安全 API 方法

Element Software

NetApp
November 18, 2025

目录

安全 API 方法

AddKeyServerToProviderKmip

你可以使用 `AddKeyServerToProviderKmip`将密钥管理互操作协议 (KMIP) 密钥服务器分配给指定密钥提供程序的方法。在任务分配过程中，会联系服务器以验证其功能。如果指定的密钥服务器已分配给指定的密钥提供程序，则不执行任何操作，也不返回任何错误。您可以使用以下方法删除分配： `RemoveKeyServerFromProviderKmip`方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥提供程序ID	要将密钥服务器分配给的密钥提供程序的ID。	整数	无	是
密钥服务器ID	要分配的密钥服务器的 ID。	整数	无	是

返回值

此方法没有返回值。只要没有返回错误，该任务就被视为成功。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

创建密钥提供程序Kmip

你可以使用 `CreateKeyProviderKmip`创建具有指定名称的密钥管理互操作性协议 (KMIP) 密钥提供程序的方法。密钥提供者定义了检索身份验证密钥的机制和位置。创建一个新的 KMIP 密钥提供程序时，它没有任何已分配的 KMIP 密钥服务器。要创建 KMIP 密钥服务器，请使用以下方法： `CreateKeyServerKmip`方法。要将其分配给提供者，请参阅 `AddKeyServerToProviderKmip`。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥提供程序名称	要与创建的 KMIP 密钥提供程序关联的名称。此名称仅用于显示目的，无需唯一。	string	无	是

返回值

此方法具有以下返回值：

名称	描述	类型
kmipKeyProvider	包含有关新创建的密钥提供程序详细信息的对象。	"密钥提供商Kmip"

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

创建密钥服务器Kmip

你可以使用 `CreateKeyServerKmip`创建具有指定属性的密钥管理互操作协议 (KMIP) 密钥服务器的方法。创建过程中不会联系服务器；使用此方法之前服务器无需存在。对于集群密钥服务器配置，您必须在 kmipKeyServerHostnames 参数中提供所有服务器节点的主机名或 IP 地址。你可以使用 `TestKeyServerKmip`测试密钥服务器的方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
kmipCa证书	外部密钥服务器根 CA 的公钥证书。这将用于验证外部密钥服务器在 TLS 通信中提供的证书。对于关键服务器集群，如果各个服务器使用不同的 CA，则提供一个包含所有 CA 根证书的连接字符串。	string	无	是
kmipClientCertificate	Solidfire KMIP 客户端使用的 PEM 格式 Base64 编码 PKCS#10 X.509 证书。	string	无	是
kmipKeyServerHostnames	与此 KMIP 密钥服务器关联的主机名或 IP 地址数组。只有当关键服务器处于集群配置中时，才需要提供多个主机名或 IP 地址。	字符串数组	无	是
kmipKeyServerName	KMIP密钥服务器的名称。此名称仅用于显示目的，无需唯一。	string	无	是
kmipKeyServerPort	与此 KMIP 密钥服务器关联的端口号（通常为 5696）。	整数	无	否

返回值

此方法具有以下返回值：

名称	描述	类型
kmip密钥服务器	包含有关新创建的密钥服务器详细信息的对象。	"密钥服务器Kmip"

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

```
{
   "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
        }
    }
}
```

自版本以来的新版本

11.7

创建公钥/私钥对

你可以使用 `CreatePublicPrivateKeyPair`创建公钥和私钥的方法。您可以使用这些密钥生

成证书签名请求。每个存储集群只能使用一对密钥。使用此方法替换现有密钥之前，请确保密钥不再被任何提供商使用。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
通用名	X.509 可分辨名称 通用名称 字段 (CN)。	string	无	否
国家	X.509 可分辨名称 国家 字段 ©。	string	无	否
电子邮件地址	X.509 专有名称 电子邮件地址 字段 (MAIL)。	string	无	否
地点	X.509 可分辨名称 本地名称 字段 (L)。	string	无	否
组织	X.509 可分辨名称 组织名称 字段 (O)。	string	无	否
组织单位	X.509 可分辨名称 组织单元名称 字段 (OU)。	string	无	否
状态	X.509 可分辨名称 州或 省名称 字段（ST或SP或 S）。	string	无	否

