

Configuración y solución de problemas de ISE 3.2 con integración de FMC 7.2.4

Contenido

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Antecedentes.](#)

[Configurar](#)

[Prepare el ISE para la integración.](#)

[Prepare el CSP para la integración.](#)

[Configuración de la conexión pxGrid entre ISE y FMC.](#)

[Verificación.](#)

[Validación en CSP.](#)

[Validación en ISE.](#)

[Troubleshoot](#)

[Resolución de problemas en FMC.](#)

[Resolución de problemas en ISE.](#)

[Problemas Comunes.](#)

[El cliente suscriptor de PxGrid no está aprobado en ISE.](#)

[Cadena de certificados PxGrid ISE incompleta.](#)

[Referencia.](#)

Introducción

En este documento se describen los procedimientos para integrar Identity Services Engine con Firewall Management Center mediante conexiones de Platform Exchange Grid.

Prerequisites

Cisco recomienda conocimientos sobre los siguientes temas:

- Identity Services Engine (ISE)
- Cuadrícula de intercambio de plataforma
- Centro de gestión de firewall (FMC)
- Certificados TLS/SSL.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- parche 3 de Identity Services Engine (ISE) versión 3.2
- Firewall Management Center versión 7.2.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes.

Esta documentación proporciona una solución para integrar FMC e ISE mediante pxGrid versión 2.

Cisco Firepower Management Center (FMC) es una plataforma centralizada para el firewall de última generación y el sistema de prevención de intrusiones que ofrece gestión de políticas, detección de amenazas y respuesta a incidentes.

Cisco Identity Services Engine es una solución completa que proporciona un acceso seguro a los terminales mediante servicios de autenticación, autorización y responsabilidad (AAA), así como la aplicación de políticas.

Platform Exchange Grid (pxGrid) le permite intercambiar información entre redes multiplataforma de varios proveedores.

Esta integración le permite obtener una supervisión segura, la detección de amenazas y el conjunto de políticas de red basadas en la información compartida.

El marco de trabajo de PxGrid tiene 2 versiones. La que se debe utilizar depende de la versión de ISE y del parche que se necesite revisar.

A partir de la versión ISE 3.1, todas las conexiones de red de ISE se basan en la versión pxgrid 2.

PxGrid versión 1.

La primera versión de este marco (pxGrid v1) se caracteriza por la facilidad de mantenimiento que se observó a través del comando `show application status ise` como se muestra en el resultado siguiente.

Cuando la función pxGrid está activada en el nodo, aparecen pxGrid funciones en estado en ejecución.

```

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

```

Mantenimiento de PxGrid versión 1.

En esta versión de esta plataforma, se sabe que solo tiene un nodo pxGrid con los procesos pxGrid en estado de ejecución mientras que los otros nodos pxGrid están en estado de espera.

Estos nodos supervisan constantemente el estado del nodo pxGrid con los servicios relacionados en ejecución.

En ese caso, el nodo principal de pxGrid era una promoción y el otro nodo de pxGrid habilitaba sus servicios de pxGrid.

Sin embargo, esto representó un tiempo de inactividad cuando ocurrió esta falla.

La primera versión de pxgrid se basó en la comunicación en el Extensible Messaging and Presence Protocol (XMPP), que es un conjunto de tecnologías utilizadas en la infraestructura de colaboración y voz.

Los temas compartidos en una conexión pxGrid v1 son:

- Directorio de sesión
- Metadatos del perfil de terminal
- Metadatos de Trustsec
- Capacidad de protección de terminales
- Control de red adaptable
- MDM_Tema sin conexión
- Identidad
- SXP

PxGrid versión 2.

Este documento describe el uso de la versión 2 de PxGrid. Esta plataforma funciona mediante

operaciones REST en los protocolos ISE y WebSocket, lo que aporta mejoras, escalabilidad mejorada, rendimiento y flexibilidad en los modelos de datos.

En esta versión, no verá las funciones de pxgrid ejecutándose como en la versión anterior con el comando `show application status ise`.

Consulte la sección de validación de ISE en este documento para saber qué mecanismos se deben comprobar para revisar la funcionalidad de pxGrid.

Con esta versión, tiene todos los nodos pxGrid que configura como nodos pxGrid activos. Estos están listos para participar en el intercambio de información en cualquier momento.

En la versión 1, solo un nodo mantenía la facilidad de mantenimiento de pxGrid en ejecución.

Los temas compartidos en una conexión pxGrid v2 son:

- Directorio de sesión
- Error de RADIUS
- Configuración del analizador
- Estado del sistema
- MDM
- Estado de ANC
- TrustSec
- Configuración de TrustSec
- SXP TrustSec
- Activo de terminal.

Componentes de pxGrid como plataforma.

Controlador PxGrid (ISE): Debe confiar en cada uno de los participantes que utilizan pxGrid.

Cliente: Puede ser suscriptor y editor de diferentes temas.

Editor: Cliente que comparte información con el controlador.

Suscriptor: Cliente que consume la información de un tema.

Esta integración le permite crear políticas de contenido en FMC basadas en la información compartida por ISE y sus temas publicados (relacionados con la actividad del terminal).

Configurar

Prepare el ISE para la integración.

Paso 1. Configure el nodo ISE para ejecutar el personaje pxGrid en el menú `Administration > System > Deployment`.

Seleccione los nodos y active la función pxGrid.

ssptise02

 Dedicated Mnt ⓘ Policy Service Enable Session Services ⓘ

Include Node in Node Group

None

 Enable Profiling Service ⓘ Enable Threat Centric NAC Service ⓘ Enable SXP Service ⓘ Enable Device Admin Service ⓘ Enable Passive Identity Service ⓘ pxGrid ⓘ

Habilitación de los servicios pxGrid de ISE en un nodo.

Paso 2. Después de habilitar los nodos con la función pxGrid, revise el estado de los Websockets relacionados con los clientes internos conectados.

Vaya a Administration > pxGrid Services > WebSocket. Observe a los clientes que apuntan a los servicios ISE directamente a través de la dirección IP 127.0.0.1.

WebSocket

Log
Tests

WebSocket

Clients Topics

Clients

Rows/Page 8 << 1 >> / 1 >> Go 8 Total Rows

🔄

Filter ⌵ ⚙️

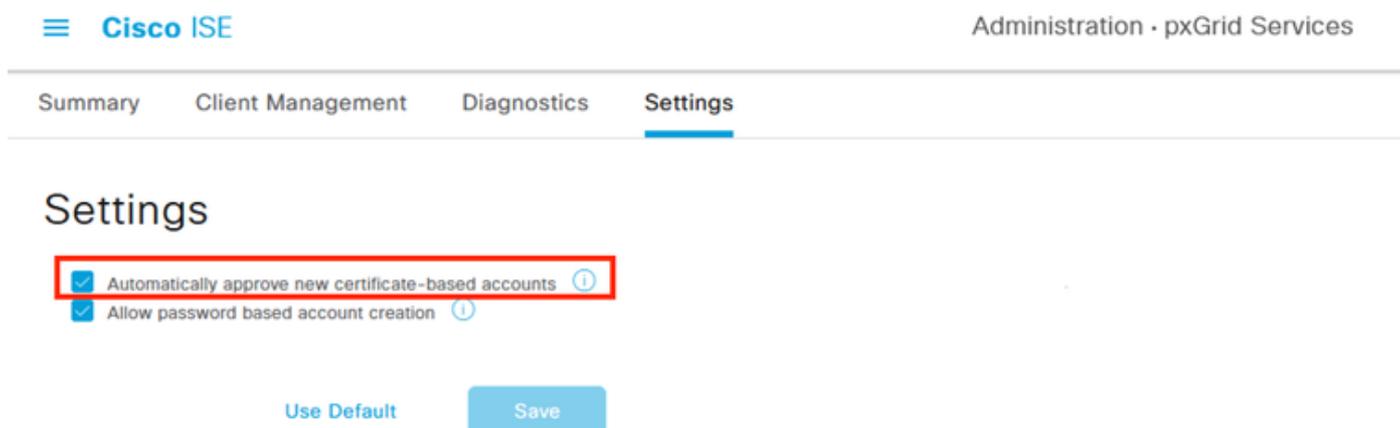
Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
-ise-fanout-ssptise01	ssptise01	ssptise01:0	CN+ssptise01.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	● Connected
-ise-fanout-ssptise02	ssptise01	ssptise01:1	CN+ssptise02.ss...	/topic/distributed	/topic/distributed	10.4.49.42	● Connected
-ise-fanout-ssptise01	ssptise01	ssptise01:2	CN+ssptise01.ss...	/topic/distributed		10.4.49.41	● Connected
-ise-fanout-ssptise02	ssptise02	ssptise02:9	CN+ssptise02.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	● Connected
-ise-mnt-ssptise02	ssptise02	ssptise02:11	CN+ssptise02.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.42	● Connected
-ise-admin-ssptise02	ssptise02	ssptise02:12	CN+ssptise02.ss...		/topic/com.cisco.ise.pxgrid...	10.4.49.42	● Connected
-ise-mnt-ssptise01	ssptise02	ssptise02:13	CN+ssptise01.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.41	● Connected
-ise-admin-ssptise01	ssptise02	ssptise02:14	CN+ssptise01.ss...	/topic/com.cisco.ise.pxgrid...	/topic/com.cisco.ise.pxgrid...	10.4.49.41	● Connected

Websockets internos de ISE.

Paso 3. Navegue por el menú Administration > pxGrid Services > Settings y seleccione la opción para Aprobar automáticamente nuevas cuentas basadas en certificados,

Este paso es opcional en este momento, sin embargo, para la conexión pxGrid, se sugiere habilitar esta casilla de verificación.

Puede aceptar el FMC como suscriptor manualmente después.



The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The navigation menu includes Summary, Client Management, Diagnostics, and Settings. The Settings page is active, showing two checkboxes: 'Automatically approve new certificate-based accounts' (checked and highlighted with a red box) and 'Allow password based account creation' (checked). Below the checkboxes are 'Use Default' and 'Save' buttons.

Habilitación de la aprobación automática para cuentas basadas en certificados pxGrid.

Paso 4. Revise los certificados relacionados con la funcionalidad pxGrid de su entorno en Administration > System > System Certificates,

Se recomienda que tenga certificados pxGrid homogéneos en todos los nodos de la implementación firmados por la misma autoridad de certificación (CA) raíz

En esta situación, estamos utilizando los certificados ISE internos generados. Para esta versión de ISE, donde en este ejemplo, la CA raíz corresponde al nodo PAN.

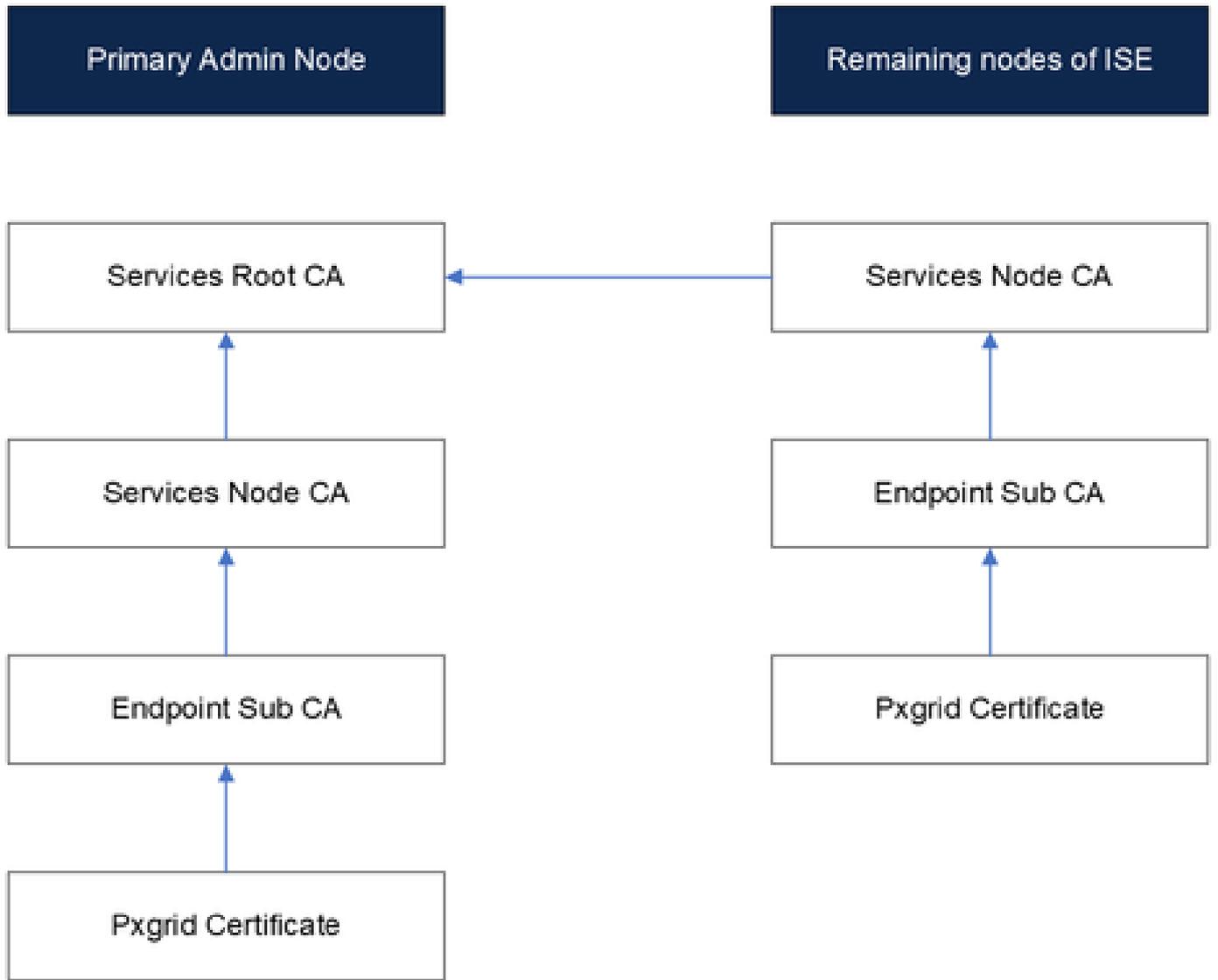


Diagrama de certificados internos en ISE.



