Comprender los servicios de autoridad de certificación interna de ISE

Contenido

Introducción

Este documento describe el servicio CA y el servicio de inscripción en transporte seguro (EST) que está presente en Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE
- Certificados e infraestructura de clave pública (PKI)
- Protocolo simple de inscripción de certificados (SCEP)
- Online Certificate Status Protocol (OCSP)

Componentes Utilizados

La información de este documento se basa en Identity Services Engine 3.0.

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.

Servicio de autoridad certificadora (CA)

Los certificados pueden ser autofirmados o firmados digitalmente por una autoridad de certificación (CA) externa. La autoridad de certificación interna de Cisco ISE (ISE CA) emite y gestiona certificados digitales para terminales desde una consola centralizada para permitir a los empleados utilizar sus dispositivos personales en la red de la empresa. Un certificado digital firmado por una CA se considera un estándar del sector y más seguro. El nodo de administración de políticas principal (PAN) es la CA raíz. Los nodos de servicios de políticas (PSN) son CA subordinadas al PAN principal.

Funcionalidad de CA de ISE

La CA de ISE ofrece esta funcionalidad:

- Emisión de certificado: valida y firma las solicitudes de firma de certificado (CSR) para los terminales que se conectan a la red.
- Gestión de claves: genera y almacena de forma segura claves y certificados en los nodos PAN y PSN.
- Almacenamiento de certificados: almacena certificados emitidos a usuarios y dispositivos.
- Compatibilidad con el protocolo de estado de certificados en línea (OCSP): proporciona un respondedor OCSP para comprobar la validez de los certificados.

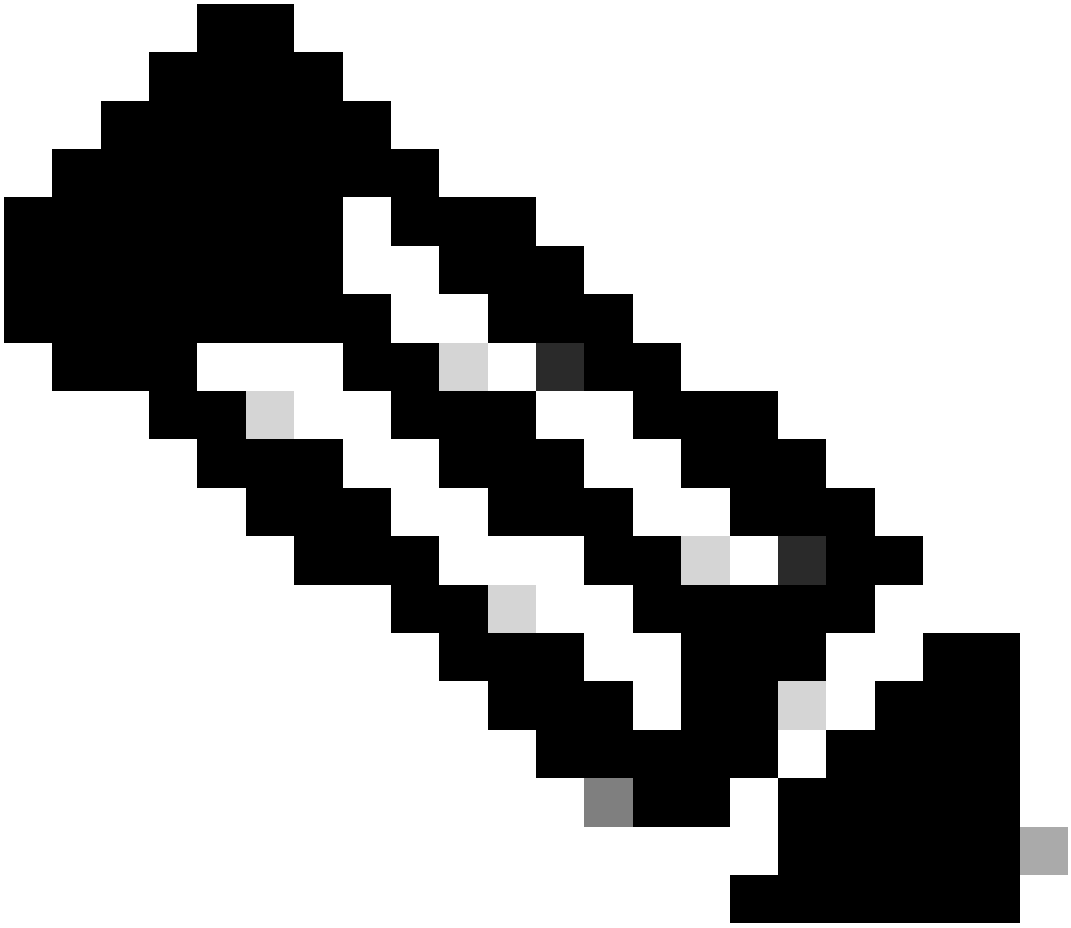
Certificados de CA de ISE aprovisionados en nodos de administración y servicio de políticas

