Étapes de dépannage de ZTD dans la solution de ventilation

Contenu

Introduction

Ce document décrit comment résoudre des problèmes courants lors du déploiement automatique (ZTD) dans une solution de réseau de zone (FAN) comprenant le routeur Connected Grid (CGR) et le directeur de réseau de terrain (FND).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le déploiement ZTD avec CGR.
Il inclut CGR (CGR1120/CGR1240), FND, Tunnel Provisioning Server (TPS), Registration Authority (RA), Certificate Authority (CA), Domain Name Server (DNS) en tant que composants.
FND et Cisco Connected Grid Network Management System (CG-NMS) sont interchangeables car CG-NMS est une version antérieure de FND.

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. If your network is live, make sure that you understand the potential impact of any command.

Étapes de dépannage selon le processus ZTD dans les solutions de VENTILATEUR

Configuration de fabrication des routeurs de zone de travail (FAR)

Tout commence à partir de cette configuration de fabrication. Cette étape est donc essentielle pour un déploiement réussi.

Cette configuration déclenchera les deux premières phases : Le protocole SCEP (Simple Certificate Enrollment Protocol) et le provisionnement de tunnel.

Un test réussi est un FAR déployé avec sa configuration de fabrication et capable de passer par le processus ZTD pour finalement s'enregistrer avec CG-NMS sans aucune intervention.

Les suspects habituels :

- Les informations d'identification entre FAR et CG-NMS ne correspondent pas.
- L'URL de l'agent NMS Connected Grid (CGNA) pour le provisionnement du tunnel est incorrecte (assurez-vous qu'il s'agit de https et non de http).
- DNS (Domain Name Server) mal configuré pour résoudre le nom de domaine complet TPS (FQDN).

Si, au moment du dépannage de ces deux phases, la configuration de fabrication doit être mise à jour, ce processus doit être suivi :

- Bloquer la connectivité FAR avec le périphérique HE (physiquement ou logiquement)
- Restaurer le FAR à sa configuration express
- Appliquer les modifications
- Créer un fichier express-setup-config
- Enregistrer la configuration dans nvram
- Restaurez la connectivité de sorte que le FAR puisse déclencher à nouveau le processus ZTD

Inscription SCEP

L'objectif de cette phase est d'autoriser FAR à recevoir son certificat d'identité de périphérique local (LDevID) de l'infrastructure à clé publique RSA (PKI) et d'obtenir un certificat après autorisation. Cette étape est une condition préalable pour la prochaine étape où FAR a besoin de son certificat pour communiquer avec le TPS et établir son tunnel IPSec avec le HER.

Les composants impliqués sont les suivants : FAR, RA, serveur SCEP, serveur Radius et sa base de données.

Un script TCL (Tool Command Language) appelé tm_ztd_scep.tcl lance automatiquement le processus SCEP et continue d'essayer jusqu'à la réussite de l'inscription.

Étapes	Composants impliqués	Directives de dépannage	Commandes utiles
event manager démarre le script tm_ztd_scep.tcl	LOIN	• Vérifier la configuration du gestionnaire d'événements • Vérifier la configuration des variables d'environnement utilisées par le script	les commandes tcl deb event manager mettent en surbrillance toutes les commandes CLI appliquées par le scri
Résolution FQDN RA	FAR, DNS	• Vérifier la connectivité entre FAR et DNS • Vérifier l'enregistrement DNS pour résoudre ce nom	envoi d'une requête ping au FQDN RA partir du FAR
Le FAR envoie une requête SCEP à l'autorité de certification	LOR, RA	• Vérifier la configuration du profil d'inscription FAR • Vérifier la connectivité entre RA et FAR • Vérifiez la configuration RA. Le serveur PKI doit être UP	debug crypto pki transactions debug crypto provisioning
Autorisation PKI	RA, RADIUS	• Vérifier la connectivité entre RA et le serveur RADIUS • Vérifier la configuration de l'autorisation PKI RA • Vérifier la configuration du serveur Radius	debug crypto pki scep debug crypto pki transactions debug crypto pki server debug crypto provisioning
Émission de certificat FAR	RA, CA émetteur	• Vérifier la connectivité entre RA et CA émettrice	RA: debug crypto pki Si l'autorité de certification émettrice es une autorité de certification IOS, la même commande debug peut également être utilisée

Provisionnement du tunnel

Au moment de cette phase, le FAR communiquera avec le TPS (agissant en tant que proxy au nom de CG-NMS) pour obtenir sa configuration de tunnel à partir de CG-NMS. Cette phase est initiée par le script tcl SCEP une fois l'inscription effectuée en activant le profil CGNA.

