Dépannage de l'intégration ISE

Table des matières

Introduction

Ce document décrit les étapes de dépannage pour l'intégration de CyberVision Center à ISE.

Présentation des meilleures pratiques

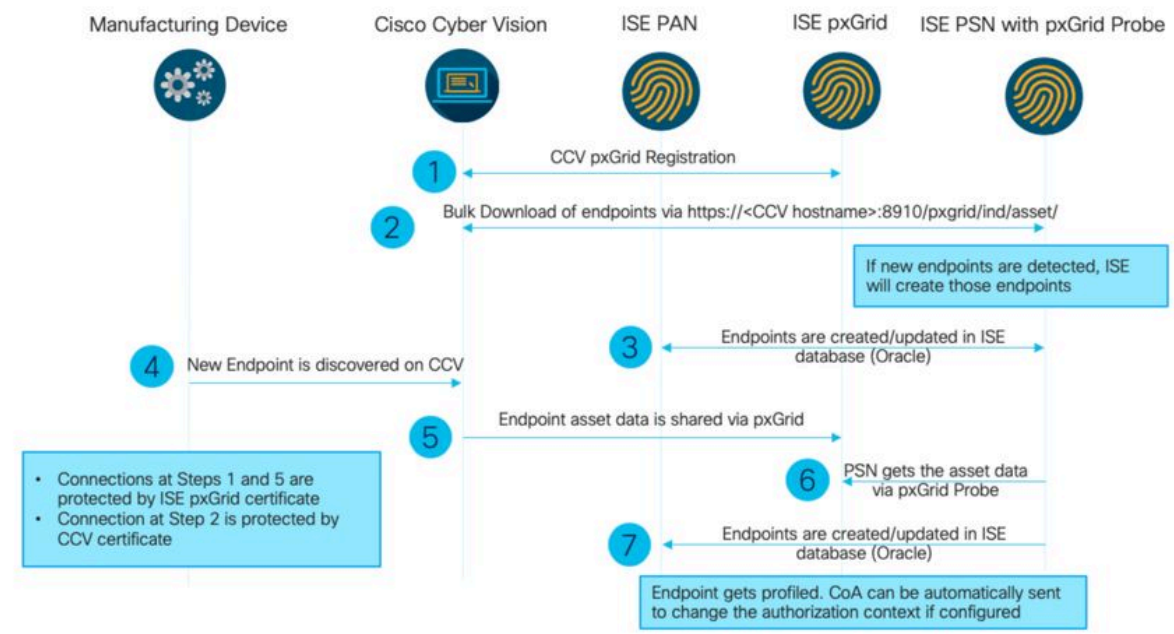
Les Méthodes Recommandées sont les étapes à prendre en compte pour garantir le bon fonctionnement de la configuration du système. Recommandations:

- Reportez-vous aux notes de version de Cisco Cyber Vision et à celles de Cisco Identity Services Engine (ISE) pour connaître les dernières fonctionnalités, directives, limites et mises en garde
- Vérifier et dépanner toute nouvelle modification de configuration après l'avoir implémentée

Diagramme de flux de haut niveau CCV-ISE

Configure

High-Level Flow Diagram



Instructions de dépannage

En répondant aux questions à venir, vous pouvez déterminer le chemin de dépannage et les composants qui nécessitent un examen plus approfondi. Répondez aux questions suivantes afin de déterminer l'état de votre installation :

- S'agit-il d'un système nouvellement installé ou d'une installation existante ?
- La solution CyberVision a-t-elle déjà été en mesure de voir l'ISE ?

