Risoluzione dei problemi relativi all'errore di trasferimento file SPOG PCCE 12.0

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a Cisco Packaged Contact Center Enterprise (PCCE) 12.0 Single Pane Of Glass (SPOG) File Transfer Failure.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PCCE
- Customer Voice Port (CVP)

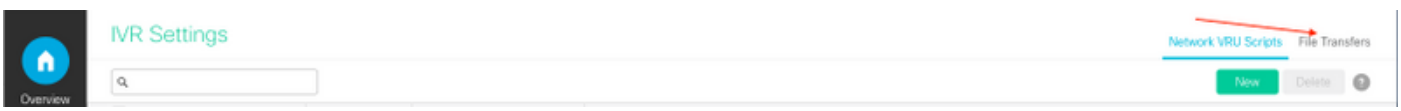
Componenti usati

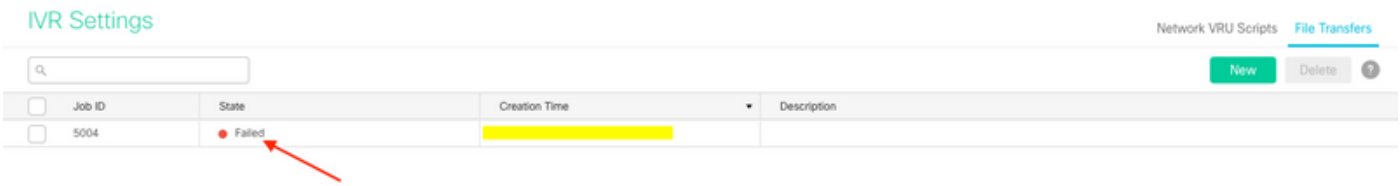
Il riferimento delle informazioni contenute in questo documento è PCCE 12.0.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

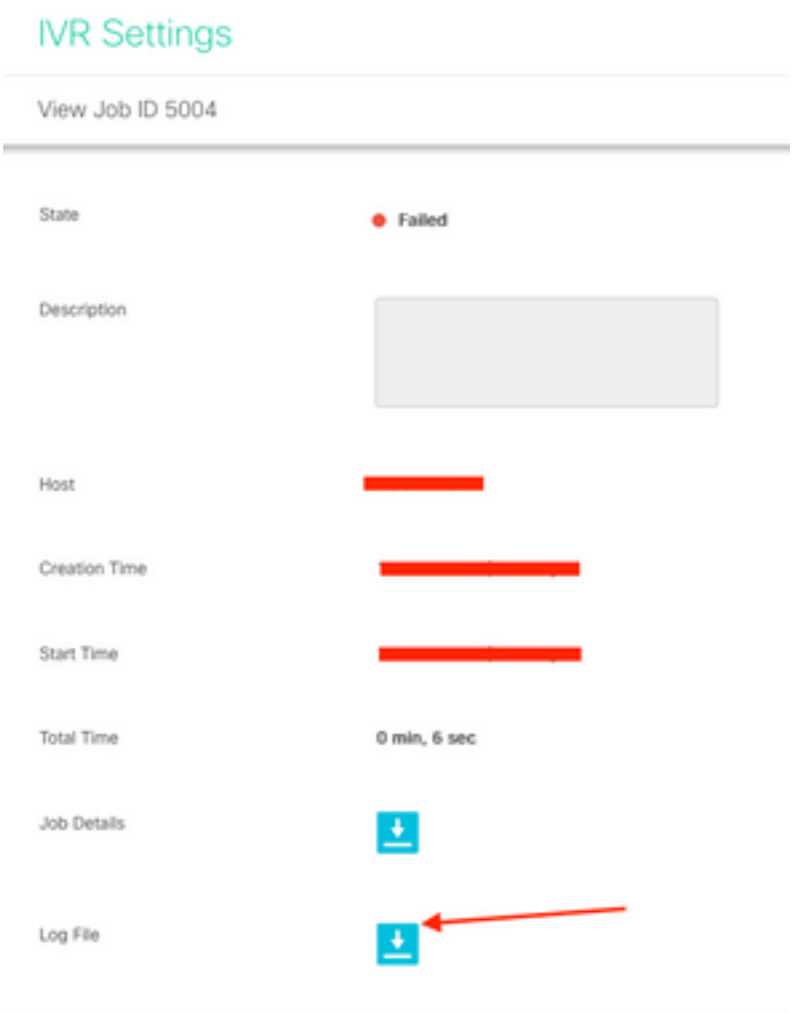
In PCCE SPOG, per il trasferimento di file, selezionare **SPOG > OverView > Call Settings > IVR Settings > File Transfers** (Trasferimenti file). A volte il trasferimento non riesce come mostrato nell'immagine:





Soluzione

1. Passare a **Job** e selezionare il **file di log** come mostrato nell'immagine.

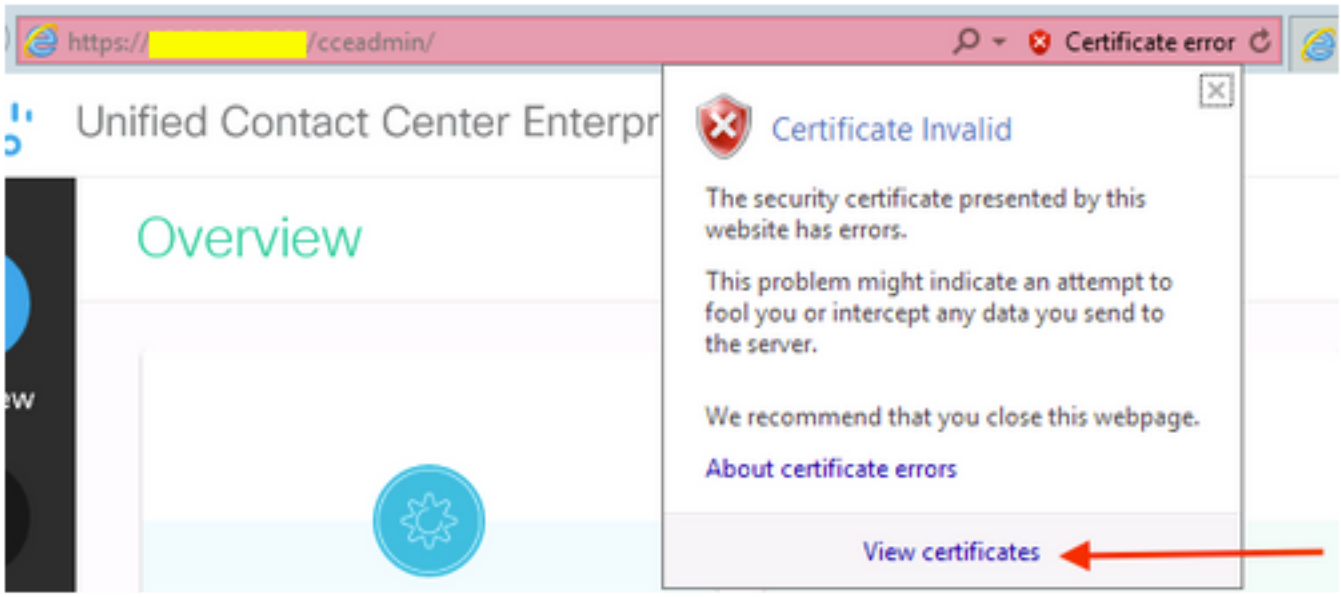


Avviso per il messaggio di errore

```
"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."
```

Questo errore indica che si è verificato un problema perché il certificato AW non è considerato attendibile da CVP. Per risolvere il problema, eseguire le operazioni seguenti:

2. Copiare il file del certificato dall'URL SPOG, come mostrato nell'immagine.



3. Copiare questo file di certificato nel nodo CVP in cui il file ZIP originale deve essere trasferito in una directory:

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

4. Quindi, copiare la password del keystore dal percorso:

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

5. Allo stesso modo, se il certificato AW è stato copiato in; aprire il prompt dei comandi come amministratore ed eseguire il comando:

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

6. Utilizzare questo comando per importare i certificati AW nel server 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. Quando viene richiesta la password, incollare la password copiata da **security.properties**.

8. Digitare **Sì** per considerare attendibile il certificato e assicurarsi di ottenere il risultato che il certificato è stato aggiunto al keystore.

Viene visualizzato un messaggio di avvertenza insieme all'importazione completata. Ciò è dovuto al formato proprietario Keystore e può essere ignorato.

9. Riavviare cvpcallserver, vxmlserver e il servizio wsm sui nodi CVP.