Métodos da API de segurança

Element Software

NetApp
November 18, 2025

Índice

Métodos da API de segurança

AddKeyServerToProviderKmip

Você pode usar o `AddKeyServerToProviderKmip` Método para atribuir um servidor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) ao provedor de chaves especificado. Durante a atribuição, o servidor é contatado para verificar a funcionalidade. Se o servidor de chaves especificado já estiver atribuído ao provedor de chaves especificado, nenhuma ação será tomada e nenhum erro será retornado. Você pode remover a tarefa usando o `RemoveKeyServerFromProviderKmip` método.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do provedor de chave	O ID do provedor de chaves ao qual o servidor de chaves será atribuído.	inteiro	Nenhum	Sim
ID do servidor de chaves	O ID do servidor de chaves a ser atribuído.	inteiro	Nenhum	Sim

Valores de retorno

Este método não possui valor de retorno. A tarefa é considerada bem-sucedida desde que nenhum erro seja retornado.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

CriarProvedorDeChavesKmip

Você pode usar o `CreateKeyProviderKmip` Método para criar um provedor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) com o nome especificado. Um provedor de chaves define um mecanismo e um local para recuperar chaves de autenticação. Ao criar um novo provedor de chaves KMIP, nenhum servidor de chaves KMIP é atribuído a ele. Para criar um servidor de chaves KMIP, use o `CreateKeyServerKmip` método. Para atribuí-lo a um provedor, consulte `AddKeyServerToProviderKmip` .

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
nomeDoProvedorDeChaves	O nome a ser associado ao provedor de chaves KMIP criado. Este nome é usado apenas para fins de exibição e não precisa ser único.	corda	Nenhum	Sim

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo

kmipKeyProvider	Um objeto contendo detalhes sobre o provedor de chaves recém-criado.	"Provedor de chave Kmip"

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

CriarKeyServerKmip

Você pode usar o `CreateKeyServerKmip` Método para criar um servidor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) com os atributos

especificados. Durante a criação, o servidor não é contatado; ele não precisa existir antes de você usar este método. Para configurações de servidor de chaves em cluster, você deve fornecer os nomes de host ou endereços IP de todos os nós do servidor no parâmetro kmipKeyServerHostnames. Você pode usar o `TestKeyServerKmip` Método para testar um servidor de chaves.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
kmipCaCertificado	O certificado de chave pública da autoridade certificadora raiz do servidor de chaves externo. Isso será usado para verificar o certificado apresentado pelo servidor de chaves externo na comunicação TLS. Para clusters de servidores principais onde servidores individuais usam diferentes CAs, forneça uma string concatenada contendo os certificados raiz de todas as CAs.	corda	Nenhum	Sim
kmipClientCertificate	Um certificado PKCS#10 X.509 codificado em Base64 no formato PEM, usado pelo cliente Solidfire KMIP.	corda	Nenhum	Sim

Nome	Descrição	Tipo	Valor padrão	Obrigatório
kmipKeyServerHostnames	Matriz de nomes de host ou endereços IP associados a este servidor de chaves KMIP. Só é necessário fornecer vários nomes de host ou endereços IP se os servidores principais estiverem em uma configuração de cluster.	matriz de strings	Nenhum	Sim
kmipKeyServerName	O nome do servidor de chaves KMIP. Este nome é usado apenas para fins de exibição e não precisa ser único.	corda	Nenhum	Sim
kmipKeyServerPort	O número da porta associada a este servidor de chaves KMIP (normalmente 5696).	inteiro	Nenhum	Não

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
kmipKeyServer	Um objeto contendo detalhes sobre o servidor de chaves recém-criado.	"Servidor de chaves Kmip"

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

```
{
   "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
        }
    }
}
```

