을 업데이트합니다".

자격 증명 유형 및 아이콘	관리자별 사용	이 지침을 참조하십시오
QoS 통합 암호입니다	• 는 *:NetApp HCI에 적용되며 SolidFire에서는 선택 사항입니다 관리자의 대화형 로그인에는 사용되지 않습니다. VMware vSphere와 Element 소프트웨어 간의 QoS 통합은 다음을 통해 활성화됩니다. • vCenter Server용 Element 플러그인 및 입니다 • mnode의 QoS 서비스. 인증을 위해 QoS 서비스는 이 컨텍스트에서만 사용되는 암호를 사용합니다. QoS 암호는 vCenter Server용 Element 플러그인을 처음 설치하는 동안 또는 NetApp HCI 구축 중에 자동으로 생성되는 동안 지정됩니다. 다른 구성 요소에 영향을 주지 않습니다.	"vCenter Server용 NetApp Element 플러그인에서 QoSSIOC 자격 증명을 업데이트합니다". vCenter Server SIOC용 NetApp Element 플러그인은 _ QoSSIOC 암호 _ 라고도 합니다. https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Plug-in_for_vCenter_server/mNode_Status_shows_as_'Network_Down'_or_'Down'_in_the_mNode_Settings_tab_of_the_Element_Plugin_for_vCenter_(VCP) [vCenter Server용 Element Plug-in KB 문서^]를 검토합니다.
vCenter Service Appliance 자격 증명	• 는 NetApp 배포 엔진에서 설정한 경우에만 *:NetApp HCI에 적용됩니다 관리자는 vCenter Server 어플라이언스 가상 머신에 로그인할 수 있습니다. NetApp HCI 배포에서는 사용자 이름이 '루트'이고 NetApp 배포 엔진에서 해당 컴퓨팅 노드를 처음 설치할 때 암호를 지정했습니다. 구축된 VMware vSphere 버전에 따라 vSphere Single Sign-On 도메인의 특정 관리자도 어플라이언스에 로그인할 수 있습니다. 다른 구성 요소에 영향을 주지 않습니다.	변경할 필요가 없습니다.
NetApp 관리 노드 관리자 자격 증명	• 는 *:NetApp HCI에 적용되며 SolidFire에서는 선택 사항입니다 관리자는 NetApp 관리 노드 가상 머신에 로그인하여 고급 구성 및 문제 해결을 수행할 수 있습니다. 구축된 관리 노드 버전에 따라 SSH를 통한 로그인은 기본적으로 사용되지 않습니다. NetApp HCI 구축 시 NetApp 구축 엔진에서 해당 컴퓨팅 노드를 처음 설치할 때 사용자가 사용자 이름과 암호를 지정했습니다. 다른 구성 요소에 영향을 주지 않습니다.	변경할 필요가 없습니다.

자세한 내용을 확인하십시오

- "Element 소프트웨어 기본 SSL 인증서를 변경합니다"

- "노드의 IPMI 암호를 변경합니다"
- "다중 요소 인증을 사용합니다"
- "외부 키 관리를 시작합니다"
- "FIPS 드라이브를 지원하는 클러스터를 생성합니다"

Element 소프트웨어 기본 SSL 인증서를 변경합니다

NetApp Element API를 사용하여 클러스터에 있는 스토리지 노드의 기본 SSL 인증서 및 개인 키를 변경할 수 있습니다.

NetApp Element 소프트웨어 클러스터가 생성되면 클러스터는 Element UI, Per-Node UI 또는 API를 통해 모든 HTTPS 통신에 사용되는 고유한 자체 서명된 SSL(Secure Sockets Layer) 인증서와 개인 키를 생성합니다. Element 소프트웨어는 자체 서명된 인증서뿐만 아니라 신뢰할 수 있는 CA(인증 기관)에서 발급 및 확인되는 인증서도 지원합니다.

다음 API 메소드를 사용하여 기본 SSL 인증서에 대한 자세한 정보를 얻고 변경할 수 있습니다.

- * GetSSLCertificate *

  를 사용할 수 있습니다 "GetSSLCertificate 메서드" 모든 인증서 세부 정보를 포함하여 현재 설치된 SSL 인증서에 대한 정보를 검색합니다.

- * SetSSLCertificate *

  를 사용할 수 있습니다 "SetSSLCertificate 메서드" 클러스터 및 노드별 SSL 인증서를 사용자가 제공하는 인증서 및 개인 키로 설정합니다. 시스템은 유효하지 않은 인증서가 적용되지 않도록 인증서와 개인 키의 유효성을 검사합니다.

- * RemoveSSLCertificate * 를 선택합니다

  를 클릭합니다 "RemoveSSLCertificate 메서드입니다" 현재 설치된 SSL 인증서 및 개인 키를 제거합니다. 그런 다음 클러스터가 새로운 자체 서명된 인증서와 개인 키를 생성합니다.

> 클러스터 SSL 인증서는 클러스터에 추가된 모든 새 노드에 자동으로 적용됩니다. 클러스터에서 제거된 노드는 자체 서명된 인증서로 되돌리며 모든 사용자 정의 인증서와 키 정보가 노드에서 제거됩니다.

자세한 내용을 확인하십시오

- "관리 노드의 기본 SSL 인증서를 변경합니다"
- "Element 소프트웨어에서 사용자 정의 SSL 인증서를 설정하는 데 필요한 요구 사항은 무엇입니까?"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

노드의 기본 IPMI 암호를 변경합니다

노드에 대한 원격 IPMI 액세스 권한이 있는 즉시 기본 IPMI(Intelligent Platform Management Interface) 관리자 암호를 변경할 수 있습니다. 설치 업데이트가 있는 경우 이 작업을 수행할 수

있습니다.

노드에 대한 IPM 액세스 구성에 대한 자세한 내용은 을 참조하십시오 "각 노드에 대해 IPMI를 구성합니다".

다음 노드의 IPM 암호를 변경할 수 있습니다.

- H410S 노드
- H610S 노드

H410S 노드의 기본 **IPMI** 암호를 변경합니다

IPMI 네트워크 포트를 구성하는 즉시 각 스토리지 노드에서 IPMI 관리자 계정의 기본 암호를 변경해야 합니다.

필요한 것
각 스토리지 노드에 대해 IPMI IP 주소를 구성해야 합니다.

단계

1. IPMI 네트워크에 연결할 수 있는 컴퓨터에서 웹 브라우저를 열고 해당 노드의 IPMI IP 주소를 찾습니다.
2. 로그인 프롬프트에 사용자 이름 admin과 암호 admin을 입력합니다.
3. 로그인 시 * 구성 * 탭을 클릭합니다.
4. 사용자 * 를 클릭합니다.
5. 'admin' 사용자를 선택하고 'Modify User'를 클릭합니다.
6. 암호 변경 * 확인란을 선택합니다.
7. 암호 * 및 * 암호 확인 * 필드에 새 암호를 입력합니다.
8. 수정 * 을 클릭한 다음 * 확인 * 을 클릭합니다.
9. 기본 IPMI 암호가 있는 다른 H410S 노드에 대해 이 절차를 반복합니다.

H610S 노드의 기본 **IPMI** 암호를 변경합니다

IPMI 네트워크 포트를 구성하는 즉시 각 스토리지 노드에서 IPMI 관리자 계정의 기본 암호를 변경해야 합니다.

필요한 것
각 스토리지 노드에 대해 IPMI IP 주소를 구성해야 합니다.

단계

1. IPMI 네트워크에 연결할 수 있는 컴퓨터에서 웹 브라우저를 열고 해당 노드의 IPMI IP 주소를 찾습니다.
2. 로그인 프롬프트에 root라는 사용자 이름과 암호 calvin을 입력합니다.
3. 로그인하면 페이지 왼쪽 상단의 메뉴 탐색 아이콘을 클릭하여 측면 표시줄 서랍을 엽니다.
4. 설정 * 을 클릭합니다.
5. 사용자 관리 * 를 클릭합니다.
6. 목록에서 * Administrator * 사용자를 선택합니다.
7. 암호 변경 * 확인란을 활성화합니다.

8. 암호 * 및 * 암호 확인 * 필드에 강력한 새 암호를 입력합니다.
9. 페이지 하단의 * 저장 * 을 클릭합니다.
10. 기본 IPMI 암호가 있는 다른 H610S 노드에 대해 이 절차를 반복합니다.

자세한 내용을 확인하십시오

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

Element 소프트웨어 UI에서 기본 옵션을 사용합니다

NetApp Element 소프트웨어 웹 사용자 인터페이스(Element UI)를 사용하면 SolidFire 시스템에서 일반적인 작업을 모니터링 및 수행할 수 있습니다.

기본 옵션에는 UI 작업에 의해 활성화된 API 명령을 보고 피드백을 제공하는 것이 포함됩니다.

- "API 활동을 봅니다"
- "Element 인터페이스의 아이콘입니다"
- "피드백을 제공합니다"

를 참조하십시오

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

API 활동을 봅니다

Element 시스템은 NetApp Element API를 기능 및 기능의 기반으로 사용합니다. Element UI를 사용하면 인터페이스를 사용할 때 시스템에서 다양한 유형의 실시간 API 작업을 볼 수 있습니다. API 로그를 사용하면 사용자 시작 및 백그라운드 시스템 API 작업과 현재 보고 있는 페이지에서 수행된 API 호출을 볼 수 있습니다.

API 로그를 사용하여 특정 작업에 사용되는 API 메서드를 식별하고 API 메서드 및 개체를 사용하여 사용자 지정 응용 프로그램을 빌드하는 방법을 확인할 수 있습니다.

각 방법에 대한 자세한 내용은 을 참조하십시오 "Element 소프트웨어 API 참조입니다".

1. Element UI 탐색 모음에서 * API 로그 * 를 클릭합니다.
2. API Log 창에 표시되는 API 작업 유형을 수정하려면 다음 단계를 수행하십시오.
   a. API 요청 트래픽을 표시하려면 * 요청 * 을 선택합니다.
   b. 응답 * 을 선택하여 API 응답 트래픽을 표시합니다.
   c. 다음 중 하나를 선택하여 API 트래픽 유형을 필터링합니다.
      - * 사용자 시작 *: 이 웹 UI 세션 동안 사용자의 활동에 의한 API 트래픽.

- * 백그라운드 폴링 *: 백그라운드 시스템 작업에 의해 생성된 API 트래픽입니다.
- * 현재 페이지 *: 현재 보고 있는 페이지의 작업에 의해 생성된 API 트래픽입니다.

자세한 내용을 확인하십시오

- "Element API를 사용하여 스토리지 관리"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

클러스터 부하의 영향을 받는 인터페이스 새로 고침 비율

API 응답 시간에 따라, 클러스터는 보고 있는 NetApp Element 소프트웨어 페이지의 특정 부분에 대해 데이터 새로 고침 간격을 자동으로 조정할 수 있습니다.

브라우저에서 페이지를 다시 로드하면 새로 고침 간격이 기본값으로 재설정됩니다. 페이지의 오른쪽 상단에 있는 클러스터 이름을 클릭하여 현재 업데이트 간격을 확인할 수 있습니다. 이 간격은 서버에서 데이터가 얼마나 빨리 다시 오는지 아니라 API 요청이 얼마나 자주 이루어지는지를 제어합니다.

클러스터가 과부하 상태일 때 Element UI에서 API 요청을 대기열에 넣을 수 있습니다. 시스템이 대기 중인 API 요청에 신속하게 응답하지 않는 경우, 사용량이 많은 클러스터와 결합된 느린 네트워크 연결과 같이 시스템 응답이 상당히 지연될 수 있습니다. 로그아웃 화면으로 리디렉션되면 초기 브라우저 인증 프롬프트를 모두 끊은 후 다시 로그인할 수 있습니다. 개요 페이지로 돌아가면 브라우저에서 클러스터 자격 증명을 저장하지 않은 경우 해당 자격 증명을 묻는 메시지가 나타날 수 있습니다.

Element 인터페이스의 아이콘입니다

NetApp Element 소프트웨어 인터페이스에는 시스템 리소스에 대해 수행할 수 있는 작업을 나타내는 아이콘이 표시됩니다.

다음 표는 빠른 참조를 제공합니다.

아이콘을 클릭합니다	설명
	작업
	백업 대상
	복제 또는 복사
	삭제 또는 삭제
	편집

	필터
	페어링
	새로 고침
	복원
	에서 복원합니다
	롤백
	스냅샷

피드백을 제공합니다

UI 전체에서 액세스할 수 있는 피드백 양식을 사용하여 Element 소프트웨어 웹 사용자 인터페이스를 개선하고 UI 문제를 해결할 수 있습니다.

1. Element UI의 페이지에서 * Feedback * 버튼을 클릭합니다.
2. 요약 및 설명 필드에 관련 정보를 입력합니다.
3. 유용한 스크린샷을 첨부하십시오.
4. 이름과 이메일 주소를 입력합니다.
5. 현재 환경에 대한 데이터를 포함하려면 이 확인란을 선택합니다.
6. 제출 * 을 클릭합니다.

자세한 내용을 확인하십시오

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

계정 관리

SolidFire 스토리지 시스템에서 테넌트는 계정을 사용하여 클라이언트가 클러스터의 볼륨에 연결할 수 있도록 설정할 수 있습니다. 볼륨을 생성하면 특정 계정에 할당됩니다. SolidFire 스토리지 시스템의 클러스터 관리자 계정을 관리할 수도 있습니다.

- "CHAP를 사용하여 계정 작업"
- "클러스터 관리자 사용자 계정을 관리합니다"

를 참조하십시오

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

CHAP를 사용하여 계정 작업

SolidFire 스토리지 시스템에서 테넌트는 계정을 사용하여 클라이언트가 클러스터의 볼륨에 연결할 수 있도록 설정할 수 있습니다. 계정에는 할당된 볼륨에 액세스하는 데 필요한 CHAP(Challenge-Handshake Authentication Protocol) 인증이 포함되어 있습니다. 볼륨을 생성하면 특정 계정에 할당됩니다.

계정에는 최대 2천 개의 볼륨이 할당될 수 있지만 볼륨은 하나의 계정에만 속할 수 있습니다.

계정을 만듭니다

볼륨에 대한 액세스를 허용하는 계정을 생성할 수 있습니다.

시스템의 각 계정 이름은 고유해야 합니다.

1. Management * > * Accounts * 를 선택합니다.
2. 계정 만들기 * 를 클릭합니다.
3. 사용자 이름 * 을 입력합니다.
4. CHAP 설정 * 섹션에서 다음 정보를 입력합니다.

   > 자격 증명 필드를 비워 두면 두 암호를 자동으로 생성할 수 있습니다.

   - CHAP 노드 세션 인증을 위한 * 초기자 암호 *.
   - CHAP 노드 세션 인증을 위한 * Target Secret * 입니다.
5. 계정 만들기 * 를 클릭합니다.

계정 세부 정보를 봅니다

개별 계정의 성능 활동을 그래픽 형식으로 볼 수 있습니다.

그래프 정보는 계정에 대한 I/O 및 처리량 정보를 제공합니다. 평균 및 최대 활동 수준은 10초 보고 기간 단위로 표시됩니다. 이러한 통계에는 계정에 할당된 모든 볼륨에 대한 활동이 포함됩니다.

1. Management * > * Accounts * 를 선택합니다.
2. 계정의 작업 아이콘을 클릭합니다.
3. 세부 정보 보기 * 를 클릭합니다.

다음은 몇 가지 세부 사항입니다.

- * 상태 *: 계정 상태입니다. 가능한 값:
  - 활성: 활성 계정.
  - 잠김: 잠긴 계정입니다.
  - 제거됨: 삭제 및 삭제된 계정입니다.
- * 활성 볼륨 *: 계정에 할당된 활성 볼륨의 수입니다.
- * 압축 *: 계정에 할당된 볼륨의 압축 효율성 점수입니다.
- * 중복 제거 *: 계정에 할당된 볼륨의 중복 제거 효율성 점수입니다.
- * 씬 프로비저닝 *: 계정에 할당된 볼륨의 씬 프로비저닝 효율성 점수입니다.
- * Overall Efficiency *: 계정에 할당된 볼륨의 전체 효율성 점수입니다.

계정을 편집합니다

계정을 편집하여 상태를 변경하거나 CHAP 암호를 변경하거나 계정 이름을 수정할 수 있습니다.

계정의 CHAP 설정을 수정하거나 액세스 그룹에서 이니시에이터 또는 볼륨을 제거하면 초기자가 예기치 않게 볼륨에 액세스할 수 없게 될 수 있습니다. 볼륨 액세스가 예기치 않게 손실되지 않는지 확인하려면 계정 또는 액세스 그룹 변경의 영향을 받는 iSCSI 세션을 항상 로그아웃하고 이니시에이터 설정 및 클러스터 설정을 변경한 후 초기자가 볼륨에 다시 연결할 수 있는지 확인합니다.

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

1. Management * > * Accounts * 를 선택합니다.
2. 계정의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Edit * 를 선택합니다.
4. * 선택 사항: * 사용자 이름 * 을 편집합니다.
5. * 선택 사항: * 상태 * 드롭다운 목록을 클릭하고 다른 상태를 선택합니다.

   > 상태를 * locked * 로 변경하면 계정에 대한 모든 iSCSI 연결이 종료되고 계정에 더 이상 액세스할 수 없습니다. 계정과 연결된 볼륨은 유지되지만 볼륨은 iSCSI를 검색할 수 없습니다.

6. * 선택 사항: * CHAP 설정 * 에서 노드 세션 인증에 사용되는 * 초기자 암호 * 및 * 대상 암호 * 자격 증명을 편집합니다.

   > CHAP 설정 * 자격 증명을 변경하지 않으면 자격 증명은 그대로 유지됩니다. 자격 증명 필드를 비워두면 새 암호가 생성됩니다.

7. 변경 내용 저장 * 을 클릭합니다.

계정을 삭제합니다

더 이상 필요하지 않은 계정은 삭제할 수 있습니다.

계정을 삭제하기 전에 계정과 연결된 모든 볼륨을 삭제하고 삭제하십시오.

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

1. Management * > * Accounts * 를 선택합니다.
2. 삭제할 계정의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 선택합니다.
4. 작업을 확인합니다.

자세한 내용을 확인하십시오

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

클러스터 관리자 사용자 계정을 관리합니다

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

스토리지 클러스터 관리자 계정 유형입니다

NetApp Element 소프트웨어를 실행하는 스토리지 클러스터에 존재할 수 있는 관리자 계정은 운영 클러스터 관리자 계정과 클러스터 관리자 계정 두 가지입니다.

- * 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 관리자의 세부 정보를 봅니다

1. 클러스터 전체(LDAP가 아닌) 클러스터 관리자 계정을 생성하려면 다음 작업을 수행합니다.
   a. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.
2. 사용자 탭의 클러스터 관리자 페이지에서 다음 정보를 볼 수 있습니다.

- * ID *: 클러스터 관리자 계정에 할당된 순차 번호입니다.
- * 사용자 이름 *: 클러스터 관리자 계정을 만들 때 지정한 이름입니다.
- * 액세스 *: 사용자 계정에 할당된 사용자 권한. 가능한 값:
  - 읽기
  - 보고
  - 노드
  - 드라이브
  - 볼륨
  - 계정
  - 클러스터 관리자
  - 관리자

    ⓘ 모든 권한은 관리자 액세스 유형에 사용할 수 있습니다.
- * 유형 *: 클러스터 관리자의 유형입니다. 가능한 값:
  - 클러스터
  - LDAP를 지원합니다
- * 특성 *: 클러스터 관리자 계정이 Element API를 사용하여 생성된 경우 이 열에는 해당 방법을 사용하여 설정된 모든 이름 값 쌍이 표시됩니다.

  을 참조하십시오 "NetApp Element 소프트웨어 API 참조서".

클러스터 관리자 계정을 생성합니다

스토리지 시스템의 특정 영역에 대한 액세스를 허용하거나 제한할 수 있는 권한이 있는 새 클러스터 관리자 계정을 생성할 수 있습니다. 클러스터 관리자 계정 권한을 설정하면 시스템은 클러스터 관리자에게 할당하지 않은 모든 권한에 대해 읽기 전용 권한을 부여합니다.

LDAP 클러스터 관리자 계정을 생성하려면 시작하기 전에 클러스터에 LDAP가 구성되어 있는지 확인하십시오.

"Element 사용자 인터페이스를 사용하여 LDAP 인증을 설정합니다"

나중에 보고, 노드, 드라이브, 볼륨, 계정 및 클러스터 레벨 액세스를 지원합니다. 사용 권한을 설정하면 시스템에서 해당 수준에 대한 쓰기 권한을 할당합니다. 시스템은 사용자가 선택하지 않은 수준에 대해 관리자 사용자에게 읽기 전용 액세스 권한을 부여합니다.

나중에 시스템 관리자가 생성한 모든 클러스터 관리자 사용자 계정을 제거할 수도 있습니다. 클러스터를 생성할 때 생성한 운영 클러스터 관리자 계정은 제거할 수 없습니다.

1. 클러스터 전체(LDAP가 아닌) 클러스터 관리자 계정을 생성하려면 다음 작업을 수행합니다.
   a. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.
   b. Create Cluster Admin * 을 클릭합니다.
   c. Cluster * 사용자 유형을 선택합니다.

d. 계정의 사용자 이름과 암호를 입력하고 암호를 확인합니다.

e. 계정에 적용할 사용자 권한을 선택합니다.

f. 최종 사용자 사용권 계약에 동의하려면 확인란을 선택합니다.

g. Create Cluster Admin * 을 클릭합니다.

2. LDAP 디렉토리에 클러스터 관리자 계정을 생성하려면 다음 작업을 수행하십시오.

   a. Cluster * > * LDAP * 를 클릭합니다.

   b. LDAP 인증이 활성화되어 있는지 확인합니다.

   c. 사용자 인증 테스트 * 를 클릭하고 사용자에게 표시되는 고유 이름 또는 사용자가 구성원인 그룹 중 하나를 복사하여 나중에 붙여 넣을 수 있습니다.

   d. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.

   e. Create Cluster Admin * 을 클릭합니다.

   f. LDAP 사용자 유형을 선택합니다.

   g. 고유 이름 필드에서 텍스트 상자의 예제를 따라 사용자 또는 그룹의 전체 고유 이름을 입력합니다. 또는 이전에 복사한 고유 이름에서 붙여 넣습니다.

      고유 이름이 그룹의 일부인 경우 LDAP 서버에서 해당 그룹의 구성원인 사용자는 이 admin 계정의 권한을 갖게 됩니다.

   LDAP 클러스터 관리자 사용자 또는 그룹을 추가하려면 사용자 이름의 일반 형식은 ""LDAP:<전체 고유 이름 >""입니다.

   a. 계정에 적용할 사용자 권한을 선택합니다.

   b. 최종 사용자 사용권 계약에 동의하려면 확인란을 선택합니다.

   c. Create Cluster Admin * 을 클릭합니다.

클러스터 관리자 권한을 편집합니다

보고, 노드, 드라이브, 볼륨, 계정 및 클러스터 레벨 액세스를 지원합니다. 사용 권한을 설정하면 시스템에서 해당 수준에 대한 쓰기 권한을 할당합니다. 시스템은 사용자가 선택하지 않은 수준에 대해 관리자 사용자에게 읽기 전용 액세스 권한을 부여합니다.

1. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.
2. 편집할 클러스터 관리자의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. 계정에 적용할 사용자 권한을 선택합니다.
5. 변경 내용 저장 * 을 클릭합니다.

클러스터 관리자 계정의 암호를 변경합니다

Element UI를 사용하여 클러스터 관리자 암호를 변경할 수 있습니다.

1. 사용자 * > * 클러스터 관리자 * 를 클릭합니다.

2. 편집할 클러스터 관리자의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. 암호 변경 필드에 새 암호를 입력하고 확인합니다.
5. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

- "Element 사용자 인터페이스를 사용하여 LDAP 인증을 설정합니다"
- "LDAP를 해제합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

LDAP를 관리합니다

LDAP(Lightweight Directory Access Protocol)를 설정하여 SolidFire 스토리지에 대한 안전한 디렉터리 기반 로그인 기능을 사용할 수 있습니다. 클러스터 레벨에서 LDAP를 구성하고 LDAP 사용자 및 그룹에 권한을 부여할 수 있습니다.

LDAP를 관리하려면 기존 Microsoft Active Directory 환경을 사용하여 SolidFire 클러스터에 LDAP 인증을 설정하고 구성을 테스트해야 합니다.

IPv4와 IPv6 주소를 모두 사용할 수 있습니다.

LDAP 활성화에는 다음과 같은 고급 단계가 포함됩니다(자세한 설명 참조).

1. * LDAP 지원을 위한 완전한 사전 구성 단계 *. LDAP 인증을 구성하는 데 필요한 모든 세부 정보가 있는지 확인합니다.
2. * LDAP 인증 활성화 *. Element UI 또는 Element API를 사용합니다.
3. * LDAP 구성 검증 *. 필요에 따라 GetLdapConfiguration API 메서드를 실행하거나 Element UI를 사용하여 LCAP 구성을 확인하여 클러스터가 올바른 값으로 구성되었는지 확인합니다.
4. * LDAP 인증 테스트 * (readonly 사용자로) TestLdapAuthentication API 메서드를 실행하거나 Element UI를 사용하여 LDAP 구성이 올바른지 테스트합니다. 이 초기 테스트에는 "재로그인" 사용자의 사용자 이름 "sAMAccountName"을 사용합니다. 이렇게 하면 클러스터가 LDAP 인증에 맞게 올바르게 구성되었는지 확인하고 "재액세스 전용" 자격 증명과 액세스가 올바른지 확인할 수 있습니다. 이 단계가 실패하면 1단계부터 3단계까지 반복합니다.
5. * LDAP 인증 * 을 테스트합니다(추가할 사용자 계정으로). Element 클러스터 관리자로 추가할 사용자 계정으로 setp 4를 반복합니다. DN(dingingued name) 또는 사용자(또는 그룹)를 복사합니다. 이 DN은 6단계에서 사용됩니다.
6. * LDAP 클러스터 관리자 추가 * (LDAP 인증 테스트 단계에서 DN 복사 및 붙여넣기) Element UI 또는 AddLdapClusterAdmin API 메서드를 사용하여 적절한 액세스 수준으로 새 클러스터 관리자 사용자를 생성합니다. 사용자 이름의 경우 5단계에서 복사한 전체 DN을 붙여 넣습니다. 이렇게 하면 DN 형식이 올바르게 지정됩니다.
7. * 클러스터 관리자 액세스 테스트 *. 새로 생성한 LDAP 클러스터 admin 사용자를 사용하여 클러스터에 로그인합니다. LDAP 그룹을 추가한 경우 해당 그룹의 모든 사용자로 로그인할 수 있습니다.

LDAP 지원을 위한 사전 구성 단계를 완료합니다

Element에서 LDAP 지원을 활성화하기 전에 Windows Active Directory Server를 설정하고 다른 사전 구성 작업을 수행해야 합니다.

단계

1. Windows Active Directory Server를 설정합니다.
2. * 선택 사항: * LDAPS 지원 활성화.
3. 사용자 및 그룹을 생성합니다.
4. LDAP 디렉토리 검색에 사용할 읽기 전용 서비스 계정("sfreadonly" 등)을 생성합니다.

Element 사용자 인터페이스를 사용하여 LDAP 인증을 설정합니다

기존 LDAP 서버와의 스토리지 시스템 통합을 구성할 수 있습니다. 이를 통해 LDAP 관리자는 사용자에 대한 스토리지 시스템 액세스를 중앙에서 관리할 수 있습니다.

Element 사용자 인터페이스 또는 Element API를 사용하여 LDAP를 구성할 수 있습니다. 이 절차에서는 Element UI를 사용하여 LDAP를 구성하는 방법에 대해 설명합니다.

이 예제에서는 SolidFire에서 LDAP 인증을 구성하는 방법과 인증 유형으로 'earchAndBind'를 사용하는 방법을 보여줍니다. 이 예에서는 단일 Windows Server 2012 R2 Active Directory Server를 사용합니다.

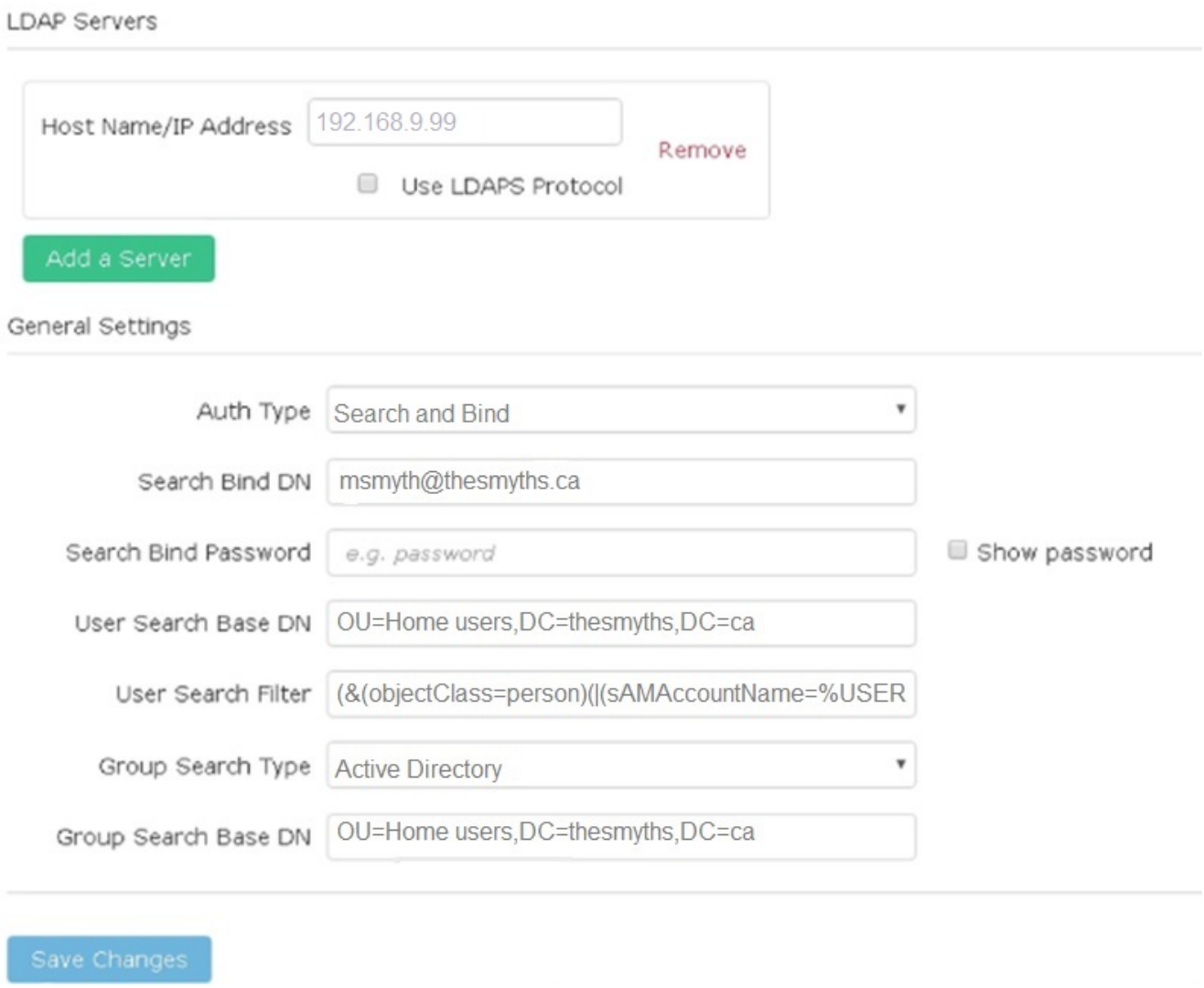
단계

1. Cluster * > * LDAP * 를 클릭합니다.
2. 예 * 를 클릭하여 LDAP 인증을 활성화합니다.
3. 서버 추가 * 를 클릭합니다.
4. 호스트 이름/IP 주소 * 를 입력합니다.

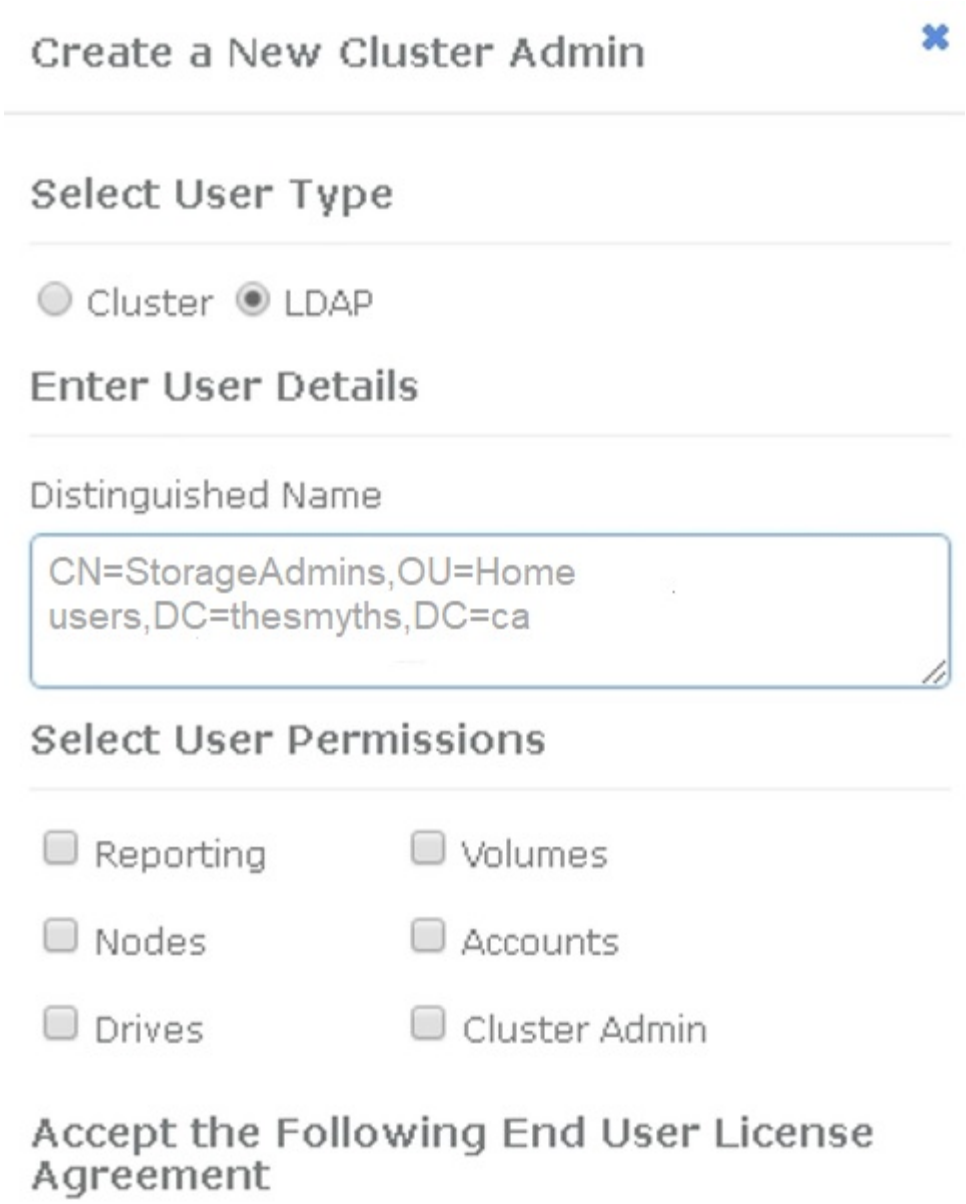
   옵션 사용자 지정 포트 번호를 입력할 수도 있습니다.

   예를 들어, 사용자 지정 포트 번호를 추가하려면 <호스트 이름 또는 IP 주소>:<포트 번호>를 입력합니다

5. * 선택 사항: * LDAPS 프로토콜 사용 * 을 선택합니다.
6. 일반 설정 * 에 필요한 정보를 입력합니다.



7. LDAP 활성화 * 를 클릭합니다.
8. 사용자에 대한 서버 액세스를 테스트하려면 * 사용자 인증 테스트 * 를 클릭합니다.
9. 클러스터 관리자를 생성할 때 나중에 사용할 수 있도록 표시되는 고유 이름 및 사용자 그룹 정보를 복사합니다.
10. 새 설정을 저장하려면 * 변경 사항 저장 * 을 클릭합니다.
11. 이 그룹에 사용자를 만들어 누구나 로그인할 수 있도록 하려면 다음을 완료합니다.
    a. 사용자 * > * 보기 * 를 클릭합니다.



b. 새 사용자의 경우 사용자 유형으로 * LDAP * 를 클릭하고 복사한 그룹을 고유 이름 필드에 붙여 넣습니다.
c. 사용 권한(일반적으로 모든 사용 권한)을 선택합니다.
d. 최종 사용자 사용권 계약까지 아래로 스크롤하여 * I accept * 를 클릭합니다.
e. Create Cluster Admin * 을 클릭합니다.

   이제 Active Directory 그룹 값을 가진 사용자가 있습니다.

이를 테스트하려면 Element UI에서 로그아웃한 후 해당 그룹의 사용자로 다시 로그인합니다.

Element API를 사용하여 **LDAP** 인증을 설정합니다

기존 LDAP 서버와의 스토리지 시스템 통합을 구성할 수 있습니다. 이를 통해 LDAP 관리자는 사용자에 대한 스토리지 시스템 액세스를 중앙에서 관리할 수 있습니다.

Element 사용자 인터페이스 또는 Element API를 사용하여 LDAP를 구성할 수 있습니다. 이 절차에서는 Element API를 사용하여 LDAP를 구성하는 방법에 대해 설명합니다.

SolidFire 클러스터에서 LDAP 인증을 활용하려면 먼저 "EnableLdapAuthentication" API 메소드를 사용하여 클러스터에서 LDAP 인증을 활성화해야 합니다.

단계

1. "EnableLdapAuthentication" API 메소드를 사용하여 클러스터에서 LDAP 인증을 먼저 설정합니다.
2. 필요한 정보를 입력합니다.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. 다음 매개 변수의 값을 변경합니다.

사용된 매개 변수	설명
AuthType: SearchAndBind	클러스터에서 인증된 사용자를 먼저 검색하고 찾은 경우 해당 사용자를 바인딩하기 위해 읽기 전용 서비스 계정을 사용하도록 지정합니다.
groupSearchBaseDN:dc=prodtest,dc=solidfire,dc=net	LDAP 트리에서 그룹 검색을 시작할 위치를 지정합니다. 이 예에서는 트리의 루트를 사용했습니다. LDAP 트리가 매우 큰 경우 검색 시간을 줄이기 위해 보다 세분화된 하위 트리로 설정할 수 있습니다.
userSearchBaseDN:dc=prodtest,dc=solidfire,dc=net	LDAP 트리에서 사용자 검색을 시작할 위치를 지정합니다. 이 예에서는 트리의 루트를 사용했습니다. LDAP 트리가 매우 큰 경우 검색 시간을 줄이기 위해 보다 세분화된 하위 트리로 설정할 수 있습니다.
groupSearchType:ActiveDirectory입니다	Windows Active Directory 서버를 LDAP 서버로 사용합니다.

사용된 매개 변수	설명

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
userPrincipalName(로그인에 대한 이메일 주소)을 사용하려면 userSearchFilter를 다음과 같이 변경합니다.
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
또는 userPrincipalName 과 sAMAccountName 을 모두 검색하려면 다음 userSearchFilter 를 사용합니다.
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%username%)(userPrincipalName=%username%))"-----

sAMAccountName을 SolidFire 클러스터에 로그인하기 위한 사용자 이름으로 활용합니다. 이 설정은 LDAP에 sAMAccountName 속성에 로그인할 때 지정된 사용자 이름을 검색하도록 하고 objectClass 속성의 값으로 ""person""이 있는 항목으로 검색을 제한합니다.	searchBindDN
LDAP 디렉토리를 검색하는 데 사용되는 읽기 전용 사용자의 고유 이름입니다. Active Directory의 경우 일반적으로 사용자에게 userPrincipalName(전자 메일 주소 형식)을 사용하는 것이 가장 쉽습니다.	searchBindPassword를 입력합니다

이를 테스트하려면 Element UI에서 로그아웃한 후 해당 그룹의 사용자로 다시 로그인합니다.

LDAP 세부 정보를 봅니다

클러스터 탭의 LDAP 페이지에서 LDAP 정보를 봅니다.

> 이러한 LDAP 구성 설정을 보려면 LDAP를 활성화해야 합니다.

1. Element UI로 LDAP 세부 정보를 보려면 * Cluster * > * LDAP * 를 클릭합니다.
   - * 호스트 이름/IP 주소 *: LDAP 또는 LDAPS 디렉토리 서버의 주소입니다.
   - * 인증 유형 *: 사용자 인증 방법. 가능한 값:
     - 직접 바인딩

    - 검색 및 바인딩
  - * Search Bind DN *: 사용자에 대한 LDAP 검색을 수행하기 위해 로그인할 수 있는 정규화된 DN(LDAP 디렉토리에 대한 바인딩 레벨 액세스 필요).
  - * 검색 바인딩 암호 *: LDAP 서버에 대한 액세스를 인증하는 데 사용되는 암호입니다.
  - * 사용자 검색 기준 DN *: 사용자 검색을 시작하는 데 사용되는 트리의 기본 DN. 시스템은 지정된 위치에서 하위 트리를 검색합니다.
  - * 사용자 검색 필터 *: 도메인 이름을 사용하여 다음을 입력합니다.

    (&(objectClass=Person) (|(sAMAccountName=%username%)(userPrincipalName=%username%)))

  - * 그룹 검색 유형 *: 사용되는 기본 그룹 검색 필터를 제어하는 검색 유형입니다. 가능한 값:
    - Active Directory: 사용자의 모든 LDAP 그룹의 중첩된 구성원
    - 그룹 없음: 그룹이 지원되지 않습니다.
    - 구성원 DN: 구성원 DN 스타일 그룹(단일 수준).
  - * 그룹 검색 기준 DN *: 그룹 검색을 시작하는 데 사용되는 트리의 기본 DN. 시스템은 지정된 위치에서 하위 트리를 검색합니다.
  - * 사용자 인증 테스트 *: LDAP가 구성된 후 이를 사용하여 LDAP 서버에 대한 사용자 이름 및 암호 인증을 테스트합니다. 이미 존재하는 계정을 입력하여 테스트합니다. 고유 이름 및 사용자 그룹 정보가 표시되며, 이 정보는 나중에 클러스터 관리자를 생성할 때 사용할 수 있도록 복사할 수 있습니다.

LDAP 구성을 테스트합니다

LDAP를 구성한 후에는 Element UI 또는 Element API 'TestLdapAuthentication' 메서드를 사용하여 LDAP를 테스트해야 합니다.

단계

1. Element UI를 사용하여 LDAP 구성을 테스트하려면 다음을 수행합니다.
   a. Cluster * > * LDAP * 를 클릭합니다.
   b. LDAP 인증 테스트 * 를 클릭합니다.
   c. 아래 표의 정보를 사용하여 문제를 해결하십시오.

오류 메시지	설명
`xLDAPUserNotFound`	• 검사 중인 사용자를 구성된 userSearchBaseDN 하위 트리에서 찾을 수 없습니다. • userSearchFilter가 잘못 설정되었다.
`xLDAPBindFailed (Error: Invalid credentials)`	• 테스트 중인 사용자 이름은 유효한 LDAP 사용자이지만 입력한 암호가 올바르지 않습니다. • 테스트 중인 사용자 이름은 유효한 LDAP 사용자이지만 계정은 현재 비활성화되어 있습니다.

오류 메시지	설명
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	LDAP 서버 URI가 잘못되었습니다.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	읽기 전용 사용자 이름 또는 암호가 잘못 구성되었습니다.
`xLDAPSearchFailed (Error: No such object)`	userSearchBaseDN은 LDAP 트리 내의 유효한 위치가 아닙니다.
`xLDAPSearchFailed (Error: Referral)`	• userSearchBaseDN은 LDAP 트리 내의 유효한 위치가 아닙니다. • userSearchBaseDN과 groupSearchBaseDN은 중첩된 OU에 있습니다. 이로 인해 권한 문제가 발생할 수 있습니다. 해결 방법은 사용자 및 그룹 기본 DN 항목에 OU를 포함하는 것입니다(예: ``ou=storage,cn=company,cn=com').

2. Element API를 사용하여 LDAP 구성을 테스트하려면 다음을 수행합니다.
   a. TestLdapAuthentication 메서드를 호출합니다.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

   b. 결과를 검토합니다. API 호출이 성공한 경우 지정된 사용자의 고유 이름과 사용자가 구성원인 그룹 목록이 결과에 포함됩니다.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

LDAP를 해제합니다

Element UI를 사용하여 LDAP 통합을 비활성화할 수 있습니다.

시작하기 전에 모든 구성 설정을 확인해야 합니다. LDAP를 비활성화하면 모든 설정이 지워지기 때문입니다.

단계

1. Cluster * > * LDAP * 를 클릭합니다.
2. 아니요 * 를 클릭합니다.
3. LDAP 비활성화 * 를 클릭합니다.

자세한 내용을 확인하십시오

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

시스템 관리

Element UI에서 시스템을 관리할 수 있습니다. 여기에는 다중 요소 인증 활성화, 클러스터 설정 관리, FIPS(Federal Information Processing Standards) 지원, 외부 키 관리 사용 등이 포함됩니다.

- "다중 요소 인증을 사용합니다"
- "클러스터 설정을 구성합니다"
- "FIPS 드라이브를 지원하는 클러스터를 생성합니다"
- "외부 키 관리를 시작합니다"

를 참조하십시오

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

다중 요소 인증을 사용합니다

MFA(Multi-factor Authentication)는 SAML(Security Assertion Markup Language)을 통해 타사 ID 공급자(IdP)를 사용하여 사용자 세션을 관리합니다. 관리자는 MFA를 사용하여 암호 및 텍스트 메시지, 암호 및 전자 메일 메시지 등 필요에 따라 추가 인증 요소를 구성할 수 있습니다.

다중 요소 인증을 설정합니다

Element API를 통해 이러한 기본 단계를 사용하여 다중 요소 인증을 사용하도록 클러스터를 설정할 수 있습니다.

각 API 메소드에 대한 자세한 내용은 에서 확인할 수 있습니다 "요소 API 참조입니다".

1. 다음 API 메서드를 호출하고 IDP 메타데이터를 JSON 형식 "CreateIdpConfiguration"으로 전달하여 클러스터에 대한 새로운 타사 ID 공급자(IDP) 구성을 생성합니다

   IDP 메타데이터는 일반 텍스트 형식으로 타사 IDP에서 검색됩니다. 이 메타데이터는 JSON으로 올바르게 포맷되었는지 확인하기 위해 유효성을 검증해야 합니다. 사용할 수 있는 JSON 포맷터 응용 프로그램은 매우 다양합니다(예: https://freeformatter.com/json-escape.html).

2. spMetadataUrl 을 통해 클러스터 메타데이터를 검색하여 다음과 같은 API 메서드('ListIdpConfigurations')를 호출하여 타사 IDP로 복사합니다

   SpMetadataUrl 은 신뢰 관계를 설정하기 위해 IDP의 클러스터에서 서비스 공급자 메타데이터를 검색하는 데 사용되는 URL입니다.