Después de la instalación, un nodo de Cisco ISE se aprovisiona con un certificado de CA raíz y un certificado de CA de nodo para administrar certificados para terminales.

Cuando se configura una implementación, el nodo designado como nodo de administración principal (PAN) se convierte en la CA raíz. PAN tiene un certificado de CA raíz y un certificado de CA de nodo firmado por la CA raíz.

Cuando se registra un nodo de administración secundario (SAN) en PAN, se genera un certificado de CA de nodo y lo firma la CA raíz en el nodo de administración principal.

Cualquier nodo de servicios de políticas (PSN) registrado con PAN recibe una CA de terminal y un certificado OCSP firmado por la CA de nodo de PAN. Los nodos de servicios de políticas (PSN) son CA subordinadas al PAN. Cuando se utiliza la CA de ISE, la CA de terminal de PSN emite los certificados a los terminales que acceden a la red.



Nota: desde ISE 3.1 Patch 2 e ISE 3.2 FCS, se ha cambiado la jerarquía de certificados de OCSP.

Según RFC 6960:

"Un emisor de certificados DEBE realizar una de las siguientes acciones:

- firmar las propias respuestas de OCSP, o

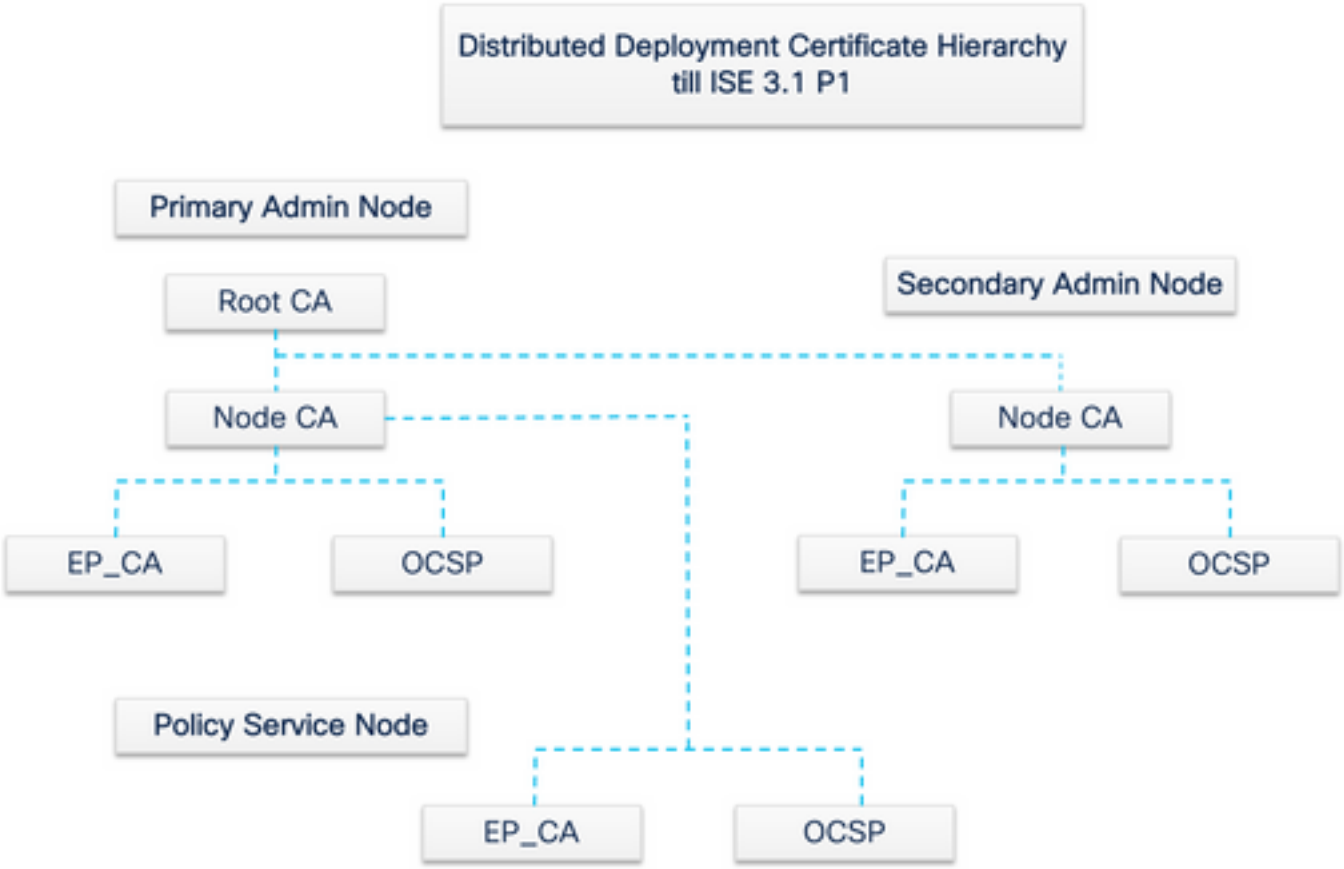
- designar explícitamente esta autoridad a otra entidad"

