보안 API 메서드

Element Software

NetApp
January 15, 2024

목차

보안 API 메서드

Element 소프트웨어를 외부 키 관리 서버와 같은 외부 보안 관련 서비스와 통합할 수 있습니다. 이러한 보안 관련 방법을 사용하면 저장된 암호화에 대한 외부 키 관리와 같은 요소 보안 기능을 구성할 수 있습니다.

- AddKeyServerToProviderKmip 를 참조하십시오
- CreateKeyProviderKmip 을 참조하십시오
- CreateKeyServerKmip 을 참조하십시오
- CreatePublicPrivateKeyPair 를 참조하십시오
- DeleteKeyProviderKmip 를 클릭합니다
- DeleteKeyServerKmip 를 클릭합니다
- DisableEncryptionAtRest
- EnableEncryptionAtRest 를 참조하십시오
- GetClientCertificateSignRequest 를 참조하십시오
- GetKeyProviderKmip 을 참조하십시오
- GetKeyServerKmip 을 참조하십시오
- ListKeyProvidersKmip 을 참조하십시오
- ListKeyServersKmip 를 참조하십시오
- ModifyKeyServerKmip
- RemoveKeyServerFromProviderKmip 를 참조하십시오
- TestKeyProviderKmip 을 참조하십시오
- TestKeyServerKmip

자세한 내용을 확인하십시오

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

AddKeyServerToProviderKmip 를 참조하십시오

'AddKeyServerToProviderKmip' 메서드를 사용하여 KMIP(Key Management Interoperability Protocol) 키 서버를 지정된 키 공급자에 할당할 수 있습니다. 할당 중에 서버에 연락하여 기능을 확인합니다. 지정된 키 서버가 이미 지정된 키 공급자에 할당된 경우 아무런 작업도 수행되지 않으며 오류가 반환되지 않습니다. "RemoveKeyServerFromProviderKmip" 메서드를 사용하여 할당을 제거할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderID를 입력합니다	키 서버를 할당할 키 공급자의 ID입니다.	정수	없음	예
KeyServerID를 입력합니다	할당할 키 서버의 ID입니다.	정수	없음	예

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 반환되지 않는 한 할당이 성공한 것으로 간주됩니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "AddKeyServerToProviderKmip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
    },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {}
    }
}
```

버전 이후 새로운 기능

11.7

CreateKeyProviderKmip 을 참조하십시오

'CreateKeyProviderKmip' 메서드를 사용하여 KMIP(Key Management Interoperability Protocol) 키 공급자를 지정된 이름으로 생성할 수 있습니다. 키 공급자는 인증 키를 검색할 메커니즘과 위치를 정의합니다. 새로운 KMIP 키 공급자를 생성할 때 KMIP 키 서버가 할당되지 않습니다. KMIP 키 서버를 생성하려면 'CreateKeyServerKmip' 방법을 사용하십시오. 공급자에 할당하려면 "AddKeyServerToProviderKmip"을 참조하십시오.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderName 을 클릭합니다	생성된 KMIP 키 공급자와 연관되는 이름입니다. 이 이름은 표시 목적으로만 사용되며 고유한 이름은 필요하지 않습니다.	문자열	없음	예

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형
KmipKeyProvider 를 참조하십시오	새로 만든 키 공급자에 대한 세부 정보가 포함된 개체입니다.	"키ProviderKmip 을 참조하십시오"

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "CreateKeyProviderKmip",
  "params": {
    "keyProviderName": "ProviderName",
    },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {
    "kmipKeyProvider": {
        "keyProviderName": "ProviderName",
        "keyProviderIsActive": true,
        "kmipCapabilities": "SSL",
        "keyServerIDs": [
            15
        ],
        "keyProviderID": 1
    }
}
}
```

