Dépannage de l'échange de certificats entre CVP 12.5 et PCCE 12.0

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Fond

Dépannage

Conclusion

Informations connexes

Introduction

Ce document décrit comment dépanner l'échange de certificats entre Cisco Customer Voice Portal (CVP) 12.5(X) et Cisco Package Contact Center Enterprise (PCCE) 12.0(X).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Package Cisco Contact Center Enterprise (PCCE) version 12.0
- CVP version 12.5
- Station de travail Admin PCCE (AW)
- Panneau de verre unique PCCE (SPOG)

Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

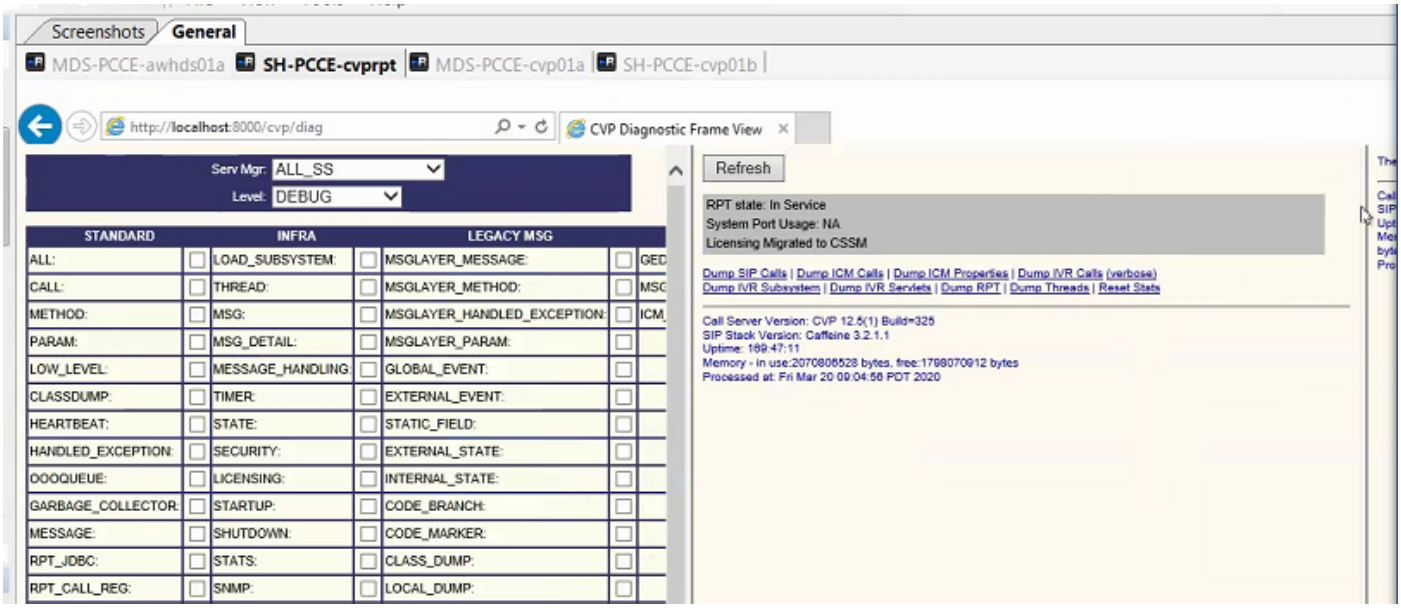
Fond

PCCE 12.5 prend en charge la mise à niveau en plusieurs étapes, ce qui signifie que CVP peut

