

Probleemoplossing bij ISE-integratie

Inhoud

[Inleiding](#)

[Overzicht van beste praktijken](#)

[CCV-ISE-stroomdiagram op hoog niveau](#)

[Richtlijnen voor probleemoplossing](#)

[Te verzamelen gegevens](#)

[Verwachte logberichten](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven voor het oplossen van problemen bij de integratie van CyberVision Center in ISE.

Overzicht van beste praktijken

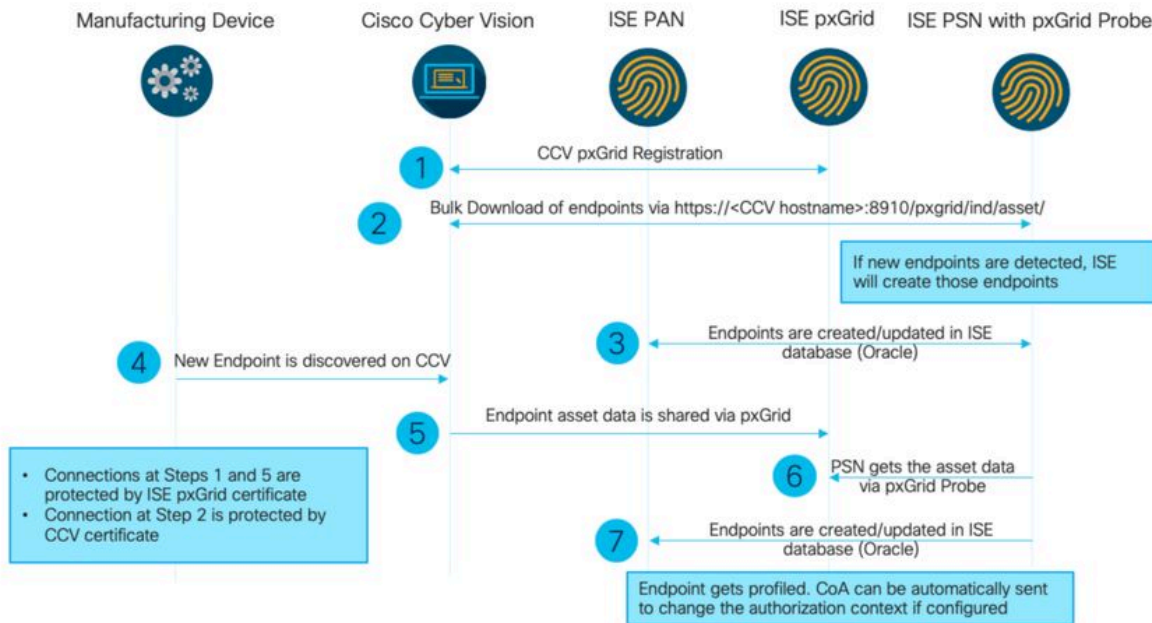
Best practices zijn de aanbevolen stappen die u moet overwegen om de juiste werking van de systeemconfiguratie te garanderen. Aanbevelingen:

- Raadpleeg de opmerkingen bij de Cisco Cyber Vision-release, en de opmerkingen bij de Cisco Identity Services Engine (ISE)-release, voor de laatste functies, richtlijnen, beperkingen en voorbehouden
- Controleer en los eventuele nieuwe configuratiewijzigingen op nadat u deze hebt geïmplementeerd

CCV-ISE-stroomdiagram op hoog niveau

Configure

High-Level Flow Diagram



Richtlijnen voor probleemoplossing

Door de komende vragen te beantwoorden, kunt u het pad voor probleemoplossing bepalen en de onderdelen die nader onderzoek nodig hebben. Antwoord op de volgende vragen om de status van uw installatie te bepalen:

- Is dit een nieuw geïnstalleerd systeem of een bestaande installatie?
- Is CyberVision ooit in staat geweest om de ISE te zien?

Controleer de status van de pxGrid-services met de opdracht `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]
```

- Voert ISE pxGrid uit in hoge beschikbaarheid?
- Wat veranderde er in de configuratie of in de algehele infrastructuur vlak voordat de toepassingen problemen begonnen te krijgen?

Om een netwerkprobleem te ontdekken, gebruik de algemene stappen van het netwerkoplossen van problemen:

Stap 1. Bent u in staat om CyberVision Center Hostname van ISE te pinggen?

```
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
```

Als kan niet pingen, maak verbinding met ISE CLI met Secure Shell (SSH) en 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
```

Stap 2. Bent u in staat om ISE Hostname te pingen vanaf 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
```

Als dit niet het geval is, probeer dan de ISE-hostnaam toe te voegen aan het /data/etc/hosts bestand in het midden.

