Incapaz de encontrar el trayecto de certificación válido a la blanco pedida cuando usted agrega el CCO

Contenido

Introducción

Este documento describe un error que usted puede recibir cuando usted configura a un nuevo Orchestrator de CloudCenter (CCO) después de la configuración de los Certificados de encargo en el administrador de CloudCenter (CCM).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Linux
- Certificados

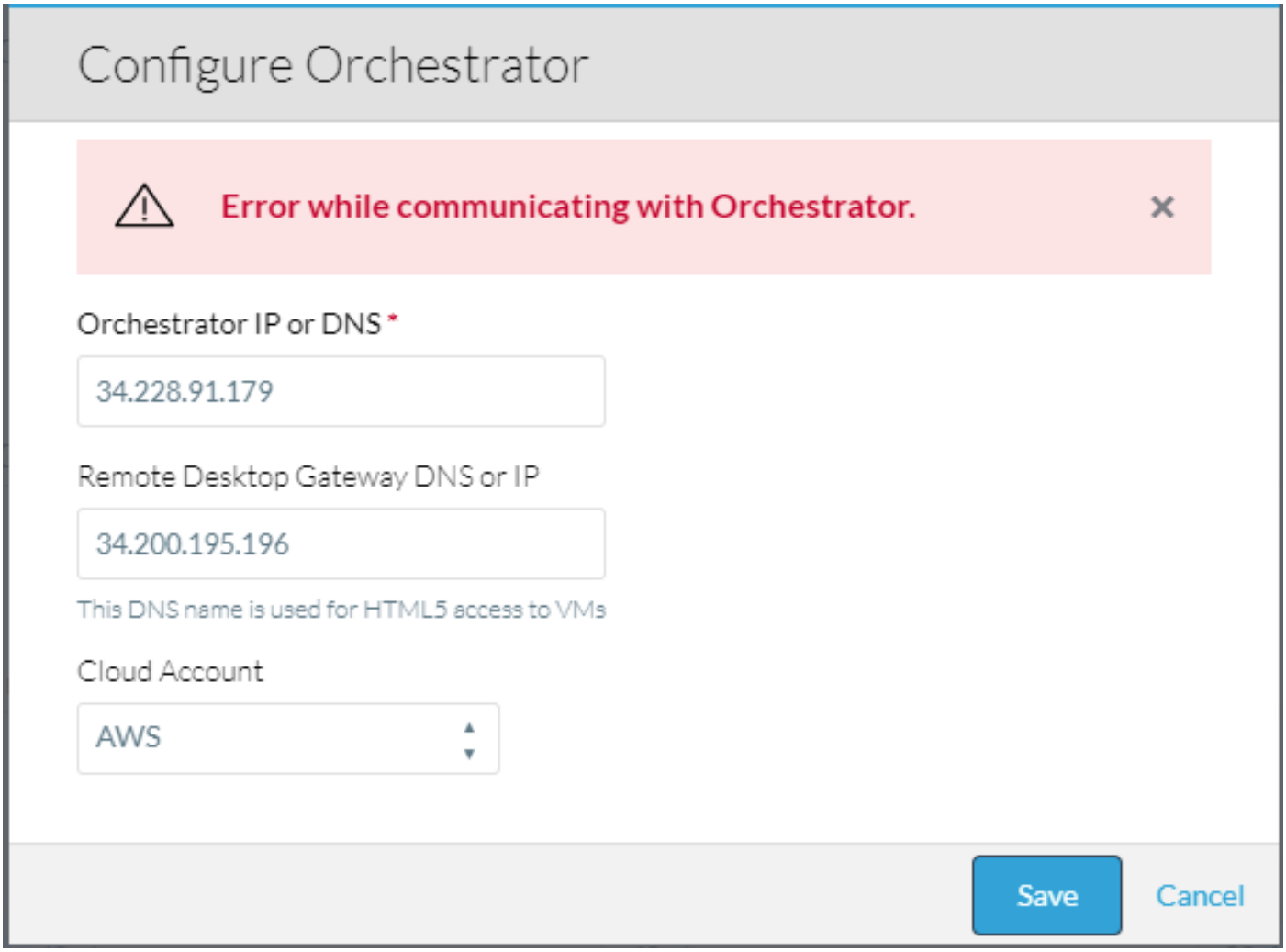
Componentes Utilizados

La información en este documento se basa en 4.8.0+.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Cuando usted configura al Orchestrator, usted recibe un mensaje de error “error mientras que comunica con el Orchestrator.” tal y como se muestra en de la imagen.