Novidade desde a versão

11,7

CriarParDeChavesPúblicasPrivadas

Você pode usar o `CreatePublicPrivateKeyPair` Método para criar chaves SSL públicas e privadas. Você pode usar essas chaves para gerar solicitações de assinatura

de certificado. Só pode haver um par de chaves em uso para cada cluster de armazenamento. Antes de usar este método para substituir chaves existentes, certifique-se de que as chaves não estejam mais em uso por nenhum provedor.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
nome comum	O campo **Nome Comum** (CN) do nome distinto X.509.	corda	Nenhum	Não
país	O campo de nome distinto X.509 **País** ©.	corda	Nenhum	Não
endereço de email	O campo de nome distinto X.509 **Endereço de e-mail** (MAIL).	corda	Nenhum	Não
localidade	O campo **Nome da Localidade** do nome distinto X.509 (L).	corda	Nenhum	Não
organização	O campo de nome distinto X.509 **Nome da Organização** (O).	corda	Nenhum	Não
Unidade organizacional	O campo **Nome da Unidade Organizacional** (OU) do nome distinto X.509.	corda	Nenhum	Não
estado	O campo **Estado** ou **Nome da Província** do nome distinto X.509 (ST, SP ou S).	corda	Nenhum	Não

Valores de retorno

Este método não possui valores de retorno. Se não houver erros, a criação da chave é considerada bem-sucedida.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

DeleteKeyProviderKmip

Você pode usar o `DeleteKeyProviderKmip` Método para excluir o provedor de chaves KMIP (Key Management Interoperability Protocol) inativo especificado.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do provedor de chave	O ID do provedor de chaves a ser excluído.	inteiro	Nenhum	Sim

Valores de retorno

Este método não possui valores de retorno. A operação de exclusão é considerada bem-sucedida desde que não haja erros.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

DeleteKeyServerKmip

Você pode usar o `DeleteKeyServerKmip` Método para excluir um servidor de chaves KMIP (Key Management Interoperability Protocol) existente. Você pode excluir um servidor de chaves, a menos que seja o último atribuído ao seu provedor e que esse provedor esteja fornecendo chaves que estejam atualmente em uso.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do servidor de chaves	O ID do servidor de chaves KMIP a ser excluído.	inteiro	Nenhum	Sim

Valores de retorno

Este método não retorna valores. A operação de exclusão é considerada bem-sucedida se não houver erros.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

Desativar a criptografia em repouso

Você pode usar o `DisableEncryptionAtRest` método para remover a criptografia que foi aplicada anteriormente ao cluster usando o `EnableEncryptionAtRest` método. Este método de desativação é assíncrono e retorna uma resposta antes que a criptografia seja desativada. Você pode usar o `GetClusterInfo` Método para consultar o sistema e verificar quando o processo foi concluído.

- Não é possível usar esse método para desativar a criptografia de software em repouso. Para desativar a criptografia de software em repouso, você precisa"criar um novo cluster" Com a criptografia de software em repouso desativada.
- Para visualizar o estado atual da criptografia em repouso, da criptografia de software em repouso ou de ambas no cluster, utilize o "método para obter informações do cluster". Você pode usar o `GetSoftwareEncryptionAtRestInfo` "Método para obter informações que o cluster usa para criptografar dados em repouso.".

Parâmetros

Este método não possui parâmetros de entrada.

Valores de retorno

Este método não possui valores de retorno.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

9,6

Encontre mais informações

- "Obter informações do cluster"
- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

Habilitar criptografia em repouso

Você pode usar o `EnableEncryptionAtRest` Método para habilitar a criptografia AES (Advanced Encryption Standard) de 256 bits em repouso no cluster, permitindo que o cluster gerencie a chave de criptografia usada para as unidades em cada nó. Essa funcionalidade não está ativada por padrão.

- Para visualizar o estado atual da criptografia em repouso e/ou da criptografia de software em repouso no cluster, utilize o"método para obter informações do cluster" . Você pode usar o `GetSoftwareEncryptionAtRestInfo` "Método para obter informações que o cluster usa para criptografar dados em repouso.".
- Este método não permite a criptografia de software em repouso. Isso só pode ser feito usando o"método de criação de cluster" com `enableSoftwareEncryptionAtRest` definido para `true` .

Ao ativar a criptografia em repouso, o cluster gerencia automaticamente as chaves de criptografia internamente para as unidades em cada nó do cluster.

Se um ID de provedor de chaves for especificado, a senha será gerada e recuperada de acordo com o tipo de provedor de chaves. Isso geralmente é feito usando um servidor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP), no caso de um provedor de chaves KMIP. Após esta operação, o provedor especificado é considerado ativo e não pode ser excluído até que a criptografia em repouso seja desativada usando o `DisableEncryptionAtRest` método.

