보안 API 메서드

Element Software

NetApp
November 18, 2025

목차

보안 API 메서드

AddKeyServerToProviderKmip

당신은 사용할 수 있습니다 `AddKeyServerToProviderKmip` 지정된 키 공급자에게 키 관리 상호 운용성 프로토콜(KMIP) 키 서버를 할당하는 방법입니다. 할당하는 동안 서버에 연락하여 기능을 확인합니다. 지정된 키 서버가 지정된 키 공급자에게 이미 할당된 경우 아무런 조치도 취해지지 않으며 오류도 반환되지 않습니다. 다음을 사용하여 할당을 제거할 수 있습니다. `RemoveKeyServerFromProviderKmip` 방법.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 제공자 ID	키 서버를 할당할 키 공급자의 ID입니다.	정수	None	예
키서버ID	할당할 키 서버의 ID입니다.	정수	None	예

반환 값

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

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

CreateKeyProviderKmip

당신은 사용할 수 있습니다 `CreateKeyProviderKmip` 지정된 이름으로 KMIP(Key Management Interoperability Protocol) 키 공급자를 생성하는 방법입니다. 키 제공자는 인증 키를 검색하는 메커니즘과 위치를 정의합니다. 새로운 KMIP 키 공급자를 생성하면 해당 공급자에 할당된 KMIP 키 서버가 없습니다. KMIP 키 서버를 생성하려면 다음을 사용하세요. `CreateKeyServerKmip` 방법. 공급자에게 할당하려면 다음을 참조하세요. `AddKeyServerToProviderKmip` .

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 공급자 이름	생성된 KMIP 키 공급자와 연결할 이름입니다. 이 이름은 표시 목적으로만 사용되며 고유할 필요는 없습니다.	끈	None	예

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
kmipKeyProvider	새로 생성된 키 공급자에 대한 세부 정보가 포함된 객체입니다.	"키프로바이더Kmip"

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

CreateKeyServerKmip

당신은 사용할 수 있습니다 `CreateKeyServerKmip` 지정된 속성을 사용하여 KMIP(Key Management Interoperability Protocol) 키 서버를 생성하는 방법입니다. 생성 중에 서버에 접속하지 않습니다. 이 방법을 사용하기 전에 서버가 존재할 필요는 없습니다. 클러스터형 키 서버 구성의 경우 kmipKeyServerHostnames 매개변수에 모든 서버 노드의 호스트 이름이나 IP 주소를 제공해야 합니다. 당신은 사용할 수 있습니다 `TestKeyServerKmip` 키 서버를 테스트하는 방법.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
kmipCa증명서	외부 키 서버의 루트 CA의 공개 키 인증서입니다. 이는 TLS 통신에서 외부 키 서버가 제시한 인증서를 검증하는 데 사용됩니다. 개별 서버가 서로 다른 CA를 사용하는 주요 서버 클러스터의 경우 모든 CA의 루트 인증서가 포함된 연결된 문자열을 제공합니다.	끈	None	예
kmip클라이언트 인증서	Solidfire KMIP 클라이언트에서 사용하는 PEM 형식의 Base64 인코딩된 PKCS#10 X.509 인증서입니다.	끈	None	예
kmipKeyServer호스트 이름	이 KMIP 키 서버와 연결된 호스트 이름 또는 IP 주소의 배열입니다. 여러 호스트 이름이나 IP 주소는 키 서버가 클러스터 구성에 있는 경우에만 제공해야 합니다.	문자열 배열	None	예
kmipKeyServerNam e	KMIP 키 서버의 이름입니다. 이 이름은 표시 목적으로만 사용되며 고유할 필요는 없습니다.	끈	None	예
kmipKeyServerPort	이 KMIP 키 서버와 연결된 포트 번호 (일반적으로 5696).	정수	None	아니요

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
kmipKeyServer	새로 생성된 키 서버에 대한 세부 정보가 포함된 객체입니다.	"키서버Kmip"