"El certificado de firmante de respuesta OCSP DEBE ser emitido directamente por la CA identificada en la solicitud. "

"El sistema (depende) de las respuestas de OCSP DEBE reconocer un certificado de delegación emitido por la CA que emitió el certificado en cuestión solo si el certificado de delegación y el

certificado (o certificados) cuya revocación se ha comprobado están firmados por la misma clave."

Para cumplir con el estándar RFC mencionado anteriormente, la jerarquía de certificados para el certificado de respondedor OCSP se cambia en ISE. El certificado de Respondedor de OCSP ahora lo emite la Sub CA de punto final del mismo nodo en lugar de la CA de nodo en PAN.



Inscripción en el servicio de transporte seguro (EST)

El concepto de infraestructura de clave pública (PKI) existe desde hace mucho tiempo. La PKI autentica la identidad de usuarios y dispositivos mediante pares de claves públicas firmadas en forma de certificados digitales. La inscripción a través de transporte seguro (EST) es un protocolo para proporcionar estos certificados. El servicio EST define cómo realizar la inscripción de certificados para los clientes que utilizan la administración de certificados a través de la sintaxis de mensajes criptográficos (CMC) en un transporte seguro. Según el IETF, "EST describe un protocolo de administración de certificados sencillo pero funcional dirigido a clientes de Infraestructura de clave pública (PKI) que necesitan adquirir certificados de cliente y certificados de Entidad de certificación (CA) asociados. También admite pares de claves públicas/privadas generadas por el cliente, así como pares de claves generadas por la CA".

Casos prácticos de EST

Se puede utilizar el protocolo EST:

- Para inscribir dispositivos de red mediante la identidad de dispositivo único seguro
- Para soluciones BYOD

¿Por qué EST?

Los protocolos EST y SCEP abordan el aprovisionamiento de certificados. EST es un sucesor del Protocolo simple de inscripción de certificados (SCEP). Debido a su simplicidad, SCEP ha sido el protocolo de facto en el aprovisionamiento de certificados durante muchos años. Sin embargo, se recomienda el uso de EST sobre SCEP por las siguientes razones:

- Uso de TLS para el transporte seguro de certificados y mensajes: en EST, la solicitud de firma de certificado (CSR) se puede vincular a un solicitante que ya es de confianza y está autenticado con TLS. Los clientes no pueden obtener un certificado para nadie más que para sí mismos. En SCEP, la CSR se autentica mediante un secreto compartido entre el cliente y la CA. Esto plantea problemas de seguridad, ya que una persona con acceso al secreto compartido puede generar certificados para entidades distintas de ella.
- Compatibilidad con la inscripción de certificados con firma ECC: EST proporciona agilidad criptográfica. Admite criptografía de curva elíptica (ECC). SCEP no admite ECC y depende del cifrado RSA. ECC ofrece más seguridad y mejor rendimiento que otros algoritmos criptográficos como RSA, incluso aunque utilice un tamaño de clave mucho más pequeño.
- EST está diseñado para admitir la reinscripción automática de certificados.