Nota: Para obtener más información sobre la estructura interna de los certificados generados en ISE, consulte [Comprensión de los servicios de autoridad de certificación interna de ISE.](#)

System Certificates									
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.									
Edit + Generate Self Signed Certificate + Import Export Delete View									
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status		
CA - ssp1se01 (RUVUUV)									
<input type="checkbox"/> CN=ssp1se01.ssp1sec.mex, O=U=Certificate Services System Certificate\Certificate Services Endpoint Sub CA - ssp1se01#00002	pxGrid		ssp1se01.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	<input checked="" type="checkbox"/>	Active	
<input type="checkbox"/> ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp1se01.ssp1sec.mex	ssp1sec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	<input checked="" type="checkbox"/>	Active	
ssp1se02									
<input type="checkbox"/> Default self-signed saml server certificate - CN=SAML_ssp1se01.ssp1sec.mex	SAML		SAML_ssp1se01.ssp1sec.mex	SAML_ssp1se01.ssp1sec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	<input checked="" type="checkbox"/>	Active	
<input type="checkbox"/> ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp1se02.ssp1sec.mex	ssp1sec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	<input checked="" type="checkbox"/>	Active	
<input type="checkbox"/> CN=ssp1se02.ssp1sec.mex, O=U=ISE Messaging Services\Certificate Services Endpoint Sub CA - ssp1se02#00004	ISE Messaging Service		ssp1se02.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	<input checked="" type="checkbox"/>	Active	
<input type="checkbox"/> CN=ssp1se02.ssp1sec.mex, O=U=Certificate Services System Certificate\Certificate Services Endpoint Sub CA - ssp1se02#00003	pxGrid		ssp1se02.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	<input checked="" type="checkbox"/>	Active	

Certificados PxGrid en una implementación distribuida.

Paso 5. Verifique el estado de los certificados de pxGrid.

En el menú anterior, seleccione una casilla de verificación de un certificado pxGrid de nodo y, a continuación, seleccione la opción Ver.

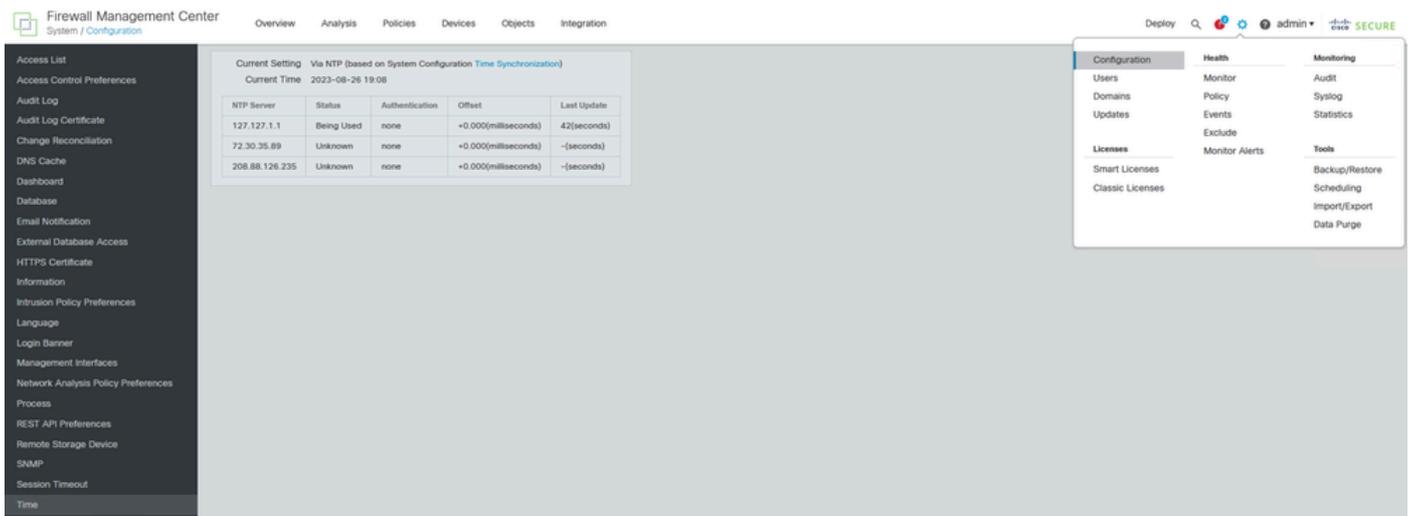
El resultado es similar al que se muestra aquí en los certificados de pxGrid.

Verificación del certificado pxGrid.

Prepare el CSP para la integración.

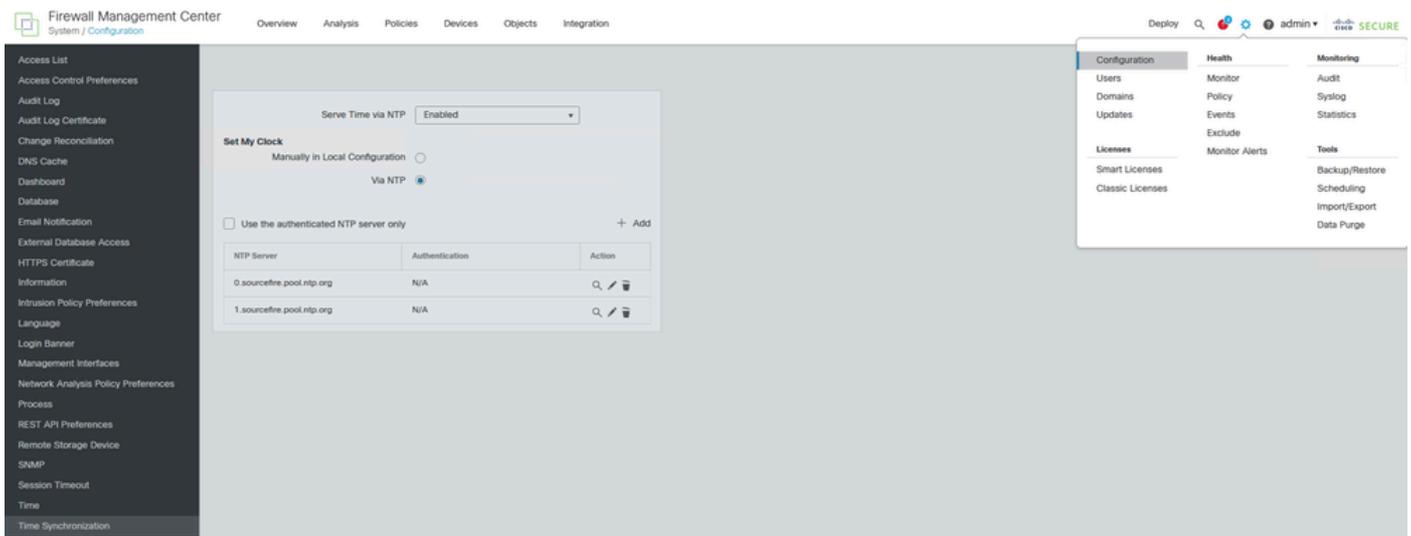
Paso 1. Confirme que la hora interna del CSP es al día.

Vaya a System > Configuration > Hora y asegúrese de que la hora configurada en el CSP es actualizado.



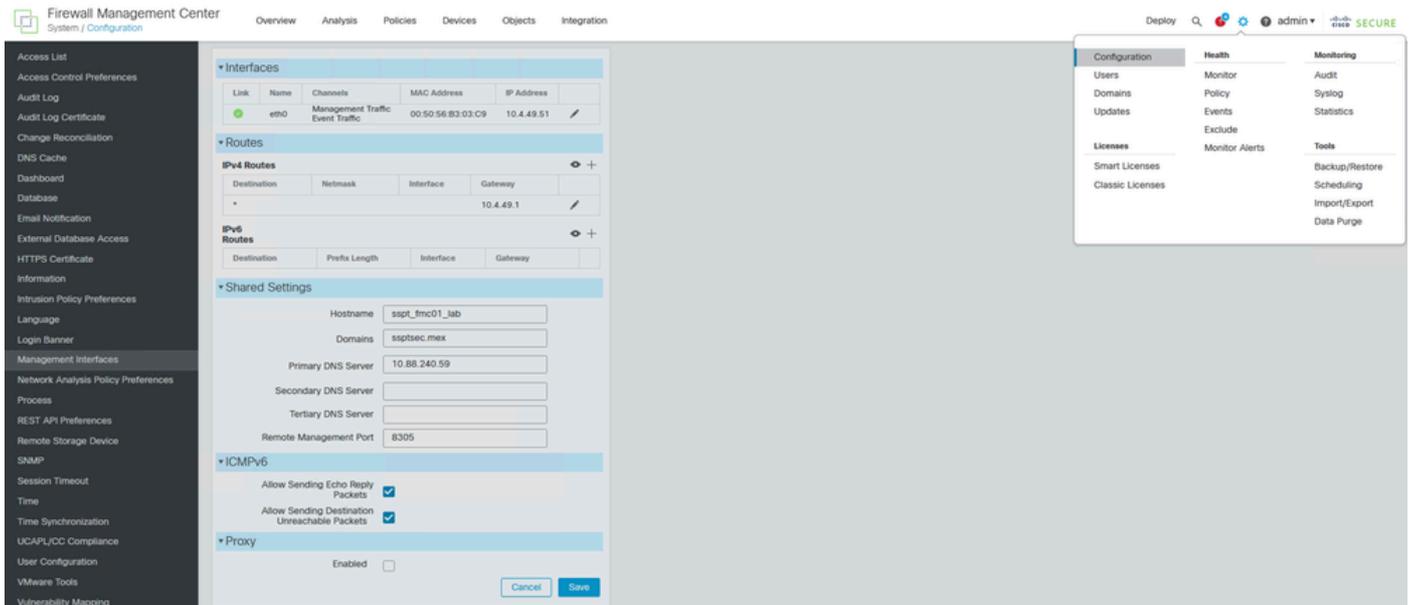
Verificación de la actualización del CSP.

Si la hora de FMC no se actualiza, asegúrese de que NTP esté configurado correctamente y in Sincrónico. NTP se puede configurar en System > Configuration > Time > + Add.



Sincronización horaria en FMC.

Paso 2. Vaya a System > Configuration > Interfaz de administración > Configuración compartida y comprobar que al menos Servidor DNS principal campo contiene a válido IP del servidor DNS.



Configuración de DNS en FMC.

Paso 3. Confirme que el nombre de host FMC está configurado.

Vaya a System > Configuration > Management Interface > Shared Settings y comprobar que Hostname contiene el nombre de host de FMC.

Puede verificar este paso mientras revisa el paso anterior en esta sección .

Configuración de la conexión pxGrid entre ISE y FMC.

Paso 1. Navegue al menú Administration > pxGrid Services > Client Management > Certificates.

En la primera opción, seleccione Deseo generar un solo certificado (sin una solicitud de firma de certificado).

En la sección Nombre común (CN), introduzca el FQDN del FMC para el que ISE debe emitir un certificado.

Proporcione una descripción.

