Generar paquete de diagnóstico para dispositivos de análisis de red seguros

Contenido

Introducción

Este documento describe los diferentes procedimientos disponibles para recopilar un paquete de diagnóstico para dispositivos de Secure Network Analytics (SNA).

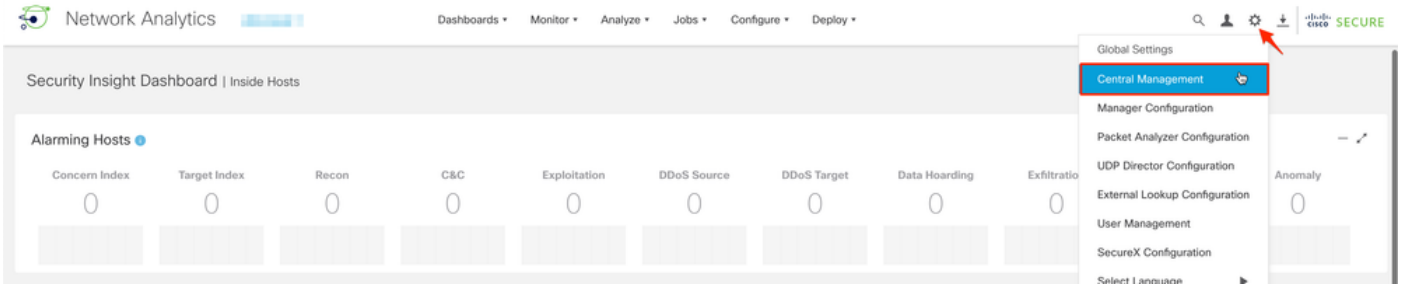
Procedimiento

Hay tres métodos principales para generar el paquete de diagnóstico para los dispositivos SNA. El método sugerido es el **Método 1. Desde la interfaz de usuario del administrador Web**, sin embargo, los otros dos métodos son una opción en caso de que la interfaz de usuario Web del jefe no esté disponible.

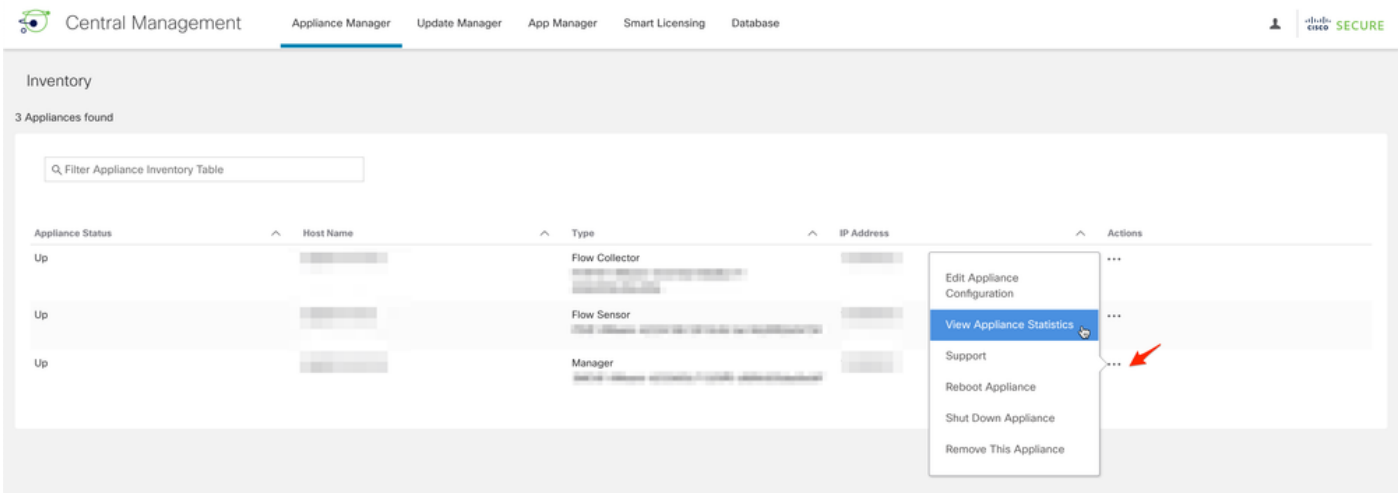
> **Nota:** Si la interfaz de usuario web del jefe no está disponible y necesita generar un paquete de diagnóstico desde el administrador, consulte el **método 3. Desde la interfaz de línea de comandos (CLI)** de cada dispositivo.

