Erste Schritte zur externen Schlüsselverwaltung

Element Software

NetApp
November 12, 2025

Inhalt

Erste Schritte zur externen Schlüsselverwaltung

Erste Schritte zur externen Schlüsselverwaltung

Externes Schlüsselmanagement (EKM) ermöglicht die sichere Verwaltung von Authentifizierungsschlüsseln (AK) in Verbindung mit einem externen Schlüsselserver (EKS) außerhalb des Clusters. Die AKs werden verwendet, um selbstverschlüsselnde Laufwerke (SEDs) zu sperren und zu entsperren, wenn"Verschlüsselung im Ruhezustand" ist auf dem Cluster aktiviert. Das EKS gewährleistet die sichere Generierung und Speicherung der AKs. Der Cluster nutzt das Key Management Interoperability Protocol (KMIP), ein von OASIS definiertes Standardprotokoll, um mit dem EKS zu kommunizieren.

- "Externes Management einrichten"
- "Rekey-Software-Verschlüsselung ruhender Masterschlüssel"
- "Unzugängliche oder ungültige Authentifizierungsschlüssel wiederherstellen"
- "API-Befehle für die externe Schlüsselverwaltung"

Weitere Informationen

- "Die CreateCluster-API kann verwendet werden, um die Softwareverschlüsselung ruhender Daten zu aktivieren."
- "SolidFire und Element-Softwaredokumentation"
- "Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte"

Einrichtung der externen Schlüsselverwaltung

Sie können diese Schritte befolgen und die aufgeführten Element-API-Methoden verwenden, um Ihre externe Schlüsselverwaltungsfunktion einzurichten.

Was du brauchst

- Wenn Sie die externe Schlüsselverwaltung in Kombination mit der Softwareverschlüsselung ruhender Daten einrichten, haben Sie die Softwareverschlüsselung ruhender Daten mithilfe von … aktiviert."CreateCluster" Methode auf einem neuen Cluster, der keine Volumes enthält.

Schritte

1. Stellen Sie eine Vertrauensbeziehung zum externen Schlüsselserver (EKS) her.
   a. Erstellen Sie ein öffentliches/privates Schlüsselpaar für den Element-Cluster, das zum Aufbau einer Vertrauensbeziehung mit dem Schlüsselserver verwendet wird, indem Sie die folgende API-Methode aufrufen:"Öffentliches/Privates Schlüsselpaar erstellen"
   b. Besorgen Sie sich die Zertifikatsignieranforderung (CSR), die die Zertifizierungsstelle unterzeichnen muss. Der CSR ermöglicht es dem Schlüsselserver zu überprüfen, ob der Elementcluster, der auf die Schlüssel zugreifen soll, als Elementcluster authentifiziert ist. Rufen Sie die folgende API-Methode auf:"GetClientCertificateSignRequest"
   c. Verwenden Sie die EKS/Zertifizierungsstelle, um den abgerufenen CSR zu signieren. Weitere Informationen finden Sie in der Dokumentation von Drittanbietern.

2. Erstellen Sie einen Server und einen Provider auf dem Cluster, um mit dem EKS zu kommunizieren. Ein Schlüsselanbieter legt fest, wo ein Schlüssel bezogen werden soll, und ein Server definiert die spezifischen Attribute des EKS, mit denen kommuniziert werden soll.
   a. Erstellen Sie einen Schlüsselanbieter, in dem die Details des Schlüsselservers gespeichert werden, indem Sie die folgende API-Methode aufrufen:"CreateKeyProviderKmip"
   b. Erstellen Sie einen Schlüsselserver, der das signierte Zertifikat und das öffentliche Schlüsselzertifikat der Zertifizierungsstelle bereitstellt, indem Sie die folgenden API-Methoden aufrufen:"CreateKeyServerKmip" "TestKeyServerKmip"

      Falls der Test fehlschlägt, überprüfen Sie Ihre Serververbindung und -konfiguration. Wiederholen Sie dann den Test.

   c. Fügen Sie den Schlüsselserver dem Schlüsselanbietercontainer hinzu, indem Sie die folgenden API-Methoden aufrufen:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      Falls der Test fehlschlägt, überprüfen Sie Ihre Serververbindung und -konfiguration. Wiederholen Sie dann den Test.

3. Führen Sie als nächsten Schritt zur Verschlüsselung ruhender Daten einen der folgenden Schritte durch:
   a. (Für Hardwareverschlüsselung ruhender Daten) Aktivieren"Hardwareverschlüsselung im Ruhezustand" indem die ID des Schlüsselanbieters angegeben wird, der den zum Speichern der Schlüssel verwendeten Schlüsselserver enthält, indem die folgende Funktion aufgerufen wird:"EnableEncryptionAtRest" API-Methode.

      > Sie müssen die Verschlüsselung ruhender Daten über die"API" Die Durch Aktivieren der Verschlüsselung ruhender Daten über die vorhandene Element UI-Schaltfläche wird die Funktion auf die Verwendung intern generierter Schlüssel zurückgesetzt.

   b. (Für die Softwareverschlüsselung im Ruhezustand) Damit"Softwareverschlüsselung im Ruhezustand" Um den neu erstellten Schlüsselanbieter zu nutzen, übergeben Sie die Schlüsselanbieter-ID an den"RekeySoftwareEncryptionAtRestMasterKey" API-Methode.

