外部キー管理を始める
Element Software

NetApp
November 12, 2025

目次

外部キー管理を始める

外部キー管理を始める

外部キー管理 (EKM) は、クラスター外の外部キー サーバー (EKS) と連携して、安全な認証キー (AK) 管理を提供します。 AKは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ます。"保存時の暗号化"クラスターで有効になっています。 EKS は、AK の安全な生成と保存を提供します。クラスターは、OASIS が定義した標準プロトコルであるキー管理相互運用性プロトコル (KMIP) を使用して EKS と通信します。

- "外部管理を設定する"
- "保存時のソフトウェア暗号化マスターキーの再キー化"
- "アクセスできない、または無効な認証キーを回復する"
- "外部キー管理APIコマンド"

詳細情報の参照

- "保存時のソフトウェア暗号化を有効にするために使用できる CreateCluster API"
- "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"

外部キー管理を設定する

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。

要件

- 保存時のソフトウェア暗号化と組み合わせて外部キー管理を設定する場合は、保存時のソフトウェア暗号化を次のように有効にする必要があります。"CreateCluster"ボリュームを含まない新しいクラスター上のメソッド。

手順

1. 外部キー サーバー (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 サーバーとの信頼関係を確立するために使用される Element クラスターの公開キー/秘密キー ペアを作成します。"公開鍵ペアの作成"
   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 により、キー サーバーは、キーにアクセスする Element クラスターが Element クラスター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/証明機関を使用して、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. EKS と通信するために、クラスター上にサーバーとプロバイダーを作成します。キープロバイダーはキーを取得する場所を定義し、サーバーは通信する 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 サーバーの詳細が保存されるキー プロバイダーを作成します。"キープロバイダーKmipの作成"

b. 次の API メソッドを呼び出して、署名付き証明書と証明機関の公開鍵証明書を提供するキー サーバーを作成します。"キーサーバーKmipの作成" "テストキーサーバーKmip"

   テストが失敗した場合は、サーバーの接続と構成を確認してください。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 サーバーをキー プロバイダー コンテナーに追加します。"プロバイダーKmipにキーサーバーを追加" "テストキープロバイダーKmip"

   テストが失敗した場合は、サーバーの接続と構成を確認してください。その後、テストを繰り返します。

3. 保存時の暗号化の次のステップとして、次のいずれかを実行します。

a. （保存時のハードウェア暗号化の場合）有効にする"保存時のハードウェア暗号化"鍵を保存するために使用する鍵サーバーを含む鍵プロバイダーのIDを指定して、"保存時の暗号化を有効にする" API メソッド。

   保存時の暗号化を有効にするには、"API" 。既存の Element UI ボタンを使用して保存時の暗号化を有効にすると、機能は内部で生成されたキーを使用するようになります。

b. （保存時のソフトウェア暗号化の場合）"保存時のソフトウェア暗号化"新しく作成されたキープロバイダーを利用するには、キープロバイダーIDを"再鍵ソフトウェア暗号化保存マスターキー"API メソッド。

詳細情報の参照

- "クラスターの暗号化を有効または無効にする"
- "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"

保存時のソフトウェア暗号化マスターキーの再キー化

Element API を使用して既存のキーを再設定できます。このプロセスにより、外部キー管理サーバー用の新しい交換マスター 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、複製または上書きされることはありません。

次のいずれかの手順の一環として、キーの再設定が必要になる場合があります。

- 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。
- セキュリティ関連のイベントへの対応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あり、キー再生成操作が完了する前に応答を返します。使用することができます"非同期結果を取得する"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。

要件

- 保存時のソフトウェア暗号化を有効にしました。"CreateCluster"ボリュームを含まず、I/O もない新しいクラスター上のメソッド。リンクを使用してください:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] 状態を確認するには `enabled`続行する前に。
- あなたが持っている"信頼関係を築いた"SolidFireクラスターと外部キー サーバー (EKS) 間。実行"テストキープロバイダーKmip"キープロバイダーへの接続が確立されていることを確認する方法。

手順

1. 実行"リストキープロバイダーKmip"コマンドを実行してキープロバイダーIDをコピーします（`keyProviderID`）。
2. 実行"再鍵ソフトウェア暗号化保存マスターキー"と `keyManagementType`パラメータとして `external`そして `keyProviderID`前のステップのキープロバイダーのID番号として:

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

3. コピー `asyncHandle`からの価値 `RekeySoftwareEncryptionAtRestMasterKey`コマンド応答。
4. 実行"非同期結果を取得する"コマンドを `asyncHandle`前の手順の値を確認して、構成の変更を確認します。コマンド応答から、古いマスター キー構成が新しいキー情報で更新されたことがわかります。後の手順で使用するために、新しいキープロバイダー ID をコピーします。

```
{
   "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. 実行 `GetSoftwareEncryptionatRestInfo`新しいキーの詳細を確認するコマンド。 `keyProviderID`が更新されました。

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

詳細情報の参照

- "Element APIでストレージを管理する"
- "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"

アクセスできない、または無効な認証キーを回復する

場合によっては、ユーザーの介入が必要なエラーが発生することがあります。エラーが発生した場合、クラスター障害 (クラスター障害コードと呼ばれる) が生成されます。最も可能性の高い 2 つのケースをここで説明します。

KmipServerFault クラスター障害のため、クラスターはドライブのロックを解除できません。

これは、クラスターが最初に起動し、キー サーバーにアクセスできない場合、または必要なキーが利用できない場合に発生する可能性があります。

1. クラスター障害コード (存在する場合) の回復手順に従います。

メタデータ ドライブが障害ありとしてマークされ、「使用可能」状態になっているため、**sliceServiceUnhealthy** 障害が設定されている可能性があります。

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、 `sliceServiceUnhealthy`障害は解消されました。

見る"クラスター障害コード"詳細についてはこちらをご覧ください。

外部キー管理APIコマンド

EKM の管理と構成に使用できるすべての API のリスト。

クラスターと外部の顧客所有サーバー間の信頼関係を確立するために使用されます。

- 公開鍵ペアの作成
- GetClientCertificateSignRequest

外部顧客所有サーバーの具体的な詳細を定義するために使用されます。

- キーサーバーKmipの作成
- キーサーバーKmipの変更
- キーサーバーKmipの削除
- GetKeyServerKmip
- リストキーサーバーKmip

- テストキーサーバーKmip

外部キー サーバーを管理するキー プロバイダーの作成と管理に使用されます。

- キープロバイダーKmipの作成
- 削除キープロバイダーKmip
- プロバイダーKmipにキーサーバーを追加
- プロバイダーKmipからキーサーバーを削除
- GetKeyProviderKmip
- リストキープロバイダーKmip
- 再鍵ソフトウェア暗号化保存マスターキー
- テストキープロバイダーKmip

APIメソッドの詳細については、以下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