버전 이후 새로운 기능

11.7

CreateKeyServerKmip 을 참조하십시오

'CreateKeyServerKmip' 메서드를 사용하여 지정된 특성으로 KMIP(Key Management Interoperability Protocol) 키 서버를 생성할 수 있습니다. 만드는 동안 서버에 연결되지 않으므로 이 방법을 사용하기 전에 이 서버가 존재하지 않아도 됩니다. 클러스터된 키 서버 구성의 경우 kmipKeyServerHostnames 매개 변수에 모든 서버 노드의 호스트 이름 또는 IP 주소를 제공해야 합니다. 'TestKeyServerKmip' 메서드를 사용하여 키 서버를 테스트할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KmipCaCertificate입니다	외부 키 서버의 루트 CA의 공개 키 인증서입니다. TLS 통신에서 외부 키 서버가 제공하는 인증서를 확인하는 데 사용됩니다. 개별 서버가 서로 다른 CA를 사용하는 키 서버 클러스터의 경우 모든 CA의 루트 인증서가 포함된 연결된 문자열을 제공합니다.	문자열	없음	예
kmipClientCertificate를 참조하십시오	SolidFire KMIP 클라이언트가 사용하는 PEM 형식 Base64 인코딩된 PKCS #10 X.509 인증서.	문자열	없음	예
kmipKeyServerHostName입니다	이 KMIP 키 서버와 연관된 호스트 이름 또는 IP 주소의 배열입니다. 키 서버가 클러스터 구성에 있는 경우에만 호스트 이름 또는 IP 주소를 여러 개 제공해야 합니다.	문자열 배열	없음	예
kmipKeyServerName입니다	KMIP 키 서버의 이름입니다. 이 이름은 표시 목적으로만 사용되며 고유한 이름은 필요하지 않습니다.	문자열	없음	예
kmipKeyServerPort를 참조하십시오	이 KMIP 키 서버와 연관된 포트 번호 (일반적으로 5696)	정수	없음	아니요

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형

KmipKeyServer를 참조하십시오	새로 만든 키 서버에 대한 세부 정보가 포함된 개체입니다.	"KeyServerKmip"

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "CreateKeyServerKmip",
  "params": {
    "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":1
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
    }
}
```

CreatePublicPrivateKeyPair 를 참조하십시오

CreatePublicPrivateKeyPair 메서드를 사용하여 공용 및 개인 SSL 키를 만들 수 있습니다. 이러한 키를 사용하여 인증서 서명 요청을 생성할 수 있습니다. 각 스토리지 클러스터마다 하나의 키 쌍만 사용할 수 있습니다. 이 방법을 사용하여 기존 키를 교체하기 전에 모든 공급자가 키를 더 이상 사용하지 않는지 확인합니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
공통 이름	X.509 고유 이름 * 일반 이름 * 필드(CN)입니다.	문자열	없음	아니요
국가	X.509 고유 이름 * Country * 필드©.	문자열	없음	아니요
이메일 주소	X.509 고유 이름 * 전자 메일 주소 * 필드(메일)	문자열	없음	아니요
지역성	X.509 고유 이름 * Locality Name * 필드(L)입니다.	문자열	없음	아니요
조직	X.509 고유 이름 * 조직 이름 * 필드(O).	문자열	없음	아니요
조직 구성 단위	X.509 고유 이름 * 조직 단위 이름 * 필드(OU).	문자열	없음	아니요
상태	X.509 고유 이름 * State * 또는 * Province Name * 필드(ST 또는 SP 또는 S)	문자열	없음	아니요

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 없으면 키 생성이 성공한 것으로 간주됩니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "CreatePublicPrivateKeyPair",
  "params": {
    "commonName": "Name",
    "country": "US",
    "emailAddress" : "email@domain.com"
   },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {}
}
```

버전 이후 새로운 기능

11.7

DeleteKeyProviderKmip 를 클릭합니다

DeleteKeyProviderKmip' 메서드를 사용하여 지정된 비활성 키 관리 상호 운용성 프로토콜(KMIP) 키 공급자를 삭제할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderID를 입력합니다	삭제할 키 공급자의 ID입니다.	정수	없음	예

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 없으면 삭제 작업이 성공한 것으로 간주됩니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
    },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {}
}
```

버전 이후 새로운 기능

11.7

DeleteKeyServerKmip 를 클릭합니다

DeleteKeyServerKmip' 방법을 사용하여 기존 KMIP(Key Management Interoperability Protocol) 키 서버를 삭제할 수 있습니다. 키 서버가 해당 공급자에 마지막으로 할당된 서버가 아닌 경우 해당 공급자가 현재 사용 중인 키를 제공하는 경우를 제외하고 키 서버를 삭제할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyServerID를 입력합니다	삭제할 KMIP 키 서버의 ID입니다.	정수	없음	예

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 없으면 삭제 작업이 성공한 것으로 간주됩니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {}
}
```

버전 이후 새로운 기능

11.7

DisableEncryptionAtRest

"EnableEncryptionAtRest" 메서드를 사용하여 이전에 클러스터에 적용된 암호화를 제거할 수 있습니다. 이 비활성화 방법은 비동기식이며 암호화를 비활성화하기 전에 응답을 반환합니다. GetClusterInfo 메서드를 사용하면 프로세스가 완료된 시점을 확인하기 위해 시스템을 폴링할 수

있습니다.

