

Solución de problemas de Secure Network Analytics (SNA): integración de Identity Services Engine (ISE) "Error de conexión: no se encuentra el servicio en este clúster de ISE"

Contenido

[Introducción](#)

[Integración con Cisco ISE](#)

[Posibles razones del fallo](#)

[Verificación y resolución de problemas](#)

[Causas conocidas](#)

[Problemas de replicación en la implementación de ISE](#)

[Verificar la cadena de certificados PxGrid de ISE](#)

Introducción

Este documento describe cómo validar los problemas de integración de ISE para SMC versión 7.3.2 en adelante. SNA presenta PxGrid v2.0 para el componente de integración de ISE con la versión 7.3.2. Este artículo se centra en algunos mensajes de error específicos que puede encontrar al configurar la integración de Cisco ISE en las versiones 7.3.2 y posteriores.

Para obtener más información sobre PxGrid v2.0 y su funcionalidad, visite [PxGrid v2.0](#)

Integración con Cisco ISE

Cuando SMC se integra con ISE, realiza una solicitud para suscribirse al servicio adecuado en función de las casillas de verificación seleccionadas en la interfaz de usuario de configuración:

Integration options ⓘ

Integrated Product ⓘ

- Cisco ISE
- Cisco ISE PIC (Passive Identity Connector)

Adaptive Network Control ⓘ

Static SGT Classifications ⓘ

Sessions ⓘ

Track sessions derived from machine authentications ⓘ

Según las casillas de verificación seleccionadas, SMC puede solicitar:

Servicio: com.cisco.ise.config.anc

Servicio: com.cisco.ise.trustsec

Servicio: com.cisco.ise.session

Servicio: com.cisco.ise.pubsub

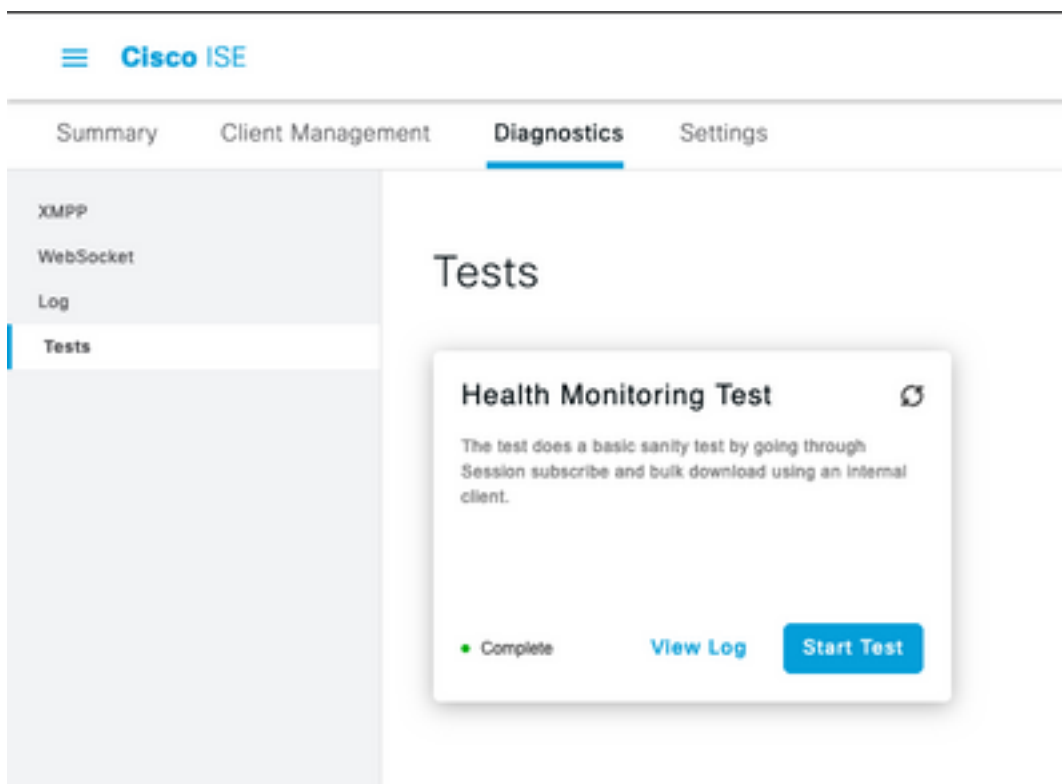
A su vez para estos servicios, SMC se comunica con un nodo ISE para suscribirse al servicio. Cuando SMC realiza una solicitud al nodo de ISE para un servicio, espera saber qué nodos de ISE pueden servir a ese tema o servicio.