3. 타사 IDP의 SAML 어설션을 구성하여 감사 로깅을 위한 사용자를 고유하게 식별하고 단일 로그아웃이 제대로 작동하는지 ""NameID"" 속성을 포함시킵니다.
4. 다음 API 메서드('AddIdpClusterAdmin')를 호출하여 인증을 위해 타사 IDP에 의해 인증된 클러스터 관리자 사용자 계정을 하나 이상 생성합니다

   > IDP 클러스터 관리자의 사용자 이름은 다음 예와 같이 원하는 효과에 대한 SAML 속성 이름/값 매핑과 일치해야 합니다.

   - email=bob@company.com — SAML 속성에서 이메일 주소를 해제하도록 IDP가 구성된 경우.
   - group=cluster-administrator - IDP가 모든 사용자가 액세스해야 하는 그룹 속성을 해제하도록 구성되어 있습니다. SAML 속성 이름/값 페어링은 보안을 위해 대/소문자를 구분합니다.
5. 다음 API 메서드 "EnableIdpAuthentication"을 호출하여 클러스터에 대한 MFA를 활성화합니다

자세한 내용을 확인하십시오

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

다중 요소 인증에 대한 추가 정보

다중 요소 인증과 관련하여 다음과 같은 주의사항을 염두에 두어야 합니다.

- 더 이상 유효하지 않은 IDP 인증서를 새로 고치려면 비 IDP 관리자 사용자를 사용하여 다음 API 메서드('UpdateIdpConfiguration')를 호출해야 합니다
- MFA는 길이가 2048비트 미만인 인증서와 호환되지 않습니다. 기본적으로 2048비트 SSL 인증서가 클러스터에 생성됩니다. API 메소드 'setSSLCertificate'를 호출할 때는 더 작은 크기의 인증서를 설정하지 않아야 합니다

> 클러스터가 2048비트 사전 업그레이드 미만의 인증서를 사용하는 경우 Element 12.0 이상으로 업그레이드한 후 2048비트 이상의 인증서로 클러스터 인증서를 업데이트해야 합니다.

- IDP 관리 사용자는 SDK 또는 Postman을 통해 API 호출을 직접 수행하거나 다른 통합(예: OpenStack Cinder 또는 vCenter 플러그인)에 사용할 수 없습니다. 이러한 기능을 가진 사용자를 생성해야 하는 경우 LDAP 클러스터 관리자 사용자 또는 로컬 클러스터 관리자 사용자를 추가합니다.

자세한 내용을 확인하십시오

- "Element API를 사용하여 스토리지 관리"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

클러스터 설정을 구성합니다

Element UI의 Cluster 탭에서 클러스터 전체 설정을 확인 및 변경하고 클러스터별 작업을 수행할 수 있습니다.

클러스터 충만 임계값, 액세스 지원, 유휴 암호화, 가상 볼륨, SnapMirror, NTP 브로드캐스트 클라이언트도 있습니다.

옵션

- 가상 볼륨 작업
- Element 및 ONTAP 클러스터 간 SnapMirror 복제 사용
- 클러스터를 최대 임계값으로 설정합니다
- 지원 액세스를 설정 및 해제합니다
- "Element에 대해 블록 공간 임계값이 계산되는 방법"
- 클러스터에 대한 암호화를 사용하거나 사용하지 않도록 설정합니다
- 이용 약관 배너를 관리합니다
- 쿼리할 클러스터에 대한 네트워크 시간 프로토콜 서버를 구성합니다
- SNMP를 관리합니다
- 드라이브 관리
- 노드 관리
- 가상 네트워크를 관리합니다
- Fibre Channel 포트 세부 정보를 봅니다

자세한 내용을 확인하십시오

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

클러스터의 유휴 데이터 암호화를 설정 및 해제합니다

SolidFire 클러스터를 사용하면 클러스터 드라이브에 저장된 모든 유휴 데이터를 암호화할 수 있습니다. 또는 을 사용하여 SED(자체 암호화 드라이브)의 클러스터 전체 보호를 활성화할 수 있습니다 "하드웨어 또는 소프트웨어 기반의 유휴 암호화".

Element UI 또는 API를 사용하여 유휴 하드웨어 암호화를 활성화할 수 있습니다. 하드웨어 유휴 암호화 기능을 활성화해도 클러스터의 성능이나 효율에는 영향을 주지 않습니다. 사용되지 않는 소프트웨어 암호화는 Element API만 사용하여 활성화할 수 있습니다.

사용되지 않는 하드웨어 기반 암호화는 기본적으로 클러스터 생성 중에 활성화되지 않으며 Element UI에서 활성화 및 비활성화할 수 있습니다.

> SolidFire All-Flash 스토리지 클러스터의 경우, 클러스터 생성 중에 유휴 소프트웨어 암호화를 활성화해야 하며, 클러스터를 생성한 후에는 비활성화할 수 없습니다.

필요한 것

- 암호화 설정을 활성화하거나 변경할 수 있는 클러스터 관리자 권한이 있습니다.
- 저장된 하드웨어 기반 암호화의 경우 암호화 설정을 변경하기 전에 클러스터가 정상 상태인지 확인했습니다.
- 암호화를 사용하지 않도록 설정하는 경우 드라이브에서 암호화를 해제하려면 두 노드가 클러스터에 참여하고 있어야 합니다.

저장된 암호화 상태를 확인하십시오

유휴 상태의 암호화 및/또는 클러스터의 유휴 상태의 소프트웨어 암호화를 확인하려면 를 사용합니다 "GetClusterInfo 를 참조하십시오" 방법. 를 사용할 수 있습니다 "GetSoftwareEncryptionAtRestInfo 를 참조하십시오" 클러스터에서 유휴 데이터를 암호화하는 데 사용하는 정보를 가져오는 방법입니다.

> https://<MVIP>/` 의 Element 소프트웨어 UI 대시보드는 현재 하드웨어 기반 암호화에 대한 저장된 암호화 상태만 표시합니다.

옵션

- 하드웨어 기반의 유휴 암호화 활성화
- 유휴 상태의 소프트웨어 기반 암호화 사용
- 저장된 하드웨어 기반 암호화를 비활성화합니다

하드웨어 기반의 유휴 암호화 활성화

> 외부 키 관리 구성을 사용하여 유휴 데이터 암호화를 활성화하려면 를 통해 유휴 상태의 암호화를 활성화해야 합니다 "API를 참조하십시오". 기존 Element UI 버튼을 사용하여 활성화하면 내부적으로 생성된 키를 사용하는 것으로 되돌아갑니다.

1. Element UI에서 * Cluster * > * Settings * 를 선택합니다.
2. 저장 시 암호화 사용 * 을 선택합니다.

유휴 상태의 소프트웨어 기반 암호화 사용

> 클러스터에서 소프트웨어 암호화를 사용하도록 설정한 후에는 사용되지 않는 소프트웨어 암호화를 해제할 수 없습니다.

1. 클러스터를 생성하는 동안 를 실행합니다 "클러스터 생성 방법" enableSoftwareEncryptionAtRest가 true로 설정되어 있습니다.

저장된 하드웨어 기반 암호화를 비활성화합니다

1. Element UI에서 * Cluster * > * Settings * 를 선택합니다.
2. 저장 시 암호화 비활성화 * 를 선택합니다.

자세한 내용을 확인하십시오

- "SolidFire 및 Element 소프트웨어 설명서"
- "이전 버전의 NetApp SolidFire 및 Element 제품에 대한 문서"

클러스터를 최대 임계값으로 설정합니다

아래 단계를 사용하여 시스템에서 블록 클러스터 충만 경고를 생성하는 레벨을 변경할 수 있습니다. 또한 ModifyClusterFullThreshold API 메서드를 사용하여 시스템에서 블록 또는 메타데이터 경고를 생성하는 수준을 변경할 수 있습니다.

필요한 것

클러스터 관리자 권한이 있어야 합니다.

단계

1. Cluster * > * Settings * 를 클릭합니다.
2. 클러스터 전체 설정 섹션에서 Helix가 노드 장애로부터 복구할 수 없을 때 _ %용량이 남아 있을 때 * 경고 알림 발생에 백분율을 입력합니다 *.
3. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

"Element에 대해 블록 공간 임계값이 계산되는 방법"

지원 액세스를 설정 및 해제합니다

문제 해결을 위해 SSH를 통해 NetApp 지원 담당자가 스토리지 노드에 액세스하도록 일시적으로 지원 액세스를 설정할 수 있습니다.

지원 액세스를 변경하려면 클러스터 관리자 권한이 있어야 합니다.

1. Cluster * > * Settings * 를 클릭합니다.
2. 지원 액세스 사용/사용 안 함 섹션에서 지원 액세스를 허용할 기간(시간)을 입력합니다.
3. 지원 액세스 사용 * 을 클릭합니다.
4. * 선택 사항: * 지원 액세스를 비활성화하려면 * 지원 액세스 비활성화 * 를 클릭합니다.

이용 약관 배너를 관리합니다

사용자에 대한 메시지가 포함된 배너를 설정, 편집 또는 구성할 수 있습니다.

옵션

사용 약관 배너를 활성화합니다 이용 약관 배너를 편집합니다 사용 약관 배너를 사용하지 않도록 설정합니다

사용 약관 배너를 활성화합니다

사용자가 Element UI에 로그인할 때 표시되는 사용 약관 배너를 활성화할 수 있습니다. 사용자가 배너를 클릭하면 클러스터에 대해 구성한 메시지가 포함된 텍스트 대화 상자가 나타납니다. 배너는 언제든지 해제할 수 있습니다.

사용 약관 기능을 활성화하려면 클러스터 관리자 권한이 있어야 합니다.

1. 사용자 * > * 이용 약관 * 을 클릭합니다.
2. [사용 약관] * 양식에서 [사용 약관] 대화상자에 표시할 텍스트를 입력합니다.

   4096자를 초과하지 마십시오.

3. 사용 * 을 클릭합니다.

이용 약관 배너를 편집합니다

사용자가 이용 약관 로그인 배너를 선택하면 표시되는 텍스트를 편집할 수 있습니다.

필요한 것

- 사용 약관을 구성하려면 클러스터 관리자 권한이 있어야 합니다.
- 사용 약관 기능이 활성화되어 있는지 확인합니다.

단계

1. 사용자 * > * 이용 약관 * 을 클릭합니다.
2. 사용 약관 * 대화 상자에서 표시할 텍스트를 편집합니다.

   4096자를 초과하지 마십시오.

3. 변경 내용 저장 * 을 클릭합니다.

사용 약관 배너를 사용하지 않도록 설정합니다

이용 약관 배너를 사용하지 않도록 설정할 수 있습니다. 배너가 비활성화된 경우 사용자는 더 이상 Element UI를 사용할 때 사용 약관에 동의하도록 요청되지 않습니다.

필요한 것

- 사용 약관을 구성하려면 클러스터 관리자 권한이 있어야 합니다.
- 사용 약관이 활성화되어 있는지 확인합니다.

단계

1. 사용자 * > * 이용 약관 * 을 클릭합니다.
2. 비활성화 * 를 클릭합니다.

네트워크 시간 프로토콜을 설정합니다

NTP(네트워크 시간 프로토콜)는 두 가지 방법 중 하나로 설정할 수 있습니다. 즉, 클러스터의 각 노드에 브로드캐스트를 청취하도록 지시하거나 각 노드에 업데이트를 쿼리하도록 지시하십시오.

NTP는 네트워크를 통해 시계를 동기화하는 데 사용됩니다. 내부 또는 외부 NTP 서버에 대한 연결은 초기 클러스터 설정의 일부여야 합니다.

쿼리할 클러스터에 대한 네트워크 시간 프로토콜 서버를 구성합니다

클러스터의 각 노드에 업데이트를 위해 NTP(Network Time Protocol) 서버를 쿼리하도록 지정할 수 있습니다. 클러스터가 구성된 서버에만 접속하여 NTP 정보를 요청합니다.

로컬 NTP 서버를 가리키도록 클러스터의 NTP를 구성합니다. IP 주소 또는 FQDN 호스트 이름을 사용할 수 있습니다. 클러스터 생성 시 기본 NTP 서버가 us.pool.ntp.org 으로 설정되지만 SolidFire 클러스터의 물리적 위치에 따라 이 사이트에 연결할 수 없는 경우도 있습니다.

FQDN 사용은 개별 스토리지 노드의 DNS 설정이 제대로 설정되어 있고 작동 중인지 여부에 따라 달라집니다. 이렇게 하려면 모든 스토리지 노드에서 DNS 서버를 구성하고 네트워크 포트 요구 사항 페이지를 검토하여 포트가 열려 있는지 확인합니다.

최대 5개의 서로 다른 NTP 서버를 입력할 수 있습니다.

> IPv4와 IPv6 주소를 모두 사용할 수 있습니다.

필요한 것

이 설정을 구성하려면 클러스터 관리자 권한이 있어야 합니다.

단계

1. 서버 설정에서 IP 및/또는 FQDN 목록을 구성합니다.
2. DNS가 노드에 올바르게 설정되었는지 확인합니다.
3. Cluster * > * Settings * 를 클릭합니다.
4. Network Time Protocol Settings(네트워크 시간 프로토콜 설정)에서 표준 NTP 구성을 사용하는 * No *(아니요 *)를 선택합니다.
5. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

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

클러스터가 **NTP** 브로드캐스트를 수신하도록 구성합니다

브로드캐스트 모드를 사용하면 클러스터의 각 노드에 특정 서버의 NTP(Network Time Protocol) 브로드캐스트 메시지를 위해 네트워크에서 수신 대기하도록 지시할 수 있습니다.

필요한 것

- 이 설정을 구성하려면 클러스터 관리자 권한이 있어야 합니다.
- 네트워크에서 NTP 서버를 브로드캐스트 서버로 구성해야 합니다.

단계

1. Cluster * > * Settings * 를 클릭합니다.
2. 브로드캐스트 모드를 사용하는 NTP 서버를 서버 목록에 입력합니다.
3. 네트워크 시간 프로토콜 설정에서 * 예 * 를 선택하여 브로드캐스트 클라이언트를 사용합니다.
4. 브로드캐스트 클라이언트를 설정하려면 * Server * 필드에 브로드캐스트 모드로 구성한 NTP 서버를 입력합니다.
5. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

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

SNMP를 관리합니다

클러스터에서 SNMP(Simple Network Management Protocol)를 구성할 수 있습니다.

SNMP 요청자를 선택하고, 사용할 SNMP 버전을 선택하고, USM(사용자 기반 보안 모델) 사용자를 식별하고, SolidFire 클러스터를 모니터링하기 위한 트랩을 구성할 수 있습니다. 관리 정보 기반 파일을 보고 액세스할 수도 있습니다.

> IPv4와 IPv6 주소를 모두 사용할 수 있습니다.

SNMP 세부 정보

Cluster 탭의 SNMP 페이지에서 다음 정보를 볼 수 있습니다.

- SNMP MIB *

  보거나 다운로드할 수 있는 MIB 파일입니다.

- * 일반 SNMP 설정 *

  SNMP를 설정하거나 해제할 수 있습니다. SNMP를 활성화한 후 사용할 버전을 선택할 수 있습니다. 버전 2를

사용하는 경우 요청자를 추가할 수 있고 버전 3을 사용하는 경우 USM 사용자를 설정할 수 있습니다.

- * SNMP 트랩 설정 *

  캡처할 트랩을 식별할 수 있습니다. 각 트랩 수신자에 대해 호스트, 포트 및 커뮤니티 문자열을 설정할 수 있습니다.

SNMP 요청자를 구성합니다

SNMP 버전 2가 활성화되면 요청자를 활성화 또는 비활성화하고 요청자가 승인된 SNMP 요청을 받도록 구성할 수 있습니다.

1. MENU: Cluster [SNMP] 를 클릭합니다.
2. 일반 SNMP 설정 * 에서 * 예 * 를 클릭하여 SNMP를 활성화합니다.
3. 버전 * 목록에서 * 버전 2 * 를 선택합니다.
4. 요청자 * 섹션에서 * 커뮤니티 문자열 * 및 * 네트워크 * 정보를 입력합니다.

   기본적으로 커뮤니티 문자열은 public이며 네트워크는 localhost입니다. 이러한 기본 설정을 변경할 수 있습니다.

5. * 선택 사항: * 다른 요청자를 추가하려면 * 요청자 추가 * 를 클릭하고 * 커뮤니티 문자열 * 및 * 네트워크 * 정보를 입력합니다.
6. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

- SNMP 트랩을 구성합니다
- 관리 정보 기준 파일을 사용하여 관리되는 개체 데이터를 봅니다

SNMP USM 사용자를 구성합니다

SNMP 버전 3을 설정하는 경우 USM 사용자가 승인된 SNMP 요청을 수신하도록 구성해야 합니다.

1. Cluster * > * SNMP * 를 클릭합니다.
2. 일반 SNMP 설정 * 에서 * 예 * 를 클릭하여 SNMP를 활성화합니다.
3. 버전 * 목록에서 * 버전 3 * 을 선택합니다.
4. USM Users * 섹션에서 이름, 암호 및 암호를 입력합니다.
5. * 선택 사항: * 다른 USM 사용자를 추가하려면 * USM 사용자 추가 * 를 클릭하고 이름, 암호 및 암호를 입력합니다.
6. 변경 내용 저장 * 을 클릭합니다.

SNMP 트랩을 구성합니다

시스템 관리자는 알림이라고도 하는 SNMP 트랩을 사용하여 SolidFire 클러스터의 상태를 모니터링할 수 있습니다.

SNMP 트랩이 설정되면 SolidFire 클러스터는 이벤트 로그 항목 및 시스템 경고와 관련된 트랩을 생성합니다. SNMP 알림을 수신하려면 생성해야 하는 트랩을 선택하고 트랩 정보의 수신자를 식별해야 합니다. 기본적으로 트랩은 생성되지 않습니다.

1. Cluster * > * SNMP * 를 클릭합니다.
2. 시스템에서 생성해야 하는 * SNMP Trap Settings * 섹션에서 트랩 유형을 하나 이상 선택합니다.
   - 클러스터 오류 트랩
   - 클러스터에서 해결된 장애 트랩입니다
   - 클러스터 이벤트 트랩
3. Trap Recipients* 섹션에서 받는 사람에 대한 호스트, 포트 및 커뮤니티 문자열 정보를 입력합니다.
4. * 선택 사항 *: 다른 트랩 수신자를 추가하려면 * 트랩 수신자 추가 * 를 클릭하고 호스트, 포트 및 커뮤니티 문자열 정보를 입력합니다.
5. 변경 내용 저장 * 을 클릭합니다.

관리 정보 기준 파일을 사용하여 관리되는 개체 데이터를 봅니다

관리되는 각 개체를 정의하는 데 사용되는 MIB(Management Information Base) 파일을 보고 다운로드할 수 있습니다. SNMP 기능은 SolidFire-StorageCluster-MIB에 정의된 객체에 대한 읽기 전용 액세스를 지원합니다.

MIB에 제공된 통계 데이터는 다음에 대한 시스템 활동을 보여줍니다.

- 클러스터 통계
- 볼륨 통계
- 계정 통계별 볼륨
- 노드 통계
- 보고서, 오류 및 시스템 이벤트와 같은 기타 데이터

또한 이 시스템은 SF 시리즈 제품에 대한 상위 수준의 액세스 포인트(OID)가 포함된 MIB 파일에 대한 액세스를 지원합니다.

단계

1. Cluster * > * SNMP * 를 클릭합니다.
2. SNMP MIB * 에서 다운로드할 MIB 파일을 클릭합니다.
3. 다운로드 창이 나타나면 MIB 파일을 열거나 저장합니다.

드라이브 관리

각 노드에는 클러스터의 데이터 일부를 저장하는 데 사용되는 하나 이상의 물리적 드라이브가 포함됩니다. 클러스터가 드라이브를 클러스터에 성공적으로 추가한 후 드라이브의 용량과 성능을 활용합니다. Element UI를 사용하여 드라이브를 관리할 수 있습니다.

를 참조하십시오

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

드라이브 세부 정보

클러스터 탭의 드라이브 페이지에는 클러스터의 활성 드라이브 목록이 표시됩니다. Active(활성), Available(사용 가능), Removing(제거), Erasing(삭제) 및 Failed(실패) 탭에서 선택하여 페이지를 필터링할 수 있습니다.

클러스터를 처음 초기화하면 활성 드라이브 목록이 비어 있습니다. 새 SolidFire 클러스터가 생성된 후 클러스터에 할당되지 않고 Available 탭에 나열된 드라이브를 추가할 수 있습니다.

다음 요소가 활성 드라이브 목록에 나타납니다.

- * 드라이브 ID *

  드라이브에 할당된 일련 번호입니다.

- * 노드 ID *

  노드가 클러스터에 추가될 때 할당된 노드 번호입니다.

- * 노드 이름 *

  드라이브가 들어 있는 노드의 이름입니다.

- * 슬롯 *

  드라이브가 물리적으로 위치한 슬롯 번호입니다.

- * 용량 *

  드라이브 크기(GB)입니다.

- * 직렬 *

  드라이브의 일련 번호입니다.

- * 남은 마모 *

  마모 수준 표시기.

  스토리지 시스템은 데이터 쓰기 및 삭제를 위해 각 SSD(Solid State Drive)에서 사용 가능한 대략적인 마모 양을 보고합니다. 설계된 쓰기 및 지우기 주기의 5%를 사용한 드라이브의 마모 잔여량은 95%입니다. 시스템에서 드라이브 마모 정보를 자동으로 새로 고치지 않습니다. 페이지를 새로 고치거나 닫고 다시 로드하여 정보를 새로 고칠 수 있습니다.

- * 유형 *

  드라이브 유형입니다. 형식은 블록 또는 메타데이터일 수 있습니다.

노드 관리

클러스터 탭의 노드 페이지에서 SolidFire 스토리지 및 파이버 채널 노드를 관리할 수 있습니다.

새로 추가된 노드가 전체 클러스터 용량의 50% 이상을 차지하는 경우 이 노드의 일부 용량을 사용할 수 없게 되어 용량 규칙을 준수합니다("고립됨"). 이는 더 많은 스토리지가 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.

자세한 내용을 확인하십시오

클러스터에 노드를 추가합니다

클러스터에 노드를 추가합니다

더 많은 스토리지가 필요하거나 클러스터를 생성한 후에 클러스터에 노드를 추가할 수 있습니다. 노드의 전원을 처음 켤 때는 초기 구성이 필요합니다. 노드가 구성되면 보류 중인 노드 목록에 나타나고 클러스터에 추가할 수 있습니다.

클러스터의 각 노드에 있는 소프트웨어 버전이 호환되어야 합니다. 클러스터에 노드를 추가하면 클러스터는 필요에 따라 새 노드에 NetApp Element 소프트웨어의 클러스터 버전을 설치합니다.

기존 클러스터에 용량을 작거나 큰 노드를 추가할 수 있습니다. 클러스터에 더 큰 노드 용량을 추가하여 용량을 확장할 수 있습니다. 더 작은 노드를 포함하는 클러스터에 더 큰 노드를 쌍으로 추가해야 합니다. 따라서 큰 노드 중 하나에 장애가 발생할 경우 이중 Helix가 데이터를 이동할 수 있는 충분한 공간이 확보됩니다. 더 작은 노드 용량을 더 큰 노드 클러스터에 추가하여 성능을 향상할 수 있습니다.

> 새로 추가된 노드가 전체 클러스터 용량의 50% 이상을 차지하는 경우 이 노드의 일부 용량을 사용할 수 없게 되어 용량 규칙을 준수합니다("고립됨"). 이는 더 많은 스토리지가 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 strandedCapacity 클러스터 장애가 throw됩니다.

"NetApp 비디오: 기업 요건에 맞게 확장: SolidFire 클러스터 확장"

NetApp HCI 어플라이언스에 노드를 추가할 수 있습니다.

단계

1. 클러스터 * > * 노드 * 를 선택합니다.
2. 보류 중인 노드 목록을 보려면 * Pending * (보류 중 *)을 클릭합니다.

   노드 추가 프로세스가 완료되면 활성 노드 목록에 나타납니다. 그 때까지 보류 중인 노드가 보류 중인 활성 목록에 나타납니다.

   SolidFire는 클러스터에 추가할 때 보류 중인 노드에 클러스터의 Element 소프트웨어 버전을 설치합니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

3. 다음 중 하나를 수행합니다.
   - 개별 노드를 추가하려면 추가할 노드에 대한 * 작업 * 아이콘을 클릭합니다.
   - 여러 노드를 추가하려면 추가할 노드의 확인란을 선택한 다음 * 대량 작업 * 을 선택합니다. * 참고: * 추가하려는

노드에 클러스터에서 실행 중인 버전과 다른 버전의 Element 소프트웨어가 있는 경우 클러스터는 노드를 클러스터 마스터에서 실행 중인 Element 소프트웨어 버전으로 비동기식으로 업데이트합니다. 노드가 업데이트되면 자동으로 클러스터에 추가됩니다. 이 비동기 프로세스 중에 노드는 pendingActive 상태가 됩니다.

4. 추가 * 를 클릭합니다.

   노드가 활성 노드 목록에 나타납니다.

자세한 내용을 확인하십시오

노드 버전 관리 및 호환성

노드 버전 관리 및 호환성

노드 호환성은 노드에 설치된 Element 소프트웨어 버전을 기반으로 합니다. Element 소프트웨어 기반 스토리지 클러스터는 노드와 클러스터가 호환되는 버전이 아닌 경우 자동으로 클러스터의 Element 소프트웨어 버전으로 노드를 이미징합니다.

다음 목록에는 Element 소프트웨어 버전 번호를 구성하는 소프트웨어 릴리스의 중요성 수준이 설명되어 있습니다.

- * 주 *

  첫 번째 숫자는 소프트웨어 릴리스를 나타냅니다. 주요 패치 번호가 1개인 노드는 다른 주요 패치 번호의 노드가 포함된 클러스터에 추가할 수 없으며, 주요 버전이 혼합된 노드를 사용하여 클러스터를 생성할 수도 없습니다.

- * 보조 *

  두 번째 숫자는 주요 릴리스에 추가된 기존 소프트웨어 기능의 향상 또는 소프트웨어 기능의 축소 기능을 나타냅니다. 이 구성 요소는 주 버전 구성 요소 내에서 증가하여 이 증분 릴리스가 다른 부 구성 요소의 다른 Element 소프트웨어 증분 릴리스와 호환되지 않음을 나타냅니다. 예를 들어 11.0은 11.1과 호환되지 않으며 11.1은 11.2와 호환되지 않습니다.

- 마이크로 *

  세 번째 숫자는 major.minor 구성 요소가 나타내는 Element 소프트웨어 버전과 호환되는 패치(증분 릴리스)를 나타냅니다. 예를 들어 11.0.1은 11.0.2와 호환되고 11.0.2는 11.0.3과 호환됩니다.

주 버전 번호와 부 버전 번호는 호환성을 위해 일치해야 합니다. 마이크로 번호는 호환성을 위해 일치하지 않아도 됩니다.

혼합 노드 환경의 클러스터 용량

클러스터에서 여러 유형의 노드를 혼합할 수 있습니다. SF-시리즈 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 및 H 시리즈는 하나의 클러스터에 공존할 수 있습니다.

H-Series는 H610S-1, H610S-2, H610S-4 및 H410S 노드로 구성됩니다. 이러한 노드는 10GbE와 25GbE 모두 지원합니다.

암호화되지 않은 노드와 암호화된 노드를 혼합하지 않는 것이 가장 좋습니다. 혼합 노드 클러스터에서 노드는 총 클러스터 용량의 33%를 초과할 수 없습니다. 예를 들어, 4개의 SF-Series 4805 노드가 있는 클러스터에서 단독으로 추가할 수 있는 가장 큰 노드는 SF-Series 9605입니다. 클러스터 용량 임계값은 이 상황에서 최대 노드의 잠재적 손실을

기준으로 계산됩니다.

Element 12.0부터 다음 SF 시리즈 스토리지 노드는 지원되지 않습니다.

- SF3010
- SF6010
- SF9010

이러한 스토리지 노드 중 하나를 Element 12.0으로 업그레이드하면 이 노드가 Element 12.0에서 지원되지 않는다는 오류가 표시됩니다.

노드 세부 정보를 봅니다

활용률과 드라이브 통계를 위해 서비스 태그, 드라이브 세부 정보 및 그래픽과 같은 개별 노드에 대한 세부 정보를 볼 수 있습니다. 클러스터 탭의 노드 페이지에는 각 노드의 소프트웨어 버전을 볼 수 있는 버전 열이 있습니다.

단계

1. 클러스터 * > * 노드 * 를 클릭합니다.
2. 특정 노드에 대한 세부 정보를 보려면 노드에 대한 * 작업 * 아이콘을 클릭합니다.
3. 세부 정보 보기 * 를 클릭합니다.
4. 노드 세부 정보 검토:
    - * 노드 ID *: 노드에 대해 시스템에서 생성한 ID입니다.
    - * 노드 이름 *: 노드의 호스트 이름입니다.
    - * 사용 가능한 4K IOPS *: 노드에 대해 구성된 IOPS
    - * 노드 역할 *: 클러스터에 있는 노드의 역할. 가능한 값:
        - Cluster Master: 클러스터 전체 관리 작업을 수행하고 MVIP 및 SVIP를 포함하는 노드입니다.
        - 앙상블 노드: 클러스터에 참여하는 노드. 클러스터 크기에 따라 3개 또는 5개의 앙상블 노드가 있습니다.
        - Fibre Channel: 클러스터의 노드
    - * 노드 유형 *: 노드의 모델 유형입니다.
    - * 활성 드라이브 *: 노드의 활성 드라이브 수입니다.
    - * 관리 IP *: 1GbE 또는 10GbE 네트워크 관리 작업을 위해 노드에 할당된 관리 IP(MIP) 주소입니다.
    - * 클러스터 IP *: 동일한 클러스터의 노드 간 통신에 사용되는 노드에 할당된 클러스터 IP(CIP) 주소입니다.
    - * 스토리지 IP *: iSCSI 네트워크 검색 및 모든 데이터 네트워크 트래픽에 사용되는 노드에 할당된 SIP(스토리지 IP) 주소입니다.
    - * 관리 VLAN ID *: 관리 로컬 영역 네트워크의 가상 ID입니다.
    - * 스토리지 VLAN ID *: 스토리지 로컬 영역 네트워크의 가상 ID입니다.
    - * 버전 *: 각 노드에서 실행되는 소프트웨어 버전.
    - * 복제 포트 *: 원격 복제를 위해 노드에서 사용되는 포트입니다.
    - * 서비스 태그 *: 노드에 할당된 고유한 서비스 태그 번호입니다.

Fibre Channel 포트 세부 정보를 봅니다

FC 포트 페이지에서 상태, 이름 및 포트 주소와 같은 파이버 채널 포트의 세부 정보를 볼 수 있습니다.

클러스터에 연결된 파이버 채널 포트에 대한 정보를 봅니다.

단계

1. Cluster * > * FC Ports * 를 클릭합니다.
2. 이 페이지의 정보를 필터링하려면 * 필터 * 를 클릭합니다.
3. 세부 정보 검토:
    - * 노드 ID *: 연결을 위해 세션을 호스팅하는 노드입니다.
    - * 노드 이름 *: 시스템에서 생성한 노드 이름
    - * Slot *: Fibre Channel 포트가 있는 슬롯 번호입니다.
    - * HBA 포트 *: Fibre Channel 호스트 버스 어댑터(HBA)의 물리적 포트
    - * WWNN *: 전 세계 노드 이름입니다.
    - * WWPN *: 타겟 전 세계 포트 이름입니다.
    - * 스위치 WWN *: Fibre Channel 스위치의 전 세계 이름입니다.
    - * 포트 상태 *: 포트의 현재 상태입니다.
    - * nport ID *: Fibre Channel 패브릭의 노드 포트 ID입니다.
    - * Speed *: 협상된 파이버 채널 속도입니다. 가능한 값은 다음과 같습니다.
        - 4Gbps
        - 8Gbps
        - 16Gbps

자세한 내용을 확인하십시오

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

가상 네트워크를 관리합니다

SolidFire 스토리지의 가상 네트워킹을 사용하면 별도의 논리 네트워크에 있는 여러 클라이언트 간의 트래픽을 하나의 클러스터에 연결할 수 있습니다. 클러스터에 대한 연결은 VLAN 태그 지정을 사용하여 네트워킹 스택에서 분리됩니다.

자세한 내용을 확인하십시오

- 가상 네트워크를 추가합니다
- 가상 라우팅 및 전달을 활성화합니다
- 가상 네트워크를 편집합니다

- VRF VLAN을 편집합니다
- 가상 네트워크를 삭제합니다

가상 네트워크를 추가합니다

새 가상 네트워크를 클러스터 구성에 추가하여 Element 소프트웨어를 실행하는 클러스터에 멀티테넌트 환경 연결을 설정할 수 있습니다.

필요한 것

- 클러스터 노드의 가상 네트워크에 할당될 IP 주소 블록을 식별합니다.
- 모든 NetApp Element 스토리지 트래픽의 엔드포인트로 사용될 스토리지 네트워크 IP(SVIP) 주소를 식별합니다.

> 이 구성에 대해 다음 기준을 고려해야 합니다.

- VRF를 지원하지 않는 VLAN은 이니시에이터가 SVIP와 동일한 서브넷에 있어야 합니다.
- VRF를 사용하는 VLAN은 이니시에이터가 SVIP와 동일한 서브넷에 있지 않아도 되며 라우팅이 지원됩니다.
- 기본 SVIP에서는 이니시에이터가 SVIP와 동일한 서브넷에 있지 않아도 되며 라우팅이 지원됩니다.

가상 네트워크가 추가되면 각 노드에 대한 인터페이스가 생성되고 각 노드에 가상 네트워크 IP 주소가 필요합니다. 새 가상 네트워크를 생성할 때 지정하는 IP 주소 수는 클러스터의 노드 수보다 크거나 같아야 합니다. 가상 네트워크 주소는 에서 대량으로 프로비저닝되고 개별 노드에 자동으로 할당됩니다. 클러스터의 노드에 가상 네트워크 주소를 수동으로 할당할 필요는 없습니다.

단계

1. Cluster * > * Network * 를 클릭합니다.
2. VLAN 만들기 * 를 클릭합니다.
3. 새 VLAN 만들기 * 대화 상자에서 다음 필드에 값을 입력합니다.
   - * VLAN 이름 *
   - VLAN 태그 *
   - * SVIP *
   - 넷마스크 *
   - (선택 사항) * 설명 *
4. IP 주소 범위의 * 시작 IP * 주소를 * IP 주소 블록 * 에 입력합니다.
5. IP 범위의 * Size * 를 블록에 포함할 IP 주소 수로 입력합니다.
6. 이 VLAN에 대해 비연속 IP 주소 블록을 추가하려면 * 블록 추가 * 를 클릭합니다.
7. VLAN 만들기 * 를 클릭합니다.

가상 네트워크 세부 정보를 봅니다

단계

1. Cluster * > * Network * 를 클릭합니다.
2. 세부 정보를 검토합니다.

- * ID *: 시스템에서 할당한 VLAN 네트워크의 고유 ID입니다.
- * 이름 *: VLAN 네트워크의 고유한 사용자 할당 이름입니다.
- * VLAN 태그 *: 가상 네트워크를 만들 때 할당된 VLAN 태그.
- * SVIP *: 가상 네트워크에 할당된 스토리지 가상 IP 주소입니다.
- * 넷마스크 *: 이 가상 네트워크의 넷마스크입니다.
- * 게이트웨이 *: 가상 네트워크 게이트웨이의 고유 IP 주소입니다. VRF가 활성화되어 있어야 합니다.
- * VRF 사용 *: 가상 라우팅 및 전달 활성화 여부를 나타냅니다.
- 사용된 IP *: 가상 네트워크에 사용되는 가상 네트워크 IP 주소의 범위입니다.

가상 라우팅 및 전달을 활성화합니다

VRF(Virtual Routing and Forwarding)를 활성화하면 라우팅 테이블의 여러 인스턴스가 라우터에 존재하고 동시에 작동할 수 있습니다. 이 기능은 스토리지 네트워크에서만 사용할 수 있습니다.

VLAN을 생성할 때만 VRF를 활성화할 수 있습니다. 비 VRF로 다시 전환하려면 VLAN을 삭제하고 다시 생성해야 합니다.

1. Cluster * > * Network * 를 클릭합니다.
2. 새 VLAN에서 VRF를 활성화하려면 * VLAN 생성 * 을 선택합니다.
   a. 새 VRF/VLAN에 대한 관련 정보를 입력합니다. 가상 네트워크 추가 를 참조하십시오.
   b. VRF * 활성화 확인란을 선택합니다.
   c. * 선택 사항 *: 게이트웨이를 입력합니다.
3. VLAN 만들기 * 를 클릭합니다.

자세한 내용을 확인하십시오

가상 네트워크를 추가합니다

가상 네트워크를 편집합니다

VLAN 이름, 넷마스크, IP 주소 블록의 크기 등과 같은 VLAN 특성을 변경할 수 있습니다. VLAN 태그 및 SVIP는 VLAN에 대해 수정할 수 없습니다. 게이트웨이 속성은 비 VRF VLAN에 대해 유효한 매개 변수가 아닙니다.

iSCSI, 원격 복제 또는 기타 네트워크 세션이 있으면 수정이 실패할 수 있습니다.

VLAN IP 주소 범위의 크기를 관리할 때 다음과 같은 제한 사항을 확인해야 합니다.

- VLAN을 생성할 때 할당된 초기 IP 주소 범위에서만 IP 주소를 제거할 수 있습니다.
- 초기 IP 주소 범위 이후에 추가된 IP 주소 블록을 제거할 수 있지만 IP 주소를 제거하여 IP 블록의 크기를 조정할 수는 없습니다.
- 클러스터의 노드에서 사용 중인 IP 주소 범위 또는 IP 블록에서 IP 주소를 제거하려고 하면 작업이 실패할 수 있습니다.

- 특정 사용 중인 IP 주소를 클러스터의 다른 노드에 재할당할 수 없습니다.

다음 절차에 따라 IP 주소 블록을 추가할 수 있습니다.

1. Cluster * > * Network * 를 선택합니다.
2. 편집할 VLAN의 작업 아이콘을 선택합니다.
3. 편집 * 을 선택합니다.
4. VLAN 편집 * 대화 상자에서 VLAN에 대한 새 속성을 입력합니다.
5. 가상 네트워크에 대해 비연속 IP 주소 블록을 추가하려면 * 블록 추가 * 를 선택합니다.
6. 변경 내용 저장 * 을 선택합니다.

KB 문서 문제 해결 링크

VLAN IP 주소 범위 관리와 관련된 문제를 해결하는 데 도움이 되는 기술 문서 링크

- "Element 클러스터의 VLAN에 스토리지 노드를 추가한 후 중복 IP 경고가 발생합니다"
- "사용 중인 VLAN IP와 해당 IP가 Element에 할당된 노드를 확인하는 방법"

VRF VLAN을 편집합니다

VLAN 이름, 넷마스크, 게이트웨이 및 IP 주소 블록과 같은 VRF VLAN 속성을 변경할 수 있습니다.

1. Cluster * > * Network * 를 클릭합니다.
2. 편집할 VLAN의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. VLAN 편집 * 대화 상자에 VRF VLAN에 대한 새 속성을 입력합니다.
5. 변경 내용 저장 * 을 클릭합니다.

가상 네트워크를 삭제합니다

가상 네트워크 개체를 제거할 수 있습니다. 가상 네트워크를 제거하기 전에 주소 블록을 다른 가상 네트워크에 추가해야 합니다.

1. Cluster * > * Network * 를 클릭합니다.
2. 삭제할 VLAN의 작업 아이콘을 클릭합니다.
3. 삭제 * 를 클릭합니다.
4. 메시지를 확인합니다.

자세한 내용을 확인하십시오

가상 네트워크를 편집합니다

FIPS 드라이브를 지원하는 클러스터를 생성합니다

많은 고객 환경에서 솔루션을 배포하는 데 있어 보안은 점점 더 중요해지고 있습니다. FIPS(Federal Information Processing Standards)는 컴퓨터 보안 및 상호 운용성에 대한 표준입니다. 사용되지 않는 데이터에 대한 FIPS 140-2 인증 암호화는 전체 보안 솔루션의 구성 요소입니다.

- "FIPS 드라이브에 노드를 혼합하지 마십시오"
- "유휴 데이터 암호화 사용"
- "노드가 FIPS 드라이브 기능을 지원할 수 있는지 확인합니다"
- "FIPS 드라이브 기능을 사용하도록 설정합니다"
- "FIPS 드라이브 상태를 확인합니다"
- "FIPS 드라이브 기능 문제를 해결합니다"

FIPS 드라이브에 노드를 혼합하지 마십시오

FIPS 드라이브 기능을 사용하도록 준비하기 위해 일부 드라이브는 FIPS 드라이브를 사용할 수 있고 일부 드라이브는 사용할 수 없는 노드를 혼합하지 말아야 합니다.

클러스터는 다음과 같은 조건을 기준으로 FIPS 드라이브를 준수합니다.

- 모든 드라이브는 FIPS 드라이브로 인증됩니다.
- 모든 노드는 FIPS 드라이브 노드입니다.
- 저장된 데이터 암호화(EAR)가 활성화되었습니다.
- FIPS 드라이브 기능이 설정되어 있습니다. FIPS 드라이브 기능을 활성화하려면 모든 드라이브와 노드가 FIPS를 지원하고 Encryption at Rest를 활성화해야 합니다.

유휴 데이터 암호화 사용

클러스터 전체의 유휴 암호화를 사용하거나 사용하지 않도록 설정할 수 있습니다. 이 기능은 기본적으로 사용되지 않습니다. FIPS 드라이브를 지원하려면 사용되지 않는 데이터에 대한 암호화를 설정해야 합니다.

1. NetApp Element 소프트웨어 UI에서 * 클러스터 * > * 설정 * 을 클릭합니다.
2. 저장 시 암호화 사용 * 을 클릭합니다.

자세한 내용을 확인하십시오

- 클러스터에 대한 암호화를 사용하거나 사용하지 않도록 설정합니다
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

노드가 **FIPS** 드라이브 기능을 지원할 수 있는지 확인합니다

NetApp Element 소프트웨어 GetFipsReport API 메서드를 사용하여 스토리지 클러스터의 모든 노드가 FIPS 드라이브를 지원할 준비가 되었는지 확인해야 합니다.

결과 보고서에는 다음 상태 중 하나가 표시됩니다.

- 없음: 노드가 FIPS 드라이브 기능을 지원할 수 없습니다.
- 부분: 노드가 FIPS를 지원하지만 모든 드라이브가 FIPS 드라이브는 아닙니다.
- 준비됨: 노드가 FIPS를 지원하며 모든 드라이브가 FIPS 드라이브로 장착되거나 드라이브가 없습니다.

단계

1. Element API를 사용하여 스토리지 클러스터의 노드와 드라이브가 다음을 입력하여 FIPS 드라이브를 사용할 수 있는지 확인합니다.

   게피프스보고서

2. Ready(준비) 상태가 표시되지 않은 노드를 확인하여 결과를 검토합니다.
3. Ready 상태가 표시되지 않은 노드의 경우 드라이브가 FIPS 드라이브 기능을 지원할 수 있는지 확인합니다.
   - Element API를 사용하여 'GetHardwareList'를 입력합니다
   - DriveEncryptionCapabilityType * 의 값을 확인합니다. "FIPS"인 경우 하드웨어에서 FIPS 드라이브 기능을 지원할 수 있습니다.

     에서 GetFipsReport 또는 ListDriveHardware에 대한 자세한 내용을 참조하십시오 "요소 API 참조입니다".
4. 드라이브가 FIPS 드라이브 기능을 지원할 수 없는 경우 하드웨어를 FIPS 하드웨어(노드 또는 드라이브)로 교체합니다.

자세한 내용을 확인하십시오

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

FIPS 드라이브 기능을 사용하도록 설정합니다

NetApp Element 소프트웨어 "EnableFeature" API 메소드를 사용하여 FIPS 드라이브 기능을 활성화할 수 있습니다.

저장 시 암호화 기능은 클러스터에서 활성화해야 하며, GetFipsReport가 모든 노드에 대해 준비 상태를 표시할 때 표시된 대로 모든 노드와 드라이브는 FIPS를 사용할 수 있어야 합니다.

단계

1. Element API를 사용하여 다음을 입력하여 모든 드라이브에서 FIPS를 사용하도록 설정합니다.

   EnableFeature params: FipsDrives

자세한 내용을 확인하십시오

- "Element API를 사용하여 스토리지를 관리합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

FIPS 드라이브 상태를 확인합니다

NetApp Element 소프트웨어 GetFeatureStatus API 메소드를 사용하여 FIPS 드라이브 기능이 클러스터에서 활성화되어 있는지 여부를 확인할 수 있습니다. 이 API 메소드에는 FIPS 드라이브 사용 상태가 true인지 false인지 여부가 표시됩니다.

1. Element API를 사용하여 다음을 입력하여 클러스터의 FIPS 드라이브 기능을 확인합니다.

   GetFeatureStatus입니다

2. GetFeatureStatus API 호출 결과를 검토합니다. FIPS Drives enabled 값이 True인 경우 FIPS 드라이브 기능이 활성화됩니다.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

자세한 내용을 확인하십시오

- "Element API를 사용하여 스토리지를 관리합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

FIPS 드라이브 기능 문제를 해결합니다

NetApp Element 소프트웨어 UI를 사용하면 FIPS 드라이브 기능과 관련된 시스템의 클러스터 장애 또는 오류에 대한 알림을 볼 수 있습니다.

1. Element UI를 사용하여 * Reporting * > * Alerts * 를 선택합니다.
2. 다음을 비롯한 클러스터 장애를 찾습니다.
   - FIPS 드라이브가 일치하지 않습니다
   - FIPS는 규정 준수를 위반합니다
3. 해결 방법은 클러스터 오류 코드 정보를 참조하십시오.

자세한 내용을 확인하십시오

- 클러스터 고장 코드
- "Element API를 사용하여 스토리지를 관리합니다"

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

클러스터에서 **HTTPS**에 **FIPS 140-2**를 사용하도록 설정합니다

EnableFeature API 메소드를 사용하여 HTTPS 통신에 FIPS 140-2 작동 모드를 활성화할 수 있습니다.

NetApp Element 소프트웨어를 사용하면 클러스터에서 FIPS(Federal Information Processing Standards) 140-2 운영 모드를 사용하도록 선택할 수 있습니다. 이 모드를 활성화하면 NCSM(NetApp Cryptographic Security Module)이 활성화되고 HTTPS를 통해 NetApp Element UI 및 API에 연결되는 모든 통신에 FIPS 140-2 Level 1 인증 암호화를 활용합니다.

> FIPS 140-2 모드를 활성화한 후에는 비활성화할 수 없습니다. FIPS 140-2 모드를 사용하도록 설정하면 클러스터의 각 노드가 재부팅되고 자체 테스트를 통해 실행되므로 NCSM이 FIPS 140-2 인증 모드에서 올바르게 설정 및 작동할 수 있습니다. 이로 인해 클러스터의 관리 및 스토리지 연결이 모두 중단됩니다. 환경에 암호화 메커니즘이 필요한 경우에만 신중하게 계획하고 이 모드를 활성화해야 합니다.