> 유휴 상태의 암호화 및/또는 클러스터의 유휴 상태의 소프트웨어 암호화를 확인하려면 를 사용합니다 "클러스터 정보 확인 방법을 참조하십시오". 를 사용할 수 있습니다 `GetSoftwareEncryptionAtRestInfo` "클러스터에서 유휴 데이터를 암호화하는 데 사용하는 정보를 가져오는 방법입니다".

> 이 방법을 사용하여 유휴 소프트웨어 암호화를 해제할 수 없습니다. 저장 시 소프트웨어 암호화를 비활성화하려면 다음을 수행해야 합니다 "새 클러스터를 생성합니다" 소프트웨어 암호화 사용 안 함.

매개 변수

이 메서드에는 입력 매개 변수가 없습니다.

반환 값

이 메서드에는 반환 값이 없습니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
   "method": "DisableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id" : 1,
  "result" : {}
}
```

버전 이후 새로운 기능

9.6

자세한 내용을 확인하십시오

- "GetClusterInfo 를 참조하십시오"

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

EnableEncryptionAtRest 를 참조하십시오

클러스터에서 각 노드의 드라이브에 사용되는 암호화 키를 관리할 수 있도록 "EnableEncryptionAtRest" 방법을 사용하여 클러스터의 유휴 상태에서 AES(Advanced Encryption Standard) 256비트 암호화를 활성화할 수 있습니다. 이 기능은 기본적으로 사용되지 않습니다.

> 유휴 상태의 암호화 및/또는 클러스터의 유휴 상태의 소프트웨어 암호화를 확인하려면 를 사용합니다 "클러스터 정보 확인 방법을 참조하십시오". 를 사용할 수 있습니다 `GetSoftwareEncryptionAtRestInfo` "클러스터에서 유휴 데이터를 암호화하는 데 사용하는 정보를 가져오는 방법입니다".

> 이 방법은 저장된 소프트웨어 암호화를 사용하지 않습니다. 이 작업은 를 통해서만 수행할 수 있습니다 "클러스터 생성 방법" 와 함께 `enableSoftwareEncryptionAtRest` 를 로 설정합니다 `true`.

유휴 데이터 암호화를 설정하면 클러스터에서 각 노드의 드라이브에 대한 암호화 키가 내부적으로 자동으로 관리됩니다.

keyProviderID 를 지정하면 키 공급자 유형에 따라 암호가 생성되고 검색됩니다. 이는 일반적으로 KMIP 키 공급자의 경우 KMIP(Key Management Interoperability Protocol) 키 서버를 사용하여 수행됩니다. 이 작업 후에는 지정된 공급자가 활성화된 것으로 간주되므로 "disableEncryptionAtRest" 메서드를 사용하여 저장된 암호화 기능을 해제할 때까지 삭제할 수 없습니다.

> 모델 번호가 "-NE"로 끝나는 노드 형식이 있는 경우 "EnableEncryptionAtRest" 메서드 호출이 실패하고 "Encryption not allowed"라는 응답이 표시됩니다. 클러스터에서 암호화할 수 없는 노드가 감지되었습니다."

> 클러스터가 실행 중이고 양호한 상태인 경우에만 암호화를 사용하거나 사용하지 않도록 설정해야 합니다. 필요에 따라 원하는 빈도로 암호화를 활성화 또는 비활성화할 수 있습니다.

> 이 프로세스는 비동기식이며 암호화를 사용하기 전에 응답을 반환합니다. GetClusterInfo 메서드를 사용하면 프로세스가 완료된 시점을 확인하기 위해 시스템을 폴링할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderID를 입력합니다	KMIP 키 공급자의 ID입니다.	정수	없음	아니요

반환 값

이 메서드에는 반환 값이 없습니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
   "method": "EnableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

답변 예

이 메서드는 EnableEncryptionAtRest 메서드에서 다음 예제와 유사한 응답을 반환합니다. 보고할 결과가 없습니다.