Les composants impliqués sont les suivants : FAR, DNS, TPS, CG-NMS.

Étapes	Composants concernés	Directives de dépannage	Commandes utiles
Script TCL pour activer le profil CGNA	LOIN	Vérifiez que le profil approprié est configuré pour la variable d'environnement ZTD_SCEP_CGNA_Profile.	show cgna profile-all pour vérifier que le profil est actif

Le profil CGNA résout TPS FQDN	FAR, DNS	• Vérifier la connectivité entre DNS et FAR • Vérifier l'enregistrement DNS pour résoudre ce nom • Vérifier la configuration du FQDN TPS dans l'URL CGNA	FAR : ping TPS FQDN
Le profil CGNA établit une session HTTPS avec TPS	FAR, TPS	• Vérifier l'exécution du service TPS • Vérifier le fichier de magasin de clés TPS • Vérifier que TPS reçoit des paquets TPS du routeur CGR • Vérifier la configuration du profil CGNA	Le fichier journal TPS se trouve à l'adresse : /opt/cgms-tpsproxy/log/tpsproxy.log
Demande de tunnel de transfert TPS vers CG-NMS	TPS, CG-NMS	• Vérifier les propriétés TPS et CG-NMS • Vérifier la connectivité entre TPS et CG-NMS • Vérifier les journaux TPS et CG-NMS	Le fichier journal FND se trouve à l'adresse : cd /opt/cgms/server/cgms/log

Le FAR contacte TPS avec une demande de provisionnement de tunnel avec HTTPS sur le port 9120

```
4351: iok-tps: Jul 13 2016 14:46:12.328 +0000: %CGMS-6-UNSPECIFIED: %[ch=1c3d5104]
[eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Inbound proxy request from [192.168.1.1] with client certificate subject
[SERIALNUMBER=PID:IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]

4352: iok-tps: Jul 13 2016 14:46:12.382 +0000: %CGMS-6-UNSPECIFIED: %[ch=1c3d5104]
[eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Completed inbound proxy request from [192.168.1.1] with client certificate subject
[SERIALNUMBER=PID:IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]
```

Journaux après que le tunnel est établi entre HER et FAR et Ci-après, FAR peut communiquer directement avec HER

```
4351: iok-tps: Jul 13 2016 14:46:12.328 +0000: %CGMS-6-UNSPECIFIED: %[ch=1c3d5104]
[eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Inbound proxy request from [192.168.1.1] with client certificate subject [SERIALNUMBER=PID:

IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]

4352: iok-tps: Jul 13 2016 14:46:12.382 +0000: %CGMS-6-UNSPECIFIED:
%[ch=1c3d5104][eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Completed inbound proxy request from [192.168.1.1] with client certificate subject [SERIALN
```

```
UMBER=PID:IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]

4353: iok-tps: Jul 13 2016 14:46:12.425 +0000: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyOutboundHandler][ip=192.168.1.1][sev=INFO][tid=qtp687776794-16]:
Outbound proxy request from [192.168.1.2] to [192.168.1.1]

4354: iok-tps: Jul 13 2016 14:46:14.176 +0000: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyOutboundHandler][ip=10.10.10.61][sev=INFO][tid=qtp687776794-16]:
Outbound proxy request from [192.168.1.2] to [192.168.1.1
```

Enregistrement de périphérique

Étape 1. Préparez-vous à l'enregistrement des périphériques

CG-NMS va pousser la configuration du profil CGNA cg-nms-register. Des commandes supplémentaires sont ajoutées afin que le profil soit exécuté immédiatement au lieu d'attendre l'expiration du compteur d'intervalle.

CG-NMS désactivera le profil CGNA cg-nms-tunnel Tunnel provisioning est considéré comme terminé à ce stade.

Étape 2. CG-NMS reçoit une demande d'enregistrement de périphérique

- Vérifier que le FAR est provisionné dans sa base de données
- Vérifiez si les fichiers cg-nms.odm et cg-nms-scripts.tcl sont manquants dans la mémoire flash FAR ou doivent être mis à jour vers une nouvelle version. CG-NMS les téléchargera automatiquement si nécessaire.
- Capturer la configuration actuelle de FAR
- Traiter toutes les sorties de commandes show incluses dans la demande. Demandez les disparus si nécessaire. La liste peut varier en fonction de la configuration du matériel FAR.

Pour plus d'informations sur la mise en oeuvre du déploiement automatique sur votre réseau, contactez votre partenaire Cisco ou votre ingénieur système Cisco.

Pour connaître la configuration express sur le routeur, contactez votre partenaire ou votre ingénieur système Cisco.

Informations connexes

- http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ztdv4_cgr1000.html
- Support et documentation techniques - Cisco Systems