返回值

此方法没有返回值。如果没有错误，则密钥创建被视为成功。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

删除密钥提供程序Kmip

你可以使用 `DeleteKeyProviderKmip`删除指定的非活动密钥管理互操作协议 (KMIP) 密钥提供程序的方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥提供程序ID	要删除的密钥提供程序的 ID。	整数	无	是

返回值

此方法没有返回值。只要没有错误，删除操作就被认为是成功的。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

删除密钥服务器Kmip

你可以使用 `DeleteKeyServerKmip`删除现有密钥管理互操作协议 (KMIP) 密钥服务器的方法。除非密钥服务器是分配给其提供商的最后一个密钥服务器，并且该提供商正在提供当前正在使用的密钥，否则您可以删除密钥服务器。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥服务器ID	要删除的 KMIP 密钥服务器的 ID。	整数	无	是

返回值

此方法没有返回值。如果没有错误，则删除操作被视为成功。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

禁用静态加密

你可以使用 `DisableEncryptionAtRest`使用以下方法移除先前应用于集群的加密：`EnableEncryptionAtRest`方法。此禁用方法是异步的，会在禁用加密之前返回响应。你可以使用 `GetClusterInfo`用于轮询系统以查看进程何时完成的方法。

- 您不能使用此方法禁用静态软件加密。要禁用静态软件加密，您需要.....“创建一个新集群”已禁用静态软件加密。
- 要查看集群上静态加密、静态软件加密或两者的当前状态，请使用以下方法： “获取集群信息方法”。你可以使用 `GetSoftwareEncryptionAtRestInfo` “获取集群用于加密静态数据的信息的方法”。

参数

此方法没有输入参数。

返回值

此方法没有返回值。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

9.6

查找更多信息

- "获取集群信息"
- "SolidFire和 Element 软件文档"
- "NetApp SolidFire和 Element 产品早期版本的文档"

启用静态加密

你可以使用 `EnableEncryptionAtRest`启用集群上静态高级加密标准 (AES) 256 位加密的方法，以便集群可以管理每个节点上驱动器使用的加密密钥。默认情况下不会启用此功能。

- 要查看集群上静态加密和/或静态软件加密的当前状态，请使用以下方法："获取集群信息方法"。你可以使用 `GetSoftwareEncryptionAtRestInfo` "获取集群用于加密静态数据的信息的方法"。
- 此方法无法实现静态软件加密。这只能通过使用以下方式完成："创建集群方法"和 `enableSoftwareEncryptionAtRest`设置为 `true`。

启用静态加密后，集群会自动在内部管理集群中每个节点上驱动器的加密密钥。

如果指定了 keyProviderID，则会根据密钥提供程序的类型生成和检索密码。对于 KMIP 密钥提供程序，这通常是通过密钥管理互操作协议 (KMIP) 密钥服务器来实现的。此操作完成后，指定的提供程序将被视为处于活动状态，并且只有在使用以下命令禁用静态加密后才能删除。 `DisableEncryptionAtRest`方法。

如果您有一个型号以“-NE”结尾的节点类型， `EnableEncryptionAtRest`方法调用将失败，并返回“不允许加密”的响应。集群检测到不可加密节点”。

只有当集群正在运行且处于健康状态时，才应启用或禁用加密。您可以根据需要随时启用或禁用加密。

此过程是异步的，会在启用加密之前返回响应。你可以使用 `GetClusterInfo`用于轮询系统以查看进程何时完成的方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥提供程序ID	要使用的KMIP密钥提供程序的ID。	整数	无	否

返回值

此方法没有返回值。

请求示例

该方法的请求类似于以下示例：

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

回答示例

此方法返回的响应类似于 EnableEncryptionAtRest 方法中的以下示例。没有结果需要报告。

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

当集群上启用静态加密时，GetClusterInfo 返回的结果会将静态加密的状态（“encryptionAtRestState”）描述为“正在启用”。静态数据加密完全启用后，返回的状态将变为“已启用”。

```
{
   "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"
      }
   }
}
```

自版本以来的新版本

9.6

查找更多信息

- "SecureEraseDrives"
- "获取集群信息"
- "SolidFire和 Element 软件文档"
- "NetApp SolidFire和 Element 产品早期版本的文档"

获取客户端证书签名请求

你可以使用 `GetClientCertificateSignRequest`生成可由证书颁发机构签名的证书签名请求的方法，以便为集群生成客户端证书。需要使用签名证书来建立与外部服务交互的信任关系。

