Comprendre les services ISE internes des autorités de certification

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Service d'autorité de certification (CA)
  - Fonctionnalité ISE CA
  - Certificats d'autorité de certification ISE provisionnés sur les noeuds de service Administration et Stratégie
- Inscription sur le service de transport sécurisé (EST)
  - Exemples d'utilisation EST
  - Pourquoi EST ?
  - EST dans ISE
  - Types de demandes dans ISE EST
    - Demande de certificats CA (basée sur RFC 7030)
    - Demande d'inscription simple (basée sur RFC 7030)
- État du service EST et CA
  - État affiché sur l'interface graphique
  - État affiché sur CLI
  - Alarmes sur le tableau de bord
  - Impact si les services CA et EST ne sont pas en cours d'exécution
- Dépannage
- Informations connexes

Introduction

Ce document décrit le service AC et le service d'inscription sur transport sécurisé (EST) qui est présent dans Cisco Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Certificats et infrastructure à clé publique (PKI)
- Protocole SCEP (Simple Certificate Enrollment Protocol)

- Protocole OCSP (Online Certificate Status Protocol)

Composants utilisés

Les informations contenues dans ce document sont basées sur Identity Services Engine 3.0.

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.

Service d'autorité de certification (CA)

Les certificats peuvent être auto-signés ou signés numériquement par une autorité de certification externe. L'autorité de certification interne Cisco ISE émet et gère les certificats numériques pour les terminaux à partir d'une console centralisée afin de permettre aux employés d'utiliser leurs périphériques personnels sur le réseau de l'entreprise. Un certificat numérique signé par une autorité de certification est considéré comme une norme industrielle et plus sûr. Le noeud PAN (Primary Policy Administration Node) est l’autorité de certification racine. Les noeuds de service de stratégie (PSN) sont des AC subordonnées au PAN principal.

Fonctionnalité ISE CA

La CA ISE offre les fonctionnalités suivantes :

- Émission du certificat : Valide et signe les demandes de signature de certificat (CSR) pour les terminaux qui se connectent au réseau.
- Gestion des clés : Génère et stocke de manière sécurisée les clés et les certificats sur les noeuds PAN et PSN.
- Stockage de certificat : Stocke les certificats délivrés aux utilisateurs et aux périphériques.
- Support OCSP (Online Certificate Status Protocol) : Fournit un répondeur OCSP pour vérifier la validité des certificats.

Certificats d'autorité de certification ISE provisionnés sur les noeuds de service Administration et Stratégie

