Configurar e solucionar problemas do ISE 3.2 com integração do FMC 7.2.4

Contents

Introdução

Este documento descreve os procedimentos para integrar o Identity Services Engine com o Firewall Management Center usando as conexões do Platform Exchange Grid.

Pré-requisitos

A Cisco recomenda conhecimento sobre estes tópicos:

- Identity services engine (ISE)
- Grade de intercâmbio de plataforma
- Centro de gerenciamento de firewall (FMC)
- Certificados TLS/SSL.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Patch 3 do Identity Services Engine (ISE) versão 3.2
- Firewall Management Center versão 7.2.4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio.

Esta documentação fornece uma solução para integrar o FMC e o ISE usando o pxGrid versão 2.

O Cisco Firepower Management Center (FMC) é uma plataforma centralizada para firewall de próxima geração e sistema de prevenção de invasões, oferecendo gerenciamento de políticas, detecção de ameaças e resposta a incidentes.

O Cisco Identity Services Engine é uma solução abrangente que fornece acesso seguro a endpoints fornecendo serviços de autenticação, autorização e responsabilidade (AAA) e aplicação de políticas.

O Platform Exchange Grid (pxGrid) permite que você troque informações entre redes de vários fornecedores e várias plataformas.

Essa integração permite que você obtenha monitoramento seguro, detecção de ameaças e o conjunto de políticas de rede com base nas informações compartilhadas.

A estrutura do PxGrid tem duas versões. A que deve ser usada depende da versão e do patch do ISE que você precisa revisar.

Começando com a versão ISE 3.1, todos os pxGas conexões de RID do ISE são baseadas na versão pxgrid 2.

PxGrid versão 1.

TA primeira versão deste framework (pxGrid v1) é caracterizado devido à facilidade de manutenção observada através do comando show application status ise conforme exibido na saída subsequente.

Quando o recurso pxGrid estiver habilitado no nó, você verá o pxGrid recursos em um status de execução.

```
ise/admin# show application status ise
ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3688
Database Server                        running          41 PROCESSES
Application Server                     running          6041
Profiler Database                      running          4533
AD Connector                           running          6447
M&T Session Database                   running          2363
M&T Log Collector                      running          6297
M&T Log Processor                      running          6324
Certificate Authority Service          running          6263
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
Identity Mapping Service               disabled
```

Manutenção do PxGrid versão 1.

Nessa versão dessa plataforma, sabe-se que há apenas um nó pxGrid com os processos pxGrid em status de execução, enquanto os outros nós pxGrid estão em status de espera.

Esses nós monitoram constantemente o status do nó pxGrid com os serviços relacionados em execução.

Nesse caso, o nó principal do pxGrid era uma promoção e o outro nó do pxGrid ativava seus serviços do pxGrid.

No entanto, isso representou um tempo de inatividade quando esse failover ocorreu.

A primeira versão do pxgrid foi baseada na comunicação no Extensible Messaging and Presence Protocol (XMPP), que é um conjunto de tecnologias usadas na infraestrutura de colaboração e voz.

Os tópicos compartilhados em uma conexão pxGrid v1 são:

- Diretório da sessão
- Metadados de Perfil de Ponto de Extremidade
- Metadados Trustsec
- Recurso de proteção de endpoint
- Controle de rede adaptável
- Tópico MDM_Offline
- Identidade
- SXP

PxGrid versão 2.

Este documento aborda o uso do PxGrid versão 2. Esta plataforma opera usando operações

REST em protocolos ISE e WebSocket que trazem aprimoramentos, melhor escalabilidade, desempenho e flexibilidade em modelos de dados.

Nesta versão, você não vê os recursos do pxgrid sendo executados como na versão anterior com o comando show application status ise.

Consulte a seção de validação do ISE neste documento para saber quais mecanismos devem ser verificados para revisar a funcionalidade do pxGrid.

Com esta versão, você tem todos os nós pxGrid configurados como nós pxGrid ativos. Estão prontos para participar no intercâmbio de informações a qualquer momento.

Na versão 1, apenas um nó mantinha a capacidade de serviço do pxGrid como em execução.

Os tópicos compartilhados em uma conexão pxGrid v2 são:

- Diretório da sessão
- Falha de raio
- Configuração do Profiler
- Integridade do Sistema
- MDM
- Status do ANC
- TrustSec
- Configuração do TrustSec
- TrustSec SXP
- Ativo de endpoint.

Componentes do pxGrid como plataforma.

Controlador PxGrid (ISE): Cada um dos participantes que usam pxGrid deve ser confiável.

Cliente: Pode ser assinante e editor de diferentes tópicos.

Editor: Cliente que compartilha informações com o controlador.

Assinante: Cliente que consome as informações de um tópico.

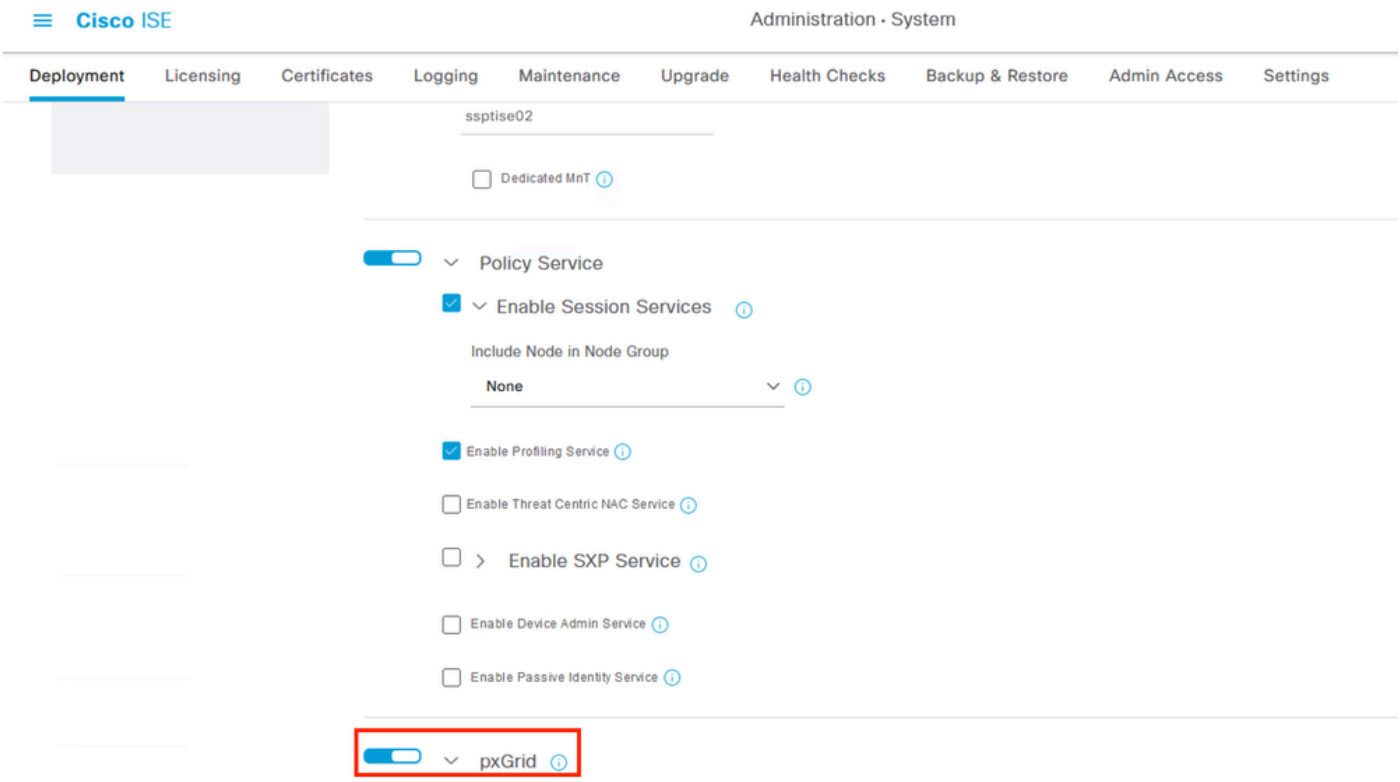
Essa integração permite criar políticas de conteúdo no FMC com base nas informações compartilhadas pelo ISE e nos tópicos publicados (relacionados à atividade de endpoint).

Configurar

Prepare o ISE para a integração.

Etapa 1. Configure o nó ISE para executar o pxGrid persona nele no menu Administração > Sistema > Implantação.

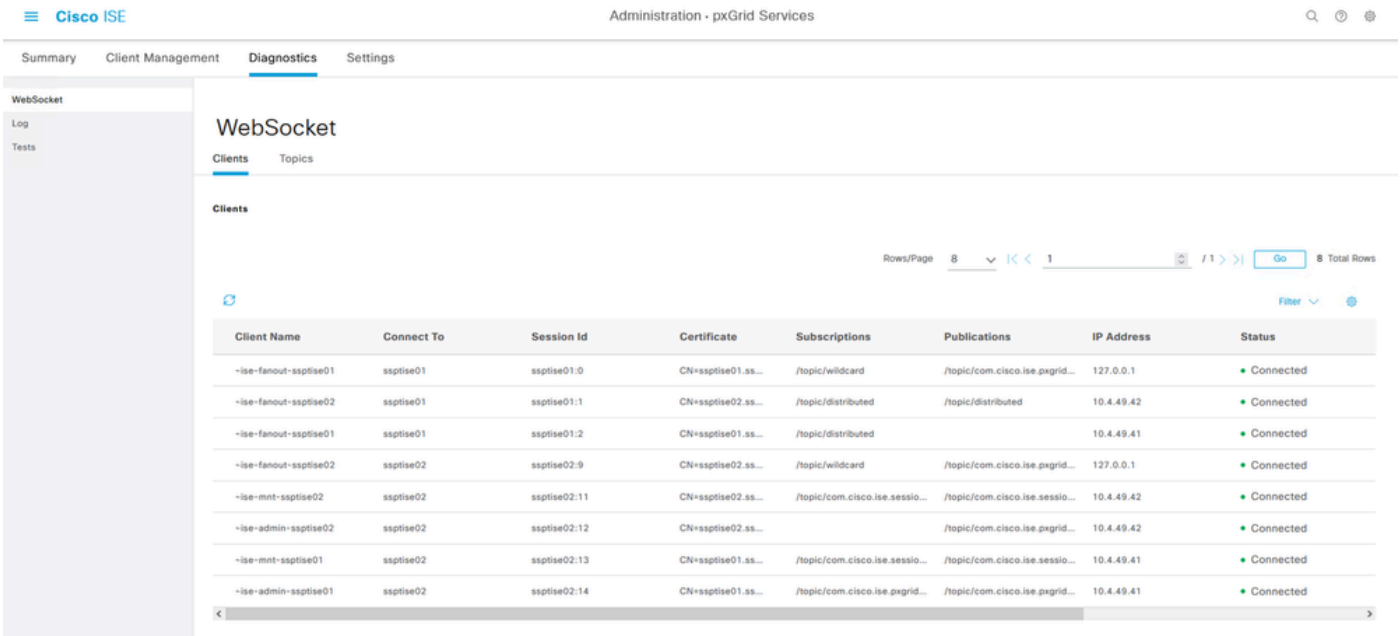
Selecione os nós e ative o recurso pxGrid.



Habilitando serviços pxGrid do ISE em um nó.

Etapa 2. Depois de ativar os nós com o recurso pxGrid, revise o status dos Websockets relacionados aos clientes internos conectados.

Navegue até Administration > pxGrid Services > Websocket. Observe os clientes que apontam para os serviços do ISE diretamente através do endereço IP 127.0.0.1.

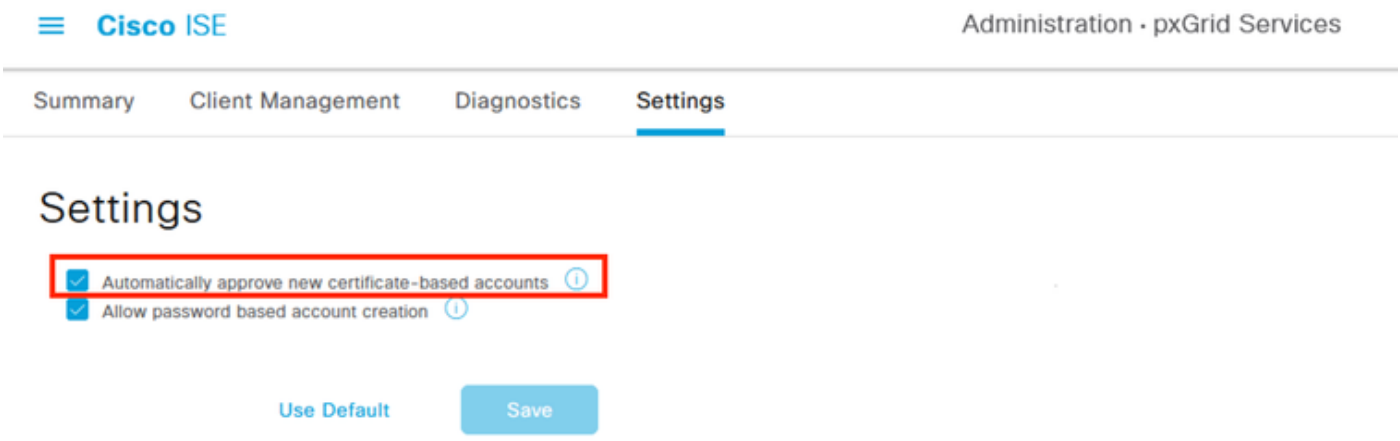


WebSockets internos do ISE.

Etapa 3. Navegue pelo menu Administration > pxGrid Services > Settings e selecione a opção para Aprovar automaticamente novas contas de base de certificado,

Essa etapa é opcional neste ponto, no entanto, para a conexão pxGrid, é recomendável ativar essa caixa de seleção.

Você pode aceitar o FMC como assinante manualmente depois.

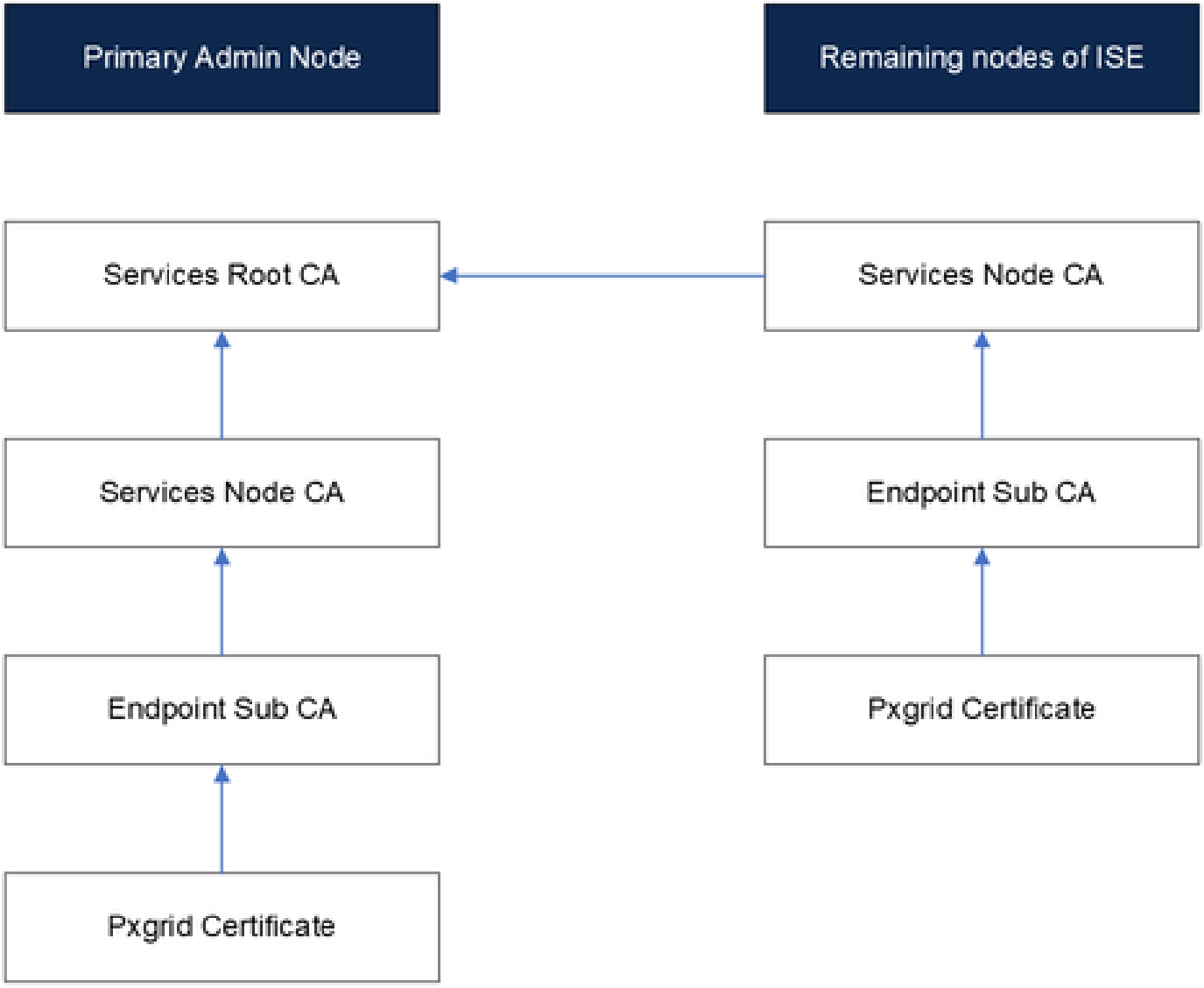


Habilitando a aprovação automática para contas baseadas em certificado pxGrid.

