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



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: /sustem.slice/nworid-acent.service
-2040/ /usr/his/20-start_2 on purid_scart
-evii/ /ust/sai/ax-state -t -i paytau-ayane
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 1xc-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 1xc-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 1xc-start[28447]: pxgrid-agent Cyber Vision is in sync with ISE [caller=assets.go:67]
Mar 17 20:23:19 center 1xc-start[20447]: pxgrid-agent AFI: 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 pingen?

```
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=3 ttl=64 time=1.98 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
```

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

```
root@center:~# openssl s_client -connect ESCISE2.ccv.local:8910
CONNECTED (0000003)
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
MTcwNQYDVQQDDC5DZXJ0aW2pY2F0ZSBTZXJ2aWN1cyBFbmRwb21udCBTdWIgQ0Eg
LSBFU0NJU0UyMB4XDTIwMTEyOTE3Mjc1M1oXDTI1MTEzMDE3Mjc1M1owTjEwMC4G
A1UECwwnQ2VydG1maWNhdGUgU2Vydm1j2XMgU31zdGVtIEN1cnRpZm1jYXR1MRow
GAYDVQQDDBFFU0NJU0UyLmNjdi5sb2NhbDCCAiIwDQYJKoZIhvcNAQEBBQADggIP
ADCCAgoCggIBANE1Ukx/7QnUdrCIXJLUxg0XWTvOFTNme4L16yDFsLvytGjFqYfR
RCRM/kzRVjDk8f/cSSP9T+5pR/JA+PbOZqkAWWDJVaQh1ndqL0kX7UaCCodKUWon
DafVimPjKqV1RSCd8bwVDxAr7qYou3S4BcCe00s1x5pL1WyZw6F6MPze2F388kSR
GuSRsn40ZM4JjDDeaxSBrs789f7zACw4eMZIfRDk0RL9qzMtoghIU089/1VuacUb
WYrF0e0mThUWg7wk7dFv4bozyWeHjdqsbEtb0Geme8ZWPX5ZYddSKjWhOrNUXeQV
NvDBUXhb5NpSsKYMoCqnvIv+JYzkIV6ukksX9xqI5bL3/vik/CyPVMeXI0Jo64dK
\verb"S0vMjrcnmpNznoLzEv3mgvgp9mJhcTROg86w1yOrOzjOoMCGGLrhpgxuLeVatFKv"
GLWjsmrWcLk/F0Ae4H+tb6/+y07KNXTSX+nP1z5epDA8stzvLxm1ylw65XdeEBho
m0qgGEKr5y/I/2b+myi24ZYrqsv64KPohCisIvZxbCG/2q77SP7ml8v8+BidpMaW
LZrZ0tD2XRJeyhPyprBYwV4QDBWPn+mCAFgpNd3KC36zAn138c2WW1Hs0PKhReMX
vNn+SwltKmyIbM090eww5zRSdMU90zPcFkY0qvrBUD31Gf5fAiWqlmkVAgMBAAGj
gcwwgckwaAYDVR0jBGEwX4AUxz+SV+KtR/CpwGiyNg+mp/xxiAqhNaQzMDExLzAt
BgNVBAMMJkN1cnRp2mljYXR1IFN1cnZpY2VzIE5v2GUgQ0EgLSBFU0NJU0UyghAx
lcB30YJL0Kwj6XolaV7SMB0GA1UdDgQWBBRigvgT63F0qKmS9m9COhW3ahdv8jA0
BgNVHQ8BAf8EBAMCBeAwIAYDVR01AQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggIBADwnDKtdHj/y3Pj4ADDV
57RrdHsiU/EkkWGLzmP/aMKJ9rY7f6eUDlig6b6gpJ8B0MnTPi9VFVduc++oZDEt
CrIMMwFexnnbhPWJfzjSNJPnAMIgFUeiPuoxBJYkjFzhiXtat0fOmdm5RbEu5Wla
f7EEBd/X0iRTMyIxqubXQCt6pE61y9gBPuQU9Hvd5QpcLX77LSfEroJhkD4dmuRs
o4uj0wWKFtXW+yLWhwjkiieoBuREEU8Gvtk+iq+11mThfpeP32fV2IO/WIo4SKh0
ILkzS206rbSzxxatKDQ6jZDs3a5YKyFtR55r7VndmX0I4sqXI9dFQjTPVfW7TEbK
GPds+vMe4J9g4c1KGRhiXNiNzfB5S3eWzOL/2092gWS1u7R7GVXKlYrvSHMieL3t
n/p+ov8cogr00o6jXFItZ+Rsnp11Kbq+DrsoCE/i26QgkTKBruMFhz6P8k/2aLqQ
MwJp0dhH1SFmkWCAQbGQpapoX31pK36FUta3sZL2mdN/XyK5UutLbLJx87elwunp
w6Cxz5MA97NXOUZIuqThnTG7Ibu8pzwl1X2Yt1f1T50luCoY2CkVbU93rqfD4zyr
WyK2a0BmizcKXD+F8Yti4fm4Kv10bpWihUNPPMTmgwJMUOW+zdC7b7g13j5rnE9X
lyFJ3uHTohidxEtXi4XsiCn5
----END CERTIFICATE----
subject=OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local
```

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 3 Version: 3.2.1 (build Uptime: 5h 33m 50s System date (UTC): Wet DHCP: disabled 	F 84 89 49 FA 9F 1E-65 F5 D4 50 92 99 1 202102011648) Inesday, March 17, 2021 8:41 PM	P FF B6	GENERATE DIAGNOSTIC
SYSTEM HEAL	ТН		
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.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","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

Verwacht berichtformaat na succesvolle integratie en assetGroup attribuut wordt gepubliceerd zonder een waarde, zoals getoond:

<#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":[]

Verwacht berichtformaat (assetGroup met een waarde, zoals getoond). Dit bevestigt dat CyberVision Center de eigenschappen verzendt en als hetzelfde niet verder wordt weergegeven aan de kant van ISE, moet u verder onderzoeken met 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"}],"assetConnected
```

Gerelateerde informatie

- <u>Samenvatting van CCV- en ISE-oplossing</u>
- Demo Lab: gebruik van Cisco Cyber Vision om dynamische micro-segmentatie te bieden met Cisco ISE
- Demo ISE en CCV
- <u>ISE-integratiegids</u>
- <u>Cisco Technical Support en downloads</u>

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.