



Métodos de API de seguridad

Element Software

NetApp
January 15, 2024

Tabla de contenidos

- Métodos de API de seguridad 1
 - Obtenga más información 1
 - AddKeyServerToProviderKmp 1
 - CreateKeyProviderKmp 3
 - CreateKeyServerKmp 4
 - CreatePublicPrivateKeyPair 7
 - DeleteKeyProviderKmp 9
 - DeleteKeyServerKmp 10
 - DisableEncryptionAttest 11
 - EnableEncryptionAttest 12
 - GetClientCertificateSignRequest 15
 - GetKeyProviderKmp 16
 - GetKeyServerKmp 17
 - GetSoftwareEncryptionAtRestInfo 19
 - ListKeyProvidersKmp 21
 - ListKeyServersKmp 24
 - ModifyKeyServerKmp 27
 - RekeySoftwareEncryptionAtRestMasterKey 30
 - RemoveKeyServerFromProviderKmp 33
 - TestKeyProviderKmp 34
 - TestKeyServerKmp 35

Métodos de API de seguridad

Es posible integrar el software Element con servicios relacionados con la seguridad externos, como un servidor de gestión de claves externo. Estos métodos relacionados con la seguridad permiten configurar funciones de seguridad de Element, como la gestión de claves externa para el cifrado en reposo.

- [AddKeyServerToProviderKmip](#)
- [CreateKeyProviderKmip](#)
- [CreateKeyServerKmip](#)
- [CreatePublicPrivateKeyPair](#)
- [DeleteKeyProviderKmip](#)
- [DeleteKeyServerKmip](#)
- [DisableEncryptionAttest](#)
- [EnableEncryptionAttest](#)
- [GetClientCertificateSignRequest](#)
- [GetKeyProviderKmip](#)
- [GetKeyServerKmip](#)
- [ListKeyProvidersKmip](#)
- [ListKeyServersKmip](#)
- [ModifyKeyServerKmip](#)
- [RemoveKeyServerFromProviderKmip](#)
- [TestKeyProviderKmip](#)
- [TestKeyServerKmip](#)

Obtenga más información

- ["Documentación de SolidFire y el software Element"](#)
- ["Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"](#)

AddKeyServerToProviderKmip

Puede utilizar el `AddKeyServerToProviderKmip` Método para asignar un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) al proveedor de claves especificado. Durante la asignación, se contacta con el servidor para verificar la funcionalidad. Si el servidor de claves especificado ya está asignado al proveedor de claves especificado, no se realiza ninguna acción y no se devuelve ningún error. Puede quitar la asignación mediante `RemoveKeyServerFromProviderKmip` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del proveedor de claves al que se asignará el servidor de claves.	entero	Ninguno	Sí
KeyServerID	El ID del servidor de claves que se asignará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene ningún valor devuelto. La asignación se considera correcta siempre que no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

CreateKeyProviderKmip

Puede utilizar el `CreateKeyProviderKmip` Método para crear un proveedor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) con el nombre especificado. Un proveedor de claves define un mecanismo y una ubicación para recuperar claves de autenticación. Cuando se crea un proveedor de claves KMIP nuevo, no tiene ningún servidor de claves KMIP asignado. Para crear un servidor de claves KMIP, use el `CreateKeyServerKmip` método. Para asignarlo a un proveedor, consulte `AddKeyServerToProviderKmip`.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderName	El nombre que se asignará al proveedor de claves KMIP creado. Este nombre sólo se utiliza con fines de visualización y no necesita ser único.	cadena	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyProvider	Objeto que contiene detalles acerca del proveedor de claves recién creado.	"KeyProviderKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

CreateKeyServerKmip

Puede utilizar el `CreateKeyServerKmip` Método para crear un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) con los atributos especificados. Durante la creación, no se contacta con el servidor; no es necesario que exista antes de utilizar este método. Para configuraciones de servidor de claves en clúster, debe proporcionar los nombres de host o direcciones IP de todos los nodos de servidor en el parámetro `kmipKeyServerHostnames`. Puede utilizar el `TestKeyServerKmip` método para probar un servidor de claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipCaCertificate	El certificado de clave pública de la CA raíz del servidor de claves externo. Esto se utilizará para verificar el certificado presentado por el servidor de claves externo en la comunicación TLS. Para los clústeres de servidores de claves en los que los servidores individuales utilizan distintas CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	Sí
KmipClientCertificate	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM que utiliza el cliente KMIP de SolidFire.	cadena	Ninguno	Sí
KmipKeyServerHostnames	Cabina de los nombres de host o las direcciones IP asociadas con este servidor de claves KMIP. Sólo se deben proporcionar varios nombres de host o direcciones IP si los servidores de claves se encuentran en una configuración en clúster.	matriz de cadenas	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre sólo se utiliza con fines de visualización y no necesita ser único.	cadena	Ninguno	Sí
KmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (por lo general, 5696).	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServer	Objeto que contiene detalles acerca del servidor de claves recién creado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:


```

{
  "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
    }
  }
}

