セキュリティ**API**メソッド

Element Software

NetApp
November 18, 2025

目次

セキュリティAPIメソッド 1
プロバイダーKmipにキーサーバーを追加 1
パラメータ 1
戻り値 1
リクエスト例 1
応答例 1
バージョン以降の新機能 2
キープロバイダーKmipの作成 2
パラメータ 2
戻り値 2
リクエスト例 3
応答例 3
バージョン以降の新機能 3
キーサーバーKmipの作成 3
パラメータ 4
戻り値 5
リクエスト例 5
応答例 5
バージョン以降の新機能 6
公開鍵ペアの作成 6
パラメータ 6
戻り値 7
リクエスト例 7
応答例 7
バージョン以降の新機能 8
削除キープロバイダーKmip 8
パラメータ 8
戻り値 8
リクエスト例 8
応答例 8
バージョン以降の新機能 9
キーサーバーKmipの削除 9
パラメータ 9
戻り値 9
リクエスト例 9
応答例 10
バージョン以降の新機能 10
保存時の暗号化を無効にする 10
パラメータ 10

戻り値 10
リクエスト例 10
応答例 11
バージョン以降の新機能 11
保存時の暗号化を有効にする 11
パラメータ 12
戻り値 12
リクエスト例 12
応答例 12
バージョン以降の新機能 13
GetClientCertificateSignRequest 14
パラメータ 14
戻り値 14
リクエスト例 14
応答例 14
バージョン以降の新機能 15
GetKeyProviderKmip 15
パラメータ 15
戻り値 15
リクエスト例 15
応答例 15
バージョン以降の新機能 16
GetKeyServerKmip 16
パラメータ 16
戻り値 16
リクエスト例 17
応答例 17
バージョン以降の新機能 17
ソフトウェア暗号化情報を取得する 17
パラメータ 18
戻り値 18
リクエスト例 18
応答例 18
バージョン以降の新機能 19
リストキープロバイダーKmip 19
パラメータ 19
戻り値 21
リクエスト例 21
応答例 22
バージョン以降の新機能 22
リストキーサーバーKmip 22

パラメータ 22
戻り値 24
リクエスト例 24
応答例 25
バージョン以降の新機能 25
キーサーバーKmipの変更 25
パラメータ 26
戻り値 27
リクエスト例 27
応答例 27
バージョン以降の新機能 28
再鍵ソフトウェア暗号化保存マスターキー 28
パラメータ 28
戻り値 29
リクエスト例 29
応答例 30
バージョン以降の新機能 30
プロバイダーKmipからキーサーバーを削除 30
パラメータ 30
戻り値 31
リクエスト例 31
応答例 31
バージョン以降の新機能 31
署名Sshキー 31
パラメータ 32
戻り値 33
リクエスト例 34
応答例 35
バージョン以降の新機能 35
テストキープロバイダーKmip 35
パラメータ 35
戻り値 36
リクエスト例 36
応答例 36
バージョン以降の新機能 36
テストキーサーバーKmip 36
パラメータ 36
戻り値 37
リクエスト例 37
応答例 37
バージョン以降の新機能 37

セキュリティAPIメソッド

プロバイダーKmipにキーサーバーを追加

使用することができます `AddKeyServerToProviderKmip`指定されたキー プロバイダーにキー管理相互運用性プロトコル (KMIP) キー サーバーを割り当てる方法。割り当て中に、サーバーに接続して機能性を確認します。指定されたキー サーバーが指定されたキー プロバイダーにすでに割り当てられている場合、アクションは実行されず、エラーも返されません。割り当てを削除するには、 `RemoveKeyServerFromProviderKmip`方法。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダーID	キー サーバーを割り当てるキー プロバイダーの ID。	integer	なし	はい
キーサーバーID	割り当てるキー サーバーの ID。	integer	なし	はい

戻り値

このメソッドには戻り値はありません。エラーが返されない限り、割り当ては成功したとみなされます。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