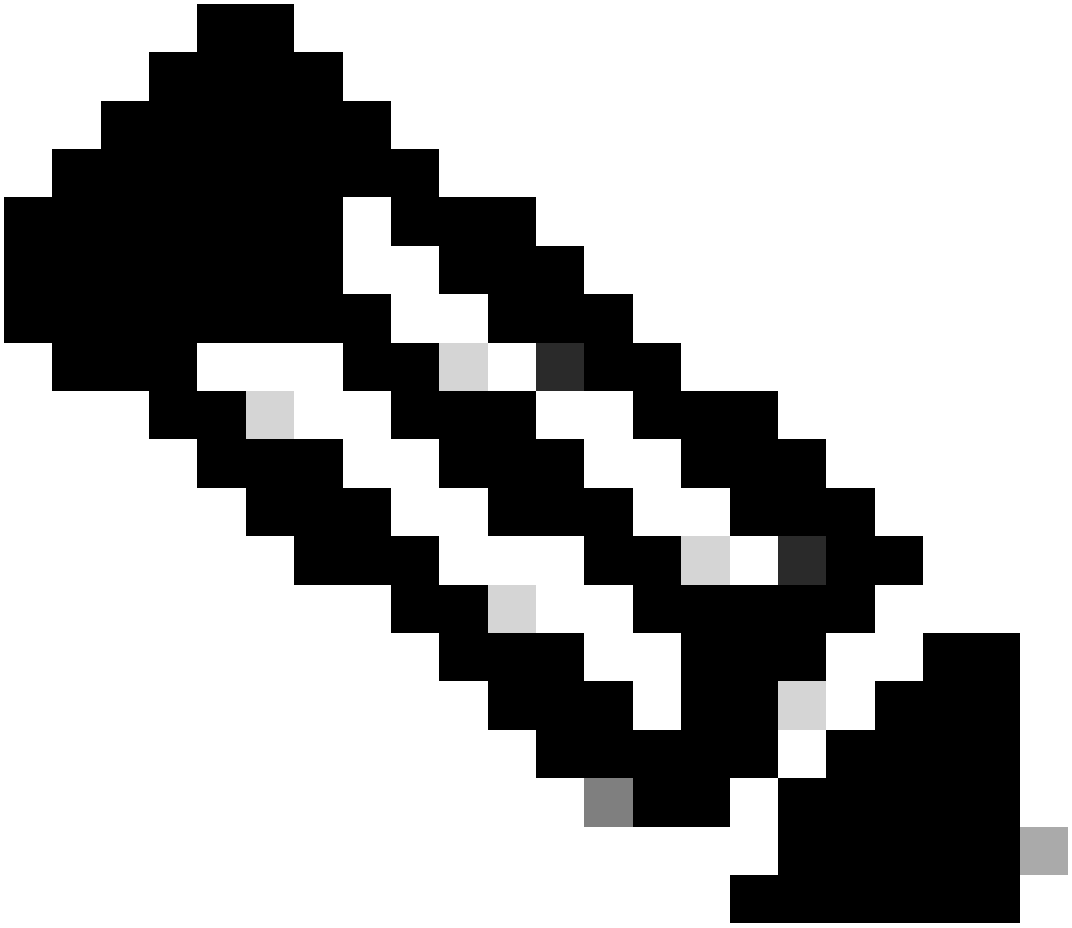
Après l'installation, un noeud Cisco ISE est doté d'un certificat CA racine et d'un certificat CA de noeud pour gérer les certificats des terminaux.

Lorsqu'un déploiement est configuré, le noeud désigné comme noeud d'administration principal (PAN) devient l'autorité de certification racine. Le PAN a un certificat d'autorité de certification racine et un certificat d'autorité de certification de noeud qui est signé par l'autorité de certification racine.



Lorsqu'un noeud d'administration secondaire (SAN) est enregistré dans le PAN, un certificat d'autorité de certification de noeud est généré et signé par l'autorité de certification racine sur le noeud d'administration principal.

Tout noeud de service de stratégie (PSN) enregistré avec le PAN est doté d'une autorité de certification de point de terminaison et d'un certificat OCSP signé par l'autorité de certification de noeud du PAN. Les noeuds de service de stratégie (PSN) sont des AC subordonnées au PAN. Lorsque l'autorité de certification ISE est utilisée, l'autorité de certification de point de terminaison sur le PSN émet les certificats aux points de terminaison qui accèdent au réseau.



Remarque : La hiérarchie de certificats OCSP a été modifiée à partir du correctif 2 ISE 3.1 et de la séquence de contrôle de trame ISE 3.2.

Conformément à la RFC 6960 :

« Un émetteur de certificat DOIT effectuer l'une des opérations suivantes :