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 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
        }
    }
}
```

버전 이후 새로운

11.7

공개 개인 키 쌍 생성

당신은 사용할 수 있습니다 `CreatePublicPrivateKeyPair` 공개 및 개인 SSL 키를 생성하는 방법. 이러한 키를 사용하여 인증서 서명 요청을 생성할 수 있습니다. 각 스토리지 클러스터에는 하나의 키 쌍만 사용할 수 있습니다. 이 방법을 사용하여 기존 키를 교체하기 전에 해당 키를 다른 공급자가 더 이상 사용하지 않는지 확인하세요.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
일반 이름	X.509 고유 이름 일반 이름 필드(CN).	끈	None	아니요
국가	X.509 고유 이름 국가 필드©.	끈	None	아니요
이메일 주소	X.509 고유 이름 이메일 주소 필드(MAIL).	끈	None	아니요
소재지	X.509 고유 이름 지역 이름 필드(L).	끈	None	아니요
조직	X.509 고유 이름 조직 이름 필드(O).	끈	None	아니요
조직 단위	X.509 고유 이름 조직 단위 이름 필드(OU).	끈	None	아니요
상태	X.509 고유 이름 주 또는 도 이름 필드(ST 또는 SP 또는 S).	끈	None	아니요

반환 값

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

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

DeleteKeyProviderKmip

당신은 사용할 수 있습니다 `DeleteKeyProviderKmip` 지정된 비활성 키 관리 상호 운용성 프로토콜(KMIP) 키 공급자를 삭제하는 방법입니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 제공자 ID	삭제할 키 공급자의 ID입니다.	정수	None	예

반환 값

이 메서드에는 반환 값이 없습니다. 오류가 발생하지 않는 한 삭제 작업은 성공한 것으로 간주됩니다.

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

DeleteKeyServerKmip

당신은 사용할 수 있습니다 `DeleteKeyServerKmip` 기존 키 관리 상호 운용성 프로토콜(KMIP) 키 서버를 삭제하는 방법입니다. 마지막으로 공급업체에 할당된 키 서버가 아니고 해당 공급업체가 현재 사용 중인 키를 제공하는 경우가 아니면 키 서버를 삭제할 수 없습니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키서버ID	삭제할 KMIP 키 서버의 ID입니다.	정수	None	예

반환 값

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

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

휴지상태에서 암호화 비활성화

당신은 사용할 수 있습니다 `DisableEncryptionAtRest` 클러스터에 이전에 적용된 암호화를 제거하는 방법 `EnableEncryptionAtRest` 방법. 이 비활성화 방법은 비동기적이며 암호화가 비활성화되기 전에 응답을 반환합니다. 당신은 사용할 수 있습니다 `GetClusterInfo` 프로세스가 완료되었는지 확인하기 위해 시스템을 폴링하는 방법입니다.

- 이 방법을 사용하면 휴면 상태의 소프트웨어 암호화를 비활성화할 수 없습니다. 휴면 상태에서 소프트웨어 암호화를 비활성화하려면 다음이 필요합니다."새로운 클러스터를 생성하다" 휴면 상태에서 소프트웨어 암호화가 비활성화된 상태입니다.
- 클러스터에서 암호화의 현재 상태, 소프트웨어 암호화의 현재 상태 또는 둘 다를 보려면 다음을 사용하세요. "클러스터 정보 가져오기 방법". 당신은 사용할 수 있습니다 `GetSoftwareEncryptionAtRestInfo` "클러스터가 저장 중인 데이터를 암호화하는 데 사용하는 정보를 얻는 방법".

매개변수

이 방법에는 입력 매개변수가 없습니다.

반환 값

이 메서드에는 반환 값이 없습니다.

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

9.6

더 많은 정보를 찾아보세요

