



安全API方法

Element Software

NetApp
October 01, 2024

目錄

安全API方法	1
如需詳細資訊、請參閱	1
AddKeyServerToProviderKmp	1
CreeKeyProviderKmp	2
CreKeyServerKmp	4
建立PublicPrivate KeyPair	6
刪除KeyProviderKmp	8
刪除KeyServerKmp	9
DisableEncryptionAtRest	10
啟用EncryptionAtRest	11
GetClientCertificateSignRequest	14
GetKeyProviderKmp	15
GetKeyServerKmp	16
GetSoftwareEncryptionAt恢復 資訊	17
listKeyProvidersKmp	19
listKeyServersKmp	21
ModifyKeyServerKmp	24
RekeySoftwareEncryptionAt恢復 主金鑰	27
RemoveKeyServerFromProviderKmp	28
SignSshKeys	29
TestKeyProviderKmp	32
TestKeyServerKmp	33

安全API方法

您可以將Element軟體與外部安全性相關服務（例如外部金鑰管理伺服器）整合。這些與安全性相關的方法可讓您設定元素安全功能、例如外部金鑰管理、以利加密閒置。

- [AddKeyServerToProviderK mip](#)
- [CreeKeyProviderK mip](#)
- [CreKeyServerK mip](#)
- [建立PublicPrivate KeyPair](#)
- [刪除KeyProviderK mip](#)
- [刪除KeyServerK mip](#)
- [DisableEncryptionAtRest](#)
- [啟用EncryptionAtRest](#)
- [GetClientCertificateSignRequest](#)
- [GetKeyProviderK mip](#)
- [GetKeyServerK mip](#)
- [listKeyProvidersK mip](#)
- [listKeyServersK mip](#)
- [ModifyKeyServerK mip](#)
- [RemoveKeyServerFromProviderK mip](#)
- [SignSshKeys](#)
- [TestKeyProviderK mip](#)
- [TestKeyServerK mip](#)

如需詳細資訊、請參閱

- ["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"](#)

AddKeyServerToProviderK mip

您可以使用此 `AddKeyServerToProviderK mip` 方法將金鑰管理互通性通訊協定（KMIP）金鑰伺服器指派給指定的金鑰提供者。在指派期間、系統會聯絡伺服器以驗證功能。如果指定的金鑰伺服器已指派給指定的金鑰提供者、則不會採取任何動作、也不會傳回錯誤。您可以使用方法移除指派 `RemoveKeyServerFromProviderK mip`。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderID	要指派金鑰伺服器的金鑰提供者ID。	整數	無	是的
KeyServerID	要指派的金鑰伺服器ID。	整數	無	是的

傳回值

此方法沒有傳回值。只要沒有傳回錯誤、指派就會被視為成功。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "AddKeyServerToProviderKnip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
    {}
}
```

新的自版本

11.7

CreeKeyProviderKnip

您可以使用此 `CreateKeyProviderKnip`` 方法建立具有指定名稱的金鑰管理互通性通訊協定 (KMIP) 金鑰提供者。金鑰提供者定義擷取驗證金鑰的機制和位置。當您建立新

的KMIP金鑰提供者時、它並未指派任何KMIP金鑰伺服器給它。若要建立 KMIP 金鑰伺服器、請使用 `CreateKeyServerK mip` 方法。若要將其指派給供應商、請參閱 `AddKeyServerToProviderK mip`。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderName	與建立的KMIP金鑰提供者建立關聯的名稱。此名稱僅供顯示用途使用、不需要唯一名稱。	字串	無	是的

傳回值

此方法具有下列傳回值：

名稱	說明	類型
k mipKeyProvider	包含新建立金鑰提供者詳細資料的物件。	"KeyProviderK mip"

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "CreateKeyProviderK mip",
  "params": {
    "keyProviderName": "ProviderName",
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```

{
  "id": 1,
  "result":
  {
    "kmipKeyProvider": {
      "keyProviderName": "ProviderName",
      "keyProviderIsActive": true,
      "kmipCapabilities": "SSL",
      "keyServerIDs": [
        15
      ],
      "keyProviderID": 1
    }
  }
}

