Métodos de la API de seguridad

Element Software

NetApp
November 18, 2025

This PDF was generated from https://docs.netapp.com/es-es/element-software-128/api/reference_element_api_addkeyservertoproviderkmip.html on November 18, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Métodos de la API de seguridad

Agregar servidor de claves al proveedor Kmip

Puedes usar el `AddKeyServerToProviderKmip` método para asignar un servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) al proveedor de claves especificado. Durante la asignación, se contacta con el servidor para verificar su 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. Puedes eliminar la asignación usando el `RemoveKeyServerFromProviderKmip` método.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID del proveedor de claves al que se asignará el servidor de claves.	entero	Ninguno	Sí
ID del servidor de claves	El ID del servidor de claves a asignar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La tarea se considera exitosa siempre y cuando no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

11,7

CrearKeyProviderKmip

Puedes usar el `CreateKeyProviderKmip` Método para crear un proveedor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) con el nombre especificado. Un proveedor de claves define un mecanismo y una ubicación para recuperar las claves de autenticación. Cuando se crea un nuevo proveedor de claves KMIP, este no tiene asignado ningún servidor de claves KMIP. Para crear un servidor de claves KMIP, utilice el `CreateKeyServerKmip` método. Para asignarlo a un proveedor, consulte `AddKeyServerToProviderKmip` .

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre del proveedor de clave	El nombre que se asociará con el proveedor de claves KMIP creado. Este nombre se utiliza únicamente con fines ilustrativos y no necesita ser único.	cadena	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo

kmipKeyProvider	Un objeto que contiene detalles sobre el proveedor de claves recién creado.	"KeyProviderKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
    }
}
}
```

Nueva versión

11,7

CrearKeyServerKmip

Puedes usar el `CreateKeyServerKmip` Método para crear un servidor de claves del 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 las direcciones IP de todos los nodos del servidor en el parámetro kmipKeyServerHostnames. Puedes usar el `TestKeyServerKmip` Método para probar un servidor de claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
Certificado kmipCa	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 clústeres de servidores clave donde los servidores individuales utilizan diferentes CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	Sí
Certificado de cliente kmip	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM utilizado por el cliente Solidfire KMIP.	cadena	Ninguno	Sí

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
Nombres de host del servidor de claves kmip	Conjunto de nombres de host o direcciones IP asociadas a este servidor de claves KMIP. Solo se deben proporcionar varios nombres de host o direcciones IP si los servidores clave están en una configuración de clúster.	matriz de cadenas	Ninguno	Sí
kmipKeyServerName	El nombre del servidor de claves KMIP. Este nombre se utiliza únicamente con fines ilustrativos y no necesita ser único.	cadena	Ninguno	Sí
kmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (normalmente 5696).	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidor de claves kmip	Un objeto que contiene detalles sobre el servidor de claves recién creado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
        }
    }
}
```

Nueva versión

11,7

Crear par de claves públicas y privadas

Puedes usar el `CreatePublicPrivateKeyPair` Método para crear claves SSL públicas y privadas. Puede utilizar estas claves para generar solicitudes de firma de

certificados. Solo puede haber un par de claves en uso por cada clúster de almacenamiento. Antes de utilizar este método para reemplazar las claves existentes, asegúrese de que ningún proveedor siga utilizando dichas claves.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
nombre común	El campo **Nombre común** (CN) del nombre distinguido X.509.	cadena	Ninguno	No
país	El campo de nombre distinguido **País** © de X.509.	cadena	Ninguno	No
dirección de correo electrónico	El nombre distinguido X.509 **Campo de dirección de correo electrónico** (MAIL).	cadena	Ninguno	No
localidad	El campo de nombre distinguido X.509 **Nombre de localidad** (L).	cadena	Ninguno	No
organización	El campo de nombre distinguido X.509 **Nombre de la organización** (O).	cadena	Ninguno	No
unidad organizativa	El campo **Nombre de la unidad organizativa** del nombre distintivo X.509 (OU).	cadena	Ninguno	No
estado	El campo de nombre distinguido X.509 **Estado** o **Nombre de provincia** (ST o SP o S).	cadena	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor. Si no hay ningún error, la creación de la clave se considera exitosa.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Nueva versión

11,7

EliminarKeyProviderKmip

Puedes usar el `DeleteKeyProviderKmip` Método para eliminar el proveedor de claves inactivo especificado del Protocolo de Interoperabilidad de Gestión de Claves (KMIP).

