Seguridad

Data Infrastructure Insights

NetApp
February 03, 2026

Tabla de contenidos

Seguridad . . . 1
Data Infrastructure Insights y seguridad . . . 1
Descripción general de seguridad . . . 1
Información y Región . . . 3
¿Qué información almacena Data Infrastructure Insights ? . . . 3
¿Dónde se almacena mi información? . . . 4
Más información . . . 5
Herramienta SecurityAdmin . . . 5
Consideraciones de actualización e instalación . . . 6
Gestión de la seguridad en la unidad de adquisición . . . 6
Antes de empezar . . . 6
Uso de la herramienta SecurityAdmin . . . 6
Especificar un usuario para ejecutar la herramienta . . . 8
Actualización o eliminación de proxy . . . 8
Recuperación de clave externa . . . 9
Cifrado de una contraseña para su uso en API . . . 10

Seguridad

Data Infrastructure Insights y seguridad

La seguridad de los datos de productos y clientes es de suma importancia en NetApp. Data Infrastructure Insights sigue las mejores prácticas de seguridad durante todo el ciclo de vida del lanzamiento para garantizar que la información y los datos del cliente estén protegidos de la mejor manera posible.

Descripción general de seguridad

Seguridad física

La infraestructura de producción de Data Infrastructure Insights está alojada en Amazon Web Services (AWS). AWS administra los controles relacionados con la seguridad física y ambiental de los servidores de producción de Data Infrastructure Insights , que incluyen edificios, así como cerraduras o llaves utilizadas en las puertas. Según AWS: “El acceso físico está controlado tanto en el perímetro como en los puntos de ingreso al edificio por personal de seguridad profesional que utiliza videovigilancia, sistemas de detección de intrusos y otros medios electrónicos. El personal autorizado utiliza mecanismos de autenticación multifactor para acceder a los pisos del centro de datos”.

Data Infrastructure Insights sigue las mejores prácticas de la"Modelo de responsabilidad compartida" descrito por AWS.

Seguridad del producto

Data Infrastructure Insights sigue un ciclo de vida de desarrollo en línea con los principios Agile, lo que nos permite abordar cualquier defecto de software orientado a la seguridad más rápidamente, en comparación con las metodologías de desarrollo de ciclos de lanzamiento más largos. Utilizando metodologías de integración continua, somos capaces de responder rápidamente a cambios tanto funcionales como de seguridad. Los procedimientos y políticas de gestión de cambios definen cuándo y cómo ocurren los cambios y ayudan a mantener la estabilidad del entorno de producción. Cualquier cambio impactante se comunica formalmente, se coordina, se revisa adecuadamente y se aprueba antes de su lanzamiento al entorno de producción.

Seguridad de la red

El acceso de red a los recursos en el entorno de Data Infrastructure Insights está controlado por firewalls basados en host. Cada recurso (como un balanceador de carga o una instancia de máquina virtual) tiene un firewall basado en host que restringe el tráfico entrante únicamente a los puertos necesarios para que ese recurso realice su función.

Data Infrastructure Insights utiliza varios mecanismos, incluidos servicios de detección de intrusiones, para monitorear el entorno de producción en busca de anomalías de seguridad.

Evaluación de riesgos

El equipo de Data Infrastructure Insights sigue un proceso formalizado de evaluación de riesgos para proporcionar una forma sistemática y repetible de identificar y evaluar los riesgos para que puedan gestionarse adecuadamente a través de un plan de tratamiento de riesgos.

Protección de datos

El entorno de producción de Data Infrastructure Insights está configurado en una infraestructura altamente redundante que utiliza múltiples zonas de disponibilidad para todos los servicios y componentes. Además de utilizar una infraestructura informática redundante y de alta disponibilidad, se realizan copias de seguridad de los datos críticos a intervalos regulares y las restauraciones se prueban periódicamente. Las políticas y procedimientos formales de respaldo minimizan el impacto de las interrupciones de las actividades comerciales y protegen los procesos de negocio contra los efectos de fallas de los sistemas de información o desastres y garantizan su reanudación oportuna y adecuada.

Autenticación y gestión de acceso

Todo acceso del cliente a Data Infrastructure Insights se realiza a través de interacciones de la interfaz de usuario del navegador mediante https. La autenticación se realiza a través del servicio de terceros, Auth0. NetApp ha centralizado esto como la capa de autenticación para todos los servicios de datos en la nube.

Data Infrastructure Insights sigue las mejores prácticas de la industria, incluido el “Mínimo privilegio” y el “Control de acceso basado en roles” en torno al acceso lógico al entorno de producción de Data Infrastructure Insights . El acceso se controla según las necesidades estrictas y solo se concede a personal autorizado seleccionado que utiliza mecanismos de autenticación de múltiples factores.