Método 1. Desde la interfaz de usuario web del jefe

1. Inicie sesión en la interfaz de usuario web del jefe.
2. Vaya a **Configuración global > Administración central**.



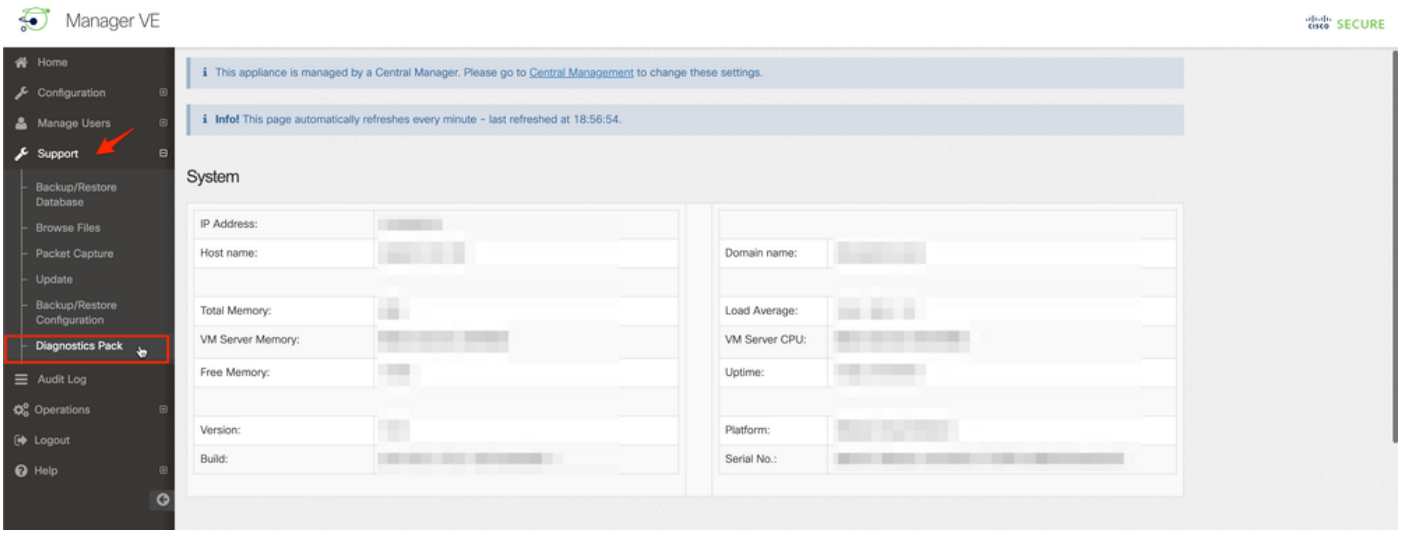
3. En los dispositivos enumerados, localice el dispositivo desde el que debe crear el paquete de diagnóstico y seleccione **Acciones (icono de puntos suspensivos) > Ver estadísticas del dispositivo**.



