Solucionar problemas de certificados de administración de ISE caducados

Contenido

Introducción

Este documento describe cómo resolver problemas y renovar un certificado de administrador caducado de Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Implementación de Cisco ISE.
- Gestión de certificados en Cisco ISE.

Componentes Utilizados

La información de este documento se basa en las siguientes versiones de software:

- Parche 4 de Cisco Identity Services Engine (ISE) versión 3.3.

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

Este documento se centra en la implementación distribuida; sin embargo, puede utilizar el mismo plan de solución de problemas en un nodo independiente.

En la implementación distribuida de ISE, el nodo es el nodo de administración principal (PPAN) o secundario.

Este documento utiliza el certificado ISE Admin como certificado autofirmado para demostrar el impacto del certificado caducado, pero este enfoque no se recomienda para un sistema de producción. Es mejor utilizar el certificado firmado por la autoridad para el uso del administrador.

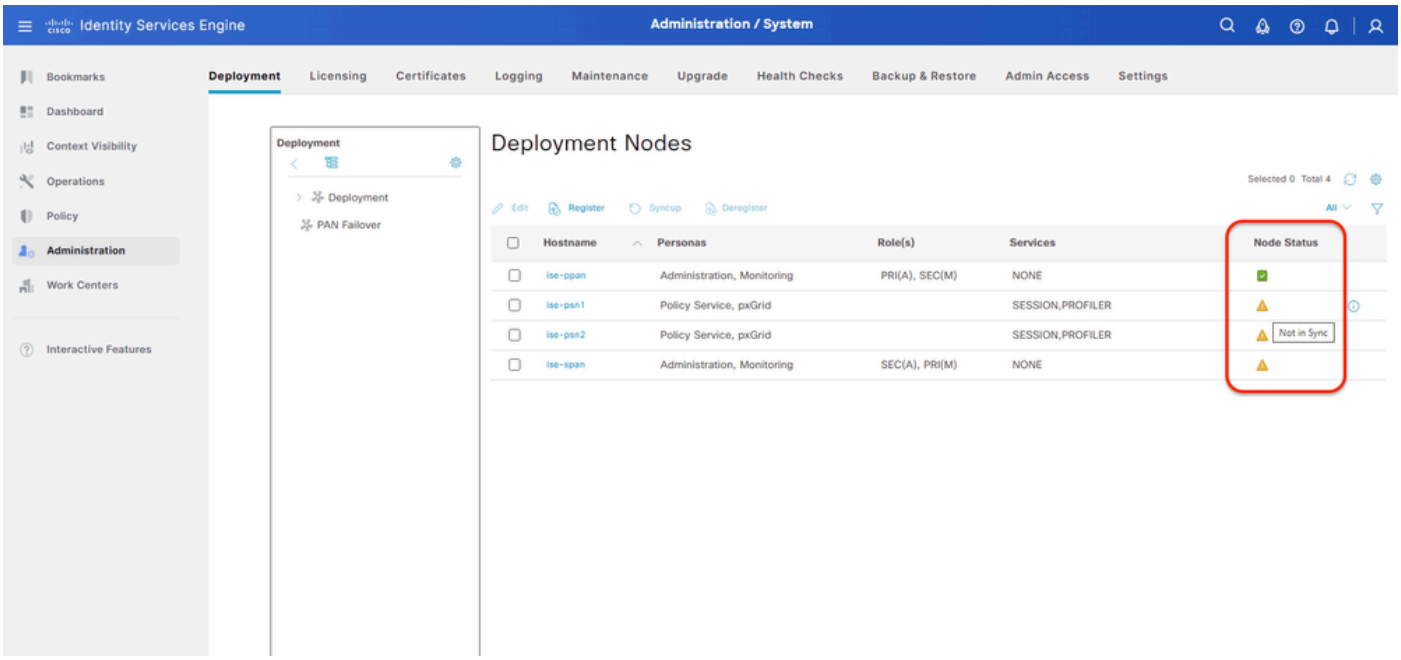
Nota: Cisco recomienda mantener el certificado de administrador en estado correcto y planificar la renovación por adelantado. Encontrará esta guía que le ayudará a realizar un seguimiento y renovar los certificados del sistema ISE (Configurar renovaciones de certificados en ISE).

Certificado de administración de ISE (caducado)

Validar estado del certificado de administrador

Paso 1. Compruebe el estado de despliegue. Navegue hasta Administración > Sistema > Despliegue.

Puede verificar el estado de los nodos secundarios, como se muestra, los tres nodos secundarios son (No sincronizado).

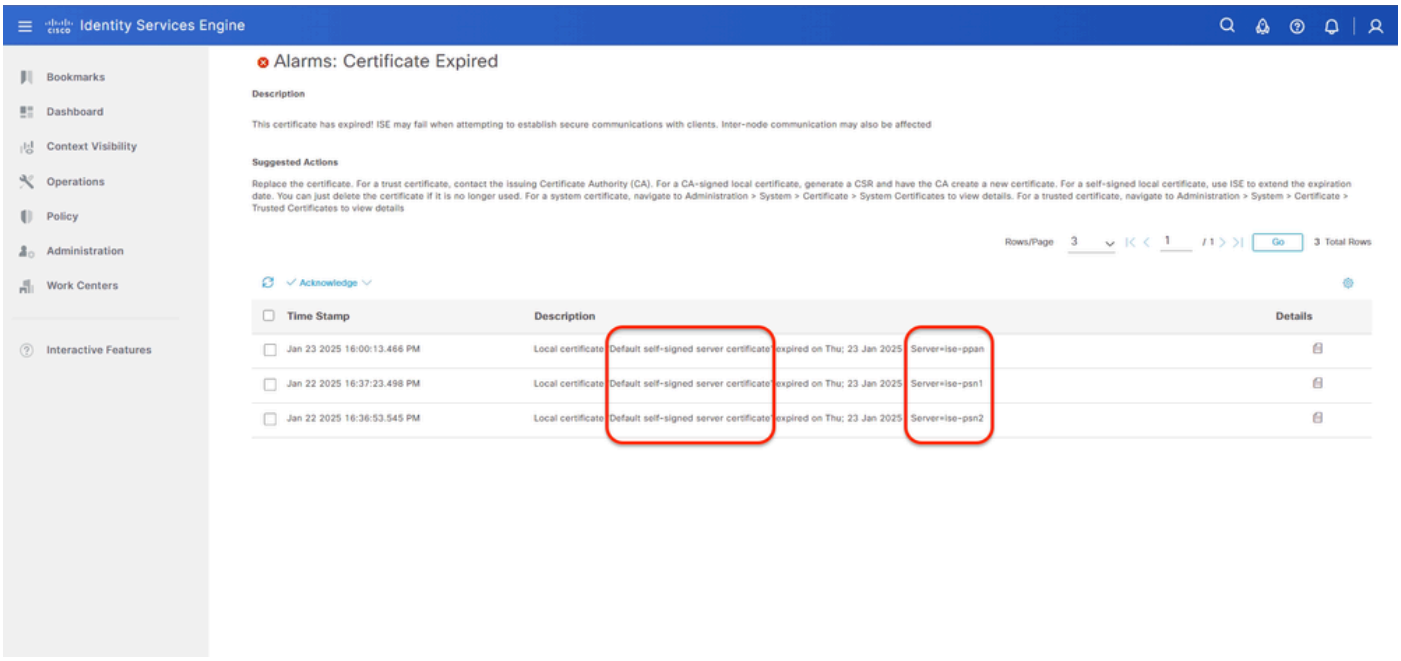


Estado de implementación

Paso 2. Revise las alarmas. Navegue hasta Panel > Alarmas > (Certificado expirado).

Para confirmar qué nodo y qué certificado ha caducado.

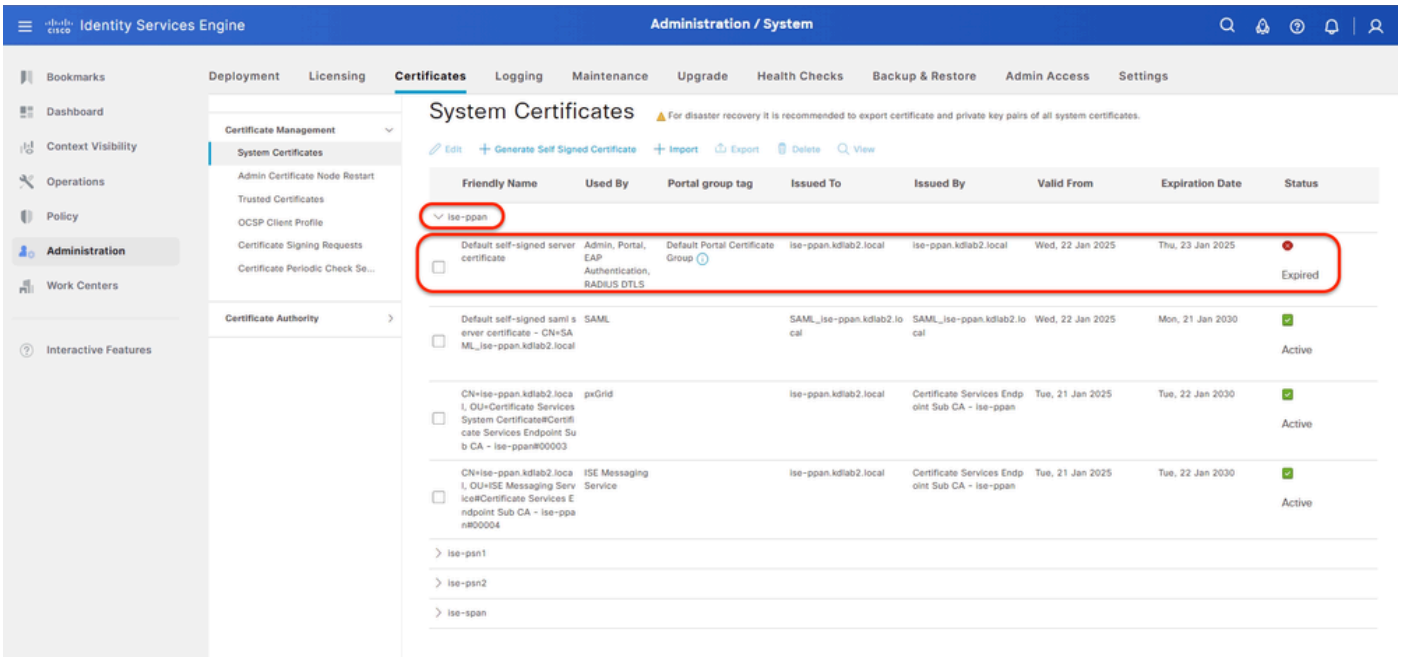
Nota: Si el nodo de administración principal (PPAN) ha caducado antes que cualquier nodo secundario, no podrá ver ninguna alarma de dicho nodo, eso es lo que ha ocurrido con el nodo de administración secundario (SPAN) en esta alarma.



Alarmas (certificado caducado)

Paso 3. Compruebe el estado del certificado de administración. Vaya a Administration > System > Certificates > Certificate Management > System Certificates > Expand node.