キープロバイダーKmipの作成

使用することができます `CreateKeyProviderKmip`指定された名前のキー管理相互運用性プロトコル （KMIP） キー プロバイダーを作成するメソッド。キー プロバイダーは、認証キーを取得するためのメカニズムと場所を定義します。新しい KMIP キー プロバイダーを作成すると、それには KMIP キー サーバーが割り当てられません。KMIPキーサーバーを作成するには、 `CreateKeyServerKmip`方法。プロバイダーに割り当てるには、 `AddKeyServerToProviderKmip 。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダー名	作成された KMIP キー プロバイダーに関連付ける名前。この名前は表示目的でのみ使用され、一意である必要はありません。	string	なし	はい

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
kmipキープロバイダー	新しく作成されたキープロバイダーに関する詳細を含むオブジェクト。	"キープロバイダーKmip"

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

キーサーバー**Kmip**の作成

使用することができます `CreateKeyServerKmip`指定された属性を持つキー管理相互運用性プロトコル (KMIP) キー サーバーを作成する方法。作成中はサーバーに接続されません。このメソッドを使用する前にサーバーが存在している必要はありません。クラスター化されたキー サーバー構成の場合、kmipKeyServerHostnames パラメーターにすべてのサーバー ノードのホスト名または IP アドレスを指定する必要があります。使用することができます `TestKeyServerKmip`キー サーバーをテストする方法。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
kmipCa証明書	外部キー サーバーのルート CA の公開キー証明書。これは、TLS 通信で外部キー サーバーによって提示される証明書を検証するために使用されます。個々のサーバーが異なる CA を使用するキー サーバー クラスターの場合は、すべての CA のルート証明書を含む連結文字列を提供します。	string	なし	はい
kmipクライアント証明書	Solidfire KMIP クライアントで使用される PEM 形式の Base64 エンコードされた PKCS#10 X.509 証明書。	string	なし	はい
kmipキーサーバーホスト名	この KMIP キー サーバーに関連付けられているホスト名または IP アドレスの配列。キー サーバーがクラスター構成になっている場合にのみ、複数のホスト名または IP アドレスを指定する必要があります。	文字列配列	なし	はい
kmipキーサーバー名	KMIP キー サーバーの名前。この名前は表示目的でのみ使用され、一意である必要はありません。	string	なし	はい
kmipキーサーバーポート	この KMIP キー サーバーに関連付けられたポート番号 (通常は 5696)。	integer	なし	いいえ

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
kmipキーサーバー	新しく作成されたキー サーバーの詳細を含むオブジェクト。	"キーサーバーKmip"

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

```
{
   "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
        }
     }
}
```

バージョン以降の新機能

11.7

公開鍵ペアの作成

使用することができます `CreatePublicPrivateKeyPair`公開 SSL キーと秘密 SSL キーを作成する方法。これらのキーを使用して証明書署名要求を生成できます。各ストレージクラスターで使用できるキー ペアは 1 つだけです。この方法を使用して既存のキーを置き換える前に、そのキーがどのプロバイダーでも使用されていないことを確認してください。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
共通名	X.509 識別名 **Common Name** フィールド (CN)。	string	なし	いいえ
国	X.509 識別名 **Country** フィールド©。	string	なし	いいえ

Name	説明	タイプ	デフォルト値	必須
電子メールアドレス	X.509 識別名 電子メール アドレス フィールド (MAIL)。	string	なし	いいえ
地域	X.509 識別名 **Locality Name** フィールド (L)。	string	なし	いいえ
組織	X.509 識別名 組織名 フィールド (O)。	string	なし	いいえ
組織単位	X.509 識別名 組織単位名 フィールド (OU)。	string	なし	いいえ
状態	X.509 識別名 **State** または **Province Name** フィールド (ST またはSPまたはS)。	string	なし	いいえ