- signer les réponses OCSP elles-mêmes, ou

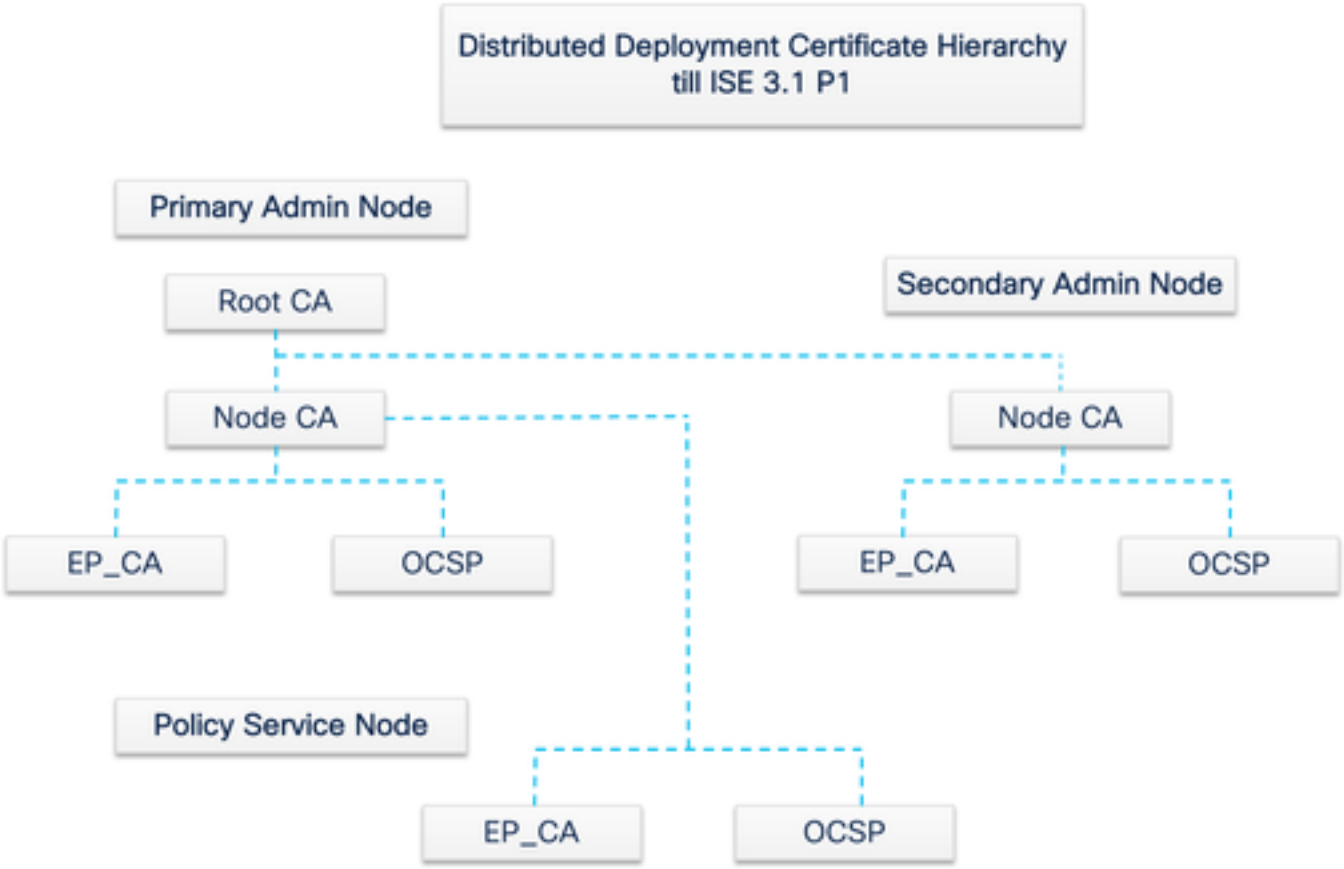
- désigner explicitement cette autorité auprès d'une autre entité »

«Le certificat de signataire de réponse OCSP DOIT être émis directement par l'autorité de certification qui est identifiée dans la demande. "

«Le système (se base) sur les réponses OCSP DOIT reconnaître un certificat de délégation tel qu'émis par l'autorité de certification qui a émis le certificat en question seulement si le certificat de

délégation et le certificat (s'il est) vérifié pour la révocation ont été signés par la même clé.»

Afin d'être conforme à la norme RFC mentionnée précédemment, la hiérarchie de certificats pour le certificat de répondeur OCSP est modifiée dans ISE. Le certificat du répondeur OCSP est désormais émis par l'autorité de certification secondaire du point d'extrémité du même noeud au lieu de l'autorité de certification du noeud dans le PAN.