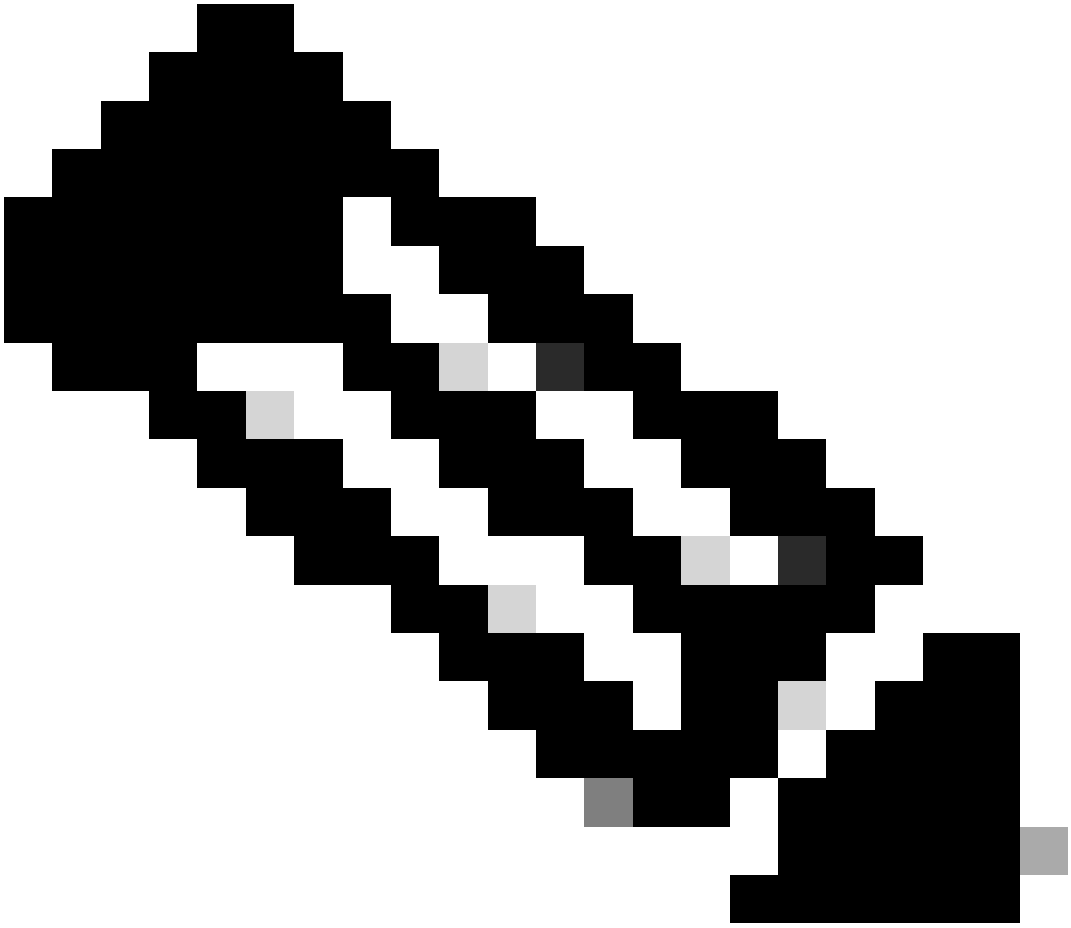
Etapa 4. Revise os certificados relacionados à funcionalidade do pxGrid de seu ambiente em Administração > Sistema > Certificados do Sistema,

É recomendável que você tenha certificados pxGrid homogêneos em todos os nós de sua implantação assinados pela mesma CA raiz

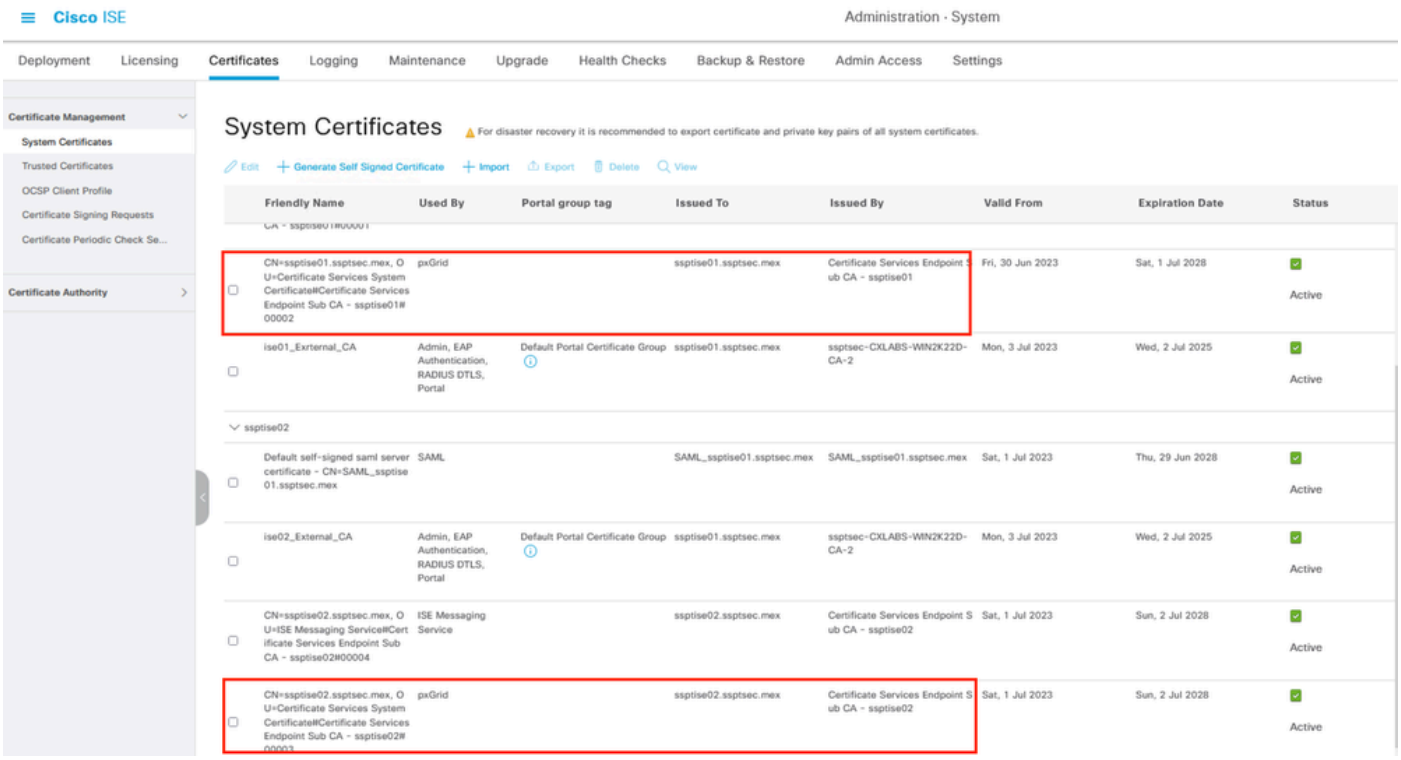
Neste cenário, estamos usando os certificados internos do ISE gerados. Para esta versão do ISE, onde neste exemplo, a CA raiz corresponde ao nó PAN.



Certificados internos do diagrama no ISE.



Note: Para obter mais informações sobre a estrutura interna de certificados gerados no ISE, consulte Compreender os serviços de autoridade de certificação interna do ISE.

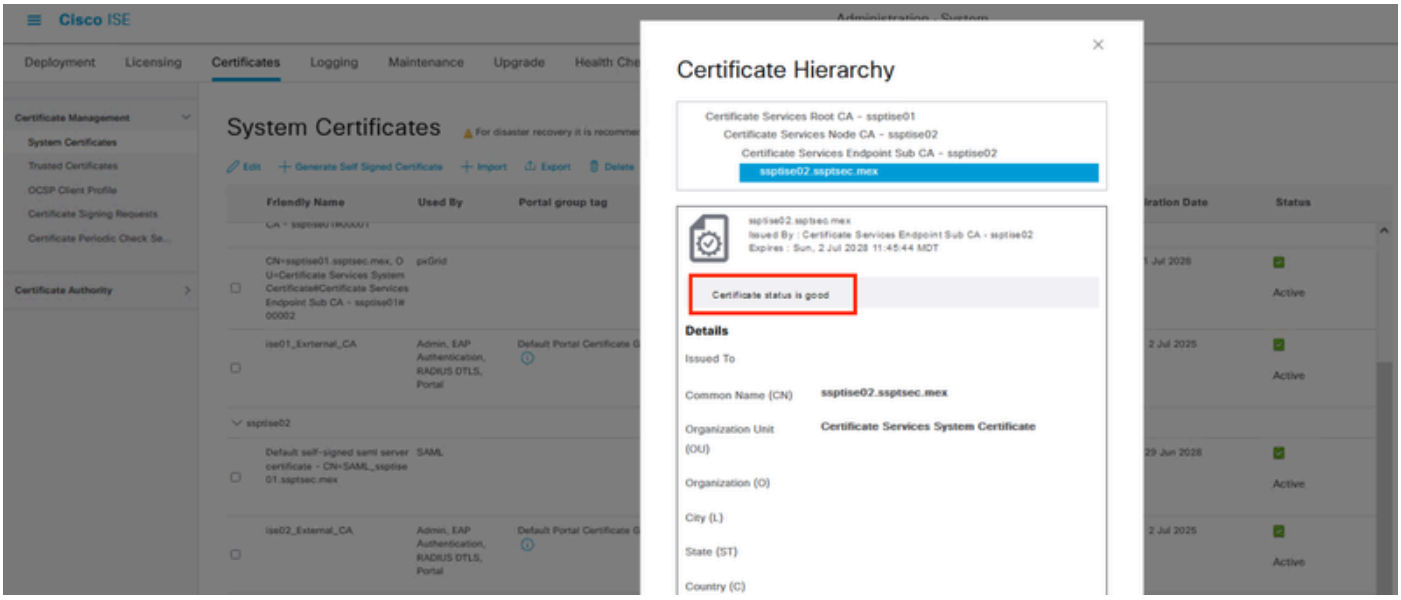


Certificados PxGrid em uma implantação distribuída.

Etapa 5. Verifique o status dos certificados pxGrid.

No menu anterior, marque uma caixa de seleção de um certificado pxGrid de nó e, em seguida, selecione a opção Exibir.

A saída se parece com a exibida aqui nos certificados pxGrid.

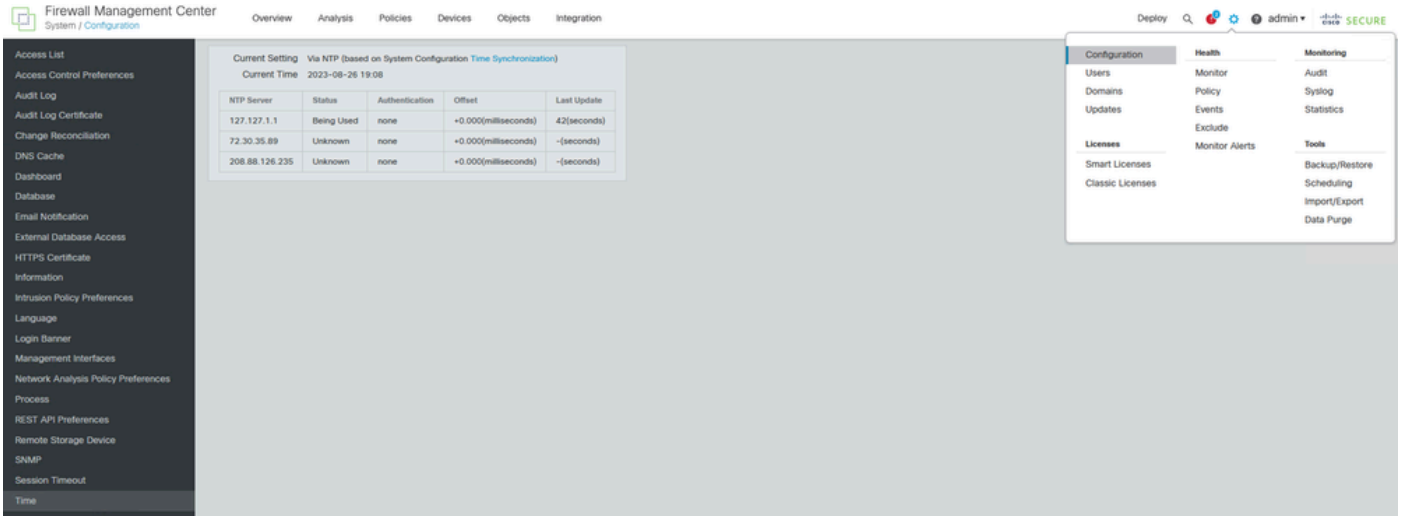


Verificação do certificado pxGrid.

Preparar o CVP para a integração.

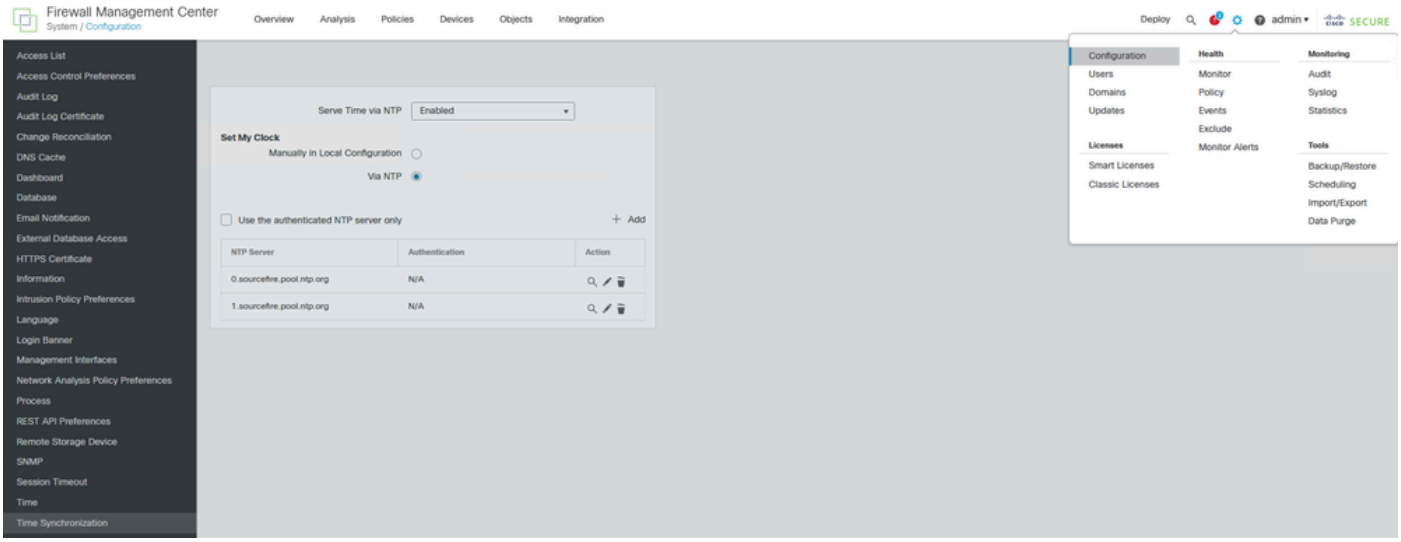
Etapa 1.Confirme se a hora interna do FMC está atualizado.

Navegue até Sistema > Configuração > Tempo e garantir que o tempo configurado no CVP atualizado.