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

휴지상태에서 암호화 활성화

당신은 사용할 수 있습니다 `EnableEncryptionAtRest` 클러스터에서 각 노드의 드라이브에 사용되는 암호화 키를 관리할 수 있도록 클러스터에서 저장 시 AES(Advanced Encryption Standard) 256비트 암호화를 활성화하는 방법입니다. 이 기능은 기본적으로 활성화되어 있지 않습니다.

- 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 얻는 방법".
- 이 방법을 사용하면 소프트웨어 암호화가 활성화되지 않습니다. 이것은 다음을 사용해서만 수행할 수 있습니다."클러스터 생성 방법" ~와 함께 `enableSoftwareEncryptionAtRest` 로 설정 `true` .

저장 중 암호화를 활성화하면 클러스터는 클러스터의 각 노드에 있는 드라이브에 대한 암호화 키를 내부적으로 자동으로 관리합니다.

keyProviderID가 지정되면 키 공급자의 유형에 따라 비밀번호가 생성되고 검색됩니다. 이 작업은 일반적으로 KMIP 키 공급자의 경우 KMIP(Key Management Interoperability Protocol) 키 서버를 사용하여 수행됩니다. 이 작업 후 지정된 공급자는 활성 상태로 간주되며 암호화가 비활성화될 때까지 삭제할 수 없습니다. `DisableEncryptionAtRest` 방법.

"-NE"로 끝나는 모델 번호가 있는 노드 유형이 있는 경우 `EnableEncryptionAtRest` 메서드 호출은 "암호화가 허용되지 않습니다."라는 응답과 함께 실패합니다. 클러스터에서 암호화할 수 없는 노드가 감지되었습니다.

클러스터가 실행 중이고 정상 상태일 때만 암호화를 활성화하거나 비활성화해야 합니다. 필요에 따라 원하는 대로 암호화를 활성화하거나 비활성화할 수 있습니다.

이 프로세스는 비동기적으로 진행되며 암호화가 활성화되기 전에 응답을 반환합니다. 당신은 사용할 수 있습니다 `GetClusterInfo` 프로세스가 완료되었는지 확인하기 위해 시스템을 폴링하는 방법입니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 제공자 ID	사용할 KMIP 키 공급자의 ID입니다.	정수	None	아니요

반환 값

이 메서드에는 반환 값이 없습니다.

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 EnableEncryptionAtRest 메서드의 다음 예와 유사한 응답을 반환합니다. 보고할 결과가 없습니다.

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

클러스터에서 휴지 상태 암호화가 활성화되는 동안 GetClusterInfo는 휴지 상태 암호화("encryptionAtRestState")의 상태를 "활성화"로 설명하는 결과를 반환합니다. 휴면 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

9.6

더 많은 정보를 찾아보세요

- "보안 삭제 드라이브"
- "클러스터 정보 가져오기"
- "SolidFire 및 Element 소프트웨어 문서"
- "NetApp SolidFire 및 Element 제품의 이전 버전에 대한 설명서"

클라이언트 인증서 서명 요청 받기

당신은 사용할 수 있습니다 `GetClientCertificateSignRequest` 클러스터에 대한 클라이언트 인증서를 생성하기 위해 인증 기관에서 서명할 수 있는 인증서 서명 요청을 생성하는 방법입니다. 외부 서비스와 상호 작용하기 위한 신뢰 관계를 구축하려면 서명된 인증서가 필요합니다.

매개변수

이 방법에는 입력 매개변수가 없습니다.

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
클라이언트 인증서 서명 요청	PEM 형식으로 Base64로 인코딩된 PKCS#10 X.509 클라이언트 인증서 서명 요청입니다.	끈

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

GetKeyProviderKmip

당신은 사용할 수 있습니다 `GetKeyProviderKmip` 지정된 키 관리 상호 운용성 프로토콜(KMIP) 키 공급자에 대한 정보를 검색하는 방법입니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 제공자 ID	반환할 KMIP 키 공급자 개체의 ID입니다.	정수	None	예

