Prime Infrastructure 3.5+ Integration Issues due to TOFU Certificate

Contents

Introduction

This document describes the integration issue that occurs due to Trust-on-first-use (TOFU) certificate mismatch after a new Certificate Signing Request (CSR) is generated in Cisco Prime Infrastructure (primary/secondary), how to troubleshoot and resolve it.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Prime Infrastructure
- High Availability

Components Used

The information in this document is based on Cisco Prime Infrastructure version 3.5 and above.

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, ensure that you understand the potential impact of any command.

Background Information

These are the reference documents that provide information on High Availability and certificate generation in Cisco Prime Infrastructure.

High Availability Guide: 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

Administrator Guide: 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

Problem

TOFU - The certificate received from the remote host is trusted when the connection is made for the first time.

TOFU certificate on prime infrastructure or the remote host that prime is connected to can change if a new certificate is generated or if the server is deployed again on VM host.

Generating and importing a new CSR on prime infrastructure server (primary/secondary) sends the new TOFU certificate information to remote servers when the connectivity is re-initiated after a service restart.

If the remote host sends a different certificate for any sub-sequent connection after the first, the connection will be rejected.

Remote host could be (Primary or Secondary server in HA deployment, Integrated Service Engine (ISE) server) where the old TOFU is still present.

This causes registration failure between Primary and Secondary servers, Prime and ISE server.

The troubleshoot section describes the error messages that can be found in the health monitor logs in such scenarios.

Troubleshoot

In Primary health monitor log, these error messages pointing the mismatch in the secondary certificate can be found.

```
[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
```

These error messages can be found on the prime infrastructure logs pointing the mismatch in ISE server certificate.

```
[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
```

In Secondary health monitor log, these error messages pointing the mismatch in the primary certificate can be found.

```
[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
```

Solution

The current TOFU certificates on prime needs to be listed, from that the old certificate entry for the corresponding remote host should be identified and removed before you attempt the integration from prime again.

Configuration

View Certificate Validation List

The command **ncs certvalidation tofu-certs listcerts** can be used to view the certificate validation list.

This output is from the Cisco Prime Infrastructure primary server [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#
```

This output is from the Cisco Prime Infrastructure secondary server [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#
```

Delete Certificate

Use command **ncs certvalidation tofu-certs deletecert host <host>** in order to delete to certificate validation.

From primary server check and delete the old entries for ISE and secondary server's TOFU certificates respectively.

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

From secondary server check and delete the old entries for primary server's tofu certificate with the use of command **ncs certvalidation tofu-certs deletecert host** 1X.XX.XX.XX_8082.

Re-initialize HA from Primary to Secondary

Step 1. Log in to Cisco Prime Infrastructure with a user ID and password that has administrator privileges.

Step 2. From the menu, navigate to **Administration > Settings > High Availability**. Cisco Prime Infrastructure displays the HA status page.

Step 3. Select HA Configuration and then complete the fields as follows:

1. Secondary Server: Enter the IP address or the host name of the secondary server.
2. Authentication Key: Enter the authentication key password you set during the secondary server installation.
3. Email Address: Enter the address (or comma-separated list of addresses) to which notification about HA state changes should be mailed. If you have already configured email notifications using the Mail Server Configuration page (see “Configure Email Server Settings”), the email addresses you enter here will be appended to the list of addresses already configured for the mail server.
4. Failover Type: Select either Manual or Automatic. It is recommended that you select Manual.

It is recommended to use DNS server in order to resolve the host name to an IP address. If you use **/etc/hosts** file instead of DNS server, you should enter the secondary IP address instead of the host name.

