Seguridad

Cloud Insights

NetApp
June 18, 2024

Tabla de contenidos

Seguridad

Seguridad Cloud Insights

La seguridad de los datos de los productos y de los clientes es de vital importancia en NetApp. Cloud Insights sigue las prácticas recomendadas de seguridad a lo largo del ciclo de vida de su versión para garantizar que la información y los datos del cliente están protegidos de la mejor forma posible.

Descripción de la seguridad

Seguridad física

La infraestructura de producción de Cloud Insights se encuentra alojada en Amazon Web Services (AWS). AWS gestiona controles físicos y ambientales relacionados con la seguridad de los servidores de producción de Cloud Insights, que incluyen edificios, así como bloqueos o claves usados en las puertas. Según AWS: “El acceso físico es controlado tanto en el perímetro como en los puntos de entrada del edificio por el personal de seguridad profesional que utiliza videovigilancia, sistemas de detección de intrusiones y otros medios electrónicos. El personal autorizado utiliza mecanismos de autenticación de múltiples factores para acceder a las plantas de los centros de datos”.

Cloud Insights sigue las prácticas recomendadas de "Modelo de responsabilidad compartida" Descrito por AWS.

Seguridad del producto

Cloud Insights sigue un ciclo de vida de desarrollo acorde con los principios ágiles, lo que nos permite abordar cualquier defecto de software orientado a la seguridad de forma más rápida, en comparación con las metodologías de desarrollo del ciclo de lanzamiento más largo. Con metodologías de integración continua, podemos responder rápidamente a los cambios funcionales y de seguridad. Los procedimientos y políticas de gestión de cambios definen cuándo y cómo se producen los cambios y ayudan a mantener la estabilidad del entorno de producción. Cualquier cambio impactante se comunica formalmente, coordina, revisa correctamente y aprueba antes de su lanzamiento al entorno de producción.

Seguridad de la red

El acceso de red a los recursos del entorno Cloud Insights se controla mediante firewalls basados en host. Cada recurso (como un equilibrador de carga o una instancia de máquina virtual) tiene un firewall basado en host que restringe el tráfico entrante sólo a los puertos necesarios para que ese recurso realice su función.

Cloud Insights utiliza diversos mecanismos, incluidos los servicios de detección de intrusiones, para supervisar el entorno de producción en busca de anomalías de seguridad.

Evaluación de riesgos

El equipo de Cloud Insights sigue un proceso formalizado de evaluación de riesgos para proporcionar una forma sistemática y repetible de identificar y evaluar los riesgos para poder gestionarlos adecuadamente a través de un plan de tratamiento de riesgos.

Protección de datos

El entorno de producción de Cloud Insights está configurado en una infraestructura altamente redundante que utiliza varias zonas de disponibilidad para todos los servicios y componentes. Además del uso de una infraestructura informática redundante y de alta disponibilidad, se realiza el backup de datos cruciales a intervalos regulares y se realizan restauraciones periódicas. Las políticas y procedimientos formales de backup minimizan el impacto de las interrupciones de las actividades empresariales y protegen los procesos empresariales contra los efectos de los fallos de los sistemas de información o los desastres y garantizan una reanudación oportuna y adecuada.

Autenticación y gestión del acceso

Todos los accesos de los clientes a Cloud Insights se realizan mediante las interacciones de la interfaz de usuario del navegador por https. La autenticación se realiza a través del servicio de terceros, Auth0. NetApp ha centralizado en esto como capa de autenticación para todos los servicios de datos en el cloud.

Cloud Insights sigue las prácticas recomendadas del sector, incluidos “privilegio mínimo” y “control de acceso basado en funciones” en relación con el acceso lógico al entorno de producción de Cloud Insights. El acceso se controla con una estricta necesidad y sólo se concede al personal autorizado seleccionado mediante mecanismos de autenticación de múltiples factores.

Recopilación y protección de los datos del cliente

Todos los datos del cliente se cifran en tránsito por redes públicas y están cifrados en reposo. Cloud Insights utiliza el cifrado en varios puntos del sistema para proteger los datos del cliente mediante tecnologías que incluyen Seguridad de la capa de transporte (TLS) y el algoritmo AES-256 estándar del sector.

Desaprovisionamiento del cliente

Las notificaciones por correo electrónico se envían en varios intervalos para informar al cliente de que su suscripción está a punto de caducar. Una vez caducada la suscripción, la interfaz de usuario está restringida y comienza un período de gracia para la recopilación de datos. A continuación, se notifica al cliente por correo electrónico. Las suscripciones de prueba tienen un período de gracia de 14 días y las cuentas de suscripción pagadas tienen un período de gracia de 28 días. Una vez caducado el período de gracia, se notifica al cliente por correo electrónico que la cuenta se eliminará en 2 días. Un cliente pagado también puede solicitar directamente estar fuera del servicio.