```
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
```

Stap 3. Ontdek certificaatproblemen.

Voer de opdracht `openssl s_client -connect YourISEHostname:8910` in vanuit CyberVision Center.

Te verzamelen gegevens

Voor netwerkproblemen:

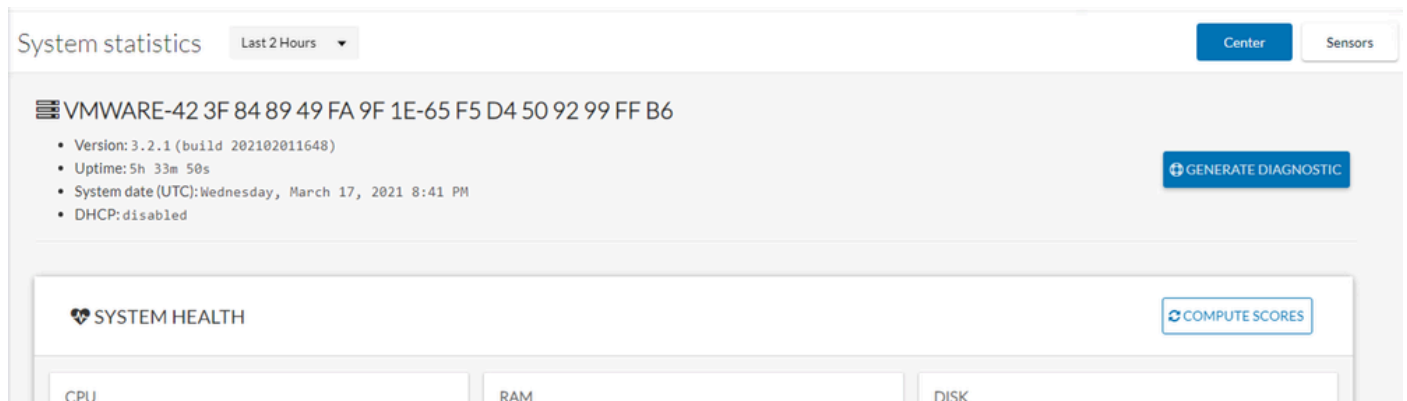
- Architectuur:

Een schema van deze details tussen het centrum en ISE is nuttig:

- Firewallregels
- Statische routes
- Configuratie van de gateway
- VLAN-configuraties

- Logbestanden te verzamelen voor alle ISE-problemen:

U kunt beginnen met het verzamelen van een diagnostisch bestand van het Centrum om te voorkomen dat gegevens verloren gaan.



System statistics Last 2 Hours Center Sensors

VMWARE-42 3F 84 89 49 FA 9F 1E-65 F5 D4 50 92 99 FF B6

- Version: 3.2.1 (build 202102011648)
- Uptime: 5h 33m 50s
- System date (UTC): Wednesday, March 17, 2021 8:41 PM
- DHCP: disabled

GENERATE DIAGNOSTIC

SYSTEM HEALTH COMPUTE SCORES

CPU RAM DISK

Vervolgens activeert u geavanceerde logbestanden op het centrum met deze procedure:

Maak twee bestanden in de map /data/etc/sbs.

Het eerste bestand moet een naam hebben listener.conf en de inhoud bevatten:

(Noteer de ruimte aan de voorkant voor het loglevel.)

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

Het tweede bestand moet een naam krijgen pxgrid-agent.conf en de inhoud bevatten:

(Noteer de ruimte aan de voorkant voor het loglevel.)

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

Wanneer beide bestanden zijn gemaakt, start u het Centrum opnieuw op of start u de services sbs-burrow en pxgrid-agent services opnieuw.

Restart service using the command:

```
#systemctl restart sbs-burrow
#systemctl restart pxgrid-agent
```

Vervolgens verzamelt u de pxGrid-logbestanden (gebruik de bestandsoverdrachtgereedschappen om de logbestanden uit het Center te exporteren).

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

Verzamel tcpdump-opnamen voor het analyseren van de communicatiestroom tussen het centrum en ISE.

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

- Schakel Debugs in op ISE en verzamel ondersteuningsbundel.

Om debugs op ISE in te schakelen, navigeer naar Administration > System > Logging > Debug Log Configuration. Logniveaus als volgt instellen:

Persona	Naam van component	Logniveau	Te controleren bestand	
PAN (optioneel)	profiler	DEBUGGEN	profiler.log	
PSN met pxGrid-sonde	profiler	DEBUGGEN	profiler.log	

ingeschakeld				
PxGrid	pxgrid	SPOREN	pxgrid-server.log	

Verwachte logberichten

Debug logboeken van de pxGrid-agent in het centrum tonen de agent die wordt gestart, de dienst die wordt geregistreerd, Cisco Cyber Vision (CCV) die Eenvoudige (of Streaming) Tekst georiënteerde Messaging Protocol (STOMP) verbinding met ISE tot stand brengt, en het verzenden van update-handeling voor een actief/component:

<#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.sock'
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"

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.