자세한 내용은 Element API 정보를 참조하십시오.

다음은 FIPS를 사용하도록 설정하는 API 요청의 예입니다.

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

이 작동 모드가 활성화된 후 모든 HTTPS 통신은 FIPS 140-2 승인 암호를 사용합니다.

자세한 내용을 확인하십시오

- SSL 암호
- "Element API를 사용하여 스토리지를 관리합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

SSL 암호

SSL 암호화는 호스트가 보안 통신을 설정하는 데 사용하는 암호화 알고리즘입니다. FIPS 140-2 모드가 활성화된 경우 Element 소프트웨어가 지원하는 표준 암호와 비표준 암호가 있습니다.

다음 목록은 Element 소프트웨어에서 지원되는 표준 SSL(Secure Socket Layer) 암호와 FIPS 140-2 모드가 활성화된 경우 지원되는 SSL 암호를 제공합니다.

- * FIPS 140-2 비활성화 *

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(DH 2048)-A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(DH 2048)-A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(DH 2048)-A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(DH 2048)-A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(secp256r1)-A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(secp256r1)-A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(secp256r1)-A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(secp256r1)-A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA(RSA 2048)-C

  TLS_RSA_WITED_AES_128_CBC_SHA(RSA 2048)-A

  TLS_RSA_WITED_AES_128_CBC_SHA256(RSA 2048)-A

  TLS_RSA_with_AES_128_GCM_SHA256(RSA 2048)-A

  TLS_RSA_WITED_AES_256_CBC_SHA(RSA 2048)-A

  TLS_RSA_WITED_AES_256_CBC_SHA256(RSA 2048)-A

  TLS_RSA_WITED_AES_256_GCM_SHA384(RSA 2048)-A

  tls_rsa_with_camellia_128_CBC_SHA(RSA 2048) -A

  tls_rsa_with_camellia_256_CBC_SHA(RSA 2048) -A

  tls_rsa_with_Idea_cbc_SHA(RSA 2048) -a

  TLS_RSA_WITED_RC4_128_MD5(RSA 2048)-C

  TLS_RSA_WITED_RC4_128_SHA(RSA 2048)-C

  TLS_RSA_WITED_SEED_CBC_SHA(RSA 2048)-A

- * FIPS 140-2 활성화 *

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(DH 2048)-A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(DH 2048)-A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(DH 2048)-A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(DH 2048)-A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(sect571r1)-A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(secp256r1)-A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(secp256r1)-A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(sect571r1)-A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(sect571r1)-A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(secp256r1)-A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(secp256r1)-A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(sect571r1)-A

TLS_RSA_WITH_3DES_EDE_CBC_SHA(RSA 2048)-C

TLS_RSA_WITED_AES_128_CBC_SHA(RSA 2048)-A

TLS_RSA_WITED_AES_128_CBC_SHA256(RSA 2048)-A

TLS_RSA_with_AES_128_GCM_SHA256(RSA 2048)-A

TLS_RSA_WITED_AES_256_CBC_SHA(RSA 2048)-A

TLS_RSA_WITED_AES_256_CBC_SHA256(RSA 2048)-A

TLS_RSA_WITED_AES_256_GCM_SHA384(RSA 2048)-A

자세한 내용을 확인하십시오

클러스터에서 HTTPS에 FIPS 140-2를 사용하도록 설정합니다

외부 키 관리를 시작합니다

EKM(외부 키 관리)은 외부 클러스터 EKS(외부 키 서버)와 함께 AK(보안 인증 키) 관리를 제공합니다. AK는 SED(자체 암호화 드라이브)를 잠그거나 잠금 해제하는 데 사용됩니다 "유휴 데이터 암호화" 클러스터에서 가 활성화됩니다. EKS는 AK의 안전한 생성 및 저장 기능을 제공합니다. 클러스터는 OASIS에서 정의한 표준 프로토콜인 KMIP(Key Management Interoperability Protocol)를 사용하여 EKS와 통신합니다.

- "외부 관리를 설정합니다"
- "소프트웨어 암호화 유휴 마스터 키를 다시 입력하다"
- "액세스할 수 없거나 잘못된 인증 키를 복구합니다"
- "외부 키 관리 API 명령"

자세한 내용을 확인하십시오

- "저장된 소프트웨어 암호화를 활성화하는 데 사용할 수 있는 CreateCluster API"
- "SolidFire 및 Element 소프트웨어 설명서"
- "이전 버전의 NetApp SolidFire 및 Element 제품에 대한 문서"

외부 키 관리를 설정합니다

다음 단계를 수행하고 나열된 Element API 메소드를 사용하여 외부 키 관리 기능을 설정할 수 있습니다.

필요한 것

- 저장된 소프트웨어 암호화와 함께 외부 키 관리를 설정하는 경우 를 사용하여 유휴 상태의 소프트웨어 암호화를 활성화했습니다 "클러스터 생성" 볼륨을 포함하지 않는 새 클러스터의 방법입니다.

단계

1. 외부 키 서버(EKS)와 트러스트 관계를 설정합니다.
   a. 다음 API 메서드를 호출하여 키 서버와 트러스트 관계를 설정하는 데 사용되는 Element 클러스터에 대한 공용/개인 키 쌍을 생성합니다. "CreatePublicPrivateKeyPair 를 참조하십시오"
   b. 인증 기관이 서명해야 하는 인증서 서명 요청(CSR)을 받습니다. CSR을 통해 키 서버가 해당 키에 액세스할 Element 클러스터가 Element 클러스터로 인증되었는지 확인할 수 있습니다. 다음 API 메서드를 호출합니다. "GetClientCertificateSignRequest 를 참조하십시오"
   c. EKS/인증 기관을 사용하여 검색된 CSR에 서명합니다. 자세한 내용은 타사 설명서를 참조하십시오.
2. 클러스터에 EKS와 통신할 서버 및 공급자를 생성합니다. 키 공급자는 키를 얻어야 하는 위치를 정의하고 서버는 전달할 EKS의 특정 속성을 정의합니다.
   a. 다음 API 메서드를 호출하여 키 서버 세부 정보가 있는 키 공급자를 만듭니다. "CreateKeyProviderKmip 을 참조하십시오"
   b. 다음 API 메소드를 호출하여 인증 기관의 서명된 인증서와 공개 키 인증서를 제공하는 키 서버를 생성합니다. "CreateKeyServerKmip 을 참조하십시오" "TestKeyServerKmip"

      테스트에 실패한 경우 서버 연결 및 구성을 확인합니다. 그런 다음 테스트를 반복합니다.

   c. 다음 API 메서드를 호출하여 키 서버를 키 공급자 컨테이너에 추가합니다."AddKeyServerToProviderKmip 를 참조하십시오" "TestKeyProviderKmip 을 참조하십시오"

      테스트에 실패한 경우 서버 연결 및 구성을 확인합니다. 그런 다음 테스트를 반복합니다.

3. 다음 단계 중 하나를 수행하여 유휴 데이터 암호화를 수행합니다.
   a. (저장된 하드웨어 암호화의 경우) 활성화 "유휴 하드웨어 암호화" 를 호출하여 키를 저장하는 데 사용되는 키 서버가 포함된 키 공급자의 ID를 제공합니다 "EnableEncryptionAtRest 를 참조하십시오" API 메소드.

      > 를 통해 유휴 상태에서 암호화를 활성화해야 합니다 "API를 참조하십시오". 기존 Element UI 버튼을 사용하여 유휴 상태에서 암호화를 활성화하면 기능이 내부적으로 생성된 키를 사용하여 되돌아갑니다.

   b. (저장된 소프트웨어 암호화용) "유휴 소프트웨어 암호화" 새로 만든 키 공급자를 사용하려면 키 공급자 ID를 에 전달합니다 "RekeySoftwareEncryptionAtRestMasterKey를 참조하십시오" API 메소드.

자세한 내용을 확인하십시오

- "클러스터에 대한 암호화를 사용하거나 사용하지 않도록 설정합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "이전 버전의 NetApp SolidFire 및 Element 제품에 대한 문서"

소프트웨어 암호화 유휴 마스터 키를 다시 입력하다

Element API를 사용하여 기존 키를 다시 입력할 수 있습니다. 이 프로세스는 외부 키 관리 서버에 대한 새 대체 마스터 키를 만듭니다. 마스터 키는 항상 새 마스터 키로 대체되며 복제 또는 덮어쓰기가 되지 않습니다.

다음 절차 중 하나로 키를 다시 입력하다

- 내부 키 관리에서 외부 키 관리로 변경 작업의 일부로 새 키를 만듭니다.
- 보안 관련 이벤트에 대한 대응 또는 보호 기능으로 새 키를 생성합니다.

> 이 프로세스는 비동기식이며 키를 다시 입력하다 를 사용할 수 있습니다 "GetAsyncResult 를 참조하십시오" 프로세스가 완료된 시점을 확인하기 위해 시스템을 폴링하는 방법입니다.

필요한 것

- 를 사용하여 저장 시 소프트웨어 암호화를 활성화했습니다 "클러스터 생성" 볼륨에 포함되어 있지 않고 I/O가 없는 새 클러스터의 방법입니다 사용 "9510c8e68784d05acbae2e947dde3cd8" 계속하기 전에 상태가 '활성화됨'인지 확인합니다.
- 있습니다 "트러스트 관계를 설정했습니다" SolidFire 클러스터와 EKS(외부 키 서버) 간. 를 실행합니다 "TestKeyProviderKmip 을 참조하십시오" 키 공급자에 대한 연결이 설정되었는지 확인하는 방법입니다.

단계

1. 를 실행합니다 "ListKeyProvidersKmip 을 참조하십시오" 키 공급자 ID('keyProviderID')를 명령 및 복사합니다.
2. 를 실행합니다 "RekeySoftwareEncryptionAtRestMasterKey를 참조하십시오" 이전 단계에서 키 공급자의 ID 번호로 keyManagementType 매개 변수를 external로, keyProviderID로 사용:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. RekeySoftwareEncryptionAtRestMasterKey 명령 응답에서 asyncHandle 값을 복사합니다.
4. 를 실행합니다 "GetAsyncResult 를 참조하십시오" 이전 단계의 asyncHandle 값을 사용하여 명령을 실행하여 구성 변경을 확인합니다. 명령 응답에서 이전 마스터 키 구성이 새 키 정보로 업데이트되었음을 확인할 수 있습니다. 나중에 사용할 수 있도록 새 키 공급자 ID를 복사합니다.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. GetSoftwareEncryptionatRestInfo 명령을 실행하여 keyProviderID를 포함한 새 키 세부 정보가 업데이트되었는지 확인합니다.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

자세한 내용을 확인하십시오

- "Element API를 사용하여 스토리지를 관리합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "이전 버전의 NetApp SolidFire 및 Element 제품에 대한 문서"

액세스할 수 없거나 잘못된 인증 키를 복구합니다

경우에 따라 사용자 개입이 필요한 오류가 발생할 수 있습니다. 오류가 발생할 경우 클러스터 장애 코드(클러스터 고장 코드)가 생성됩니다. 이 슬라이드에는 가장 가능성이 높은 두 가지 사례가 나와 있습니다.

KmipServerFault 클러스터 오류로 인해 클러스터가 드라이브를 잠금 해제할 수 없습니다**.**

이 문제는 클러스터를 처음 부팅하고 키 서버에 액세스할 수 없거나 필요한 키를 사용할 수 없을 때 발생할 수 있습니다.

1. 클러스터 고장 코드(있는 경우)의 복구 단계를 따르십시오.

메타데이터 드라이브가 실패로 표시되고 **"**사용 가능**"** 상태로 배치되었기 때문에 슬라이싱**ServiceUnsalisted** 오류가 설정될 수 있습니다**.**

지우기 단계:

1. 드라이브를 다시 추가합니다.
2. 3-4분 후 'liceServiceUnhealthy' 장애가 해결되었는지 확인한다.

을 참조하십시오 "클러스터 고장 코드" 를 참조하십시오.

외부 키 관리 **API** 명령

EKM 관리 및 구성에 사용할 수 있는 모든 API의 목록입니다.

클러스터와 외부 고객 소유 서버 간의 신뢰 관계를 설정하는 데 사용됩니다.

- CreatePublicPrivateKeyPair 를 참조하십시오
- GetClientCertificateSignRequest 를 참조하십시오

외부 고객 소유 서버의 특정 세부 정보를 정의하는 데 사용됩니다.

- CreateKeyServerKmip 을 참조하십시오
- ModifyKeyServerKmip
- DeleteKeyServerKmip 를 클릭합니다
- GetKeyServerKmip 을 참조하십시오
- ListKeyServersKmip 를 참조하십시오
- TestKeyServerKmip

외부 키 서버를 관리하는 주요 공급자를 만들고 유지 관리하는 데 사용됩니다.

- CreateKeyProviderKmip 을 참조하십시오

- DeleteKeyProviderKmip 를 클릭합니다
- AddKeyServerToProviderKmip 를 참조하십시오
- RemoveKeyServerFromProviderKmip 를 참조하십시오
- GetKeyProviderKmip 을 참조하십시오
- ListKeyProvidersKmip 을 참조하십시오
- RekeySoftwareEncryptionAtRestMasterKey를 참조하십시오
- TestKeyProviderKmip 을 참조하십시오

API 메소드에 대한 자세한 내용은 를 참조하십시오 "API 참조 정보입니다".

볼륨 및 가상 볼륨 관리

Element UI의 관리 탭에서 Element 소프트웨어를 실행하는 클러스터의 데이터를 관리할 수 있습니다. 사용 가능한 클러스터 관리 기능에는 데이터 볼륨, 볼륨 액세스 그룹, 이니시에이터, QoS(서비스 품질) 정책의 생성 및 관리가 포함됩니다.

- "볼륨 작업"
- "가상 볼륨 작업"
- "볼륨 액세스 그룹 및 이니시에이터와 작업합니다"

를 참조하십시오

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

볼륨 작업

SolidFire 시스템은 볼륨을 사용하여 스토리지를 프로비저닝합니다. 볼륨은 iSCSI 또는 파이버 채널 클라이언트가 네트워크를 통해 액세스하는 블록 디바이스입니다. 관리 탭의 볼륨 페이지에서 노드에서 볼륨을 생성, 수정, 클론 복제 및 삭제할 수 있습니다. 볼륨 대역폭 및 I/O 사용량에 대한 통계도 볼 수 있습니다.

자세한 내용을 확인하십시오

- "서비스 품질 정책 관리"
- "볼륨을 생성합니다"
- "개별 볼륨 성능 세부 정보를 봅니다"
- "활성 볼륨을 편집합니다"
- "볼륨을 삭제합니다"
- "삭제된 볼륨을 복원합니다"
- "볼륨을 제거합니다"

- "볼륨의 클론을 생성합니다"
- "Fibre Channel 볼륨에 LUN을 할당합니다"
- "볼륨에 QoS 정책을 적용합니다"
- "볼륨의 QoS 정책 연결을 제거합니다"

서비스 품질 정책 관리

서비스 품질(QoS) 정책을 사용하면 여러 볼륨에 적용할 수 있는 표준화된 서비스 품질 설정을 생성하여 저장할 수 있습니다. 관리 탭의 QoS 정책 페이지에서 QoS 정책을 생성, 편집 및 삭제할 수 있습니다.

> QoS 정책을 사용하는 경우 볼륨에 대해 사용자 지정 QoS를 사용하지 마십시오. 사용자 지정 QoS는 볼륨 QoS 설정에 대한 QoS 정책 값을 재정의하고 조정합니다.

"NetApp 비디오: SolidFire 서비스 품질 정책"

을 참조하십시오 "성능 및 서비스 품질".

- QoS 정책을 생성합니다
- QoS 정책을 편집합니다
- QoS 정책을 삭제합니다

QoS 정책을 생성합니다

볼륨을 생성할 때 QoS 정책을 생성하고 적용할 수 있습니다.

1. Management * > * QoS Policies * 를 선택합니다.
2. QoS 정책 생성 * 을 클릭합니다.
3. 정책 이름 * 을 입력합니다.
4. 최소 IOPS**, * 최대 IOPS * 및 * 버스트 IOPS * 값을 입력합니다.
5. QoS 정책 생성 * 을 클릭합니다.

QoS 정책을 편집합니다

기존 QoS 정책의 이름을 변경하거나 정책과 연결된 값을 편집할 수 있습니다. QoS 정책을 변경하면 정책에 연결된 모든 볼륨에 영향을 줍니다.

1. Management * > * QoS Policies * 를 선택합니다.
2. 편집할 QoS 정책의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 편집을 선택합니다.
4. QoS 정책 편집 * 대화 상자에서 필요에 따라 다음 속성을 수정합니다.
    - 정책 이름
    - 최소 IOPS

- 최대 IOPS
- 버스트 IOPS

5. 변경 내용 저장 * 을 클릭합니다.

QoS 정책을 삭제합니다

QoS 정책이 더 이상 필요하지 않은 경우 삭제할 수 있습니다. QoS 정책을 삭제할 경우 정책에 연결된 모든 볼륨은 QoS 설정을 유지하지만 정책과 연결되지 않습니다.

> 대신 QoS 정책에서 볼륨을 연결 해제하려는 경우 해당 볼륨의 QoS 설정을 사용자 지정으로 변경할 수 있습니다.

1. Management * > * QoS Policies * 를 선택합니다.
2. 삭제할 QoS 정책에 대한 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 선택합니다.
4. 작업을 확인합니다.

자세한 내용을 확인하십시오

- "볼륨의 QoS 정책 연결을 제거합니다"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

볼륨 관리

SolidFire 시스템은 볼륨을 사용하여 스토리지를 프로비저닝합니다. 볼륨은 iSCSI 또는 파이버 채널 클라이언트가 네트워크를 통해 액세스하는 블록 디바이스입니다.

관리 탭의 볼륨 페이지에서 노드에서 볼륨을 생성, 수정, 클론 복제 및 삭제할 수 있습니다.

볼륨을 생성합니다

볼륨을 생성하고 해당 볼륨을 지정된 계정에 연결할 수 있습니다. 모든 볼륨은 계정과 연결되어 있어야 합니다. 이 연결은 CHAP 자격 증명을 사용하여 iSCSI 초기자를 통해 볼륨에 대한 액세스 권한을 계정에 부여합니다.

생성 중에 볼륨의 QoS 설정을 지정할 수 있습니다.

1. Management * > * Volumes * 를 선택합니다.
2. Create Volume * 을 클릭합니다.
3. 새 볼륨 만들기 * 대화 상자에서 * 볼륨 이름 * 을 입력합니다.
4. 볼륨의 총 크기를 입력합니다.

> 기본 볼륨 크기 선택은 GB입니다. GB 또는 GiB 단위로 측정된 크기를 사용하여 볼륨을 생성할 수 있습니다.

- 1GB = 1,000,000바이트
- 1GiB = 1 073 741 824바이트

5. 볼륨의 * 블록 크기 * 를 선택합니다.
6. 계정 * 드롭다운 목록을 클릭하고 볼륨에 액세스할 수 있는 계정을 선택합니다.

   계정이 없는 경우 * 계정 만들기 * 링크를 클릭하고 새 계정 이름을 입력한 다음 * 만들기 * 를 클릭합니다. 계정이 생성되고 새 볼륨과 연결됩니다.

   > 계정이 50개를 초과하는 경우 목록이 나타나지 않습니다. 입력을 시작하면 자동 완성 기능에 선택 가능한 값이 표시됩니다.

7. 서비스 품질 * 을 설정하려면 다음 중 하나를 수행합니다.
   a. 정책 * 에서 기존 QoS 정책을 선택할 수 있습니다(사용 가능한 경우).
   b. 사용자 지정 설정 * 에서 IOPS에 대한 사용자 지정 최소, 최대 및 버스트 값을 설정하거나 기본 QoS 값을 사용합니다.

      최대 또는 버스트 IOPS 값이 20,000 IOPS 이상인 볼륨은 단일 볼륨에서 이러한 IOPS 수준을 달성하기 위해 큐 길이가 크거나 여러 세션이 필요할 수 있습니다.

8. Create Volume * 을 클릭합니다.

볼륨 세부 정보를 봅니다

1. Management * > * Volumes * 를 선택합니다.
2. 세부 정보를 검토합니다.
   - * ID *: 볼륨에 대해 시스템에서 생성한 ID입니다.
   - * 이름 *: 볼륨을 생성할 때 볼륨에 지정된 이름입니다.
   - * 계정 *: 볼륨에 할당된 계정의 이름입니다.
   - * 액세스 그룹 *: 볼륨이 속한 볼륨 액세스 그룹 또는 그룹의 이름입니다.
   - * 액세스 *: 볼륨을 생성할 때 볼륨에 할당된 액세스 유형입니다. 가능한 값:
     - 읽기/쓰기: 모든 읽기 및 쓰기가 허용됩니다.
     - 읽기 전용: 모든 읽기 작업이 허용되며 쓰기가 허용되지 않습니다.
     - 잠김: 관리자 액세스만 허용됩니다.
     - ReplicationTarget: 복제된 볼륨 쌍의 타겟 볼륨으로 지정됩니다.
   - * used * (사용 *): 볼륨에서 사용된 공간의 비율입니다.
   - * 크기 *: 볼륨의 총 크기(GB)입니다.
   - * 스냅샷 *: 볼륨에 대해 생성된 스냅샷의 수입니다.
   - * QoS 정책 *: 사용자 정의 QoS 정책에 대한 이름 및 링크입니다.
   - * 최소 IOPS *: 볼륨에 대해 보장된 최소 IOPS 수입니다.
   - * 최대 IOPS *: 볼륨에 허용되는 최대 IOPS 수입니다.

- * 버스트 IOPS *: 짧은 기간 동안 볼륨에 허용되는 최대 IOPS 수입니다. 기본값 = 15,000.
- * 특성 *: API 메서드를 통해 볼륨에 키/값 쌍으로 할당된 특성
- * 512e *: 볼륨에서 512e가 활성화되었는지 여부를 나타냅니다. 가능한 값:
  - 예
  - 아니요
- * Created on *(생성 날짜): 볼륨이 생성된 날짜 및 시간입니다.

개별 볼륨 세부 정보를 봅니다

개별 볼륨의 성능 통계를 볼 수 있습니다.

1. 보고 * > * 볼륨 성능 * 을 선택합니다.
2. 볼륨 목록에서 볼륨에 대한 작업 아이콘을 클릭합니다.
3. 세부 정보 보기 * 를 클릭합니다.

   용지 맨 아래에 용적에 대한 일반 정보가 들어 있는 용지함이 나타납니다.

4. 볼륨에 대한 자세한 정보를 보려면 * 자세한 정보 보기 * 를 클릭하십시오.

   볼륨에 대한 성능 그래프와 자세한 정보가 표시됩니다.

활성 볼륨을 편집합니다

QoS 값, 볼륨 크기 및 바이트 값이 계산되는 측정 단위와 같은 볼륨 특성을 수정할 수 있습니다. 복제 사용에 대한 계정 액세스를 수정하거나 볼륨에 대한 액세스를 제한할 수도 있습니다.

다음 조건에서 클러스터에 공간이 충분할 때 볼륨 크기를 조정할 수 있습니다.

- 정상 작동 조건.
- 볼륨 오류 또는 오류가 보고됩니다.
- 볼륨을 클론 복제 중입니다.
- 볼륨이 재동기화 중입니다.

단계

1. Management * > * Volumes * 를 선택합니다.
2. Active * (활성 *) 창에서 편집할 볼륨의 Actions (동작) 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. * 선택 사항: * 볼륨의 총 크기를 변경합니다.
   - 볼륨 크기를 늘릴 수 있지만 줄일 수는 없습니다. 단일 크기 조정 작업에서만 볼륨 크기를 조정할 수 있습니다. 가비지 수집 작업 및 소프트웨어 업그레이드로 크기 조정 작업이 중단되지 않습니다.
   - 복제를 위해 볼륨 크기를 조정하는 경우 먼저 복제 대상으로 할당된 볼륨의 크기를 늘려야 합니다. 그런 다음 소스 볼륨의 크기를 조정할 수 있습니다. 타겟 볼륨의 크기는 소스 볼륨과 같거나 더 클 수 있지만 크기는 작을 수 없습니다.

기본 볼륨 크기 선택은 GB입니다. GB 또는 GiB 단위로 측정된 크기를 사용하여 볼륨을 생성할 수 있습니다.

- 1GB = 1,000,000바이트
- 1GiB = 1 073 741 824바이트

5. * 선택 사항: * 다음 중 하나의 다른 계정 액세스 수준을 선택하십시오.
   - 읽기 전용
   - 읽기/쓰기
   - 잠금
   - 복제 타겟
6. * 선택 사항: * 볼륨에 액세스할 수 있는 계정을 선택합니다.

   계정이 없는 경우 * 계정 만들기 * 링크를 클릭하고 새 계정 이름을 입력한 다음 * 만들기 * 를 클릭합니다. 계정이 생성되고 볼륨과 연결됩니다.

   > 계정이 50개를 초과하는 경우 목록이 나타나지 않습니다. 입력을 시작하면 자동 완성 기능에 선택 가능한 값이 표시됩니다.

7. * 선택 사항: * 서비스 품질 * 에서 선택 사항을 변경하려면 다음 중 하나를 수행합니다.
   a. 정책 * 에서 기존 QoS 정책을 선택할 수 있습니다(사용 가능한 경우).
   b. 사용자 지정 설정 * 에서 IOPS에 대한 사용자 지정 최소, 최대 및 버스트 값을 설정하거나 기본 QoS 값을 사용합니다.

   > 볼륨에 QoS 정책을 사용하는 경우 사용자 지정 QoS를 설정하여 볼륨에 대한 QoS 정책 가입을 제거할 수 있습니다. 사용자 지정 QoS는 볼륨 QoS 설정에 대한 QoS 정책 값을 재정의하고 조정합니다.

   > IOPS 값을 변경할 때는 수십 또는 수백 단위로 증분해야 합니다. 입력 값에는 유효한 정수가 필요합니다.

   > 매우 높은 버스트 값으로 볼륨을 구성합니다. 따라서 시스템에서 가끔 발생하는 대규모 블록 순차적 워크로드를 더 빠르게 처리하는 동시에 볼륨에 대해 일관된 IOPS를 유지할 수 있습니다.

8. 변경 내용 저장 * 을 클릭합니다.

볼륨을 삭제합니다

Element 스토리지 클러스터에서 하나 이상의 볼륨을 삭제할 수 있습니다.

시스템은 삭제된 볼륨을 즉시 제거하지 않으며, 볼륨은 약 8시간 동안 계속 사용할 수 있습니다. 시스템이 볼륨을 제거하기 전에 볼륨을 복원하면 볼륨이 다시 온라인 상태가 되고 iSCSI 연결이 복원됩니다.

스냅샷을 생성하는 데 사용된 볼륨이 삭제되면 연결된 스냅샷이 비활성화됩니다. 삭제된 소스 볼륨이 제거되면 연결된 비활성 스냅샷도 시스템에서 제거됩니다.

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

단계

1. Management * > * Volumes * 를 선택합니다.
2. 단일 볼륨을 삭제하려면 다음 단계를 수행하십시오.
   a. 삭제할 볼륨의 작업 아이콘을 클릭합니다.
   b. 결과 메뉴에서 * 삭제 * 를 클릭합니다.
   c. 작업을 확인합니다.

   시스템이 볼륨을 * Volumes * 페이지의 * Deleted * (삭제됨 *) 영역으로 이동합니다.
3. 여러 볼륨을 삭제하려면 다음 단계를 수행하십시오.
   a. 볼륨 목록에서 삭제할 볼륨 옆의 확인란을 선택합니다.
   b. 대량 작업 * 을 클릭합니다.
   c. 결과 메뉴에서 * 삭제 * 를 클릭합니다.
   d. 작업을 확인합니다.

      볼륨이 * Volumes * 페이지의 * Deleted * (삭제됨 *) 영역으로 이동합니다.

삭제된 볼륨을 복원합니다

삭제되었으나 아직 제거되지 않은 경우 시스템의 볼륨을 복원할 수 있습니다. 시스템은 삭제된 후 약 8시간 후에 자동으로 볼륨을 삭제합니다. 시스템에서 볼륨을 제거한 경우에는 복원할 수 없습니다.

1. Management * > * Volumes * 를 선택합니다.
2. 삭제된 볼륨 목록을 보려면 * Deleted * (삭제됨 *) 탭을 클릭합니다.
3. 복원하려는 볼륨의 작업 아이콘을 클릭합니다.
4. 결과 메뉴에서 * 복원 * 을 클릭합니다.
5. 작업을 확인합니다.

   볼륨은 * 활성 * 볼륨 목록에 배치되고 볼륨에 대한 iSCSI 연결이 복원됩니다.

볼륨을 제거합니다

볼륨이 제거되면 시스템에서 영구적으로 제거됩니다. 볼륨의 모든 데이터가 손실됩니다.

삭제 8시간 후 시스템에서 삭제된 볼륨을 자동으로 삭제합니다. 그러나 예약된 시간 전에 볼륨을 제거하려면 제거할 수 있습니다.

1. Management * > * Volumes * 를 선택합니다.
2. DELETED * 버튼을 클릭합니다.
3. 단일 볼륨 또는 여러 볼륨을 제거하는 단계를 수행합니다.

옵션을 선택합니다	단계
단일 볼륨을 제거합니다	a. 제거할 볼륨의 작업 아이콘을 클릭합니다. b. Purge * 를 클릭합니다. c. 작업을 확인합니다.
여러 볼륨을 제거합니다	a. 제거할 볼륨을 선택합니다. b. 대량 작업 * 을 클릭합니다. c. 결과 메뉴에서 * Purge * 를 선택합니다. d. 작업을 확인합니다.

볼륨의 클론을 생성합니다

단일 볼륨 또는 여러 볼륨의 클론을 생성하여 데이터의 시점 복사본을 만들 수 있습니다. 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.

> 운영 체제는 복제된 볼륨을 처리하는 방식에 따라 다릅니다. VMware ESXi는 복제된 볼륨을 볼륨 복사본 또는 스냅샷 볼륨으로 처리합니다. 볼륨은 새 데이터 저장소를 생성하는 데 사용할 수 있는 디바이스가 됩니다. 클론 볼륨을 마운트하고 스냅샷 LUN을 처리하는 방법에 대한 자세한 내용은 의 VMware 설명서를 참조하십시오 "VMFS 데이터 저장소 복제본 마운트" 및 "중복 VMFS 데이터 저장소 관리".

> 작은 크기로 복제하여 복제된 볼륨을 잘라내려면 먼저 작은 볼륨에 맞도록 파티션을 준비해야 합니다.

단계

1. Management * > * Volumes * 를 선택합니다.
2. 단일 볼륨을 클론하려면 다음 단계를 수행하십시오.
   a. Active * 페이지의 볼륨 목록에서 복제할 볼륨의 작업 아이콘을 클릭합니다.
   b. 결과 메뉴에서 * Clone * 을 클릭합니다.
   c. 클론 볼륨 * 창에서 새로 복제된 볼륨의 볼륨 이름을 입력합니다.
   d. 체적 크기 * 스핀 상자 및 목록을 사용하여 체적의 크기와 측정을 선택합니다.

      > 기본 볼륨 크기 선택은 GB입니다. GB 또는 GiB 단위로 측정된 크기를 사용하여 볼륨을 생성할 수 있습니다.

      - 1GB = 1,000,000바이트
      - 1GiB = 1 073 741 824바이트

   e. 새로 복제된 볼륨에 대한 액세스 유형을 선택합니다.

f. 계정 * 목록에서 새로 복제된 볼륨과 연결할 계정을 선택합니다.

> 계정 만들기 * 링크를 클릭하고 계정 이름을 입력한 다음 * 만들기 * 를 클릭하면 이 단계에서 계정을 만들 수 있습니다. 계정을 만든 후에는 시스템에서 자동으로 * 계정 * 목록에 계정을 추가합니다.

3. 여러 볼륨을 클론하려면 다음 단계를 수행하십시오.
   a. Active * 페이지의 볼륨 목록에서 복제할 볼륨 옆의 확인란을 선택합니다.
   b. 대량 작업 * 을 클릭합니다.
   c. 결과 메뉴에서 * Clone * 을 선택합니다.
   d. 여러 볼륨 클론 * 대화 상자의 * 새 볼륨 이름 접두사 * 필드에 복제된 볼륨의 접두사를 입력합니다.
   e. Account * 목록에서 복제된 볼륨과 연결할 계정을 선택합니다.
   f. 클론 복제된 볼륨에 대한 액세스 유형을 선택합니다.
4. 클로닝 시작 * 을 클릭합니다.

> 클론의 볼륨 크기를 늘리면 새 볼륨의 끝에 추가 여유 공간이 있는 새 볼륨이 됩니다. 볼륨 사용 방법에 따라 파티션을 확장하거나 사용 가능한 공간에 새 파티션을 만들어야 사용할 수 있습니다.

를 참조하십시오

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

Fibre Channel 볼륨에 **LUN**을 할당합니다

볼륨 액세스 그룹에서 파이버 채널 볼륨의 LUN 할당을 변경할 수 있습니다. 볼륨 액세스 그룹을 생성할 때 파이버 채널 볼륨 LUN을 할당할 수도 있습니다.

새 Fibre Channel LUN을 할당하는 것은 고급 기능이며 접속 호스트에서 알 수 없는 결과를 초래할 수 있습니다. 예를 들어, 새 LUN ID가 호스트에서 자동으로 검색되지 않을 수 있으며 호스트에서 새 LUN ID를 재검색해야 할 수 있습니다.

1. Management * > * Access Groups * 를 선택합니다.
2. 편집할 액세스 그룹의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 편집을 선택합니다.
4. Edit Volume Access Group * 대화 상자의 * Assign LUN ID * 아래에서 * LUN Assignments * 목록의 화살표를 클릭합니다.
5. LUN을 할당할 목록의 각 볼륨에 대해 해당하는 * LUN * 필드에 새 값을 입력합니다.
6. 변경 내용 저장 * 을 클릭합니다.

볼륨에 **QoS** 정책을 적용합니다

하나 이상의 볼륨에 기존 QoS 정책을 일괄 적용할 수 있습니다.

일괄 적용하려는 QoS 정책이 있어야 합니다.

1. Management * > * Volumes * 를 선택합니다.
2. 볼륨 목록에서 QoS 정책을 적용할 볼륨 옆의 확인란을 선택합니다.
3. 대량 작업 * 을 클릭합니다.
4. 결과 메뉴에서 * QoS 정책 적용 * 을 클릭합니다.
5. 드롭다운 목록에서 QoS 정책을 선택합니다.
6. 적용 * 을 클릭합니다.

자세한 내용을 확인하십시오

서비스 품질 정책

볼륨의 **QoS** 정책 연결을 제거합니다

사용자 지정 QoS 설정을 선택하여 볼륨에서 QoS 정책 연결을 제거할 수 있습니다.

수정하려는 볼륨은 QoS 정책과 연계되어야 합니다.

1. Management * > * Volumes * 를 선택합니다.
2. 수정하려는 QoS 정책이 포함된 볼륨의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. 결과 메뉴의 * 서비스 품질 * 에서 * 사용자 정의 설정 * 을 클릭합니다.
5. 최소 IOPS *, * 최대 IOPS * 및 * 버스트 IOPS * 를 수정하거나 기본 설정을 유지합니다.
6. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

QoS 정책을 삭제합니다

가상 볼륨 작업

Element UI를 사용하여 가상 볼륨 및 관련 스토리지 컨테이너, 프로토콜 엔드포인트, 바인딩 및 호스트에 대한 정보를 보고 작업을 수행할 수 있습니다.

NetApp Element 소프트웨어 스토리지 시스템은 VVOL(가상 볼륨) 기능을 비활성화한 상태로 제공됩니다. Element UI를 통해 vSphere VVol 기능을 수동으로 활성화하는 일회성 작업을 수행해야 합니다.

VVOL 기능을 활성화하면 VVOL 관련 모니터링 및 제한된 관리 옵션을 제공하는 사용자 인터페이스에 VVol 탭이 나타납니다. 또한 VASA Provider라고 하는 스토리지 측 소프트웨어 구성 요소는 vSphere에 대한 스토리지 인식 서비스 역할을 합니다. VVOL 생성, 클론 복제 및 편집과 같은 대부분의 VVOL 명령은 vCenter Server 또는 ESXi 호스트에서 시작되며 VASA Provider가 Element 소프트웨어 스토리지 시스템의 Element API로 변환합니다. 스토리지 컨테이너를 생성, 삭제 및 관리하고 가상 볼륨을 삭제하는 명령은 Element UI를 사용하여 시작할 수 있습니다.

Element 소프트웨어 스토리지 시스템에서 가상 볼륨 기능을 사용하는 데 필요한 대부분의 구성은 vSphere에서 이루어집니다. VMware vSphere Virtual Volumes for SolidFire Storage 구성 가이드 _ 를 참조하여 vCenter에 VASA

Provider를 등록하고, VVOL 데이터 저장소를 생성 및 관리하고, 정책에 따라 스토리지를 관리하십시오.

> 단일 vCenter 인스턴스에 둘 이상의 NetApp Element VASA 공급자를 등록하지 마십시오. 두 번째 NetApp Element VASA 공급자를 추가하면 모든 VVOL 데이터 저장소에 액세스할 수 없게 됩니다.

> vCenter에 VASA 공급자를 이미 등록한 경우 여러 vCenter에 대한 VASA 지원을 업그레이드 패치로 사용할 수 있습니다. 설치하려면 에서 VASA39 .tar.gz 파일을 다운로드하십시오 "NetApp 소프트웨어 다운로드" 사이트를 방문하여 매니페스트의 지침을 따르십시오. NetApp Element VASA 공급자는 NetApp 인증서를 사용합니다. 이 패치를 사용하면 vCenter에서 인증서를 수정하지 않고 사용하여 VASA 및 VVol 사용을 위한 여러 vCenter를 지원합니다. 인증서를 수정하지 마십시오. 사용자 지정 SSL 인증서는 VASA에서 지원되지 않습니다.

자세한 내용을 확인하십시오

- 가상 볼륨을 설정합니다
- 가상 볼륨 세부 정보를 봅니다
- 가상 볼륨을 삭제합니다
- 스토리지 컨테이너를 생성합니다
- 저장소 컨테이너를 편집합니다
- 저장소 컨테이너를 삭제합니다
- 프로토콜 엔드포인트
- 바인딩
- 호스트 세부 정보입니다

가상 볼륨을 설정합니다

NetApp Element 소프트웨어를 통해 VVOL(vSphere 가상 볼륨) 기능을 수동으로 활성화해야 합니다. Element 소프트웨어 시스템에는 기본적으로 VVOL 기능이 비활성화되어 있으며 새 설치 또는 업그레이드의 일부로 자동 활성화되지 않습니다. VVOL 기능을 활성화하는 것은 일회성 구성 작업입니다.

필요한 것

- 클러스터는 Element 9.0 이상을 실행해야 합니다.
- 클러스터는 VVol과 호환되는 ESXi 6.0 이상 환경에 연결되어야 합니다.
- Element 11.3 이상을 사용하는 경우 클러스터가 ESXi 6.0 업데이트 3 이상 환경에 연결되어 있어야 합니다.

> vSphere 가상 볼륨 기능을 활성화하면 Element 소프트웨어 구성이 영구적으로 변경됩니다. 클러스터가 VMware ESXi VVol 호환 환경에 연결된 경우에만 VVol 기능을 활성화해야 합니다. 시스템에서 모든 데이터를 삭제하는 공장 출하 시 이미지로 클러스터를 되돌리시기만 하면 VVOL 기능을 비활성화하고 기본 설정을 복원할 수 있습니다.

단계

1. 클러스터 * > * 설정 * 을 선택합니다.

2. 가상 볼륨에 대한 클러스터별 설정을 찾습니다.
3. Enable Virtual Volumes * 를 클릭합니다.
4. Yes * 를 클릭하여 가상 볼륨 구성 변경을 확인합니다.

   요소 UI에 * VVol * 탭이 나타납니다.

   > VVOL 기능이 활성화되면 SolidFire 클러스터가 VASA Provider를 시작하고, VASA 트래픽에 대해 포트 8444를 열고, vCenter 및 모든 ESXi 호스트에서 검색할 수 있는 프로토콜 엔드포인트를 생성합니다.

5. 클러스터 * > * 설정 * 의 가상 볼륨(VVol) 설정에서 VASA Provider URL을 복사합니다. 이 URL을 사용하여 vCenter에 VASA Provider를 등록합니다.
6. VVol * > * Storage Containers * 에서 저장소 컨테이너를 만듭니다.

   > VM을 VVOL 데이터 저장소에 프로비저닝할 수 있도록 스토리지 컨테이너를 하나 이상 생성해야 합니다.

7. VVol * > * Protocol Endpoints * 를 선택합니다.
8. 클러스터의 각 노드에 대해 프로토콜 엔드포인트가 생성되었는지 확인합니다.

   > vSphere에 추가 구성 작업이 필요합니다. VMware vSphere Virtual Volumes for SolidFire Storage 구성 가이드 _ 를 참조하여 vCenter에 VASA Provider를 등록하고, VVOL 데이터 저장소를 생성 및 관리하고, 정책에 따라 스토리지를 관리하십시오.

자세한 내용을 확인하십시오

"SolidFire 스토리지용 VMware vSphere 가상 볼륨 구성 가이드 를 참조하십시오"

가상 볼륨 세부 정보를 봅니다

Element UI에서 클러스터의 모든 활성 가상 볼륨에 대한 가상 볼륨 정보를 검토할 수 있습니다. 또한 입력, 출력, 처리량, 지연 시간, 지연 시간 등 각 가상 볼륨의 성능 활동을 대기열 길이 및 볼륨 정보.

필요한 것

- 클러스터의 Element UI에서 VVOL 기능을 활성화해야 합니다.
- 연결된 저장소 컨테이너를 만들어야 합니다.
- Element 소프트웨어 VVol 기능을 사용하도록 vSphere 클러스터를 구성해야 합니다.
- vSphere에서 하나 이상의 VM을 생성해야 합니다.

단계

1. VVol * > * Virtual Volumes * 를 클릭합니다.

   모든 활성 가상 볼륨에 대한 정보가 표시됩니다.

2. 검토할 가상 볼륨에 대한 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 세부 정보 보기 * 를 선택합니다.

세부 정보

VVol 탭의 Virtual Volumes 페이지에서는 볼륨 ID, 스냅샷 ID, 상위 가상 볼륨 ID 및 가상 볼륨 ID와 같은 클러스터의 각 활성 가상 볼륨에 대한 정보를 제공합니다.

- * 볼륨 ID *: 기본 볼륨의 ID입니다.
- * 스냅샷 ID *: 기본 볼륨 스냅샷의 ID입니다. 가상 볼륨이 SolidFire 스냅샷을 나타내지 않는 경우 값은 0입니다.
- * 상위 가상 볼륨 ID *: 상위 가상 볼륨의 가상 볼륨 ID입니다. ID가 모두 0인 경우 가상 볼륨은 상위 볼륨에 대한 링크 없이 독립적입니다.
- * 가상 볼륨 ID *: 가상 볼륨의 UUID
- * 이름 *: 가상 볼륨에 할당된 이름입니다.
- * 저장소 컨테이너 *: 가상 볼륨을 소유하는 저장소 컨테이너입니다.
- * 게스트 OS 유형 *: 가상 볼륨과 연결된 운영 체제입니다.
- * 가상 볼륨 유형 *: 가상 볼륨 유형: 구성, 데이터, 메모리, 스왑 또는 기타.
- * 액세스 *: 가상 볼륨에 할당된 읽기-쓰기 권한
- * 크기 *: 가상 볼륨의 크기(GB 또는 GiB)입니다.
- * 스냅샷 *: 연결된 스냅샷의 수입니다. 스냅샷 세부 정보에 연결할 번호를 클릭합니다.
- * 최소 IOPS *: 가상 볼륨의 최소 IOPS QoS 설정입니다.
- * 최대 IOPS *: 가상 볼륨의 최대 IOPS QoS 설정입니다.
- * 버스트 IOPS *: 가상 볼륨의 최대 버스트 QoS 설정.
- * VMW_VmID *: "VMW_" 앞에 있는 필드의 정보는 VMware에서 정의합니다.
- * 생성 시간 *: 가상 볼륨 생성 작업이 완료된 시간입니다.

개별 가상 볼륨 세부 정보입니다

개별 가상 볼륨을 선택하고 세부 정보를 볼 때 VVol 탭의 Virtual Volumes 페이지는 다음과 같은 가상 볼륨 정보를 제공합니다.

- * VMW_XXX *: "VMW_"가 앞에 있는 필드의 정보는 VMware에서 정의합니다.
- * 상위 가상 볼륨 ID *: 상위 가상 볼륨의 가상 볼륨 ID입니다. ID가 모두 0인 경우 가상 볼륨은 상위 볼륨에 대한 링크 없이 독립적입니다.
- * 가상 볼륨 ID *: 가상 볼륨의 UUID
- * 가상 볼륨 유형 *: 가상 볼륨 유형: 구성, 데이터, 메모리, 스왑 또는 기타.
- * 볼륨 ID *: 기본 볼륨의 ID입니다.
- * 액세스 *: 가상 볼륨에 할당된 읽기-쓰기 권한
- * 계정 이름 *: 볼륨이 포함된 계정의 이름입니다.
- * 액세스 그룹 *: 연결된 볼륨 액세스 그룹

- * 총 볼륨 크기 *: 프로비저닝된 총 용량(바이트)입니다.
- * 0이 아닌 블록 *: 마지막 가비지 수집 작업이 완료된 후 데이터가 포함된 총 4KiB 블록 수입니다.
- * 제로 블록 *: 가비지 수집 작업의 마지막 라운드 완료 후 데이터가 없는 총 4KiB 블록 수입니다.
- * 스냅샷 *: 연결된 스냅샷의 수입니다. 스냅샷 세부 정보에 연결할 번호를 클릭합니다.
- * 최소 IOPS *: 가상 볼륨의 최소 IOPS QoS 설정입니다.
- * 최대 IOPS *: 가상 볼륨의 최대 IOPS QoS 설정입니다.
- * 버스트 IOPS *: 가상 볼륨의 최대 버스트 QoS 설정.
- * Enable 512 *: 가상 볼륨은 항상 512바이트 블록 크기 에뮬레이션을 사용하므로 값은 항상 yes입니다.
- * Volumes Paired *: 볼륨이 페어링되었는지 여부를 나타냅니다.
- * 생성 시간 *: 가상 볼륨 생성 작업이 완료된 시간입니다.
- * 블록 크기 *: 볼륨의 블록 크기입니다.
- * Unaligned Writes *: 512e 볼륨의 경우 4K 섹터 경계에 있지 않은 쓰기 작업 수입니다. 정렬되지 않은 쓰기 횟수가 많은 경우 잘못된 파티션 정렬이 표시될 수 있습니다.
- * 정렬되지 않은 읽기 *: 512e 볼륨의 경우 4K 섹터 경계에 있지 않은 읽기 작업 수입니다. 정렬되지 않은 읽기 수가 많은 경우 파티션 정렬이 잘못되었을 수 있습니다.
- * scsiEUIDeviceID *: EUI-64 기반 16바이트 형식의 볼륨에 대한 전역적으로 고유한 SCSI 디바이스 식별자입니다.
- **scsiNADeviceID**: NAA IEEE 등록 확장 형식의 볼륨에 대한 전역적으로 고유한 SCSI 장치 식별자입니다.
- * 특성 *: JSON 개체 형식의 이름 값 쌍 목록입니다.