1. Nodo de administración principal (PPAN):

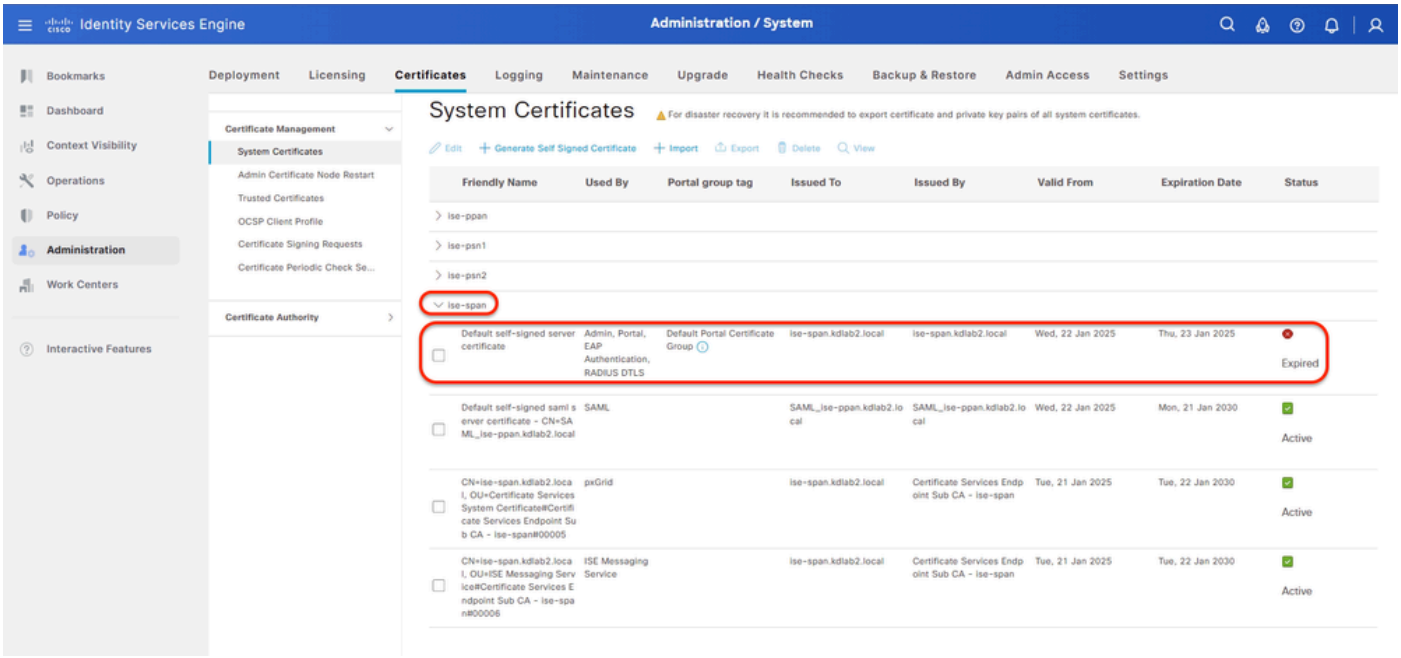


Estado del certificado de administración de PPAN

2. Nodos secundarios.

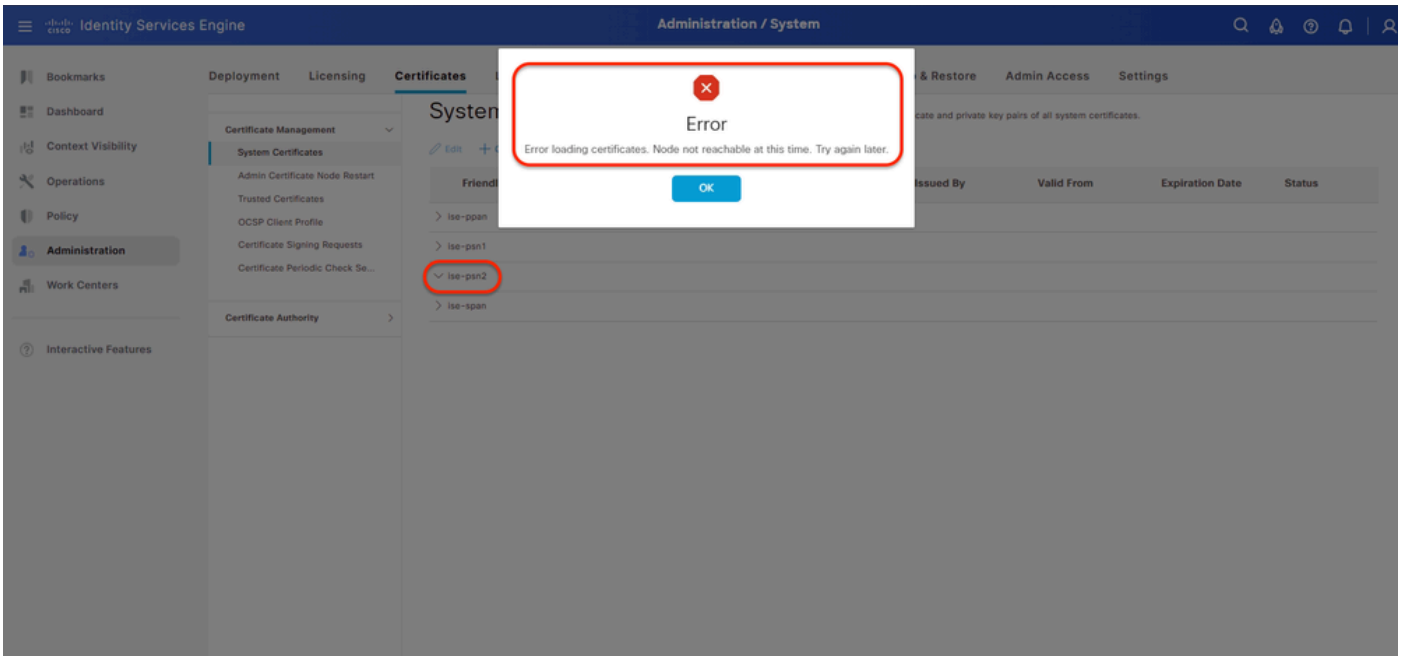
Para los nodos secundarios podría ser 1 de 2 opciones y en ambos casos debe aplicar el mismo plan de acción:

A. Puede Expandir el certificado del sistema de nodo y confirmar que el certificado de administración ha caducado:



Estado del certificado de administrador del nodo secundario

B. Error de lanzamiento ("Error al cargar certificados. No se puede alcanzar el nodo en este momento. Inténtelo de nuevo más tarde.") como se muestra para (ise-psn2



Nodo secundario no alcanzable

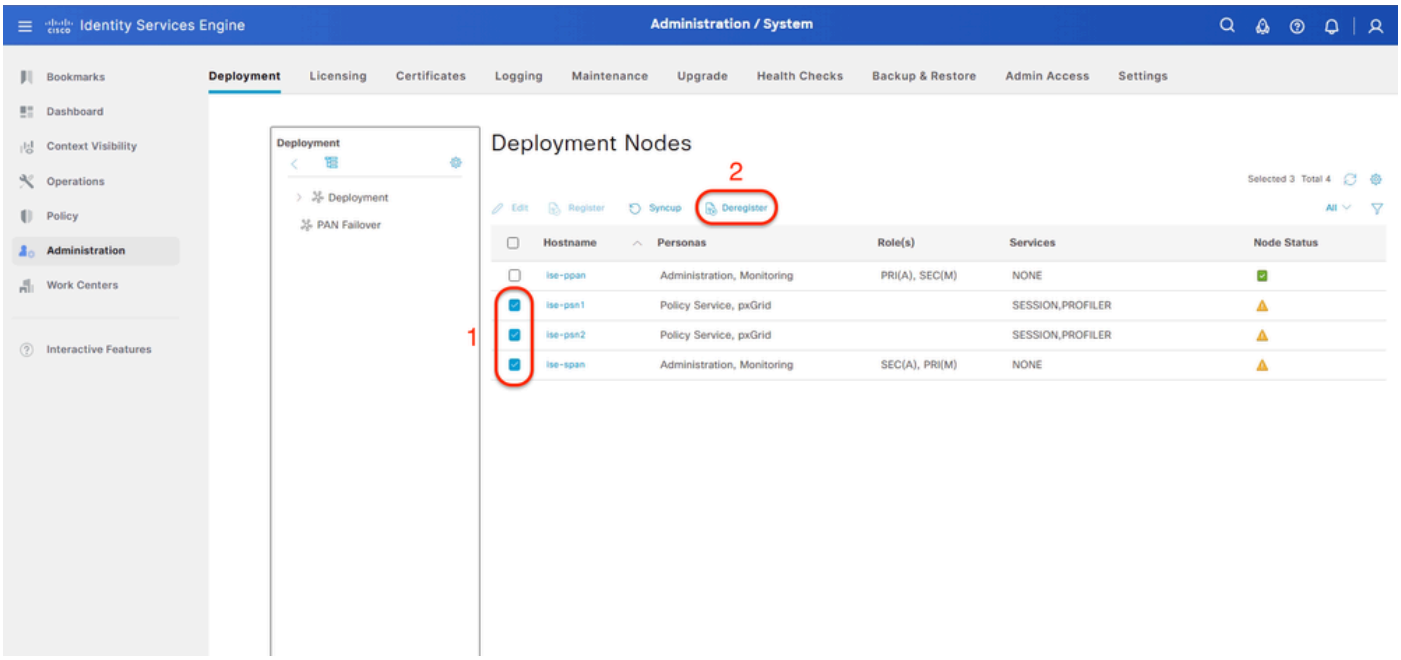
Plan de acción

Después de confirmar que el certificado de administrador ha caducado para los 4 nodos, debe seguir estos pasos:

Paso 1. Anule el registro de todos los nodos secundarios de la implementación distribuida (solo si el certificado de administrador ha caducado).

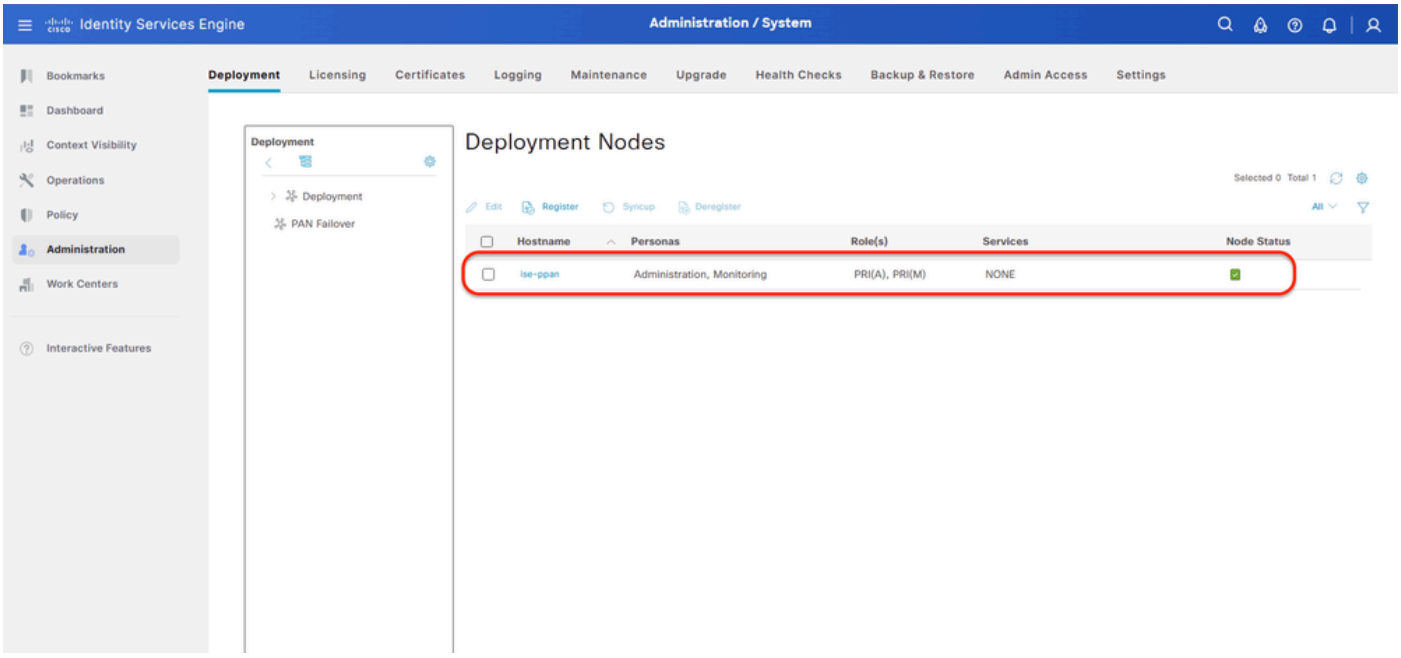
Vaya a Administration > System > Deployment > Check [√] de los nodos secundarios y haga clic en Deregister.