```

Nuevo desde la versión

11.7

CreatePublicPrivateKeyPair

Puede utilizar el `CreatePublicPrivateKeyPair` Método para crear claves SSL públicas y privadas. Es posible usar estas claves para generar solicitudes de firma de certificados. Solo puede haber una pareja de claves en uso para cada clúster de almacenamiento. Antes de utilizar este método para reemplazar las claves existentes, asegúrese de que ningún proveedor ya utilice las claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
CommonName	El campo X.509 Nombre distintivo Nombre común (CN).	cadena	Ninguno	No
país	El campo X 509 de nombre completo país ©.	cadena	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
Dirección de correo electrónico	El campo X 509 Nombre distintivo Dirección de correo electrónico (CORREO).	cadena	Ninguno	No
localidad	El campo X 509 Nombre distintivo Nombre de localidad (L).	cadena	Ninguno	No
organización	El campo X 509 Nombre distintivo Nombre de organización (o).	cadena	Ninguno	No
Unidad organizativa	El campo X.509 Nombre distintivo Nombre de unidad organizativa (OU).	cadena	Ninguno	No
estado	El campo X 509 Nombre distinguido Estado o Nombre de provincia (ST o SP o S).	cadena	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos. Si no hay ningún error, la creación de claves se considera correcta.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

DeleteKeyProviderKmip

Puede utilizar el `DeleteKeyProviderKmip` Método para eliminar el proveedor de claves de interoperabilidad de gestión de claves inactiva especificado (KMIP).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del proveedor de claves que se eliminará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La operación de eliminación se considera correcta siempre que no haya error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

DeleteKeyServerKmip

Puede utilizar el `DeleteKeyServerKmip` Método para eliminar un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) existente. Puede eliminar un servidor de claves a menos que sea el último asignado a su proveedor, y ese proveedor proporciona claves que están en uso actualmente.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP que se desea eliminar.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los valores no return. La operación de eliminación se considera correcta si no hay errores.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

DisableEncryptionAtRest

Puede utilizar el `DisableEncryptionAtRest` método para quitar el cifrado que se aplicó previamente al clúster mediante el `EnableEncryptionAtRest` método. Este método disable es asíncrono y devuelve una respuesta antes de que se deshabilite el cifrado. Puede utilizar el `GetClusterInfo` método para sondear el sistema para ver cuándo se ha completado el proceso.



Para ver el estado actual del cifrado en reposo y/o el cifrado de software en reposo en el clúster, use el ["obtenga el método de información del clúster"](#). Puede utilizar el `GetSoftwareEncryptionAtRestInfo` ["método para obtener información que utiliza el clúster para cifrar datos en reposo"](#).



No se puede usar este método para deshabilitar el cifrado de software en reposo. Para deshabilitar el cifrado de software en reposo, debe hacerlo [" Cree un nuevo clúster "](#) con el cifrado de software en reposo deshabilitado.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

9.6

Obtenga más información

- ["GetClusterInfo"](#)
- ["Documentación de SolidFire y el software Element"](#)
- ["Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"](#)

EnableEncryptionAtRest

Puede utilizar el `EnableEncryptionAtRest` Método para habilitar el cifrado AES (estándar de cifrado avanzado) de 256 bits en reposo en el clúster de manera que el clúster pueda gestionar la clave de cifrado utilizada para las unidades de cada nodo. Esta función no está habilitada de forma predeterminada.



Para ver el estado actual del cifrado en reposo y/o el cifrado de software en reposo en el clúster, use el ["obtenga el método de información del clúster"](#). Puede utilizar el `GetSoftwareEncryptionAtRestInfo` ["método para obtener información que utiliza el clúster para cifrar datos en reposo"](#).



Este método no habilita el cifrado de software en reposo. Esto sólo se puede hacer usando "cree el método de clúster" con `enableSoftwareEncryptionAtRest` establezca en `true`.