Vérifiez l'état des services pxGrid à l'aide de la commande systemctl status pxgrid-agent.

```
root@center:~# systemctl status pxgrid-agent
● pxgrid-agent.service - Agent for interfacing with pxGrid
   Loaded: loaded (/lib/systemd/system/pxgrid-agent.service; enabled)
   Active: active (running) since Wed 2021-03-17 20:12:15 UTC; 17min ago
  Process: 28434 ExecStop=/usr/bin/lxc-stop -n pxgrid-agent (code=exited, status=0/SUCCESS)
 Main PID: 28447 (lxc-start)
   CGroup: /system.slice/pxgrid-agent.service
           └─28447 /usr/bin/lxc-start -F -n pxgrid-agent

Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: create_path_for_hierarchy: 1306 Path "/sys/fs/cgroup/pids//lxc/pxgrid-agent-6" already existed.
Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: cgfsng_create: 1363 File exists - Failed to create /sys/fs/cgroup/pids//lxc/pxgrid-agent-6: File exists
Mar 17 20:12:15 center lxc-start[28447]: pxgrid-agent Center type: standalone [caller=postgres.go:290]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [caller=main.go:135]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.sock' [caller=main.go:102]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Account activated [caller=pxgrid.go:81]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Service registered, ID: 3d7bee0f-3840-4dc7-a121-a8740f86fa06 [caller=pxgrid.go:99]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent Cyber Vision is in sync with ISE [caller=assets.go:67]
Mar 17 20:23:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
```

- ISE exécute-t-il pxGrid en haute disponibilité ?

- Qu'est-ce qui a changé dans la configuration ou dans l'infrastructure globale juste avant que les applications ne commencent à avoir des problèmes ?

Afin de détecter un problème réseau, suivez les étapes générales de dépannage réseau :

Étape 1. Pouvez-vous envoyer une requête ping à CyberVision Center Hostname depuis ISE ?

```
ESCISE2/admin# ping center
PING center (10.2.3.138) 56(84) bytes of data.
64 bytes from 10.2.3.138: icmp_seq=1 ttl=64 time=1.53 ms
64 bytes from 10.2.3.138: icmp_seq=2 ttl=64 time=1.73 ms
64 bytes from 10.2.3.138: icmp_seq=3 ttl=64 time=1.87 ms
64 bytes from 10.2.3.138: icmp_seq=4 ttl=64 time=1.80 ms

--- center ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.539/1.737/1.878/0.125 ms
```

Si vous ne parvenez pas à envoyer une requête ping, connectez-vous à ISE CLI à l'aide de Secure Shell (SSH) et Add hostname.

```
ESCISE2/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ESCISE2/admin(config)# ip host 10.2.3.138 center
Add Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
```

Étape 2. Pouvez-vous envoyer une requête ping à ISE Hostname depuis CyberVision Center ?

```
root@center:~# ping ESCISE2.ccv.local
PING ESCISE2.ccv.local (10.2.3.118) 56(84) bytes of data.
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=1 ttl=64 time=2.04 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=2 ttl=64 time=1.88 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=3 ttl=64 time=1.75 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=4 ttl=64 time=1.98 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=5 ttl=64 time=2.02 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=6 ttl=64 time=1.97 ms
^C
--- ESCISE2.ccv.local ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.754/1.945/2.045/0.109 ms
```

Si ce n'est pas le cas, essayez d'ajouter le nom d'hôte ISE dans le/data/etc/hosts fichier de Center.

```
root@Center:~# cat /data/etc/hosts
127.0.0.1       localhost.localdomain           localhost

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.1.1 center
10.48.60.131 ise31-tm2.cisco.com
```

Étape 3. Détecter les problèmes de certificat.