Nota: Anular el registro del nodo significa que se mueve a independiente y, a continuación, puede renovar el certificado de administrador en este nodo.



Anulación del registro de nodos secundarios

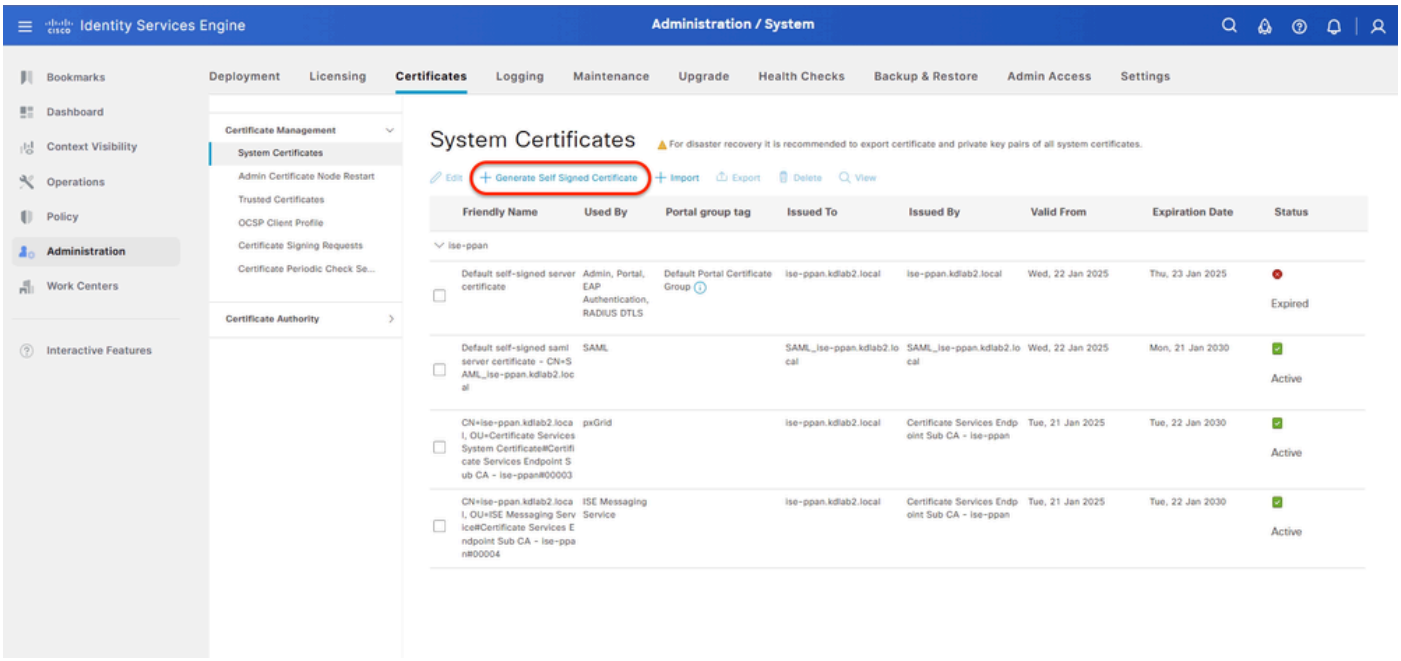
Nota: Recuerde anular el registro solo de los nodos secundarios en los que el certificado de administrador ya haya caducado y conservar el resto. En este documento, todos los nodos secundarios han caducado.



Se anulará el registro de todos los nodos secundarios

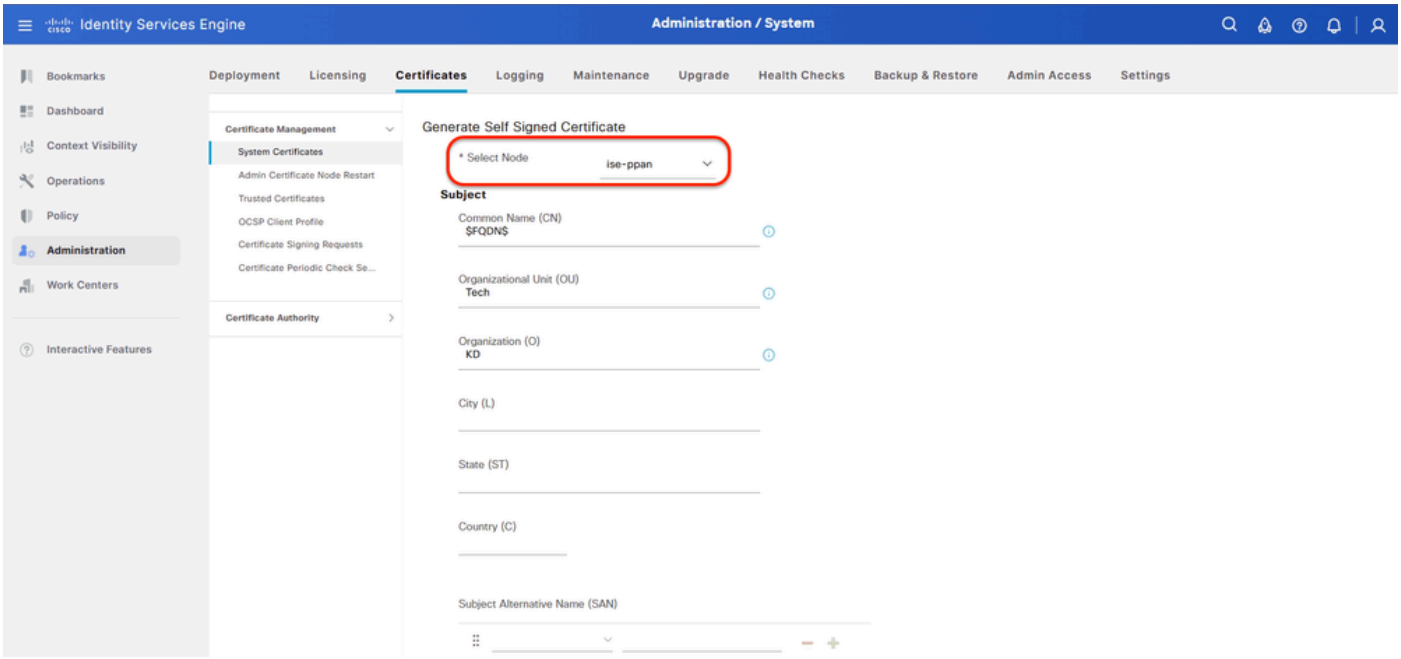
Paso 2. Renueve el certificado de administrador del nodo de administración principal (PPAN).

1. Vaya a Administración > Sistema > Certificados > Administración de certificados > Certificados del sistema > Haga clic en +Generar certificado con firma automática:



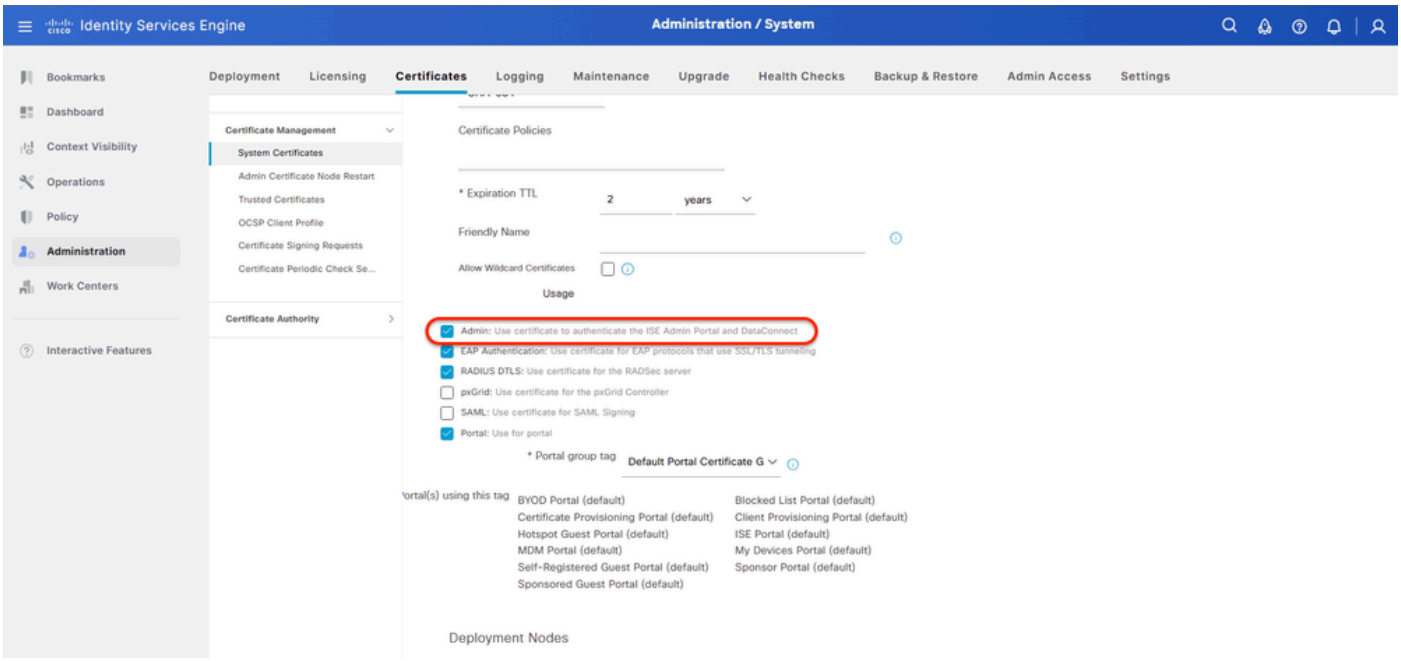
Generar nuevo certificado de administrador autofirmado

2. Seleccione el nodo de administración principal (PPAN) (ise-ppan) y rellene la información del certificado:



Seleccione el nodo de administración principal (PPAN)

