Troubleshoot ISE Integration

Contents

Introduction

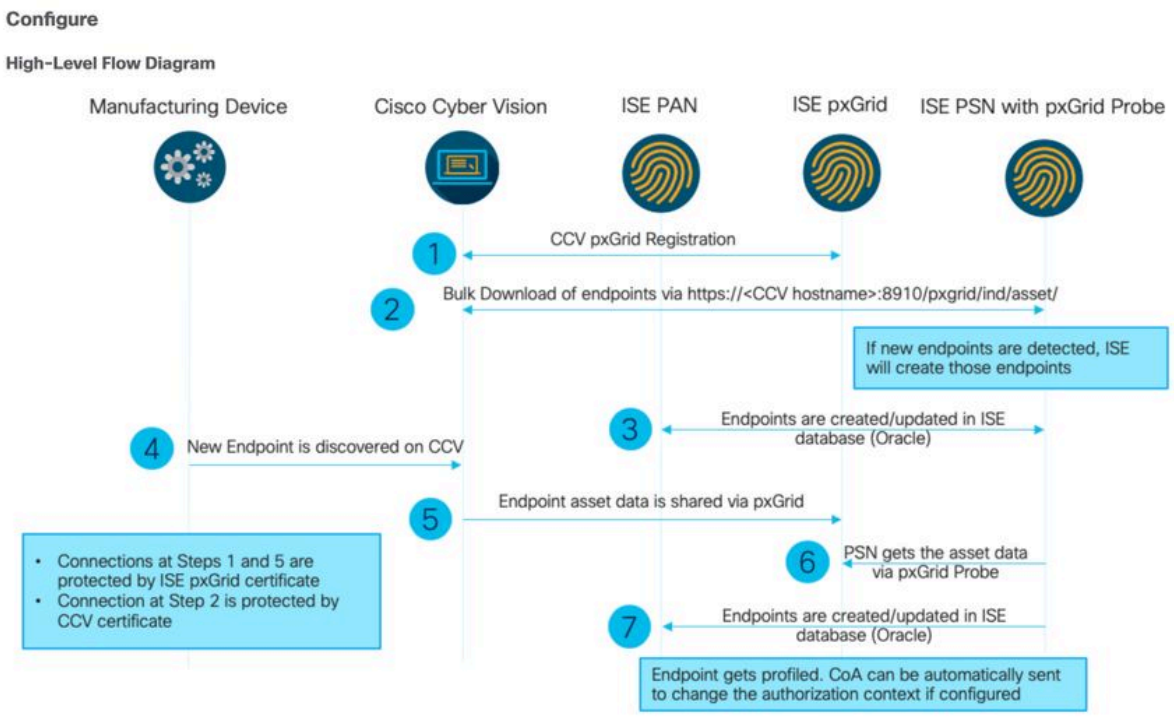
This document describes the troubleshooting steps for CyberVision Center to ISE integration.

Overview of Best Practices

Best practices are the recommended steps that you must consider in order to ensure the correct operation of system configuration. Recommendations:

- Refer to the Cisco Cyber Vision release notes, and Cisco Identity Services Engine (ISE) release notes, for the latest features, guidelines, limitations, and caveats
- Verify and troubleshoot any new configuration changes after implementing them

CCV-ISE High-Level Flow Diagram



Troubleshooting Guidelines

By answering the upcoming questions, you can determine the troubleshooting path and the components that need further investigation. Respond to the subsequent questions in order to determine the status of your installation:

- Is this a newly installed system or an existing installation?
- Has the CyberVision ever been able to see the ISE?