Cuando habilita el cifrado en reposo, el clúster gestiona automáticamente las claves de cifrado internamente para las unidades de cada nodo del clúster.

Si se especifica un `keyProviderID`, la contraseña se genera y recupera según el tipo de proveedor de claves. Esto suele realizarse mediante un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) en el caso de un proveedor de claves KMIP. Después de esta operación, el proveedor especificado se considera activo y no se puede eliminar hasta que se deshabilite el cifrado en reposo con el `DisableEncryptionAtRest` método.



Si tiene un tipo de nodo con un número de modelo que termina en "-NE", la `EnableEncryptionAtRest` La llamada al método fallará y la respuesta será "no se permite el cifrado. Cluster detectado nodo no encriptable".



Solo tendrá que habilitar o deshabilitar el cifrado cuando el clúster se ejecute y esté en buen estado. Puede activar o desactivar el cifrado a su discreción y con la frecuencia que necesite.



Este proceso es asíncrono y devuelve una respuesta antes de activar el cifrado. Puede utilizar el `GetClusterInfo` método para sondear el sistema para ver cuándo se ha completado el proceso.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
<code>KeyProviderID</code>	El ID de un proveedor de claves KMIP que se debe usar.	entero	Ninguno	No

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplos de respuestas

Este método devuelve una respuesta similar al siguiente ejemplo del método `EnableEncryptionAtRest`. No hay resultados para informar.

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

Mientras que el cifrado en reposo se está habilitando en un clúster, `GetClusterInfo` muestra un resultado que describe el estado del cifrado en reposo ("cifrado `AtRestState`") como "habilitando". Una vez que el cifrado en reposo está completamente habilitado, el estado devuelto cambia a "habilitado".

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

Nuevo desde la versión

9.6

Obtenga más información

- ["SecureEraseDrives"](#)
- ["GetClusterInfo"](#)
- ["Documentación de SolidFire y el software Element"](#)

- ["Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"](#)

GetClientCertificateSignRequest

Puede utilizar el `GetClientCertificateSignRequest` método para generar una solicitud de firma de certificación que puede estar firmada por una entidad de certificación a fin de generar un certificado de cliente para el clúster. Los certificados firmados son necesarios para establecer una relación de confianza para interactuar con servicios externos.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
ClientCertificadosSignRequest	Una solicitud de firma de certificado de cliente PKCS#10 X.509 codificada con PEM Base64.	cadena

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "id": 1,
  "result":
  {
    "clientCertificateSignRequest":
    "MIIBYjCCATMCAQAwgYkxCzAJBgNVBAYTALVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
  }
}

```

Nuevo desde la versión

11.7

GetKeyProviderK mip

Puede utilizar el `GetKeyProviderK mip` Método para recuperar información sobre el proveedor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del objeto de proveedor de claves KMIP que se va a devolver.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
K mipKeyProvider	Objeto que contiene detalles sobre el proveedor de claves solicitado.	"KeyProviderK mip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

GetKeyServerKmip

Puede utilizar el `GetKeyServerKmip` Método para obtener información sobre el servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP acerca de la cual se desea obtener información.	entero	Ninguno	Sí

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServer	Objeto que contiene detalles acerca del servidor de claves solicitado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "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
    }
  }
}

```

Nuevo desde la versión

11.7

GetSoftwareEncryptionAtRestInfo

Puede utilizar el `GetSoftwareEncryptionAtRestInfo` método para obtener información de cifrado por software que el clúster utiliza para cifrar datos en reposo.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método tiene los siguientes valores devueltos:

Parámetro	Descripción	Tipo	Opcional
MasterKeyInfo	Información acerca de la clave maestra actual de cifrado en reposo de software.	Cifrar KeyInfo	Verdadero

Parámetro	Descripción	Tipo	Opcional
RekeyMasterKeyAsyncResultID	El ID de resultado asíncrono de la operación de reclave actual o más reciente (si existe), si aún no se ha eliminado. <code>GetAsyncResult</code> la salida incluirá una <code>newKey</code> campo que contiene información acerca de la nueva clave maestra y un <code>keyToDecommission</code> campo que contiene información acerca de la clave anterior.	entero	Verdadero
estado	El estado actual del cifrado de software en reposo. Los valores posibles son <code>disabled</code> o <code>enabled</code> .	cadena	Falso
versión	Un número de versión que aumenta cada vez que se habilita el cifrado de software en reposo.	entero	Falso