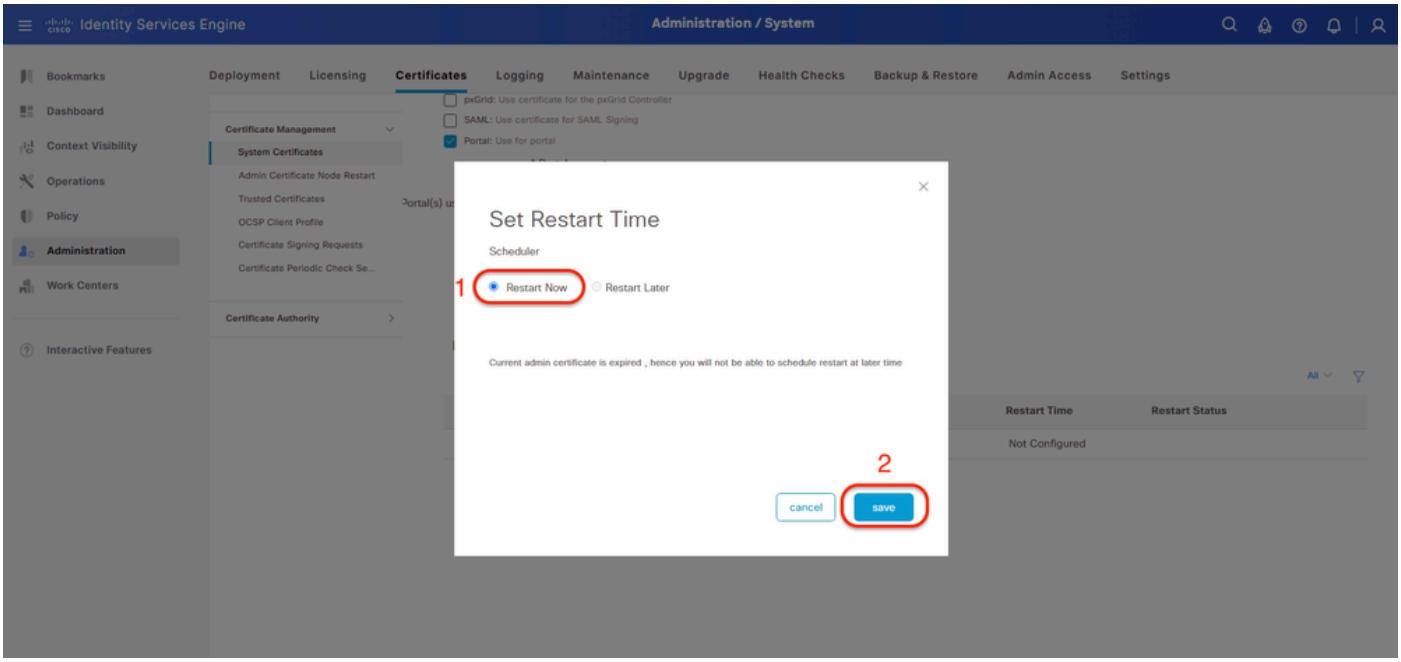
3. Marque [√] el uso de Admin.



Uso del administrador

4. Establezca el Tiempo de reinicio en Reiniciar ahora para el nodo de administración principal (PPAN). Establezca todos los nodos de la implementación en Reiniciar ahora o Reiniciar más tarde.

Después de renovar un certificado de administrador (un certificado configurado para el uso del administrador) en el nodo de administración principal (PPAN), se deben reiniciar todos los nodos de la implementación.



Establezca la hora de reinicio en Now

5. Haga clic en Enviar.

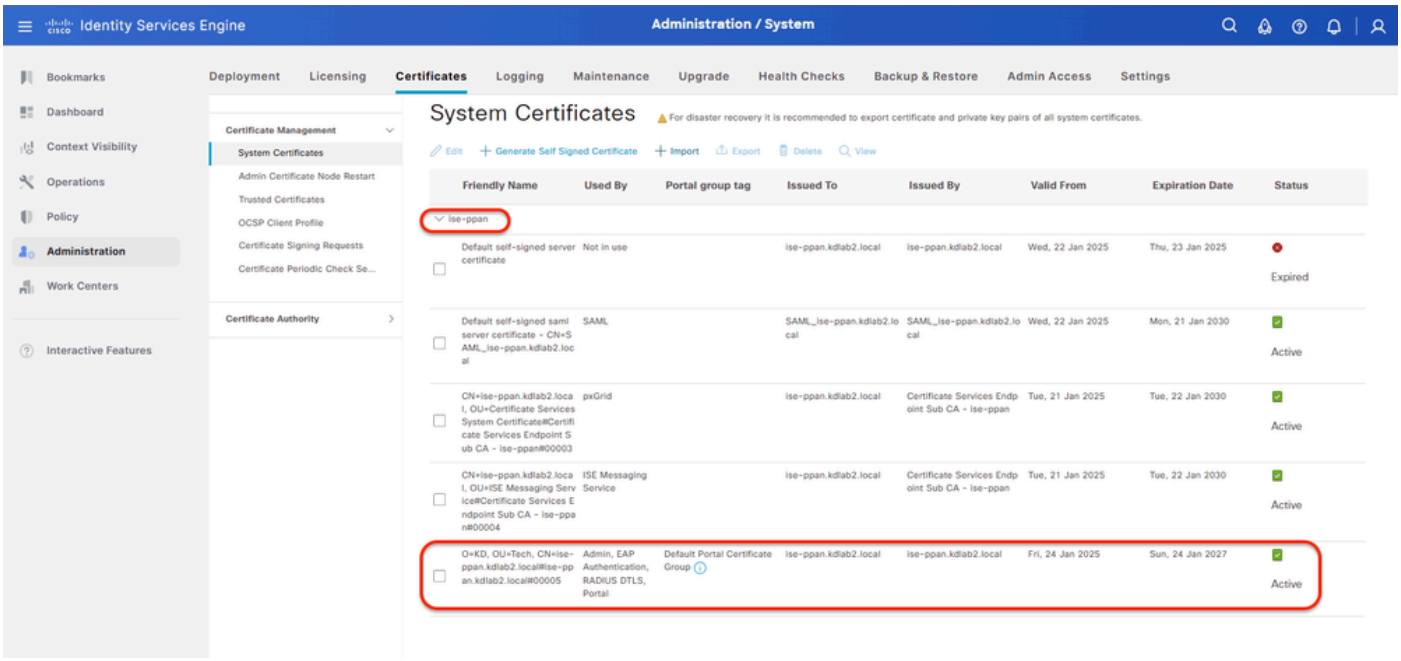
Nota: Después de renovar un certificado de administrador (un certificado configurado para el

uso del administrador) en el nodo de administración principal (PPAN), se deben reiniciar todos los nodos de la implementación. Puede reiniciar cada nodo inmediatamente o programar los reinicios más tarde. Esta función le permite asegurarse de que los reinicios automáticos no interrumpen ningún proceso en ejecución, lo que le proporciona un mayor control sobre el proceso.

Puede ver y editar los reinicios programados en la ventana Administration > System > Certificates > Admin Certificate Node Restart, que está disponible en Cisco ISE Release 3.3.

6. Compruebe el nuevo certificado de administrador del nodo de administración principal (PPAN).

Vaya a Administration > System > Certificates > Certificate Management > System Certificates > Expand (ise-ppan).

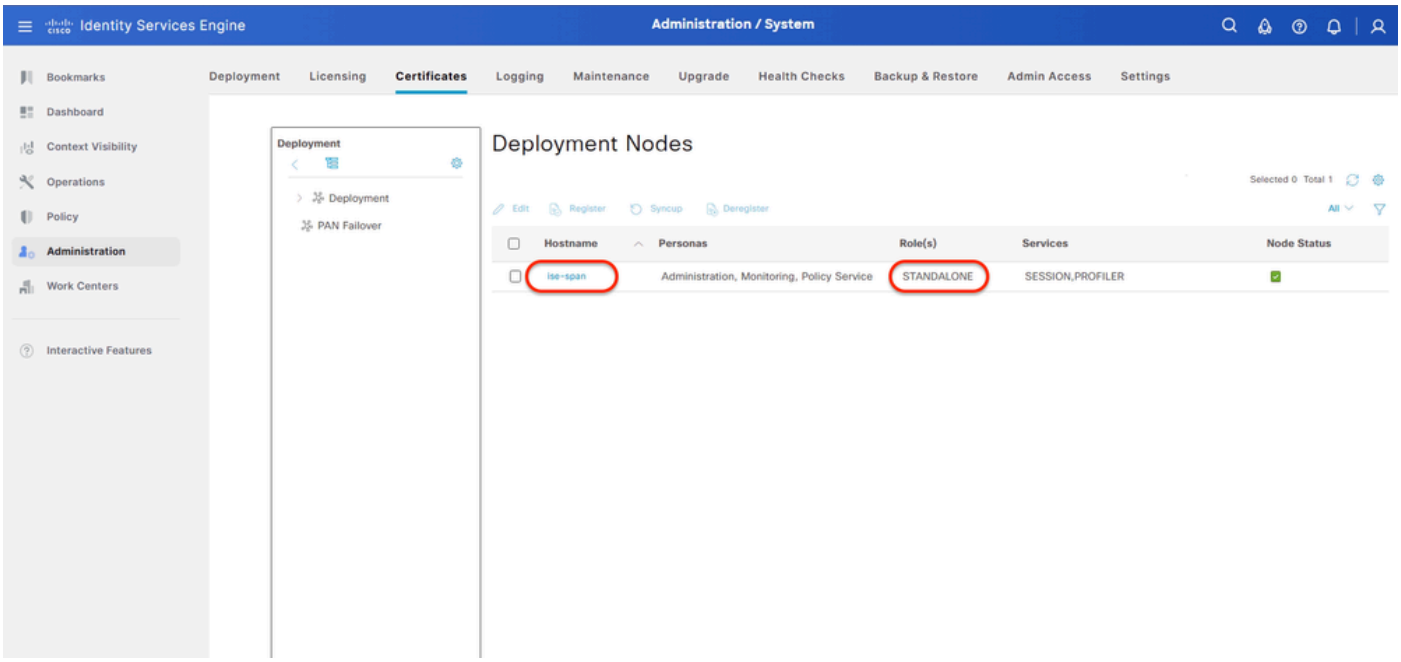


Nuevo certificado de administrador (ise-ppan)

Paso 3. Renueve el certificado de administrador de los nodos secundarios.