```
{
   "id": 1,
   "result": {}
}
```

클러스터에서 저장된 암호화 기능을 사용하는 동안 GetClusterInfo 는 저장된 암호화("encryptionAtRestState") 상태를 "enabled"로 설명하는 결과를 반환합니다. 저장된 데이터 암호화가 완전히 활성화되면 반환된 상태가 "활성화됨"으로 변경됩니다.

```
{
   "id": 1,
      "result": {
         "clusterInfo": {
            "attributes": { },
               "encryptionAtRestState": "enabling",
            "ensemble": [
               "10.10.5.94",
               "10.10.5.107",
               "10.10.5.108"
            ],
            "mvip": "192.168.138.209",
            "mvipNodeID": 1,
            "name": "Marshall",
            "repCount": 2,
            "svip": "10.10.7.209",
            "svipNodeID": 1,
            "uniqueID": "91dt"
      }
   }
}
```


버전 이후 새로운 기능

9.6

자세한 내용을 확인하십시오

- "SecureEraseDrives"
- "GetClusterInfo 를 참조하십시오"
- "SolidFire 및 Element 소프트웨어 설명서"
- "이전 버전의 NetApp SolidFire 및 Element 제품에 대한 문서"

GetClientCertificateSignRequest 를 참조하십시오

"GetClientCertificateSignRequest" 메서드를 사용하면 인증 기관이 클러스터의 클라이언트 인증서를 생성하는 데 서명할 수 있는 인증서 서명 요청을 생성할 수 있습니다. 서명된 인증서는 외부 서비스와 상호 작용하기 위한 신뢰 관계를 설정하는 데 필요합니다.

매개 변수

이 메서드에는 입력 매개 변수가 없습니다.

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형
clientCertificateSignRequest 를 참조하십시오	PEM 형식 Base64 인코딩된 PKCS #10 X.509 클라이언트 인증서 서명 요청	문자열

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {
        "clientCertificateSignRequest":
"MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
   }
}
```

버전 이후 새로운 기능

11.7

GetKeyProviderKmip 을 참조하십시오

"GetKeyProviderKmip" 메서드를 사용하여 지정된 KMIP(Key Management Interoperability Protocol) 키 공급자에 대한 정보를 검색할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderID를 입력합니다	KMIP 키 공급자 객체의 반환 ID입니다.	정수	없음	예

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형
KmipKeyProvider 를 참조하십시오	요청된 키 공급자에 대한 세부 정보가 포함된 개체입니다.	"키ProviderKmip 을 참조하십시오"

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "GetKeyProviderKmip",
  "params": {
    "keyProviderID": 15
    },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProvider": {
        "keyProviderID": 15,
        "kmipCapabilities": "SSL",
        "keyProviderIsActive": true,
        "keyServerIDs": [
            1
        ],
        "keyProviderName": "ProviderName"
    }
   }
}
```

버전 이후 새로운 기능

11.7

GetKeyServerKmip 을 참조하십시오

"GetKeyServerKmip" 메서드를 사용하면 지정된 KMIP(Key Management Interoperability Protocol) 키 서버에 대한 정보를 반환할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyServerID를 입력합니다	정보를 반환할 KMIP 키 서버의 ID입니다.	정수	없음	예

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형
KmipKeyServer를 참조하십시오	요청된 키 서버에 대한 세부 정보가 포함된 개체입니다.	"KeyServerKmip"

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "GetKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":15
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
    }
}
```

버전 이후 새로운 기능

11.7

GetSoftwareEncryptionAtRestInfo 를 참조하십시오

"GetSoftwareEncryptionAtRestInfo" 메서드를 사용하면 유휴 데이터를 암호화하는 데 클러스터에서 사용하는 유휴 소프트웨어 암호화 정보를 가져올 수 있습니다.

매개 변수

이 메서드에는 입력 매개 변수가 없습니다.

반환 값

이 메서드의 반환 값은 다음과 같습니다.

