安全 API 方法

Element Software

NetApp
November 18, 2025

目錄

安全 API 方法 1
AddKeyServerToProviderKmip 1
參數 1
傳回值 1
請求範例 1
回應範例 1
自版本以來的新版本 2
建立金鑰提供者Kmip 2
參數 2
傳回值 2
請求範例 2
回應範例 3
自版本以來的新版本 3
建立金鑰伺服器Kmip 3
參數 3
傳回值 4
請求範例 4
回應範例 5
自版本以來的新版本 5
創建公鑰/私鑰對 5
參數 6
傳回值 6
請求範例 6
回應範例 7
自版本以來的新版本 7
刪除金鑰提供者Kmip 7
參數 7
傳回值 7
請求範例 8
回應範例 8
自版本以來的新版本 8
刪除金鑰伺服器Kmip 8
參數 8
傳回值 8
請求範例 9
回應範例 9
自版本以來的新版本 9
停用靜態加密 9
參數 9

傳回值 10
請求範例 10
回應範例 10
自版本以來的新版本 10
啟用靜態加密 10
參數 11
傳回值 11
請求範例 11
回答範例 11
自版本以來的新版本 12
取得用戶端憑證簽署請求 13
參數 13
傳回值 13
請求範例 13
回應範例 13
自版本以來的新版本 14
GetKeyProviderKmip 14
參數 14
傳回值 14
請求範例 14
回應範例 14
自版本以來的新版本 15
GetKeyServerKmip 15
參數 15
傳回值 15
請求範例 16
回應範例 16
自版本以來的新版本 16
取得靜態軟體加密訊息 16
參數 17
傳回值 17
請求範例 17
回應範例 17
自版本以來的新版本 18
ListKeyProvidersKmip 18
參數 18
傳回值 19
請求範例 20
回應範例 20
自版本以來的新版本 20
ListKeyServersKmip 20

參數 21
傳回值 22
請求範例 22
回應範例 22
自版本以來的新版本 23
修改金鑰伺服器Kmip 23
參數 23
傳回值 24
請求範例 24
回應範例 25
自版本以來的新版本 25
重新金鑰軟體靜態加密主金鑰 26
參數 26
傳回值 26
請求範例 27
回應範例 27
自版本以來的新版本 27
從提供者中移除金鑰伺服器Kmip 27
參數 27
傳回值 28
請求範例 28
回應範例 28
自版本以來的新版本 28
SignSshKeys 28
參數 29
傳回值 30
請求範例 30
回應範例 31
自版本以來的新版本 31
測試密鑰提供者Kmip 31
參數 31
傳回值 32
請求範例 32
回應範例 32
自版本以來的新版本 32
測試金鑰伺服器Kmip 32
參數 32
傳回值 33
請求範例 33
回應範例 33
自版本以來的新版本 33

安全 API 方法

AddKeyServerToProviderKmip

你可以使用 `AddKeyServerToProviderKmip`將金鑰管理互通協定 (KMIP) 金鑰伺服器指派給指定金鑰提供者的方法。在任務分配過程中，會聯絡伺服器以驗證其功能。如果指定的金鑰伺服器已指派給指定的金鑰提供程序，則不執行任何操作，也不傳回任何錯誤。您可以使用以下方法刪除分配： `RemoveKeyServerFromProviderKmip`方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰提供者ID	要將密鑰伺服器指派給的密鑰提供者的 ID。	整數	沒有任何	是的
密鑰伺服器ID	要分配的密鑰伺服器的 ID。	整數	沒有任何	是的

傳回值

此方法沒有傳回值。只要沒有回傳錯誤，該任務就被視為成功。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

建立金鑰提供者Kmip

你可以使用 `CreateKeyProviderKmip`建立具有指定名稱的金鑰管理互通性協定 (KMIP) 金鑰提供者的方法。金鑰提供者定義了檢索身份驗證金鑰的機制和位置。建立一個新的 KMIP 金鑰提供者時，它沒有任何已指派的 KMIP 金鑰伺服器。若要建立 KMIP 金鑰伺服器，請使用下列方法： `CreateKeyServerKmip`方法。若要將其指派給提供者，請參閱 `AddKeyServerToProviderKmip`。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰提供者名稱	若要與建立的 KMIP 金鑰提供者關聯的名稱。此名稱僅用於顯示目的，無需唯一。	細繩	沒有任何	是的

