セキュリティ **API** メソッド

Element Software

NetApp
October 01, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/element-software-125/api/reference_element_api_addkeyservertoproviderkmip.html on October 01, 2024. Always check docs.netapp.com for the latest.

目次

セキュリティ API メソッド

Element ソフトウェアは、外部キー管理サーバなどの外部セキュリティ関連サービスと統合できます。これらのセキュリティ関連のメソッドを使用して、保存データの暗号化のための外部キー管理などの Element セキュリティ機能を設定できます。

- AddKeyServerToProviderKmip のように指定します
- CreateKeyProviderKmip
- CreateKeyServerKmip のように指定します
- CreatePublicPrivateKeyPair
- DeleteKeyProviderKmip
- DeleteKeyServerKmip
- DisableEncryptionAtRest
- EnableEncryptionAtRest
- GetClientCertificateSignRequest
- GetKeyProviderKmip
- GetKeyServerKmip
- ListKeyProvidersKmip
- ListKeyServersKmip
- ModifyKeyServerKmip のように指定します
- RemoveKeyServerFromProviderKmip
- SigSshKeys
- TestKeyProviderKmip
- TestKeyServerKmip

詳細情報

- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

AddKeyServerToProviderKmip のように指定します

メソッドを使用すると、指定したキープロバイダにKey Management Interoperability Protocol（KMIP）キーサーバを割り当てることができます `AddKeyServerToProviderKmip`。割り当て中に、サーバに接続して機能を確認します。指定したキーサーバが指定したキープロバイダにすでに割り当てられている場合、処理は実行されず、エラーは返されません。メソッドを使用して割り当てを削除できます `RemoveKeyServerFromProviderKmip`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyProviderID	キーサーバを割り当てるキープロバイダの ID 。	整数	なし	はい
KeyServerID	割り当てるキーサーバの ID 。	整数	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かぎり、割り当ては成功したとみなされます。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

CreateKeyProviderKmip

メソッドを使用すると、指定した名前のKey Management Interoperability Protocol（KMIP）キープロバイダを作成できます `CreateKeyProviderKmip`。キープロバイダは、認証キーを取得するメカニズムと場所を定義します。KMIP キープロバイダの新規作成時には、そのプロバイダに割り当てられている KMIP キーサーバはありません。KMIPキーサーバを作成するには、メソッドを使用し `CreateKeyServerKmip`ます。プロバイダに割り当てるには、を参照してください `AddKeyServerToProviderKmip`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyProviderName の略	作成する KMIP キープロバイダに関連付ける名前。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。	文字列	なし	はい

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
kmipKeyProvider のいずれかです	作成されたキープロバイダの詳細を含むオブジェクト。	"KeyProviderKmip"

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

CreateKeyServerKmip のように指定します

メソッドを使用すると、指定した属性を使用してKey Management Interoperability Protocol（KMIP）キーサーバを作成できます `CreateKeyServerKmip`。作成中にサーバに接続されることはありません。このメソッドを使用する前に、サーバが存在している必要はありません。クラスタ化されたキーサーバ設定の場合、すべてのサーバノードのホスト名または IP アドレスを kmipKeyServerHostnames パラメータで指定する必要があります。メソッドを使用すると、キーサーバをテストできます `TestKeyServerKmip`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
kmipCaCertificate	外部キーサーバのルート CA の公開鍵証明書。これは、 TLS 通信で外部キーサーバから提示された証明書を検証するために使用されます。個々のサーバが異なる CA を使用するキーサーバクラスタの場合は、すべての CA のルート証明書を含む連結文字列を指定します。	文字列	なし	はい
kmipClientCertificate	SolidFire KMIP クライアントで使用される PEM 形式 Base64 エンコード PKCS#10 X.509 証明書。	文字列	なし	はい
kmipKeyServerHostName のように指定します	KMIP キーサーバ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。キーサーバがクラスタ構成の場合にのみ、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。	文字列の配列	なし	はい
kmipKeyServerName	KMIP キーサーバの名前。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。	文字列	なし	はい
kmipKeyServerPort の 1 つです	KMIP キーサーバに関連付けられているポート番号（通常は 5696 ）。	整数	なし	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
kmipKeyServer	作成されたキーサーバの詳細を含むオブジェクト。	"KeyServerKmip"

要求例

このメソッドの要求例を次に示します。

```
{
  "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

このメソッドの応答例を次に示します。