Inscription sur le service de transport sécurisé (EST)

Le concept d'infrastructure à clé publique (ICP) existe depuis longtemps. L'ICP authentifie l'identité des utilisateurs et des périphériques au moyen de paires de clés publiques signées sous la forme de certificats numériques. L'inscription sur le transport sécurisé (EST) est un protocole qui fournit ces certificats. Le service EST définit comment effectuer l'inscription de certificats pour les clients qui utilisent la gestion de certificats sur la syntaxe de message cryptographique (CMC) sur un transport sécurisé. Selon l'IETF, « EST » décrit un protocole de gestion des certificats simple mais fonctionnel qui cible les clients PKI (Public Key Infrastructure) devant acquérir des certificats clients et les certificats CA associés. Il prend également en charge les paires de clés publiques/privées générées par le client, ainsi que les paires de clés générées par l'autorité de certification. »

Exemples d'utilisation EST

Le protocole EST peut être utilisé :

- Pour inscrire des périphériques réseau à l'aide de l'identité unique sécurisée des périphériques
- Pour les solutions BYOD

Pourquoi EST ?

Les protocoles EST et SCEP traitent de la mise en service des certificats. EST est le successeur du protocole SCEP (Simple Certificate Enrollment Protocol). En raison de sa simplicité, le protocole SCEP est le protocole de facto dans le provisionnement des certificats depuis de nombreuses années. Cependant, l'utilisation de l'EST au lieu du SCEP est recommandée pour les raisons suivantes :

- Utilisation de TLS pour le transport sécurisé des certificats et des messages - Dans EST, la demande de signature de certificat (CSR) peut être liée à un demandeur qui est déjà approuvé et authentifié avec TLS. Les clients ne peuvent obtenir de certificat que pour eux-mêmes. Dans SCEP, le CSR est authentifié par un secret partagé entre le client et l'autorité de certification. Cela pose des problèmes de sécurité, car une personne ayant accès au secret partagé peut générer des certificats pour des entités autres qu'elle-même.
- Prise en charge de l'inscription des certificats signés ECC - EST offre une agilité cryptographique. Il prend en charge la cryptographie à courbe elliptique (ECC). SCEP ne prend pas en charge ECC et dépend du chiffrement RSA. ECC offre plus de sécurité et de meilleures performances que d'autres algorithmes cryptographiques tels que RSA, même s'il utilise une taille de clé beaucoup plus petite.
- EST est conçu pour prendre en charge la réinscription automatique des certificats.