Recopilación y protección de datos de clientes

Todos los datos del cliente se cifran en tránsito a través de redes públicas y se cifran en reposo. Data Infrastructure Insights utiliza cifrado en varios puntos del sistema para proteger los datos de los clientes utilizando tecnologías que incluyen seguridad de la capa de transporte (TLS) y el algoritmo AES-256 estándar de la industria.

Desaprovisionamiento de clientes

Se envían notificaciones por correo electrónico a distintos intervalos para informar al cliente que su suscripción está a punto de expirar. Una vez que expira la suscripción, la interfaz de usuario se restringe y comienza un período de gracia para la recopilación de datos. Posteriormente se notifica al cliente por correo electrónico. Las suscripciones de prueba tienen un período de gracia de 14 días y las cuentas de suscripción paga tienen un período de gracia de 28 días. Una vez transcurrido 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 la baja del servicio.

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

Gestión de incidentes de seguridad

Data Infrastructure Insights está integrado con el proceso del Equipo de respuesta a incidentes de seguridad de productos (PSIRT) de NetApp para encontrar, evaluar y resolver vulnerabilidades conocidas. PSIRT obtiene información sobre vulnerabilidades de múltiples canales, incluidos informes de clientes, ingeniería interna y fuentes ampliamente reconocidas como la base de datos CVE.

Si el equipo de ingeniería de Data Infrastructure Insights detecta un problema, iniciará el proceso PSIRT, evaluará y potencialmente solucionará el problema.

También es posible que un cliente o investigador de Data Infrastructure Insights identifique un problema de

seguridad con el producto Data Infrastructure Insights e informe el problema al Soporte técnico o directamente al equipo de respuesta a incidentes de NetApp. En estos casos, el equipo de Data Infrastructure Insights iniciará el proceso PSIRT, evaluará y potencialmente solucionará el problema.

Pruebas de vulnerabilidad y penetración

Data Infrastructure Insights sigue las mejores prácticas de la industria y realiza pruebas periódicas de vulnerabilidad y penetración con profesionales y empresas de seguridad internas y externas.

Capacitación en concientización sobre seguridad

Todo el personal de Data Infrastructure Insights recibe capacitación en seguridad, desarrollada para roles individuales, para garantizar que cada empleado esté equipado para manejar los desafíos específicos de seguridad de sus roles.

Cumplimiento

Data Infrastructure Insights realiza auditorías y validaciones de terceros independientes a través de una firma de contabilidad pública externa autorizada sobre su seguridad, procesos y servicios, incluida la finalización de la auditoría SOC 2.

Avisos de seguridad de NetApp

Puede ver los avisos de seguridad disponibles de NetApp"aquí" .

Información y Región

NetApp se toma muy en serio la seguridad de la información de los clientes. Aquí se explica cómo y dónde Data Infrastructure Insights almacena su información.

¿Qué información almacena Data Infrastructure Insights ?

Data Infrastructure 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/fuente monitoreado. Esto incluye, por ejemplo, la cantidad de E/S entregadas por un sistema de almacenamiento, el rendimiento de un puerto FibreChannel, la cantidad de páginas entregadas por un servidor web, el tiempo de respuesta de una base de datos y más.

- Datos de inventario

  Los datos de inventario constan de metadatos que describen el dispositivo/fuente monitoreado y cómo está configurado. 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, espacios de tabla de una base de datos, la cantidad y el tipo de puertos en un conmutador SAN, nombres de directorio/archivo (si la seguridad de carga de trabajo de almacenamiento está habilitada), etc.

- Datos de configuración

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

- Misterios

  Los secretos consisten en las credenciales utilizadas por la Unidad de Adquisición de Data Infrastructure Insights para acceder a los dispositivos y servicios del cliente. Estas credenciales se cifran mediante un cifrado asimétrico fuerte y las claves privadas se almacenan únicamente en las Unidades de Adquisición y nunca salen del entorno del cliente. Incluso los SRE de Data Infrastructure Insights privilegiados no pueden acceder a los secretos de los clientes en texto sin formato debido a este diseño.

- Datos funcionales

  Estos son datos generados como resultado de que NetApp proporcione el Servicio de datos en la nube, que informa a NetApp sobre el desarrollo, la implementación, las operaciones, el mantenimiento y la protección de dicho Servicio. Los datos funcionales no contienen información del cliente ni información personal.

- Datos de acceso del usuario

  Información de autenticación y acceso que permite a NetApp Console comunicarse con los sitios regionales de Data Infrastructure Insights , incluidos los datos relacionados con la autorización del usuario.

- Seguridad de la carga de trabajo de almacenamiento Datos del directorio de usuarios

  En los casos en que la funcionalidad de Seguridad de carga de trabajo está habilitada Y el cliente elige habilitar el recopilador de Directorio de usuarios, el sistema almacenará los nombres para mostrar de los usuarios, las direcciones de correo electrónico corporativas y otra información recopilada de Active Directory.

