Dépannage de l'échec du transfert de fichiers SPOG PCCE 12.0

Contenu

Introduction

Ce document décrit comment dépanner l'échec du transfert de fichiers de Cisco Packaged Contact Center Enterprise (PCCE) 12.0 Single Pane Of Glass (SPOG).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- PCCE
- Port vocal du client (CVP)

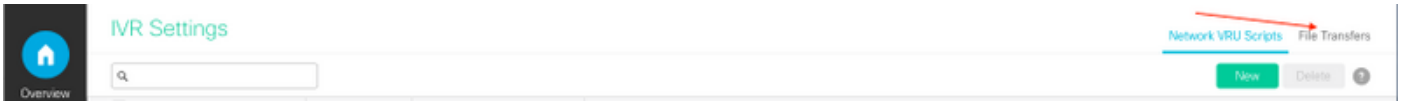
Components Used

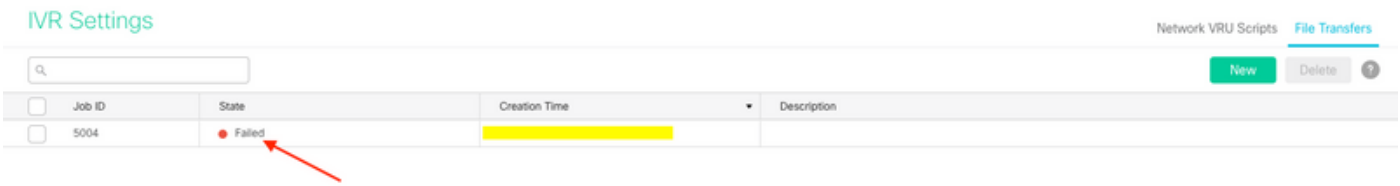
Les informations de ce document sont basées sur PCCE 12.0.1.

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.

Problème

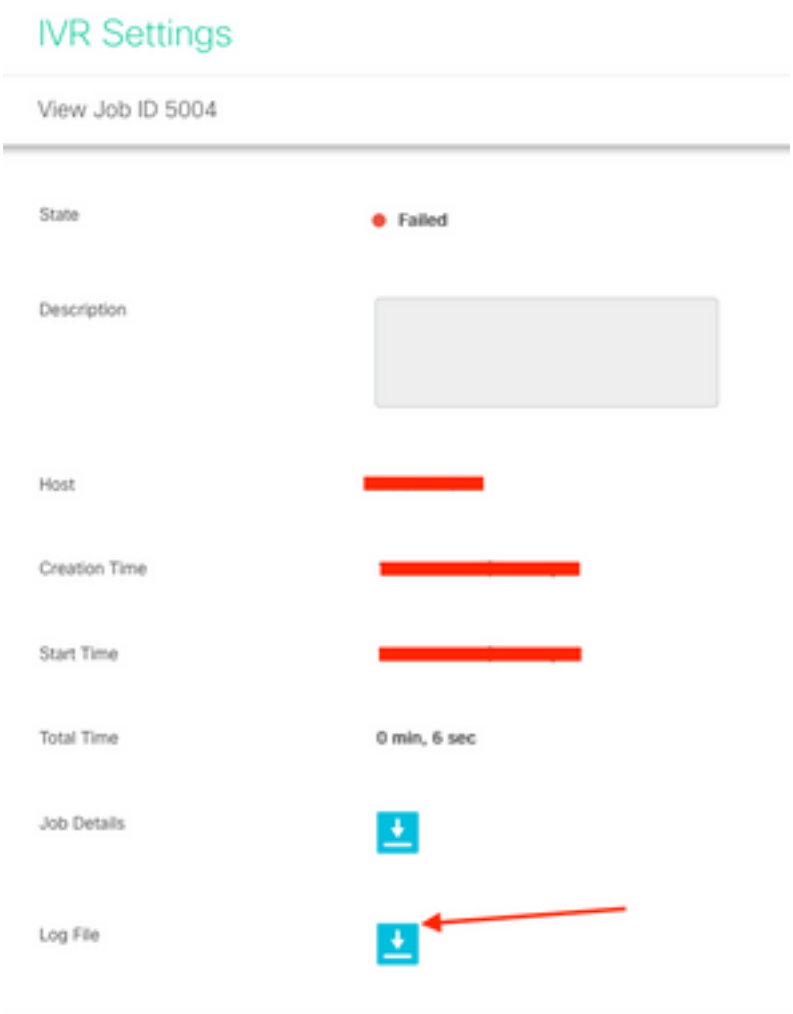
Dans PCCE SPOG, pour le transfert de fichiers, accédez à **SPOG > OverView > Call Settings > IVR Settings > File Transfer**. Parfois, le transfert échoue, comme le montre l'image :