```
{
   "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
        }
    }
}
```

新規導入バージョン

11.7

CreatePublicPrivateKeyPair

メソッドを使用すると、SSLの公開鍵と秘密鍵を作成できます `CreatePublicPrivateKeyPair`。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で使用できるキーペアは 1 組だけです。このメソッドを使用して既存のキーを置き換える前に、プロバイダがそのキーを使用していないことを確認してください。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
CommonName （共通名	X.509 識別名 * Common Name * フィールド（ CN ）。	文字列	なし	いいえ
国名	X.509 識別名 * Country * フィールド（ C ）。	文字列	なし	いいえ
E 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（メール）。	文字列	なし	いいえ
ローカリティ	X.509 識別名 *Locality Name * フィールド（ L ）。	文字列	なし	いいえ
組織	X.509 識別名 * 組織名 * フィールド（ O ）。	文字列	なし	いいえ
OrganizationalUnit	X.509 識別名 * 組織単位名 * フィールド（ OU ）。	文字列	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 ）。	文字列	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。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

DeleteKeyProviderKmip

メソッドを使用すると、指定した非アクティブなKey Management Interoperability Protocol（KMIP）キープロバイダを削除できます `DeleteKeyProviderKmip`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyProviderID	削除するキープロバイダの ID 。	整数	なし	はい

戻り値

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

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

DeleteKeyServerKmip

メソッドを使用すると、既存のKey Management Interoperability Protocol（KMIP）キーサーバを削除できます `DeleteKeyServerKmip`。キーサーバは、プロバイダに割り当てられた最後のサーバであり、そのプロバイダが現在使用中のキーを提供していないかぎり、削除できます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyServerID	削除する KMIP キーサーバの ID 。	整数	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。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

DisableEncryptionAtRest

メソッドを使用すると、以前にメソッドを使用してクラスタに適用した暗号化を解除 `EnableEncryptionAtRest`できます `DisableEncryptionAtRest`。このメソッドは非同期で、暗号化が無効になる前に応答を返します。メソッドを使用すると、シス

テムをポーリングしてプロセスがいつ完了したかを確認できます `GetClusterInfo`。

クラスタ上の保存データの暗号化または保存データのソフトウェア暗号化の現在のステータスを確認するには、を使用し"クラスタ情報メソッドを取得します"ます。を使用できます `GetSoftwareEncryptionAtRestInfo` "クラスタが保存データの暗号化に使用する情報を取得する方法"。

このメソッドを使用して保存データのソフトウェア暗号化を無効にすることはできません。保存データのソフトウェア暗号化を無効にするには、保存データのソフトウェア暗号化を無効にする必要があり"新しいクラスタを作成します。"ます。

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

このメソッドには戻り値はありません。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

9.6

詳細情報

- "GetClusterInfo を使用します"

- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

EnableEncryptionAtRest

メソッドを使用すると、クラスタの保存データのAdvanced Encryption Standard（AES）256ビット暗号化を有効にして、各ノードのドライブで使用される暗号化キーをクラスタで管理できるようになります `EnableEncryptionAtRest`。この機能はデフォルトでは有効になっていません。

クラスタ上の保存データの暗号化または保存データのソフトウェア暗号化の現在のステータスを確認するには、を使用し"クラスタ情報メソッドを取得します"ます。を使用できます `GetSoftwareEncryptionAtRestInfo` "クラスタが保存データの暗号化に使用する情報を取得する方法"。

この方法では、保存データのソフトウェア暗号化は有効になりません。これは、をに設定した `true`場合に `enableSoftwareEncryptionAtRest`のみ実行でき"クラスタメソッドを作成します"ます。

保存データの暗号化を有効にすると、クラスタ内の各ノードのドライブについて、暗号化キーがクラスタ内部で自動的に管理されます。

keyProviderID を指定すると、キープロバイダのタイプに応じてパスワードが生成され、取得されます。KMIP キープロバイダの場合は、通常 Key Management Interoperability Protocol （ KMIP ）キーサーバが使用されます。この処理の実行後、指定したプロバイダはアクティブとみなされ、メソッドを使用して保存データの暗号化を無効にするまで削除できません `DisableEncryptionAtRest`。

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「Encryption not allowed」という応答で失敗します。Cluster detected non-encryptable node. 」という応答で失敗します。

暗号化を有効または無効にできるのは、クラスタが正常な状態で稼働している場合のみです。必要に応じて、必要に応じて暗号化を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。メソッドを使用すると、システムをポーリングしてプロセスがいつ完了したかを確認できます `GetClusterInfo`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyProviderID	使用する KMIP キープロバイダの ID 。	整数	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。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの EnableEncryptionAtRest メソッドの応答例を次に示します。レポートする結果はありません。

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

GetClusterInfo でクラスタの保存データの暗号化を有効にしている間、保存データの暗号化の状態（「 encryptionAtRestState 」）は「 enabling 」と出力されます。保存データの暗号化の有効化が完了すると、返される状態は「 enabled 」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"
      }
   }
}
```


