Comprender el procedimiento de inicio de sesión en la CLI del sensor para Cyber Vision

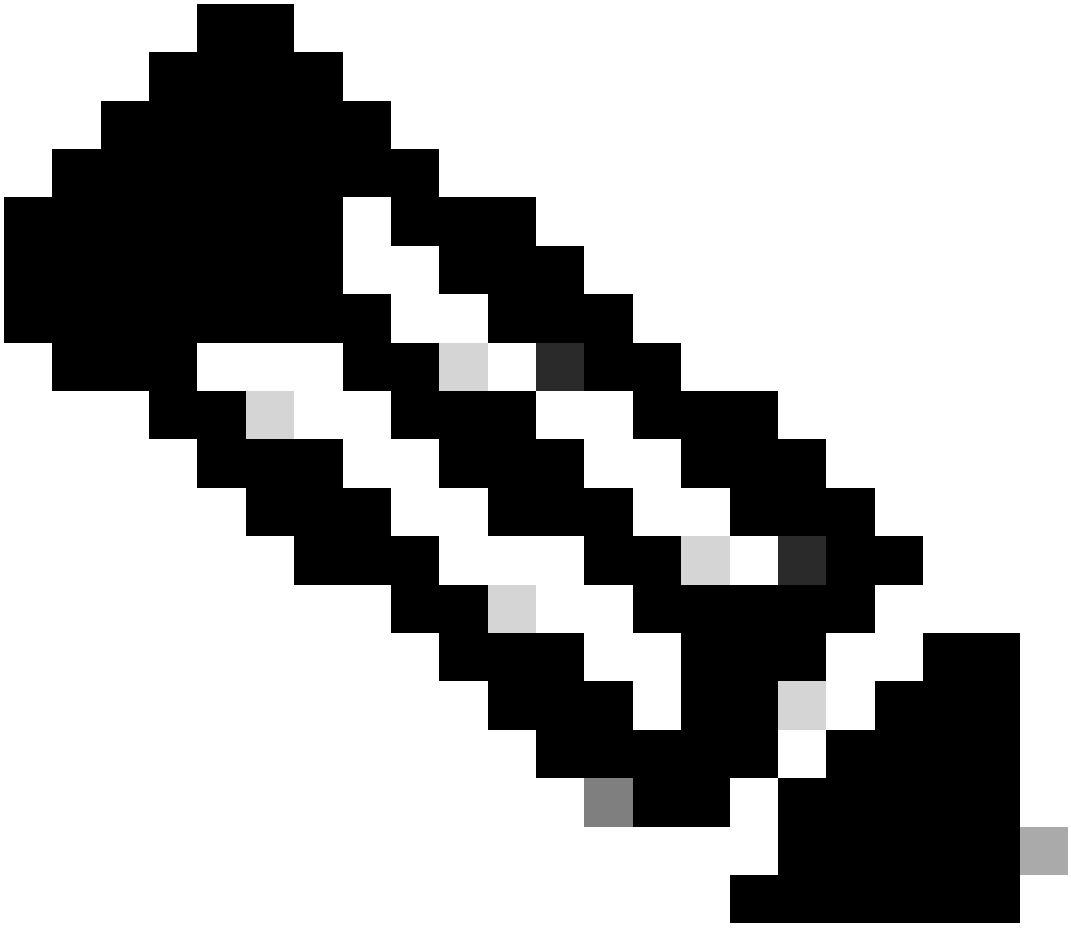
Contenido

Introducción

Este documento describe el procedimiento de inicio de sesión de la CLI del sensor para los sensores de red y hardware de Cisco Cyber Vision.