매개 변수	설명	유형	선택 사항
마스터키정보	현재 소프트웨어 암호화 - 유휴 상태 마스터 키에 대한 정보입니다.	암호화키정보	참
rekeyMasterKeyAsyncResultID 를 참조하십시오	아직 삭제되지 않은 경우 현재 또는 최근 키를 다시 입력하다 GetAsyncResult 출력에는 새 마스터 키에 대한 정보가 들어 있는 newKey 필드와 이전 키에 대한 정보가 들어 있는 keyToDecommission 필드가 포함됩니다.	정수	참
상태	현재 소프트웨어 유휴 데이터의 암호화 상태입니다. 가능한 값은 비활성화 또는 활성화 입니다.	문자열	거짓
버전	저장된 소프트웨어 암호화가 활성화될 때마다 증가하는 버전 번호입니다.	정수	거짓

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
 "method": "getsoftwareencryptionatrestinfo"
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
    "id": 1,
    "result": {
        "masterKeyInfo": {
            "keyCreatedTime": "2021-09-20T23:15:56Z",
            "keyID": "4d80a629-a11b-40ab-8b30-d66dd5647cfd",
            "keyManagementType": "internal"
        },
        "state": "enabled",
        "version": 1
    }
}
```

버전 이후 새로운 기능

12.3

자세한 내용을 확인하십시오

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

ListKeyProvidersKmip 을 참조하십시오

"ListKeyProvidersKmip" 방법을 사용하여 기존의 모든 KMIP(Key Management Interoperability Protocol) 키 공급자 목록을 검색할 수 있습니다. 추가 매개 변수를 지정하여 목록을 필터링할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderIsActive 를 참조하십시오	필터가 활성 여부에 따라 KMIP 주요 서버 객체를 반환했습니다. 가능한 값: • 참: KMIP 키 공급자만 사용 (현재 사용 중인 키 제공)합니다. • False: 비활성화된 KMIP 키 공급자만 반환합니다(키를 제공하지 않고 삭제할 수 있음). 이 인수를 생략하면 KMIP 키 공급자가 활성 상태인지 여부를 기준으로 필터링되지 않습니다.	부울	없음	아니요
KmipKeyProviderHasServerAsSigned 를 참조하십시오	필터가 KMIP 키 서버가 할당되었는지 여부를 기준으로 KMIP 키 공급자를 반환했습니다. 가능한 값: • 참: KMIP 키 서버가 할당된 KMIP 키 공급자만 반환합니다. • False: KMIP 키 서버가 할당되지 않은 KMIP 키 공급자만 반환합니다. 이 인수를 생략하면 KMIP 키 서버가 할당되었는지 여부를 기준으로 KMIP 키 공급자가 반환되었습니다.	부울	없음	아니요

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형
KmipKeyProviders 를 참조하십시오	KMIP 키 공급자 목록이 생성되었습니다.	"키ProviderKmip 을 참조하십시오" 스토리지

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "ListKeyProvidersKmip",
  "params": {},
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProviders": [
        {
            "keyProviderID": 15,
            "kmipCapabilities": "SSL",
            "keyProviderIsActive": true,
            "keyServerIDs": [
                1
            ],
            "keyProviderName": "KeyProvider1"
        }
    ]
}
}
```

버전 이후 새로운 기능

11.7

ListKeyServersKmip 를 참조하십시오

'ListKeyServersKmip' 방법을 사용하여 생성된 모든 KMIP(Key Management Interoperability Protocol) 키 서버를 나열할 수 있습니다. 추가 매개 변수를 지정하여 결과를 필터링할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderID를 입력합니다	이 방법을 지정하면 지정된 KMIP 키 공급자에 할당된 KMIP 키 서버만 반환됩니다. 이 인수를 생략하면 KMIP 키 서버가 지정된 KMIP 키 공급자에 할당되었는지 여부에 따라 반환되는 KMIP 키 서버가 필터링되지 않습니다.	정수	없음	아니요
KmipAssignedProviderIsActive 를 참조하십시오	필터가 활성 여부에 따라 KMIP 주요 서버 객체를 반환했습니다. 가능한 값: • 참: KMIP 키 서버가 활성화된 경우에만 반환합니다(현재 사용 중인 키를 제공). • False: 비활성화된 KMIP 키 서버만 반환합니다(키를 제공하지 않고 삭제할 수 있음). 이 인수를 생략하면 KMIP 키 서버가 활성 상태인지 여부를 기준으로 필터링되지 않습니다.	부울	없음	아니요