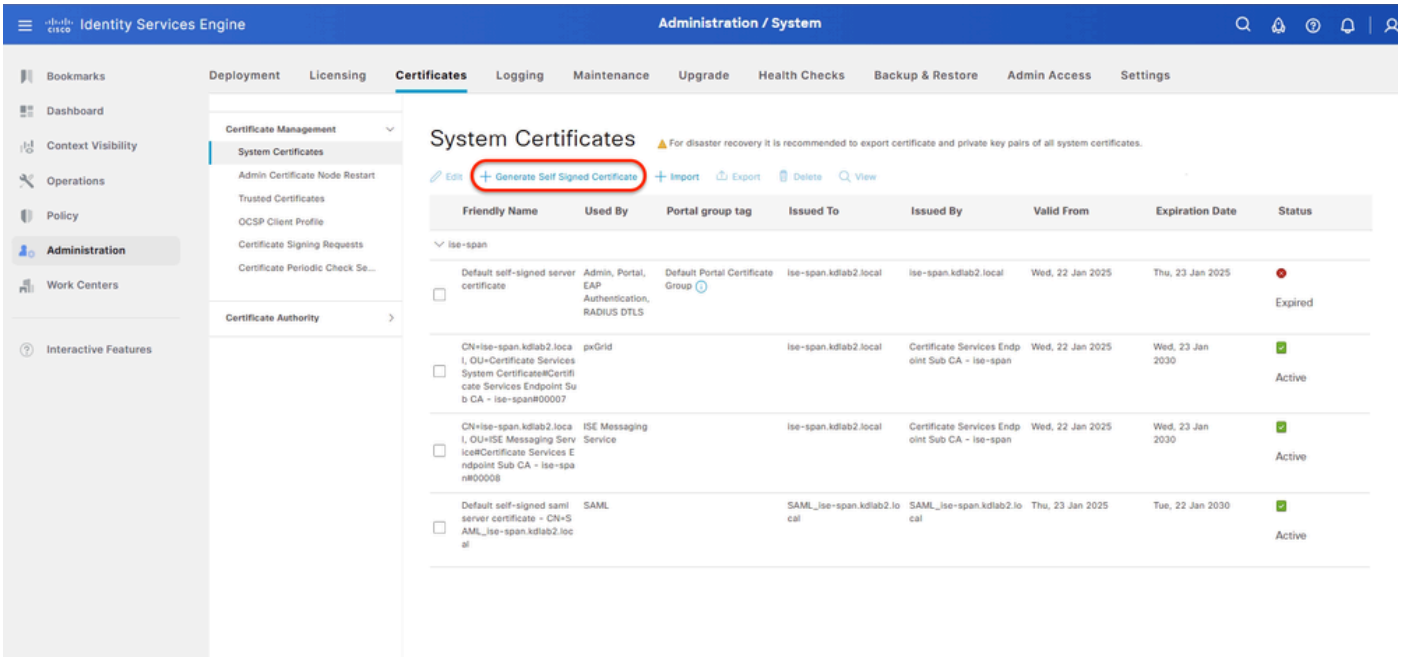
1. Confirme el nodo secundario en la implementación independiente después de darse de baja de la implementación distribuida.

Navegue por el nodo a través de la GUI (https://<FQDN/IP>) y navegue hasta Administration > System > Deployment.



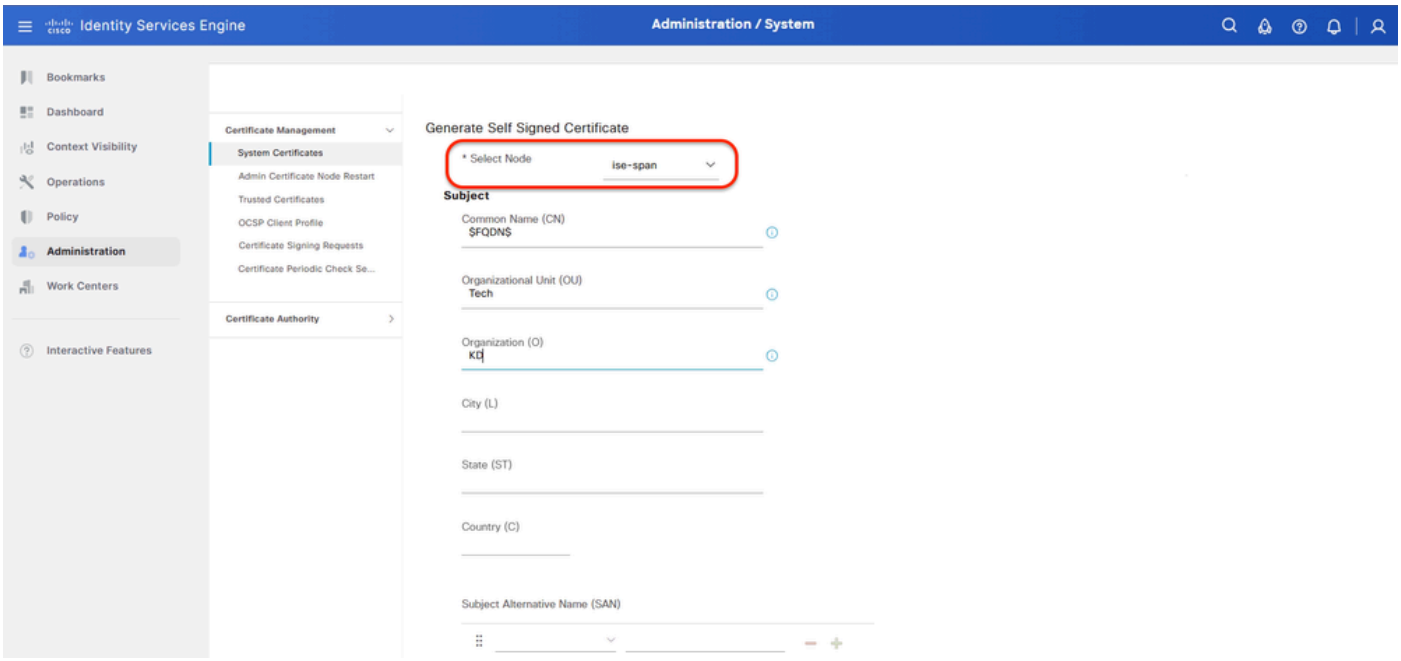
(ise-span) en la implementación independiente

2. Vaya a Administración > Sistema > Certificados > Administración de certificados > Certificados del sistema > Haga clic en +Generar certificado con firma automática.



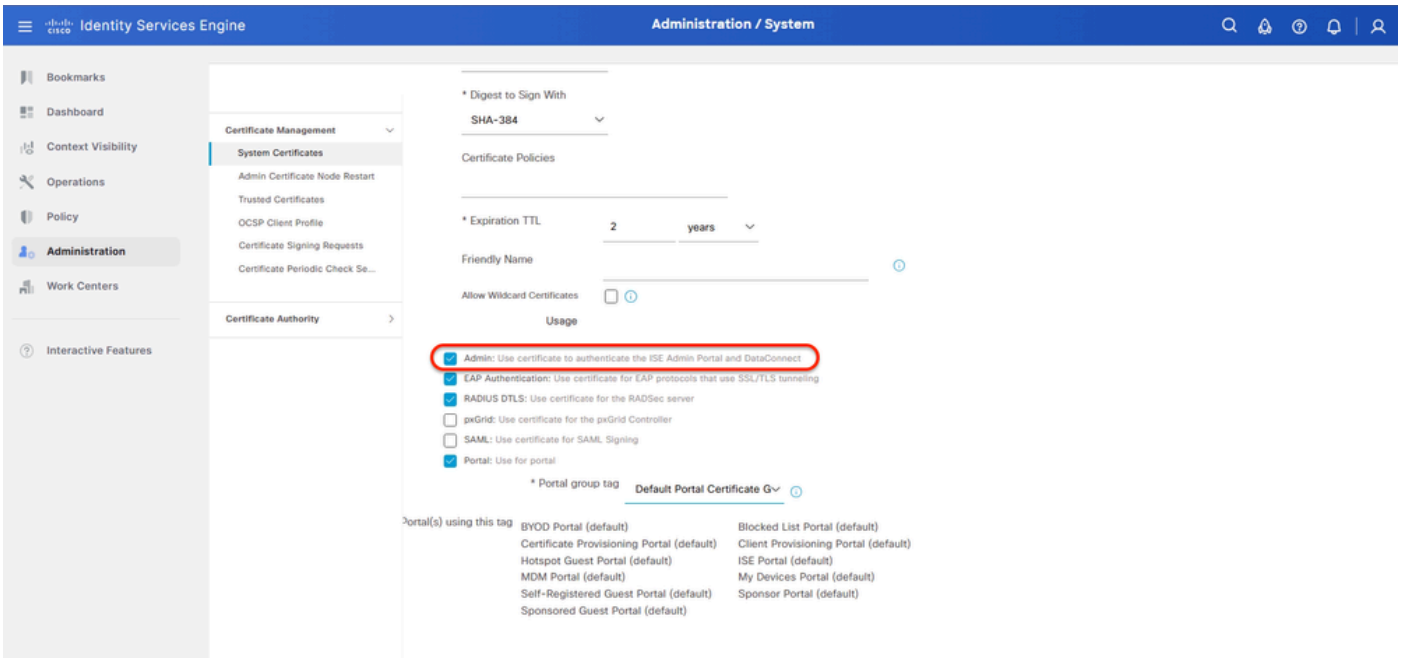
Generar nuevo certificado de administrador autofirmado

3. Seleccione el (ise-span) y rellene la información del certificado.



Seleccione el nodo

4. Marque [√] el uso de Admin.



Uso del administrador

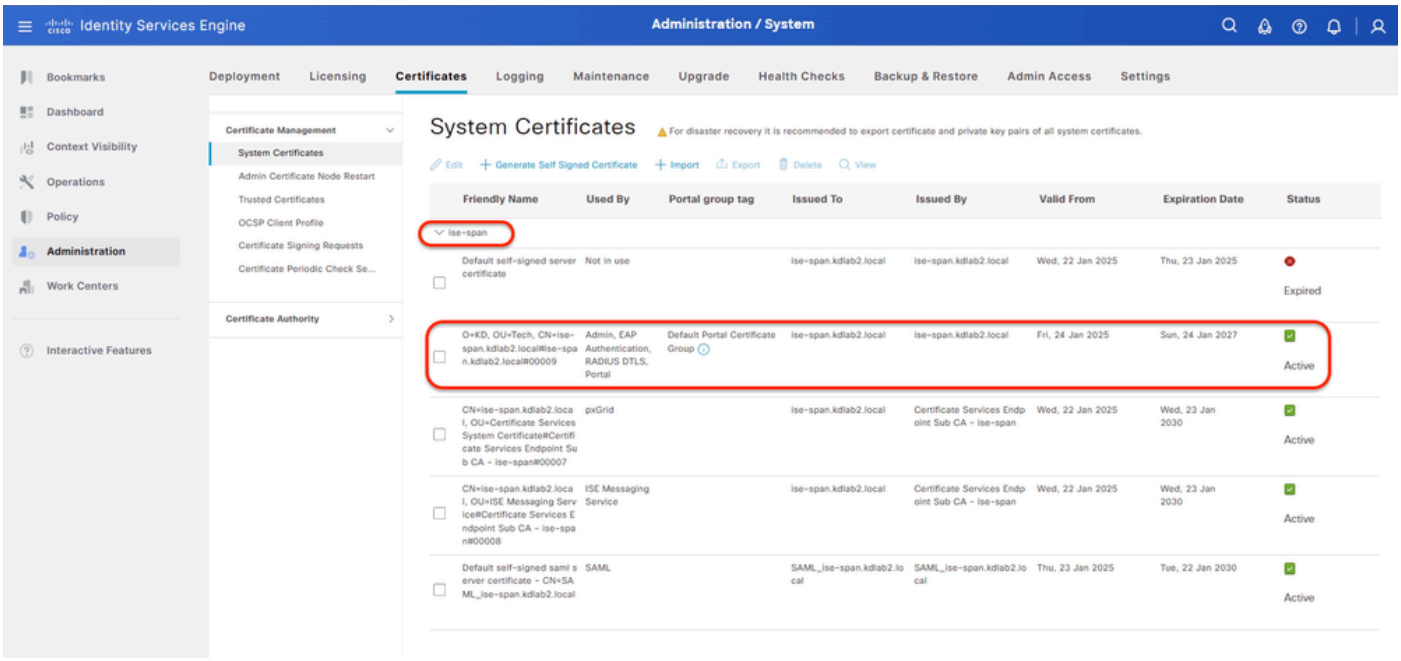
Nota: Al cambiar el certificado del certificado del rol de administrador en el nodo ISE, se reinician los servicios.

