Servicio CA y servicio EST en ISE

Contenido

Introducción

Este documento describe el servicio de autoridad certificadora (CA) y el servicio de inscripción sobre transporte seguro (EST) que están presentes en Cisco Identity Services Engine (ISE).

prerrequisitos

Requisitos

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 que contiene este documento se basa en las siguientes versiones de software y

hardware.

- 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 comenzaron con una configuración (predeterminada) despejada. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Servicio de autoridad certificadora (CA)

Los certificados pueden ser firmados automáticamente o firmados digitalmente por una autoridad certificadora externa (CA). 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 CA se considera estándar del sector y más seguro. El nodo de administración de políticas principal (PAN) es la CA raíz. Los nodos de servicio de políticas (PSN) son CA subordinadas al PAN principal.

Funciones de CA de ISE

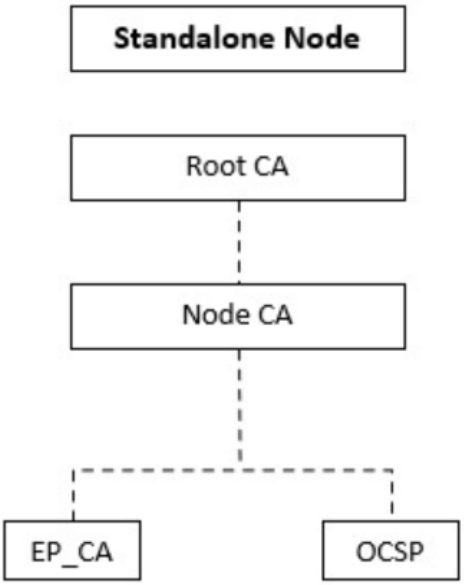
La CA ISE ofrece estas funcionalidades:

- Emisión de certificado: Valida y firma las solicitudes de firma de certificados (CSR) para los terminales que se conectan a la red.
- Gestión de claves: Genera y almacena de forma segura claves y certificados tanto en nodos PAN como PSN.
- Almacenamiento de certificados: Almacena certificados que se emiten 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 CA de ISE aprovisionados en nodos de servicio de administración y políticas

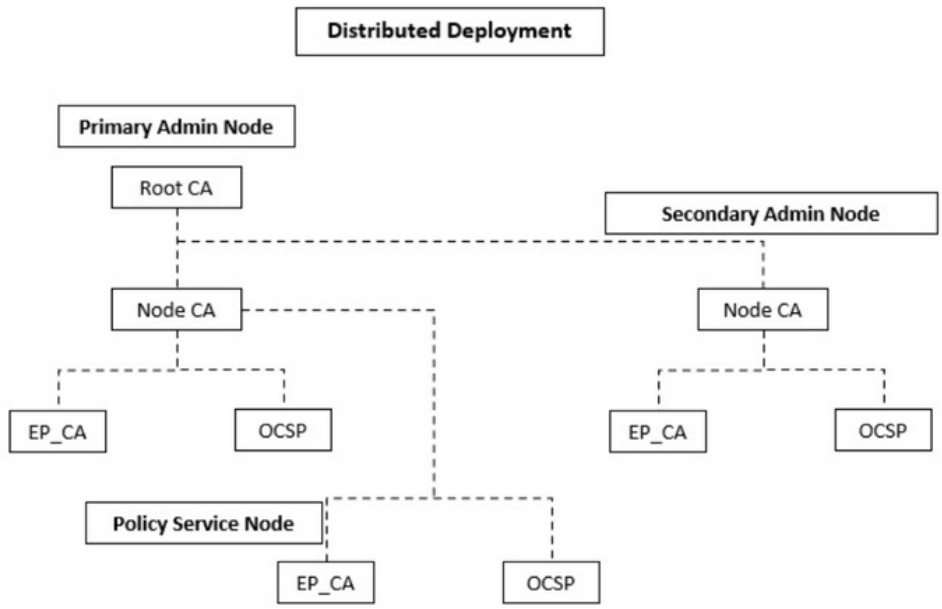
Después de la instalación, se proporciona un nodo Cisco ISE con un certificado de CA raíz y un certificado de CA de nodo para administrar certificados para terminales.

Cuando se configura una implementación, el nodo designado como nodo de administración principal (PAN) se convierte en la CA raíz. El 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 el PAN, se genera un certificado de CA de nodo y la CA raíz lo firma en el nodo de administración principal.

