

Comprendre la procédure de connexion à l'interface de ligne de commande du capteur pour Cyber Vision

Table des matières

[Introduction](#)

[Capteur matériel - IC3000](#)

[Avant Cyber Vision Version 4.3.0](#)

[Cyber Vision 4.3.0 version ultérieure](#)

[Capteurs réseau](#)

Introduction

Ce document décrit la procédure de connexion à l'interface de ligne de commande du capteur pour les capteurs réseau et matériels de Cisco Cyber Vision.

Capteur matériel - IC3000

Avant Cyber Vision Version 4.3.0



Remarque : avant la version 4.3.0 de Cyber Vision, le capteur IC3000 était déployé en tant que machine virtuelle (VM) dans le gestionnaire local Cisco IOx (Cisco IOs + linuX) est une structure d'applications de bout en bout qui fournit des fonctionnalités d'hébergement d'applications pour différents types d'applications sur les plates-formes réseau Cisco).

Connectez-vous à l'interface du gestionnaire local IC3000 (https://ip_address:8443) en tant qu'utilisateur admin, accédez aux applications, puis cliquez sur l'option manage app.

Applications

App Groups

Remote Docker Workflow

Docker Layers

Cisco_Cyber_Vision

RUNNING

Cyber Vision Sensor Image for IC3000

TYPE
vm

VERSION
4.2.4+202308232047

PROFILE
custom

Memory *

90.0%

CPU *

100.0%

■ Stop

⚙ Manage

Choisissez le menu App-info, et cliquez sur l'option Cisco_Cyber_Vision.pem présente dans la section App Access comme indiqué :

Application information	
ID:	Cisco_Cyber_Vision
State:	RUNNING
Name:	Cisco Cyber Vision
Cartridge Required:	<ul style="list-style-type: none">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

Copiez la clé RSA (Rivest-Shamir-Addleman) présente dans le fichier `Cisco_Cyber_Vision.pem`. Désormais, connectez-vous à l'interface de ligne de commande de Cyber Vision Center, puis créez un nouveau fichier contenant la clé RSA.

À l'aide d'un éditeur Linux, par exemple, vi editor (éditeur visuel) crée un fichier et colle le contenu du fichier de clé RSA dans ce fichier (`Cisco_Cyber_Vision.pem` est le nom de fichier dans cet exemple).

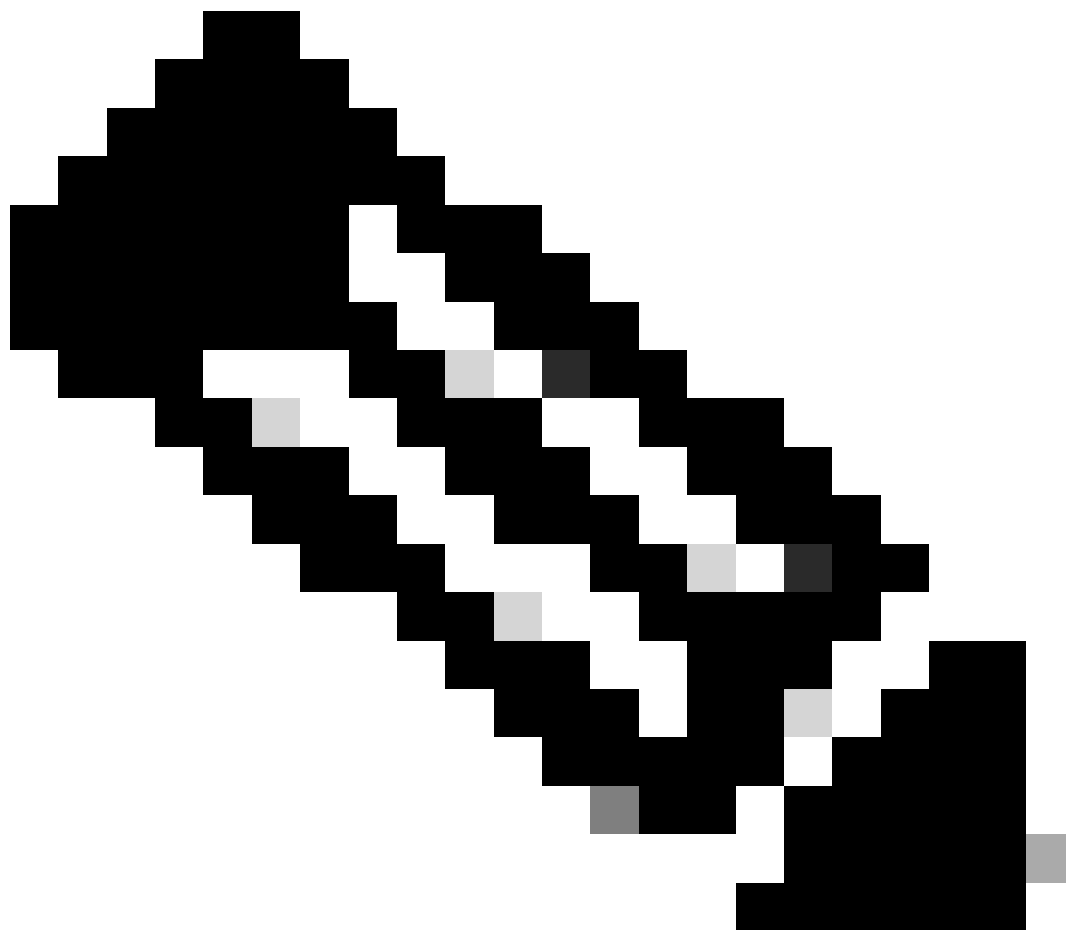
```
cv-admin@Center-4:~$
cv-admin@Center-4:~$ sudo su -
root@Center-4:~#
root@Center-4:~# vi Cisco_cyber_Vision.pem
root@Center-4:~#
root@Center-4:~# chmod 400 Cisco_cyber_Vision.pem
root@Center-4:~#
```

