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

Contenu

Introduction

Ce document décrit le problème d'intégration qui se produit en raison d'une incompatibilité de certificat TOFU (Trust-on-first-use) après qu'une nouvelle demande de signature de certificat (CSR) a été générée dans l'infrastructure Cisco Prime (primaire/secondaire), comment la dépanner et la résoudre.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Infrastructure Cisco Prime
- Haute disponibilité

Components Used

Les informations de ce document sont basées sur Cisco Prime Infrastructure version 3.5 et ultérieure.

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_AdminGuide_chapter_01011.html

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_AdminGuide_chapter_0100.html

Problème

TOFU : le certificat reçu de l'hôte distant est approuvé lors de la première connexion.

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

La génération et l'importation d'une nouvelle 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 toute connexion ultérieure après la première, la connexion sera rejetée.

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

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

La section de dépannage décrit les messages d'erreur qui se trouvent dans les journaux du moniteur d'intégrité dans de tels scénarios.

Dépannage

Dans le journal du moniteur de santé primaire, ces messages d'erreur pointant la non-correspondance dans le certificat secondaire 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-sec, OU=Prime Infra, O=Cisco Systems, L=SJ, ST=CA, C=US
```

```
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 sur les journaux d'infrastructure principaux qui indiquent l'incompatibilité dans le certificat du serveur ISE.

```
[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

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 pointant l'incompatibilité 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


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, de sorte que l'ancienne entrée de certificat pour l'hôte distant correspondant doit être identifiée et supprimée avant de recommencer l'intégration à partir de Prime.

Configuration

Afficher la liste de validation de certificat

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

Ce résultat provient du serveur principal de l'infrastructure Cisco Prime [IP=1XX.XX.XX.XX] :

```
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 de l'infrastructure Cisco Prime [IP=1YY.YY.YY.YY]

```
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.

Àpartir du serveur principal, vérifiez et supprimez les anciennes entrées pour les certificats ISE et TOFU 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

Àpartir du serveur secondaire, vérifiez et supprimez les anciennes entrées pour le 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 principal au secondaire

Étape 1. Connectez-vous à l'infrastructure Cisco Prime 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**. Cisco Prime Infrastructure affiche la page d'état de la haute disponibilité.

Étape 3. Sélectionnez Configuration HA, 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 : Saisissez le mot de passe de clé d'authentification que vous avez défini lors de l'installation du serveur secondaire.
3. Adresse e-mail : Entrez l'adresse (ou la liste d'adresses séparées par des virgules) à laquelle la notification des modifications d'état HA doit être envoyée par courrier. Si vous avez déjà configuré des 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 Manual (Manuelle) ou Automatic (Automatique). Il est recommandé de sélectionner Manual (Manuel).

Il est recommandé d'utiliser le serveur DNS afin de résoudre le nom d'hôte en adresse IP. Si vous

utilisez **/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 fonctionnalité d'IP virtuelle, activez la case à cocher **Activer l'IP virtuelle**, puis renseignez les champs supplémentaires comme suit :

1. IP virtuelle IPV4 : Saisissez l'adresse IPv4 virtuelle que vous souhaitez utiliser par les deux serveurs HA.
2. IP virtuelle IPV6 : (Facultatif) Entrez l'adresse IPv6 que vous souhaitez utiliser par les deux serveurs HA.

L'adressage IP virtuel ne fonctionne pas, sauf 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 de monodiffusion link-local.

Étape 5. Cliquez sur **Vérifier le niveau de préparation** afin de vous assurer que les paramètres environnementaux associés à la HA sont prêts pour la configuration.

Étape 6. Cliquez sur **S'inscrire** afin d'afficher la barre d'état d'avancement de l'étape, pour vérifier que 100 % des inscriptions pré-HA, réplication de base de données et post-HA sont terminées comme indiqué ici. L'infrastructure Cisco Prime lance le processus d'enregistrement de la haute disponibilité. Une fois l'enregistrement terminé, le **mode de configuration** affiche la valeur de Primary Active.

Reconfigurer les serveurs ISE

Étape 1. Accédez à **Administration > Serveurs > Serveurs ISE**

Étape 2. Accédez à **Sélectionner une commande > Ajouter un serveur ISE**, puis cliquez sur **Aller**
Étape 3. Saisissez l'adresse IP, le nom d'utilisateur et le mot de passe du serveur ISE.

Étape 4. Confirmez le mot de passe du serveur ISE.

Étape 5. Click **Save**.

Vérification

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 l'infrastructure Cisco Prime : 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 d'utilisation de l'infrastructure Cisco Prime : http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Guide de l'administrateur de l'infrastructure Cisco Prime : http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **Support et documentation techniques - Cisco Systems**