戻り値

このメソッドには戻り値はありません。エラーがなければ、キーの作成は成功したとみなされます。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

削除キープロバイダーKmip

使用することができます `DeleteKeyProviderKmip`指定された非アクティブなキー管理相互運用プロトコル (KMIP) キー プロバイダーを削除する方法。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダーID	削除するキープロバイダーの ID。	integer	なし	はい

戻り値

このメソッドには戻り値はありません。エラーがない限り、削除操作は成功したとみなされます。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

キーサーバーKmipの削除

使用することができます `DeleteKeyServerKmip`既存のキー管理相互運用性プロトコル (KMIP) キー サーバーを削除する方法。キー サーバーは、そのプロバイダーに割り当てられた最後のキー サーバーでない限り、またそのプロバイダーが現在使用中のキーを提供している場合を除き、削除できます。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キーサーバーID	削除する KMIP キー サーバーの ID。	integer	なし	はい

戻り値

このメソッドには戻り値はありません。エラーがない場合、削除操作は成功したとみなされます。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

保存時の暗号化を無効にする

使用することができます `DisableEncryptionAtRest`以前にクラスタに適用された暗号化を削除する方法 `EnableEncryptionAtRest`方法。この無効化メソッドは非同期であり、暗号化が無効化される前に応答を返します。使用することができます `GetClusterInfo`プロセスをいつ完了したかを確認するためにシステムをポーリングするメソッド。

- この方法を使用して、保存時のソフトウェア暗号化を無効にすることはできません。保存時のソフトウェア暗号化を無効にするには、"新しいクラスターを作成する"保存時のソフトウェア暗号化は無効です。
- クラスタ上の保存時の暗号化、保存時のソフトウェア暗号化、またはその両方の現在のステータスを表示するには、 "クラスター情報を取得する方法"。使用することができます `GetSoftwareEncryptionAtRestInfo` "保存データを暗号化するためにクラスターが使用する情報を取得する方法"。

パラメータ

このメソッドには入力パラメータはありません。

戻り値

このメソッドには戻り値はありません。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

9.6

詳細情報の参照

- "クラスター情報を取得"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

保存時の暗号化を有効にする

使用することができます `EnableEncryptionAtRest`クラスタ上で保存されている Advanced Encryption Standard (AES) 256 ビット暗号化を有効にして、クラスタが各ノードのドライブに使用される暗号化キーを管理できるようにする方法。この機能は、デフォルトでは有効になっていません。

- クラスタ上の保存時の暗号化および/または保存時のソフトウェア暗号化の現在の状態を確認するには、"クラスター情報を取得する方法" 。使用することができます `GetSoftwareEncryptionAtRestInfo` "保存データを暗号化するためにクラスターが使用する情報を取得する方法"。
- この方法では、保存時のソフトウェア暗号化は有効になりません。これは、"クラスター作成方法"と `enableSoftwareEncryptionAtRest`に設定 `true`。

保存時の暗号化を有効にすると、クラスターはクラスター内の各ノードのドライブの暗号化キーを内部的に自動的に管理します。

keyProviderID が指定されている場合は、キープロバイダーの種類に応じてパスワードが生成され、取得され

ます。これは通常、KMIP キー プロバイダーの場合は、キー管理相互運用性プロトコル (KMIP) キー サーバーを使用して行われます。この操作の後、指定されたプロバイダーはアクティブとみなされ、保存時の暗号化が無効になるまで削除できません。 `DisableEncryptionAtRest`方法。

モデル番号が「-NE」で終わるノードタイプの場合、 `EnableEncryptionAtRest`メソッド呼び出しは失敗し、「暗号化は許可されていません」という応答が返されます。クラスターは暗号化できないノードを検出しました。