4. Debe ser redirigido a la interfaz de usuario del administrador del dispositivo seleccionado.

5. Inicie sesión en la interfaz de usuario de administración del dispositivo con credenciales **de administrador**.

6. En el menú de la izquierda, vaya a **Soporte > Paquete de diagnóstico**.

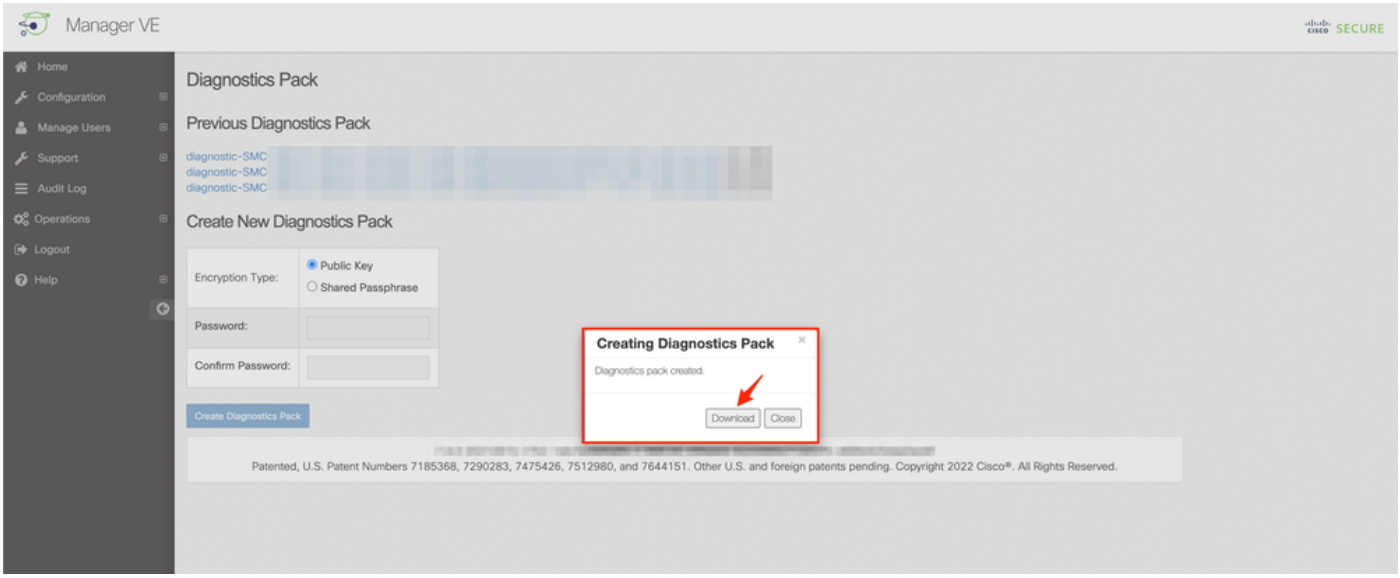


7. Una vez en la página Diagnostics Pack (Paquete de diagnóstico), debe seleccionar la encriptación **Public Key predeterminada** o proporcionar una clave compartida/frase de paso para utilizarla en el cifrado.

> **Nota:** Si decide utilizar una clave/contraseña personalizada, debe proporcionar esa frase de paso en la descripción del archivo cuando cargue el paquete de diagnóstico en el Support Case Manager.

8. Seleccione **Create Diagnostics Pack** para generar el paquete de diagnóstico del dispositivo.

9. Una vez finalizado, se le debe presentar un cuadro emergente que incluya el botón **Descargar** para descargar el paquete de diagnóstico.



Método 2. Desde la interfaz de usuario del administrador de cada dispositivo

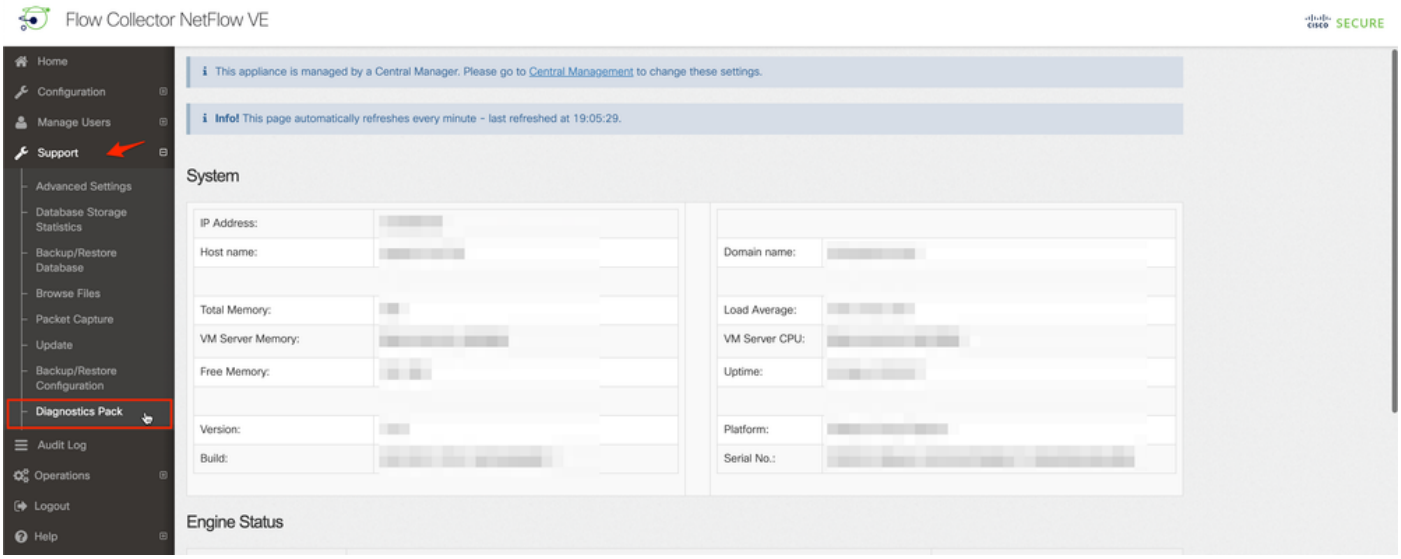
Para este método, debe tener acceso al dispositivo desde el que desea generar el paquete de diagnóstico, a través de Hypertext Transfer Protocol Secure (HTTPS).