参数

此方法没有输入参数。

返回值

此方法具有以下返回值：

名称	描述	类型
客户端证书签名请求	PEM 格式 Base64 编码的 PKCS#10 X.509 客户端证书签名请求。	string

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

GetKeyProviderKmip

你可以使用 `GetKeyProviderKmip`检索有关指定密钥管理互操作协议 (KMIP) 密钥提供程序的信息的方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥提供程序ID	要返回的 KMIP 密钥提供程序对象的 ID。	整数	无	是

返回值

此方法具有以下返回值：

名称	描述	类型
kmipKeyProvider	包含有关所请求密钥提供程序详细信息的对象。	"密钥提供商Kmip"

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

GetKeyServerKmip

你可以使用 `GetKeyServerKmip`返回有关指定密钥管理互操作协议 (KMIP) 密钥服务器的信息的方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥服务器ID	要返回信息的 KMIP 密钥服务器的 ID。	整数	无	是

返回值

此方法具有以下返回值：

名称	描述	类型
kmip密钥服务器	包含所请求密钥服务器详细信息的对象。	"密钥服务器Kmip"

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

```
{
   "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
        }
    }
}
```

自版本以来的新版本

11.7

获取静态软件加密信息

你可以使用 `GetSoftwareEncryptionAtRestInfo`获取集群用于加密静态数据的软件静态加密信息的方法。

参数

此方法没有输入参数。

返回值

此方法具有以下返回值：

参数	描述	类型	可选
主密钥信息	有关当前软件静态加密主密钥的信息。	加密密钥信息	True
重新密钥主密钥异步结果ID	当前或最近一次重新密钥操作的异步结果 ID（如果有），如果尚未删除。`GetAsyncResult`输出将包含 `newKey`包含有关新主密钥的信息的字段以及`keyToDecommission`包含旧密钥信息的字段。	整数	True
状态	当前软件静态加密状态。可能的值有 `disabled`或者 `enabled`。	string	False
version	每次启用静态软件加密时，版本号都会递增。	整数	False

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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


自版本以来的新版本

12.3

查找更多信息

- "SolidFire和 Element 软件文档"
- "NetApp SolidFire和 Element 产品早期版本的文档"

ListKeyProvidersKmip

你可以使用 `ListKeyProvidersKmip`检索所有现有密钥管理互操作协议 (KMIP) 密钥提供程序列表的方法。您可以通过指定其他参数来筛选列表。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
keyProviderIsActive	过滤器根据 KMIP 密钥服务器对象是否处于活动状态返回这些对象。可能值： • true：仅返回处于活动状态的 KMIP 密钥提供程序（提供当前正在使用的密钥）。 • false：仅返回不活跃的 KMIP 密钥提供程序（不提供任何密钥且可以删除）。 如果省略，则返回的 KMIP 密钥提供程序不会根据其是否处于活动状态进行筛选。	布尔值	无	否
kmipKeyProviderHasServerAssigned	根据是否已分配 KMIP 密钥服务器，筛选出 KMIP 密钥提供程序。可能值： • true：仅返回已分配 KMIP 密钥服务器的 KMIP 密钥提供程序。 • false：仅返回未分配 KMIP 密钥服务器的 KMIP 密钥提供程序。 如果省略，则返回的 KMIP 密钥提供程序不会根据其是否已分配 KMIP 密钥服务器进行筛选。	布尔值	无	否

返回值

此方法具有以下返回值：

名称	描述	类型

kmipKeyProviders	已创建的 KMIP 密钥提供程序列表。	"密钥提供商Kmip"大批

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

ListKeyServersKmip

你可以使用 `ListKeyServersKmip`列出所有已创建的密钥管理互操作协议 (KMIP) 密钥服务器的方法。您可以通过指定其他参数来筛选结果。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥提供程序ID	如果指定了该方法，则该方法仅返回分配给指定 KMIP 密钥提供程序的 KMIP 密钥服务器。如果省略，则返回的 KMIP 密钥服务器将不会根据它们是否分配给指定的 KMIP 密钥提供程序进行筛选。	整数	无	否
kmipAssignedProviderIsActive	过滤器根据 KMIP 密钥服务器对象是否处于活动状态返回这些对象。可能值： • true：仅返回处于活动状态的 KMIP 密钥服务器（提供当前正在使用的密钥）。 • false：仅返回不活跃的 KMIP 密钥服务器（不提供任何密钥且可以删除）。 如果省略，则返回的 KMIP 密钥服务器不会根据其是否处于活动状态进行筛选。	布尔值	无	否