Posibles razones del fallo

- "Estado de la conexión:No se ha podido encontrar el servicio erróneo com.cisco.ise.pubsub en este clúster de ISE"
- "Estado de la conexión:Servicio erróneo com.cisco.ise.anc no se encuentra en este clúster de ISE."
- "Estado de la conexión:No se ha encontrado el servicio con errores com.cisco.ise.session en este clúster de ISE."
- "Estado de la conexión:Servicio erróneo com.cisco.ise.trustsec no se encuentra en este clúster de ISE."

Verificación y resolución de problemas

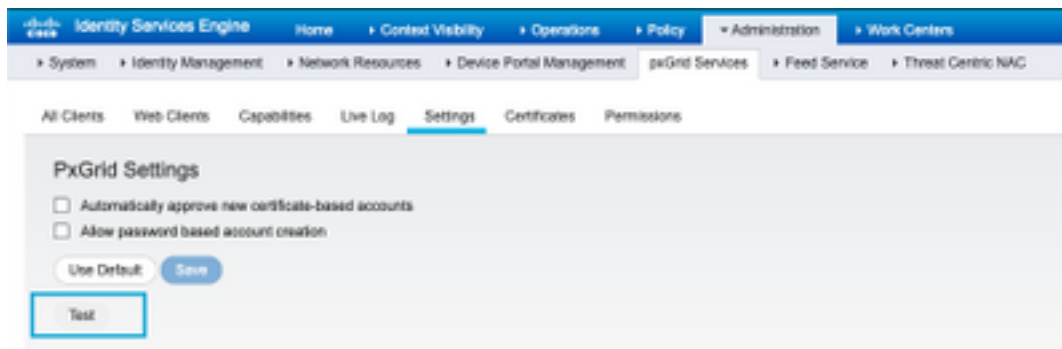
Vaya a **Administration > PxGrid Services > Diagnostics > Tests** y ejecute la herramienta Health Monitoring Test Tool (ISE 3.0 y versiones posteriores)



prueba de supervisión de estado

Herramienta de

Para ISE 2.4, 2.6 y 2.7:



Herramienta de

prueba de supervisión de estado

Los resultados de la prueba se pueden ver en la CLI del nodo PXGrid indicado en el pie de página de la nota Conectado mediante XMPP <nombre de host>.

Ejecute el comando "**show logging application pxgrid/pxgrid-test.log**"

El resultado cuando está conectado y funciona correctamente indica:

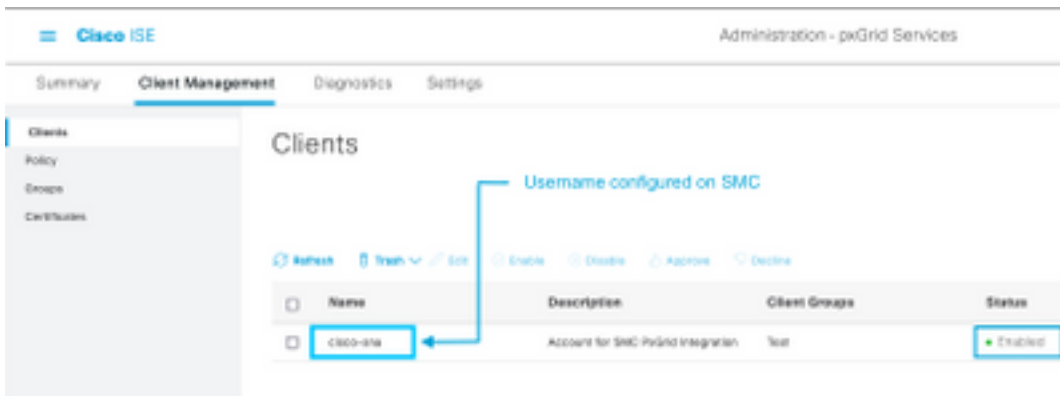
```
asc-ise24p12-347/admin# show logging application pxgrid/pxgrid-test.log
2021-10-29 01:46:32 INFO TestGridConnection:55 - Inicio de la conexión de prueba pxgrid.....
2021-10-29 01:46:33 INFO TestGridConnectionHelper:307 - SUMMARY>
Subscribe=CONNECTING,session-cnt=0; BulkDownload=NOT STARTED,bd-session-cnt=0
2021-10-29 01:46:33 INFO Configuración:313 - Conexión al host asc-ise24p12-347.rtpaaa.net
2021-10-29 01:46:33 INFO Configuración:318 - Conectado OK al host asc-ise24p12-
347.rtpaaa.net
2021-10-29 01:46:33 INFO Configuración:343 - Cliente Inicie sesión en el host asc-ise24p12-
347.rtpaaa.net
2021-10-29 01:46:34 INFO Configuración:345 - Cliente Login Aceptar para alojar asc-ise24p12-
347.rtpaaa.net
2021-10-29 01:46:35 INFO NotificationHandlerSmack:70 - terminado de actualizar el estado de
conexión.
2021-10-29 01:46:35 INFO TestGridConnectionHelper:312 - SUMMARY>
Subscribe=CONNECTED,session-cnt=0; BulkDownload=NOT STARTED,bd-session-cnt=0
2021-10-29 01:50:36 INFO TestGridConnection:164 - SUMMARY>
Subscribe=CONNECTED,session-cnt=0;BulkDownload=SUCCESS,bd-session-cnt=0
2021-10-29 01:50:36 INFO NotificationHandlerSmack:81 - estado de conexión despejado...
2021-10-29 01:50:36 INFO TestGridConnectionHelper:322 - Cliente desconectado
2021-10-29 01:50:36 INFO TestGridConnection:75 - SUMMARY>
Subscribe=DISCONNECTED,session-cnt=0;BulkDownload=DISCONNECTED,bd-session-cnt=0
```

Verifique si la cuenta utilizada para conectar SMC a ISE está habilitada:

Compruebe que el cliente está aprobado y, si está pendiente, apruébelo

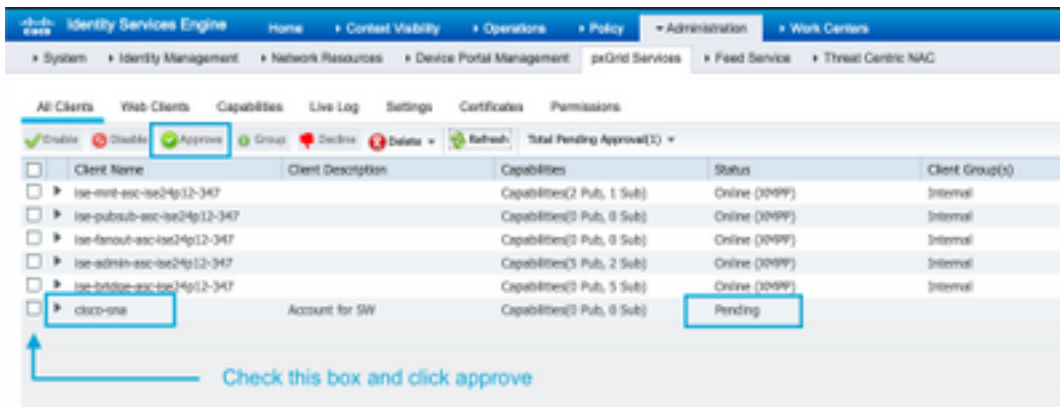
ISE 3.0 y versiones posteriores:

Administration > PxGrid Services > Client Management > Clients:



ISE 2.4, 2.6 y 2.7:

Administration > PxGrid Services > All Clients



Para comprobar el estado de conexión del cliente SMC PxGrid y a qué nodo ISE está conectado, vaya a **Administration > PxGrid Services > Diagnostics > WebSocket**



Causas conocidas

- Nodos con PxGrid Personal habilitado que se enfrentan a problemas de replicación en la implementación de ISE
- Problemas de confianza del certificado PxGrid

Problemas de replicación en la implementación de ISE

La replicación es fundamental para mantener la información actualizada en todos los nodos miembros de una implementación. Si un nodo que ejecuta el rol PxGrid informa de problemas de replicación, es posible que no tenga información actualizada sobre los temas y servicios que

puede servir a los clientes de PxGrid.

Si el nodo informa de alarmas de error de replicación o replicación lenta:



Replication Failed

O



Slow Replication Error

Esta es una causa potencial del fallo de integración.

Para tomar medidas correctivas:

Verifique la conectividad IP con el nodo ISE, inicie sesión a través de SSH y verifique que los servicios se estén ejecutando mediante:

```
# show application status ise
```

P. ej.

```
asc-ise30p2-353/admin# show application status ise
```

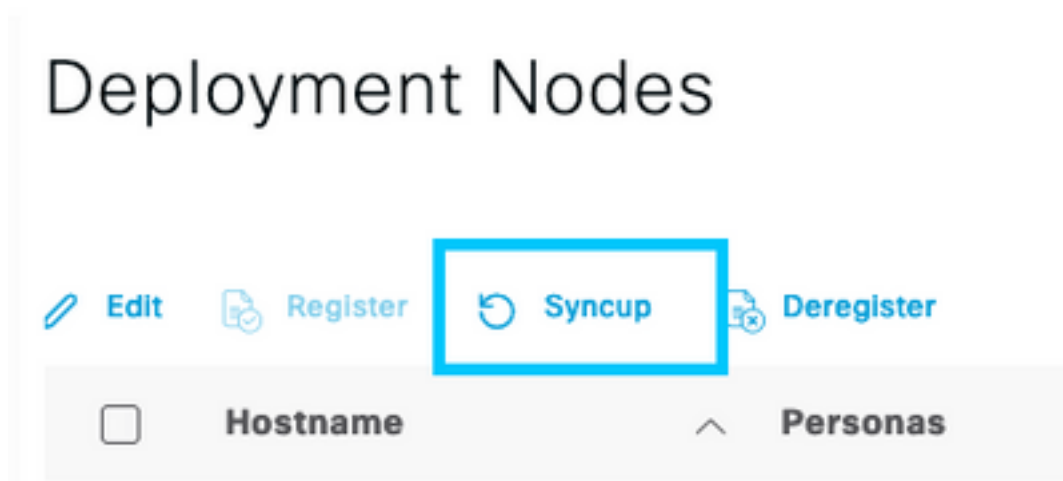
```
ID DE PROCESO DE ESTADO DE NOMBRE DE PROCESO ISE
```

```
-----  
Database Listener que ejecuta 24872  
Servidor de base de datos con 114 PROCESOS  
Servidor de aplicaciones que ejecuta 40137  
Base de datos de perfiles que ejecuta 35916  
Motor de indexación ISE deshabilitado  
Conector AD con 40746  
Base de datos de sesiones de M&T deshabilitada  
Procesador de registro de M&T deshabilitado  
Certificate Authority Service que ejecuta 40609  
Servicio EST con 77903  
Servicio de motor SXP deshabilitado  
Docker Daemon ejecutando 28517  
Servicio TC-NAC deshabilitado  
pxGrid Infrastructure Service deshabilitado  
pxGrid Publisher Subscriber Service deshabilitado  
Administrador de conexiones pxGrid deshabilitado  
Controlador pxGrid deshabilitado  
Servicio WMI PassiveID deshabilitado  
Servicio Syslog PassiveID deshabilitado  
Servicio API PassiveID deshabilitado  
Servicio de agente PassiveID deshabilitado  
PassiveID Endpoint Service deshabilitado  
Servicio SPAN de PassiveID deshabilitado  
Servidor DHCP (dhcpd) deshabilitado
```