El equipo de operaciones de Cloud Insights (SRE) elimina los inquilinos caducados y todos los datos de clientes asociados al final del período de gracia o tras la confirmación de la solicitud de un cliente para cancelar su cuenta. En cualquier caso, el equipo de SRE ejecuta una llamada API para eliminar la cuenta. La llamada API elimina la instancia de inquilino y todos los datos de cliente. La eliminación del cliente se verifica llamando a la misma API y verificando que el estado del inquilino del cliente es "ELIMINADO".

Gestión de incidentes de seguridad

Cloud Insights se integra con el proceso del equipo de respuesta a incidentes de seguridad de productos (PSIRT) de NetApp para encontrar, evaluar y resolver vulnerabilidades conocidas. PSIRT recoge información de vulnerabilidad de varios canales, incluidos informes de clientes, ingeniería interna y fuentes ampliamente reconocidas como la base de datos CVE.

Si el equipo de ingeniería de Cloud Insights detecta un problema, el equipo iniciará el proceso, evaluará y posiblemente solucionará el problema.

También es posible que un cliente o investigador de Cloud Insights pueda identificar un problema de seguridad con el producto de Cloud Insights e informar el problema al soporte técnico o directamente al equipo de

respuesta a incidentes de NetApp. En estos casos, el equipo de Cloud Insights iniciará el proceso de PSIRT, evaluará y potencialmente solucionará el problema.

Pruebas de vulnerabilidad y penetración

Cloud Insights sigue las prácticas recomendadas del sector y realiza pruebas periódicas de vulnerabilidad y penetración con profesionales y empresas de seguridad internos y externos.

Formación sobre seguridad

Todo el personal de Cloud Insights se somete a una formación en seguridad, desarrollada para desempeñar funciones individuales, para asegurarse de que cada empleado está equipado para ocuparse de los retos específicos relacionados con la seguridad que plantea sus funciones.

Cumplimiento de normativas

Cloud Insights realiza auditorías y validaciones independientes de terceros de la empresa de APEM externa con licencia de su seguridad, procesos y servicios, incluida la finalización de la auditoría SOC 2.

Notificaciones de seguridad de NetApp

Es posible ver las notificaciones de seguridad disponibles de NetApp "aquí".

Información y Región

NetApp se toma muy en serio la seguridad de la información del cliente. Aquí está cómo y dónde Cloud Insights almacena su información.

¿Qué información almacena Cloud Insights?

Cloud Insights almacena la siguiente información:

- Datos de rendimiento

  Los datos de rendimiento son datos de series temporales que proporcionan información sobre el rendimiento del dispositivo/origen monitorizado. Esto incluye, por ejemplo, el número de iOS proporcionados por un sistema de almacenamiento, el rendimiento de un puerto FibreChannel, el número de páginas entregadas por un servidor web, el tiempo de respuesta de una base de datos y mucho más.

- Datos de inventario

  Los datos de inventario se componen de metadatos que describen el dispositivo/origen supervisado y cómo se configuran. Esto incluye, por ejemplo, versiones de hardware y software instaladas, discos y LUN en un sistema de almacenamiento, núcleos de CPU, RAM y discos de una máquina virtual, los espacios de tablas de una base de datos, el número y tipo de puertos en un switch SAN, nombres de directorios/archivos (si la seguridad de la carga de trabajo de almacenamiento está activada), etc.

- Datos de configuración

  Esto resume los datos de configuración proporcionados por el cliente que se utilizan para gestionar el inventario y las operaciones del cliente, por ejemplo, nombres de host o direcciones IP de los dispositivos supervisados, intervalos de sondeo, valores de tiempo de espera, etc.

- Secretos

  Los secretos consisten en las credenciales utilizadas por la Unidad de adquisición de Cloud Insights para acceder a los servicios y dispositivos del cliente. Estas credenciales se cifran mediante un cifrado asimétrico fuerte, y las claves privadas se almacenan solo en las Unidades de adquisición y nunca salen del entorno del cliente. Incluso los SRES privilegiados de Cloud Insights no pueden acceder a los secretos del cliente en texto simple debido a este diseño.

- Datos funcionales

  Estos son los datos generados como resultado de la prestación del Servicio de datos en el cloud de NetApp, que informa a NetApp sobre el desarrollo, la puesta en marcha, las operaciones, el mantenimiento y la protección del Servicio de datos en el cloud. Los datos funcionales no incluyen información del cliente ni información personal.

- Acceso de usuarios a datos

  Información de autenticación y acceso que permite a NetApp BlueXP comunicarse con sitios regionales de Cloud Insights, incluidos los datos relacionados con la autorización de usuarios.

- Datos del directorio de usuario de seguridad de la carga de trabajo de almacenamiento

  En los casos en que la funcionalidad de seguridad de carga DE trabajo esté activada Y el cliente elija habilitar el recopilador de directorios de usuarios, el sistema almacenará los nombres de visualización de los usuarios, las direcciones de correo electrónico de la empresa y otra información recopilada de Active Directory.

> Los datos del directorio de usuarios hacen referencia a la información del directorio de usuarios recopilada por el recopilador de datos del directorio de usuarios de Workload Security, no a los datos acerca de los usuarios de Cloud Insights/Workload Security ellos mismos.