가상 볼륨을 삭제합니다

가상 볼륨은 항상 VMware 관리 계층에서 삭제해야 하지만 가상 볼륨을 삭제하는 기능은 Element UI에서 사용하도록 설정됩니다. vSphere에서 SolidFire 스토리지의 가상 볼륨을 정리하지 못하는 경우와 같이 꼭 필요한 경우에만 Element UI에서 가상 볼륨을 삭제해야 합니다.

1. VVol * > * Virtual Volumes * 를 선택합니다.
2. 삭제할 가상 볼륨에 대한 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 선택합니다.

> 가상 볼륨을 삭제하기 전에 먼저 VMware Management Layer에서 가상 볼륨을 삭제하여 가상 볼륨을 적절히 바인딩 해제해야 합니다. vSphere에서 SolidFire 스토리지의 가상 볼륨을 정리하지 못하는 경우와 같이 꼭 필요한 경우에만 Element UI에서 가상 볼륨을 삭제해야 합니다. Element UI에서 가상 볼륨을 삭제하면 볼륨이 즉시 제거됩니다.

4. 작업을 확인합니다.
5. 가상 볼륨 목록을 새로 고쳐 가상 볼륨이 제거되었는지 확인합니다.
6. * 선택 사항 *: * 보고 * > * 이벤트 로그 * 를 선택하여 퍼지가 성공했는지 확인합니다.

스토리지 컨테이너는 Element 소프트웨어를 실행하는 클러스터에서 생성된 vSphere 데이터 저장소 표현입니다.

스토리지 컨테이너는 NetApp Element 계정에 생성되고 연결되어 있습니다. Element 스토리지에 생성된 스토리지 컨테이너는 vCenter 및 ESXi에서 vSphere 데이터 저장소로 표시됩니다. 스토리지 컨테이너는 Element 스토리지에 공간을 할당하지 않습니다. 가상 볼륨을 논리적으로 연결하는 데 사용됩니다.

클러스터당 최대 4개의 스토리지 컨테이너가 지원됩니다. VVOL 기능을 활성화하려면 최소 하나의 스토리지 컨테이너가 필요합니다.

스토리지 컨테이너를 생성합니다

Element UI에서 스토리지 컨테이너를 생성하고 vCenter에서 검색할 수 있습니다. VVOL 지원 가상 머신 프로비저닝을 시작하려면 하나 이상의 스토리지 컨테이너를 생성해야 합니다.

시작하기 전에 클러스터의 Element UI에서 VVOL 기능을 활성화합니다.

단계

1. VVol * > * Storage Containers * 를 선택합니다.
2. Create Storage Containers * 버튼을 클릭합니다.
3. Create a New Storage Container * (새 저장소 컨테이너 생성 *) 대화 상자에 저장소 컨테이너 정보를 입력합니다.
   a. 저장소 컨테이너의 이름을 입력합니다.
   b. CHAP에 대한 이니시에이터 및 타겟 암호를 구성합니다.

      CHAP 설정 필드를 비워 두면 자동으로 암호가 생성됩니다.

   c. Create Storage Container * 버튼을 클릭합니다.
4. 새 저장소 컨테이너가 * 저장소 컨테이너 * 하위 탭의 목록에 나타나는지 확인합니다.

   NetApp Element 계정 ID는 자동으로 생성되어 저장소 컨테이너에 할당되므로 계정을 수동으로 생성할 필요가 없습니다.

저장소 컨테이너 세부 정보를 봅니다

VVol 탭의 Storage Containers 페이지에서 클러스터의 모든 활성 저장소 컨테이너에 대한 정보를 볼 수 있습니다.

- * 계정 ID *: 저장소 컨테이너와 연결된 NetApp Element 계정의 ID입니다.
- * 이름 *: 저장소 컨테이너의 이름입니다.
- * 상태 *: 저장소 컨테이너의 상태입니다. 가능한 값:
  - Active(활성): 저장소 컨테이너가 사용 중입니다.
  - 잠김: 저장소 컨테이너가 잠겨 있습니다.
- * PE 유형 *: 프로토콜 엔드포인트 유형(SCSI는 Element 소프트웨어에 대해 사용 가능한 유일한 프로토콜입니다).
- * 저장소 컨테이너 ID *: 가상 볼륨 저장소 컨테이너의 UUID

- * 활성 가상 볼륨 *: 스토리지 컨테이너와 연결된 활성 가상 볼륨의 수입니다.

개별 저장소 컨테이너 세부 정보를 봅니다

VVol 탭의 Storage Containers(저장소 컨테이너) 페이지에서 선택하여 개별 저장소 컨테이너의 저장소 컨테이너 정보를 볼 수 있습니다.

- * 계정 ID *: 저장소 컨테이너와 연결된 NetApp Element 계정의 ID입니다.
- * 이름 *: 저장소 컨테이너의 이름입니다.
- * 상태 *: 저장소 컨테이너의 상태입니다. 가능한 값:
  - Active(활성): 저장소 컨테이너가 사용 중입니다.
  - 잠김: 저장소 컨테이너가 잠겨 있습니다.
- * CHAP 초기자 암호 *: 초기자에 대한 고유한 CHAP 암호입니다.
- * CHAP 대상 암호 *: 타겟의 고유한 CHAP 암호입니다.
- * 저장소 컨테이너 ID *: 가상 볼륨 저장소 컨테이너의 UUID
- * Protocol Endpoint Type * : 프로토콜 엔드포인트 유형을 나타냅니다(SCSI는 유일한 사용 가능 프로토콜입니다).

저장소 컨테이너를 편집합니다

Element UI에서 스토리지 컨테이너 CHAP 인증을 수정할 수 있습니다.

1. VVol * > * Storage Containers * 를 선택합니다.
2. 편집할 저장 컨테이너의 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Edit * 를 선택합니다.
4. CHAP 설정 에서 인증에 사용되는 초기자 암호 및 대상 암호 자격 증명을 편집합니다.

> CHAP 설정 자격 증명을 변경하지 않으면 자격 증명은 그대로 유지됩니다. 자격 증명 필드를 비워 두면 시스템에서 자동으로 새 암호를 생성합니다.

5. 변경 내용 저장 * 을 클릭합니다.

저장소 컨테이너를 삭제합니다

Element UI에서 스토리지 컨테이너를 삭제할 수 있습니다.

필요한 것

모든 가상 머신이 VVol 데이터 저장소에서 제거되었는지 확인합니다.

단계

1. VVol * > * Storage Containers * 를 선택합니다.
2. 삭제할 저장소 컨테이너의 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 선택합니다.
4. 작업을 확인합니다.

5. 저장소 컨테이너 * 하위 탭의 저장소 컨테이너 목록을 새로 고쳐 저장소 컨테이너가 제거되었는지 확인합니다.

프로토콜 엔드포인트

프로토콜 엔드포인트는 호스트에서 NetApp Element 소프트웨어를 실행하는 클러스터의 스토리지를 해결하기 위해 사용하는 액세스 포인트입니다. 프로토콜 끝점은 사용자가 삭제하거나 수정할 수 없으며, 계정과 연결되어 있지 않으며, 볼륨 액세스 그룹에 추가할 수 없습니다.

Element 소프트웨어를 실행하는 클러스터는 클러스터의 스토리지 노드당 하나의 프로토콜 엔드포인트를 자동으로 생성합니다. 예를 들어, 6노드 스토리지 클러스터에는 각 ESXi 호스트에 매핑된 6개의 프로토콜 엔드포인트가 있습니다. 프로토콜 엔드포인트는 Element 소프트웨어에 의해 동적으로 관리되며 아무런 개입 없이 필요에 따라 생성, 이동 또는 제거됩니다. 프로토콜 엔드포인트는 경로 다중화를 위한 타겟이며 자회사 LUN의 I/O 프록시 역할을 합니다. 각 프로토콜 끝점은 표준 iSCSI 타겟과 마찬가지로 사용 가능한 SCSI 주소를 사용합니다. 프로토콜 엔드포인트는 vSphere Client에서 단일 블록(512바이트) 스토리지 디바이스로 나타나지만 이 스토리지 디바이스는 스토리지 형식으로 포맷하거나 사용할 수 없습니다.

iSCSI는 유일하게 지원되는 프로토콜입니다. Fibre Channel 프로토콜은 지원되지 않습니다.

프로토콜 엔드포인트 세부 정보

VVol 탭의 Protocol Endpoints(프로토콜 엔드포인트) 페이지는 프로토콜 엔드포인트 정보를 제공합니다.

- * 기본 공급자 ID *

  기본 프로토콜 끝점 공급자의 ID입니다.

- * 보조 제공자 ID *

  보조 프로토콜 엔드포인트 공급자의 ID입니다.

- * 프로토콜 엔드포인트 ID *

  프로토콜 종점의 UUID입니다.

- * 프로토콜 엔드포인트 상태 *

  프로토콜 끝점의 상태. 가능한 값은 다음과 같습니다.

  - Active(활성): 프로토콜 끝점이 사용 중입니다.
  - Start(시작): 프로토콜 끝점이 시작됩니다.
  - 페일오버: 프로토콜 엔드포인트가 페일오버되었습니다.
  - 예약됨: 프로토콜 엔드포인트가 예약되었습니다.

- * 공급자 유형 *

  프로토콜 끝점의 공급자 유형입니다. 가능한 값은 다음과 같습니다.

  - 기본
  - 보조

- * SCSI NAA 장치 ID *

  NAA IEEE Registered Extended Format의 프로토콜 종점에 대한 전역적으로 고유한 SCSI 장치 식별자입니다.

바인딩

가상 볼륨에서 입출력 작업을 수행하려면 ESXi 호스트가 먼저 가상 볼륨을 바인딩해야 합니다.

SolidFire 클러스터는 최적의 프로토콜 엔드포인트를 선택하고 ESXi 호스트 및 가상 볼륨을 프로토콜 끝점과 연결하는 바인딩을 생성한 다음 ESXi 호스트에 대한 바인딩을 반환합니다. 바인딩한 후 ESXi 호스트는 바인딩된 가상 볼륨에서 입출력 작업을 수행할 수 있습니다.

바인딩 세부 정보

VVol 탭의 바인딩 페이지에서는 각 가상 볼륨에 대한 바인딩 정보를 제공합니다.

다음 정보가 표시됩니다.

- * 호스트 ID *

  가상 볼륨을 호스팅하고 클러스터에 알려진 ESXi 호스트의 UUID입니다.

- * 프로토콜 엔드포인트 ID *

  SolidFire 클러스터의 각 노드에 해당하는 프로토콜 엔드포인트 ID입니다.

- * 대역 ID * 의 프로토콜 엔드포인트

  프로토콜 끝점의 SCSI NAA 장치 ID입니다.

- * 프로토콜 엔드포인트 유형 *

  프로토콜 엔드포인트 유형입니다.

- * VVol Binding ID *

  가상 볼륨의 바인딩 UUID입니다.

- * VVol ID *

  가상 볼륨의 UUID(Universally Unique Identifier)입니다.

- * VVOL 보조 ID *

  SCSI 2차 레벨 LUN ID인 가상 볼륨의 2차 ID입니다.

호스트 세부 정보입니다

가상 볼륨을 호스팅하는 VMware ESXi 호스트에 대한 정보는 VVol 탭의 Hosts 페이지에 나와 있습니다.

다음 정보가 표시됩니다.

- * 호스트 ID *

  가상 볼륨을 호스팅하고 클러스터에 알려진 ESXi 호스트의 UUID입니다.

- * 호스트 주소 *

  ESXi 호스트의 IP 주소 또는 DNS 이름입니다.

- * 바인딩 *

  ESXi 호스트에 바인딩된 모든 가상 볼륨의 바인딩 ID입니다.

- * ESX 클러스터 ID *

  vSphere 호스트 클러스터 ID 또는 vCenter GUID.

- * 초기자 IQN *

  가상 볼륨 호스트에 대한 이니시에이터 IQN입니다.

- * SolidFire 프로토콜 엔드포인트 ID *

  현재 ESXi 호스트에 표시되는 프로토콜 엔드포인입니다.

볼륨 액세스 그룹 및 이니시에이터와 작업합니다

iSCSI 이니시에이터 또는 Fibre Channel 이니시에이터를 사용하여 볼륨 액세스 그룹 내에 정의된 볼륨에 액세스할 수 있습니다.

볼륨 컬렉션에 iSCSI 이니시에이터 IQN 또는 파이버 채널 WWPN을 매핑하여 액세스 그룹을 생성할 수 있습니다. 액세스 그룹에 추가하는 각 IQN은 CHAP 인증 없이 그룹의 각 볼륨에 액세스할 수 있습니다.

CHAP 인증 방법에는 두 가지가 있습니다.

- 계정 수준 CHAP 인증: 계정에 CHAP 인증을 할당할 수 있습니다.
- 이니시에이터 수준 CHAP 인증: 단일 계정의 단일 CHAP에 바인딩되지 않고 특정 이니시에이터에 대한 고유 CHAP 대상 및 암호를 할당할 수 있습니다. 이 이니시에이터 레벨 CHAP 인증은 계정 레벨 자격 증명을 대체합니다.

필요에 따라 이니시에이터당 CHAP를 사용하여 이니시에이터 인증 및 이니시에이터당 CHAP 인증을 적용할 수 있습니다. 이러한 옵션은 이니시에이터별로 정의할 수 있으며 액세스 그룹에는 다양한 옵션이 있는 여러 이니시에이터가 포함될 수 있습니다.

액세스 그룹에 추가하는 각 WWPN은 액세스 그룹의 볼륨에 대한 파이버 채널 네트워크 액세스를 설정합니다.

볼륨 액세스 그룹은 다음과 같은 제한 사항이 있습니다.

- 액세스 그룹에는 최대 64개의 IQN 또는 WWPN이 허용됩니다.
- 액세스 그룹은 최대 2000개의 볼륨으로 구성할 수 있습니다.

- IQN 또는 WWPN은 하나의 액세스 그룹에만 속할 수 있습니다.
- 단일 볼륨은 최대 4개의 액세스 그룹에 속할 수 있습니다.

자세한 내용을 확인하십시오

- 볼륨 액세스 그룹을 생성합니다
- 액세스 그룹에 볼륨을 추가합니다
- 액세스 그룹에서 볼륨을 제거합니다
- 이니시에이터를 생성합니다
- 이니시에이터를 편집합니다
- 볼륨 액세스 그룹에 단일 이니시에이터를 추가합니다
- 볼륨 액세스 그룹에 여러 이니시에이터를 추가합니다
- 액세스 그룹에서 이니시에이터를 제거합니다
- 액세스 그룹을 삭제합니다
- 이니시에이터를 삭제합니다

볼륨 액세스 그룹을 생성합니다

보안 액세스를 위해 이니시에이터를 볼륨 컬렉션에 매핑하여 볼륨 액세스 그룹을 생성할 수 있습니다. 그런 다음 계정 CHAP 이니시에이터 암호 및 대상 암호를 사용하여 그룹의 볼륨에 대한 액세스 권한을 부여할 수 있습니다.

이니시에이터 기반 CHAP를 사용하는 경우 볼륨 액세스 그룹의 단일 이니시에이터에 대한 CHAP 자격 증명을 추가하여 보안을 강화할 수 있습니다. 따라서 이미 존재하는 볼륨 액세스 그룹에 이 옵션을 적용할 수 있습니다.

단계

1. 관리 * > * 액세스 그룹 * 을 클릭합니다.
2. Create Access Group * 을 클릭합니다.
3. 이름 * 필드에 볼륨 액세스 그룹의 이름을 입력합니다.
4. 다음 방법 중 하나로 볼륨 액세스 그룹에 이니시에이터를 추가합니다.

옵션을 선택합니다	설명
Fibre Channel 이니시에이터 추가	a. 이니시에이터 추가 아래의 Unbound Fibre Channel 이니시에이터 목록에서 기존 Fibre Channel 이니시에이터를 선택합니다. b. FC 이니시에이터 추가 * 를 클릭합니다. 이 단계에서 * 이니시에이터 생성 * 링크를 클릭하고 이니시에이터 이름을 입력한 다음 * 생성 * 을 클릭하면 이니시에이터를 생성할 수 있습니다. 이니시에이터 목록을 생성하면 이니시에이터가 자동으로 이니시에이터 목록에 추가됩니다. 형식의 예는 다음과 같습니다. `5f:47:ac:c0:5c:74:d4:02`
iSCSI 이니시에이터 추가	이니시에이터 추가 아래의 이니시에이터 목록에서 기존 이니시에이터를 선택합니다. * 참고: * 이 단계에서 * 이니시에이터 생성 * 링크를 클릭하고 이니시에이터 이름을 입력한 다음 * 생성 * 을 클릭하면 이니시에이터를 생성할 수 있습니다. 이니시에이터 목록을 생성하면 이니시에이터가 자동으로 이니시에이터 목록에 추가됩니다. 형식의 예는 다음과 같습니다. `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` Management * > * Volumes * > * Active * 목록의 볼륨에 대한 Actions 메뉴에서 * View Details * 를 선택하여 각 볼륨의 이니시에이터 IQN을 찾을 수 있습니다. 이니시에이터를 수정할 때 requiredCHAP 속성을 True로 전환하면 타겟 이니시에이터 암호를 설정할 수 있습니다. 자세한 내용은 ModifyInitiator API 메서드에 대한 API 정보를 참조하십시오. "Element API를 사용하여 스토리지를 관리합니다"

5. * 선택 사항: * 필요에 따라 이니시에이터를 더 추가합니다.
6. Add Volumes 아래의 * Volumes * 목록에서 볼륨을 선택합니다.

   볼륨이 * Attached Volumes * 목록에 나타납니다.
7. * 선택 사항: * 필요에 따라 볼륨을 더 추가합니다.
8. Create Access Group * 을 클릭합니다.

자세한 내용을 확인하십시오

액세스 그룹에 볼륨을 추가합니다

개별 액세스 그룹 세부 정보를 봅니다

연결된 볼륨 및 이니시에이터와 같은 개별 액세스 그룹의 세부 정보를 그래픽 형식으로 볼 수 있습니다.

1. 관리 * > * 액세스 그룹 * 을 클릭합니다.
2. 액세스 그룹에 대한 작업 아이콘을 클릭합니다.
3. 세부 정보 보기 * 를 클릭합니다.

볼륨 액세스 그룹 세부 정보

관리 탭의 액세스 그룹 페이지에서는 볼륨 액세스 그룹에 대한 정보를 제공합니다.

다음 정보가 표시됩니다.

- * ID *: 액세스 그룹에 대해 시스템에서 생성한 ID입니다.
- * 이름 *: 액세스 그룹을 생성할 때 지정한 이름입니다.
- * 활성 볼륨 *: 액세스 그룹의 활성 볼륨 수입니다.
- * 압축 *: 액세스 그룹의 압축 효율성 점수입니다.
- * 중복 제거 *: 액세스 그룹의 중복 제거 효율성 점수입니다.
- * 씬 프로비저닝 *: 액세스 그룹의 씬 프로비저닝 효율성 점수입니다.
- * Overall Efficiency *: 액세스 그룹의 전체 효율성 점수입니다.
- * 이니시에이터 *: 액세스 그룹에 연결된 이니시에이터 수입니다.

액세스 그룹에 볼륨을 추가합니다

볼륨 액세스 그룹에 볼륨을 추가할 수 있습니다. 각 볼륨은 둘 이상의 볼륨 액세스 그룹에 속할 수 있습니다. 각 볼륨이 속한 그룹은 * Active * 볼륨 페이지에서 볼 수 있습니다.

이 절차를 사용하여 Fibre Channel 볼륨 액세스 그룹에 볼륨을 추가할 수도 있습니다.

1. 관리 * > * 액세스 그룹 * 을 클릭합니다.
2. 볼륨을 추가할 액세스 그룹의 작업 아이콘을 클릭합니다.
3. 편집 * 버튼을 클릭합니다.
4. Add Volumes 아래의 * Volumes * 목록에서 볼륨을 선택합니다.

   이 단계를 반복하여 볼륨을 더 추가할 수 있습니다.

5. 변경 내용 저장 * 을 클릭합니다.

액세스 그룹에서 볼륨을 제거합니다

액세스 그룹에서 볼륨을 제거하면 해당 그룹은 더 이상 해당 볼륨에 액세스할 수 없습니다.

계정의 CHAP 설정을 수정하거나 액세스 그룹에서 이니시에이터 또는 볼륨을 제거하면 초기자가 예기치 않게 볼륨에 액세스할 수 없게 될 수 있습니다. 볼륨 액세스가 예기치 않게 손실되지 않는지 확인하려면 계정 또는 액세스 그룹 변경의 영향을 받는 iSCSI 세션을 항상 로그아웃하고 이니시에이터 설정 및 클러스터 설정을 변경한 후 초기자가 볼륨에 다시 연결할 수 있는지 확인합니다.

1. 관리 * > * 액세스 그룹 * 을 클릭합니다.
2. 볼륨을 제거할 액세스 그룹에 대한 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. Edit Volume Access Group * (볼륨 액세스 그룹 편집 *) 대화 상자의 Add Volumes (볼륨 추가)에서 * Attached Volumes * (연결된 볼륨 *) 목록의 화살표를 클릭합니다.
5. 목록에서 제거할 볼륨을 선택하고 * x * 아이콘을 클릭하여 목록에서 볼륨을 제거합니다.

   이 단계를 반복하여 더 많은 볼륨을 제거할 수 있습니다.

6. 변경 내용 저장 * 을 클릭합니다.

이니시에이터를 생성합니다

iSCSI 또는 파이버 채널 이니시에이터를 생성하고 선택적으로 별칭을 할당할 수 있습니다.

API 호출을 사용하여 이니시에이터 기반 CHAP 특성을 할당할 수도 있습니다. 이니시에이터당 CHAP 계정 이름과 자격 증명을 추가하려면 "CreateInitiator" API 호출을 사용하여 CHAP 액세스 및 특성을 제거하고 추가해야 합니다. "CreateInitiators" 및 "ModifyInitiators" API 호출을 통해 하나 이상의 virtualNetworkID를 지정하여 이니시에이터 액세스를 하나 이상의 VLAN으로 제한할 수 있습니다. 가상 네트워크를 지정하지 않으면 이니시에이터는 모든 네트워크에 액세스할 수 있습니다.

자세한 내용은 API 참조 정보를 참조하십시오."Element API를 사용하여 스토리지를 관리합니다"

단계

1. 관리 * > * 이니시에이터 * 를 클릭합니다.
2. 이니시에이터 생성 * 을 클릭합니다.
3. 다음 단계를 수행하여 단일 이니시에이터 또는 여러 이니시에이터를 생성합니다.

옵션을 선택합니다	단계
단일 이니시에이터를 생성합니다	a. Create a Single Initiator * 를 클릭합니다. b. IQN/WWPN * 필드에 이니시에이터의 IQN 또는 WWPN을 입력합니다. c. 별칭 * 필드에 초기자의 이름을 입력합니다. d. 이니시에이터 생성 * 을 클릭합니다.

옵션을 선택합니다	단계
여러 이니시에이터를 생성합니다	a. 이니시에이터 대량 생성 * 을 클릭합니다. b. 텍스트 상자에 IQN 또는 WWPN 목록을 입력합니다. c. 이니시에이터 추가 * 를 클릭합니다. d. 결과 목록에서 이니시에이터를 선택하고 * Alias * 열에서 해당하는 추가 아이콘을 클릭하여 이니시에이터의 별칭을 추가합니다. e. 확인 표시를 클릭하여 새 별칭을 확인합니다. f. 이니시에이터 생성 * 을 클릭합니다.

이니시에이터를 편집합니다

기존 이니시에이터의 별칭을 변경하거나 별칭이 없는 경우 추가할 수 있습니다.

이니시에이터당 CHAP 계정 이름과 자격 증명을 추가하려면 ModfyInitiator API 호출을 사용하여 CHAP 액세스 및 속성을 제거하고 추가해야 합니다.

을 참조하십시오 "Element API를 사용하여 스토리지를 관리합니다".

단계

1. 관리 * > * 이니시에이터 * 를 클릭합니다.
2. 편집할 이니시에이터에 대한 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. Alias * 필드에 초기자의 새 별칭을 입력합니다.
5. 변경 내용 저장 * 을 클릭합니다.

볼륨 액세스 그룹에 단일 이니시에이터를 추가합니다

기존 볼륨 액세스 그룹에 이니시에이터를 추가할 수 있습니다.

볼륨 액세스 그룹에 이니시에이터를 추가하면 해당 이니시에이터는 해당 볼륨 액세스 그룹의 모든 볼륨에 액세스할 수 있습니다.

> 작업 아이콘을 클릭한 다음 활성 볼륨 목록에서 볼륨에 대해 * 세부 정보 보기 * 를 선택하면 각 볼륨의 이니시에이터를 찾을 수 있습니다.

이니시에이터 기반 CHAP를 사용하는 경우 볼륨 액세스 그룹의 단일 이니시에이터에 대한 CHAP 자격 증명을 추가하여 보안을 강화할 수 있습니다. 따라서 이미 존재하는 볼륨 액세스 그룹에 이 옵션을 적용할 수 있습니다.

단계

1. 관리 * > * 액세스 그룹 * 을 클릭합니다.
2. 편집할 액세스 그룹의 * 작업 * 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.

4. 볼륨 액세스 그룹에 Fibre Channel 이니시에이터를 추가하려면 다음 단계를 수행하십시오.

   a. 이니시에이터 추가 아래의 * Unbound Fibre Channel Initiators * 목록에서 기존 Fibre Channel 이니시에이터를 선택합니다.

   b. FC 이니시에이터 추가 * 를 클릭합니다.

   > 이 단계에서 * 이니시에이터 생성 * 링크를 클릭하고 이니시에이터 이름을 입력한 다음 * 생성 * 을 클릭하면 이니시에이터를 생성할 수 있습니다. 이니시에이터를 생성하면 * Initiators * 목록에 자동으로 추가됩니다.

   형식의 예는 다음과 같습니다.

```
5f:47:ac:c0:5c:74:d4:02
```

5. iSCSI 이니시에이터를 볼륨 액세스 그룹에 추가하려면 이니시에이터 추가 아래의 * 이니시에이터 * 목록에서 기존 이니시에이터를 선택합니다.

   > 이 단계에서 * 이니시에이터 생성 * 링크를 클릭하고 이니시에이터 이름을 입력한 다음 * 생성 * 을 클릭하면 이니시에이터를 생성할 수 있습니다. 이니시에이터를 생성하면 * Initiators * 목록에 자동으로 추가됩니다.

   이니시에이터 IQN에서 허용되는 형식은 iqn.yyyy-mm이며, 여기서 y와 m은 숫자이고, 그 뒤에 숫자, 소문자 알파벳 문자, 마침표(.), 콜론(:) 또는 대시(-)만 포함되어야 하는 텍스트가 옵니다.

   형식의 예는 다음과 같습니다.

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

   > Actions 아이콘을 클릭한 다음 볼륨에 대해 * View Details * 를 선택하여 * Management * > * Volumes * Active Volumes 페이지에서 각 볼륨의 이니시에이터 IQN을 찾을 수 있습니다.

6. 변경 내용 저장 * 을 클릭합니다.

볼륨 액세스 그룹에 여러 이니시에이터를 추가합니다

CHAP 인증을 사용하거나 사용하지 않고 볼륨 액세스 그룹의 볼륨에 액세스할 수 있도록 기존 볼륨 액세스 그룹에 여러 이니시에이터를 추가할 수 있습니다.

볼륨 액세스 그룹에 이니시에이터를 추가하면 해당 이니시에이터는 해당 볼륨 액세스 그룹의 모든 볼륨에 액세스할 수 있습니다.

> 활성 볼륨 목록에서 작업 아이콘을 클릭한 다음 볼륨에 대한 * 세부 정보 보기 * 를 클릭하여 각 볼륨의 이니시에이터를 찾을 수 있습니다.

기존 볼륨 액세스 그룹에 여러 이니시에이터를 추가하여 볼륨에 대한 액세스를 설정하고 해당 볼륨 액세스 그룹 내의 각 이니시에이터에 대해 고유한 CHAP 자격 증명을 할당할 수 있습니다. 따라서 이미 존재하는 볼륨 액세스 그룹에 이

옵션을 적용할 수 있습니다.

API 호출을 사용하여 이니시에이터 기반 CHAP 특성을 할당할 수 있습니다. 이니시에이터당 CHAP 계정 이름 및 자격 증명을 추가하려면 ModifyInitiator API 호출을 사용하여 CHAP 액세스 및 특성을 제거하고 추가해야 합니다.

자세한 내용은 을 참조하십시오 "Element API를 사용하여 스토리지를 관리합니다".

단계

1. 관리 * > * 이니시에이터 * 를 클릭합니다.
2. 액세스 그룹에 추가할 이니시에이터를 선택합니다.
3. 대량 작업 * 버튼을 클릭합니다.
4. 볼륨 액세스 그룹에 추가 * 를 클릭합니다.
5. 볼륨 액세스 그룹에 추가 대화 상자의 * 볼륨 액세스 그룹 * 목록에서 액세스 그룹을 선택합니다.
6. 추가 * 를 클릭합니다.

액세스 그룹에서 이니시에이터를 제거합니다

액세스 그룹에서 이니시에이터를 제거하면 해당 볼륨 액세스 그룹의 볼륨에 더 이상 액세스할 수 없습니다. 볼륨에 대한 일반 계정 액세스가 중단되지 않습니다.

계정의 CHAP 설정을 수정하거나 액세스 그룹에서 이니시에이터 또는 볼륨을 제거하면 초기자가 예기치 않게 볼륨에 액세스할 수 없게 될 수 있습니다. 볼륨 액세스가 예기치 않게 손실되지 않는지 확인하려면 계정 또는 액세스 그룹 변경의 영향을 받는 iSCSI 세션을 항상 로그아웃하고 이니시에이터 설정 및 클러스터 설정을 변경한 후 초기자가 볼륨에 다시 연결할 수 있는지 확인합니다.

단계

1. 관리 * > * 액세스 그룹 * 을 클릭합니다.
2. 제거할 액세스 그룹에 대한 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Edit * 를 선택합니다.
4. Edit Volume Access Group * 대화 상자의 Add Initiators 아래에서 * Initiators * 목록의 화살표를 클릭합니다.
5. 액세스 그룹에서 제거할 각 이니시에이터에 대해 x 아이콘을 선택합니다.
6. 변경 내용 저장 * 을 클릭합니다.

액세스 그룹을 삭제합니다

더 이상 필요하지 않은 액세스 그룹을 삭제할 수 있습니다. 그룹을 삭제하기 전에 볼륨 액세스 그룹에서 이니시에이터 ID 및 볼륨 ID를 삭제할 필요가 없습니다. 액세스 그룹을 삭제하면 볼륨에 대한 그룹 액세스가 중단됩니다.

1. 관리 * > * 액세스 그룹 * 을 클릭합니다.
2. 삭제할 액세스 그룹의 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 클릭합니다.
4. 이 액세스 그룹과 연결된 이니시에이터도 삭제하려면 * 이 액세스 그룹에서 이니시에이터 삭제 * 확인란을 선택합니다.

5. 작업을 확인합니다.

이니시에이터를 삭제합니다

더 이상 필요하지 않은 이니시에이터를 삭제할 수 있습니다. 이니시에이터를 삭제하면 연결된 볼륨 액세스 그룹에서 이니시에이터가 제거됩니다. 초기자를 사용하는 모든 연결은 연결이 재설정될 때까지 유효합니다.

단계

1. 관리 * > * 이니시에이터 * 를 클릭합니다.
2. 단일 이니시에이터 또는 여러 이니시에이터를 삭제하는 단계를 수행합니다.

옵션을 선택합니다	단계
단일 이니시에이터를 삭제합니다	a. 삭제하려는 이니시에이터에 대한 * 작업 * 아이콘을 클릭합니다. b. 삭제 * 를 클릭합니다. c. 작업을 확인합니다.
여러 이니시에이터를 삭제합니다	a. 삭제할 이니시에이터 옆의 확인란을 선택합니다. b. 대량 작업 * 버튼을 클릭합니다. c. 결과 메뉴에서 * 삭제 * 를 선택합니다. d. 작업을 확인합니다.

데이터 보호

NetApp Element 소프트웨어를 사용하면 개별 볼륨 또는 볼륨 그룹에 대한 스냅샷, Element에서 실행되는 클러스터와 볼륨 간 복제, ONTAP 시스템에 복제 등과 같은 기능을 사용하여 데이터를 다양한 방법으로 보호할 수 있습니다.

- 스냅샷 *

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

  데이터 보호를 위해 볼륨 스냅샷을 사용합니다

- * Element * 에서 실행되는 클러스터와 볼륨 간의 원격 복제

  장애 조치 및 장애 복구 시나리오를 위해 Element에서 실행 중인 클러스터 쌍 중 하나에서 볼륨 데이터를 동기적 또는 비동기적으로 복제할 수 있습니다.

  NetApp Element 소프트웨어를 실행하는 클러스터 간에 원격 복제를 수행합니다

- * SnapMirror 기술을 사용하여 Element와 ONTAP 클러스터 간 복제 *

NetApp SnapMirror 기술을 사용하면 재해 복구를 위해 Element를 사용하여 생성한 스냅샷을 ONTAP에 복제할 수 있습니다. SnapMirror 관계에서 Element는 하나의 엔드포인트이고 ONTAP는 다른 엔드포인트입니다.

Element 및 ONTAP 클러스터 간 SnapMirror 복제 사용

- * SolidFire, S3 또는 Swift 오브젝트 저장소 * 에서 볼륨을 백업 및 복원합니다

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

  SolidFire, S3 또는 Swift 오브젝트 저장소에 볼륨을 백업 및 복원합니다

를 참조하십시오

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

데이터 보호를 위해 볼륨 스냅샷을 사용합니다

볼륨 스냅샷은 볼륨의 시점 복제본입니다. 볼륨을 스냅샷이 생성된 시점의 상태로 롤백해야 하는 경우 볼륨의 스냅샷을 생성한 후 나중에 스냅샷을 사용할 수 있습니다.

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

개별 볼륨 또는 볼륨 세트의 스냅샷을 생성할 수 있습니다.

필요에 따라 스냅샷을 원격 클러스터로 복제하고 볼륨의 백업 복사본으로 사용합니다. 이렇게 하면 복제된 스냅샷을 사용하여 볼륨을 특정 시점으로 롤백할 수 있습니다. 또는 복제된 스냅샷으로부터 볼륨의 클론을 생성할 수 있습니다.

자세한 내용을 확인하십시오

- 데이터 보호를 위해 개별 볼륨 스냅샷을 사용합니다
- 데이터 보호 작업에 그룹 스냅샷 사용
- 스냅샷 예약

데이터 보호를 위해 개별 볼륨 스냅샷을 사용합니다

볼륨 스냅샷은 볼륨의 시점 복제본입니다. 스냅샷에 대한 볼륨 그룹 대신 개별 볼륨을 사용할 수 있습니다.

자세한 내용을 확인하십시오

- 볼륨 스냅샷을 생성합니다
- 스냅샷 보존 편집
- 스냅샷을 삭제하는 중입니다

- 스냅숏에서 볼륨 클론 생성
- 볼륨을 스냅샷으로 롤백하는 중입니다
- 볼륨 스냅샷을 Amazon S3 오브젝트 저장소에 백업
- OpenStack Swift 오브젝트 저장소에 볼륨 스냅샷 백업
- SolidFire 클러스터에 볼륨 스냅샷 백업

볼륨 스냅샷을 생성합니다

활성 볼륨의 스냅샷을 생성하여 언제든지 볼륨 이미지를 보존할 수 있습니다. 단일 볼륨에 대해 최대 32개의 스냅샷을 생성할 수 있습니다.

1. Management * > * Volumes * 를 클릭합니다.
2. 스냅숏에 사용할 볼륨의 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Snapshot * 을 선택합니다.
4. 볼륨 스냅샷 생성 * 대화 상자에서 새 스냅샷 이름을 입력합니다.
5. * 선택 사항: * 상위 볼륨이 페어링될 때 복제에 스냅샷이 캡처되도록 하려면 * 쌍으로 된 경우 복제에 스냅샷 포함 * 확인란을 선택합니다.
6. 스냅샷에 대한 보존을 설정하려면 다음 옵션 중 하나를 선택합니다.
   - 영구 유지 * 를 클릭하여 시스템에 스냅샷을 무한정 유지합니다.
   - 보존 기간 설정 * 을 클릭하고 날짜 스핀 상자를 사용하여 시스템에서 스냅샷을 보존할 기간을 선택합니다.
7. 즉각적인 단일 스냅샷을 생성하려면 다음 단계를 수행하십시오.
   a. 지금 스냅샷 촬영 * 을 클릭합니다.
   b. 스냅샷 생성 을 클릭합니다.
8. 스냅샷이 나중에 실행되도록 예약하려면 다음 단계를 수행하십시오.
   a. 스냅샷 일정 생성 * 을 클릭합니다.
   b. 새 일정 이름 * 을 입력합니다.
   c. 목록에서 * 스케줄 유형 * 을 선택합니다.
   d. * 선택 사항: * 예약된 스냅샷을 주기적으로 반복하려면 * 반복 일정 * 확인란을 선택합니다.
   e. Create Schedule * 을 클릭합니다.

자세한 내용을 확인하십시오

스냅샷을 예약합니다

스냅샷 보존 편집

스냅샷의 보존 기간을 변경하여 스냅샷이 삭제되는 시기와 시기를 제어할 수 있습니다. 지정한 보존 기간은 새 간격을 입력할 때 시작됩니다. 보존 기간을 설정할 때 현재 시간에 시작되는 기간을 선택할 수 있습니다(스냅샷 생성 시간으로부터 보존이 계산되지 않음). 분, 시간 및 일 단위로 간격을 지정할 수 있습니다.

단계

1. 데이터 보호 * > * 스냅샷 * 을 클릭합니다.
2. 편집할 스냅샷의 * Actions * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 편집 * 을 클릭합니다.
4. * 선택 사항: * 상위 볼륨이 페어링될 때 복제에서 스냅샷이 캡처되도록 하려면 쌍으로 된 경우 복제에 스냅샷 포함 확인란을 선택합니다.
5. * 선택 사항: * 스냅샷에 대한 보존 옵션을 선택합니다.
   - 영구 유지 * 를 클릭하여 시스템에 스냅샷을 무한정 유지합니다.
   - 보존 기간 설정 * 을 클릭하고 날짜 스핀 상자를 사용하여 시스템에서 스냅샷을 보존할 기간을 선택합니다.
6. 변경 내용 저장 * 을 클릭합니다.

스냅샷을 삭제합니다

Element 소프트웨어를 실행하는 스토리지 클러스터에서 볼륨 스냅샷을 삭제할 수 있습니다. 스냅샷을 삭제하면 시스템에서 즉시 스냅샷을 제거합니다.

소스 클러스터에서 복제 중인 스냅샷을 삭제할 수 있습니다. 스냅샷을 삭제할 때 스냅샷이 타겟 클러스터와 동기화되는 경우 동기화 복제가 완료되고 소스 클러스터에서 스냅샷이 삭제됩니다. 스냅샷이 타겟 클러스터에서 삭제되지 않습니다.

타겟 클러스터에서 타겟으로 복제된 스냅샷을 삭제할 수도 있습니다. 삭제된 스냅샷은 소스 클러스터에서 스냅샷을 삭제했다는 것을 시스템이 감지할 때까지 타겟의 삭제된 스냅샷 목록에 유지됩니다. 타겟이 소스 스냅샷을 삭제했다는 것을 감지하면 타겟은 스냅샷 복제를 중지합니다.

소스 클러스터에서 스냅샷을 삭제하면 타겟 클러스터 스냅샷도 영향을 받지 않습니다(반대의 경우도 마찬가지임).

1. 데이터 보호 * > * 스냅샷 * 을 클릭합니다.
2. 삭제할 스냅샷에 대한 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 선택합니다.
4. 작업을 확인합니다.

스냅숏에서 볼륨의 클론을 생성합니다

볼륨의 스냅숏에서 새 볼륨을 생성할 수 있습니다. 이렇게 하면 시스템이 스냅샷 정보를 사용하여 스냅샷을 생성할 때 볼륨에 포함된 데이터를 사용하여 새 볼륨을 복제합니다. 이 프로세스는 새로 생성된 볼륨에 있는 볼륨의 다른 스냅샷에 대한 정보를 저장합니다.

1. 데이터 보호 * > * 스냅샷 * 을 클릭합니다.
2. 볼륨 클론에 사용할 스냅샷에 대한 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Clone Volume from Snapshot * 을 클릭합니다.
4. 스냅샷에서 볼륨 클론 * 대화 상자에 * 볼륨 이름 * 을 입력합니다.
5. 새 볼륨의 * 총 크기 * 와 크기 단위를 선택합니다.
6. 볼륨에 대한 * Access * 유형을 선택합니다.
7. 목록에서 새 볼륨과 연결할 * 계정 * 을 선택합니다.

8. 클로닝 시작 * 을 클릭합니다.

볼륨을 스냅샷으로 롤백합니다

언제든지 볼륨을 이전 스냅샷으로 롤백할 수 있습니다. 이렇게 하면 스냅샷이 생성된 이후 볼륨에 대한 모든 변경 사항이 복구됩니다.

단계

1. 데이터 보호 * > * 스냅샷 * 을 클릭합니다.
2. 볼륨 롤백에 사용할 스냅샷의 * Actions * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Rollback Volume to Snapshot * 을 선택합니다.
4. * 선택 사항: * 스냅샷으로 롤백하기 전에 볼륨의 현재 상태를 저장하려면:
   a. 스냅샷으로 롤백 * 대화 상자에서 * 볼륨의 현재 상태를 스냅샷으로 저장 * 을 선택합니다.
   b. 새 스냅샷의 이름을 입력합니다.
5. 스냅샷 롤백 * 을 클릭합니다.

볼륨 스냅샷을 백업합니다

통합 백업 기능을 사용하여 볼륨 스냅샷을 백업할 수 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.

- "볼륨 스냅샷을 Amazon S3 오브젝트 저장소에 백업합니다"
- "OpenStack Swift 오브젝트 저장소에 볼륨 스냅샷을 백업합니다"
- "볼륨 스냅샷을 SolidFire 클러스터에 백업합니다"

볼륨 스냅샷을 **Amazon S3** 오브젝트 저장소에 백업합니다

SolidFire S3와 호환되는 외부 오브젝트 저장소에 스냅샷을 백업할 수 있습니다.

1. 데이터 보호>* 스냅샷*을 클릭합니다.
2. 백업하려는 스냅샷의 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Backup to * 를 클릭합니다.
4. 통합 백업 * 대화 상자의 * 백업 대상 * 에서 * S3 * 를 선택합니다.
5. 데이터 형식 * 에서 옵션을 선택합니다.
   - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
   - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
6. 호스트 이름 * 필드에 개체 저장소에 액세스하는 데 사용할 호스트 이름을 입력합니다.
7. 계정의 액세스 키 ID를 * 액세스 키 ID * 필드에 입력합니다.
8. 비밀 액세스 키 * 필드에 계정의 비밀 액세스 키를 입력합니다.

9. 백업을 저장할 S3 버킷을 * S3 Bucket * 필드에 입력합니다.
10. * 선택 사항 *: * nametag * 필드의 접두사에 추가할 이름 태그를 입력합니다.
11. 읽기 시작 * 을 클릭합니다.

OpenStack Swift 오브젝트 저장소에 볼륨 스냅샷을 백업합니다

SolidFire 스냅샷을 OpenStack Swift와 호환되는 2차 오브젝트 저장소에 백업할 수 있습니다.

1. 데이터 보호 * > * 스냅샷 * 을 클릭합니다.
2. 백업하려는 스냅샷의 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Backup to * 를 클릭합니다.
4. 통합 백업 * 대화 상자의 * 백업 대상 * 에서 * Swift * 를 선택합니다.
5. 데이터 형식 * 에서 옵션을 선택합니다.
    - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
    - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
6. 오브젝트 저장소에 액세스하는 데 사용할 * URL * 을 입력합니다.
7. 계정의 * 사용자 이름 * 을 입력합니다.
8. 계정의 * 인증 키 * 를 입력합니다.
9. 백업을 저장할 * 컨테이너 * 를 입력합니다.
10. * 선택 사항 *: * nametag * 을 입력합니다.
11. 읽기 시작 * 을 클릭합니다.

볼륨 스냅샷을 **SolidFire** 클러스터에 백업합니다

SolidFire 클러스터에 있는 볼륨 스냅샷을 원격 SolidFire 클러스터에 백업할 수 있습니다.

소스 및 타겟 클러스터가 페어링되었는지 확인합니다.

한 클러스터에서 다른 클러스터로 백업하거나 복구할 때 시스템은 클러스터 간 인증으로 사용할 키를 생성합니다. 이 대량 볼륨 쓰기 키를 사용하면 소스 클러스터가 대상 클러스터에 인증되어 대상 볼륨에 쓸 때 보안 수준을 제공할 수 있습니다. 백업 또는 복원 프로세스의 일부로 작업을 시작하기 전에 대상 볼륨에서 대량 볼륨 쓰기 키를 생성해야 합니다.

1. 대상 클러스터에서 * 관리 * > * 볼륨 * 을 클릭합니다.
2. 대상 볼륨에 대한 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Restore from * 을 클릭합니다.
4. 통합 복원 * 대화 상자의 * 복원 위치 * 에서 * SolidFire * 를 선택합니다.
5. 데이터 형식 * 에서 데이터 형식을 선택합니다.
    - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
    - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.

6. 키 생성 * 을 클릭합니다.
7. Bulk Volume Write Key *(대량 볼륨 쓰기 키) 상자의 키를 클립보드로 복사합니다.
8. 소스 클러스터에서 * 데이터 보호 * > * 스냅샷 * 을 클릭합니다.
9. 백업에 사용할 스냅샷의 작업 아이콘을 클릭합니다.
10. 결과 메뉴에서 * Backup to * 를 클릭합니다.
11. 통합 백업** 대화 상자의 * 백업 대상 * 아래에서 * SolidFire * 를 선택합니다.
12. 데이터 형식 * 필드에서 이전에 선택한 것과 동일한 데이터 형식을 선택합니다.
13. 원격 클러스터 MVIP * 필드에 대상 볼륨 클러스터의 관리 가상 IP 주소를 입력합니다.
14. 원격 클러스터 사용자 이름 * 필드에 원격 클러스터 사용자 이름을 입력합니다.
15. 원격 클러스터 암호 * 필드에 원격 클러스터 암호를 입력합니다.
16. Bulk Volume Write Key * (대량 볼륨 쓰기 키 *) 필드에서 이전에 대상 클러스터에서 생성한 키를 붙여 넣습니다.
17. 읽기 시작 * 을 클릭합니다.

데이터 보호 작업에 그룹 스냅샷 사용

관련 볼륨 세트의 그룹 스냅샷을 생성하여 각 볼륨의 메타데이터 시점 복사본을 보존할 수 있습니다. 나중에 그룹 스냅샷을 백업 또는 롤백으로 사용하여 볼륨 그룹의 상태를 이전 상태로 복원할 수 있습니다.

