시스템 관리

Element Software

NetApp
November 12, 2025

목차

시스템 관리 . . . 1
- 시스템 관리 . . . 1
  - 더 많은 정보를 원하시면 . . . 1
- 다중 요소 인증 활성화 . . . 1
  - 다중 요소 인증 설정 . . . 1
  - 다중 요소 인증에 대한 추가 정보 . . . 2
- 클러스터 설정 구성 . . . 2
  - 클러스터에 대한 휴면 암호화 활성화 및 비활성화 . . . 2
  - 클러스터 전체 임계값 설정 . . . 4
  - 볼륨 로드 밸런싱 활성화 및 비활성화 . . . 4
  - 지원 액세스 활성화 및 비활성화 . . . 5
  - 이용약관 배너 관리 . . . 5
  - 네트워크 시간 프로토콜 설정 . . . 6
  - SNMP 관리 . . . 7
  - 드라이브 관리 . . . 10
  - 노드 관리 . . . 11
  - 파이버 채널 포트 세부 정보 보기 . . . 14
  - 가상 네트워크 관리 . . . 15
- FIPS 드라이브를 지원하는 클러스터 만들기 . . . 18
  - FIPS 드라이브 기능을 위한 Element 클러스터 준비 . . . 18
  - 휴면 상태에서 암호화 활성화 . . . 19
  - 노드가 FIPS 드라이브 기능을 사용할 준비가 되었는지 확인합니다. . . . 19
  - FIPS 드라이브 기능 활성화 . . . 20
  - FIPS 드라이브 상태 확인 . . . 20
  - FIPS 드라이브 기능 문제 해결 . . . 21
- 안전한 통신을 구축하세요 . . . 21
  - 클러스터에서 HTTPS에 대해 FIPS 140-2를 활성화합니다. . . . 21
  - SSL 암호 . . . 22
- 외부 키 관리 시작하기 . . . 24
  - 외부 키 관리 시작하기 . . . 24
  - 외부 키 관리 설정 . . . 24
  - 휴면 마스터 키에서 소프트웨어 암호화 재키 . . . 25
  - 접근 불가능하거나 잘못된 인증 키 복구 . . . 28
  - 외부 키 관리 API 명령 . . . 28

시스템 관리

시스템 관리

Element UI에서 시스템을 관리할 수 있습니다. 여기에는 다중 요소 인증 활성화, 클러스터 설정 관리, FIPS(연방 정보 처리 표준) 지원, 외부 키 관리 사용이 포함됩니다.

- "다중 요소 인증 활성화"
- "클러스터 설정 구성"
- "FIPS 드라이브를 지원하는 클러스터 만들기"
- "외부 키 관리 시작하기"

더 많은 정보를 원하시면

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

다중 요소 인증 활성화

다중 요소 인증 설정

다중 인증 요소(MFA)는 SAML(Security Assertion Markup Language)을 통해 타사 ID 공급자(IdP)를 사용하여 사용자 세션을 관리합니다. MFA를 사용하면 관리자가 비밀번호와 문자 메시지, 비밀번호와 이메일 메시지 등 필요에 따라 추가적인 인증 요소를 구성할 수 있습니다.

Element API를 통해 이러한 기본 단계를 사용하여 클러스터를 설정하여 다중 요소 인증을 사용할 수 있습니다.

각 API 메서드의 세부 사항은 다음에서 확인할 수 있습니다. "요소 API 참조".

1. 다음 API 메서드를 호출하고 JSON 형식으로 IdP 메타데이터를 전달하여 클러스터에 대한 새로운 타사 ID 공급자(IdP) 구성을 만듭니다. `CreateIdpConfiguration`

   일반 텍스트 형식의 IdP 메타데이터는 타사 IdP에서 검색됩니다. 이 메타데이터는 JSON으로 올바르게 형식화되었는지 확인하기 위해 검증이 필요합니다. 사용할 수 있는 JSON 포매터 애플리케이션은 여러 가지가 있습니다. 예를 들어 https://freeformatter.com/json-escape.html.

2. 다음 API 메서드를 호출하여 spMetadataUrl을 통해 클러스터 메타데이터를 검색하여 타사 IdP에 복사합니다. `ListIdpConfigurations`

   spMetadataUrl은 IdP의 클러스터에서 서비스 공급자 메타데이터를 검색하여 신뢰 관계를 구축하는 데 사용되는 URL입니다.

3. 감사 로깅과 단일 로그아웃이 제대로 작동하도록 사용자를 고유하게 식별하기 위해 타사 IdP에서 SAML 어설션을 "NameID" 속성이 포함되도록 구성합니다.
4. 다음 API 메서드를 호출하여 타사 IdP에서 인증한 하나 이상의 클러스터 관리자 사용자 계정을 생성하여 권한을

부여합니다.`AddIdpClusterAdmin`

> 다음 예에서 볼 수 있듯이, IdP 클러스터 관리자의 사용자 이름은 원하는 효과에 대한 SAML 속성 이름/값 매핑과 일치해야 합니다.

- email=bob@company.com — IdP가 SAML 속성에서 이메일 주소를 해제하도록 구성된 경우.
- group=cluster-administrator - IdP가 모든 사용자가 액세스할 수 있는 그룹 속성을 해제하도록 구성된 경우입니다. 보안상의 이유로 SAML 속성 이름/값 쌍은 대소문자를 구분합니다.

5. 다음 API 메서드를 호출하여 클러스터에 대해 MFA를 활성화합니다. `EnableIdpAuthentication`

더 많은 정보를 찾아보세요

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

다중 요소 인증에 대한 추가 정보

다중 인증과 관련하여 다음 주의 사항을 알고 있어야 합니다.

- 더 이상 유효하지 않은 IdP 인증서를 새로 고치려면 IdP 관리자가 아닌 사용자를 사용하여 다음 API 메서드를 호출해야 합니다. `UpdateIdpConfiguration`
- MFA는 길이가 2048비트 미만인 인증서와 호환되지 않습니다. 기본적으로 2048비트 SSL 인증서가 클러스터에 생성됩니다. API 메서드를 호출할 때 더 작은 크기의 인증서를 설정하지 마세요. `SetSSLCertificate`

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

- IdP 관리자 사용자는 API 호출을 직접 수행하는 데 사용할 수 없습니다(예: SDK 또는 Postman을 통해) 또는 다른 통합(예: OpenStack Cinder 또는 vCenter 플러그인)에 사용할 수 없습니다. 이러한 권한이 있는 사용자를 생성해야 하는 경우 LDAP 클러스터 관리자 사용자나 로컬 클러스터 관리자 사용자를 추가합니다.

더 많은 정보를 찾아보세요

- "Element API를 사용한 저장소 관리"
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

클러스터 설정 구성

클러스터에 대한 휴면 암호화 활성화 및 비활성화

SolidFire 클러스터를 사용하면 클러스터 드라이브에 저장된 모든 저장 데이터를 암호화할 수 있습니다. 다음 중 하나를 사용하여 클러스터 전체에서 자체 암호화 드라이브(SED) 보호를 활성화할 수 있습니다."하드웨어 또는 소프트웨어 기반 암호화" .