No se recopilan datos personales explícitos de los recursos de infraestructura y servicios. La información recopilada consiste en métricas de rendimiento, información de configuración y solo metadatos en la infraestructura, del mismo modo que muchos hogares de proveedores, como el soporte automático de NetApp y ActiveIQ. No obstante, según las convenciones de nomenclatura de un cliente, los datos para recursos compartidos, los volúmenes, las máquinas virtuales, los qtrees, las aplicaciones, etc. pueden contener información de identificación personal.

Si está activada la seguridad de la carga de trabajo, el sistema también examina los nombres de archivos y directorios en SMB u otros recursos compartidos, que pueden contener información de identificación personal. Cuando los clientes habilitan el recopilador de directorios de usuarios de seguridad de carga de trabajo (que esencialmente asigna SID de Windows a nombres de usuario a través de Active Directory), Cloud Insights recopilará y almacenará el nombre para mostrar, la dirección de correo electrónico de la empresa y cualquier atributo adicional seleccionado.

Además, se mantienen los registros de acceso a Cloud Insights y contienen las direcciones IP y de correo electrónico de los usuarios que se utilizan para iniciar sesión en el servicio.

¿Dónde se almacena mi información?

Cloud Insights almacena información según la región en la que se crea el entorno.

La siguiente información se almacena en la región de host:

- Información sobre telemetría y activos/objetos, incluidos contadores y métricas de rendimiento
- Información de la unidad de adquisición
- Datos funcionales
- Información de auditoría sobre las actividades de los usuarios dentro de Cloud Insights
- Seguridad de la carga de trabajo Información de Active Directory
- Información de auditoría de seguridad de carga de trabajo

La siguiente información reside en los Estados Unidos, independientemente de la región donde se aloje su entorno de Cloud Insights:

- Información del sitio de entorno (a veces denominado "inquilino"), como el propietario del sitio/cuenta.
- Información que permite a NetApp BlueXP comunicarse con sitios regionales de Cloud Insights, incluida cualquier cosa que tenga que ver con la autorización de usuarios.
- Información relacionada con la relación entre el usuario de Cloud Insights y el inquilino.

Regiones de acogida

Las regiones de host incluyen:

- EE.UU.: Este-1
- EMEA: eu-central-1
- APAC: ap-sureste-2

Más información

Puede obtener más información sobre la privacidad y la seguridad de NetApp en los siguientes enlaces:

- "Centro de confianza"
- "Transferencias de datos internacionales"
- "Normas Corporativas vinculantes"
- "Respuesta a solicitudes de datos de terceros"
- "Principios de privacidad de NetApp"

Herramienta securityadmin

Cloud Insights incluye funciones de seguridad que permiten que su entorno funcione con una seguridad mejorada. Las características incluyen mejoras en el cifrado, hash de contraseñas y la capacidad de cambiar contraseñas de usuario internas, así como pares de claves que cifran y descifran contraseñas.

Para proteger los datos confidenciales, NetApp recomienda cambiar las claves predeterminadas y la contraseña de usuario *Acquisition* después de realizar una instalación o actualización.

Las contraseñas cifradas del origen de datos se almacenan en Cloud Insights, que utiliza una clave pública para cifrar contraseñas cuando un usuario las introduce en una página de configuración del recopilador de datos. Cloud Insights no tiene las claves privadas necesarias para descifrar las contraseñas del recopilador de datos; solo las Unidades de Adquisición (AUS) tienen la clave privada del recopilador de datos necesaria para

descifrar las contraseñas del recopilador de datos.

Consideraciones sobre la actualización y la instalación

Cuando el sistema Insight contiene configuraciones de seguridad no predeterminadas (es decir, contraseñas recodificadas), debe realizar una copia de seguridad de sus configuraciones de seguridad. La instalación de software nuevo o, en algunos casos, la actualización de software, revierte el sistema a una configuración de seguridad predeterminada. Cuando el sistema vuelve a la configuración predeterminada, debe restaurar la configuración no predeterminada para que el sistema funcione correctamente.

Gestión de la seguridad en la unidad de adquisición

La herramienta SecurityAdmin le permite administrar opciones de seguridad para Cloud Insights y se ejecuta en el sistema de unidades de adquisición. La gestión de seguridad incluye la gestión de claves y contraseñas, el guardado y la restauración de configuraciones de seguridad que se crean o restauran con la configuración predeterminada.

Antes de empezar

- Debe tener privilegios de administrador en el sistema AU para instalar el software de la unidad de adquisición (que incluye la herramienta SecurityAdmin).
- Si tiene usuarios que no son administradores y que posteriormente necesitarán acceder a la herramienta SecurityAdmin, deben agregarse al grupo *cisys*. El grupo *cisys* se crea durante la instalación de AU.

