Fehlerbehebung bei ISE-Integration

Inhalt

Einleitung
Überblick über Best Practices
Übergeordnetes Flussdiagramm zu CCV-ISE
Richtlinien zur Fehlerbehebung
Zu erfassende Daten
Erwartete Protokollnachrichten
Zugehörige Informationen

Einleitung

In diesem Dokument werden die Schritte zur Fehlerbehebung bei der Integration von CyberVision Center in die ISE beschrieben.

Überblick über Best Practices

Best Practices sind die empfohlenen Schritte, die Sie berücksichtigen müssen, um den korrekten Betrieb der Systemkonfiguration sicherzustellen. Empfehlungen:

- Die neuesten Funktionen, Richtlinien, Einschränkungen und Probleme finden Sie in den Versionshinweisen zu Cisco Cyber Vision und der Cisco Identity Services Engine (ISE).
- Überprüfung und Problembehebung bei neuen Konfigurationsänderungen nach deren Implementierung

CCV-ISE - Detailliertes Flussdiagramm

Configure



Richtlinien zur Fehlerbehebung

Indem Sie die folgenden Fragen beantworten, können Sie den Fehlerbehebungspfad und die Komponenten ermitteln, die weiter untersucht werden müssen. Beantworten Sie die folgenden Fragen, um den Status Ihrer Installation zu ermitteln:

- · Handelt es sich um ein neu installiertes System oder um eine bestehende Installation?
- Konnte CyberVision die ISE jemals sehen?

Überprüfen Sie den Status der pxGrid-Dienste mithilfe des Befehls 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 (lyn-start)
(Construction allocation and a service
Cology, / system struct pagine service
-zost//usr/bin/ixc-start =r =n pxgrid-agent
Mar 17 20:12:15 center 1xc-start[28447]: 1xc-start: cgfsng.c: create path for hierarchy: 1306 Path "/sys/fs/cgroup/pids//1xc/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 RFC 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 1xc-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]

- Wird pxGrid auf der ISE in hoher Verfügbarkeit ausgeführt?
- Was hat sich in der Konfiguration oder in der Infrastruktur insgesamt geändert, unmittelbar bevor die Anwendungen Probleme aufwiesen?

Um ein Netzwerkproblem zu erkennen, gehen Sie zur allgemeinen Fehlerbehebung wie folgt vor:

```
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
```

Wenn Sie keinen Ping-Befehl senden können, stellen Sie über Secure Shell (SSH) und Add hostname eine Verbindung mit der ISE-CLI her.

```
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
```

Schritt 2: Können Sie einen Ping an den ISE-Hostnamen im CyberVision Center senden?

```
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=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
```

Falls nicht, versuchen Sie, den ISE-Hostnamen zur /data/etc/hosts Datei im Center hinzuzufügen.

```
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
```

Geben Sie den Befehl openssl s_client -connect YourISEHostname:8910 von CyberVision Center ein.

```
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
```

Zu erfassende Daten

Netzwerkprobleme:

• Architektur:

Ein Schema, das diese Details zwischen dem Center und der ISE zeigt, ist hilfreich:

- Firewall-Regeln
- Statische Routen
- Konfiguration des Gateways
- VLAN-Konfigurationen
- Protokolle für alle ISE-Probleme:

Sie können beginnen, indem Sie eine Center-Diagnosedatei sammeln, um Datenverlust zu vermeiden.

System statistics	Last 2 Hours 🔹			Center Sensors
VMWARE-42 3 Version: 3.2.1 (build Uptime: 5h 33m 50s System date (UTC): We DHCP: disabled 	F 84 89 49 FA 9F 1E-65 F 1 202102011648) dnesday, March 17, 2021 8:41 PM	5 D4 50 92 99 FF B6		GENERATE DIAGNOSTIC
SYSTEM HEAL	тн			
CPU		RAM	DISK	

Aktivieren Sie dann erweiterte Protokolle auf dem Center mit diesem Verfahren:

Erstellen Sie zwei Dateien im Ordner /data/etc/sbs.

Die erste Datei muss einen Namen haben und den folgenden Inhalt enthaltenlistener.conf:

(Beachten Sie die führenden Leerzeichen vor der Protokollstufe.)

root@Center:~# cat /data/etc/sbs/listener.conf configlog: loglevel: debug root@Center:~# Die zweite Datei muss einen Namen haben und den folgenden Inhalt enthaltenpxgrid-agent.conf:

(Beachten Sie die führenden Leerzeichen vor der Protokollstufe.)

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

Wenn beide Dateien erstellt wurden, starten Sie das Center neu, oder starten Sie den sbs-burrow Server und die pxgrid-agent Dienste neu.

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

Sammeln Sie dann die pxGrid-Protokolle (verwenden Sie die Dateiübertragungstools, um die Protokolle aus dem Center zu exportieren).

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

Sammeln Sie tcpdump-Aufnahmen für die Analyse des Kommunikationsflusses zwischen dem Center und der ISE.

coot@Center:~# tcpdump -i eth0 -n host	CCV_IP and host ISE_	_IP -w /data/tmp/ccv_	ise.pcap
--	----------------------	-----------------------	----------

Aktivieren Sie Debugs auf der ISE, und sammeln Sie das Supportpaket.

Um das Debuggen auf der ISE zu aktivieren, navigieren Sie zu Administration > System > Logging > Debug Log Configuration. Protokollstufen auf folgende Werte festlegen:

Person	Komponentenname	Protokollstufe	Zu prüfende Datei	
PAN (optional)	Profiler	DEBUG	Profiler.log	
PSN mit aktivierter pxGrid- Überprüfung	Profiler	DEBUG	Profiler.log	

Erwartete Protokollnachrichten

Debug-Protokolle des pxGrid-Agenten in der Zentrale zeigen den gestarteten Agenten, den registrierten Service, Cisco Cyber Vision (CCV) Herstellen einer einfachen (oder Streaming) Text Oriented Messaging Protocol (STOMP)-Verbindung mit ISE und Senden eines Update-Vorgangs für eine Ressource/Komponente:

<#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

Das erwartete Nachrichtenformat nach erfolgreicher Integration und das Attribut 'assetGroup' wird ohne Wert veröffentlicht, wie dargestellt:

<#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":[]

Erwartetes Nachrichtenformat (AssetGroup mit einem Wert, wie dargestellt). Dies bestätigt, dass CyberVision Center die Attribute sendet. Wenn diese Attribute auf der ISE-Seite nicht weiter berücksichtigt werden, müssen Sie die Informationen zusammen mit der ISE weiter untersuchen.

<#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"}],"assetConnecte
```

Zugehörige Informationen

- Lösungsübersicht zu CCV und ISE
- Demo-Labor: Cisco Cyber Vision für dynamische Mikrosegmentierung mit der Cisco ISE
- Demo zu ISE und CCV
- ISE-Integrationsleitfaden
- <u>Technischer Support und Downloads von Cisco</u>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.