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
kmipKeyProvider	요청된 키 공급자에 대한 세부 정보가 포함된 개체입니다.	"키프로바이더Kmip"

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

GetKeyServerKmip

당신은 사용할 수 있습니다 `GetKeyServerKmip` 지정된 KMIP(Key Management Interoperability Protocol) 키 서버에 대한 정보를 반환하는 방법입니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키서버ID	정보를 반환할 KMIP 키 서버의 ID입니다.	정수	None	예

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
kmipKeyServer	요청된 키 서버에 대한 세부 정보가 포함된 개체입니다.	"키서버Kmip"

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 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

11.7

GetSoftwareEncryptionAtRestInfo

당신은 사용할 수 있습니다 `GetSoftwareEncryptionAtRestInfo` 클러스터가 저장 데이터를 암호화하는 데 사용하는 저장 데이터 암호화 정보를 얻는 방법입니다.

매개변수

이 방법에는 입력 매개변수가 없습니다.

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

매개변수	설명	유형	선택 과목
마스터키정보	현재 소프트웨어 암호화 마스터 키에 대한 정보입니다.	암호화 키 정보	진실
rekeyMasterKeyAsyncResultID	아직 삭제되지 않은 경우 현재 또는 가장 최근의 재키 작업의 비동기 결과 ID입니다(있는 경우). `GetAsyncResult` 출력에는 다음이 포함됩니다. `newKey` 새 마스터 키에 대한 정보가 포함된 필드 `keyToDecommission` 이전 키에 대한 정보가 포함된 필드입니다.	정수	진실
상태	현재 소프트웨어 암호화 상태입니다. 가능한 값은 다음과 같습니다. `disabled` 또는 `enabled` .	끈	거짓
버전	휴면 상태의 소프트웨어 암호화가 활성화될 때마다 증가하는 버전 번호입니다.	정수	거짓

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 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

12.3

더 많은 정보를 찾아보세요

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

ListKeyProvidersKmip

당신은 사용할 수 있습니다 `ListKeyProvidersKmip` 기존의 모든 키 관리 상호 운용성 프로토콜(KMIP) 키 공급자 목록을 검색하는 방법입니다. 추가 매개변수를 지정하여 목록을 필터링할 수 있습니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 공급자가 활성화되었습니다	필터는 활성화 여부에 따라 KMIP 키 서버 객체를 반환했습니다. 가능한 값: • true: 활성화된 KMIP 키 공급자만 반환합니다(현재 사용 중인 키 제공). • false: 비활성 상태(키를 제공하지 않고 삭제 가능)인 KMIP 키 공급자만 반환합니다. 생략하면 반환된 KMIP 키 공급자는 활성화 여부에 따라 필터링되지 않습니다.	부울	None	아니요
kmipKeyProviderHasServerAssigned	KMIP 키 서버가 할당되었는지 여부에 따라 KMIP 키 공급자를 필터링하여 반환했습니다. 가능한 값: • true: KMIP 키 서버가 할당된 KMIP 키 공급자만 반환합니다. • false: KMIP 키 서버가 할당되지 않은 KMIP 키 공급자만 반환합니다. 생략하면 반환된 KMIP 키 공급자는 KMIP 키 서버가 할당되었는지 여부에 따라 필터링되지 않습니다.	부울	None	아니요

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
kmipKeyProviders	생성된 KMIP 키 공급자 목록입니다.	"키프로바이더Kmip"정렬

