

Pasos de solución de problemas de ZTD en la solución FAN

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Pasos de solución de problemas según el proceso ZTD en las soluciones FAN](#)

[Configuración de fabricación del router de área de campo \(FAR\)](#)

[Inscripción en SCEP](#)

[Aprovisionamiento de túneles](#)

[El FAR se pone en contacto con el TPS con una solicitud de aprovisionamiento de túnel con HTTPS en el puerto 9120](#)

[Registros después de que el túnel está establecido entre ELLA y FAR y después, FAR puede comunicarse directamente con HER](#)

[Registro de dispositivos](#)

[Paso 1. Prepárese para el registro de dispositivos](#)

[Paso 2. CG-NMS recibe una solicitud de registro de dispositivos](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo resolver problemas comunes mientras se implementa sin intervención (ZTD) en una solución de red de área de campo (FAN) que consta de Connected Grid Router (CGR) y Field Network Director (FND).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en la implementación de ZTD con CGR. Incluye CGR (CGR1120/CGR1240), FND, Servidor de aprovisionamiento de túnel (TPS), Autoridad de registro (RA), Autoridad de certificación (CA), Servidor de nombres de dominio (DNS) como componentes. FND y Cisco Connected Grid Network Management System (CG-NMS) son intercambiables, ya que CG-NMS es una versión anterior 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.

Pasos de solución de problemas según el proceso ZTD en las soluciones FAN

Configuración de fabricación del router de área de campo (FAR)

Todo comienza con esta configuración de fabricación, por lo que este paso es clave para una implementación correcta.

Esta configuración activará las dos primeras fases: Protocolo simple de inscripción de certificados (SCEP) y aprovisionamiento de túnel.

Una prueba exitosa es una FAR implementada con su configuración de fabricación y capaz de atravesar el proceso ZTD para finalmente registrarse en CG-NMS sin ninguna intervención.

Sospechosos habituales:

- Las credenciales entre FAR y CG-NMS no coinciden.
- La URL del agente NMS de Connected Grid (CGNA) para el aprovisionamiento de túneles es incorrecta (asegúrese de que es https y no http).
- El servidor de nombres de dominio (DNS) no se ha configurado correctamente para resolver el nombre de dominio completo (FQDN) de TPS.

Si en el momento de resolver el problema de esas dos fases, se debe actualizar la configuración de fabricación, se debe seguir este proceso:

- Bloquear la conectividad FAR con el HE (física o lógicamente)
- Vuelva a colocar el FAR en su express-setup-config
- Aplicar los cambios
- Cree un nuevo archivo express-setup-config
- Guardar la configuración en nvram
- Restaurar la conectividad para que FAR pueda activar de nuevo el proceso ZTD

Inscripción en SCEP

Los objetivos de esta fase son autorizar a FAR a recibir su certificado de identidad de dispositivo local (LDevID) de la Infraestructura de Clave Pública (PKI) de RSA y obtener el certificado después de la autorización. Este paso es un requisito previo para el siguiente, donde FAR necesita su certificado para comunicarse con el TPS y establecer su túnel IPsec con el HER.

Los componentes implicados son: FAR, RA, servidor SCEP, servidor Radius y su base de datos.

Una secuencia de comandos del lenguaje de comandos de herramientas (TCL) llamada tm_ztd_scep.tcl iniciará automáticamente el proceso SCEP y lo seguirá intentando hasta que la inscripción se realice correctamente.

Pasos Componentes Pautas para la resolución de Comandos útiles

	involucrados	problemas	
event manager inicia el script tm_ztd_scep.tcl	LEJOS	<ul style="list-style-type: none"> • Verificar la configuración del administrador de eventos • Verificar la configuración de variables de entorno utilizada por el script • Verifique la conectividad entre FAR y DNS 	los comandos tcl del administrador de eventos deb resaltarán todos los comandos CLI aplicados por el script
Resolución de FQDN de RA	FAR, DNS	<ul style="list-style-type: none"> • Verifique el registro DNS para resolver este nombre • Comprobar la configuración del perfil de inscripción FAR • Verifique la conectividad entre RA y FAR 	ping del FQDN de RA desde el FAR
FAR envía la solicitud SCEP al RA	LEJOS, RA	<ul style="list-style-type: none"> • Verifique la configuración de RA. El servidor PKI debe estar ACTIVO • Verifique la conectividad entre el servidor RA y RADIUS 	debug crypto pki Transactions debug crypto provisioning
Autorización PKI	RA, RADIUS	<ul style="list-style-type: none"> • Verificar la configuración de la autorización PKI de RA • Comprobar la configuración del servidor Radius 	debug crypto pki scep debug crypto pki Transactions debug crypto pki server debug crypto provisioning
emisión de certificado FAR	RA, CA del emisor	<ul style="list-style-type: none"> • Verifique la conectividad entre RA y CA emisor 	RA: debug crypto pki Si la CA del emisor es un IOS-CA, también se puede utilizar el mismo comando debug