Element UI나 API를 사용하여 하드웨어 암호화를 활성화할 수 있습니다. 휴면 상태의 하드웨어 암호화 기능을 활성화해도 클러스터의 성능이나 효율성에는 영향을 미치지 않습니다. Element API를 사용해서만 소프트웨어 암호화를 활성화할 수 있습니다.

클러스터 생성 중에는 하드웨어 기반 암호화가 기본적으로 활성화되지 않으며 Element UI에서 활성화 및 비활성화할 수 있습니다.

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

필요한 것

- 암호화 설정을 활성화하거나 변경하려면 클러스터 관리자 권한이 있어야 합니다.
- 하드웨어 기반 암호화의 경우 암호화 설정을 변경하기 전에 클러스터가 정상 상태인지 확인해야 합니다.
- 암호화를 비활성화하는 경우 드라이브의 암호화를 비활성화하는 키에 액세스하려면 두 개의 노드가 클러스터에 참여해야 합니다.

휴면 상태에서 암호화 확인

클러스터에서 암호화의 현재 상태 및/또는 소프트웨어 암호화의 현재 상태를 보려면 다음을 사용하십시오."클러스터 정보 가져오기" 방법. 당신은 사용할 수 있습니다"GetSoftwareEncryptionAtRestInfo" 클러스터가 저장 중인 데이터를 암호화하는 데 사용하는 정보를 가져오는 방법입니다.

Element 소프트웨어 UI 대시보드 `https://<MVIP>/` 현재는 하드웨어 기반 암호화의 경우 암호화가 정지된 상태만 표시합니다.

옵션

- 하드웨어 기반 암호화를 휴면 상태로 활성화
- 휴면 상태에서 소프트웨어 기반 암호화 활성화
- 휴면 상태에서 하드웨어 기반 암호화 비활성화

하드웨어 기반 암호화를 휴면 상태로 활성화

외부 키 관리 구성을 사용하여 휴면 암호화를 활성화하려면 다음을 통해 휴면 암호화를 활성화해야 합니다."API" . 기존 Element UI 버튼을 사용하도록 설정하면 내부적으로 생성된 키를 사용하게 됩니다.

1. Element UI에서 클러스터 > *설정*을 선택합니다.
2. *저장 시 암호화 사용*을 선택합니다.

휴면 상태에서 소프트웨어 기반 암호화 활성화

클러스터에서 소프트웨어 암호화를 활성화한 후에는 비활성화할 수 없습니다.

1. 클러스터 생성 중에 다음을 실행합니다."클러스터 생성 방법" ~와 함께 `enableSoftwareEncryptionAtRest` 로 설정 `true` .

휴면 상태에서 하드웨어 기반 암호화 비활성화

1. Element UI에서 클러스터 > *설정*을 선택합니다.
2. *저장 시 암호화 비활성화*를 선택합니다.

더 많은 정보를 찾아보세요

- "SolidFire 및 Element 소프트웨어 문서"
- "NetApp SolidFire 및 Element 제품의 이전 버전에 대한 설명서"

클러스터 전체 임계값 설정

아래 단계에 따라 시스템이 블록 클러스터 충만 경고를 생성하는 수준을 변경할 수 있습니다. 또한 ModifyClusterFullThreshold API 메서드를 사용하여 시스템이 차단 또는 메타데이터 경고를 생성하는 수준을 변경할 수 있습니다.

필요한 것

클러스터 관리자 권한이 있어야 합니다.

단계

1. 클러스터 > *설정*을 클릭합니다.
2. 클러스터 전체 설정 섹션에서 *Helix가 노드 장애에서 복구할 수 없게 되기 전에 _% 용량이 남을 때 경고 알림을 발생시킵니다*에 백분율을 입력합니다.
3. *변경 사항 저장*을 클릭하세요.

더 많은 정보를 찾아보세요

"Element에 대한 blockSpace 임계값은 어떻게 계산됩니까?"

볼륨 로드 밸런싱 활성화 및 비활성화

Element 12.8부터 볼륨 부하 분산을 사용하여 QoS 정책에 구성된 최소 IOPS 대신 각 볼륨의 실제 IOPS를 기준으로 노드 간에 볼륨을 분산할 수 있습니다. 기본적으로 비활성화되어 있는 볼륨 부하 분산을 Element UI 또는 API를 사용하여 활성화하거나 비활성화할 수 있습니다.

단계

1. 클러스터 > *설정*을 선택합니다.
2. 클러스터별 섹션에서 볼륨 로드 밸런싱의 상태를 변경합니다.

   볼륨 로드 밸런싱 활성화

   *실제 IOPS에서 부하 분산 활성화*를 선택하고 선택 사항을 확인합니다.

   볼륨 부하 분산 비활성화:

   *실제 IOPS에서 부하 분산 비활성화*를 선택하고 선택 사항을 확인합니다.

3. 선택적으로 보고 > *개요*를 선택하여 실제 IOPS 잔액의 상태 변경을 확인합니다. 상태를 보려면 클러스터 상태 정보를 아래로 스크롤해야 할 수도 있습니다.

더 많은 정보를 찾아보세요

- "API를 사용하여 볼륨 로드 밸런싱 활성화"
- "API를 사용하여 볼륨 로드 밸런싱 비활성화"
- "볼륨 QoS 정책을 생성하고 관리합니다."

지원 액세스 활성화 및 비활성화

지원 액세스를 활성화하면 NetApp 지원 담당자가 문제 해결을 위해 SSH를 통해 스토리지 노드에 일시적으로 액세스할 수 있습니다.

지원 액세스를 변경하려면 클러스터 관리자 권한이 있어야 합니다.

1. 클러스터 > *설정*을 클릭합니다.
2. 지원 액세스 활성화/비활성화 섹션에서 지원팀의 액세스를 허용할 기간(시간)을 입력합니다.
3. *지원 액세스 활성화*를 클릭하세요.
4. 선택 사항: 지원 액세스를 비활성화하려면 *지원 액세스 비활성화*를 클릭합니다.

이용약관 배너 관리

사용자에게 메시지가 포함된 배너를 활성화, 편집 또는 구성할 수 있습니다.

옵션

이용 약관 배너 활성화 이용약관 배너 편집 이용 약관 배너 비활성화

이용 약관 배너 활성화

사용자가 Element UI에 로그인할 때 나타나는 이용 약관 배너를 활성화할 수 있습니다. 사용자가 배너를 클릭하면 클러스터에 대해 구성한 메시지가 포함된 텍스트 대화 상자가 나타납니다. 배너는 언제든지 해제될 수 있습니다.

이용 약관 기능을 사용하려면 클러스터 관리자 권한이 있어야 합니다.

1. 사용자 > *이용약관*을 클릭하세요.
2. 이용 약관 양식에서 이용 약관 대화 상자에 표시될 텍스트를 입력합니다.

   4096자를 초과하지 마세요.

3. *활성화*를 클릭합니다.

이용약관 배너 편집

사용자가 이용 약관 로그인 배너를 선택할 때 표시되는 텍스트를 편집할 수 있습니다.

