Prime-infrastructuur 3.5+ integratieproblemen veroorzaakt door het TOFU-certificaat

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[Probleem](#)
[Problemen oplossen](#)
[Oplossing](#)
[Configuratie](#)
[Certificaatvalideringslijst bekijken](#)
[Certificaat verwijderen](#)
[Herinitialiseren HA van primair tot secundair](#)
[ISE-servers opnieuw configureren](#)
[Verifiëren](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de integratiekwestie die zich voordoet vanwege de mismatch van het Truston-first-use (TOFU)-certificaat nadat een nieuw CSR-verzoek (certificaataanvraag) is gegenereerd in Cisco Prime-infrastructuur (primair/secundair), hoe u de oplossing kunt oplossen en oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Prime-infrastructuur
- Hoge beschikbaarheid

Gebruikte componenten

De informatie in dit document is gebaseerd op versie 3.5 en hoger van Cisco Prime-infrastructuur.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Dit zijn de referentiedocumenten die informatie over hoge beschikbaarheid en het genereren van certificaten in Cisco Prime-infrastructuur bieden.

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

Probleem

TOFU - Het certificaat dat van de afstandsbediening wordt ontvangen, is betrouwbaar wanneer de verbinding voor het eerst wordt gemaakt.

Het TOFU-certificaat op primaire infrastructuur of de externe host waarop de Prime is aangesloten, kan veranderen indien een nieuw certificaat wordt gegenereerd of indien de server opnieuw op VM-host wordt ingezet.

Het genereren en importeren van een nieuwe CSR op een primaire/secundaire server van de infrastructuur verstuurt de nieuwe TOFU certificaatinformatie naar externe servers wanneer de connectiviteit na een servicestart opnieuw wordt gestart.

Als de afstandsbediening een ander certificaat verstuurt voor elke volgende verbinding na de eerste, wordt de verbinding verworpen.

Afstandshost kan zijn (Primaire of Secundaire server in HA-implementatie, Integrated Service Engine (ISE) server) waar de oude TOFU nog aanwezig is.

Dit veroorzaakt een falende registratie tussen primaire en secundaire servers, Prime- en ISE-server.

In het gedeelte Problemen oplossen worden de foutmeldingen beschreven die in de logbestanden van de gezondheidsmonitor in dergelijke scenario's kunnen worden gevonden.

Problemen oplossen

In het logboek van de primaire gezondheidsmonitor, kunnen deze foutmeldingen die op de mismatch in het secundaire certificaat wijzen, worden gevonden.

```
[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
```

Deze foutmeldingen kunnen worden gevonden in de primaire infrastructuuraanslagen waarin de fout in het ISE-servercertificaat wordt aangegeven.

```
[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 het logboek van de secundaire gezondheidsmonitor kunnen deze foutmeldingen die wijzen op de mismatch in het primaire certificaat worden gevonden.

```
[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
```

Oplossing

De huidige TOFU-certificaten op priemgetallen moeten worden vermeld, van waaruit blijkt dat de oude certificaatvermelding voor de corresponderende externe host moet worden geïdentificeerd en verwijderd voordat u opnieuw probeert de integratie uit priemgetallen te laten plaatsvinden.

Configuratie

Certificaatvalideringslijst bekijken

De commando **ncs certvalidatie tofu-certs lijsten** kunnen worden gebruikt om de certificatie lijst te bekijken.

Deze output komt van de primaire server van Cisco Prime Infrastructuur [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#
```

