Installation, renouvellement et dépannage des certificats numériques SSL sur Cisco ISE

Table des matières

Introduction

Ce document décrit l'installation, le renouvellement et la résolution des problèmes les plus

courants observés sur Identity Services Engine.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Interface utilisateur graphique Identity Service Engine

Composants utilisés

Les informations contenues dans ce document sont basées sur la version logicielle suivante :

- Cisco Identity Service Engine 2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document présente les étapes recommandées et la liste de contrôle des problèmes courants à vérifier et à résoudre avant de commencer à dépanner et à appeler l'assistance technique Cisco.

Un certificat est un document électronique qui identifie un individu, un serveur, une société ou une autre entité et associe cette entité à une clé publique.

Un certificat auto-signé est signé par son propre créateur. Les certificats peuvent être auto-signés ou signés numériquement par une autorité de certification externe.

Un certificat numérique signé par une autorité de certification est considéré comme une norme industrielle et plus sûr.

Les certificats sont utilisés dans un réseau pour fournir un accès sécurisé.

Cisco ISE utilise des certificats pour la communication entre les noeuds et pour la communication avec des serveurs externes tels que le serveur Syslog, le serveur de flux et tous les portails d'utilisateurs finaux (portails d'invité, de sponsor et de périphériques personnels).

Les certificats identifient un noeud Cisco ISE à un terminal et sécurisent la communication entre ce terminal et le noeud Cisco ISE.

Les certificats sont utilisés pour toutes les communications HTTPS et EAP (Extensible Authentication Protocol).

Ce document présente les étapes recommandées et la liste de contrôle des problèmes courants à

vérifier et à résoudre avant de commencer à dépanner et à appeler l'assistance technique Cisco.

Ces solutions proviennent directement de demandes de service que l'assistance technique Cisco a résolues. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel des étapes que vous avez suivies pour résoudre les problèmes.

Configurer

Les guides suivants expliquent comment importer et remplacer des certificats :

Importation d'un certificat système

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

Remplacement d'un certificat expiré

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

Problèmes courants

Scénario 1 : impossible de remplacer un certificat de portail arrivant à expiration sur un noeud ISE

Erreur

Lors de la liaison du nouveau certificat du portail avec le CSR, le processus de liaison de certificat échoue avec l'erreur ci-dessous :

Erreur interne. Demandez à votre administrateur ISE de vérifier les journaux pour plus de détails

Les raisons les plus courantes de cette erreur sont :

- Le nouveau certificat porte le même nom de sujet que le certificat existant

- Importer un certificat renouvelé qui utilise la même clé privée qu'un certificat existant

Solution

1. Affecter temporairement l'utilisation du portail à un autre certificat sur le même noeud
2. Supprimer le certificat du portail arrivant à expiration
3. Installez le nouveau certificat du portail, puis attribuez l'utilisation du portail

Par exemple, si vous souhaitez attribuer temporairement l'utilisation du portail à un certificat existant avec l'utilisation de l'authentification EAP, procédez comme suit :

Étape 1. Sélectionnez et modifiez le certificat avec l'utilisation de l'authentification EAP, ajoutez le rôle de portail sous Utilisation et enregistrez

Étape 2. Supprimer le certificat du portail arrivant à expiration

Étape 3. Téléchargez le nouveau certificat du portail sans sélectionner de rôle (sous Utilisation) et cliquez sur Envoyer

Étape 4. Sélectionnez et modifiez le nouveau certificat de portail, attribuez un rôle de portail sous Utilisation et Enregistrer

Scénario 2 : impossible de générer deux CSR pour le même noeud ISE avec une utilisation multi-utilisation

Erreur

La création d'une nouvelle CSR pour le même noeud avec utilisation multiple échoue avec l'erreur :
Un autre certificat portant le même nom convivial existe déjà. Les noms conviviaux doivent être uniques.

Solution

Les noms CSR sont codés en dur pour chaque noeud ISE, de sorte qu'il n'est pas possible de créer 2 CSR pour le même noeud avec une utilisation multifonction. L'exemple d'utilisation est sur un noeud spécifique, il y a un certificat signé par une autorité de certification qui est utilisé pour l'utilisation de l'authentification Admin et EAP et un autre certificat signé par une autorité de certification qui est utilisé pour l'utilisation de SAML et Portal et les deux certificats vont expirer.

