Incapable de trouver le chemin valide de certification à la cible demandée quand vous ajoutez CCO

Contenu

Introduction

Ce document décrit une erreur que vous pouvez recevoir quand vous avez installé un nouvel orchestrator de CloudCenter (CCO) après la configuration des Certificats faits sur commande sur le gestionnaire de CloudCenter (CCM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Linux
- Certificats

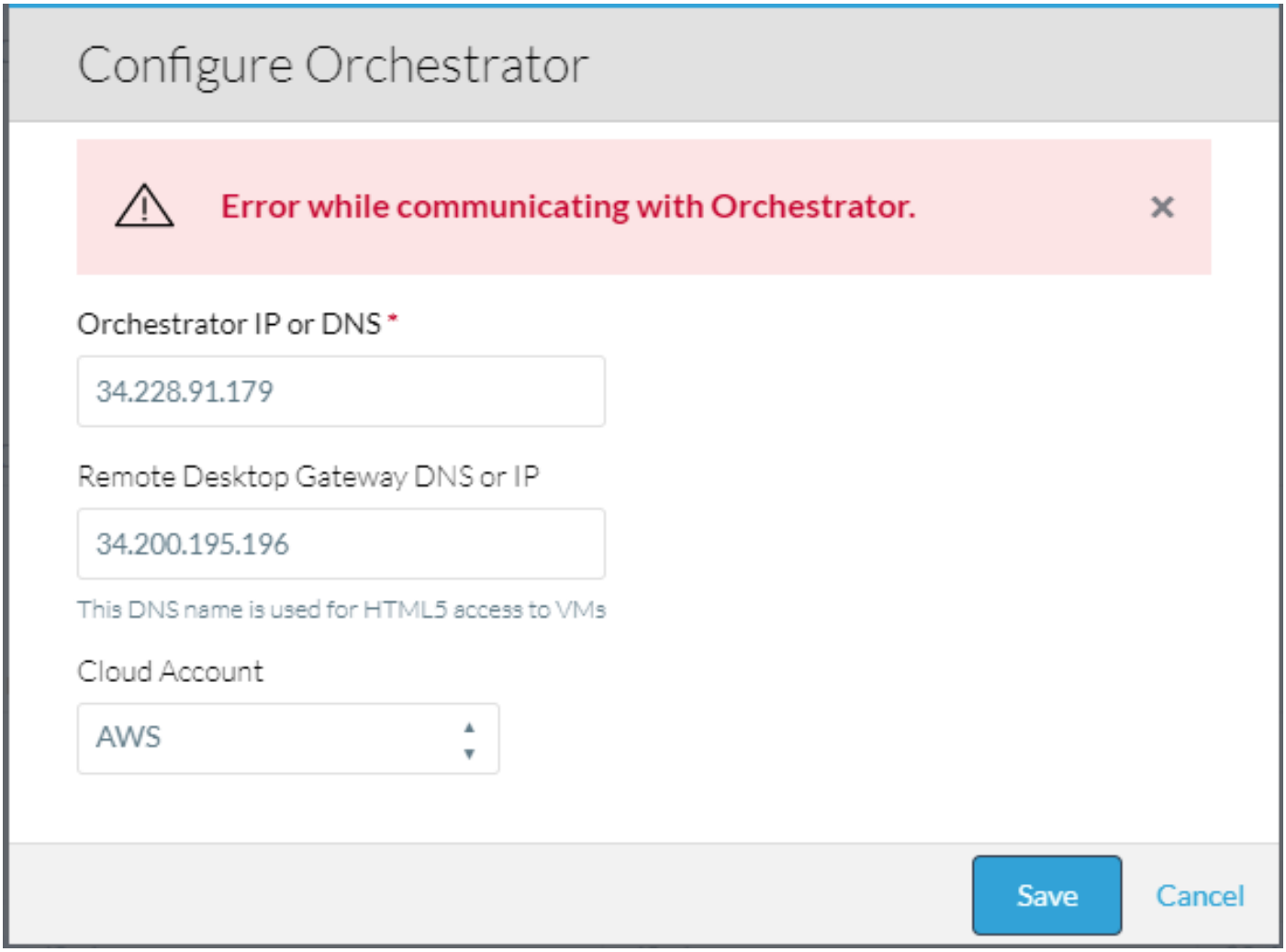
Composants utilisés

Les informations dans ce document sont basées sur 4.8.0+.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

Quand vous configurez l'orchestrator, vous recevez un message d'erreur « erreur tout en communiquant avec l'orchestrator. » suivant les indications de l'image.



