Problemi di integrazione di Prime Infrastructure 3.5+ dovuti al certificato TOFU

Sommario

Introduzione

Questo documento descrive il problema di integrazione che si verifica a causa di una mancata corrispondenza del certificato Trust-on-first-use (TOFU) dopo che una nuova richiesta di firma del certificato (CSR) è stata generata in Cisco Prime Infrastructure (primario/secondario), come risolverlo e risolvere i problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Prime Infrastructure
- Alta disponibilità

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Prime Infrastructure versione 3.5 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questi sono i documenti di riferimento che forniscono informazioni sull'alta disponibilità e sulla generazione di certificati in Cisco Prime Infrastructure.

Guida all'alta disponibilità: 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

Guida dell'amministratore: 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

Problema

TOFU - Il certificato ricevuto dall'host remoto è attendibile quando viene stabilita la connessione per la prima volta.

Il certificato TOFU nell'infrastruttura primaria o nell'host remoto a cui è connesso prime può cambiare se viene generato un nuovo certificato o se il server viene distribuito nuovamente nell'host VM.

La generazione e l'importazione di un nuovo CSR su un server di infrastruttura principale (primario/secondario) invia le informazioni del nuovo certificato TOFU ai server remoti quando la connettività viene riavviata dopo un riavvio del servizio.

Se l'host remoto invia un certificato diverso per qualsiasi connessione successiva alla prima, la connessione verrà rifiutata.

L'host remoto potrebbe essere (server primario o secondario nell'implementazione di HA, server ISE (Integrated Service Engine)) dove è ancora presente il vecchio TOFU.

Ciò causa un errore di registrazione tra i server primario e secondario, Prime e ISE.

Nella sezione Risoluzione dei problemi vengono descritti i messaggi di errore che è possibile trovare nei registri di Health Monitor in tali scenari.

Risoluzione dei problemi

Nel registro di Health Monitor primario sono presenti questi messaggi di errore che indicano la mancata corrispondenza nel certificato secondario.

```
[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
```

Questi messaggi di errore si trovano nei log dell'infrastruttura primaria e indicano una mancata corrispondenza nel certificato del server ISE.

```
[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
```

Nel registro secondario di Health Monitor, è possibile trovare questi messaggi di errore che indicano la mancata corrispondenza nel certificato primario.

```
[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
```

Soluzione

Ènecessario elencare gli attuali certificati TOFU su prime, da cui la voce precedente del certificato per l'host remoto corrispondente deve essere identificata e rimossa prima di tentare di nuovo l'integrazione da prime.

Configurazione

Visualizza elenco di convalida certificati

Il comando **ncs certvalidation tofu-certs listcerts** può essere utilizzato per visualizzare l'elenco di convalida dei certificati.

Questo output viene generato dal server primario Cisco Prime Infrastructure [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#
```

Questo output viene generato dal server secondario Cisco Prime Infrastructure [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#
```

Elimina certificato

Utilizzare il comando **ncs certvalidation tofu-certs deletecert host <host>** per eseguire l'eliminazione alla convalida del certificato.

Dal server primario controllare ed eliminare le voci precedenti rispettivamente per i certificati ISE e TOFU del server secondario.

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

Dal server secondario controllare ed eliminare le vecchie voci per il certificato tofu del server primario con il comando **ncs certvalidation tofu-certs deletecert host** 1X.XX.XX.XX_8082.

Reinizializzare HA da primario a secondario

Passaggio 1. Accedere a Cisco Prime Infrastructure con un ID utente e una password con privilegi di amministratore.

Passaggio 2. Dal menu, selezionare **Amministrazione > Impostazioni > Alta disponibilità**. Cisco Prime Infrastructure visualizza la pagina di stato HA.

Passaggio 3. Selezionare Configurazione HA, quindi completare i campi come indicato di seguito:

1. Server secondario: Immettere l'indirizzo IP o il nome host del server secondario.
2. Chiave di autenticazione: Immettere la password della chiave di autenticazione impostata durante l'installazione del server secondario.
3. Indirizzo e-mail: Immettere l'indirizzo (o l'elenco di indirizzi separati da virgole) a cui inviare la notifica relativa alle modifiche dello stato HA. Se le notifiche e-mail sono già state configurate utilizzando la pagina Configurazione del server di posta (vedere "Configurazione delle impostazioni del server e-mail"), gli indirizzi e-mail immessi qui verranno aggiunti all'elenco di indirizzi già configurati per il server di posta.
4. Tipo di failover: Selezionare Manuale o Automatico. Si consiglia di selezionare Manuale.

Èconsigliabile utilizzare il server DNS per risolvere il nome host in un indirizzo IP. Se si utilizza il file **/etc/hosts** anziché il server DNS, è necessario immettere l'indirizzo IP secondario anziché il nome host.

Passaggio 4. Se si utilizza la funzionalità IP virtuale, selezionare la casella di controllo **Abilita IP virtuale**, quindi completare i campi aggiuntivi come indicato di seguito:

1. IP virtuale IPV4: Immettere l'indirizzo IPv4 virtuale che entrambi i server HA devono utilizzare.
2. IP virtuale IPV6: (Facoltativo) Immettere l'indirizzo IPv6 che entrambi i server HA devono utilizzare.

L'indirizzamento IP virtuale non funzionerà a meno che entrambi i server non si trovino nella stessa subnet. Non è consigliabile utilizzare il blocco di indirizzi IPV6 fe80 perché è stato riservato per l'indirizzamento unicast locale del collegamento.

Passaggio 5. Fare clic su **Verifica preparazione** per verificare se i parametri ambientali relativi alla disponibilità sono pronti per la configurazione.

Passaggio 6. Fare clic su **Registra** per visualizzare la barra di avanzamento della fase cardine e verificare che la registrazione pre-HA, la replica del database e la registrazione post-HA siano state completate al 100%, come illustrato di seguito. Cisco Prime Infrastructure avvia il processo di registrazione della disponibilità elevata. Una volta completata correttamente la registrazione, nella **modalità di configurazione** verrà visualizzato il valore di Primary Active.

Riconfigurare i server ISE

Passaggio 1. Passare a **Amministrazione > Server > ISE Server**

Passaggio 2. Selezionare **un comando > Aggiungi server ISE**, quindi fare clic su **Vai**
Passaggio 3. Inserire l'indirizzo IP, il nome utente e la password del server ISE

Passaggio 4. Confermare la password del server ISE.

Passaggio 5. Fare clic su **Salva**.

Verifica

Il comando **ncs certvalidation tofu-certs listcerts** può essere utilizzato per verificare il nuovo certificato.

Informazioni correlate

- Note sulla release di Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Guida rapida di Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Guida di riferimento ai comandi di Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Guida per l'utente di Cisco Prime Infrastructure: 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
- Documentazione e supporto tecnico – Cisco Systems