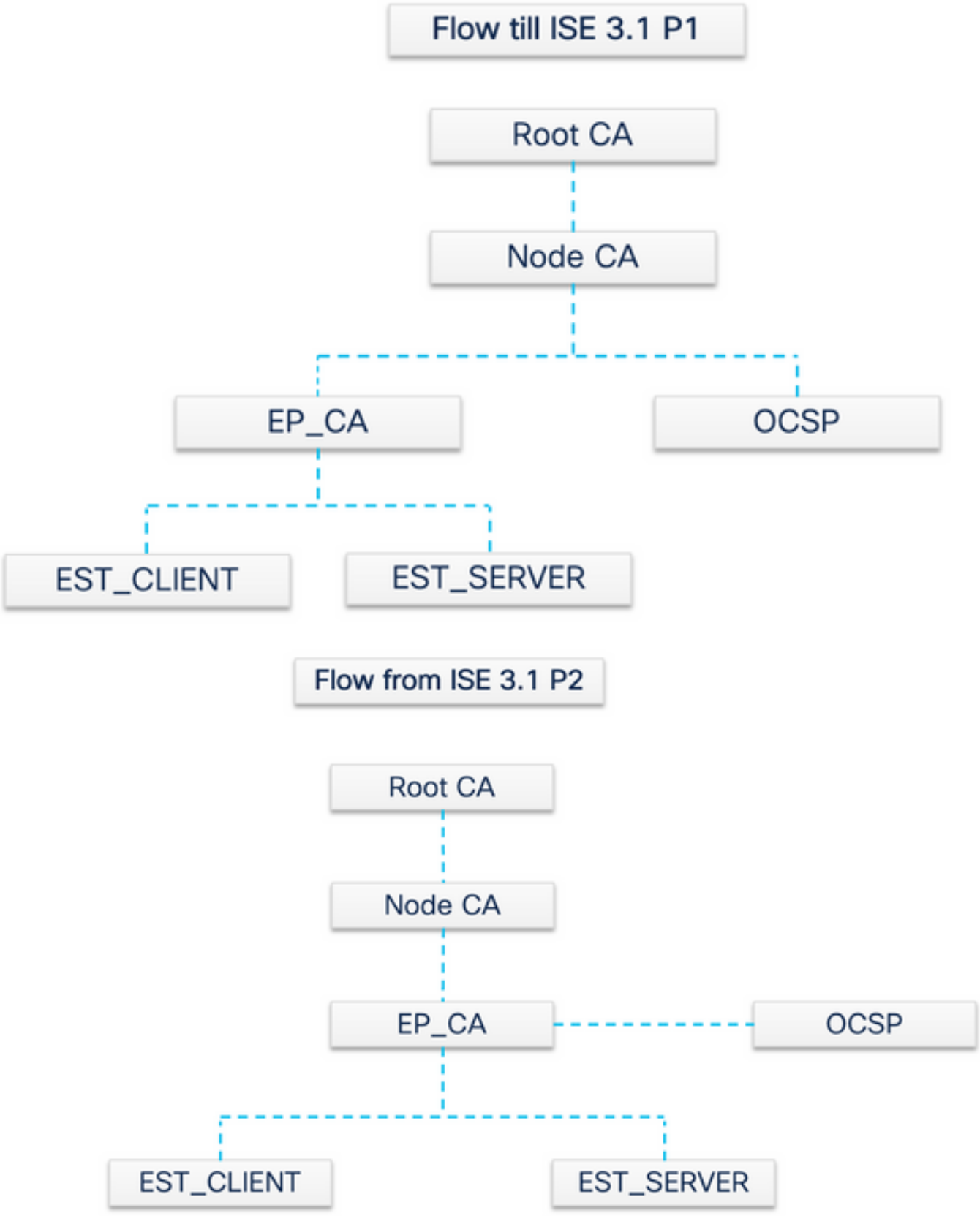
La seguridad probada de TLS y la mejora continua ayudan a garantizar que las transacciones de EST sean seguras en términos de protección criptográfica. La estrecha integración de SCEP con RSA para proteger los datos plantea problemas de seguridad a medida que avanza la tecnología.

EST en ISE

Para implementar este protocolo, se necesitan un cliente y un módulo de servidor:

- Cliente EST: integrado en el tomcat de ISE normal.
- Servidor EST: implementado en un servidor web de código abierto llamado NGINX. Esto se ejecuta como un proceso independiente y escucha en el puerto 8084.

