# Problèmes d'intégration Prime Infrastructure 3.5+ dus au certificat TOFU

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Problème
- Dépannage
- Solution
  - Configuration
    - Afficher la liste de validation des certificats
    - Supprimer le certificat
    - Réinitialiser la haute disponibilité du primaire au secondaire
    - Reconfigurer les serveurs ISE
- Vérifier
- Informations connexes


## Introduction

Ce document décrit le problème d'intégration qui se produit en raison d'une non-concordance de certificat d'approbation lors de la première utilisation (TOFU) après qu'une nouvelle demande de signature de certificat (CSR) a été générée dans l'infrastructure Cisco Prime (principale/secondaire), comment la dépanner et la résoudre.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Infrastructure Cisco Prime
- Haute disponibilité

### Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Prime Infrastructure version 3.5 et ultérieures.

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

Il s'agit des documents de référence qui fournissent des informations sur la haute disponibilité et la génération de certificats dans l'infrastructure Cisco Prime.

Guide de haute disponibilité : https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/admin/guide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide/bk_CiscoPrimeInfrastructure_3_6_AdminGu

Guide de l'administrateur : https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/admin/guide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide/bk_CiscoPrimeInfrastructure_3_6_AdminGu

## Problème

TOFU - Le certificat reçu de l'hôte distant est approuvé lors de la première connexion.

Le certificat TOFU de l'infrastructure principale ou de l'hôte distant auquel prime est connecté peut changer si un nouveau certificat est généré ou si le serveur est à nouveau déployé sur l'hôte VM.

La génération et l'importation d'un nouveau CSR sur le serveur d'infrastructure principal (principal/secondaire) envoie les nouvelles informations de certificat TOFU aux serveurs distants lorsque la connectivité est relancée après un redémarrage du service.

Si l'hôte distant envoie un certificat différent pour une connexion ultérieure après la première connexion, la connexion est rejetée.

L'hôte distant peut être (serveur principal ou secondaire dans le déploiement haute disponibilité, serveur ISE (Integrated Service Engine)) où l'ancienne unité TOFU est toujours présente.

Cela entraîne l'échec de l'enregistrement entre les serveurs principal et secondaire, Prime et ISE.

La section de dépannage décrit les messages d'erreur qui peuvent être trouvés dans les journaux du moniteur d'intégrité dans de tels scénarios.

## Dépannage

Dans le journal du moniteur d'intégrité principal, ces messages d'erreur signalant la non-correspondance dans le certificat secondaire sont trouvés.

<#root>

```
[system] [HealthMonitorThread] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
-
```

**CN=prime-sec**

, OU=Prime Infra, O=Cisco Systems, L=SJ, ST=CA, C=US

<#root>

javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:
Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
-

**CN=prime-sec**

Ces messages d'erreur se trouvent dans les journaux de l'infrastructure principale et signalent la non-correspondance dans le certificat du serveur ISE.

<#root>

[system] [seqtaskexecutor-3069] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
-

**CN=ISE-server**

<#root>

javax.net.ssl.SSLHandshakeException: java.security.cert.
CertificateException: Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
-

**CN=ISE-server**

Dans le journal du moniteur d'intégrité secondaire, ces messages d'erreur signalant la non-correspondance dans le certificat principal sont détectés.

[system] [HealthMonitorThread] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-pri, OU=Prime Infra, O=Cisco Systems, L=SJ, ST=CA, C=US

<#root>

javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:

```
Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
-
```

**CN=prime-pri**

# Solution

Les certificats TOFU actuels sur prime doivent être répertoriés, à partir de là l'ancienne entrée de certificat pour l'hôte distant correspondant doit être identifiée et supprimée avant que vous ne retentez l'intégration à partir de prime.

## Configuration

Afficher la liste de validation des certificats

La commande ncs certvalidation tofu-certs listcerts peut être utilisée pour afficher la liste de validation de certificat.

Ce résultat provient du serveur principal Cisco Prime Infrastructure [IP=1XX.XX.XX.XX] :

<#root>

```
prime-pri/admin#
```

**ncs certvalidation tofu-certs listcerts**

```
Host certificate are automatically added to this list on first connection,
if trust-on-first-use is configured - ncs certvalidation certificate-check ...
```

**host=1X.XX.XX.XX**

```
_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/
```

**CN=prime-pri**

**host=1Z.ZZ.ZZ.ZZ**

```
_443;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra
```

**/CN=ISE-server**

**host=1YY.YY.YY.YY**

```
_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra
```

**/CN=prime-sec**

```
prime-pri/admin#
```

Ce résultat provient du serveur secondaire Cisco Prime Infrastructure [IP=1YY.YY.YY.YY]

<#root>

```
prime-sec/admin#
ncs certvalidation tofu-certs listcerts


Host certificate are automatically added to this list on first connection,
if trust-on-first-use is configured - ncs certvalidation certificate-check ...


host=1YY.YY.YY.YY
_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/
CN=prime-sec

host=127.0.0.1_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-sec

host=1X.XX.XX.XX
_8082; subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/
CN=prime-pri


prime-sec/admin#
```

Supprimer le certificat

Utilisez la commande ncs certvalidation tofu-certs deletecert host <host> afin de supprimer à la validation du certificat.

