Instalación, renovación y solución de problemas de certificados digitales SSL en Cisco ISE

Contenido

Introducción

Este documento describe la instalación, renovación y soluciones de certificados SSL para los problemas más comunes observados en Identity Services Engine.

Prerequisites

Requirements

Cisco recomienda conocer la GUI de Identity Service Engine.

Componentes Utilizados

La información de este documento se basa en Cisco Identity Service Engine 3.x.

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 proporciona los pasos recomendados y la lista de verificación de problemas comunes que se deben verificar y abordar antes de comenzar a resolver problemas y llamar al Soporte Técnico de Cisco.

Un certificado es un documento electrónico que identifica a una persona, un servidor, una empresa u otra entidad y asocia esa entidad a una clave pública.

Un certificado autofirmado está firmado por su propio creador. Los certificados pueden ser autofirmados o firmados digitalmente por una autoridad de certificación (CA) externa.

Un certificado digital firmado por una CA se considera un estándar del sector y más seguro.

Los certificados se utilizan en una red para proporcionar un acceso seguro.

Cisco ISE utiliza certificados para la comunicación entre nodos y para comunicarse con servidores externos como el servidor Syslog, el servidor de fuentes y todos los portales de usuarios finales (portales de invitados, patrocinadores y dispositivos personales).

Los certificados identifican un nodo de Cisco ISE en un terminal y aseguran la comunicación entre dicho terminal y el nodo de Cisco ISE.

Los certificados se utilizan para todas las comunicaciones HTTPS y el protocolo de autenticación extensible (EAP).

Este documento proporciona los pasos recomendados y la lista de verificación de problemas comunes que se deben verificar y abordar antes de comenzar a resolver problemas y llamar al Soporte Técnico de Cisco.

Estas soluciones provienen directamente de las solicitudes de servicio que el soporte técnico de Cisco ha resuelto. Si su red está activa, asegúrese de comprender el impacto potencial de los

pasos que debe realizar para solucionar los problemas.

Configurar

Las guías siguientes explican cómo importar y reemplazar certificados:

Importación de un certificado del sistema

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

Sustitución de un certificado caducado

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

Problemas comunes

Situación 1: no se puede sustituir un certificado de portal que vence en un nodo ISE

Error

Mientras se enlaza el nuevo certificado del portal con el CSR, el proceso de enlace del certificado falla con el siguiente error:

Internal Error. Pida al administrador de ISE que compruebe los registros para obtener más información

Las razones más comunes de este error son:

- El nuevo certificado tiene el mismo nombre de sujeto que el certificado existente

- Importar un certificado renovado que utiliza la misma clave privada de un certificado existente

Solución

1. Asignar temporalmente el uso del portal a otro certificado en el mismo nodo
2. Eliminar el certificado de portal que caduca
3. Instale el nuevo certificado del portal y, a continuación, asigne el uso del portal

Por ejemplo, si desea asignar temporalmente el uso del portal a un certificado existente con el uso de autenticación EAP, siga los pasos siguientes:

Paso 1. Seleccione y edite el certificado con el uso de autenticación EAP, agregue la función Portal en Uso y guarde

Paso 2. Eliminar el certificado de portal que caduca

Paso 3. Cargue el nuevo certificado del portal sin seleccionar ningún rol (en Uso) y haga clic en Enviar

Paso 4. Seleccione y edite el nuevo certificado de portal, asigne la función Portal en Uso y Guardar

Situación 2: no se pueden generar dos CSR para el mismo nodo de ISE con el uso de varios usos

Error

La nueva creación de CSR para el mismo nodo con uso multiuso falla con el siguiente error: Ya existe otro certificado con el mismo nombre descriptivo. Los nombres descriptivos deben ser únicos.

Solución

Los nombres descriptivos de CSR están codificados para cada nodo de ISE, por lo que no permiten la creación de 2 CSR para el mismo nodo con uso multiuso. El caso práctico se encuentra en un nodo específico, hay un certificado firmado por CA que se utiliza para el uso de autenticación de administración y EAP y otro certificado firmado por CA que se utiliza para el uso de SAML y Portal y ambos certificados van a caducar.

