



## 開始使用外部金鑰管理 Element Software

NetApp  
January 15, 2024

# 目錄

開始使用外部金鑰管理 .....	1
設定外部金鑰管理 .....	1
在REST主要金鑰重新輸入軟體加密 .....	2
恢復無法存取或無效的驗證金鑰 .....	4
外部金鑰管理API命令 .....	5

# 開始使用外部金鑰管理

外部金鑰管理（EKM）可搭配叢集外的外部金鑰伺服器（EKS）、提供安全驗證金鑰（AK）管理。當自動加密磁碟機（SED）處於鎖定和解除鎖定狀態時、即會使用這些AKs ["加密閒置"](#) 已在叢集上啟用。EKS提供安全的AKs世代與儲存設備。叢集利用金鑰管理互通性傳輸協定（KMIP）（OASIS定義的標準傳輸協定）與EKS通訊。

- ["設定外部管理"](#)
- ["在REST主要金鑰重新輸入軟體加密"](#)
- ["恢復無法存取或無效的驗證金鑰"](#)
- ["外部金鑰管理API命令"](#)

## 如需詳細資訊、請參閱

- ["可用來在閒置時啟用軟體加密的叢集API"](#)
- ["零件與元件軟體文件SolidFire"](#)
- ["先前版本的NetApp SolidFire 產品及元素產品文件"](#)

## 設定外部金鑰管理

您可以遵循下列步驟、並使用列出的Element API方法來設定外部金鑰管理功能。

### 您需要的產品

- 如果您要設定外部金鑰管理、並在閒置時搭配軟體加密、則已使用啟用軟體加密功能 ["建立叢集"](#) 不含磁碟區的新叢集方法。

### 步驟

1. 與外部金鑰伺服器（EKS）建立信任關係。
  - a. 針對元素叢集建立公開/私密金鑰配對、以呼叫下列API方法來建立與金鑰伺服器的信任關係：["建立PublicPrivate KeyPair"](#)
  - b. 取得認證機構需要簽署的認證簽名要求（CSR）。CSR可讓金鑰伺服器驗證要存取金鑰的元素叢集是否已驗證為元素叢集。請撥打下列API方法：["GetClientCertificateSignRequest"](#)
  - c. 使用EKS/Certificate Authority簽署擷取的CSR。如需詳細資訊、請參閱第三方文件。
2. 在叢集上建立伺服器和供應商、以便與EKS通訊。金鑰供應商會定義金鑰的取得位置、而伺服器則會定義要與之通訊的EKS特定屬性。
  - a. 透過呼叫下列API方法、建立主要伺服器詳細資料所在的主要供應商：["CreeKeyProviderKmpip"](#)
  - b. 透過呼叫下列API方法來建立金鑰伺服器、以提供已簽署的憑證和憑證授權單位的公開金鑰憑證：["CreKeyServerKmpip"](#) ["TestKeyServerKmpip"](#)

如果測試失敗、請確認您的伺服器連線能力和組態。然後重複測試。

  - c. 透過呼叫下列API方法、將金鑰伺服器新增至金鑰提供者容器：["AddKeyServerToProviderKmpip"](#) ["TestKeyProviderKmpip"](#)

如果測試失敗、請確認您的伺服器連線能力和組態。然後重複測試。

3. 請執行下列其中一項、做為靜止加密的下一步：

- a. (用於靜止時的硬體加密) 啟用 **"硬體加密功能"** 提供金鑰提供者的ID、其中包含用來透過呼叫來儲存金鑰的金鑰伺服器 **"啟用EncryptionAtRest"** API方法。



您必須透過啟用加密功能 **"API"**。使用現有元素UI按鈕啟用靜止加密、將會導致功能回復為使用內部產生的金鑰。

- b. (用於閒置時的軟體加密) **"軟體加密功能"** 若要使用新建立的金鑰提供者、請將金鑰提供者ID傳送至 **"RekeySoftwareEncryptionAt恢復 主金鑰"** API方法。

如需詳細資訊、請參閱

- ["啟用及停用叢集的加密"](#)
- ["零件與元件軟體文件SolidFire"](#)
- ["先前版本的NetApp SolidFire 產品及元素產品文件"](#)