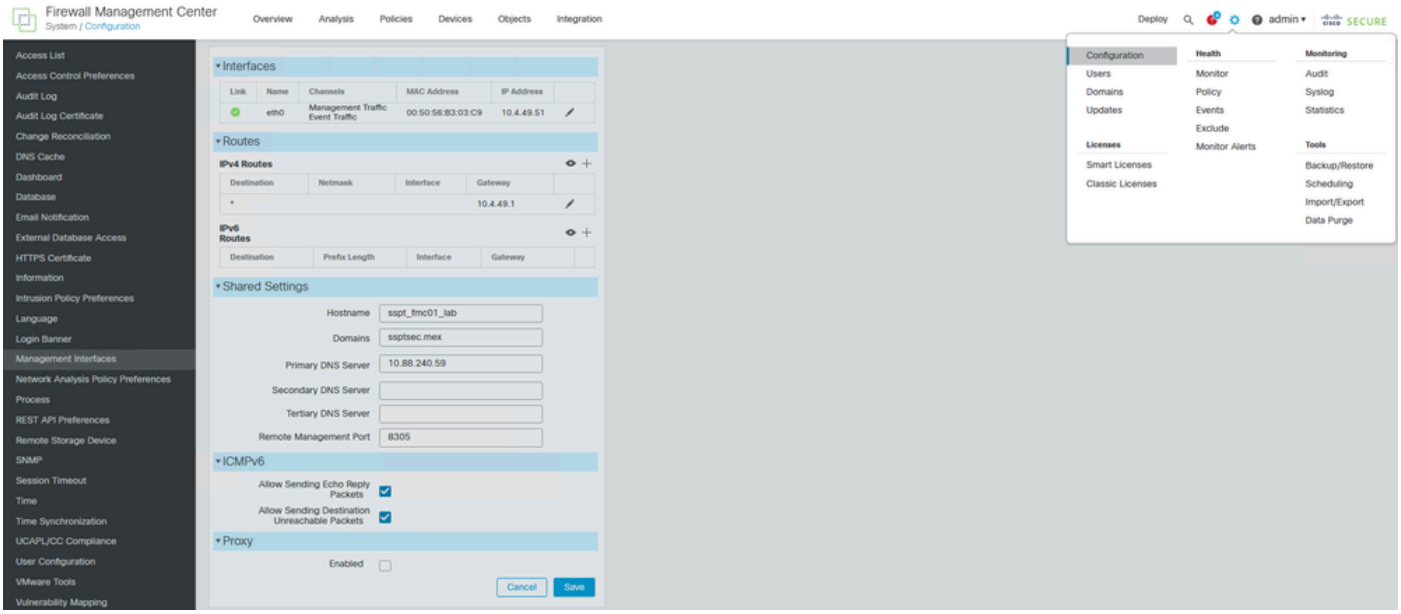
Verificação da atualização do CVP.

Se a hora do FMC não for atualizada, verifique se o NTP está configurado corretamente e in Sync. O NTP pode ser configurado em Sistema > Configuração > Tempo > + Adicionar.



Time Synchronization on FMC (Sincronização de horário no FMC).

Etapa 2. Navegue até Sistema > Configuração > Interface de gerenciamento > Configurações compartilhadas e verificar se pelo menos Servidor DNS primário campo contém um IP do servidor DNS.



Configuração DNS no FMC.

Etapa 3. Confirme se o nome de host FMC está configurado.

Navegue até Sistema > Configuração > Interface de Gerenciamento > Configurações Compartilhadas e verificar se Hostname contém o nome de host do FMC.

Você pode verificar esta etapa ao revisar a etapa anterior nesta seção .

Configurando a conexão pxGrid entre o ISE e o FMC.

Etapa 1. Navegue até o menu Administration > pxGrid Services > Client Management > Certificates.

Na primeira opção, selecione Desejo gerar um único certificado (sem uma solicitação de assinatura de certificado).

Na seção Nome comum (CN), introduza o FQDN do CVP em que o ISE emitirá um certificado.

Forneça uma Descrição.

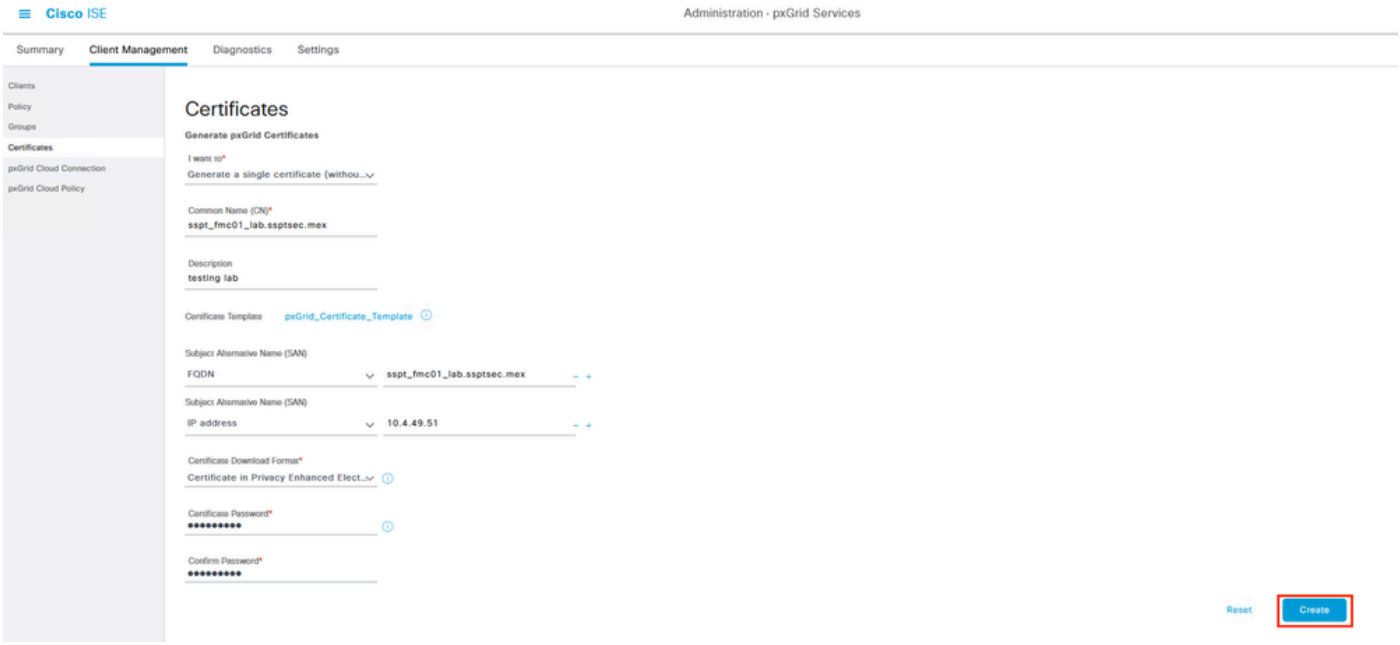
Na seção Nome alternativo do assunto (SAN), insira o FQDN e o endereço IP do FMC para conexão.

Na parte inferior do Formato de Download do Certificado, selecione no menu suspenso a opção Certificado no formato Privacy Enhanced Electronic Mail (PEM).

Insira o formato PKCSS PEM (incluindo a cadeia de certificados).

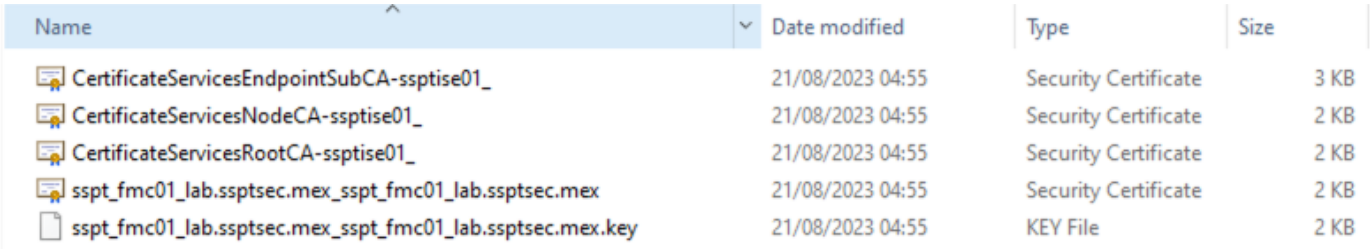
Insira e armazene uma senha em Certificate Password ao usá-la posteriormente no FMC.

Confirme a senha e selecione Create.



Exemplo de geração de certificado pxGrid.

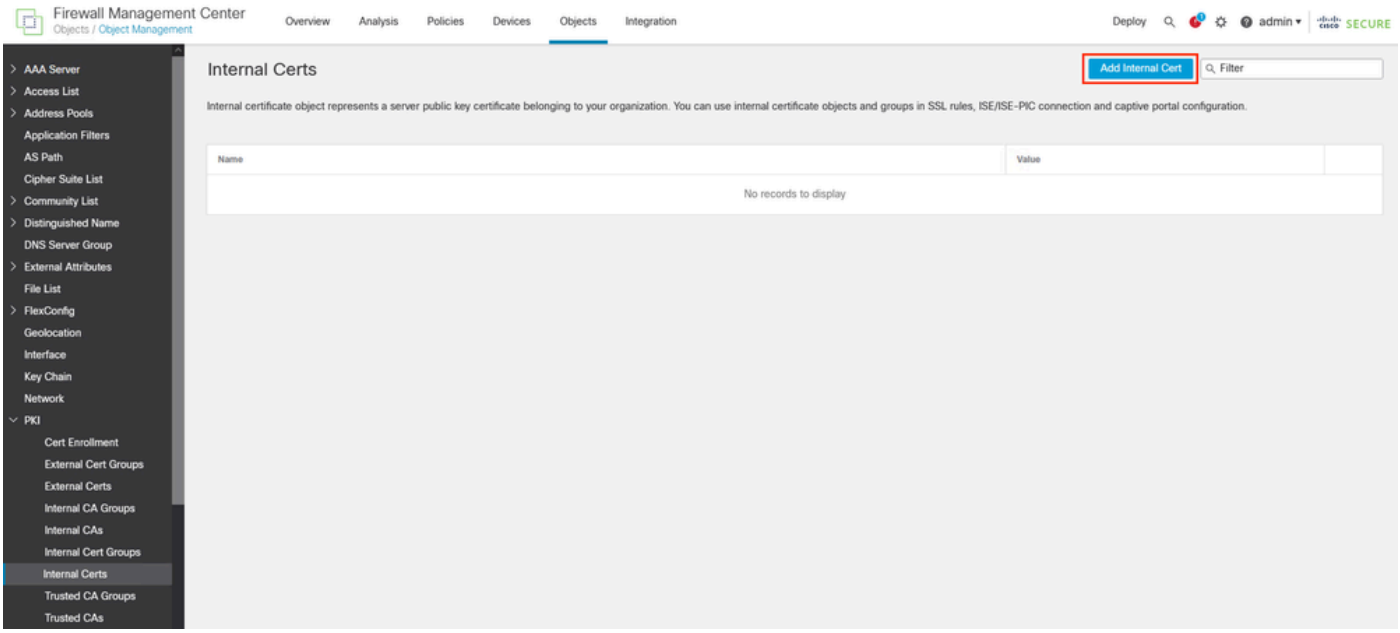
Etapa 2. É feito o download de um arquivo zip em seu computador. Descompacte o arquivo e confirme se você tem estes arquivos do seu ambiente:



Certificados PxGrid gerados pelo ISE.

Etapa 3. No FMC, navegue até o menu Objetos > Gerenciamento de objetos > PKI > Certificados internos.

Selecione a opção Add Internal Cert.



Acrescentar o certificado FMC como certificado interno.

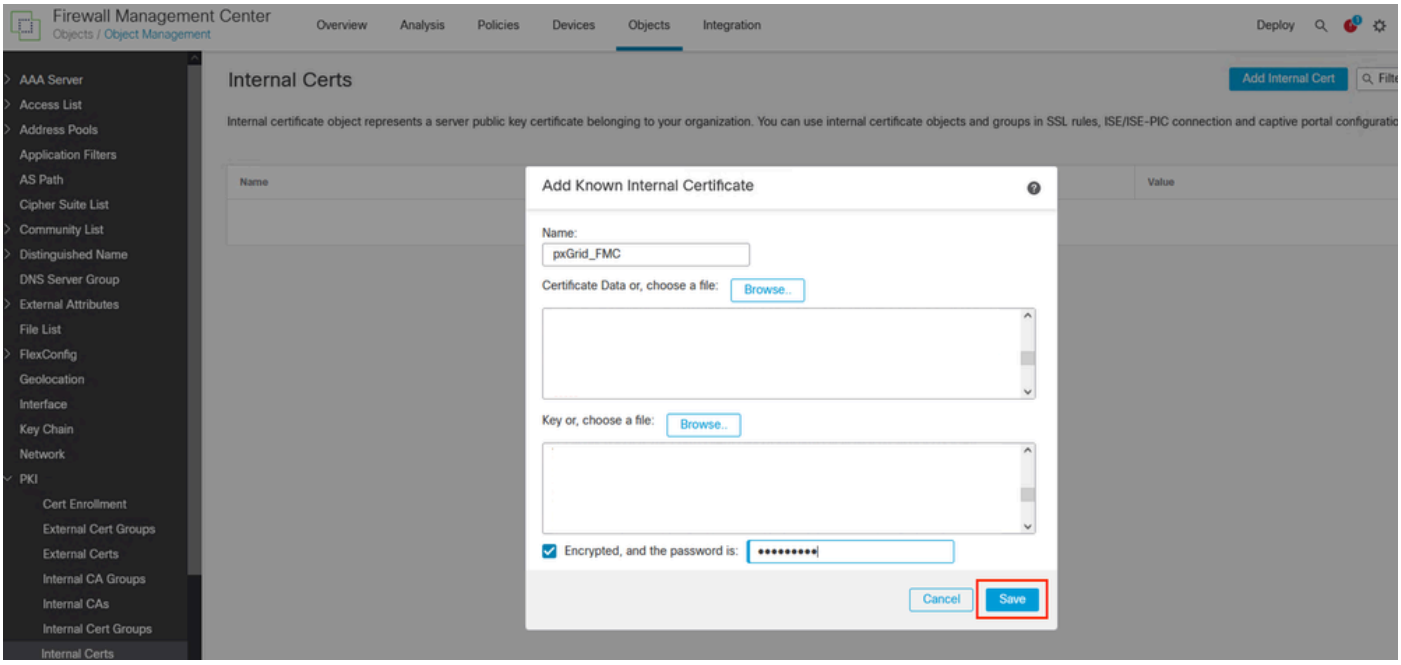
Etapa 4. Nomear o certificado que está alocado no FMC.

Procure o certificado criado para o FMC no ISE na seção Dados do certificado.

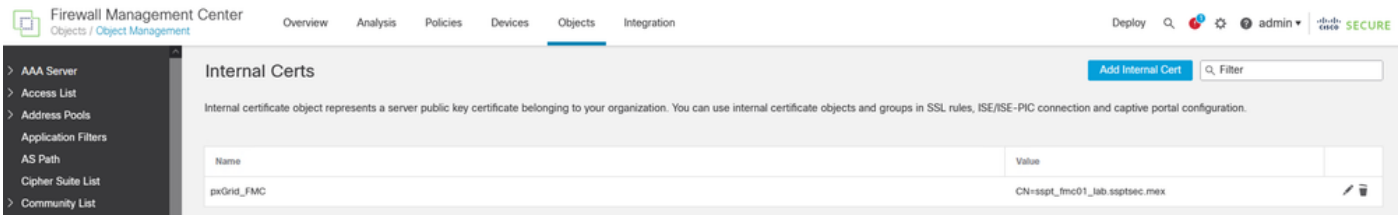
Procure o arquivo com a extensão .key para preencher o próximo campo.

Selecione a opção Encrypted e insira a senha que você usou quando criou o certificado no ISE.

Salve a configuração.



