Comience con la administración de claves externas

Element Software

NetApp
November 12, 2025

Tabla de contenidos

Comience con la administración de claves externas

Comience con la administración de claves externas

La gestión de claves externas (EKM) proporciona una gestión segura de claves de autenticación (AK) junto con un servidor de claves externas fuera del clúster (EKS). Las AK se utilizan para bloquear y desbloquear unidades de autocifrado (SED) cuando"cifrado en reposo" está habilitado en el clúster. El EKS proporciona generación y almacenamiento seguros de los AK. El clúster utiliza el protocolo de interoperabilidad de gestión de claves (KMIP), un protocolo estándar definido por OASIS, para comunicarse con el EKS.

- "Establecer la gestión externa"
- "Rekey cifrado de software en reposo clave maestra"
- "Recuperar claves de autenticación inaccesibles o no válidas"
- "Comandos de la API de administración de claves externas"

Encuentra más información

- "API CreateCluster que se puede usar para habilitar el cifrado de software en reposo"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Configurar la gestión de claves externas

Puedes seguir estos pasos y usar los métodos de la API de Element que se enumeran para configurar tu función de administración de claves externas.

Lo que necesitarás

- Si está configurando la administración de claves externas en combinación con el cifrado de software en reposo, habrá habilitado el cifrado de software en reposo mediante el uso de"CrearClúster" método en un nuevo clúster que no contiene volúmenes.

Pasos

1. Establecer una relación de confianza con el servidor de claves externo (EKS).
   a. Cree un par de claves pública/privada para el clúster de Element que se utiliza para establecer una relación de confianza con el servidor de claves llamando al siguiente método de la API:"Crear par de claves públicas y privadas"
   b. Obtenga la solicitud de firma de certificado (CSR) que la Autoridad de Certificación necesita firmar. La CSR permite al servidor de claves verificar que el clúster de Element que accederá a las claves esté autenticado como tal. Llama al siguiente método de la API:"Solicitud de firma de certificado de cliente"
   c. Utilice la EKS/Autoridad de Certificación para firmar la CSR recuperada. Consulte la documentación de terceros para obtener más información.

2. Cree un servidor y un proveedor en el clúster para comunicarse con EKS. Un proveedor de claves define dónde se debe obtener una clave, y un servidor define los atributos específicos del EKS con el que se comunicará.
   a. Cree un proveedor de claves donde residirán los detalles del servidor de claves llamando al siguiente método de la API:"CrearKeyProviderKmip"
   b. Cree un servidor de claves que proporcione el certificado firmado y el certificado de clave pública de la Autoridad de Certificación llamando a los siguientes métodos de la API:"CrearKeyServerKmip" "Servidor de claves de prueba Kmip"

      Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.

   c. Agregue el servidor de claves al contenedor del proveedor de claves llamando a los siguientes métodos de la API:"Agregar servidor de claves al proveedor Kmip" "TestKeyProviderKmip"

      Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.

3. Como siguiente paso para el cifrado en reposo, realice una de las siguientes acciones:
   a. (Para cifrado de hardware en reposo) Habilitar"Cifrado de hardware en reposo" proporcionando el ID del proveedor de claves que contiene el servidor de claves utilizado para almacenar las claves mediante una llamada a"Habilitar cifrado en reposo" Método API.

      > Debe habilitar el cifrado en reposo a través de"API" . Habilitar el cifrado en reposo mediante el botón existente de la interfaz de usuario de Element hará que la función vuelva a utilizar claves generadas internamente.

   b. (Para el cifrado de software en reposo) Para"Cifrado de software en reposo" Para utilizar el proveedor de claves recién creado, pase el ID del proveedor de claves al"Clave maestra de cifrado de software en reposo" Método API.

Encuentra más información

- "Habilitar y deshabilitar el cifrado para un clúster"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Rekey cifrado de software en reposo clave maestra

Puedes usar la API de Element para volver a generar una clave existente. Este proceso crea una nueva clave maestra de reemplazo para su servidor de administración de claves externo. Las claves maestras siempre se reemplazan por nuevas claves maestras y nunca se duplican ni se sobrescriben.