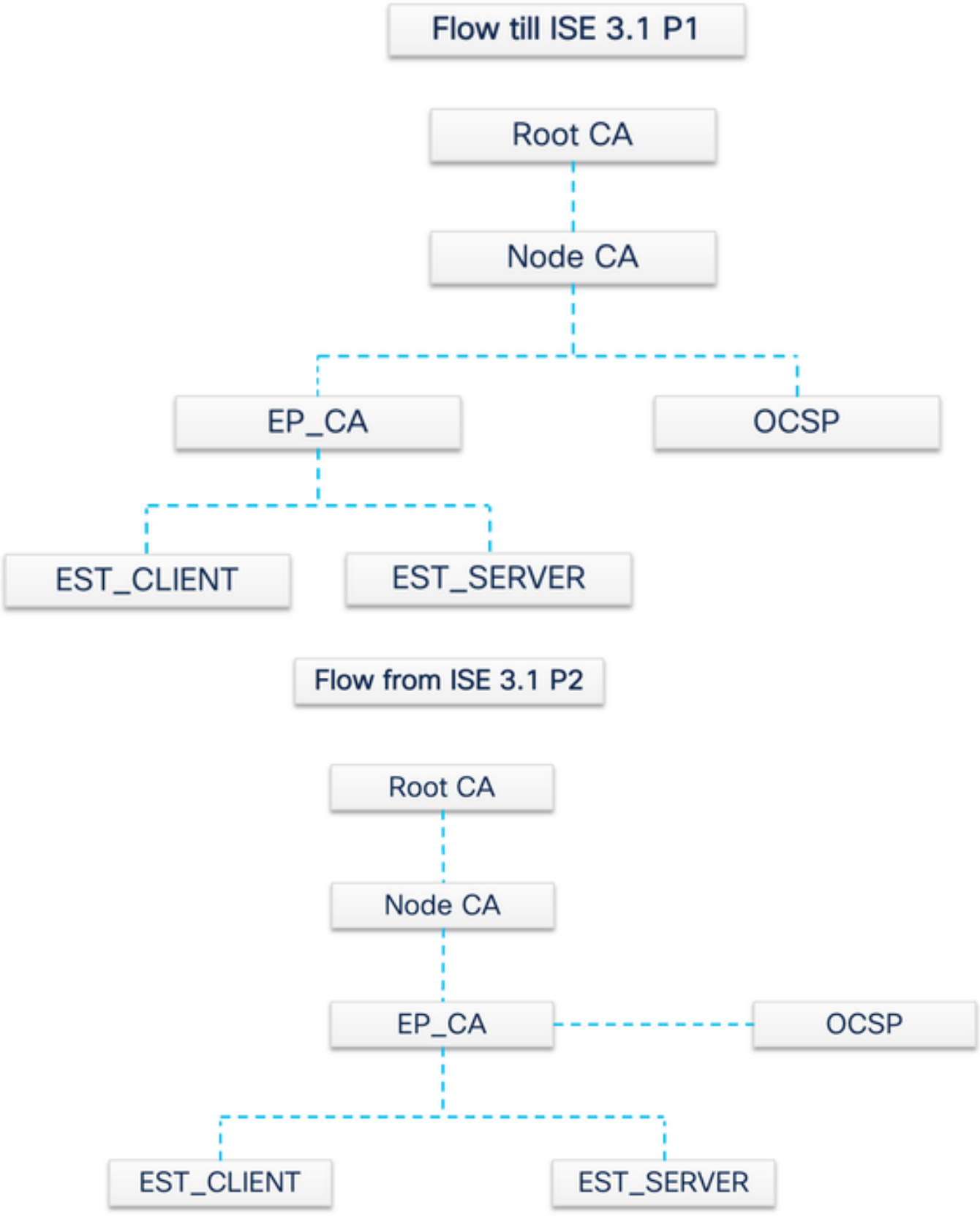
La sécurité éprouvée de TLS et l'amélioration continue garantissent la sécurité des transactions EST en termes de protection cryptographique. L'intégration étroite du SCEP avec RSA pour protéger les données pose des problèmes de sécurité à mesure que la technologie évolue.

EST dans ISE

Pour implémenter ce protocole, un client et un module serveur sont nécessaires :

- Client EST - intégré dans le tomcat ISE standard.
- Serveur EST : déployé sur un serveur Web open source appelé NGINX. Ce processus s'exécute comme un processus distinct et il écoute sur le port 8084.

L'authentification client et serveur basée sur les certificats est prise en charge par EST. L’autorité de certification du point de terminaison émet le certificat pour le client EST et le serveur EST. Les certificats du client et du serveur EST et leurs clés respectives sont stockés dans la base de données NSS de l'autorité de certification ISE.



Types de demandes dans ISE EST

Chaque fois que le serveur EST apparaît, il obtient la dernière copie de tous les certificats CA du serveur CA et la stocke. Ensuite, le client EST peut faire une demande de certificat CA pour obtenir toute la chaîne de ce serveur EST. Avant d'effectuer une simple demande d'inscription, le client EST doit d'abord émettre la demande de certificat CA.