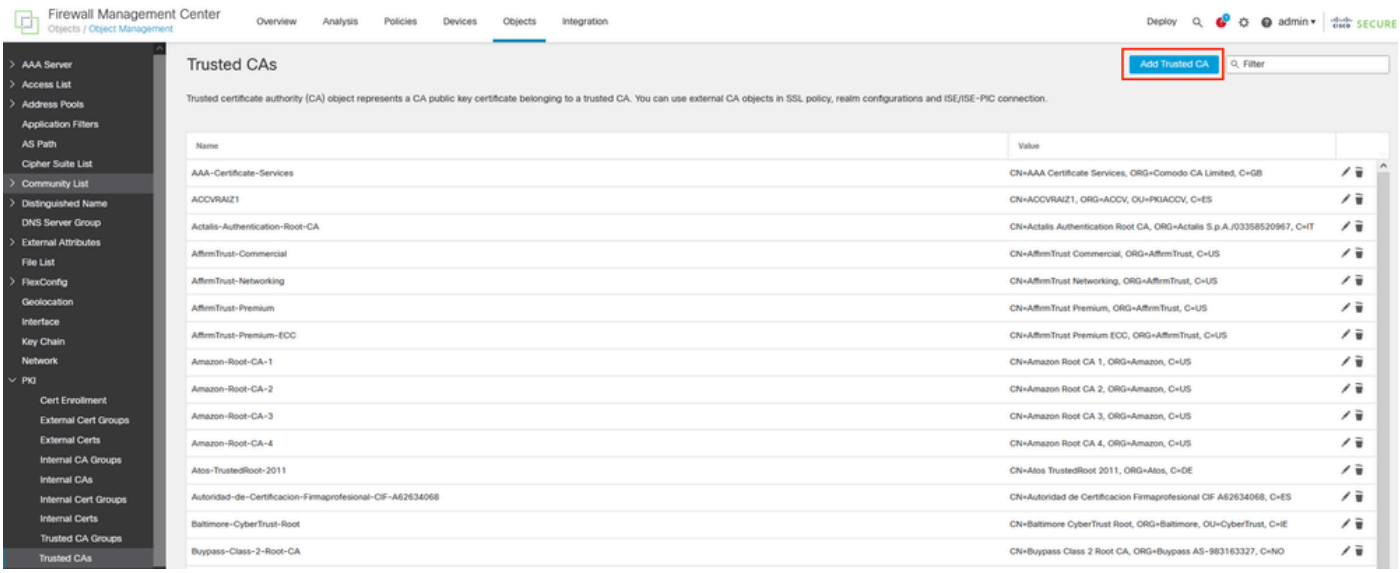
Exportando o certificado FMC gerado pelo ISE.



Certificado FMC.

Etapa 5. Navegue até o menu Objetos > Gerenciamento de objetos > PKI > CAs confiáveis,

Selecione Adicionar CAs confiáveis.

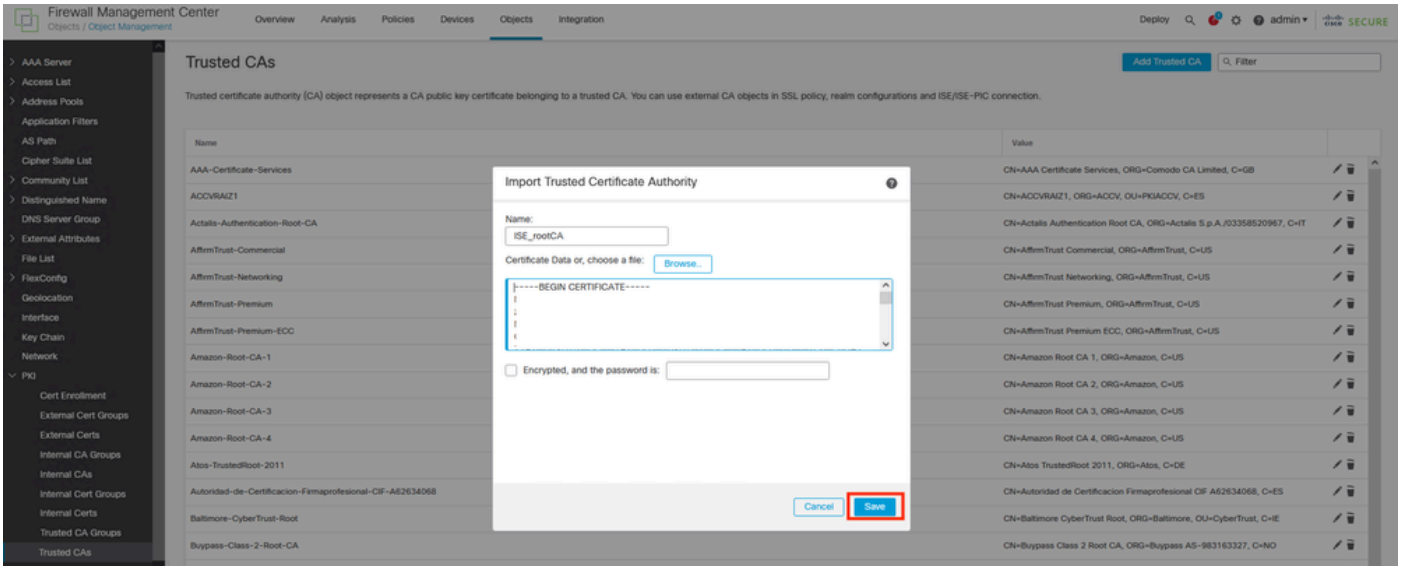


Adicionando a rootCA do ISE como certificado confiável.

Etapa 6. Nomeie a Autoridade de Certificação.

Procure e selecione o rootCA do ISE que foi baixado do arquivo do ISE.

Salve sua configuração.



Exportando o rootCA do ISE.

Etapa 7. Navegue até o menu Integração > Outras integrações > Origens de identidade.

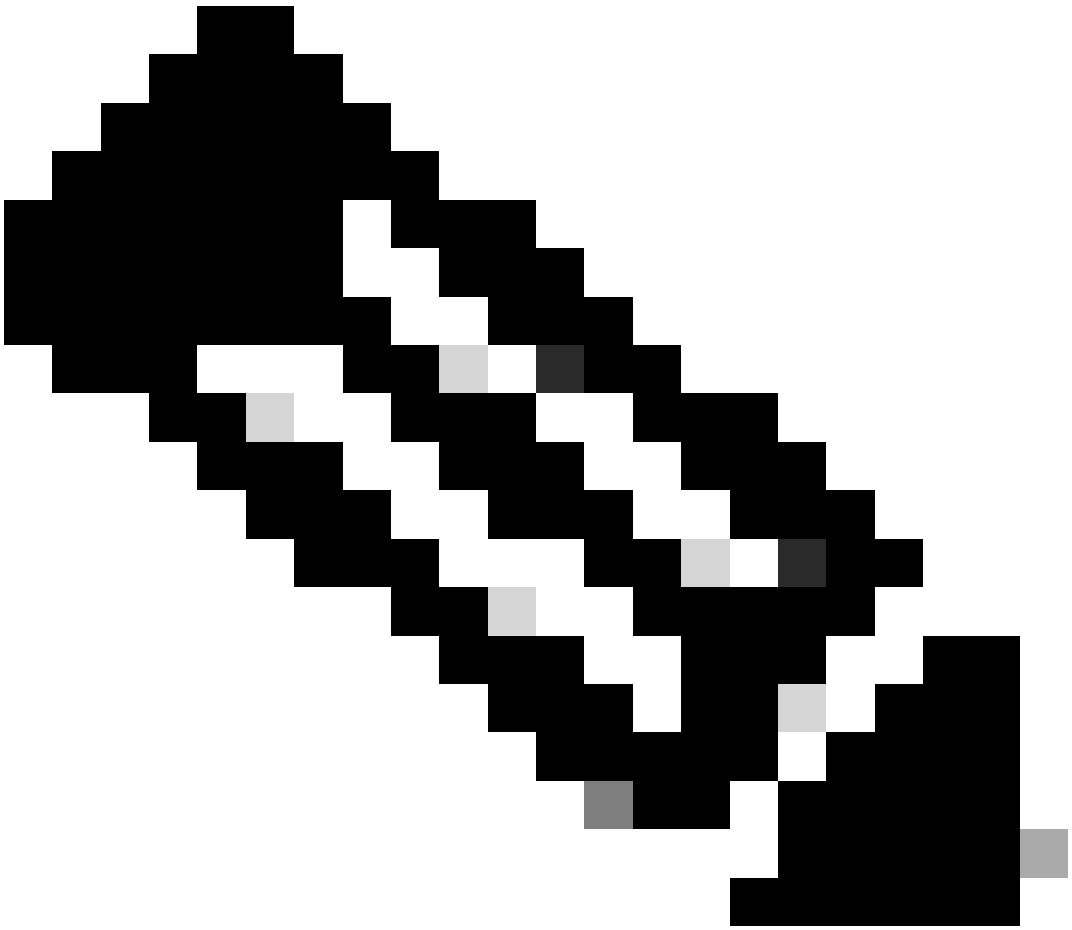
Selecione em Tipo de serviço: Identity Services Engine,

Insira o endereço IP ou o FQDN do nó pxGrid que se tornará o nó primário.

Repita o procedimento para o nó pxGrid secundário.

Selecione, no menu suspenso, o certificado pxGrid gerado pelo ISE para a seção pxGrid Client Certificate,

Na seção MNT Server CA e pxGrid Server CA, selecione a rootCA do ISE que você exportou na última etapa.

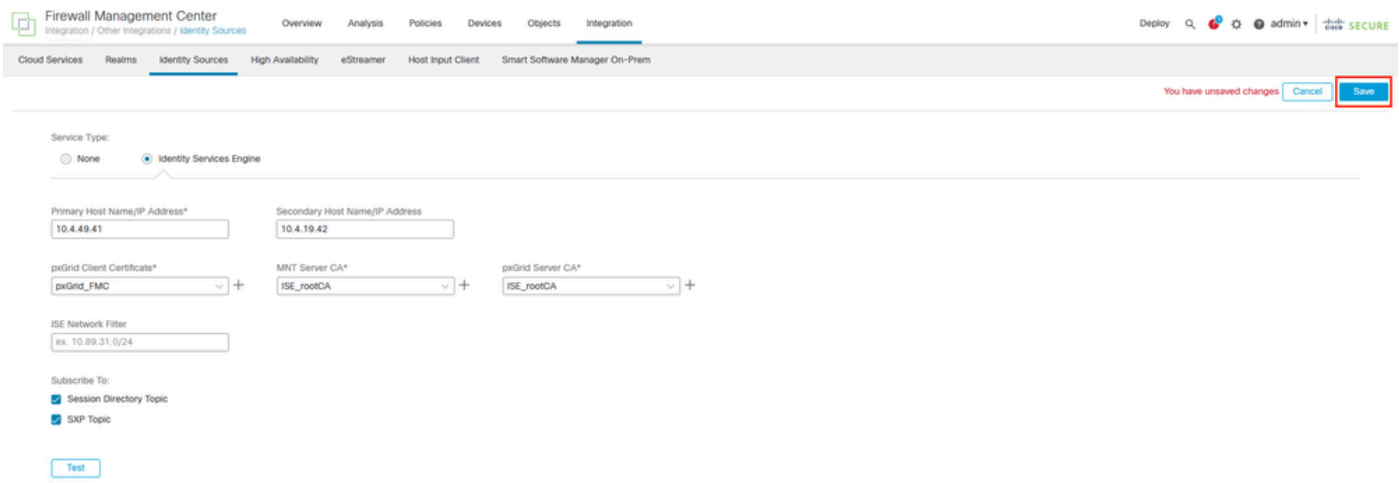


Note: A CA do servidor pxGrid corresponde à Autoridade de certificação raiz do certificado que está sendo usado pelo pxGrid nos nós pxGrid.

A CA do servidor MNT corresponde à Autoridade de certificação do certificado que está sendo usado pelo pxGrid nos nós MNT.

(Opcional) Você pode assinar o Diretório de sessão e o tópico do SXP no ISE.

Salve a configuração.

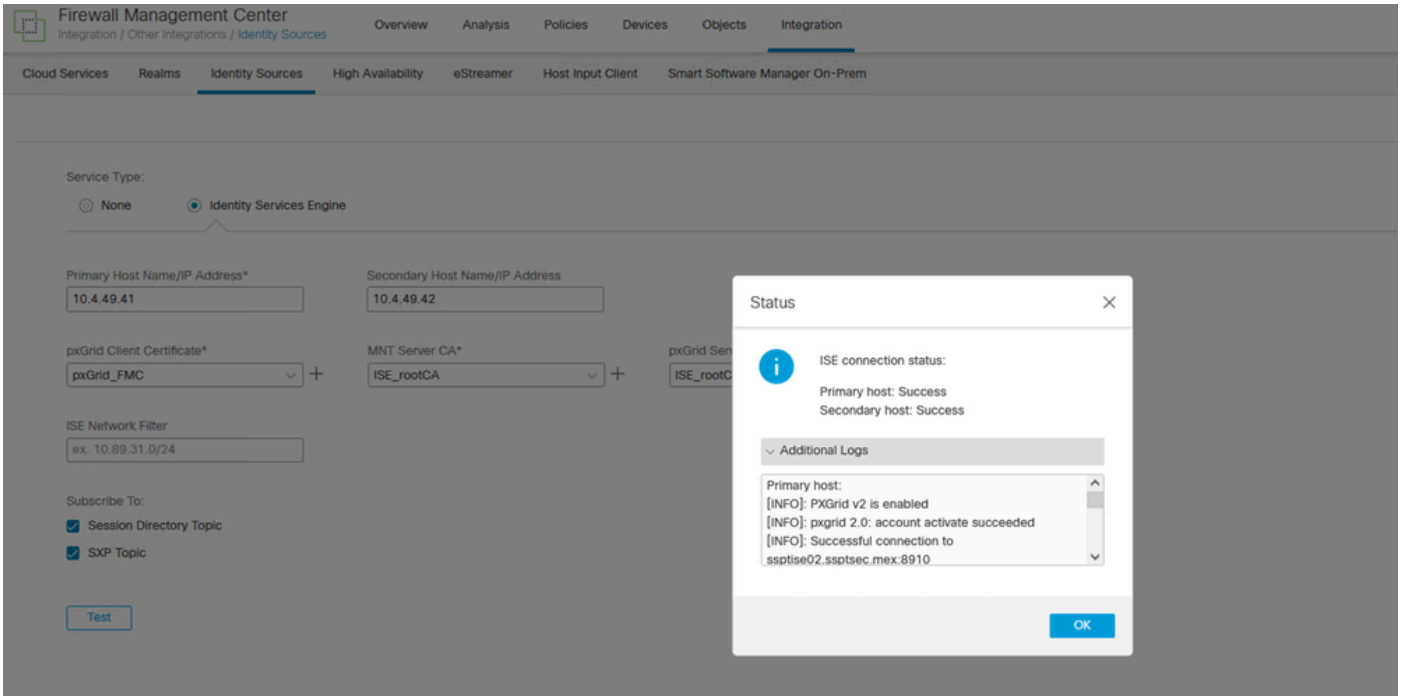


Configuração do ISE como fonte de identidade no FMC.

Verificar.

Validação no CVP.

No menu, navegue para Integração > Outras integrações > Origens de identidade > Identity Services Engine antes de salvar sua configuração. Você pode testar as configurações do link pxGrid.