자세한 내용을 확인하십시오

- 그룹 스냅샷을 생성합니다
- 그룹 스냅샷을 편집합니다
- 그룹 스냅샷의 구성원을 편집합니다
- 그룹 스냅샷을 삭제합니다
- 볼륨을 그룹 스냅샷으로 롤백합니다
- 여러 볼륨의 클론을 생성합니다
- 그룹 스냅샷에서 여러 볼륨의 클론을 생성합니다

그룹 스냅샷 세부 정보

데이터 보호 탭의 그룹 스냅샷 페이지에서는 그룹 스냅샷에 대한 정보를 제공합니다.

- * ID *

  그룹 스냅샷에 대한 시스템 생성 ID입니다.

- * UUID *

  그룹 스냅샷의 고유 ID입니다.

- * 이름 *

그룹 스냅샷에 대한 사용자 정의 이름입니다.

- * 생성 시간 *

  그룹 스냅샷이 생성된 시간입니다.

- * 상태 *

  스냅샷의 현재 상태입니다. 가능한 값:

  - 준비: 스냅샷을 사용할 준비가 되어 있으며 아직 쓸 수 없습니다.
  - 완료: 이 스냅샷은 준비를 완료했으며 이제 사용할 수 있습니다.
  - Active(활성): 스냅샷이 활성 분기입니다.

- * # 볼륨 *

  그룹에 있는 볼륨의 수입니다.

- * 보존 기간 *

  스냅샷이 삭제되는 요일 및 시간입니다.

- * 원격 복제 *

  원격 SolidFire 클러스터로의 복제에 대해 스냅샷이 설정되었는지 여부를 나타냅니다. 가능한 값:

  - Enabled(사용): 원격 복제에 대해 스냅샷이 설정되었습니다.
  - Disabled(사용 안 함): 원격 복제에 대해 스냅샷이 사용되지 않습니다.

그룹 스냅샷 생성

볼륨 그룹의 스냅샷을 생성할 수 있으며 그룹 스냅샷 스케줄을 생성하여 그룹 스냅샷을 자동화할 수도 있습니다. 단일 그룹 스냅샷은 한 번에 최대 32개의 볼륨을 일관되게 스냅샷할 수 있습니다.

단계

1. Management * > * Volumes * 를 클릭합니다.
2. 확인란을 사용하여 볼륨 그룹에 대해 여러 볼륨을 선택합니다.
3. 대량 작업 * 을 클릭합니다.
4. 그룹 스냅샷 * 을 클릭합니다.
5. Create Group Snapshot of Volumes(볼륨의 그룹 스냅샷 생성) 대화 상자에 새 그룹 스냅샷 이름을 입력합니다.
6. * 선택 사항: * 상위 볼륨이 페어링될 때 각 스냅샷이 복제에 캡처되도록 * Include each Group Snapshot Member in Replication when paired * 확인란을 선택합니다.
7. 그룹 스냅샷에 대한 보존 옵션을 선택합니다.
   - 영구 유지 * 를 클릭하여 시스템에 스냅샷을 무한정 유지합니다.
   - 보존 기간 설정 * 을 클릭하고 날짜 스핀 상자를 사용하여 시스템에서 스냅샷을 보존할 기간을 선택합니다.
8. 즉각적인 단일 스냅샷을 생성하려면 다음 단계를 수행하십시오.

a. 지금 그룹 스냅샷 생성 * 을 클릭합니다.

b. 그룹 스냅샷 생성 * 을 클릭합니다.

9. 스냅샷이 나중에 실행되도록 예약하려면 다음 단계를 수행하십시오.

a. Create Group Snapshot Schedule * 을 클릭합니다.

b. 새 일정 이름 * 을 입력합니다.

c. 목록에서 * 스케줄 유형 * 을 선택합니다.

d. * 선택 사항: * 예약된 스냅샷을 주기적으로 반복하려면 * 반복 일정 * 확인란을 선택합니다.

e. Create Schedule * 을 클릭합니다.

그룹 스냅샷 편집

기존 그룹 스냅샷에 대한 복제 및 보존 설정을 편집할 수 있습니다.

1. 데이터 보호 * > * 그룹 스냅샷 * 을 클릭합니다.
2. 편집할 그룹 스냅숏의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Edit * 를 선택합니다.
4. * 선택 사항: * 그룹 스냅샷의 복제 설정을 변경하려면:

a. 현재 복제 * 옆에 있는 * 편집 * 을 클릭합니다.

b. 상위 볼륨이 페어링될 때 각 스냅샷이 복제에서 캡처되도록 하려면 * Include each Group Snapshot Member in Replication when paired * 확인란을 선택합니다.

5. * 선택 사항: * 그룹 스냅샷의 보존 설정을 변경하려면 다음 옵션 중 하나를 선택합니다.

a. Current Retention * 옆에 있는 * Edit * 를 클릭합니다.

b. 그룹 스냅샷에 대한 보존 옵션을 선택합니다.

- 영구 유지 * 를 클릭하여 시스템에 스냅샷을 무한정 유지합니다.
- 보존 기간 설정 * 을 클릭하고 날짜 스핀 상자를 사용하여 시스템에서 스냅샷을 보존할 기간을 선택합니다.

6. 변경 내용 저장 * 을 클릭합니다.

그룹 스냅샷 삭제

시스템에서 그룹 스냅샷을 삭제할 수 있습니다. 그룹 스냅샷을 삭제할 때 그룹과 연결된 모든 스냅샷을 개별 스냅샷으로 삭제 또는 보존할지 여부를 선택할 수 있습니다.

그룹 스냅샷의 구성원인 볼륨이나 스냅샷을 삭제하면 더 이상 그룹 스냅샷으로 롤백할 수 없습니다. 그러나 각 볼륨을 개별적으로 롤백할 수 있습니다.

1. 데이터 보호 * > * 그룹 스냅샷 * 을 클릭합니다.
2. 삭제할 스냅샷에 대한 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 클릭합니다.
4. 확인 대화 상자에서 다음 옵션 중 하나를 선택합니다.

- 그룹 스냅샷 및 모든 구성원 스냅샷을 삭제하려면 * 그룹 스냅샷 및 모든 그룹 스냅샷 구성원 삭제 * 를

클릭합니다.

- 그룹 스냅샷 구성원을 개별 스냅샷으로 유지 * 를 클릭하여 그룹 스냅샷을 삭제하지만 모든 구성원 스냅샷은 유지합니다.

5. 작업을 확인합니다.

볼륨을 그룹 스냅샷으로 롤백합니다

언제든지 볼륨 그룹을 그룹 스냅샷으로 롤백할 수 있습니다.

볼륨 그룹을 롤백하면 그룹의 모든 볼륨이 그룹 스냅샷이 생성된 시점의 상태로 복구됩니다. 또한 롤백하면 볼륨 크기가 원래 스냅샷에 기록된 크기로 복원됩니다. 시스템에서 볼륨을 제거한 경우 해당 볼륨의 모든 스냅숏도 삭제 시점에 삭제되었으며 시스템은 삭제된 볼륨 스냅숏을 복원하지 않습니다.

1. 데이터 보호 * > * 그룹 스냅샷 * 을 클릭합니다.
2. 볼륨 롤백에 사용할 그룹 스냅숏의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Rollback Volumes to Group Snapshot * 을 선택합니다.
4. * 선택 사항 *: 스냅샷으로 롤백하기 전에 볼륨의 현재 상태를 저장하려면
   a. 스냅샷으로 롤백 * 대화 상자에서 * 볼륨의 현재 상태를 그룹 스냅샷으로 저장 * 을 선택합니다.
   b. 새 스냅샷의 이름을 입력합니다.
5. 그룹 스냅샷 롤백 * 을 클릭합니다.

그룹 스냅샷의 구성원 편집

기존 그룹 스냅샷의 구성원에 대한 보존 설정을 편집할 수 있습니다.

1. 데이터 보호 * > * 스냅샷 * 을 클릭합니다.
2. 구성원 * 탭을 클릭합니다.
3. 편집할 그룹 스냅샷 구성원의 작업 아이콘을 클릭합니다.
4. 결과 메뉴에서 * Edit * 를 선택합니다.
5. 스냅샷의 복제 설정을 변경하려면 다음 옵션 중에서 선택합니다.
   - 영구 유지 * 를 클릭하여 시스템에 스냅샷을 무한정 유지합니다.
   - 보존 기간 설정 * 을 클릭하고 날짜 스핀 상자를 사용하여 시스템에서 스냅샷을 보존할 기간을 선택합니다.
6. 변경 내용 저장 * 을 클릭합니다.

여러 볼륨의 클론을 생성합니다

단일 작업으로 여러 볼륨 클론을 생성하여 볼륨 그룹에 있는 데이터의 시점 복사본을 생성할 수 있습니다.

볼륨을 클론하면 시스템에서 볼륨의 스냅샷을 생성한 다음 스냅샷의 데이터에서 새 볼륨을 생성합니다. 새 볼륨 클론을 마운트하고 쓸 수 있습니다. 여러 볼륨의 클론 복제는 비동기식 프로세스이며 클론 복제할 볼륨의 크기와 수에 따라 시간이 달라집니다.

볼륨 크기와 현재 클러스터 로드는 클론 복제 작업을 완료하는 데 필요한 시간에 영향을 줍니다.

단계

1. Management * > * Volumes * 를 클릭합니다.
2. Active * 탭을 클릭합니다.
3. 확인란을 사용하여 여러 볼륨을 선택하고 볼륨 그룹을 생성합니다.
4. 대량 작업 * 을 클릭합니다.
5. 결과 메뉴에서 * Clone * 을 클릭합니다.
6. 여러 볼륨 클론 * 대화 상자에 * 새 볼륨 이름 접두사 * 를 입력합니다.

   접두사는 그룹의 모든 볼륨에 적용됩니다.

7. * 선택 사항: * 클론이 속할 다른 계정을 선택합니다.

   계정을 선택하지 않으면 시스템에서 새 볼륨을 현재 볼륨 계정에 할당합니다.

8. * 선택 사항: * 클론의 볼륨에 대해 다른 액세스 방법을 선택합니다.

   액세스 방법을 선택하지 않으면 시스템이 현재 볼륨 액세스를 사용합니다.

9. 클로닝 시작 * 을 클릭합니다.

그룹 스냅샷에서 여러 볼륨을 클론 생성합니다

시점 그룹 스냅샷에서 볼륨 그룹을 복제할 수 있습니다. 그룹 스냅샷은 볼륨을 생성하기 위한 기반으로 사용되므로 이 작업을 수행하려면 볼륨의 그룹 스냅샷이 이미 있어야 합니다. 볼륨을 생성한 후에는 시스템의 다른 볼륨과 마찬가지로 사용할 수 있습니다.

볼륨 크기와 현재 클러스터 로드는 클론 복제 작업을 완료하는 데 필요한 시간에 영향을 줍니다.

1. 데이터 보호 * > * 그룹 스냅샷 * 을 클릭합니다.
2. 볼륨 클론에 사용할 그룹 스냅숏의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Clone Volumes from Group Snapshot * 을 선택합니다.
4. 그룹 스냅샷의 볼륨 클론 * 대화 상자에 * 새 볼륨 이름 접두사 * 를 입력합니다.

   접두사는 그룹 스냅샷으로부터 생성된 모든 볼륨에 적용됩니다.

5. * 선택 사항: * 클론이 속할 다른 계정을 선택합니다.

   계정을 선택하지 않으면 시스템에서 새 볼륨을 현재 볼륨 계정에 할당합니다.

6. * 선택 사항: * 클론의 볼륨에 대해 다른 액세스 방법을 선택합니다.

   액세스 방법을 선택하지 않으면 시스템이 현재 볼륨 액세스를 사용합니다.

7. 클로닝 시작 * 을 클릭합니다.

스냅샷을 예약합니다

볼륨 스냅샷이 지정된 간격으로 발생하도록 예약하여 볼륨 또는 볼륨 그룹의 데이터를 보호할 수 있습니다. 단일 볼륨 스냅샷이나 그룹 스냅샷이 자동으로 실행되도록 예약할 수 있습니다.

스냅샷 스케줄을 구성할 때 해당 월의 일 또는 일을 기준으로 시간 간격 중에서 선택할 수 있습니다. 다음 스냅샷이 발생하기 전 일, 시간 및 분을 지정할 수도 있습니다. 볼륨이 복제되는 경우 원격 스토리지 시스템에 결과 스냅샷을 저장할 수 있습니다.

자세한 내용을 확인하십시오

- 스냅샷 스케줄을 생성합니다
- 스냅샷 스케줄을 편집합니다
- 스냅샷 스케줄을 삭제합니다
- 스냅샷 스케줄을 복제합니다

스냅샷 스케줄 세부 정보입니다

데이터 보호 > 스케줄 페이지에서 스냅샷 스케줄 목록에서 다음 정보를 볼 수 있습니다.

- * ID *

  스냅샷에 대한 시스템 생성 ID입니다.

- * 유형 *

  일정 유형입니다. 스냅샷은 현재 지원되는 유일한 유형입니다.

- * 이름 *

  일정이 생성될 때 지정한 이름입니다. 스냅샷 스케줄 이름은 최대 223자까지 가능하며 a-z, 0-9 및 대시(-) 문자를 포함할 수 있습니다.

- * 주파수 *

  스케줄이 실행되는 빈도입니다. 빈도는 시간 및 분, 주 또는 월 단위로 설정할 수 있습니다.

- * 반복 *

  일정이 한 번만 실행되는지 또는 일정한 간격으로 실행되는지 여부를 나타냅니다.

- * 수동 일시 중지됨 *

  스케줄이 수동으로 일시 중지되었는지 여부를 나타냅니다.

- * 볼륨 ID *

  스케줄이 실행될 때 스케줄에서 사용할 볼륨의 ID입니다.

- * 마지막 러닝 *

스케줄이 마지막으로 실행된 시간입니다.

- * 마지막 실행 상태 *

  마지막 일정 실행의 결과. 가능한 값:

  - 성공
  - 실패

스냅샷 스케줄을 생성합니다

지정된 간격으로 볼륨 또는 볼륨의 스냅샷이 자동으로 발생하도록 예약할 수 있습니다.

스냅샷 스케줄을 구성할 때 해당 월의 일 또는 일을 기준으로 시간 간격 중에서 선택할 수 있습니다. 또한 반복 스케줄을 생성하고 다음 스냅샷이 발생하기 전 일, 시간 및 분을 지정할 수 있습니다.

5분 동안 나눌 수 없는 기간에 스냅샷을 실행하도록 예약하는 경우 5분 동안 나눌 수 있는 다음 기간에 스냅샷이 실행됩니다. 예를 들어 스냅샷을 12:42:00 UTC에서 실행하도록 예약하는 경우 12:45:00 UTC에서 실행됩니다. 5분 미만의 간격으로 실행되도록 스냅샷을 예약할 수 없습니다.

단계

1. 데이터 보호 * > * 스케줄 * 을 클릭합니다.
2. Create Schedule * 을 클릭합니다.
3. 볼륨 ID CSV * 필드에 스냅샷 작업에 포함할 단일 볼륨 ID 또는 쉼표로 구분된 볼륨 ID 목록을 입력합니다.
4. 새 일정 이름을 입력합니다.
5. 일정 유형을 선택하고 제공된 옵션에서 일정을 설정합니다.
6. * 선택 사항: * 반복 일정 * 을 선택하여 스냅샷 일정을 무한정 반복합니다.
7. * 선택 사항: * 새 스냅샷 이름 * 필드에 새 스냅샷의 이름을 입력합니다.

   필드를 비워 두면 스냅샷 생성 날짜와 시간이 이름으로 사용됩니다.

8. * 선택 사항: * 부모 볼륨이 페어링될 때 복제에 스냅샷이 캡처되도록 하려면 * 쌍으로 된 경우 복제에 스냅샷 포함 * 확인란을 선택합니다.
9. 스냅샷에 대한 보존을 설정하려면 다음 옵션 중에서 선택합니다.
   - 영구 유지 * 를 클릭하여 시스템에 스냅샷을 무한정 유지합니다.
   - 보존 기간 설정 * 을 클릭하고 날짜 스핀 상자를 사용하여 시스템에서 스냅샷을 보존할 기간을 선택합니다.
10. Create Schedule * 을 클릭합니다.

스냅샷 스케줄을 편집합니다

기존 스냅샷 스케줄을 수정할 수 있습니다. 수정 후 다음 번에 스케줄이 실행될 때 업데이트된 속성이 사용됩니다. 원래 스케줄에 의해 생성된 모든 스냅샷은 스토리지 시스템에 남아 있습니다.

단계

1. 데이터 보호 * > * 스케줄 * 을 클릭합니다.

2. 변경할 일정에 대한 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 편집 * 을 클릭합니다.
4. 볼륨 ID CSV * 필드에서 스냅샷 작업에 현재 포함되어 있는 단일 볼륨 ID 또는 쉼표로 구분된 볼륨 ID 목록을 수정합니다.
5. 일정을 일시 중지하거나 다시 시작하려면 다음 옵션 중에서 선택합니다.
   - 활성 일정을 일시 중지하려면 * 수동 일정 일시 중지 * 목록에서 * 예 * 를 선택합니다.
   - 일시 중지된 일정을 다시 시작하려면 * 수동 일정 일시 중지 * 목록에서 * 아니요 * 를 선택합니다.
6. 원하는 경우 * New Schedule Name * (새 일정 이름 *) 필드에 일정에 대한 다른 이름을 입력합니다.
7. 주별 또는 월의 다른 요일에 실행되도록 스케줄을 변경하려면 * Schedule Type * 을 선택하고 제공된 옵션에서 스케줄을 변경합니다.
8. * 선택 사항: * 반복 일정 * 을 선택하여 스냅샷 일정을 무한정 반복합니다.
9. * 선택 사항: * 새 스냅샷 이름 * 필드에 새 스냅샷의 이름을 입력하거나 수정합니다.

   필드를 비워 두면 스냅샷 생성 날짜와 시간이 이름으로 사용됩니다.

10. * 선택 사항: * 부모 볼륨이 페어링될 때 복제에 스냅샷이 캡처되도록 하려면 * 쌍으로 된 경우 복제에 스냅샷 포함 * 확인란을 선택합니다.
11. 보존 설정을 변경하려면 다음 옵션 중에서 선택합니다.
    - 영구 유지 * 를 클릭하여 시스템에 스냅샷을 무한정 유지합니다.
    - 보존 기간 설정 * 을 클릭하고 날짜 스핀 상자를 사용하여 시스템에서 스냅샷을 보존할 기간을 선택합니다.
12. 변경 내용 저장 * 을 클릭합니다.

스냅샷 스케줄을 복제합니다

스케줄을 복사하고 현재 속성을 유지 관리할 수 있습니다.

1. 데이터 보호 * > * 스케줄 * 을 클릭합니다.
2. 복사할 일정에 대한 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 복사본 만들기 * 를 클릭합니다.

   스케줄의 현재 속성이 채워진 * 일정 생성 * 대화 상자가 나타납니다.

4. * 선택 사항: * 새 스케줄의 이름과 업데이트된 속성을 입력합니다.
5. Create Schedule * 을 클릭합니다.

스냅샷 스케줄을 삭제합니다

스냅샷 스케줄을 삭제할 수 있습니다. 스케줄을 삭제한 후에는 예약된 스냅샷이 실행되지 않습니다. 스케줄에 따라 생성된 모든 스냅샷은 스토리지 시스템에 남아 있습니다.

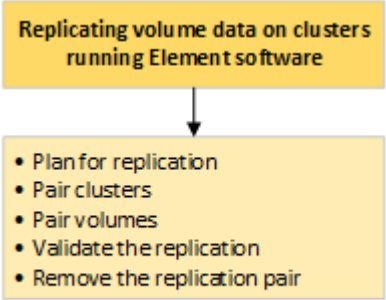
1. 데이터 보호 * > * 스케줄 * 을 클릭합니다.
2. 삭제할 일정에 대한 * 작업 * 아이콘을 클릭합니다.

3. 결과 메뉴에서 * 삭제 * 를 클릭합니다.
4. 작업을 확인합니다.

NetApp Element 소프트웨어를 실행하는 클러스터 간에 원격 복제를 수행합니다

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.

복제 프로세스에는 다음 단계가 포함됩니다.



- "실시간 복제를 위해 클러스터 및 볼륨 페어링을 계획합니다"
- "복제를 위해 클러스터를 쌍으로 설정합니다"
- "볼륨을 페어링합니다"
- "볼륨 복제를 확인합니다"
- "복제 후 볼륨 관계를 삭제합니다"
- "볼륨 관계 관리"

실시간 복제를 위해 클러스터 및 볼륨 페어링을 계획합니다

실시간 원격 복제를 수행하려면 Element 소프트웨어를 실행하는 두 스토리지 클러스터를 페어링하고, 각 클러스터에서 볼륨을 페어링하고, 복제를 확인해야 합니다. 복제가 완료되면 볼륨 관계를 삭제해야 합니다.

필요한 것

- 페어링되는 하나 또는 두 클러스터에 대한 클러스터 관리자 권한이 있어야 합니다.
- 페어링된 클러스터의 관리 및 스토리지 네트워크 모두에 있는 모든 노드 IP 주소는 서로 라우팅됩니다.
- 페어링된 모든 노드의 MTU는 동일해야 하며 클러스터 간 엔드 투 엔드를 지원해야 합니다.
- 두 스토리지 클러스터에는 고유한 클러스터 이름, MVIP, SVIP 및 모든 노드 IP 주소가 있어야 합니다.
- 클러스터의 Element 소프트웨어 버전 간의 차이는 하나의 주요 버전 이상일 수 없습니다. 차이가 크면 클러스터 중 하나를 업그레이드하여 데이터 복제를 수행해야 합니다.

NetApp은 데이터 복제 시 WAN 가속기 어플라이언스를 사용하지 않았습니다. 이러한 어플라이언스는 데이터를 복제하는 두 클러스터 간에 구축될 경우 압축 및 중복 제거를 방해할 수 있습니다. 프로덕션 환경에 배포하기 전에 WAN 가속기 어플라이언스의 효과를 완벽하게 검증해야 합니다.

자세한 내용을 확인하십시오

- 복제를 위해 클러스터를 쌍으로 설정합니다
- 볼륨을 페어링합니다
- 복제 소스와 타겟을 페어링된 볼륨에 할당합니다

복제를 위해 클러스터를 쌍으로 설정합니다

실시간 복제 기능을 사용하려면 먼저 두 클러스터를 페어링해야 합니다. 두 클러스터를 페어링하고 연결한 후, 한 클러스터의 활성 볼륨을 구성하여 두 번째 클러스터에 지속적으로 복제함으로써 CDP(무중단 데이터 보호)를 제공할 수 있습니다.

필요한 것

- 페어링되는 하나 또는 두 클러스터에 대한 클러스터 관리자 권한이 있어야 합니다.
- 모든 노드 MIP 및 SIP가 서로 라우팅됩니다.
- 클러스터 간 왕복 지연 시간 2000ms 미만
- 두 스토리지 클러스터에는 고유한 클러스터 이름, MVIP, SVIP 및 모든 노드 IP 주소가 있어야 합니다.
- 클러스터의 Element 소프트웨어 버전 간의 차이는 하나의 주요 버전 이상일 수 없습니다. 차이가 크면 클러스터 중 하나를 업그레이드하여 데이터 복제를 수행해야 합니다.

클러스터 페어링은 관리 네트워크의 노드 간에 완벽하게 연결되어 있어야 합니다. 복제를 수행하려면 스토리지 클러스터 네트워크의 개별 노드 간에 접속해야 합니다.

볼륨 복제를 위해 하나의 클러스터를 최대 4개의 다른 클러스터와 페어링할 수 있습니다. 클러스터 그룹 내의 클러스터를 서로 페어링할 수도 있습니다.

자세한 내용을 확인하십시오

네트워크 포트 요구 사항

MVIP 또는 페어링 키를 사용하여 클러스터를 페어링합니다

두 클러스터에 대한 클러스터 관리자 액세스 권한이 있는 경우 대상 클러스터의 MVIP를 사용하여 소스 클러스터와 타겟 클러스터를 페어링할 수 있습니다. 클러스터 관리자 액세스가 클러스터 쌍의 클러스터 한 클러스터에서만 사용 가능한 경우, 타겟 클러스터에서 페어링 키를 사용하여 클러스터 페어링을 완료할 수 있습니다.

1. 클러스터를 페어링하려면 다음 방법 중 하나를 선택합니다.
   - MVIP를 사용하여 클러스터 페어링: 두 클러스터에 대한 클러스터 관리자 액세스 권한이 있는 경우 이 방법을 사용합니다. 이 방법은 원격 클러스터의 MVIP를 사용하여 두 클러스터를 페어링합니다.
   - 페어링 키를 사용하여 클러스터 페어링: 클러스터 관리자 액세스 권한이 클러스터 중 하나에만 있는 경우 이

방법을 사용합니다. 이 방법은 타겟 클러스터에서 클러스터 페어링을 완료하는 데 사용할 수 있는 페어링 키를 생성합니다.

자세한 내용을 확인하십시오

- MVIP를 사용하여 클러스터를 페어링합니다
- 페어링 키를 사용하여 클러스터를 페어링합니다

MVIP를 사용하여 클러스터를 페어링합니다

한 클러스터의 MVIP를 사용하여 다른 클러스터와의 연결을 설정하여 실시간 복제를 위해 두 클러스터를 페어링할 수 있습니다. 이 방법을 사용하려면 두 클러스터 모두에서 클러스터 관리자 액세스가 필요합니다. 클러스터를 페어링하기 전에 클러스터 관리자 사용자 이름 및 암호를 사용하여 클러스터 액세스를 인증합니다.

1. 로컬 클러스터에서 * 데이터 보호 * > * 클러스터 쌍 * 을 선택합니다.
2. 클러스터 페어링 * 을 클릭합니다.
3. 페어링 시작 * 을 클릭하고 * 예 * 를 클릭하여 원격 클러스터에 액세스할 수 있음을 나타냅니다.
4. 원격 클러스터 MVIP 주소를 입력합니다.
5. 원격 클러스터에서 페어링 완료 * 를 클릭합니다.

   Authentication Required * (인증 필요 *) 창에서 원격 클러스터의 클러스터 관리자 사용자 이름과 암호를 입력합니다.

6. 원격 클러스터에서 * 데이터 보호 * > * 클러스터 쌍 * 을 선택합니다.
7. 클러스터 페어링 * 을 클릭합니다.
8. 페어링 완료 * 를 클릭합니다.
9. 페어링 완료 * 버튼을 클릭합니다.

자세한 내용을 확인하십시오

- 페어링 키를 사용하여 클러스터를 페어링합니다
- "MVIP를 사용한 클러스터 페어링(비디오)"

페어링 키를 사용하여 클러스터를 페어링합니다

원격 클러스터가 아닌 로컬 클러스터에 대한 클러스터 관리자 액세스 권한이 있는 경우 페어링 키를 사용하여 클러스터를 페어링할 수 있습니다. 로컬 클러스터에서 페어링 키가 생성된 후 원격 사이트의 클러스터 관리자에게 안전하게 전송되어 연결을 설정하고 실시간 복제를 위해 클러스터 페어링을 완료합니다.

1. 로컬 클러스터에서 * 데이터 보호 * > * 클러스터 쌍 * 을 선택합니다.
2. 클러스터 페어링 * 을 클릭합니다.
3. 페어링 시작 * 을 클릭하고 * 아니요 * 를 클릭하여 원격 클러스터에 액세스할 수 없음을 표시합니다.

4. 키 생성 * 을 클릭합니다.

> 이렇게 하면 페어링을 위한 텍스트 키가 생성되고 로컬 클러스터에 구성되지 않은 클러스터 쌍이 생성됩니다. 이 절차를 완료하지 않으면 클러스터 쌍을 수동으로 삭제해야 합니다.

5. 클러스터 페어링 키를 클립보드에 복사합니다.
6. 원격 클러스터 사이트의 클러스터 관리자가 페어링 키를 액세스할 수 있도록 합니다.

> 클러스터 페어링 키에는 원격 복제를 위한 볼륨 연결을 허용하는 MVIP 버전, 사용자 이름, 암호 및 데이터베이스 정보가 포함되어 있습니다. 이 키는 안전한 방식으로 취급해야 하며 사용자 이름 또는 암호에 우발적이거나 안전하지 않은 액세스를 허용하는 방식으로 저장되지 않아야 합니다.

> 페어링 키의 문자를 수정하지 마십시오. 키를 수정하면 키가 무효화됩니다.

7. 원격 클러스터에서 * 데이터 보호 * > * 클러스터 쌍 * 을 선택합니다.
8. 클러스터 페어링 * 을 클릭합니다.
9. 페어링 완료 * 를 클릭하고 * 페어링 키 * 필드에 페어링 키를 입력합니다(붙여넣기가 권장 방법임).
10. 페어링 완료 * 를 클릭합니다.

자세한 내용을 확인하십시오

- MVIP를 사용하여 클러스터를 페어링합니다
- "클러스터 페어링 키를 사용하여 클러스터 페어링(비디오)"

클러스터 쌍 연결을 확인합니다

클러스터 페어링이 완료된 후 클러스터 쌍 연결을 확인하여 복제가 성공했는지 확인할 수 있습니다.

1. 로컬 클러스터에서 * 데이터 보호 * > * 클러스터 쌍 * 을 선택합니다.
2. Cluster Pairs * 창에서 클러스터 페어가 연결되어 있는지 확인합니다.
3. * 선택 사항: * 로컬 클러스터와 * 클러스터 쌍 * 창으로 다시 이동하여 클러스터 쌍이 연결되었는지 확인합니다.

볼륨을 페어링합니다

클러스터 쌍의 클러스터 간에 연결을 설정한 후에는 한 클러스터의 볼륨을 해당 쌍의 다른 클러스터의 볼륨과 페어링할 수 있습니다. 볼륨 페어링 관계가 설정되면 어떤 볼륨이 복제 타겟인지 확인해야 합니다.

연결된 클러스터 쌍의 서로 다른 스토리지 클러스터에 저장된 실시간 복제를 위해 두 볼륨을 페어링할 수 있습니다. 두 클러스터를 쌍으로 지정한 후 한 클러스터의 활성 볼륨을 구성하여 두 번째 클러스터에 지속적으로 복제함으로써 CDP(무중단 데이터 보호)를 제공할 수 있습니다. 복제 소스 또는 타겟이 될 볼륨을 할당할 수도 있습니다.

볼륨 페어링은 항상 일대일 입니다. 볼륨이 다른 클러스터의 볼륨과 페어링의 일부이면 다른 볼륨과 다시 페어링할 수 없습니다.

필요한 것

- 클러스터 쌍의 클러스터 간에 연결이 설정되었습니다.
- 페어링되는 하나 또는 두 클러스터에 대한 클러스터 관리자 권한이 있습니다.

단계

1. 읽기 또는 쓰기 권한이 있는 타겟 볼륨을 생성합니다
2. 볼륨 ID 또는 페어링 키를 사용하여 볼륨을 페어링합니다
3. 복제 소스와 타겟을 페어링된 볼륨에 할당합니다

읽기 또는 쓰기 권한이 있는 타겟 볼륨을 생성합니다

복제 프로세스에는 소스 볼륨과 타겟 볼륨의 두 엔드포인트가 포함됩니다. 타겟 볼륨을 생성할 때 볼륨이 복제 중에 데이터를 수락하도록 읽기/쓰기 모드로 자동 설정됩니다.

1. Management * > * Volumes * 를 선택합니다.
2. Create Volume * 을 클릭합니다.
3. 새 볼륨 생성 대화 상자에서 볼륨 이름을 입력합니다.
4. 볼륨의 총 크기를 입력하고 볼륨의 블록 크기를 선택한 다음 볼륨에 액세스할 수 있는 계정을 선택합니다.
5. Create Volume * 을 클릭합니다.
6. Active(활성) 창에서 볼륨에 대한 Actions(작업) 아이콘을 클릭합니다.
7. 편집 * 을 클릭합니다.
8. 계정 액세스 수준을 복제 타겟으로 변경합니다.
9. 변경 내용 저장 * 을 클릭합니다.

볼륨 **ID** 또는 페어링 키를 사용하여 볼륨을 페어링합니다

페어링 프로세스는 볼륨 ID 또는 페어링 키를 사용하여 두 볼륨을 페어링하는 것입니다.

1. 다음 방법 중 하나를 선택하여 볼륨을 페어링합니다.
   - 볼륨 ID 사용: 볼륨을 페어링할 두 클러스터에 클러스터 관리자가 액세스할 수 있는 경우 이 방법을 사용합니다. 이 방법은 원격 클러스터에 있는 볼륨의 볼륨 ID를 사용하여 연결을 시작합니다.
   - 페어링 키 사용: 클러스터 관리자가 소스 클러스터에만 액세스할 수 있는 경우 이 방법을 사용합니다. 이 방법을 사용하면 원격 클러스터에서 볼륨 쌍을 완료하는 데 사용할 수 있는 페어링 키가 생성됩니다.

> ⓘ 볼륨 페어링 키는 볼륨 정보의 암호화된 버전을 포함하며 중요한 정보를 포함할 수 있습니다. 이 키는 안전한 방식으로만 공유합니다.

자세한 내용을 확인하십시오

- 볼륨 ID를 사용하여 볼륨을 페어링합니다
- 페어링 키를 사용하여 볼륨을 페어링합니다

볼륨 **ID**를 사용하여 볼륨을 페어링합니다

원격 클러스터에 대한 클러스터 관리자 자격 증명이 있는 경우 원격 클러스터의 다른 볼륨과 볼륨을 페어링할 수 있습니다.

필요한 것

- 볼륨이 포함된 클러스터가 페어링되었는지 확인합니다.
- 원격 클러스터에 새 볼륨을 생성합니다.

> 페어링 프로세스 후 복제 소스와 타겟을 할당할 수 있습니다. 복제 소스 또는 타겟은 볼륨 쌍의 볼륨일 수 있습니다. 데이터를 포함하지 않고 볼륨의 크기, 블록 크기 설정(512e 또는 4K) 및 QoS 구성과 같은 소스 볼륨의 정확한 특성을 가진 타겟 볼륨을 생성해야 합니다. 기존 볼륨을 복제 타겟으로 할당할 경우 해당 볼륨의 데이터를 덮어씁니다. 타겟 볼륨의 크기는 소스 볼륨과 같거나 더 클 수 있지만 크기는 작을 수 없습니다.

- 타겟 볼륨 ID를 확인합니다.

단계

1. Management * > * Volumes * 를 선택합니다.
2. 페어링할 볼륨의 * 작업 * 아이콘을 클릭합니다.
3. 페어링 * 을 클릭합니다.
4. 볼륨 페어링 * 대화 상자에서 * 페어링 시작 * 을 선택합니다.
5. 원격 클러스터에 액세스할 수 있음을 나타내려면 * I DO * 를 선택합니다.
6. 목록에서 * 복제 모드 * 를 선택합니다.
   - * 실시간(비동기식) *: 소스 클러스터에서 커밋된 쓰기가 클라이언트에 확인됩니다.
   - * 실시간(동기식) *: 쓰기가 소스 및 타겟 클러스터 모두에서 커밋된 후 클라이언트에 인식됩니다.
   - * 스냅샷만 *: 소스 클러스터에서 생성된 스냅샷만 복제됩니다. 소스 볼륨의 활성 쓰기는 복제되지 않습니다.
7. 목록에서 원격 클러스터를 선택합니다.
8. 원격 볼륨 ID를 선택합니다.
9. 페어링 시작 * 을 클릭합니다.

   시스템에서 원격 클러스터의 Element UI에 연결되는 웹 브라우저 탭을 엽니다. 클러스터 관리자 자격 증명을 사용하여 원격 클러스터에 로그온해야 할 수 있습니다.

10. 원격 클러스터의 Element UI에서 * Complete Pairing * 을 선택합니다.
11. 볼륨 페어링 확인 * 에서 세부 정보를 확인합니다.
12. 페어링 완료 * 를 클릭합니다.

    페어링을 확인한 후 두 클러스터는 페어링을 위해 볼륨을 연결하는 프로세스를 시작합니다. 페어링 프로세스 중에 * 볼륨 쌍 * 창의 * 볼륨 상태 * 열에 메시지가 표시됩니다. 볼륨 쌍 소스와 타겟이 할당될 때까지 볼륨 페어에 PausedMisconfigured가 표시됩니다.

    페어링을 완료한 후 볼륨 테이블을 새로 고쳐 페어링된 볼륨에 대한 * Actions * 목록에서 * Pair * 옵션을 제거해야 합니다. 테이블을 새로 고치지 않으면 * Pair * 옵션을 선택할 수 있습니다. 페어링 * 옵션을 다시 선택하면 새 탭이

열리고 볼륨이 이미 페어링되었기 때문에 시스템에서 를 보고합니다 `StartVolumePairing Failed: xVolumeAlreadyPaired` Element UI 페이지의 * Pair Volume * (볼륨 페어링 *) 창에 오류 메시지가 표시됩니다.

자세한 내용을 확인하십시오

- 볼륨 페어링 메시지
- 볼륨 페어링 경고
- 복제 소스와 타겟을 페어링된 볼륨에 할당합니다

페어링 키를 사용하여 볼륨을 페어링합니다

원격 클러스터에 대한 클러스터 관리자 자격 증명이 없는 경우 페어링 키를 사용하여 원격 클러스터의 다른 볼륨과 볼륨을 페어링할 수 있습니다.

필요한 것

- 볼륨이 포함된 클러스터가 페어링되었는지 확인합니다.
- 원격 클러스터에 페어링에 사용할 볼륨이 있는지 확인합니다.

> 페어링 프로세스 후 복제 소스와 타겟을 할당할 수 있습니다. 복제 소스 또는 타겟은 볼륨 쌍의 볼륨일 수 있습니다. 데이터를 포함하지 않고 볼륨의 크기, 블록 크기 설정(512e 또는 4K) 및 QoS 구성과 같은 소스 볼륨의 정확한 특성을 가진 타겟 볼륨을 생성해야 합니다. 기존 볼륨을 복제 타겟으로 할당할 경우 해당 볼륨의 데이터를 덮어씁니다. 타겟 볼륨의 크기는 소스 볼륨과 같거나 더 클 수 있지만 크기는 작을 수 없습니다.

단계

1. Management * > * Volumes * 를 선택합니다.
2. 페어링할 볼륨에 대해 * 작업 * 아이콘을 클릭합니다.
3. 페어링 * 을 클릭합니다.
4. 볼륨 페어링 * 대화 상자에서 * 페어링 시작 * 을 선택합니다.
5. 원격 클러스터에 대한 액세스 권한이 없음을 나타내려면 * 하지 않음 * 을 선택합니다.
6. 목록에서 * 복제 모드 * 를 선택합니다.
   - * 실시간(비동기식) *: 소스 클러스터에서 커밋된 쓰기가 클라이언트에 확인됩니다.
   - * 실시간(동기식) *: 쓰기가 소스 및 타겟 클러스터 모두에서 커밋된 후 클라이언트에 인식됩니다.
   - * 스냅샷만 *: 소스 클러스터에서 생성된 스냅샷만 복제됩니다. 소스 볼륨의 활성 쓰기는 복제되지 않습니다.
7. 키 생성 * 을 클릭합니다.

> 이렇게 하면 페어링을 위한 텍스트 키가 생성되고 로컬 클러스터에 구성되지 않은 볼륨 쌍이 생성됩니다. 이 절차를 완료하지 않으면 볼륨 쌍을 수동으로 삭제해야 합니다.

8. 페어링 키를 컴퓨터의 클립보드에 복사합니다.
9. 원격 클러스터 사이트의 클러스터 관리자가 페어링 키를 액세스할 수 있도록 합니다.

> 볼륨 페어링 키는 안전한 방식으로 취급해야 하며, 우발적 또는 비보안 액세스를 허용하는 방식으로 사용해서는 안 됩니다.

> 페어링 키의 문자를 수정하지 마십시오. 키를 수정하면 키가 무효화됩니다.

10. 원격 클러스터 요소 UI에서 * 관리 * > * 볼륨 * 을 선택합니다.
11. 페어링할 볼륨에 대한 작업 아이콘을 클릭합니다.
12. 페어링 * 을 클릭합니다.
13. 볼륨 페어링 * 대화 상자에서 * 페어링 완료 * 를 선택합니다.
14. 다른 클러스터의 페어링 키를 * 페어링 키 * 상자에 붙여 넣습니다.
15. 페어링 완료 * 를 클릭합니다.

    페어링을 확인한 후 두 클러스터는 페어링을 위해 볼륨을 연결하는 프로세스를 시작합니다. 페어링 프로세스 중에 * 볼륨 쌍 * 창의 * 볼륨 상태 * 열에 메시지가 표시됩니다. 볼륨 쌍 소스와 타겟이 할당될 때까지 볼륨 페어에 PausedMisconfigured가 표시됩니다.

    페어링을 완료한 후 볼륨 테이블을 새로 고쳐 페어링된 볼륨에 대한 * Actions * 목록에서 * Pair * 옵션을 제거해야 합니다. 테이블을 새로 고치지 않으면 * Pair * 옵션을 선택할 수 있습니다. 페어링 * 옵션을 다시 선택하면 새 탭이 열리고 볼륨이 이미 페어링되었기 때문에 시스템에서 를 보고합니다 `StartVolumePairing Failed: xVolumeAlreadyPaired` Element UI 페이지의 * Pair Volume * (볼륨 페어링 *) 창에 오류 메시지가 표시됩니다.

자세한 내용을 확인하십시오

- 볼륨 페어링 메시지
- 볼륨 페어링 경고
- 복제 소스와 타겟을 페어링된 볼륨에 할당합니다

복제 소스와 타겟을 페어링된 볼륨에 할당합니다

볼륨이 페어링된 후에는 소스 볼륨과 해당 복제 타겟 볼륨을 할당해야 합니다. 복제 소스 또는 타겟은 볼륨 쌍의 볼륨일 수 있습니다. 소스 볼륨을 사용할 수 없는 경우 소스 볼륨으로 전송된 데이터를 원격 타겟 볼륨으로 리디렉션하는 경우에도 이 절차를 사용할 수 있습니다.

필요한 것

소스 볼륨과 타겟 볼륨이 포함된 클러스터에 액세스할 수 있습니다.

단계

1. 소스 볼륨 준비:
    a. 소스로 할당할 볼륨이 포함된 클러스터에서 * Management * > * Volumes * 를 선택합니다.
    b. 소스로 할당할 볼륨의 * 작업 * 아이콘을 클릭하고 * 편집 * 을 클릭합니다.
    c. 액세스 * 드롭다운 목록에서 * 읽기/쓰기 * 를 선택합니다.

> 소스 및 타겟 할당을 반대로 전환하는 경우 이 작업을 수행하면 새 복제 타겟이 할당될 때까지 볼륨 쌍에 다음 메시지가 표시됩니다. "PausedMisconfigured"

액세스를 변경하면 볼륨 복제가 일시 중지되고 데이터 전송이 중지됩니다. 두 사이트에서 이러한 변경 내용을 조정했는지 확인합니다.

a. 변경 내용 저장 * 을 클릭합니다.

2. 타겟 볼륨 준비:

   a. 타겟으로 할당할 볼륨이 포함된 클러스터에서 * 관리 * > * 볼륨 * 을 선택합니다.

   b. 타겟으로 할당할 볼륨의 작업 아이콘을 클릭하고 * 편집 * 을 클릭합니다.

   c. Access * 드롭다운 목록에서 * Replication Target * 을 선택합니다.

   > 기존 볼륨을 복제 타겟으로 할당할 경우 해당 볼륨의 데이터를 덮어씁니다. 데이터가 없고 소스 볼륨의 정확한 특성(예: 크기, 512e 설정 및 QoS 구성)이 있는 새 타겟 볼륨을 사용해야 합니다. 타겟 볼륨의 크기는 소스 볼륨과 같거나 더 클 수 있지만 크기는 작을 수 없습니다.

   d. 변경 내용 저장 * 을 클릭합니다.

자세한 내용을 확인하십시오

- 볼륨 ID를 사용하여 볼륨을 페어링합니다
- 페어링 키를 사용하여 볼륨을 페어링합니다

볼륨 복제를 확인합니다

볼륨이 복제된 후에는 소스 볼륨과 타겟 볼륨이 활성 상태인지 확인해야 합니다. 활성 상태에서 볼륨이 페어링되면 데이터가 소스에서 타겟 볼륨으로 전송되고 데이터가 동기화됩니다.

1. 두 클러스터 모두에서 * 데이터 보호 * > * 볼륨 쌍 * 을 선택합니다.
2. 볼륨 상태가 활성인지 확인합니다.

자세한 내용을 확인하십시오

볼륨 페어링 경고

복제 후 볼륨 관계를 삭제합니다

복제가 완료되고 더 이상 볼륨 쌍 관계가 필요하지 않으면 볼륨 관계를 삭제할 수 있습니다.

1. 데이터 보호 * > * 볼륨 쌍 * 을 선택합니다.
2. 삭제하려는 볼륨 쌍의 * 작업 * 아이콘을 클릭합니다.
3. 삭제 * 를 클릭합니다.
4. 메시지를 확인합니다.

볼륨 관계 관리

복제 일시 중지, 볼륨 페어링 되돌리기, 복제 모드 변경, 볼륨 쌍 삭제, 클러스터 쌍 삭제 등 다양한 방법으로 볼륨 관계를 관리할 수 있습니다.

자세한 내용을 확인하십시오

- 복제를 일시 중지합니다
- 복제 모드를 변경합니다
- 볼륨 쌍을 삭제합니다

복제를 일시 중지합니다

짧은 시간 동안 입출력 처리를 중지해야 하는 경우 복제를 수동으로 일시 중지할 수 있습니다. 입출력 처리 시 과부하가 발생할 경우 복제를 일시 중지하고 처리 부하를 줄일 수 있습니다.

1. 데이터 보호 * > * 볼륨 쌍 * 을 선택합니다.
2. 볼륨 쌍의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. Edit Volume Pair * 창에서 복제 프로세스를 수동으로 일시 중지합니다.

> 볼륨 복제를 수동으로 일시 중지하거나 다시 시작하면 데이터 전송이 중단되거나 다시 시작됩니다. 두 사이트에서 이러한 변경 내용을 조정했는지 확인합니다.

5. 변경 내용 저장 * 을 클릭합니다.

복제 모드를 변경합니다

볼륨 쌍 속성을 편집하여 볼륨 쌍 관계의 복제 모드를 변경할 수 있습니다.

1. 데이터 보호 * > * 볼륨 쌍 * 을 선택합니다.
2. 볼륨 쌍의 작업 아이콘을 클릭합니다.
3. 편집 * 을 클릭합니다.
4. Edit Volume Pair * 창에서 새 복제 모드를 선택합니다.
   - * 실시간(비동기식) *: 소스 클러스터에서 커밋된 쓰기가 클라이언트에 확인됩니다.
   - * 실시간(동기식) *: 쓰기가 소스 및 타겟 클러스터 모두에서 커밋된 후 클라이언트에 인식됩니다.
   - * 스냅샷만 *: 소스 클러스터에서 생성된 스냅샷만 복제됩니다. 소스 볼륨의 활성 쓰기는 복제되지 않습니다. * 주의: * 복제 모드를 변경하면 모드가 즉시 변경됩니다. 두 사이트에서 이러한 변경 내용을 조정했는지 확인합니다.
5. 변경 내용 저장 * 을 클릭합니다.