Entrez la commande openssl s_client -connect YourISEHostname:8910 à partir de CyberVision Center.

```
root@center:~# openssl s_client -connect ESCISE2.ccv.local:8910
CONNECTED(00000003)
depth=3 CN = Certificate Services Root CA - ESCISE2
verify error:num=19:self signed certificate in certificate chain
verify return:1
depth=3 CN = Certificate Services Root CA - ESCISE2
verify return:1
depth=2 CN = Certificate Services Node CA - ESCISE2
verify return:1
depth=1 CN = Certificate Services Endpoint Sub CA - ESCISE2
verify return:1
depth=0 OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local
verify return:1
---
Certificate chain
 0 s:OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local
   i:CN = Certificate Services Endpoint Sub CA - ESCISE2
 1 s:CN = Certificate Services Endpoint Sub CA - ESCISE2
   i:CN = Certificate Services Node CA - ESCISE2
 2 s:CN = Certificate Services Node CA - ESCISE2
   i:CN = Certificate Services Root CA - ESCISE2
 3 s:CN = Certificate Services Root CA - ESCISE2
   i:CN = Certificate Services Root CA - ESCISE2
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIF3jCCA8agAwIBAgIQUKVBBihpQhWBK5cZEjFpeDANBgkqhkiG9w0BAQsFADA5
MTcwNQYDVQQDDC5DZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBFbmRwb2ludCBTdWIgQ0Eg
LSBFU0NJU0UyMB4XDTIwMTEyOTE3Mjc1M1oXDTI1MTEzMDE3Mjc1M1owTjEwMC4G
A1UECwwnQ2VydGlmaWNhdGUgU2VydmljZXMgU3lzdGVtIEN1cnRpZmljYXRlMRow
GAYDVQQDDBFFU0NJU0UyLmNjdi5sb2NhbDCCAiIwDQYJKoZIhvcNAQEBBQADggIP
ADCCAgoCggIBANE1Ukx/7QnUdrCIXJLUxg0XWTvOFTNme4L16yDFsLvytGjFqYfR
RCRM/kzRVjDk8f/cSSP9T+5pR/JA+PbOZqkAWWDJVaQh1ndqL0kX7UaCCodKUWon
DafVimPjKqV1RSCd8bwVDxAr7gYou3S4BcCe0Os1x5pL1WyZw6F6MPze2F388kSR
GuSRsn40ZM4JjDDeaxSBrs789f7zACw4eMZIfRDk0RL9qzMtoghIU089/1VuacUb
WYrF0e0mThUWg7wk7dFv4bozyWeHjdqsbEtb0Geme8ZWPX5ZYddSKjWhOrNUXeQV
NvDBUXhb5NpSsKYMoCqnvIv+JYzkIV6ukksX9xqI5bL3/vik/CyPVMeXIOJo64dK
S0vMjrcnmpNznoLzEv3mgvgp9mJhcTROg86w1yOrOzjOoMCGGLrhpgxuLeVatFKv
GLWjsmrWcLk/F0Ae4H+tb6/+yO7KNXTSX+nP1z5epDA8stzvLxm1ylw65XdeEBho
m0qgGEKr5y/I/2b+myi24ZYrqsv64KPohCisIvZxbCG/2q77SP7ml8v8+BidpMaW
LZrZ0tD2XRJeyhPyprBYwV4QDBWPn+mCAFgpNd3KC36zAn138c2WWlHs0PKhReMX
vNn+SwltKmyIbM09Oeww5zRSdMU90zPcFkY0qvrBUD31Gf5fAiWqlmkVAgMBAAGj
gcwwgckwaAYDVR0jBGEwX4AUxz+SV+KtR/CpwGiyNg+mp/xxiAqhNaQzMDExLzAt
BgNVBAMMJkNlcnRpZmljYXRlIFNlcnZpY2VzIE5vZGUgQ0EgLSBFU0NJU0UyghAx
lcB30YJL0Kwj6XolaV7SMB0GA1UdDgQWBBRigvgT63FOqKmS9m9COhW3ahdv8jAO
BgNVHQ8BAf8EBAMCBeAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggIBADwnDKtdHj/y3Pj4ADDV
57RrdHsiU/EkkWGLzmP/aMKJ9rY7f6eUDlig6b6gpJ8B0MnTPi9VFVduc++oZDEt
CrIMMwFexnnbhPWJfzjSNJPnAMIgFUeiPuoxBJYkjFzhiXtat0fOmdm5RbEu5W1a
f7EEBd/XOiRTMyIxqubXQCt6pE61y9gBPuQU9Hvd5QpcLX77LSfEroJhkD4dmuRs
o4uj0wWKFtXW+yLWhwjkiieoBuREEU8Gvtk+iq+11mThfpeP32fV2IO/WIo4SKh0
ILkzSZ06rbSzxxatKDQ6jZDs3a5YKyFtR55r7VndmX0I4sqXI9dFQjTPVfW7TEbK
GPds+vMe4J9g4c1KGRhiXNiNzfB5S3eWzOL/2o9ZgWS1u7R7GVXKlYrvSHMieL3t
n/p+ov8cogr0Oo6jXFItZ+Rsnp11Kbq+DrsoCE/i26QgkTKBruMFhz6P8k/2aLqQ
MwJp0dhH1SFmkWCAQbGQpapoX3lpK36FUta3sZL2mdN/XyK5UutLbLJx87elwunp
w6Cxz5MA97NXOUZIuqThnTG7Ibu8pzwl1XZYt1flT50luCoY2CkVbU93rqfD4zyr
WyK2a0BmizcKXD+F8Yti4fm4Kvl0bpWihUNPPMTmgwJMUOW+zdC7b7gl3j5rnE9X
lyFJ3uHTohidxEtXi4XsiCn5
-----END CERTIFICATE-----
subject=OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local
```