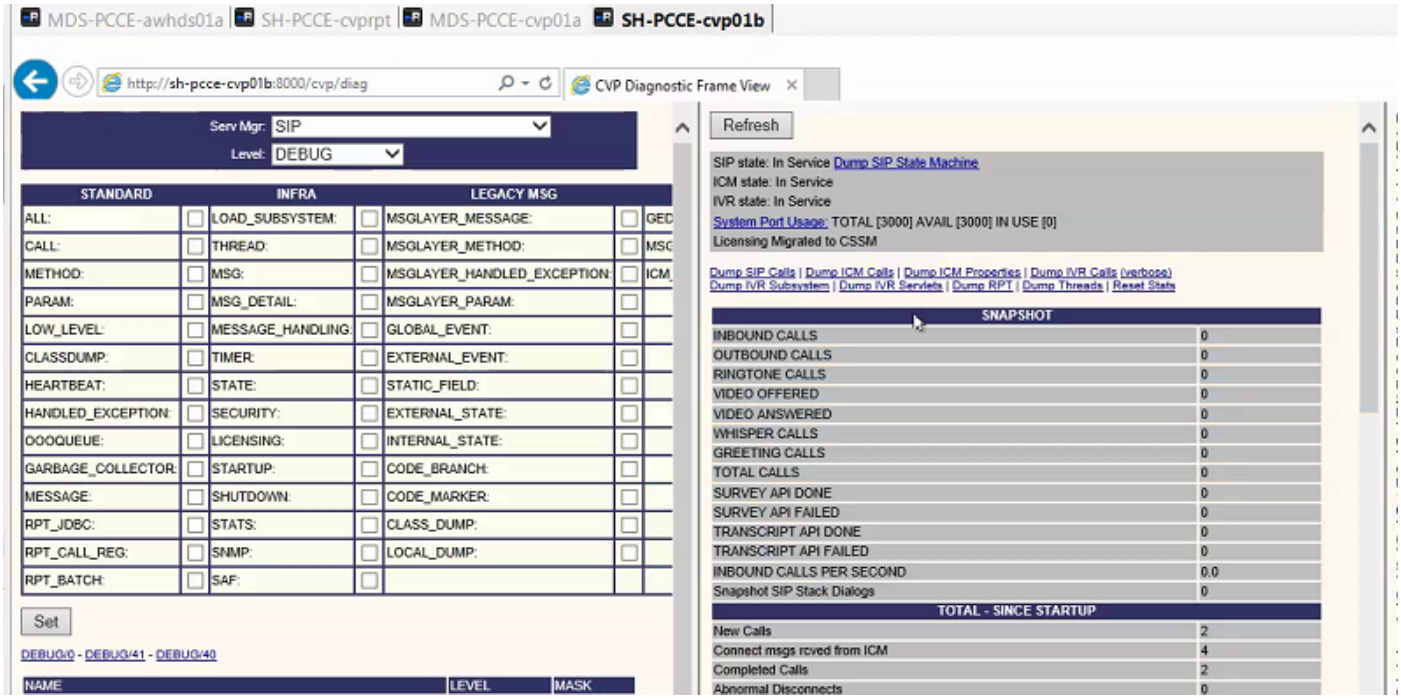
être mis à niveau vers 12.5 alors que PCCE est toujours dans la version 12.0. Dans ce scénario, CVP a été mis à niveau vers 12.5 alors que PCCE reste dans la version 12.0. Après la mise à niveau lorsque vous accédez à SPOG et que vous essayez de configurer le serveur CVP Reporting, une erreur est signalée indiquant qu'il ne peut pas communiquer avec le serveur.

Dépannage

Étape 1 : vérification de l'état du serveur de rapports CVP Accédez à CVP Diagnostic Portico et vérifiez que l'état du système de création de rapports est En service.



Étape 2. Vérifiez l'état du serveur CVP côté A et côté B. Accédez à CVP Diagnostic Portico et assurez-vous que l'état des sous-systèmes est En service.



Étape 3 : vérification de l'état du certificat depuis SPOG

Répertoriez le certificat d'AW et assurez-vous que le serveur CVP Reporting a été importé dans le magasin de certificats AW.

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

Lorsque vous êtes invité à saisir le mot de passe, tapez changeit.

> Remarque : Si le certificat du Gestionnaire de services Web (WSM) du serveur de rapports CVP n'a pas été importé dans le magasin de certificats AW, suivez les procédures d'exportation et d'importation des sections Exporter les certificats du serveur CVP et Importer le certificat WSM des serveurs CVP vers le serveur ADS dans ce document : Échange de certificats autosignés PCCE.

Étape 4 : vérification de l'état du certificat à partir du serveur CVP Reporting

Répertoriez le certificat du serveur CVP Reporting et assurez-vous que le certificat AW a été importé dans le magasin de certificats du serveur CVP Reporting.