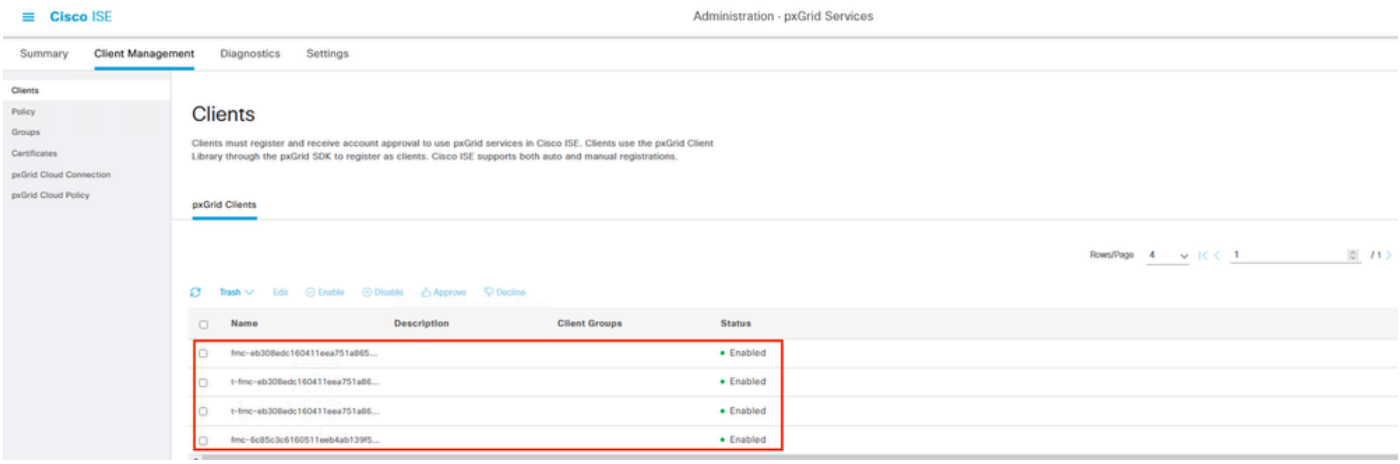
Comunicação bem-sucedida do PxGrid.

```
Primary host:
```

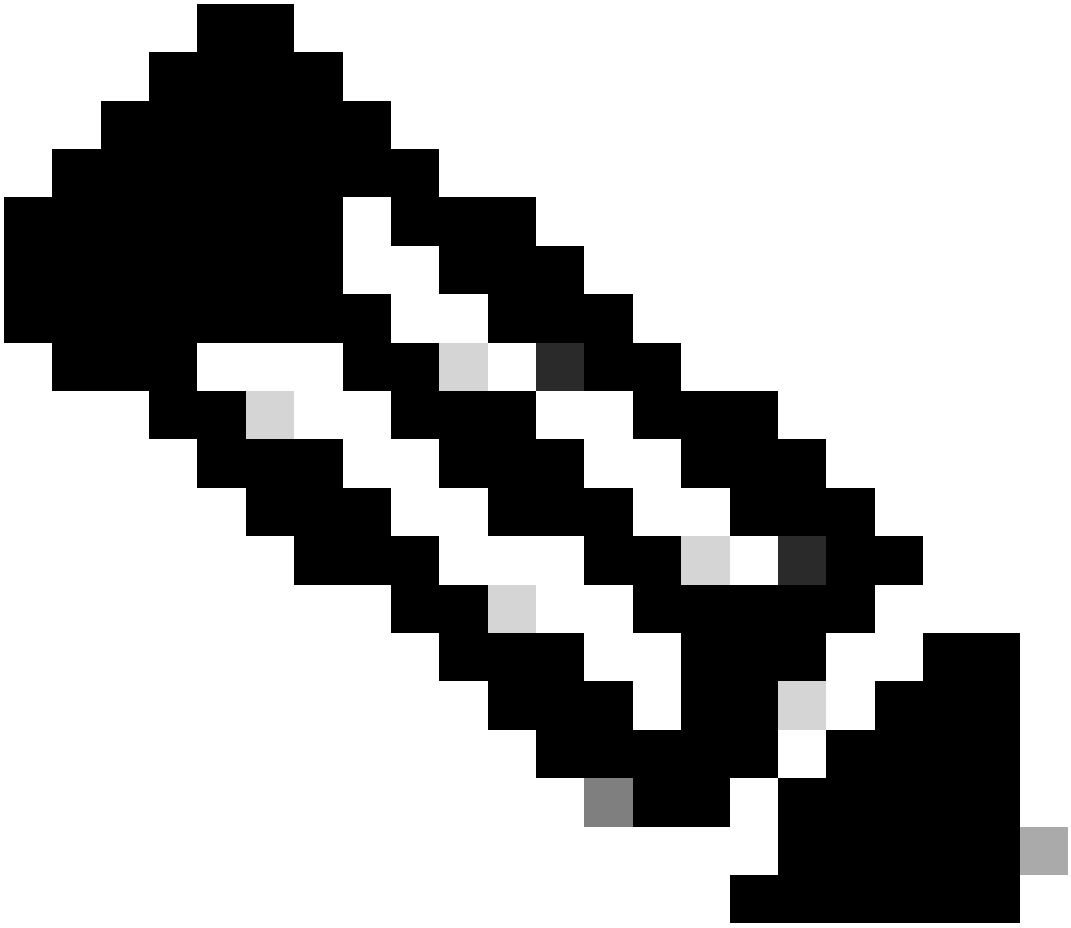
```
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetw
[INFO]: All requested ISE Services are online.

Secondary host:

[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetw
[INFO]: All requested ISE Services are online.
```

Validação no ISE.

Quando o cliente pxGrid do FMC tiver sido integrado com êxito ao ISE, você em seguida, consulte (no Administração > pxGrid Services > Gerenciamento de clientes > Clientes) clientes com o nome fmc estão incluídos e habilitado.



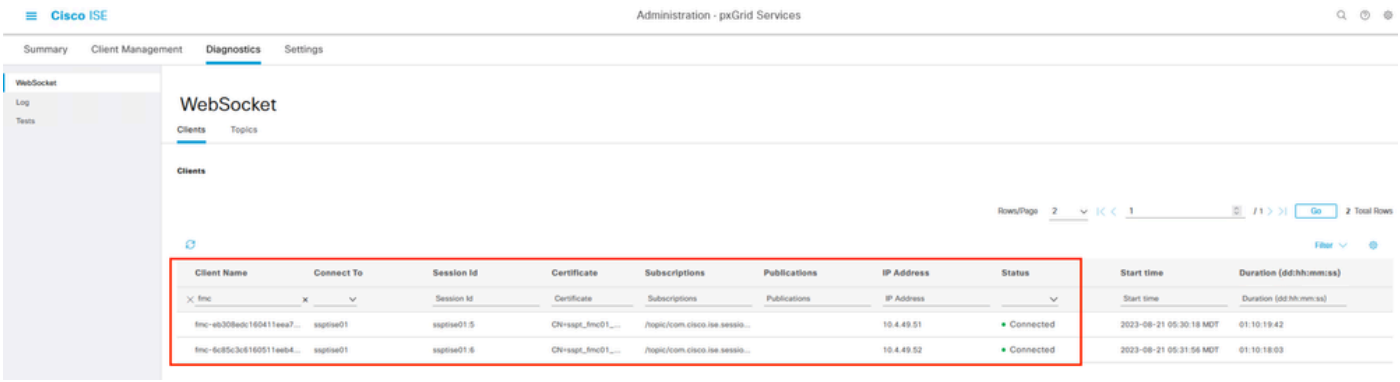
Clientes PxGrid disponíveis e ativados.



Note: Os clientes pxGrid cujo prefixo começa com "t-fmc" são aqueles usados através do botão de teste do FMC.

Além disso, se você navegar para o menu Administration > pxGrid Services > Diagnostics > WebSocket, você verá a conexãos para a CVP.

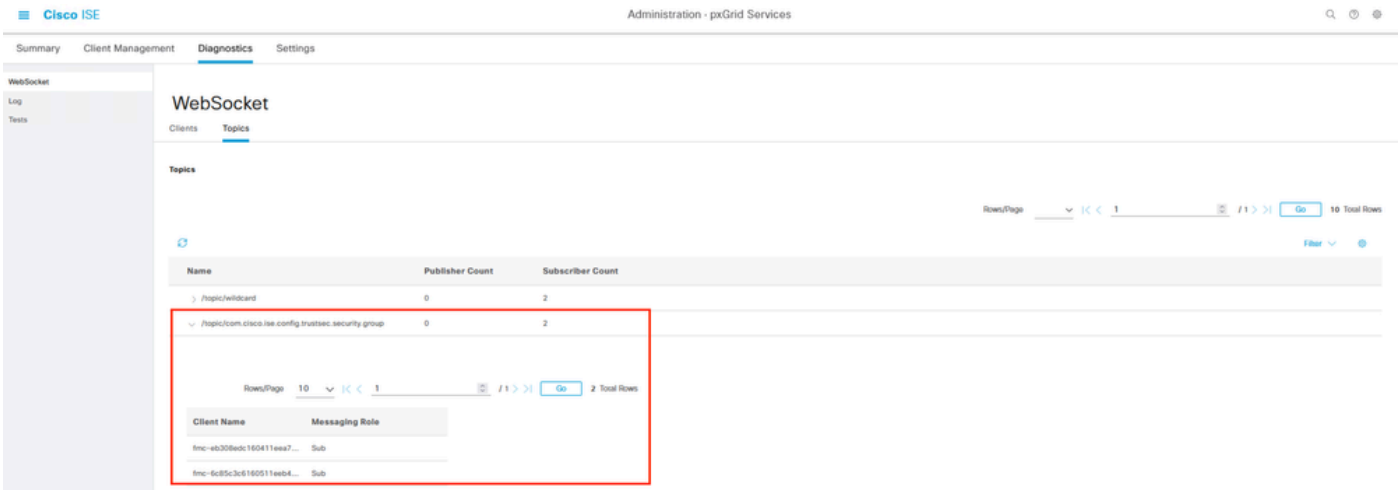
No cenário em que você tem o FMC em alta disponibilidade, você verá então as unidades principal e secundária como são exibidas neste exemplo:



WebSockets disponíveis no ISE.

Na próxima guia neste menu nomeado Tópicos, você pode verificar se os assinantes do FMC foram adicionados aos tópicos pxGrid publicados pelo ISE.

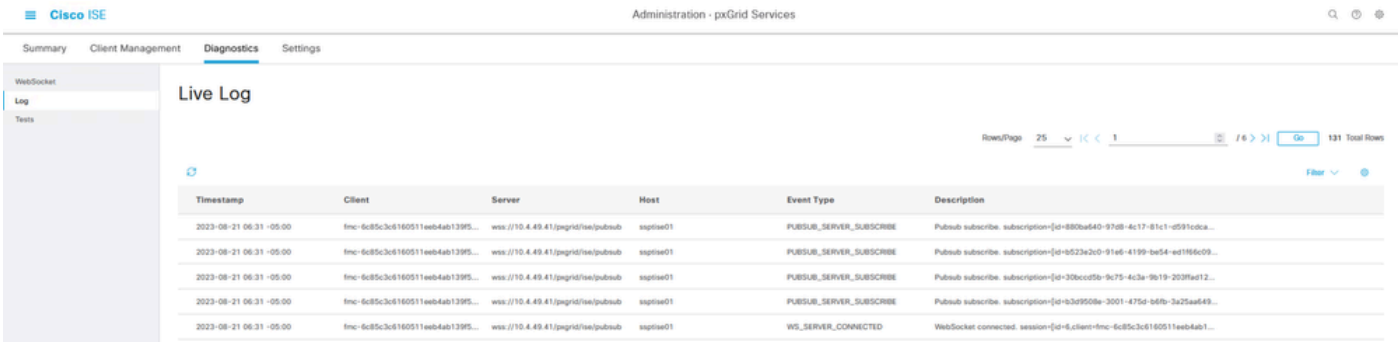
Por exemplo, há um tópico relacionado ao grupo de segurança de where você podem ver que ambos os CVP são assinados e recebem informações relacionadas para SGT postado pelo ISE.



Tópicos por assinante do pxGrid.

INo menu Administration > pxGrid Services > Diagnostics > Log, eventos importantes relacionados na comunicação pxGrid (para os nós com o recurso habilitado habilitado) são exibidos.

Eles retratam as informações relacionadas à integração.



Logs ao vivo do PxGrid.

Troubleshooting

Solução de problemas no FMC.

Confirme se o FMC pode resolver seu próprio nome de host e nós do ISE por nomes de host.

Por exemplo:

<#root>

```
> expert
admin@sspt_fmc01_lab:~$ ping sspt_fmc01_lab

PING sspt_fmc01_lab (10.4.49.51) 56(84) bytes of data.
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=3 ttl=64 time=0.055 ms
^C
--- sspt_fmc01_lab ping statistics ---
```

3 packets transmitted, 3 received,

```
 0% packet loss, time 27ms

admin@sspt_fmc01_lab:~$ ping ssptise01
PING ssptise01.ssptsec.mex (10.4.49.41) 56(84) bytes of data.
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=2 ttl=64 time=0.646 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=3 ttl=64 time=0.743 ms
^C
--- ssptise01.ssptsec.mex ping statistics ---
```

3 packets transmitted, 3 received,

```
 0% packet loss, time 82ms
rtt min/avg/max/mdev = 0.586/0.658/0.743/0.068 ms
admin@sspt_fmc01_lab:~$
admin@sspt_fmc01_lab:~$ ping ssptise02

PING ssptise02.ssptsec.mex (10.4.49.42) 56(84) bytes of data.
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=2 ttl=64 time=0.609 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=3 ttl=64 time=0.628 ms
^C
--- ssptise02.ssptsec.mex ping statistics ---
```

3 packets transmitted, 3 received

```
, 0% packet loss, time 45ms
rtt min/avg/max/mdev = 0.588/0.608/0.628/0.025 ms
```

Assegure que O processo ADI está ativo e em execução:

<#root>

>

expert

sudo suadmin@sspt_fmc01_lab:~$

sudo su

root@sspt_fmc01_lab:/Volume/home/admin#

pmtool status | grep adi

adi (normal) - Running 7911

EAssegurar que a comunicação entre o CVP e o port O TCPP 8910 é permitido. Do CVP CLI podemos configurar a tcpudump captura de pacotes para confirmar a comunicação bidirecional.

<#root>

>

expert

sudo suadmin@sspt_fmc01_lab:~$

sudo su

root@sspt_fmc01_lab:/Volume/home/admin#

tcpdump -i any tcp and port 8910

22:34:08.415370 IP

sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910

: Flags [S], seq 3033526171, win 29200, options [mss 1460,sackOK,TS val 2701166399 ecr 0,nop,wscale 7],
22:34:08.415840 IP

ssptise01.ssptsec.mex.8910 > sspt_fmc01_lab.46248

: Flags [S.], seq 3024877968, ack 3033526172, win 28960, options [mss 1460,sackOK,TS val 2268665064 ecr
22:34:08.415894 IP

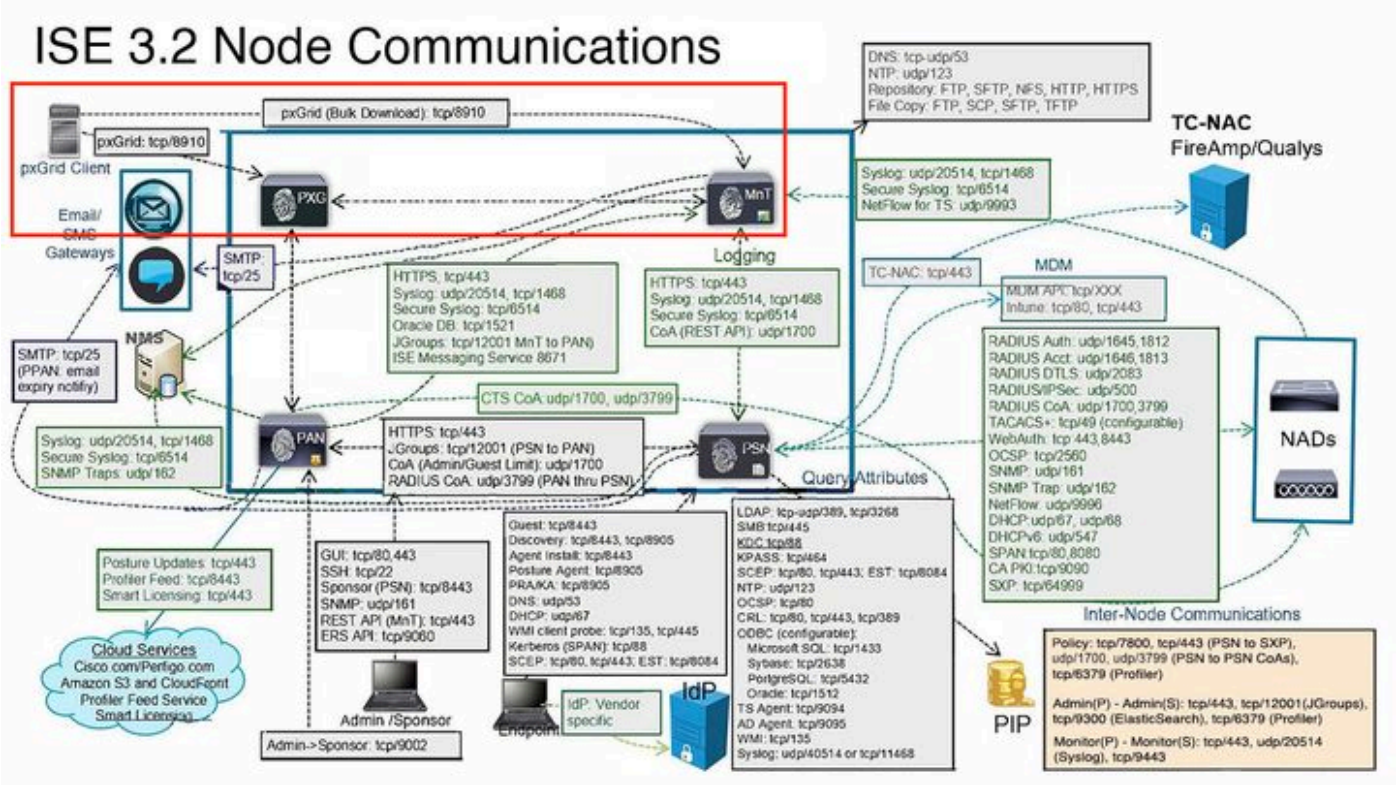
sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910

: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0
[...]