```

新的自版本

11.7

CreKeyServerKmip

您可以使用此 `CreateKeyServerKmip` 方法建立具有指定屬性的金鑰管理互通性通訊協定 (KMIP) 金鑰伺服器。在建立期間、伺服器不會連絡；使用此方法之前不需要存在伺服器。對於叢集式金鑰伺服器組態、您必須在 `kmipKeyServerHostnames` 參數中提供所有伺服器節點的主機名稱或IP位址。您可以使用此 `TestKeyServerKmip` 方法來測試金鑰伺服器。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KmipCaCertificate	外部金鑰伺服器根CA的公開金鑰憑證。這將用來驗證外部金鑰伺服器在TLS通訊中所提供的憑證。對於個別伺服器使用不同CA的金鑰伺服器叢集、請提供包含所有CA根憑證的串聯字串。	字串	無	是的

名稱	說明	類型	預設值	必要
kmipClientCertificate	由WSIKMIP用戶端使用的PEE格式Base64編碼的PKCS#10 X.509憑證SolidFire。	字串	無	是的
kmipKeyServerHostnames	與此KMIP金鑰伺服器相關聯的主機名稱或IP位址陣列。只有當主要伺服器位於叢集式組態時、才能提供多個主機名稱或IP位址。	字串陣列	無	是的
kmipKeyServerName	KMIP金鑰伺服器的名稱。此名稱僅供顯示用途使用、不需要唯一名稱。	字串	無	是的
kmipKeyServerPort	與此KMIP金鑰伺服器相關的連接埠號碼（通常為5696）。	整數	無	否

傳回值

此方法具有下列傳回值：

名稱	說明	類型
kmipKeyServer	包含新建立金鑰伺服器詳細資料的物件。	"KeyServerKmp"

申請範例

此方法的要求類似於下列範例：

```

{
  "method": "CreateKeyServerKmip",
  "params": {
    "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
  "id": 1
}

```

回應範例

此方法會傳回類似下列範例的回應：

```

{
  "id": 1,
  "result":
  {
    "kmipKeyServer": {
      "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
      "kmipKeyServerHostnames": [
        "server1.hostname.com", "server2.hostname.com"
      ],
      "keyProviderID": 1,
      "kmipKeyServerName": "keyserverName",
      "keyServerID": 1,
      "kmipKeyServerPort": 1,
      "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
      "kmipAssignedProviderIsActive": true
    }
  }
}

```

新的自版本

11.7

建立PublicPrivate KeyPair

您可以使用此 `CreatePublicPrivateKeyPair` 方法來建立公開和私密 SSL 金鑰。您可以使

用這些金鑰來產生憑證簽署要求。每個儲存叢集只能使用一組金鑰配對。在使用此方法來取代現有金鑰之前、請先確定任何供應商都不再使用金鑰。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
通用名稱	「X·509辨別名稱*一般名稱*」欄位（中國）。	字串	無	否
國家/地區	X.509辨別名稱*國家/地區*欄位（C）。	字串	無	否
電子郵件地址	「X·509辨別名稱*電子郵件地址*」欄位（郵件）。	字串	無	否
位置	「X·509辨別名稱*位置名稱*」欄位（L）。	字串	無	否
組織	「X·509辨別名稱*組織名稱*」欄位（O）。	字串	無	否
組織單位	「X·509辨別名稱*組織單位名稱*」欄位（OU）。	字串	無	否
州/省	「X·509辨別名稱*州*」或「省名稱」欄位（ST或SP或S）。	字串	無	否

傳回值

此方法沒有傳回值。如果沒有錯誤、則會將金鑰建立視為成功。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "CreatePublicPrivateKeyPair",
  "params": {
    "commonName": "Name",
    "country": "US",
    "emailAddress" : "email@domain.com"
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
    {}
}
```

新的自版本

11.7

刪除KeyProviderKmpip

您可以使用此 `DeleteKeyProviderKmpip` 方法刪除指定的非作用中金鑰管理互通性通訊協定 (KMIP) 金鑰提供者。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderID	要刪除的金鑰提供者ID。	整數	無	是的

傳回值

此方法沒有傳回值。只要沒有錯誤、刪除作業就會被視為成功。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
    {}
}
```

新的自版本

11.7

刪除KeyServerKmip

您可以使用此 `DeleteKeyServerKmip` 方法刪除現有的金鑰管理互通性通訊協定（KMIP）金鑰伺服器。除非金鑰伺服器是最後指派給其供應商的金鑰伺服器、而且該供應商提供目前使用中的金鑰、否則您可以刪除該金鑰伺服器。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyServerID	要刪除的KMIP金鑰伺服器ID。	整數	無	是的