Demande de certificats CA (basée sur RFC 7030)

1. Le client EST demande une copie des certificats CA actuels.
2. Message GET HTTPS avec une valeur de chemin d'opération de /cacerts.
3. Cette opération est effectuée avant toute autre requête EST.
4. Une demande est faite toutes les 5 minutes pour obtenir une copie des certificats d'autorité de certification les plus à jour.
5. Le serveur EST ne doit pas nécessiter d'authentification client.

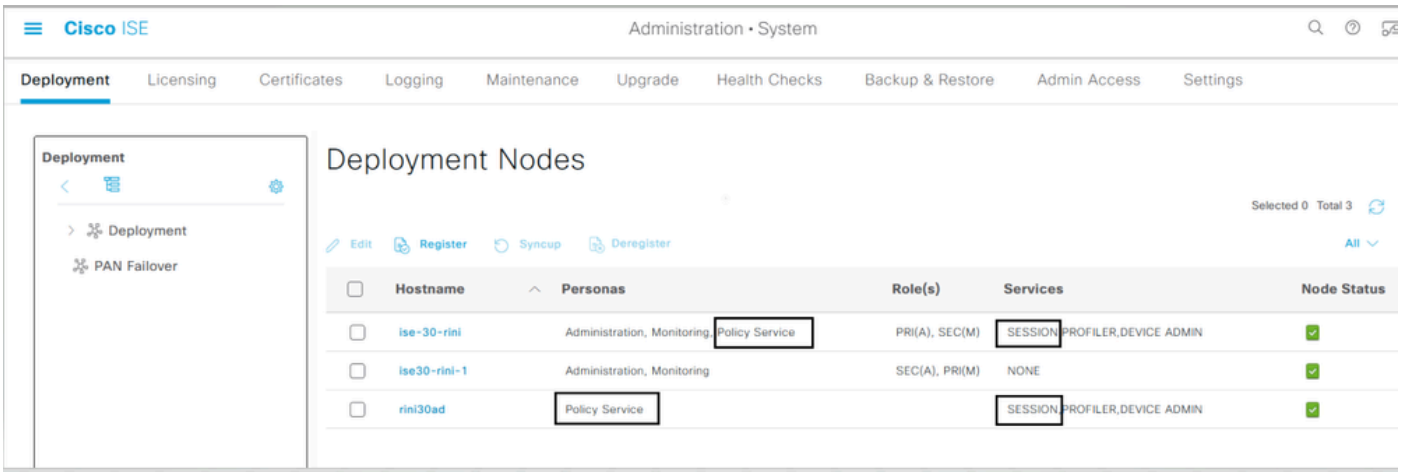
La deuxième demande est une simple demande d'inscription et nécessite une authentification entre le client EST et le serveur EST. Cela se produit chaque fois qu'un terminal se connecte à ISE et fait une demande de certificat.

Demande d'inscription simple (basée sur RFC 7030)

1. Le client EST demande un certificat au serveur EST.
2. Message HTTPS POST avec la valeur du chemin d'opération de/simpleenroll.
3. Le client EST intègre la requête PKCS#10 dans cet appel qui est envoyé à ISE.
4. Le serveur EST doit authentifier le client.