傳回值

此方法具有以下傳回值：

Name	描述	類型
kmipKeyProvider	包含有關新建立的密鑰提供者詳細資訊的物件。	"金鑰提供者Kmip"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

建立金鑰伺服器Kmip

你可以使用 `CreateKeyServerKmip`建立具有指定屬性的金鑰管理互通協定 (KMIP) 金鑰伺服器的方法。創建過程中不會聯繫伺服器；使用此方法之前伺服器無需存在。對於叢集金鑰伺服器配置，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。你可以使用 `TestKeyServerKmip`測試密鑰伺服器的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
kmipCa證書	外部金鑰伺服器根 CA 的公鑰憑證。這將用於驗證外部金鑰伺服器在 TLS 通訊中提供的憑證。對於關鍵伺服器集群，如果各個伺服器使用不同的 CA，則提供包含所有 CA 根憑證的連接字串。	細繩	沒有任何	是的
kmipClientCertificate	Solidfire KMIP 用戶端使用的 PEM 格式 Base64 編碼 PKCS#10 X.509 憑證。	細繩	沒有任何	是的
kmipKeyServerHostnames	與此 KMIP 金鑰伺服器關聯的主機名稱或 IP 位址陣列。只有當關鍵伺服器處於叢集配置時，才需要提供多個主機名稱或 IP 位址。	字串數組	沒有任何	是的
kmipKeyServerName	KMIP密鑰伺服器的名稱。此名稱僅用於顯示目的，無需唯一。	細繩	沒有任何	是的
kmipKeyServerPort	與此 KMIP 金鑰伺服器關聯的連接埠號碼（通常為 5696）。	整數	沒有任何	不

傳回值

此方法具有以下傳回值：

Name	描述	類型
kmip金鑰伺服器	包含有關新建立的密鑰伺服器詳細資訊的物件。	"金鑰伺服器Kmip"

請求範例

該方法的請求類似於以下範例：

```
{
  "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

此方法傳回類似以下範例的回應：