新規導入バージョン

9.6

詳細情報

- "SecureEraseDrives"
- "GetClusterInfo を使用します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

GetClientCertificateSignRequest

メソッドを使用すると、認証局による署名が可能な証明書署名要求を生成してクラスタのクライアント証明書を生成できます `GetClientCertificateSignRequest`。署名付き証明書は、外部サービスとの通信における信頼関係を確立するために必要です。

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

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
clientCertificateSignRequest	PEM 形式 Base64 エンコード PKCS#10 X.509 クライアント証明書の署名要求。	文字列

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

GetKeyProviderKmip

メソッドを使用すると、指定したKey Management Interoperability Protocol（KMIP）キープロバイダの情報を取得できます `GetKeyProviderKmip`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyProviderID	取得する KMIP キープロバイダオブジェクトの ID 。	整数	なし	はい

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
kmipKeyProvider のいずれかです	要求されたキープロバイダの詳細を含むオブジェクト。	"KeyProviderKmip"

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

GetKeyServerKmip

メソッドを使用すると、指定したKey Management Interoperability Protocol（KMIP）キーサーバの情報を取得できます `GetKeyServerKmip`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyServerID	情報を返す KMIP キーサーバの ID 。	整数	なし	はい

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
kmipKeyServer	要求されたキーサーバの詳細を含むオブジェクト。	"KeyServerKmip"

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

```
{
   "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
        }
    }
}
```

新規導入バージョン

11.7

GetSoftwareEncryptionAtRestInfo

メソッドを使用すると、ソフトウェアで保存データの暗号化にクラスタで使用される保存データ暗号化情報を取得できます `GetSoftwareEncryptionAtRestInfo`。

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

このメソッドの戻り値は次のとおりです。

パラメータ	製品説明	タイプ	オプション
masterKeyInfo の順に選択します	現在のソフトウェア保存データ暗号化マスターキーに関する情報。	EncryptionKeyInfo	正しい
rekeyMasterKeyAsyncResultID	現在または最新のキー変更処理（存在する場合）の非同期結果ID（まだ削除されていない場合）。 `GetAsyncResult`出力には、新しいマスターキーに関する情報を含むフィールドと、 `keyToDecommission`古いキーに関する情報を含むフィールドが含まれ `newKey`ます。	整数	正しい
状態	現在のソフトウェアの保存データの暗号化状態。指定できる値は `disabled`、または `enabled`です。	文字列	正しくない
バージョン	保存データのソフトウェア暗号化が有効になるたびに増分されるバージョン番号。	整数	正しくない

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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


新規導入バージョン

12.3

詳細情報

- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

ListKeyProvidersKmip

メソッドを使用すると、既存のすべてのKey Management Interoperability Protocol（KMIP）キープロバイダのリストを取得できます `ListKeyProvidersKmip`。追加のパラメータを指定することで、リストをフィルタリングできます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
keyProviderIsActive	アクティブかどうかでフィルタリングした KMIP キーサーバオブジェクトを返します。有効な値： • true ：アクティブな（現在使用中のキーを提供している） KMIP キープロバイダのみを返します。 • false ：非アクティブな（いずれのキーも提供せず、削除可能な） KMIP キープロバイダのみを返します。 省略すると、返される KMIP キープロバイダは、アクティブかどうかでフィルタリングされません。	ブーリアン	なし	いいえ

名前	製品説明	タイプ	デフォルト値	必須
kmipKeyProviderHasServer の署名	割り当てられた KMIP キーサーバがあるかどうかでフィルタリングされた KMIP キープロバイダが返されます。有効な値： • true ：割り当てられた KMIP キーサーバがある KMIP キープロバイダのみを返します。 • false ：割り当てられた KMIP キーサーバがない KMIP キープロバイダのみを返します。 省略すると、返される KMIP キープロバイダは、割り当てられた KMIP キーサーバがあるかどうかでフィルタリングされません。	ブーリアン	なし	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
kmipKeyProviders のマニュアルページです	作成された KMIP キープロバイダのリスト。	"KeyProviderKmip"アレイ

