安全API方法

Element Software

NetApp
April 17, 2024

目錄

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。

- AddKeyServerToProviderKmip
- CreeKeyProviderKmip
- CreKeyServerKmip
- 建立PublicPrivate KeyPair
- 刪除KeyProviderKmip
- 刪除KeyServerKmip
- DisableEncryptionAtRest
- 啟用EncryptionAtRest
- GetClientCertificateSignRequest
- GetKeyProviderKmip
- GetKeyServerKmip
- listKeyProvidersKmip
- listKeyServersKmip
- ModifyKeyServerKmip
- RemoveKeyServerFromProviderKmip
- SignSshKeys
- TestKeyProviderKmip
- TestKeyServerKmip

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"

AddKeyServerToProviderKmip

您可以使用「AddKeyServerToProviderKmip」方法、將金鑰管理互通性傳輸協定（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「RemoveKeyServerFromProviderKmip」方法移除指派。

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": "AddKeyServerToProviderKmip",
  "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

CreeKeyProviderKmip

您可以使用「Create KeyProviderKmip」方法、建立具有指定名稱的金鑰管理互通性傳輸協定（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「Create KeyServerKmip」方法。若要將其指派給供應商、請參閱「AddKeyServerToProviderKmip」。

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
kmipKeyProvider	包含新建立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": "CreateKeyProviderKmip",
  "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「Create KeyServerKmip」方法、建立具有指定屬性的金鑰管理互通性傳輸協定（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「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。	"KeyServerKmip"

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「Create PublicPrivate KeyPair」方法來建立公開和私有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KeyProviderKmip

您可以使用「刪除KeyProviderKmip」方法刪除指定的非作用中金鑰管理互通性傳輸協定（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「刪除KeyServerKmip」方法刪除現有的金鑰管理互通性傳輸協定（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「DisableEncryptionAtRest」方法、移除先前使用「EnablEncryptionAtRest」方法套用至叢集的加密。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加密和/或軟體加密的目前狀態、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。若要停用閒置的軟體加密功能、您需要 "建立新叢集" 停用閒置時的軟體加密。

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「EnablEncryptionAtRest」方法、在叢集上啟用閒置的進階加密標準（AES）256位元加密、讓叢集能夠管理用於每個節點磁碟機的加密金鑰。此功能預設為未啟用。

若要查看叢集上閒置加密和/或軟體加密的目前狀態、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。這只能使用來完成 "建立叢集方法" 將「enableSoftwareEncryptionAtRest」設為「true」。

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。執行此作業之後、指定的供應商會被視為作用中、且在使用「disableEncryptionAtRest」方法停用靜止加密之前、無法刪除。

> 如果您的節點類型的型號以「-NE」結尾、則「EnablEncryptionAtRest」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EnablEncryptionAtRest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「GetClientCertificateSignRequest」方法來產生憑證簽署要求、並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":
"MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
   }
}
```

新的自版本

11.7

GetKeyProviderKmip

您可以使用「GetKeyProviderKmip」方法來擷取有關指定金鑰管理互通性傳輸協定（KMIP）金鑰提供者的資訊。

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

GetKeyServerKmip

您可以使用「GetKeyServerKmip」方法來傳回指定金鑰管理互通性傳輸協定（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。	"KeyServerKmip"

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "GetKeyServerKmip",
  "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「GetSoftwareEncryptionAtRestInfo」方法、取得叢集用來加密閒置資料的軟體加密閒置資訊。

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的非同步結果ID（若有）、如果尚未刪除。「GetSuccessynresult」輸出將包含一個「newkey」欄位、其中包含有關新主金鑰的資訊、以及包含舊金鑰相關資訊的「keyToDecommation」欄位。	整數	是的
州/省	目前的軟體閒置加密狀態。可能的值包括「停用」或「啟用」。	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「ListKeyProvidersKmip」方法擷取所有現有金鑰管理互通性傳輸協定（KMIP）金鑰供應商的清單。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	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： • 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）。 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。	布林值	無	否
kmipKeyProviderHasServerAssigned	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： • 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。 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。	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。	"KeyProviderKmip" 陣列

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "ListKeyProvidersKmip",
  "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

listKeyServersKmip

您可以使用「ListKeyServersKmip」方法、列出已建立的所有金鑰管理互通性傳輸協定（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
kmipAssignedProviderIsActive	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： • 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
kmipHasProviderAssigned	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： • 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。 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。	布林值	無	否

傳回值

此方法具有下列傳回值：

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

申請範例

此方法的要求類似於下列範例：

```
{
  "method": "ListKeyServersKmip",
  "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「ModifyKeyServerKmip」方法、將現有的金鑰管理互通性傳輸協定（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「RekeySoftwareEncryptionAtRestMasterKey」方法重新輸入用來加密DEK（資料加密金鑰）的軟體加密閒置主金鑰。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「keyManagementType」參數、則會使用現有的金鑰管理組態執行重新輸入作業。如果指定了「keyManagementType」、而且金鑰提供者是外部的、則也必須使用「keyProviderID」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」（內部）：使用內部金鑰管理重新輸入金鑰。「外部」：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。這是作爲其中一種"CreateKeyProvider."方法的一部分返回的唯一值。只有當「keyManagementType」為「Extern外部」且無效時、才需要ID。	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「asyncdyle」值搭配「Get非 同步結果」來判斷重新輸入作業的狀態。「GetSuccessynresult」輸出將包含一個「newkey」欄位、其中包含有關新主金鑰的資訊、以及包含舊金鑰相關資訊的「keyToDecommation」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「RemoveKeyServerFromProviderKmip」方法、將指定的金鑰管理互通性傳輸協定（KMIP）金鑰伺服器從指派給它的供應商中取消指派。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「ignSshKeys」方法來存取節點上的Shell。

從元素12.5開始、「sfreadonly」是新的系統帳戶、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「sfreadonly」系統帳戶來啟用SSH存取。

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鏈、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檔案」是用來讀取公開金鑰驗證身分識別（私密金鑰）的檔案、而「node_IP」是節點的IP位址。如需「identity檔案」的詳細資訊、請參閱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	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鏈給使用者。 在瀏覽器中使用URL列提交的公開金鑰若使用「+」、則會解譯為間隔和中斷簽署。	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鏈時、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鏈時、才會傳回公開SSH金鑰值。 ⓘ 當您將public_key參數傳遞給API方法時、回應中只會傳回「inized_public_keys」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%

TestKeyProviderKmip

您可以使用「TestKeyProviderKmip」方法來測試指定的金鑰管理互通性傳輸協定（KMIP）金鑰供應商是否可連線且正常運作。

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「TestKeyServerKmip」方法來測試指定的金鑰管理互通性傳輸協定（KMIP）金鑰伺服器是否可連線且正常運作。

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