시스템 관리

Element Software

NetApp
October 01, 2024

목차

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

1. 다음 API 메서드를 호출하고 IDP 메타데이터를 JSON 형식으로 전달하여 클러스터에 대한 새로운 타사 IDP(Identity Provider) 구성을 생성합니다. `CreateIdpConfiguration`

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

2. 다음 API 메서드를 호출하여 spMetadataUrl 을 통해 클러스터 메타데이터를 검색하여 타사 IDP에 복사합니다. `ListIdpConfigurations`

   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 메서드를 호출하여 타사 IDP에서 인증을 받은 하나 이상의 클러스터 관리자 사용자 계정을 생성합니다

.AddIdpClusterAdmin

> 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 메서드를 호출하여 클러스터에 MFA를 사용하도록 설정합니다. `EnableIdpAuthentication`

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 관리자를 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 않아야 합니다. `SetSSLCertificate`

> 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
- SNMP 관리
- 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. 다음 중 하나를 사용하여 SED(자체 암호화 드라이브)의 클러스터 전체 보호를 활성화할 수 "하드웨어 또는 소프트웨어 기반의 유휴 암호화"있습니다.

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

저장 시 암호화 상태 및/또는 클러스터에서 유휴 시 소프트웨어 암호화의 현재 상태를 확인하려면 "GetClusterInfo 를 참조하십시오"방법을 사용합니다. 메소드를 사용하여 클러스터에서 유휴 데이터의 암호화에 사용되는 정보를 가져올 수 "GetSoftwareEncryptionAtRestInfo 를 참조하십시오"있습니다.

현재 Element 소프트웨어 UI 대시보드에는 `https://<MVIP>/` 하드웨어 기반 암호화에 대한 유휴 상태의 암호화만 표시됩니다.

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 시 암호화를 활성화하려면 를 통해 유휴 시 암호화를 활성화해야 "API를 참조하십시오"합니다. 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. 클러스터 생성 중에 를 로 설정한 `true` 상태에서 `enableSoftwareEncryptionAtRest` 를 "클러스터 생성 방법"실행합니다.

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"

SNMP 관리

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 정보입니다

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 * 를 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 소프트웨어 버전에 따라 다음 SF-시리즈 스토리지 노드는 지원되지 않습니다.

다음으로 시작...	스토리지 노드가 지원되지 않음...
요소 12.7	• SF2405를 참조하십시오 • SF9608를 참조하십시오
요소 12.0	• SF3010를 참조하십시오 • SF6010를 참조하십시오 • SF9010를 참조하십시오

이러한 노드 중 하나를 지원되지 않는 Element 버전으로 업그레이드하려고 하면 이 노드가 Element 12.x에서 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.
  - 4Gbps를 참조하십시오
  - 8Gbps를 참조하십시오
  - 16Gbps를 참조하십시오

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 사용 * 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.

   ```
   GetFipsReport
   ```

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 다음을 입력합니다. `GetHardwareList`
   - DriveEncryptionCapabilityType * 의 값을 확인합니다. "FIPS"인 경우 하드웨어에서 FIPS 드라이브 기능을 지원할 수 있습니다.

     또는 `ListDriveHardware` 에 대한 자세한 `GetFipsReport` 내용은 "요소 API 참조입니다"을 참조하십시오.
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 API 방법을 사용하여 FIPS 드라이브 기능을 활성화할 수 `EnableFeature` 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 API 방법을 사용하여 클러스터에서 FIPS 드라이브 기능이 활성화되어 있는지 확인할 수 `GetFeatureStatus` 있습니다. 이 방법은 FIPS 드라이브 사용 상태가 참인지 거짓인지 여부를 보여 줍니다.

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

   ```
   GetFeatureStatus
   ```

2. API 호출 결과를 `GetFeatureStatus` 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 HTTPS에 FIPS 140-2를 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 가 클러스터에서 활성화되어 있을 때 SED(자체 암호화 드라이브)를 잠그고 잠금 해제하는 데 "유휴 데이터 암호화"사용됩니다. 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

- 유휴 시 소프트웨어 암호화와 함께 외부 키 관리를 설정하는 경우, 볼륨을 포함하지 않는 새 클러스터에서 해당 방법으로 유휴 시 소프트웨어 암호화를 사용하도록 설정한 것입니다"클러스터 생성".

단계

1. 외부 키 서버(EKS)와 트러스트 관계를 설정합니다.
   a. 다음 API 메서드를 호출하여 키 서버와의 신뢰 관계를 설정하는 데 사용되는 Element 클러스터에 대한 공개/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 메소드를 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 메서드를 호출하여 인증 기관의 서명된 인증서 및 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) API 메서드를 호출하여 키를 저장하는 데 사용되는 키 서버가 포함된 키 공급자의 ID를 "EnableEncryptionAtRest 를 참조하십시오"제공하여 활성화합니다"유휴 하드웨어 암호화".

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

   b. (저장 시 소프트웨어 암호화의 경우) "유휴 소프트웨어 암호화"새로 생성된 키 공급자를 사용하려면 키 공급자 ID를 "RekeySoftwareEncryptionAtRestMasterKey를 참조하십시오"API 메서드에 전달합니다.

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 메소드를 사용하여 시스템을 폴링하여 프로세스가 언제 완료되었는지 확인할 수 "GetAsyncResult 를 참조하십시오"있습니다.

필요한 것

- 볼륨을 포함하지 않고 I/O가 없는 새 클러스터에서 해당 방법을 사용하여 유휴 시 소프트웨어 암호화를 활성화했습니다"클러스터 생성" 계속하기 전에 링크:../api/reference_element_api_getsoftwareencryptionatrestinfo.html 을 사용하여 [`GetSoftwareEncryptionatRestInfo` 상태가 `enabled` 올바른지 확인하십시오.
- "트러스트 관계를 설정했습니다"SolidFire 클러스터와 EKS(외부 키 서버) 사이에 있습니다. "TestKeyProviderKmip 을 참조하십시오"메서드를 실행하여 키 공급자에 대한 연결이 설정되었는지 확인합니다.

단계

1. "ListKeyProvidersKmip 을 참조하십시오"명령을 실행하고 키 공급자 ID를 (`keyProviderID`복사합니다.)
2. 이전 단계에서 키 공급자의 ID 번호로 및 `keyProviderID` 로 매개 변수를 `external` 사용하여 `keyManagementType` 를 실행합니다"RekeySoftwareEncryptionAtRestMasterKey를 참조하십시오".

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

3. `asyncHandle`명령 응답에서 값을 `RekeySoftwareEncryptionAtRestMasterKey` 복사합니다.
4. "GetAsyncResult 를 참조하십시오"이전 단계의 값으로 명령을 `asyncHandle` 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 를 포함한 새로운 주요 정보가 업데이트되었는지 `keyProviderID`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 고장이 해결되었는지 `sliceServiceUnhealthy` 점검한다.

자세한 내용은 을 "클러스터 고장 코드" 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 메서드에 대한 자세한 내용은 을 참조하십시오"API 참조 정보입니다".

저작권 정보

상표 정보