Solution

1. Accédez à **Job** et sélectionnez le **fichier journal** comme indiqué dans l'image.

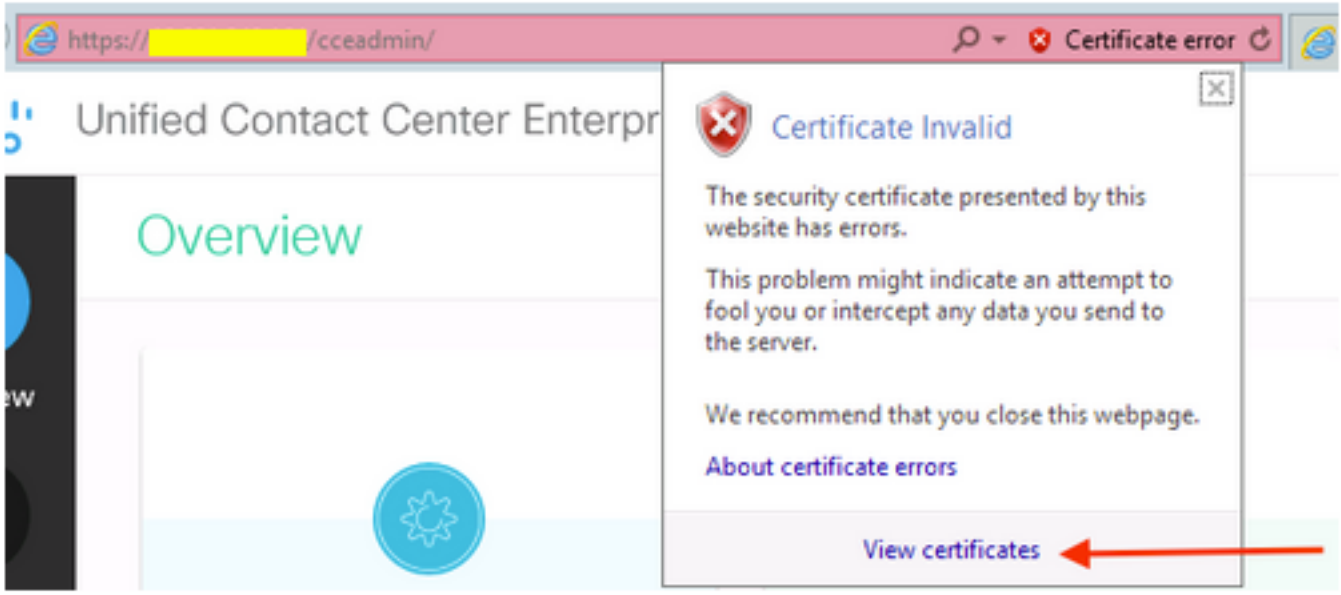


Avis de message d'erreur

```
"Deployment of https://<FQDN of AW
node>:443/unifiedconfig/config/downloadablefiles/ivrapplication/
<FileName>.zip completed on <CVP FQDN> with status as sun.security.validator.ValidatorException:
No trusted certificate found."
```

Cette erreur implique qu'il y a un problème ici, car le certificat AW n'est pas approuvé par CVP. Les étapes permettant de résoudre cette situation sont les suivantes :

2. Copiez le fichier de certificat à partir de l'URL SPOG, comme indiqué dans l'image.



3. Copiez ce fichier de certificat dans le noeud CVP où le fichier ZIP d'origine doit être transféré dans un répertoire :

```
C:\cisco\cvp\conf\security
```

4. Ensuite, copiez le mot de passe de la banque de clés à partir de l'emplacement :

```
keystore password from : %CVP_HOME%\conf\ and open the security.properties
```

5. De la même manière, où le certificat AW a été copié ; ouvrez Invite de commandes en tant qu'administrateur, puis exécutez la commande suivante :

```
cd %CVP_HOME%\jre\bin
```

6. Utilisez cette commande afin d'importer les certificats AW sur le serveur CVP.

```
keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -
alias
<FQDN of AW Node> -file C:\Cisco\CVP\conf\security\<Name of the AW SPOG certificate>.cer
```

7. À l'invite du mot de passe, collez le mot de passe copié à partir du **fichier security.properties**.

8. Tapez **Oui** afin de faire confiance au certificat et de vous assurer que vous obtenez le résultat que le certificat a été ajouté à la banque de clés.

Un avertissement s'affiche avec l'importation réussie. Ceci est dû au format propriétaire Keystore et peut être ignoré.

9. Redémarrez le service cvpcallserver, vxmlserver et wsm sur les noeuds CVP.