Prime基础设施3.5+集成问题，因为STOW证书

目录

简介

本文档介绍在Cisco Prime基础设施（主/辅助）中生成新的证书签名请求(CSR)后，由于首次使用时信任(STOW)证书不匹配而导致的集成问题，以及如何进行故障排除和解决此问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Prime基础设施
- 高可用性

使用的组件

本文档中的信息基于Cisco Prime基础设施3.5版及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

这些参考文档提供有关Cisco Prime基础设施中高可用性和证书生成的信息。

高可用性指南：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

管理员指南：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

问题

STOW — 首次建立连接时，从远程主机收到的证书是可信的。

如果生成新证书或服务器在VM主机上再次部署，则prime基础设施或prime所连接的远程主机上的STO证书可能会更改。

在主基础设施服务器（主/辅助）上生成和导入新CSR时，当服务重新启动后重新启动连接时，会将新STO证书信息发送到远程服务器。

如果远程主机在第一个子序列连接之后为任何子序列连接发送不同的证书，该连接将被拒绝。

远程主机可以是(HA部署中的主服务器或辅助服务器，集成服务引擎(ISE)服务器)，旧STO仍然存在。

这会导致主服务器和辅助服务器、Prime和ISE服务器之间的注册失败。

故障排除部分介绍在此类情况下的运行状况监控器日志中可以找到的错误消息。

故障排除

在主运行状况监控器日志中，可以找到指示辅助证书不匹配的错误消息。

```
[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
```

这些错误消息可在指示ISE服务器证书不匹配的主要基础设施日志中找到。

```
[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
```

在辅助运行状况监控器日志中，可以找到这些错误消息，指示主证书不匹配。

```
[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
```

解决方案

需要列出prime上的当前STOW证书，因为在您再次尝试从prime集成之前，应识别并删除相应远程主机的旧证书条目。

配置

查看证书验证列表

命令ncs certvalidation botu-certs listcerts可用于查看证书验证列表。

此输出来自Cisco Prime基础设施主服务器[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#
```

此输出来自Cisco Prime基础设施辅助服务器[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#
```

删除证书

使用命令ncs certvalidation boto-certs deletecert host <host>以删除证书验证。

从主服务器检查并分别删除ISE和辅助服务器的STO证书的旧条目。

- **ncs certvalidation botu-certs deletecert host** 1YY.YY.YY.YY_8082
- **ncs certvalidation botu-certs deletecert host** 1Z.ZZ.ZZ.ZZ_443

使用命令ncs certvalidation boto-certs deletecert host 1X.XX.XX.XX_8082，从辅助服务器检查并删除主服务器**豆腐证书的旧**条目。

从主HA重新初始化到辅助HA

步骤1.使用具有管理员权限的用户ID和密码登录Cisco Prime基础设施。

步骤2.从菜单导航至Administration > Settings > High Availability。Cisco Prime基础设施显示HA状态页面。

步骤3.选择HA Configuration，然后填写以下字段：

1. 辅助服务器:输入辅助服务器的IP地址或主机名。
2. 验证密钥:输入在辅助服务器安装期间设置的身份验证密钥密码。
3. 电子邮件地址：输入应将有关HA状态更改的通知邮寄到的地址（或逗号分隔的地址列表）。如果您已使用邮件服务器配置页面（请参阅“配置邮件服务器设置”）配置邮件通知，则在此处输入的邮件地址将附加到已为邮件服务器配置的地址列表。
4. 故障转移类型：选择手动或自动。建议您选择手动。

