Fehlerbehebung bei PCCE 12.0 SPOG-Dateiübertragungsfehler

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Fehlerbehebung für den Dateiübertragungsfehler Cisco Packaged Contact Center Enterprise (PCCE) 12.0 Single Pane of Glass (SPOG) durchführen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- PCCE
- Customer Voice Port (CVP)

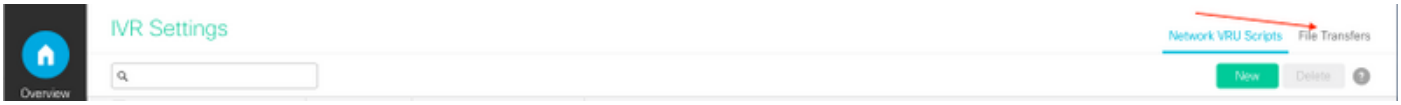
Verwendete Komponenten

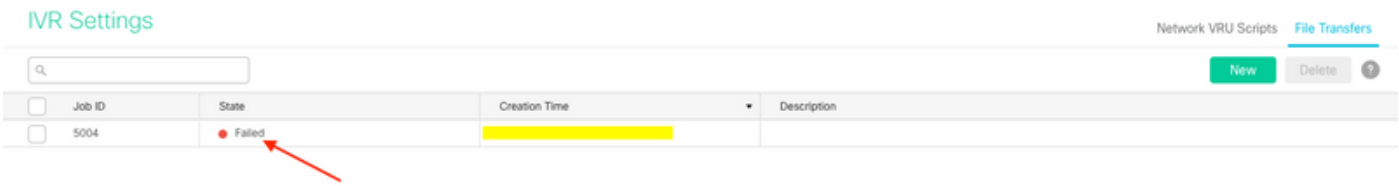
Die Informationen in diesem Dokument basieren auf PCCE 12.0.1.

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.

Problem

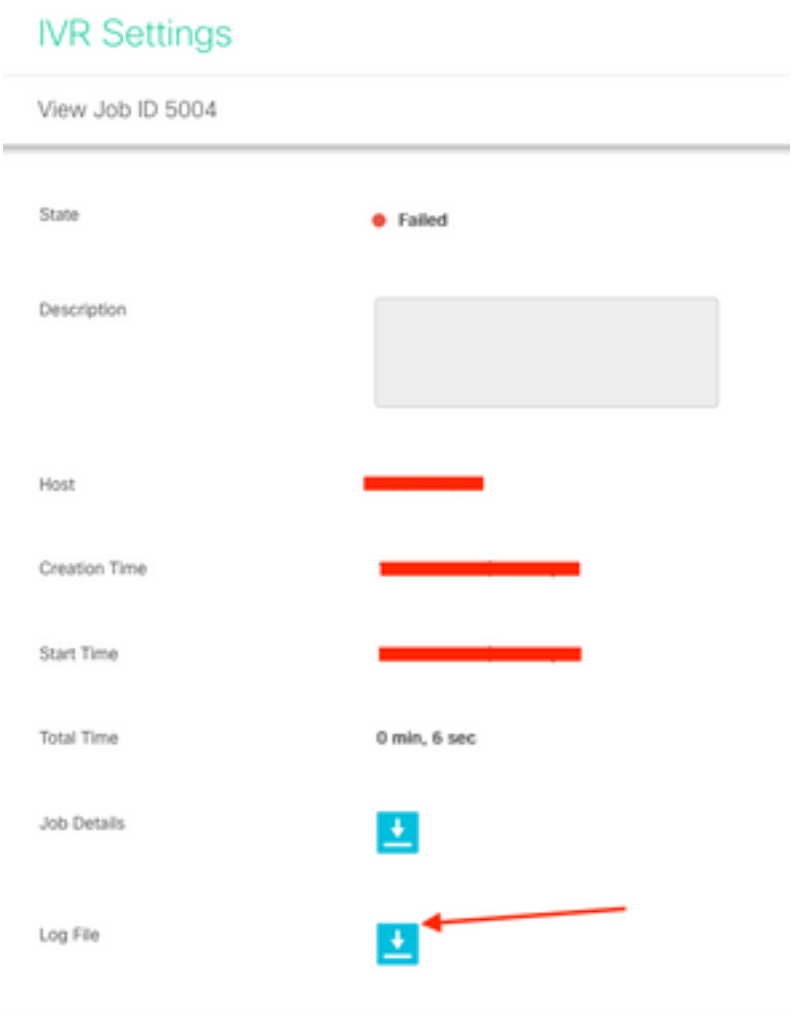
Navigieren Sie für die Dateiübertragung im PCCE SPOG zu **SPOG > OverView > Call Settings > IVR Settings > File Transfers (SPOG > OverView > Anrufeinstellungen > IVR-Einstellungen > Dateiübertragungen)**. Manchmal schlägt die Übertragung fehl, wie im Bild gezeigt:





Lösung

1. Navigieren Sie zu **Job** und wählen Sie die **Protokolldatei** aus, wie im Bild gezeigt.

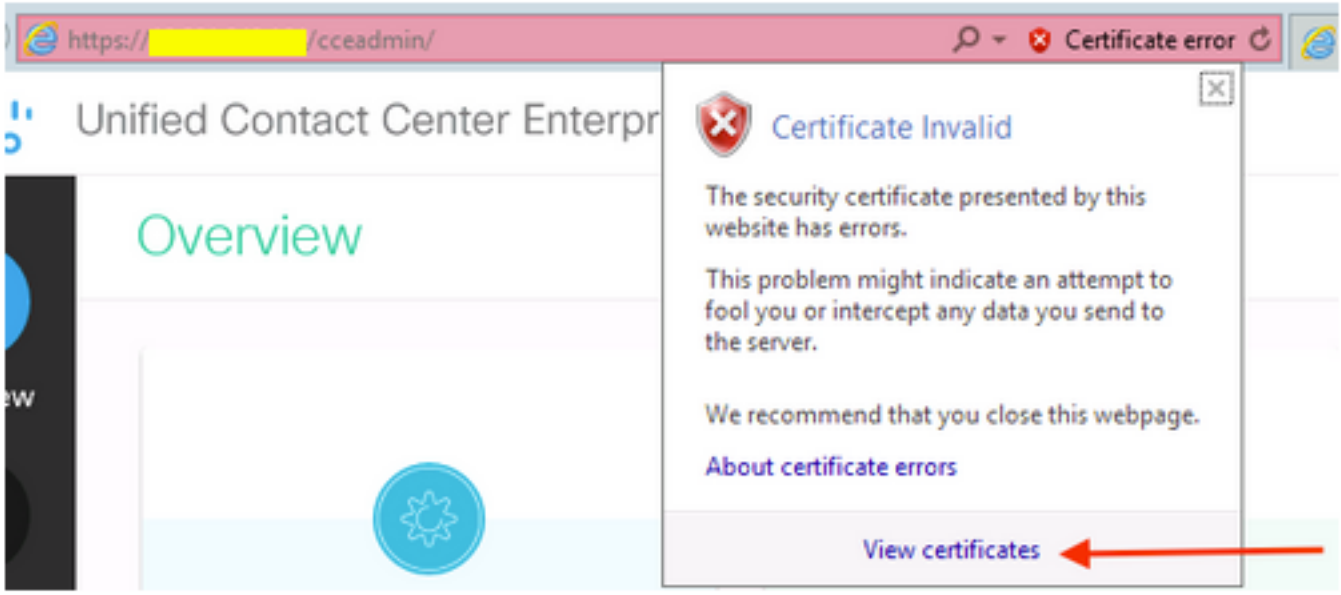


Hinweis für die Fehlermeldung

```
"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."
```

Dieser Fehler impliziert, dass ein Problem vorliegt, da das AW-Zertifikat vom CVP nicht als vertrauenswürdig eingestuft wurde. Folgende Schritte können zur Behebung dieser Situation unternommen werden:

2. Kopieren Sie die Zertifikatsdatei von der SPOG-URL, wie im Bild gezeigt.



3. Kopieren Sie diese Zertifikatsdatei in den CVP-Knoten, wo die ursprüngliche ZIP-Datei in ein Verzeichnis übertragen werden muss:

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

4. Kopieren Sie anschließend das Keystore-Kennwort vom Speicherort:

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

5. auf dieselbe Weise, in die das AW-Zertifikat kopiert wurde; Öffnen Sie die Eingabeaufforderung als Administrator, und führen Sie den folgenden Befehl aus:

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

6. Verwenden Sie diesen Befehl, um die AW-Zertifikate in den CVP-Server zu importieren.

```
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. Fügen Sie an der Kennworteingabeaufforderung das aus der **security.properties** kopierte Kennwort ein.

8. Geben Sie **Yes** ein, um das Zertifikat zu vertrauen, und stellen Sie sicher, dass das Zertifikat zum Keystore hinzugefügt wurde.

Bei einem erfolgreichen Import wird eine Warnung angezeigt. Dies liegt an dem proprietären Format Keystore und kann ignoriert werden.

9. Starten Sie den Dienst cvpcallserver, vxmlserver und wsm auf CVP-Knoten neu.