Servidor DNS (con nombre) deshabilitado
Servicio de mensajería ISE con 29277
ISE API Gateway Database Service con 32173
ISE API Gateway Service con 38161
Servicio de políticas de segmentación deshabilitado
Servicio de autenticación REST deshabilitado
Conector SSE deshabilitado

Realice la sincronización manual del nodo afectado en **Administration > System > Deployment** .

Seleccione el nodo que informa de problemas y haga clic en **Syncup**



Nota: Esto da como resultado un reinicio de los servicios en el nodo que se está sincronizando y podría hacer que el nodo deje de funcionar durante 30 minutos. Se recomienda realizar esta actividad en una ventana de cambio controlado.

Verificar la cadena de certificados PxGrid de ISE

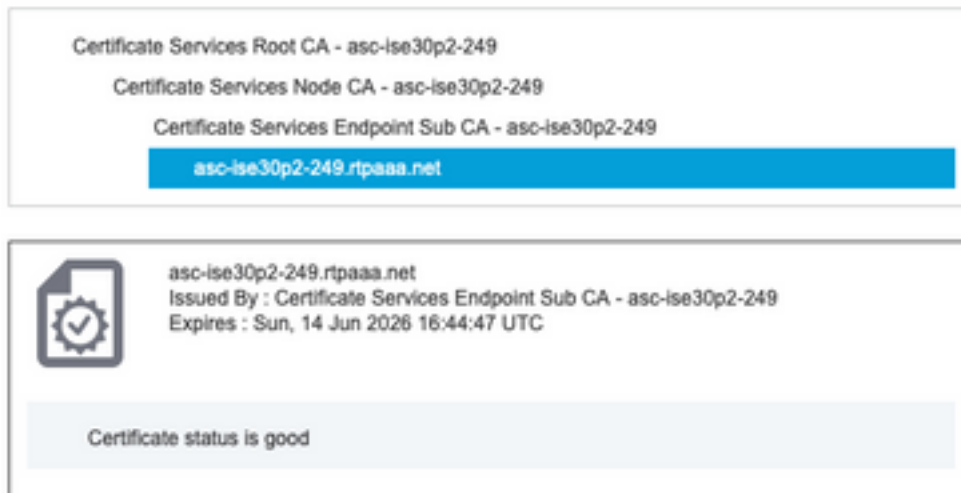
Vaya a **Administration > System > Certificates** en la GUI de ISE

Cada nodo con PxGrid Persona habilitado tiene un certificado con el rol PxGrid asociado.

Estos certificados pueden estar firmados por una CA de terceros o la CA interna de ISE. Marque la casilla junto al certificado y presione la vista. Debe mostrar los detalles del certificado y la cadena de certificados. También hay un indicador de estado en los detalles del certificado que indica si el certificado es bueno o si la cadena está incompleta.

Si el certificado está firmado por la CA interna de ISE:

Certificate Hierarchy



Hay 4 niveles, empezando desde arriba:

1. CA raíz de ISE: se trata del certificado de CA y cada implementación solo tiene una CA raíz de ISE, que es el nodo de administración principal.
2. CA de nodo de ISE: se trata de una CA intermedia cuyo certificado lo emite la CA raíz de ISE y también es el nodo de administración principal
3. ISE Endpoint Sub CA: es el tercer nivel y el emisor del certificado de identidad PxGrid. Cada nodo de la implementación tiene su propia subCA de terminal de ISE emitida por la CA de nodo de ISE (nodo de administración principal)
4. Certificado de identidad PxGrid: Es el certificado que el nodo ISE presenta a un cliente PxGrid, es decir, SMC, durante la integración y la comunicación