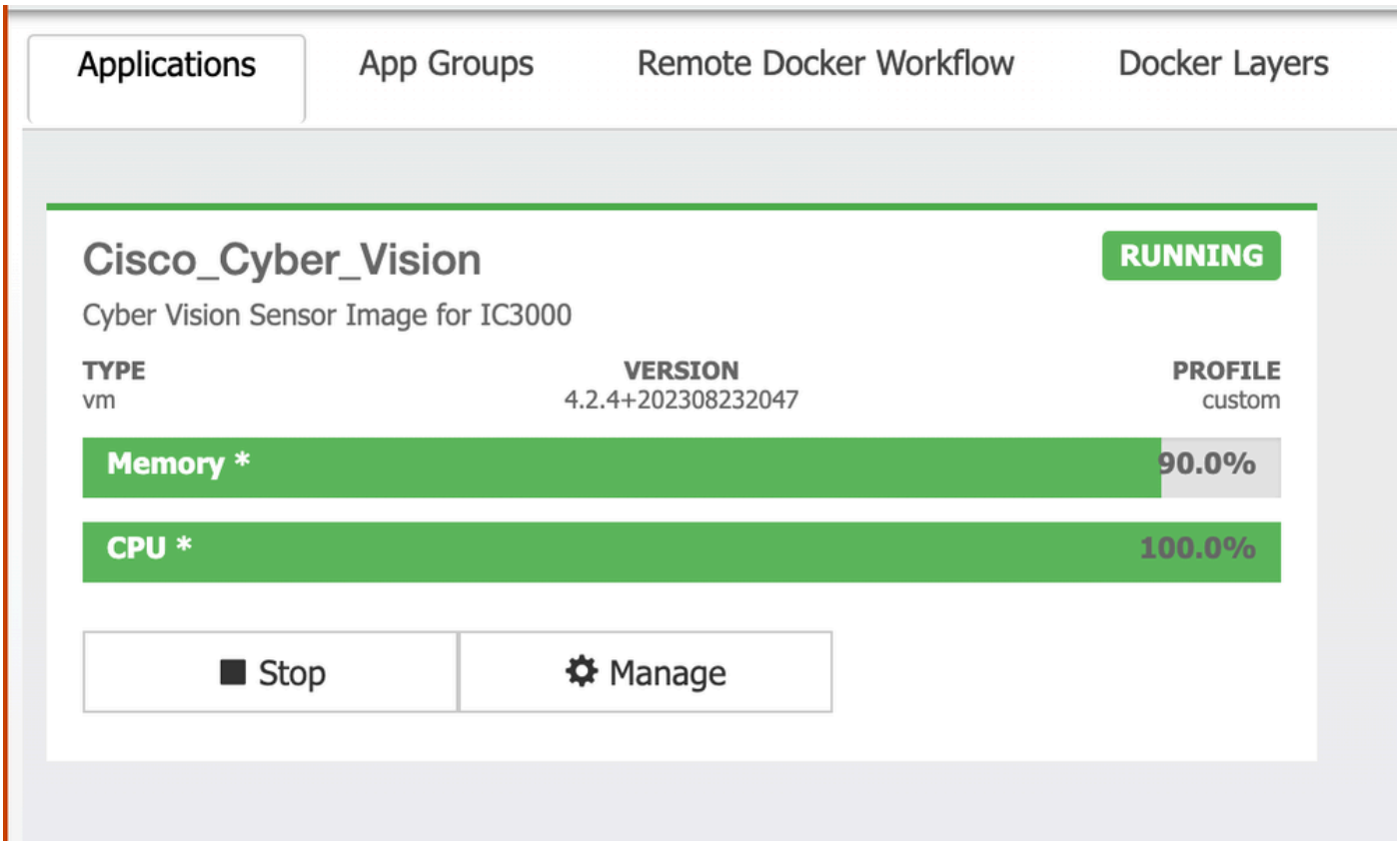
Sensor de hardware: IC3000

Antes de Cyber Vision Versión 4.3.0



Nota: antes de la versión 4.3.0 de Cyber Vision, el sensor IC3000 se implementaba como máquina virtual (VM) en el administrador local de Cisco IOSx (Cisco IOS + LinuxX), un marco de aplicaciones integral que proporciona capacidades de alojamiento de aplicaciones para diferentes tipos de aplicaciones en las plataformas de red de Cisco).

Inicie sesión en la interfaz de administrador local de IC3000 (https://ip_address:8443) como usuario administrador, navegue hasta las aplicaciones y haga clic en la opción manage app (administrar aplicación).