Restreignez les autorisations au fichier Cisco_Cyber_Vision.pem, en utilisant la commande chmod 400.

La console du capteur IC3000 est désormais accessible à l'aide des éléments suivants :

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

Par exemple, si le port Secure Shell (SSH) configuré dans la configuration est 22, Cisco_Cyber_Vision.pem est le nom de fichier et l'adresse IP du gestionnaire local (LMIP) est l'adresse IP de LocalManager, alors le résultat est `ssh -p 22 -i Cisco_Cyber_Vision.pem appconsole@LMIP`.



Remarque : le certificat IC3000 change à chaque redémarrage du commutateur et cette procédure doit donc être répétée.

Cyber Vision 4.3.0 version ultérieure

L'application de capteur Cisco Cyber Vision pour le format IC3000 est passée de VM à Docker dans la version 4.3.0. Pour plus d'informations à ce sujet, reportez-vous à [Cisco-Cyber-Vision Release-Notes-4-3-0.pdf](#).

Connectez-vous à l'interface du gestionnaire local IC3000 (https://ip_address:8443) en tant qu'utilisateur admin, accédez aux applications, puis cliquez sur l'option **manage** app.

Applications App Groups Remote Docker Workflow Docker Layers

ccv_sensor_iox_activ... **RUNNING**

CISCO Cyber Vision sensor with Active Discovery for IC...

TYPE	VERSION	PROFILE
docker	4.3.0-202311161552	exclusive

Memory * **100.0%**

CPU * **100.0%**

Accédez ensuite à l'onglet App-Console afin d'accéder à l'application du capteur.

ns App Groups Remote Docker Workflow Docker Layers System Info System Setting System Troubleshoot

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

>_ Command

```
sh-5.0#  
sh-5.0#  
sh-5.0#  
sh-5.0#  
sh-5.0#
```

Capteurs réseau

Connectez-vous à l'interface de ligne de commande du commutateur concerné et copiez l'ID d'application du capteur à l'aide de cette commande :

show app-hosting list

```
C9300L-24P-4G#sh app-hosting list
App id                               State
-----
ccv_sensor_iox_x86_64                RUNNING
```

Connectez-vous à l'application du capteur en utilisant :

app-hosting connect appid sensor_app_name session

Par exemple, dans ce cas, il est **app-hosting connect appid ccv_sensor_iox_x86_64 session**.

```
C9300L-24P-4G#app-hosting connect appid ccv_sensor_iox_x86_64 session
sh-5.0#
sh-5.0#
sh-5.0#
```

L'invite affichée dans la capture d'écran confirme que la connexion du capteur a réussi.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.