La autenticación de cliente y servidor basada en certificados es compatible con EST. La CA del extremo emite el certificado para el cliente EST y el servidor EST. Los certificados de cliente y servidor de ISE y sus respectivas claves se almacenan en la base de datos de NSS de la CA de ISE.



Tipos de solicitudes en ISE EST

Siempre que se activa el servidor de la CA, obtiene la copia más reciente de todos los certificados de la CA del servidor de la CA y la almacena. A continuación, el cliente EST puede realizar una solicitud de certificado de CA para obtener toda la cadena de este servidor EST. Antes de realizar una solicitud de inscripción simple, el cliente de la prueba de compatibilidad debe emitir primero la

solicitud de certificado de la CA.

Solicitud de certificados de CA (basada en RFC 7030)

1. El cliente de prueba solicita una copia de los certificados de CA actuales.
2. Mensaje HTTPS GET con un valor de ruta de operación de /cacerts.

- Esta operación se realiza antes que cualquier otra solicitud EST.
- Se realiza una solicitud cada 5 minutos para obtener una copia de los certificados de CA más actualizados.
- El servidor de prueba no debe requerir autenticación de cliente.

La segunda solicitud es una solicitud de inscripción simple y necesita autenticación entre el cliente EST y el servidor EST. Esto sucede cada vez que un terminal se conecta a ISE y realiza una solicitud de certificado.

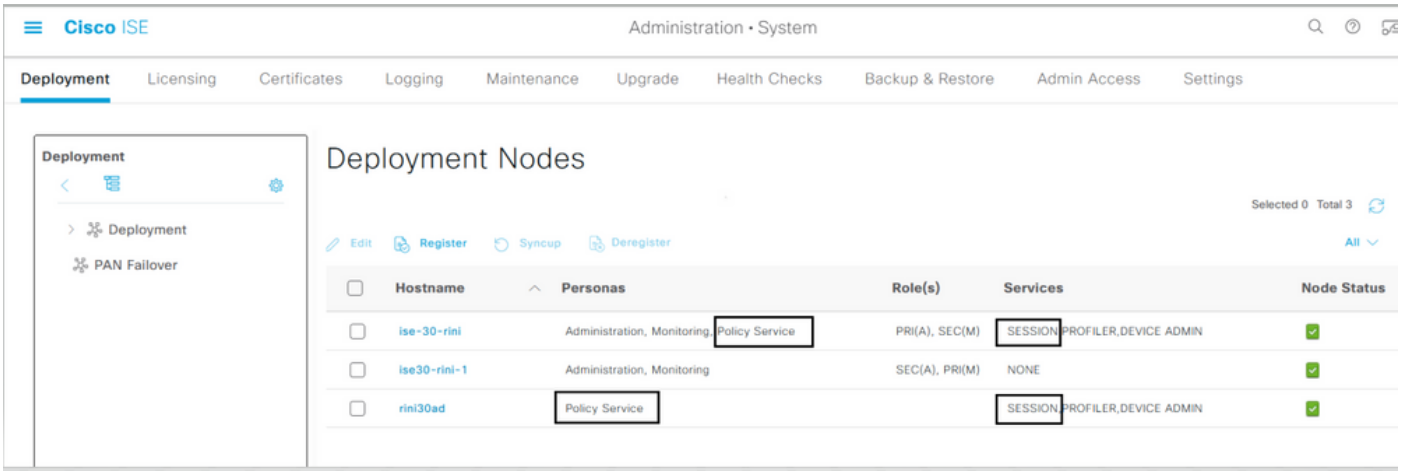
Solicitud de inscripción sencilla (basada en RFC 7030)

1. El cliente EST solicita un certificado del servidor EST.
2. Mensaje HTTPS POST con el valor de ruta de operación /simpleenroll.

- El cliente EST integra la solicitud PKCS#10 en esta llamada que se envía a ISE.
- El servidor EST debe autenticar el cliente.

