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



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 systemati 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 DTh: 20447 (lyn-start)
Inden East Evity (ANG-SUBER)
Coroup: / system: silder pagrad-agent. Bervice
-28447 /usr/bin/ixc-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 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 1xc-start(28447): pxgrid-agent API: getSyncStatus (caller=sync status.go:34)
Mar 1. 20113:10 cantan lan sustement (2014), marid_anant Cubar Dision is in sum uith TSF (callarmassate do:671
Har 1 bolsols center in outpetternin part dent of of instant of a sine about 10 [caller-asses.ju.or]
Mar 1/ 20123112 Center INC-Start[2013/]: bWdrIn-adeut Mer, dersAuchstarns [Carter-sAuchstart]20123]

• ¿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:

```
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=3 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
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
```

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

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 Ser	nsors
VMWARE-42 3 • Version: 3.2.1 (build • Uptime: 5h 33m 50s • System date (UTC): Wee • DHCP: disabled	F 84 89 49 FA 9F 1E-6 202102011648) inesday, March 17, 2021 8:4:	5 F5 D4 50 92 99 FF [86		Generate diagnostic	1
SYSTEM HEAL	ТН					
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.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

El formato de mensaje esperado tras la integración correcta y el atributo assetGroup se publica sin valor, como se muestra a continuación:

<#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":[]

Formato de mensaje esperado (assetGroup con un valor, como se muestra). Esto confirma que CyberVision Center está enviando los atributos y, si no se refleja más en el lado de ISE, debe investigar con ISE más a fondo.

<#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
```

Información Relacionada

- <u>Resumen de la solución CCV e ISE</u>
- Laboratorio de demostración: uso de Cisco Cyber Vision para proporcionar microsegmentación dinámica con Cisco ISE
- Demostración de ISE y CCV
- Guía de integración de ISE
- <u>Soporte técnico y descargas de Cisco</u>

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).