Elija el menú App-info, y haga clic en la opción Cisco_Cyber_Vision.pem presente en la sección App Access como se muestra:

Resources | App-Console | App-Config | App-info | App-DataDir | Logs

Application information	
ID:	Cisco_Cyber_Vision
State:	RUNNING
Name:	Cisco Cyber Vision
Cartridge Required:	• None
Version:	4.2.4+202308232047
Author:	Cisco
Author link:	
Application type:	vm
Description:	Cyber Vision Sensor Image for IC3000
Debug mode:	false

App Access	
Console Access	ssh -p {SSH_PORT} -i Cisco_Cyber_Vision.pem appconsole@10.106.13.143

Copie la clave Rivest-Shamir-Addleman (RSA) presente en el archivo Cisco_Cyber_Vision.pem. Ahora, inicie sesión en la CLI de Cyber Vision Center y cree un nuevo archivo con el contenido de la clave RSA en el archivo.

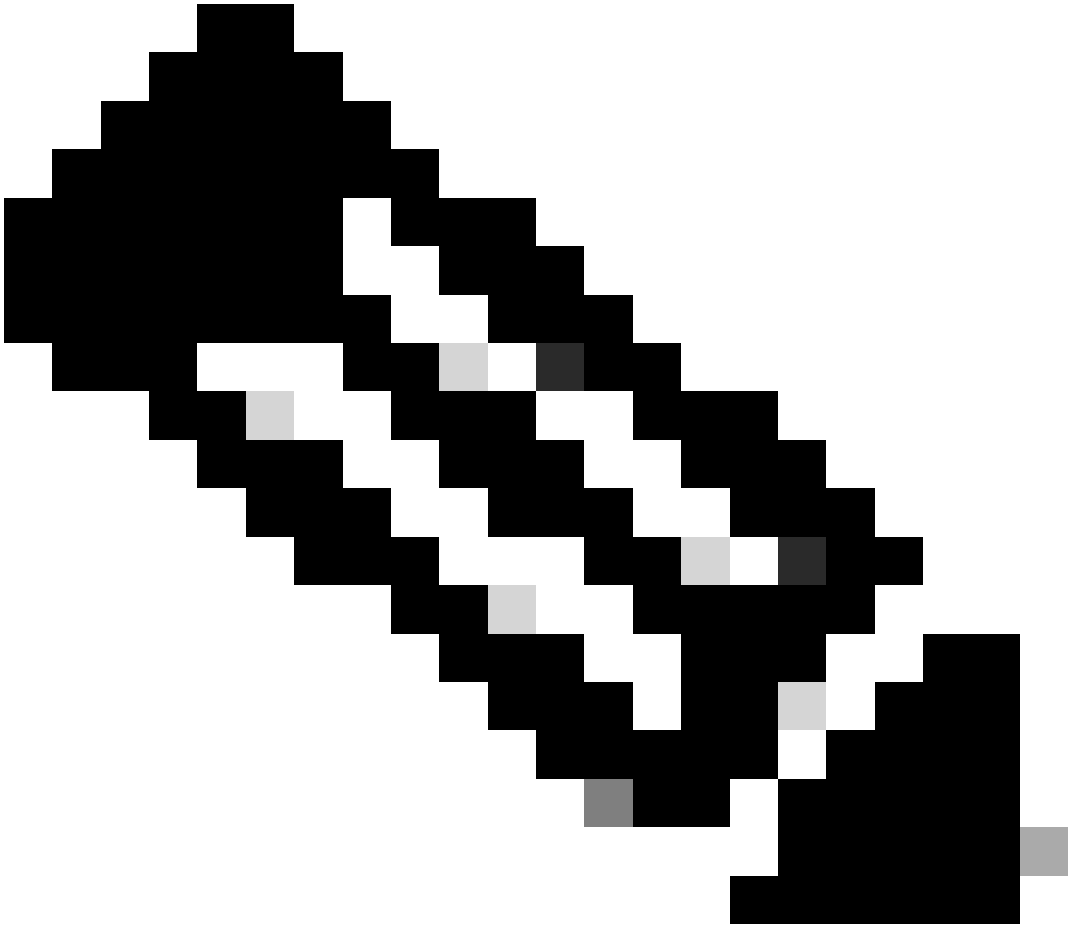
Utilizando cualquier editor de Linux, por ejemplo, vi editor (editor visual) crea un archivo y pega el contenido del archivo de clave RSA en este archivo (Cisco_Cyber_Vision.pem es el nombre de archivo en este ejemplo).

```
cv-admin@Center-4:~$
cv-admin@Center-4:~$ sudo su -
root@Center-4:~#
root@Center-4:~# vi Cisco_cyber_Vision.pem
root@Center-4:~#
root@Center-4:~# chmod 400 Cisco_cyber_Vision.pem
root@Center-4:~#
```