> **Nota:** Para acceder directamente a la **interfaz de usuario del administrador**, debe utilizar la dirección URL: https://<Manager_IP_address>/smc/index.html, de lo contrario se le redirige a la interfaz de usuario web del jefe.

Por ejemplo, para generar el paquete de diagnóstico de un Flow Collector con este método, debe seguir los siguientes pasos:

1. Desde un navegador web, navegue hasta **https://<FC_IP_address>**
2. Inicie sesión en la interfaz de usuario del administrador del dispositivo con las credenciales del administrador.

3. En el menú de la izquierda, vaya a **Support > Diagnostics Pack**.

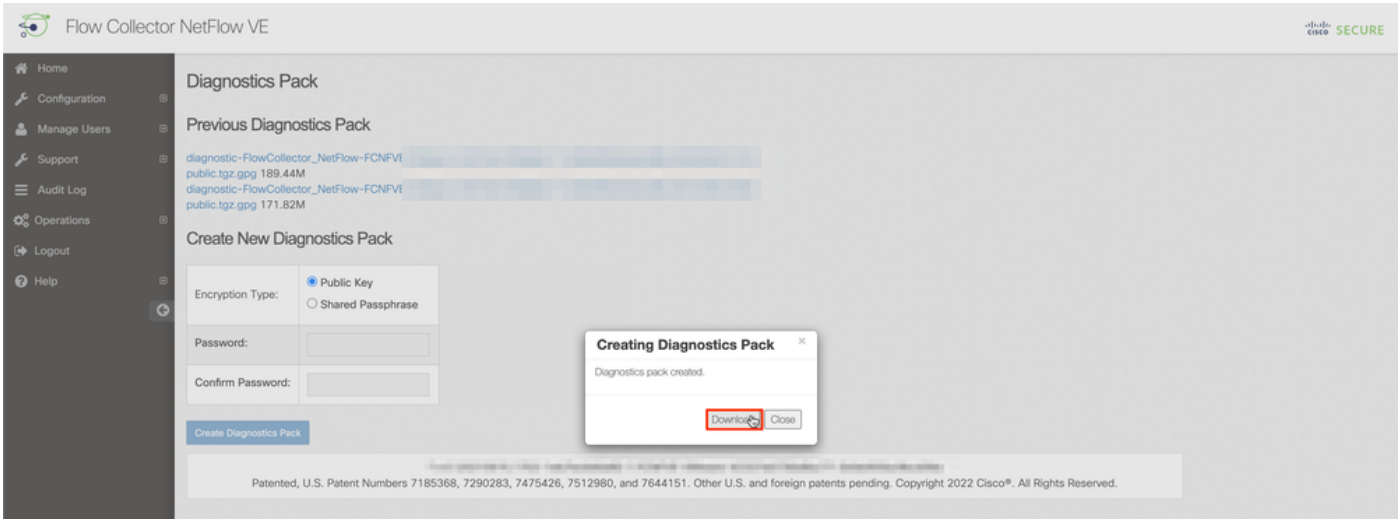


4. Una vez en la página Diagnostics Pack (Paquete de diagnóstico), debe seleccionar la encriptación **Public Key predeterminada** o proporcionar una clave compartida/frase de paso para utilizarla en el cifrado.