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID del proveedor de claves que se va a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La operación de eliminación se considera exitosa siempre y cuando no haya ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

11,7

EliminarKeyServerKmip

Puedes usar el `DeleteKeyServerKmip` Método para eliminar un servidor de claves KMIP (Key Management Interoperability Protocol) existente. Puedes eliminar un servidor de claves a menos que sea el último asignado a su proveedor y que dicho proveedor esté proporcionando claves que se encuentren actualmente en uso.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a eliminar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La operación de eliminación se considera exitosa si no hay errores.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

11,7

Deshabilitar el cifrado en reposo

Puedes usar el `DisableEncryptionAtRest` método para eliminar el cifrado que se aplicó previamente al clúster utilizando el `EnableEncryptionAtRest` método. Este método de desactivación es asíncrono y devuelve una respuesta antes de que se

desactive el cifrado. Puedes usar el `GetClusterInfo` Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.

- No puede utilizar este método para deshabilitar el cifrado de software en reposo. Para deshabilitar el cifrado de software en reposo, necesita"crear un nuevo clúster" con el cifrado de software en reposo desactivado.
- Para ver el estado actual del cifrado en reposo, el cifrado de software en reposo o ambos en el clúster, utilice la siguiente información: "método para obtener información del clúster". Puedes usar el `GetSoftwareEncryptionAtRestInfo` "Método para obtener información sobre el clúster que utiliza para cifrar los datos en reposo.".

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

9,6

Encuentra más información

- "Obtener información del clúster"
- "Documentación del software SolidFire y Element"

- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Habilitar cifrado en reposo

Puedes usar el `EnableEncryptionAtRest` Método para habilitar el cifrado en reposo del Estándar de Cifrado Avanzado (AES) de 256 bits en el clúster, de modo que el clúster pueda administrar la clave de cifrado utilizada para las unidades en cada nodo. Esta función no está habilitada de forma predeterminada.

- Para ver el estado actual del cifrado en reposo y/o del cifrado de software en reposo en el clúster, utilice la siguiente información:"método para obtener información del clúster" . Puedes usar el `GetSoftwareEncryptionAtRestInfo` "Método para obtener información sobre el clúster que utiliza para cifrar los datos en reposo.".
- Este método no permite el cifrado de software en reposo. Esto solo se puede hacer utilizando el"método de creación de clúster" con `enableSoftwareEncryptionAtRest` empezar a `true` .

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

Si se especifica un keyProviderID, la contraseña se genera y se recupera según el tipo de proveedor de claves. Normalmente, esto se realiza utilizando un servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) en el caso de un proveedor de claves KMIP. Tras esta operación, el proveedor especificado se considera activo y no se puede eliminar hasta que se deshabilite el cifrado en reposo mediante el `DisableEncryptionAtRest` método.

Si tiene un tipo de nodo con un número de modelo que termina en "-NE", el `EnableEncryptionAtRest` La llamada al método fallará con la respuesta "Cifrado no permitido". El clúster detectó un nodo no cifrable.

Solo debe habilitar o deshabilitar el cifrado cuando el clúster esté en funcionamiento y 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 que se habilite el cifrado. Puedes usar el `GetClusterInfo` Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID de un proveedor de claves KMIP a utilizar.	entero	Ninguno	No

Valores de retorno

Este método no devuelve ningún valor.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplos de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo del método EnableEncryptionAtRest. No hay resultados que reportar.