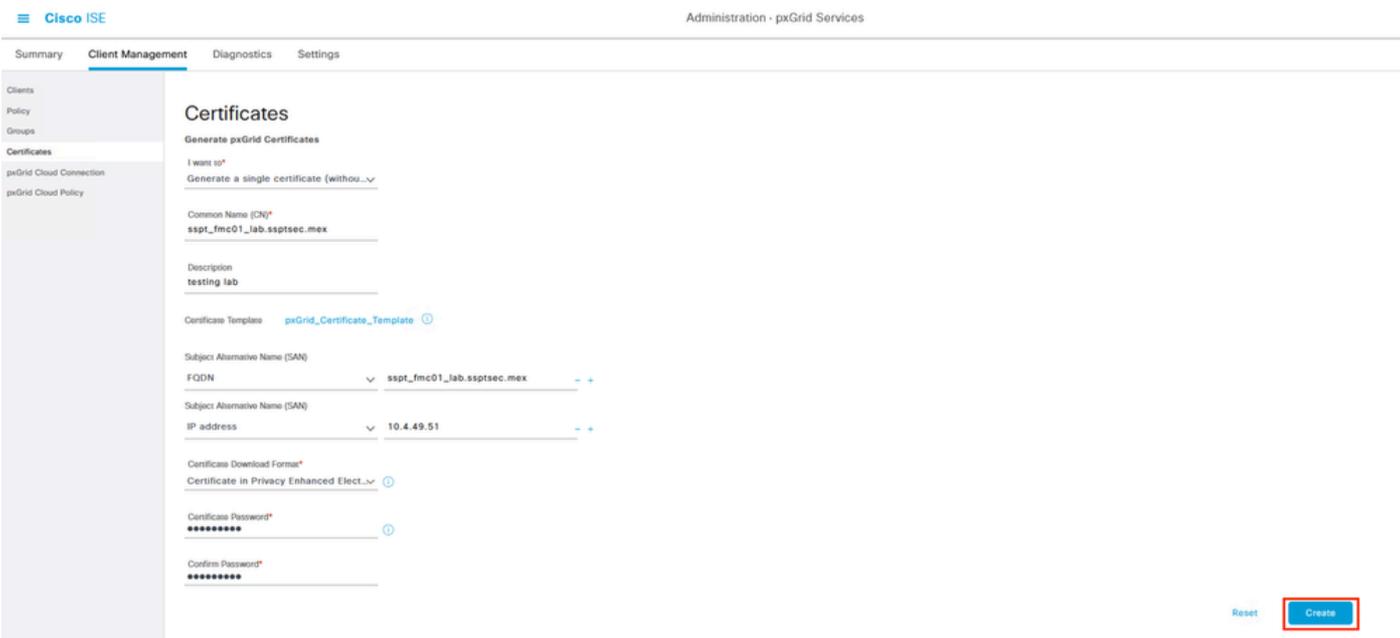
En la sección Nombre alternativo del sujeto (SAN), introduzca el FQDN y la dirección IP del CSP al que desea conectarse.

En la parte inferior de Certificate Download Format (Formato de descarga de certificados), seleccione en el menú desplegable la opción Certificate in Privacy Enhanced Electronic Mail (PEM) format (Certificado en correo electrónico con privacidad mejorada [PEM]).

Introduzca el formato PEM PKCSS (incluida la cadena de certificados).

Introduzca y almacene una contraseña en Certificate Password cuando la utilice más adelante en el FMC.

Confirme la contraseña y, a continuación, seleccione Create.



Ejemplo de generación de certificados de pxGrid.

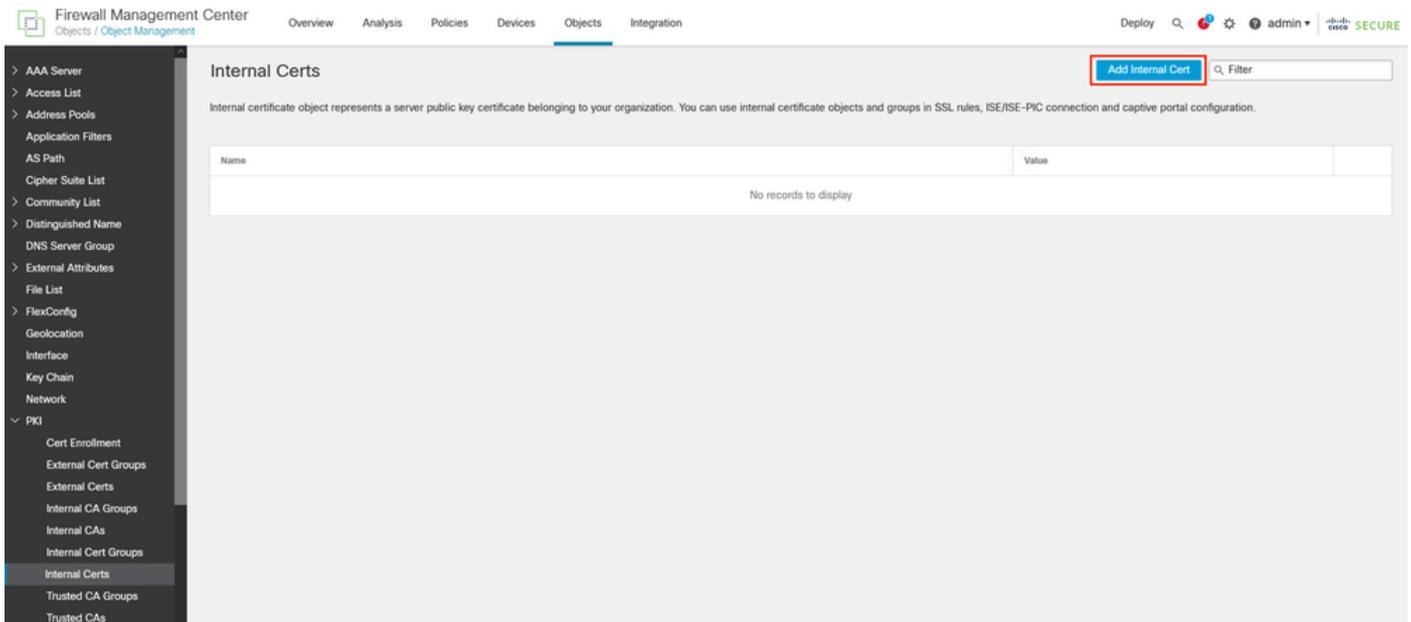
Paso 2. Se descarga un archivo zip en el equipo. Descomprima el archivo y confirme que dispone de estos archivos de su entorno:

Name	Date modified	Type	Size
CertificateServicesEndpointSubCA-ssptise01_	21/08/2023 04:55	Security Certificate	3 KB
CertificateServicesNodeCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
CertificateServicesRootCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex.key	21/08/2023 04:55	KEY File	2 KB

Certificados PxGrid generados por ISE.

Paso 3. En el FMC, Navegue al menú Objetos > Administración de Objetos > PKI > Certificados Internos.

Seleccione la opción Add Internal Cert.



Adición del certificado de CSP como certificado interno.

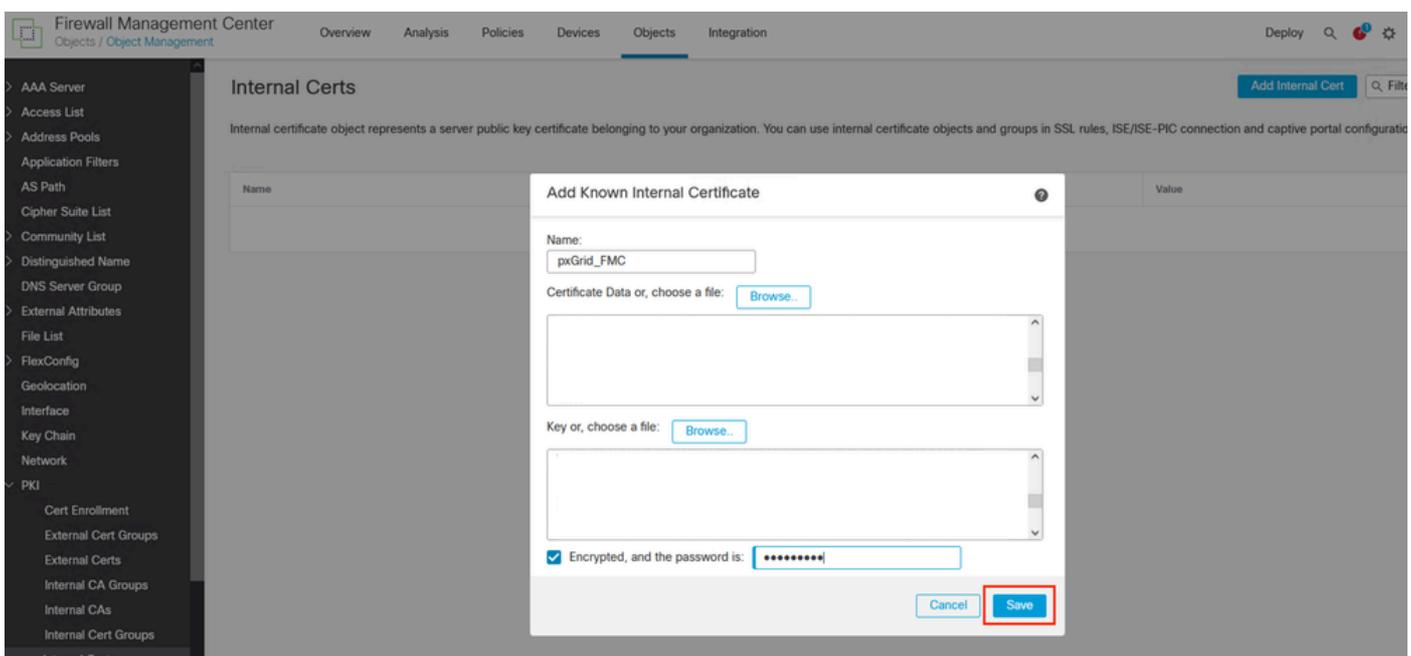
Paso 4. Nombre el certificado asignado en FMC.

Examine el certificado que ha creado para el FMC desde ISE en la sección Datos del certificado.

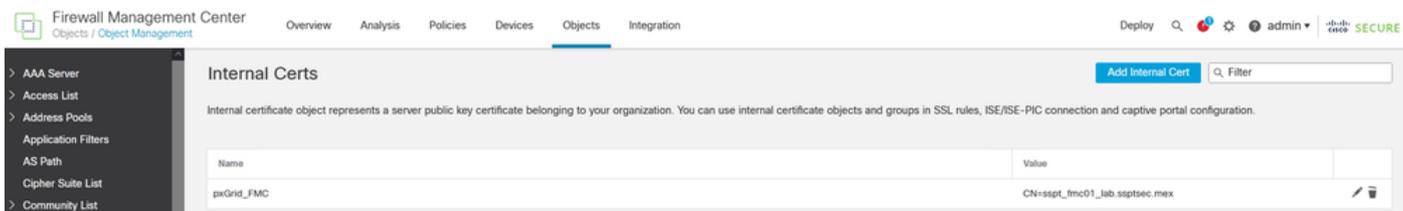
Examine el archivo con la extensión .key para rellenar el siguiente campo.

Seleccione la opción Encrypted e introduzca la contraseña que utilizó al crear el certificado en ISE.

Guarde la configuración.

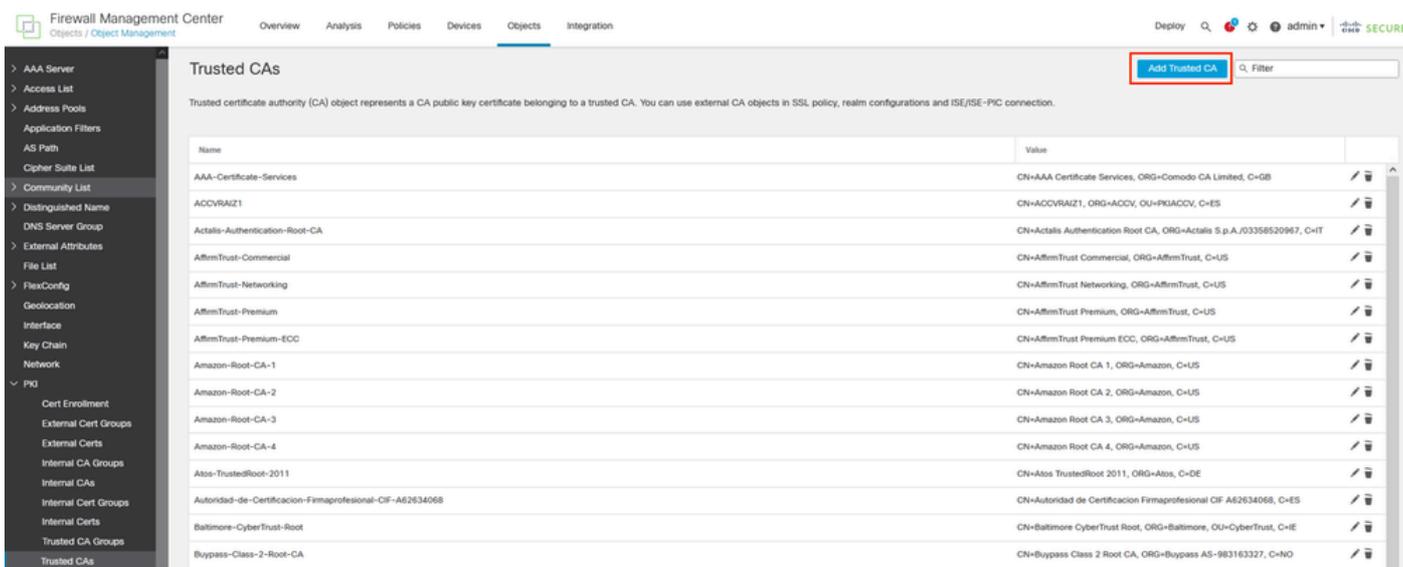


Exportación del certificado FMC generado por ISE.



