Etapas de solução de problemas para ZTD na solução FAN

Contents

Introduction

Este documento descreve como solucionar problemas comuns enquanto a solução ZTD (Zero Touch Deployment, Implantação Zero Touch Zero) em FAN (Field Area Network, Rede de Área de Campo) consiste em CGR (Connected Grid Router, Roteador de Grade Conectada) e FND (Field Network Diretor, Diretor de Rede de Campo).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas na implantação ZTD com CGR.
Inclui CGR (CGR1120/CGR1240), FND, TPS (Tunnel Provisioning Server), RA (Registration Authority), CA (Certificate Authority), DNS (Domain Name Server) como componentes. O FND e o Cisco Connected Grid Network Management System (CG-NMS) são intercambiáveis porque o CG-NMS é uma versão anterior do 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.

Etapas de solução de problemas de acordo com o processo ZTD em soluções de FAN

Configuração do FAR (Field Area Router, roteador de área de campo)

Tudo começa com essa configuração de fabricação, portanto, essa etapa é essencial para uma implantação bem-sucedida.

Essa configuração acionará as duas primeiras fases: Simple Certificate Enrollment Protocol (SCEP) e provisionamento de túnel.

Um teste bem-sucedido é um FAR implantado com sua configuração de fabricação e capaz de passar pelo processo ZTD para finalmente se registrar no CG-NMS sem qualquer intervenção.

Suspeitos comuns:

- As credenciais entre FAR e CG-NMS não correspondem.
- A URL do Agente NMS da rede conectada (CGNA - Connected Grid NMS Agent) para provisionamento de túnel está incorreta (verifique se é https e não http).
- Servidor de Nomes de Domínio (DNS) configurado incorretamente para resolver o FQDN (Nome de Domínio Totalmente Qualificado) do TPS.

Se no momento da solução de problemas dessas duas fases, a configuração de fabricação precisar ser atualizada, este processo deve ser seguido:

- Bloquear a conectividade FAR com o HE (física ou logicamente)
- Reverta o FAR para sua configuração de configuração expressa
- Aplicar as alterações
- Crie um novo arquivo express-setup-config
- Salvar a configuração na nvram
- Restaure a conectividade para que o FAR possa disparar o processo ZTD novamente

Inscrição no SCEP

Os objetivos desta fase são autorizar o FAR a receber seu certificado de identidade de dispositivo local (LDevID) do PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) RSA e a obter um certificado após a autorização. Esta etapa é um pré-requisito para a próxima, onde o FAR precisa de seu certificado para se comunicar com o TPS e estabelecer seu túnel IPSec com o HER.

Os componentes envolvidos são: FAR, RA, servidor SCEP, servidor Radius e seu DB.

Um script TCL (Tool Command Language) chamado tm_ztd_scep.tcl iniciará automaticamente o processo SCEP e continuará tentando até que a inscrição seja bem-sucedida.

Etapas	Componentes envolvidos	Diretrizes de Troubleshooting	Comandos úteis
o gerenciador de eventos inicia o script tm_ztd_scep.tcl	LONGE	• Verificar a configuração do gerenciador de eventos • Verificar a configuração das variáveis de ambiente usadas pelo script • Verificar a conectividade entre FAR e DNS	os comandos deb event manager tcl destacarão todos os comandos CLI aplicados pelo script
resolução de RA FQDN	LONGE, DNS	• Verifique o registro DNS para resolver esse nome • Verificar a configuração do perfil de inscrição FAR	Faça ping no RA FQDN a partir do FAR
FAR envia solicitação SCEP ao RA	LONGE, RA	• Verificar a conectividade entre RA e FAR • Verifique a configuração do RA. O servidor PKI deve estar UP	debug crypto pki transactions debug crypto provisionamento
autorização de PKI	RA, RADIUS	• Verificar a conectividade entre o servidor RA e RADIUS • Verificar a configuração de autorização de PKI RA • Verificar a configuração do servidor Radius	debug crypto pki scep debug crypto pki transactions debug crypto pki server debug crypto provisionamento
Emissão de certificado FAR	RA, CA do emissor	• Verificar a conectividade entre RA e CA do Emitente	RA: debug crypto pki Se a AC do emitente for um IOS-CA, o mesmo comando de depuração também poderá ser usado

Provisionamento de túnel

No momento dessa fase, o FAR se comunicará com o TPS (atua como proxy em nome do CG-NMS) para obter sua configuração de túnel do CG-NMS. Essa fase é iniciada pelo script tcl do SCEP quando a inscrição é feita ativando o perfil do CGNA.

Os componentes envolvidos são: LONGE, DNS, TPS, CG-NMS.

Etapas	Componentes envolvidos	Guias de solução de problemas	Comandos úteis
Script TCL para ativar o perfil CGNA	LONGE	Verifique se o perfil correto está configurado para a variável de ambiente ZTD_SCEP_CGNA_Profile	"show cgna profile-all" para verificar se o perfil está ativo
perfil CGNA resolver TPS FQDN	LONGE, DNS	• Verificar a conectividade entre DNS e FAR • Verifique o registro	LONGE: ping TPS FQDN

		DNS para resolver esse nome • Verifique a configuração de FQDN do TPS no URL do CGNA • Verificar se o serviço TPS está em execução • Verificar arquivo de armazenamento de chaves TPS • Verificar se o TPS recebe pacotes TPS do CGR • Verificar a configuração do perfil CGNA	
Perfil CGNA estabelece sessão HTTPS com TPS	LONGE, TPS		O arquivo de log do TPS está localizado em: /opt/cgms-tpsproxy/log/tpsproxy.log
Solicitação de túnel de encaminhamento TPS para CG-NMS	TPS, CG-NMS	• Verificar propriedades de TPS e CG-NMS • Verificar a conectividade entre TPS e CG-NMS • Verificar registros TPS e CG-NMS	O arquivo de log do FND está localizado em: cd /opt/cgms/server/cgms/log

O FAR entra em contato com o TPS com uma solicitação de provisionamento de túnel com HTTPS na porta 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 depois que o túnel é estabelecido entre HER e FAR e, a seguir, FAR pode se comunicar diretamente com 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 do dispositivo

Etapa 1. Prepare-se para o registro de dispositivos

O CG-NMS encaminhará a configuração do perfil CGNA cg-nms-register. Comandos adicionais são adicionados para que o perfil seja executado imediatamente, em vez de esperar que o temporizador de intervalo expire.

O CG-NMS desativará o provisionamento de túnel cg-nms-tunnel do perfil do CGNA considerado concluído neste ponto.

Etapa 2. CG-NMS recebe uma solicitação de registro de dispositivo

- Verifique se o FAR está provisionado em seu DB
- Verifique se os arquivos cg-nms.odm e cg-nms-scripts.tcl estão ausentes na flash do FAR ou se devem ser atualizados para uma nova versão. O CG-NMS os carregará automaticamente, se necessário.
- Capturar configuração atual FAR
- Processar todas as saídas dos comandos show incluídas na solicitação. Peça os que estão faltando, se necessário. A lista pode variar com base na configuração de hardware FAR.

Para obter detalhes sobre como implementar a implantação Zero Touch em sua rede, entre em contato com seu parceiro da Cisco ou engenheiro de sistemas da Cisco.

Para configuração expressa no roteador, entre em contato com seu parceiro ou engenheiro de sistema da Cisco.

Informações Relacionadas

- http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ztdv4_cgr1000.html
- Suporte Técnico e Documentação - Cisco Systems