

Solución de problemas de integración de ISE

Contenido

[Introducción](#)

[Descripción general de las prácticas recomendadas](#)

[Diagrama de flujo de alto nivel de CCV-ISE](#)

[Pautas para la resolución de problemas](#)

[Datos que recopilar](#)

[Mensajes de registro esperados](#)

[Información Relacionada](#)

Introducción

En este documento se describen los pasos para la solución de problemas de la integración de CyberVision Center a ISE.

Descripción general de las prácticas recomendadas

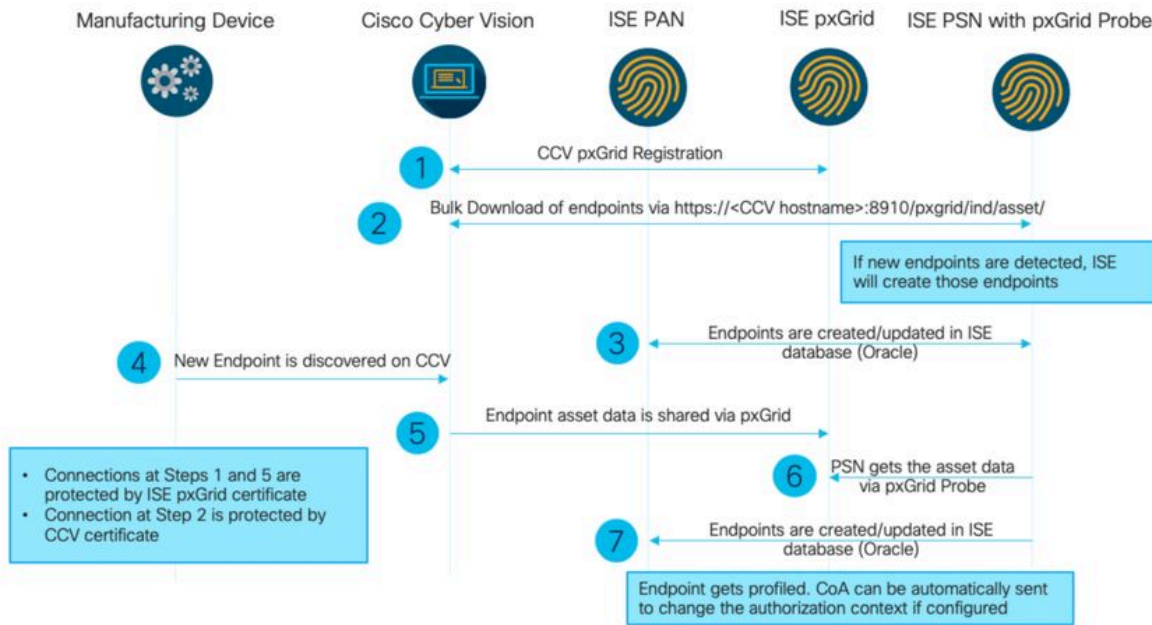
Las prácticas recomendadas son los pasos recomendados que debe considerar para garantizar el funcionamiento correcto de la configuración del sistema. Recomendaciones:

- Consulte las notas de la versión de Cisco Cyber Vision y las notas de la versión de Cisco Identity Services Engine (ISE) para conocer las últimas características, directrices, limitaciones y advertencias
- Verifique y solucione cualquier cambio de configuración nuevo después de implementarlo

Diagrama de flujo de alto nivel de CCV-ISE

Configure

High-Level Flow Diagram



Pautas para la resolución de problemas

Respondiendo a las próximas preguntas, puede determinar la ruta de solución de problemas y los componentes que necesitan más investigación. Responda a las siguientes preguntas para determinar el estado de su instalación:

- ¿Se trata de un sistema recién instalado o de una instalación existente?
- ¿CyberVision ha podido ver alguna vez el ISE?

Verifique el estado de los servicios pxGrid mediante el comando `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 ejecuta pxGrid con alta disponibilidad?
- ¿Qué cambió en la configuración o en la infraestructura general inmediatamente antes de que las aplicaciones comenzaran a tener problemas?