> Los datos del Directorio de usuarios se refieren a la información del Directorio de usuarios recopilada por el recopilador de datos del Directorio de usuarios de Workload Security, no a datos sobre los usuarios de Data Infrastructure Insights/Workload Security en sí.

No se recopilan datos personales explícitos de los recursos de infraestructura y servicios. La información recopilada consta únicamente de métricas de rendimiento, información de configuración y metadatos de infraestructura, de forma muy similar a muchos servicios telefónicos de proveedores, incluidos el soporte automático de NetApp y ActiveIQ. Sin embargo, dependiendo de las convenciones de nomenclatura del cliente, los datos de recursos compartidos, volúmenes, máquinas virtuales, qtrees, aplicaciones, etc. pueden contener información de identificación personal.

Si la seguridad de carga de trabajo está habilitada, el sistema también analiza 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 directorio de usuarios de Workload Security (que básicamente asigna SID de Windows a nombres de usuario a través de Active Directory), Data Infrastructure Insights recopilará y almacenará el nombre para mostrar, la dirección de correo electrónico corporativa y cualquier atributo adicional seleccionado.

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

¿Dónde se almacena mi información?

Data Infrastructure Insights almacena información según la región en la que se crea su entorno.

La siguiente información se almacena en la región host:

- Telemetría e información de 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 Data Infrastructure Insights
- Información de Active Directory sobre seguridad de la carga de trabajo
- Información de auditoría de seguridad de la carga de trabajo

La siguiente información reside en los Estados Unidos, independientemente de la región que aloje su entorno de Data Infrastructure Insights :

- Información del sitio del entorno (a veces llamado "inquilino"), como el propietario del sitio/cuenta.
- Información que permite que NetApp Console se comunique con los sitios regionales de Data Infrastructure Insights , incluido todo lo relacionado con la autorización del usuario.
- Información relacionada con la relación entre el usuario de Data Infrastructure Insights y el inquilino.

Regiones anfitrionas

Las regiones anfitrionas incluyen:

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

Más información

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

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

Herramienta SecurityAdmin

Data Infrastructure Insights Incluye funciones de seguridad que permiten que su entorno funcione con mayor seguridad. Las características incluyen mejoras en el cifrado, el hash de contraseñas y la capacidad de cambiar las contraseñas de usuarios internos, así como los pares de claves que cifran y descifran las contraseñas.

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

Las contraseñas cifradas de la fuente de datos se almacenan en Data Infrastructure Insights, que utiliza una clave pública para cifrar las contraseñas cuando un usuario las ingresa en una página de configuración del recopilador de datos. Data Infrastructure Insights no tiene las claves privadas necesarias para descifrar las contraseñas del recopilador de datos; solo las unidades de adquisición (AU) tienen la clave privada del

recopilador de datos necesaria para descifrar las contraseñas del recopilador de datos.

Consideraciones de actualización e instalación

Cuando su sistema Insight contiene configuraciones de seguridad no predeterminadas (es decir, ha reingresado contraseñas), debe realizar una copia de seguridad de sus configuraciones de seguridad. Instalar software nuevo, o en algunos casos actualizar software, revierte el sistema a una configuración de seguridad predeterminada. Cuando el sistema vuelva a la configuración predeterminada, deberá 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 las opciones de seguridad para Data Infrastructure Insights y se ejecuta en el sistema de la unidad de adquisición. La gestión de seguridad incluye la gestión de claves y contraseñas, el guardado y la restauración de las configuraciones de seguridad creadas o la restauración de las configuraciones a los valores predeterminados.

Antes de empezar

- Debe tener privilegios de administrador en el sistema AU para poder instalar el software de la Unidad de Adquisición (que incluye la herramienta SecurityAdmin).
- Si tiene usuarios que no sean 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 instalar AU, la herramienta SecurityAdmin se encuentra en el sistema de la unidad de adquisición en cualquiera de estas ubicaciones:

```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Uso de 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 pueden quedar capturados en los registros.

Se muestran las siguientes opciones:

[Opciones para la herramienta SecurityAdmin (Linux)]

1. **Respaldo**

   Crea un archivo zip de respaldo de la bóveda 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 - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\backup\vault
Linux - /var/log/netapp/oci/backup/vault
```

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

2. **Restaurar**

   Restaura la copia de seguridad zip de la bóveda que se creó. Una vez restaurada, todas las contraseñas y claves vuelven a los valores existentes en el momento de la creación de la copia de seguridad.

   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) Cree una copia de seguridad de la bóveda. 3) Restaure la copia de seguridad de la bóveda en cada una de las AU.

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.

   Cuando cambie las claves de cifrado, deberá realizar una copia de seguridad de su nueva configuración de seguridad para poder restaurarla después de una actualización o instalación.