En esta situación:

Paso 1. Generación de la primera CSR con uso multiuso

Paso 2. Enlace el certificado firmado por la CA con la primera CSR y asigne el rol de administración y autenticación EAP

Paso 3. Generar un segundo CSR con uso multiuso

Paso 4. Enlazar el certificado firmado por la CA con el segundo CSR y asignar la función SAML y Portal

Situación 3: no se puede enlazar el certificado firmado por la CA para el uso del portal o no se puede asignar la etiqueta del portal al certificado y se obtiene un error

Error

El enlace de un certificado firmado por una CA para el uso del portal produce el error:

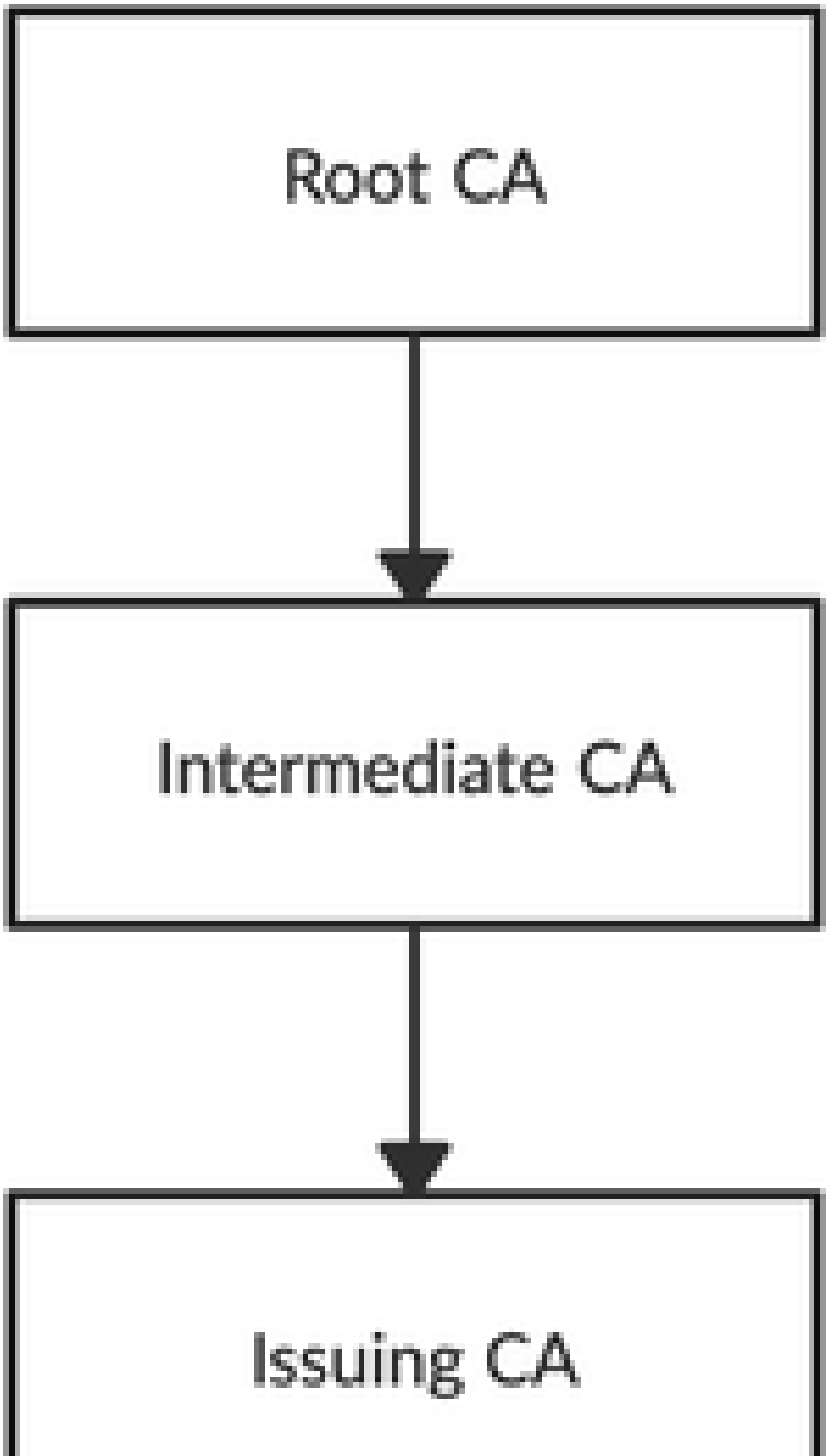
Hay uno o más certificados de confianza que forman parte de la cadena de certificados del

