Erste Schritte mit externem Verschlüsselungsmanagement

Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/de-de/element-software-123/storage/task_system_manage_key_set_up_external_key_management.html on November 19, 2025. Always check docs.netapp.com for the latest.

Inhalt

Erste Schritte mit externem Verschlüsselungsmanagement 1
Externes Verschlüsselungsmanagement einrichten 1
Verschlüsselung der Software beim Rest-Master-Schlüssel 2
Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln 5
Das Cluster kann die Laufwerke nicht entsperren, da ein KmipServerFault-Clusterfehler vorliegt. 5
Es kann ein SliceServiceUnHealthy Fehler gesetzt werden, weil die Metadaten-Laufwerke als fehlgeschlagen markiert und in den Status „verfügbar“ gesetzt wurden. 5
Befehle für externes Verschlüsselungsmanagement-API 5

Erste Schritte mit externem Verschlüsselungsmanagement

EKM (External Key Management) bietet eine sichere Verwaltung des Authentifizierungsschlüssels (AK) in Verbindung mit einem externen EKS-Server (Off-Cluster). Die AKS werden verwendet, um Self-Encrypting Drives (SEDs) zu sperren und zu entsperren "Verschlüsselung für Daten im Ruhezustand" Ist auf dem Cluster aktiviert. Der EKS sorgt für die sichere Erzeugung und Lagerung der AKS. Der Cluster verwendet für die Kommunikation mit dem EKS das Key Management Interoperability Protocol (KMIP), ein OASIS-definiertes Standardprotokoll.

- "Externe Verwaltung einrichten"
- "Verschlüsselung der Software beim Rest-Master-Schlüssel"
- "Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln"
- "Befehle für externes Verschlüsselungsmanagement-API"

Weitere Informationen

- "CreateCluster API, die zur Aktivierung der Softwareverschlüsselung im Ruhezustand verwendet werden kann"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Externes Verschlüsselungsmanagement einrichten

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

Was Sie benötigen

- Wenn Sie externes Verschlüsselungsmanagement in Kombination mit Softwareverschlüsselung im Ruhezustand einrichten, ist die Softwareverschlüsselung im Ruhezustand aktiviert "CreateCluster erstellen" Methode auf einem neuen Cluster, das keine Volumes enthält.

Schritte

1. Bauen Sie eine Vertrauensbeziehung mit dem externen Key Server (EKS) auf.
   a. Erstellen Sie ein öffentliches/privates Schlüsselpaar für das Element Cluster, das zur Schaffung einer Vertrauensbeziehung mit dem Schlüsselserver verwendet wird, indem Sie die folgende API-Methode aufrufen: "CreatePublicPrivateKeyPair"
   b. Holen Sie sich die Zertifikatsign-Anforderung (CSR), die die Zertifizierungsstelle unterzeichnen muss. Der CSR ermöglicht dem Schlüsselserver zu überprüfen, ob das Element-Cluster, das auf die Schlüssel zugreift, als Element-Cluster authentifiziert ist. Rufen Sie die folgende API-Methode auf: "GetClientCertificateSignRequest"
   c. Verwenden Sie die EKS/Zertifizierungsstelle, um den abgerufenen CSR zu unterzeichnen. Weitere Informationen finden Sie in der Dokumentation von Drittanbietern.
2. Erstellen Sie auf dem Cluster einen Server und Provider, um mit dem EKS zu kommunizieren. Ein

Schlüsselanbieter legt fest, wo ein Schlüssel abgerufen werden soll, und ein Server definiert die spezifischen Attribute der EKS, die mit kommuniziert werden.

a. Erstellen Sie einen Schlüsselanbieter, bei dem die Schlüsselserverdetails gespeichert werden, indem Sie die folgende API-Methode aufrufen: "CreateKeyProviderKmip"

b. Erstellen Sie einen Schlüsselserver mit dem signierten Zertifikat und dem öffentlichen Schlüsselzertifikat der Zertifizierungsstelle, indem Sie die folgenden API-Methoden aufrufen: "CreateKeyServerkmip" "TestKeyServerkmip"

   Wenn der Test fehlschlägt, überprüfen Sie die Serverkonnektivität und -Konfiguration. Wiederholen Sie dann den Test.

c. Fügen Sie den Schlüsselserver in den Container des Schlüsselanbieters hinzu, indem Sie die folgenden API-Methoden aufrufen:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

   Wenn der Test fehlschlägt, überprüfen Sie die Serverkonnektivität und -Konfiguration. Wiederholen Sie dann den Test.

3. Führen Sie als nächsten Schritt für die Verschlüsselung im Ruhezustand einen der folgenden Schritte aus:

   a. (Für Hardware-Verschlüsselung im Ruhezustand) aktivieren "Hardware-Verschlüsselung für Daten im Ruhezustand" Durch Angabe der ID des Schlüsselanbieters, der den Schlüsselserver enthält, der zum Speichern der Schlüssel verwendet wird, indem der angerufen wird "EnableVerschlüsselungAtZiel" API-Methode.