Si dispone de un certificado firmado por la CA de su organización independiente de ISE o por una CA conocida de terceros:

Verifique que la CA raíz y cualquier CA intermedia que haya firmado el certificado PxGrid estén instaladas en el almacén de certificados de seguridad de confianza en ISE, en **Administration > System > Certificates > Certificate Management > Trusted Certificates**

En ambos casos, al ver el certificado, la interfaz de usuario debe indicar **"El estado del certificado es bueno"**.

Condición de error:

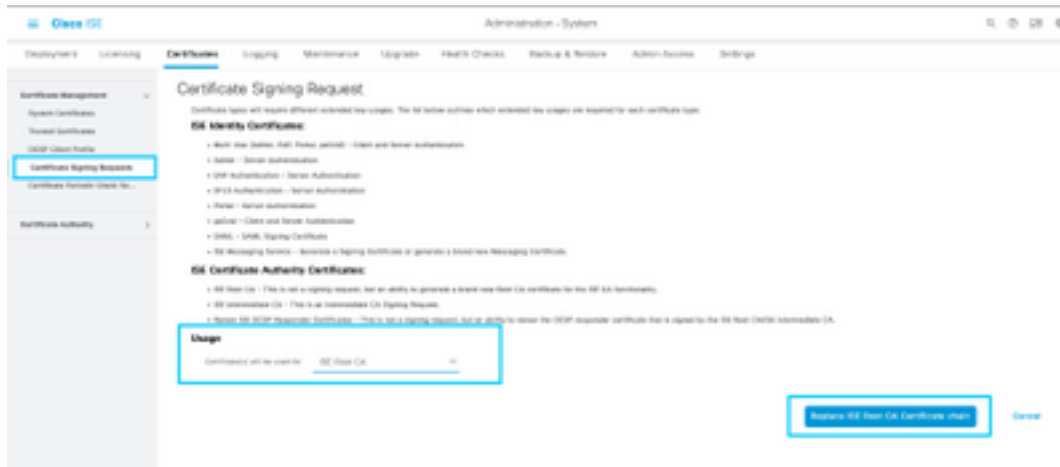
✘ Certificate trust chain is incomplete

Problemas de confianza del certificado PxGrid

Si la cadena de confianza de certificados está incompleta cuando la CA interna de ISE está en uso, es necesario volver a generar la CA raíz de ISE, que a su vez regenerará los certificados PxGrid de ISE como parte del proceso. Actualice el almacén de confianza de su SMC con la CA

raíz de ISE y la CA de nodo de ISE recién generadas desde el administrador principal y el certificado de CA secundaria de terminal de ISE de cada nodo de PxGrid.

Para reemplazar la cadena de CA raíz de ISE, navegue hasta **Administration > System > Certificates > Certificate Management > Certificate Signing Requests** y seleccione **Generate Certificate Signing Request** que presenta esta interfaz de usuario:



En el menú desplegable, seleccione **ISE Root CA** y seleccione **Replace ISE Root CA Certificate Chain**

Si la cadena de confianza de certificados está incompleta cuando una CA externa está en uso, agregue los certificados que faltan al almacén de confianza de ISE en **Administration > System > Certificates > Certificate Management > Trusted Certificates** y reinicie los servicios en el nodo mediante la emisión de "application stop ise" seguida de "application start ise" en la CLI de ISE. Los certificados de CA se agregan accediendo a la GUI de la implementación de ISE en el nodo de administración principal, pero los servicios deben reiniciarse mediante CLI en el nodo que muestra el error de estado del certificado.

Nota: El reinicio de los servicios desconecta el nodo durante 15-20 minutos.

Si los problemas persisten después de tomar estas medidas correctivas, por favor solicite [apoyo](#) para obtener asistencia.

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).