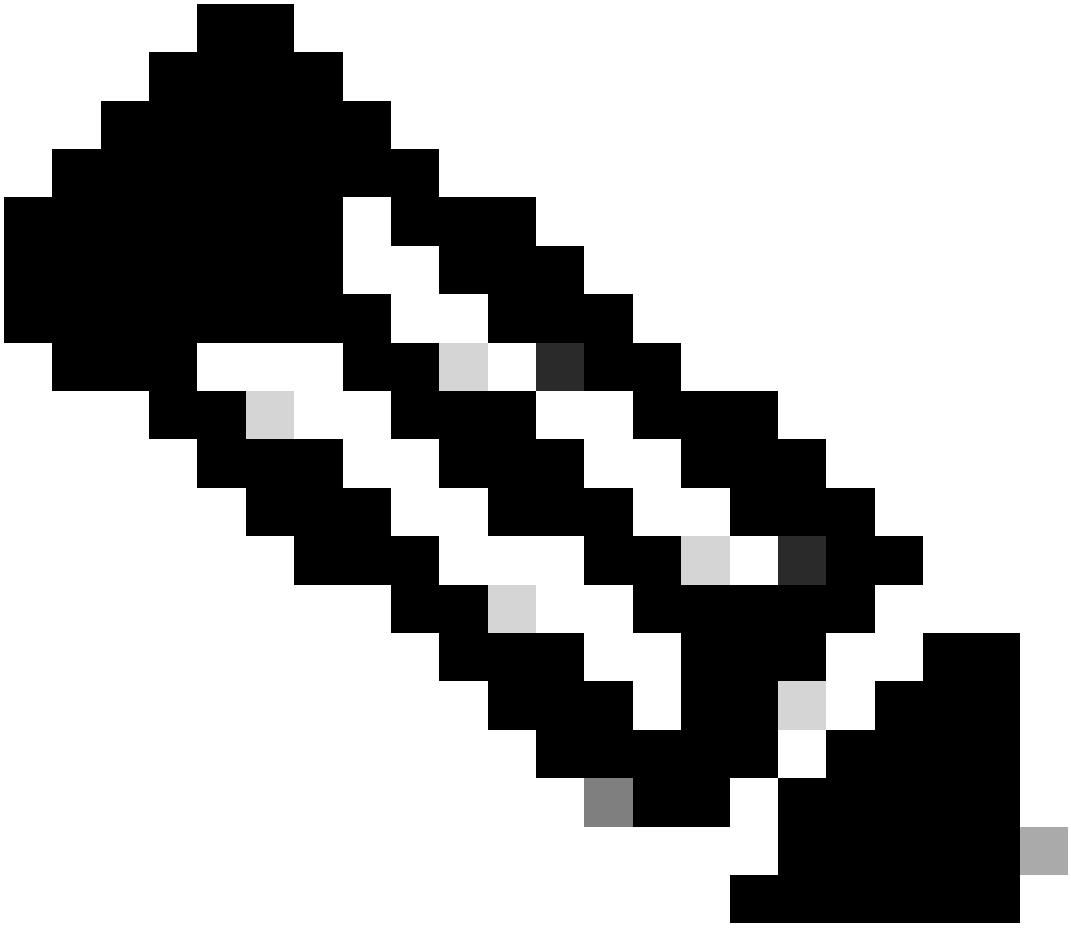
Solução de problemas no ISE.

Verifique se as comunicações na porta 8910 está operacional.

Esta é a porta usada pelo cliente pxGrids para se comunicar com nós pxGrid e nós MnT para o download em massa de informações.



Interação do PxGrid no ambiente ISE.



Note: O cliente pxGrid, nesse caso o FMC se comunica com os nós pxGrid e o nó MNT secundário (SMNT) para obter o (Download em massa) das informações. Em caso de falha no SMNT, ele procura as informações por meio do MNT primário.

INos nós do ISE onde a comunicação com o cliente pxGrid é mantida, você pode revisar se a a porta está aberta ou se houver soquetes conectados a naquela porta.

```
#show ports | include 8910
tcp: (output omitted), :::8910,
```

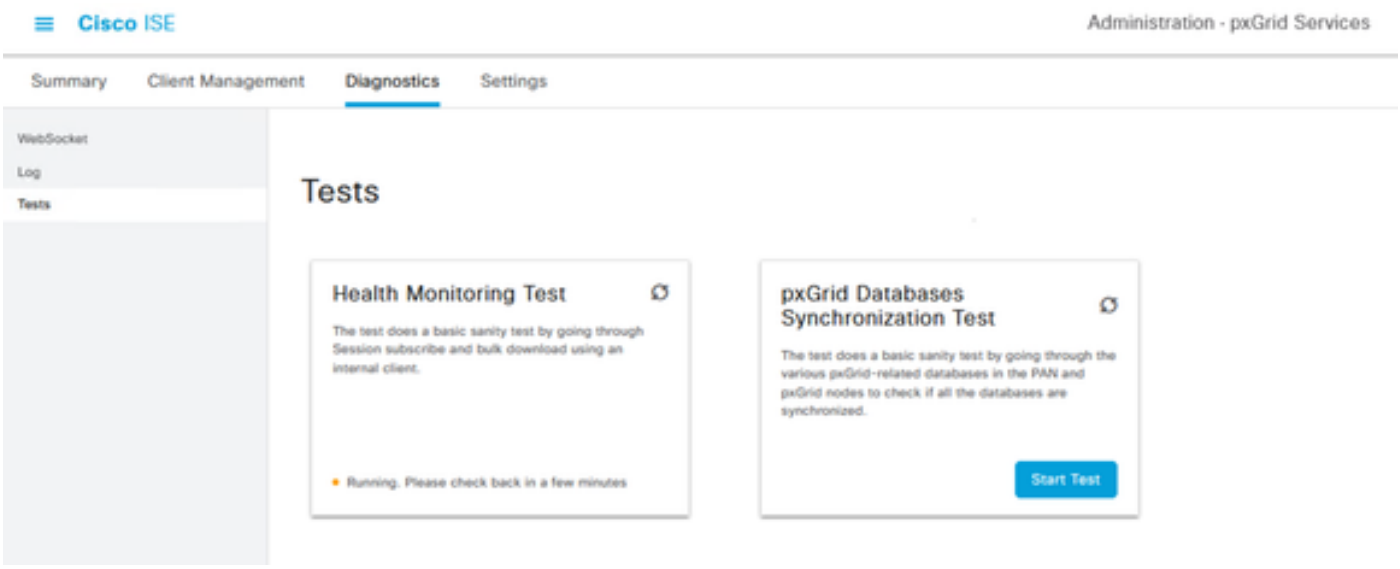
Há dois testes disponíveis no ISE que diagnosticam o status geral das implementações do pxGrid.

Eles podem ser encontrados no menu Administração > Serviços do pxGrid > Diagnóstico > Teste.

Os testes exibidos nesta seção são executados internamente no ISE.

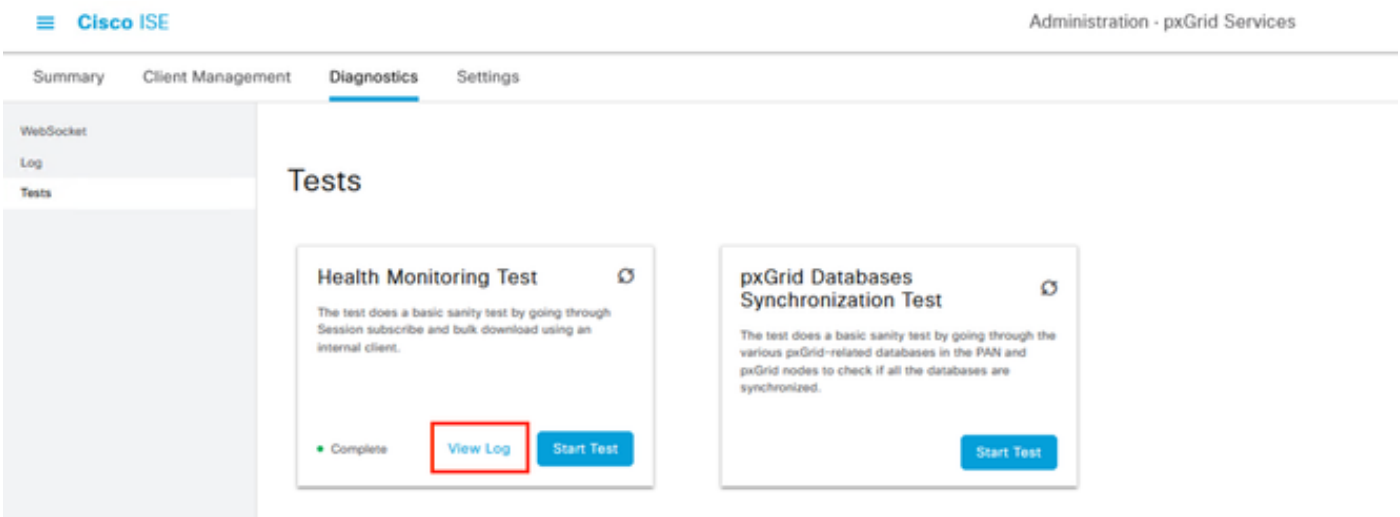
Teste de Monitoramento de Integridade analisa a aparência do serviço pxGridup, que avalia se um cliente pode acessar o Diretório de sessão, o serviço e os tópicos publicados pelo controlador pxGrid.

Selecione a opção opção Iniciar Teste e aguarde até que os logs sejam coletados.



PxGrid Health Monitoring Test (Teste de monitoramento de integridade do PxGrid).

Após a conclusão do teste, selecione a opção opção Exibir log. Para este exemplo, o conteúdo do log é:



Revisão do teste de monitoramento de integridade.

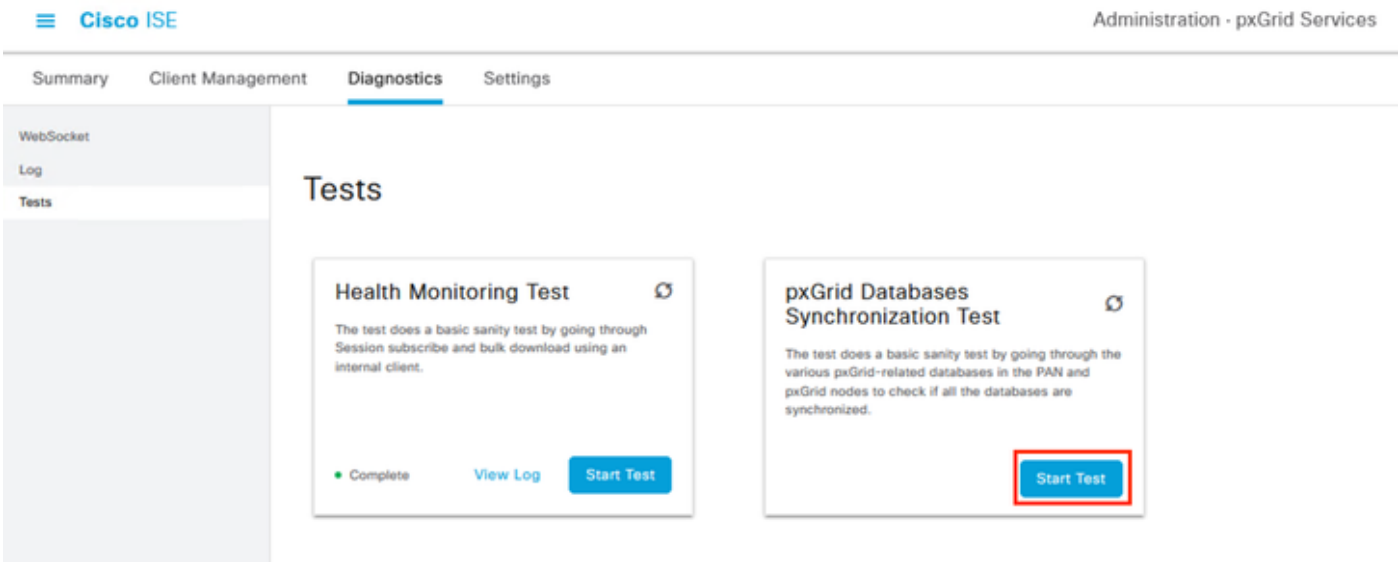
```
22-Aug-2023 17:03:13 [INFO] ************** pxGrid Session Directory Test ***************
22-Aug-2023 17:03:13 [INFO] ----------------- Starting Connection Test -----------------
22-Aug-2023 17:03:14 [INFO] pxGrid Node: ssptise01.ssptsec.mex
22-Aug-2023 17:03:14 [INFO] wsPubsubServiceName=com.cisco.ise.pubsub
22-Aug-2023 17:03:14 [INFO] sessionTopic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:14 [INFO] sessionRestBaseUrl=https://ssptise01.ssptsec.mex:8910/pxgrid/mnt/sd
22-Aug-2023 17:03:14 [INFO] wsUrl=wss://ssptise02.ssptsec.mex:8910/pxgrid/ise/pubsub
```

```
22-Aug-2023 17:03:15 [INFO] ---------------- Connection Test Completed ----------------
22-Aug-2023 17:03:15 [INFO] ------------------ Starting Download Test ------------------
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions read: 0
22-Aug-2023 17:03:15 [INFO] ------------------ Download Test Completed ------------------
22-Aug-2023 17:03:15 [INFO] ------------------ Starting Subscribe Test ------------------
22-Aug-2023 17:03:16 [INFO] STOMP CONNECT host=ssptise02.ssptsec.mex
22-Aug-2023 17:03:16 [INFO] STOMP SUBSCRIBE topic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:16 [INFO] STOMP CONNECTED version=1.2
22-Aug-2023 17:07:16 [INFO] A total of 0 notifications were received.
22-Aug-2023 17:07:16 [INFO] STOMP RECEIPT id=77
22-Aug-2023 17:07:19 [INFO] ------------------ Subscribe Test Completed ------------------
22-Aug-2023 17:07:19 [INFO] ********** pxGrid Session Directory Test Complete **********
```

O teste de sincronização de banco de dados do PxGrid verifica se as informações dentro dos bancos de dados está correto entre os nós PAN e pxGrid e sincronizado.

Portanto, as informações enviadas aos assinantes do pxGrid são precisa.

Selecione a opção opção Iniciar teste e esperar que os resultados venham a ser avaliados.



Teste de sincronização de bancos de dados PxGrid.

A partir dos registros gerados, essa saída foi obtida.

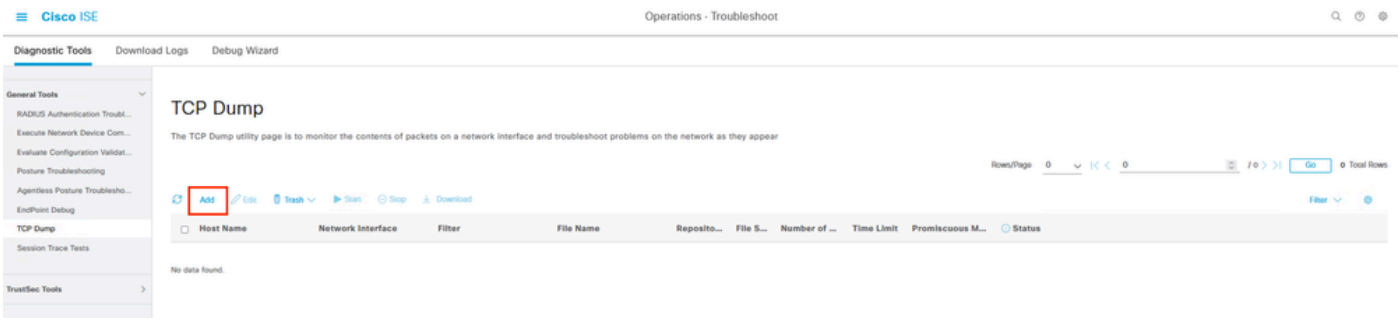
```
ssptise01.ssptsec.mex : In Sync
ssptise02.ssptsec.mex : In Sync

Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex
```

Coletar uma captura em a partir dos nós pxGrid apontando em direção ao nó FMC primário.

Navegar até o menu Operações > Solução de Problemas > Ferramentas de Diagnóstico >

Despejo TCP,

Selecione a opção opção para adi uma nova captura.