傳回值

此方法沒有傳回值。如果沒有錯誤、刪除作業就會被視為成功。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
    {}
}
```

新的自版本

11.7

DisableEncryptionAtRest

您可以使用此 `DisableEncryptionAtRest`` 方法移除先前套用至叢集的加密 ``EnableEncryptionAtRest`。此停用方法為非同步、會在停用加密之前傳回回應。您可以使用 ``GetClusterInfo`` 方法輪詢系統、查看程序何時完成。



若要查看叢集上閒置時的加密狀態和 / 或軟體加密狀態，請使用["取得叢集資訊方法"](#)。您可以使用 `GetSoftwareEncryptionAtRestInfo` ["取得叢集用來加密閒置資料的資訊方法"](#)。



您無法使用此方法停用閒置的軟體加密。若要停用靜態的軟體加密、您需要["建立新叢集"](#)停用靜止時的軟體加密。

參數

此方法沒有輸入參數。

傳回值

此方法沒有傳回值。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "DisableEncryptionAtRest",
  "params": {},
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id" : 1,
  "result" : {}
}
```

新的自版本

9.6

如需詳細資訊、請參閱

- ["GetClusterInfo"](#)
- ["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"](#)

啟用EncryptionAtRest

您可以使用此 `EnableEncryptionAtRest` 方法在叢集上啟用進階加密標準（AES）256 位元加密、以便叢集管理每個節點上用於磁碟機的加密金鑰。此功能預設為未啟用。



若要查看叢集上閒置時的加密狀態和 / 或軟體加密狀態，請使用["取得叢集資訊方法"](#)。您可以使用 `GetSoftwareEncryptionAtRestInfo` ["取得叢集用來加密閒置資料的資訊方法"](#)。



此方法無法在閒置時啟用軟體加密。只能使用 [設為] 的 `true` 來 `enableSoftwareEncryptionAtRest` 完成此["建立叢集方法"](#)作業。

在閒置時啟用加密時、叢集會自動在叢集中每個節點的磁碟機內部管理加密金鑰。

如果指定了keyProviderID、則會根據金鑰提供者的類型產生和擷取密碼。這通常是使用金鑰管理互通性傳輸協定 (KMIP) 金鑰伺服器 (KMIP金鑰提供者) 來完成。完成此作業後、指定的提供者即視為作用中、且在使用方法停用「閒置加密」之前、無法刪除 DisableEncryptionAtRest。



如果您的節點類型的型號以「-NE」結尾、`EnableEncryptionAtRest`方法呼叫將會失敗、並回應「不允許加密」。叢集偵測到非加密節點"。



只有在叢集執行且狀態良好時、才應啟用或停用加密。您可以自行決定、視需要隨時啟用或停用加密功能。



此程序是非同步的、會在啟用加密之前傳回回應。您可以使用 `GetClusterInfo`方法輪詢系統、查看程序何時完成。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderID	要使用的KMIP金鑰提供者ID。	整數	無	否

傳回值

此方法沒有傳回值。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "EnableEncryptionAtRest",
  "params": {},
  "id": 1
}
```

回應範例

此方法會傳回類似於下列來自於EnableEncryptionAtRest方法的回應。沒有報告結果。

```
{
  "id": 1,
  "result": {}
}
```

在叢集上啟用靜止加密時、GetClusterInfo會傳回將靜止加密狀態（「加密AtRestState」）描述為「啟用」的結果。完全啟用「靜止加密」之後、傳回的狀態會變更為「已啟用」。

```
{
  "id": 1,
  "result": {
    "clusterInfo": {
      "attributes": { },
      "encryptionAtRestState": "enabling",
      "ensemble": [
        "10.10.5.94",
        "10.10.5.107",
        "10.10.5.108"
      ],
      "mvip": "192.168.138.209",
      "mvipNodeID": 1,
      "name": "Marshall",
      "repCount": 2,
      "svip": "10.10.7.209",
      "svipNodeID": 1,
      "uniqueID": "91dt"
    }
  }
}
```

新的自版本

9.6

如需詳細資訊、請參閱

- ["SecureEraseDrives"](#)
- ["GetClusterInfo"](#)
- ["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"](#)

GetClientCertificateSignRequest

您可以使用此 `GetClientCertificateSignRequest` 方法產生憑證簽署要求、由憑證授權單位簽署、以產生叢集的用戶端憑證。需要簽署憑證、才能建立與外部服務互動的信任關係。

參數

此方法沒有輸入參數。

傳回值

此方法具有下列傳回值：

名稱	說明	類型
用戶端認證登入要求	一種PEE格式的Base64編碼的PKCS#10 X.509用戶端憑證簽署要求。	字串

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result": {
    "clientCertificateSignRequest":
    "MIIBYjCCATMCAQAwgYkxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
  }
}
```