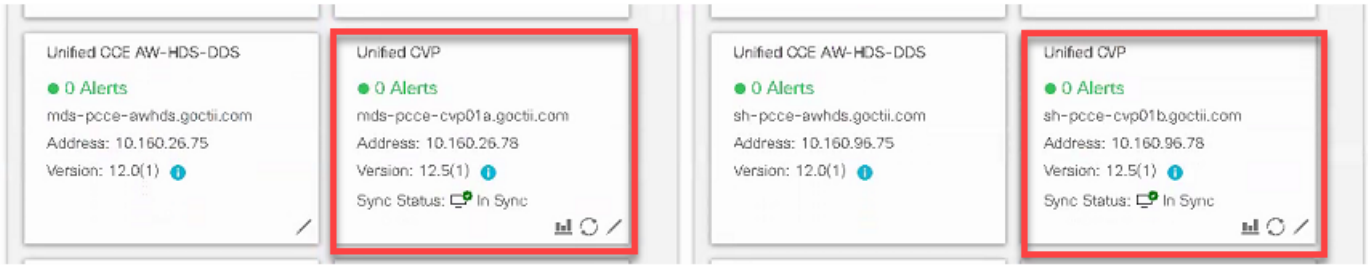
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list -sto
```

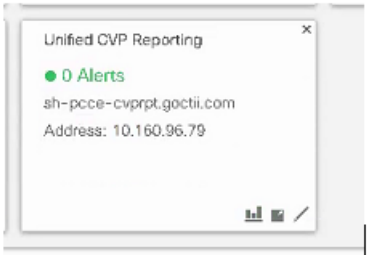
Lorsque vous êtes invité à saisir le mot de passe, tapez le mot de passe trouvé dans C:\cisco\cvp\conf\Security.properties.

> **Remarque :** Si le certificat AW n'a pas été importé dans le magasin de certificats du serveur de rapports CVP, suivez les procédures d'exportation et d'importation **Import ADS Servers to CVP Servers and Reporting Server** dans ce document : Échange de certificats autosignés PCCE.

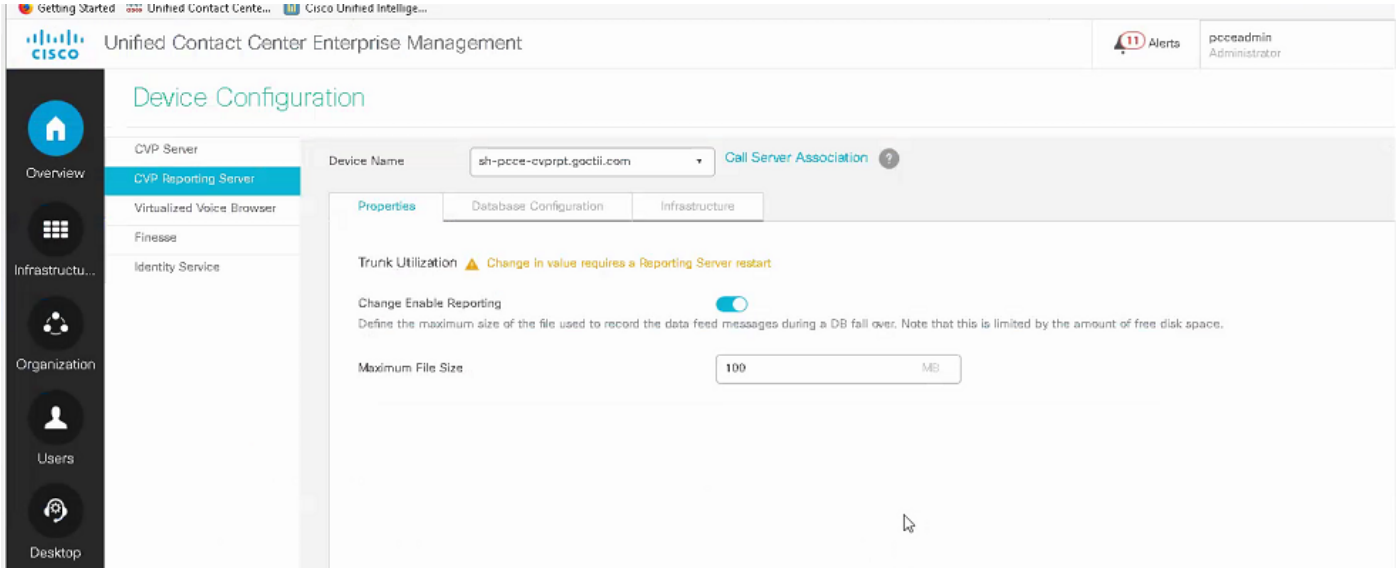
Étape 5. Assurez-vous d'avoir importé les certificats du Gestionnaire de services Web (WSM) CVP Reporting dans tous les PAW PCCE. Vérifiez également que vous avez importé tous les certificats des serveurs AW dans le serveur CVP Reporting.

Étape 6 : vérification des alertes dans SPOG et vérification de la synchronisation des serveurs CVP Accédez à Aperçu > Stock.

