Probleemoplossing PCCE 12.0 SPOG-fouten bij bestandsoverdracht

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Probleem](#)
[Oplossing](#)

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij Cisco Packaged Contact Center Enterprise (PCCE) 12.0 eenmalig venster van Glass (SPOG) fouten bij bestandsoverdracht.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PCCE
- Customer Voice Port (CVP)

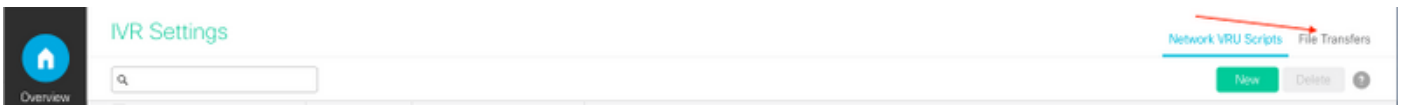
Gebruikte componenten

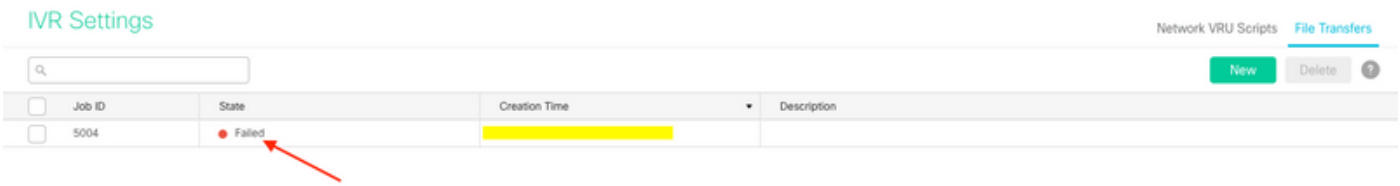
De informatie in dit document is gebaseerd op PCCE 12.0.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem

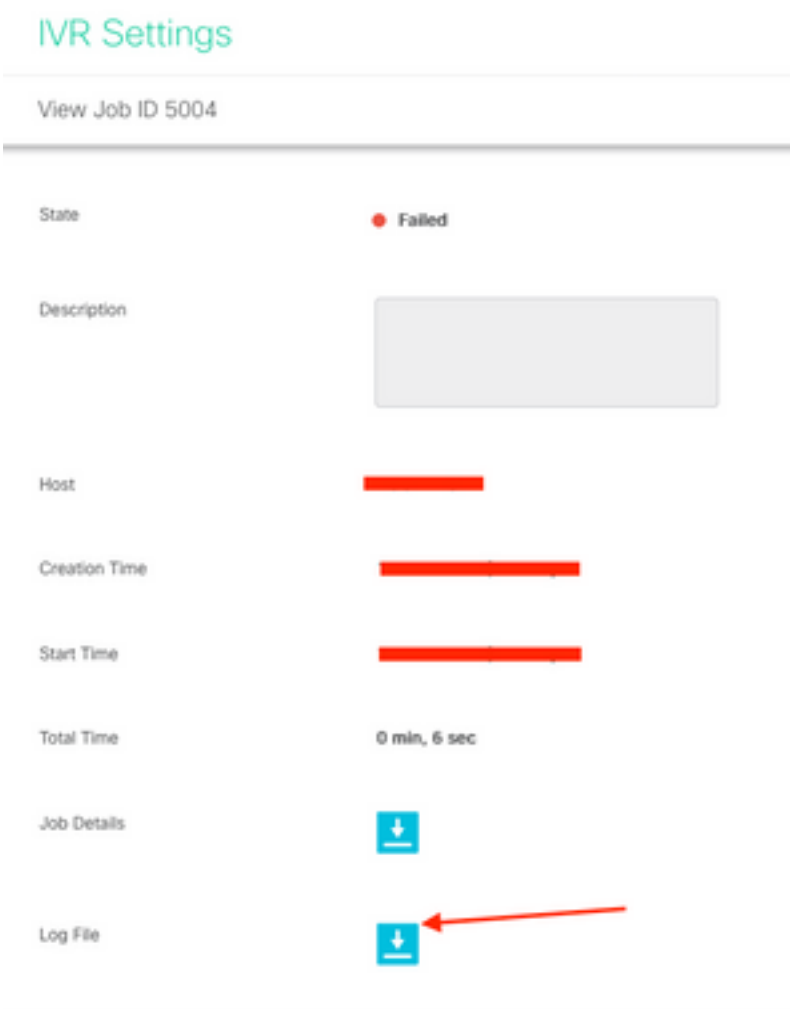
In PCCE SPOG, voor bestandsoverdracht, navigeer naar **SPOG > OverView > Call Settings > IVR-instellingen > File Transfer**. Soms faalt de overdracht zoals in de afbeelding:





Oplossing

1. Blader naar **taak** en selecteer het **logbestand** zoals in de afbeelding.

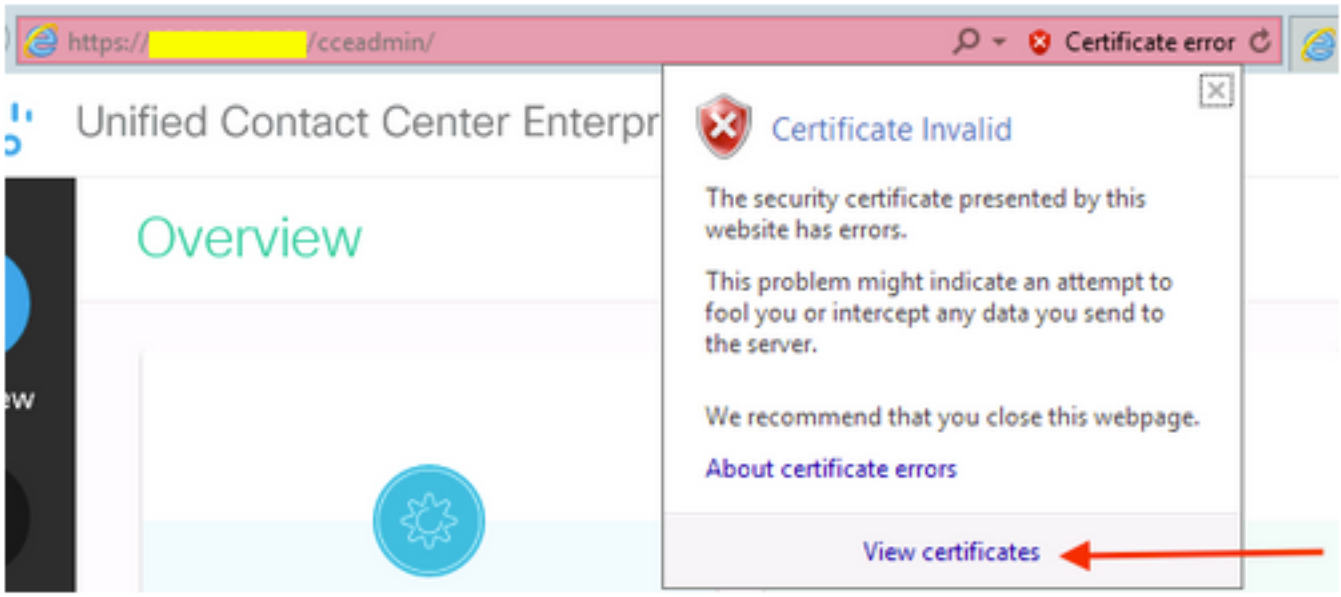


Opmerking voor het foutbericht

```
"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."
```

Deze fout houdt in dat er hier een probleem is omdat het AW-certificaat niet door CVP wordt vertrouwd. Stappen die deze situatie kunnen oplossen zijn:

2. Kopieer het certificaatbestand vanuit SPOG-URL, zoals in de afbeelding.



3. Kopieer dit certificaatbestand naar het CVP-knooppunt, waarbij het oorspronkelijke ZIP-bestand naar een directory moet worden overgebracht:

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

4. Kopieer vervolgens het wachtwoord voor de sleutelwinkel van de locatie:

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

5. Op dezelfde wijze waarop het AW-certificaat is gekopieerd naar het AW-certificaat; Opdracht Wachtwoord als beheerder openen en voer de opdracht uit:

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

6. Gebruik deze opdracht om de AW-certificaten in de CVP-server te importeren.

```
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. Plaats het wachtwoord in de Password-prompt dat is gekopieerd van de **security.eigenschappen**.

8. Type **Ja** om het certificaat te vertrouwen en ervoor te zorgen dat het resultaat dat het Certificaat aan de toetsencombinatie is toegevoegd, wordt ontvangen.

Er wordt een waarschuwing samen met de geslaagde invoer gevraagd. Dit is een gevolg van het eigen formaat Keystore en kan worden genegeerd.

9. Start de omroep server, vxmlserver en wsm service opnieuw op de CVP-knooppunten.