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



Inscripción en el servicio de transporte seguro (EST)

El concepto de infraestructura de clave pública (ICP) existe desde hace mucho tiempo. La PKI autentica la identidad de los usuarios y dispositivos mediante pares de claves públicas firmadas en forma de certificados digitales. La inscripción en Secure Transport (EST) es un protocolo para

aprovisionar estos certificados. El servicio EST define cómo realizar la inscripción de certificados para los clientes que utilizan la Administración de certificados sobre sintaxis de mensajes criptográficos (CMC) en un transporte seguro. Según IETF: "EST describe un protocolo de gestión de certificados simple 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 y privadas generadas por el cliente, así como pares de claves generadas por la CA".

casos prácticos EST

Se puede utilizar el protocolo EST:

- Para inscribir dispositivos de red mediante una identidad de dispositivo única segura
- 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 estas 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 autenticado con TLS. Los clientes no pueden obtener un certificado para nadie más que ellos mismos. En SCEP, la CSR se autentica mediante un secreto compartido entre el cliente y la CA. Esto plantea problemas de seguridad porque alguien con acceso al secreto compartido puede generar certificados para entidades distintas de ellas.
- Soporte para la inscripción de certificados firmados por 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 un mejor rendimiento que otros algoritmos criptográficos como RSA, aunque utiliza un tamaño de clave mucho menor.
- EST se ha creado para admitir la reinscripción automática de certificados.

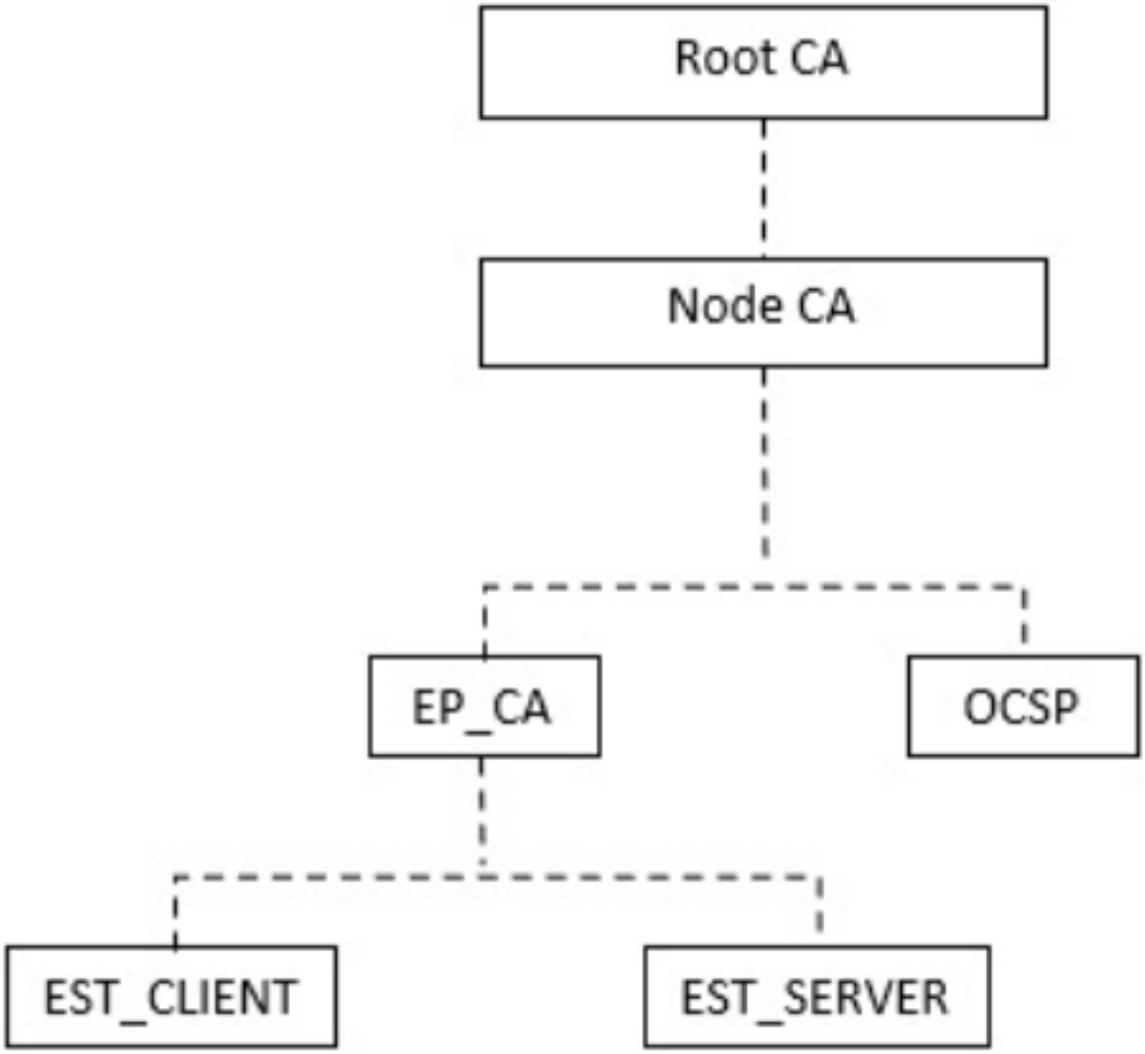
La seguridad demostrada y la mejora continua de TLS ayudan a garantizar que las transacciones EST sean seguras en términos de protección criptográfica. La estrecha integración de SCEP con RSA para proteger los datos plantea problemas de seguridad a medida que avanza la tecnología.