Después de la instalación de AU, la herramienta SecurityAdmin se encuentra en el sistema de unidades de adquisición en cualquiera de estas ubicaciones:

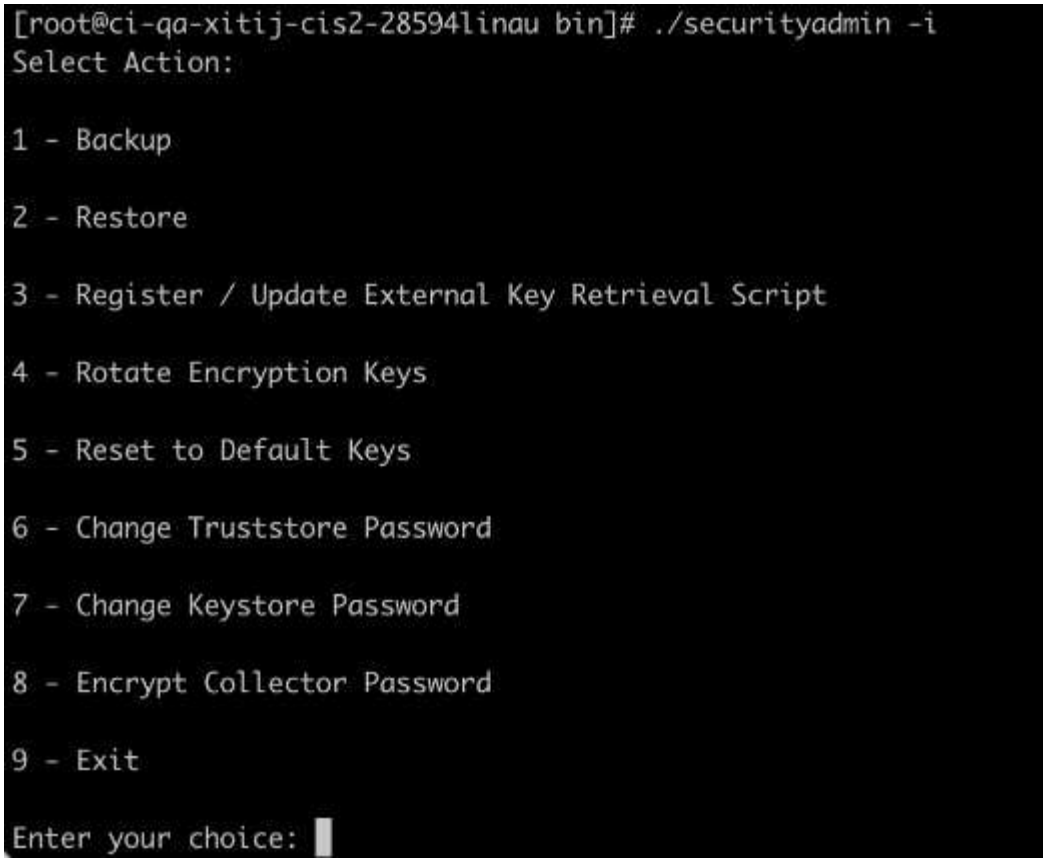
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Con la herramienta SecurityAdmin

Inicie la herramienta SecurityAdmin en modo interactivo (-i).

Se recomienda utilizar la herramienta SecurityAdmin en modo interactivo, para evitar pasar secretos en la línea de comandos, que se pueden capturar en los registros.

Se muestran las siguientes opciones:



1. **Backup**

   Crea un archivo zip de copia de seguridad del almacén que contiene todas las contraseñas y claves y coloca el archivo en una ubicación especificada por el usuario o en las siguientes ubicaciones predeterminadas:

   ```
   Windows - C:\Program Files\SANscreen\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Se recomienda que las copias de seguridad de vault se mantengan seguras, ya que incluyen información confidencial.

2. **Restaurar**

   Restaura la copia de seguridad zip del almacén que se creó. Una vez restaurada, todas las contraseñas y claves se revierten a valores existentes en el momento de la creación del backup.

   La restauración se puede utilizar para sincronizar contraseñas y claves en varios servidores, por ejemplo, siguiendo estos pasos: 1) Cambiar las claves de cifrado en la AU. 2) Crear una copia de seguridad del almacén. 3) Restaurar la copia de seguridad del almacén en cada uno de los AUS.

3. **Registrar / Actualizar Script de Recuperación de Clave Externa**

   Utilice un script externo para registrar o cambiar las claves de cifrado AU utilizadas para cifrar o descifrar las contraseñas del dispositivo.

   Al cambiar las claves de cifrado, debe realizar un backup de la nueva configuración de seguridad para

poder restaurarla después de una actualización o instalación.

Nota Esta opción solo está disponible en Linux.

Cuando utilice su propio script de recuperación de claves con la herramienta SecurityAdmin, tenga en cuenta lo siguiente:

- El algoritmo soportado actual es RSA con un mínimo de 2048 bits.
- El script debe devolver las claves privadas y públicas en texto sin formato. El script no debe devolver claves públicas y privadas cifradas.
- El script debe devolver contenido sin procesar y codificado (solo en formato PEM).
- El script externo debe tener permisos *execute*.

4. * Girar claves de cifrado*

   Gire sus claves de cifrado (anula el registro de las claves actuales y registra las nuevas claves). Para usar una clave desde un sistema de gestión de claves externa, se deben especificar el identificador de clave pública y el identificador de clave privada.

5. **Restablecer a las teclas predeterminadas**

   Restablece la contraseña de usuario de adquisición y las claves de cifrado de usuario de adquisición a los valores predeterminados, los valores predeterminados son los que se proporcionan durante la instalación.

6. **Cambiar contraseña de Truststore**

   Cambie la contraseña del almacén de confianza.

7. **Cambiar Contraseña de Almacén de Claves**

   Cambie la contraseña del almacén de claves.

8. * Cifrar contraseña de recopilador*

   Cifrar contraseña del recopilador de datos.

9. **Salida**

   Salga de la herramienta SecurityAdmin.

Elija la opción que desea configurar y siga las indicaciones.

Especificación de un usuario para ejecutar la herramienta

Si se encuentra en un entorno controlado y consciente de la seguridad, es posible que no tenga el grupo *cisys*, pero aún así desee que usuarios específicos ejecuten la herramienta SecurityAdmin.

Puede lograr esto instalando manualmente el software AU y especificando el usuario/grupo al que desea acceder.

- Con la API, descargue el instalador de CI en el sistema AU y descomprima.
  - Necesitará un token de autorización única. Consulte la documentación de API Swagger (*Admin* > *API Access* y seleccione el enlace *API Documentation*) y busque la sección *GET /au/oneTimeToken* API.

    - Una vez que tenga el token, utilice la API *GET /au/installers/{platform}/{version}* para descargar el archivo del instalador. Deberá proporcionar la plataforma (Linux o Windows), así como la versión del instalador.
- Copie el archivo de instalación descargado en el sistema AU y descomprima el archivo.
- Navegue a la carpeta que contiene los archivos y ejecute el instalador como root, especificando el usuario y el grupo:

```
./cloudinsights-install.sh <User> <Group>
```

Si el usuario y/o grupo especificados no existen, se crearán. El usuario tendrá acceso a la herramienta SecurityAdmin.

Actualizando o eliminando proxy

La herramienta SecurityAdmin se puede utilizar para establecer o eliminar información de proxy para la unidad de adquisición ejecutando la herramienta con el parámetro *-pr*:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Cloud Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Por ejemplo, para eliminar el proxy, ejecute este comando:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Debe reiniciar la unidad de adquisición después de ejecutar el comando.
```

Para actualizar un proxy, el comando es

```
./securityadmin -pr -upr <arg>
```

Recuperación de clave externa

Si proporciona un script de shell UNIX, puede ser ejecutado por la unidad de adquisición para recuperar la **clave privada** y la **clave pública** de su sistema de gestión de claves.

Para recuperar la clave, Cloud Insights ejecutará el script, pasando dos parámetros: *Key id* y *key type*. *Key id* se puede usar para identificar la clave en su sistema de gestión de claves. *Key type* es “public” o “private”. Cuando el tipo de clave es “public”, el script debe devolver la clave public. Cuando el tipo de clave es privado, se debe devolver la clave privada.

Para devolver la tecla a la unidad de adquisición, el script debe imprimir la tecla en la salida estándar. El script debe imprimir *ONLY* la clave para la salida estándar; no se debe imprimir ningún otro texto en la salida estándar. Una vez que la clave solicitada se imprime en la salida estándar, el script debe salir con un código de salida de 0; cualquier otro código de retorno se considera un error.

El script debe registrarse en la unidad de adquisición mediante la herramienta SecurityAdmin, que ejecutará el script junto con la unidad de adquisición. El script debe tener permisos *READ* y *EXECUTE* para el usuario root y cisys. Si el script de shell se modifica después de registrarse, el script de shell modificado debe volver a registrarse con la unidad de adquisición.

parámetro de entrada: id de clave	Identificador de clave utilizado para identificar la clave en el sistema de gestión de claves de los clientes.
parámetro de entrada: tipo de clave	público o privado.
salida	La clave solicitada debe imprimirse en la salida estándar. Actualmente se admite la clave RSA de 2048 bits. Las llaves deben estar codificadas e impresas en el siguiente formato - Formato de clave privada - PEM, DER-codificado PKCS8 PrivateKeyInfo RFC 5958 Formato de clave pública - PEM, DER-encoded X,509 SubjectPublicKeyInfo RFC 5280
código de salida	Código de salida cero para éxito. Todos los demás valores de salida se consideran fallidos.
permisos de script	El script debe tener permisos de lectura y ejecución para el usuario root y cisys.
registros	Se registran las ejecuciones de script. Los registros se pueden encontrar en - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Cifrado de una contraseña para su uso en la API

La opción 8 le permite cifrar una contraseña, que luego puede pasar a un recopilador de datos a través de API.

