

Cyber VisionのセンサーCLIログイン手順について

内容

[はじめに](#)

[ハードウェアセンサー – IC3000](#)

[Cyber Visionバージョン4.3.0以前](#)

[Cyber Vision 4.3.0/バージョン](#)

[ネットワークセンサー](#)

はじめに

このドキュメントでは、Cisco Cyber Visionのネットワークセンサーとハードウェアセンサーの両方のセンサーCLIログイン手順について説明します。

ハードウェアセンサー – IC3000

Cyber Visionバージョン4.3.0以前



注：Cyber Visionバージョン4.3.0より前では、IC3000センサーは仮想マシン(VM)としてCisco IOxに導入されていました((Cisco IOs + linuX)は、シスコネットワークプラットフォームのさまざまなアプリケーションタイプにアプリケーションホスティング機能を提供するエンドツーエンドのアプリケーションフレームワークです)。ローカルマネージャ。

IC3000ローカルマネージャインターフェイス(https://ip_address:8443)に管理ユーザとしてログインし、アプリケーションに移動して、[manage](#) appオプションをクリックします。

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

App-infoメニューを選択し、次に示すようにApp Accessセクションにある Cisco_Cyber_Vision.pem オプションをクリックします。

| 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 | <code>ssh -p {SSH_PORT} -i Cisco_Cyber_Vision.pem appconsole@10.106.13.143</code> |

Cisco_Cyber_Vision.pemファイルにあるRivest-Shamir-Addleman(RSA)キーをコピーします。次に、Cyber Vision Center CLIにログインし、ファイル内にRSAキーの内容を含む新しいファイルを作成します。

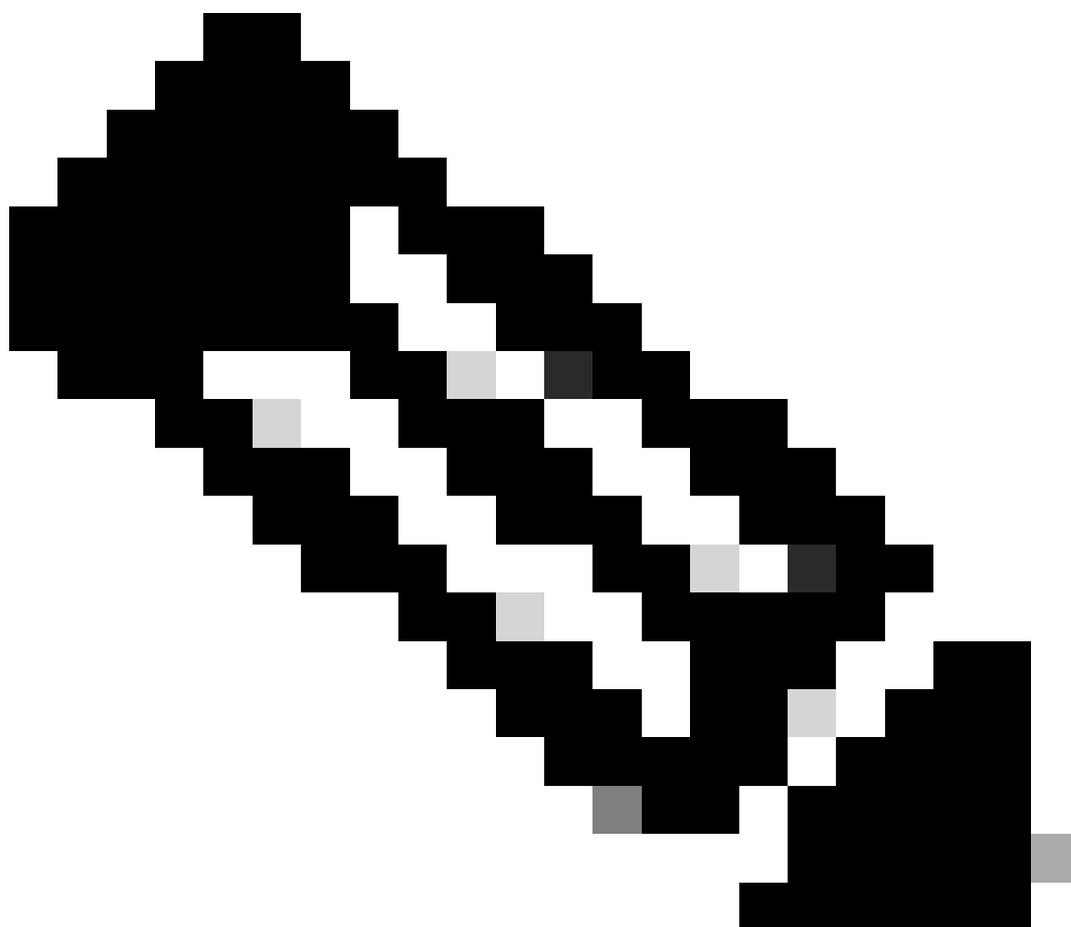
任意のLinuxエディタ、たとえばviエディタ(ビジュアルエディタ)を使用してファイルを作成し、RSAキーファイルの内容をこのファイルにペーストします(この例では、Cisco_Cyber_Vision.pemがファイル名です)。

```
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:~#
```

chmod 400コマンドを使用して、ファイルCisco_Cyber_Vision.pemへの権限を制限します。
これで、IC3000センサーコンソールに次の方法でアクセスできるようになりました。

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

たとえば、セットアップで設定されたセキュアシェル(SSH)ポートが22、
Cisco_Cyber_Vision.pemがファイル名、Local Manager IP address(LMIP)がLocalManagerのIPア
ドレスの場合、結果はssh -p 22 -i Cisco_Cyber_Vision.pem appconsole@LMIPになります。



注:IC3000証明書はスイッチがリブートされるたびに変更されるため、この手順を繰り返す必要があります。

Cyber Vision 4.3.0バージョン

IC3000形式のCisco Cyber Visionセンサーアプリケーションは、バージョン4.3.0でVMからDockerに変更されました。これに関する詳細は、[Cisco-Cyber-Vision Release-Notes-4-3-0.pdf](#)を参照してください。

IC3000ローカルマネージャインターフェイス(https://ip_address:8443)に管理ユーザとしてログインし、アプリケーションに移動して、[manage](#) appオプションをクリックします。

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%

■ Stop ⚙ Manage

次に、App-Consoleタブに移動して、センサーアプリケーションにアクセスします。

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 /bin/sh Disconnect

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

ネットワークセンサー

各スイッチのCLIにログインし、次のコマンドを使用してセンサーアプリケーションIDをコピーします。

```
show app-hosting list
```

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

次を使用してセンサーアプリケーションにログインします。

```
app-hosting connect appid sensor_app_name session
```

たとえば、この場合は `app-hosting connect appid ccv_sensor_iox_x86_64 session` です。

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

画面キャプチャに示されているプロンプトは、センサーのログインが成功したことを示しています。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。