```
{
   "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
        }
    }
}
```

自版本以來的新版本

11.7

創建公鑰/私鑰對

你可以使用 `CreatePublicPrivateKeyPair`創建公鑰和私鑰的方法。您可以使用這些金鑰產

生憑證簽署請求。每個儲存叢集只能使用一對密鑰。在使用此方法替換現有金鑰之前，請確保金鑰不再被任何提供者使用。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
通用名	X.509 可分辨名稱 通用名稱 欄位 (CN)。	細繩	沒有任何	不
國家	X.509 可分辨名稱 國家 欄位 ©。	細繩	沒有任何	不
電子郵件地址	X.509 專有名稱 電子郵件地址 欄位 (MAIL)。	細繩	沒有任何	不
地點	X.509 可分辨名稱 本地名稱 欄位 (L)。	細繩	沒有任何	不
組織	X.509 可分辨名稱 組織名稱 欄位 (O)。	細繩	沒有任何	不
組織單位	X.509 可分辨名稱 組織單元名稱 欄位 (OU)。	細繩	沒有任何	不
狀態	X.509 可分辨名稱 州或 省名稱 欄位（ST或SP或 S）。	細繩	沒有任何	不

傳回值

此方法沒有傳回值。如果沒有錯誤，則密鑰建立被視為成功。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

刪除金鑰提供者Kmip

你可以使用 `DeleteKeyProviderKmip`刪除指定的非活動金鑰管理互通協定 (KMIP) 金鑰提供者的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰提供者ID	要刪除的密鑰提供者的 ID。	整數	沒有任何	是的

傳回值

此方法沒有傳回值。只要沒有錯誤，刪除操作就被認為是成功的。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

刪除金鑰伺服器Kmip

你可以使用 `DeleteKeyServerKmip`刪除現有金鑰管理互通協定 (KMIP) 金鑰伺服器的方法。除非密鑰伺服器是分配給其提供者的最後一個密鑰伺服器，並且該提供者正在提供當前正在使用的密鑰，否則您可以刪除密鑰伺服器。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰伺服器ID	要刪除的 KMIP 金鑰伺服器的 ID。	整數	沒有任何	是的

傳回值

此方法沒有傳回值。如果沒有錯誤，則刪除操作被視為成功。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

停用靜態加密

你可以使用 `DisableEncryptionAtRest`使用以下方法移除先前應用於叢集的加密：`EnableEncryptionAtRest`方法。此停用方法是異步的，會在加密停用之前回傳回應。你可以使用 `GetClusterInfo`用於輪詢系統以查看進程何時完成的方法。

- 您不能使用此方法停用靜態軟體加密。要停用靜態軟體加密，您需要...“建立一個新集群”已禁用靜態軟體加密。
- 若要查看叢集上靜態加密、靜態軟體加密或兩者的目前狀態，請使用下列方法： “取得集群資訊方法”。你可以使用 `GetSoftwareEncryptionAtRestInfo` “獲取集群用於加密靜態資料的資訊的方法”。

參數

此方法沒有輸入參數。

傳回值

此方法沒有傳回值。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

9.6

查找更多信息

- "獲取集群資訊"
- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

啟用靜態加密

你可以使用 `EnableEncryptionAtRest`啟用叢集上靜態進階加密標準 (AES) 256 位元加密的方法，以便叢集可以管理每個節點上磁碟機使用的加密金鑰。此功能預設未啟用。

- 若要查看叢集上靜態加密和/或靜態軟體加密的目前狀態，請使用下列方法："取得集群資訊方法" 。你可以使用 `GetSoftwareEncryptionAtRestInfo` "獲取集群用於加密靜態資料的資訊的方法"。
- 此方法無法實作靜態軟體加密。這只能透過使用以下方式完成："建立集群方法"和 `enableSoftwareEncryptionAtRest`**設定為** `true`。

啟用靜態加密後，叢集會自動在內部管理叢集中每個節點上磁碟機的加密金鑰。

如果指定了 keyProviderID，則會根據金鑰提供者的類型產生和檢索密碼。對於 KMIP 金鑰提供程序，這通常是透過金鑰管理互通協定 (KMIP) 金鑰伺服器來實現的。此操作完成後，指定的提供者將被視為處於活動狀態，並且只有在使用以下命令停用靜態加密後才能刪除。 `DisableEncryptionAtRest`方法。

如果您有一個型號以“-NE”結尾的節點類型， `EnableEncryptionAtRest`方法呼叫將失敗，並傳回「不允許加密」的回應。叢集偵測到不可加密節點」。

只有當叢集正在運作且處於健康狀態時，才應啟用或停用加密。您可以根據需要隨時啟用或停用加密。

此過程是異步的，會在啟用加密之前回傳回應。你可以使用 `GetClusterInfo`用於輪詢系統以查看進程何時完成的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰提供者ID	要使用的KMIP金鑰提供者的ID。	整數	沒有任何	不

傳回值

此方法沒有傳回值。

請求範例

該方法的請求類似於以下範例：

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

回答範例

此方法傳回的回應類似於 EnableEncryptionAtRest 方法中的下列範例。沒有結果需要報告。

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

當叢集上啟用靜態加密時，GetClusterInfo 傳回的結果會將靜態加密的狀態（「encryptionAtRestState」）描述為「正在啟用」。靜態資料加密完全啟用後，傳回的狀態將變為「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"
      }
   }
}
```

自版本以來的新版本

9.6

查找更多信息

- "安全擦除驅動器"
- "獲取集群資訊"
- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

取得用戶端憑證簽署請求

你可以使用 `GetClientCertificateSignRequest`產生可由憑證授權單位簽署的憑證簽署要求的方法，以便為叢集產生用戶端憑證。需要使用簽章憑證來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

此方法具有以下傳回值：

Name	描述	類型
用戶端憑證簽署請求	PEM 格式 Base64 編碼的 PKCS#10 X.509 用戶端憑證簽署請求。	細繩

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

```
{
   "id": 1,
   "result":
      {
        "clientCertificateSignRequest":
"MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
   }
}
```

自版本以來的新版本

11.7

GetKeyProviderKmip

你可以使用 `GetKeyProviderKmip`檢索指定金鑰管理互通協定 (KMIP) 金鑰提供者的資訊的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰提供者ID	要傳回的 KMIP 金鑰提供者物件的 ID。	整數	沒有任何	是的

傳回值

此方法具有以下傳回值：

Name	描述	類型
kmipKeyProvider	包含有關所請求密鑰提供者詳細資訊的物件。	"金鑰提供者Kmip"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