新的自版本

11.7

GetKeyProviderKmip

您可以使用此 `GetKeyProviderKmip` 方法擷取指定金鑰管理互通性通訊協定 (KMIP) 金鑰提供者的相關資訊。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderID	要傳回的KMIP金鑰提供者物件ID。	整數	無	是的

傳回值

此方法具有下列傳回值：

名稱	說明	類型
kmipKeyProvider	包含所要求金鑰提供者詳細資料的物件。	"KeyProviderKmip"

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "GetKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```

{
  "id": 1,
  "result":
  {
    "kmipKeyProvider": {
      "keyProviderID": 15,
      "kmipCapabilities": "SSL",
      "keyProviderIsActive": true,
      "keyServerIDs": [
        1
      ],
      "keyProviderName": "ProviderName"
    }
  }
}

```

新的自版本

11.7

GetKeyServerKmp

您可以使用此 `GetKeyServerKmp` 方法傳回指定金鑰管理互通性通訊協定（KMIP）金鑰伺服器的相關資訊。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyServerID	要傳回相關資訊的KMIP金鑰伺服器ID。	整數	無	是的

傳回值

此方法具有下列傳回值：

名稱	說明	類型
kmipKeyServer	包含所要求金鑰伺服器詳細資料的物件。	"KeyServerKmp"

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "GetKeyServerKnip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result": {
    "kmipKeyServer": {
      "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
      "kmipKeyServerHostnames": [
        "server1.hostname.com", "server2.hostname.com"
      ],
      "keyProviderID": 1,
      "kmipKeyServerName": "keyserverName",
      "keyServerID": 15,
      "kmipKeyServerPort": 1,
      "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
      "kmipAssignedProviderIsActive": true
    }
  }
}
```

新的自版本

11.7

GetSoftwareEncryptionAt恢復 資訊

您可以使用此 `GetSoftwareEncryptionAtRestInfo` 方法取得叢集用來加密靜止資料的閒置時軟體加密資訊。

參數

此方法沒有輸入參數。

傳回值

此方法具有下列傳回值：

參數	說明	類型	選用
主KeyInfo	目前軟體加密閒置主要金鑰的相關資訊。	EncryptionKeyInfo	是的
rekeyMasterKey 非ResultID	目前或最近重新輸入作業（若有）的非同步結果 ID（若尚未刪除）。 `GetAsyncResult` 輸出將包含 `newKey` 新主金鑰的相關資訊欄位、以及 `keyToDecommission` 包含舊金鑰相關資訊的欄位。	整數	是的
州/省	目前的軟體閒置加密狀態。可能的值為 `disabled` 或 `enabled`。	字串	錯
版本	每次啟用閒置軟體加密時、會遞增的版本編號。	整數	錯

申請範例

此方法的要求類似於下列範例：

```
{  
  "method": "getsoftwareencryptionatrestinfo"  
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result": {
    "masterKeyInfo": {
      "keyCreatedTime": "2021-09-20T23:15:56Z",
      "keyID": "4d80a629-a11b-40ab-8b30-d66dd5647cfd",
      "keyManagementType": "internal"
    },
    "state": "enabled",
    "version": 1
  }
}
```

