



외부 키 관리 시작하기

Element Software

NetApp
November 12, 2025

목차

외부 키 관리 시작하기	1
외부 키 관리 시작하기	1
외부 키 관리 설정	1
휴면 마스터 키에서 소프트웨어 암호화 재키	2
접근 불가능하거나 잘못된 인증 키 복구	4
KmpServerFault 클러스터 오류로 인해 클러스터가 드라이브 잠금을 해제할 수 없습니다.	4
메타데이터 드라이브가 실패로 표시되고 "사용 가능" 상태로 전환되었기 때문에 sliceServiceUnhealthy 오류가 설정될 수 있습니다.....	4
외부 키 관리 API 명령	5

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 공급자는 키를 어디에서 얻어야 하는지 정의하고, 서버는 통신할 EKS의 구체적인 속성을 정의합니다.
 - a. 다음 API 메서드를 호출하여 키 서버 세부 정보가 저장될 키 공급자를 만듭니다."CreateKeyProviderKmpip"
 - b. 다음 API 메서드를 호출하여 서명된 인증서와 인증 기관의 공개 키 인증서를 제공하는 키 서버를 만듭니다

[."CreateKeyServerKmpip" "테스트키서버Kmpip"](#)

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

- c. 다음 API 메서드를 호출하여 키 제공자 컨테이너에 키 서버를 추가합니다.["AddKeyServerToProviderKmpip" "테스트키공급자Kmpip"](#)

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.



다음은 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 ["테스트키공급자Kmpip"](#) 키 공급자와의 연결이 설정되었는지 확인하는 방법입니다.

단계

1. 실행하다 "ListKeyProvidersKmp" 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.

- CreateKeyServerKmpip
- ModifyKeyServerKmpip
- DeleteKeyServerKmpip
- GetKeyServerKmpip
- ListKeyServersKmpip
- 테스트키서버Kmpip

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

- CreateKeyProviderKmpip
- DeleteKeyProviderKmpip
- AddKeyServerToProviderKmpip
- ProviderKmpip에서 KeyServer 제거
- GetKeyProviderKmpip
- ListKeyProvidersKmpip
- RekeySoftwareEncryptionAtRestMasterKey
- 테스트키공급자Kmpip

API 메소드에 대한 정보는 다음을 참조하세요. "[API 참조 정보](#)".

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.