Certificado de CSP.

Paso 5. Navegue al menú Objetos > Administración de Objetos > PKI > CA Confiables, Seleccione Agregar CA fiables.

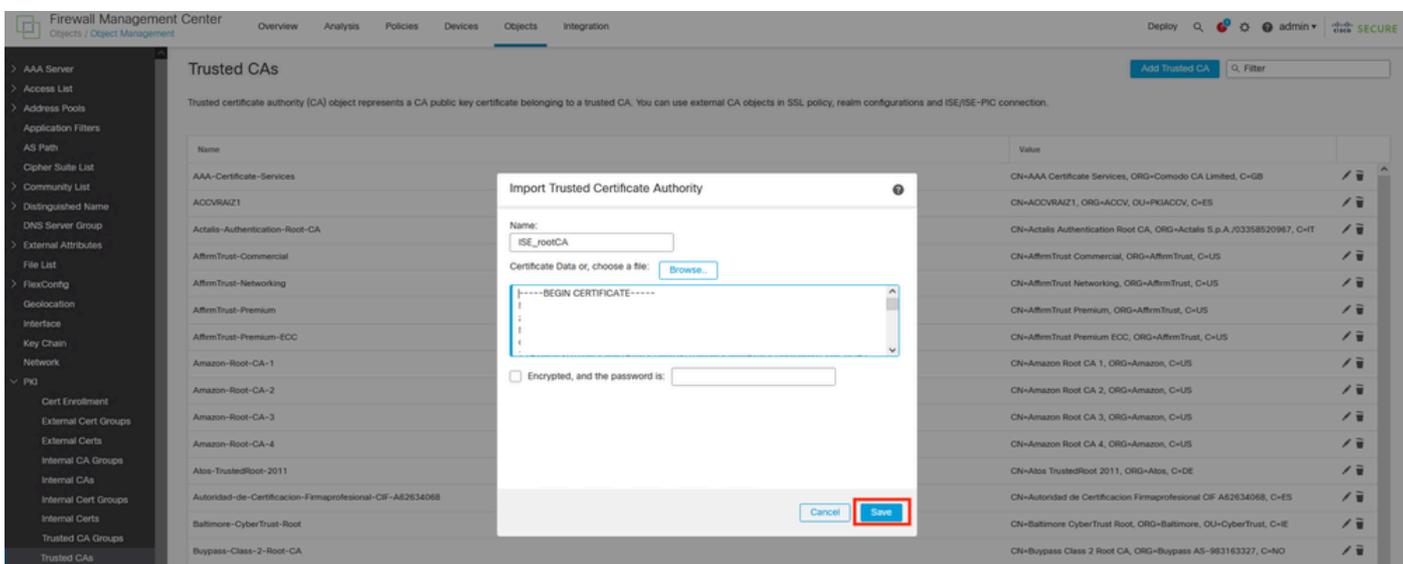


Agregando ISE rootCA como certificado de confianza.

Paso 6. Nombre de la autoridad certificadora.

Busque y seleccione la entidad emisora de certificados raíz de ISE que se descargó del archivo de ISE.

Guarde su configuración.



Exportación de la CA raíz de ISE.

Paso 7. Navegue al menú Integración > Otras integraciones > Orígenes de identidad.

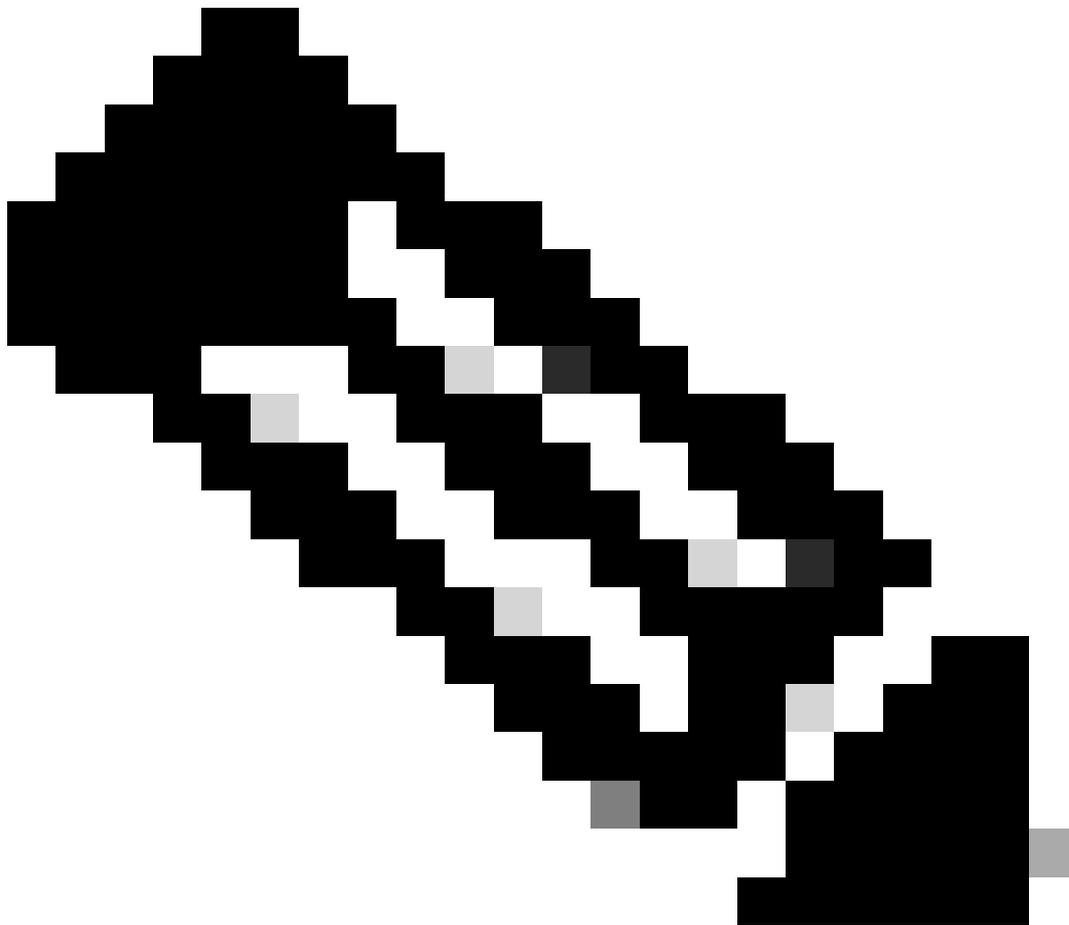
Seleccionar en Tipo de servicio: Identity Services Engine,

Introduzca la dirección IP o el FQDN del nodo pxGrid que se convierte en el nodo principal.

Repita el procedimiento para el nodo pxGrid secundario.

Seleccione en el menú desplegable el certificado pxGrid generado por ISE para la sección certificado de cliente pxGrid,

En la sección CA de servidor MNT y CA de servidor pxGrid, seleccione la CA raíz de ISE que exportó en el último paso.



Nota: La CA del servidor pxGrid corresponde a la autoridad certificadora raíz del certificado que está siendo utilizado por pxGrid en los nodos pxGrid.

La CA del servidor MNT corresponde a la autoridad certificadora del certificado que está siendo utilizado por pxGrid en los nodos MNT.

(Opcional) Puede suscribirse al tema Session Directory y SXP desde ISE.

Guarde la configuración.

Firewall Management Center
Integration / Other Integrations / Identity Sources

Overview Analysis Policies Devices Objects Integration

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

You have unsaved changes Cancel Save

Service Type:
 None Identity Services Engine

Primary Host Name/IP Address*
10.4.49.41

Secondary Host Name/IP Address
10.4.19.42

pxGrid Client Certificate*
pxGrid_FMC

MNT Server CA*
ISE_rootCA

pxGrid Server CA*
ISE_rootCA

ISE Network Filter
ex. 10.89.31.0/24

Subscribe To:
 Session Directory Topic
 SXP Topic

Test

Configuración de ISE como fuente de identidad en FMC.

Verificación.

Validación en CSP.

En el menú, navegue hasta Integración > Otras integraciones > Orígenes de identidad > Identity Services Engine antes de guardar la configuración. Puede probar la configuración del vínculo pxGrid.

Firewall Management Center
Integration / Other Integrations / Identity Sources

Overview Analysis Policies Devices Objects Integration

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Service Type:
 None Identity Services Engine

Primary Host Name/IP Address*
10.4.49.41

Secondary Host Name/IP Address
10.4.49.42

pxGrid Client Certificate*
pxGrid_FMC

MNT Server CA*
ISE_rootCA

pxGrid Server CA*
ISE_rootCA

ISE Network Filter
ex. 10.89.31.0/24

Subscribe To:
 Session Directory Topic
 SXP Topic

Test

Status

ISE connection status:
Primary host: Success
Secondary host: Success

Additional Logs

Primary host:
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to sspitise02.sspitsec.mex.8910