GetKeyServerKmip

你可以使用 `GetKeyServerKmip`傳回指定金鑰管理互通協定 (KMIP) 金鑰伺服器的資訊的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰伺服器ID	要傳回資訊的 KMIP 金鑰伺服器的 ID。	整數	沒有任何	是的

傳回值

此方法具有以下傳回值：

Name	描述	類型
kmip金鑰伺服器	包含所請求密鑰伺服器詳細資訊的物件。	"金鑰伺服器Kmip"

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

```
{
   "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
        }
    }
}
```

自版本以來的新版本

11.7

取得靜態軟體加密訊息

你可以使用 `GetSoftwareEncryptionAtRestInfo`取得集群用於加密靜態資料的軟體靜態加密資訊的方法。

參數

此方法沒有輸入參數。

傳回值

此方法具有以下傳回值：

範圍	描述	類型	選修的
主密鑰資訊	有關目前軟體靜態加密主金鑰的資訊。	加密金鑰訊息	真的
重新密鑰主密鑰異步結果ID	目前或最近一次重新金鑰操作的非同步結果 ID（如果有），如果尚未刪除。 `GetAsyncResult`輸出將包含 `newKey`包含新主密鑰的資訊的欄位以及 `keyToDecommission`包含舊密鑰資訊的欄位。	整數	真的
狀態	目前軟體靜態加密狀態。可能的值有 `disabled`或者 `enabled`。	細繩	錯誤的
版本	每次啟用靜態軟體加密時，版本號碼都會增加。	整數	錯誤的

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.3

查找更多信息

- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

ListKeyProvidersKmip

你可以使用 `ListKeyProvidersKmip`檢索所有現有金鑰管理互通協定 (KMIP) 金鑰提供者清單的方法。您可以透過指定其他參數來篩選清單。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
keyProviderIsActive	過濾器根據 KMIP 密鑰伺服器物件是否處於活動狀態傳回這些物件。可能的值： • true：僅傳回處於活動狀態的 KMIP 金鑰提供者（提供目前正在使用的金鑰）。 • false：僅傳回不活躍的 KMIP 金鑰提供者（不提供任何金鑰且可以刪除）。 如果省略，則傳回的 KMIP 金鑰提供者不會根據其是否處於活動狀態進行篩選。	布林值	沒有任何	不
kmipKeyProviderHasServerAssigned	根據是否已指派 KMIP 金鑰伺服器，篩選出 KMIP 金鑰提供者。可能的值： • true：僅傳回已指派 KMIP 金鑰伺服器的 KMIP 金鑰提供者。 • false：僅傳回未指派 KMIP 金鑰伺服器的 KMIP 金鑰提供者。 如果省略，則傳回的 KMIP 金鑰提供者不會根據其是否已指派 KMIP 金鑰伺服器進行篩選。	布林值	沒有任何	不

傳回值

此方法具有以下傳回值：

Name	描述	類型

kmipKeyProviders	已建立的 KMIP 金鑰提供者清單。	"金鑰提供者Kmip"大批

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

ListKeyServersKmip

你可以使用 `ListKeyServersKmip`列出所有已建立的金鑰管理互通協定 (KMIP) 金鑰伺服器的方法。您可以透過指定其他參數來篩選結果。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰提供者ID	如果指定了該方法，則該方法僅傳回指派給指定 KMIP 金鑰提供者的 KMIP 金鑰伺服器。如果省略，則傳回的 KMIP 金鑰伺服器將不會根據它們是否指派給指定的 KMIP 金鑰提供者進行篩選。	整數	沒有任何	不
kmipAssignedProviderIsActive	過濾器根據 KMIP 密鑰伺服器物件是否處於活動狀態傳回這些物件。可能的值： • true：僅傳回處於活動狀態的 KMIP 金鑰伺服器（提供目前正在使用的金鑰）。 • false：僅傳回不活躍的 KMIP 金鑰伺服器（不提供任何金鑰且可以刪除）。 如果省略，則傳回的 KMIP 金鑰伺服器不會根據其是否處於活動狀態進行篩選。	布林值	沒有任何	不

Name	描述	類型	預設值	必需的
kmipHasProviderAssigned	根據是否已指派 KMIP 金鑰提供程序，篩選出 KMIP 金鑰伺服器。可能的值： • true：僅傳回已指派 KMIP 金鑰提供者的 KMIP 金鑰伺服器。 • false：僅傳回未指派 KMIP 金鑰提供者的 KMIP 金鑰伺服器。 如果省略，則傳回的 KMIP 金鑰伺服器不會根據其是否已指派 KMIP 金鑰提供者進行篩選。	布林值	沒有任何	不