Quand vous passez en revue le login d'osmosix le CCM cette erreur est présente.

```
VENDOR_ID::1::USER_ID::2::2017-11-06 15:06:29,103 ERROR impl.GatewayServiceImpl [http-apr-10443-
exec-17]  - Activate gateway exception message: I/O error on POST request for
"https://34.228.91.179:8443/service/v1/gateway/config/activate":sun.security.validator.Validator
Exception: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification
path to requested target; nested exception is javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification
path to requested target
org.springframework.web.client.ResourceAccessException: I/O error on POST request for
"https://34.228.91.179:8443/service/v1/gateway/config/activate":sun.security.validator.Validator
Exception: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification
path to requested target; nested exception is javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification
path to requested target

Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX
path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

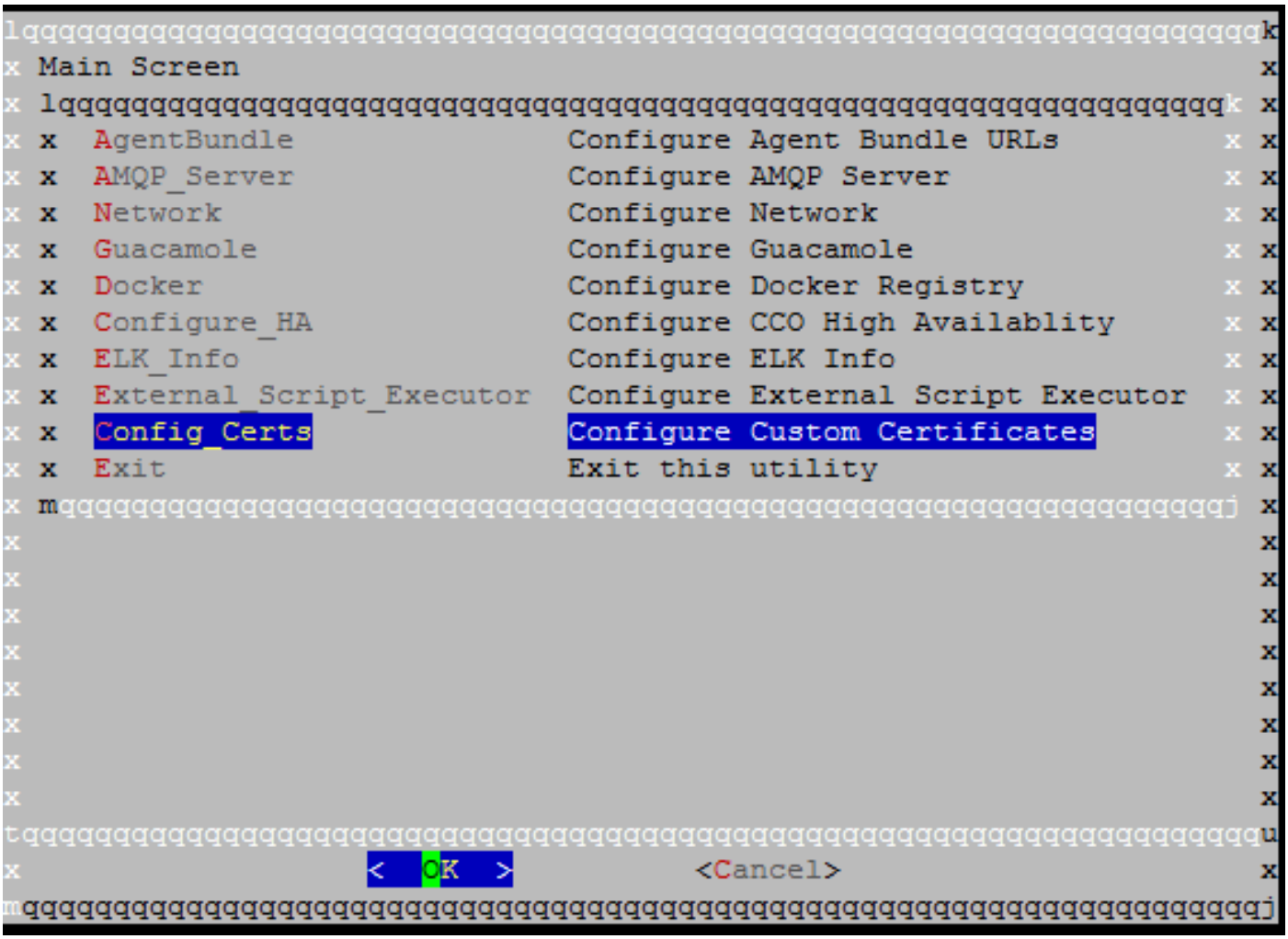
Solution

Ceci est provoqué par par une non-concordance de certificat entre le CCO et le CCM.

Si les Certificats sur le CCM étaient créés avec l'utilisation de l'assistant de la configuration CCM exécutez ces étapes :

Étape 1. Copiez le **répertoire certs.zip** qui a été fait dans le **répertoire de** /tmp du CCM au CCO et présentez l'assistant de configuration CCO situé à /usr/local/cliqr/bin/cco_config_wizard.sh**.**

Étape 2. **Config_Certs** choisi suivant les indications de l'image.



Étape 3. Saisissez le chemin au répertoire certs.zip.

Ceci copie automatiquement les Certificats appropriés et met le fichier nécessaire à jour pour indiquer eux.

Si vous avez manuellement créé le certificat CCM alors exécutez ces étapes :

Étape 1. Copiez le certificat du CCM, l'introduisez, et le certificat de l'autorité de certification au CCO et placez-les dans le répertoire de **/usr/local/tomcat/conf/ssl/**.

Étape 2. Mise à jour **/usr/local/tomcat/conf/server.xml**.

- Localisez la section qui commence par le **<Connector port="8443" maxHttpHeaderSize="8192"**.
- Mettez à jour le **SSLCertificateFile**, le **SSLCertificateKeyFile**, et le **SSLCACertificateFile** pour indiquer les nouveaux fichiers que vous avez copiés plus de suivant les indications de l'image.

```
<Connector port="8443" maxHttpHeaderSize="8192"
           maxThreads="100"
           enableLookups="false" disableUploadTimeout="true"
           acceptCount="100" scheme="https" secure="true"
           SSLEnabled="true"
           SSLCertificateFile="${catalina.base}/conf/ssl/gateway.crt"
           SSLCertificateKeyFile="${catalina.base}/conf/ssl/gateway.key"
           SSLCACertificateFile="${catalina.base}/conf/ssl/ca.crt"
           SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
           SSLCipherSuite="ALL:!aNULL:!EDH:!ADH:!eNULL:!LOW:!EXP:!RC4:+HIGH:+MEDIUM"
           SSLVerifyClient="require" />
```

Étape 3. Afin de redémarrer le serveur, exécutez l'**arrêt de chat de service de** commande, suivi de **début de chat de service**.

La Connectivité entre le CCM et le CCO doit maintenant être possible.