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

ListKeyServersKmip

당신은 사용할 수 있습니다 `ListKeyServersKmip` 생성된 모든 키 관리 상호 운용성 프로토콜(KMIP) 키 서버를 나열하는 방법입니다. 추가 매개변수를 지정하여 결과를 필터링할 수 있습니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 제공자 ID	이 옵션을 지정하면 해당 메서드는 지정된 KMIP 키 공급자에 할당된 KMIP 키 서버만 반환합니다. 생략하면 반환된 KMIP 키 서버는 지정된 KMIP 키 공급자에 할당되었는지 여부에 따라 필터링되지 않습니다.	정수	None	아니요
kmipAssignedProviderIsActive	필터는 활성화 여부에 따라 KMIP 키 서버 객체를 반환했습니다. 가능한 값: • true: 활성화된 KMIP 키 서버만 반환합니다(현재 사용 중인 키 제공). • false: 비활성 상태(키를 제공하지 않고 삭제 가능)인 KMIP 키 서버만 반환합니다. 생략하면 반환된 KMIP 키 서버는 활성화 여부에 따라 필터링되지 않습니다.	부울	None	아니요

이름	설명	유형	기본값	필수의
kmipHasProviderAssigned	필터는 KMIP 키 공급자가 할당되었는지 여부에 따라 KMIP 키 서버를 반환했습니다. 가능한 값: • true: KMIP 키 공급자가 할당된 KMIP 키 서버만 반환합니다. • false: KMIP 키 공급자가 할당되지 않은 KMIP 키 서버만 반환합니다. 생략하면 반환된 KMIP 키 서버는 KMIP 키 공급자가 할당되었는지 여부에 따라 필터링되지 않습니다.	부울	None	아니요

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
kmipKeyServers	생성된 KMIP 키 서버의 전체 목록입니다.	"키서버Kmip"정렬

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 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

11.7

ModifyKeyServerKmip

당신은 사용할 수 있습니다 `ModifyKeyServerKmip` 기존 키 관리 상호 운용성 프로토콜(KMIP) 키 서버를 지정된 속성으로 수정하는 방법입니다. 유일하게 필요한 매개변수는 keyServerID이지만, keyServerID만 포함된 요청은 아무런 작업도 수행하지 않고 오류도 반환하지 않습니다. 지정한 다른 매개변수는 키 서버의 기존 값을 지정된 keyServerID로 대체합니다. 작업 중에 주요 서버에 접속하여 제대로 작동하는지 확인합니다. kmipKeyServerHostnames 매개변수를 사용하여 여러 호스트 이름이나 IP 주소를 제공할 수 있지만, 키 서버가 클러스터 구성에 있는 경우에만 가능합니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키서버ID	수정할 KMIP 키 서버의 ID입니다.	정수	None	예

kmipCa증명서	외부 키 서버의 루트 CA의 공개 키 인증서입니다. 이는 TLS 통신에서 외부 키 서버가 제시한 인증서를 검증하는 데 사용됩니다. 개별 서버가 서로 다른 CA를 사용하는 주요 서버 클러스터의 경우 모든 CA의 루트 인증서가 포함된 연결된 문자열을 제공합니다.	끈	None	아니요
kmip클라이언트 인증서	Solidfire KMIP 클라이언트에서 사용하는 PEM 형식의 Base64 인코딩된 PKCS#10 X.509 인증서입니다.	끈	None	아니요
kmipKeyServer호스트 이름	이 KMIP 키 서버와 연결된 호스트 이름 또는 IP 주소의 배열입니다. 여러 호스트 이름이나 IP 주소는 키 서버가 클러스터 구성에 있는 경우에만 제공해야 합니다.	문자열 배열	None	아니요
kmipKeyServerName	KMIP 키 서버의 이름입니다. 이 이름은 표시 목적으로만 사용되며 고유할 필요는 없습니다.	끈	None	아니요
kmipKeyServerPort	이 KMIP 키 서버와 연결된 포트 번호(일반적으로 5696).	정수	None	아니요

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형

kmipKeyServer	새로 수정된 키 서버에 대한 세부 정보가 포함된 개체입니다.	"키서버Kmip"

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