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

12.3

Obtenga más información

- ["Documentación de SolidFire y el software Element"](#)
- ["Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"](#)

ListKeyProvidersKmip

Puede utilizar el `ListKeyProvidersKmip` Método para recuperar una lista de todos los proveedores de claves del protocolo de interoperabilidad de gestión de claves (KMIP) existentes. Puede filtrar la lista especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderIsActive	<p>Los filtros regresaron objetos del servidor de claves KMIP en función de si están activos. Los posibles valores son los siguientes:</p> <ul style="list-style-type: none"> • True: Devuelve solo los proveedores de claves KMIP activos (que proporcionan claves en uso actualmente). • False: Devuelve solo los proveedores de claves KMIP inactivos (sin ofrecer ninguna clave y sin poder eliminarla). <p>Si se omite, los proveedores de claves KMIP que se devuelven no se filtran en función de si están activos.</p>	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipKeyProviderHasServerAssigned	<p>Los filtros devuelven proveedores de claves KMIP en función de si tienen asignado un servidor de claves KMIP. Los posibles valores son los siguientes:</p> <ul style="list-style-type: none"> • True: Solo devuelve los proveedores de claves KMIP que tienen asignado un servidor de claves KMIP. • False: Devuelve solo los proveedores de claves KMIP que no tienen asignado un servidor de claves KMIP. <p>Si se omite, los proveedores de claves KMIP que se devuelven no se filtran en función de si tienen asignado un servidor de claves KMIP.</p>	booleano	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyProviders	Una lista de los proveedores de claves KMIP que se hayan creado.	"KeyProviderKmip" cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

ListKeyServersKmip

Puede utilizar el `ListKeyServersKmip` Método para enumerar todos los servidores de claves de protocolo de interoperabilidad de gestión de claves (KMIP) creados. Los resultados se pueden filtrar especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	<p>Cuando se especifica, el método solo devuelve los servidores de claves KMIP asignados al proveedor de claves KMIP especificado. Si se omite, los servidores de claves KMIP devueltos no se filtrarán en función de si se asignan al proveedor de claves KMIP especificado.</p>	entero	Ninguno	No
KmpAssignedProvidersActive	<p>Los filtros regresaron objetos del servidor de claves KMIP en función de si están activos. Los posibles valores son los siguientes:</p> <ul style="list-style-type: none"> • True: Devuelve solo los servidores de claves KMIP activos (que proporcionan claves en uso actualmente). • False: Devuelve solo los servidores de claves KMIP inactivos (sin proporcionar ninguna clave y sin poder eliminarse). <p>Si se omite, los servidores de claves KMIP devueltos no se filtran en función de si están activos.</p>	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KmipHasProviderAs signed	<p>Los filtros devuelven servidores de claves KMIP en función de si tienen asignado un proveedor de claves KMIP. Los posibles valores son los siguientes:</p> <ul style="list-style-type: none"> • True: Solo devuelve los servidores de claves KMIP que tienen asignado un proveedor de claves KMIP. • False: Devuelve solo los servidores de claves KMIP que no tienen asignado un proveedor de claves KMIP. <p>Si se omite, los servidores de claves KMIP que se devuelven no se filtran en función de si tienen asignado un proveedor de claves KMIP.</p>	booleano	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServers	La lista completa de los servidores de claves KMIP que se crearon.	"KeyServerKmip" cabina

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

ModifyKeyServerKmip

Puede utilizar el `ModifyKeyServerKmip` Método para modificar un servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) existente en los atributos especificados. Aunque el único parámetro requerido es `keyServerID`, una solicitud que contiene sólo el `keyServerID` no realizará ninguna acción y no devolverá ningún error. Cualquier otro parámetro que especifique reemplazará los valores existentes para el servidor de claves con el `keyServerID` especificado. Se contacta con el servidor de claves durante la operación para garantizar que funciona. Puede proporcionar varios nombres de host o direcciones IP con el parámetro `kmipKeyServerHostnames`, pero sólo si los servidores de claves están en una configuración en clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP que se desea modificar.	entero	Ninguno	Sí
KmipCaCertificate	El certificado de clave pública de la CA raíz del servidor de claves externo. Esto se utilizará para verificar el certificado presentado por el servidor de claves externo en la comunicación TLS. Para los clústeres de servidores de claves en los que los servidores individuales utilizan distintas CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	No
KmipClientCertificate	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM que utiliza el cliente KMIP de SolidFire.	cadena	Ninguno	No