필요한 것

- 이용 약관을 구성하려면 클러스터 관리자 권한이 있어야 합니다.
- 이용 약관 기능이 활성화되어 있는지 확인하세요.

단계

1. 사용자 > *이용약관*을 클릭하세요.
2. 이용 약관 대화 상자에서 표시할 텍스트를 편집합니다.

   4096자를 초과하지 마세요.

3. *변경 사항 저장*을 클릭하세요.

이용 약관 배너 비활성화

이용 약관 배너를 비활성화할 수 있습니다. 배너를 비활성화하면 사용자는 Element UI를 사용할 때 이용 약관에 동의하라는 요청을 받지 않습니다.

필요한 것

- 이용 약관을 구성하려면 클러스터 관리자 권한이 있어야 합니다.
- 이용약관이 활성화되어 있는지 확인하세요.

단계

1. 사용자 > *이용약관*을 클릭하세요.
2. *비활성화*를 클릭합니다.

네트워크 시간 프로토콜 설정

클러스터가 쿼리할 수 있도록 네트워크 시간 프로토콜 서버를 구성합니다.

클러스터의 각 노드에 NTP(네트워크 시간 프로토콜) 서버에 업데이트를 쿼리하도록 지시할 수 있습니다. 클러스터는 구성된 서버에만 접속하여 해당 서버에서 NTP 정보를 요청합니다.

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

클러스터에서 NTP를 구성하여 로컬 NTP 서버를 가리키도록 합니다. IP 주소나 FQDN 호스트 이름을 사용할 수 있습니다. 클러스터 생성 시 기본 NTP 서버는 us.pool.ntp.org로 설정됩니다. 그러나 SolidFire 클러스터의 물리적 위치에 따라 이 사이트에 대한 연결이 항상 이루어지지 않을 수 있습니다.

FQDN을 사용할지는 개별 스토리지 노드의 DNS 설정이 제대로 작동하고 있는지 여부에 따라 달라집니다. 이를 위해 모든 스토리지 노드에서 DNS 서버를 구성하고 네트워크 포트 요구 사항 페이지를 검토하여 포트가 열려 있는지 확인하세요.

최대 5개의 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. 노드에 DNS가 올바르게 설정되었는지 확인하세요.
3. 클러스터 > *설정*을 클릭합니다.
4. 네트워크 시간 프로토콜 설정에서 *아니요*를 선택하면 표준 NTP 구성이 사용됩니다.
5. *변경 사항 저장*을 클릭하세요.

더 많은 정보를 찾아보세요

- "NTP 브로드캐스트를 수신하도록 클러스터를 구성합니다."
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

NTP 브로드캐스트를 수신하도록 클러스터를 구성합니다**.**

브로드캐스트 모드를 사용하면 클러스터의 각 노드가 특정 서버로부터 네트워크 시간 프로토콜(NTP) 브로드캐스트 메시지를 네트워크에서 수신하도록 지시할 수 있습니다.

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

필요한 것

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

단계

1. 클러스터 > *설정*을 클릭합니다.
2. 브로드캐스트 모드를 사용하는 NTP 서버를 서버 목록에 입력합니다.
3. 네트워크 시간 프로토콜 설정에서 브로드캐스트 클라이언트를 사용하려면 *예*를 선택합니다.
4. 브로드캐스트 클라이언트를 설정하려면 서버 필드에 브로드캐스트 모드에서 구성한 NTP 서버를 입력합니다.
5. *변경 사항 저장*을 클릭하세요.

더 많은 정보를 찾아보세요

- "클러스터가 쿼리할 수 있도록 네트워크 시간 프로토콜 서버를 구성합니다."
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

SNMP 관리

SNMP에 대해 알아보세요

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

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

IPv4와 IPv6 주소를 모두 사용할 수 있습니다.

SNMP 세부 정보

클러스터 탭의 SNMP 페이지에서 다음 정보를 볼 수 있습니다.

- **SNMP MIB**

  여러분이 보거나 다운로드할 수 있는 MIB 파일입니다.

- 일반 **SNMP** 설정

  SNMP를 활성화하거나 비활성화할 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

  어떤 함정을 잡고 싶은지 식별할 수 있습니다. 각 트랩 수신자에 대해 호스트, 포트 및 커뮤니티 문자열을 설정할 수 있습니다.

SNMP 요청자 구성

SNMP 버전 2를 활성화하면 요청자를 활성화하거나 비활성화할 수 있으며, 요청자가 승인된 SNMP 요청을 받도록 구성할 수 있습니다.

1. 메뉴:클러스터[SNMP]를 클릭합니다.
2. *일반 SNMP 설정*에서 *예*를 클릭하여 SNMP를 활성화합니다.
3. 버전 목록에서 *버전 2*를 선택합니다.
4. 요청자 섹션에 커뮤니티 문자열*과 *네트워크 정보를 입력합니다.

   기본적으로 커뮤니티 문자열은 공개이고 네트워크는 로컬호스트입니다. 이러한 기본 설정을 변경할 수 있습니다.

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

더 많은 정보를 찾아보세요

- SNMP 트랩 구성
- 관리 정보 기반 파일을 사용하여 관리되는 개체 데이터 보기

SNMP USM 사용자 구성

SNMP 버전 3을 활성화하는 경우 USM 사용자가 승인된 SNMP 요청을 받도록 구성해야 합니다.

1. 클러스터 > *SNMP*를 클릭합니다.
2. *일반 SNMP 설정*에서 *예*를 클릭하여 SNMP를 활성화합니다.
3. 버전 목록에서 *버전 3*을 선택합니다.
4. **USM** 사용자 섹션에 이름, 비밀번호, 암호구를 입력합니다.
5. 선택 사항**:** 다른 USM 사용자를 추가하려면 *USM 사용자 추가*를 클릭하고 이름, 비밀번호, 암호구를 입력합니다.
6. *변경 사항 저장*을 클릭하세요.

SNMP 트랩 구성

시스템 관리자는 SNMP 트랩(알림이라고도 함)을 사용하여 SolidFire 클러스터의 상태를 모니터링할 수 있습니다.

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

1. 클러스터 > *SNMP*를 클릭합니다.
2. **SNMP** 트랩 설정 섹션에서 시스템이 생성해야 하는 하나 이상의 트랩 유형을 선택합니다.
   - 클러스터 결함 트랩
   - 클러스터 해결 오류 트랩
   - 클러스터 이벤트 트랩
3. 트랩 수신자 섹션에서 수신자의 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 사항 저장*을 클릭하세요.

관리 정보 기반 파일을 사용하여 관리되는 개체 데이터 보기

각 관리 객체를 정의하는 데 사용되는 관리 정보 기반(MIB) 파일을 보고 다운로드할 수 있습니다. SNMP 기능은 SolidFire-StorageCluster-MIB에 정의된 개체에 대한 읽기 전용 액세스를 지원합니다.

MIB에 제공된 통계 데이터는 다음에 대한 시스템 활동을 보여줍니다.

