Solução de problemas de integração do ISE

Contents

ntrodução	
Visão geral das práticas recomendadas	
Diagrama de fluxo de alto nível do CCV-ISE	
Diretrizes de Troubleshooting	
Dados a Serem Coletados	
Mensagens de log esperadas	
nformações Relacionadas	

Introdução

Este documento descreve as etapas de solução de problemas para a integração do CyberVision Center com o ISE.

Visão geral das práticas recomendadas

As práticas recomendadas são as etapas recomendadas que você deve considerar para garantir a operação correta da configuração do sistema. Recomendações:

- Consulte as notas de versão do Cisco Cyber Vision e do Cisco Identity Services Engine (ISE) para obter os recursos, diretrizes, limitações e advertências mais recentes
- · Verificar e solucionar problemas de novas alterações de configuração após implementá-las

Diagrama de fluxo de alto nível do CCV-ISE

Configure



Diretrizes de Troubleshooting

Ao responder às próximas perguntas, você pode determinar o caminho de solução de problemas e os componentes que precisam de investigação adicional. Responda às perguntas subsequentes para determinar o status da instalação:

- Este é um sistema instalado recentemente ou uma instalação existente?
- O CyberVision já conseguiu visualizar o ISE?

Verifique o status dos serviços pxGrid usando o comando 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 FID: 28447 (lxc-start)
CGroup: /system.slice/pxgrid-agent.service
L28447 /usr/bin/lxc-start -F -n pxgrid-agent
Mar 17 20:12:15 center lxc-start/284471: 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 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 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 AFI: getSyncStatus [caller=sync status.go:34]

- O ISE executa o pxGrid em alta disponibilidade?
- O que mudou na configuração ou na infraestrutura geral imediatamente antes de os aplicativos começarem a ter problemas?

Para descobrir um problema de rede, use as etapas gerais de solução de problemas de rede:

Etapa 1. Você consegue fazer ping do nome de host do CyberVision Center a partir do 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
```

Se não for possível fazer ping, conecte-se ao CLI do ISE usando Secure Shell (SSH) e Adicionar nome 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
```

Etapa 2. Você consegue fazer ping no nome de host do ISE a partir do 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=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
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
```

Caso contrário, tente adicionar o nome de host do ISE ao arquivo/data/etc/hosts no Centro.

```
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
```

Insira o comandoopenssl s_client -connect YourISEHostname:8910 do 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
```

Dados a Serem Coletados

Para problemas de rede:

• Arquitetura:

Um esquema mostrando esses detalhes entre o centro e o ISE é útil:

- Regras de firewall
- Rotas estáticas
- Configuração do Gateway
- Configurações de VLAN
- Logs a serem coletados para todos os problemas do ISE:

Você pode começar coletando um arquivo de diagnóstico Center para evitar a perda de dados.

System statistics	Last 2 Hours 👻			Center Sensors		
 VMWARE-42 3 Version: 3.2.1 (build Uptime: 5h 33m 50s System date (UTC): Wer DHCP: disabled 	E 84 89 49 FA 9F 1E-65 F5 D4 5 202102011648) Inesday, March 17, 2021 8:41 PM	50 92 99 FF B6		GENERATE DIAGNOSTIC		
SYSTEM HEAL	ТН					
CPU	RAM	4	DISK			
Em seguida, ative os logs avançados no centro usando este procedimento:						

Crie dois arquivos na pasta /data/etc/sbs.

O primeiro arquivo deve ser nomeado listener.conf e conter o conteúdo:

(Observe o espaço à esquerda na frente do nível de log.)

root@Center:~# cat /data/etc/sbs/listener.conf configlog: loglevel: debug root@Center:~# O segundo arquivo deve ser nomeado pxgrid-agent.conf e conter o conteúdo:

(Observe o espaço à esquerda na frente do nível de log.)

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

Depois que os dois arquivos forem criados, reinicialize o Centro ou reinicie os serviços sbs-burrow epxgrid-agent.

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

Em seguida, colete os logs do pxGrid (use as ferramentas de transferência de arquivos para exportar os logs do Centro).

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

Colete capturas tcpdump para analisar o fluxo de comunicação entre o Centro e o ISE.

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

• Ative as depurações no ISE e colete o pacote de suporte.

Para habilitar depurações no ISE, navegue até Administration > System > Logging > Debug Log Configuration. Defina níveis de log para:

Persona	Nome do componente	Nível de log	Arquivo a ser verificado	
PAN (opcional)	profiler	DEBUG	profiler.log	
PSN com sonda pxGrid habilitada	profiler	DEBUG	profiler.log	

			., ,	
PxGrid	pxgrid	RASTREAR	pxgrid-server.log	
				ł

Mensagens de log esperadas

Os logs de depuração do agente do pxGrid no centro mostram o agente sendo iniciado, o serviço registrado, o Cisco Cyber Vision (CCV) Estabelecendo uma conexão STOMP (Text Oriented Messaging Protocol) simples (ou de fluxo contínuo) com o ISE e enviando a operação de atualização para um ativo/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 box

"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

Formato de mensagem esperado após integração bem-sucedida e o atributo assetGroup é publicado sem um valor, como mostrado:

<#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 mensagem esperado (assetGroup com um valor, como mostrado). Isso confirma que o CyberVision Center está enviando os atributos e, se o mesmo não for refletido no ISE, você deverá investigar mais com o 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

Informações Relacionadas

- <u>Resumo da solução CCV e ISE</u>
- Laboratório de demonstração: Usando a Cisco Cyber Vision para fornecer microssegmentação dinâmica usando o Cisco ISE
- Demonstração do ISE e do CCV
- Guia de integração do ISE
- Suporte técnico e downloads da Cisco

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.