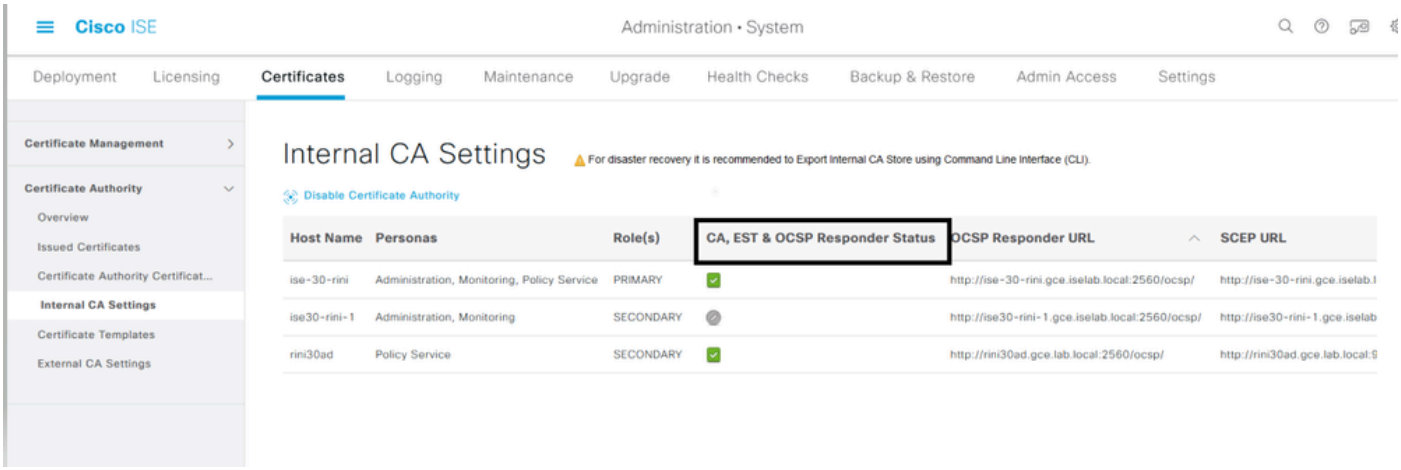
État du service EST et CA

Les services AC et EST ne peuvent s'exécuter que sur un noeud Service de stratégie sur lequel les services de session sont activés. Pour activer les services de session sur un noeud, accédez àAdministration > System > Deployment. Sélectionnez le nom d'hôte du serveur sur lequel les services de session doivent être activés et cliquez surEdit. Activez la case à cocher située **Enable Session Services** sous Profil du service de stratégie.



État affiché sur l'interface graphique

L'état du service EST est lié à l'état du service AC ISE sur ISE. Si le service AC est actif, le service EST est actif et si le service AC est inactif, le service EST est également inactif.



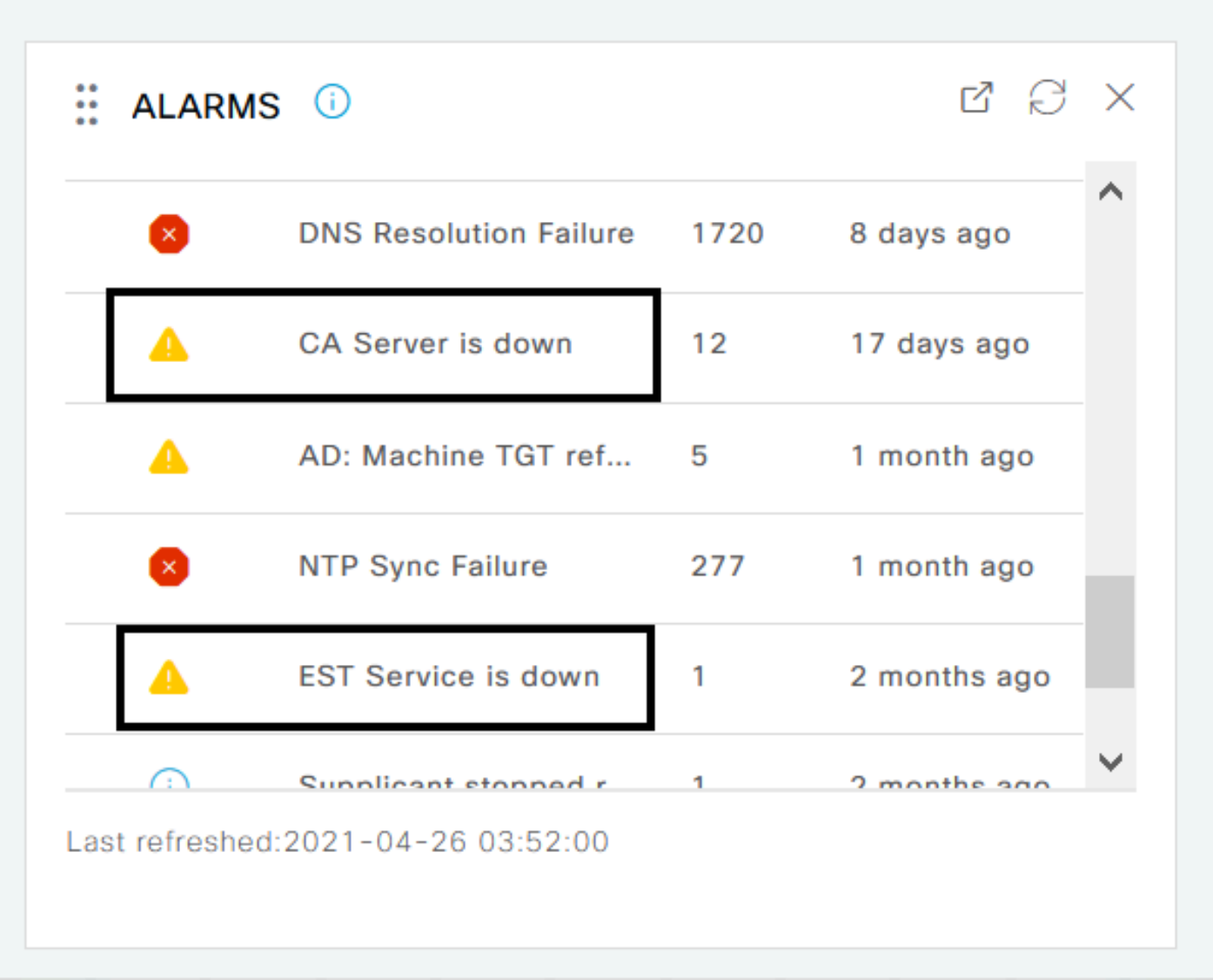
État affiché sur CLI

```
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
```