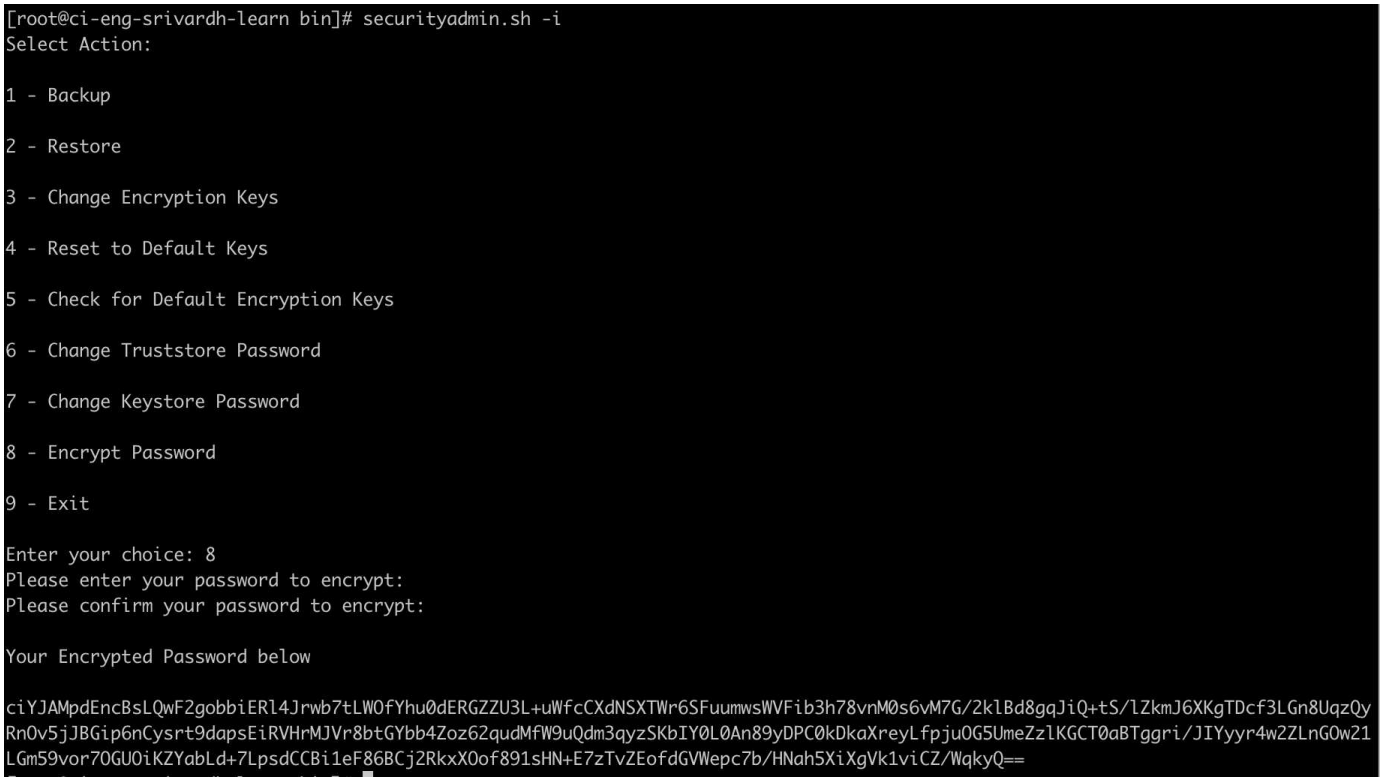
Inicie la herramienta SecurityAdmin en modo interactivo y seleccione la opción 8: *Encrypt Password*.

```
 securityadmin.sh -i
Se le pedirá que introduzca la contraseña que desea cifrar. Tenga en
cuenta que los caracteres que escriba no se muestran en la pantalla.
Vuelva a introducir la contraseña cuando se le solicite.
```