Weitere Informationen

- "Aktivieren und Deaktivieren der Verschlüsselung für einen Cluster"
- "SolidFire und Element-Softwaredokumentation"
- "Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte"

Rekey-Software-Verschlüsselung ruhender Masterschlüssel

Sie können die Element-API verwenden, um einen bestehenden Schlüssel neu zu verschlüsseln. Dieser Prozess erstellt einen neuen Ersatz-Masterschlüssel für Ihren externen Schlüsselverwaltungsserver. Generalschlüssel werden stets durch neue Generalschlüssel ersetzt und niemals dupliziert oder überschrieben.

Möglicherweise müssen Sie im Rahmen eines der folgenden Verfahren die Daten neu eingeben:

- Erstellen Sie einen neuen Schlüssel im Rahmen der Umstellung von interner auf externe Schlüsselverwaltung.

- Erstellen Sie einen neuen Schlüssel als Reaktion auf oder zum Schutz vor einem sicherheitsrelevanten Ereignis.

> Dieser Prozess ist asynchron und liefert eine Antwort, bevor die Schlüsselerneuerung abgeschlossen ist. Sie können die"GetAsyncResult" Methode, um das System abzufragen und festzustellen, wann der Prozess abgeschlossen ist.

Was du brauchst

- Sie haben die Softwareverschlüsselung ruhender Daten mithilfe der folgenden Methode aktiviert:"CreateCluster" Methode auf einem neuen Cluster, der keine Volumes enthält und keine E/A hat. Verwenden Sie den Link:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo` um zu bestätigen, dass der Staat `enabled` vor dem Fortfahren.
- Du hast"eine Vertrauensbeziehung aufgebaut" zwischen dem SolidFire -Cluster und einem externen Schlüsselserver (EKS). Führe die"TestKeyProviderKmip" Methode zur Überprüfung, ob eine Verbindung zum Schlüsselanbieter hergestellt wurde.

Schritte

1. Führe die"ListKeyProvidersKmip" Befehl ausführen und die Schlüsselanbieter-ID kopieren(`keyProviderID`).
2. Führe die"RekeySoftwareEncryptionAtRestMasterKey" mit dem `keyManagementType` Parameter als `external` Und `keyProviderID` als die ID-Nummer des Schlüsselanbieters aus dem vorherigen Schritt:

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

3. Kopiere die `asyncHandle` Wert aus dem `RekeySoftwareEncryptionAtRestMasterKey` Befehlsantwort.
4. Führe die"GetAsyncResult" Befehl mit dem `asyncHandle` Wert aus dem vorherigen Schritt zur Bestätigung der Konfigurationsänderung. Aus der Befehlsantwort sollte ersichtlich sein, dass die ältere Master-Key-Konfiguration mit neuen Schlüsselinformationen aktualisiert wurde. Kopieren Sie die neue Schlüsselanbieter-ID zur Verwendung in einem späteren Schritt.

```
{
   "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. Führe die `GetSoftwareEncryptionatRestInfo` Befehl zur Bestätigung der neuen Schlüsseldetails, einschließlich der `keyProviderID` wurden aktualisiert.

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

Weitere Informationen

- "Speicherverwaltung mit der Element-API"
- "SolidFire und Element-Softwaredokumentation"
- "Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte"

Unzugängliche oder ungültige Authentifizierungsschlüssel wiederherstellen

Gelegentlich kann ein Fehler auftreten, der ein Eingreifen des Benutzers erfordert. Im Fehlerfall wird ein Clusterfehler (auch Clusterfehlercode genannt) generiert. Die beiden wahrscheinlichsten Fälle werden hier beschrieben.

Aufgrund eines KmipServerFault-Clusterfehlers kann der Cluster die Laufwerke nicht entsperren.

Dies kann vorkommen, wenn der Cluster zum ersten Mal hochfährt und der Schlüsselserver nicht erreichbar ist oder der benötigte Schlüssel nicht verfügbar ist.

1. Befolgen Sie die Wiederherstellungsschritte in den Cluster-Fehlercodes (falls vorhanden).

Ein sliceServiceUnhealthy-Fehler kann auftreten, weil die Metadaten-Laufwerke als ausgefallen markiert und in den Status „Verfügbar“ versetzt wurden.

Schritte zur Behebung:

1. Fügen Sie die Laufwerke erneut hinzu.
2. Überprüfen Sie nach 3 bis 4 Minuten, ob `sliceServiceUnhealthy` Die Störung wurde behoben.

Sehen"Cluster-Fehlercodes" für weitere Informationen.

API-Befehle für die externe Schlüsselverwaltung

Liste aller verfügbaren APIs zur Verwaltung und Konfiguration von EKM.

Wird verwendet, um eine Vertrauensbeziehung zwischen dem Cluster und externen, kundeneigenen Servern herzustellen:

- Öffentliches/Privates Schlüsselpaar erstellen
- GetClientCertificateSignRequest

Wird verwendet, um die spezifischen Details externer, kundeneigener Server zu definieren:

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

Wird zur Erstellung und Wartung von Schlüsselanbietern verwendet, die externe Schlüsselserver verwalten:

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Informationen zu den API-Methoden finden Sie unter "API-Referenzinformationen"Die