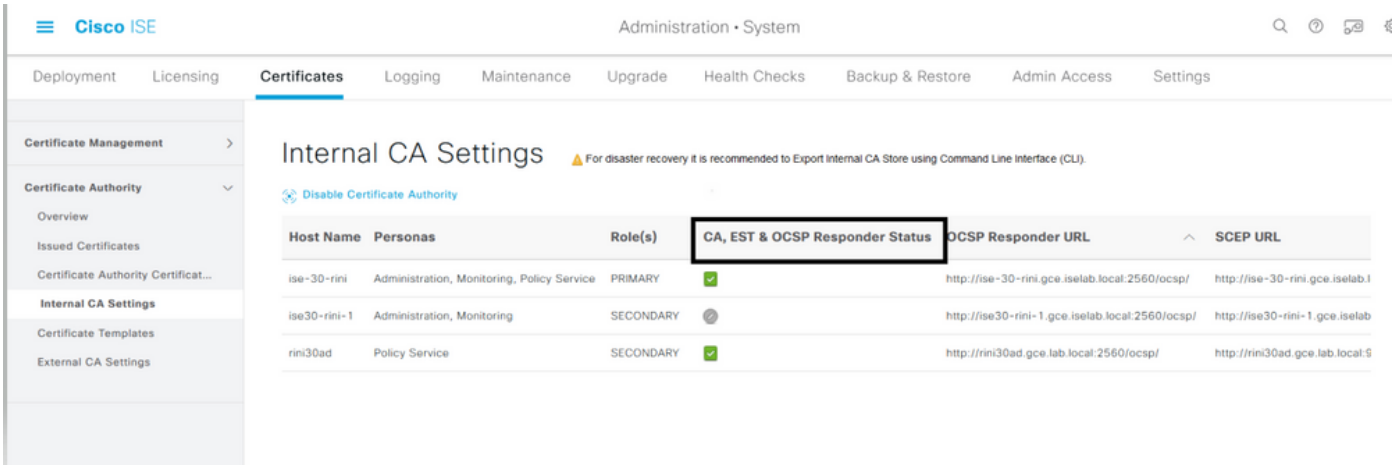
Estado del servicio EST y CA

Los servicios de CA y EST sólo se pueden ejecutar en un nodo de Servicio de directivas que tenga habilitados los servicios de sesión. Para habilitar los servicios de sesión en un nodo, navegue hasta Administration > System > Deployment . Seleccione el nombre de host del servidor en el que deben activarse los servicios de sesión y haga clic en Edit . Active la **Enable Session Services** casilla de verificación en Persona de Policy Service.



Estado mostrado en la GUI

El estado del servicio de ISE está vinculado al estado del servicio de la CA de ISE en ISE. Si el servicio CA está activo, el servicio EST está activo y si el servicio CA está inactivo, el servicio EST también está inactivo.