   Tenga en cuenta que esta opción sólo está disponible en Linux.

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

   - El algoritmo admitido actualmente 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 (sólo formato PEM).
   - El script externo debe tener permisos de *ejecución*.

4. **Rotar claves de cifrado**

   Rota tus claves de cifrado (anula el registro de las claves actuales y registra claves nuevas). Para utilizar una clave de un sistema de administración de claves externo, debe especificar el ID de la clave pública y el ID de la clave privada.

5. **Restablecer claves predeterminadas**

   Restablece la contraseña del usuario de adquisición y las claves de cifrado del usuario de adquisición a los valores predeterminados. Los valores predeterminados son los proporcionados durante la instalación.

6. **Cambiar contraseña de Truststore**

   Cambiar la contraseña del almacén de confianza.

7. **Cambiar la contraseña del almacén de claves**

Cambiar la contraseña del almacén de claves.

8. **Contraseña del recopilador de cifrado**

   Cifrar la contraseña del recopilador de datos.

9. **Salida**

   Salga de la herramienta SecurityAdmin.

Elija la opción que desea configurar y siga las instrucciones.

Especificar 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 para el cual desea acceso.

- Usando la API, descargue el instalador CI al sistema AU y descomprímalo.
  - Necesitará un token de autorización de un solo uso. Consulte la documentación de API Swagger (*Admin > Acceso a API* y seleccione el enlace *Documentación de API*) y busque la sección API *GET /au/oneTimeToken*.
  - Una vez que tenga el token, use la API *GET /au/installers/{platform}/{version}* para descargar el archivo de instalación. Necesitará proporcionar la plataforma (Linux o Windows) así como la versión del instalador.
- Copie el archivo de instalación descargado al sistema AU y descomprímalo.
- 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 especificado no existe, se crearán. El usuario tendrá acceso a la herramienta SecurityAdmin.

Actualización o eliminación de proxy

La herramienta SecurityAdmin se puede utilizar para configurar 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 Data
Infrastructure 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 de UNIX, la unidad de adquisición puede ejecutarlo para recuperar la **clave**

privada y la **clave pública** de su sistema de administración de claves.

Para recuperar la clave, Data Infrastructure Insights ejecutará el script, pasando dos parámetros: *key id* y *key type*. *Key id* se puede utilizar para identificar la clave en su sistema de gestión de claves. El tipo de clave es "pública" o "privada". Cuando el tipo de clave es "pública", el script debe devolver la clave pública. Cuando el tipo de clave es "privada", se debe devolver la clave privada.

Para enviar la clave de vuelta a la unidad de adquisición, el script debe imprimir la clave en la salida estándar. El script debe imprimir *sólo* la clave en 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 de *lectura* y *ejecución* para el usuario root y "cisys". Si el script de shell se modifica después del registro, el script de shell modificado debe volver a registrarse en 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 del cliente.
parámetro de entrada: tipo de clave	público o privado.
producción	La clave solicitada debe imprimirse en la salida estándar. Actualmente se admite una clave RSA de 2048 bits. Las claves deben codificarse e imprimirse en el siguiente formato: formato de clave privada: PEM, codificado en DER PKCS8 PrivateKeyInfo RFC 5958 formato de clave pública: PEM, codificado en DER X.509 SubjectPublicKeyInfo RFC 5280
código de salida	Código de salida de cero para el éxito. Todos los demás valores de salida se consideran un fracaso.
permisos de script	El script debe tener permisos de lectura y ejecución para el usuario root y "cisys".
registros	Las ejecuciones de scripts se registran. 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 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: *Cifrar contraseña*.

```
 securityadmin.sh -i
Se le solicitará que ingrese la contraseña que desea cifrar.  Tenga en
cuenta que los caracteres que escribe no se muestran en la pantalla.
Vuelva a ingresar la contraseña cuando se le solicite.
```

Alternativamente, si va a utilizar el comando en un script, en una línea de comando use *securityadmin.sh* con

el parámetro "-enc", pasando su contraseña sin cifrar:

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

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

[Modo interactivo Cifrar contraseña, ancho=640]

Para enviar la contraseña cifrada a un recopilador de datos, puede utilizar la API de recopilación de datos. La documentación de esta API se puede encontrar en **Admin > Acceso a la API** y hacer clic en el enlace "Documentación de la API". Seleccione el tipo de API "Recopilación de datos". Bajo el encabezado *data_collection.data_collector*, elija la API POST */collector/datasources* para este ejemplo.

[API para la recopilación de datos]

Si establece la opción *preEncrypted* en *True*, cualquier contraseña que pase a través del comando API será tratada como **ya cifrada**; la API no volverá a cifrar las contraseñas. Al crear su API, simplemente pegue la contraseña previamente cifrada en la ubicación adecuada.

[Ejemplo de API, ancho=600]