- 클러스터 통계
- 볼륨 통계
- 계정별 볼륨 통계
- 노드 통계

- 보고서, 오류, 시스템 이벤트 등의 기타 데이터

이 시스템은 SF 시리즈 제품에 대한 상위 레벨 액세스 포인트(OIDS)를 포함하는 MIB 파일에 대한 액세스도 지원합니다.

단계

1. 클러스터 > *SNMP*를 클릭합니다.
2. *SNMP MIB*에서 다운로드하려는 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 포함되어 있습니다. 클러스터는 드라이브가 클러스터에 성공적으로 추가된 후 드라이브의 용량과 성능을 활용합니다. Element UI를 사용하여 드라이브를 관리할 수 있습니다.

드라이브 세부 정보

클러스터 탭의 드라이브 페이지는 클러스터의 활성 드라이브 목록을 제공합니다. 활성, 사용 가능, 제거 중, 삭제 중, 실패 탭을 선택하여 페이지를 필터링할 수 있습니다.

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

활성 드라이브 목록에는 다음 요소가 나타납니다.

- 드라이브 **ID**

  드라이브에 할당된 순차 번호입니다.

- 노드 **ID**

  클러스터에 노드가 추가될 때 할당되는 노드 번호입니다.

- 노드 이름

  드라이브를 수용하는 노드의 이름입니다.

- 슬롯

  드라이브가 물리적으로 위치한 슬롯 번호입니다.

- 용량

  드라이브의 크기(GB)입니다.

- 연속물

  드라이브의 일련번호.

- 남은 마모량

  마모 수준 표시기.

  저장 시스템은 각 솔리드 스테이트 드라이브(SSD)에서 데이터 쓰기 및 지우기에 사용할 수 있는 대략적인 마모량을 보고합니다. 설계된 쓰기 및 지우기 주기의 5%를 소모한 드라이브는 95%의 마모가 남아 있다고 보고합니다. 시스템은 드라이브 마모 정보를 자동으로 새로 고치지 않습니다. 새로 고치거나 페이지를 닫았다가 다시 로드하여 정보를 새로 고칠 수 있습니다.

- 유형

  드라이브의 유형. 유형은 블록이나 메타데이터가 될 수 있습니다.

더 많은 정보를 원하시면

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

노드 관리

노드 관리

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

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

더 많은 정보를 찾아보세요

클러스터에 노드 추가

클러스터에 노드 추가

더 많은 저장 공간이 필요하거나 클러스터를 생성한 후에 클러스터에 노드를 추가할 수 있습니다. 노드는 처음 전원을 켤 때 초기 구성이 필요합니다. 노드가 구성된 후에는 보류 중인 노드 목록에 나타나고 클러스터에 추가할 수 있습니다.

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

기존 클러스터에 더 작거나 더 큰 용량의 노드를 추가할 수 있습니다. 클러스터에 더 큰 노드 용량을 추가하여 용량 증가를 허용할 수 있습니다. 작은 노드가 있는 클러스터에 큰 노드를 추가하려면 쌍으로 추가해야 합니다. 이를 통해 큰 노드 중 하나에 장애가 발생하더라도 Double Helix가 데이터를 이동할 수 있는 충분한 공간이 확보됩니다. 성능을 향상시키려면 더 큰 노드 클러스터에 더 작은 노드 용량을 추가할 수 있습니다.

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

"NetApp 비디오: 원하는 조건으로 확장: SolidFire 클러스터 확장"

NetApp HCI 어플라이언스에 노드를 추가할 수 있습니다.

단계

1. 클러스터 > *노드*를 선택합니다.
2. 보류 중인 노드 목록을 보려면 *보류*를 클릭하세요.

   노드 추가 프로세스가 완료되면 활성 노드 목록에 해당 노드가 나타납니다. 그때까지 보류 중인 노드는 보류 중인 활성 목록에 나타납니다.

   SolidFire 클러스터에 노드를 추가하면 해당 노드에 클러스터의 Element 소프트웨어 버전을 설치합니다. 몇 분 정도 걸릴 수 있습니다.

3. 다음 중 하나를 수행하세요.
   - 개별 노드를 추가하려면 추가하려는 노드의 작업 아이콘을 클릭합니다.
   - 여러 노드를 추가하려면 추가할 노드의 확인란을 선택한 다음 대량 작업*을 선택합니다**.** *참고**:** 추가하는 노드에 클러스터에서 실행되는 Element 소프트웨어 버전과 다른 버전이 있는 경우, 클러스터는 노드를 클러스터 마스터에서 실행되는 Element 소프트웨어 버전으로 비동기적으로 업데이트합니다. 노드가 업데이트되면 자동으로 클러스터에 추가됩니다. 이 비동기 프로세스 동안 노드는 pendingActive 상태가 됩니다.
4. *추가*를 클릭하세요.

   노드가 활성 노드 목록에 나타납니다.

더 많은 정보를 찾아보세요

노드 버전 관리 및 호환성

노드 버전 관리 및 호환성

노드 호환성은 노드에 설치된 Element 소프트웨어 버전을 기준으로 합니다. Element 소프트웨어 기반 스토리지 클러스터는 노드와 클러스터의 버전이 호환되지 않으면 클러스터의 Element 소프트웨어 버전으로 노드를 자동으로 이미지화합니다.

다음 목록은 Element 소프트웨어 버전 번호를 구성하는 소프트웨어 릴리스 중요도 수준을 설명합니다.

- 주요한

  첫 번째 숫자는 소프트웨어 릴리스를 나타냅니다. 하나의 주요 구성 요소 번호를 가진 노드는 다른 주요 패치 번호를 가진 노드가 포함된 클러스터에 추가할 수 없으며, 혼합된 주요 버전의 노드로 클러스터를 생성할 수도 없습니다.

- 미성년자

두 번째 숫자는 주요 릴리스에 추가된 작은 소프트웨어 기능이나 기존 소프트웨어 기능에 대한 개선 사항을 나타냅니다. 이 구성 요소는 다른 하위 구성 요소를 포함하는 Element 소프트웨어 증분 릴리스와 호환되지 않음을 나타내기 위해 주요 버전 구성 요소 내에서 증분됩니다. 예를 들어, 11.0은 11.1과 호환되지 않고, 11.1은 11.2와 호환되지 않습니다.

- 마이크로

  세 번째 숫자는 major.minor 구성 요소로 표현되는 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.

호환성을 위해서는 주요 버전 번호와 부 버전 번호가 일치해야 합니다. 호환성을 위해 마이크로 숫자가 일치할 필요는 없습니다.

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 클러스터로 공존할 수 있습니다.

H 시리즈는 H610S-1, H610S-2, H610S-4, H410S 노드로 구성됩니다. 이 노드는 모두 10GbE와 25GbE를 지원합니다.

암호화되지 않은 노드와 암호화된 노드를 섞어 사용하지 않는 것이 가장 좋습니다. 혼합 노드 클러스터에서는 어떤 노드도 전체 클러스터 용량의 33%보다 클 수 없습니다. 예를 들어, SF-시리즈 4805 노드가 4개 있는 클러스터에서 단독으로 추가할 수 있는 가장 큰 노드는 SF-시리즈 9605입니다. 클러스터 용량 임계값은 이 상황에서 가장 큰 노드의 잠재적 손실에 따라 계산됩니다.