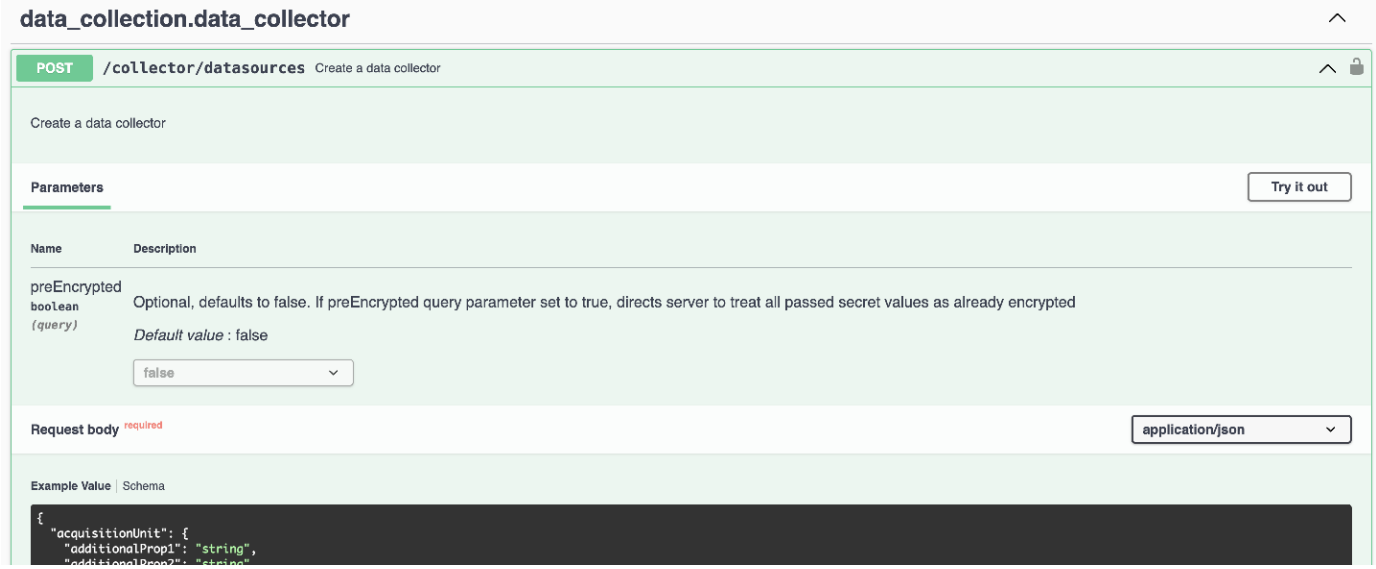
Alternativamente, si va a utilizar el comando en un script, en una línea de comandos utilice *securityadmin.sh* con el parámetro «-enc», pasando su contraseña no cifrada:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Ejemplo de CLI"]
```

La contraseña cifrada se muestra en la pantalla. Copie toda la cadena, incluidos los símbolos iniciales o finales.



Para enviar la contraseña cifrada a un recopilador de datos, puede utilizar la API de recopilación de datos. El Swagger para esta API se puede encontrar en **Admin > API Access** y haga clic en el enlace «Documentación de API». Seleccione el tipo de API de recopilación de datos. En el encabezado *data_collection.data_collector*, seleccione la API */collector/datasources* POST para este ejemplo.



Si establece la opción *preEncrypted* en *True*, cualquier contraseña que pase a través del comando API se tratará como **ya cifrada**; la API no volverá a cifrar la(s) contraseña(s). Al crear su API, simplemente pegue la contraseña cifrada previamente en la ubicación adecuada.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```


Cifrado de una contraseña para su uso en la API

La opción 8 le permite cifrar una contraseña, que luego puede pasar a un recopilador de datos a través de API.

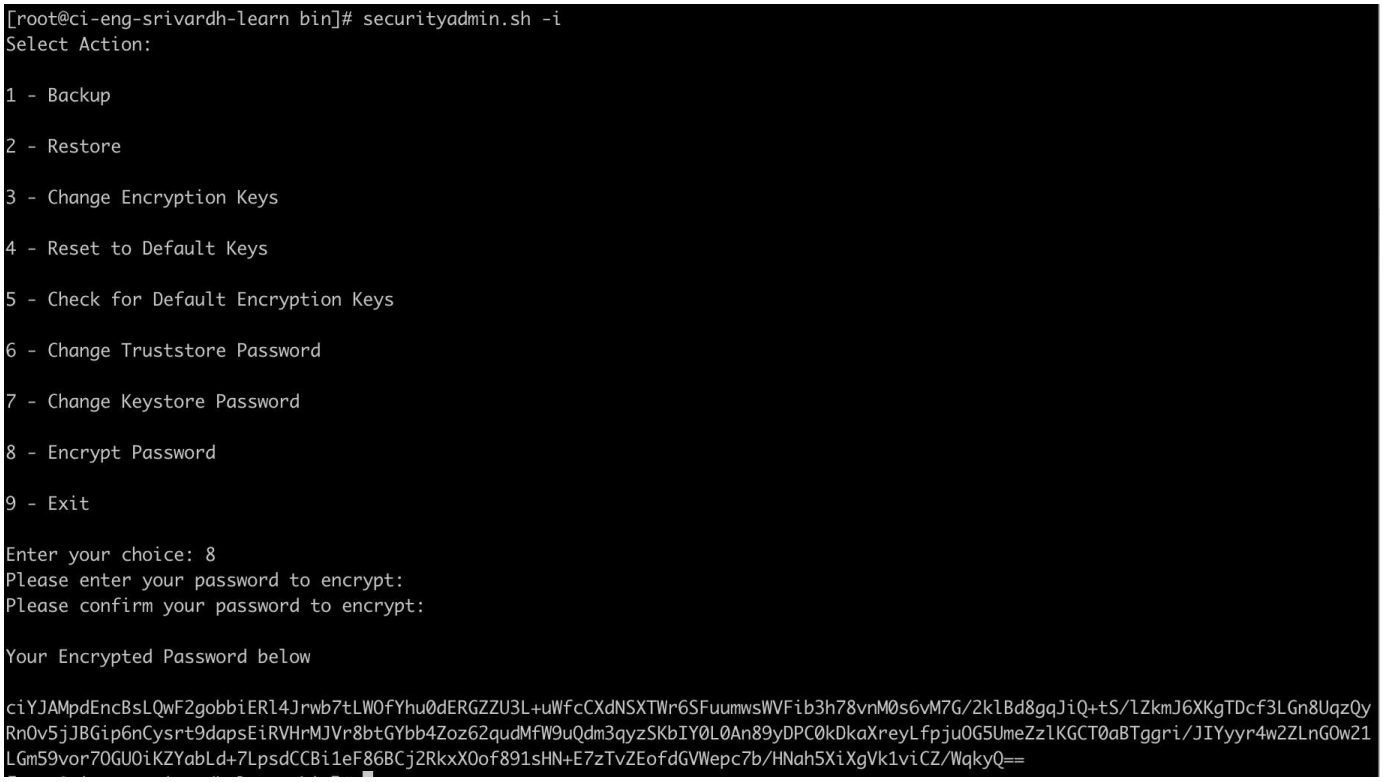
Inicie la herramienta SecurityAdmin en modo interactivo y seleccione la opción 8: *Encrypt Password*.