```
{
  "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 예시

이 메서드는 다음 예와 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
        }
    }
}
```

버전 이후 새로운

11.7

RekeySoftwareEncryptionAtRestMasterKey

당신은 사용할 수 있습니다 `RekeySoftwareEncryptionAtRestMasterKey` DEK(데이터 암호화 키)를 암호화하는 데 사용되는 소프트웨어 암호화 마스터 키를 다시 키로 사용하는 방법입니다. 클러스터 생성 중에 휴면 상태의 소프트웨어 암호화는 내부 키 관리(IKM)를 사용하도록 구성됩니다. 이 키 변경 방법은 클러스터 생성 후 IKM이나 외부 키 관리(EKM)를 사용하는 데 사용할 수 있습니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다. 만약 `keyManagementType` 매개변수가 지정되지 않으면 기존 키 관리 구성을 사용하여 키 재지정 작업이 수행됩니다. 만약 `keyManagementType` 지정되어 있고 키 공급자가 외부인 경우 `keyProviderID` 매개변수도 사용해야 합니다.

매개변수	설명	유형	선택 과목
키 관리 유형	마스터 키를 관리하는 데 사용되는 키 관리 유형입니다. 가능한 값은 다음과 같습니다. `Internal` : 내부 키 관리를 사용하여 키를 다시 지정합니다. `External` : 외부 키 관리를 사용하여 키를 다시 지정합니다. 이 매개변수가 지정되지 않으면 기존 키 관리 구성을 사용하여 키 재지정 작업이 수행됩니다.	끈	진실
키 제공자 ID	사용할 키 공급자의 ID입니다. 이는 다음 중 하나의 일부로 반환되는 고유한 값입니다. `CreateKeyProvider` 행동 양식. 신분증은 다음과 같은 경우에만 필요합니다. `keyManagementType` ~이다 `External` 그 외에는 무효입니다.	정수	진실

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

매개변수	설명	유형	선택 과목
비동기 핸들	이것을 사용하여 재키 작업의 상태를 확인하십시오. `asyncHandle` 가치와 함께 `GetAsyncResult` . `GetAsyncResult` 출력에는 다음이 포함됩니다. `newKey` 새 마스터 키에 대한 정보가 포함된 필드 `keyToDecommission` 이전 키에 대한 정보가 포함된 필드입니다.	정수	거짓

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

12.3

더 많은 정보를 찾아보세요

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

ProviderKmip에서 KeyServer 제거

당신은 사용할 수 있습니다 `RemoveKeyServerFromProviderKmip` 지정된 키 관리 상호 운용성 프로토콜(KMIP) 키 서버를 할당된 공급자로부터 할당 해제하는 방법입니다. 해당 키 서버가 마지막 키 서버가 아니고 해당 공급자가 활성화되어 있는 경우(현재 사용 중인 키를 제공하는 경우)를 제외하고는 공급자로부터 키 서버의 할당을 해제할 수 있습니다. 지정된 키 서버가 공급자에게 할당되지 않은 경우 아무런 조치도 취해지지 않으며 오류도 반환되지 않습니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키서버ID	할당 해제할 KMIP 키 서버의 ID입니다.	정수	None	예

반환 값

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

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

SignSshKeys

클러스터에서 SSH가 활성화된 후"EnableSSH 메서드" , 당신은 사용할 수 있습니다 `SignSshKeys` 노드의 셸에 접근하는 방법.

Element 12.5부터 시작하여, `sfreadonly` 새로운 시스템 계정을 사용하면 노드에서 기본적인 문제 해결이 가능합니다. 이 API는 다음을 사용하여 SSH 액세스를 활성화합니다. `sfreadonly` 클러스터의 모든 노드에 대한 시스템 계정입니다.

NetApp 지원팀의 별도 안내 없이 시스템을 변경하는 것은 지원되지 않으며, 지원 계약이 무효화되고 데이터 불안정이나 접근 불가 현상이 발생할 수 있습니다.

해당 방법을 사용한 후에는 응답에서 키체인을 복사하여 SSH 연결을 시작할 시스템에 저장한 후 다음 명령을 실행해야 합니다.

