

# Problemas de integração do Prime Infrastructure 3.5+ devido ao certificado TOFU

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Troubleshoot](#)

[Solução](#)

[Configuração](#)

[Exibir lista de validação de certificado](#)

[Excluir certificado](#)

[Reinicializar HA do primário para o secundário](#)

[Reconfigurar servidores ISE](#)

[Verificar](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve o problema de integração que ocorre devido à incompatibilidade de certificado de Confiança na primeira utilização (TOFU) depois que uma nova Solicitação de Assinatura de Certificado (CSR) é gerada na Cisco Prime Infrastructure (primária/secundária), como solucioná-la e resolvê-la.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Infraestrutura Cisco Prime
- Alta Disponibilidade

## Componentes Utilizados

As informações neste documento são baseadas na versão 3.5 e superior do Cisco Prime Infrastructure.

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. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Esses são os documentos de referência que fornecem informações sobre alta disponibilidade e geração de certificados na Cisco Prime Infrastructure.

Guia de alta disponibilidade:

[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](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)

Guia do administrador: [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](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)

## Problema

TOFU - O certificado recebido do host remoto é confiável quando a conexão é feita pela primeira vez.

O certificado TOFU na infraestrutura principal ou o host remoto ao qual o prime está conectado pode ser alterado se um novo certificado for gerado ou se o servidor for implantado novamente no host VM.

Gerar e importar um novo CSR no servidor de infraestrutura principal (principal/secundário) envia as informações do novo certificado TOFU para servidores remotos quando a conectividade é reiniciada após a reinicialização do serviço.

Se o host remoto enviar um certificado diferente para qualquer conexão subsequencial após a primeira, a conexão será rejeitada.

O host remoto pode ser (servidor primário ou secundário na implantação de HA, servidor ISE (Integrated Service Engine, mecanismo de serviço integrado) onde a TOFU antiga ainda está presente.

Isso causa falha de registro entre servidores Primário e Secundário, Prime e ISE.

A seção de solução de problemas descreve as mensagens de erro que podem ser encontradas nos registros do monitor de integridade nesses cenários.

## Troubleshoot

No registro do monitor de integridade principal, essas mensagens de erro apontando a incompatibilidade no certificado secundário podem ser encontradas.

```
[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
```

Essas mensagens de erro podem ser encontradas nos logs de infraestrutura principal indicando a incompatibilidade no certificado do servidor 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
```

No log do monitor de integridade secundário, essas mensagens de erro indicando a incompatibilidade no certificado principal podem ser encontradas.

```
[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
```

## Solução

Os certificados TOFU atuais no prime precisam ser listados, a partir do qual a entrada de certificado antigo para o host remoto correspondente deve ser identificada e removida antes de tentar a integração do prime novamente.

## Configuração

### Exibir lista de validação de certificado

O comando **ncs certvalidation tofu-certs listcerts** pode ser usado para exibir a lista de validação do certificado.

Esta saída é do servidor principal do Cisco Prime Infrastructure [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#
```

Esta saída é do servidor secundário do Cisco Prime Infrastructure [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#
```

## Excluir certificado

Use o comando **ncs certvalidation tofu-certs deletecert host <host>** para excluir a validação do certificado.

A partir do servidor principal, verifique e exclua as entradas antigas para certificados TOFU do ISE e do servidor secundário, respectivamente.

- **ncs certvalidation tofu-certs deletecert host 1YY.YY.YY.YY\_8082**
- **ncs certvalidation tofu-certs deletecert host 1Z.ZZ.ZZ.ZZ\_443**

A partir do servidor secundário, verifique e exclua as entradas antigas do certificado tofu do servidor primário com o uso do comando **ncs certvalidation tofu-certs deletecert host 1X.XX.XX.XX\_8082**.

## Reinicializar HA do primário para o secundário

Etapa 1. Faça login na Cisco Prime Infrastructure com uma ID de usuário e senha que tenham privilégios de administrador.

Etapa 2. No menu, navegue para **Administration > Settings > High Availability (Administração > Configurações > Alta disponibilidade)**. O Cisco Prime Infrastructure exibe a página de status do HA.

Etapa 3. Selecione HA Configuration (Configuração de HA) e preencha os campos da seguinte maneira:

1. Servidor secundário: Insira o endereço IP ou o nome do host do servidor secundário.
2. Chave de autenticação: Insira a senha da chave de autenticação definida durante a instalação do servidor secundário.
3. Endereço de e-mail: Insira o endereço (ou lista de endereços separada por vírgulas) para o qual a notificação sobre alterações de estado HA deve ser enviada por e-mail. Se você já configurou notificações por e-mail usando a página de Configuração do Servidor de e-mail (consulte "Definir configurações do Servidor de e-mail"), os endereços de e-mail digitados aqui serão anexados à lista de endereços já configurados para o servidor de e-mail.
4. Tipo de failover: Selecione Manual ou Automático. É recomendável selecionar Manual.

Recomenda-se usar o servidor DNS para resolver o nome do host para um endereço IP. Se você usar **/etc/hosts** em vez do servidor DNS, insira o endereço IP secundário em vez do nome do host.

Etapa 4. Se você usar o recurso IP virtual, marque a caixa de seleção **Enable Virtual IP** e preencha os campos adicionais da seguinte maneira:

1. IP virtual IPV4: Insira o endereço IPv4 virtual que deseja que os dois servidores HA usem.
2. IP virtual IPV6: (Opcional) Insira o endereço IPv6 que deseja que os dois servidores HA usem.

O endereçamento IP virtual não funcionará a menos que ambos os servidores estejam na mesma sub-rede. Você não deve usar o bloco de endereços IPV6 fe80, ele foi reservado para o endereçamento unicast link local.

Etapa 5. Clique em **Verificar prontidão** para garantir se os parâmetros ambientais relacionados ao HA estão prontos para a configuração.

Etapa 6. Clique em **Register** para visualizar a barra de progresso do Marco, para verificar a conclusão de 100% do Pre-HA Registration, Database Replication e Post HA Registration conforme mostrado aqui. O Cisco Prime Infrastructure inicia o processo de registro de HA. Quando o registro for concluído com êxito, o **Modo de configuração** exibirá o valor de Principal ativo.



## Reconfigurar servidores ISE

Etapa 1. Navegue até **Administração > Servidores > Servidores ISE**

Etapa 2. Navegue até **Select a command > Add ISE Server** e clique em **Ir**

Etapa 3. Insira o endereço IP, o nome de usuário e a senha do servidor ISE

Etapa 4. Confirme a senha do servidor ISE.

Etapa 5. Click **Save**.

## Verificar

O comando `ncs certvalidation tofu-certs listcerts` pode ser usado para verificar o novo certificado.

## Informações Relacionadas

- Notas de versão do Cisco Prime Infrastructure: <http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html>
- Guia de início rápido do Cisco Prime Infrastructure: <http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html>
- Guia de referência de comando do Cisco Prime Infrastructure: <http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html>
- Guia do usuário do Cisco Prime Infrastructure: <http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html>
- Guia do administrador do Cisco Prime Infrastructure: <http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html>
- [Suporte Técnico e Documentação - Cisco Systems](#)