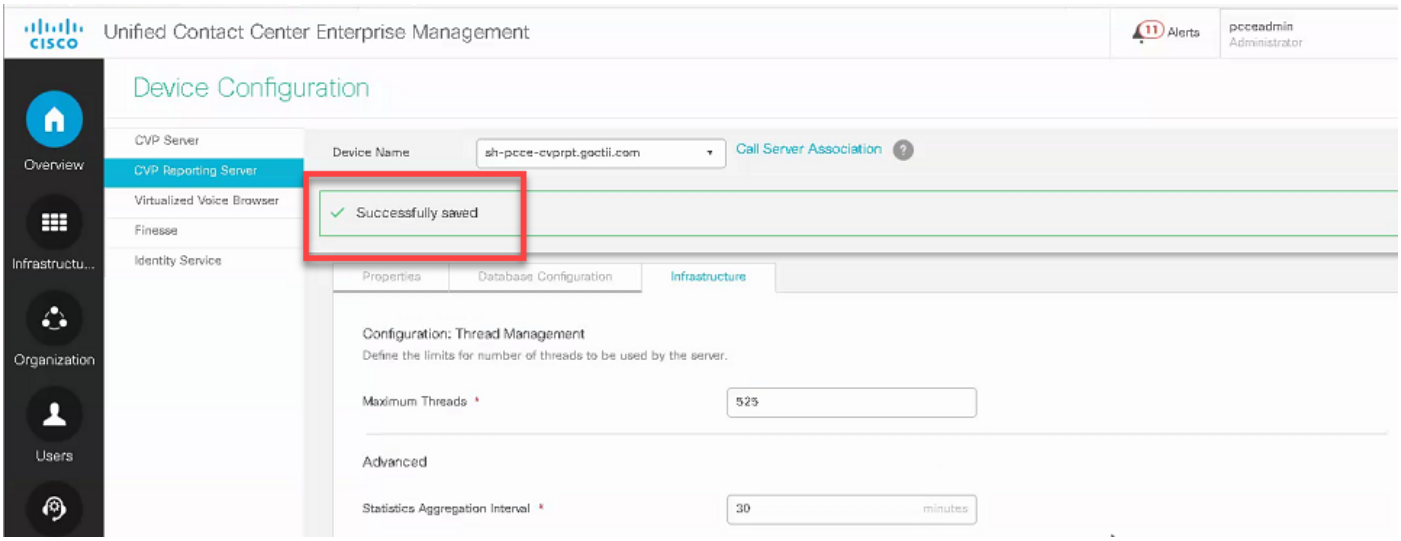




Étape 7. Accédez au serveur CVP Reporting pour vous assurer qu'aucune erreur n'a été signalée. Accédez à Overview > Device Configuration > CVP Reporting server.



Étape 8. Modifier la configuration et l'enregistrer Accédez à Overview > Device Configuration > CVP Reporting server et cliquez sur Save.



Conclusion

- PCCE ES_37 est requis pour que PCCE 12.0 fonctionne avec les composants CVP 12.5.
- Les certificats des serveurs CVP Reporting doivent être échangés entre CVP Reporting Server et AW.
- Pour PCCE 12.0 et CVP 12.5, il n'est pas nécessaire d'échanger des certificats entre les serveurs CVP (serveur d'appels, serveur VXML) et les serveurs AW. Cependant, pour le transfert d'applications VXML depuis SPOG et Smart Licensing, l'échange de certificats est requis entre ces serveurs.

Informations connexes

Échange de certificats autosignés PCCE

Guide d'administration et de configuration de PCCE

Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.