新的自版本

12.3

如需詳細資訊、請參閱

- ["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"](#)

listKeyProvidersKmip

您可以使用此 `ListKeyProvidersKmip` 方法擷取所有現有金鑰管理互通性通訊協定（KMIP）主要供應商的清單。您可以指定其他參數來篩選清單。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderIsActive	<p>篩選器會根據金鑰伺服器物件是否處於作用中狀態而傳回KMIP金鑰伺服器物件。可能值：</p> <ul style="list-style-type: none"> • true：僅傳回作用中的KMIP金鑰提供者（提供目前使用中的金鑰）。 • 否：僅傳回非作用中的KMIP金鑰提供者（不提供任何金鑰且可刪除）。 <p>如果省略、則不會根據傳回的KMIP金鑰提供者是否處於作用中狀態來篩選。</p>	布林值	無	否
kmipKeyProviderHasServerAssigned	<p>篩選器會根據是否指派KMIP金鑰伺服器而傳回KMIP金鑰提供者。可能值：</p> <ul style="list-style-type: none"> • true：僅傳回已指派KMIP金鑰伺服器的KMIP金鑰提供者。 • 否：僅傳回未指派KMIP金鑰伺服器的KMIP金鑰提供者。 <p>如果省略、則不會根據傳回的KMIP金鑰提供者是否已指派KMIP金鑰伺服器來篩選。</p>	布林值	無	否

傳回值

此方法具有下列傳回值：

名稱	說明	類型
----	----	----

kmipKeyProviders	已建立的KMIP金鑰提供者清單。	"KeyProviderKmpip"陣列
------------------	------------------	----------------------

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "ListKeyProvidersKmpip",
  "params": {},
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
  {
    "kmipKeyProviders": [
      {
        "keyProviderID": 15,
        "kmipCapabilities": "SSL",
        "keyProviderIsActive": true,
        "keyServerIDs": [
          1
        ],
        "keyProviderName": "KeyProvider1"
      }
    ]
  }
}
```

新的自版本

11.7

listKeyServersKmpip

您可以使用此 `ListKeyServersKmpip` 方法列出所有已建立的金鑰管理互通性通訊協定（KMIP）金鑰伺服器。您可以指定其他參數來篩選結果。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderID	指定時、方法只會傳回指派給指定KMIP金鑰提供者的KMIP金鑰伺服器。如果省略、傳回的KMIP金鑰伺服器將不會根據是否指派給指定的KMIP金鑰提供者來篩選。	整數	無	否
kmpAssignedProvidersActive	篩選器會根據金鑰伺服器物件是否處於作用中狀態而傳回KMIP金鑰伺服器物件。可能值： <ul style="list-style-type: none">• true：僅傳回作用中的KMIP金鑰伺服器（提供目前使用中的金鑰）。• 否：僅傳回非作用中的KMIP金鑰伺服器（不提供任何金鑰且可刪除）。 如果省略、傳回的KMIP金鑰伺服器將不會根據其是否處於作用中狀態而加以篩選。	布林值	無	否

名稱	說明	類型	預設值	必要
kmpHasProviderAsSigned	<p>篩選器會根據是否指派KMIP金鑰提供者而傳回KMIP金鑰伺服器。可能值：</p> <ul style="list-style-type: none"> • true：僅傳回已指派KMIP金鑰提供者的KMIP金鑰伺服器。 • 否：僅傳回未指派KMIP金鑰提供者的KMIP金鑰伺服器。 <p>如果省略、傳回的KMIP金鑰伺服器將不會根據是否指派KMIP金鑰提供者來篩選。</p>	布林值	無	否

傳回值

此方法具有下列傳回值：

名稱	說明	類型
kmpKeyServers	已建立的KMIP金鑰伺服器完整清單。	"KeyServerKmp"陣列

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "ListKeyServersKmp",
  "params": {},
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```

{
  "kmipKeyServers": [
    {
      "kmipKeyServerName": "keyserverName",
      "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
      "keyServerID": 15,
      "kmipAssignedProviderIsActive": true,
      "kmipKeyServerPort": 5696,
      "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
      "kmipKeyServerHostnames": [
        "server1.hostname.com", "server2.hostname.com"
      ],
      "keyProviderID": 1
    }
  ]
}

```

新的自版本

11.7

ModifyKeyServerKmip

您可以使用此 `ModifyKeyServerKmip` 方法、將現有的金鑰管理互通性通訊協定（KMIP）金鑰伺服器修改為指定的屬性。雖然唯一需要的參數是keyServerID、但只包含keyServerID的要求將不會採取任何動作、也不會傳回任何錯誤。您指定的任何其他參數都會以指定的keyServerID取代金鑰伺服器的現有值。在作業期間會聯絡金鑰伺服器、以確保其正常運作。您可以使用kmipKeyServerHostnames參數來提供多個主機名稱或IP位址、但只有當主要伺服器位於叢集式組態時才會提供。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyServerID	要修改的KMIP金鑰伺服器ID。	整數	無	是的