Element 소프트웨어 버전에 따라 다음 SF 시리즈 스토리지 노드는 지원되지 않습니다.

...부터 시작해서	저장 노드가 지원되지 않습니다...
원소 12.8	• SF4805 • SF9605 • SF19210 • SF38410
원소 12.7	• SF2405 • SF9608
원소 12.0	• SF3010 • SF6010 • SF9010

이러한 노드 중 하나를 지원되지 않는 Element 버전으로 업그레이드하려고 하면 해당 노드가 Element 12.x에서 지원되지 않는다는 오류가 표시됩니다.

노드 세부 정보 보기

서비스 태그, 드라이브 세부 정보, 활용도 및 드라이브 통계에 대한 그래픽 등 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 노드의 작업 아이콘을 클릭하세요.
3. *자세히 보기*를 클릭하세요.
4. 노드 세부 정보를 검토하세요.
   - 노드 **ID**: 노드에 대해 시스템에서 생성한 ID입니다.
   - 노드 이름: 노드의 호스트 이름입니다.
   - 노드 역할: 클러스터에서 노드가 맡는 역할입니다. 가능한 값:
     - 클러스터 마스터: 클러스터 전체의 관리 작업을 수행하고 MVIP와 SVIP를 포함하는 노드입니다.
     - 앙상블 노드: 클러스터에 참여하는 노드. 클러스터 크기에 따라 앙상블 노드는 3개 또는 5개가 있습니다.
     - 파이버 채널: 클러스터의 노드.
   - 노드 유형: 노드의 모델 유형입니다.
   - 활성 드라이브: 노드의 활성 드라이브 수입니다.
   - 노드 활용도: nodeHeat을 기반으로 한 노드 활용도의 백분율입니다. 표시되는 값은 recentPrimaryTotalHeat의 백분율입니다. Element 12.8부터 사용 가능합니다.
   - 관리 **IP**: 1GbE 또는 10GbE 네트워크 관리 작업을 위해 노드에 할당된 관리 IP(MIP) 주소입니다.
   - 클러스터 **IP**: 동일 클러스터 내 노드 간 통신에 사용되는 노드에 할당된 클러스터 IP(CIP) 주소입니다.
   - 저장소 **IP**: iSCSI 네트워크 검색 및 모든 데이터 네트워크 트래픽에 사용되는 노드에 할당된 저장 IP(SIP) 주소입니다.
   - 관리 **VLAN ID**: 관리 LAN의 가상 ID입니다.
   - 저장 **VLAN ID**: 스토리지 로컬 영역 네트워크의 가상 ID입니다.
   - 버전: 각 노드에서 실행되는 소프트웨어의 버전입니다.
   - 복제 포트: 원격 복제에 노드에서 사용되는 포트입니다.
   - 서비스 태그: 노드에 할당된 고유한 서비스 태그 번호입니다.
   - 사용자 지정 보호 도메인: 노드에 할당된 사용자 지정 보호 도메인입니다.

파이버 채널 포트 세부 정보 보기

FC 포트 페이지에서 파이버 채널 포트의 상태, 이름, 포트 주소 등의 세부 정보를 볼 수 있습니다.

클러스터에 연결된 파이버 채널 포트에 대한 정보를 확인합니다.

단계

1. 클러스터 > *FC 포트*를 클릭합니다.
2. 이 페이지의 정보를 필터링하려면 *필터*를 클릭하세요.
3. 자세한 내용을 검토하세요:

- 노드 **ID**: 연결을 위한 세션을 호스팅하는 노드입니다.
- 노드 이름: 시스템에서 생성된 노드 이름입니다.
- 슬롯: 파이버 채널 포트가 있는 슬롯 번호입니다.
- **HBA** 포트: 파이버 채널 호스트 버스 어댑터(HBA)의 물리적 포트입니다.
- **WWNN**: 월드 와이드 노드 이름.
- **WWPN**: 대상 월드 와이드 포트 이름입니다.
- 스위치 **WWN**: 파이버 채널 스위치의 전 세계 이름입니다.
- 항구 상태: 항구의 현재 상태.
- **nPort ID**: 파이버 채널 패브릭의 노드 포트 ID입니다.
- 속도: 협상된 파이버 채널 속도입니다. 가능한 값은 다음과 같습니다.
  - 4Gbps
  - 8Gbps
  - 16Gbps

더 많은 정보를 찾아보세요

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

가상 네트워크 관리

가상 네트워크 관리

SolidFire 스토리지의 가상 네트워킹을 사용하면 별도의 논리적 네트워크에 있는 여러 클라이언트 간의 트래픽을 하나의 클러스터에 연결할 수 있습니다. 클러스터에 대한 연결은 VLAN 태깅을 통해 네트워킹 스택에서 분리됩니다.

더 많은 정보를 찾아보세요

- 가상 네트워크 추가
- 가상 라우팅 및 전달 활성화
- 가상 네트워크 편집
- VRF VLAN 편집
- 가상 네트워크 삭제

가상 네트워크 추가

Element 소프트웨어를 실행하는 클러스터에 대한 멀티 테넌트 환경 연결을 활성화하기 위해 클러스터 구성에 새로운 가상 네트워크를 추가할 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 대해서는 다음 기준을 고려해야 합니다.

- VRF가 지원되지 않는 VLAN의 경우 이니시에이터가 SVIP와 동일한 서브넷에 있어야 합니다.
- VRF 지원 VLAN은 개시자가 SVIP와 동일한 서브넷에 있을 필요가 없으며 라우팅이 지원됩니다.
- 기본 SVIP는 개시자가 SVIP와 동일한 서브넷에 있을 것을 요구하지 않으며, 라우팅이 지원됩니다.

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

단계

1. 클러스터 > *네트워크*를 클릭합니다.
2. *VLAN 생성*을 클릭합니다.
3. 새 **VLAN** 만들기 대화 상자에서 다음 필드에 값을 입력합니다.
   - **VLAN** 이름
   - **VLAN** 태그
   - **SVIP**
   - 넷마스크
   - (선택사항) 설명
4. **IP** 주소 블록*의 **IP** 주소 범위에 대한 *시작 **IP** 주소를 입력합니다.
5. 블록에 포함할 IP 주소의 수로 IP 범위의 *크기*를 입력합니다.
6. 이 VLAN에 대한 비연속 IP 주소 블록을 추가하려면 *블록 추가*를 클릭합니다.
7. *VLAN 생성*을 클릭합니다.

가상 네트워크 세부 정보 보기

단계

1. 클러스터 > *네트워크*를 클릭합니다.
2. 자세한 내용을 검토하세요.
   - **ID**: 시스템에서 할당한 VLAN 네트워크의 고유 ID입니다.
   - 이름: VLAN 네트워크에 대한 고유한 사용자 지정 이름입니다.
   - **VLAN** 태그: 가상 네트워크가 생성될 때 할당된 VLAN 태그입니다.
   - **SVIP**: 가상 네트워크에 할당된 스토리지 가상 IP 주소입니다.
   - 넷마스크: 이 가상 네트워크의 넷마스크입니다.
   - 게이트웨이: 가상 네트워크 게이트웨이의 고유한 IP 주소입니다. VRF를 활성화해야 합니다.
   - **VRF** 활성화: 가상 라우팅 및 전달이 활성화되어 있는지 여부를 나타냅니다.