暗号化を有効または無効にするのは、クラスターが実行中で正常な状態にある場合のみにしてください。暗号化は、必要に応じていつでも有効または無効にすることができます。

このプロセスは非同期であり、暗号化が有効になる前に応答を返します。使用することができます `GetClusterInfo`プロセスをいつ完了したかを確認するためにシステムをポーリングするメソッド。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダーID	使用する KMIP キープロバイダーの ID。	integer	なし	いいえ

戻り値

このメソッドには戻り値はありません。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、EnableEncryptionAtRest メソッドからの次の例のような応答を返します。報告する結果はありません。

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


クラスターで Encryption at Rest が有効になっている間、GetClusterInfo は Encryption at Rest の状態 ("encryptionAtRestState") を "有効" として記述する結果を返します。保存時の暗号化が完全に有効になると、返される状態は「有効」に変わります。


```
{
   "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"
      }
   }
}
```


バージョン以降の新機能

9.6

詳細情報の参照

- "SecureEraseDrives"
- "クラスター情報を取得"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

GetClientCertificateSignRequest

使用することができます `GetClientCertificateSignRequest`クラスターのクライアント証明書を生成するために、証明機関によって署名できる証明書署名要求を生成する方法。外部サービスと対話するための信頼関係を確立するには、署名された証明書が必要です。

パラメータ

このメソッドには入力パラメータはありません。

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
クライアント証明書署名リクエスト	PEM 形式の Base64 エンコードされた PKCS#10 X.509 クライアント証明書署名要求。	string

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

GetKeyProviderKmip

使用することができます `GetKeyProviderKmip`指定されたキー管理相互運用性プロトコル (KMIP) キー プロバイダーに関する情報を取得するメソッド。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダーID	返される KMIP キープロバイダー オブジェクトの ID。	integer	なし	はい

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
kmipキープロバイダー	要求されたキープロバイダーに関する詳細を含むオブジェクト。	"キープロバイダーKmip"

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

GetKeyServerKmip

使用することができます `GetKeyServerKmip`指定されたキー管理相互運用性プロトコル (KMIP) キー サーバーに関する情報を返すメソッド。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キーサーバーID	情報を返す KMIP キー サーバーの ID。	integer	なし	はい

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
kmipキーサーバー	要求されたキー サーバーの詳細を含むオブジェクト。	"キーサーバーKmip"

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

```
{
   "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
        }
    }
}
```

バージョン以降の新機能

11.7

ソフトウェア暗号化情報を取得する

使用することができます `GetSoftwareEncryptionAtRestInfo`クラスターが保存データの暗号化に使用するソフトウェア保存時暗号化情報を取得する方法。

パラメータ

このメソッドには入力パラメータはありません。

戻り値

このメソッドには次の戻り値があります。

パラメータ	説明	タイプ	オプション
マスターキー情報	現在のソフトウェア保存時暗号化マスター キーに関する情報。	暗号化キー情報	True
再キーマスターキー非同期結果ID	まだ削除されていない場合の、現在のまたは最新のキー再生成操作の非同期結果 ID (存在する場合)。 `GetAsyncResult`出力には `newKey`新しいマスターキーに関する情報と `keyToDecommission`古いキーに関する情報が含まれるフィールド。	integer	True
状態	現在のソフトウェアの保存時暗号化の状態。可能な値は `disabled`または `enabled`。	string	間違い
version	保存時のソフトウェア暗号化が有効になるたびに増加するバージョン番号。	integer	間違い

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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


バージョン以降の新機能

12.3

詳細情報の参照

- "SolidFireおよびElementソフトウェアのドキュメント"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

リストキープロバイダーKmip

使用することができます `ListKeyProvidersKmip`既存のすべてのキー管理相互運用性プロトコル (KMIP) キー プロバイダーのリストを取得するメソッド。追加のパラメータを指定してリストをフィルタリングできます。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダーがアクティブ	返された KMIP キーサーバー オブジェクトを、アクティブかどうかに基づいてフィルターします。有効な値は次のとおりです。 • true: アクティブな KMIP キー プロバイダーのみを返します (現在使用中のキーを提供します)。 • false: 非アクティブな (キーを提供しておらず、削除可能な) KMIP キー プロバイダーのみを返します。 省略した場合、返される KMIP キー プロバイダーは、アクティブかどうかに基づいてフィルター処理されません。	ブーリアン	なし	いいえ