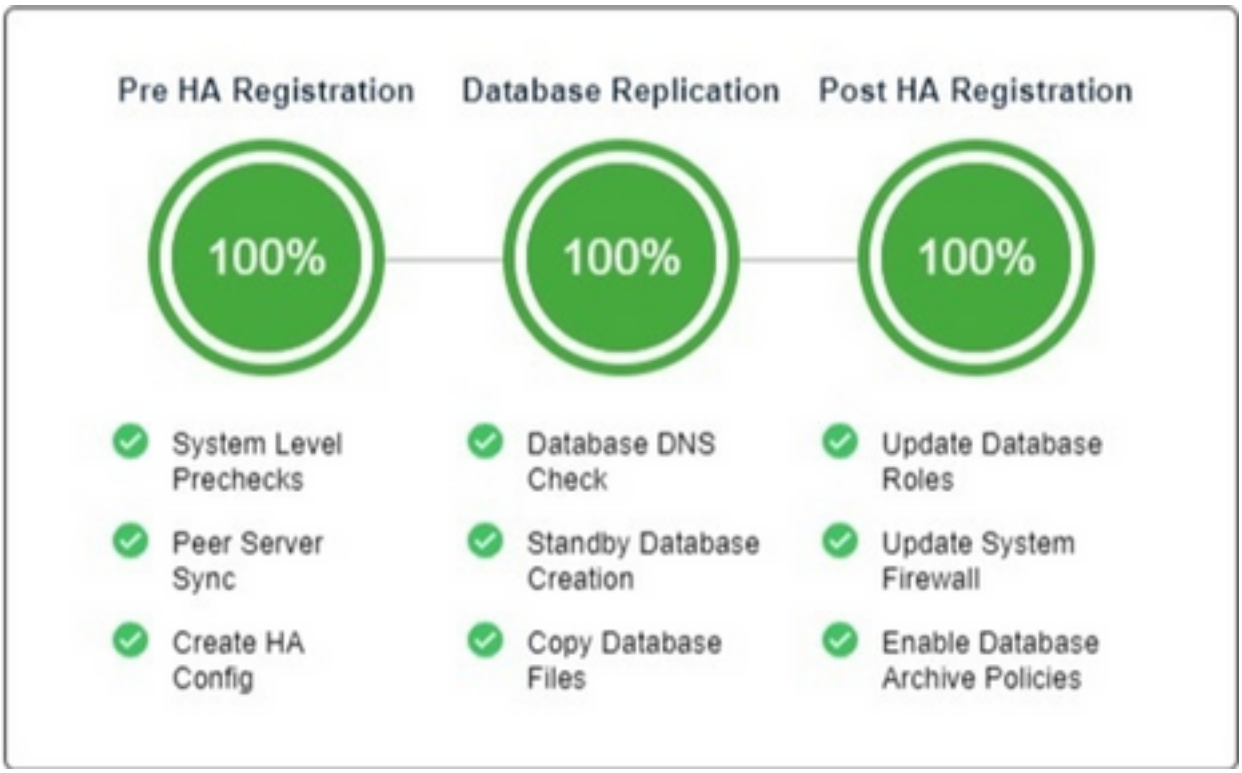
Step 4. If you use the virtual IP feature, select the **Enable Virtual IP** checkbox, then complete the additional fields as follows:

1. IPV4 Virtual IP: Enter the virtual IPv4 address you want both HA servers to use.
2. IPV6 Virtual IP: (Optional) Enter the IPv6 address you want both HA servers to use.

Virtual IP addressing will not work unless both the servers are on the same subnet. You should not use IPV6 address block fe80, it has been reserved for link-local unicast addressing.

Step 5. Click **Check Readiness** in order to ensure if the HA related environmental parameters are ready for the configuration.

Step 6. Click **Register** in order to view the Milestone progress bar, to check the 100% completion of Pre-HA Registration, Database Replication and Post HA Registration as shown here. Cisco Prime Infrastructure initiates the HA registration process. When registration completes successfully, the **Configuration Mode** will display the value of Primary Active.



Re-configure ISE Servers

Step 1. Navigate to **Administration > Servers > ISE Servers**

Step 2. Navigate to **Select a command > Add ISE Server**, then click **Go**
Step 3. Enter the ISE server's IP address, user name, and password

Step 4. Confirm the ISE server password.

Step 5. Click **Save**.

Verify

The command **ncs certvalidation tofu-certs listcerts** can be used to verify the new certificate.

Related Information

- Cisco Prime Infrastructure Release Notes: http://www.cisco.com/c/en/us/support/cloud-

systems-management/prime-infrastructure/products-release-notes-list.html

- Cisco Prime Infrastructure Quick Start Guide: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Cisco Prime Infrastructure Command Reference Guide: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Cisco Prime Infrastructure User Guide: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Cisco Prime Infrastructure Administrator Guide: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **Technical Support & Documentation - Cisco Systems**