

PCCE 12.0 SPOGファイル転送障害のトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決方法](#)

概要

このドキュメントでは、Cisco Packaged Contact Center(PCCE)Enterprise(PCCE)12.0 Single Pane Of Glass(SPOG)ファイル転送障害のトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- PCCE
- 顧客音声ポート(CVP)

使用するコンポーネント

このドキュメントの情報は、PCCE 12.0.1に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

問題

PCCE SPOGで、ファイル転送について、[SPOG] > [OverView] > [Call Settings] > [IVR Settings] > [File Transfers]に移動します。図に示すように、転送が失敗することがあります。



Job ID	State	Creation Time	Description
<input type="checkbox"/> 5004	● Failed		

解決方法

1. 「ジョブ」に移動し、図に示すように「ログ・ファイル」を選択します。

IVR Settings

View Job ID 5004

State ● Failed

Description

Host

Creation Time

Start Time

Total Time

0 min, 6 sec

Job Details

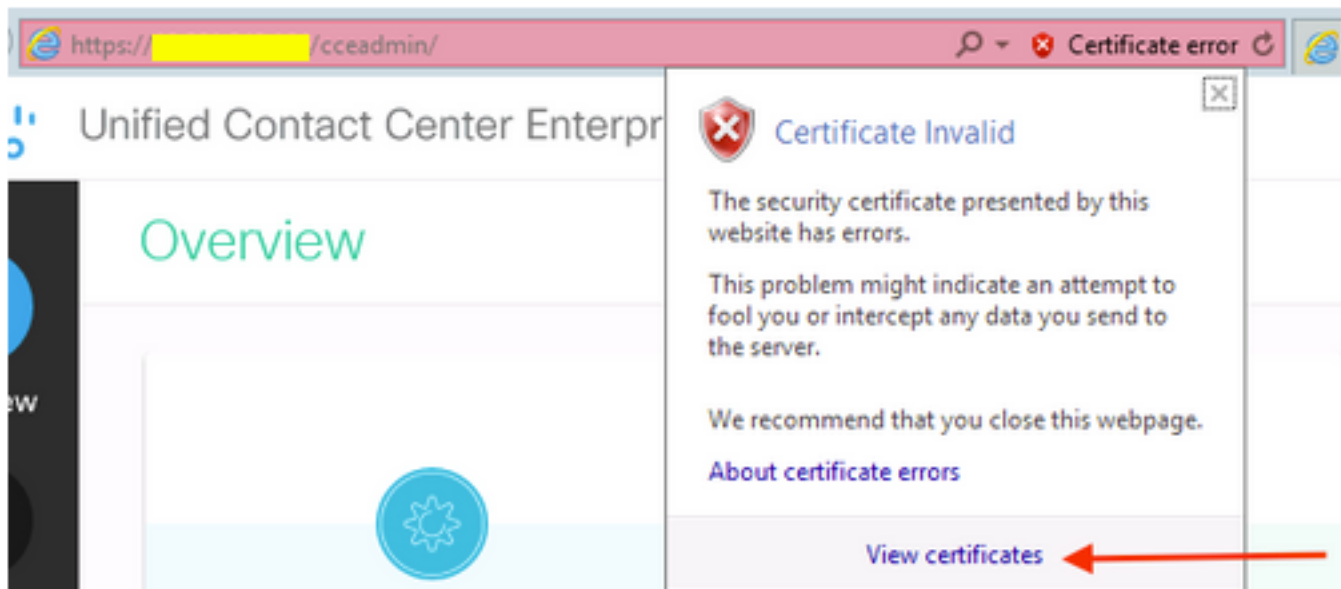
Log File

エラーメッセージの通知

```
"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."
```

このエラーは、AW証明書がCVPによって信頼されていないために問題が発生していることを示します。この状況を修正する手順は次のとおりです。

2. 図に示すように、SPOG URLから証明書ファイルをコピーします。



3.この証明書ファイルを、元のZIPファイルをディレクトリに転送する必要があるCVPノードにコピーします。

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

4.次に、次の場所からキーストアパスワードをコピーします。

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

5. AW証明書のコピー先も同じです。管理者としてコマンドプロンプトを開き、次のコマンドを実行します。

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

6.このコマンドを使用して、AW証明書をCVPサーバにインポートします。

```
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.パスワードプロンプトで、security.propertiesからコピーしたパスワードを貼り付けます。

8. **Yes**と入力して、証明書を信頼し、証明書がキーストアに追加された結果が得られることを確認します。

インポートが成功すると、警告が表示されます。これは独自の形式であるキーストアが原因で、無視できます。

9. CVPノードでcvpcallserver、vxmlserverおよびwsmサービスを再起動します。