

Fehlerbehebung beim Zertifikataustausch zwischen CVP 12.5 und PCCE 12.0

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Fehlerbehebung](#)

[Schlussfolgerung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird die Fehlerbehebung beim Zertifikataustausch zwischen Cisco Customer Voice Portal (CVP) 12.5(X) und Cisco Package Contact Center Enterprise (PCCE) 12.0(X) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Package Contact Center Enterprise (PCCE) Version 12.0
- CVP Version 12.5
- PCCE Admin Workstation (AW)
- PCCE Single Pane of Glass (SPOG)

Verwendete Komponenten

- Cisco Package Contact Center Enterprise (PCCE) Version 12.0
- CVP Version 12.5

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.

Hintergrund

PCCE 12.5 unterstützt mehrstufige Upgrades, d. h. CVP kann auf 12.5 aktualisiert werden, während PCCE noch in Version 12.0 ist. In diesem Szenario wurde CVP auf 12,5 aktualisiert,

während PCCE in 12.0 bleibt. Nach dem Upgrade wird ein Fehler gemeldet, dass der CVP Reporting Server nicht mit dem Server kommunizieren kann, wenn Sie auf SPOG zugreifen und versuchen, den CVP-Reporting-Server zu konfigurieren.

Fehlerbehebung

Schritt 1: Überprüfen Sie den Status des CVP Reporting-Servers. Navigieren Sie zu CVP Diagnostic Portico, und stellen Sie sicher, dass der Status des Reporting-Systems aktiv ist.

The screenshot shows the CVP Diagnostic Frame View for the Reporting Server. The 'RPT state' is 'In Service'. The 'System Port Usage' is 'NA'. The 'Licensing' is 'Migrated to CSSM'. The 'Call Server Version' is 'CVP 12.5(1) Build=325'. The 'SIP Stack Version' is 'Caffeine 3.2.1.1'. The 'Uptime' is '169:47:11'. The 'Memory' is 'In use: 2070806528 bytes, free: 1768070912 bytes'. The 'Processed at' is 'Fri Mar 20 09:04:58 PDT 2020'.

Schritt 2: Überprüfen Sie den Status der CVP-Server Seite A und Seite B. Navigieren Sie zu CVP Diagnostic Portico, und stellen Sie sicher, dass der Status der Subsysteme aktiv ist.

The screenshot shows the CVP Diagnostic Frame View for the Server. The 'SIP state' is 'In Service'. The 'ICM state' is 'In Service'. The 'IVR state' is 'In Service'. The 'System Port Usage' is 'TOTAL [3000] AVAIL [3000] IN USE [0]'. The 'Licensing' is 'Migrated to CSSM'. The 'Snapshot' table shows various call metrics.

SNAPSHOT	
INBOUND CALLS	0
OUTBOUND CALLS	0
RINGTONE CALLS	0
VIDEO OFFERED	0
VIDEO ANSWERED	0
WHISPER CALLS	0
GREETING CALLS	0
TOTAL CALLS	0
SURVEY API DONE	0
SURVEY API FAILED	0
TRANSCRIPT API DONE	0
TRANSCRIPT API FAILED	0
INBOUND CALLS PER SECOND	0.0
Snapshot SIP Stack Dialogs	0
TOTAL - SINCE STARTUP	
New Calls	2
Connect msgs rcvd from ICM	4
Completed Calls	2
Abnormal Disconnects	0

Schritt 3: Überprüfen Sie den Zertifikatsstatus vom SPOG.

Geben Sie das Zertifikat von AW an, und stellen Sie sicher, dass der CVP Reporting-Server in den Zertifikatspeicher von AW importiert wurde.

```
C:\Program Files (x86)\Java\jre1.8.0_221\bin>keytool -list -v -keystore ..\lib\security\cacerts
```

Wenn Sie nach dem Kennwort gefragt werden, geben Sie **changeit ein**.

Hinweis: Wenn das Zertifikat des CVP Reporting Server Web Service Manager (WSM) nicht in den Zertifikatsspeicher des AW importiert wurde, befolgen Sie die Export- und Importverfahren in den Abschnitten **CVP-Serverzertifikate exportieren** und **CVP-Server-WSM-Zertifikat in ADS Server-Server** in diesem Dokument **importieren**: [Selbstsigniertes PCCE-Zertifikat-Exchange](#).

Schritt 4: Überprüfen Sie den Zertifikatsstatus vom CVP-Reporting-Server.

Listet das Zertifikat des CVP Reporting Servers auf und stellt sicher, dass das AW-Zertifikat in den Zertifikatsspeicher des CVP Reporting Server importiert wurde.