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

Mientras se habilita el cifrado en reposo en un clúster, GetClusterInfo devuelve un resultado que describe el estado del cifrado en reposo ("encryptionAtRestState") como "habilitado". Una vez que el cifrado en reposo esté completamente habilitado, el estado devuelto cambiará 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"
      }
   }
}
```


Nueva versión

9,6

Encuentra más información

- "Unidades de borrado seguro"
- "Obtener información del clúster"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Solicitud de firma de certificado de cliente

Puedes usar el `GetClientCertificateSignRequest` Método para generar una solicitud de firma de certificado que pueda ser firmada por una autoridad de certificación para generar un certificado de cliente para el clúster. Se necesitan certificados firmados para establecer una relación de confianza para interactuar con servicios externos.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Solicitud de firma de certificado de cliente	Solicitud de firma de certificado de cliente X.509 con codificación Base64 en formato PEM y formato PKCS#10.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

11,7

ObtenerProveedorDeClavesKmip

Puedes usar el `GetKeyProviderKmip` método para recuperar información sobre el proveedor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	El ID del objeto proveedor de claves KMIP que se devolverá.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
kmipKeyProvider	Un objeto que contiene detalles sobre el proveedor de claves solicitado.	"KeyProviderKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Nueva versión

11,7

ObtenerKeyServerKmip

Puedes usar el `GetKeyServerKmip` método para devolver información sobre el servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) especificado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP del que se devolverá información.	entero	Ninguno	Sí

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidor de claves kmip	Un objeto que contiene detalles sobre el servidor de claves solicitado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
        }
    }
}
```

Nueva versión

11,7

Obtener información de cifrado de software en reposo

Puedes usar el `GetSoftwareEncryptionAtRestInfo` Método para obtener información sobre el cifrado de software en reposo que utiliza el clúster para cifrar los datos en reposo.

Parámetros

Este método no tiene parámetros de entrada.

Valores de retorno

Este método tiene los siguientes valores de retorno:

Parámetro	Descripción	Tipo	Opcional
Información de clave maestra	Información sobre la clave maestra actual de cifrado en reposo del software.	Información de clave de cifrado	Verdadero
rekeyMasterKeyAsyncResultID	El ID del resultado asíncrono de la operación de re-clave actual o más reciente (si la hay), si aún no se ha eliminado. `GetAsyncResult` La salida incluirá un `newKey` campo que contiene información sobre la nueva clave maestra y un `keyToDecommission` campo que contiene información sobre la clave anterior.	entero	Verdadero
estado	Estado actual del cifrado de software en reposo. Los valores posibles son `disabled` o `enabled`.	cadena	FALSO
versión	Un número de versión que se incrementa cada vez que se habilita el cifrado de software en reposo.	entero	FALSO

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
 "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
    }
}
```


Nueva versión

12,3

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Proveedores de claves de lista Kmip

Puedes usar el `ListKeyProvidersKmip` Método para recuperar una lista de todos los proveedores de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) existentes. Puedes filtrar la lista especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
keyProviderIsActive	Los filtros devolvieron objetos de servidor de claves KMIP en función de si están activos o no. Valores posibles: • verdadero: Devuelve solo los proveedores de claves KMIP que están activos (proporcionando claves que se están utilizando actualmente). • false: Devuelve solo los proveedores de claves KMIP que están inactivos (no proporcionan ninguna clave y pueden ser eliminados). Si se omite, los proveedores de claves KMIP devueltos no se filtran en función de si están activos o no.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
kmipKeyProviderHasServerAssigned	Los filtros devolvieron proveedores de claves KMIP en función de si tenían asignado un servidor de claves KMIP. Valores posibles: • verdadero: Devuelve solo 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. Si se omite, los proveedores de claves KMIP devueltos no se filtran en función de si tienen asignado un servidor de claves KMIP.	booleano	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Proveedores de claves kmip	Lista de proveedores de claves KMIP que se han creado.	"KeyProviderKmip"formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Nueva versión

11,7

Lista de servidores clave Kmip

Puedes usar el `ListKeyServersKmip` Método para listar todos los servidores de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) que se han creado. Puede filtrar los resultados especificando parámetros adicionales.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del proveedor de clave	Cuando se especifica, el método solo devuelve los servidores de claves KMIP que están asignados al proveedor de claves KMIP especificado. Si se omite, los servidores de claves KMIP devueltos no se filtrarán en función de si están asignados al proveedor de claves KMIP especificado.	entero	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
kmipAssignedProviderIsActive	Los filtros devolvieron objetos de servidor de claves KMIP en función de si están activos o no. Valores posibles: • verdadero: Devuelve solo los servidores de claves KMIP que están activos (proporcionando claves que se están utilizando actualmente). • false: Devuelve solo los servidores de claves KMIP que están inactivos (no proporcionan ninguna clave y pueden ser eliminados). Si se omite, los servidores de claves KMIP devueltos no se filtran en función de si están activos o no.	booleano	Ninguno	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
kmipTieneProveedorAsignado	Los filtros devolvieron servidores de claves KMIP en función de si tenían asignado un proveedor de claves KMIP. Valores posibles: • verdadero: Devuelve solo 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. Si se omite, los servidores de claves KMIP devueltos no se filtran en función de si tienen asignado un proveedor de claves KMIP.	booleano	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidores de claves kmip	La lista completa de servidores clave KMIP que se han creado.	"KeyServerKmip"formación

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
        }
    ]
}
```