> **Nota:** Si decide utilizar una clave o frase de paso personalizada, debe proporcionar esa frase de paso en la descripción del archivo cuando cargue el paquete de diagnóstico en el Support Case Manager.

5. Seleccione **Create Diagnostics Pack** para generar el paquete de diagnóstico del dispositivo.

6. Una vez finalizado, se le debe presentar un cuadro emergente que incluya el botón **Descargar** para descargar el paquete de diagnóstico.



Método 3. Desde la interfaz de línea de comandos (CLI) de cada dispositivo

Hay ocasiones en las que no es posible generar el paquete de diagnóstico de un dispositivo con el uso de los métodos descritos anteriormente, sin embargo, se puede generar directamente desde la CLI del dispositivo. Los pasos para completar esta tarea son:

1. Conéctese al dispositivo SNA deseado mediante el protocolo Secure Shell (SSH) o directamente a través del acceso a la consola.

   Nota: En caso de que necesite recopilar el paquete de diagnóstico de un dispositivo de hardware sin acceso SSH, también se puede utilizar la consola de máquina virtual (KVM) basada en el núcleo de la interfaz del controlador de gestión integrada (CIMC) de Cisco.

2. Inicie sesión con las credenciales **raíz**.
3. Ingrese uno de los siguientes comandos (esto depende de la versión de SNA que está en uso):

SNA versión 7.1.x a 7.3.x

Ingrese el comando **doDiagPack**

SNA versión 7.4.x

Ingrese el comando **diagnostics start**

4. Espere a que se complete la tarea.
5. Una vez finalizada la tarea, el archivo de paquete de diagnóstico se almacena en el directorio **/lancope/var/admin/diagnostics/** con un esquema de nombre de "**diagnostic-<Device_type>-<Device_ID>.<YYYYMMDD>.<HHMM>-*.tgz.gpg**"

```
smc:/# doDiagPack
smc:/# ls -l /lancope/var/admin/diagnostics/
total 32740
-rw-r--r-- 1 root root 33522766 Feb 24 02:29 diagnostic-SMC-SMCVE-VMware-4
        -6                .20220224.0227-public.tgz.gpg
smc:/#
```

6. Copie el archivo generado del dispositivo en su equipo local o en un servidor de archivos con protocolo de copia segura (SCP) o con un cliente de protocolo de transferencia de archivos (SFTP) SSH como WinSCP. El paquete de diagnóstico se encuentra en el **/lancope/var/admin/diagnostics/** directorio.

   Nota: Cabe mencionar que SNA versión 7.4.0 introdujo una nueva función que permite que el paquete de diagnóstico se genere desde el menú SystemConfig (inicio de sesión de CLI con credenciales **root** > Introducir **SystemConfig** > Navegar a **Recuperación >** Paquete de diagnóstico**).**

   Para obtener más información sobre este método, revise la Guía de Configuración de Secure Network Analytics System 7.4.x.

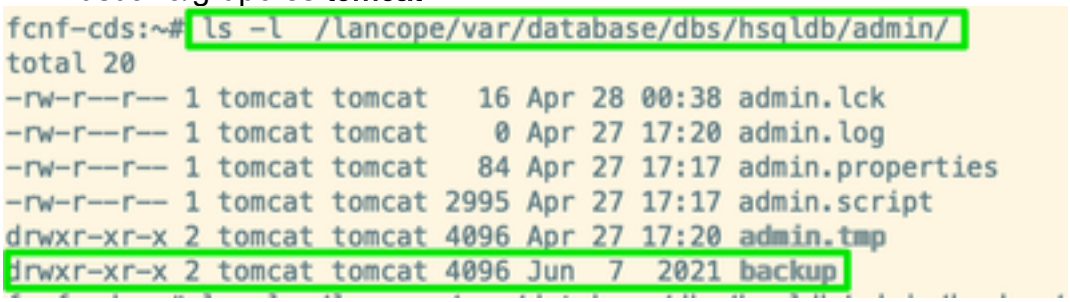
Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Hay ocasiones en las que la creación del paquete de diagnóstico falla. El síntoma más común es cuando recibe un error que dice "Se produjo un error al crear el paquete de diagnóstico. No hay archivos disponibles" después de hacer clic en el botón **Create Diagnostics Pack**.