```
ssh -i <identity_file> sfreadonly@<node_ip>
```

`identity_file`공개 키 인증을 위한 `ID(개인 키)`를 읽어들이는 파일입니다. `node_ip` 는 노드의 `IP` 주소입니다. 자세한 내용은 `identity_file` `SSH` 매뉴얼 페이지를 참조하세요.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
지속	서명된 키가 유효한 데 걸리는 시간을 나타내는 1~24의 정수입니다. 기간이 지정되지 않으면 기본값이 사용됩니다.	정수	1	아니요

이름	설명	유형	기본값	필수의
공개키	이 매개변수가 제공되면 사용자에게 전체 키체인을 생성하는 대신 signed_public_key만 반환합니다. 브라우저의 URL 표시줄을 사용하여 제출된 공개 키 + 간격을 두고 끊어서 표기하는 것으로 해석됩니다.	끈	널	아니요
sfadmin	supportAdmin 클러스터 액세스로 API 호출을 하거나 노드가 클러스터에 없을 때 sfadmin 셸 계정에 액세스할 수 있도록 허용합니다.	부울	거짓	아니요

반환 값

이 메서드는 다음과 같은 반환 값을 갖습니다.

이름	설명	유형
키젠 상태	서명된 키의 ID, 허용되는 주체, 키의 유효한 시작 및 종료 날짜가 포함되어 있습니다.	끈

이름	설명	유형
개인 키	API가 최종 사용자를 위한 완전한 키체인을 생성하는 경우에만 개인 SSH 키 값이 반환됩니다. 값은 Base64로 인코딩되어 있습니다. 유효한 개인 키로 읽히는지 확인하려면 파일에 쓸 때 값을 디코딩해야 합니다.	끈
공개키	공개 SSH 키 값은 API가 최종 사용자를 위한 완전한 키체인을 생성하는 경우에만 반환됩니다. API 메서드에 public_key 매개변수를 전달하는 경우 `signed_public_key` 응답에서 값이 반환됩니다.	끈
서명된 공개 키	사용자가 제공했거나 API에서 생성한 공개 키에 서명하여 생성되는 SSH 공개 키입니다.	끈

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

```
{
    "method": "SignSshKeys",
    "params": {
        "duration": 2,
        "publicKey":<string>
    },
    "id": 1
}
```

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

```
{
  "id": null,
  "result": {
    "signedKeys": {
      "keygen_status": <keygen_status>,
      "signed_public_key": <signed_public_key>
    }
  }
}
```

이 예에서는 공개 키가 서명되어 유효 기간(1~24시간) 동안 반환됩니다.

버전 이후 새로운

12.5

테스트키공급자Kmip

당신은 사용할 수 있습니다 `TestKeyProviderKmip` 지정된 키 관리 상호 운용성 프로토콜(KMIP) 키 공급자에 접근 가능하고 정상적으로 작동하는지 테스트하는 방법입니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키 제공자 ID	테스트할 키 공급자의 ID입니다.	정수	None	예

반환 값

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

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

테스트키서버Kmip

당신은 사용할 수 있습니다 `TestKeyServerKmip` 지정된 키 관리 상호 운용성 프로토콜(KMIP) 키 서버에 접근 가능하고 정상적으로 작동하는지 테스트하는 방법입니다.

매개변수

이 방법에는 다음과 같은 입력 매개변수가 있습니다.

이름	설명	유형	기본값	필수의
키서버ID	테스트할 KMIP 키 서버의 ID입니다.	정수	None	예

반환 값

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

요청 예시

이 방법에 대한 요청은 다음 예와 유사합니다.

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

응답 예시

이 메서드는 다음 예와 유사한 응답을 반환합니다.

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

버전 이후 새로운

11.7

저작권 정보

상표 정보