---

5. Haga clic en Enviar.

6. Compruebe el nuevo certificado de administrador en (ise-span).

Vaya a Administration > System > Certificates > Certificate Management > System Certificates > Expandir (ise-span).

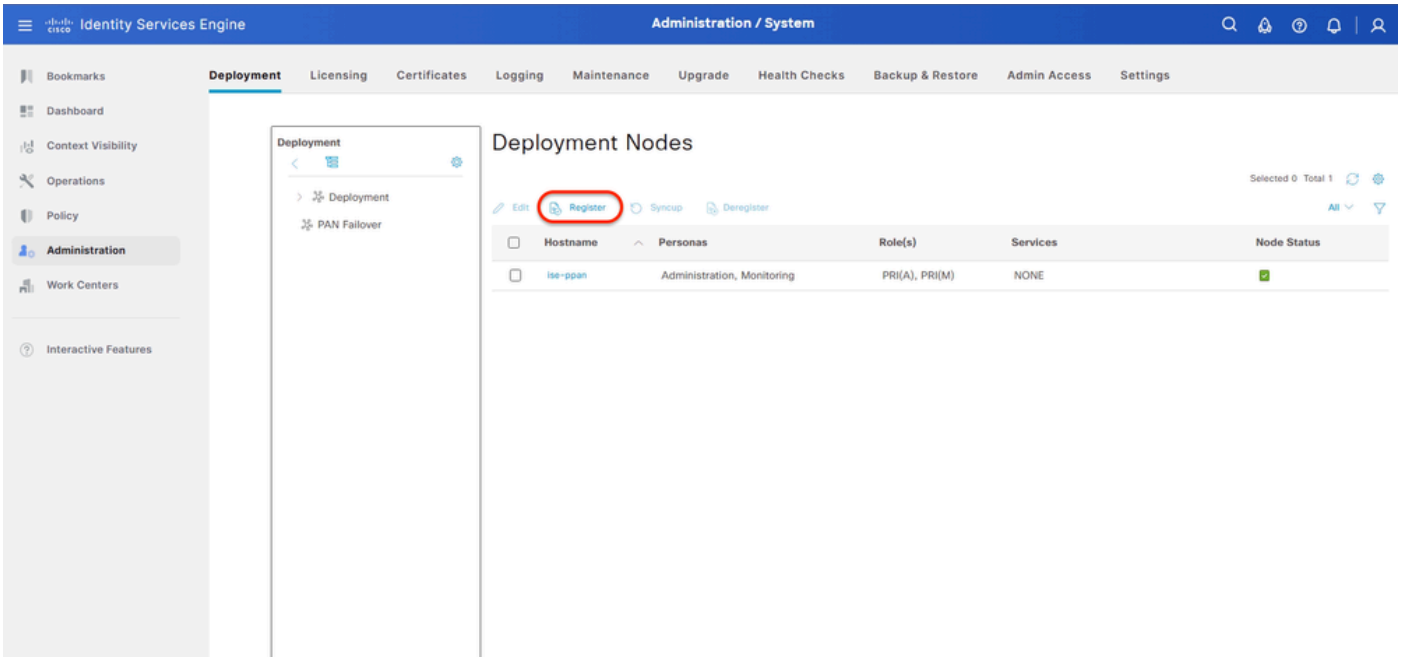


Nuevo certificado de administrador (ise-span)

Paso 4. Registre los nodos secundarios en la implementación distribuida.

Configure las personas y los roles de implementación tal y como estaban antes (Admin, MNT, PSN, etc.).

1. En la GUI del nodo de administración principal (PPAN), vaya a Administración > Sistema > Implementación > Haga clic en Registrar.

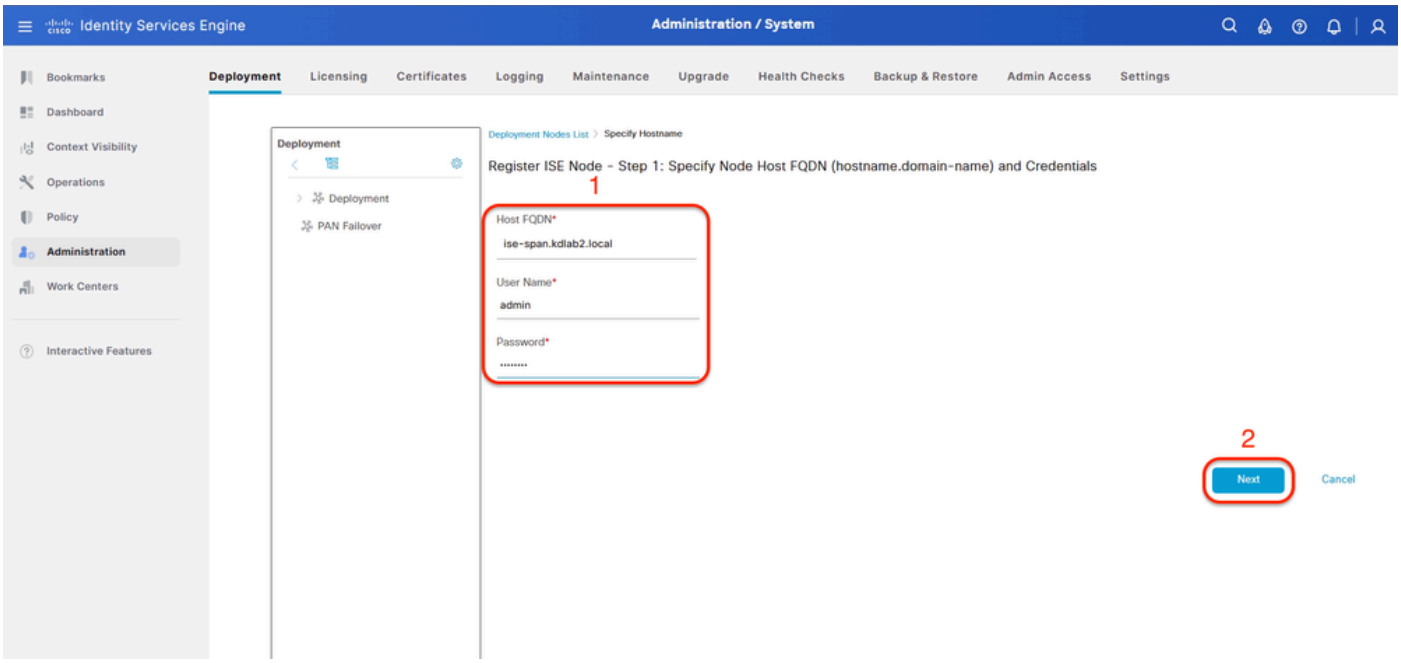


GUI del nodo de administración principal (PPAN)

2. Introduzca el FQDN y las credenciales del nodo secundario (Nombre de usuario/Contraseña).

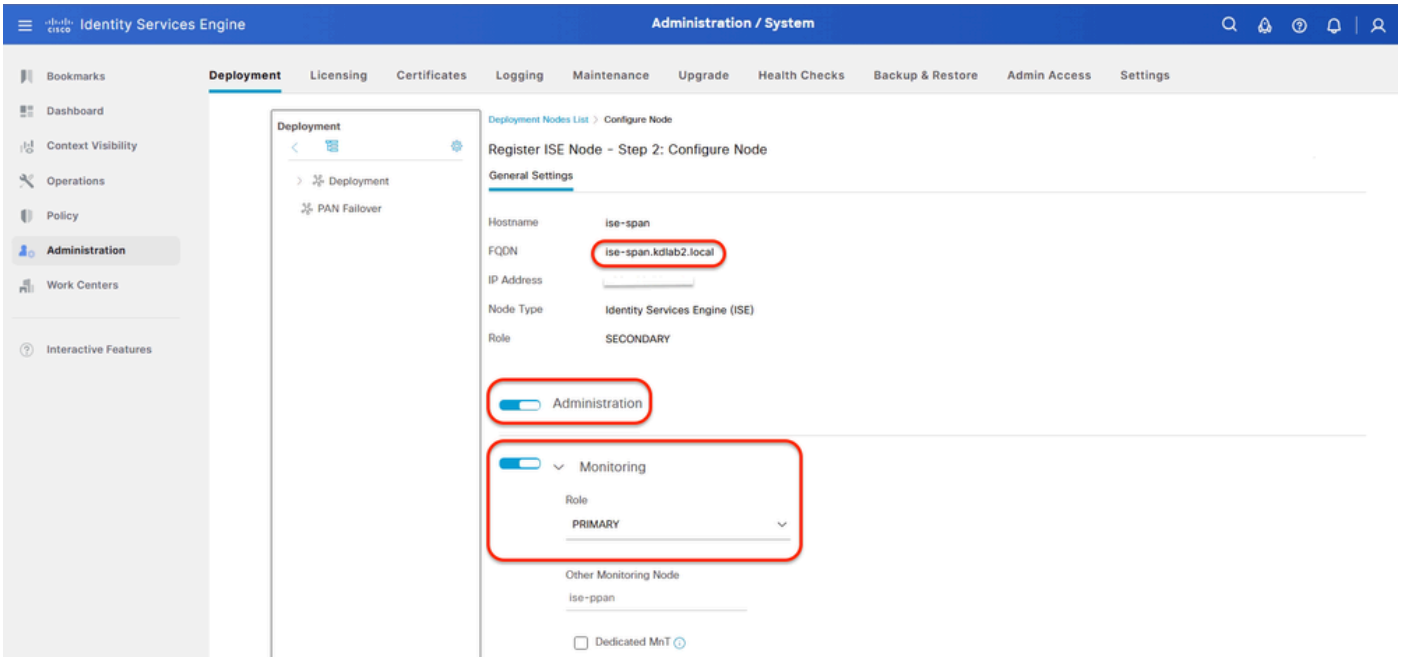
Introduzca el nombre de dominio completo (FQDN) que se puede resolver mediante DNS del nodo independiente que va a registrar. El FQDN del (PPAN) y el nodo que se está registrando

deben poder resolverse entre sí.