◦ 사용된 **IP**: 가상 네트워크에 사용된 가상 네트워크 IP 주소의 범위입니다.

가상 라우팅 및 전달 활성화

가상 라우팅 및 포워딩(VRF)을 활성화하면 라우팅 테이블의 여러 인스턴스가 라우터에 존재하고 동시에 작동할 수 있습니다. 이 기능은 저장 네트워크에서만 사용할 수 있습니다.

VLAN을 생성할 때만 VRF를 활성화할 수 있습니다. VRF가 아닌 상태로 다시 전환하려면 VLAN을 삭제하고 다시 만들어야 합니다.

1. 클러스터 > *네트워크*를 클릭합니다.
2. 새로운 VLAN에서 VRF를 활성화하려면 *VLAN 생성*을 선택하세요.
   a. 새로운 VRF/VLAN에 대한 관련 정보를 입력하세요. 가상 네트워크 추가를 참조하세요.
   b. **VRF** 사용 확인란을 선택합니다.
   c. 선택사항: 게이트웨이를 입력하세요.
3. *VLAN 생성*을 클릭합니다.

더 많은 정보를 찾아보세요

가상 네트워크 추가

가상 네트워크 편집

VLAN 이름, 넷마스크, IP 주소 블록 크기 등의 VLAN 속성을 변경할 수 있습니다. VLAN에 대한 VLAN 태그와 SVIP는 수정할 수 없습니다. 게이트웨이 속성은 VRF가 아닌 VLAN에 대한 유효한 매개변수가 아닙니다.

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

VLAN IP 주소 범위의 크기를 관리할 때 다음과 같은 제한 사항에 유의해야 합니다.

- VLAN이 생성될 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 주소를 초기 IP 주소 범위나 IP 블록에서 제거하려고 하면 작업이 실패할 수 있습니다.
- 클러스터의 다른 노드에 사용 중인 특정 IP 주소를 다시 할당할 수 없습니다.

다음 절차에 따라 IP 주소 블록을 추가할 수 있습니다.

1. 클러스터 > *네트워크*를 선택합니다.
2. 편집하려는 VLAN에 대한 작업 아이콘을 선택합니다.
3. *편집*을 선택하세요.
4. **VLAN** 편집 대화 상자에서 VLAN의 새 속성을 입력합니다.
5. 가상 네트워크에 대한 비연속적인 IP 주소 블록을 추가하려면 *블록 추가*를 선택합니다.

6. *변경 사항 저장*을 선택하세요.

문제 해결 **KB** 문서 링크

VLAN IP 주소 범위 관리와 관련된 문제 해결에 도움이 되는 지식 기반 문서에 대한 링크입니다.

- "Element 클러스터의 VLAN에 스토리지 노드를 추가한 후 중복 IP 경고 발생"
- "Element에서 사용 중인 VLAN IP와 해당 IP가 할당된 노드를 확인하는 방법"

VRF VLAN 편집

VLAN 이름, 넷마스크, 게이트웨이, IP 주소 블록 등의 VRF VLAN 속성을 변경할 수 있습니다.

1. 클러스터 > *네트워크*를 클릭합니다.
2. 편집하려는 VLAN에 대한 작업 아이콘을 클릭합니다.
3. *편집*을 클릭하세요.
4. **VLAN** 편집 대화 상자에 VRF VLAN의 새 속성을 입력합니다.
5. *변경 사항 저장*을 클릭하세요.

가상 네트워크 삭제

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

1. 클러스터 > *네트워크*를 클릭합니다.
2. 삭제하려는 VLAN에 대한 작업 아이콘을 클릭합니다.
3. *삭제*를 클릭하세요.
4. 메시지를 확인하세요.

더 많은 정보를 찾아보세요

가상 네트워크 편집

FIPS 드라이브를 지원하는 클러스터 만들기

FIPS 드라이브 기능을 위한 Element 클러스터 준비

다양한 고객 환경에서 솔루션을 배포할 때 보안이 점점 더 중요해지고 있습니다. 연방 정보 처리 표준(FIPS)은 컴퓨터 보안 및 상호 운용성에 대한 표준입니다. 저장 중인 데이터에 대한 FIPS 140-2 인증 암호화는 전반적인 보안 솔루션의 구성 요소입니다.

FIPS 드라이브 기능을 활성화하기 위한 준비로, 일부는 FIPS 드라이브를 지원하고 일부는 지원하지 않는 노드를 섞어서 사용하지 않도록 해야 합니다.

클러스터는 다음 조건에 따라 FIPS 드라이브 규격을 준수하는 것으로 간주됩니다.

- 모든 드라이브는 FIPS 드라이브로 인증되었습니다.
- 모든 노드는 FIPS 드라이브 노드입니다.
- EAR(Encryption at Rest)이 활성화되었습니다.
- FIPS 드라이브 기능이 활성화되었습니다. 모든 드라이브와 노드는 FIPS 기능을 갖춰야 하며, FIPS 드라이브 기능을 사용하려면 휴면 상태 암호화를 활성화해야 합니다.

휴면 상태에서 암호화 활성화

클러스터 전체의 암호화를 저장 상태에서 활성화하거나 비활성화할 수 있습니다. 이 기능은 기본적으로 활성화되어 있지 않습니다. FIPS 드라이브를 지원하려면 저장 데이터 암호화를 활성화해야 합니다.

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

더 많은 정보를 찾아보세요

- 클러스터에 대한 암호화 활성화 및 비활성화
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

노드가 **FIPS** 드라이브 기능을 사용할 준비가 되었는지 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.
- 부분적: 노드는 FIPS를 지원하지만, 모든 드라이브가 FIPS 드라이브는 아닙니다.
- 준비: 노드가 FIPS를 지원하고 모든 드라이브가 FIPS 드라이브이거나 드라이브가 없습니다.

단계

1. Element API를 사용하여 다음을 입력하여 스토리지 클러스터의 노드와 드라이브가 FIPS 드라이브를 지원하는지 확인합니다.

   ```
   GetFipsReport
   ```

2. 결과를 검토하여 준비 상태가 표시되지 않은 노드가 있는지 확인합니다.
3. 준비 상태가 표시되지 않은 노드의 경우 드라이브가 FIPS 드라이브 기능을 지원할 수 있는지 확인하세요.
   - Element API를 사용하여 다음을 입력합니다. `GetHardwareList`
   - *DriveEncryptionCapabilityType*의 값을 확인하세요. "fips"인 경우 하드웨어가 FIPS 드라이브 기능을 지원할 수 있습니다.

자세한 내용을 확인하세요 `GetFipsReport` 또는 `ListDriveHardware` 에서 "요소 API 참조".

4. 드라이브가 FIPS 드라이브 기능을 지원할 수 없는 경우 하드웨어를 FIPS 하드웨어(노드 또는 드라이브)로 교체하세요.