```
 securityadmin.sh -i
Se le pedirá que introduzca la contraseña que desea cifrar. Tenga en
cuenta que los caracteres que escriba no se muestran en la pantalla.
Vuelva a introducir la contraseña cuando se le solicite.
```

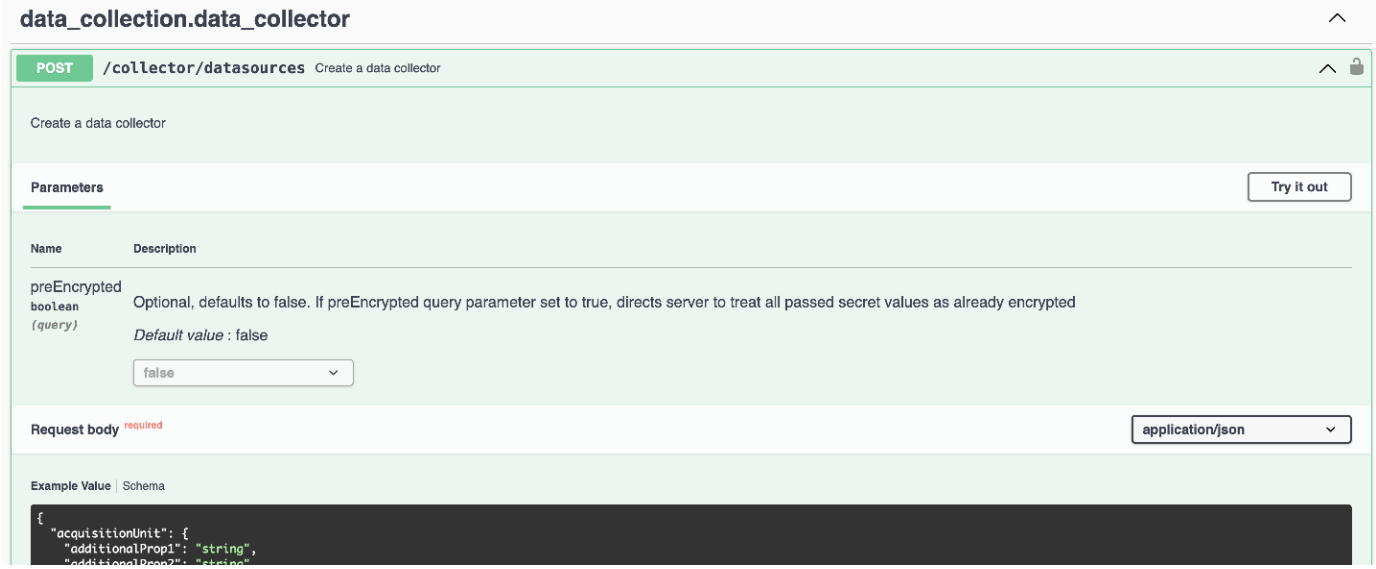
Alternativamente, si va a utilizar el comando en un script, en una línea de comandos utilice *securityadmin.sh* con el parámetro «-enc», pasando su contraseña no cifrada:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Ejemplo de CLI"]
```

La contraseña cifrada se muestra en la pantalla. Copie toda la cadena, incluidos los símbolos iniciales o finales.



Para enviar la contraseña cifrada a un recopilador de datos, puede utilizar la API de recopilación de datos. El Swagger para esta API se puede encontrar en **Admin > API Access** y haga clic en el enlace «Documentación de API». Seleccione el tipo de API de recopilación de datos. En el encabezado *data_collection.data_collector*, seleccione la API */collector/datasources* POST para este ejemplo.



Si establece la opción *preEncrypted* en *True*, cualquier contraseña que pase a través del comando API se tratará como **ya cifrada**; la API no volverá a cifrar la(s) contraseña(s). Al crear su API, simplemente pegue la contraseña cifrada previamente en la ubicación adecuada.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```