Prime基礎設施3.5+整合問題（由於TOFU證書）

目錄

簡介

本檔案介紹在Cisco Prime基礎架構（主要/輔助）中產生新的憑證簽署請求(CSR)後，由於首次使用時信任(TOFU)憑證不相符而出現的整合問題，以及如何排解和解決此問題。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Prime Infrastructure
- 高可用性

採用元件

本檔案中的資訊是根據Cisco Prime基礎架構3.5版及更新版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

這些是提供有關Cisco Prime基礎設施中的高可用性和證書生成的資訊的參考文檔。

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

管理員指南：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

問題

豆腐 — 第一次建立連線時，從遠端主機收到的證書是受信任的。

如果生成了新證書，或者如果伺服器再次部署在VM主機上，則主基礎設施或主基礎設施連線的遠端主機上的豆腐證書可以更改。

當服務重新啟動後重新啟動連線時，在主基礎設施伺服器（主/輔助）上生成並匯入新的CSR會將新的TOFU證書資訊傳送到遠端伺服器。

如果遠端主機在第一個連線之後為任何子後續連線傳送不同的證書，則該連線將被拒絕。

遠端主機可以是舊TOFU仍然存在的遠端主機(HA部署中的主伺服器或輔助伺服器、整合服務引擎(ISE)伺服器)。

這會導致主伺服器和輔助伺服器、主伺服器和ISE伺服器之間的註冊失敗。

故障排除部分描述了在這樣的情形下可以在運行狀況監視器日誌中找到的錯誤消息。

疑難排解

在主運行狀況監視器日誌中，可以找到這些指向輔助證書中的不匹配的錯誤消息。

```
[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
```

在指向ISE伺服器證書中的不匹配的主基礎設施日誌上可以找到這些錯誤消息。

```
[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
```

在輔助運行狀況監視器日誌中，可以找到這些錯誤消息指出主證書中的不匹配。

```
[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
```

解決方案

需要列出主用上的當前TOFU證書，從中應標識並刪除相應遠端主機的舊證書條目，然後再次嘗試從主用整合。

組態

檢視證書驗證清單

ncs certvalidation tofu-certs listcerts 命令可用於檢視證書驗證清單。

此輸出來自Cisco Prime基礎設施主伺服器[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#
```

此輸出來自Cisco Prime基礎設施輔助伺服器[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#
```

刪除證書

使用命令ncs certvalidation tofu-certs deletecert host <host>可刪除到證書驗證。

從主伺服器分別檢查並刪除ISE和輔助伺服器的TOFU證書的舊條目。

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

從輔助伺服器使用**ncs certvalidation tofu-certs deletecert host** 1X.XX.XX.XX_8082命令檢查並刪除主伺服器的豆腐證書的舊條目。

將HA從主重新初始化為輔助

步驟1.使用具有管理員許可權的使用者ID和密碼登入到Cisco Prime基礎設施。

步驟2.從選單導航到**管理>設定>高可用性**。Cisco Prime Infrastructure顯示HA狀態頁面。

步驟3.選擇HA配置，然後按如下方式填寫欄位：

1. 輔助伺服器：輸入輔助伺服器的IP地址或主機名。
2. 身份驗證金鑰：輸入您在輔助伺服器安裝過程中設定的身份驗證金鑰密碼。
3. 電子郵件地址：輸入應向其傳送有關HA狀態更改通知的地址（或逗號分隔的地址清單）。如果已經使用「郵件伺服器配置」頁配置了電子郵件通知（請參閱「配置郵件伺服器設定」），則在此處輸入的電子郵件地址將附加到已經為郵件伺服器配置的地址清單中。
4. 故障切換型別：選擇「手動」或「自動」。建議您選擇「手動」。