EST en ISE

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

- Cliente EST: integrado en el tomcat de ISE normal.
- EST Server (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 soportada por EST. La CA del terminal emite el certificado para el cliente EST y el servidor EST. Los certificados EST Client y Server y sus respectivas claves se almacenan en la base de datos NSS de la CA de ISE.



Tipos de solicitudes en ISE EST

Siempre que se activa el servidor EST, obtiene la última copia de todos los certificados de CA del servidor de la CA y la almacena. Luego, el cliente EST puede hacer una solicitud de certificado de CA para obtener la cadena completa de este servidor EST. Antes de realizar una solicitud de inscripción sencilla, el cliente EST debe emitir primero la solicitud de certificado CA.

Solicitud de certificados de CA (basada en RFC 7030)

1. El cliente EST solicita una copia de los certificados de CA actuales
2. Mensaje HTTPS GET con un valor de trayectoria de operación de "/cacerts"
3. Esta operación se realiza antes que cualquier otra solicitud EST
4. Se realiza una solicitud cada 5 minutos para obtener una copia de los certificados de CA más actualizados
5. El servidor EST no debe requerir autenticación de cliente

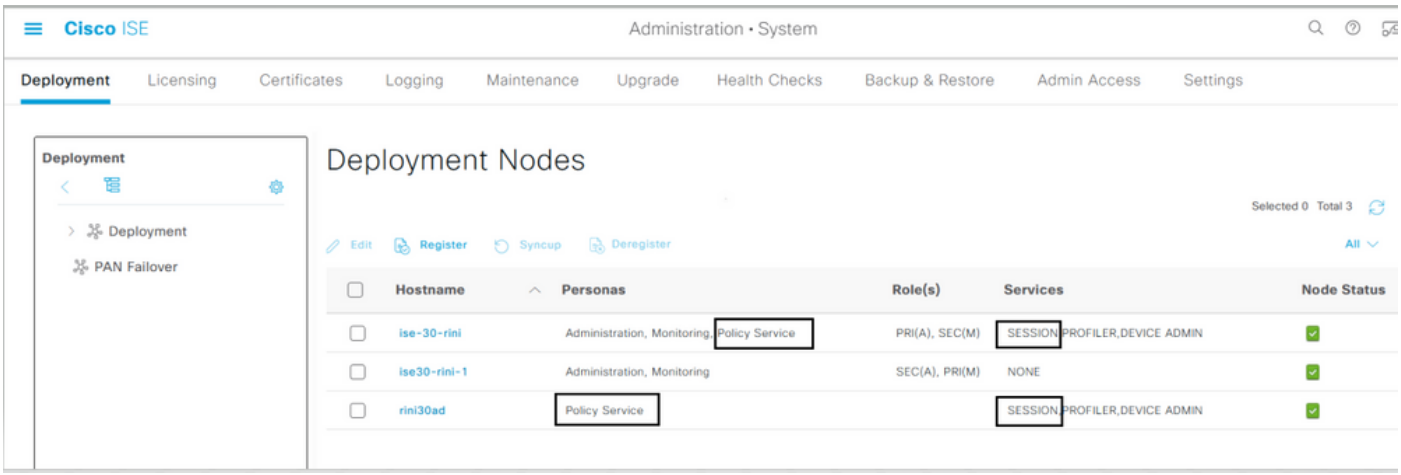
La segunda solicitud es una simple solicitud de inscripción y necesita autenticación entre el cliente EST y el servidor EST. Esto sucede cada vez que un terminal se conecta a ISE y realiza una solicitud de certificado.