OK

Comunicación correcta con 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, AdaptiveNetwork
[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, AdaptiveNetwork
[INFO]: All requested ISE Services are online.
```

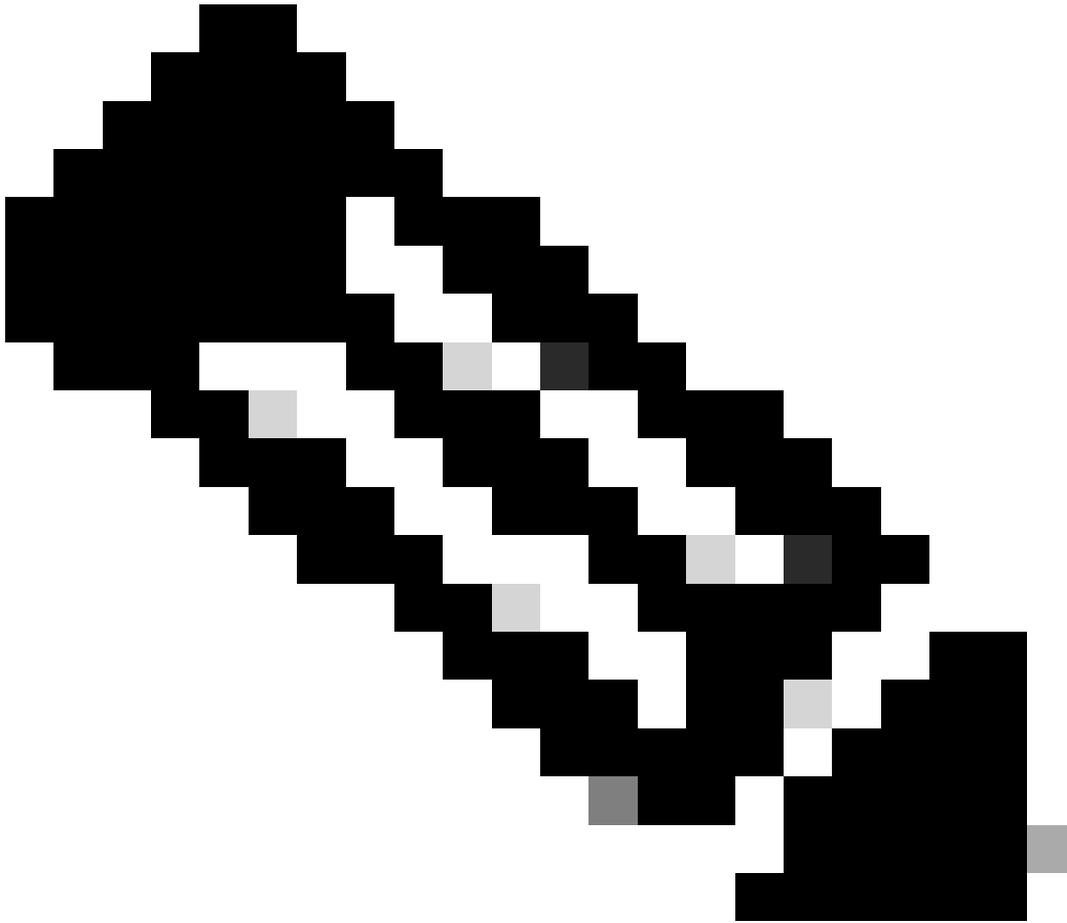
Validación en ISE.

Cuando el cliente FMC pxGrid se ha integrado correctamente en ISE, usted a continuación consulte (en el Administration > pxGrid Services > Client Management > menú Clientes) se incluyen clientes con el nombre fmc y habilitado.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration - pxGrid Services'. The main menu on the left includes 'Clients', 'Policy', 'Groups', 'Certificates', 'pxGrid Cloud Connection', and 'pxGrid Cloud Policy'. The 'Client Management' tab is active, and the 'Clients' sub-tab is selected. The main content area shows a table of pxGrid clients. The table has columns for Name, Description, Client Groups, and Status. The first four rows are highlighted with a red box, and all have a status of 'Enabled'.

Name	Description	Client Groups	Status
fmc-eb308edc160411ea751a86...			Enabled
t-fmc-eb308edc160411ea751a86...			Enabled
t-fmc-eb308edc160411ea751a86...			Enabled
fmc-6c85c3c6160511eb4ab139f5...			Enabled

Clientes PxGrid disponibles y habilitados.



Nota: Los clientes pxGrid cuyo prefijo comienza con "t-fmc" son los que se utilizan a través del botón de prueba de FMC.

Además, si navega al menú Administration > pxGrid Services > Diagnostics > WebSocket, a continuación, verá la conexiones hacia el CSP.

En el escenario en el que tiene el FMC en Alta disponibilidad, a continuación, verá las unidades primarias y secundarias tal como se muestran en este ejemplo:

Cisco ISE Administration - pxGrid Services

Summary Client Management Diagnostics Settings

WebSocket

Log

Texts

WebSocket

Clients Topics

Clients

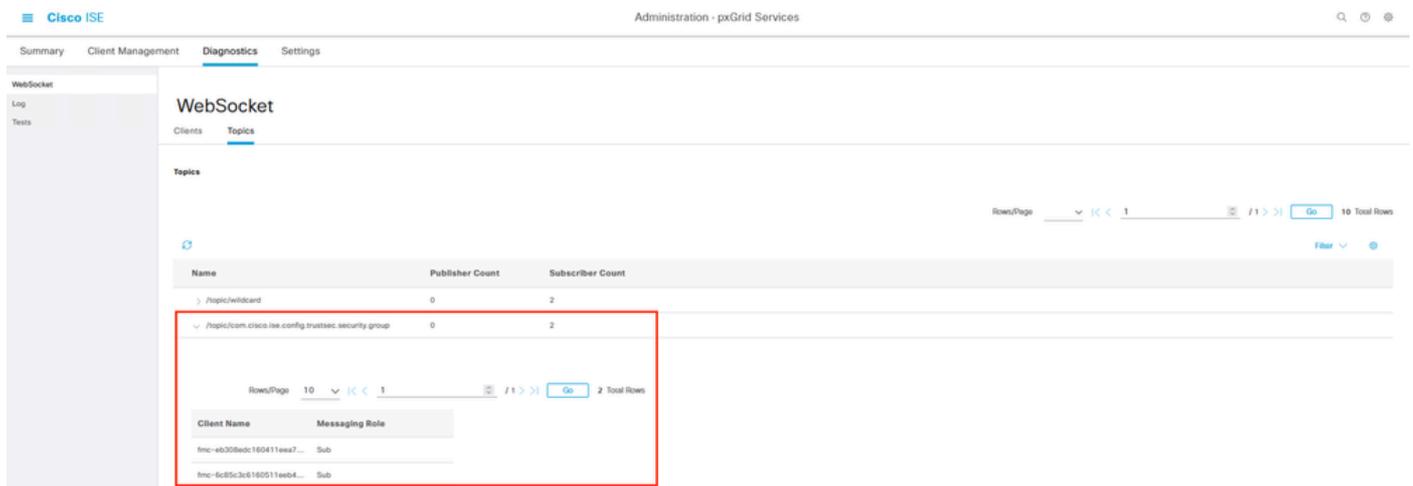
Rows/Page 2 << 1 >> Go 2 Total Rows

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration (dd:hh:mm:ss)
fmc-eb308edc160411ea47...	x ssp1se01	ssptse01.5	CN=sspt_fmc01...	/topic/com.cisco.ise.sessio...	Publications	10.4.49.51	• Connected	2023-08-21 05:30:18 MDT	01:10:19.42
fmc-6d5c3d160511ea4...	x ssp1se01	ssptse01.6	CN=sspt_fmc01...	/topic/com.cisco.ise.sessio...	Publications	10.4.49.52	• Connected	2023-08-21 05:31:56 MDT	01:10:18.03

WebSockets disponibles en ISE.

En la ficha siguiente desde este menú nombrado Tema, usted puede comprobar que los suscriptores de FMC se han agregado a los temas de pxGrid publicados por ISE.

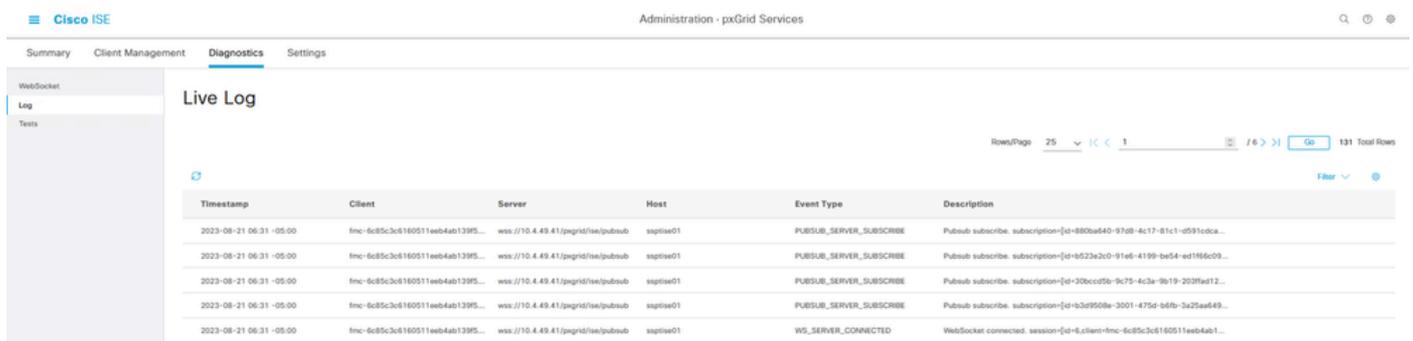
Por ejemplo, está el tema relacionado con el grupo de seguridad de where usted puede ver que tanto FMC están suscritos y reciben información relacionada a SGT publicado por ISE.



Temas por suscriptor de pxGrid.

En el menú Administration > pxGrid Services > Diagnostics > Log, eventos importantes se muestran las comunicaciones relacionadas con en pxGrid (para los nodos con la función activada).

Éstos muestran la información relacionada con la integración.



Registros activos de PxGrid.

Troubleshoot

Resolución de problemas en FMC.

Confirme que FMC puede resolver sus propios nodos de ISE y nombres de host.

Por ejemplo:

<#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
```

Asegúrese de lo siguiente El proceso ADI está en funcionamiento:

```
<#root>
```

```
>
```

```
expert
```

```
sudo suadmin@sspt_fmc01_lab:~$
```

```
sudo su
```

```
root@sspt_fmc01_lab:/Volume/home/admin#
```

```
pmtool status | grep adi
```

adi (normal) - Running 7911

EGarantizar que la comunicación de FMC a ISE en pobreSe permite t TCPP 8910. Desde FMC CLI podemos configurar a tcpdump captura de paquetes para confirmar la comunicación bidireccional.

```
<#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
```

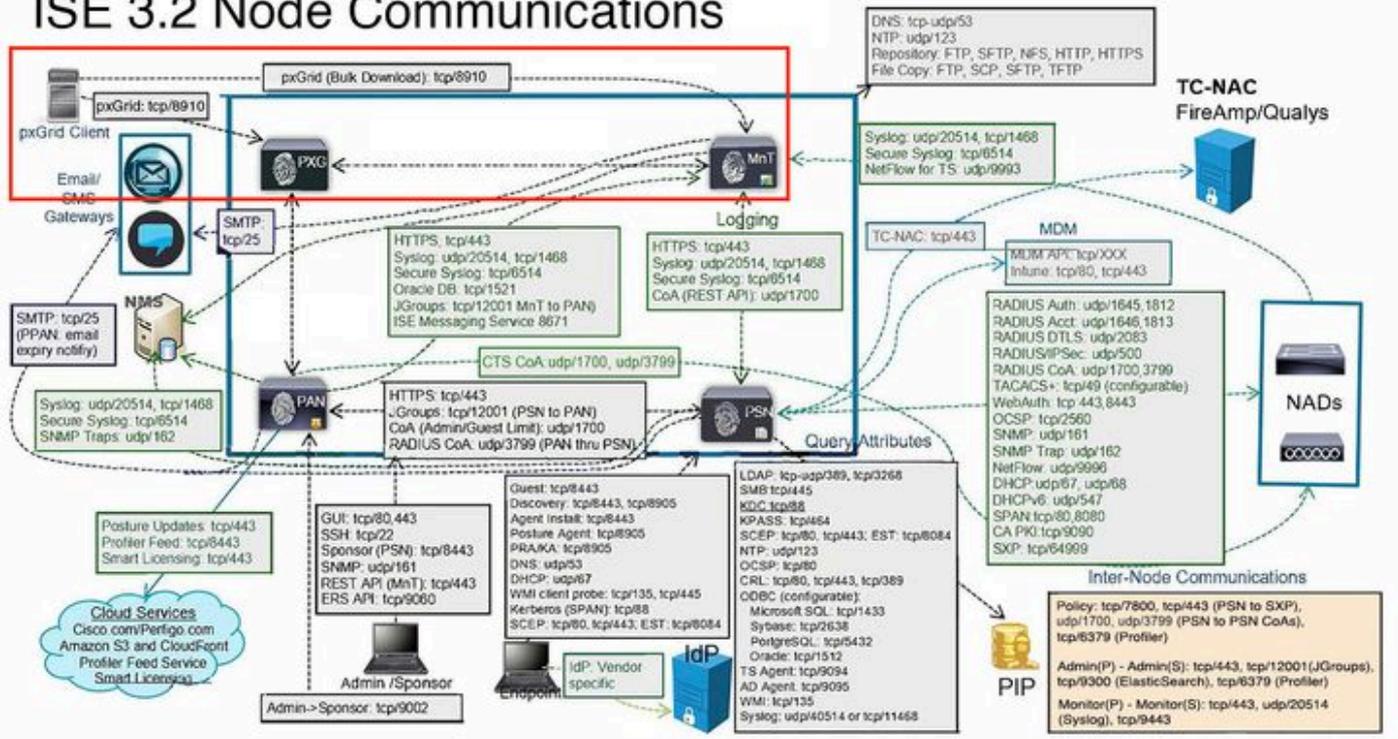
```
: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0  
[...]
```

Resolución de problemas en ISE.

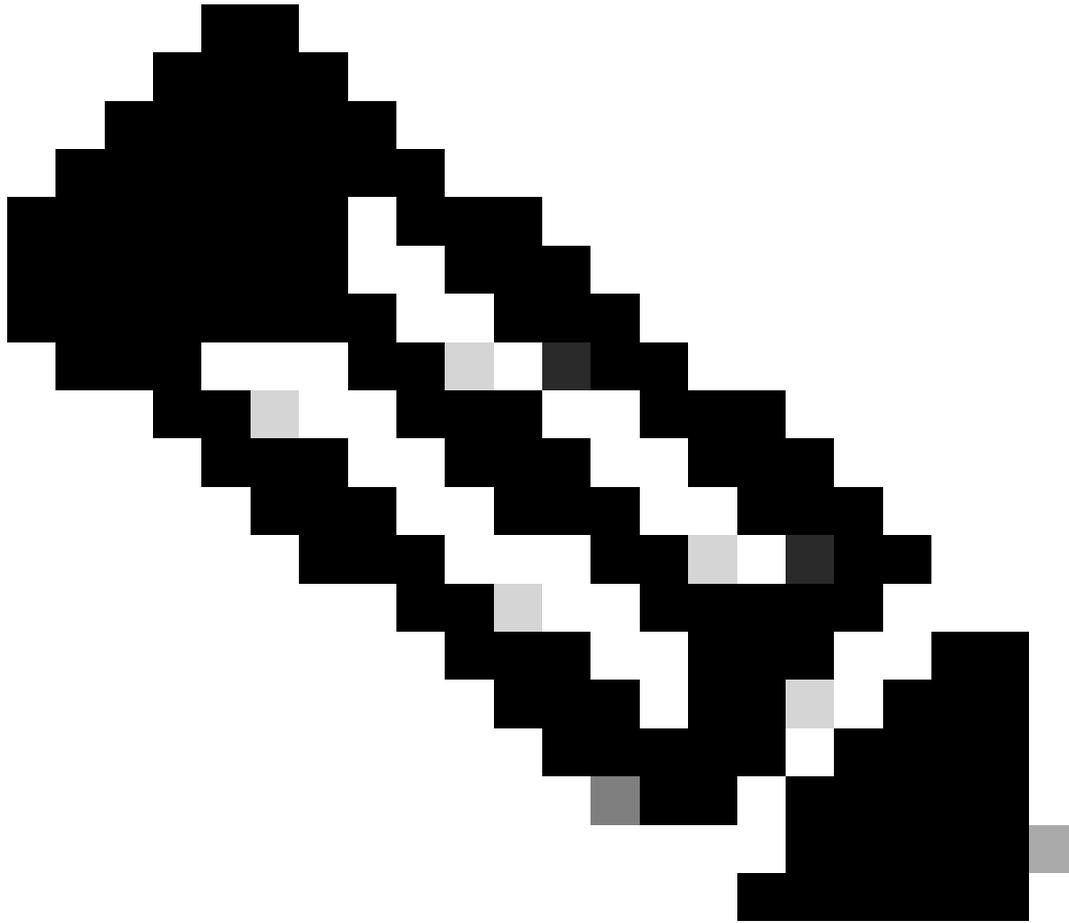
Verifique que las comunicaciones en el puerto 8910 está en funcionamiento.