傳回值

此方法具有以下傳回值：

Name	描述	類型
kmip金鑰伺服器	已建立的 KMIP 金鑰伺服器完整清單。	"金鑰伺服器Kmip"大批

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

修改金鑰伺服器Kmip

你可以使用 `ModifyKeyServerKmip`修改現有金鑰管理互通協定 (KMIP) 金鑰伺服器以使其具有指定屬性的方法。雖然唯一必要的參數是 keyServerID，但僅包含 keyServerID 的請求不會執行任何操作，也不會回傳任何錯誤。您指定的任何其他參數將用指定的 keyServerID 取代金鑰伺服器的現有值。操作過程中會聯繫關鍵伺服器，以確保其正常運作。您可以使用 kmipKeyServerHostnames 參數提供多個主機名稱或 IP 位址，但前提是金鑰伺服器處於叢集配置中。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰伺服器ID	要修改的KMIP金鑰伺服器的ID。	整數	沒有任何	是的

kmipCa證書	外部金鑰伺服器根 CA 的公鑰憑證。這將用於驗證外部金鑰伺服器在 TLS 通訊中提供的憑證。對於關鍵伺服器集群，如果各個伺服器使用不同的 CA，則提供包含所有 CA 根憑證的連接字串。	細繩	沒有任何	不
kmipClientCertificate	Solidfire KMIP 用戶端使用的 PEM 格式 Base64 編碼 PKCS#10 X.509 憑證。	細繩	沒有任何	不
kmipKeyServerHostnames	與此 KMIP 金鑰伺服器關聯的主機名稱或 IP 位址陣列。只有當關鍵伺服器處於叢集配置時，才需要提供多個主機名稱或 IP 位址。	字串數組	沒有任何	不
kmipKeyServerName	KMIP密鑰伺服器的名稱。此名稱僅用於顯示目的，無需唯一。	細繩	沒有任何	不
kmipKeyServerPort	與此 KMIP 金鑰伺服器關聯的連接埠號碼（通常為 5696）。	整數	沒有任何	不

傳回值

此方法具有以下傳回值：

Name	描述	類型
kmip金鑰伺服器	包含有關新修改的密鑰伺服器詳細資訊的物件。	"金鑰伺服器Kmip"

請求範例

該方法的請求類似於以下範例：

```
{
  "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

此方法傳回類似以下範例的回應：