더 많은 정보를 찾아보세요

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

FIPS 드라이브 기능 활성화

NetApp Element 소프트웨어를 사용하여 FIPS 드라이브 기능을 활성화할 수 있습니다. `EnableFeature` API 방식.

클러스터에서 휴면 상태 암호화를 활성화해야 하며, 모든 노드와 드라이브는 FIPS를 지원해야 합니다. 이는 GetFipsReport에서 모든 노드에 대해 준비 상태가 표시되는 것을 통해 알 수 있습니다.

단계

1. Element API를 사용하여 다음을 입력하여 모든 드라이브에서 FIPS를 활성화합니다.

```
EnableFeature params: FipsDrives
```

더 많은 정보를 찾아보세요

- "Element API로 저장소 관리"
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

FIPS 드라이브 상태 확인

NetApp Element 소프트웨어를 사용하여 클러스터에서 FIPS 드라이브 기능이 활성화되어 있는지 확인할 수 있습니다. `GetFeatureStatus` FIPS 드라이브 활성화 상태가 참인지 거짓인지를 보여주는 API 메서드입니다.

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

```
GetFeatureStatus
```

2. 결과를 검토하세요 `GetFeatureStatus` API 호출. FIPS 드라이브 활성화 값이 True이면 FIPS 드라이브 기능이 활성화됩니다.

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

더 많은 정보를 찾아보세요

- "Element API로 저장소 관리"
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

FIPS 드라이브 기능 문제 해결

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

1. Element UI를 사용하여 보고 > *알림*을 선택합니다.
2. 다음을 포함한 클러스터 오류를 찾아보세요.
   - FIPS 드라이브가 일치하지 않습니다
   - FIPS로 인해 규정 준수가 불가능해졌습니다.
3. 해결 방법에 대한 제안은 클러스터 오류 코드 정보를 참조하세요.

더 많은 정보를 찾아보세요

- 클러스터 오류 코드
- "Element API로 저장소 관리"
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

안전한 통신을 구축하세요

클러스터에서 HTTPS에 대해 FIPS 140-2를 활성화합니다.

EnableFeature API 메서드를 사용하면 HTTPS 통신에 대해 FIPS 140-2 운영 모드를 활성화할 수 있습니다.

NetApp Element 소프트웨어를 사용하면 클러스터에서 FIPS(연방 정보 처리 표준) 140-2 운영 모드를 활성화할 수 있습니다. 이 모드를 활성화하면 NetApp 암호화 보안 모듈(NCSM)이 활성화되고 HTTPS를 통한 NetApp Element UI 및 API와의 모든 통신에 FIPS 140-2 레벨 1 인증 암호화가 활용됩니다.

> FIPS 140-2 모드를 활성화한 후에는 비활성화할 수 없습니다. FIPS 140-2 모드가 활성화되면 클러스터의 각 노드가 재부팅되고 자체 테스트를 통해 NCSM이 올바르게 활성화되어 있고 FIPS 140-2 인증 모드에서 작동하는지 확인합니다. 이로 인해 클러스터의 관리 및 스토리지 연결이 모두 중단됩니다. 신중하게 계획하고 해당 환경에서 암호화 메커니즘이 필요한 경우에만 이 모드를 활성화해야 합니다.

자세한 내용은 Element API 정보를 참조하세요.

다음은 FIPS를 활성화하기 위한 API 요청의 예입니다.

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

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

더 많은 정보를 찾아보세요

- SSL 암호
- "Element API로 저장소 관리"
- "SolidFire 및 Element 소프트웨어 문서"
- "vCenter Server용 NetApp Element 플러그인"

SSL 암호

SSL 암호는 호스트가 안전한 통신을 구축하는 데 사용하는 암호화 알고리즘입니다. Element 소프트웨어가 지원하는 표준 암호와 FIPS 140-2 모드가 활성화된 경우 지원하는 비표준 암호가 있습니다.

다음 목록은 Element 소프트웨어에서 지원하는 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_WITH_AES_128_CBC_SHA(rsa 2048) - A

  TLS_RSA_WITH_AES_128_CBC_SHA256(rsa 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256(rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA(rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA256(rsa 2048) - A

TLS_RSA_WITH_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_WITH_RC4_128_MD5(rsa 2048) - C

TLS_RSA_WITH_RC4_128_SHA(rsa 2048) - C

TLS_RSA_WITH_SEED_CBC_SHA(rsa 2048) - A

- **FIPS 140-2** 지원

  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(섹션 571r1) - 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_WITH_AES_128_CBC_SHA(rsa 2048) - A

  TLS_RSA_WITH_AES_128_CBC_SHA256(rsa 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256(rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA(rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA256(rsa 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384(rsa 2048) - A

더 많은 정보를 찾아보세요

클러스터에서 HTTPS에 대해 FIPS 140-2를 활성화합니다.

외부 키 관리 시작하기

외부 키 관리 시작하기

외부 키 관리(EKM)는 클러스터 외부 키 서버(EKS)와 함께 안전한 인증 키(AK) 관리를 제공합니다. AK는 SED(자체 암호화 드라이브)를 잠그거나 잠금 해제하는 데 사용됩니다."휴면 암호화" 클러스터에서 활성화되었습니다. EKS는 AK의 안전한 생성 및 저장을 제공합니다. 클러스터는 OASIS에서 정의한 표준 프로토콜인 KMIP(Key Management Interoperability Protocol)를 활용하여 EKS와 통신합니다.

- "외부 관리 설정"
- "휴면 마스터 키에서 소프트웨어 암호화 재키"
- "접근 불가능하거나 잘못된 인증 키 복구"
- "외부 키 관리 API 명령"

더 많은 정보를 찾아보세요

- "휴면 상태에서 소프트웨어 암호화를 활성화하는 데 사용할 수 있는 CreateCluster API"
- "SolidFire 및 Element 소프트웨어 문서"
- "NetApp SolidFire 및 Element 제품의 이전 버전에 대한 설명서"

외부 키 관리 설정

다음 단계를 따르고 나열된 Element API 메서드를 사용하여 외부 키 관리 기능을 설정할 수 있습니다.

필요한 것

- 휴면 상태의 소프트웨어 암호화와 함께 외부 키 관리를 설정하는 경우 다음을 사용하여 휴면 상태의 소프트웨어 암호화를 활성화했습니다."클러스터 생성" 볼륨을 포함하지 않는 새 클러스터에 대한 메서드입니다.

단계

1. 외부 키 서버(EKS)와 신뢰 관계를 구축합니다.
   a. 다음 API 메서드를 호출하여 키 서버와의 신뢰 관계를 구축하는 데 사용되는 Element 클러스터에 대한 공개/개인 키 쌍을 만듭니다."공개 개인 키 쌍 생성"
   b. 인증 기관이 서명해야 하는 인증서 서명 요청(CSR)을 가져옵니다. CSR을 통해 키 서버는 키에 액세스할 Element 클러스터가 Element 클러스터로 인증되었는지 확인할 수 있습니다. 다음 API 메서드를 호출합니다. "클라이언트 인증서 서명 요청 받기"

c. EKS/인증 기관을 사용하여 검색된 CSR에 서명합니다. 자세한 내용은 타사 문서를 참조하세요.