Données à collecter

Pour les problèmes réseau :

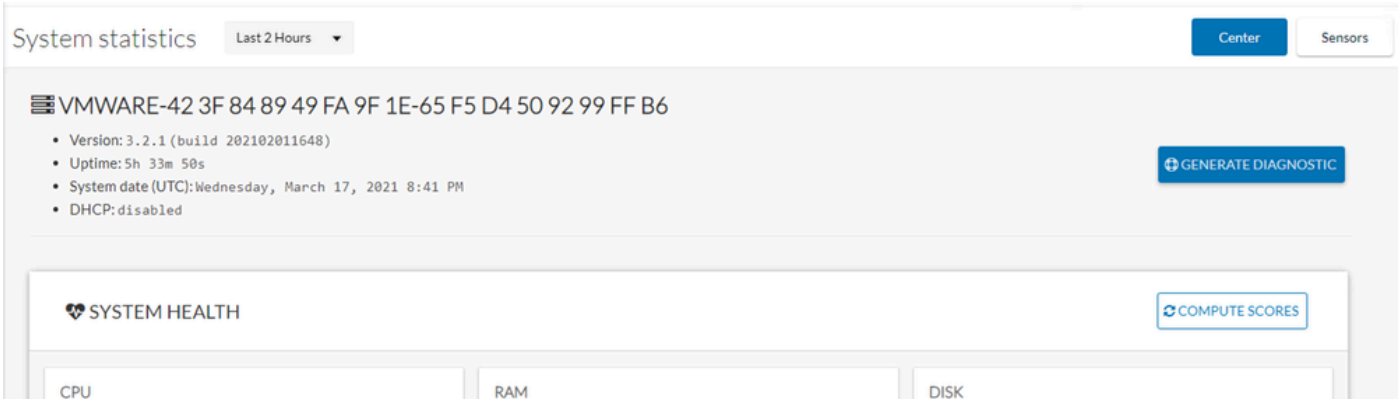
- Architecture:

Un schéma montrant ces détails entre le centre et ISE est utile :

- Règles de pare-feu
- Routes statique
- Configuration de la passerelle
- Configurations VLAN

- Journaux à collecter pour tous les problèmes ISE :

Vous pouvez commencer par collecter un fichier de diagnostic du Centre afin d'éviter de perdre des données.



Activez ensuite les journaux avancés sur le centre à l'aide de la procédure suivante :

Créez deux fichiers dans le dossier /data/etc/sbs.

Le premier fichier doit être nommé listener.conf et contenir le contenu suivant :

(Notez l'espace d'en-tête devant le niveau de journalisation.)

```
root@Center:~# cat /data/etc/sbs/listener.conf
configlog:
 loglevel: debug
root@Center:~#
```

Le deuxième fichier doit être nommé pxgrid-agent.conf et contenir le contenu suivant :

(Notez l'espace d'en-tête devant le niveau de journalisation.)

```
root@Center:~# cat /data/etc/sbs/pxgrid-agent.conf
configlog:
 loglevel: debug
```

Une fois les deux fichiers créés, redémarrez le Centre ou redémarrez les services sbs-burrow etpxgrid-agent.