Name	説明	タイプ	デフォルト値	必須
kmipKeyProviderHasServerAssigned	返された KMIP キープロバイダー を、KMIP キー サーバーが割り当てられているかどうかに基づいてフィルターします。有効な値は次のとおりです。 • true: KMIP キー サーバーが割り当てられている KMIP キー プロバイダーのみを返します。 • false: KMIP キー サーバーが割り当てられていない KMIP キー プロバイダーのみを返します。 省略した場合、返される KMIP キー プロバイダー は、KMIP キー サーバーが割り当てられているかどうかに基づいてフィルター処理されません。	ブーリアン	なし	いいえ

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
kmipキープロバイダー	作成された KMIP キープロバイダーのリスト。	"キープロバイダーKmip"配列

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

リストキーサーバーKmip

使用することができます `ListKeyServersKmip`作成されたすべてのキー管理相互運用性プロトコル (KMIP) キー サーバーを一覧表示するメソッド。追加のパラメータを指定して結果をフィルタリングできます。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダーID	指定すると、このメソッドは指定された KMIP キー プロバイダーに割り当てられている KMIP キー サーバーのみを返します。省略した場合、返される KMIP キー サーバーは、指定された KMIP キー プロバイダーに割り当てられているかどうかに基づいてフィルター処理されません。	integer	なし	いいえ
kmip割り当てプロバイダーがアクティブ	返された KMIP キー サーバー オブジェクトを、アクティブかどうかに基づいてフィルターします。有効な値は次のとおりです。 • true: アクティブな KMIP キー サーバーのみを返します (現在使用中のキーを提供します)。 • false: 非アクティブな (キーを提供しておらず、削除可能な) KMIP キー サーバーのみを返します。 省略した場合、返される KMIP キー サーバーはアクティブかどうかに基づいてフィルター処理されません。	ブーリアン	なし	いいえ

Name	説明	タイプ	デフォルト値	必須
kmipプロバイダー割り当て済み	返された KMIP キー サーバーを、KMIP キー プロバイダーが割り当てられているかどうかに基づいてフィルターします。有効な値は次のとおりです。 • true: KMIP キー プロバイダーが割り当てられている KMIP キー サーバーのみを返します。 • false: KMIP キー プロバイダーが割り当てられていない KMIP キー サーバーのみを返します。 省略した場合、返される KMIP キー サーバーは、KMIP キー プロバイダーが割り当てられているかどうかに基づいてフィルター処理されません。	ブーリアン	なし	いいえ

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
kmipキーサーバー	作成された KMIP キー サーバーの完全なリスト。	"キーサーバーKmip"配列

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

キーサーバー**Kmip**の変更

使用することができます `ModifyKeyServerKmip`既存のキー管理相互運用性プロトコル (KMIP) キー サーバーを指定された属性に変更する方法。必須のパラメータは keyServerID のみですが、keyServerID のみを含むリクエストではアクションは実行されず、エラーも返されません。指定するその他のパラメータにより、キー サーバーの既存の値が指定された keyServerID に置き換えられます。操作中にキー サーバーに接続して、キー サーバーが機能しているかどうかを確認します。 kmipKeyServerHostnames パラメータを使用して複数のホスト名または IP アドレスを指定できますが、キー サーバーがクラスター構成になっている場合のみです。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キーサーバーID	変更する KMIP キー サーバーの ID。	integer	なし	はい
kmipCa証明書	外部キー サーバーのルート CA の公開キー証明書。これは、TLS 通信で外部キー サーバーによって提示される証明書を検証するために使用されます。個々のサーバーが異なる CA を使用するキー サーバー クラスターの場合は、すべての CA のルート証明書を含む連結文字列を提供します。	string	なし	いいえ
kmipクライアント証明書	Solidfire KMIP クライアントで使用される PEM 形式の Base64 エンコードされた PKCS#10 X.509 証明書。	string	なし	いいえ
kmipキーサーバーホスト名	この KMIP キー サーバーに関連付けられているホスト名または IP アドレスの配列。キー サーバーがクラスター構成になっている場合にのみ、複数のホスト名または IP アドレスを指定する必要があります。	文字列配列	なし	いいえ
kmipキーサーバー名	KMIP キー サーバーの名前。この名前は表示目的でのみ使用され、一意である必要はありません。	string	なし	いいえ