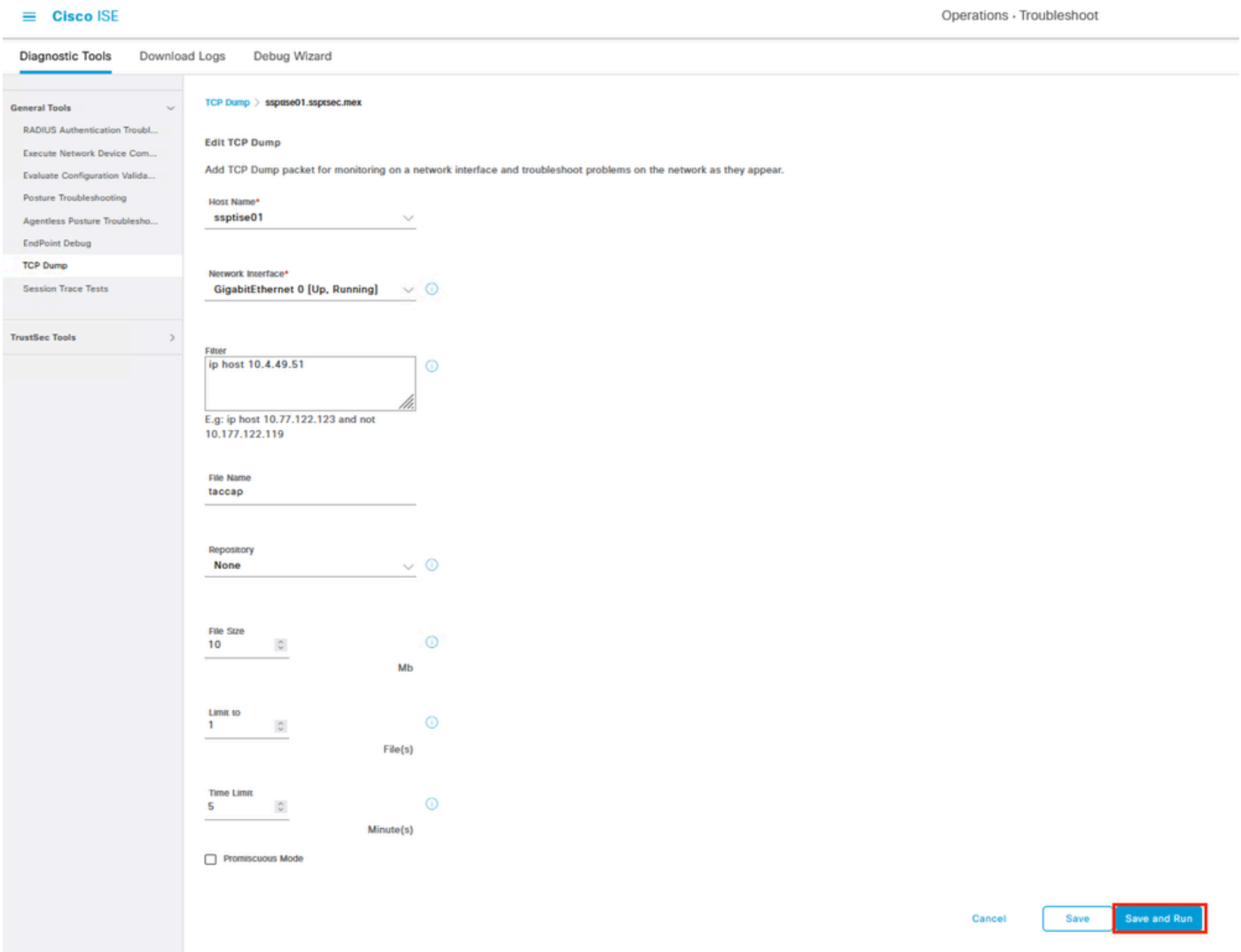
Gerando uma captura de pacote no ISE.

Configure os parâmetros para a captura.

IN Nome de Host, selecione o nó pxGrid primário selecionado no FMC.

Filtrar o tráfego com este sintaxe ip host <FMC IP>

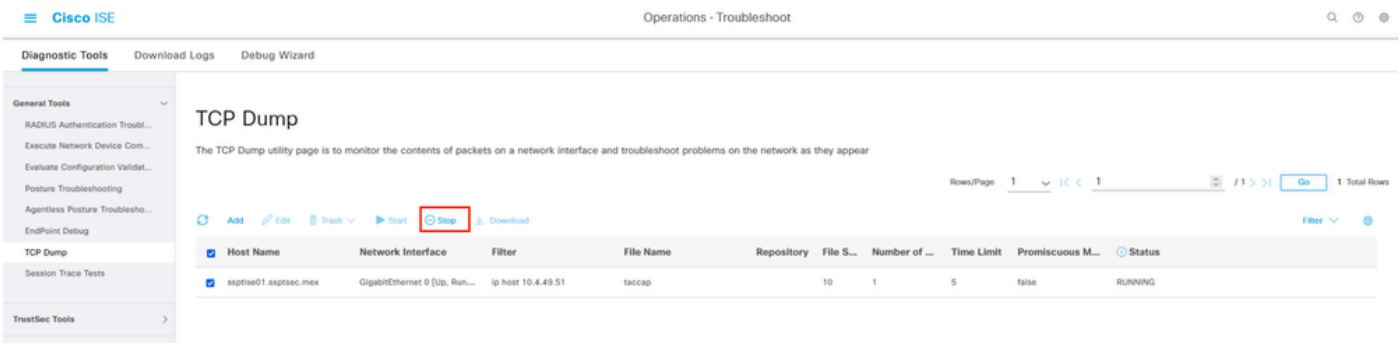
Nomear a captura e depois continuar para Save e Executar.



Exemplo de configuração de captura de pacotes.

Em outra janela, no menu FMC Integração > Outras integrações > Identidade Origens, Teste a conexão com o ISE através do canal pxGrid.

WQuando você obtém o resultado do teste, continuar para Ssuperior a captura no ISE.



Interrompendo uma captura de pacote no ISE.

Download a captura e iniciar a análise. Este cenário exibe uma captura de uma conexão em funcionamento que pode servir como referência.

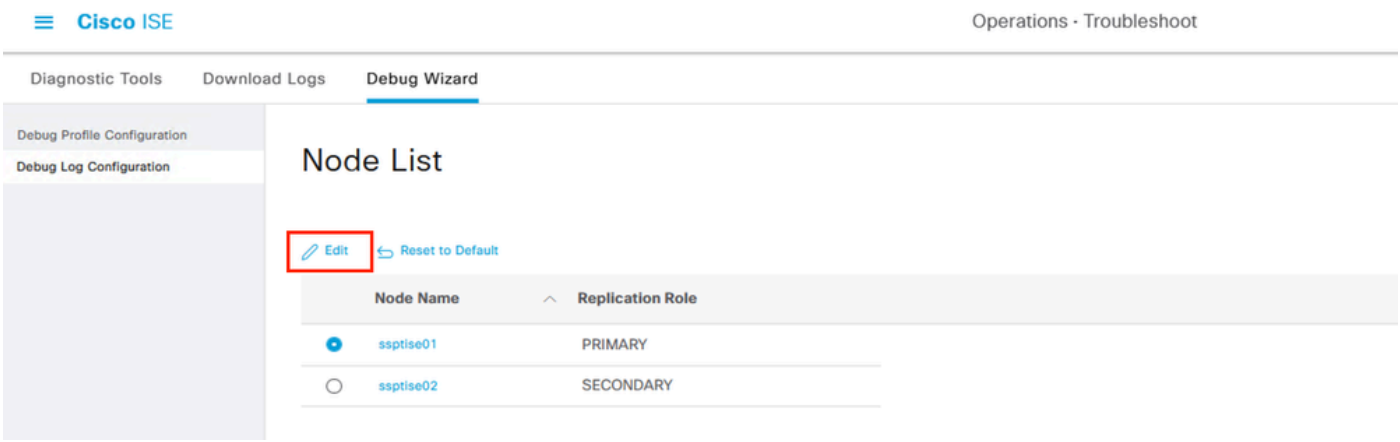
```
10.4.49.51      10.4.49.41      TCP       74 47508 → 8910 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=2738457626 TSecr=0 WS=128
10.4.49.41      10.4.49.51      TCP       74 8910 → 47508 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=2305956319 TSecr=2738457626 WS=128
10.4.49.51      10.4.49.41      TCP       66 47508 → 8910 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2738457627 TSecr=2305956319
10.4.49.51      10.4.49.41      TLSv1.2  389 Client Hello
10.4.49.41      10.4.49.51      TCP       66 8910 → 47508 [ACK] Seq=1 Ack=324 Win=30080 Len=0 TSval=2305956319 TSecr=2738457627
10.4.49.41      10.4.49.51      TCP     7306 8910 → 47508 [ACK] Seq=1 Ack=324 Win=30080 Len=7240 TSval=2305956341 TSecr=2738457627 [TCP segment of a reassembled PDU]
10.4.49.41      10.4.49.51      TLSv1.2  462 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
10.4.49.51      10.4.49.41      TCP       66 47508 → 8910 [ACK] Seq=324 Ack=7637 Win=44544 Len=0 TSval=2738457650 TSecr=2305956341
10.4.49.51      10.4.49.41      TLSv1.2 1783 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
10.4.49.41      10.4.49.51      TCP       66 8910 → 47508 [ACK] Seq=7637 Ack=2041 Win=33536 Len=0 TSval=2305956345 TSecr=2738457653
10.4.49.41      10.4.49.51      TLSv1.2   72 Change Cipher Spec
10.4.49.41      10.4.49.51      TLSv1.2  111 Encrypted Handshake Message
10.4.49.51      10.4.49.41      TCP       66 47508 → 8910 [ACK] Seq=2041 Ack=7688 Win=44544 Len=0 TSval=2738457658 TSecr=2305956349
10.4.49.51      10.4.49.41      TLSv1.2   99 Application Data
10.4.49.41      10.4.49.51      TCP       66 8910 → 47508 [ACK] Seq=7688 Ack=2074 Win=33536 Len=0 TSval=2305956391 TSecr=2738457658
10.4.49.51      10.4.49.41      TLSv1.2  615 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
10.4.49.41      10.4.49.51      TCP       66 8910 → 47508 [ACK] Seq=7688 Ack=2623 Win=36480 Len=0 TSval=2305956391 TSecr=2738457699
10.4.49.41      10.4.49.51      TLSv1.2  515 Application Data
10.4.49.41      10.4.49.51      TLSv1.2  100 Application Data
10.4.49.51      10.4.49.41      TCP       66 47508 → 8910 [ACK] Seq=2623 Ack=8171 Win=47488 Len=0 TSval=2738457708 TSecr=2305956400
10.4.49.51      10.4.49.41      TCP       66 47508 → 8910 [FIN, ACK] Seq=2623 Ack=8171 Win=47488 Len=0 TSval=2738457708 TSecr=2305956400
10.4.49.41      10.4.49.51      TLSv1.2   97 Encrypted Alert
10.4.49.41      10.4.49.51      TCP       66 8910 → 47508 [FIN, ACK] Seq=8202 Ack=2624 Win=36480 Len=0 TSval=2305956401 TSecr=2738457708
```

Comunicação PxGrid entre ISE e FMC.

Além disso, no ISE, você pode coletar depurações relacionadas ao pxProcessamento de grade.

Navegar pelo menu Operações > Solução de Problemas > Assistente de Depuração > Depurar Configuração de log,

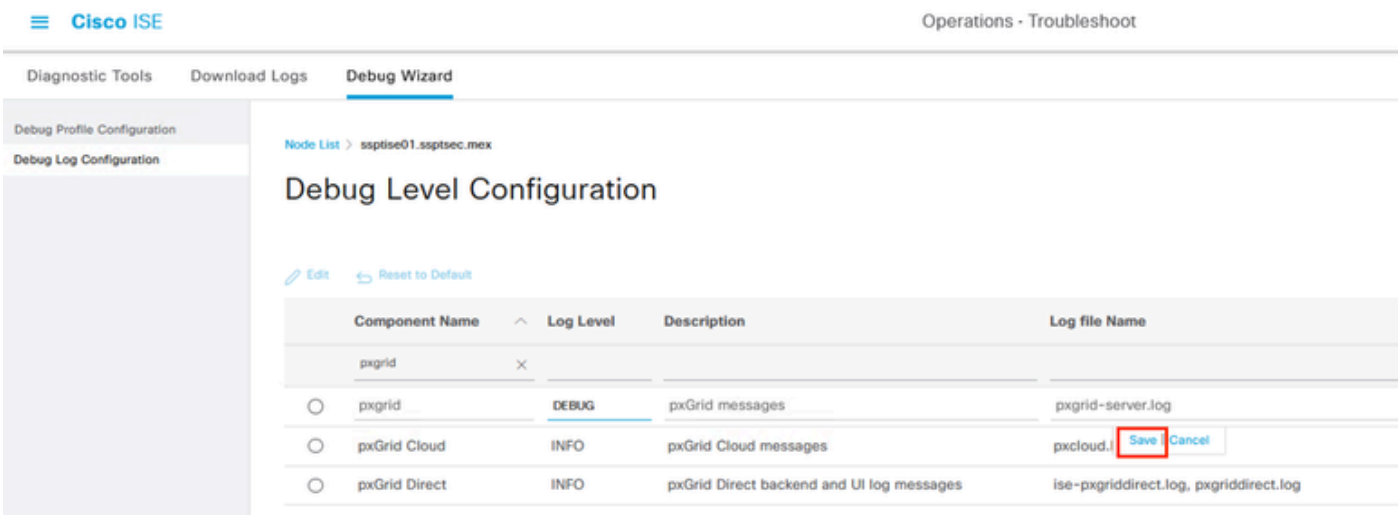
Selecione o nó do ISE correspondente para analisar e Editar.



Selecionando um nó para depurar no ISE.

Filtrar os componentes exibidos e alterar o Nível de log para DEBUG the pxgrid componente para continuar com uma análise.

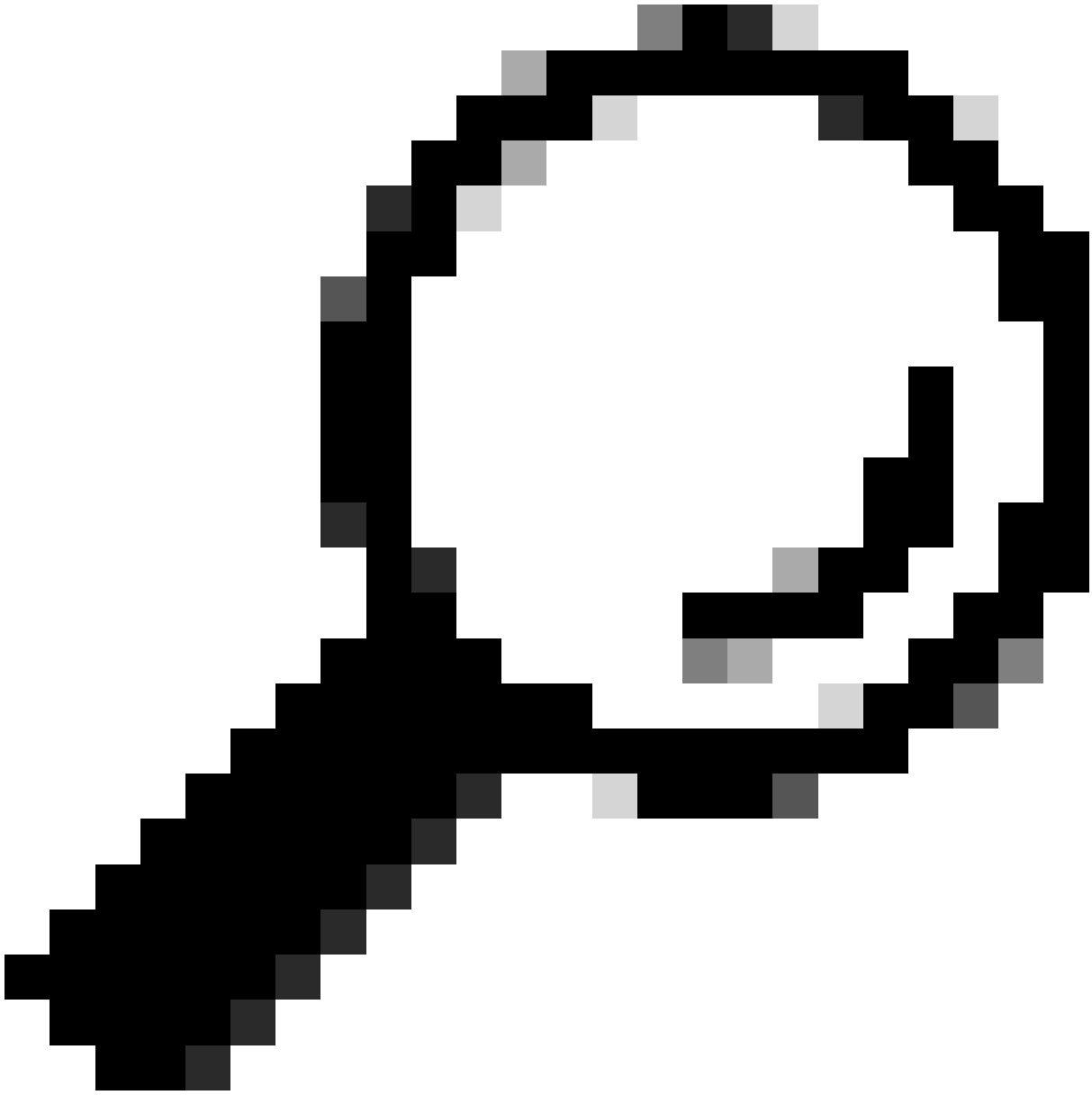
Save a configuração.



Alterando o componente pxGrid para o nível de depuração.