Restart service using the command:
#systemctl restart sbs-burrow
#systemctl restart pxgrid-agent

Ensuite, collectez les journaux pxGrid (utilisez les outils de transfert de fichiers afin d'exporter les journaux à partir du Centre).

```
root@Center:~# journalctl -u pxgrid-agent > /data/tmp/pxgridLogs.log
```

Collecter des captures tcpdump pour analyser le flux de communication entre le Centre et ISE.

```
root@Center:~# tcpdump -i eth0 -n host CCV_IP and host ISE_IP -w /data/tmp/ccv_ise.pcap
```

- Activez les débogages sur ISE et collectez le bundle de support.

Pour activer les débogages sur ISE, accédez à Administration > System > Logging > Debug Log Configuration. Définissez les niveaux de journalisation suivants :

Persona	Nom du composant	Niveau de consignation	Fichier à vérifier	
PAN (facultatif)	profileur	DÉBOGUER	profiler.log	
PSN avec sonde pxGrid activée	profileur	DÉBOGUER	profiler.log	

PxGrid	grille pxgrid	TRACE	pxgrid-server.log	

Messages de journal attendus

Les journaux de débogage de l'agent pxGrid du centre indiquent l'agent en cours de démarrage, le service enregistré, la connexion STOMP (Simple Text Oriented Messaging Protocol) de Cisco Cyber Vision (CCV) avec ISE et l'envoi d'une opération de mise à jour pour un actif/composant :

<#root>

Jul 11 13:05:02 center systemd[1]:

Started Agent

 for interfacing with pxGrid.
Jul 11 13:05:02 center pxgrid-agent[5404]: pxgrid-agent Center type: standalone [caller=postgres.go:543
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.soc
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccountActivate bo
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent

Account activated

 [caller=pxgrid.go:58]
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceRegister bo

"assetTopic":"/topic/com.cisco.endpoint.asset"

,"restBaseUrl":"https://Center:8910/
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent

Service registered

, ID: c514c790-2361-47b5-976d-4a1b5ccfa8b7 [caller=pxgrid.go:76]
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceLookup body
Jul 11 13:05:05 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccessSecret body=
Jul 11 13:05:06 center pxgrid-agent[5404]: pxgrid-agent

Websocket connect url

=wss://labise. aaalab .com:

8910

/pxgrid/ise/pubsub [caller=endpoint.go:129]
Jul 11 13:05:07 center pxgrid-agent[5404]: pxgrid-agent

STOMP CONNECT host

=10.48.78.177 [caller=endpoint.go:138]
Jul 11 13:06:59 center pxgrid-agent[5404]: pxgrid-agent

STOMP SEND destination

=/topic/com.cisco.endpoint.asset body={

"opType":"UPDATE"

,"asset":{"assetId":"01:80:c2:00:00:00","assetName":"LLDP/STP bridges Multicast 0:0:0","assetIpAddress"

```
Jul 11 13:10:04 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceReregister
```

Le format de message attendu après l'intégration réussie et l'attribut assetGroup est publié sans valeur, comme indiqué :

<#root>

Jan 25 11:05:49 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endpoint.asset body={"opType":"UPDATE","as

{"key":"assetGroup","value":""}

,{"key":"assetCustomName","value":"test"},{"key":"assetGroupPath","value":""}],"assetConnectedLinks":[]

Format de message attendu (assetGroup avec une valeur, comme illustré). Cela confirme que CyberVision Center envoie les attributs et si ceux-ci ne sont pas reflétés dans le côté ISE, vous devez approfondir votre enquête avec ISE.

<#root>

Jan 25 11:09:28 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endpoint.asset body={"opType":"UPDATE","as

{"key":"assetGroup","value":"test group"}

,{"key":"assetCustomName","value":"test"},{"key":"assetGroupPath","value":"test group"}],"assetConnecte

Informations connexes

- Présentation des solutions CCV et ISE
- Travaux pratiques de démonstration : Utilisation de Cisco Cyber Vision pour fournir une microsegmentation dynamique à l'aide de Cisco ISE
- Démonstration d'ISE et CCV
- Guide d'intégration ISE
- Assistance technique de Cisco et téléchargements

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.