Introducir acceso al nodo secundario

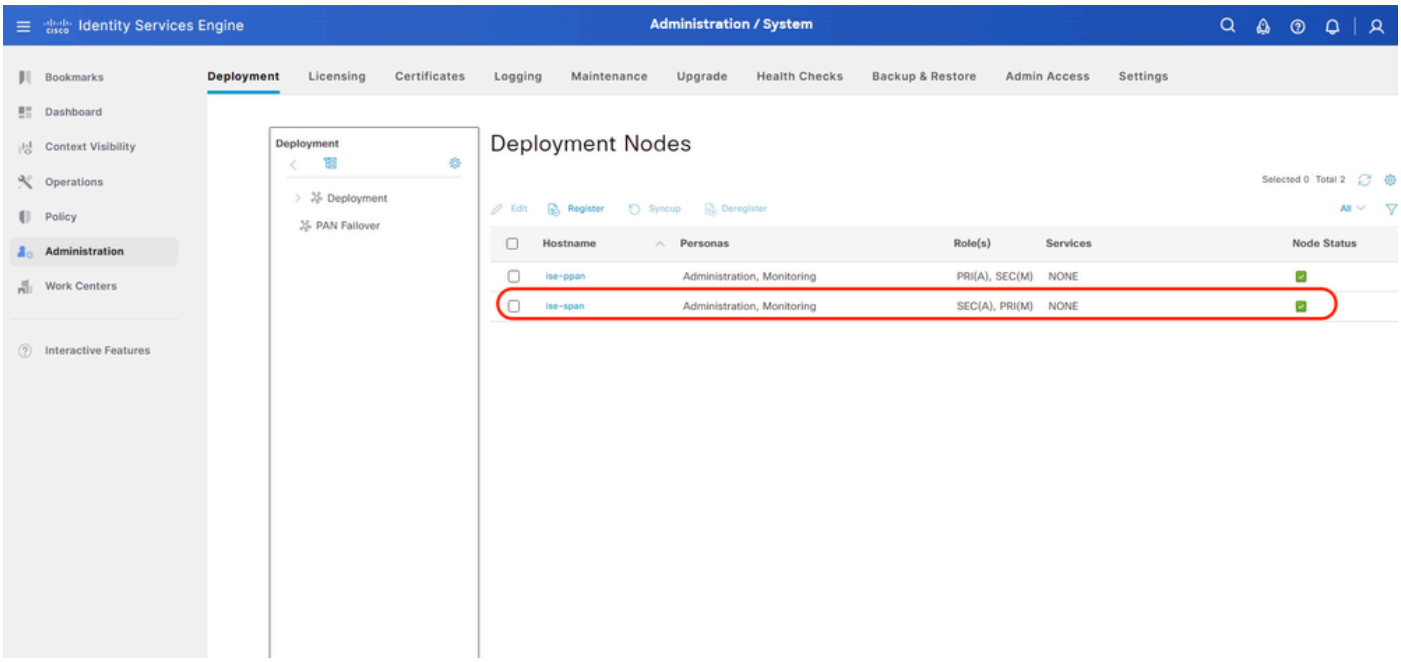
3. Habilite la persona y los servicios correctos.



Registrar nodo secundario (ise-span)

Paso 5. Verifique el estado de implementación.

Vaya a Administration > System > Deployment.



(ise-span) Añadido a la implementación

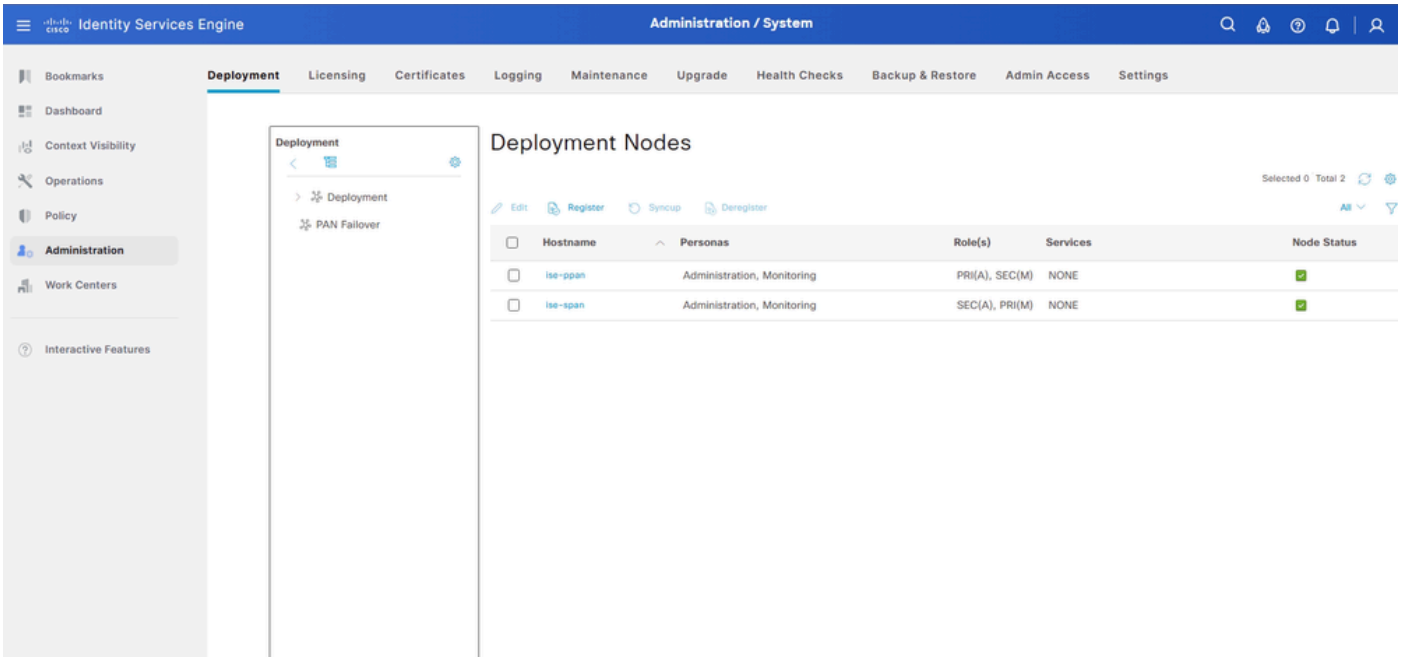
Troubleshoot

Caso práctico 1: Nodo secundario no registrado bloqueado en estado distribuido (ise-psn1)

Validar el estado

Paso 1. Confirme el estado de despliegue distribuido.

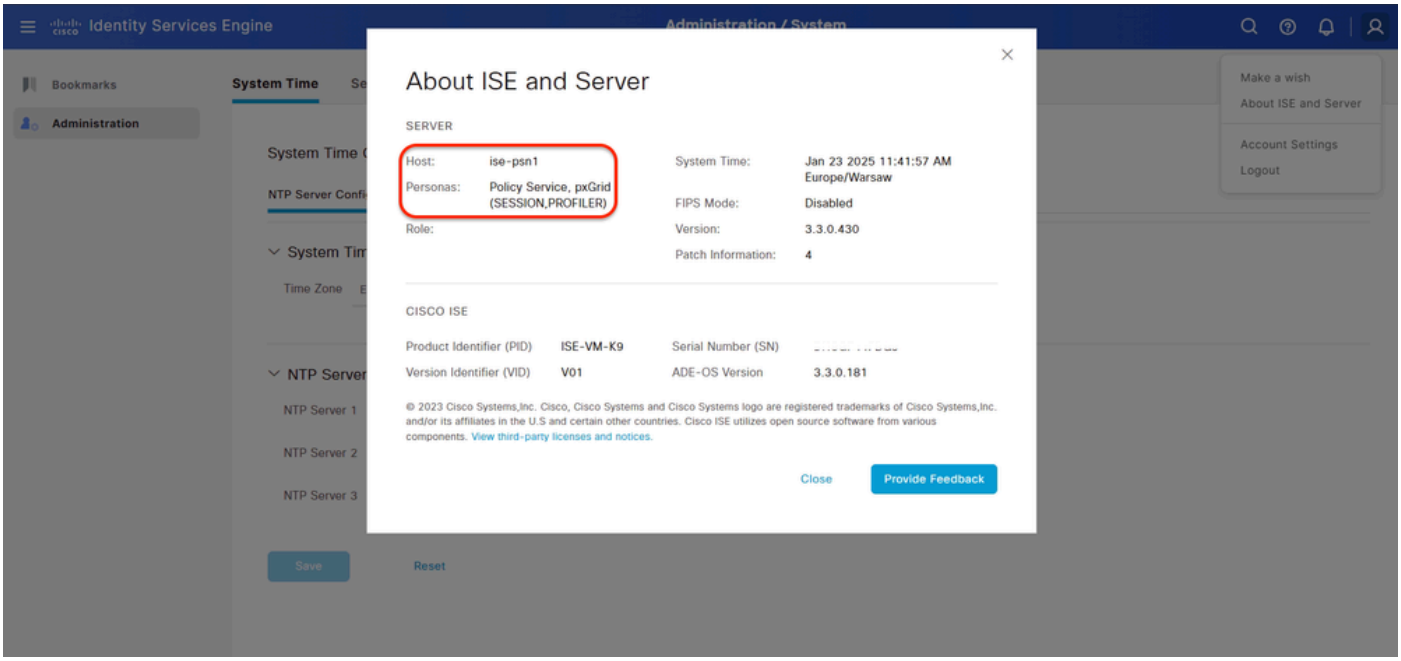
Desde la GUI del nodo de administración principal (PPAN), vaya a Administration > System > Deployment. Puede confirmar que este nodo (ise-psn1) ya está dado de baja.



(PPAN) Nodos de implementación

Paso 2. Confirme el estado del nodo (ise-psn1).

Navegue por el nodo secundario a través de la GUI (https://ise-psn1.kdlab.local) y navegue Login > About ISE and Server.