Es posible que necesite volver a introducir las teclas como parte de uno de los siguientes procedimientos:

- Cree una nueva clave como parte de un cambio de gestión de claves interna a gestión de claves externa.
- Cree una nueva clave como reacción a un evento relacionado con la seguridad o como protección contra el mismo.

Este proceso es asíncrono y devuelve una respuesta antes de que se complete la operación de reenvío de claves. Puedes usar el"ObtenerResultadoAsíncrono" Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.

Lo que necesitarás

- Has habilitado el cifrado de software en reposo mediante"CrearClúster" método en un nuevo clúster que no contiene volúmenes y no tiene E/S. Utilice el siguiente enlace: ../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] para confirmar que el estado es `enabled` antes de continuar.
- Tienes"Se estableció una relación de confianza" entre el clúster SolidFire y un servidor de claves externo (EKS). Ejecutar el"TestKeyProviderKmip" Método para verificar que se ha establecido una conexión con el proveedor de claves.

Pasos

1. Ejecutar el"Proveedores de claves de lista Kmip" comando y copia del ID del proveedor de claves(`keyProviderID`).
2. Ejecutar el"Clave maestra de cifrado de software en reposo" con el `keyManagementType` parámetro como `external` y `keyProviderID` como el número de identificación del proveedor de claves del paso anterior:

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

3. Copia el `asyncHandle` valor de la `RekeySoftwareEncryptionAtRestMasterKey` Respuesta al comando.
4. Ejecutar el"ObtenerResultadoAsíncrono" comando con el `asyncHandle` Valor del paso anterior para confirmar el cambio de configuración. En la respuesta del comando, debería ver que la configuración de la clave maestra anterior se ha actualizado con la nueva información de la clave. Copie el nuevo ID del proveedor de claves para usarlo en un paso posterior.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Ejecutar el `GetSoftwareEncryptionatRestInfo` orden para confirmar que los nuevos detalles clave, incluyendo el `keyProviderID` , han sido actualizados.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Encuentra más información

- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Recuperar claves de autenticación inaccesibles o no válidas

Ocasionalmente, puede producirse un error que requiere la intervención del usuario. En caso de error, se generará un fallo de clúster (denominado código de fallo de clúster). Aquí se describen los dos casos más probables.

El clúster no puede desbloquear las unidades debido a un fallo de clúster KmipServerFault.

Esto puede ocurrir cuando el clúster se inicia por primera vez y el servidor de claves es inaccesible o la clave requerida no está disponible.

1. Siga los pasos de recuperación indicados en los códigos de error del clúster (si los hay).

Es posible que se establezca un fallo sliceServiceUnhealthy porque las unidades de metadatos se han marcado como fallidas y se han colocado en el estado "Disponible".

Pasos para despejar:

1. Vuelva a agregar las unidades.
2. Después de 3 a 4 minutos, compruebe que el `sliceServiceUnhealthy` La avería se ha solucionado.

Ver"códigos de falla del clúster" Para más información.

Comandos de la API de administración de claves externas

Lista de todas las API disponibles para gestionar y configurar EKM.

Se utiliza para establecer una relación de confianza entre el clúster y los servidores externos propiedad del cliente:

- Crear par de claves públicas y privadas
- Solicitud de firma de certificado de cliente

Se utiliza para definir los detalles específicos de los servidores externos propiedad del cliente:

- CrearKeyServerKmip
- ModificarKeyServerKmip
- EliminarKeyServerKmip
- ObtenerKeyServerKmip
- Lista de servidores clave Kmip

- Servidor de claves de prueba Kmip

Se utiliza para crear y mantener proveedores de claves que gestionan servidores de claves externos:

- CrearKeyProviderKmip
- EliminarKeyProviderKmip
- Agregar servidor de claves al proveedor Kmip
- Eliminar servidor de claves del proveedor Kmip
- ObtenerProveedorDeClavesKmip
- Proveedores de claves de lista Kmip
- Clave maestra de cifrado de software en reposo
- TestKeyProviderKmip

Para obtener información sobre los métodos de la API, consulte "Información de referencia de la API".

Información de copyright

Información de la marca comercial