Solicitud de inscripción simple (basada en RFC 7030)

1. El cliente EST solicita un certificado del servidor EST
2. mensaje HTTPS POST con el valor de trayectoria de operación de "/simpleenroll"
3. El cliente EST integra la solicitud PKCS#10 en esta llamada que se envía a ISE
4. El servidor EST debe autenticar al cliente

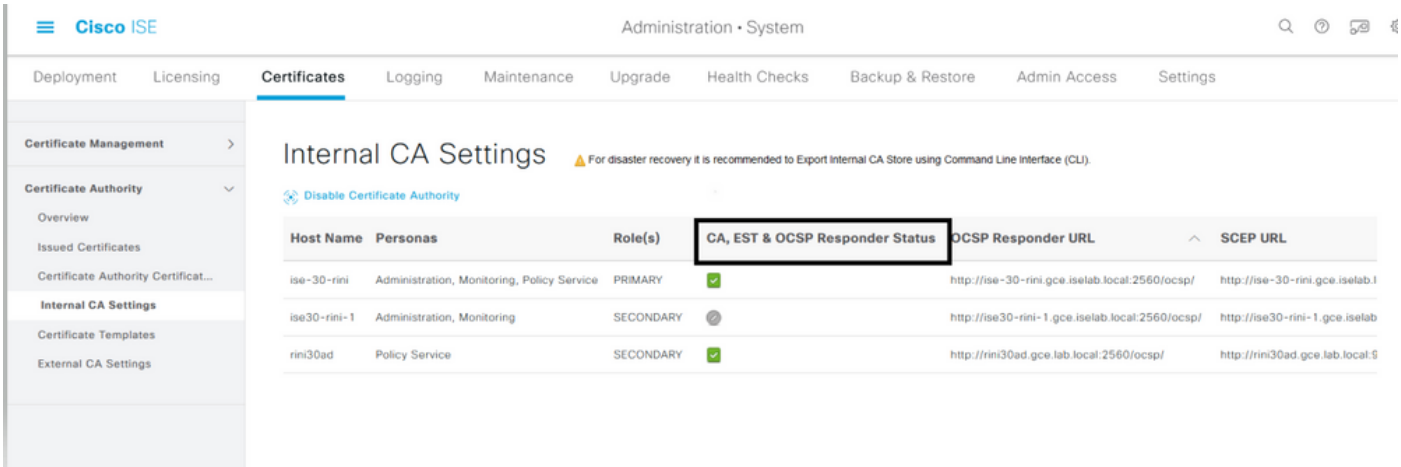
Estado del servicio EST y CA

Los servicios CA y EST sólo se pueden ejecutar en un nodo de servicio de políticas que tenga los servicios de sesión habilitados. Para habilitar los servicios de sesión en un nodo, vaya a **Administration > System > Deployment**. Seleccione el nombre de host del servidor en el que deben habilitarse los servicios de sesión y haga clic en **Editar**. Seleccione la casilla de verificación **"Habilitar servicios de sesión"** bajo la persona Servicio de políticas.