Para descubrir un problema de red, utilice los pasos generales de troubleshooting de la red:

Paso 1. ¿Puede hacer ping al nombre de host de CyberVision Center desde 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 no puede hacer ping, conéctese a ISE CLI mediante Secure Shell (SSH) y Add hostname (Agregar nombre de host).

```

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

```

Paso 2. ¿Puede hacer ping al nombre de host de ISE desde el 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 no es así, intente agregar el nombre de host de ISE al /data/etc/hosts archivo en 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

```

Paso 3. Detectar problemas de certificados.

Ingrese el comando `openssl s_client -connect YourISEHostname:8910` de CyberVision Center.

Datos que recopilar

Para problemas de red:

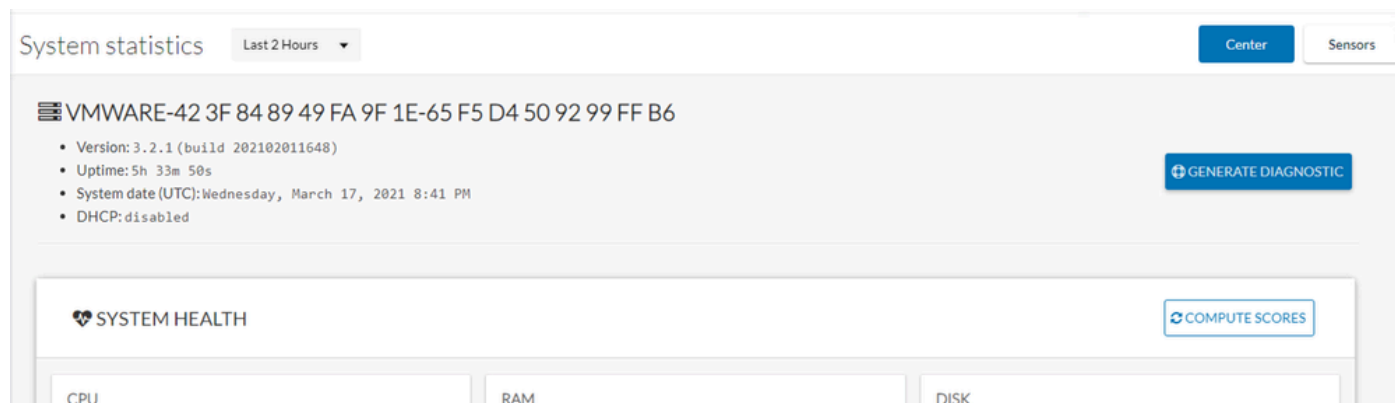
- Arquitectura:

Es útil contar con un esquema que muestre esos detalles entre el centro e ISE:

- Reglas de firewall
- Rutas estáticas
- Configuración del gateway
- Configuraciones de VLAN

- Registros que recopilar para todos los problemas de ISE:

Puede empezar por recopilar un archivo de diagnóstico del centro para evitar la pérdida de datos.



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

A continuación, active los registros avanzados en el centro mediante este procedimiento:

Cree dos archivos en la carpeta /data/etc/sbs.

El primer archivo debe tener nombre listener.conf y contener el contenido:

(Observe el espacio inicial delante del nivel de registro.)

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

El segundo archivo debe tener nombre pxgrid-agent.conf y contener el contenido:

(Observe el espacio inicial delante del nivel de registro.)

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

Una vez creados ambos archivos, reinicie el Centro o reinicie los servicios sbs-burrow y pxgrid-agent.

Restart service using the command:

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

Luego recopile los registros de pxGrid (utilice las herramientas de transferencia de archivos para exportar los registros desde el Centro).

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

Recopile capturas de tcpdump para analizar el flujo de comunicación entre el centro e ISE.

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

- Habilite las depuraciones en ISE y recopile el paquete de asistencia.

Para habilitar los debugs en ISE, navegue hasta Administration > System > Logging > Debug Log Configuration. Establezca los niveles de registro en los siguientes:

Persona	Nombre del componente	Nivel de registro	Archivo para comprobar	
PAN (opcional)	generador de perfiles	DEPURAR	profiler.log	
PSN con la sonda pxGrid	generador de	DEPURAR	profiler.log	

habilitada	perfiles			
PxGrid	pxgrid	RASTREAR	pxgrid-server.log	

Mensajes de registro esperados

Los logs de depuración del pxGrid-agent en el centro muestran el agente que se está iniciando, el servicio que se ha registrado, Cisco Cyber Vision (CCV) Estableciendo una conexión simple (o de transmisión) de protocolo de mensajería orientada a texto (STOMP) con ISE y enviando la operación de actualización para un activo/componente:

<#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' [caller=pxgrid.go:58]
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccountActivate body={
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 body={
"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"

```


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).