이름	설명	유형	기본값	필수 요소입니다
KmipHasProviderAssigned 를 참조하십시오	필터가 KMIP 키 공급자가 할당되어 있는지 여부를 기준으로 KMIP 키 서버를 반환했습니다. 가능한 값: • 참: KMIP 키 공급자가 할당된 KMIP 키 서버만 반환합니다. • False: KMIP 키 공급자가 할당되지 않은 KMIP 키 서버만 반환합니다. 이 인수를 생략하면 KMIP 키 서버가 할당되어 있는지 여부에 따라 KMIP 키 서버가 필터링되지 않습니다.	부울	없음	아니요

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형
KmipKeyServers를 선택합니다	KMIP 키 서버가 생성된 전체 목록입니다.	"KeyServerKmip" 스토리지

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "ListKeyServersKmip",
  "params": {},
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
    "kmipKeyServers": [
        {
            "kmipKeyServerName": "keyserverName",
            "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "keyServerID": 15,
            "kmipAssignedProviderIsActive": true,
            "kmipKeyServerPort": 5696,
            "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames": [
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID": 1
        }
    ]
}
```

버전 이후 새로운 기능

11.7

ModifyKeyServerKmip

ModifyKeyServerKmip 방식을 사용하여 기존 KMIP(Key Management Interoperability Protocol) 키 서버를 지정된 속성으로 수정할 수 있습니다. 유일하게 필요한 매개 변수는 keyServerID이지만 keyServerID만 포함하는 요청은 아무런 조치를 취하지 않고 오류가 발생하지 않습니다. 지정하는 다른 모든 매개 변수는 키 서버의 기존 값을 지정된 keyServerID로 바꿉니다. 작동 중에 키 서버가 제대로 작동하는지 확인하기 위해 키 서버에 접촉합니다. kmipKeyServerHostnames 매개 변수를 사용하여 호스트 이름 또는 IP 주소를 여러 개 제공할 수 있지만 키 서버가 클러스터 구성에 있는 경우에만 가능합니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyServerID를 입력합니다	수정할 KMIP Key Server의 ID입니다.	정수	없음	예

KmipCaCertificate입니다	외부 키 서버의 루트 CA의 공개 키 인증서입니다. TLS 통신에서 외부 키 서버가 제공하는 인증서를 확인하는 데 사용됩니다. 개별 서버가 서로 다른 CA를 사용하는 키 서버 클러스터의 경우 모든 CA의 루트 인증서가 포함된 연결된 문자열을 제공합니다.	문자열	없음	아니요
kmipClientCertificate를 참조하십시오	SolidFire KMIP 클라이언트가 사용하는 PEM 형식 Base64 인코딩된 PKCS #10 X.509 인증서.	문자열	없음	아니요
kmipKeyServerHostName입니다	이 KMIP 키 서버와 연관된 호스트 이름 또는 IP 주소의 배열입니다. 키 서버가 클러스터 구성에 있는 경우에만 호스트 이름 또는 IP 주소를 여러 개 제공해야 합니다.	문자열 배열	없음	아니요
kmipKeyServerName입니다	KMIP 키 서버의 이름입니다. 이 이름은 표시 목적으로만 사용되며 고유한 이름은 필요하지 않습니다.	문자열	없음	아니요
kmipKeyServerPort를 참조하십시오	이 KMIP 키 서버와 연관된 포트 번호 (일반적으로 5696)	정수	없음	아니요

반환 값

이 메서드의 반환 값은 다음과 같습니다.

이름	설명	유형

KmipKeyServer를 참조하십시오	새로 수정된 키 서버에 대한 세부 정보가 포함된 개체입니다.	"KeyServerKmip"

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":1
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"kirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
    }
}
```

RekeySoftwareEncryptionAtRestMasterKey를 참조하십시오

"RekeySoftwareEncryptionAtRestMasterKey" 메서드를 사용하여 DEK(데이터 암호화 키)를 암호화하는 데 사용되는 소프트웨어 암호화 유휴 마스터 키를 다시 설정할 수 있습니다. 클러스터를 생성하는 동안 저장된 소프트웨어 암호화는 IKM(내부 키 관리)을 사용하도록 구성됩니다. 이 키를 다시 입력하다 IKM 또는 EKM(외부 키 관리)을 사용하려면 클러스터를 생성한 후 이 방법을 사용할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다. keyManagementType 매개 변수가 지정되지 않은 경우 기존 키 관리 구성을 사용하여 키를 다시 입력하다 keyManagementType을 지정하고 key provider가 external인 경우 keyProviderID 매개 변수도 사용해야 합니다.