## 在REST主要金鑰重新輸入軟體加密

您可以使用Element API重新輸入現有的金鑰。此程序會為您的外部金鑰管理伺服器建立新的替代主金鑰。主金鑰一律由新的主金鑰取代、永遠不會複製或覆寫。

您可能需要重新輸入以下程序的一部分：

- 在從內部金鑰管理變更為外部金鑰管理的過程中、建立新的金鑰。
- 建立新的金鑰、做為對安全性相關事件的回應或保護。



此程序是非同步的、會在重新輸入作業完成之前傳回回應。您可以使用 **"Get非 同步結果"** 輪詢系統以查看程序何時完成的方法。

您需要的產品

- 您已使用啟用軟體加密功能 **"建立叢集"** 不含磁碟區且沒有I/O的新叢集上的方法使用 **"9510c8e68784d05acbae2e947dde3cd8"** 確認狀態為「已啟用」、然後再繼續。
- 您有 **"建立信任關係"** 在整個叢集與外部金鑰伺服器SolidFire (EKS) 之間。執行 **"TestKeyProviderKmpip"** 驗證是否已建立與金鑰提供者的連線的方法。

步驟

1. 執行 **"listKeyProvidersKmpip"** 命令並複製金鑰提供者ID (「keyProviderID」) 。
2. 執行 **"RekeySoftwareEncryptionAt恢復 主金鑰"** 將「keyManagementType」參數設為「external」、「keyProviderID」作為上一步金鑰提供者的ID號碼：

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

3. 從「RekeySoftwareEncryptionAt恢復 金鑰」命令回應中複製「asyncdyle」值。
4. 執行 ["Get非 同步結果"](#) 以上一個步驟的「asyncdyle」值來確認組態變更的命令。從命令回應中、您應該會看到舊版主金鑰組態已更新為新的金鑰資訊。複製新的金鑰提供者ID以供後續步驟使用。

```
{
  "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. 執行「GetSoftwareEncryptionatRestInfo」命令、確認已更新新的金鑰詳細資料、包括「keyProviderID」。

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

如需詳細資訊、請參閱

- ["使用Element API管理儲存設備"](#)
- ["零件與元件軟體文件SolidFire"](#)
- ["先前版本的NetApp SolidFire 產品及元素產品文件"](#)

## 恢復無法存取或無效的驗證金鑰

偶爾會發生需要使用者介入的錯誤。發生錯誤時、會產生叢集故障（稱為叢集故障代碼）。此處說明兩種最可能的案例。

由於**KmipServerFault**叢集故障、叢集無法解除鎖定磁碟機。

當叢集第一次開機且金鑰伺服器無法存取或所需的金鑰無法使用時、就會發生這種情況。

1. 請遵循叢集故障代碼（若有）中的還原步驟。

可能會設定交叉分析**eServiceUnhealthy**故障、因為中繼資料磁碟機已標示為故障、並置於「可用」狀態。

清除步驟：

1. 再次新增磁碟機。
2. 3到4分鐘後、請檢查「交叉服務不健全」故障是否已清除。

請參閱 ["叢集故障代碼"](#) 以取得更多資訊。

# 外部金鑰管理API命令

可用於管理及設定EKM的所有API清單。

用於建立叢集與外部客戶擁有伺服器之間的信任關係：

- 建立PublicPrivate KeyPair
- GetClientCertificateSignRequest

用於定義外部客戶擁有伺服器的特定詳細資料：

- CreKeyServerKmp
- ModifyKeyServerKmp
- 刪除KeyServerKmp
- GetKeyServerKmp
- listKeyServersKmp
- TestKeyServerKmp

用於建立及維護管理外部金鑰伺服器的主要供應商：

- CreeKeyProviderKmp
- 刪除KeyProviderKmp
- AddKeyServerToProviderKmp
- RemoveKeyServerFromProviderKmp
- GetKeyProviderKmp
- listKeyProvidersKmp
- RekeySoftwareEncryptionAt恢復 主金鑰
- TestKeyProviderKmp

如需API方法的相關資訊、請參閱 "[API參考資訊](#)"。

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。