Se você tiver um tipo de nó com um número de modelo que termina em "-NE", o `EnableEncryptionAtRest` A chamada do método falhará com a resposta "Criptografia não permitida". O cluster detectou um nó não criptografável.

Você só deve habilitar ou desabilitar a criptografia quando o cluster estiver em execução e funcionando corretamente. Você pode ativar ou desativar a criptografia conforme sua necessidade e com a frequência que desejar.

Este processo é assíncrono e retorna uma resposta antes que a criptografia seja ativada. Você pode usar o `GetClusterInfo` Método para consultar o sistema e verificar quando o processo foi concluído.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do provedor de chave	O ID de um provedor de chaves KMIP a ser utilizado.	inteiro	Nenhum	Não

Valores de retorno

Este método não possui valores de retorno.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplos de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir, proveniente do método EnableEncryptionAtRest. Não há resultados a relatar.

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

Enquanto a criptografia em repouso estiver sendo habilitada em um cluster, GetClusterInfo retorna um resultado descrevendo o estado da criptografia em repouso ("encryptionAtRestState") como "habilitando". Após a criptografia em repouso estar totalmente ativada, o estado retornado muda para "ativado".

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


Novidade desde a versão

9,6

Encontre mais informações

- "Unidades SecureErase"
- "Obter informações do cluster"
- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

Solicitação de assinatura de certificado de cliente

Você pode usar o `GetClientCertificateSignRequest` Método para gerar uma solicitação de assinatura de certificado que pode ser assinada por uma autoridade certificadora para gerar um certificado de cliente para o cluster. Certificados assinados são necessários para estabelecer uma relação de confiança para a interação com serviços externos.

Parâmetros

Este método não possui parâmetros de entrada.

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
Solicitação de assinatura de certificado do cliente	Solicitação de assinatura de certificado de cliente X.509 codificada em Base64 no formato PEM (PKCS#10).	corda

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

GetKeyProviderKmip

Você pode usar o `GetKeyProviderKmip` Método para recuperar informações sobre o provedor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) especificado.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do provedor de chave	O ID do objeto provedor de chaves KMIP a ser retornado.	inteiro	Nenhum	Sim

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
kmipKeyProvider	Um objeto contendo detalhes sobre o provedor de chaves solicitado.	"Provedor de chave Kmip"

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

GetKeyServerKmip

Você pode usar o `GetKeyServerKmip` Método para retornar informações sobre o servidor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) especificado.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do servidor de chaves	O ID do servidor de chaves KMIP sobre o qual retornar informações.	inteiro	Nenhum	Sim

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
kmipKeyServer	Um objeto contendo detalhes sobre o servidor de chaves solicitado.	"Servidor de chaves Kmip"

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

```
{
   "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
        }
    }
}
```

Novidade desde a versão

11,7

GetSoftwareEncryptionAtRestInfo

Você pode usar o `GetSoftwareEncryptionAtRestInfo` Método para obter informações sobre a criptografia de software em repouso que o cluster usa para criptografar dados em repouso.

Parâmetros

Este método não possui parâmetros de entrada.

Valores de retorno

Este método tem os seguintes valores de retorno:

Parâmetro	Descrição	Tipo	Opcional
masterKeyInfo	Informações sobre a chave mestra de criptografia em repouso do software atual.	Informações da chave de criptografia	Verdadeiro
rekeyMasterKeyAsyncResultID	O ID do resultado assíncrono da operação de recodificação atual ou mais recente (se houver), caso ainda não tenha sido excluído. `GetAsyncResult` A saída incluirá um `newKey` campo que contém informações sobre a nova chave mestra e um `keyToDecommission` Campo que contém informações sobre a chave antiga.	inteiro	Verdadeiro
estado	O estado atual da criptografia de software em repouso. Os valores possíveis são `disabled` ou `enabled`.	corda	Falso
versão	Um número de versão que é incrementado cada vez que a criptografia de software em repouso é ativada.	inteiro	Falso