매개 변수	설명	유형	선택 사항
키 관리유형	마스터 키를 관리하는 데 사용되는 키 관리 유형입니다. 가능한 값은 '내부': 내부 키 관리를 사용하여 키를 다시 입력합니다. 외부 키 관리 기능을 사용하여 키를 다시 누릅니다. 이 매개 변수를 지정하지 않으면 기존 키 관리 구성을 사용하여 키를 다시 입력하다	문자열	참
KeyProviderID를 입력합니다	사용할 키 공급자의 ID입니다. 이 값은 CreateKeyProvider 메서드 중 하나로 반환되는 고유 값입니다. keyManagementType이 External인 경우에만 ID가 필요하며, 그렇지 않으면 유효하지 않습니다.	정수	참

반환 값

이 메서드의 반환 값은 다음과 같습니다.

매개 변수	설명	유형	선택 사항
asyncHandle	GetAsyncResult 로 이 asyncHandle 값을 사용하여 키를 다시 입력하다 GetAsyncResult 출력에는 새 마스터 키에 대한 정보가 들어 있는 newKey 필드와 이전 키에 대한 정보가 들어 있는 keyToDecommission 필드가 포함됩니다.	정수	거짓

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

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

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
    "asyncHandle": 1
}
```

버전 이후 새로운 기능

12.3

자세한 내용을 확인하십시오

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

RemoveKeyServerFromProviderKmip 를 참조하십시오

"RemoveKeyServerFromProviderKmip" 메서드를 사용하여 지정된 공급자에서 지정된

KMIP(Key Management Interoperability Protocol) 키 서버를 할당 해제할 수 있습니다. 키 서버가 마지막 서버이고 해당 공급자가 활성 상태인 경우(현재 사용 중인 키 제공)가 아닌 경우 해당 공급자에서 키 서버의 할당을 취소할 수 있습니다. 지정된 키 서버가 공급자에 할당되지 않은 경우 아무런 작업도 수행되지 않으며 오류가 반환되지 않습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyServerID를 입력합니다	할당을 취소할 KMIP 키 서버의 ID입니다.	정수	없음	예

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 반환되지 않는 한 제거가 성공한 것으로 간주됩니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "RemoveKeyServerFromProviderKmip",
  "params": {
    "keyServerID": 1
   },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {}
    }
}
```

버전 이후 새로운 기능

11.7

TestKeyProviderKmip 을 참조하십시오

'TestKeyProviderKmip' 메서드를 사용하여 지정된 KMIP(Key Management Interoperability Protocol) 키 공급자에 연결할 수 있고 정상적으로 작동하는지 테스트할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyProviderID를 입력합니다	테스트할 키 공급자의 ID입니다.	정수	없음	예

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 반환되지 않는 한 테스트가 성공한 것으로 간주됩니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "TestKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {}
    }
}
```

버전 이후 새로운 기능

11.7

TestKeyServerKmip

'TestKeyServerKmip' 방법을 사용하여 지정된 KMIP(Key Management Interoperability Protocol) 키 서버에 연결할 수 있고 정상적으로 작동하는지 테스트할 수 있습니다.

매개 변수

이 메서드에는 다음과 같은 입력 매개 변수가 있습니다.

이름	설명	유형	기본값	필수 요소입니다
KeyServerID를 입력합니다	테스트할 KMIP 키 서버의 ID입니다.	정수	없음	예

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 반환되지 않으면 테스트가 성공한 것으로 간주됩니다.

요청 예

이 메서드에 대한 요청은 다음 예제와 비슷합니다.

```
{
  "method": "TestKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
"id": 1
}
```

응답 예

이 메서드는 다음 예제와 유사한 응답을 반환합니다.

```
{
   "id": 1,
   "result":
      {}
    }
```

버전 이후 새로운 기능

11.7