外部キー管理の開始

Element Software

NetApp
October 01, 2024

目次

外部キー管理の開始 1
外部キー管理をセットアップする 1
保存マスターキーでのソフトウェア暗号化のキーを変更します 2
アクセス不可または無効な認証キーをリカバリします 4
外部キー管理 API コマンド 5

外部キー管理の開始

外部キー管理（ EKM ）は、クラスタ外の外部キーサーバ（ EKS ）と連携して、安全な認証キー（ AK ）管理を実現します。AKは、クラスタでが有効になっている場合に、自己暗号化ドライブ（SED）のロックとロック解除に使用され"保存データの暗号化"ます。EKS を使用することで、 AK の安全な生成と保管が可能になります。クラスタは、 OASIS で定義された標準プロトコルである Key Management Interoperability Protocol （ KMIP ）を使用して、 EKS と通信します。

- "外部管理をセットアップする"
- "保存マスターキーでのソフトウェア暗号化のキーを変更します"
- "アクセス不可または無効な認証キーをリカバリします"
- "外部キー管理 API コマンド"

詳細情報

- "CreateCluster API ：保存データのソフトウェア暗号化を有効にすることができます"
- "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"

外部キー管理をセットアップする

以下の手順に従い、リストされている Element API メソッドを使用して外部キー管理機能を設定できます。

必要なもの

- 外部キー管理と保存データのソフトウェア暗号化を組み合わせて設定する場合は、ボリュームが含まれていない新しいクラスタで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有効にしておきます"クラスタの作成"。

手順

1. 外部キーサーバ（ EKS ）との信頼関係を確立します。
   a. 次のAPIメソッドを呼び出して、キーサーバとの信頼関係の確立に使用するElementクラスタの公開鍵と秘密鍵のペアを作成します。"CreatePublicPrivateKeyPair"
   b. 認証局が署名する必要がある証明書署名要求（ CSR ）を取得します。CSR によって、キーサーバはキーにアクセスする Element クラスタが Element クラスタとして認証されていることを確認できます。次のAPIメソッドを呼び出します。"GetClientCertificateSignRequest"
   c. EKS と認証局を使用して、取得した CSR に署名します。詳細については、サードパーティのドキュメントを参照してください。
2. クラスタにサーバとプロバイダを作成して、 EKS と通信します。キープロバイダはキーを取得する場所を定義し、サーバは通信する EKS の特定の属性を定義します。
   a. 次のAPIメソッドを呼び出して、キーサーバの詳細を格納するキープロバイダを作成します。"CreateKeyProviderKmip"

b. 次のAPIメソッドを呼び出して、署名済み証明書と認証局の公開鍵証明書を提供するキーサーバを作成します。"CreateKeyServerKmip のように指定します" "TestKeyServerKmip"

   テストに失敗した場合は、サーバの接続と設定を確認します。その後、テストを繰り返します。

c. 次のAPIメソッドを呼び出して、キーサーバをキープロバイダコンテナに追加します。"AddKeyServerToProviderKmip のように指定します" "TestKeyProviderKmip"

   テストに失敗した場合は、サーバの接続と設定を確認します。その後、テストを繰り返します。

3. 保存データの暗号化の次の手順として、次のいずれかを実行します。

   a. （保存データのハードウェア暗号化の場合）"保存データのハードウェア暗号化"APIメソッドを呼び出して、キーの格納に使用するキーサーバを含むキープロバイダのIDを指定します"EnableEncryptionAtRest"。

   > で保存データの暗号化を有効にする必要があります"API"。既存の Element UI ボタンを使用して保存データの暗号化を有効にすると、原因機能で内部で生成されたキーの使用に戻ります。

   b. （保存データのソフトウェア暗号化の場合）新しく作成されたキープロバイダを利用するに"ソフトウェアによる保存データの暗号化"は、キープロバイダIDをAPIメソッドに渡します"RekeySoftwareEncryptionAtRestMasterKey"。

詳細情報

- "クラスタの暗号化を有効または無効にします"
- "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"

保存マスターキーでのソフトウェア暗号化のキーを変更します

Element API を使用して既存のキーを変更できます。このプロセスにより、外部キー管理サーバ用の新しい交換用マスターキーが作成されます。マスターキーは常に新しいマスターキーに置き換えられ、複製や上書きは行われません。

次のいずれかの手順で、キーの変更が必要になることがあります。

- 内部キー管理から外部キー管理への変更の一環として、新しいキーを作成します。
- セキュリティ関連イベントに対する応答または保護として、新しいキーを作成します。

> このプロセスは非同期で、キー変更処理が完了す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"GetAsyncResult"。

必要なもの

- ボリュームがなくI/Oもない新しいクラスタで、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有効にした"クラスタの作成"。続行する前に、link:../api/reference_element_api_getsoftwareencryptionatrestinfo.htmlを使用して[`GetSoftwareEncryptionatRestInfo`状態がであることを確認し `enabled`てください。

- SolidFireクラスタと外部キーサーバ（EKS）の間に配置しておき"信頼関係を確立しました"ます。メソッドを実行し"TestKeyProviderKmip"て、キープロバイダへの接続が確立されたことを確認します。

手順

1. コマンドを実行し"ListKeyProvidersKmip"てキープロバイダID(`keyProviderID`をコピーします）。
2. 前の手順で取得したキープロバイダのID番号として、パラメータにとを `keyProviderID`指定 `external`し `keyManagementType`てを実行し"RekeySoftwareEncryptionAtRestMasterKey"ます。

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

3. コマンド応答から値 `RekeySoftwareEncryptionAtRestMasterKey`をコピーし `asyncHandle`ます。
4. 前の手順の値を指定してコマンドを `asyncHandle`実行し"GetAsyncResult"、設定の変更を確認します。コマンド応答から、古いマスターキー設定が新しいキー情報で更新されたことがわかります。新しいキープロバイダ ID をコピーして以降の手順で使用します。

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. コマンドを実行し `GetSoftwareEncryptionatRestInfo`て、新しいキーの詳細（を含む）が更新されたことを確認します `keyProviderID。

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

詳細情報

- "Element API を使用してストレージを管理します"
- "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"

アクセス不可または無効な認証キーをリカバリします

場合によっては、ユーザの介入を必要とするエラーが発生することがあります。エラーが発生すると、クラスタ障害（クラスタ障害コードと呼ばれる）が生成されます。ここでは、最も可能性の高い 2 つのケースについて説明します。

「 **KmipServerFault** 」クラスタエラーが原因で、クラスタがドライブのロックを解除できません。

これは、クラスタの初回ブート時にキーサーバにアクセスできないか、必要なキーを使用できない場合に発生します。

1. クラスタ障害コードのリカバリ手順に従います（該当する場合）。

メタデータドライブが障害としてマークされ、「 **Available** 」状態になっているため、 **sliceServiceUnhealthy** エラーが表示される場合があります。

クリアする手順：

1. ドライブを再度追加します。

2. 3～4分後に、故障が解消したことを確認します `sliceServiceUnhealthy`。

詳細については、を参照してください "クラスタ障害コード" 。

外部キー管理 API コマンド

EKM の管理と設定に使用できるすべての API のリストです。

クラスタと外部の顧客所有サーバ間の信頼関係を確立するために使用されます。

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

外部の顧客所有サーバの具体的な詳細を定義するために使用されます。

- CreateKeyServerKmip のように指定します
- ModifyKeyServerKmip のように指定します
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

外部キーサーバを管理するキープロバイダの作成と保守に使用されます。

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip のように指定します
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

APIメソッドの詳細については、を参照してください"API リファレンス情報"。

著作権に関する情報

商標に関する情報