Este es el puerto utilizado por el cliente pxGrids para comunicarse con nodos pxGrid y nodos MnT para la descarga masiva de información.

ISE 3.2 Node Communications



Interacción de PxGrid en el entorno de ISE.



Nota: El cliente pxGrid, en este caso el FMC se comunica con los nodos pxGrid y el nodo MNT secundario (SMNT) para obtener la (descarga masiva) de la información, en caso de fallo en el SMNT busca la información a través del MNT primario.

IEEn los nodos de ISE en los que se mantiene la comunicación con el cliente pxGrid, puede revisar si el puerto es abierto o si hay sockets conectados a ese puerto.

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

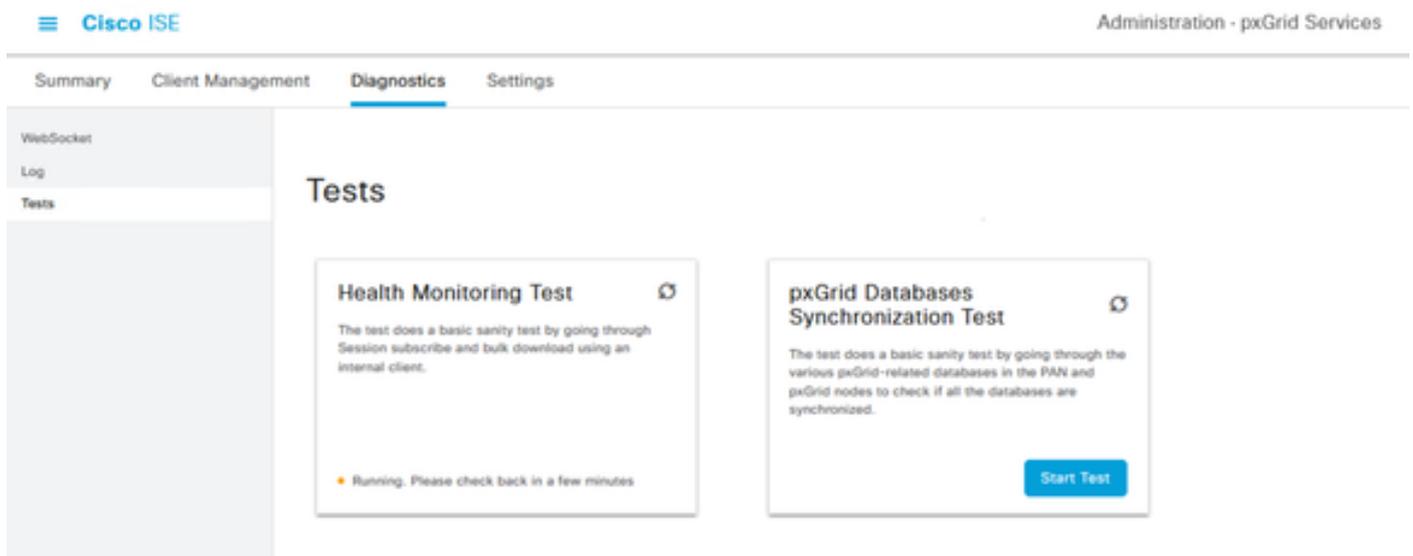
Hay dos pruebas disponibles en ISE que diagnostican el estado general de las implementaciones de pxGrid.

Estos se pueden encontrar en el menú Administration > pxGrid Services > Diagnostics > Test.

Las pruebas que se muestran en esta sección se realizan internamente en ISE.

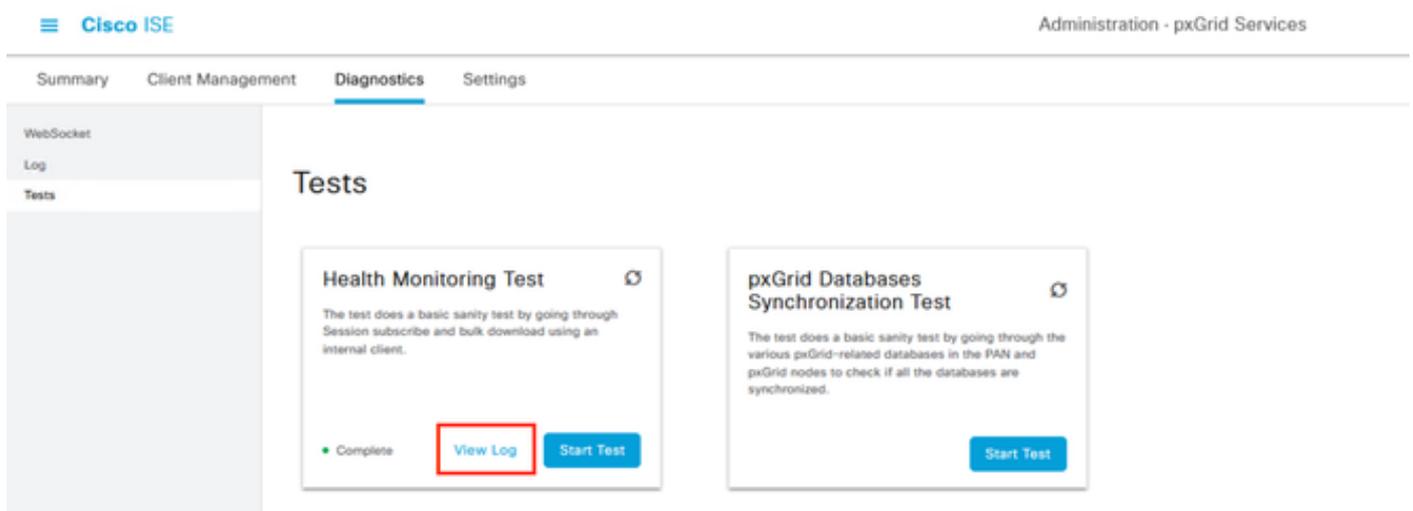
Prueba de supervisión de estado revisa el aspecto del servicio pxGriden funcionamiento, que evalúa si un cliente puede acceder al directorio de sesión, servicio y temas publicados por el controlador pxGrid.

Seleccione el opción Inicio Prueba y espere a que se recopilen los registros.



Prueba de supervisión de estado de PxGrid.

Una vez finalizada la prueba, seleccione el opción Ver registro. En este ejemplo, el contenido del registro es:



Revisión de la prueba de supervisión de estado.

```
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] sessionRestBaseUr1=https://ssptise01.ssptsec.mex:8910/pxgrid/mnt/sd
22-Aug-2023 17:03:14 [INFO] wsUr1=wss://ssptise02.ssptsec.mex:8910/pxgrid/ise/pubsub
```

```

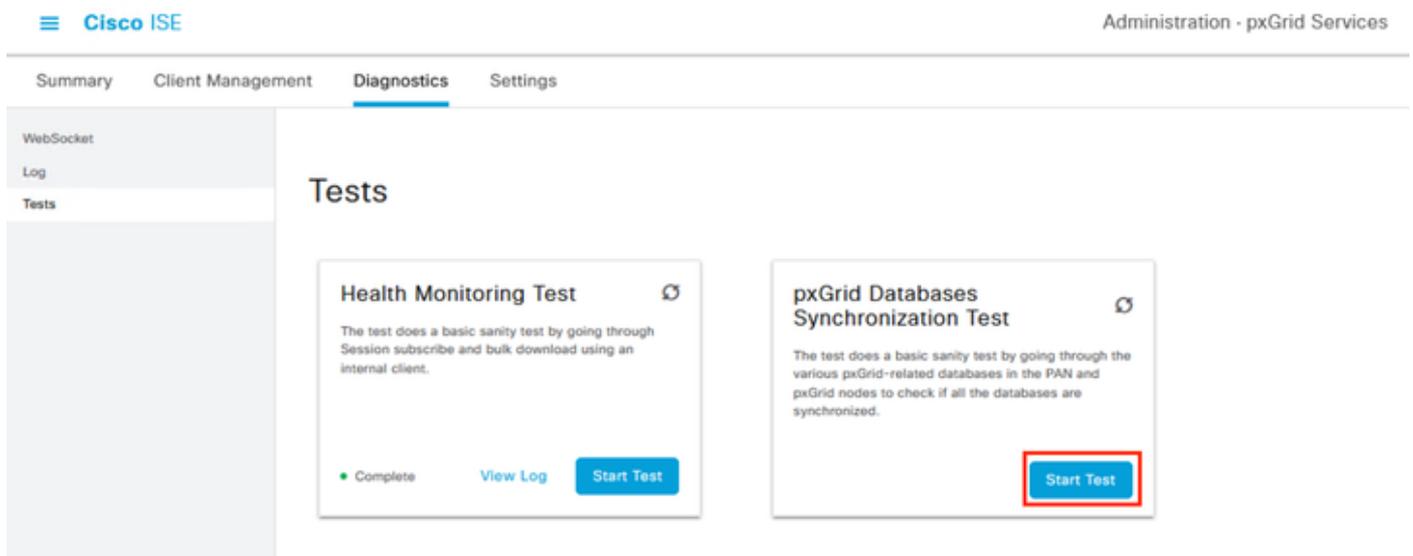
22-Aug-2023 17:03:15 [INFO] ----- Connection Test Completed -----
22-Aug-2023 17:03:15 [INFO] ----- Starting Download Test -----
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions 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 *****

```

La prueba de sincronización de la base de datos PxGrid comprueba si la información dentro de las bases de datos es correcto entre los nodos PAN y pxGrid y sincronizado.

Por lo tanto, la información enviada a los suscriptores de pxGrid es preciso.

Seleccione el opción Iniciar prueba y esperar a que los resultados lleguen a ser evaluados.



Prueba de sincronización de bases de datos PxGrid.

A partir de los registros generados, se obtuvo esta salida.

```

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

```

```

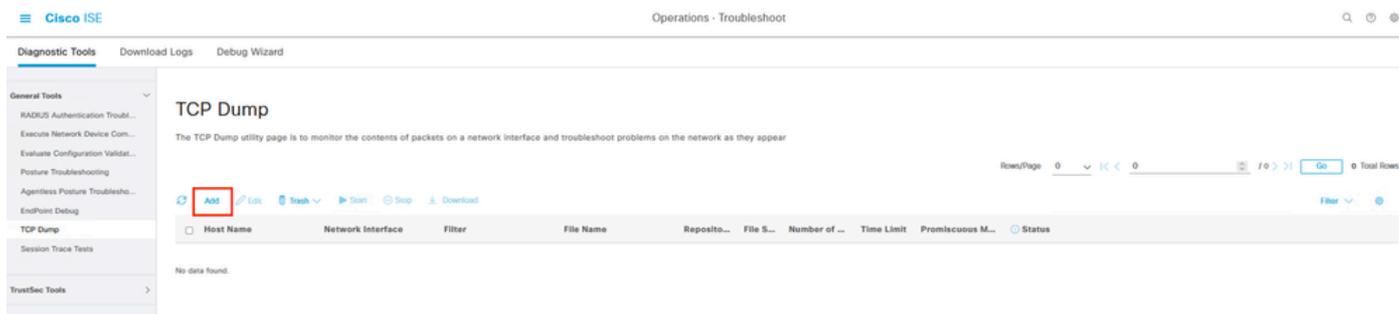
Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex

```

Recopilar una captura en desde los nodos pxGrid que apuntan hacia el nodo FMC principal.

Desplácese al menú Operations > Troubleshoot > Diagnostic Tools > TCP Dump,

Seleccione el opción a Agregar una nueva captura.



