排除ISE整合故障

目錄

簡介

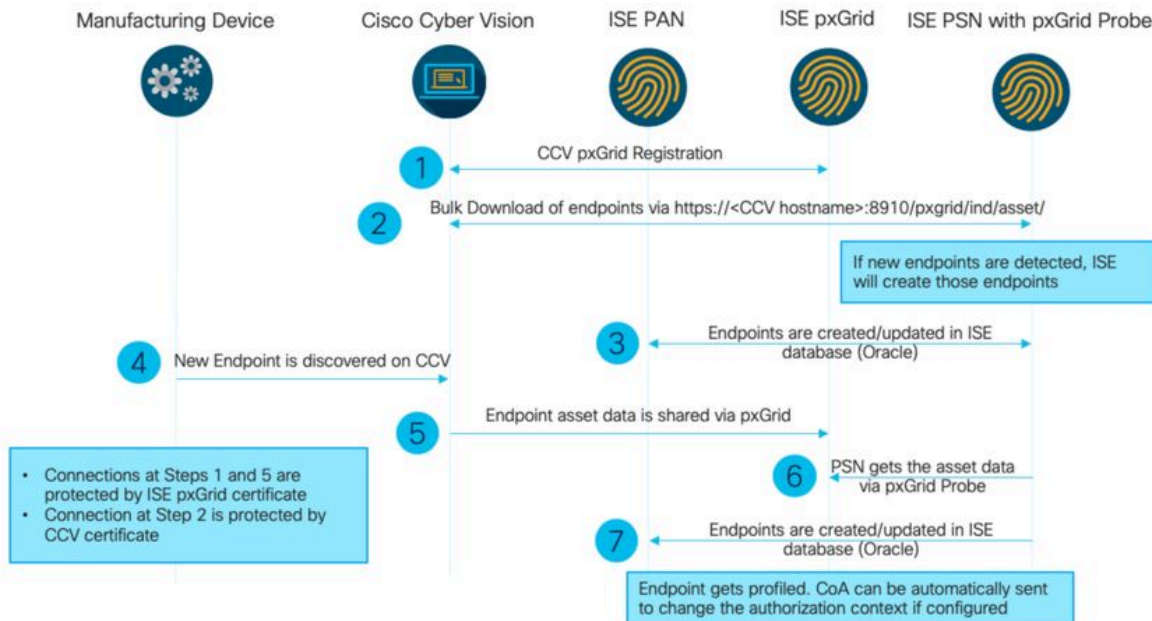本文檔介紹CyberVision Center與ISE整合的故障排除步驟。

最佳實踐概述

最佳做法是您必須考慮的建議步驟，以確保系統配置的正確操作。建議：

- 請參閱思科網路願景版本說明和思科身份服務引擎(ISE)版本說明，瞭解最新功能、指南、限制和警告
- 實施新配置更改後，驗證這些更改並對其進行故障排除

CCV-ISE高級流程圖

Configure

High-Level Flow Diagram

| Manufacturing Device | Cisco Cyber Vision | ISE PAN | ISE pxGrid | ISE PSN with pxGrid Probe |

1 — CCV pxGrid Registration

2 — Bulk Download of endpoints via https://<CCV hostname>:8910/pxgrid/ind/asset/

If new endpoints are detected, ISE will create those endpoints

3 — Endpoints are created/updated in ISE database (Oracle)

4 — New Endpoint is discovered on CCV

5 — Endpoint asset data is shared via pxGrid

6 — PSN gets the asset data via pxGrid Probe

- Connections at Steps 1 and 5 are protected by ISE pxGrid certificate
- Connection at Step 2 is protected by CCV certificate

7 — Endpoints are created/updated in ISE database (Oracle)

Endpoint gets profiled. CoA can be automatically sent to change the authorization context if configured

疑難排解指南

透過回答即將出現的問題,您可以確定故障排除路徑和需要進一步調查的元件。回答後續問題,以確定安裝狀態:

- 這是新安裝的系統還是現有安裝?
- CyberVision是否曾經能夠看到ISE?

使用命令systemctl status pxgrid-agent檢查pxGrid服務狀態。

```
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是否以高可用性運行pxGrid?

- 在應用程式出現問題之前,配置或整個基礎架構中發生了什麼變化?

要發現網路問題,請使用常規網路故障排除步驟:

步驟 1.您是否能從ISE對CyberVision Center主機名執行ping操作?

