开始使用外部密钥管理

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/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.

目录

开始使用外部密钥管理 . . . 1
开始使用外部密钥管理 . . . 1
设置外部密钥管理 . . . 1
重新设置 REST 主密钥的软件加密密钥 . . . 2
恢复不可访问或无效的身份验证密钥 . . . 4
由于 KmipServerFault 集群故障，集群无法解锁驱动器。 . . . 4
可能会设置 sliceServiceUnhealthy 故障，因为元数据驱动器已标记为 Failed 并置于 "available" 状态。 . . . 4
外部密钥管理 API 命令 . . . 5

开始使用外部密钥管理

开始使用外部密钥管理

外部密钥管理（External Key Management， EKM）可与集群外外部密钥服务器（External Key Server， EKS）结合使用，提供安全身份验证密钥（Authentication Key，AK）管理。在这种情况下，可以使用这些 AK 锁定和解锁自加密驱动器（SED） "空闲加密" 已在集群上启用。EKS 可以安全地生成和存储 AK 。集群利用密钥管理互操作性协议（Key Management Interoperability Protocol， KMIP）（OASIS 定义的标准协议）与 EKS 进行通信。

- "设置外部管理"
- "重新设置 REST 主密钥的软件加密密钥"
- "恢复不可访问或无效的身份验证密钥"
- "外部密钥管理 API 命令"

了解更多信息

- "CreateCluster API，可用于启用空闲软件加密"
- "SolidFire 和 Element 软件文档"
- "早期版本的 NetApp SolidFire 和 Element 产品的文档"

设置外部密钥管理

您可以按照以下步骤操作，并使用列出的 Element API 方法设置外部密钥管理功能。

您需要的内容

- 如果要将外部密钥管理与空闲软件加密结合使用，则已使用启用空闲软件加密 "CreateCluster" 方法。

步骤

1. 与外部密钥服务器（EKS）建立信任关系。
   a. 通过调用以下 API 方法，为 Element 集群创建一个公共 / 专用密钥对，用于与密钥服务器建立信任关系： "CreatePublicPrivateKeyPair"
   b. 获取证书颁发机构需要签名的证书签名请求（CSR）。通过 CSR，密钥服务器可以验证要访问密钥的 Element 集群是否已作为 Element 集群进行身份验证。调用以下 API 方法： "GetClientCertificateSignRequest"
   c. 使用 EKS/ 证书颁发机构对检索到的 CSR 进行签名。有关详细信息，请参见第三方文档。
2. 在集群上创建服务器和提供程序以与 EKS 进行通信。密钥提供程序用于定义应从何处获取密钥，服务器用于定义要与之通信的 EKS 的特定属性。
   a. 通过调用以下 API 方法创建密钥服务器详细信息所在的密钥提供程序： "CreateKeyProviderKmip"
   b. 通过调用以下 API 方法，创建一个提供证书颁发机构的签名证书和公有密钥证书的密钥服务器： "CreateKeyServerKmip" "TestKeyServerKmip"

如果测试失败，请验证您的服务器连接和配置。然后重复测试。

c. 通过调用以下 API 方法将密钥服务器添加到密钥提供程序容器中："AddKeyServerToProviderKmip" "TestKeyProviderKmip"

如果测试失败，请验证您的服务器连接和配置。然后重复测试。

3. 执行以下操作之一作为空闲加密的下一步：

a. （用于空闲硬件加密）启用 "空闲硬件加密" 通过调用来提供用于存储密钥的密钥服务器所在的密钥提供程序的 ID "EnableEncryptionAtRest" API 方法。

> 您必须通过启用空闲加密 "API"。使用现有 Element UI 按钮启用空闲加密将使用内部生成的密钥对功能进行发生原因还原。

b. （用于空闲软件加密） "空闲软件加密" 要使用新创建的密钥提供程序，请将密钥提供程序 ID 传递到 "RekeySoftwareEncryptionAtRestMasterKey" API 方法。

了解更多信息

- "为集群启用和禁用加密"
- "SolidFire 和 Element 软件文档"
- "早期版本的 NetApp SolidFire 和 Element 产品的文档"

重新设置 REST 主密钥的软件加密密钥

您可以使用 Element API 重新设置现有密钥的密钥。此过程将为外部密钥管理服务器创建一个新的替换主密钥。主密钥始终会替换为新的主密钥，并且不会复制或覆盖。

您可能需要在以下过程之一中重新设置密钥：

- 在从内部密钥管理到外部密钥管理的变更过程中创建新密钥。
- 创建一个新密钥，作为对安全相关事件的响应或保护。

> 此过程是异步的，在重新设置密钥操作完成之前返回响应。您可以使用 "GetAsyncResult" 对系统进行轮询以查看进程何时完成的方法。

您需要的内容

- 您已使用启用空闲软件加密 "CreateCluster" 方法，用于新集群，该集群不包含卷，也不具有 I/O使用 … "9510c8e68784d05acbae2e947dde3cd8" 在继续操作之前，确认状态为 `enabled` 。
- 您已拥有 "建立信任关系" 在 SolidFire 集群和外部密钥服务器（ EKS ）之间。运行 "TestKeyProviderKmip" 用于验证是否已建立与密钥提供程序的连接的方法。

步骤

1. 运行 "ListKeyProvidersKmip" 命令并复制密钥提供程序 ID （`keyProviderID`）。
2. 运行 "RekeySoftwareEncryptionAtRestMasterKey" 将 `keyManagementType` 参数设置为 `external` ，并将 `keyProviderID` 作为上一步中密钥提供程序的 ID 编号：

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

3. 从 `RekeySoftwareEncryptionAtRestMasterKey` 命令响应中复制 `asyncHandle` 值。
4. 运行 "GetAsyncResult" 包含上一步中的 `asyncHandle` 值的命令，用于确认配置更改。在命令响应中，您应看到旧主密钥配置已使用新密钥信息进行更新。复制新密钥提供程序 ID ，以供稍后使用。

```
{
   "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. 运行 `GetSoftwareEncryptionatRestInfo` 命令以确认新密钥详细信息（包括 `keyProviderID` ）已更新。

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

了解更多信息

- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "早期版本的 NetApp SolidFire 和 Element 产品的文档"

恢复不可访问或无效的身份验证密钥

有时，可能会发生需要用户干预的错误。如果发生错误，将生成集群故障（称为集群故障代码）。下面介绍了两种最可能的情况。

由于 **KmipServerFault** 集群故障，集群无法解锁驱动器。

当集群首次启动，密钥服务器不可访问或所需密钥不可用时，可能会发生这种情况。

1. 按照集群故障代码（如果有）中的恢复步骤进行操作。

可能会设置 **sliceServiceUnhealthy** 故障，因为元数据驱动器已标记为 **Failed** 并置于 **"available"** 状态。

清除步骤：

1. 重新添加驱动器。
2. 3 到 4 分钟后，检查 `sliceServiceUnhealthy` 故障是否已清除。

请参见 "集群故障代码" 有关详细信息 ...

外部密钥管理 API 命令

列出可用于管理和配置 EKM 的所有 API 。

用于在集群与客户拥有的外部服务器之间建立信任关系：

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

用于定义客户拥有的外部服务器的特定详细信息：

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

用于创建和维护用于管理外部密钥服务器的密钥提供程序：

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

有关 API 方法的信息，请参阅 "API 参考信息"。

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。