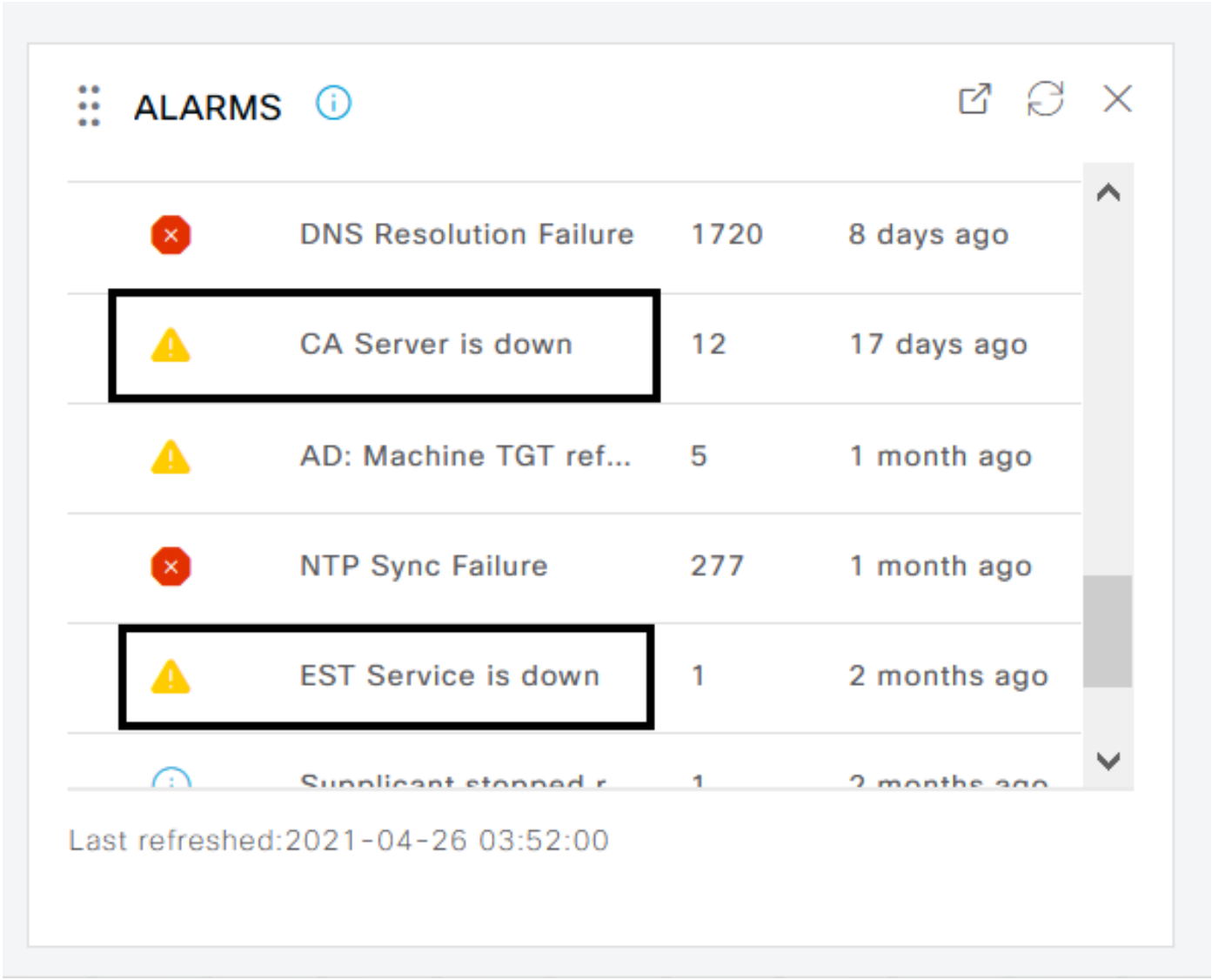
Estado mostrado en CLI

```
ise-30-rini/admin# sh app status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          61993
Database Server                        running          159 PROCESSES
Application Server                     running          72240
Profiler Database                      running          68224
ISE Indexing Engine                    running          74972
AD Connector                           running          78912
M&T Session Database                   running          68007
M&T Log Processor                      running          70533
Certificate Authority Service          running          63090
EST Service                            running          64492
SXP Engine Service                     disabled
Docker Daemon                          running          64427
TC-NAC Service                         disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
```

Alarmas en el panel

La alarma se muestra en el panel de ISE si los servicios EST y CA no funcionan.



Impacto si los servicios de CA y EST no se están ejecutando

- La falla de llamada del cliente/cacerts EST puede ocurrir cuando el servidor EST está inactivo. El /cacerts error de llamada también puede ocurrir si la cadena de CA del certificado de cadena de la CA de la EST está incompleta.

-

  Error en las solicitudes de inscripción de certificados de terminales basados en ECC.

- El flujo de BYOD se interrumpe si se produce alguno de los dos fallos anteriores.
- Se pueden generar alarmas de error de link de cola.

Troubleshoot

Si el flujo de BYOD con el protocolo EST no funciona correctamente, compruebe estas condiciones:

- La cadena de certificados de CA secundaria del extremo de Servicios de Certificate Server ha finalizado. Para verificar si la cadena de certificados está completa:

  1. Vaya a Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates .

     - Seleccione la casilla de verificación junto al certificado y haga clic en **Ver** para verificar un certificado determinado.

- Asegúrese de que los servicios de CA y EST estén en funcionamiento. Si los servicios no se están ejecutando, navegue hasta Administration > System > Certificates > Certificate Authority > Internal CA Settings para habilitar el servicio CA.

- Si se ha realizado una actualización, reemplace la cadena de certificados de la CA raíz de ISE después de la actualización. A tal efecto:

  1. Elija Administration > System > Certificates > Certificate Management > Certificate Signing Requests .

     -

Haga clic en Generate Certificate Signing Requests (CSR).

•

Seleccione ISE Root CA en laCertificate(s) will be used for lista desplegable.

•

Haga clic en Replace ISE Root CA Certificate Chain .

• La depuración útil que se puede habilitar para verificar los registros incluye est , provisioning , ca-service , y ca-service-cert . Consulte ise-psc.log , catalina.out , caservice.log , y error.log archivos.

Información Relacionada

- **Soporte técnico y descargas de Cisco**

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).