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

ListKeyServersKmip

メソッドを使用すると `ListKeyServersKmip`、作成されたすべてのKey Management Interoperability Protocol（KMIP）キーサーバをリストできます。追加のパラメータを指定することで、結果をフィルタリングできます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyProviderID	このメソッドを指定すると、指定した KMIP キープロバイダに割り当てられている KMIP キーサーバのみが返されます。省略すると、返される KMIP キーサーバは、指定した KMIP キープロバイダに割り当てられているかどうかでフィルタリングされません。	整数	なし	いいえ
kmipAssignedProviderIsActive のいずれかです	アクティブかどうかでフィルタリングした KMIP キーサーバオブジェクトを返します。有効な値： • true ：アクティブな（現在使用中のキーを提供している） KMIP キーサーバのみを返します。 • false ：非アクティブな（いずれのキーも提供せず、削除可能な） KMIP キーサーバのみを返します。 省略すると、返される KMIP キーサーバはアクティブかどうかでフィルタリングされません。	ブーリアン	なし	いいえ

名前	製品説明	タイプ	デフォルト値	必須
kmipHasProviderAssigned の一つです	割り当てられた KMIP キープロバイダがあるかどうかでフィルタリングされた KMIP キーサーバが返されます。有効な値： • true ：割り当てられた KMIP キープロバイダがある KMIP キーサーバのみを返します。 • false ：割り当てられた KMIP キープロバイダがない KMIP キーサーバのみを返します。 省略すると、返される KMIP キーサーバは、割り当てられた KMIP キープロバイダがあるかどうかでフィルタリングされません。	ブーリアン	なし	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
kmipKeyServers	作成された KMIP キーサーバの完全なリスト。	"KeyServerKmip"アレイ

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

ModifyKeyServerKmip のように指定します

メソッドを使用すると、既存のKey Management Interoperability Protocol（KMIP）キーサーバを指定した属性に変更できます `ModifyKeyServerKmip`。必須パラメータは keyServerID だけですが、 keyServerID のみを含む要求は処理を行いません。エラーは返されません。その他のパラメータを指定すると、キーサーバの既存の値が、指定したキーサーバ ID で置き換えられます。キーサーバは、機能していることを確認するために、処理中に接続されます。複数のホスト名または IP アドレスを指定するには、kmipKeyServerHostnames パラメータを使用します。ただし、キーサーバがクラスタ構成の場合にのみ指定できます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyServerID	変更する KMIP キーサーバの ID 。	整数	なし	はい
kmipCaCertificate	外部キーサーバのルート CA の公開鍵証明書。これは、 TLS 通信で外部キーサーバから提示された証明書を検証するために使用されます。個々のサーバが異なる CA を使用するキーサーバクラスタの場合は、すべての CA のルート証明書を含む連結文字列を指定します。	文字列	なし	いいえ
kmipClientCertificate	SolidFire KMIP クライアントで使用される PEM 形式 Base64 エンコード PKCS#10 X.509 証明書。	文字列	なし	いいえ
kmipKeyServerHostName のように指定します	KMIP キーサーバ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。キーサーバがクラスタ構成の場合にのみ、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。	文字列の配列	なし	いいえ
kmipKeyServerName	KMIP キーサーバの名前。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。	文字列	なし	いいえ

kmipKeyServerPort の 1 つです	KMIP キーサーバに関連付けられているポート番号（通常は 5696 ）。	整数	なし	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
kmipKeyServer	変更されたキーサーバの詳細を含むオブジェクト。	"KeyServerKmip"

要求例

このメソッドの要求例を次に示します。

```
{
  "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

このメソッドの応答例を次に示します。