Deze uitvoer komt van de secundaire server van de Cisco Prime Infrastructuur [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#
```

Certificaat verwijderen

Gebruik commando **ncs certvalidatie tofu-certs Deletecert host <host>** om te verwijderen naar certificatie.

Vanaf primaire server controle en verwijder de oude ingangen voor de certificaten van ISE en secundaire server TOFU.

- **NCS certvalidatie tofu-certs Deletecert host** 1YY.YY.YY.YY_8082
- **NCS certvalidatie tofu-certs Deletecert host** 1Z.ZZ.ZZ.ZZ_443

Vanaf secondaire server controleer en verwijder de oude waarden voor tofu certificaat van primaire server met het gebruik van commando **ncs certvalidatie tofu-certs deletecert host** 1X.XX.XX.XX_8082.

Herinitialiseren HA van primair tot secundair

Stap 1. Meld u aan bij Cisco Prime-infrastructuur met een gebruikers-id en een wachtwoord dat beheerrechten heeft.

Stap 2. Ga in het menu naar **Administratie > Instellingen > Hoge beschikbaarheid**. Cisco Prime-infrastructuur geeft de statuspagina van het bestand weer.

Stap 3. Selecteer HA Configuration en vul de velden als volgt in:

1. Secundaire server: Voer het IP-adres of de hostnaam van de secundaire server in.
2. Verificatiesleutel: Voer het wachtwoord in van de verificatiesleutel dat u tijdens de installatie van de secundaire server hebt ingesteld.
3. E-mailadres: Voer het adres in (of komma-gescheiden lijst van adressen) waarop het bericht over de verandering van de staat van de HA moet worden gemaild. Als u al e-mailberichten hebt ingesteld met behulp van de pagina Mail Server Configuration (zie "Instellingen e-mailserver configureren"), worden de e-mailadressen die u hier invoert toegevoegd aan de lijst met adressen die al zijn ingesteld voor de mailserver.
4. Type failover: Selecteer Handmatig of Automatisch. Aanbevolen wordt om Handmatig te selecteren.

Het wordt aanbevolen om DNS-server te gebruiken om de hostnaam op te lossen aan een IP-

adres. Als u een bestand gebruikt/etc/hosts in plaats van een DNS-server, moet u het secundaire IP-adres invoeren in plaats van de naam van de host.

Stap 4. Als u de virtuele IP-functie gebruikt, selecteert u het selectieteken **Virtuele IP** inschakelen en vult u de extra velden als volgt in:

1. IPV4 virtuele IP: Voer het virtuele IPv4-adres in dat u beide HA-servers wilt gebruiken.
2. IPV6 virtuele IP: (Optioneel) Voer het IPv6-adres in dat u beide HA-servers wilt gebruiken.

Virtuele IP-adressering werkt niet tenzij beide servers op hetzelfde subtype zijn. U dient geen IPV6-adresblok FE80 te gebruiken, het is gereserveerd voor link-lokale unicast-adressering.

Stap 5. Klik op **Controleer** of de met HA samenhangende milieuparameters klaar zijn voor de configuratie.

Stap 6. Klik op **Registreer** om de voortgangsbalk van de mijlpaal te bekijken, om de voltooiing van 100% van Pre-HA Registratie, Databaseverdeling en Post HA Registratie te controleren zoals hier weergegeven. Cisco Prime-infrastructuur start het registratieproces voor AH. Wanneer de registratie met succes is voltooid, wordt in de **Configuration Mode** de waarde van Primair Actief weergegeven.

ISE-servers opnieuw configureren

Stap 1. Navigeer naar **Administratie > servers > ISE-servers**

Stap 2. Navigeer om **een opdracht > Add ISE Server** te **selecteren** en klik vervolgens op **Ga**
Stap 3. Voer het IP-adres, de gebruikersnaam en het wachtwoord van de ISE-server in

Stap 4. Bevestig het ISE-serverwachtwoord.

Stap 5. Klik op **Opslaan**.

Verifiëren

De opdracht **ncs certvalidatie tofu-certs lijsten** kunnen worden gebruikt om het nieuwe certificaat te controleren.

Gerelateerde informatie

- Opmerkingen bij Cisco Prime-infrastructuur release: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Cisco Prime-gids voor infrastructuur en snelle start: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Referentiegids voor Cisco Prime-infrastructuur: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Gebruikershandleiding Cisco Prime-infrastructuur: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Cisco Prime-infrastructuurbeheerdershandleiding: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **Technische ondersteuning en documentatie – Cisco Systems**