Check the pxGrid services status using the command 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]
```

- Does ISE run pxGrid in high availability?
- What changed in the configuration or in the overall infrastructure immediately before the applications started to have problems?

In order to discover a network problem, use the general network troubleshooting steps:

Step 1. Are you able to ping CyberVision Center Hostname from 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
```

If unable to ping, connect to ISE CLI using Secure Shell (SSH) and 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
```

Step 2. Are you able to ping ISE Hostname from CyberVisiion 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
```

If not, try to add the ISE hostname to the /data/etc/hosts file in 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
```

Step 3. Discover certificate issues.

Enter the command openssl s_client -connect YourISEHostname:8910 from 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
```

Data to Collect

For network issues:

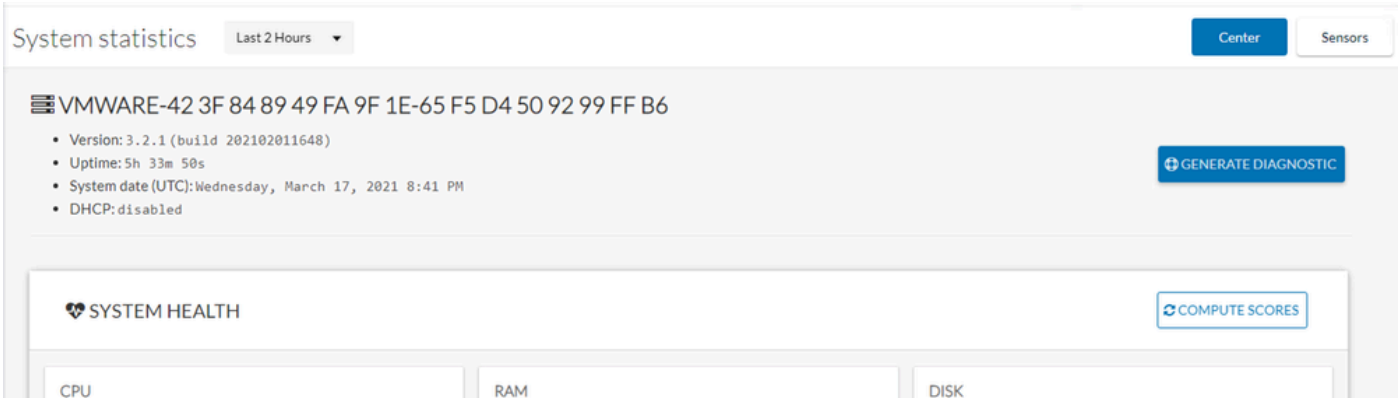
- Architecture:

A scheme showing those details between the center and ISE is helpful:

- Firewall rules
- Static routes
- Configuration of the Gateway
- VLAN configurations

- Logs to collect for all ISE issues:

You can start by collecting a Center diagnostic file in order to avoid losing data.



Then activate advanced logs on the center using this procedure:
Create two files in the folder /data/etc/sbs.
The first file must be named listener.conf and contain the content:

(Note the leading space in front of the loglevel.)

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

The second file must be named pxgrid-agent.conf and contain the content:

(Note the leading space in front of the loglevel.)

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

Once both files are created, reboot the Center, or restart the sbs-burrow and pxgrid-agent services.

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

Then collect the pxGrid logs (use the filetransfer tools in order to export the logs from the Center).

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

Collect tcpdump captures for analyzing communication flow between the Center and ISE.

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

- Enable Debugs on ISE and collect support bundle.

In order to enable debugs on ISE, navigate to Administration > System > Logging > Debug Log Configuration. Set log levels to these:

Persona	Component Name	Log Level	File to Check	
PAN (optional)	profiler	DEBUG	profiler.log	
PSN with pxGrid probe enabled	profiler	DEBUG	profiler.log	
PxGrid	pxgrid	TRACE	pxgrid-server.log	

Expected Log Messages

Debug logs of the pxGrid-agent in the center show the agent being started, service registered, Cisco Cyber Vision (CCV) Establishing Simple (or Streaming) Text Orientated Messaging Protocol (STOMP) connection with ISE, and sending update operation for an asset/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.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
```

Expected message format post successful integration and assetGroup attribute is published without a value, as shown:

<#root>

```
 Jan 25 11:05:49 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endp

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

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

Expected message format (assetGroup with a value, as shown). This confirms that CyberVision Center is sending the attributes and if the same is not further reflected on the ISE side, you must investigate with ISE further.

<#root>

```
Jan 25 11:09:28 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endp
```

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

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

Related Information

- CCV and ISE Solution Brief
- Demo Lab: Using Cisco Cyber Vision to Provide Dynamic Micro-segmentation using Cisco ISE
- Demo ISE and CCV
- ISE Integration Guide
- Cisco Technical Support & Downloads