```
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
```

如果無法ping，請使用安全外殼(SSH)和增加主機名連線到ISE CLI。

```
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
```

步驟 2.您是否能從CyberVision Center對ISE主機名執行ping操作？

```
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
root@center:~#
```

否則，嘗試將ISE主機名增加到Center中的/data/etc/hosts檔案。

```
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
```

步驟 3.發現證書問題。

從CyberVision Center輸入命令openssl s_client -connect YourISEHostname:8910。

```
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
A1UECwwnQ2VydGlmaWNhdGUgU2VydmljZXMgU3lzdGVtIENlcnRpZmljYXRlMRow
GAYDVQQDDBFFU0NJU0UyLmNjdi5sb2NhDCCAiIwDQYJKoZIhvcNAQEBBQADggIP
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
1cB30YJL0Kwj6XolaV7SMB0GA1UdDgQWBBRigvgT63FOqKmS9m9COhW3ahdv8jAO
BgNVHQ8BAf8EBAMCBeAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggIBADwnDKtdHj/y3Pj4ADDV
57RrdHsiU/EkkWGLzmP/aMKJ9rY7f6eUDlig6b6gpJ8B0MnTPi9VFVduc++oZDEt
CrIMMwFexnnbhPWJfzjSNJPnAMIgFUeiPuoxBJYkjFzhiXtat0fOmdm5RbEu5Wla
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
```
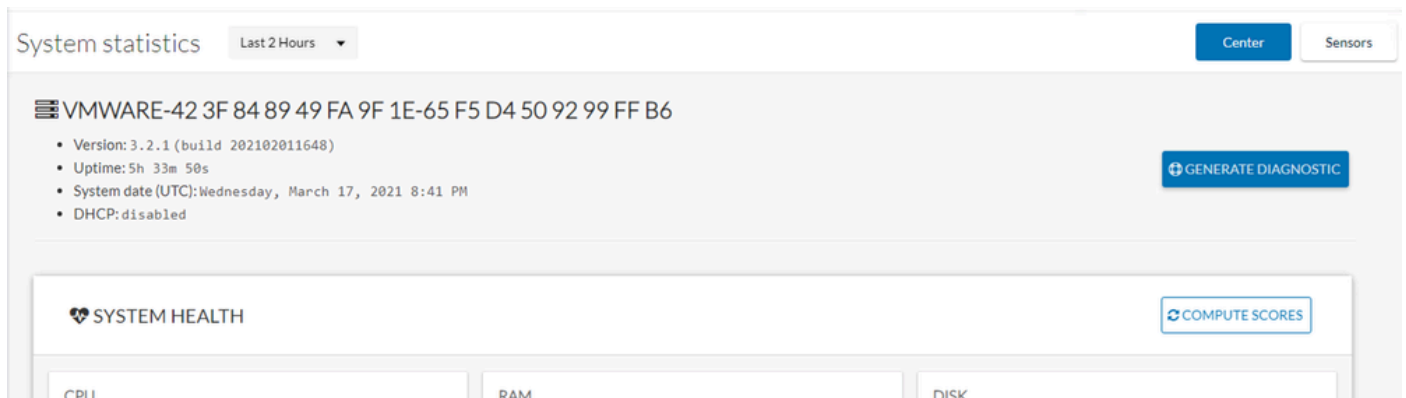
要收集的資料

對於網路問題：

- 架構：

顯示中心和ISE之間的這些詳細資訊的方案非常有用：

- 防火牆規則

- 靜態路由

- 網關配置

- VLAN配置

- 所有ISE問題要收集的日誌：

您可以從收集中心診斷檔案開始，以避免遺失資料。

然後使用以下程式在中心啟用進階記錄：
在資料夾中建立兩個檔案/data/etc/sbs。
第一個檔案必須命名為listener.conf，且包含下列內容：

（請注意日誌級別前面的前導空格。）

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

第二個檔案必須命名為pxgrid-agent.conf，且包含下列內容：

（請注意日誌級別前面的前導空格。）

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

建立這兩個檔案後，請重新啟動中心，或者重新啟動sbs-burrow和pxgrid-agent服務。

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

然後收集pxGrid日誌（使用檔案傳輸工具從中心導出日誌）。

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

收集tcpdump捕獲，用於分析中心和ISE之間的通訊流。

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

- 在ISE上啟用調試並收集支援捆綁包。

為了在ISE上啟用調試，請導航到Administration > System > Logging > Debug Log Configuration。將記錄層級設定為：

角色	元件名稱	記錄層級	要檢查的檔案	
PAN（可選）	效能評測器	除錯	效能分析工具 .log	
已啟用pxGrid探測功能的 PSN	效能評測器	除錯	效能分析工具 .log	

畫素網格	pxgrid	追蹤	pxgrid-server.log	

預期的記錄訊息

中心中pxGrid-agent的調試日誌顯示正在啟動的代理、已註冊的服務、Cisco Cyber Vision (CCV)與ISE建立簡單（或流）文本導向消息協定(STOMP)連線，以及傳送資產/元件的更新操作：

<#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
```

成功整合後所需的消息格式和assetGroup屬性發佈時沒有值，如下所示：

<#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":[]

預期的訊息格式（具有值的assetGroup，如下所示）。這確認了CyberVision Center正在傳送屬性，如果ISE端沒有進一步反映這些屬性，則必須進一步與ISE一起調查。

<#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"}],"assetConnected

相關資訊

- [CCV和ISE解決方案簡介](#)

- [演示實驗：使用思科網路願景提供使用思科ISE的動態微分段](#)

- [演示ISE和CCV](#)

- [ISE整合指南](#)

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。