   > Sie müssen die Verschlüsselung im Ruhezustand über das aktivieren "API". Die Aktivierung der Verschlüsselung im Ruhezustand mithilfe der vorhandenen Element UI-Schaltfläche bewirkt, dass die Funktion mithilfe intern generierter Schlüssel zurückgesetzt wird.

   b. (Für Softwareverschlüsselung im Ruhezustand) in der Reihenfolge "Softwareverschlüsselung für Daten im Ruhezustand" Um den neu erstellten Schlüsselanbieter nutzen zu können, geben Sie die Schlüssel-Provider-ID an den weiter "RekeySoftwareVerschlüsselungAtRestMasterKey" API-Methode.

Weitere Informationen

- "Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Verschlüsselung der Software beim Rest-Master-Schlüssel

Mit der Element-API können Sie einen vorhandenen Schlüssel neu Schlüssel rekeykey. Durch diesen Prozess wird ein neuer Master-Ersatzschlüssel für Ihren externen Verschlüsselungsmanagement-Server erstellt. Master-Schlüssel werden immer durch neue Master-Schlüssel ersetzt und nie dupliziert oder überschrieben.

Unter Umständen müssen Sie die Daten im Rahmen eines der folgenden Verfahren erneut keywichtigen:

- Erstellen Sie einen neuen Schlüssel im Rahmen einer Änderung vom internen Verschlüsselungsmanagement bis zum externen Verschlüsselungsmanagement.
- Erstellen Sie einen neuen Schlüssel als Reaktion auf oder als Schutz gegen sicherheitsrelevante

Ereignisse.

> Dieser Prozess ist asynchron und gibt eine Antwort zurück, bevor der Rekeyvorgang abgeschlossen ist. Sie können das verwenden "GetAsyncResult" Methode zum Abfragen des Systems, um zu sehen, wann der Prozess abgeschlossen ist.

Was Sie benötigen

- Mithilfe des haben Sie die Softwareverschlüsselung im Ruhezustand aktiviert "CreateCluster erstellen" Methode in einem neuen Cluster, das keine Volumes enthält und keinen I/O enthält Verwenden Sie den Link:./API/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] Um zu bestätigen, dass der Staat ist `enabled` Bevor Sie fortfahren.
- Das ist schon "Sie haben eine Vertrauensbeziehung aufgebaut" Zwischen dem SolidFire-Cluster und einem externen Schlüsselserver (EKS). Führen Sie die aus "TestKeyProviderKmip" Methode, um zu überprüfen, ob eine Verbindung zum Schlüsselanbieter hergestellt wurde.

Schritte

1. Führen Sie die aus "ListKeyProvidersKmip" Befehl und Kopie der Schlüssel-Provider-ID (`keyProviderID`).
2. Führen Sie die aus "RekeySoftwareVerschlüsselungAtRestMasterKey" Mit dem `keyManagementType` Parameter als `external` Und `keyProviderID` Als ID-Nummer des Schlüsselanbieters aus dem vorherigen Schritt:

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

3. Kopieren Sie die `asyncHandle` Wert aus dem `RekeySoftwareEncryptionAtRestMasterKey` Befehlsantwort.
4. Führen Sie die aus "GetAsyncResult" Befehl mit dem `asyncHandle` Wert aus dem vorherigen Schritt, um die Änderung der Konfiguration zu bestätigen. In der Befehlsantwort sollten Sie sehen, dass die ältere Master Key-Konfiguration mit neuen Schlüsselinformationen aktualisiert wurde. Kopieren Sie die neue Schlüssel-Provider-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. Führen Sie die aus `GetSoftwareEncryptionatRestInfo` Befehl, um zu bestätigen, dass neue wichtige Details, einschließlich `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

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln

Gelegentlich kann es zu einem Fehler kommen, der Benutzereingriff erfordert. Im Fehlerfall wird ein Cluster-Fehler (auch als Cluster-Fehlercode bezeichnet) generiert. Die beiden wahrscheinlichsten Fälle werden hier beschrieben.

Das Cluster kann die Laufwerke nicht entsperren, da ein KmipServerFault-Clusterfehler vorliegt.

Dies kann auftreten, wenn das Cluster zum ersten Mal gebootet wird und der Schlüsselserver nicht zugänglich ist oder der erforderliche Schlüssel nicht verfügbar ist.

1. Befolgen Sie ggf. die Wiederherstellungsschritte in den Cluster-Fehlercodes.

Es kann ein SliceServiceUnHealthy Fehler gesetzt werden, weil die Metadaten-Laufwerke als fehlgeschlagen markiert und in den Status „verfügbar“ gesetzt wurden.

Schritte zum Löschen:

1. Fügen Sie die Laufwerke erneut hinzu.
2. Prüfen Sie nach 3 bis 4 Minuten, dass der `sliceServiceUnhealthy` Fehler wurde behoben.

Siehe "Cluster-Fehlercodes" Finden Sie weitere Informationen.

Befehle für externes Verschlüsselungsmanagement-API

Liste aller zur Verwaltung und Konfiguration von EKM verfügbaren APIs.

Wird zum Aufbau einer Vertrauensbeziehung zwischen dem Cluster und externen Servern im Kundenbesitz verwendet:

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

Wird zur Definition der spezifischen Details externer kundeneigener Server verwendet:

- CreateKeyServerkmip
- ModifyKeyServerkmip
- DeleteKeyServerkmip
- GetKeyServerkmip
- ListKeyServersKmip

- TestKeyServerkmip

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

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

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.