TOFU証明書によるPrime Infrastructure 3.5+統合の問題

内容

概要

このドキュメントでは、新しい証明書署名要求(CSR)がCisco Prime Infrastructure（プライマリ/セカンダリ）で生成された後に、Trust-on-first-use(TOFU)証明書の不一致によって発生する統合の問題について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Prime Infrastructure
- ハイ アベイラビリティ

使用するコンポーネント

このドキュメントの情報は、Cisco Prime Infrastructureバージョン3.5以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

これらは、Cisco Prime Infrastructureのハイアベイラビリティと証明書の生成に関する情報を提供する参考資料です。

高可用性ガイド：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

管理者ガイド：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

問題

TOFU：リモートホストから受信した証明書は、初めて接続が確立されたときに信頼されます。

Prime InfrastructureまたはPrimeが接続されているリモートホストのTOFU証明書は、新しい証明書が生成された場合、またはサーバがVMホストに再度導入された場合に変更されることがあります。

新しいCSRをprime infrastructureサーバ（プライマリ/セカンダリ）で生成してインポートすると、サービスの再起動後に接続が再開されると、新しいTOFU証明書情報がリモートサーバに送信されます。

リモートホストが最初の接続後にサブシーケンス接続に対して別の証明書を送信すると、接続は拒否されます。

リモートホストには、古いTOFUがまだ存在するHA展開のプライマリサーバまたはセカンダリサーバ、Integrated Service Engine(ISE)サーバなどがあります。

これにより、プライマリサーバとセカンダリサーバ、PrimeサーバとISEサーバの間の登録が失敗します。

トラブルシューティングセクションでは、このようなシナリオのヘルスモニタログに表示されるエラーメッセージについて説明します。

トラブルシュート

プライマリのヘルスモニタログでは、セカンダリ証明書の不一致を示す次のエラーメッセージが見つかります。

```
[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**

これらのエラーメッセージは、ISEサーバ証明書の不一致を示すPrime Infrastructureログに記録されます。

```
[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
```

セカンダリのヘルスモニタログでは、プライマリ証明書の不一致を示す次のエラーメッセージが見つかります。

```
[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
```

解決方法

primeからの統合を再試行する前に、対応するリモートホストの古い証明書エントリを特定して削除する必要があるため、primeの現在のTOFU証明書をリストする必要があります。

コンフィギュレーション

証明書検証リストの表示

コマンド**ncs certvalidation tofu-certs listcertsを使用**して、証明書検証リストを表示できます。

次の出力は、Cisco Prime Infrastructureプライマリサーバ[IP=1XX.XX.XX.XX]からの出力です。

```
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#
```

この出力は、Cisco Prime Infrastructureセカンダリサーバ[IP=1YY.YY.YY.YY]からのものです