KmipCaCertificate	外部金鑰伺服器根CA的公開金鑰憑證。這將用來驗證外部金鑰伺服器在TLS通訊中所提供的憑證。對於個別伺服器使用不同CA的金鑰伺服器叢集、請提供包含所有CA根憑證的串聯字串。	字串	無	否
kmipClientCertificate	由WSIKMIP用戶端使用的PEE格式Base64編碼的PKCS#10 X.509憑證SolidFire。	字串	無	否
kmipKeyServerHostnames	與此KMIP金鑰伺服器相關聯的主機名稱或IP位址陣列。只有當主要伺服器位於叢集式組態時、才能提供多個主機名稱或IP位址。	字串陣列	無	否
kmipKeyServerName	KMIP金鑰伺服器的名稱。此名稱僅供顯示用途使用、不需要唯一名稱。	字串	無	否
kmipKeyServerPort	與此KMIP金鑰伺服器相關的連接埠號碼（通常為5696）。	整數	無	否

傳回值

此方法具有下列傳回值：

名稱	說明	類型
kmipKeyServer	包含新修改金鑰伺服器詳細資料的物件。	"KeyServerKmip"

申請範例

此方法的要求類似於下列範例：

```

{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAAUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
  "id": 1
}

```

回應範例

此方法會傳回類似下列範例的回應：

```

{
  "id": 1,
  "result":
  {
    "kmipKeyServer": {
      "kmipCaCertificate": "CPDCCAAUCEDyRMcsf9tAbDpq40ES/E...",
      "kmipKeyServerHostnames": [
        "server1.hostname.com", "server2.hostname.com"
      ],
      "keyProviderID": 1,
      "kmipKeyServerName": "keyserverName",
      "keyServerID": 1
      "kmipKeyServerPort": 1,
      "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
      "kmipAssignedProviderIsActive": true
    }
  }
}

```

新的自版本

11.7

RekeySoftwareEncryptionAt恢復 主金鑰

您可以使用此 `RekeySoftwareEncryptionAtRestMasterKey` 方法重新輸入用於加密 DEK (資料加密金鑰) 的軟體閒置加密主金鑰。在建立叢集期間、閒置時的軟體加密會設定為使用內部金鑰管理 (IKM)。此重新輸入方法可在建立叢集之後使用、以使用IKM或外部金鑰管理 (EKM)。

參數

此方法具有下列輸入參數。如果未指定參數、則 `keyManagementType` 會使用現有的金鑰管理組態來執行重新輸入作業。如果已指定且金鑰提供者為外部、`keyProviderID` 則 `keyManagementType` 也必須使用參數。

參數	說明	類型	選用
KeyManagement類型	用於管理主金鑰的金鑰管理類型。可能的值包括 Internal：使用內部金鑰管理重新輸入金鑰。 External：使用外部金鑰管理重新輸入金鑰。如果未指定此參數、則會使用現有的金鑰管理組態執行重新輸入作業。	字串	是的
KeyProviderID	要使用的金鑰提供者ID。這是傳回的唯一值、屬於其中一種方法的一部分 CreateKeyProvider。ID 只有在為 External 和其他無效時才需要 `keyManagementType`。	整數	是的

傳回值

此方法具有下列傳回值：

參數	說明	類型	選用
asyncdle	使用此值與一起 GetAsyncResult 確定重新鍵操作的狀態 `asyncHandle`。 `GetAsyncResult` 輸出將包含 `newKey` 新主金鑰的相關資訊欄位、以及 `keyToDecommission` 包含舊金鑰相關資訊的欄位。	整數	錯

申請範例

此方法的要求類似於下列範例：

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

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "asyncHandle": 1
}
```

新的自版本

12.3

如需詳細資訊、請參閱

- ["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"](#)

RemoveKeyServerFromProviderKmip

您可以使用此 `RemoveKeyServerFromProviderKmip` 方法、從指派給它的提供者取消指派指定的金鑰管理互通性通訊協定（KMIP）金鑰伺服器。您可以取消指派金鑰伺服器給其供應商、除非該金鑰伺服器是最後一個、而且其供應商處於作用中狀態（提供目前使用中的金鑰）。如果指定的金鑰伺服器未指派給供應商、則不會採取任何行動、也不會傳回錯誤。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyServerID	要取消指派的KMIP金鑰伺服器ID。	整數	無	是的

傳回值

此方法沒有傳回值。只要沒有傳回錯誤、就會將移除視為成功。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "RemoveKeyServerFromProviderKmip",
  "params": {
    "keyServerID": 1
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
    {}
}
```