kmipキーサーバーポート	この KMIP キー サーバーに関連付けられたポート番号 (通常は 5696)。	integer	なし	いいえ

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
kmipキーサーバー	新しく変更されたキー サーバーの詳細を含むオブジェクト。	"キーサーバーKmip"

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

```
{
   "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
        }
     }
}
```

バージョン以降の新機能

11.7

再鍵ソフトウェア暗号化保存マスターキー

使用することができます `RekeySoftwareEncryptionAtRestMasterKey`DEK (データ暗号化キー) の暗号化に使用されるソフトウェア暗号化マスター キーを再生成する方法。クラスターの作成中に、保存時のソフトウェア暗号化は内部キー管理 (IKM) を使用するように構成されます。このキー再生成方法は、クラスターの作成後に IKM または外部キー管理 (EKM) のいずれかを使用するために使用できます。

パラメータ

このメソッドには次の入力パラメータがあります。もし `keyManagementType`パラメータが指定されていない場合、既存のキー管理構成を使用してキー再生成操作が実行されます。もし `keyManagementType`が指定されており、鍵プロバイダーが外部の場合、 `keyProviderID`パラメータも使用する必要があります。

パラメータ	説明	タイプ	オプション
キー管理タイプ	マスター キーを管理するために使用されるキー管理のタイプ。可能な値は次のとおりです。 `Internal` : 内部キー管理を使用してキーを再生成します。 `External` : 外部キー管理を使用してキーを再生成します。このパラメータを指定しない場合は、既存のキー管理構成を使用してキー再生成操作が実行されます。	string	True
キープロバイダーID	使用するキープロバイダーの ID。これは、 `CreateKeyProvider`方法。 IDは次の場合にのみ必要です `keyManagementType`は `External`それ以外の場合は無効です。	integer	True

戻り値

このメソッドには次の戻り値があります。

パラメータ	説明	タイプ	オプション
非同期ハンドル	これを使用してキー再生成操作のステータスを確認します `asyncHandle`価値を持つ `GetAsyncResult`。 `GetAsyncResult`出力には `newKey`新しいマスターキーに関する情報と `keyToDecommission`古いキーに関する情報が含まれるフィールド。	integer	間違い

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

12.3

詳細情報の参照

- "SolidFireおよびElementソフトウェアのドキュメント"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

プロバイダーKmipからキーサーバーを削除

使用することができます `RemoveKeyServerFromProviderKmip`指定されたキー管理相互運用プロトコル (KMIP) キー サーバーを、割り当て先のプロバイダーから割り当て解除する方法。キー サーバーが最後のもので、そのプロバイダーがアクティブ (現在使用中のキーを提供している) でない限り、キー サーバーの割り当てをプロバイダーから解除できます。指定されたキー サーバーがプロバイダーに割り当てられていない場合、アクションは実行されず、エラーも返されません。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キーサーバーID	割り当てを解除する KMIP キー サーバーの ID。	integer	なし	はい

戻り値

このメソッドには戻り値はありません。エラーが返されない限り、削除は成功したとみなされます。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