Nueva versión

11,7

ModificarKeyServerKmip

Puedes usar el `ModifyKeyServerKmip` Método para modificar un servidor de claves KMIP (Key Management Interoperability Protocol) existente a los atributos especificados. Aunque el único parámetro obligatorio es el keyServerID, una solicitud que contenga únicamente el keyServerID no realizará ninguna acción ni devolverá ningún error. Cualquier otro parámetro que especifique reemplazará los valores existentes para el servidor de claves con el keyServerID especificado. Durante la operación se contacta con el servidor clave para asegurar que funciona correctamente. Puede proporcionar varios nombres de host o direcciones IP con el parámetro kmipKeyServerHostnames, pero solo si los servidores clave están en una configuración de clúster.

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a modificar.	entero	Ninguno	Sí
Certificado kmipCa	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 clústeres de servidores clave donde los servidores individuales utilizan diferentes CA, proporcione una cadena concatenada que contenga los certificados raíz de todas las CA.	cadena	Ninguno	No
Certificado de cliente kmip	Un certificado PKCS#10 X.509 codificado en Base64 con formato PEM utilizado por el cliente Solidfire KMIP.	cadena	Ninguno	No

Nombres de host del servidor de claves kmip	Conjunto de nombres de host o direcciones IP asociadas a este servidor de claves KMIP. Solo se deben proporcionar varios nombres de host o direcciones IP si los servidores clave están en una configuración de clúster.	matriz de cadenas	Ninguno	No
kmipKeyServerNam e	El nombre del servidor de claves KMIP. Este nombre se utiliza únicamente con fines ilustrativos y no necesita ser único.	cadena	Ninguno	No
kmipKeyServerPort	El número de puerto asociado con este servidor de claves KMIP (normalmente 5696).	entero	Ninguno	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
Servidor de claves kmip	Un objeto que contiene detalles sobre el servidor de claves recientemente modificado.	"KeyServerKmip"

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

```
{
  "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
        }
    }
}
```

Nueva versión

11,7

Clave maestra de cifrado de software en reposo

Puedes usar el `RekeySoftwareEncryptionAtRestMasterKey` Método para volver a

generar la clave maestra de cifrado en reposo del software utilizada para cifrar las DEK (claves de cifrado de datos). Durante la creación del clúster, el cifrado de software en reposo se configura para utilizar la gestión de claves internas (IKM). Este método de re-clave se puede utilizar después de la creación del clúster para usar IKM o Administración de claves externas (EKM).

Parámetros

Este método tiene los siguientes parámetros de entrada. Si el `keyManagementType` Si no se especifica ningún parámetro, la operación de cambio de clave se realiza utilizando la configuración de gestión de claves existente. Si el `keyManagementType` está especificado y el proveedor de claves es externo, el `keyProviderID` También debe utilizarse el parámetro.

Parámetro	Descripción	Tipo	Opcional
tipo de gestión de claves	El tipo de gestión de claves utilizado para administrar la clave maestra. Los valores posibles son: `Internal` : Recodificar utilizando la gestión interna de claves. `External` : Recodificar utilizando la gestión de claves externa. Si no se especifica este parámetro, la operación de cambio de clave se realiza utilizando la configuración de gestión de claves existente.	cadena	Verdadero
ID del proveedor de clave	El identificador del proveedor de claves a utilizar. Este es un valor único que se devuelve como parte de uno de los `CreateKeyProvider` métodos. El ID solo es necesario cuando `keyManagementType` es `External` y, por lo demás, no es válido.	entero	Verdadero

Valores de retorno

Este método tiene los siguientes valores de retorno:

Parámetro	Descripción	Tipo	Opcional
manejador asíncrono	Determine el estado de la operación de recodificación utilizando esto `asyncHandle` valor con `GetAsyncResult` . `GetAsyncResult` La salida incluirá un `newKey` campo que contiene información sobre la nueva clave maestra y un `keyToDecommission` campo que contiene información sobre la clave anterior.	entero	FALSO