2. 클러스터에 서버와 공급자를 생성하여 EKS와 통신합니다. 키 제공자는 키를 어디에서 얻어야 하는지 정의하고, 서버는 통신할 EKS의 구체적인 속성을 정의합니다.

   a. 다음 API 메서드를 호출하여 키 서버 세부 정보가 저장될 키 공급자를 만듭니다."CreateKeyProviderKmip"

   b. 다음 API 메서드를 호출하여 서명된 인증서와 인증 기관의 공개 키 인증서를 제공하는 키 서버를 만듭니다 ."CreateKeyServerKmip" "테스트키서버Kmip"

      테스트에 실패하면 서버 연결 및 구성을 확인하세요. 그런 다음 테스트를 반복합니다.

   c. 다음 API 메서드를 호출하여 키 제공자 컨테이너에 키 서버를 추가합니다."AddKeyServerToProviderKmip" "테스트키공급자Kmip"

      테스트에 실패하면 서버 연결 및 구성을 확인하세요. 그런 다음 테스트를 반복합니다.

3. 저장 중 암호화를 위한 다음 단계로 다음 중 하나를 수행하세요.

   a. (휴면 하드웨어 암호화의 경우) 활성화"휴면 상태의 하드웨어 암호화" 키를 저장하는 데 사용되는 키 서버를 포함하는 키 공급자의 ID를 제공하여 호출합니다."휴지상태에서 암호화 활성화" API 방식.

      > 다음을 통해 휴면 암호화를 활성화해야 합니다."API" . 기존 Element UI 버튼을 사용하여 저장 상태에서 암호화를 활성화하면 해당 기능이 내부적으로 생성된 키를 사용하도록 되돌아갑니다.

   b. (휴면 상태의 소프트웨어 암호화를 위해)"휴면 상태의 소프트웨어 암호화" 새로 생성된 키 공급자를 활용하려면 키 공급자 ID를 다음 항목에 전달합니다."RekeySoftwareEncryptionAtRestMasterKey" API 방식.

더 많은 정보를 찾아보세요

- "클러스터에 대한 암호화 활성화 및 비활성화"
- "SolidFire 및 Element 소프트웨어 문서"
- "NetApp SolidFire 및 Element 제품의 이전 버전에 대한 설명서"

휴면 마스터 키에서 소프트웨어 암호화 재키

Element API를 사용하면 기존 키를 다시 키로 사용할 수 있습니다. 이 프로세스는 외부 키 관리 서버에 대한 새로운 대체 마스터 키를 생성합니다. 마스터 키는 항상 새로운 마스터 키로 교체되며, 복제되거나 덮어쓰여지지 않습니다.

다음 절차 중 하나로 키를 다시 입력해야 할 수도 있습니다.

- 내부 키 관리에서 외부 키 관리로 변경하는 일환으로 새 키를 만듭니다.
- 보안 관련 이벤트에 대한 대응이나 보호 수단으로 새로운 키를 생성합니다.

> 이 프로세스는 비동기적으로 진행되며 재키 작업이 완료되기 전에 응답을 반환합니다. 당신은 사용할 수 있습니다"비동기 결과 가져오기" 프로세스가 완료되었는지 확인하기 위해 시스템을 폴링하는 방법입니다.

필요한 것

- 다음을 사용하여 휴면 상태의 소프트웨어 암호화를 활성화했습니다."클러스터 생성" 볼륨이 없고 I/O가 없는 새 클러스터에 대한 방법입니다. 링크 사용 :../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] 상태가 확인됨 `enabled` 계속하기 전에.
- 당신은 가지고있다"신뢰 관계를 구축했다" SolidFire 클러스터와 외부 키 서버(EKS) 사이. 실행하다 "테스트키공급자Kmip" 키 공급자와의 연결이 설정되었는지 확인하는 방법입니다.

단계

1. 실행하다"ListKeyProvidersKmip" 명령을 입력하고 키 공급자 ID를 복사합니다.(`keyProviderID`).
2. 실행하다"RekeySoftwareEncryptionAtRestMasterKey" 와 함께 `keyManagementType` 매개변수로 `external` 그리고 `keyProviderID` 이전 단계의 키 공급자 ID 번호와 같습니다.

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

3. 복사하다 `asyncHandle` 에서 가치 `RekeySoftwareEncryptionAtRestMasterKey` 명령 응답.
4. 실행하다"비동기 결과 가져오기" 명령으로 `asyncHandle` 이전 단계의 값을 사용하여 구성의 변경 사항을 확인합니다. 명령 응답을 통해 이전 마스터 키 구성이 새로운 키 정보로 업데이트되었음을 확인할 수 있습니다. 이후 단계에서 사용할 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. 실행하다 `GetSoftwareEncryptionatRestInfo` 새로운 키 세부 정보를 포함하여 확인하는 명령 `keyProviderID` , 업데이트되었습니다.

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

더 많은 정보를 찾아보세요

- "Element API로 저장소 관리"
- "SolidFire 및 Element 소프트웨어 문서"
- "NetApp SolidFire 및 Element 제품의 이전 버전에 대한 설명서"

접근 불가능하거나 잘못된 인증 키 복구

때로는 사용자 개입이 필요한 오류가 발생할 수 있습니다. 오류가 발생하면 클러스터 오류(클러스터 오류 코드라고 함)가 생성됩니다. 여기서는 가장 가능성 있는 두 가지 사례를 설명합니다.

KmipServerFault 클러스터 오류로 인해 클러스터가 드라이브 잠금을 해제할 수 없습니다**.**

이는 클러스터가 처음 부팅될 때 키 서버에 액세스할 수 없거나 필요한 키를 사용할 수 없는 경우 발생할 수 있습니다.

1. 클러스터 오류 코드(있는 경우)의 복구 단계를 따르세요.

메타데이터 드라이브가 실패로 표시되고 **"**사용 가능**"** 상태로 전환되었기 때문에 **sliceServiceUnhealthy** 오류가 설정될 수 있습니다**.**

지우기 단계:

1. 드라이브를 다시 추가합니다.
2. 3~4분 후에 확인하세요 `sliceServiceUnhealthy` 오류가 해결되었습니다.

보다"클러스터 오류 코드" 자세한 내용은.

외부 키 관리 **API** 명령

EKM을 관리하고 구성하는 데 사용할 수 있는 모든 API 목록입니다.

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

- 공개 개인 키 쌍 생성
- 클라이언트 인증서 서명 요청 받기

외부 고객 소유 서버의 구체적인 세부 정보를 정의하는 데 사용됩니다.

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- 테스트키서버Kmip

외부 키 서버를 관리하는 키 공급자를 생성하고 유지 관리하는 데 사용됩니다.

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- ProviderKmip에서 KeyServer 제거
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- 테스트키공급자Kmip

API 메소드에 대한 정보는 다음을 참조하세요. "API 참조 정보".

저작권 정보

상표 정보