署名Sshキー

SSHをクラスタ上で有効にした後、"EnableSSHメソッド" 、あなたは `SignSshKeys`ノード上のシェルにアクセスする方法。

要素12.5から、 `sfreadonly`新しいシステム アカウントにより、ノード上の基本的なトラブルシューティングが可能になります。このAPIは、 `sfreadonly`クラスター内のすべてのノードにわたるシステム アカウント。

> NetAppサポートからのアドバイスがない限り、システムへの変更はサポートされず、サポート契約が無効になり、データが不安定になったり、アクセスできなくなる可能性があります。

この方法を使用した後、応答からキーチェーンをコピーし、SSH 接続を開始するシステムに保存して、次のコマンドを実行する必要があります。

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

`identity_file`公開鍵認証のためのID（秘密鍵）が読み取られるファイルであり、`node_ip`ノードの IP アドレスです。詳細については `identity_file`については、SSH のマニュアル ページを参照してください。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
duration	署名されたキーの有効時間数を表す 1 から 24 までの整数。期間が指定されていない場合は、デフォルトが使用されます。	integer	1	いいえ

Name	説明	タイプ	デフォルト値	必須
公開鍵	指定されている場合、このパラメータは、ユーザーに対して完全なキーチェーンを作成するのではなく、signed_public_key のみを返します。 ブラウザのURLバーを使用して送信された公開鍵 `+` スペースとブレークサインとして解釈されます。	string	Null	いいえ
sfadmin	supportAdmin クラスター アクセスを使用して API 呼び出しを行うとき、またはノードがクラスター内にない場合に、sfadmin シェルアカウントへのアクセスを許可します。	ブーリアン	間違い	いいえ

戻り値

このメソッドには次の戻り値があります。

Name	説明	タイプ
キー生成ステータス	署名されたキーの ID、許可されたプリンシパル、およびキーの有効な開始日と終了日が含まれます。	string
秘密鍵	秘密 SSH キー値は、API がエンドユーザー用の完全なキーチェーンを生成する場合にのみ返されます。 値は Base64 でエンコードされているため、有効な秘密キーとして読み取られることを確認するために、ファイルに書き込むときに値をデコードする必要があります。	string
公開鍵	公開 SSH キー値は、API がエンドユーザー用の完全なキーチェーンを生成している場合にのみ返されます。 APIメソッドにpublic_keyパラメータを渡すと、`signed_public_key`応答で値が返されます。	string
署名済み公開鍵	公開キーの署名から得られる SSH 公開キー。ユーザーが提供したものでも、API によって生成されたものでもかまいません。	string

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

この例では、一定期間（1 ～ 24 時間）有効な公開キーが署名され、返されます。

バージョン以降の新機能

12.5

テストキープロバイダーKmip

使用することができます `TestKeyProviderKmip`指定されたキー管理相互運用性プロトコル (KMIP) キー プロバイダーが到達可能であり、正常に機能しているかどうかをテストするメソッド。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キープロバイダーID	テストするキープロバイダーの ID。	integer	なし	はい

戻り値

このメソッドには戻り値はありません。エラーが返されない限り、テストは成功したとみなされます。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

テストキーサーバー**Kmip**

使用することができます `TestKeyServerKmip`指定されたキー管理相互運用性プロトコル (KMIP) キー サーバーが到達可能であり、正常に機能しているかどうかをテストする方法。

パラメータ

このメソッドには次の入力パラメータがあります。

Name	説明	タイプ	デフォルト値	必須
キーサーバーID	テストする KMIP キー サーバーの ID。	integer	なし	はい

戻り値

このメソッドには戻り値はありません。エラーが返されない場合は、テストは成功したとみなされます。

リクエスト例

このメソッドのリクエストは次の例のようになります。

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

応答例

このメソッドは、次の例のような応答を返します。

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

バージョン以降の新機能

11.7

著作権に関する情報

商標に関する情報