볼륨 쌍을 삭제합니다

두 볼륨 간의 쌍 연결을 제거하려면 볼륨 쌍을 삭제할 수 있습니다.

1. 데이터 보호 * > * 볼륨 쌍 * 을 선택합니다.
2. 삭제할 볼륨 쌍의 작업 아이콘을 클릭합니다.
3. 삭제 * 를 클릭합니다.
4. 메시지를 확인합니다.

클러스터 쌍을 삭제합니다

쌍에 있는 클러스터 중 하나의 Element UI에서 클러스터 쌍을 삭제할 수 있습니다.

1. 데이터 보호 * > * 클러스터 쌍 * 을 클릭합니다.
2. 클러스터 쌍의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * 삭제 * 를 클릭합니다.
4. 작업을 확인합니다.
5. 클러스터 페어링의 두 번째 클러스터에서 단계를 다시 수행합니다.

클러스터 쌍 세부 정보

데이터 보호 탭의 클러스터 쌍 페이지에는 페어링되었거나 페어링 중인 클러스터에 대한 정보가 제공됩니다. 상태 열에 페어링 및 진행 메시지가 표시됩니다.

- * ID *

  각 클러스터 쌍에 부여되는 시스템 생성 ID입니다.

- * 원격 클러스터 이름 *

  페어에 있는 다른 클러스터의 이름입니다.

- * 원격 MVIP *

  페어에 있는 다른 클러스터의 관리 가상 IP 주소입니다.

- * 상태 *

  원격 클러스터의 복제 상태입니다

- * 볼륨 복제 *

  복제용으로 페어링된 클러스터에 포함된 볼륨 수입니다.

- * UUID *

  페어의 각 클러스터에 부여된 고유 ID입니다.

볼륨 쌍 세부 정보

데이터 보호 탭의 볼륨 쌍 페이지에는 페어링되었거나 페어링 중인 볼륨에 대한 정보가 제공됩니다. 볼륨 상태 열에 페어링 및 진행 메시지가 표시됩니다.

- * ID *

  볼륨에 대한 시스템 생성 ID입니다.

- * 이름 *

  볼륨을 생성할 때 볼륨에 지정한 이름입니다. 볼륨 이름은 최대 223자까지 가능하며 a-z, 0-9 및 대시(-)를 포함할 수 있습니다.

- * 계정 *

  볼륨에 할당된 계정의 이름입니다.

- * 볼륨 상태 *

  볼륨의 복제 상태입니다

- * 스냅샷 상태 *

  스냅샷 볼륨의 상태입니다.

- * 모드 *

  클라이언트 쓰기 복제 방법입니다. 가능한 값은 다음과 같습니다.

  - 비동기식
  - 스냅샷 전용
  - 동기화

- * 방향 *

  볼륨 데이터의 방향:

  - 소스 볼륨 아이콘(→) 는 데이터가 클러스터 외부의 타겟에 기록되는 중임을 나타냅니다.
  - 타겟 볼륨 아이콘(←)는 데이터가 외부 소스에서 로컬 볼륨에 기록되고 있음을 나타냅니다.

- * 비동기 지연 *

  볼륨이 원격 클러스터와 마지막으로 동기화된 이후의 시간입니다. 볼륨이 페어링되지 않은 경우 값은 null입니다.

- * 원격 클러스터 *

  볼륨이 상주하는 원격 클러스터의 이름입니다.

- * 원격 볼륨 ID *

  원격 클러스터에 있는 볼륨의 볼륨 ID입니다.

- * 원격 볼륨 이름 *

  원격 볼륨을 생성할 때 지정한 이름입니다.

볼륨 페어링 메시지

초기 페어링 프로세스 중에 데이터 보호 탭의 볼륨 쌍 페이지에서 볼륨 페어링 메시지를 볼 수 있습니다. 이러한 메시지는 Replicating Volumes 목록 보기에서 쌍의 소스 및 타겟 끝에 모두 표시될 수 있습니다.

- * PausedDisconnected *(PausedDisconnected *)

  소스 복제 또는 동기화 RPC 시간이 초과되었습니다. 원격 클러스터에 대한 연결이 끊어졌습니다. 클러스터에 대한 네트워크 연결을 확인합니다.

- * ResumingConnected *

  이제 원격 복제 동기화가 활성화되었습니다. 동기화 프로세스를 시작하고 데이터를 기다리는 중입니다.

- * ResumingRSync * 를 선택합니다

  볼륨 메타데이터의 단일 나선형 복제본이 페어링된 클러스터에 만들어집니다.

- * LocalSync * ResumingLocalSync * 를 선택합니다

  볼륨 메타데이터의 이중 나선형 복제본이 페어링된 클러스터에 만들어집니다.

- * 재전송 *

  데이터 전송이 다시 시작되었습니다.

- * 활성 *

  볼륨이 페어링되고 데이터가 소스에서 타겟 볼륨으로 전송되고 데이터가 동기화됩니다.

- * 유휴 *

  복제 작업이 발생하지 않습니다.

볼륨 페어링 경고

데이터 보호 탭의 볼륨 쌍 페이지에는 볼륨을 페어링한 후 이러한 메시지가 표시됩니다. 이러한 메시지는 Replicating Volumes(볼륨 복제) 목록 보기에서 페어의 소스 끝과 타겟 끝 모두에 표시될 수 있습니다(달리 명시되지 않은 경우).

- * PausedClusterFull *

  타겟 클러스터가 가득 차서 소스 복제 및 대량 데이터 전송을 계속할 수 없습니다. 메시지는 페어의 소스 끝에만 표시됩니다.

- * PausedExcededMaxSnapshotCount *

  타겟 볼륨에 이미 최대 스냅샷 수가 있으며 추가 스냅샷을 복제할 수 없습니다.

- * PausedManual *(PausedManual *)

로컬 볼륨이 수동으로 일시 중지되었습니다. 복제를 다시 시작하기 전에 일시 중지 해제되어야 합니다.

- * PausedManualRemote *

  원격 볼륨이 수동 일시 중지 모드에 있습니다. 복제를 다시 시작하기 전에 원격 볼륨의 일시 중지를 해제하는 데 수동 개입이 필요합니다.

- * PausedMisconfigured *

  활성 소스 및 타겟을 기다리는 중입니다. 복제를 다시 시작하려면 수동 작업이 필요합니다.

- * PausedQoS *

  타겟 QoS가 들어오는 IO를 유지할 수 없습니다. 복제가 자동으로 재개됩니다. 메시지는 페어의 소스 끝에만 표시됩니다.

- * PausedSlowLink *

  느린 링크가 감지되어 복제가 중지되었습니다. 복제가 자동으로 재개됩니다. 메시지는 페어의 소스 끝에만 표시됩니다.

- * PausedVolumeSizeMismatch *

  타겟 볼륨이 소스 볼륨과 크기가 다릅니다.

- * PausedXCopy *

  소스 볼륨에 SCSI XCOPY 명령이 실행 중입니다. 복제를 다시 시작하려면 명령을 완료해야 합니다. 메시지는 페어의 소스 끝에만 표시됩니다.

- * StoppedMisconfigured *

  영구적인 구성 오류가 감지되었습니다. 원격 볼륨이 제거되었거나 페어링되지 않았습니다. 수정 조치가 가능하지 않습니다. 새 페어링을 설정해야 합니다.

Element 및 ONTAP 클러스터 간 SnapMirror 복제 사용

NetApp Element UI의 데이터 보호 탭에서 SnapMirror 관계를 생성할 수 있습니다. 사용자 인터페이스에서 이를 보려면 SnapMirror 기능이 활성화되어 있어야 합니다.

IPv6은 NetApp Element 소프트웨어와 ONTAP 클러스터 간의 SnapMirror 복제에 지원되지 않습니다.

"NetApp 비디오: NetApp HCI용 SnapMirror 및 Element 소프트웨어"

NetApp Element 소프트웨어를 실행하는 시스템에서는 SnapMirror 기능을 지원하여 NetApp ONTAP 시스템에서 스냅샷 복사본을 복사 및 복원할 수 있습니다. 이 기술을 사용하는 가장 큰 이유는 NetApp HCI에서 ONTAP로 재해 복구 때문입니다. 엔드포인트에는 ONTAP, ONTAP Select 및 Cloud Volumes ONTAP가 포함됩니다. TR-4641 NetApp HCI 데이터 보호 를 참조하십시오.

"NetApp 기술 보고서 4641: NetApp HCI 데이터 보호"

자세한 내용을 확인하십시오

- "NetApp HCI, ONTAP 및 통합 인프라를 통해 데이터 패브릭 구축"
- "NetApp Element 소프트웨어와 ONTAP 간의 복제"

SnapMirror 개요

NetApp Element 소프트웨어를 실행하는 시스템에서는 SnapMirror 기능을 지원하여 NetApp ONTAP 시스템에서 스냅샷을 복사 및 복원할 수 있습니다.

Element를 실행하는 시스템은 ONTAP 시스템 9.3 이상에서 SnapMirror와 직접 통신할 수 있습니다. NetApp Element API는 클러스터, 볼륨 및 스냅숏에서 SnapMirror 기능을 활성화하는 방법을 제공합니다. 또한 Element UI에는 Element 소프트웨어와 ONTAP 시스템 간의 SnapMirror 관계를 관리하는 데 필요한 모든 기능이 포함되어 있습니다.

기능이 제한된 특정 사용 사례에서 ONTAP 생성 볼륨을 Element 볼륨으로 복제할 수 있습니다. 자세한 내용은 ONTAP 설명서를 참조하십시오.

자세한 내용을 확인하십시오

"Element 소프트웨어와 ONTAP 간 복제"

클러스터에서 **SnapMirror**를 활성화합니다

NetApp Element UI를 통해 클러스터 레벨에서 SnapMirror 기능을 수동으로 활성화해야 합니다. 시스템에는 SnapMirror 기능이 기본적으로 비활성화되어 있으며, 새로운 설치 또는 업그레이드의 일부로 자동 활성화되지 않습니다. SnapMirror 기능을 설정하는 것은 일회성 구성 작업입니다.

SnapMirror는 NetApp ONTAP 시스템의 볼륨과 함께 사용되는 Element 소프트웨어를 실행하는 클러스터에 대해서만 활성화할 수 있습니다. 클러스터가 NetApp ONTAP 볼륨과 함께 사용하도록 연결된 경우에만 SnapMirror 기능을 사용하도록 설정해야 합니다.

필요한 것

스토리지 클러스터에서 NetApp Element 소프트웨어가 실행되고 있어야 합니다.

단계

1. 클러스터 * > * 설정 * 을 클릭합니다.
2. SnapMirror에 대한 클러스터별 설정을 찾습니다.
3. SnapMirror 사용 * 을 클릭합니다.

> SnapMirror 기능을 활성화하면 Element 소프트웨어 구성이 영구적으로 변경됩니다. SnapMirror 기능을 사용하지 않도록 설정하고 클러스터를 공장 출하 시 이미지로 되돌릴 수만 기본 설정을 복원할 수 있습니다.

4. SnapMirror 구성 변경을 확인하려면 * 예 * 를 클릭합니다.

볼륨에서 **SnapMirror**를 사용하도록 설정합니다

Element UI에서 볼륨에 대해 SnapMirror를 활성화해야 합니다. 이렇게 하면 지정된 ONTAP 볼륨에 데이터를 복제할 수 있습니다. 이 권한은 SnapMirror용 NetApp Element 소프트웨어를 실행하는 클러스터의 관리자가 볼륨을 제어할 수 있도록 합니다.

필요한 것

- 클러스터의 Element UI에서 SnapMirror를 활성화했습니다.
- SnapMirror 엔드포인트를 사용할 수 있습니다.
- 볼륨은 512e 블록 크기여야 합니다.
- 볼륨이 원격 복제에 사용되고 있지 않습니다.
- 볼륨 액세스 유형이 복제 대상이 아닙니다.

> 볼륨을 생성하거나 클론 생성할 때 이 속성을 설정할 수도 있습니다.

단계

1. Management * > * Volumes * 를 클릭합니다.
2. SnapMirror를 활성화할 볼륨의 * 작업 * 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Edit * 를 선택합니다.
4. 볼륨 편집 * 대화 상자에서 * SnapMirror 사용 * 확인란을 선택합니다.
5. 변경 내용 저장 * 을 클릭합니다.

SnapMirror 끝점을 만듭니다

관계를 만들려면 NetApp Element UI에서 SnapMirror 끝점을 만들어야 합니다.

SnapMirror 엔드포인트는 Element 소프트웨어를 실행하는 클러스터의 복제 타겟 역할을 하는 ONTAP 클러스터입니다. SnapMirror 관계를 생성하기 전에 먼저 SnapMirror 끝점을 만듭니다.

Element 소프트웨어를 실행하는 스토리지 클러스터에서 SnapMirror 엔드포인트를 최대 4개 생성하고 관리할 수 있습니다.

> 기존 끝점이 원래 API를 사용하여 생성되었고 자격 증명이 저장되지 않은 경우 요소 UI에서 끝점을 보고 그 존재를 확인할 수 있지만 Element UI를 사용하여 관리할 수는 없습니다. 그런 다음 이 끝점은 Element API를 통해서만 관리할 수 있습니다.

API 메소드에 대한 자세한 내용은 를 참조하십시오 "Element API를 사용하여 스토리지를 관리합니다".

필요한 것

- 스토리지 클러스터의 Element UI에서 SnapMirror를 사용하도록 설정해야 합니다.
- 끝점에 대한 ONTAP 자격 증명을 알고 있습니다.

단계

1. 데이터 보호 * > * SnapMirror 엔드포인트 * 를 클릭합니다.

2. 끝점 만들기 * 를 클릭합니다.
3. 새 엔드포인트 생성 * 대화 상자에서 ONTAP 시스템의 클러스터 관리 IP 주소를 입력합니다.
4. 끝점과 연결된 ONTAP 관리자 자격 증명을 입력합니다.
5. 추가 세부 정보 검토:
    - LIF: Element와 통신하는 데 사용되는 ONTAP 인터클러스터 논리 인터페이스를 나열합니다.
    - 상태: SnapMirror 끝점의 현재 상태를 표시합니다. 가능한 값은 연결, 연결 해제 및 관리되지 않는 값입니다.
6. 끝점 만들기 * 를 클릭합니다.

SnapMirror 관계를 생성합니다

NetApp Element UI에서 SnapMirror 관계를 만들어야 합니다.

> SnapMirror에 대해 볼륨이 아직 활성화되어 있지 않고 Element UI에서 관계를 생성하도록 선택하면 해당 볼륨에서 SnapMirror가 자동으로 활성화됩니다.

필요한 것

볼륨에 SnapMirror가 활성화되어 있습니다.

단계

1. Management * > * Volumes * 를 클릭합니다.
2. 관계의 일부로 사용할 볼륨의 * 작업 * 아이콘을 클릭합니다.
3. SnapMirror 관계 만들기 * 를 클릭합니다.
4. SnapMirror 관계 만들기 * 대화 상자의 * 끝점 * 목록에서 끝점을 선택합니다.
5. 새 ONTAP 볼륨이나 기존 ONTAP 볼륨을 사용하여 관계를 생성하려는 경우 선택합니다.
6. 요소 UI에서 새 ONTAP 볼륨을 만들려면 * 새 볼륨 생성 * 을 클릭합니다.
    a. 이 관계를 위해 * 스토리지 가상 머신 * 을 선택합니다.
    b. 드롭다운 목록에서 * Aggregate * 를 선택합니다.
    c. 볼륨 이름 접미사 * 필드에 접미사를 입력합니다.

    > 시스템이 소스 볼륨 이름을 감지하여 * Volume Name * 필드에 복사합니다. 입력하는 접미사는 이름을 추가합니다.

    d. Create Destination Volume * 을 클릭합니다.
7. 기존 ONTAP 볼륨을 사용하려면 * 기존 볼륨 사용 * 을 클릭합니다.
    a. 이 관계를 위해 * 스토리지 가상 머신 * 을 선택합니다.
    b. 이 새 관계의 대상인 볼륨을 선택합니다.
8. [관계 상세정보 *] 섹션에서 정책을 선택합니다. 선택한 정책에 Keep 규칙이 있는 경우 Rules 테이블에 규칙 및 관련 레이블이 표시됩니다.
9. * 선택 사항 *: 일정을 선택합니다.

이 경우 관계의 복제본 생성 빈도가 결정됩니다.

10. * 선택 사항 *: * 대역폭 제한 대상 * 필드에 이 관계와 연결된 데이터 전송에 사용할 수 있는 최대 대역폭 양을 입력합니다.
11. 추가 세부 정보 검토:
    - * 상태 *: 대상 볼륨의 현재 관계 상태입니다. 가능한 값은 다음과 같습니다.
        - 초기화되지 않음: 대상 볼륨이 초기화되지 않았습니다.
        - snapmirred: 대상 볼륨이 초기화되었으며 SnapMirror 업데이트를 받을 준비가 되었습니다.
        - 부분 해제: 대상 볼륨이 읽기/쓰기 이고 스냅샷이 있습니다.
    - * 상태 *: 관계의 현재 상태입니다. 가능한 값은 유휴, 전송, 확인, 중지, 중지, 일시 중지, 대기, 준비, 종료, 중단 및 중단
    - * 지연 시간 *: 대상 시스템이 소스 시스템 뒤에 걸쳐지는 시간(초)입니다. 지연 시간은 전송 스케줄 간격보다 길지 않아야 합니다.
    - 대역폭 제한 *: 이 관계와 연결된 데이터 전송에 사용할 수 있는 최대 대역폭 양입니다.
    - * 마지막 전송 *: 마지막으로 전송된 스냅샷의 타임 스탬프입니다. 자세한 내용을 보려면 클릭하십시오.
    - * 정책 이름 *: 관계에 대한 ONTAP SnapMirror 정책의 이름입니다.
    - * 정책 유형 *: 관계에 대해 선택한 ONTAP SnapMirror 정책의 유형입니다. 가능한 값은 다음과 같습니다.
        - Async_mirror입니다
        - mirror_vault 를 선택합니다
    - 별표 이름 * : 이 관계에 대해 선택한 ONTAP 시스템의 기존 스케줄의 이름입니다.
12. 지금 초기화하지 않도록 * Initialize * (초기화 *) 확인란이 선택되어 있지 않은지 확인합니다.

> 초기화에는 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 이 기능을 실행할 수 있습니다. 초기화는 기본 전송을 수행합니다. 소스 볼륨의 스냅샷 복사본을 만든 다음 해당 복사본과 대상 볼륨에 참조하는 모든 데이터 블록을 전송합니다. 수동으로 초기화하거나 일정을 사용하여 일정에 따라 초기화 프로세스 및 후속 업데이트를 시작할 수 있습니다.

13. [관계 작성]을 클릭합니다.
14. 이 새로운 SnapMirror 관계를 보려면 * 데이터 보호 * > * SnapMirror 관계 * 를 클릭하십시오.

SnapMirror 관계 동작

데이터 보호 탭의 SnapMirror 관계 페이지에서 관계를 구성할 수 있습니다. 작업 아이콘의 옵션은 여기에 설명되어 있습니다.

- * 편집 *: 관계에 사용되는 정책이나 일정을 편집합니다.
- * 삭제 *: SnapMirror 관계를 삭제합니다. 이 기능은 대상 볼륨을 삭제하지 않습니다.
- * Initialize *(초기화 *): 첫 번째 초기 데이터 베이스라인 전송을 수행하여 새 관계를 설정합니다.
- * 업데이트 *: 대상에 대한 마지막 업데이트 이후 포함된 새 데이터와 스냅샷 복사본을 복제하여 필요에 따라 관계를 업데이트합니다.
- * 정지 *: 관계에 대한 추가 업데이트를 방지합니다.

- * Resume *: 중지된 관계를 재개합니다.
- * Break *: 대상 볼륨을 읽기-쓰기로 설정하고 현재 및 미래의 모든 전송을 중지합니다. 역방향 재동기화 작업으로 인해 원본 소스 볼륨이 읽기 전용이 되므로 클라이언트가 원본 소스 볼륨을 사용하지 않는지 확인합니다.
- * 재동기화 *: 파손되기 전에 동일한 방향으로 끊어진 관계를 다시 설정합니다.
- * 역방향 재동기화 *: 반대 방향으로 새 관계를 만들고 초기화하는 데 필요한 단계를 자동화합니다. 이 작업은 기존 관계가 끊어진 상태인 경우에만 수행할 수 있습니다. 이 작업은 현재 관계를 삭제하지 않습니다. 원래 소스 볼륨은 가장 최근의 공통 스냅샷 복사본으로 되돌려져서 대상과 재동기화됩니다. 마지막으로 성공한 SnapMirror 업데이트 이후 원래 소스 볼륨에 대한 모든 변경 사항이 손실됩니다. 변경된 내용 또는 현재 대상 볼륨에 기록된 새 데이터는 원래 소스 볼륨으로 다시 전송됩니다.
- * Abort * (중단 *): 진행 중인 현재 전송을 취소합니다. 중단된 관계에 대해 SnapMirror 업데이트가 실행되면 중단이 발생하기 전에 생성된 마지막 재시작 체크포인트에서 마지막 전송을 통해 관계가 계속됩니다.

SnapMirror 레이블

SnapMirror 레이블은 관계의 보존 규칙에 따라 지정된 스냅샷을 전송하기 위한 마커로 사용됩니다.

스냅샷에 레이블을 적용하면 해당 레이블이 SnapMirror 복제의 타겟으로 표시됩니다. 관계의 역할은 데이터 전송 시 일치하는 레이블이 지정된 스냅샷을 선택하고 대상 볼륨에 복사한 다음 올바른 수의 복제본을 유지하여 규칙을 적용하는 것입니다. 유지 수와 보존 기간을 결정하는 정책을 나타냅니다. 정책에는 다양한 규칙이 있을 수 있으며 각 규칙에는 고유한 레이블이 있습니다. 이 레이블은 스냅샷과 보존 규칙 간의 링크 역할을 합니다.

선택한 스냅샷, 그룹 스냅샷 또는 일정에 적용되는 규칙을 나타내는 SnapMirror 레이블입니다.

스냅샷에 **SnapMirror** 레이블을 추가합니다

SnapMirror 레이블은 SnapMirror 엔드포인트에 대한 스냅샷 보존 정책을 지정합니다. 스냅샷 및 그룹 스냅샷에 레이블을 추가할 수 있습니다.

기존 SnapMirror 관계 대화 상자 또는 NetApp ONTAP System Manager에서 사용 가능한 레이블을 볼 수 있습니다.

> 그룹 스냅샷에 레이블을 추가하면 개별 스냅샷에 대한 기존 레이블이 덮어쓰여집니다.

필요한 것

- SnapMirror가 클러스터에서 활성화되어 있습니다.
- 추가하려는 레이블이 ONTAP에 이미 있습니다.

단계

1. 데이터 보호 * > * 스냅샷 * 또는 * 그룹 스냅샷 * 페이지를 클릭합니다.
2. SnapMirror 레이블을 추가할 스냅숏 또는 그룹 스냅숏에 대한 * 작업 * 아이콘을 클릭합니다.
3. 스냅샷 편집 * 대화 상자에서 * SnapMirror 레이블 * 필드에 텍스트를 입력합니다. 레이블은 SnapMirror 관계에 적용되는 정책의 규칙 레이블과 일치해야 합니다.
4. 변경 내용 저장 * 을 클릭합니다.

스냅샷 일정에 **SnapMirror** 레이블을 추가합니다

SnapMirror 정책이 적용되도록 스냅샷 일정에 SnapMirror 레이블을 추가할 수 있습니다. 기존 SnapMirror 관계 대화 상자 또는 NetAppONTAP System Manager에서 사용 가능한 레이블을 볼 수 있습니다.

필요한 것

- 클러스터 수준에서 SnapMirror가 활성화되어 있어야 합니다.
- 추가하려는 레이블이 ONTAP에 이미 있습니다.

단계

1. 데이터 보호 * > * 스케줄 * 을 클릭합니다.
2. 다음 방법 중 하나로 일정에 SnapMirror 레이블을 추가합니다.

옵션을 선택합니다	단계
새 일정 생성	a. Create Schedule * 을 선택합니다. b. 기타 모든 관련 세부 정보를 입력합니다. c. Create Schedule * 을 선택합니다.
기존 일정을 수정합니다	a. 레이블을 추가할 일정의 * Actions * 아이콘을 클릭하고 * Edit * 를 선택합니다. b. 결과 대화 상자에서 * SnapMirror Label * 필드에 텍스트를 입력합니다. c. 변경 내용 저장 * 을 선택합니다.

자세한 내용을 확인하십시오

스냅샷 스케줄을 생성합니다

SnapMirror를 사용한 재해 복구

NetApp Element 소프트웨어를 실행하는 볼륨 또는 클러스터에 문제가 있는 경우 SnapMirror 기능을 사용하여 관계를 중단시키고 대상 볼륨에 대한 페일오버를 수행합니다.

> 원래 클러스터에 장애가 완전히 발생했거나 클러스터가 없는 경우 NetApp 지원 팀에 추가 지원을 문의하십시오.

Element 클러스터에서 페일오버를 수행합니다

Element 클러스터에서 페일오버를 수행하여 대상 볼륨을 읽기/쓰기로 만들고 대상 측의 호스트에서 액세스할 수 있도록 할 수 있습니다. Element 클러스터에서 페일오버를 수행하기 전에 SnapMirror 관계를 끊어야 합니다.

NetApp Element UI를 사용하여 페일오버를 수행합니다. Element UI를 사용할 수 없는 경우 ONTAP System Manager 또는 ONTAP CLI를 사용하여 Break Relationship 명령을 실행할 수도 있습니다.

필요한 것

- SnapMirror 관계가 있으며 타겟 볼륨에 유효한 스냅샷이 하나 이상 있습니다.
- 운영 사이트에서 계획되지 않은 운영 중단 또는 계획된 이벤트로 인해 타겟 볼륨으로 페일오버해야 합니다.

단계

1. Element UI에서 * 데이터 보호 * > * SnapMirror 관계 * 를 클릭합니다.
2. 페일오버하려는 소스 볼륨과의 관계를 찾습니다.
3. 작업 * 아이콘을 클릭합니다.
4. 파단 * 을 클릭합니다.
5. 작업을 확인합니다.

   이제 타겟 클러스터의 볼륨에 읽기-쓰기 액세스가 부여되며 애플리케이션 호스트에 마운트하여 운영 워크로드를 재개할 수 있습니다. 이 작업의 결과로 모든 SnapMirror 복제가 중단됩니다. 관계에 끊어진 상태가 표시됩니다.

Element에 대한 장애 복구를 수행합니다

기본 측의 문제가 완화되면 원본 소스 볼륨을 재동기화하여 NetApp Element 소프트웨어로 페일백해야 합니다. 수행하는 단계는 원래 소스 볼륨이 여전히 있는지 또는 새로 생성된 볼륨으로 페일백해야 하는지 여부에 따라 달라집니다.

자세한 내용을 확인하십시오

- 소스 볼륨이 아직 있을 때 페일백을 수행합니다
- 소스 볼륨이 더 이상 존재하지 않는 경우 장애 복구를 수행합니다
- SnapMirror 페일백 시나리오

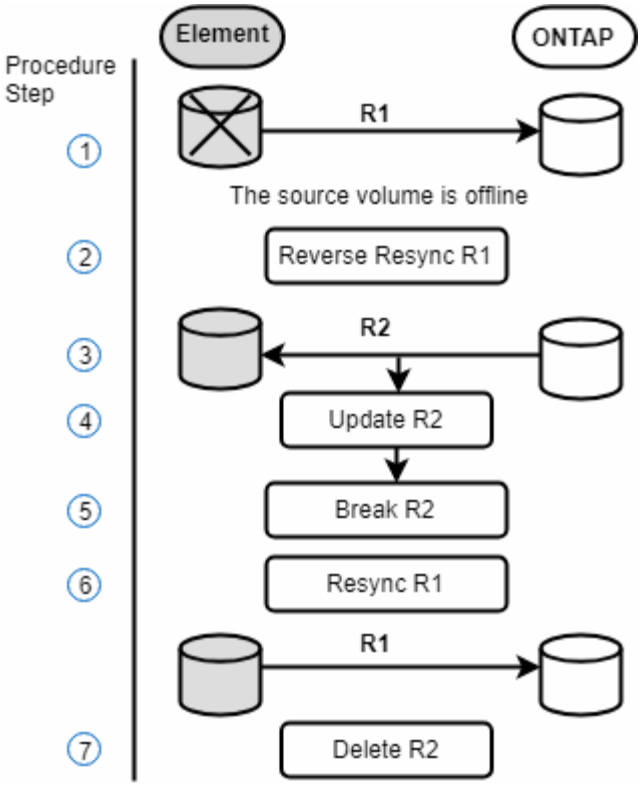
SnapMirror 페일백 시나리오

SnapMirror 재해 복구 기능은 두 가지 장애 복구 시나리오에서 설명됩니다. 이 경우 원래 관계가 장애 발생(장애)된 것으로 간주됩니다.

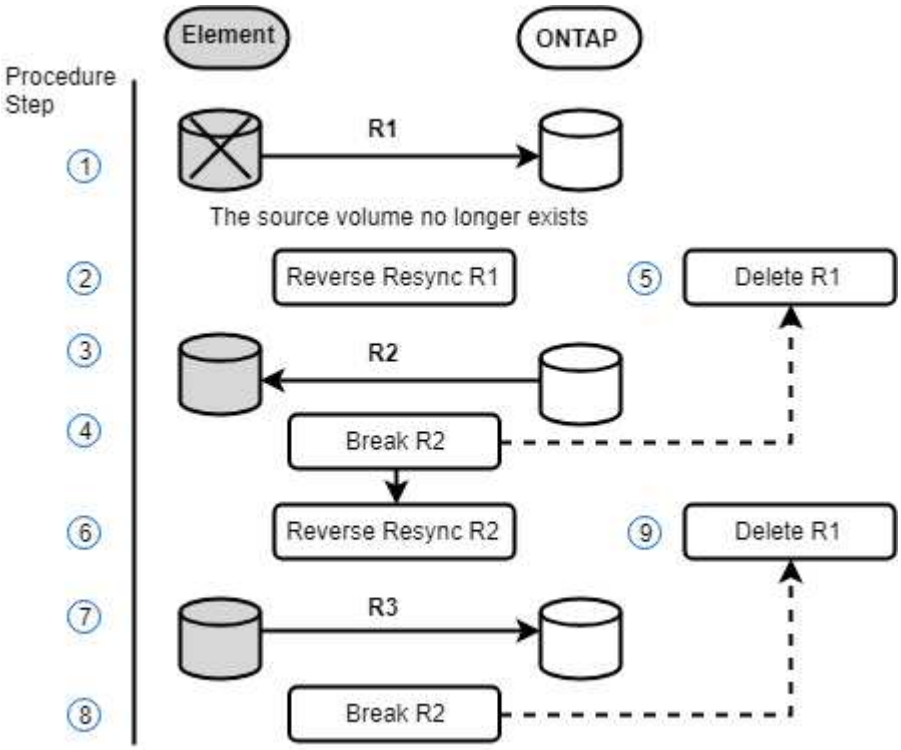
해당 절차의 단계가 참조용으로 추가됩니다.

> 이 예에서 R1 = NetApp Element 소프트웨어를 실행하는 클러스터가 원래 소스 볼륨(요소)이고 ONTAP가 원래 대상 볼륨(ONTAP)인 원래 관계입니다. R2와 R3은 역재동기화 작업을 통해 생성된 역 관계를 나타냅니다.

다음 이미지는 소스 볼륨이 여전히 존재할 때의 장애 복구 시나리오를 보여 줍니다.



다음 이미지는 소스 볼륨이 더 이상 존재하지 않는 경우의 장애 복구 시나리오를 보여 줍니다.



자세한 내용을 확인하십시오

- 소스 볼륨이 아직 있을 때 페일백을 수행합니다
- 소스 볼륨이 더 이상 존재하지 않는 경우 장애 복구를 수행합니다

소스 볼륨이 아직 있을 때 페일백을 수행합니다

NetApp Element UI를 사용하여 원본 소스 볼륨을 재동기화하고 페일백할 수 있습니다. 이 절차는 원래 소스 볼륨이 여전히 존재하는 시나리오에 적용됩니다.

1. Element UI에서 페일오버를 수행하기 위해 끊은 관계를 찾습니다.
2. Actions 아이콘을 클릭하고 * Reverse Resync * 를 클릭합니다.
3. 작업을 확인합니다.

> 역방향 재동기화 작업은 원래 소스 볼륨과 대상 볼륨의 역할이 반전되는 새 관계를 생성합니다. 이로 인해 원래 관계가 유지됨에 따라 두 개의 관계가 형성됩니다. 원래 대상 볼륨의 새 데이터는 역방향 재동기화 작업의 일부로 원래 소스 볼륨으로 전송됩니다. 대상 측의 활성 볼륨에 계속 액세스하고 데이터를 쓸 수 있지만 원래 기본 볼륨으로 리디렉션하기 전에 모든 호스트를 소스 볼륨에서 분리하고 SnapMirror 업데이트를 수행해야 합니다.

4. 방금 만든 역관계의 작업 아이콘을 클릭하고 * 업데이트 * 를 클릭합니다.

   역방향 재동기화를 완료했으며 대상 측의 볼륨에 연결된 활성 세션이 없고 최신 데이터가 원래 운영 볼륨에 있는지 확인했습니다. 다음 단계를 수행하여 페일백을 완료하고 원래 기본 볼륨을 다시 활성화할 수 있습니다.

5. 역관계의 작업 아이콘을 클릭하고 * 중단 * 을 클릭합니다.
6. 원래 관계의 작업 아이콘을 클릭하고 * 재동기화 * 를 클릭합니다.

> 이제 원래 운영 볼륨을 마운트하여 원래 운영 볼륨에서 운영 워크로드를 재개할 수 있습니다. 관계에 대해 구성된 정책 및 일정에 따라 원래 SnapMirror 복제가 재개됩니다.

7. 원래 관계 상태가 "스냅샷 미러링"임을 확인한 후 역관계의 작업 아이콘을 클릭하고 * 삭제 * 를 클릭합니다.

자세한 내용을 확인하십시오

SnapMirror 페일백 시나리오

소스 볼륨이 더 이상 존재하지 않는 경우 장애 복구를 수행합니다

NetApp Element UI를 사용하여 원본 소스 볼륨을 재동기화하고 페일백할 수 있습니다. 이 섹션은 원래 소스 볼륨이 손실되었지만 원래 클러스터가 그대로 유지되는 시나리오에 적용됩니다. 새 클러스터로 복원하는 방법에 대한 자세한 내용은 NetApp Support 사이트 설명서를 참조하십시오.

필요한 것

- Element 및 ONTAP 볼륨 간에 분리된 복제 관계가 있습니다.
- Element 볼륨이 복구할 수 없는 손실입니다.
- 원래 볼륨 이름이 찾을 수 없음 으로 표시됩니다.

단계

1. Element UI에서 페일오버를 수행하기 위해 끊은 관계를 찾습니다.

- 모범 사례: * SnapMirror 정책을 기록하고 원래의 부분 신뢰 관계에 대한 세부 사항을 예약합니다. 이 정보는 관계를 다시 생성할 때 필요합니다.

2. Actions * 아이콘을 클릭하고 * Reverse Resync * 를 클릭합니다.
3. 작업을 확인합니다.

> 역방향 재동기화 작업은 원래 소스 볼륨과 대상 볼륨의 역할이 반전되는 새 관계를 생성합니다. 이로 인해 원래 관계가 유지됨에 따라 두 개의 관계가 형성됩니다. 원래 볼륨이 더 이상 존재하지 않기 때문에 시스템은 원래 소스 볼륨과 동일한 볼륨 이름 및 볼륨 크기의 새로운 Element 볼륨을 생성합니다. 새 볼륨에는 SM-RECOVERY라는 기본 QoS 정책이 할당되며 SM-RECOVERY라는 기본 계정과 연결됩니다. 또한, SnapMirror에서 생성된 모든 볼륨의 계정 및 QoS 정책을 수동으로 편집하여 제거된 원래 소스 볼륨을 대체할 수 있습니다.

역방향 재동기화 작업의 일부로 최신 스냅샷의 데이터가 새 볼륨으로 전송됩니다. 대상 측의 활성 볼륨에 계속 액세스하여 데이터를 쓸 수 있지만 모든 호스트의 액티브 볼륨 연결을 끊고 SnapMirror 업데이트를 수행한 후에 원래 기본 관계를 이후의 단계에서 복구해야 합니다. 역방향 재동기화를 완료하고 대상 측의 볼륨에 연결된 활성 세션이 없는지, 그리고 최신 데이터가 원래 운영 볼륨에 있는지 확인한 후 다음 단계를 계속 수행하여 페일백을 완료하고 원래 운영 볼륨을 다시 활성화합니다.

4. 역재동기화 작업 중에 생성된 역관계의 * 작업 * 아이콘을 클릭하고 * 중단 * 을 클릭합니다.
5. 원본 볼륨이 없는 원본 관계의 * 작업 * 아이콘을 클릭하고 * 삭제 * 를 클릭합니다.
6. 4단계에서 깬 역관계의 * 작업 * 아이콘을 클릭하고 * 역재동기화 * 를 클릭합니다.
7. 이렇게 하면 소스 및 대상이 반전되고 원래 관계와 동일한 볼륨 소스 및 볼륨 대상과 관계가 형성됩니다.
8. 작업 * 아이콘과 * 편집 * 을 클릭하여 이 관계를 원래의 QoS 정책 및 일정 설정과 함께 업데이트합니다.
9. 이제 6단계에서 다시 동기화한 역 관계를 삭제하는 것이 안전합니다.

자세한 내용을 확인하십시오

SnapMirror 페일백 시나리오

ONTAP에서 요소로 전송 또는 **1**회 마이그레이션을 수행합니다

일반적으로 NetApp Element 소프트웨어를 실행하는 SolidFire 스토리지 클러스터에서 ONTAP 소프트웨어로 재해 복구를 위해 SnapMirror를 사용하는 경우, Element가 소스이고 ONTAP가 타겟입니다. 하지만 경우에 따라 ONTAP 스토리지 시스템이 소스 및 Element를 타겟으로 사용할 수 있습니다.

- 두 가지 시나리오가 있습니다.
  - 이전의 재해 복구 관계가 없습니다. 이 절차의 모든 단계를 따릅니다.
  - 이전 재해 복구 관계가 존재하지만 이 완화 조치에 사용되는 볼륨 간에는 존재하지 않습니다. 이 경우 아래 3단계와 4단계만 수행하십시오.

필요한 것

- ONTAP에서 Element 대상 노드에 액세스할 수 있어야 합니다.
- SnapMirror 복제에 대해 Element 볼륨이 활성화되어 있어야 합니다.

hostip:/lun/<id_number> 형식으로 Element 대상 경로를 지정해야 합니다. 여기서 lun은 실제 문자열 ""lun""이고

id_number는 Element 볼륨의 ID입니다.

단계

1. ONTAP를 사용하여 Element 클러스터와 관계를 생성합니다.

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. ONTAP SnapMirror show 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

   복제 관계 생성에 대한 자세한 내용은 ONTAP 설명서를 참조하고, 전체 명령 구문은 ONTAP man 페이지를 참조하십시오.

3. 'ElementCreateVolume' API를 사용하여 타겟 볼륨을 생성하고 타겟 볼륨 액세스 모드를 SnapMirror로 설정합니다.

   Element API를 사용하여 Element 볼륨을 생성합니다

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. ONTAP 'napmirror initialize' 명령어를 사용하여 복제 관계를 초기화한다.

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

볼륨 백업 및 복원

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

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.

자세한 내용을 확인하십시오

- Amazon S3 오브젝트 저장소에 볼륨을 백업합니다
- OpenStack Swift 오브젝트 저장소에 볼륨을 백업합니다
- SolidFire 스토리지 클러스터에 볼륨을 백업합니다
- Amazon S3 오브젝트 저장소 의 백업에서 볼륨을 복원합니다
- OpenStack Swift 오브젝트 저장소 의 백업에서 볼륨을 복원합니다
- SolidFire 스토리지 클러스터의 백업에서 볼륨을 복원합니다

Amazon S3 오브젝트 저장소에 볼륨을 백업합니다

Amazon S3와 호환되는 외부 오브젝트 저장소에 볼륨을 백업할 수 있습니다.

1. Management * > * Volumes * 를 클릭합니다.
2. 백업할 볼륨에 대한 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Backup to * 를 클릭합니다.
4. 통합 백업 * 대화 상자의 * 백업 대상 * 에서 * S3 * 를 선택합니다.
5. 데이터 형식 * 에서 옵션을 선택합니다.
   - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
   - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
6. 호스트 이름 * 필드에 개체 저장소에 액세스하는 데 사용할 호스트 이름을 입력합니다.
7. 계정의 액세스 키 ID를 * 액세스 키 ID * 필드에 입력합니다.
8. 비밀 액세스 키 * 필드에 계정의 비밀 액세스 키를 입력합니다.
9. 백업을 저장할 S3 버킷을 * S3 Bucket * 필드에 입력합니다.
10. nametag * 필드에 접두사에 추가할 이름 태그를 입력합니다.
11. 읽기 시작 * 을 클릭합니다.

OpenStack Swift 오브젝트 저장소에 볼륨을 백업합니다

OpenStack Swift와 호환되는 외부 오브젝트 저장소에 볼륨을 백업할 수 있습니다.

1. Management * > * Volumes * 를 클릭합니다.
2. 백업할 볼륨에 대한 작업 아이콘을 클릭합니다.

3. 결과 메뉴에서 * Backup to * 를 클릭합니다.
4. 통합 백업 * 대화 상자의 * 백업 대상 * 에서 * Swift * 를 선택합니다.
5. 데이터 형식 * 에서 데이터 형식을 선택합니다.
    - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
    - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
6. URL * 필드에 개체 저장소에 액세스하는 데 사용할 URL을 입력합니다.
7. 사용자 이름 * 필드에 계정의 사용자 이름을 입력합니다.
8. 인증 키 * 필드에 계정의 인증 키를 입력합니다.
9. Container * 필드에 백업을 저장할 컨테이너를 입력합니다.
10. * 선택 사항 *: * nametag * 필드의 접두사에 추가할 이름 태그를 입력합니다.
11. 읽기 시작 * 을 클릭합니다.

SolidFire 스토리지 클러스터에 볼륨을 백업합니다

Element 소프트웨어를 실행하는 스토리지 클러스터의 경우 클러스터에 상주하는 볼륨을 원격 클러스터에 백업할 수 있습니다.

소스 및 타겟 클러스터가 페어링되었는지 확인합니다.

을 참조하십시오 "복제를 위해 클러스터를 쌍으로 설정합니다".

한 클러스터에서 다른 클러스터로 백업하거나 복구할 때 시스템은 클러스터 간 인증으로 사용할 키를 생성합니다. 이 대량 볼륨 쓰기 키를 사용하면 소스 클러스터가 대상 클러스터에 인증되어 대상 볼륨에 쓸 때 보안 수준을 제공할 수 있습니다. 백업 또는 복원 프로세스의 일부로 작업을 시작하기 전에 대상 볼륨에서 대량 볼륨 쓰기 키를 생성해야 합니다.

1. 대상 클러스터에서 * 관리 * > * 볼륨 *.
2. 대상 볼륨에 대한 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Restore from * 을 클릭합니다.
4. 통합 복원 * 대화 상자의 * 복원 위치 * 에서 * SolidFire * 를 선택합니다.
5. 데이터 형식 * 에서 옵션을 선택합니다.
    - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
    - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
6. 키 생성 * 을 클릭합니다.
7. Bulk Volume Write Key *(대량 볼륨 쓰기 키) 상자의 키를 클립보드로 복사합니다.
8. 소스 클러스터에서 * 관리 * > * 볼륨 * 으로 이동합니다.
9. 백업할 볼륨에 대한 작업 아이콘을 클릭합니다.
10. 결과 메뉴에서 * Backup to * 를 클릭합니다.
11. 통합 백업 * 대화 상자의 * 백업 대상 * 에서 * SolidFire * 를 선택합니다.
12. 데이터 형식 * 필드에서 이전에 선택한 것과 동일한 옵션을 선택합니다.

13. 원격 클러스터 MVIP * 필드에 대상 볼륨 클러스터의 관리 가상 IP 주소를 입력합니다.
14. 원격 클러스터 사용자 이름 * 필드에 원격 클러스터 사용자 이름을 입력합니다.
15. 원격 클러스터 암호 * 필드에 원격 클러스터 암호를 입력합니다.
16. Bulk Volume Write Key * (대량 볼륨 쓰기 키 *) 필드에서 이전에 대상 클러스터에서 생성한 키를 붙여 넣습니다.
17. 읽기 시작 * 을 클릭합니다.

Amazon S3 오브젝트 저장소 의 백업에서 볼륨을 복원합니다

Amazon S3 오브젝트 저장소의 백업에서 볼륨을 복원할 수 있습니다.

1. 보고 * > * 이벤트 로그 * 를 클릭합니다.
2. 복원할 백업을 만든 백업 이벤트를 찾습니다.
3. 이벤트의 * Details * 열에서 * Show Details * 를 클릭합니다.
4. 매니페스트 정보를 클립보드에 복사합니다.
5. Management * > * Volumes * 를 클릭합니다.
6. 복원하려는 볼륨의 작업 아이콘을 클릭합니다.
7. 결과 메뉴에서 * Restore from * 을 클릭합니다.
8. 통합 복원 * 대화 상자의 * 복원 위치 * 에서 * S3 * 를 선택합니다.
9. 데이터 형식 * 에서 백업과 일치하는 옵션을 선택합니다.
    - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
    - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
10. 호스트 이름 * 필드에 개체 저장소에 액세스하는 데 사용할 호스트 이름을 입력합니다.
11. 계정의 액세스 키 ID를 * 액세스 키 ID * 필드에 입력합니다.
12. 비밀 액세스 키 * 필드에 계정의 비밀 액세스 키를 입력합니다.
13. 백업을 저장할 S3 버킷을 * S3 Bucket * 필드에 입력합니다.
14. 매니페스트 정보 * 필드에 매니페스트 정보를 붙여 넣습니다.
15. 쓰기 시작 * 을 클릭합니다.

OpenStack Swift 오브젝트 저장소 의 백업에서 볼륨을 복원합니다

OpenStack Swift 오브젝트 저장소 의 백업에서 볼륨을 복원할 수 있습니다.

1. 보고 * > * 이벤트 로그 * 를 클릭합니다.
2. 복원할 백업을 만든 백업 이벤트를 찾습니다.
3. 이벤트의 * Details * 열에서 * Show Details * 를 클릭합니다.
4. 매니페스트 정보를 클립보드에 복사합니다.
5. Management * > * Volumes * 를 클릭합니다.
6. 복원하려는 볼륨의 작업 아이콘을 클릭합니다.

7. 결과 메뉴에서 * Restore from * 을 클릭합니다.
8. Integrated Restore * 대화 상자의 * Restore from * 에서 * Swift * 를 선택합니다.
9. 데이터 형식 * 에서 백업과 일치하는 옵션을 선택합니다.
    - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
    - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
10. URL * 필드에 개체 저장소에 액세스하는 데 사용할 URL을 입력합니다.
11. 사용자 이름 * 필드에 계정의 사용자 이름을 입력합니다.
12. 인증 키 * 필드에 계정의 인증 키를 입력합니다.
13. 백업이 저장되는 컨테이너의 이름을 * Container * 필드에 입력합니다.
14. 매니페스트 정보 * 필드에 매니페스트 정보를 붙여 넣습니다.
15. 쓰기 시작 * 을 클릭합니다.