Dans ce scénario :

Étape 1. Génération de la première RSE avec utilisation multifonction

Étape 2. Liez le certificat signé par l'autorité de certification au premier CSR et attribuez le rôle d'authentification Admin et EAP

Étape 3. Générer une deuxième CSR avec utilisation multifonction

Étape 4. Lier le certificat signé par l'autorité de certification à un deuxième CSR et attribuer un rôle SAML et Portal

Scénario 3 : impossible de lier le certificat signé par l'autorité de certification pour l'utilisation du portail ou impossible d'attribuer la balise de portail au certificat et obtention d'une erreur

Erreur

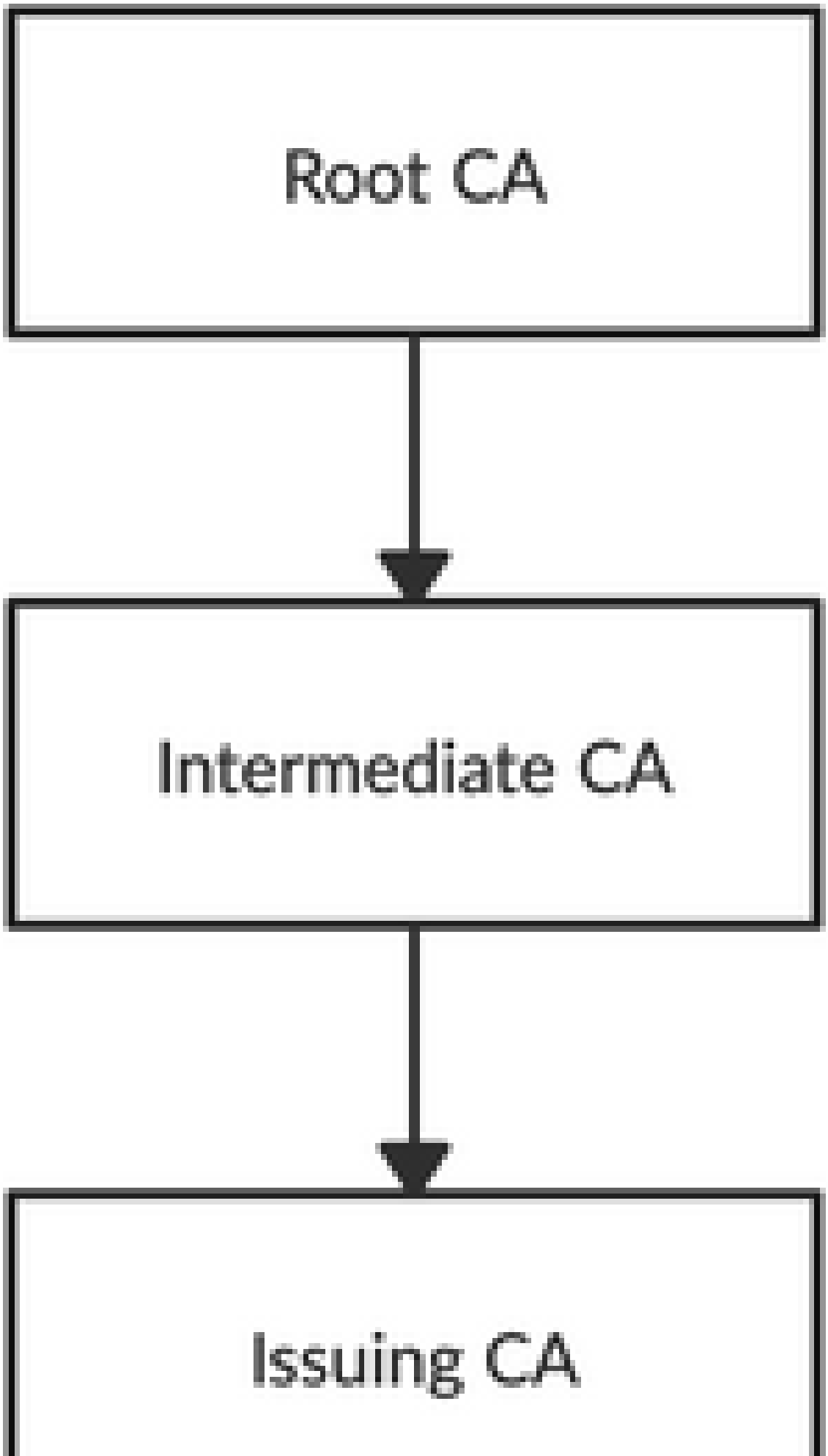
La liaison du certificat signé par l'autorité de certification pour l'utilisation du portail renvoie l'erreur :