```
{
   "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
        }
     }
}
```

新規導入バージョン

11.7

RekeySoftwareEncryptionAtRestMasterKey

メソッドを使用すると、DEK（データ暗号化キー）の暗号化に使用するソフトウェアの保存データ暗号化マスターキーのキーを変更できます `RekeySoftwareEncryptionAtRestMasterKey`。クラスタ作成時に、保存データのソフトウェア暗号化が内部キー管理（ IKM ）を使用するように設定されます。このキー再生成方法は、クラスタの作成後に IKM または外部キー管理（ EKM ）を使用するために使用できます。

パラメータ

このメソッドの入力パラメータは次のとおりです。パラメータを指定しない場合 `keyManagementType`、既存のキー管理設定を使用してキー変更処理が実行されます。を指定し、キープロバイダが外部の場合は `keyManagementType`、 `keyProviderID`パラメータも使用する必要があります。

パラメータ	製品説明	タイプ	オプション
keyManagementType をクリックします	マスターキーの管理に使用されるキー管理のタイプ。有効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変更します。 `External`:外部キー管理を使用してキーを変更します。このパラメータを指定しない場合は、既存のキー管理設定を使用してキー変更処理が実行されます。	文字列	正しい
KeyProviderID	使用するキープロバイダの ID 。これは、いずれかのメソッドの一部として返される一意の値です `CreateKeyProvider`。IDは、がで `External`ない場合にのみ必要で、それ以外の場合 `keyManagementType`は無効です。	整数	正しい

戻り値

このメソッドの戻り値は次のとおりです。

パラメータ	製品説明	タイプ	オプション
asyncHandle	この値をに指定して `GetAsyncResult`、キー変更処理のステータスを確認します `asyncHandle`。 `GetAsyncResult`出力には、新しいマスターキーに関する情報を含むフィールドと、 `keyToDecommission`古いキーに関する情報を含むフィールドが含まれ `newKey`ます。	整数	正しくない

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

12.3

詳細情報

- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

RemoveKeyServerFromProviderKmip

メソッドを使用すると、指定したKey Management Interoperability Protocol（KMIP）キーサーバを割り当て先のプロバイダから解除できます `RemoveKeyServerFromProviderKmip`。キーサーバが最後のサーバであり、そのプロバイダがアクティブ（現在使用中のキーを提供している）でないかぎり、プロバイダからキーサーバの割り当てを解除できます。指定したキーサーバがプロバイダに割り当てられていない場合、処理は実行されず、エラーは返されません。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyServerID	割り当てを解除する KMIP キーサーバの ID 。	整数	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かぎり、削除は成功したとみなされます。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

SigSshKeys

を使用してクラスタでSSHを有効にする"EnableSSHメソッド"と、メソッドを使用してノードのシェルにアクセスできます `SignSshKeys`。

Element 12.5以降では、 `sfreadonly`新しいシステムアカウントでノードの基本的なトラブルシューティングを実行できます。このAPIを使用すると、クラスタ内のすべてのノードで、システムアカウントを使用したSSHアクセスが可能になり `sfreadonly`ます。

> ネットアップサポートから指示されないかぎり、システムに対する変更はサポートされず、サポート契約にも取り消しが含まれ、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。

メソッドを使用した後、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から、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`は、公開鍵認証用のID（秘密鍵）の読み取り元のファイルで、はノードのIPアドレスです。 `node_ip`詳細については `identity_file`、SSHのマニュアルページを参照してください。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
期間	符号付きキーが有効である時間数を示す1～24の整数。durationを指定しなかった場合は、デフォルト値が使用されます。	整数	1	いいえ

名前	製品説明	タイプ	デフォルト値	必須
publickey	このパラメータを指定すると、ユーザに完全なキーチェーンを作成するのではなく、signed_public_keyのみが返されます。 を使用してブラウザでURLバーを使用して送信された公開鍵 `+` は、スペース署名およびブレーク署名として解釈されます。	文字列	ヌル	いいえ
sfadmin	supportAdminクラスタアクセスを使用してAPI呼び出しを行う場合、またはノードがクラスタにない場合に、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	正しくない	いいえ

戻り値

このメソッドの戻り値は次のとおりです。

名前	製品説明	タイプ
keygen_statusのように入力します	署名付きキーのID、許可されているプリンシパル、およびキーの有効な開始日と終了日が含まれます。	文字列
private_key を使用します	プライベートSSHキーの値は、APIがエンドユーザ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。 値はBase64でエンコードされます。値がファイルに書き込まれるときに値をデコードして、有効な秘密鍵として読み取られるようにする必要があります。	文字列
公開鍵	公開SSHキーの値は、APIがエンドユーザ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パラメータを渡した場合、応答では値のみが `signed_public_key` 返されます。	文字列
signed_public_key	ユーザが指定したか生成したかに関係なく、公開鍵への署名で生成されたSSH公開鍵。	文字列

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

この例では、期間（1～24時間）に有効な公開鍵が署名され、返されます。

新規導入バージョン

12.5

TestKeyProviderKmip

メソッドを使用すると、指定したKey Management Interoperability Protocol（KMIP）キープロバイダが到達可能で、正常に機能しているかどうかをテストでき`TestKeyProviderKmip`ます。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyProviderID	テストするキープロバイダの ID 。	整数	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かぎり、テストは成功したとみなされます。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

TestKeyServerKmip

メソッドを使用すると、指定したKey Management Interoperability Protocol（KMIP）キーサーバが到達可能で正常に機能しているかどうかをテストできます `TestKeyServerKmip`。

パラメータ

このメソッドの入力パラメータは次のとおりです。

名前	製品説明	タイプ	デフォルト値	必須
KeyServerID	テストする KMIP キーサーバの ID 。	整数	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、テストは成功したとみなされます。

要求例

このメソッドの要求例を次に示します。

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

応答例

このメソッドの応答例を次に示します。

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

新規導入バージョン

11.7

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。