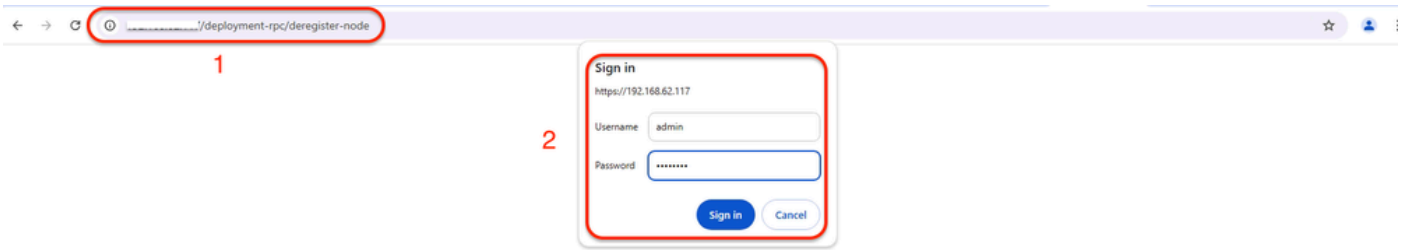


Nodo secundario (ise-psn1) bloqueado en el estado de implementación distribuida

Solución Aternativa

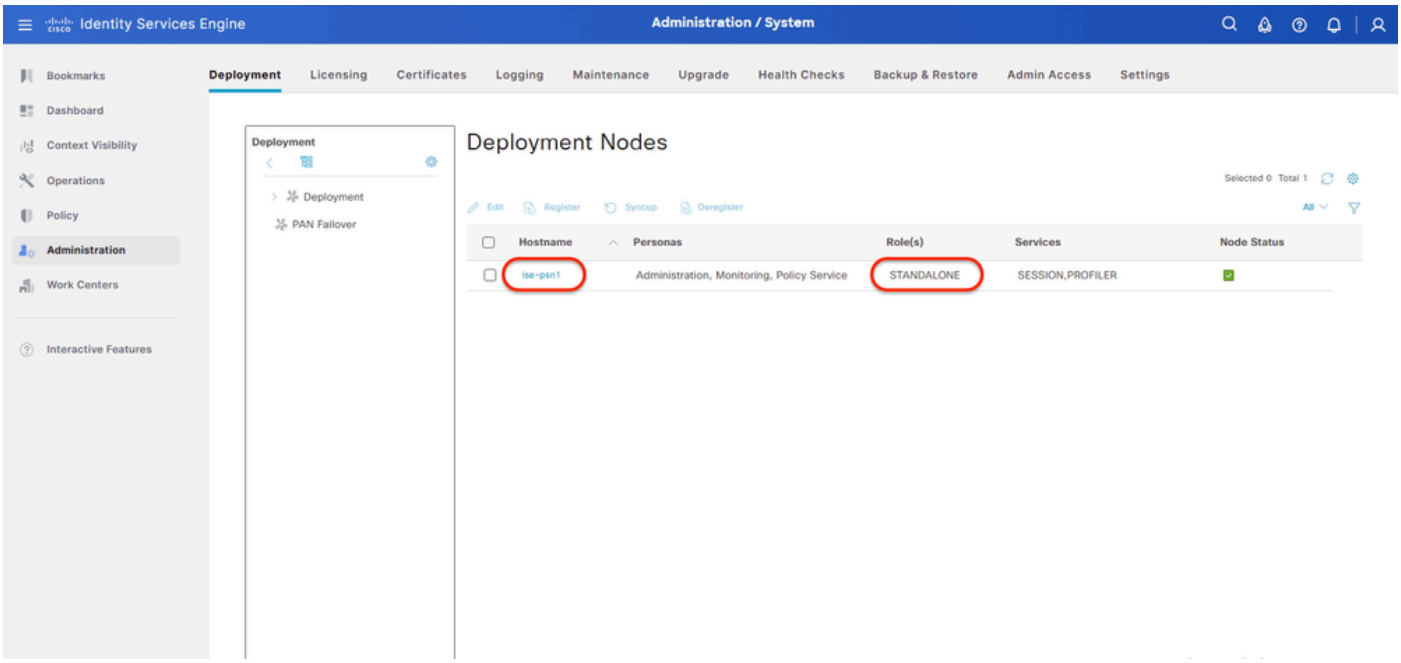
Paso 1. Anule el registro del nodo (ise-psn1) manualmente.

Aplique el nodo (ise-psn1) a la implementación independiente mediante la GUI (https://<ise-psn1 IP>/deployment-rpc/deregister-node).



Anulación manual del registro del nodo: GUI

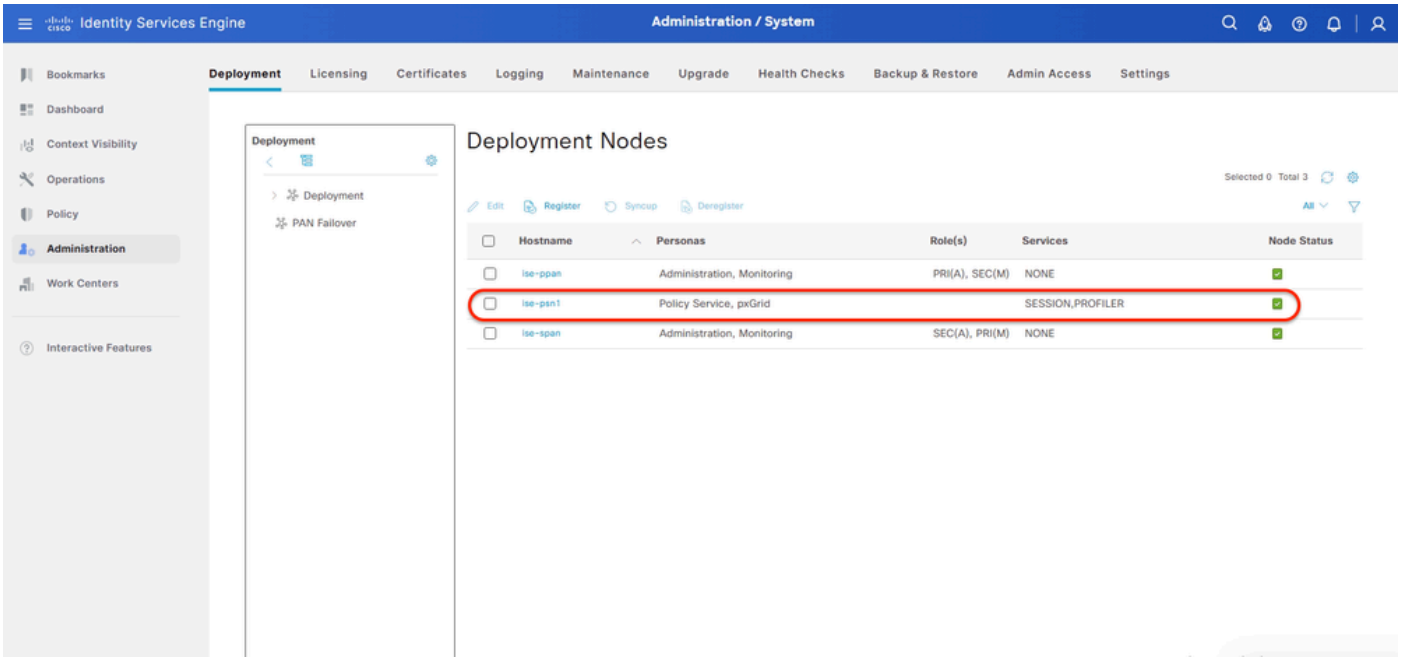
Paso 2. Verifique el (ise-psn1) ahora en la implementación independiente.



(ise-psn1) en implementaciones independientes

Paso 3. Una vez que pueda confirmar el nodo en estado autónomo, continúe con los mismos pasos en la sección Plan de Acción:

1. Renueve el certificado de administrador del nodo (ise-psn1).
2. Registre el nodo (ise-psn1) en la implementación distribuida.
3. Verifique el estado de la implementación.



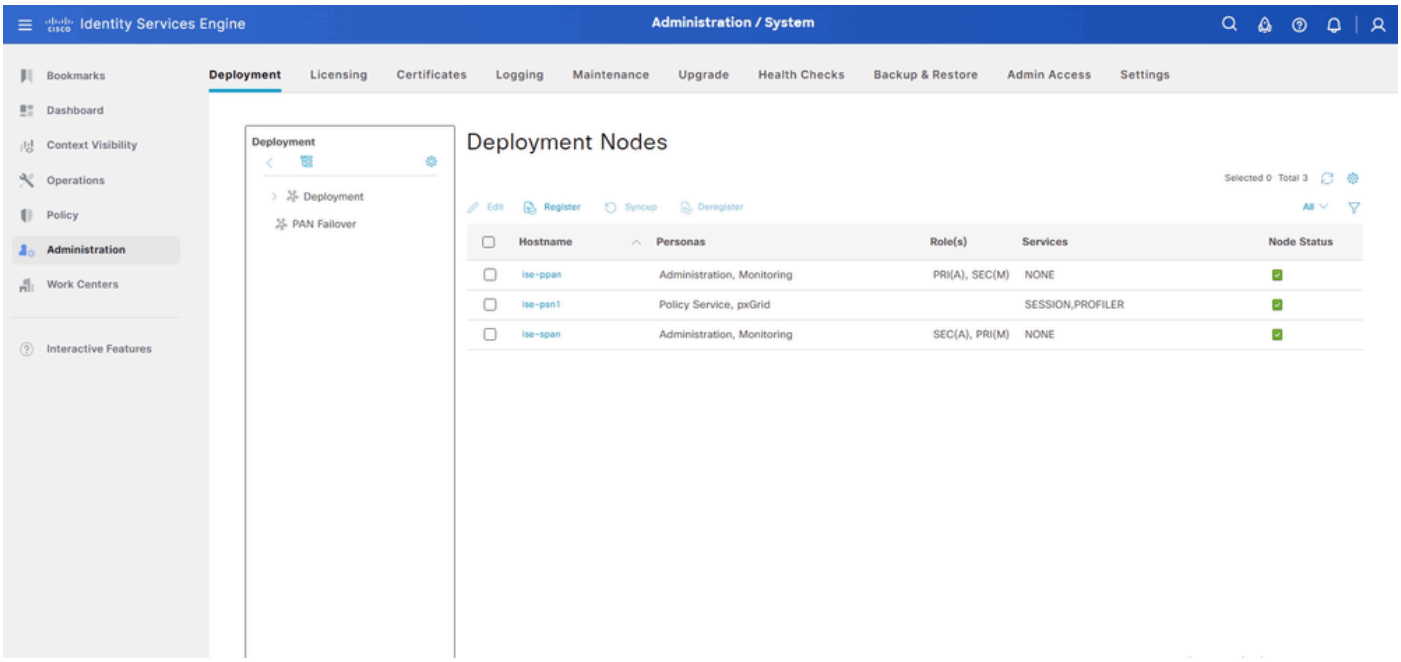
(ise-psn1) Añadido a la implementación

Caso práctico 2: GUI de nodo secundario anulada y no accesible (ise-psn2)

Validar el estado

Paso 1. Confirme el estado de despliegue distribuido.

Desde la GUI del nodo de administración principal (PPAN), vaya a Administration > System > Deployment. Puede confirmar que este nodo (ise-psn2) ya está dado de baja.



(PPAN) Nodos de implementación

Paso 2. Confirme el (ise-psn2) del nodo.

Debido a que el certificado de administración ha caducado en algunos casos, puede notar estos síntomas:

- (ise-psn2) GUI inalcanzable.
- (ise-psn2) La aplicación CLI (show application status ise) de ISE está bloqueada en (inicializando o no ejecutándose).
- (ise-psn2) CLI (show tech) el nodo ya se encuentra en una implementación independiente.

```
**********************************************
Displaying ISE deployment ...
**********************************************
Node Config Details

NAME                 PERSONA          ROLE       ACTIVE     REPLICATION
-------------------- ---------------- ---------- ---------- ---------------
ise-psn2             PAN,MNT,PSN      STANDALONE ACTIVE     SYNC COMPLETED
```

(ise-psn2) en implementaciones independientes

Solución Aternativa

Paso 1. Renueve el certificado de administrador del nodo (ise-psn2).

1. Inicie sesión en (ise-psn2) mediante CLI.
2. Ingrese application configure ise.
3. Ingrese 31 ([31] Generate Self-Signed Admin Certificate).
4. ¿Desea continuar? y/[n]: s
5. ¿Desea reemplazar el certificado existente después de la generación? y/[n]: s

```
ise-psn2/admin#
ise-psn2/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Reset Upgrade Tables
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[31]Generate Self-Signed Admin Certificate
[33]Recreate REPLOGNS tablespace
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
[38]Localised ISE Install
[39]Reset System 360 Monitoring Page
[40]Enable/Disable Explicit EC Check
[41]Gather Diagnostic data for Certificates
[42]Enable/Disable Parse SAN DirName Extension
[0]Exit

31
After this operation, the ISE node will restart
Do you want to continue? y/[n]: y
Certificate Subject
  *Common Name (CN) : ise-psn2.kdlab2.local
  Enter Organization Unit (OU) : Tech
  Enter Organization (O) : KD
Do you want to replace existing certificate after generation? y/[n]: y
Old Memory Size : 32639004
```

Renovar (ise-psn1) certificado de administrador

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).