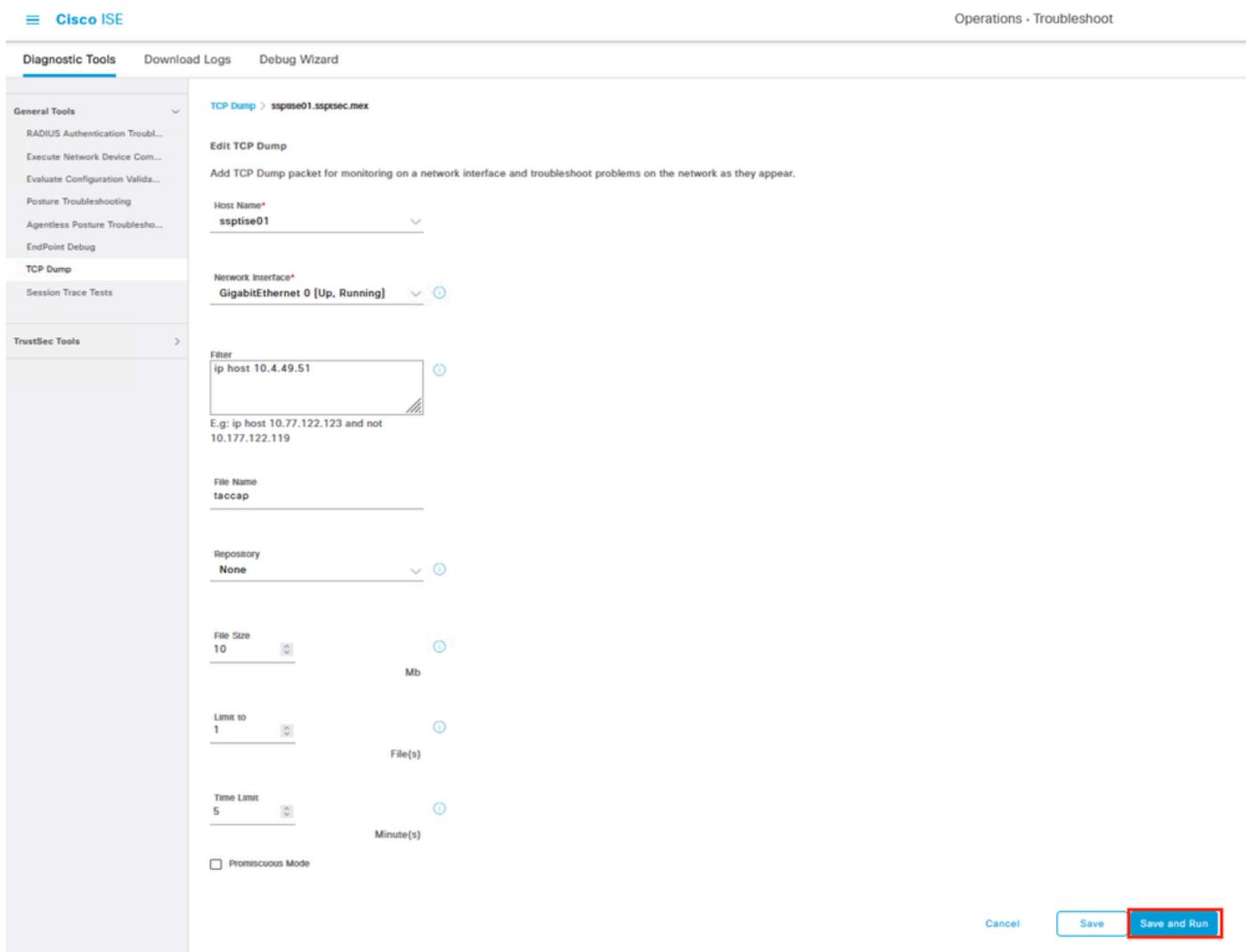
Generación de una captura de paquetes en ISE.

Configure los parámetros para la captura.

IN Nombre de host, seleccione el nodo pxGrid principal seleccionado en el FMC.

Filtro el tráfico con este sintaxis ip host <FMC IP>

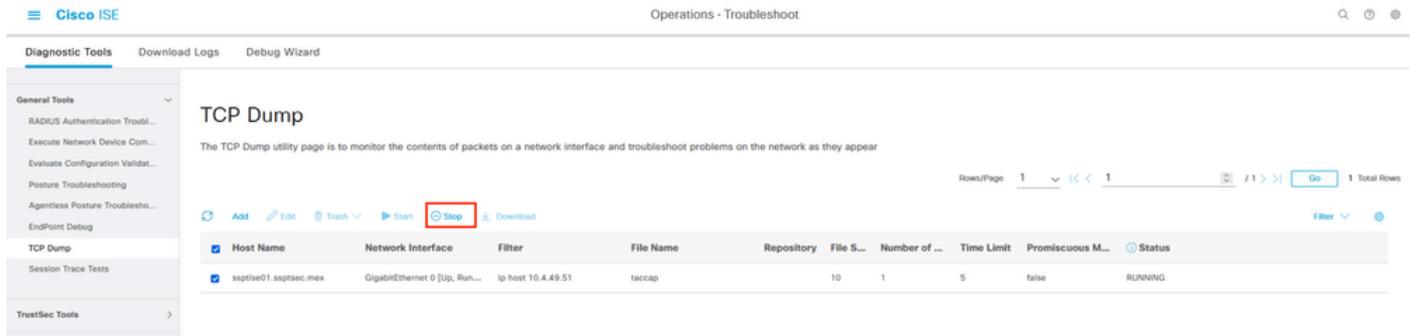
Nombre la captura y luego continuar a Guardar y Ejecutar.



Ejemplo de configuración de captura de paquetes.

En otra ventana, en el menú FMC Integration > Other Integrations > Identity Fuentes, Pruebe la conexión con ISE a través del canal pxGrid.

WCuando se obtiene el resultado de la prueba, continuar a Sarriba la captura en ISE.



Detención de una captura de paquetes en ISE.

Descargar captura e inicia el análisis. Este escenario muestra una captura de una conexión en funcionamiento que puede servir de referencia.

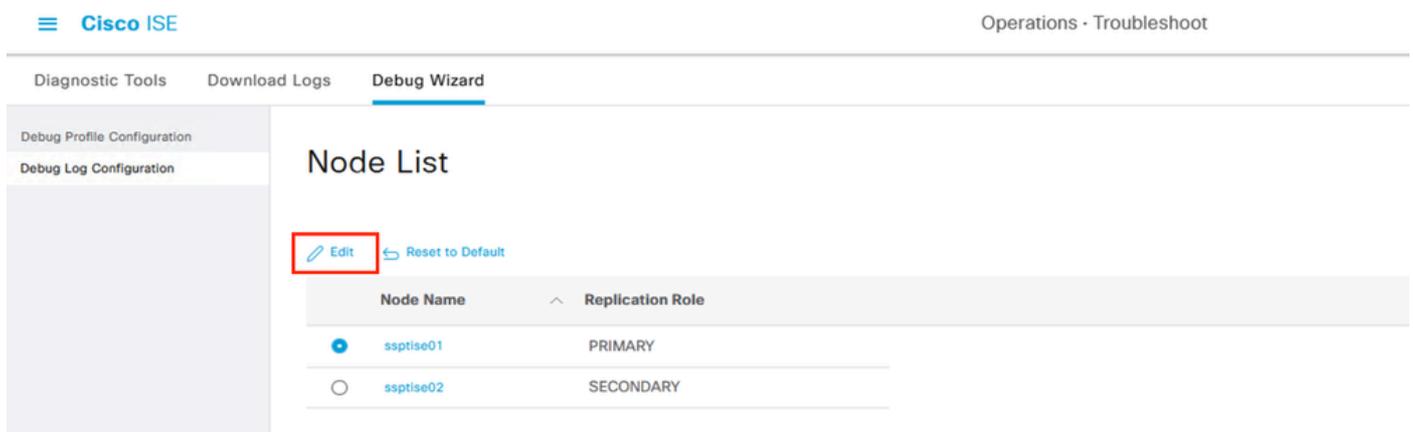
The screenshot shows a network packet capture with columns for Time, Source, Destination, Protocol, Length, and Details. The capture shows a successful TLS handshake between 10.4.49.51 and 10.4.49.41. Key packets include: SYN, ACK, Client Hello, Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message, Application Data, and FIN, ACK.

Comunicación de PxGrid entre ISE y FMC.

Además, en ISE, puede recopilar depuraciones relacionadas con pxProcesamiento de cuadrícula.

Navegar por el menú Operations > Troubleshoot > Debug Wizard > Debug Configuración de registro,

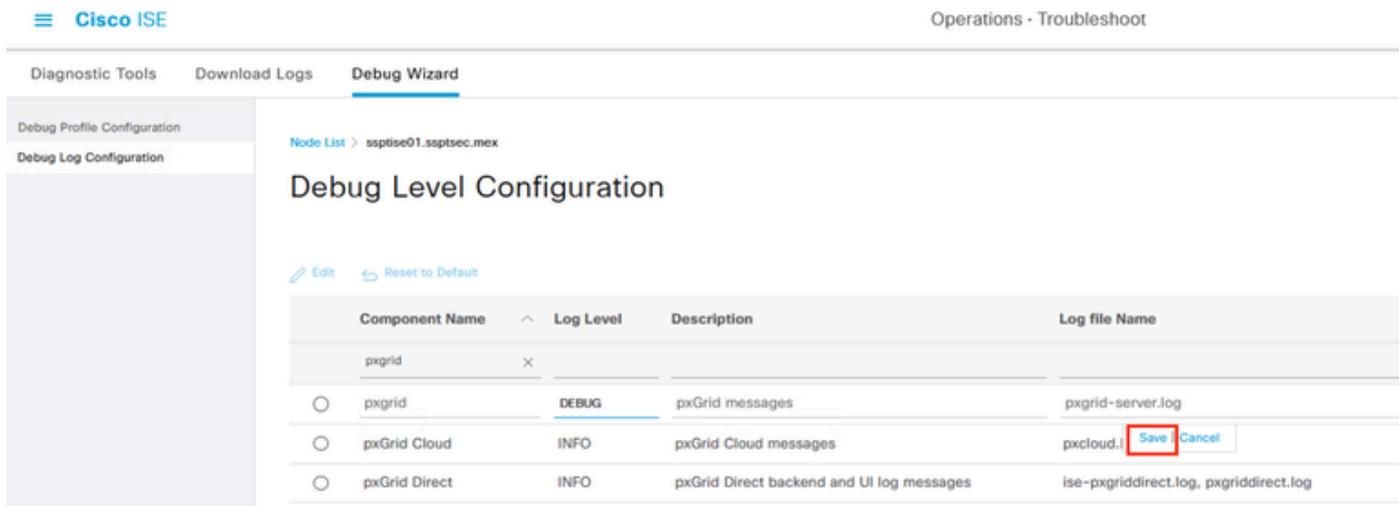
Seleccione el nodo de ISE correspondiente que desee analizar y, a continuación, Editar.



Selección de un nodo para depurar en ISE.

Filtre los componentes mostrados y cambie el Nivel de registro a DEBUG the pxgrid componente a continuar con un análisis.