```
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#
```

証明書の削除

ncs certvalidation tofu-certs deletecercert host <host>コマンドを使用して、証明書の検証を削除します。

プライマリサーバで、ISE証明書とセカンダリサーバのTOFU証明書の古いエントリをそれぞれ確認して削除します。

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

セカンダリサーバから、コマンド**ncs certvalidation tofu-certs deletecercert host 1X.XX.XX.XX_8082を使用して、プライマリサーバの豆腐証明書の古いエントリを確認し**て削除します。

プライマリからセカンダリへのHAの再初期化

ステップ1：管理者権限を持つユーザIDとパスワードでCisco Prime Infrastructureにログインします。

ステップ2：メニューから、[**Administration**] > [**Settings**] > [**High Availability]に移動します**。Cisco Prime InfrastructureにHAステータスページが表示されます。

ステップ3:[HA Configuration]を選択し、次のようにフィールドに入力します。

1. セカンダリサーバ：セカンダリサーバのIPアドレスまたはホスト名を入力します。
2. 認証キー：セカンダリサーバのインストール時に設定した認証キーパスワードを入力します。
3. 電子メールアドレス：HA状態の変更に関する通知を送信するアドレス（またはアドレスのカンマ区切りリスト）を入力します。[メールサーバの設定(Mail Server Configuration)]ページを使用して電子メール通知をすでに設定している場合（「電子メールサーバの設定の設定」を参照）、ここで入力した電子メールアドレスが、メールサーバに対して設定済みのアドレスのリストに追加されます。
4. フェールオーバータイプ：[手動]または[自動]を選択します。[Manual]を選択することをお勧めします。

ホスト名をIPアドレスに解決するには、DNSサーバを使用することを推奨します。DNSサーバの代わりに**/etc/hostsファイルを使用**する場合は、ホスト名の代わりにセカンダリIPアドレスを入力する必要があります。

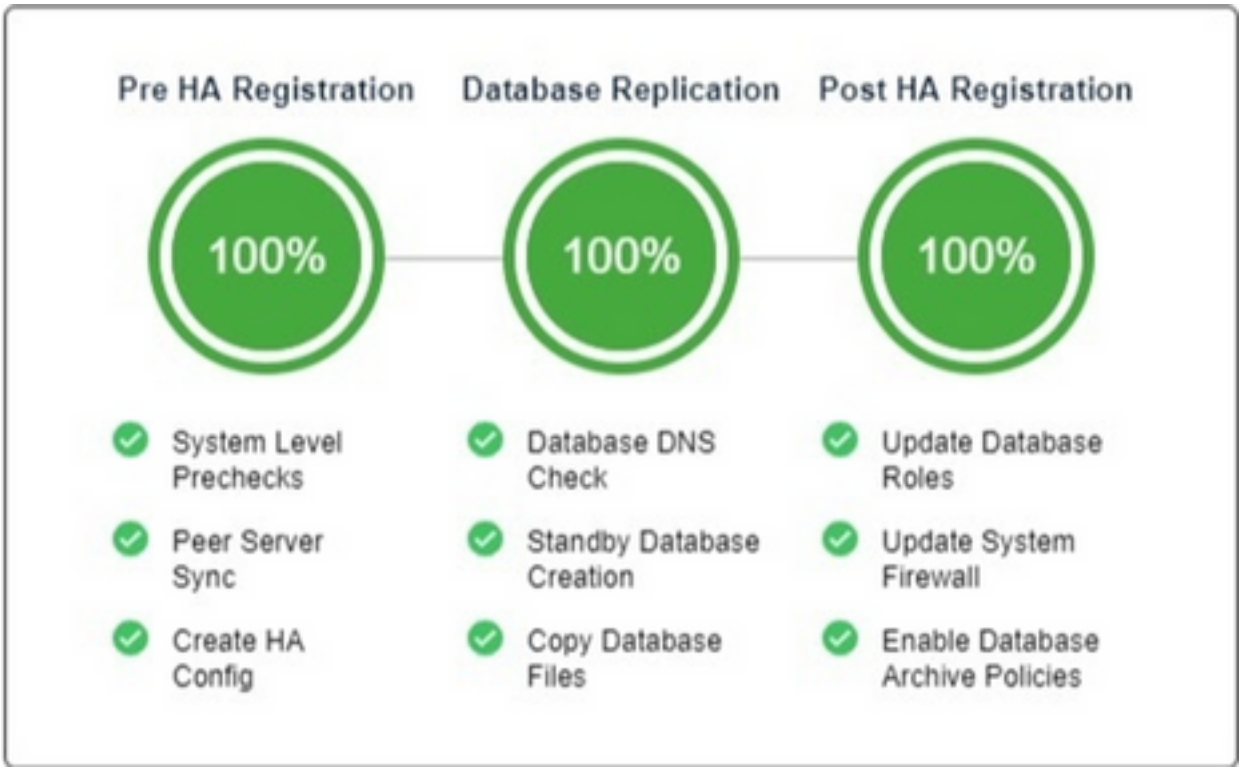
ステップ4：仮想IP機能を使用する場合は、[仮想IPの有効化(**Enable Virtual IP**)]**チェックボックスをオン**にし、次の追加フィールドに入力します。

1. IPV4仮想IP:両方のHAサーバで使用する仮想IPv4アドレスを入力します。
2. IPV6仮想IP:（オプション）両方のHAサーバで使用するIPv6アドレスを入力します。

両方のサーバが同じサブネット上に存在しない限り、仮想IPアドレスは機能しません。IPV6アドレスブロックfe80は使用しないでください。リンクローカルユニキャストアドレス用に予約されています。

ステップ5:[Check Readiness]をクリックして、HA関連の環境パラメータが構成に対応できるかどうかを確認します。

ステップ6:[Register] をクリックして[Milestone]経過表示バーを表示し、次に示すように[Pre-HA Registration]、[Database Replication]、および[Post HA Registration]の100%完了を確認します。Cisco Prime InfrastructureがHA登録プロセスを開始します。登録が正常に完了すると、[Configuration Mode]に[Primary Active]の値が表示されます。



ISEサーバの再設定

ステップ1:[Administration] > [Servers] > [ISE Servers]に移動します。

ステップ2:[Select a command] > [Add ISE Server]に移動し、 Go
ステップ3:ISEサーバのIPアドレス、ユーザ名、およびパスワードを入力します

ステップ4:ISEサーバのパスワードを確認します。

ステップ5:[Save]をクリックします。

確認

コマンドncs certvalidation tofu-certs listcertsを使用して、新しい証明書を確認できます。

関連情報

- Cisco Prime Infrastructureリリースノート：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Cisco Prime Infrastructureクイックスタートガイド：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Cisco Prime Infrastructureコマンドリファレンスガイド：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Cisco Prime Infrastructureユーザガイド：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Cisco Prime Infrastructure管理者ガイド：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **テクニカル サポートとドキュメント – Cisco Systems**