建议使用DNS服务器将主机名解析为IP地址。如果使用**/etc/hosts文**件而不是DNS服务器，则应输入辅助IP地址而不是主机名。

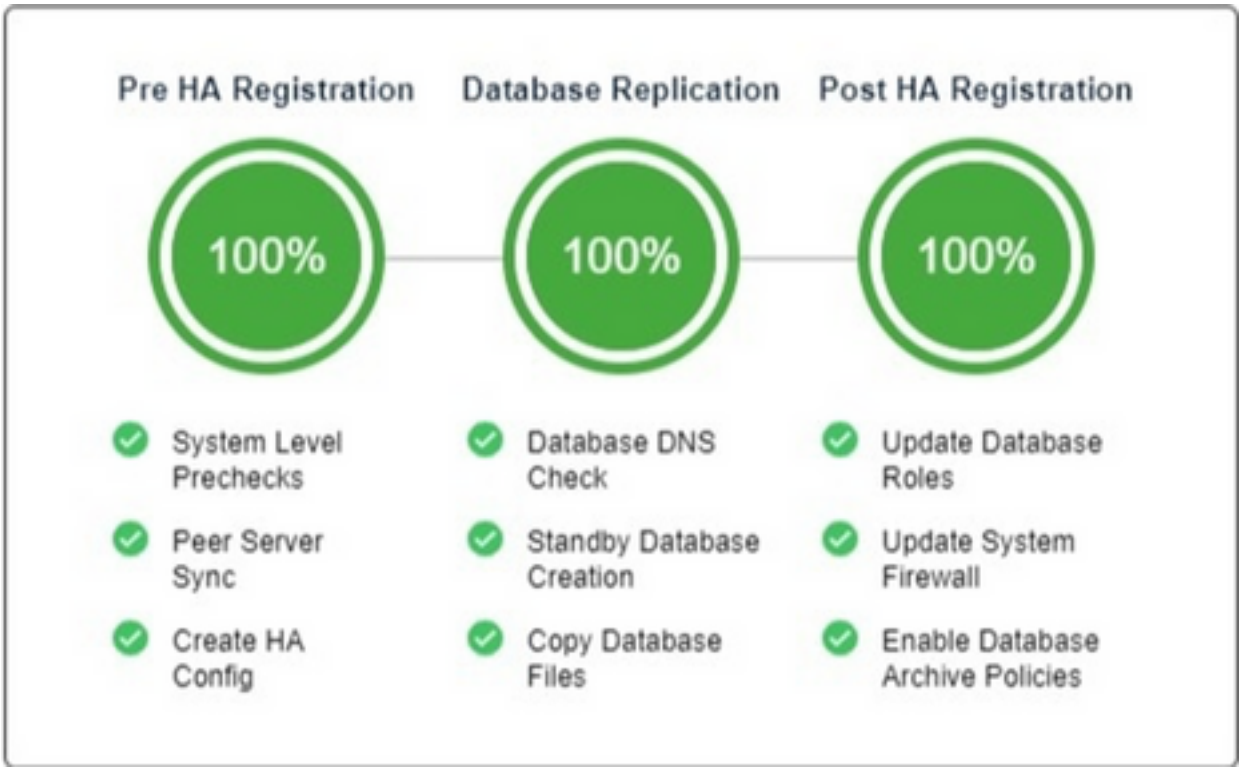
步骤4.如果使用虚拟IP功能，请选中“启用虚拟IP”复选框，然后按如**下方式填**写其他字段：

1. IPV4虚拟IP:输入希望两个HA服务器使用的虚拟IPv4地址。
2. IPV6虚拟IP:（可选）输入您希望两个HA服务器都使用的IPv6地址。

虚拟IP编址将无法工作，除非两台服务器位于同一子网。您不应使用IPV6地址块fe80，它已保留用于本地链路单播寻址。

步骤5.单击**Check Readiness**，以确保HA相关环境参数是否已准备好进行配置。

步骤6.单击**Register**以查看里程碑进度栏，以检查100%完成的Pre-HA Registration、Database Replication和Post HA Registration，如图所示。Cisco Prime基础设施启动HA注册流程。成功完成注册后，**配置模**式将显示主活动的值。



重新配置ISE服务器

步骤1.导航至**Administration > Servers > ISE Servers**

步骤2.导航至**选择命令>添加ISE服**务器，然后单击 **去**
步骤3.输入ISE服务器的IP地址、用户名和密码

步骤4.确认ISE服务器密码。

步骤5.单击**Save**。

验证

命令ncs **certvalidation boto-certs listcerts**可用于验证新证书。

相关信息

- Cisco Prime基础设施版本说明：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Cisco Prime基础设施快速入门指南：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Cisco Prime基础设施命令参考指南： http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Cisco Prime基础设施用户指南：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Cisco Prime基础设施管理员指南：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **技术支持和文档 - Cisco Systems**