Para corregir este comportamiento, continúe de la siguiente manera:

1. Inicie sesión en el dispositivo que tiene este comportamiento con las credenciales **raíz** a través de SSH.
2. Ejecute el comando **ls -l /lancope/var/database/dbs/hsqldb/admin/** para verificar el contenido del directorio.
3. Asegúrese de que el subdirectorio **de copia de seguridad** existe y que el propietario del usuario/grupo es **tomcat**.

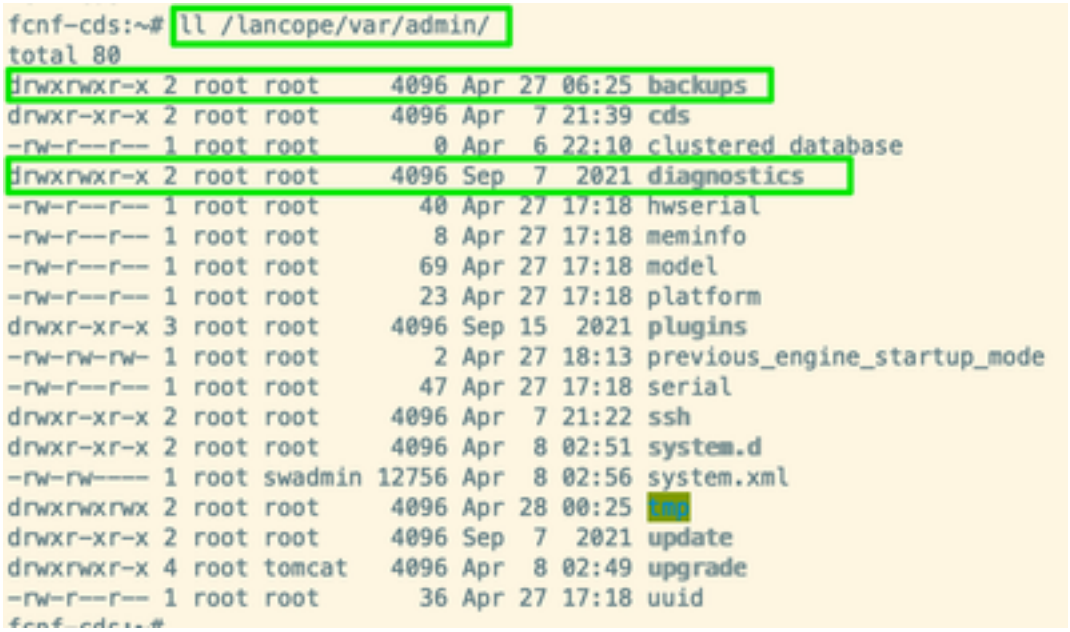


Si el subdirectorio **de respaldo** no existe en la **/lancope/var/database/dbs/hsqldb/admin/** path, se debe crear y asignar la propiedad correcta. Para esto, ejecute estos comandos:

1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
2. chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup

4. Ejecute el **comando ls -l /lancope/var/admin/** para verificar el contenido del directorio.

5. Asegúrese de que existan **copias de seguridad** y **diagnósticos** subdirectorios y de que el usuario/grupo propietario sea **root**.



Si uno o ninguno de los subdirectorios mencionados no existe en la ruta **/lancope/var/admin/**, se deben crear y asignar la propiedad correcta. Para esto, ejecute estos comandos:

1. mkdir /lancope/var/admin/backups
2. mkdir /lancope/var/admin/diagnostics

Una vez que se haya verificado, intente generar el paquete de diagnóstico del dispositivo SNA de nuevo.

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el Centro de asistencia técnica de Cisco (TAC). Se requiere un contrato de soporte válido: Contactos de soporte a nivel mundial de Cisco.
- Soporte Técnico y Documentación - Cisco Systems