À partir du serveur principal, vérifiez et supprimez les anciennes entrées des certificats TOFU du serveur ISE et du serveur secondaire, respectivement.

- ncs certvalidation tofu-certs deletecert host 1YY.YY.YY.YY_8082
- ncs certvalidation tofu-certs deletecert host 1Z.ZZ.ZZ.ZZ_443

À partir du serveur secondaire, vérifiez et supprimez les anciennes entrées du certificat tofu du serveur principal à l'aide de la commande ncs certvalidation tofu-certs deletecert host 1X.XX.XX.XX_8082.

Réinitialiser la haute disponibilité du primaire au secondaire

Étape 1. Connectez-vous à Cisco Prime Infrastructure avec un ID utilisateur et un mot de passe disposant de privilèges d'administrateur.

Étape 2. Dans le menu, accédez à Administration > Settings > High Availability. L'infrastructure Cisco Prime affiche la page d'état HA.

Étape 3. Sélectionnez Configuration haute disponibilité, puis renseignez les champs comme suit :

1. Serveur secondaire : Saisissez l'adresse IP ou le nom d'hôte du serveur secondaire.
2. Clé d'authentification : Entrez le mot de passe de clé d'authentification que vous avez défini lors de l'installation du serveur secondaire.
3. Adresse électronique : Saisissez l'adresse (ou la liste d'adresses séparées par des virgules) à laquelle envoyer la notification de changement d'état de haute disponibilité. Si vous avez déjà configuré les notifications par e-mail à l'aide de la page Configuration du serveur de messagerie (voir « Configurer les paramètres du serveur de messagerie »), les adresses e-mail que vous entrez ici seront ajoutées à la liste des adresses déjà configurées pour le serveur de messagerie.
4. Type de basculement : Sélectionnez Manuel ou Automatique. Il est recommandé de sélectionner Manual (Manuel).

Il est recommandé d'utiliser un serveur DNS afin de convertir le nom d'hôte en adresse IP. Si vous utilisez le fichier /etc/hosts au lieu du serveur DNS, vous devez entrer l'adresse IP secondaire au lieu du nom d'hôte.

Étape 4. Si vous utilisez la fonction IP virtuelle, cochez la case Enable Virtual IP, puis renseignez les champs supplémentaires comme suit :

1. IP virtuelle IPV4 : Saisissez l'adresse IPv4 virtuelle que les deux serveurs haute disponibilité doivent utiliser.
2. IP virtuelle IPV6 : (Facultatif) Entrez l'adresse IPv6 que les deux serveurs haute disponibilité doivent utiliser.

L'adressage IP virtuel ne fonctionne que si les deux serveurs se trouvent sur le même sous-réseau. Vous ne devez pas utiliser le bloc d'adresses IPV6 fe80, il a été réservé à l'adressage monodiffusion link-local.

Étape 5. Cliquez sur Check Readiness afin de vous assurer que les paramètres environnementaux liés à la haute disponibilité sont prêts pour la configuration.

Étape 6. Cliquez sur Register afin de visualiser la barre de progression de l'étape, pour vérifier l'achèvement à 100 % de l'enregistrement de pré-HA, la réplication de base de données et l'enregistrement de post-HA comme indiqué ici. L'infrastructure Cisco Prime lance le processus d'enregistrement HA. Une fois l'inscription terminée avec succès, le mode de configuration affiche la valeur de Primary Active.




Reconfigurer les serveurs ISE

Étape 1. Accédez à Administration > Servers > ISE Servers

Étape 2. Accédez à Select a command > Add ISE Server, puis cliquez sur Aller
Étape 3. Entrez l'adresse IP, le nom d'utilisateur et le mot de passe du serveur ISE

Étape 4 : confirmation du mot de passe du serveur ISE

Étape 5. Cliquez sur Save.

## Vérifier

La commande ncs certvalidation tofu-certs listcerts peut être utilisée pour vérifier le nouveau certificat.

## Informations connexes

- Notes de version de Cisco Prime Infrastructure : http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Guide de démarrage rapide de Cisco Prime Infrastructure : http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Guide de référence des commandes de l'infrastructure Cisco Prime : http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Guide de l'utilisateur de Cisco Prime Infrastructure : http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Guide de l'administrateur d'infrastructure Cisco Prime : http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-

infrastructure/products-maintenance-guides-list.html

- Assistance et documentation techniques - Cisco Systems

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.