Restrinja los permisos al archivo Cisco_Cyber_Vision.pem, mediante el comando chmod 400. Ahora se puede acceder a la consola del sensor IC3000 mediante:

```
ssh -p {SSH_PORT} -i file_name appconsole@LocalManagerIP
```

Por ejemplo, si el puerto Secure Shell (SSH) configurado en la configuración es 22, Cisco_Cyber_Vision.pem es el nombre de archivo y la dirección IP (LMIP) del administrador local es la dirección IP de LocalManager, el resultado es ssh -p 22 -i Cisco_Cyber_Vision.pem appconsole@LMIP.

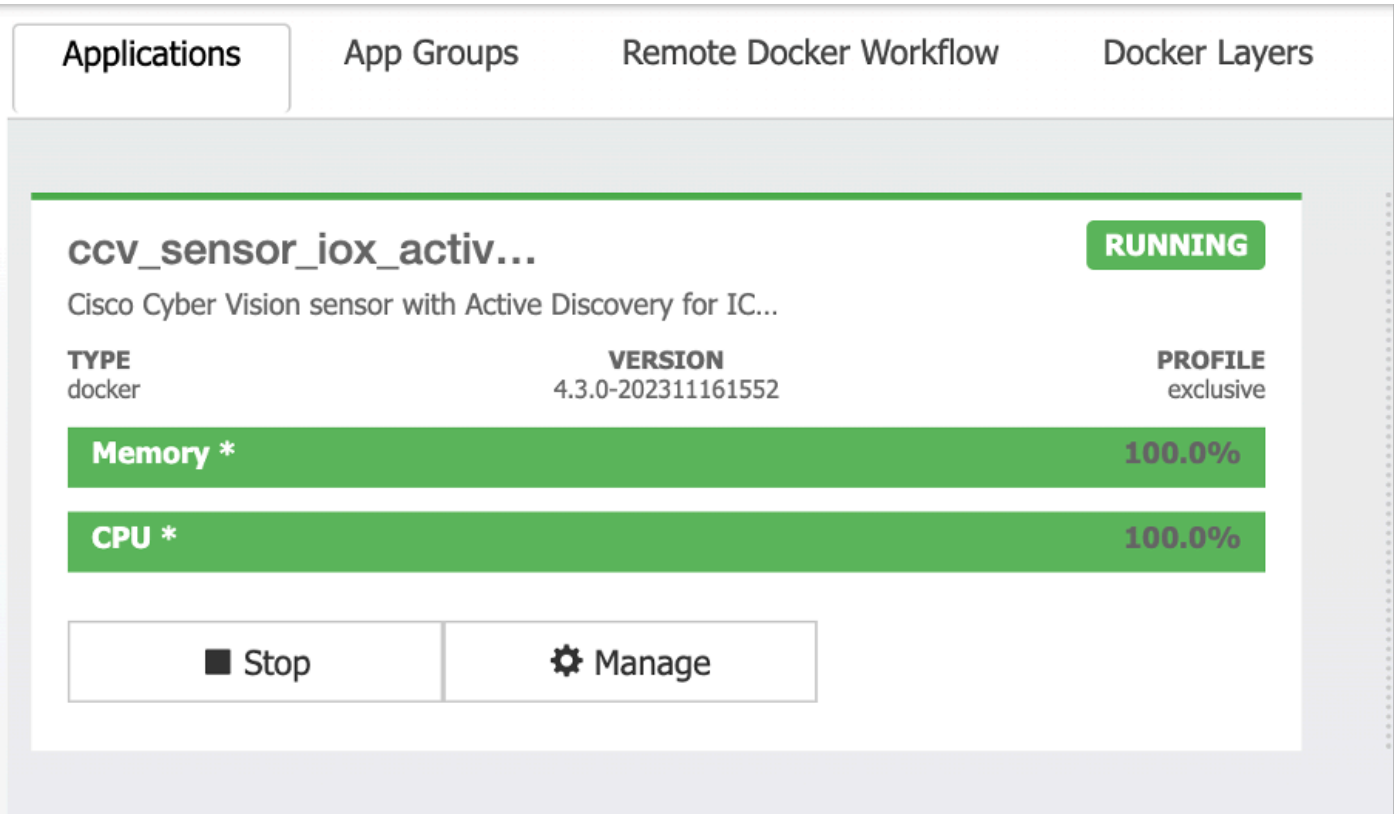


Nota: El certificado IC3000 cambia cada vez que se reinicia el switch y, por lo tanto, es necesario repetir este procedimiento.