Aprovisionamiento de túneles

En el momento de esta fase, el FAR se comunicará con el TPS (actúa como proxy en nombre de CG-NMS) para obtener su configuración de túnel de CG-NMS. Esta fase es iniciada por la secuencia de comandos tcl SCEP una vez que se realiza la inscripción activando el perfil CGNA.

Los componentes involucrados son: FAR, DNS, TPS, CG-NMS.

Pasos	Componentes involucrados	Guías de resolución de problemas	Comandos útiles
script TCL para activar el perfil CGNA CGNA profile	LEJOS FAR, DNS	<p>Verifique que el perfil correcto esté configurado para la variable de entorno ZTD_SCEP_CGNA_Profile</p> <ul style="list-style-type: none"> • Verifique la conectividad entre 	"show cgna profile-all" para verificar que el perfil esté activo LEJOS: ping TPS FQDN

resolver el FQDN de TPS	<p>DNS y FAR</p> <ul style="list-style-type: none"> • Verifique el registro DNS para resolver este nombre • Verifique la configuración del FQDN de TPS en la URL de CGNA • Verificar que el servicio TPS se esté ejecutando 	El archivo de registro de TPS se encuentra en: /opt/cgms-tpsproxy/log/tpsproxy.log
El perfil CGNA establece la sesión HTTPS con TPS	<ul style="list-style-type: none"> • Comprobar archivo de almacén de claves TPS • Verificar TPS recibe paquetes TPS de CGR • Comprobar la configuración del perfil CGNA • Verificar las propiedades TPS y CG-NMS 	El archivo de registro de TPS se encuentra en: /opt/cgms-tpsproxy/log/tpsproxy.log
Solicitud de túnel de reenvío de TPS a CG-NMS	<ul style="list-style-type: none"> • Verifique la conectividad entre TPS y CG-NMS • Verificar registros TPS y CG-NMS 	El archivo de registro FND se encuentra en :cd /opt/cgms/server/cgms/log

El FAR se pone en contacto con el TPS con una solicitud de aprovisionamiento de túnel con HTTPS en el puerto 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]
```

Registros después de que el túnel está establecido entre ELLA y FAR y después, FAR puede comunicarse directamente con 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]

Registro de dispositivos

Paso 1. Prepárese para el registro de dispositivos

CG-NMS impulsará la configuración del perfil CGNA cg-nms-register. Se agregan comandos adicionales para que el perfil se ejecute inmediatamente en lugar de esperar a que caduque el temporizador de intervalo.

CG-NMS desactivará el aprovisionamiento de túnel de túnel cg-nms-tunnel del perfil CGNA que se considera completo en este punto.

Paso 2. CG-NMS recibe una solicitud de registro de dispositivos

- Verifique que FAR esté aprovisionado en su base de datos
- Verifique si los archivos cg-nms.odm y cg-nms-scripts.tcl faltan en la memoria flash FAR o deben actualizarse a una nueva versión. CG-NMS los cargará automáticamente si es necesario.
- Capturar la configuración actual de FAR
- Procese todos los resultados de los comandos show incluidos en la solicitud. Pregunte por los que faltan si es necesario. La lista puede variar en función de la configuración de hardware FAR.

Para obtener más información sobre cómo implementar la implementación sin intervención en su red, póngase en contacto con su partner de Cisco o con el ingeniero de sistemas de Cisco.

Para express-setup-config en el router, póngase en contacto con su partner o el ingeniero de sistemas de Cisco.

Información Relacionada

- http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ztdv4_cgr1000.html
- [Soporte Técnico y Documentación - Cisco Systems](#)