SolidFire 스토리지 클러스터의 백업에서 볼륨을 복원합니다

SolidFire 스토리지 클러스터의 백업에서 볼륨을 복구할 수 있습니다.

한 클러스터에서 다른 클러스터로 백업하거나 복구할 때 시스템은 클러스터 간 인증으로 사용할 키를 생성합니다. 이 대량 볼륨 쓰기 키를 사용하면 소스 클러스터가 대상 클러스터에 인증되어 대상 볼륨에 쓸 때 보안 수준을 제공할 수 있습니다. 백업 또는 복원 프로세스의 일부로 작업을 시작하기 전에 대상 볼륨에서 대량 볼륨 쓰기 키를 생성해야 합니다.

1. 대상 클러스터에서 * 관리 * > * 볼륨 * 을 클릭합니다.
2. 복원하려는 볼륨의 작업 아이콘을 클릭합니다.
3. 결과 메뉴에서 * Restore from * 을 클릭합니다.
4. 통합 복원 * 대화 상자의 * 복원 위치 * 에서 * SolidFire * 를 선택합니다.
5. 데이터 형식 * 에서 백업과 일치하는 옵션을 선택합니다.
    - * 기본 *: SolidFire 스토리지 시스템에서만 읽을 수 있는 압축 형식입니다.
    - * 비압축 *: 다른 시스템과 호환되는 비압축 형식입니다.
6. 키 생성 * 을 클릭합니다.
7. Bulk Volume Write Key * 정보를 클립보드에 복사합니다.
8. 소스 클러스터에서 * 관리 * > * 볼륨 * 을 클릭합니다.
9. 복원에 사용할 볼륨의 작업 아이콘을 클릭합니다.
10. 결과 메뉴에서 * Backup to * 를 클릭합니다.
11. 통합 백업 * 대화 상자의 * 백업 대상 * 에서 * SolidFire * 를 선택합니다.
12. 데이터 형식 * 에서 백업과 일치하는 옵션을 선택합니다.
13. 원격 클러스터 MVIP * 필드에 대상 볼륨 클러스터의 관리 가상 IP 주소를 입력합니다.
14. 원격 클러스터 사용자 이름 * 필드에 원격 클러스터 사용자 이름을 입력합니다.
15. 원격 클러스터 암호 * 필드에 원격 클러스터 암호를 입력합니다.

16. 클립보드의 키를 * Bulk Volume Write Key * 필드에 붙여 넣습니다.
17. 읽기 시작 * 을 클릭합니다.

시스템 문제를 해결합니다

진단 목적으로 시스템을 모니터링하고 다양한 시스템 작업의 성능 추세 및 상태에 대한 정보를 확인해야 합니다. 유지보수를 위해 노드 또는 SSD를 교체해야 할 수 있습니다.

- "시스템 이벤트에 대한 정보를 봅니다"
- "실행 중인 작업의 상태를 봅니다"
- "시스템 경고를 봅니다"
- "노드 성능 작업을 봅니다"
- "볼륨 성능을 봅니다"
- "iSCSI 세션을 봅니다"
- "Fibre Channel 세션을 봅니다"
- "드라이브 문제를 해결합니다"
- "노드 문제 해결"
- "스토리지 노드용 노드별 유틸리티 작업"
- "관리 노드와 작업합니다"
- "클러스터 전체 수준 이해"

를 참조하십시오

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

시스템 이벤트에 대한 정보를 봅니다

시스템에서 감지된 다양한 이벤트에 대한 정보를 볼 수 있습니다. 30초마다 이벤트 메시지가 새로 고쳐집니다. 이벤트 로그에는 클러스터의 주요 이벤트가 표시됩니다.

1. Element UI에서 * Reporting * > * Event Log * 를 선택합니다.

   모든 이벤트에 대해 다음 정보가 표시됩니다.

항목	설명
ID입니다	각 이벤트와 연결된 고유 ID입니다.
이벤트 유형	로깅되는 이벤트 유형(예: API 이벤트 또는 클론 이벤트)

메시지	이벤트와 연결된 메시지입니다.
세부 정보	이벤트가 발생한 이유를 식별하는 데 도움이 되는 정보입니다.
서비스 ID입니다	이벤트를 보고한 서비스(해당하는 경우)
노드	이벤트를 보고한 노드입니다(해당하는 경우).
드라이브 ID입니다	이벤트를 보고한 드라이브입니다(해당하는 경우).
이벤트 시간	이벤트가 발생한 시간입니다.

자세한 내용을 확인하십시오

이벤트 유형

이벤트 유형

시스템은 여러 유형의 이벤트를 보고합니다. 각 이벤트는 시스템이 완료한 작업입니다. 이벤트는 일상적인 이벤트, 정상적인 이벤트 또는 관리자 주의가 필요한 이벤트일 수 있습니다. 이벤트 로그 페이지의 이벤트 유형 열은 이벤트가 발생한 시스템의 일부를 나타냅니다.

> 시스템은 이벤트 로그에 읽기 전용 API 명령을 기록하지 않습니다.

다음 목록에서는 이벤트 로그에 나타나는 이벤트 유형을 설명합니다.

- * apiEvent *

  설정을 수정하는 API 또는 웹 UI를 통해 사용자가 시작한 이벤트입니다.

- * binAssignmentEvent *

  데이터 저장소 할당과 관련된 이벤트입니다. 빈은 기본적으로 데이터를 보관하며 클러스터 전체에 매핑된 컨테이너입니다.

- * binSyncEvent *

  블록 서비스 간의 데이터 재할당과 관련된 시스템 이벤트입니다.

- * bsCheckEvent *

  Block 서비스 검사와 관련된 시스템 이벤트입니다.

- * bsKillEvent *

  Block 서비스 종료와 관련된 시스템 이벤트입니다.

- * bulkOpEvent *

  백업, 복원, 스냅샷 또는 클론과 같은 전체 볼륨에서 수행된 작업과 관련된 이벤트입니다.

- * cloneEvent *

  볼륨 클론 생성과 관련된 이벤트입니다.

- * 클러스터 마스터 이벤트 *

  클러스터 초기화 시 또는 노드 추가 또는 제거와 같은 클러스터 구성 변경 시 나타나는 이벤트입니다.

- * csumEvent *

  디스크의 잘못된 데이터 체크섬과 관련된 이벤트입니다.

- * 데이터 이벤트 *

  데이터 읽기 및 쓰기와 관련된 이벤트입니다.

- * dbEvent *

  클러스터의 앙상블 노드에 의해 유지되는 글로벌 데이터베이스와 관련된 이벤트입니다.

- * 드라이브 이벤트 *

  드라이브 작업과 관련된 이벤트입니다.

- * encryptionAtRestEvent *

  클러스터의 암호화 프로세스와 관련된 이벤트입니다.

- * ensembleEvent *

  앙상블의 노드 수를 늘리거나 줄이는 것과 관련된 이벤트입니다.

- * 광섬유 채널 이벤트 *

  노드의 구성 및 연결과 관련된 이벤트입니다.

- * gcEvent *

  프로세스와 관련된 이벤트는 60분마다 실행되어 블록 드라이브에서 스토리지를 재확보할 수 있습니다. 이 프로세스를 가비지 수집이라고도 합니다.

- * ieEvent *

  내부 시스템 오류입니다.

- * 설치 이벤트 *

  자동 소프트웨어 설치 이벤트. 소프트웨어가 보류 중인 노드에 자동으로 설치됩니다.

- * iSCSIEvent *

시스템의 iSCSI 문제와 관련된 이벤트입니다.

- * limitEvent *

  계정 또는 클러스터에 있는 볼륨 또는 가상 볼륨의 수가 허용되는 최대값에 근접하는 것과 관련된 이벤트입니다.

- 유지 관리 모드 이벤트

  노드 비활성화 등과 같은 노드 유지보수 모드와 관련된 이벤트입니다.

- * 네트워크 이벤트 *

  가상 네트워킹 상태와 관련된 이벤트입니다.

- * platformHardwareEvent *

  하드웨어 장치에서 감지된 문제와 관련된 이벤트입니다.

- * 원격 클러스터 이벤트 *

  원격 클러스터 페어링과 관련된 이벤트입니다.

- * 일정 이벤트 *

  예약된 스냅샷과 관련된 이벤트입니다.

- 서비스 이벤트 *

  시스템 서비스 상태와 관련된 이벤트입니다.

- * 슬라이스 이벤트 *

  메타데이터 드라이브 또는 볼륨 제거와 같은 슬라이스 서버와 관련된 이벤트입니다.

  볼륨이 할당된 서비스에 대한 정보를 포함하는 3가지 유형의 슬라이스 재할당 이벤트가 있습니다.

  - 대칭 이동: 기본 서비스를 새 기본 서비스로 변경합니다

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - 이동: 2차 서비스를 새 2차 서비스로 변경

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - 잘라내기: 서비스 집합에서 볼륨 제거

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- * snmpTrapEvent *

  SNMP 트랩과 관련된 이벤트입니다.

- 상태 이벤트 *

  시스템 통계와 관련된 이벤트입니다.

- * 이벤트 *

  시스템 전송 서비스와 관련된 이벤트입니다.

- * 예기치 않은 예외 *

  예기치 않은 시스템 예외와 관련된 이벤트입니다.

- * ureEvent *

  스토리지 디바이스에서 읽는 동안 발생하는 복구할 수 없는 읽기 오류와 관련된 이벤트입니다.

- * 혈관 제공자 이벤트 *

  VASA(vSphere APIs for Storage Awareness) Provider와 관련된 이벤트입니다.

실행 중인 작업의 상태를 봅니다

ListSyncJobs 및 ListBulkVolumeJobs API 메서드가 보고하는 웹 UI에서 실행 중인 작업의 진행 상태와 완료 상태를 볼 수 있습니다. 요소 UI의 보고 탭에서 실행 중인 작업 페이지에 액세스할 수 있습니다.

많은 작업이 있는 경우 시스템에서 작업을 대기열에 넣고 일괄적으로 실행할 수 있습니다. 실행 중인 작업 페이지에는 현재 동기화 중인 서비스가 표시됩니다. 작업이 완료되면 대기 중인 다음 동기화 작업으로 대체됩니다. 완료할 작업이 더 이상 없을 때까지 동기화 작업이 실행 중인 작업 페이지에 계속 나타날 수 있습니다.

> 타겟 볼륨이 포함된 클러스터의 실행 중인 작업 페이지에서 복제 진행 중인 볼륨에 대한 복제 동기화 데이터를 볼 수 있습니다.

시스템 경고를 봅니다

시스템의 클러스터 장애 또는 오류에 대한 알림을 볼 수 있습니다. 경고는 정보, 경고 또는 오류일 수 있으며 클러스터의 실행 상태를 나타내는 좋은 지표입니다. 대부분의 오류는 자동으로 해결됩니다.

ListClusterFats API 메서드를 사용하여 경고 모니터링을 자동화할 수 있습니다. 이렇게 하면 발생한 모든 경고에 대한 알림을 받을 수 있습니다.

1. Element UI에서 * Reporting * > * Alerts * 를 선택합니다.

   시스템은 30초마다 페이지의 경고를 새로 고칩니다.

모든 이벤트에 대해 다음 정보가 표시됩니다.

항목	설명
ID입니다	클러스터 경고와 관련된 고유 ID입니다.
심각도입니다	알림의 중요도입니다. 가능한 값: • 경고: 곧 주의가 필요할 수 있는 사소한 문제입니다. 시스템 업그레이드는 여전히 허용됩니다. • 오류: 성능 저하 또는 고가용성(HA)을 잃을 수 있는 장애입니다. 그렇지 않으면 오류는 서비스에 영향을 주지 않습니다. • 위험: 서비스에 영향을 미치는 심각한 장애입니다. 시스템에서 API 또는 클라이언트 I/O 요청을 처리할 수 없습니다. 이 상태에서 작동하면 데이터가 손실될 수 있습니다. • 모범 사례: 권장되는 시스템 구성 모범 사례는 사용되지 않습니다.
유형	고장이 영향을 미치는 구성 요소입니다. 노드, 드라이브, 클러스터, 서비스 또는 볼륨일 수 있습니다.
노드	이 장애가 참조하는 노드의 노드 ID입니다. 노드 및 드라이브 장애에 대해 포함되며, 그렇지 않을 경우 -(대시)로 설정됩니다.
드라이브 ID입니다	이 결함이 참조하는 드라이브의 드라이브 ID입니다. 드라이브 고장에 대해 포함되며, 그렇지 않으면 -(대시)로 설정됩니다.
오류 코드	고장의 원인을 나타내는 설명 코드입니다.
세부 정보	고장에 대한 설명과 추가 세부 정보
날짜	고장이 기록된 날짜 및 시간입니다.

2. 개별 경고에 대한 정보를 보려면 * 세부 정보 표시 * 를 클릭합니다.
3. 페이지에 있는 모든 경고의 세부 정보를 보려면 자세히 열을 클릭합니다.

   시스템에서 경고를 해결한 후에는 해결된 날짜를 포함한 모든 경고 정보가 해결된 영역으로 이동됩니다.

자세한 내용을 확인하십시오

- 클러스터 고장 코드
- "Element API를 사용하여 스토리지를 관리합니다"

시스템에서 경고 페이지에 나열된 오류 코드를 생성하여 관심 있는 오류 또는 상태를 보고합니다. 이러한 코드를 통해 시스템에서 어떤 구성 요소에 경고가 발생했는지, 경고가 발생한 이유를 확인할 수 있습니다.

다음 목록에서는 다양한 코드 유형을 설명합니다.

- * authenticationServiceFault *

  하나 이상의 클러스터 노드에서 인증 서비스가 예상대로 작동하지 않습니다.

  NetApp 지원 팀에 문의하십시오.

- * 가용한 VirtualNetworkIPAddressLow *

  IP 주소 블록의 가상 네트워크 주소 수가 적습니다.

  이 오류를 해결하려면 가상 네트워크 주소 블록에 더 많은 IP 주소를 추가하십시오.

- * 블록클러스터풀 *

  단일 노드 손실을 지원하기에 충분한 여유 블록 스토리지 공간이 없습니다. 클러스터 충만 수준에 대한 자세한 내용은 GetClusterFullThreshold API 메서드를 참조하십시오. 이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - stage3Low(경고): 사용자 정의 임계값이 초과되었습니다. Cluster Full(클러스터 전체) 설정을 조정하거나 노드를 더 추가합니다.
  - stage4Critical(오류): 1노드 장애를 복구할 수 있는 공간이 부족합니다. 볼륨, 스냅샷 및 클론을 생성할 수 없습니다.
  - stage5CompletyConsumered (Critical) 1; 쓰기 또는 새 iSCSI 연결이 허용되지 않습니다. 현재 iSCSI 연결이 유지됩니다. 클러스터에 용량을 더 추가할 때까지 쓰기에 실패합니다. 이 오류를 해결하려면 볼륨을 제거 또는 삭제하거나 스토리지 클러스터에 다른 스토리지 노드를 추가하십시오.

- * 블록성능이 저하됨 *

  장애로 인해 블록 데이터가 더 이상 완전히 복제되지 않습니다.

심각도입니다	설명
경고	블록 데이터의 전체 복사본을 두 개만 액세스할 수 있습니다.
오류	블록 데이터의 전체 복사본을 하나만 액세스할 수 있습니다.
심각	블록 데이터의 전체 복사본을 액세스할 수 없습니다.

- 참고: * 경고 상태는 Triple Helix 시스템에서만 발생할 수 있습니다.

이 오류를 해결하려면 오프라인 노드 또는 블록 서비스를 복원하거나 NetApp Support에 지원을 문의하십시오.

- * BLOCKServiceTooFull *

  블록 서비스가 너무 많은 공간을 사용하고 있습니다.

  이 오류를 해결하려면 프로비저닝된 용량을 더 추가합니다.

- * blockServiceUnhealthy *

  블록 서비스가 정상 상태가 아닌 것으로 감지되었습니다.

  - 심각도 = 경고: 작업이 수행되지 않습니다. 이 경고 기간은 cTimeUntilBSIsKilledMSec = 3300ms로 만료됩니다.
  - 심각도 = 오류: 시스템이 자동으로 데이터를 사용 중지하여 다른 정상 드라이브로 데이터를 재복제합니다.
  - 심각도 = 위험: 복제 개수보다 크거나 같은 여러 노드에서 장애가 발생한 블록 서비스가 있습니다(이중 나선형의 경우 2개). 데이터를 사용할 수 없으며 입력 용지함 동기화가 완료되지 않습니다. 네트워크 연결 문제 및 하드웨어 오류를 확인합니다. 특정 하드웨어 구성 요소에 장애가 발생한 경우 다른 장애가 발생할 수 있습니다. 이 고장은 블록 서비스에 액세스하거나 서비스를 폐기한 경우 삭제됩니다.

- * ClockSkewExceedsFaultThreshold *

  클러스터 마스터와 토큰을 제공하는 노드 간의 시간 차이가 권장 임계값을 초과합니다. 스토리지 클러스터는 노드 간의 시간 차이를 자동으로 수정할 수 없습니다.

  이 오류를 해결하려면 설치 기본값이 아닌 네트워크 내부의 NTP 서버를 사용하십시오. 내부 NTP 서버를 사용하는 경우 NetApp 지원 팀에 지원을 문의하십시오.

- * 클러스터 동기화 *

  공간 부족 상태가 있으며 오프라인 블록 저장소 드라이브의 데이터를 아직 활성 상태인 드라이브와 동기화할 수 없습니다.

  이 오류를 해결하려면 스토리지를 더 추가하십시오.

- * 클러스터풀 *

  스토리지 클러스터에 사용 가능한 스토리지 공간이 더 이상 없습니다.

  이 오류를 해결하려면 스토리지를 더 추가하십시오.

- * 클러스터로IOPSARREOverProvisioned *

  클러스터 IOPS가 초과 프로비저닝됩니다. 모든 최소 QoS IOPS의 합이 클러스터의 예상 IOPS보다 큽니다. 모든 볼륨에 대해 최소 QoS를 동시에 유지할 수는 없습니다.

  이 문제를 해결하려면 볼륨에 대한 최소 QoS IOPS 설정을 낮추십시오.

- * disableDriveSecurityFailed *

  클러스터가 드라이브 보안(저장 시 암호화)을 사용하도록 구성되지 않았지만 하나 이상의 드라이브에 드라이브 보안이 설정되어 있습니다. 즉, 해당 드라이브에서 드라이브 보안을 해제하지 못했습니다. 이 고장은 "경고" 심각도로 기록됩니다.

이 고장을 해결하려면 드라이브 보안을 비활성화할 수 없는 이유에 대한 고장 세부 정보를 확인하십시오. 가능한 원인은 다음과 같습니다.

  - 암호화 키를 가져올 수 없습니다. 키 또는 외부 키 서버에 대한 액세스 문제를 조사하십시오.
  - 드라이브에서 비활성화 작업이 실패했습니다. 잘못된 키를 획득했을 수 있는지 확인하십시오. 두 가지 모두 고장의 원인이 아니라면 드라이브를 교체해야 할 수 있습니다.

  올바른 인증 키를 제공하더라도 보안이 비활성화되지 않는 드라이브를 복구할 수 있습니다. 이 작업을 수행하려면 시스템에서 드라이브를 Available(사용 가능) 으로 이동하여 드라이브를 제거하고 드라이브에서 보안 삭제를 수행한 다음 Active(활성) 로 다시 이동합니다.

- * 연결 해제 클러스터 쌍 *

  클러스터 쌍의 연결이 끊어지거나 잘못 구성되었습니다. 클러스터 간의 네트워크 연결을 확인합니다.

- * 연결 해제 RemoteNode *

  원격 노드의 연결이 끊겼거나 잘못 구성되었습니다. 노드 간 네트워크 연결을 확인합니다.

- * 연결 해제 SnapMirror 엔드포인트 *

  원격 SnapMirror 엔드포인트의 연결이 끊어지거나 잘못 구성되었습니다. 클러스터와 원격 SnapMirrorEndpoint 간의 네트워크 연결을 확인합니다.

- * 드라이브 사용 가능 *

  클러스터에서 하나 이상의 드라이브를 사용할 수 있습니다. 일반적으로 모든 클러스터에는 모든 드라이브가 추가되어야 하며 사용 가능한 상태에서는 없어야 합니다. 이 오류가 예기치 않게 나타날 경우 NetApp 지원 팀에 문의하십시오.

  이 오류를 해결하려면 사용 가능한 드라이브를 스토리지 클러스터에 추가하십시오.

- * 드라이브 실패 *

  하나 이상의 드라이브에 장애가 발생하면 클러스터가 이 오류를 반환하고 다음 조건 중 하나를 표시합니다.

  - 드라이브 관리자가 드라이브에 액세스할 수 없습니다.
  - 슬라이스 또는 블록 서비스가 너무 많은 번 실패했으며, 이는 아마도 드라이브 읽기 또는 쓰기 오류로 인해 발생할 수 있으며 다시 시작할 수 없습니다.
  - 드라이브가 없습니다.
  - 노드의 마스터 서비스에 액세스할 수 없습니다(노드의 모든 드라이브가 누락/실패로 간주됨).
  - 드라이브가 잠겨 있고 드라이브의 인증 키를 가져올 수 없습니다.
  - 드라이브가 잠겨 있고 잠금 해제 작업이 실패합니다. 이 문제를 해결하려면:
  - 노드의 네트워크 연결을 확인합니다.
  - 드라이브를 교체합니다.
  - 인증 키를 사용할 수 있는지 확인합니다.

- * 드라이브 상태 결함 *

드라이브가 SMART 상태 점검에 실패하여 드라이브의 기능이 저하되었습니다. 이 결함의 심각도는 다음과 같습니다.

  - 슬롯 <node slot><drive slot>에 일련 번호 <serial number>이(가) 있는 드라이브가 SMART Overall 상태 검사에 실패했습니다. 이 고장을 해결하려면 드라이브를 교체하십시오.

- * driveWearFault *

  드라이브의 남은 수명이 임계값 아래로 떨어졌지만 여전히 작동하고 있습니다. 이 결함에는 위험 및 경고라는 두 가지 심각도 수준이 있을 수 있습니다.

  - 슬롯이 <node slot><drive slot>인 일련 번호가 <serial number>인 드라이브의 마모 수준이 매우 중요합니다.
  - 슬롯이 <node slot><drive slot>인 슬롯에 일련 번호 <serial number>가 있는 드라이브의 마모 예비량이 적습니다. 이 고장을 해결하려면 드라이브를 곧 교체하십시오.

- * duplicateClusterMasterCandidate *

  둘 이상의 스토리지 클러스터 마스터 후보가 감지되었습니다. NetApp 지원 팀에 문의하십시오.

- * enableDriveSecurityFailed *

  클러스터가 드라이브 보안(저장된 암호화)을 요구하도록 구성되었지만 하나 이상의 드라이브에서 드라이브 보안을 활성화할 수 없습니다. 이 고장은 "경고" 심각도로 기록됩니다.

  이 고장을 해결하려면 드라이브 보안을 활성화할 수 없는 이유에 대한 고장 세부 정보를 확인하십시오. 가능한 원인은 다음과 같습니다.

  - 암호화 키를 가져올 수 없습니다. 키 또는 외부 키 서버에 대한 액세스 문제를 조사하십시오.
  - 드라이브에서 활성화 작업이 실패했습니다. 잘못된 키를 획득했을 수 있는지 확인하십시오. 두 가지 모두 고장의 원인이 아니라면 드라이브를 교체해야 할 수 있습니다.

  올바른 인증 키가 제공되었더라도 보안이 설정되지 않은 드라이브를 복구할 수 있습니다. 이 작업을 수행하려면 시스템에서 드라이브를 Available(사용 가능) 으로 이동하여 드라이브를 제거하고 드라이브에서 보안 삭제를 수행한 다음 Active(활성) 로 다시 이동합니다.

- * EnembleDegraded *

  하나 이상의 앙상블 노드에 대한 네트워크 연결 또는 전원이 손실되었습니다.

  이 오류를 해결하려면 네트워크 연결 또는 전원을 복원하십시오.

- * 예외 *

  고장이 루틴 고장을 제외한 것으로 보고되었습니다. 이러한 고장은 오류 대기열에서 자동으로 삭제되지 않습니다. NetApp 지원 팀에 문의하십시오.

- * failedSpaceTooFull *

  블록 서비스가 데이터 쓰기 요청에 응답하지 않습니다. 이로 인해 슬라이스 서비스의 공간이 부족하여 실패한 쓰기를 저장할 수 없습니다.

  이 오류를 해결하려면 블록 서비스 기능을 복원하여 쓰기가 정상적으로 계속되고 장애가 발생한 공간이 슬라이스 서비스에서 플러시되도록 합니다.

- * 팬센서 *

  팬 센서가 고장났거나 없습니다.

  이 고장을 해결하려면 장애가 발생한 하드웨어를 모두 교체하십시오.

- * 광섬유 채널 액세스 저하됨 *

  Fibre Channel 노드가 스토리지 IP를 통해 스토리지 클러스터의 다른 노드에 일정 기간 응답하지 않습니다. 이 상태에서는 노드가 응답하지 않는 것으로 간주되어 클러스터 장애가 발생합니다. 네트워크 연결을 확인합니다.

- * 광섬유 채널 액세스사용할 수 없음 *

  모든 Fibre Channel 노드가 응답하지 않습니다. 노드 ID가 표시됩니다. 네트워크 연결을 확인합니다.

- * 광섬유 채널 ActiveIxL *

  IxL Nexus 수가 Fibre Channel 노드당 지원되는 활성 세션 8000개 한도에 근접하고 있습니다.

  - 모범 사례 제한은 5500입니다.
  - 경고 한계는 7500입니다.
  - 최대 제한(시행되지 않음)은 8192입니다. 이 고장을 해결하려면 IxL Nexus 수를 Best Practice Limit 인 5500 미만으로 줄이십시오.

- * 광섬유 채널 구성 *

  이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - PCI 슬롯에 예기치 않은 Fibre Channel 포트가 있습니다.
  - 예기치 않은 Fibre Channel HBA 모델이 있습니다.
  - Fibre Channel HBA의 펌웨어에 문제가 있습니다.
  - Fibre Channel 포트가 온라인 상태가 아닙니다.
  - Fibre Channel 패스스루 구성에 지속적인 문제가 있습니다. NetApp 지원 팀에 문의하십시오.

- * 광섬유 채널 IOPS *

  총 IOPS 수가 클러스터의 파이버 채널 노드에 대한 IOPS 제한에 근접하고 있습니다. 제한 사항은 다음과 같습니다.

  - FC0025:450K IOPS는 파이버 채널 노드당 4K 블록 크기로 제한됩니다.
  - FCN001:625K OPS는 파이버 채널 노드당 4K 블록 크기에서 제한됩니다. 이 오류를 해결하려면 사용 가능한 모든 Fibre Channel 노드에서 로드 밸런싱을 조정합니다.

- * 광섬유 채널 StaticIxL *

  IxL Nexus 수가 Fibre Channel 노드당 지원되는 16000개의 정적 세션 제한에 근접하고 있습니다.

  - 모범 사례 제한은 11000입니다.
  - 경고 한계는 15000입니다.
  - 최대 제한(강제 적용)은 16384입니다. 이 고장을 해결하려면 IxL Nexus 개수를 11000의 모범 사례 한도

미만으로 줄이십시오.

- 파일시스템 용량 낮음*

  파일 시스템 중 하나에 공간이 부족합니다.

  이 오류를 해결하려면 파일 시스템에 용량을 더 추가하십시오.

- * fipsDrivesMismatch *

  FIPS가 아닌 드라이브가 FIPS가 지원되는 스토리지 노드에 물리적으로 삽입되었거나 FIPS 드라이브가 아닌 스토리지 노드에 물리적으로 삽입되었습니다. 노드당 단일 장애가 발생하고 영향을 받는 모든 드라이브가 나열됩니다.

  이 고장을 해결하려면 문제가 있는 일치하지 않는 드라이브를 제거하거나 교체합니다.

- * fipsDrivesOutOfCompliance * 를 참조하십시오

  시스템에서 FIPS 드라이브 기능이 활성화된 후 저장된 암호화 기능이 비활성화되었음을 감지했습니다. 이 장애는 FIPS 드라이브 기능이 설정되어 있고 스토리지 클러스터에 비 FIPS 드라이브 또는 노드가 있을 때도 생성됩니다.

  이 오류를 해결하려면 저장 시 암호화 를 설정하거나 스토리지 클러스터에서 비 FIPS 하드웨어를 제거합니다.

- * fipsSelfTestFailure *

  자체 테스트 중에 FIPS 서브시스템에서 오류가 감지되었습니다.

  NetApp 지원 팀에 문의하십시오.

- * 하드웨어 구성 불일치 *

  이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - 구성이 노드 정의와 일치하지 않습니다.
  - 이 노드 유형에 잘못된 드라이브 크기가 있습니다.
  - 지원되지 않는 드라이브가 감지되었습니다. 설치된 Element 버전이 이 드라이브를 인식하지 못하는 이유가 있을 수 있습니다. 이 노드에서 Element 소프트웨어를 업데이트할 것을 권장합니다.
  - 드라이브 펌웨어가 일치하지 않습니다.
  - 드라이브 암호화 가능 상태가 노드와 일치하지 않습니다. NetApp 지원 팀에 문의하십시오.

- * idPCertificateExpiration *

  타사 ID 공급자(IDP)와 함께 사용할 클러스터의 서비스 공급자 SSL 인증서가 만료되었거나 이미 만료되었습니다. 이 결함은 긴급도에 따라 다음과 같은 심각도를 사용합니다.

심각도입니다	설명
경고	인증서가 30일 이내에 만료됩니다.
오류	인증서가 7일 이내에 만료됩니다.

심각	인증서가 3일 이내에 만료되거나 이미 만료되었습니다.

이 오류를 해결하려면 SSL 인증서가 만료되기 전에 업데이트하십시오. 업데이트된 SSL 인증서를 제공하려면 UpdateIdpConfiguration API 메서드와 RefreshCertificateExpirationTime = true 를 사용합니다.

- * 비일관성 모델 *

  VLAN 장치의 연결 모드가 누락되었습니다. 이 고장은 예상 본드 모드와 현재 사용 중인 본드 모드를 표시합니다.

- * 비일관성 InterfaceConfiguration *

  인터페이스 구성이 일치하지 않습니다.

  이 오류를 해결하려면 스토리지 클러스터의 노드 인터페이스가 일관되게 구성되어 있는지 확인합니다.

- * 불일치 *

  이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - Bond1G 불일치: Bond1G 인터페이스에서 일치하지 않는 MTU가 감지되었습니다.
  - Bond10G 불일치: Bond10G 인터페이스에서 일치하지 않는 MTU가 감지되었습니다. 이 장애는 관련된 MTU 값과 함께 문제의 노드나 노드를 표시합니다.

- * 비일관성 RoutingRules *

  이 인터페이스의 라우팅 규칙이 일치하지 않습니다.

- * 불일관된 SubnetMasks *

  VLAN 장치의 네트워크 마스크가 VLAN에 대해 내부적으로 기록된 네트워크 마스크와 일치하지 않습니다. 이 고장은 예상 네트워크 마스크와 현재 사용 중인 네트워크 마스크를 표시합니다.

- * incorrectBondPortCount *

  연결 포트 수가 올바르지 않습니다.

- * invalidConfiguredFiberChannelNodeCount * 입니다

  두 예상 Fibre Channel 노드 연결 중 하나의 성능이 저하되었습니다. 이 오류는 하나의 Fibre Channel 노드만 연결되어 있을 때 나타납니다.

  이 오류를 해결하려면 클러스터 네트워크 연결 및 네트워크 케이블을 확인하고 실패한 서비스가 있는지 확인합니다. 네트워크 또는 서비스 문제가 없는 경우 NetApp Support에서 파이버 채널 노드 교체를 문의하십시오.

- * irqBalancepFailed *

  인터럽트의 균형을 맞추는 동안 예외가 발생했습니다.

  NetApp 지원 팀에 문의하십시오.

- * kmipCertificateFault *

- 루트 인증 기관(CA) 인증서의 만료 시기가 다가오고 있습니다.

  이 오류를 해결하려면 만료 날짜가 30일 이상 지난 루트 CA에서 새 인증서를 얻고 ModifyKeyServerKmip을 사용하여 업데이트된 루트 CA 인증서를 제공하십시오.

- 클라이언트 인증서 만료 시기가 다가오고 있습니다.

  이 오류를 해결하려면 GetClientCertificateSigningRequest를 사용하여 새 CSR을 생성하고 새 만료 날짜가 30일 이상 경과되도록 서명한 후 ModifyKeyServerKmip을 사용하여 만료되는 KMIP 클라이언트 인증서를 새 인증서로 교체합니다.

- 루트 인증 기관(CA) 인증서가 만료되었습니다.

  이 오류를 해결하려면 만료 날짜가 30일 이상 지난 루트 CA에서 새 인증서를 얻고 ModifyKeyServerKmip을 사용하여 업데이트된 루트 CA 인증서를 제공하십시오.

- 클라이언트 인증서가 만료되었습니다.

  이 오류를 해결하려면 GetClientCertificateSigningRequest를 사용하여 새 CSR을 생성하고 새 만료 날짜가 30일 이상 경과되도록 서명한 후 ModifyKeyServerKmip을 사용하여 만료된 KMIP 클라이언트 인증서를 새 인증서로 교체합니다.

- 루트 인증 기관(CA) 인증서 오류입니다.

  이 오류를 해결하려면 올바른 인증서가 제공되었는지 확인하고 필요한 경우 루트 CA에서 인증서를 다시 획득합니다. ModifyKeyServerKmip을 사용하여 올바른 KMIP 클라이언트 인증서를 설치합니다.

- 클라이언트 인증서 오류입니다.

  이 고장을 해결하려면 올바른 KMIP 클라이언트 인증서가 설치되었는지 확인하십시오. 클라이언트 인증서의 루트 CA가 EKS에 설치되어야 합니다. ModifyKeyServerKmip을 사용하여 올바른 KMIP 클라이언트 인증서를 설치합니다.

- * kmipServerFault *
  - 연결 실패

    이 고장을 해결하려면 외부 키 서버가 활성 상태인지, 네트워크를 통해 연결할 수 있는지 확인하십시오. 연결을 테스트하려면 TestKeyServerKimp 및 TestKeyProviderKmip 을 사용합니다.

  - 인증에 실패했습니다

    이 문제를 해결하려면 올바른 루트 CA 및 KMIP 클라이언트 인증서를 사용하고 있고 개인 키와 KMIP 클라이언트 인증서가 일치하는지 확인하십시오.

  - 서버 오류입니다

    이 고장을 해결하려면 오류에 대한 세부 정보를 확인하십시오. 반환된 오류에 따라 외부 키 서버의 문제 해결이 필요할 수 있습니다.

- * 암기편임계값 *

  수정 가능 또는 수정할 수 없는 많은 ECC 오류가 감지되었습니다. 이 결함은 긴급도에 따라 다음과 같은 심각도를 사용합니다.

이벤트	심각도입니다	설명
단일 DIMM cErrorCount는 cDimmCorrectableErrWarnThreshold에 도달합니다.	경고	DIMM:<프로세서><DIMM 슬롯>에서 수정 가능한 ECC 메모리 오류가 임계값보다 높습니다
단일 DIMM cErrorCount는 cErrorFaultTimer 가 DIMM에 대해 만료될 때까지 immCorrectableErrWarnThreshold를 유지합니다.	오류	DIMM:<프로세서><DIMM>에서 수정 가능한 ECC 메모리 오류가 임계값보다 높습니다
메모리 컨트롤러는 cErrorCount above cMemCtlCorrectableErrWarnThreshold 를 보고하고 cMemCtlrCorrectableErrWarnDuration 을 지정합니다.	경고	수정 가능한 ECC 메모리 오류가 메모리 컨트롤러의 임계값보다 높음:<프로세서><메모리 컨트롤러>
메모리 컨트롤러는 메모리 컨트롤러에 대해 cErrorFaultTimer 가 만료될 때까지 cErrorCount 를 cMemCtlCorrectableErrWarnThreshold 보다 높게 보고합니다.	오류	DIMM:<프로세서><DIMM>에서 수정 가능한 ECC 메모리 오류가 임계값보다 높습니다
단일 DIMM은 0보다 큰 uErrorCount를 보고하지만 cDimmUncorrectableErrFaultThreshold보다 작습니다.	경고	DIMM:<프로세서><DIMM 슬롯>에서 수정할 수 없는 ECC 메모리 오류가 감지되었습니다
단일 DIMM은 적어도 cDimmUncorrectableErrFaultThreshold의 uErrorCount를 보고합니다.	오류	DIMM:<프로세서><DIMM 슬롯>에서 수정할 수 없는 ECC 메모리 오류가 감지되었습니다
메모리 컨트롤러는 uErrorCount 가 0보다 크지만 cMemCtlrUncorrectableErrFaultThreshold 보다 작다는 것을 보고합니다.	경고	메모리 컨트롤러 <Processor><Memory Controller>에서 수정할 수 없는 ECC 메모리 오류가 감지되었습니다
메모리 컨트롤러는 cMemCtlrUncorrectableErrFaultThreshold의 uErrorCount를 보고합니다.	오류	메모리 컨트롤러 <Processor><Memory Controller>에서 수정할 수 없는 ECC 메모리 오류가 감지되었습니다

이 고장을 해결하려면 NetApp 지원에 문의하여 지원을 받으십시오.

- * 메모리 사용 임계값 *

  메모리 사용량이 정상보다 높습니다. 이 결함은 긴급도에 따라 다음과 같은 심각도를 사용합니다.

고장 유형에 대한 자세한 내용은 오류 결함의 * 세부 정보 * 표제를 참조하십시오.

심각도입니다	설명
경고	시스템 메모리가 부족합니다.
오류	시스템 메모리가 매우 부족합니다.
심각	시스템 메모리가 완전히 소모되었습니다.

이 고장을 해결하려면 NetApp 지원에 문의하여 지원을 받으십시오.

- * 메타 클러스터풀 *

  단일 노드 손실을 지원하기에 충분한 여유 메타데이터 스토리지 공간이 없습니다. 클러스터 충만 수준에 대한 자세한 내용은 GetClusterFullThreshold API 메서드를 참조하십시오. 이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - stage3Low(경고): 사용자 정의 임계값이 초과되었습니다. Cluster Full(클러스터 전체) 설정을 조정하거나 노드를 더 추가합니다.
  - stage4Critical(오류): 1노드 장애를 복구할 수 있는 공간이 부족합니다. 볼륨, 스냅샷 및 클론을 생성할 수 없습니다.
  - stage5CompletyConsumered (Critical) 1; 쓰기 또는 새 iSCSI 연결이 허용되지 않습니다. 현재 iSCSI 연결이 유지됩니다. 클러스터에 용량을 더 추가할 때까지 쓰기에 실패합니다. 데이터를 삭제 또는 삭제하거나 노드를 더 추가합니다. 이 오류를 해결하려면 볼륨을 제거 또는 삭제하거나 스토리지 클러스터에 다른 스토리지 노드를 추가하십시오.
- * mbuCheckFailure *

  네트워크 디바이스가 적절한 MTU 크기로 구성되지 않았습니다.

  이 고장을 해결하려면 모든 네트워크 인터페이스 및 스위치 포트가 점보 프레임(최대 9000바이트 크기)에 맞게 구성되었는지 확인하십시오.

- * 네트워크 구성 *

  이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - 예상된 인터페이스가 존재하지 않습니다.
  - 중복된 인터페이스가 있습니다.
  - 구성된 인터페이스가 다운되었습니다.
  - 네트워크를 다시 시작해야 합니다. NetApp 지원 팀에 문의하십시오.
- * nobaableVirtualNetworkIPAddresses *

  IP 주소 블록에 사용 가능한 가상 네트워크 주소가 없습니다.

  - virtualNetworkID# 태그(#)에 사용 가능한 스토리지 IP 주소가 없습니다. 클러스터에 노드를 추가할 수 없습니다. 이 오류를 해결하려면 가상 네트워크 주소 블록에 더 많은 IP 주소를 추가하십시오.

- * nodeHardwareFault(네트워크 인터페이스 <name>이(가) 다운되었거나 케이블이 뽑혀 있음) *

  네트워크 인터페이스가 다운되었거나 케이블이 분리되었습니다.

  이 고장을 해결하려면 노드나 노드의 네트워크 연결을 확인하십시오.

- * nodeHardwareFault(드라이브 암호화 가능 상태가 슬롯 <node slot><drive slot>) * 의 드라이브에 대한 노드의 암호화 가능 상태와 일치하지 않습니다

  드라이브가 설치된 스토리지 노드의 암호화 기능과 일치하지 않습니다.

- * nodeHardwareFault(이 노드 유형에 대해 슬롯 <node slot><drive slot>의 드라이브에 대해 <드라이브 유형> 드라이브 크기 <실제 크기>가 올바르지 않음 - 예상 크기>) *

  스토리지 노드에는 이 노드의 크기가 잘못된 드라이브가 포함되어 있습니다.

- * nodeHardwareFault(슬롯 <node slot><drive slot>에서 지원되지 않는 드라이브가 감지되었습니다. 드라이브 통계 및 상태 정보를 사용할 수 없습니다.) *

  스토리지 노드에 지원되지 않는 드라이브가 포함되어 있습니다.

- * nodeHardwareFault(슬롯 <node slot><드라이브 슬롯>의 드라이브가 펌웨어 버전 <예상 버전>을(를) 사용해야 하지만 지원되지 않는 버전 <실제 버전>을(를) 사용하고 있음) *

  스토리지 노드에는 지원되지 않는 펌웨어 버전을 실행하는 드라이브가 포함되어 있습니다.

- * 노드 유지보수모드 *

  노드가 유지보수 모드로 전환되었습니다. 이 결함은 긴급도에 따라 다음과 같은 심각도를 사용합니다.

심각도입니다	설명
경고	노드가 아직 유지보수 모드에 있음을 나타냅니다.
오류	장애 발생 또는 활성 스탠바이로 인해 유지보수 모드가 비활성화되지 않았음을 나타냅니다.

  이 고장을 해결하려면 유지보수가 완료된 후 유지보수 모드를 비활성화하십시오. 오류 수준 고장이 지속될 경우 NetApp 지원에 지원을 문의하십시오.

- * 노드 오프라인 *

  Element 소프트웨어가 지정된 노드와 통신할 수 없습니다. 네트워크 연결을 확인합니다.

- * notUsingLCPBondMode *

  LACP 결합 모드가 구성되지 않았습니다.

  이 오류를 해결하려면 스토리지 노드를 구축할 때 LACP 결합을 사용합니다. LACP가 활성화되어 있지 않고 올바르게 구성되지 않은 경우 클라이언트에서 성능 문제를 겪을 수 있습니다.

- * ntpServerUnreachable *

스토리지 클러스터가 지정된 NTP 서버 또는 서버와 통신할 수 없습니다.

이 오류를 해결하려면 NTP 서버, 네트워크 및 방화벽에 대한 구성을 확인하십시오.

- * ntpTimeNotInSync * 를 선택합니다

  스토리지 클러스터 시간과 지정된 NTP 서버 시간 간의 차이가 너무 큽니다. 스토리지 클러스터가 자동으로 차이를 수정할 수 없습니다.

  이 오류를 해결하려면 설치 기본값이 아닌 네트워크 내부의 NTP 서버를 사용하십시오. 내부 NTP 서버를 사용하고 있고 문제가 지속되면 NetApp 지원 팀에 지원을 문의하십시오.

- nvramDeviceStatus *

  NVRAM 장치에 오류가 있거나, 오류가 발생했거나, 오류가 발생했습니다. 이 결함에는 다음과 같은 심각도가 있습니다.

심각도입니다	설명
경고	하드웨어에 의해 경고가 감지되었습니다. 이 조건은 온도 경고와 같이 일시적인 것일 수 있습니다. • nvmLifetimeError 를 참조하십시오 • nvmLifetimeStatus를 참조하십시오 • energySourceLifetimeStatus를 참조하십시오 • energySourceTemperatureStatus를 참조하십시오 • WarningThresholdExceeded(경고 임계홀더제외)
오류	하드웨어에서 오류 또는 위험 상태가 감지되었습니다. 클러스터 마스터가 슬라이스 드라이브를 작업에서 제거하려고 합니다. 이렇게 하면 드라이브 제거 이벤트가 생성됩니다. 보조 슬라이스 서비스를 사용할 수 없는 경우 드라이브가 제거되지 않습니다. 경고 수준 오류와 함께 반환된 오류: • NVRAM 디바이스 마운트 지점이 없습니다. • NVRAM 장치 파티션이 존재하지 않습니다. • NVRAM 장치 파티션이 있지만 마운트되지 않았습니다.

심각	하드웨어에서 오류 또는 위험 상태가 감지되었습니다. 클러스터 마스터가 슬라이스 드라이브를 작업에서 제거하려고 합니다. 이렇게 하면 드라이브 제거 이벤트가 생성됩니다. 보조 슬라이스 서비스를 사용할 수 없는 경우 드라이브가 제거되지 않습니다. • 지속 • 팔StatusSaveNArmed 를 선택합니다 • csaveStatusError입니다

노드에서 장애가 발생한 하드웨어를 교체합니다. 그래도 문제가 해결되지 않으면 NetApp Support에 문의하십시오.

- 전원 공급 장치 오류

  이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - 전원 공급 장치가 없습니다.
  - 전원 공급 장치에 장애가 발생했습니다.
  - 전원 공급 장치 입력이 없거나 범위를 벗어났습니다. 이 오류를 해결하려면 중복 전원이 모든 노드에 공급되는지 확인합니다. NetApp 지원 팀에 문의하십시오.

- * 프로비저닝됨 스페이스투풀 *

  클러스터의 전체 프로비저닝 용량이 너무 가득 찼습니다.

  이 오류를 해결하려면 프로비저닝된 공간을 추가하거나 볼륨을 삭제 및 퍼지합니다.

- * remoteRepAsyncDelayExceeded *

  복제에 대해 구성된 비동기 지연을 초과했습니다. 클러스터 간 네트워크 연결을 확인합니다.

- * remoteRepClusterFull *

  타겟 스토리지 클러스터가 너무 가득 차 볼륨이 원격 복제를 일시 중지했습니다.

  이 오류를 해결하려면 타겟 스토리지 클러스터에서 공간을 확보하십시오.

- * remoteRepSnapshotClusterFull *

  타겟 스토리지 클러스터가 너무 가득 차 있어 볼륨이 스냅샷의 원격 복제를 일시 중지했습니다.

  이 오류를 해결하려면 타겟 스토리지 클러스터에서 공간을 확보하십시오.

- * remoteRepSnapshotsExcedLimit *

  타겟 스토리지 클러스터 볼륨이 스냅샷 제한을 초과했기 때문에 볼륨이 스냅샷의 원격 복제를 일시 중지했습니다.

  이 오류를 해결하려면 타겟 스토리지 클러스터에서 스냅샷 제한을 늘리십시오.