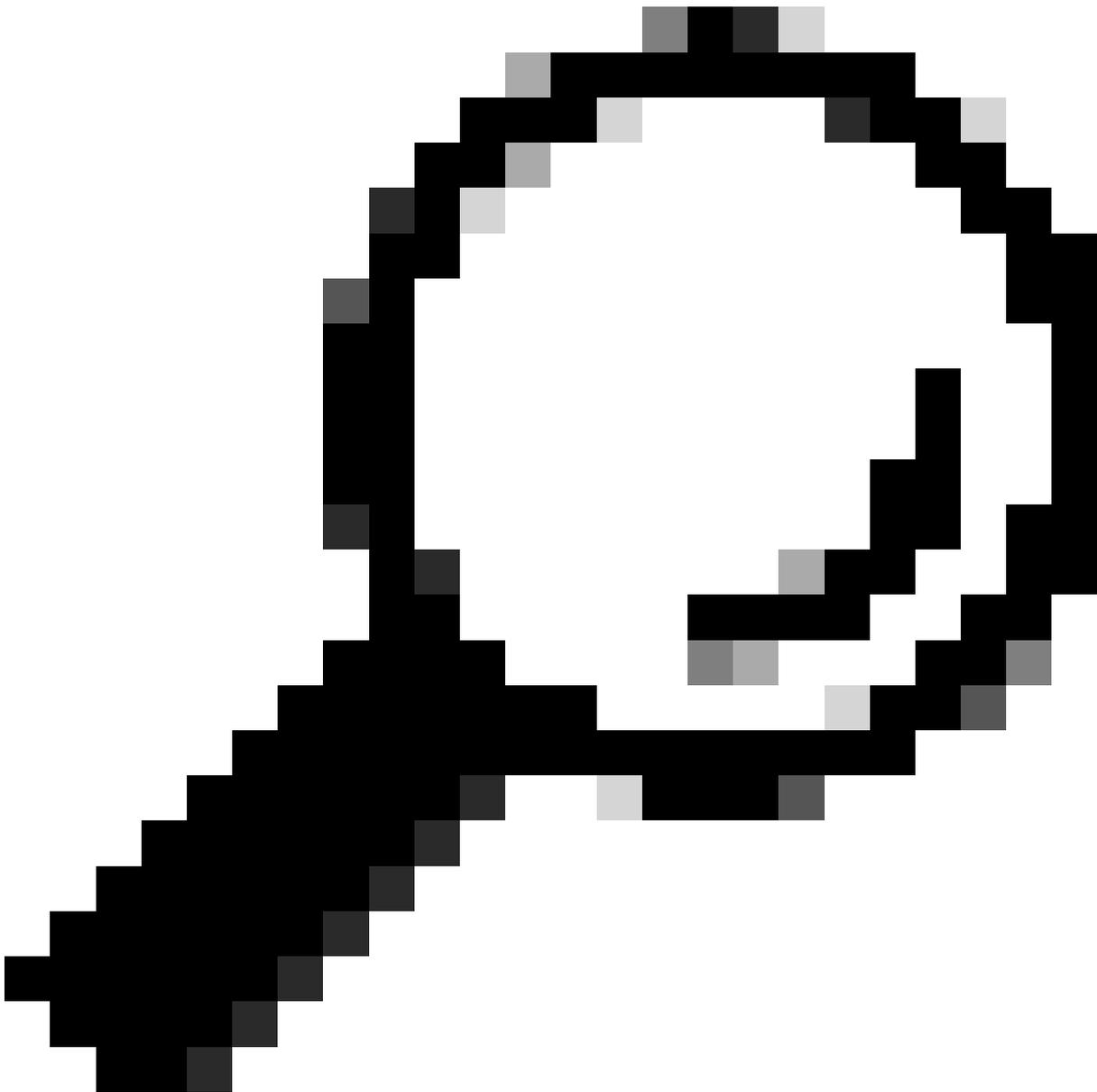
Guardar la configuración.



Cambio del componente pxGrid al nivel de depuración.

Reproduzca el comportamiento que desea analizar. Continuar para analizar los registros recopilados en el archivo pxgrid-server.log. Otros registros que puede revisar en el nodo de ISE para solucionar problemas son:

```
#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
```

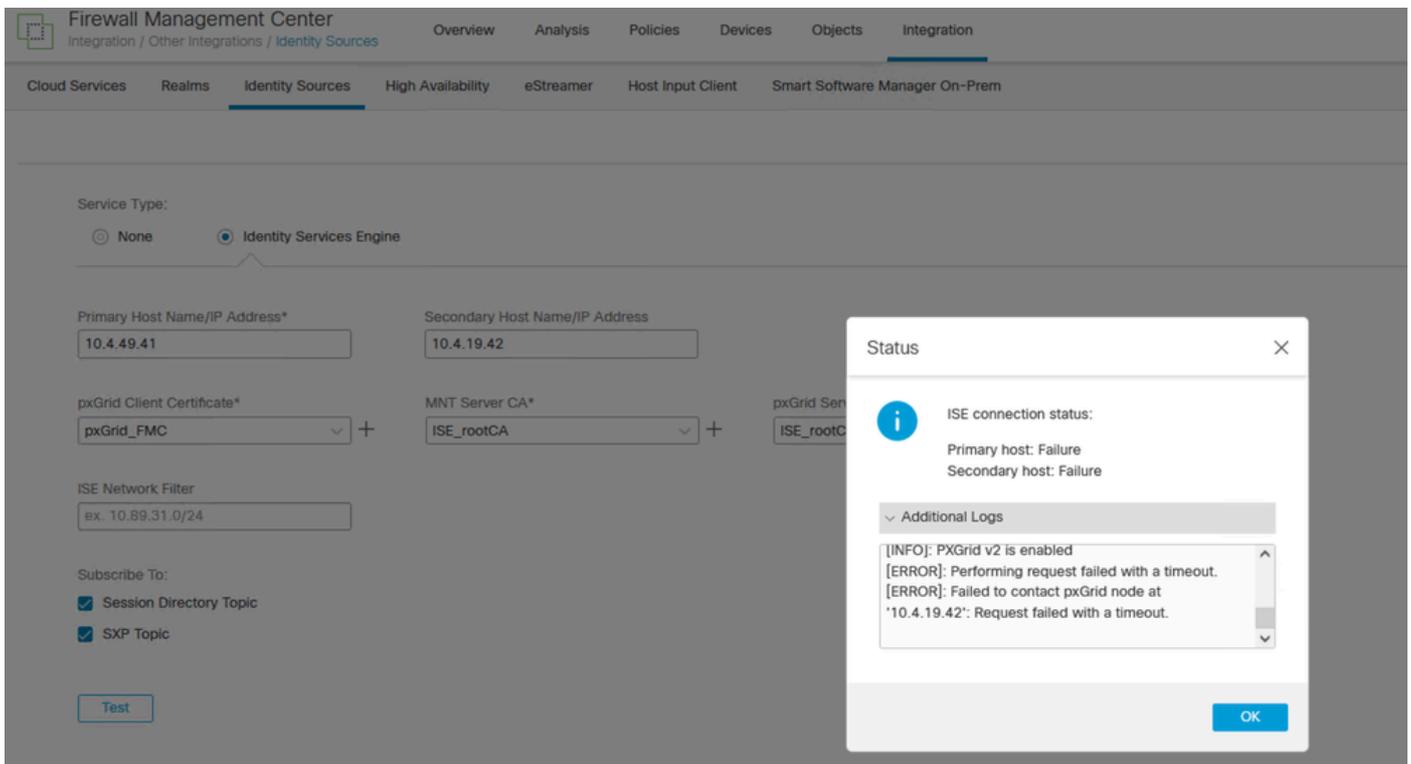


Consejo: Para obtener más recomendaciones sobre la recopilación de registros, consulte el vídeo [How to Enable Debugs on ISE 3.x Versions.](#)

Problemas Comunes.

El cliente suscriptor de PxGrid no está aprobado en ISE.

Para este caso de uso, el resultado relacionado con el botón pxGrid de prueba de FMC muestra este comportamiento:



Error en la conexión PxGrid de FMC.

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.
```

En ISE, observe el comportamiento en el menú Administration > PxGrid Services > Client Management > Clients que indica que el cliente pxGrid (FMC) está pendiente de aprobación.

Seleccione el botón Aprobar, confirme la selección en la siguiente ventana e intente la integración de nuevo.

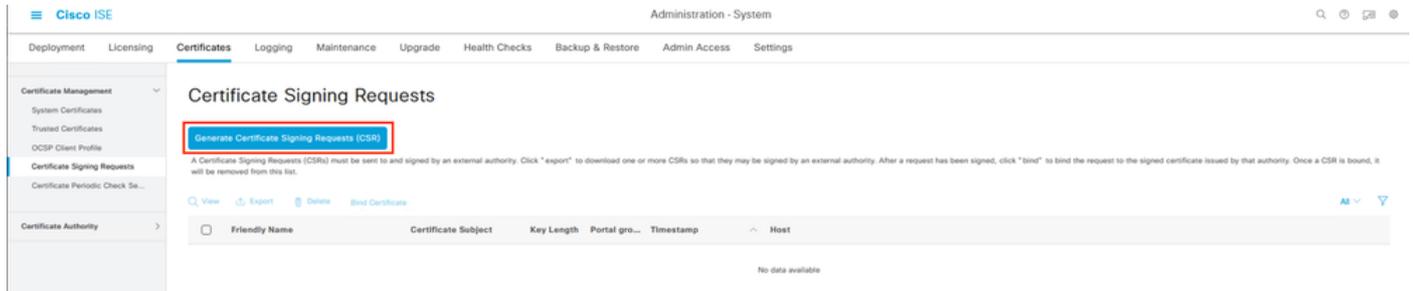
Esta vez la integración se realiza correctamente.

Error relacionado con la cadena de certificados incompleta.

El primer paso que debe comprobar es si la CA raíz de ISE está completada en la opción Ver.

En caso de que falte un certificado en la jerarquía, puede emitir la CA raíz de implementación de ISE completa.

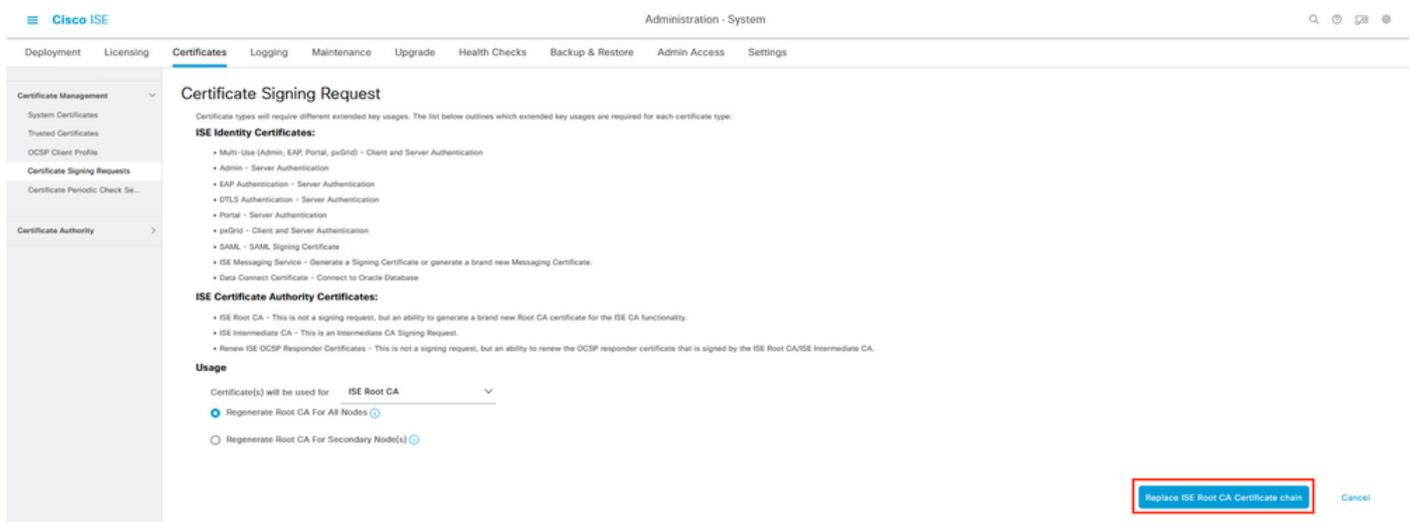
Vaya al menú Administration > System > Certificates > Certificate Management > Certificate Signing Request (CSR) y seleccione ese botón.



Generación de una CSR en ISE.

En este menú, seleccione en Uso CA raíz de ISE y regenerar la CA raíz de ISE para todos los nodos.

Continúe con el botón Reemplace la cadena de certificados de CA raíz de ISE.



Configuración de la solicitud de firma de certificado.

Espere a que se generen los certificados en todos los nodos del implementación.

Al finalizar, ISE muestra la siguiente notificación.

The screenshot shows the Cisco ISE Administration interface. The main navigation bar includes 'Administration - System' and various tabs like 'Deployment', 'Licensing', 'Certificates', 'Logging', etc. The left sidebar shows 'Certificate Management' and 'Certificate Authority' sections. The main content area is titled 'CA Certificates' and contains a table of certificates. A modal dialog box is open, indicating a delay in certificate generation and showing an 'OK' button.

Friendly Name	Status	Trusted For	Serial Number	Issued To
Certificate Services Root CA - n1ise32w00021	Enabled	Infrastructure,Endpoints	56 1C BA C5 B6 69 43 FF 9F E1 7B 84 02 91 F5 52	Certificate Services Root CA - n1ise32
Certificate Services Node CA - n1ise32w00022	Enabled	Infrastructure,Endpoints	2F 9D AC 27 FF 20 43 71 8D 3E FB 2A 85 1D 5D B7	Certificate Services Node CA - n1ise32
Certificate Services Endpoint Sub CA - n1ise32w00023	Enabled	Infrastructure,Endpoints	13 A5 F8 63 5F 5E 4C 24 AE 7A 0A 98 2D 9E 01 BC	Certificate Services Endpoint Sub CA - n1ise32
Certificate Services OCSP Responder - n1ise32w00024	Enabled	Infrastructure,Endpoints		

Confirmación de la generación de certificados.

Confirme si el pxGse completó la cadena de confianza del certificado RID seleccionando la opción Ver en Certificados del sistema.

Referencia.

[Página de desarrolladores de PxGrid de Cisco.](#)

[Guía del administrador de Cisco Identity Services Engine, versión 3.2, capítulo: Cisco pxGrid.](#)

[Guía de instalación de Cisco Identity Services Engine, versión 3.2, capítulo: Referencia de puertos de Cisco ISE](#)

[Guía de referencia CLI de Cisco Identity Services Engine, versión 2.4](#)

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).