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

12,3

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Eliminar servidor de claves del proveedor Kmip

Puedes usar el `RemoveKeyServerFromProviderKmip` método para desasignar el servidor de claves del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) especificado del proveedor al que estaba asignado. Puedes desasignar un servidor de claves de su proveedor a menos que sea el último y su proveedor esté activo (proporcionando claves que se están utilizando 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	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a desasignar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La eliminación se considera exitosa siempre que no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

11,7

Firmar claves Ssh

Después de habilitar SSH en el clúster mediante"Método HabilitarSSH" , puedes usar el `SignSshKeys` Método para obtener acceso a una shell en un nodo.

A partir del elemento 12.5, `sfreadonly` Es una nueva cuenta del sistema que permite la resolución de problemas básicos en un nodo. Esta API permite el acceso SSH mediante `sfreadonly` Cuenta del sistema en todos los nodos del clúster.

> Salvo indicación expresa del Soporte de NetApp , cualquier modificación del sistema no está soportada, anulará su contrato de soporte y puede provocar inestabilidad o inaccesibilidad de los datos.

Después de utilizar este método, debe copiar el llavero de la respuesta, guardarlo en el sistema que iniciará la conexión SSH y, a continuación, ejecutar el siguiente comando:

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

```
`identity_file`es un archivo del cual se lee la identidad (clave privada)
para la autenticación de clave pública y `node_ip` es la dirección IP del
nodo.  Para obtener más información sobre `identity_file` , consulte la
página del manual de SSH.
```

Parámetros

Este método tiene los siguientes parámetros de entrada:

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
duración	Número entero del 1 al 24 que refleja el número de horas que la clave firmada será válida. Si no se especifica la duración, se utiliza el valor predeterminado.	entero	1	No
clave pública	Si se proporciona, este parámetro solo devolverá la clave pública firmada en lugar de crear un llavero completo para el usuario. Las claves públicas se envían utilizando la barra de direcciones de un navegador con + se interpretan como signos espaciados y de ruptura.	cadena	Nulo	No

Nombre	Descripción	Tipo	Valor predeterminado	Requerido
sfadmin	Permite el acceso a la cuenta de shell sfadmin cuando se realiza la llamada a la API con acceso al clúster supportAdmin, o cuando el nodo no está en un clúster.	booleano	FALSO	No

Valores de retorno

Este método tiene los siguientes valores de retorno:

Nombre	Descripción	Tipo
estado del generador de claves	Contiene la identidad en la clave firmada, las entidades autorizadas y las fechas de inicio y fin válidas para la clave.	cadena
clave_privada	El valor de una clave SSH privada solo se devuelve si la API genera un llavero completo para el usuario final.  El valor está codificado en Base64; debe decodificarlo cuando se escriba en un archivo para garantizar que se lea como una clave privada válida.	cadena

Nombre	Descripción	Tipo
clave_pública	El valor de una clave SSH pública solo se devuelve si la API genera un llavero completo para el usuario final. Cuando se pasa un parámetro public_key al método de la API, solo se tiene en cuenta el parámetro public_key. `signed_public_key` El valor se devuelve en la respuesta.	cadena
clave pública firmada	La clave pública SSH que resulta de firmar la clave pública, ya sea que esta haya sido proporcionada por el usuario o generada por la API.	cadena

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

En este ejemplo, se firma y se devuelve una clave pública que es válida durante un período de tiempo de entre 1 y 24 horas.

Nueva versión

12,5

TestKeyProviderKmip

Puedes usar el `TestKeyProviderKmip` método para comprobar si el proveedor 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	Requerido
ID del proveedor de clave	El ID del proveedor de claves a probar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La prueba se considera exitosa siempre y cuando no se devuelva ningún error.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

11,7

Servidor de claves de prueba Kmip

Puedes usar el `TestKeyServerKmip` método para comprobar 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	Requerido
ID del servidor de claves	El ID del servidor de claves KMIP que se va a probar.	entero	Ninguno	Sí

Valores de retorno

Este método no devuelve ningún valor. La prueba se considera exitosa si no se devuelven errores.

Ejemplo de solicitud

Las solicitudes para este método son similares al siguiente ejemplo:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

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

Nueva versión

11,7

Información de copyright

Copyright © 2025 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 INTERRUPCIÓN 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.