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

12,3

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

ListKeyProvidersKmip

Você pode usar o `ListKeyProvidersKmip` Método para recuperar uma lista de todos os provedores de chaves existentes do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). Você pode filtrar a lista especificando parâmetros adicionais.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
provedor_chaveEstáAtivo	Os filtros retornaram objetos do servidor de chaves KMIP com base em se eles estavam ativos ou não. Valores possíveis: • true: Retorna apenas os provedores de chaves KMIP que estão ativos (fornecendo chaves que estão em uso no momento). • false: Retorna apenas os provedores de chaves KMIP que estão inativos (não fornecem nenhuma chave e podem ser excluídos). Se omitidos, os provedores de chaves KMIP retornados não são filtrados com base em seu status de atividade.	booleano	Nenhum	Não

Nome	Descrição	Tipo	Valor padrão	Obrigatório
kmipKeyProviderHasServerAssigned	Os filtros retornaram provedores de chaves KMIP com base na existência ou não de um servidor de chaves KMIP atribuído a eles. Valores possíveis: • true: Retorna apenas os provedores de chaves KMIP que possuem um servidor de chaves KMIP atribuído. • falso: Retorna apenas os provedores de chaves KMIP que não possuem um servidor de chaves KMIP atribuído. Se omitidos, os provedores de chaves KMIP retornados não são filtrados com base na existência de um servidor de chaves KMIP atribuído.	booleano	Nenhum	Não

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
kmipKeyProviders	Segue uma lista dos principais fornecedores de chaves KMIP que foram criados.	"Provedor de chave Kmip"variedade

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

ListKeyServersKmip

Você pode usar o `ListKeyServersKmip` Método para listar todos os servidores de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) que foram criados. Você pode filtrar os resultados especificando parâmetros adicionais.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do provedor de chave	Quando especificado, o método retorna apenas os servidores de chaves KMIP que estão atribuídos ao provedor de chaves KMIP especificado. Caso sejam omitidos, os servidores de chaves KMIP retornados não serão filtrados com base em sua atribuição ao provedor de chaves KMIP especificado.	inteiro	Nenhum	Não

Nome	Descrição	Tipo	Valor padrão	Obrigatório
kmipProvedorAtribuídoEstáAtivo	Os filtros retornaram objetos do servidor de chaves KMIP com base em se eles estavam ativos ou não. Valores possíveis: • true: Retorna apenas os servidores de chaves KMIP que estão ativos (fornecendo chaves que estão em uso no momento). • false: Retorna apenas os servidores de chaves KMIP que estão inativos (não fornecem nenhuma chave e podem ser excluídos). Se omitidos, os servidores de chaves KMIP retornados não são filtrados com base em seu status de atividade.	booleano	Nenhum	Não

Nome	Descrição	Tipo	Valor padrão	Obrigatório
kmipTemProvedorAtribuído	Os filtros retornaram servidores de chaves KMIP com base na existência ou não de um provedor de chaves KMIP atribuído a eles. Valores possíveis: • true: Retorna apenas os servidores de chaves KMIP que possuem um provedor de chaves KMIP atribuído. • falso: Retorna apenas servidores de chaves KMIP que não possuem um provedor de chaves KMIP atribuído. Se omitidos, os servidores de chaves KMIP retornados não são filtrados com base no fato de terem ou não um provedor de chaves KMIP atribuído.	booleano	Nenhum	Não

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
Servidores de chave kmip	A lista completa dos servidores de chaves KMIP que foram criados.	"Servidor de chaves Kmip"variedade

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

ModifyKeyServerKmip

Você pode usar o `ModifyKeyServerKmip` Método para modificar um servidor de chaves KMIP (Key Management Interoperability Protocol) existente para os atributos especificados. Embora o único parâmetro obrigatório seja o keyServerID, uma solicitação contendo apenas o keyServerID não executará nenhuma ação e não retornará nenhum erro. Quaisquer outros parâmetros que você especificar substituirão os valores existentes para o servidor de chaves pelo keyServerID especificado. O servidor de chaves é contatado durante a operação para garantir que esteja funcionando