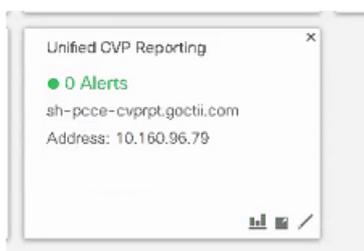
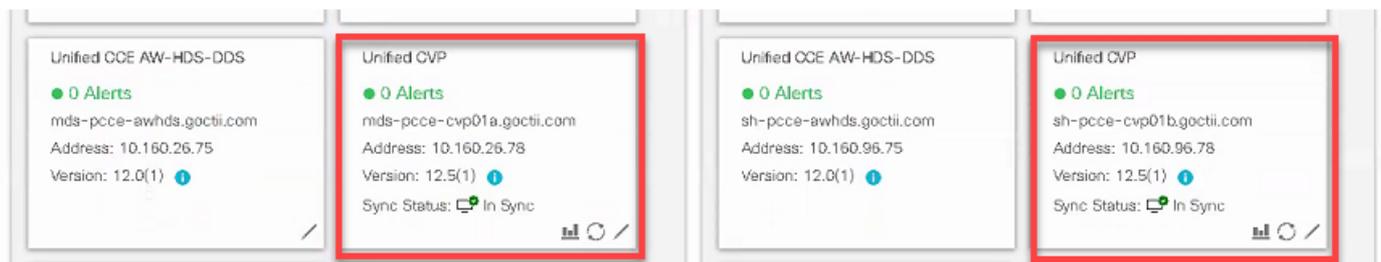
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list -storepass
```

Wenn Sie nach dem Kennwort gefragt werden, geben Sie das Kennwort unter `C:\cisco\cvp\conf\Security.properties` ein.

Hinweis: Wenn das AW-Zertifikat nicht in den Zertifikatsspeicher des CVP-Berichtsservers importiert wurde, befolgen Sie die Export- und Importverfahren aus den Abschnitten **ADS-Serverzertifikate exportieren** und **ADS-Server auf CVP-Server und Reporting Server importieren** in diesem Dokument [Selbstsigniertes PCCE-Zertifikat-Exchange](#).

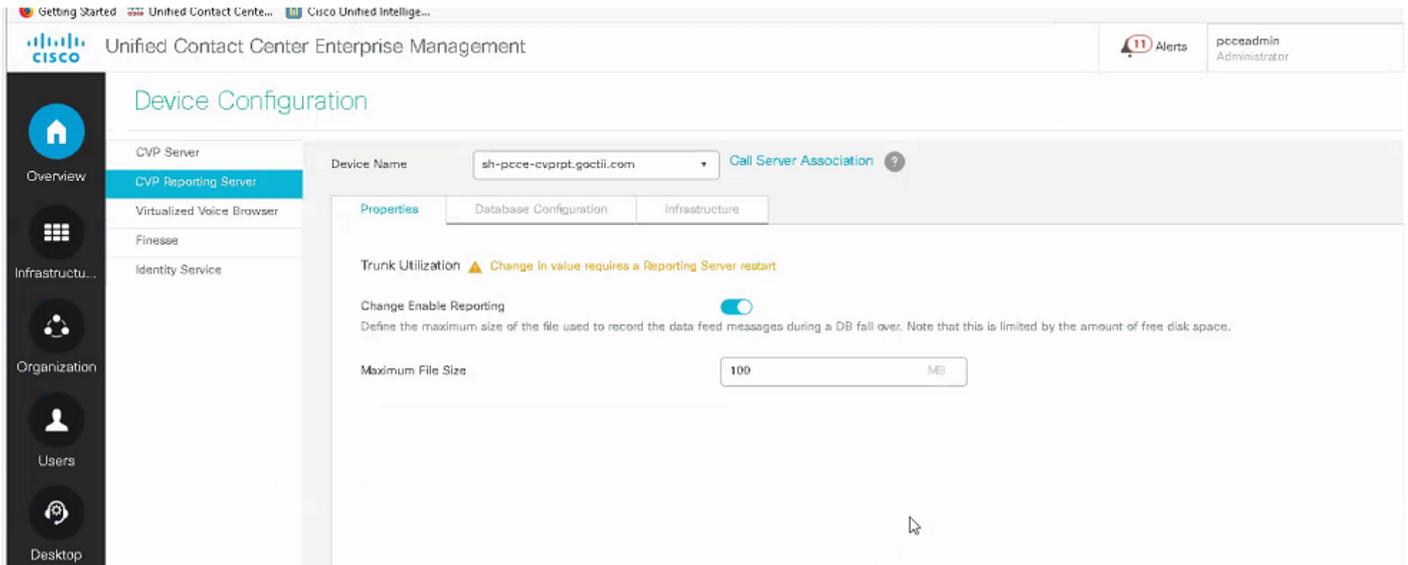
Schritt 5: Stellen Sie sicher, dass Sie die CVP Reporting Web Service Manager (WSM)-Zertifikate in alle PCCE AWs importiert haben. Stellen Sie außerdem sicher, dass Sie alle AW-Server-Zertifikate in den CVP-Reporting-Server importiert haben.

Schritt 6: Überprüfen Sie die Warnmeldungen im SPOG, und stellen Sie sicher, dass die CVP-Server synchronisiert sind. Navigieren Sie zu Übersicht > Bestand.