Un ou plusieurs certificats de confiance font partie de la chaîne de certificats du système de portail ou sont sélectionnés avec un rôle d'auth. admin basé sur les certificats avec le même nom de sujet mais avec un numéro de série différent. L'importation/mise à jour a été abandonnée. Pour réussir l'importation/la mise à jour, vous devez désactiver le rôle d'authentification admin basé sur le panier à partir d'un certificat sécurisé dupliqué ou modifier le rôle de portail à partir du certificat système qui contient le certificat sécurisé dupliqué dans sa chaîne.

Solution

Étape 1. Vérifiez la chaîne de certificats du certificat signé par l'autorité de certification (pour l'utilisation du portail) et dans le magasin Certificats approuvés, vérifiez si vous avez des certificats dupliqués de la chaîne de certificats.
Étape 2. Supprimez le certificat dupliqué ou décochez la case Approuver pour l'authentification d'administrateur basée sur certificat du certificat dupliqué.

Par exemple, le certificat du portail signé par l'autorité de certification possède la chaîne de certificats ci-dessous :


Root CA
Intermediate CA
Issuing CA

2. Vérifiez que le certificat auto-signé par défaut expiré n'est associé à aucun rôle spécifique (utilisation). Ceci peut être vérifié sous Administration > Système > Certificats > Certificats système.

Si le problème persiste, contactez le TAC.

Scénario 5 : impossible de lier le certificat pxGrid signé par l'autorité de certification au CSR sur un noeud ISE

Erreur

Lors de la liaison du nouveau certificat pxGrid avec le CSR, le processus de liaison de certificat échoue avec l'erreur :

Le certificat pour pxGrid doit contenir l'authentification client et serveur dans l'extension Extended Key Usage (EKU).

Solution

Assurez-vous que le certificat pxGrid signé par l'autorité de certification doit avoir à la fois l'authentification de serveur Web TLS (1.3.6.1.5.5.7.3.1) et l'authentification de client Web TLS (1.3.6.1.5.5.7.3.2) pour une utilisation de clé étendue, car il est utilisé pour l'authentification du client et du serveur (pour sécuriser la communication entre le client et le serveur pxGrid)

Lien de référence : 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

Scénario 6 : impossible de supprimer le certificat auto-signé par défaut expiré du magasin de certificats de confiance en raison de la configuration existante du profil d'autorité de certification LDAP ou SCEP

Erreur

La suppression du certificat auto-signé par défaut expiré du magasin de certificats approuvés entraîne l'erreur suivante :

Le certificat d'approbation n'a pas pu être supprimé car il est référencé ailleurs, peut-être à partir d'un profil SCEP RA ou d'une source d'identité LDAP

* Certificat de serveur auto-signé par défaut

Afin de supprimer le(s) certificat(s), supprimez le profil SCEP RA ou modifiez la source d'identité LDAP pour ne pas utiliser ce certificat.

Solution

1. Accédez à Administration > Identity Management > External Identity Sources > LDAP > Server Name > Connection
2. Assurez-vous que l'autorité de certification racine du serveur LDAP n'utilise pas le certificat de serveur auto-signé par défaut
3. Si le serveur LDAP n'utilise pas le certificat requis pour une connexion sécurisée, accédez à Administration > System > Certificates > Certificate Authority > External CA Settings > SCEP RA Profiles
4. Assurez-vous qu'aucun des profils SCEP RA n'utilise le certificat auto-signé par défaut

Ressources supplémentaires

Comment installer un certificat générique
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

Gérer les certificats 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

Installer un certificat CA tiers sur 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.