外部キー管理の開始
Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/element-software/storage/concept_system_manage_key_get_started_with_external_key_management.html on November 12, 2025. Always check docs.netapp.com for the latest.

目次

外部キー管理の開始 . . . 1
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 . . . 5
「 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。 . . . 5
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。 . . . 5
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、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 "保存データの暗号化" クラスタでを有効にしておきます。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"

詳細については、こちらをご覧ください

- "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暗号化を組み合わせて設定する場合は、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 "クラスタを作成" ボリュームを含まない新しいクラスタ上のメソッド。

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を確立するために使用する、 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、キーサーバの詳細が格納され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. （保存中のハードウェア暗号化の場合）有効にします "保存データのハードウェア暗号化" 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 を指定するには、を呼び出します "EnableEncryptionAtRest" API メソッド。

> ⓘ 保存データの暗号化はを使用して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. （ソフトウェアによる保存データの暗号化）を実行します "ソフトウェアによる保存データの暗号化" 新しく作成したキープロバイダを使用するには、キープロバイダ ID をに渡します "RekeySoftwareEncryptionAtRestMasterKey" API メソッド。

詳細については、こちらをご覧ください

- "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。を使用できます "GetAsyncResult" 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する方法。

必要なもの

- 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 "クラスタを作成" ボリュームを含ま

ず、 I/O を含まない新しいクラスタ上のメソッド使用 "9510c8e68784d05acbae2e947dde3cd8" 続行する前に状態が「有効」であることを確認します。

- これで完了です "信頼関係を確立しました" SolidFire クラスタと外部キーサーバ（ EKS ）の間の接続に使用します。を実行します "TestKeyProviderKmip" キープロバイダへの接続が確立されていることを確認する方法。

手順

1. を実行します "ListKeyProvidersKmip" キープロバイダ ID (keyProviderID') をコピーします
2. を実行します "RekeySoftwareEncryptionAtRestMasterKey" 'keyManagementType' パラメータを 'external' および 'keyProviderID' として ' 前の手順で作成したキープロバイダの ID 番号を指定します

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

3. 「 RekeySoftwareEncryptionAtRestMasterKey 」コマンド応答から「 asyncHandle 」値をコピーします。
4. を実行します "GetAsyncResult" 前の手順の「 asyncHandle 」値を使用してコマンドを実行し、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. 「 GetSoftwareEncryptionatRestInfo 」コマンドを実行して、「 keyProviderID 」などの新しいキーの詳細が更新されたことを確認します。

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

詳細については、こちらをご覧ください

- "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 'lseServiceUnhealthy の障害がクリアされていることを確認します

を参照してください "クラスタ障害コード" を参照してください。

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、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

Copyright © 2025 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。