Probleme bei der Prime-Infrastruktur 3.5+-Integration aufgrund des TOFU-Zertifikats

Inhalt

Einführung

In diesem Dokument wird das Integrationsproblem beschrieben, das aufgrund einer nicht übereinstimmenden Trust-on-First-Use (TOFU)-Zertifikatsanforderung auftritt, nachdem eine neue CSR-Anfrage (Certificate Signing Request) in der Cisco Prime-Infrastruktur (primär/sekundär) generiert wurde. Außerdem wird beschrieben, wie Fehler behoben und behoben werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Prime-Infrastruktur
- Hohe Verfügbarkeit

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Prime Infrastructure Version 3.5 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Dies sind die Referenzdokumente, die Informationen über Hochverfügbarkeit und Zertifikatsgenerierung in der Cisco Prime-Infrastruktur bereitstellen.

Leitfaden zur Hochverfügbarkeit: 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

Administratoranleitung: 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 - Das Zertifikat, das vom Remotehost empfangen wird, wird als vertrauenswürdig angesehen, wenn die Verbindung zum ersten Mal hergestellt wird.

Das TOFU-Zertifikat für die primäre Infrastruktur oder den Remote-Host, mit dem Prime verbunden ist, kann sich ändern, wenn ein neues Zertifikat generiert wird oder wenn der Server erneut auf dem VM-Host bereitgestellt wird.

Beim Generieren und Importieren eines neuen CSR auf primärem Infrastruktur-Server (primär/sekundär) werden die neuen TOFU-Zertifikatsinformationen an Remote-Server gesendet, wenn die Verbindung nach einem Neustart des Services wieder initiiert wird.

Wenn der Remotehost nach der ersten Verbindung ein anderes Zertifikat für eine untergeordnete Verbindung sendet, wird die Verbindung abgelehnt.

Der Remote-Host kann (primärer oder sekundärer Server in HA-Bereitstellung, Integrated Service Engine (ISE)-Server) sein, auf dem die alte TOFU noch vorhanden ist.

Dies führt zu einem Registrierungsfehler zwischen primären und sekundären Servern, dem Prime-Server und dem ISE-Server.

Im Abschnitt "Fehlerbehebung" werden die Fehlermeldungen beschrieben, die in den Systemüberwachungsprotokollen in solchen Szenarien enthalten sind.

Fehlerbehebung

Im primären Gesundheitsüberwachungsprotokoll finden Sie diese Fehlermeldungen, die auf die Diskrepanz im sekundären Zertifikat hinweisen.

```
[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
```

Diese Fehlermeldungen finden Sie in den primären Infrastrukturprotokollen, die auf die Diskrepanz im ISE-Serverzertifikat hinweisen.

```
[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
```

Im sekundären Systemüberwachungsprotokoll finden Sie diese Fehlermeldungen, die auf die Diskrepanz im primären Zertifikat hinweisen.

```
[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
```

Lösung

Die aktuellen TOFU-Zertifikate für Prime müssen aufgelistet werden, aus denen hervorgeht, dass der alte Zertifikatseintrag für den entsprechenden Remotehost identifiziert und entfernt werden muss, bevor Sie erneut versuchen, die Integration vom Prime zu starten.

Konfiguration

Zertifikatsvalidierungsliste anzeigen

Mit dem Befehl **ncs certvalidation tofu-certs listcerts** können Sie die Liste der Zertifikatsvalidierungen anzeigen.

Diese Ausgabe stammt vom primären Cisco Prime Infrastructure-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#
```

Diese Ausgabe stammt vom sekundären Cisco Prime Infrastructure-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#
```

Zertifikat löschen

Verwenden Sie den Befehl **ncs certvalidation tofu-certs deletecert host <host>,** um zur Zertifikatsvalidierung zu löschen.

Überprüfen und löschen Sie vom primären Server die alten Einträge für die TOFU-Zertifikate der ISE und der sekundären Server.