corretamente. É possível fornecer vários nomes de host ou endereços IP com o parâmetro kmipKeyServerHostnames, mas somente se os servidores de chaves estiverem em uma configuração em cluster.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do servidor de chaves	O ID do servidor de chaves KMIP a ser modificado.	inteiro	Nenhum	Sim
kmipCaCertificado	O certificado de chave pública da autoridade certificadora raiz do servidor de chaves externo. Isso será usado para verificar o certificado apresentado pelo servidor de chaves externo na comunicação TLS. Para clusters de servidores principais onde servidores individuais usam diferentes CAs, forneça uma string concatenada contendo os certificados raiz de todas as CAs.	corda	Nenhum	Não
kmipClientCertificate	Um certificado PKCS#10 X.509 codificado em Base64 no formato PEM, usado pelo cliente Solidfire KMIP.	corda	Nenhum	Não

kmipKeyServerHostnames	Matriz de nomes de host ou endereços IP associados a este servidor de chaves KMIP. Só é necessário fornecer vários nomes de host ou endereços IP se os servidores principais estiverem em uma configuração de cluster.	matriz de strings	Nenhum	Não
kmipKeyServerName	O nome do servidor de chaves KMIP. Este nome é usado apenas para fins de exibição e não precisa ser único.	corda	Nenhum	Não
kmipKeyServerPort	O número da porta associada a este servidor de chaves KMIP (normalmente 5696).	inteiro	Nenhum	Não

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
kmipKeyServer	Um objeto contendo detalhes sobre o servidor de chaves recém-modificado.	"Servidor de chaves Kmip"

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

```
{
   "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
        }
    }
}
```

Novidade desde a versão

11,7

RekeySoftwareEncryptionAtRestMasterKey

Você pode usar o `RekeySoftwareEncryptionAtRestMasterKey` Método para

recodificar a chave mestra de criptografia em repouso do software usada para criptografar DEKs (Chaves de Criptografia de Dados). Durante a criação do cluster, a criptografia de software em repouso é configurada para usar o Gerenciamento de Chaves Internas (IKM). Este método de recodificação pode ser usado após a criação do cluster para utilizar tanto o IKM quanto o Gerenciamento de Chaves Externas (EKM).

Parâmetros

Este método possui os seguintes parâmetros de entrada. Se o `keyManagementType` Se nenhum parâmetro for especificado, a operação de renegociação de chave será realizada usando a configuração de gerenciamento de chaves existente. Se o `keyManagementType` se especificado e o provedor de chaves for externo, o `keyProviderID` O parâmetro também deve ser usado.

Parâmetro	Descrição	Tipo	Opcional
keyManagementType	O tipo de gerenciamento de chaves utilizado para gerenciar a chave mestra. Os valores possíveis são: `Internal` Recodificação usando gerenciamento de chaves interno. `External` Recodificação usando gerenciamento de chaves externo. Caso esse parâmetro não seja especificado, a operação de renegociação de chave será realizada utilizando a configuração de gerenciamento de chaves existente.	corda	Verdadeiro
ID do provedor de chave	O ID do provedor de chaves a ser utilizado. Este é um valor único retornado como parte de um dos `CreateKeyProvider` métodos. O documento de identificação só é necessário quando `keyManagementType` é `External` e, caso contrário, é inválido.	inteiro	Verdadeiro

Valores de retorno

Este método tem os seguintes valores de retorno:

Parâmetro	Descrição	Tipo	Opcional
manipulador assíncrono	Determine o status da operação de recodificação usando este método. `asyncHandle` valor com `GetAsyncResult` . `GetAsyncResult` A saída incluirá um `newKey` campo que contém informações sobre a nova chave mestra e um `keyToDecommission` Campo que contém informações sobre a chave antiga.	inteiro	Falso

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

12,3

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

RemoverKeyServerFromProviderKmip

Você pode usar o `RemoveKeyServerFromProviderKmip` Método para desatribuir o servidor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) especificado do provedor ao qual ele foi atribuído. Você pode desatribuir um servidor de chaves de seu provedor, a menos que seja o último e seu provedor esteja ativo (fornecendo chaves que estão atualmente em uso). Se o servidor de chaves especificado não estiver atribuído a um provedor, nenhuma ação será tomada e nenhum erro será retornado.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do servidor de chaves	O ID do servidor de chaves KMIP a ser desvinculado.	inteiro	Nenhum	Sim

Valores de retorno

Este método não possui valores de retorno. A remoção é considerada bem-sucedida desde que nenhum erro seja retornado.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

Assinar chaves Ssh

Após o SSH ser habilitado no cluster usando o"Método EnableSSH" , você pode usar o `SignSshKeys` Método para obter acesso a um shell em um nó.