名称	描述	类型	默认值	必填项
kmipHasProviderAssigned	根据是否已分配 KMIP 密钥提供程序，筛选出 KMIP 密钥服务器。可能值： • true：仅返回已分配 KMIP 密钥提供程序的 KMIP 密钥服务器。 • false：仅返回未分配 KMIP 密钥提供程序的 KMIP 密钥服务器。 如果省略，则返回的 KMIP 密钥服务器不会根据其是否已分配 KMIP 密钥提供程序进行筛选。	布尔值	无	否

返回值

此方法具有以下返回值：

名称	描述	类型
kmip密钥服务器	已创建的 KMIP 密钥服务器完整列表。	"密钥服务器Kmip"大批

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

修改密钥服务器Kmip

你可以使用 `ModifyKeyServerKmip`修改现有密钥管理互操作协议 (KMIP) 密钥服务器以使其具有指定属性的方法。虽然唯一必需的参数是 keyServerID，但仅包含 keyServerID 的请求不会执行任何操作，也不会返回任何错误。您指定的任何其他参数都将用指定的 keyServerID 替换密钥服务器的现有值。操作过程中会联系关键服务器，以确保其正常运行。您可以使用 kmipKeyServerHostnames 参数提供多个主机名或 IP 地址，但前提是密钥服务器处于集群配置中。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥服务器ID	要修改的KMIP密钥服务器的ID。	整数	无	是

kmipCa证书	外部密钥服务器根 CA 的公钥证书。这将用于验证外部密钥服务器在 TLS 通信中提供的证书。对于关键服务器集群，如果各个服务器使用不同的 CA，则提供一个包含所有 CA 根证书的连接字符串。	string	无	否
kmipClientCertificate	Solidfire KMIP 客户端使用的 PEM 格式 Base64 编码 PKCS#10 X.509 证书。	string	无	否
kmipKeyServerHostnames	与此 KMIP 密钥服务器关联的主机名或 IP 地址数组。只有当关键服务器处于集群配置中时，才需要提供多个主机名或 IP 地址。	字符串数组	无	否
kmipKeyServerName	KMIP密钥服务器的名称。此名称仅用于显示目的，无需唯一。	string	无	否
kmipKeyServerPort	与此 KMIP 密钥服务器关联的端口号（通常为 5696）。	整数	无	否

返回值

此方法具有以下返回值：

名称	描述	类型
kmip密钥服务器	包含有关新修改的密钥服务器详细信息的对象。	"密钥服务器Kmip"

请求示例

该方法的请求类似于以下示例：

```
{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

响应示例

此方法返回类似于以下示例的响应：