```
{
   "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
        }
    }
}
```

自版本以來的新版本

11.7

重新金鑰軟體靜態加密主金鑰

你可以使用 `RekeySoftwareEncryptionAtRestMasterKey`用於重新產生軟體靜態加密主金鑰的方法，該主金鑰用於加密 DEK（資料加密金鑰）。在叢集建立期間，靜態軟體加密配置為使用內部金鑰管理（IKM）。叢集建立後，可以使用此重新密鑰方法來使用 IKM 或外部密鑰管理 (EKM)。

參數

此方法有以下輸入參數。如果 `keyManagementType`如果未指定參數，則使用現有的金鑰管理組態執行重新金鑰操作。如果 `keyManagementType`已指定金鑰提供者，且金鑰提供者是外部的， `keyProviderID`也必須使用參數。

範圍	描述	類型	選修的
密鑰管理類型	用於管理主密鑰的密鑰管理類型。可能的值有： `Internal` ：使用內部密鑰管理重新產生密鑰。 `External` ：使用外部密鑰管理重新產生密鑰。如果未指定此參數，則使用現有的金鑰管理組態執行重新金鑰操作。	細繩	真的
密鑰提供者ID	要使用的密鑰提供者的ID。這是作為其中一個返回的唯一值 `CreateKeyProvider`方法。僅在以下情況下需要ID： `keyManagementType`是 `External`否則無效。	整數	真的

傳回值

此方法具有以下傳回值：

範圍	描述	類型	選修的
非同步句柄	使用此功能決定重新密鑰操作的狀態。 `asyncHandle`價值 `GetAsyncResult`。 `GetAsyncResult`輸出將包含 `newKey`包含新主密鑰的資訊的欄位以及 `keyToDecommission`包含舊密鑰資訊的欄位。	整數	錯誤的

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

12.3

查找更多信息

- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

從提供者中移除金鑰伺服器Kmip

你可以使用 `RemoveKeyServerFromProviderKmip`從指派給它的提供者取消指派指定的金鑰管理互通協定 (KMIP) 金鑰伺服器的方法。除非是最後一個金鑰伺服器且其提供者處於活動狀態（提供目前正在使用的金鑰），否則您可以從其提供者取消指派金鑰伺服器。如果指定的金鑰伺服器未指派給提供者，則不執行任何操作，也不傳回任何錯誤。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰伺服器ID	若要取消已指派的 KMIP 金鑰伺服器的 ID。	整數	沒有任何	是的

傳回值

此方法沒有傳回值。只要沒有回傳錯誤，刪除操作就被認為是成功的。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

SignSshKeys

在叢集上啟用 SSH 後，使用下列方法："啟用SSH方法"你可以使用 `SignSshKeys`取得節點上 shell 的方法。

從第 12.5 節開始， `sfreadonly`新的系統帳戶允許對節點進行基本故障排除。此 API 允許使用 SSH 進行存取 `sfreadonly`叢集中所有節點上的系統帳戶。

除非NetApp支援部門另行通知，否則對系統進行的任何變更均不受支持，這將使您的支援合約失效，並可能導致資料不穩定或無法存取。

使用此方法後，必須從回應複製金鑰鏈，將其儲存到將發起 SSH 連線的系統，然後執行下列命令：

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

`identity_file`這是一個用於讀取公鑰認證的身份資訊（私鑰）的檔案； `node_ip`是節點的 IP 位址。欲了解更多信息 `identity_file`請參閱 SSH 手冊頁。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
期間	1 到 24 之間的整數，表示簽署金鑰的有效小時數。如果未指定持續時間，則使用預設值。	整數	1	不
公鑰	如果提供此參數，則只會傳回已簽署的公鑰，而不會為使用者建立完整的金鑰鏈。 使用瀏覽器網址列提交的公鑰 `+` 被解讀為間隔和斷斷續續的手語。	細繩	無效的	不

Name	描述	類型	預設值	必需的
sfadmin	允許在使用 supportAdmin 叢集存取權限進行 API 呼叫時，或節點不在叢集中時，存取 sfadmin shell 帳戶。	布林值	錯誤的	不

傳回值

此方法具有以下傳回值：

Name	描述	類型
密鑰產生器狀態	包含已簽署金鑰中的身分資訊、允許的主體以及金鑰的有效開始日期和結束日期。	細繩
私鑰	只有當 API 為最終使用者產生完整的金鑰鏈時，才會傳回私有 SSH 金鑰值。 該值採用 Base64 編碼；寫入檔案時必須對其進行解碼，以確保其能被讀取為有效的私鑰。	細繩
公鑰	只有當 API 為最終使用者產生完整的金鑰鏈時，才會傳回公共 SSH 金鑰值。 當您將 public_key 參數傳遞給 API 方法時，只有 `signed_public_key` 響應中會傳回該值。	細繩
已簽署公鑰	透過對公鑰進行簽署而產生的 SSH 公鑰，無論該公鑰是用戶提供的還是由 API 產生的。	細繩

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

在這個例子中，會簽署並傳回一個在指定時間（1-24 小時）內有效的公鑰。

自版本以來的新版本

12.5

測試密鑰提供者Kmip

你可以使用 `TestKeyProviderKmip`測試指定的金鑰管理互通協定 (KMIP) 金鑰提供者是否可達且運作正常的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰提供者ID	要測試的密鑰提供者的 ID。	整數	沒有任何	是的

傳回值

此方法沒有傳回值。只要沒有回傳錯誤，測試就被認為是成功的。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7

測試金鑰伺服器Kmip

你可以使用 `TestKeyServerKmip`測試指定的金鑰管理互通協定 (KMIP) 金鑰伺服器是否可達且運作正常的方法。

參數

此方法有以下輸入參數：

Name	描述	類型	預設值	必需的
密鑰伺服器ID	要測試的KMIP金鑰伺服器的ID。	整數	沒有任何	是的

傳回值

此方法沒有傳回值。如果沒有傳回錯誤，則測試被視為成功。

請求範例

該方法的請求類似於以下範例：

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

回應範例

此方法傳回類似以下範例的回應：

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

自版本以來的新版本

11.7