新的自版本

11.7

SignSshKeys

使用在叢集上啟用 SSH 之後["啟用SSH方法"](#)、您可以使用 `SignSshKeys` 方法來存取節點上的 Shell。

從元素 12.5 開始、`sfreadonly` 新的系統帳戶可在節點上進行基本疑難排解。此 API 可在叢集中的所有節點上使用系統帳戶來啟用 SSH 存取 `sfreadonly`。



除非NetApp支援部門告知、否則系統的任何變更均不受支援、會使您的支援合約失效、並可能導致資料不穩定或無法存取。

使用方法之後、您必須從回應複製金鑰鍵、將其儲存至要啟動SSH連線的系統、然後執行下列命令：

```
ssh -i <identity_file> sfreadonly@<node_ip>
```

`identity_file` 是用於讀取公開金鑰驗證之身分識別（私密金鑰）的檔案、
 `node_ip` 是節點的 IP 位址。有關的更多信息 `identity_file`，請參見 SSH 手冊頁。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
持續時間	介於1到24之間的整數、反映簽署金鑰有效的小時數。如果未指定持續時間、則會使用預設值。	整數	1	否
公共金鑰	<p>如果提供、此參數只會傳回簽署的_public_key、而不會建立完整的金鑰鍵給使用者。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p style="text-align: center;"></p> <p>在瀏覽器中使用 URL 列提交的公開金鑰 '+' 會解譯為間隔和中斷簽署。</p> </div>	字串	null	否

名稱	說明	類型	預設值	必要
sfadmin	當您透過supportAdmin叢集存取進行API呼叫、或當節點不在叢集內時、允許存取sfadmin Shell帳戶。	布林值	錯	否

傳回值

此方法具有下列傳回值：

名稱	說明	類型
Keygen_STATUS	包含已簽署金鑰中的身分識別、允許的主體、以及金鑰的有效開始和結束日期。	字串
Private金鑰	只有當API為終端使用者產生完整的金鑰鍵時、才會傳回私有SSH金鑰值。  此值為Base64編碼；寫入檔案時必須解碼此值、以確保其讀取為有效的私密金鑰。	字串
公開金鑰	只有當API為終端使用者產生完整的金鑰鍵時、才會傳回公開SSH金鑰值。  當您將 <code>public_key</code> 參數傳遞至 API 方法時、回應中只 <code>`signed_public_key`</code> 會傳回該值。	字串
簽名的_public_key	簽署公開金鑰所產生的SSH公開金鑰、無論是由API提供或產生的使用者。	字串

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "SignSshKeys",
  "params": {
    "duration": 2,
    "publicKey": <string>
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": null,
  "result": {
    "signedKeys": {
      "keygen_status": <keygen_status>,
      "signed_public_key": <signed_public_key>
    }
  }
}
```

在此範例中、會簽署並傳回有效的公開金鑰（1-24小時）。

新的自版本

12.5

TestKeyProviderKmpip

您可以使用此 `TestKeyProviderKmpip` 方法來測試指定的金鑰管理互通性通訊協定（KMIP）金鑰提供者是否可連線且運作正常。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyProviderID	要測試的金鑰提供者ID。	整數	無	是的

傳回值

此方法沒有傳回值。只要沒有傳回錯誤、測試就會被視為成功。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "TestKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
    {}
}
```

新的自版本

11.7

TestKeyServerKmip

您可以使用此 `TestKeyServerKmip` 方法來測試指定的金鑰管理互通性通訊協定（KMIP）金鑰伺服器是否可連線且運作正常。

參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
KeyServerID	要測試的KMIP金鑰伺服器ID。	整數	無	是的

傳回值

此方法沒有傳回值。如果未傳回錯誤、則測試視為成功。

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "TestKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

回應範例

此方法會傳回類似下列範例的回應：

```
{
  "id": 1,
  "result":
    {}
}
```

新的自版本

11.7

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 保留隨時變更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。