- 별표(* scheduleActionError*)

하나 이상의 예약된 작업이 실행되었지만 실패했습니다.

예약된 활동이 다시 실행되고 성공하거나, 예약된 활동이 삭제되거나, 활동이 일시 중지되어 재개되면 결함이 지워집니다.

- * sensorReadingFailed *

  베이스보드 관리 컨트롤러(BMC) 자체 테스트에 실패했거나 센서가 BMC와 통신할 수 없습니다.

  NetApp 지원 팀에 문의하십시오.

- * serviceNotRunning *

  필요한 서비스가 실행되고 있지 않습니다.

  NetApp 지원 팀에 문의하십시오.

- * 슬라이서 서비스전체 *

  슬라이스 서비스에 할당된 프로비저닝 용량이 너무 적습니다.

  이 오류를 해결하려면 프로비저닝된 용량을 더 추가합니다.

- * 슬라이슬리서비스건강하지 않음 *

  시스템에서 슬라이스 서비스가 정상 상태가 아닌 것을 감지하여 자동으로 서비스 해제를 합니다.

  - 심각도 = 경고: 작업이 수행되지 않습니다. 이 경고 기간은 6분 후에 만료됩니다.
  - 심각도 = 오류: 시스템이 자동으로 데이터를 사용 중지하여 다른 정상 드라이브로 데이터를 재복제합니다. 네트워크 연결 문제 및 하드웨어 오류를 확인합니다. 특정 하드웨어 구성 요소에 장애가 발생한 경우 다른 장애가 발생할 수 있습니다. 슬라이스 서비스에 액세스할 수 있거나 서비스가 해체되면 결함이 지워집니다.

- * sshEnabled *

  SSH 서비스는 스토리지 클러스터의 하나 이상의 노드에서 설정됩니다.

  이 오류를 해결하려면 해당 노드에서 SSH 서비스를 비활성화하거나 NetApp 지원에 연락하여 지원을 받으십시오.

- * sslCertificateExpiration *

  이 노드와 연결된 SSL 인증서가 만료되었거나 만료되었습니다. 이 결함은 긴급도에 따라 다음과 같은 심각도를 사용합니다.

심각도입니다	설명
경고	인증서가 30일 이내에 만료됩니다.
오류	인증서가 7일 이내에 만료됩니다.
심각	인증서가 3일 이내에 만료되거나 이미 만료되었습니다.

  이 고장을 해결하려면 SSL 인증서를 갱신하십시오. 필요한 경우 NetApp Support에 지원을 요청하십시오.

- * 용량 *

  단일 노드는 스토리지 클러스터 용량의 절반 이상을 차지합니다.

  시스템은 데이터 이중화를 유지하기 위해 최대 노드의 용량을 줄여 일부 블록 용량이 고립되도록 합니다(미사용).

  이 오류를 해결하려면 기존 스토리지 노드에 드라이브를 추가하거나 클러스터에 스토리지 노드를 추가합니다.

- * tempSensor *

  온도 센서가 정상 온도보다 높은 온도를 보고하고 있습니다. 이 고장은 전원 공급 장치 오류 또는 팬센서 오류와 함께 발생할 수 있습니다.

  이 고장을 해결하려면 저장소 클러스터 근처의 공기 흐름을 방해하는 물체가 있는지 확인하십시오. 필요한 경우 NetApp Support에 지원을 요청하십시오.

- * 업그레이드 *

  24시간 이상 업그레이드가 진행 중입니다.

  이 고장을 해결하려면 업그레이드를 재개하거나 NetApp 지원에 지원을 문의하십시오.

- * 무응답 서비스 *

  서비스가 응답하지 않습니다.

  NetApp 지원 팀에 문의하십시오.

- * virtualNetworkConfig *

  이 클러스터 고장은 다음 상태 중 하나를 나타냅니다.

  - 인터페이스가 없습니다.
  - 인터페이스에 잘못된 네임스페이스가 있습니다.
  - 잘못된 넷마스크가 있습니다.
  - 잘못된 IP 주소가 있습니다.
  - 인터페이스가 실행되고 있지 않습니다.
  - 노드에 불필요한 인터페이스가 있습니다. NetApp 지원 팀에 문의하십시오.

- * 볼륨이 저하됨 *

  보조 볼륨의 복제 및 동기화가 완료되지 않았습니다. 동기화가 완료되면 메시지가 지워집니다.

- * volumesOffline *

  스토리지 클러스터에 있는 하나 이상의 볼륨이 오프라인 상태입니다. 볼륨 디그레이드 * 오류도 나타납니다.

  NetApp 지원 팀에 문의하십시오.

노드 성능 작업을 봅니다

각 노드의 성능 활동을 그래픽 형식으로 볼 수 있습니다. 이 정보는 노드의 각 드라이브에 대한 CPU 및 초당 읽기/쓰기 입출력 작업(IOPS)에 대한 실시간 통계를 제공합니다. 활용률 그래프는 5초마다 업데이트되고, 드라이브 통계 그래프는 10초마다 업데이트됩니다.

1. 클러스터 * > * 노드 * 를 클릭합니다.
2. 보려는 노드에 대해 * 작업 * 을 클릭합니다.
3. 세부 정보 보기 * 를 클릭합니다.

> 선 또는 막대 위에 커서를 놓으면 선 및 막대 그래프에서 특정 시점을 볼 수 있습니다.

볼륨 성능을 봅니다

클러스터의 모든 볼륨에 대한 자세한 성능 정보를 볼 수 있습니다. 볼륨 ID 또는 성능 열을 기준으로 정보를 정렬할 수 있습니다. 특정 기준에 따라 정보를 필터링할 수도 있습니다.

모든 * 새로 고침 * 목록을 클릭하고 다른 값을 선택하여 시스템에서 페이지의 성능 정보를 새로 고치는 빈도를 변경할 수 있습니다. 클러스터의 볼륨이 1,000개 미만인 경우 기본 업데이트 간격은 10초입니다. 그렇지 않으면 기본값은 60초입니다. Never 값을 선택하면 자동 페이지 새로 고침이 비활성화됩니다.

자동 새로 고침 * 자동 새로 고침 * 을 클릭하여 자동 새로 고침을 다시 설정할 수 있습니다.

1. Element UI에서 * Reporting * > * Volume Performance * 를 선택합니다.
2. 볼륨 목록에서 볼륨에 대한 작업 아이콘을 클릭합니다.
3. 세부 정보 보기 * 를 클릭합니다.

   용지 하단에는 용적에 대한 일반 정보가 들어 있는 용지함이 표시됩니다.

4. 볼륨에 대한 자세한 정보를 보려면 * 자세한 정보 보기 * 를 클릭하십시오.

   볼륨에 대한 성능 그래프와 자세한 정보가 표시됩니다.

자세한 내용을 확인하십시오

볼륨 성능 세부 정보입니다

볼륨 성능 세부 정보입니다

Element UI의 Reporting(보고) 탭에 있는 Volume Performance(볼륨 성능) 페이지에서 볼륨의 성능 통계를 볼 수 있습니다.

다음 목록에서는 사용 가능한 세부 사항을 설명합니다.

- * ID *

  볼륨에 대한 시스템 생성 ID입니다.

- * 이름 *

  볼륨을 생성할 때 볼륨에 지정한 이름입니다.

- * 계정 *

  볼륨에 할당된 계정의 이름입니다.

- * 액세스 그룹 *

  볼륨이 속한 볼륨 액세스 그룹 또는 그룹의 이름입니다.

- * 볼륨 활용률 *

  클라이언트가 볼륨을 얼마나 사용하고 있는지 설명하는 백분율 값입니다.

  가능한 값:

  - 0 = 클라이언트가 볼륨을 사용하고 있지 않습니다
  - 100 = 클라이언트가 최대값을 사용 중입니다
  - 100 초과 = 클라이언트가 버스트를 사용 중입니다

- * 총 IOPS *

  해당 볼륨에 대해 현재 실행 중인 총 IOPS(읽기 및 쓰기) 수입니다.

- * 읽기 IOPS *

  해당 볼륨에 대해 현재 실행 중인 총 읽기 IOPS 수입니다.

- * 쓰기 IOPS *

  해당 볼륨에 대해 현재 실행 중인 총 쓰기 IOPS 수입니다.

- * 총 처리량 *

  현재 볼륨에 대해 실행 중인 총 처리량(읽기 및 쓰기)입니다.

- * 읽기 처리량 *

  해당 볼륨에 대해 현재 실행 중인 총 읽기 처리량입니다.

- * 쓰기 처리량 *

  해당 볼륨에 대해 현재 실행 중인 총 쓰기 처리량입니다.

- * 총 지연 시간 *

  볼륨에 대한 읽기 및 쓰기 작업을 완료하는 데 걸리는 평균 시간(마이크로초)입니다.

- * 읽기 지연 시간 *

마지막 500밀리초 동안 볼륨에 대한 읽기 작업을 완료하는 데 걸리는 평균 시간(마이크로초)입니다.

- * 쓰기 지연 시간 *

  마지막 500밀리초 동안 볼륨에 대한 쓰기 작업을 완료하는 데 걸리는 평균 시간(마이크로초)입니다.

- * 대기열 길이 *

  볼륨에 대한 미해결 읽기 및 쓰기 작업 수입니다.

- * 평균 IO 크기 *

  최근 500밀리초 동안 볼륨에 대한 최근 I/O의 평균 크기(바이트)입니다.

iSCSI 세션을 봅니다

클러스터에 연결된 iSCSI 세션을 볼 수 있습니다. 원하는 세션만 포함하도록 정보를 필터링할 수 있습니다.

1. Element UI에서 * Reporting * > * iSCSI Sessions * 를 선택합니다.
2. 필터 조건 필드를 보려면 * 필터 * 를 클릭합니다.

자세한 내용을 확인하십시오

iSCSI 세션 세부 정보입니다

iSCSI 세션 세부 정보입니다

클러스터에 연결된 iSCSI 세션에 대한 정보를 볼 수 있습니다.

다음 목록에서는 iSCSI 세션에 대해 찾을 수 있는 정보를 설명합니다.

- * 노드 *

  볼륨의 기본 메타데이터 파티션을 호스팅하는 노드입니다.

- * 계정 *

  볼륨을 소유하는 계정의 이름입니다. 값이 비어 있으면 대시(-)가 표시됩니다.

- * 볼륨 *

  노드에서 식별된 볼륨 이름입니다.

- * 볼륨 ID *

  타겟 IQN과 연결된 볼륨의 ID입니다.

- * 초기자 ID *

  이니시에이터에 대한 시스템 생성 ID입니다.

- * 초기자 별칭 *

  긴 목록에서 이니시에이터를 쉽게 찾을 수 있도록 해 주는 이니시에이터의 선택적 이름입니다.

- * 이니시에이터 IP *

  세션을 시작하는 엔드포인트의 IP 주소입니다.

- * 초기자 IQN *

  세션을 시작하는 엔드포인트의 IQN입니다.

- * 대상 IP *

  볼륨을 호스팅하는 노드의 IP 주소입니다.

- * 타겟 IQN *

  볼륨의 IQN입니다.

- * 작성일: *

  세션이 설정된 날짜입니다.

Fibre Channel 세션을 봅니다

클러스터에 연결된 파이버 채널(FC) 세션을 볼 수 있습니다. 창에 표시할 연결만 포함하도록 정보를 필터링할 수 있습니다.

1. Element UI에서 * Reporting * > * FC Sessions * 를 선택합니다.
2. 필터 조건 필드를 보려면 * 필터 * 를 클릭합니다.

자세한 내용을 확인하십시오

Fibre Channel 세션 세부 정보입니다

Fibre Channel 세션 세부 정보입니다

클러스터에 연결된 활성 FC(Fibre Channel) 세션에 대한 정보를 찾을 수 있습니다.

다음 목록에는 클러스터에 연결된 FC 세션에 대한 정보가 정리되어 있습니다.

- * 노드 ID *

  연결을 위해 세션을 호스팅하는 노드입니다.

- * 노드 이름 *

  시스템에서 생성된 노드 이름입니다.

- * 초기자 ID *

  이니시에이터에 대한 시스템 생성 ID입니다.

- * 이니시에이터 WWPN *

  시작 전 세계 포트 이름입니다.

- * 초기자 별칭 *

  긴 목록에서 이니시에이터를 쉽게 찾을 수 있도록 해 주는 이니시에이터의 선택적 이름입니다.

- * 대상 WWPN *

  대상 Worldwide 포트 이름입니다.

- * 볼륨 액세스 그룹 *

  세션이 속한 볼륨 액세스 그룹의 이름입니다.

- * 볼륨 액세스 그룹 ID *

  액세스 그룹에 대해 시스템에서 생성한 ID입니다.

드라이브 문제를 해결합니다

오류가 발생한 SSD(Solid-State Drive)를 교체 드라이브로 교체할 수 있습니다. SolidFire 스토리지 노드용 SSD는 핫 스왑이 가능합니다. SSD에 장애가 발생했다고 의심되는 경우 NetApp 지원 팀에 문의하여 장애를 확인하고 적절한 해결 절차를 안내합니다. NetApp Support는 또한 귀사와 협력하여 서비스 수준 계약에 따라 교체 드라이브를 제공합니다.

이 경우 어떻게 스왑이 가능하면 활성 노드에서 장애가 발생한 드라이브를 제거하고 NetApp에서 새 SSD 드라이브로 교체할 수 있습니다. 활성 클러스터에서 장애가 발생하지 않은 드라이브를 제거하는 것은 권장되지 않습니다.

장애가 발생할 경우 드라이브를 즉시 교체할 수 있도록 NetApp Support에서 제안한 현장 예비 부품을 유지보수해야 합니다.

> 테스트를 위해 노드에서 드라이브를 잡아당겨 드라이브 장애를 시뮬레이트하는 경우 드라이브를 드라이브 슬롯에 다시 삽입하기 전에 30초 정도 기다려야 합니다.

드라이브에 장애가 발생하면 이중 Helix는 클러스터의 나머지 노드에 데이터를 재배포합니다. Element 소프트웨어는 동일한 노드에 있는 두 개의 데이터 복사본을 보호하므로 동일한 노드에서 여러 드라이브 장애가 발생해도 문제가 되지 않습니다. 드라이브 장애가 발생하면 다음과 같은 이벤트가 발생합니다.

- 데이터가 드라이브에서 마이그레이션됩니다.
- 전체 클러스터 용량은 드라이브 용량에 따라 감소합니다.
- 이중 Helix 데이터 보호로 2개의 유효한 데이터 복사본이 보장됩니다.

SolidFire 스토리지 시스템은 데이터를 마이그레이션할 스토리지 양이 부족한 경우 드라이브 제거를 지원하지 않습니다.

를 참조하십시오

- 클러스터에서 장애가 발생한 드라이브를 제거합니다
- 기본 MDSS 드라이브 문제 해결
- MDSS 드라이브를 제거합니다
- "SolidFire 스토리지 노드의 드라이브 교체"
- "H600S 시리즈 스토리지 노드의 드라이브 교체"
- "H410S 및 H610S 하드웨어 정보"
- "SF-시리즈 하드웨어 정보"

클러스터에서 장애가 발생한 드라이브를 제거합니다

SolidFire 시스템은 드라이브의 자체 진단 유틸리티에서 장애가 발생했다고 진단하거나 드라이브와의 통신이 5분 30분 이상 중지되는 경우 드라이브를 오류 상태로 전환합니다. 장애가 발생한 드라이브 목록이 표시됩니다. NetApp Element 소프트웨어의 실패한 드라이브 목록에서 오류가 발생한 드라이브를 제거해야 합니다.

노드가 오프라인일 때 * Alerts * 목록의 드라이브가 * blockServiceUnhealy * 로 표시됩니다. 노드를 다시 시작할 때 5분 30분 이내에 노드와 드라이브가 온라인 상태로 돌아오면 드라이브가 자동으로 업데이트되고 클러스터의 활성 드라이브로 계속 진행됩니다.

1. Element UI에서 * Cluster * > * Drives * 를 선택합니다.
2. 실패한 드라이브 목록을 보려면 * 실패 * 를 클릭합니다.
3. 장애가 발생한 드라이브의 슬롯 번호를 확인합니다.

   섀시에서 오류가 발생한 드라이브를 찾으려면 이 정보가 필요합니다.

4. 다음 방법 중 하나를 사용하여 장애가 발생한 드라이브를 제거합니다.

옵션을 선택합니다	단계
개별 드라이브를 제거합니다	a. 제거할 드라이브에 대해 * 작업 * 을 클릭합니다. b. 제거 * 를 클릭합니다.
여러 드라이브를 제거합니다	a. 제거할 드라이브를 모두 선택하고 * 대량 작업 * 을 클릭합니다. b. 제거 * 를 클릭합니다.

기본 **MDSS** 드라이브 문제 해결

하나 또는 두 메타데이터 드라이브 모두에 장애가 발생할 경우 메타데이터(또는 슬라이스) 드라이브를 클러스터에 다시 추가하여 복구할 수 있습니다. 노드에서 MDSS 기능이 이미 활성화된 경우 NetApp Element UI에서 복구 작업을 수행할 수 있습니다.

노드의 메타데이터 드라이브 중 하나 또는 둘 다에 장애가 발생하면 슬라이스 서비스가 종료되고 두 드라이브의 데이터가 노드의 다른 드라이브에 백업됩니다.

다음 시나리오는 발생 가능한 실패 시나리오를 설명하고 문제를 해결하기 위한 기본 권장 사항을 제공합니다.

시스템 슬라이스 드라이브가 작동하지 않습니다

- 이 시나리오에서는 슬롯 2가 확인되어 사용 가능한 상태로 돌아갑니다.
- 슬라이스 서비스를 다시 온라인으로 전환하기 전에 시스템 슬라이스 드라이브를 다시 채워야 합니다.
- 시스템 슬라이스 드라이브를 교체해야 합니다. 시스템 슬라이스 드라이브를 사용할 수 있게 되면 드라이브와 슬롯 2 드라이브를 동시에 추가해야 합니다.

> 슬롯 2의 드라이브는 메타데이터 드라이브로 추가할 수 없습니다. 두 드라이브를 동시에 노드에 다시 추가해야 합니다.

슬롯 **2**에 장애가 있습니다

- 이 시나리오에서는 시스템 슬라이스 드라이브를 확인하고 사용 가능한 상태로 돌아갑니다.
- 슬롯 2를 스페어로 교체해야 합니다. 슬롯 2를 사용할 수 있게 되면 시스템 슬라이스 드라이브와 슬롯 2 드라이브를 동시에 추가합니다.

시스템 슬라이스 드라이브 및 슬롯 **2**에 장애가 있습니다

- 시스템 슬라이스 드라이브와 슬롯 2를 모두 스페어 드라이브로 교체해야 합니다. 두 드라이브를 모두 사용할 수 있게 되면 시스템 슬라이스 드라이브와 슬롯 2 드라이브를 동시에 추가합니다.

작업 순서

- 장애가 발생한 하드웨어 드라이브를 스페어 드라이브로 교체합니다(둘 다 장애가 발생한 경우 두 드라이브를 모두 교체합니다).
- 드라이브가 다시 채워지고 사용 가능 상태가 되면 클러스터에 다시 드라이브를 추가합니다.

작업을 확인합니다

- 슬롯 0(또는 내부) 및 슬롯 2의 드라이브가 활성 드라이브 목록에서 메타데이터 드라이브로 식별되는지 확인합니다.
- 모든 슬라이스 균형 조정이 완료되었는지 확인합니다(이벤트 로그에 최소 30분 동안 더 이상 슬라이스 이동 메시지가 없습니다).

를 참조하십시오

MDSS 드라이브를 추가합니다

MDSS 드라이브를 추가합니다

슬롯 2의 블록 드라이브를 슬라이스 드라이브로 변환하여 SolidFire 노드에 두 번째 메타데이터 드라이브를 추가할 수 있습니다. 이 작업은 다중 드라이브 슬라이스 서비스(MDSS) 기능을 활성화하여 수행합니다. 이 기능을 활성화하려면 NetApp 지원 팀에 문의해야 합니다.

슬라이스 드라이브를 사용 가능 상태로 하려면 장애가 발생한 드라이브를 새 드라이브 또는 스페어 드라이브로 교체해야 할 수 있습니다. 슬롯 2용 드라이브를 추가할 때 시스템 슬라이스 드라이브를 추가해야 합니다. 슬롯 2 슬라이스 드라이브만 추가하거나 시스템 슬라이스 드라이브를 추가하기 전에 시스템에서 오류를 생성합니다.

1. Cluster * > * Drives * 를 클릭합니다.
2. 사용 가능한 드라이브 목록을 보려면 * 사용 가능 * 을 클릭합니다.
3. 추가할 슬라이스 드라이브를 선택합니다.
4. 대량 작업 * 을 클릭합니다.
5. 추가 * 를 클릭합니다.
6. 활성 드라이브 * 탭에서 드라이브가 추가되었는지 확인합니다.

MDSS 드라이브를 제거합니다

다중 드라이브 슬라이스 서비스(MDSS) 드라이브를 제거할 수 있습니다. 이 절차는 노드에 여러 개의 슬라이스 드라이브가 있는 경우에만 적용됩니다.

> 시스템 슬라이스 드라이브와 슬롯 2 드라이브에 장애가 발생하면 시스템은 슬라이스 서비스를 종료하고 드라이브를 제거합니다. 장애가 발생하지 않고 드라이브를 분리하는 경우 두 드라이브를 동시에 제거해야 합니다.

1. Cluster * > * Drives * 를 클릭합니다.
2. Available * drives(사용 가능한 * 드라이브) 탭에서 제거할 슬라이스 드라이브의 확인란을 클릭합니다.
3. 대량 작업 * 을 클릭합니다.
4. 제거 * 를 클릭합니다.
5. 작업을 확인합니다.

노드 문제 해결

유지보수 또는 교체를 위해 클러스터에서 노드를 제거할 수 있습니다. 노드를 오프라인으로 전환하기 전에 NetApp Element UI 또는 API를 사용하여 노드를 제거해야 합니다.

스토리지 노드를 제거하는 절차는 다음과 같습니다.

- 클러스터에 노드에서 데이터 복사본을 생성할 수 있는 충분한 용량이 있는지 확인합니다.
- UI 또는 RemoveDrives API 메소드를 사용하여 클러스터에서 드라이브를 제거합니다.

  따라서 시스템이 노드의 드라이브에서 클러스터의 다른 드라이브로 데이터를 마이그레이션합니다. 이 프로세스에 걸리는 시간은 마이그레이션해야 하는 데이터의 양에 따라 달라집니다.

- 클러스터에서 노드를 제거합니다.

노드 전원을 끄기 전에 다음 사항을 고려하십시오.

- 노드 및 클러스터의 전원을 끄는 것은 올바르게 수행되지 않을 경우 위험이 수반됩니다.

  노드의 전원을 끄는 작업은 NetApp Support의 지시에 따라 수행해야 합니다.

- 어떤 유형의 종료 조건에서든 노드가 5.5분 이상 중단된 경우, 이중 Helix 데이터 보호는 복제된 단일 블록을 다른 노드에 작성하여 데이터를 복제하는 작업을 시작합니다. 이 경우 NetApp Support에 문의하여 장애 노드 분석에 대한 도움을 받으십시오.
- 노드를 안전하게 재부팅하거나 전원을 끄기 위해 Shutdown API 명령을 사용할 수 있습니다.
- 노드가 중단 상태이거나 꺼짐 상태인 경우 온라인 상태로 되돌리기 전에 NetApp 지원에 문의해야 합니다.
- 노드가 다시 온라인 상태가 된 후 서비스 제공 기간에 따라 드라이브를 클러스터에 다시 추가해야 합니다.

를 참조하십시오

"장애가 발생한 SolidFire 섀시 교체"

"장애가 발생한 H600S 시리즈 노드 교체"

클러스터 전원을 끕니다

전체 클러스터의 전원을 차단하려면 다음 절차를 수행하십시오.

단계

1. (선택 사항) 사전 단계를 완료하는 데 도움이 필요하면 NetApp 지원에 문의하십시오.
2. 모든 입출력이 중지되었는지 확인합니다.
3. 모든 iSCSI 세션 연결 끊기:
   a. 클러스터의 관리 가상 IP(MVIP) 주소로 이동하여 Element UI를 엽니다.
   b. 노드 목록에 나열된 노드를 확인합니다.
   c. 클러스터의 각 노드 ID에 지정된 중지 옵션으로 Shutdown API 메서드를 실행합니다.

> 클러스터를 재시작할 때 모든 노드가 온라인 상태인지 확인하려면 특정 단계를 수행해야 합니다.
>
> 1. 모든 Critical severity 및 를 확인합니다 `volumesOffline` 클러스터 장애가 해결되었습니다.
> 2. 클러스터가 안정될 때까지 10~15분 정도 기다립니다.
> 3. 데이터 액세스를 위해 호스트를 시작합니다.
>
> 노드 전원을 켜고 상태가 양호한지 확인하는 데 더 많은 시간을 할애하려면 기술 지원 부서에 문의하여 불필요한 입력 용지함 동기화를 방지하기 위해 데이터 동기화를 지연하는 방법에 대해 문의하십시오.

자세한 내용을 확인하십시오

"NetApp Solidfire/HCI 스토리지 클러스터를 올바르게 종료하고 전원을 켜는 방법"

스토리지 노드용 노드별 유틸리티 작업

NetApp Element 소프트웨어 UI의 표준 모니터링 도구가 문제 해결을 위한 충분한 정보를 제공하지 않는 경우 노드별 유틸리티를 사용하여 네트워크 문제를 해결할 수 있습니다. 노드별 유틸리티는 노드 간 또는 관리 노드와의 네트워크 문제를 해결하는 데 도움이 되는 특정 정보와 도구를 제공합니다.

자세한 내용을 확인하십시오

- 노드별 UI를 사용하여 노드별 설정에 액세스합니다
- 노드별 UI에서 네트워크 설정 세부 정보
- 노드별 UI에서 클러스터 설정 세부 정보
- 노드별 UI를 사용하여 시스템 테스트를 실행합니다
- 노드별 UI를 사용하여 시스템 유틸리티를 실행합니다

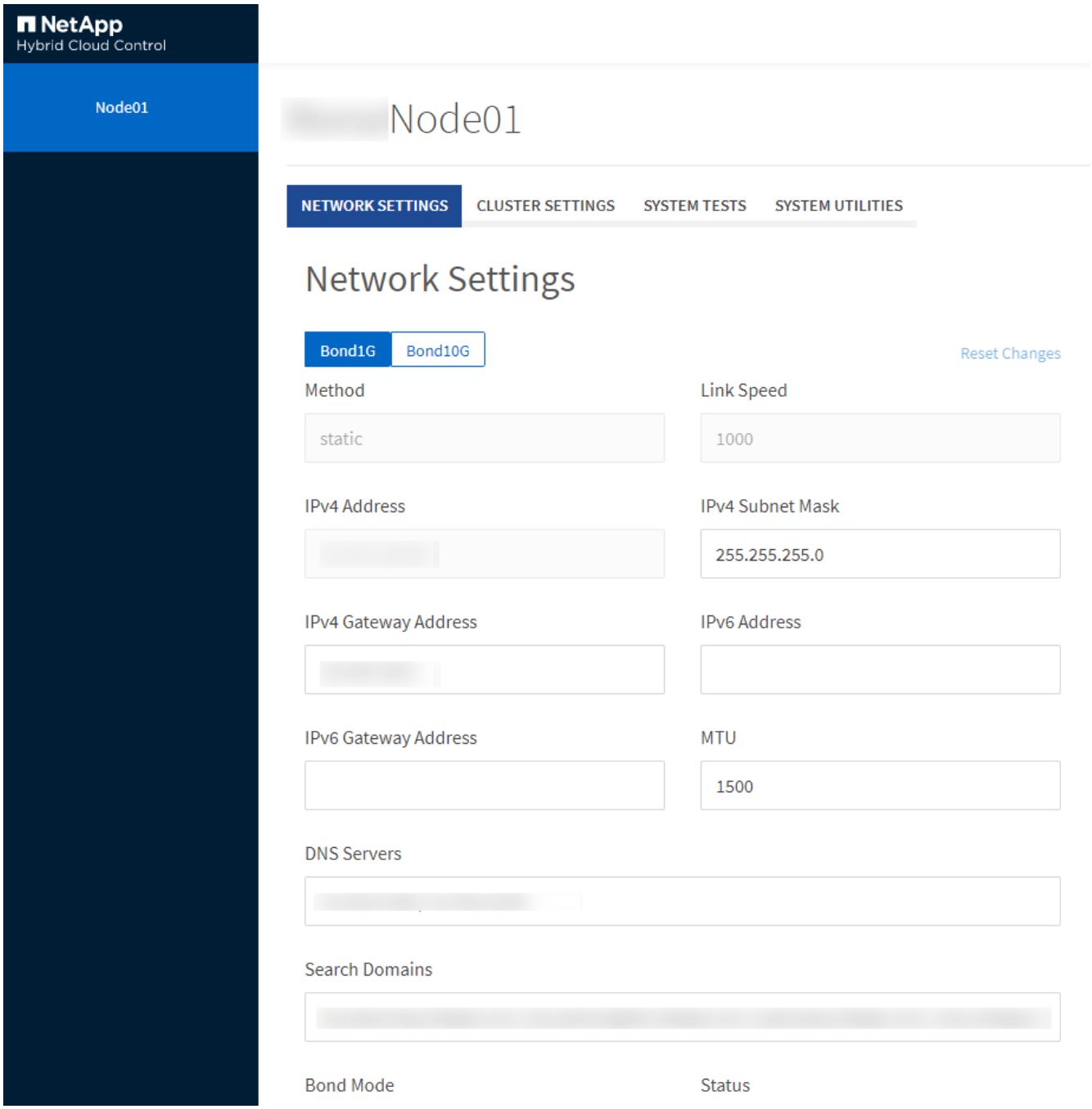
노드별 **UI**를 사용하여 노드별 설정에 액세스합니다

관리 노드 IP를 입력하고 인증한 후 노드별 사용자 인터페이스에서 네트워크 설정, 클러스터 설정, 시스템 테스트 및 유틸리티에 액세스할 수 있습니다.

클러스터의 일부인 활성 상태의 노드 설정을 수정하려면 클러스터 관리자 사용자로 로그인해야 합니다.

> 한 번에 하나의 노드를 구성하거나 수정해야 합니다. 지정된 네트워크 설정이 예상 효과를 가지는지, 다른 노드를 수정하기 전에 네트워크가 안정적이고 잘 작동하는지 확인해야 합니다.

1. 다음 방법 중 하나를 사용하여 노드별 UI를 엽니다.
   - 브라우저 창에 관리 IP 주소와 442를 차례로 입력하고 admin 사용자 이름 및 암호를 사용하여 로그인합니다.
   - Element UI에서 * Cluster * > * Nodes * 를 선택하고 구성하거나 수정할 노드의 관리 IP 주소 링크를 클릭합니다. 브라우저 창이 열리면 노드의 설정을 편집할 수 있습니다.



노드별 **UI**에서 네트워크 설정 세부 정보

스토리지 노드 네트워크 설정을 변경하여 노드에 새 네트워크 속성 세트를 제공할 수 있습니다.

노드에 로그인하면 * 네트워크 설정 * 페이지에서 스토리지 노드에 대한 네트워크 설정을 확인할 수 있습니다 (https://<node IP>:442/HCC/노드/네트워크 설정). Bond1G * (관리) 또는 * Bond10G * (스토리지) 설정을 선택할 수 있습니다. 다음 목록에서는 스토리지 노드가 사용 가능, 보류 중 또는 활성 상태일 때 수정할 수 있는 설정을 설명합니다.

- * 방법 *

  인터페이스를 구성하는 데 사용되는 방법입니다. 가능한 방법:

  - Loopback: IPv4 루프백 인터페이스를 정의하는 데 사용됩니다.

  - Manual(수동): 기본적으로 구성이 수행되지 않는 인터페이스를 정의하는 데 사용됩니다.
  - DHCP: DHCP를 통해 IP 주소를 가져오는 데 사용됩니다.
  - 정적: 정적으로 할당된 IPv4 주소를 사용하여 이더넷 인터페이스를 정의하는 데 사용됩니다.
- * 링크 속도 *

  가상 NIC가 협상하는 속도입니다.

- * IPv4 주소 *

  eth0 네트워크의 IPv4 주소입니다.

- * IPv4 서브넷 마스크 *

  IPv4 네트워크의 주소 부분.

- * IPv4 게이트웨이 주소 *

  로컬 네트워크 외부로 패킷을 전송하기 위한 라우터 네트워크 주소입니다.

- * IPv6 주소 *

  eth0 네트워크의 IPv6 주소입니다.

- * IPv6 게이트웨이 주소 *

  로컬 네트워크 외부로 패킷을 전송하기 위한 라우터 네트워크 주소입니다.

- * MTU *

  네트워크 프로토콜이 전송할 수 있는 최대 패킷 크기입니다. 1500보다 크거나 같아야 합니다. 두 번째 스토리지 NIC를 추가하는 경우 값은 9000이어야 합니다.

- DNS 서버 *

  클러스터 통신에 사용되는 네트워크 인터페이스입니다.

- * 검색 도메인 *

  시스템에서 사용할 수 있는 추가 MAC 주소를 검색합니다.

- * 본드 모드 *

  다음 모드 중 하나일 수 있습니다.

  - ActivePassive(기본값)
  - ALB를 클릭합니다
  - LACP
- * 상태 *

  가능한 값:

    - 업그레이드 실행
    - 아래로
    - 위로
- * 가상 네트워크 태그 *

  가상 네트워크를 생성할 때 할당된 태그입니다.

- * 루트 *

  연결된 인터페이스를 통해 특정 호스트 또는 네트워크에 대한 정적 라우트는 사용하도록 구성됩니다.

노드별 **UI**에서 클러스터 설정 세부 정보

클러스터 구성 후 스토리지 노드에 대한 클러스터 설정을 확인하고 노드 호스트 이름을 수정할 수 있습니다.

다음 목록에서는 노드별 UI의 * 클러스터 설정 * 페이지에 표시된 스토리지 노드에 대한 클러스터 설정을 설명합니다 (https://<node IP>:442/HCC/노드/클러스터 설정).

- * 역할 *

  클러스터에서 노드의 역할 가능한 값:

    - 스토리지: 스토리지 또는 Fibre Channel 노드
    - 관리: 노드는 관리 노드입니다.
- * 호스트 이름 *

  노드의 이름입니다.

- * 클러스터 *

  클러스터의 이름입니다.

- * 클러스터 구성원 *

  노드의 상태입니다. 가능한 값:

    - 사용 가능: 노드에 연결된 클러스터 이름이 없으며 아직 클러스터의 일부가 아닙니다.
    - 보류 중: 노드가 구성되었으며 지정된 클러스터에 추가할 수 있습니다. 노드를 액세스하는 데 인증이 필요하지 않습니다.
    - PendingActive: 시스템이 노드에 호환되는 소프트웨어를 설치하는 중입니다. 완료되면 노드가 활성 상태로 이동합니다.
    - Active(활성): 노드가 클러스터에 참여하고 있습니다. 노드를 수정하려면 인증이 필요합니다.
- * 버전 *

  노드에서 실행되는 Element 소프트웨어의 버전입니다.

- * 통합 *

  데이터베이스 앙상블의 일부인 노드입니다.

- * 노드 ID *

  노드가 클러스터에 추가될 때 할당되는 ID입니다.

- * 클러스터 인터페이스 *

  클러스터 통신에 사용되는 네트워크 인터페이스입니다.

- * 관리 인터페이스 *

  관리 네트워크 인터페이스. 이 기본값은 Bond1G이지만 Bond10G도 사용할 수 있습니다.

- * 스토리지 인터페이스 *

  Bond10G를 사용하는 스토리지 네트워크 인터페이스.

- * 암호화 가능 *

  노드가 드라이브 암호화를 지원하는지 여부를 나타냅니다.

노드별 **UI**를 사용하여 시스템 테스트를 실행합니다

네트워크 구성에 변경한 후 네트워크 설정에 대한 변경 사항을 테스트할 수 있습니다. 테스트를 실행하여 스토리지 노드가 안정적이며 문제 없이 온라인 상태가 될 수 있는지 확인할 수 있습니다.

스토리지 노드의 노드별 UI에 로그인했습니다.

1. 시스템 테스트 * 를 클릭합니다.
2. 실행하려는 테스트 옆에 있는 * 테스트 실행 * 을 클릭하거나 * 모든 테스트 실행 * 을 선택합니다.

   > 모든 테스트 작업을 실행하려면 시간이 오래 걸릴 수 있으며 NetApp Support 부서의 지시에 따라서만 수행해야 합니다.

   - * 연결된 통합 테스트 *

     데이터베이스 앙상블에 대한 연결을 테스트하고 확인합니다. 기본적으로 이 테스트에서는 노드가 연결된 클러스터에 대해 앙상블을 사용합니다. 또는 다른 앙상블을 제공하여 연결을 테스트할 수도 있습니다.

   - * Mvip 연결 테스트 *

     지정된 관리 가상 IP(MVIP) 주소를 ping하여 MVIP에 대한 간단한 API 호출을 실행하여 연결을 확인합니다. 기본적으로 이 테스트에서는 노드가 연결된 클러스터에 MVIP를 사용합니다.

   - * 테스트 연결 Svip *

     네트워크 어댑터에 설정된 MTU(Maximum Transmission Unit) 크기와 일치하는 ICMP(Internet Control

Message Protocol) 패킷을 사용하여 지정된 SVIP(Storage Virtual IP) 주소를 ping합니다. 그런 다음 SVIP에 iSCSI 이니시에이터로 연결합니다. 기본적으로 이 테스트에서는 노드가 연결된 클러스터에 대해 SVIP를 사용합니다.

- * 하드웨어 구성 테스트 *

  모든 하드웨어 구성이 올바른지 테스트하고, 펌웨어 버전이 올바른지 확인하고, 모든 드라이브가 설치되어 올바르게 실행 중인지 확인합니다. 이는 공장 테스트와 동일합니다.

  > 이 테스트는 리소스 집약적이며 NetApp Support에서 요청한 경우에만 실행해야 합니다.

- * 로컬 연결 테스트 *

  각 노드의 CIP(클러스터 IP)에 대해 Ping을 수행하여 클러스터의 다른 모든 노드에 대한 연결을 테스트합니다. 이 테스트는 노드가 액티브 클러스터의 일부인 경우에만 노드에 표시됩니다.

- * 테스트 찾기 클러스터 *

  노드에서 클러스터 구성에 지정된 클러스터를 찾을 수 있는지 확인합니다.

- * 네트워크 구성 테스트 *

  구성된 네트워크 설정이 시스템에서 사용 중인 네트워크 설정과 일치하는지 확인합니다. 이 테스트는 노드가 클러스터에 적극적으로 참여하는 경우 하드웨어 장애를 감지하기 위한 것이 아닙니다.

- * Ping 테스트 *

  지정된 호스트 목록을 ping합니다. 지정된 호스트가 없으면 클러스터에 등록된 모든 노드 목록을 동적으로 구축하고 각 노드를 ping하여 간단한 접속으로 구성합니다.

- * 원격 연결 테스트 *

  각 노드의 CIP(클러스터 IP)를 Ping하여 원격으로 연결된 클러스터의 모든 노드에 대한 연결을 테스트합니다. 이 테스트는 노드가 액티브 클러스터의 일부인 경우에만 노드에 표시됩니다.

노드별 **UI**를 사용하여 시스템 유틸리티를 실행합니다

스토리지 노드의 노드별 UI를 사용하여 지원 번들을 생성 또는 삭제하고, 드라이브의 구성 설정을 재설정하고, 네트워크 또는 클러스터 서비스를 다시 시작할 수 있습니다.

스토리지 노드의 노드별 UI에 로그인했습니다.

1. 시스템 유틸리티 * 를 클릭합니다.
2. 실행할 시스템 유틸리티의 단추를 클릭합니다.
   - * 제어 전원 *

     노드를 재부팅, 전원 사이클 또는 종료합니다.

     > 이 작업으로 인해 네트워크 연결이 일시적으로 끊기게 됩니다.

다음 매개 변수를 지정합니다.

- 조치: 옵션에는 재시작 및 중지(전원 끄기)가 포함됩니다.
- Wakeup Delay(웨이크업 지연): 노드가 다시 온라인 상태로 전환되기 전에 추가 시간

◦ * 노드 로그 수집 *

노드의 /tmp/bunds 디렉토리 아래에 지원 번들을 생성합니다.

다음 매개 변수를 지정합니다.

- 번들 이름: 생성된 각 지원 번들의 고유 이름입니다. 이름이 제공되지 않으면 "supportbundle"과 노드 이름이 파일 이름으로 사용됩니다.
- Extra Args: 이 매개 변수는 sf_make_support_bundle 스크립트에 공급됩니다. 이 매개 변수는 NetApp Support의 요청에만 사용해야 합니다.
- timeout sec(시간 초과 초): 각 개별 ping 응답을 대기하는 시간(초)을 지정합니다.

◦ * 노드 로그 삭제 *

Create Cluster Support Bundle* 또는 CreateSupportBundle API 메소드를 사용하여 생성된 노드에서 현재 지원 번들을 삭제합니다.

◦ * 드라이브 재설정 *

드라이브를 초기화하고 현재 드라이브에 있는 모든 데이터를 제거합니다. 기존 노드 또는 업그레이드된 노드에서 드라이브를 재사용할 수 있습니다.

다음 매개 변수를 지정합니다.

- 드라이브: 재설정할 장치 이름 목록(드라이브 ID 아님).

◦ * 네트워크 구성 재설정 *

개별 노드의 네트워크 구성 문제를 해결하고 개별 노드의 네트워크 구성을 공장 출하시 기본 설정으로 재설정합니다.

◦ * 노드 재설정 *

노드를 공장 초기 설정으로 재설정합니다. 모든 데이터가 제거되지만 이 작업 중에 노드의 네트워크 설정이 유지됩니다. 노드가 클러스터에 할당되지 않고 사용 가능한 상태인 경우에만 재설정할 수 있습니다.

> 이 옵션을 사용하면 모든 데이터, 패키지(소프트웨어 업그레이드), 구성 및 로그 파일이 노드에서 삭제됩니다.

◦ * 네트워킹 재시작 *

노드에서 모든 네트워킹 서비스를 다시 시작합니다.

> 이 작업으로 인해 네트워크 연결이 일시적으로 끊어질 수 있습니다.

◦ * 서비스를 다시 시작합니다 *

노드에서 Element 소프트웨어 서비스를 다시 시작합니다.

> 이 작업은 일시적인 노드 서비스를 중단시킬 수 있습니다. 이 작업은 NetApp Support의 지시에 따라서만 수행해야 합니다.

다음 매개 변수를 지정합니다.

- 서비스: 다시 시작할 서비스 이름입니다.
- 조치: 서비스에 대해 수행할 조치. 시작, 중지 및 재시작 옵션이 있습니다.

관리 노드와 작업합니다

관리 노드(mNode)를 사용하여 시스템 서비스를 업그레이드하고, 클러스터 자산 및 설정을 관리하고, 시스템 테스트 및 유틸리티를 실행하고, 시스템 모니터링을 위한 Active IQ를 구성하고, 문제 해결을 위해 NetApp 지원 액세스를 지원할 수 있습니다.

> 모범 사례로서, 하나의 관리 노드만 하나의 VMware vCenter 인스턴스와 연결하고 여러 관리 노드에서 동일한 스토리지 및 컴퓨팅 리소스 또는 vCenter 인스턴스를 정의하지 않는 것이 좋습니다.

을 참조하십시오 "관리 노드 설명서" 를 참조하십시오.

클러스터 전체 수준 이해

Element 소프트웨어를 실행하는 클러스터는 클러스터 장애를 생성하여 클러스터 용량이 부족해지면 스토리지 관리자에게 경고합니다. 세 가지 수준의 클러스터 충만도가 있으며 모두 NetApp Element UI에 표시됩니다(경고, 오류 및 위험).

시스템은 BlockClusterFull 오류 코드를 사용하여 클러스터 블록 스토리지 충만성에 대해 경고합니다. Element UI의 Alerts 탭에서 클러스터의 전체 심각도 수준을 볼 수 있습니다.

다음 목록에는 BlockClusterFull 심각도 수준에 대한 정보가 포함되어 있습니다.

- * 경고 *

  클러스터의 블록 용량이 오류 심각도 수준에 접근하고 있을 때 표시되는 고객 구성 가능 경고입니다. 기본적으로 이 수준은 오류 수준에서 3%로 설정되며 Element UI 및 API를 통해 조정할 수 있습니다. 용량을 추가하거나 가능한 한 빨리 용량을 확보하십시오.

- * 오류 *

  클러스터가 이 상태일 때 노드가 손실된 경우 이중 Helix 데이터 보호를 재구축하기에 충분한 용량이 클러스터에 없습니다. 클러스터가 이 상태인 동안에는 새 볼륨 생성, 클론 및 스냅샷이 모두 차단됩니다. 이 상태는 클러스터에 대한 안전 또는 권장 상태가 아닙니다. 용량을 추가하거나 즉시 용량을 확장해야 합니다.

- * 심각 *

  이 심각한 오류는 클러스터가 100% 사용되었기 때문에 발생했습니다. 읽기 전용 상태이며 클러스터에 새 iSCSI 연결을 설정할 수 없습니다. 이 단계에 도달하면 즉시 용량을 확보하거나 추가해야 합니다.

시스템은 MetadataClusterFull 오류 코드를 사용하여 클러스터 메타데이터 스토리지 충만성에 대해 경고합니다. Element UI의 Reporting(보고) 탭의 Overview(개요) 페이지에 있는 Cluster Capacity(클러스터 용량) 섹션에서 클러스터 메타데이터 스토리지 충만 을 볼 수 있습니다.

다음 목록에는 MetadataClusterFull 심각도 수준에 대한 정보가 포함되어 있습니다.

- * 경고 *

  이 경고는 클러스터의 메타데이터 용량이 오류 심각도 수준에 접근하고 있을 때 고객이 구성할 수 있는 경고입니다. 기본적으로 이 수준은 오류 수준에서 3%로 설정되며 Element API를 통해 조정할 수 있습니다. 용량을 추가하거나 가능한 한 빨리 용량을 확보하십시오.

- * 오류 *

  클러스터가 이 상태일 때 노드가 손실된 경우 이중 Helix 데이터 보호를 재구축하기에 충분한 용량이 클러스터에 없습니다. 클러스터가 이 상태인 동안에는 새 볼륨 생성, 클론 및 스냅샷이 모두 차단됩니다. 이 상태는 클러스터에 대한 안전 또는 권장 상태가 아닙니다. 용량을 추가하거나 즉시 용량을 확장해야 합니다.

- * 심각 *

  이 심각한 오류는 클러스터가 100% 사용되었기 때문에 발생했습니다. 읽기 전용 상태이며 클러스터에 새 iSCSI 연결을 설정할 수 없습니다. 이 단계에 도달하면 즉시 용량을 확보하거나 추가해야 합니다.

다음은 2노드 클러스터 임계값에 적용되는 사항입니다.

- 메타데이터 충만 오류는 위험 보다 20% 낮습니다.
- 블록 충만 오류는 1개 블록 드라이브(고립된 용량 포함)가 중요 오류 보다 낮다는 의미입니다. 즉, 2개 블록 드라이브에서 용량이 중요 용량보다 더 적다는 의미입니다.