Começando com o Elemento 12.5, `sfreadonly` É uma nova conta de sistema que permite a resolução de problemas básicos em um nó. Esta API permite o acesso SSH usando o `sfreadonly` conta do sistema em todos os nós do cluster.

> A menos que seja instruído pelo Suporte da NetApp , quaisquer alterações no sistema não são suportadas, anulando seu contrato de suporte e podendo resultar em instabilidade ou inacessibilidade dos dados.

Após utilizar o método, você deve copiar o chaveiro da resposta, salvá-lo no sistema que iniciará a conexão SSH e, em seguida, executar o seguinte comando:

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

```
`identity_file`é um arquivo do qual a identidade (chave privada) para
autenticação por chave pública é lida e `node_ip` é o endereço IP do nó.
Para obter mais informações sobre `identity_file` , consulte a página do
manual do SSH.
```

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
duração	Número inteiro de 1 a 24 que reflete a quantidade de horas durante as quais a chave assinada permanece válida. Se a duração não for especificada, será utilizado o valor padrão.	inteiro	1	Não
chave pública	Se fornecido, este parâmetro retornará apenas a chave pública assinada, em vez de criar um chaveiro completo para o usuário.  Chaves públicas enviadas usando a barra de URL em um navegador com + são interpretadas como espaçamento e quebra de sinalização.	corda	Nulo	Não

Nome	Descrição	Tipo	Valor padrão	Obrigatório
sfadmin	Permite o acesso à conta shell sfadmin quando você faz a chamada de API com acesso de cluster supportAdmin ou quando o nó não está em um cluster.	booleano	Falso	Não

Valores de retorno

Este método tem os seguintes valores de retorno:

Nome	Descrição	Tipo
status_da_geração_de_chaves	Contém a identidade na chave assinada, as entidades permitidas e as datas de início e término válidas para a chave.	corda
chave_privada	O valor de uma chave SSH privada só é retornado se a API estiver gerando um conjunto completo de chaves para o usuário final. O valor está codificado em Base64; você deve decodificá-lo ao gravá-lo em um arquivo para garantir que seja lido como uma chave privada válida.	corda

Nome	Descrição	Tipo
chave_pública	O valor de uma chave SSH pública só é retornado se a API estiver gerando um conjunto de chaves completo para o usuário final. Ao passar um parâmetro `public_key` para o método da API, somente o `signed_public_key` O valor é retornado na resposta.	corda
chave_pública_assinada	A chave pública SSH resultante da assinatura da chave pública, seja ela fornecida pelo usuário ou gerada pela API.	corda

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Neste exemplo, uma chave pública é assinada e retornada, sendo válida por um período de tempo (de 1 a 24 horas).

Novidade desde a versão

12,5

TestKeyProviderKmip

Você pode usar o `TestKeyProviderKmip` Método para testar se o provedor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) especificado está acessível e funcionando normalmente.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do provedor de chave	O ID do provedor de chaves a ser testado.	inteiro	Nenhum	Sim

Valores de retorno

Este método não possui valores de retorno. O teste é considerado bem-sucedido desde que nenhum erro seja retornado.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

TestKeyServerKmip

Você pode usar o `TestKeyServerKmip` Método para testar se o servidor de chaves do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) especificado está acessível e funcionando normalmente.

Parâmetros

Este método possui os seguintes parâmetros de entrada:

Nome	Descrição	Tipo	Valor padrão	Obrigatório
ID do servidor de chaves	O ID do servidor de chaves KMIP a ser testado.	inteiro	Nenhum	Sim

Valores de retorno

Este método não possui valores de retorno. O teste é considerado bem-sucedido se nenhum erro for retornado.

Exemplo de solicitação

As solicitações para esse método são semelhantes ao seguinte exemplo:

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

Exemplo de resposta

Este método retorna uma resposta semelhante ao exemplo a seguir:

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

Novidade desde a versão

11,7

Informações sobre direitos autorais

Informações sobre marcas comerciais