Alarmes sur le tableau de bord

L'alarme est affichée sur le tableau de bord ISE si les services EST et CA sont désactivés.



Impact si les services CA et EST ne sont pas en cours d'exécution

- Un échec d'appel du client EST/cacertspeut se produire lorsque le serveur EST est arrêté. /cacertsL'échec de l'appel peut également se produire si la chaîne de certificat CA de la chaîne EST est incomplète.
- Les demandes d'inscription de certificat de point de terminaison ECC échouent.
- Le flux BYOD se rompt si l'une des deux défaillances précédentes se produit.
- Des alarmes d'erreur Queue Link peuvent être générées.

Dépannage

Si le flux BYOD avec le protocole EST ne fonctionne pas correctement, vérifiez les conditions suivantes :

- La chaîne de certificats du point de terminaison des services de certificats est terminée. Afin de vérifier si la chaîne de certificats est complète :

  1. Accédez àAdministration > System > Certificates > Certificate Authority > Certificate Authority Certificates.

2. Activez la case à cocher en regard du certificat et cliquez sur View afin de vérifier un certificat particulier.

- Assurez-vous que les services AC et EST sont opérationnels. Si les services ne sont pas en cours d'exécution, accédez à pourAdministration > System > Certificates > Certificate Authority > Internal CA Settingsactiver le service AC.
- Si une mise à niveau a été effectuée, remplacez la chaîne de certificats de l'autorité de certification racine ISE après la mise à niveau. Pour ce faire :

1. SélectionnezAdministration > System > Certificates > Certificate Management > Certificate Signing Requests.
2. Cliquez surGenerate Certificate Signing Requests (CSR).
3. SélectionnezISE Root CAdans la liste déroulanteCertificate(s) will be used for.
4. Cliquez surReplace ISE Root CA Certificate Chain.

- Le débogage utile qui peut être activé pour vérifier les journaux incluttest,provisioning,ca-serviceetca-service-cert. Reportez-vous àise-psc.log,catalina.out,caservice.log , et fichierserror.log.

Informations connexes

- Assistance technique de Cisco et téléchargements

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.

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.