Cuando usted revisa el inicio del osmosix CCM este error está presente.

```
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
```

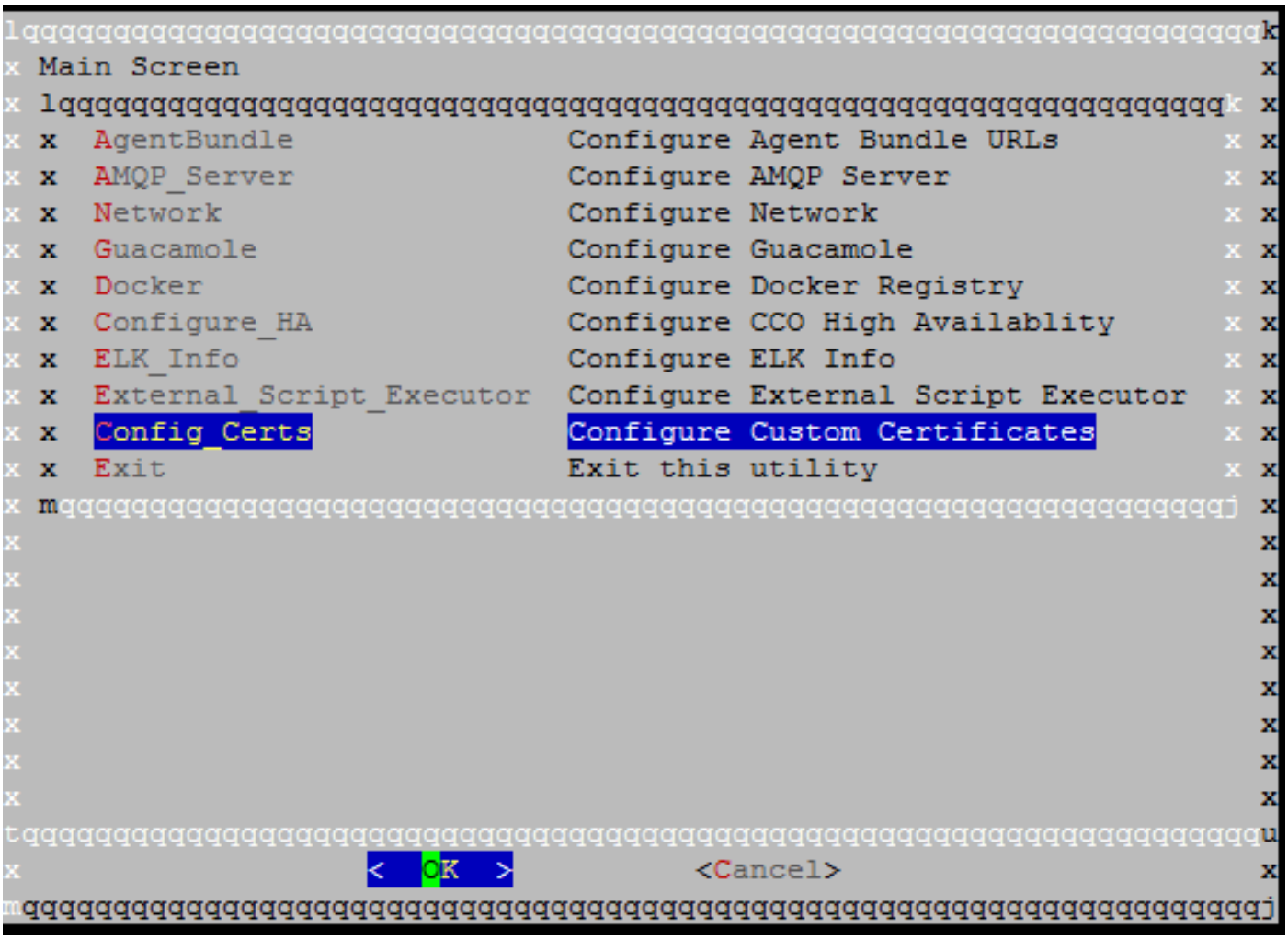
Solución

Esto es causada por una discordancía del certificado entre el CCO y CCM.

Si los Certificados en CCM fueron creados con el uso del Asisitente de la Configuración CCM realice estos pasos:

Paso 1. Copie la **carpeta certs.zip** que fue hecha en el **directorio de** /tmp del CCM al CCO y ingrese al asistente de configuración CCO situado en /usr/local/cliqr/bin/cco_config_wizard.sh**.**

Paso 2. Seleccione **Config_Certs** tal y como se muestra en de la imagen.



Paso 3. Teclee adentro la trayectoria a la carpeta certs.zip.

Esto copia automáticamente los Certificados relevantes y pone al día el archivo necesario para señalar a ellos.

Si usted ha creado manualmente el certificado de CCM después realice estos pasos:

Paso 1. Copie el certificado de CCM, la clave, y el certificado de la autoridad de certificación al CCO y coloqúelos en el directorio de **/usr/local/tomcat/conf/ssl/**.

Paso 2. Actualización **/usr/local/tomcat/conf/server.xml**.

- Localice la sección que comienza con el **<Connector el port="8443" el maxHttpHeaderSize="8192"**.
- Ponga al día el **SSLCertificateFile**, el **SSLCertificateKeyFile**, y el **SSLCACertificateFile** para señalar a los nuevos archivos que usted copió encima tal y como se muestra en de la imagen.

```
<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" />
```

Paso 3. Para recomenzar el servidor, ejecute la **parada del tomcat del** comando service, seguida por el **comienzo del tomcat del servicio**.

La Conectividad entre CCM y el CCO debe ahora ser posible.