Estado mostrado en la interfaz gráfica de usuario

El estado del servicio EST 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

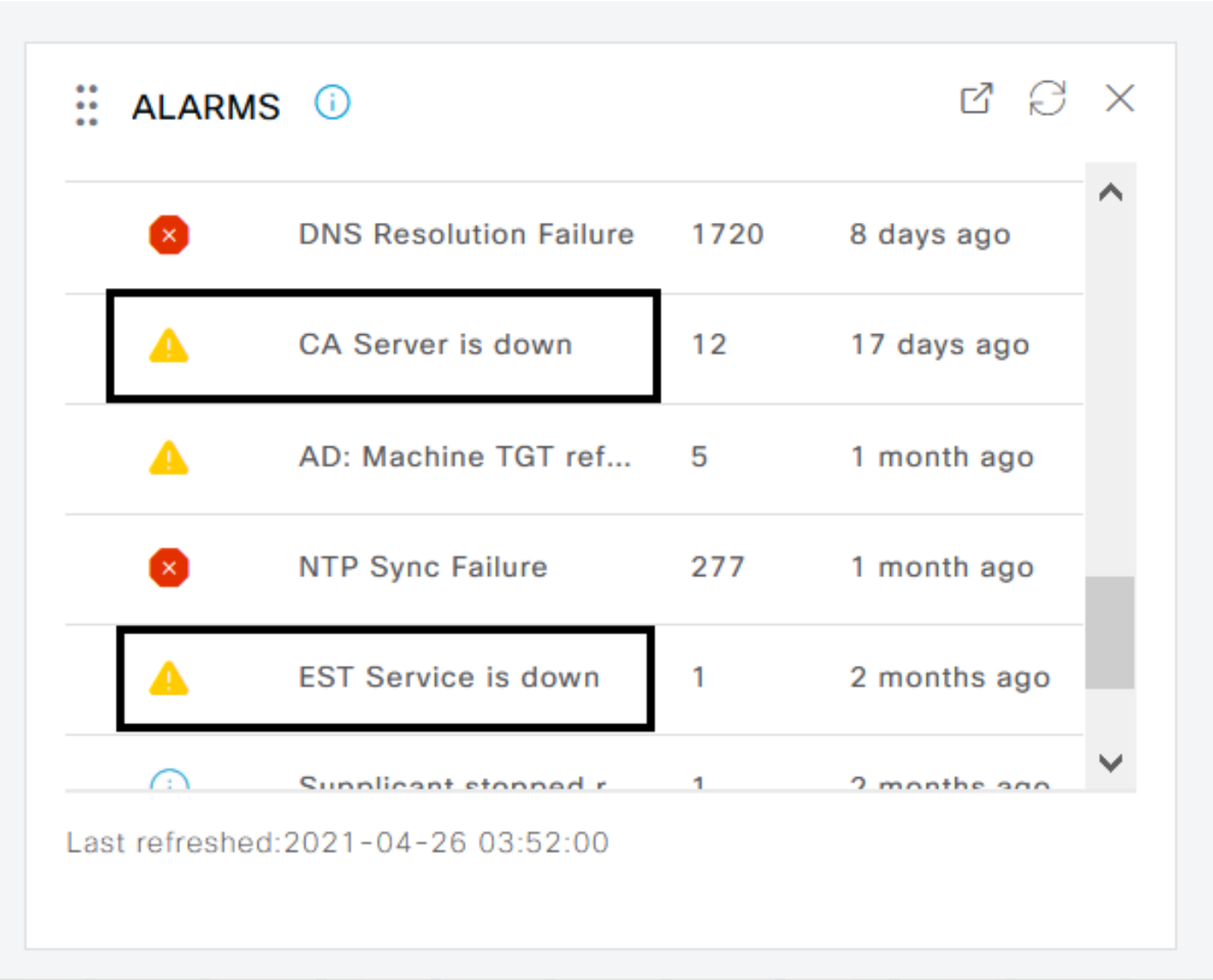
```
ise-30-rini/admin# sh app status ise

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
```

```
ise30-rini-1/admin# sh app stat ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          21387
Database Server                        running          101 PROCESSES
Application Server                     running          33099
Profiler Database                      running          29212
ISE Indexing Engine                    running          34969
AD Connector                           running          36017
M&T Session Database                   running          29020
M&T Log Processor                      running          33296
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          24186
TC-NAC Service                         disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
```

```
rini30ad/admin# sh app status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          18903
Database Server                        running          93 PROCESSES
Application Server                     running          35168
Profiler Database                      running          30941
ISE Indexing Engine                    disabled
AD Connector                           running          35800
M&T Session Database                   disabled
M&T Log Processor                      disabled
Certificate Authority Service          running          92557
EST Service                            running          99310
SXP Engine Service                     disabled
Docker Daemon                          running          23637
TC-NAC Service                         disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
```

Alarmas en el panel

La alarma se mostrará en el panel ISE si los servicios EST y CA están inactivos.



Impacto si los servicios CA y EST no se ejecutan

- El error de llamada "/cacerts" del cliente EST puede ocurrir cuando el servidor EST está inactivo. La falla de llamada "/cacerts" también puede ocurrir si la cadena de CA del certificado EST está incompleta.
- Las solicitudes de inscripción de certificados de punto final basadas en ECC fallarán.
- El flujo de BYOD se interrumpirá si se produce alguna de las dos fallas anteriores.
- Se pueden generar alarmas de error de link de cola.

Troubleshoot

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

- La cadena de certificados Sub CA de terminal de servicios de certificados está completa. Para verificar si la cadena de certificados está completa:Elija **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.Active la casilla de verificación junto al certificado y haga clic en **Ver para verificar un certificado determinado**.

- Asegúrese de que los servicios CA y EST estén en funcionamiento. Si los servicios no se están ejecutando, vaya a **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 CA raíz de ISE después de la actualización. A tal efecto:Elija **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.Haga clic en **Generar solicitudes de firma de certificado (CSR)**.Elija **"ISE Root CA"** en la **lista** desplegable **de certificados se utilizarán para**Haga clic en **Reemplazar cadena de certificado de CA raíz de ISE**.
- Las depuraciones útiles que se pueden habilitar para comprobar los registros incluyen: prueba, aprovisionamiento, ca-service y ca-service-cert. Consulte los archivos ise-psc.log, catalina.out, caservice.log y error.log.