sistema del portal o que se han seleccionado con un rol de autenticación de administrador basado en certificados con el mismo nombre de asunto pero con un número de serie diferente. Se anuló la importación/actualización. Para que la importación/actualización sea correcta, debe deshabilitar el rol de autenticación de administrador basado en carrito de un certificado de confianza duplicado o cambiar el rol de portal del certificado del sistema que contiene el certificado de confianza duplicado en su cadena.

Solución

Paso 1. Compruebe la cadena de certificados del certificado firmado por la CA (para el uso del portal) y, en el almacén de certificados de confianza, compruebe si tiene certificados duplicados de la cadena de certificados.
Paso 2. Quite el certificado duplicado o desmarque la casilla Trust for certificate-based admin authentication del certificado duplicado.

Por ejemplo, el certificado de portal firmado por la CA tiene la siguiente cadena de certificados:


Root CA
Intermediate CA
Issuing CA

2. Verifique que el certificado autofirmado predeterminado caducado no esté asociado con ningún rol específico (uso). Esto se puede verificar en Administración > Sistema > Certificados > Certificados del sistema.

Si el problema continúa, póngase en contacto con el TAC.

Situación 5: no se puede enlazar el certificado pxGrid firmado por la CA con el CSR en un nodo ISE

Error

Al enlazar el nuevo certificado pxGrid con el CSR, el proceso de enlace del certificado falla con el error:

El certificado para pxGrid debe contener tanto la autenticación del cliente como la del servidor en la extensión de uso extendido de claves (EKU).

Solución

Asegúrese de que el certificado pxGrid firmado por la CA debe tener el uso de clave extendido Autenticación de servidor web TLS (1.3.6.1.5.5.7.3.1) y Autenticación de cliente web TLS (1.3.6.1.5.5.7.3.2) porque se utiliza para la autenticación de cliente y servidor (para proteger la comunicación entre el cliente pxGrid y el servidor)

Enlace de referencia: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

Situación 6: no se puede eliminar el certificado autofirmado predeterminado caducado del almacén de certificados de confianza debido a una configuración de perfil LDAP o SCEP RA existente

Error

Si elimina el certificado autofirmado predeterminado caducado del almacén de certificados de confianza, se producirá el error:

No se pudo eliminar el certificado de confianza porque se hace referencia a él en otro lugar, posiblemente desde un perfil SCEP RA o un origen de identidad LDAP

* Certificado de servidor autofirmado predeterminado

Para eliminar los certificados, elimine el perfil SCEP RA o edite el origen de identidad LDAP para no utilizar este certificado.

Solución

1. Vaya a Administration > Identity Management > External Identity Sources > LDAP > Server Name > Connection
2. Asegúrese de que la CA raíz del servidor LDAP no esté utilizando el "certificado de servidor autofirmado predeterminado"
3. Si el servidor LDAP no está utilizando el certificado necesario para una conexión segura, navegue hasta Administración > Sistema > Certificados > Autoridad de certificación > Configuración de CA externa > Perfiles SCEP RA
4. Asegúrese de que ninguno de los perfiles de SCEP RA esté utilizando un certificado autofirmado predeterminado

Recursos adicionales

Cómo instalar un certificado comodín
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

Administrar certificados ISE
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

Instalación de un certificado de CA de terceros en ISE
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html

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).