Reproduzir o comportamento a ser analisado e, em seguida, continuar para analisar os logs coletados no arquivo pxgrid-server.log. Outros logs que você pode examinar no nó ISE para solucionar problemas são:

```
#show logging application | include pxgrid
ise-pxgriddirect.log
pxgrid/pxgrid-server.log
pxgrid/pxgrid-test.log
pxgrid/pxgrid_dbsync_summary.log
pxgrid/pxgrid_internal_dbsync_summary.log
pxgriddirect.log
```

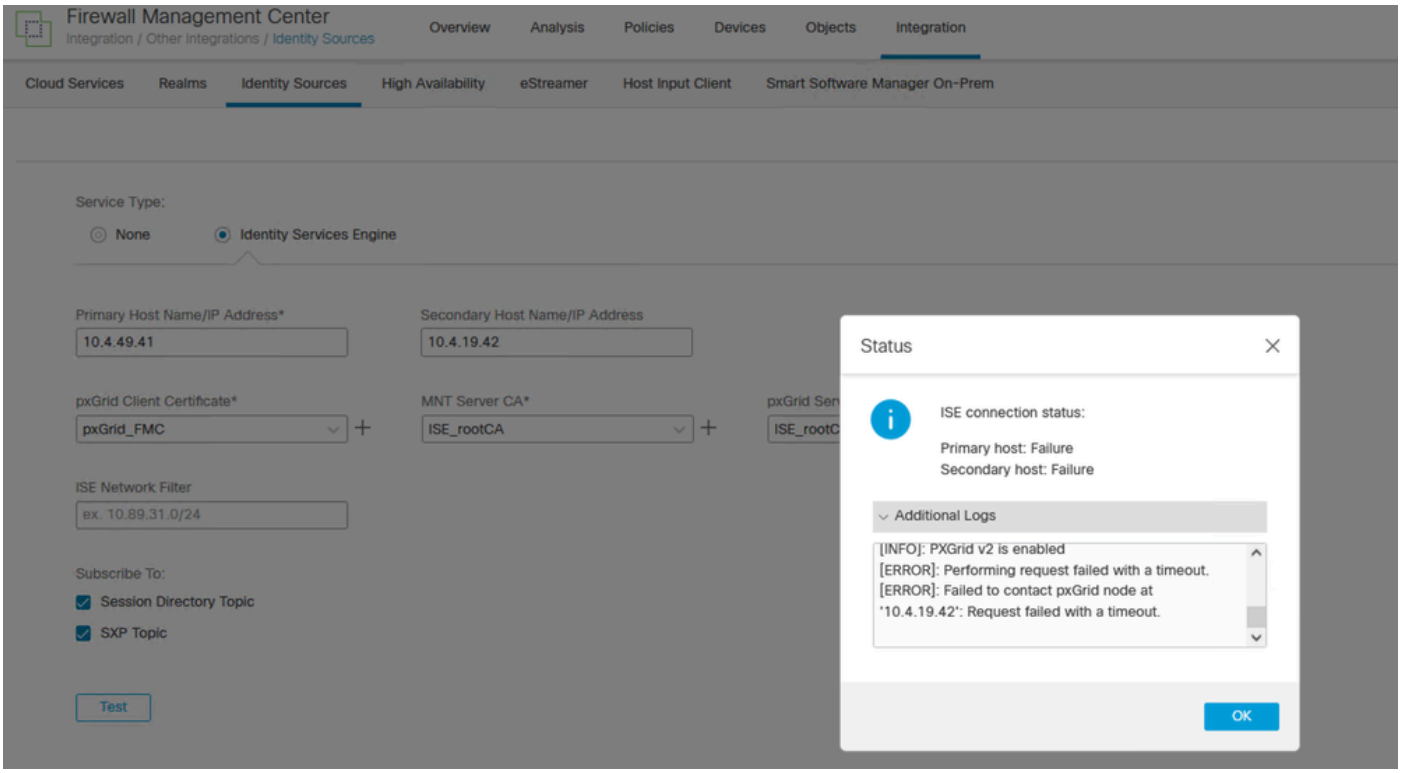


Tip: Para obter mais recomendações de coleta de logs, reveja o vídeo Como habilitar depurações em versões do ISE 3.x.

Problemas comuns.

O cliente assinante PxGrid não foi aprovado no ISE.

Para este caso de uso, a saída relacionada ao botão FMC test pxGrid mostra este comportamento:



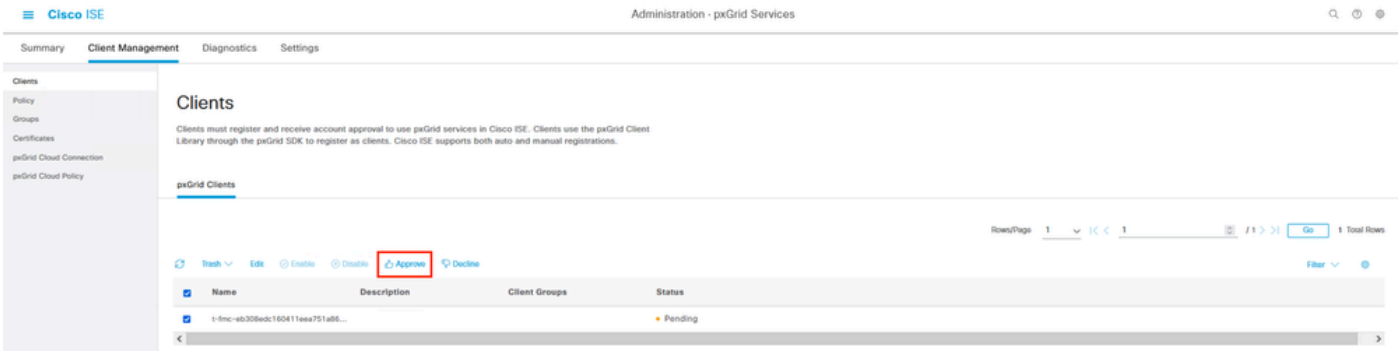
Falha na conexão do FMC pxGrid.

```
Primary host:

[INFO]: PXGrid v2 is enabled
[ERROR]: pxgrid 2.0: failed account activation. accountState=PENDING
[ERROR]: Failed to contact pxGrid node at '10.4.49.41': pxgrid2.0: Could not activate account

Secondary host:

[INFO]: PXGrid v2 is enabled
[ERROR]: Performing request failed with a timeout.
[ERROR]: Failed to contact pxGrid node at '10.4.19.42': Request failed with a timeout.
```

No ISE, observe o comportamento no menu Administration > PxGrid Services > Client Management > Clients indicando que o cliente pxGrid (FMC) está pendente para aprovação.

Selecione o botão Aprovar, confirme a seleção na próxima janela e tente a integração novamente.

Desta vez, a integração é bem-sucedida.

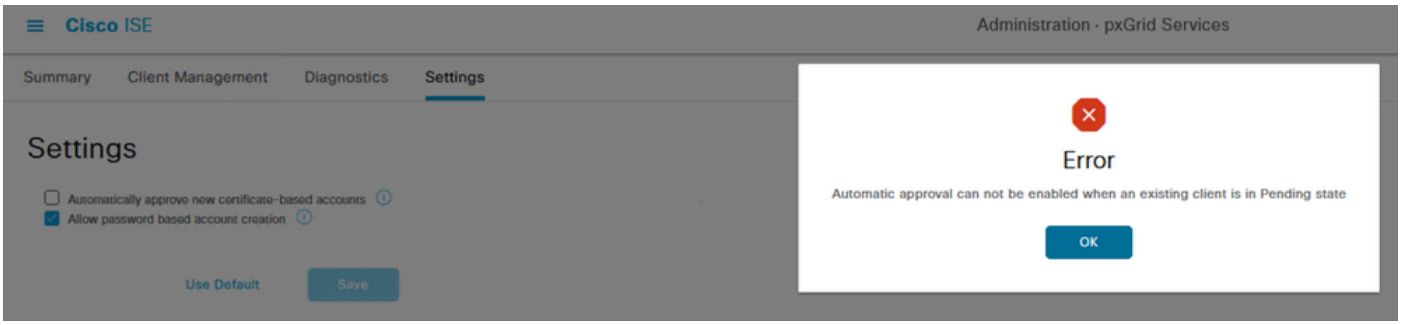


Cliente FMC com status pendente.

Confirmação da aprovação do cliente pxGrid.

Observe se você deseja habilitar a aprovação automática de clientes pxGrid baseados em certificado.

Aprovar/Recusar os clientes da página anterior, pois este alarme pode aparecer.



Erro relacionado à aprovação de clientes pxGrid.

Certificado ISE PxGrid cadeia incompleto.

Neste cenário, se você navegar para o menu Administração > Sistema > Certificado, selecione o certificado pxgrid e selecione a opção Exibir,

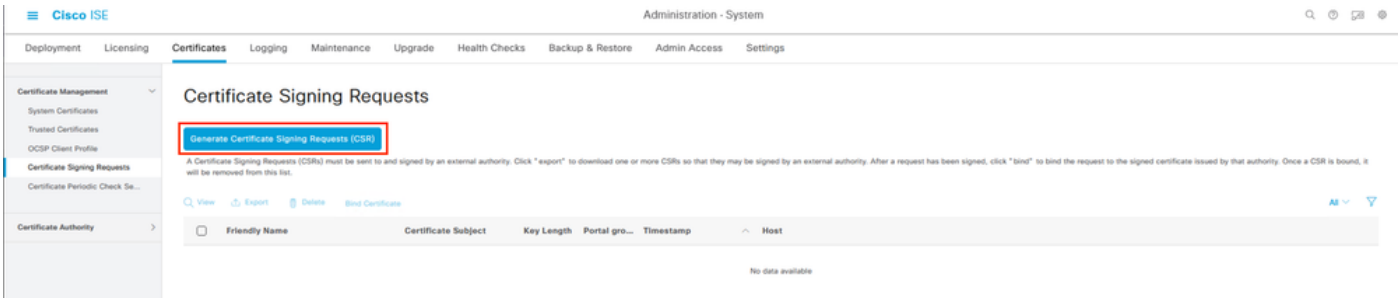
No caso de você ter um problema com o certificado, esses erros relacionados são possíveis.

Erro relacionado à cadeia de certificados incompleto.

TA primeira etapa a ser verificada é se a CA raiz do ISE está completana opção Exibir.

No caso de um certificado ausente na hierarquia, você pode emitir toda a CA raiz de implantação do ISE.

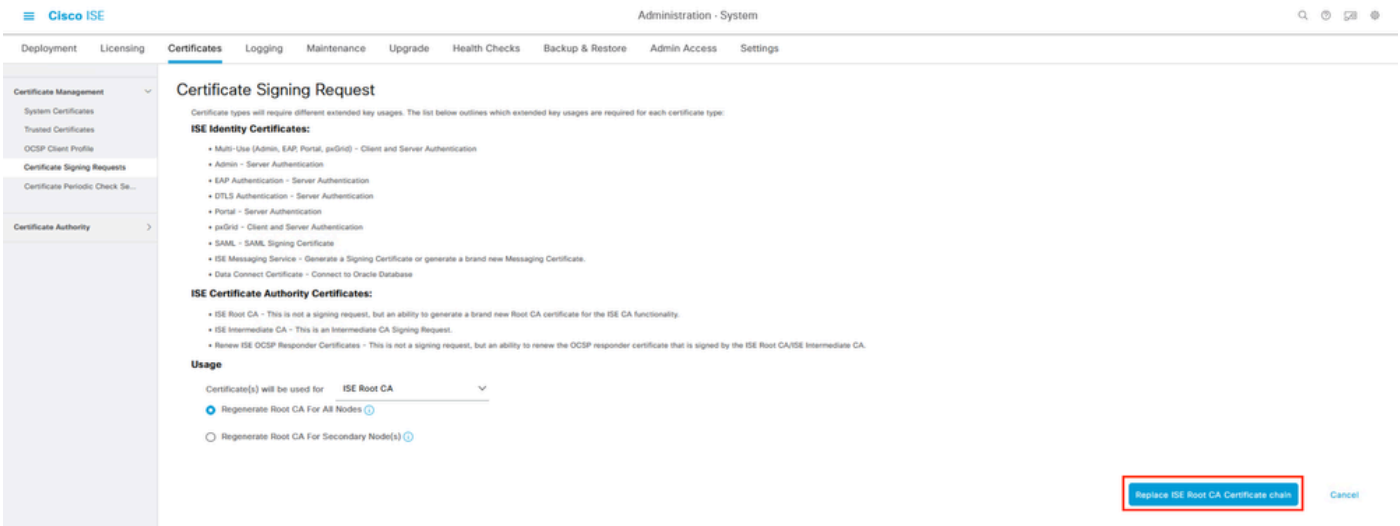
BNavegue até o menu Administration > System > Certificates > Certificate Management > Certificate Signing Request (RSE) e selecione esse botão.



Geração de um CSR no ISE.

Neste menu, selecione em Uso da CA raiz do ISE e recriar a CA raiz do ISE para todos os nós.

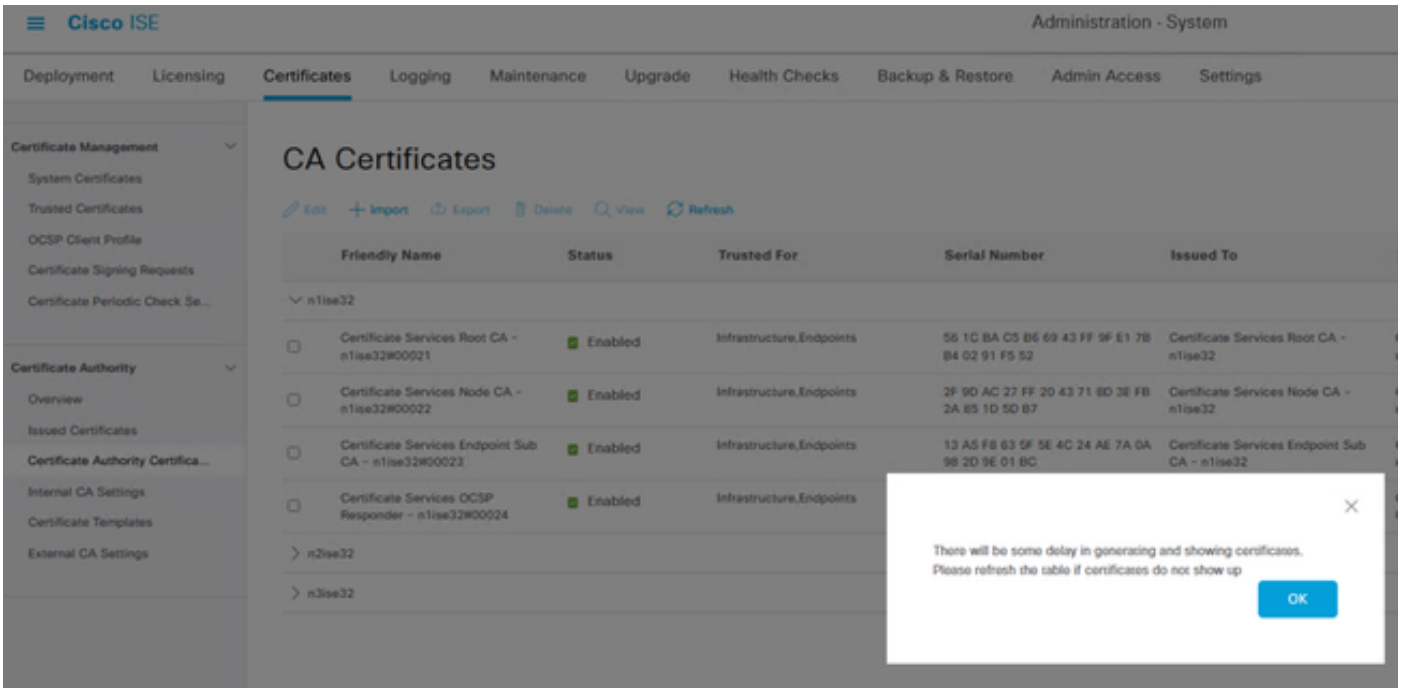
Prosseguir com o botão Substituir a cadeia de certificados da CA raiz do ISE.



Configurando a solicitação de assinatura de certificado.

Aguarde até que os certificados sejam gerados em todos os nós do impImplementação.

Após a conclusão, o ISE exibe a próxima notificação.



Confirmação de geração de certificados.

Confirme se o pxGa cadeia de confiança do certificado rid foi concluída selecionando a opção Exibir em Certificados do sistema.

Referência.

Página do Cisco Developer do PxGrid.

Guia do Administrador do Cisco Identity Services Engine, Versão 3.2 , Capítulo: Cisco pxGrid.

Guia de Instalação do Cisco Identity Services Engine, Versão 3.2, Capítulo: Referência de portas do Cisco ISE

Guia de referência da CLI do Cisco Identity Services Engine, versão 2.4

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.