```
{
   "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
        }
    }
}
```

自版本以来的新版本

11.7

重新密钥软件静态加密主密钥

你可以使用 `RekeySoftwareEncryptionAtRestMasterKey`用于重新生成软件静态加密主密钥的方法，该主密钥用于加密 DEK（数据加密密钥）。在集群创建期间，静态软件加密配置为使用内部密钥管理（IKM）。集群创建后，可以使用此重新密钥方法来使用 IKM 或外部密钥管理 (EKM)。

参数

该方法有以下输入参数。如果 `keyManagementType`如果未指定参数，则使用现有的密钥管理配置执行重新密钥操作。如果 `keyManagementType`已指定密钥提供者，且密钥提供者是外部的， `keyProviderID`还必须使用参数。

参数	描述	类型	可选
密钥管理类型	用于管理主密钥的密钥管理类型。可能的值有：`Internal`： 使用内部密钥管理重新生成密钥。`External`： 使用外部密钥管理重新生成密钥。如果未指定此参数，则使用现有的密钥管理配置执行重新密钥操作。	string	True
密钥提供程序ID	要使用的密钥提供程序的ID。这是作为其中一个返回的唯一值 `CreateKeyProvider`方法。仅在以下情况下需要ID： `keyManagementType`是 `External`否则无效。	整数	True

返回值

此方法具有以下返回值：

参数	描述	类型	可选
异步句柄	使用此功能确定重新密钥操作的状态。`asyncHandle`具有价值 `GetAsyncResult`。 `GetAsyncResult`输出将包含 `newKey`包含有关新主密钥的信息的字段以及 `keyToDecommission`包含旧密钥信息的字段。	整数	False

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

12.3

查找更多信息

- "SolidFire和 Element 软件文档"
- "NetApp SolidFire和 Element 产品早期版本的文档"

从提供程序中移除密钥服务器Kmip

你可以使用 `RemoveKeyServerFromProviderKmip`从分配给它的提供商处取消分配指定的密钥管理互操作协议 (KMIP) 密钥服务器的方法。除非是最后一个密钥服务器且其提供商处于活动状态（提供当前正在使用的密钥），否则您可以从其提供商处取消分配密钥服务器。如果指定的密钥服务器未分配给提供商，则不执行任何操作，也不返回任何错误。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥服务器ID	要取消分配的 KMIP 密钥服务器的 ID。	整数	无	是

返回值

此方法没有返回值。只要没有返回错误，删除操作就被认为是成功的。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

SignSshKeys

在集群上启用 SSH 后，使用以下方法："启用SSH方法"你可以使用 `SignSshKeys`获取节点上 shell 的方法。

从第 12.5 节开始， `sfreadonly`新的系统帐户允许对节点进行基本故障排除。此 API 允许使用 SSH 进行访问 `sfreadonly`集群中所有节点上的系统帐户。

除非NetApp支持部门另行通知，否则对系统进行的任何更改均不受支持，这将使您的支持合同失效，并可能导致数据不稳定或无法访问。

使用此方法后，必须从响应中复制密钥链，将其保存到将发起 SSH 连接的系统，然后运行以下命令：

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

`identity_file`这是一个用于读取公钥认证的身份信息（私钥）的文件； `node_ip`是节点的 IP 地址。欲了解更多信息 `identity_file`请参阅 SSH 手册页。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
期间	1 到 24 之间的整数，表示签名密钥的有效小时数。如果未指定持续时间，则使用默认值。	整数	1	否
公钥	如果提供此参数，则只会返回签名的公钥，而不会为用户创建完整的密钥链。 使用浏览器地址栏提交的公钥 `+` 被解读为间隔和断续的手语。	string	无效的	否
sfadmin	允许在使用 supportAdmin 集群访问权限进行 API 调用时，或者当节点不在集群中时，访问 sfadmin shell 帐户。	布尔值	False	否

返回值

此方法具有以下返回值：

名称	描述	类型
密钥生成器状态	包含已签名密钥中的身份信息、允许的主体以及密钥的有效开始日期和结束日期。	string
私钥	只有当 API 为最终用户生成完整的密钥链时，才会返回私有 SSH 密钥值。 该值采用 Base64 编码；写入文件时必须对其进行解码，以确保其能被读取为有效的私钥。	string
公钥	只有当 API 为最终用户生成完整的密钥链时，才会返回公共 SSH 密钥值。 当您将 public_key 参数传递给 API 方法时，只有 `signed_public_key` 响应中会返回该值。	string
已签名公钥	通过对公钥进行签名而生成的 SSH 公钥，无论该公钥是用户提供的还是 API 生成的。	string

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

在这个例子中，会签名并返回一个在指定时间（1-24 小时）内有效的公钥。

自版本以来的新版本

12.5

测试密钥提供程序Kmip

你可以使用 `TestKeyProviderKmip`测试指定的密钥管理互操作协议 (KMIP) 密钥提供程序是否可达且运行正常的方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥提供程序ID	要测试的密钥提供程序的 ID。	整数	无	是

返回值

此方法没有返回值。只要没有返回错误，测试就被认为是成功的。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7

测试密钥服务器Kmip

你可以使用 `TestKeyServerKmip`测试指定的密钥管理互操作协议 (KMIP) 密钥服务器是否可达且运行正常的方法。

参数

该方法有以下输入参数：

名称	描述	类型	默认值	必填项
密钥服务器ID	要测试的KMIP密钥服务器的ID。	整数	无	是

返回值

此方法没有返回值。如果没有返回错误，则测试被视为成功。

请求示例

该方法的请求类似于以下示例：

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

响应示例

此方法返回类似于以下示例的响应：

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

自版本以来的新版本

11.7