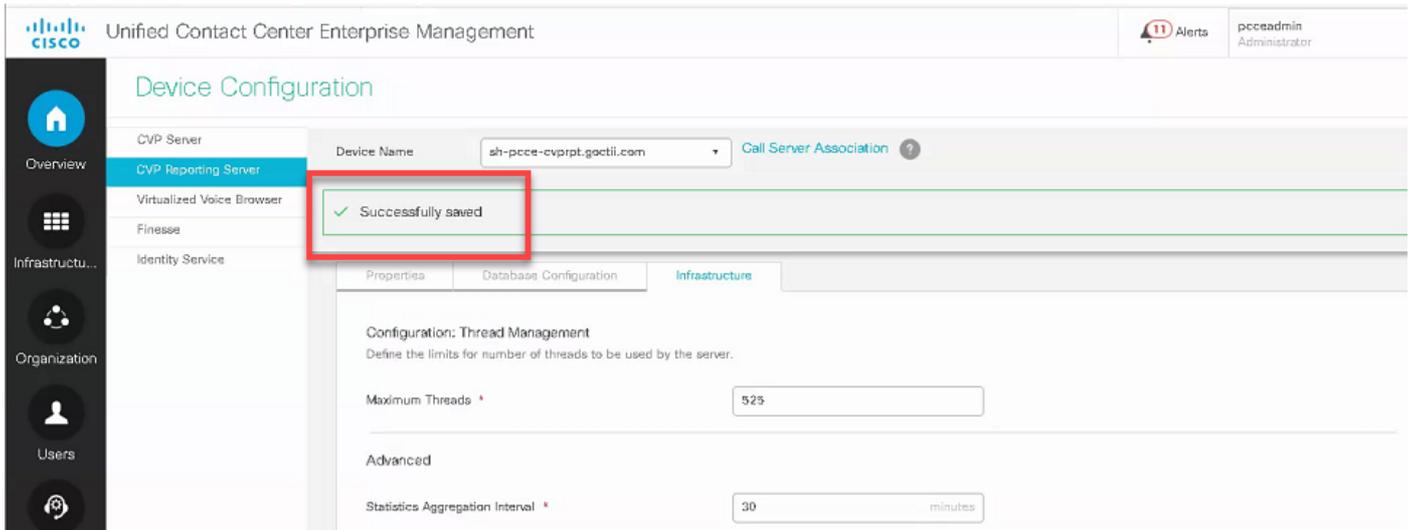


Schritt 7: Rufen Sie den CVP Reporting Server auf, um sicherzustellen, dass kein Fehler gemeldet

wird. Navigieren Sie zu Übersicht > Gerätekonfiguration > CVP Reporting Server.



Schritt 8: Ändern Sie die Konfiguration, und speichern Sie sie. Navigieren Sie zu Übersicht > Gerätekonfiguration > CVP Reporting Server, und klicken Sie auf Save (Speichern).



Schlussfolgerung

- PCCE ES_37 ist erforderlich, damit PCCE 12.0 mit CVP 12.5-Komponenten arbeiten kann.
- CVP Reporting Server-Zertifikate müssen zwischen dem CVP Reporting Server und AW ausgetauscht werden.
- Für PCCE 12.0 und CVP 12.5 ist kein Austausch von Zertifikaten zwischen CVP-Servern (Anrufserver, VXML-Server) und AW-Servern erforderlich. Für die VXML-Anwendungsübertragung von SPOG und Smart Licensing ist jedoch der Zertifikataustausch zwischen diesen Servern erforderlich.

Zugehörige Informationen

[Selbstsigniertes PCCE-Zertifikat-Exchange](#)

[PCCE-Administrations- und Konfigurationsleitfaden](#)