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

Vom sekundären Server überprüfen und löschen Sie die alten Einträge für das Tofu-Zertifikat des primären Servers mit dem Befehl **ncs certvalidierung tofu-certs deletecert host** 1X.XX.XX.XX_8082.

Erneute Initialisierung von HA von Primär zu Sekundär

Schritt 1: Melden Sie sich mit einer Benutzer-ID und einem Kennwort mit Administratorrechten bei der Cisco Prime-Infrastruktur an.

Schritt 2: Navigieren Sie im Menü zu **Administration > Settings > High Availability**. Die Cisco Prime-Infrastruktur zeigt die Seite für den HA-Status an.

Schritt 3: Wählen Sie HA-Konfiguration aus, und füllen Sie die Felder wie folgt aus:

1. Sekundärer Server: Geben Sie die IP-Adresse oder den Hostnamen des Sekundärservers ein.
2. Authentifizierungsschlüssel: Geben Sie das Authentifizierungsschlüsselkennwort ein, das Sie bei der Installation des Sekundärservers festgelegt haben.
3. E-Mail-Adresse: Geben Sie die Adresse (oder eine kommagetrennte Adressenliste) ein, an die Benachrichtigungen über HA-Zustandsänderungen gesendet werden sollen. Wenn Sie E-Mail-Benachrichtigungen bereits über die Konfigurationsseite des Mail-Servers konfiguriert haben (siehe "Konfigurieren der E-Mail-Servereinstellungen"), werden die hier eingegebenen E-Mail-Adressen an die Liste der Adressen angehängt, die bereits für den Mail-Server konfiguriert wurden.

4. Failover-Typ: Wählen Sie Manuell oder Automatisch aus. Es wird empfohlen, Manual (Manuell) auszuwählen.

Es wird empfohlen, den DNS-Server zu verwenden, um den Hostnamen in eine IP-Adresse aufzulösen. Wenn Sie anstelle des DNS-Servers eine **/etc/hosts**-Datei verwenden, sollten Sie statt des Hostnamens die sekundäre IP-Adresse eingeben.

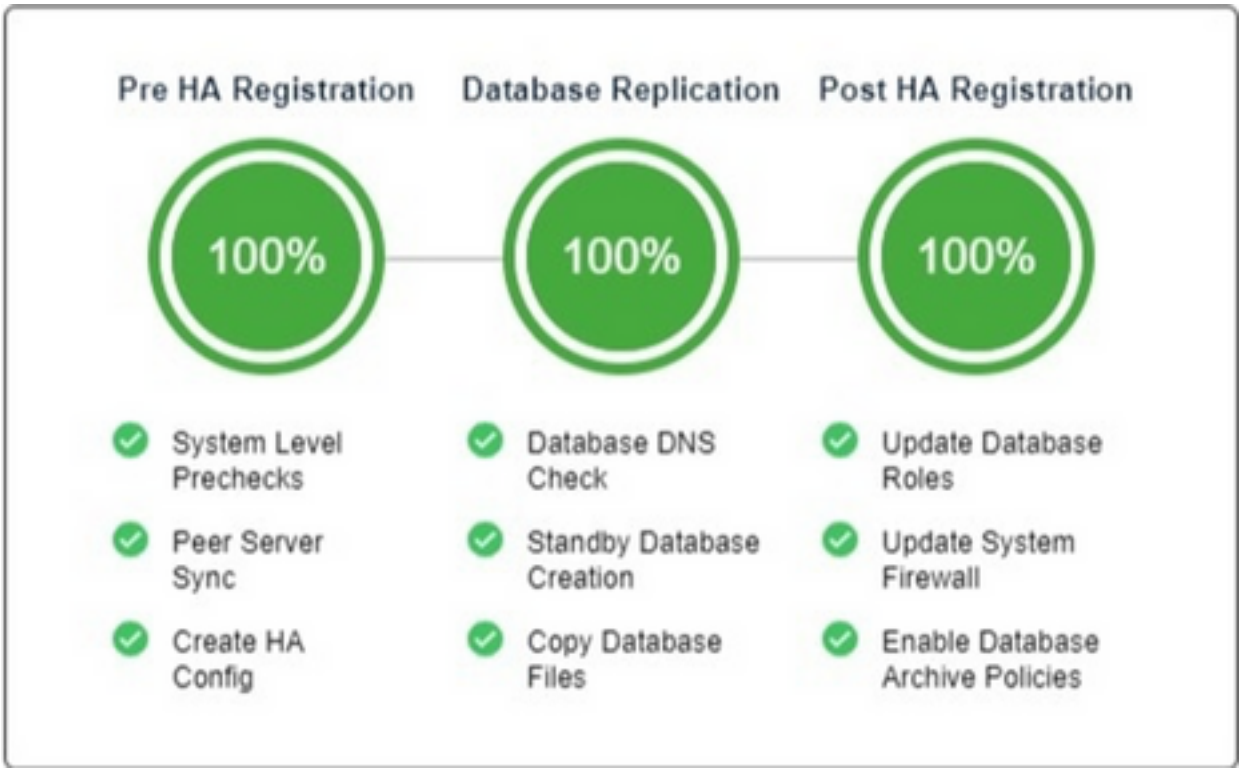
Schritt 4: Wenn Sie die virtuelle IP-Funktion verwenden, aktivieren Sie das Kontrollkästchen **Virtuelle IP aktivieren**, und füllen Sie die weiteren Felder wie folgt aus:

1. IPV4 Virtual IP: Geben Sie die virtuelle IPv4-Adresse ein, die beide HA-Server verwenden sollen.
2. Virtuelle IP IPV6: (Optional) Geben Sie die IPv6-Adresse ein, die beide HA-Server verwenden sollen.

Die virtuelle IP-Adressierung funktioniert nur, wenn sich beide Server im gleichen Subnetz befinden. Sie sollten den IPV6-Adressblock fe80 nicht verwenden. Er ist für die lokale Unicast-Adressierung reserviert.

Schritt 5: Klicken Sie auf **Check Readiness**, um sicherzustellen, dass die HA-bezogenen Umgebungsparameter für die Konfiguration bereit sind.

Schritt 6: Klicken Sie auf **Registrieren**, um die MeilensteinFortschrittsleiste anzuzeigen, um den 100%igen Abschluss der Pre-HA-Registrierung, der Datenbankreplikation und Post HA-Registrierung zu überprüfen, wie hier gezeigt. Die Cisco Prime-Infrastruktur initiiert den HA-Registrierungsprozess. Wenn die Registrierung erfolgreich abgeschlossen wurde, zeigt der **Konfigurationsmodus** den Wert Primary Active (Primärer Aktiv) an.



ISE-Server neu konfigurieren

Schritt 1: Navigieren Sie zu **Administration > Servers > ISE Servers.**

Schritt 2: Navigieren Sie zu **Befehl auswählen > ISE-Server hinzufügen**, und klicken Sie dann auf

Los
Schritt 3: Geben Sie die IP-Adresse, den Benutzernamen und das Kennwort des ISE-Servers ein.

Schritt 4: Bestätigen Sie das ISE-Serverkennwort.

Schritt 5: Klicken Sie auf **Speichern**.

Überprüfen

Der Befehl **ncs certvalidation tofu-certs listcerts** kann zum Überprüfen des neuen Zertifikats verwendet werden.

Zugehörige Informationen

- Versionshinweise zur Cisco Prime-Infrastruktur: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Schnellstartanleitung zur Cisco Prime-Infrastruktur: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Cisco Prime Infrastructure - Befehlsreferenz: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Cisco Prime-Infrastruktur - Benutzerhandbuch: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Administratorhandbuch für die Cisco Prime-Infrastruktur: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **Technischer Support und Dokumentation - Cisco Systems**