KmipKeyServerHost names	Cabina de los nombres de host o las direcciones IP asociadas con este servidor de claves KMIP. Sólo se deben proporcionar varios nombres de host o direcciones IP si los servidores de claves se encuentran en una configuración en clúster.	matriz de cadenas	Ninguno	No
KmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre sólo se utiliza con fines de visualización y no necesita ser único.	cadena	Ninguno	No
KmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (por lo general, 5696).	entero	Ninguno	No

Valores devueltos

Este método tiene los siguientes valores devueltos:

Nombre	Descripción	Tipo
KmipKeyServer	Un objeto que contiene detalles acerca del servidor de claves recién modificado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```

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

```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "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
    }
  }
}

```

Nuevo desde la versión

11.7

RekeySoftwareEncryptionAtRestMasterKey

Puede utilizar el `RekeySoftwareEncryptionAtRestMasterKey` Método para volver

a introducir la clave maestra de cifrado en reposo de software utilizada para cifrar los depósitos (claves de cifrado de datos). Durante la creación de clústeres, el cifrado de software en reposo se configura para utilizar Internal Key Management (IKM). Este método de nueva clave se puede utilizar después de la creación de un clúster para utilizar IKM o Gestión de claves externas (EKM).

Parámetros

Este método tiene los siguientes parámetros de entrada. Si la `keyManagementType` no se especifica el parámetro; la operación de nueva clave se realiza mediante la configuración de gestión de claves existente. Si la `keyManagementType` se especifica y el proveedor de claves es externo, el `keyProviderID` también se debe utilizar el parámetro.

Parámetro	Descripción	Tipo	Opcional
Tipo de material de la columna	El tipo de gestión de claves utilizado para gestionar la clave maestra. Los valores posibles son: <code>Internal: ReKey</code> utilizando la gestión de claves internas. <code>External: ReKey</code> mediante la gestión de claves externas. Si no se especifica este parámetro, se ejecuta la operación de nueva clave mediante la configuración de gestión de claves existente.	cadena	Verdadero
<code>KeyProviderID</code>	El ID del proveedor de claves que se utilizará. Se trata de un valor único devuelto como parte de uno de los <code>CreateKeyProvider</code> métodos. El ID sólo es necesario cuando <code>keyManagementType</code> es <code>External</code> y, de lo contrario, no es válido.	entero	Verdadero

Valores devueltos

Este método tiene los siguientes valores devueltos:

Parámetro	Descripción	Tipo	Opcional
Establish asyncHandle	Determine el estado de la operación de reclaves con este método asyncHandle valor con GetAsyncResult. GetAsyncResult la salida incluirá una newKey campo que contiene información acerca de la nueva clave maestra y un keyToDecommission campo que contiene información acerca de la clave anterior.	entero	Falso

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

12.3

Obtenga más información

- ["Documentación de SolidFire y el software Element"](#)
- ["Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"](#)

RemoveKeyServerFromProviderKmip

Puede utilizar el `RemoveKeyServerFromProviderKmip` Método para anular la asignación del servidor de claves de protocolo de interoperabilidad de gestión de claves (KMIP) especificado del proveedor al que se asignó. Puede anular la asignación de un servidor de claves de su proveedor a menos que sea el último y su proveedor esté activo (proporcionando claves que estén en uso actualmente). Si el servidor de claves especificado no está asignado a un proveedor, no se realiza ninguna acción y no se devuelve ningún error.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP para anular la asignación.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La eliminación se considera correcta siempre que no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

TestKeyProviderKmip

Puede utilizar el `TestKeyProviderKmip` Método para probar si el proveedor de claves del protocolo de interoperabilidad de gestión de claves (KMIP) especificado es accesible y funciona normalmente.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyProviderID	El ID del proveedor de claves que se probará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La prueba se considera correcta mientras no se devuelve ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

TestKeyServerKmip

Puede utilizar el `TestKeyServerKmip` Método para probar si el servidor de claves del protocolo de interoperabilidad de gestión de claves (KMIP) especificado es accesible y funciona con normalidad.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Obligatorio
KeyServerID	El ID del servidor de claves KMIP que se probará.	entero	Ninguno	Sí

Valores devueltos

Este método no tiene valores devueltos. La prueba se considera correcta si no se devuelve ningún error.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nuevo desde la versión

11.7

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.