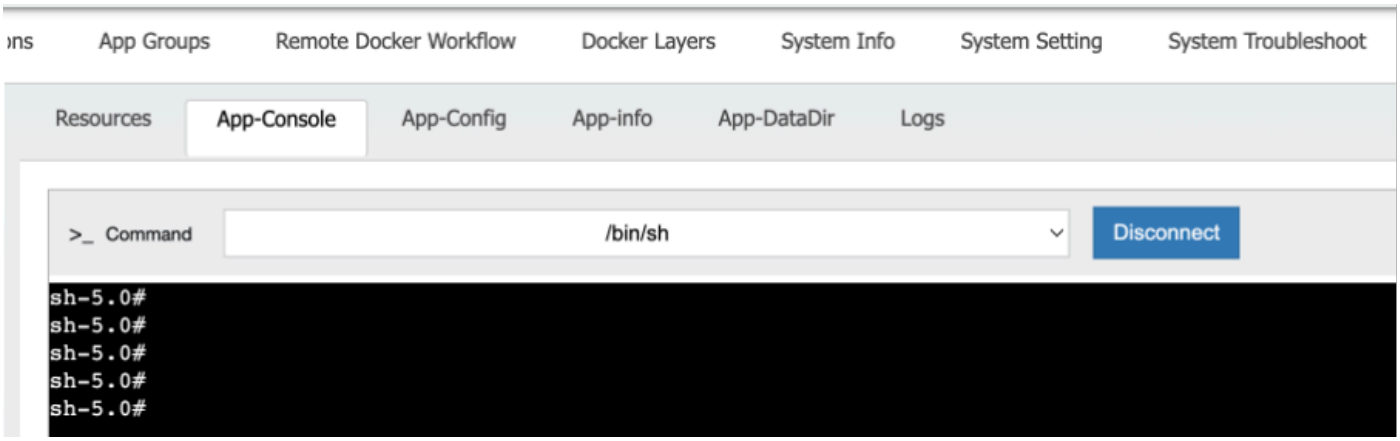
Cyber Vision versión 4.3.0 en adelante

La aplicación del sensor Cisco Cyber Vision para el formato IC3000 cambió de VM a Docker en la versión 4.3.0. Para obtener más detalles sobre lo mismo, consulte Cisco-Cyber-Vision_Release-Notes-4-3-0.pdf.

Inicie sesión en la interfaz de administrador local de IC3000 (https://ip_address:8443) como usuario administrador, navegue hasta las aplicaciones y haga clic en la opción **manage** app (**administrar** aplicación).



A continuación, vaya a la ficha App-Console para acceder a la aplicación del sensor.



Sensores de red

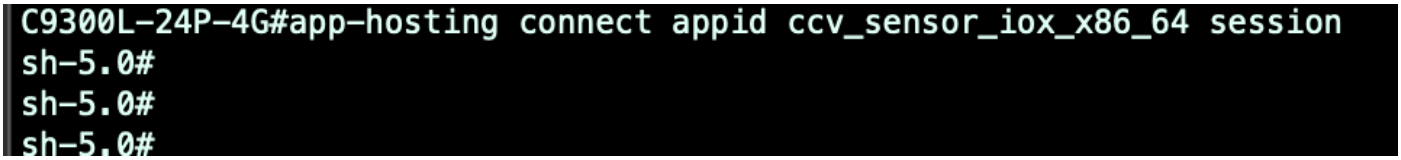
Inicie sesión en la CLI del switch correspondiente y copie el ID de aplicación del sensor mediante este comando:

show app-hosting list

Inicie sesión en la aplicación de sensor mediante:

app-hosting connect appid sensor_app_name session

Por ejemplo, en este caso, es **app-hosting connect appid ccv_sensor_iox_x86_64 session**.



El mensaje que aparece en la captura de pantalla confirma que el inicio de sesión del sensor se ha realizado correctamente.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).