建議使用DNS伺服器將主機名解析為IP地址。如果使用**/etc/hosts**檔案而不是DNS伺服器，則應輸入輔助IP地址，而不是主機名。

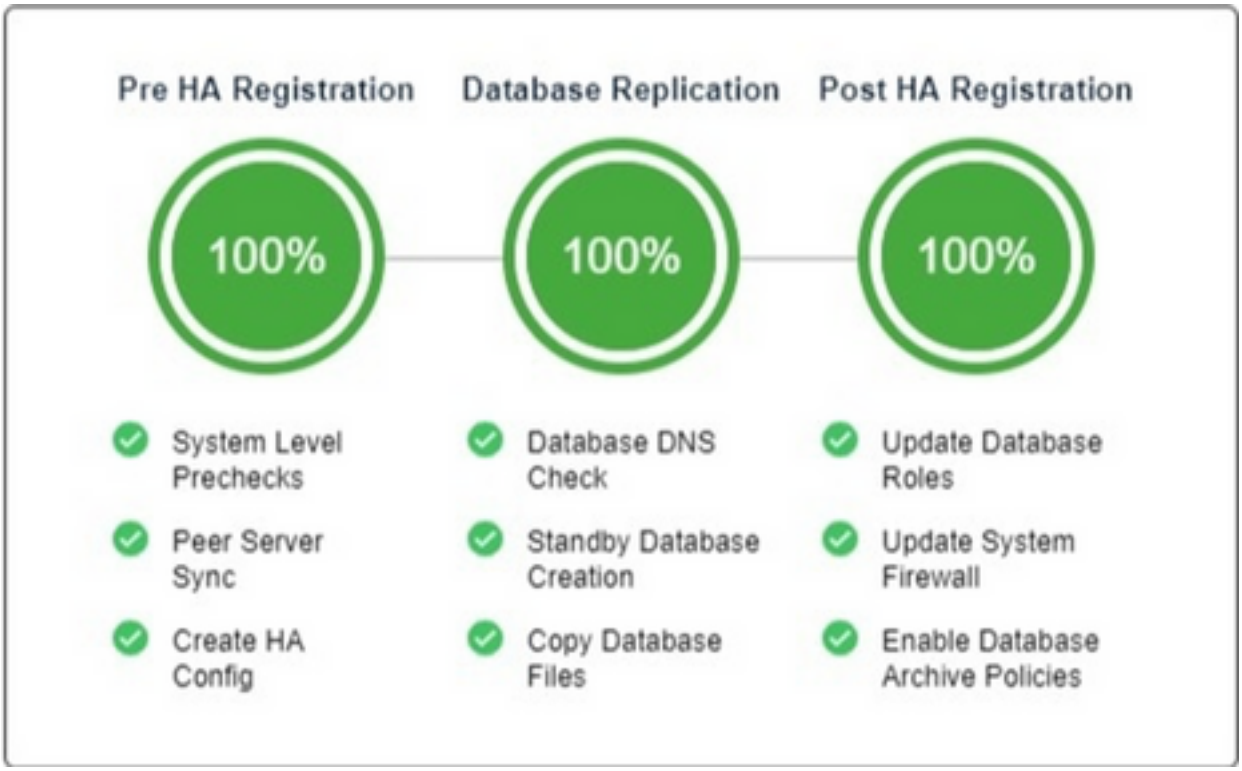
步驟4.如果使用虛擬IP功能，請選中**Enable Virtual IP**覈取方塊，然後按如下方式填寫其他欄位：

1. IPV4虛擬IP:輸入希望兩個HA伺服器使用的虛擬IPv4地址。
2. IPV6虛擬IP:（可選）輸入希望兩個HA伺服器使用的IPv6地址。

虛擬IP定址不起作用，除非兩台伺服器位於同一子網中。不應使用IPV6地址塊fe80，該地址塊已保留用於本地鏈路單播定址。

步驟5.按一下**Check Readiness**以確保與HA相關的環境引數是否已準備好進行設定。

步驟6.按一下**註冊**以檢視里程碑進度條，檢查HA前註冊、資料庫複製和HA後註冊是否完成100%，如此處所示。Cisco Prime Infrastructure啟動HA註冊流程。成功完成註冊後，**配置模式**將顯示Primary Active的值。



重新配置ISE伺服器

步驟1.導航到**管理>伺服器> ISE伺服器**

步驟2.導航至**選擇命令>新增ISE伺服器**，然後按一下 **開始**
步驟3.輸入ISE伺服器的IP地址、使用者名稱和密碼

步驟4.確認ISE伺服器密碼。

步驟5.按一下**Save**。

驗證

ncs certvalidation tofu-certs listcerts命令可用於驗證新證書。

相關資訊

- Cisco Prime Infrastructure發行說明：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Cisco Prime基礎設施快速入門手冊：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Cisco Prime Infrastructure命令參考指南： http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Cisco Prime基礎設施使用手冊：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Cisco Prime Infrastructure管理員指南：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **技術支援與文件 - Cisco Systems**