Unable to Find Valid Certification Path to Requested Target When You Add CCO

Contents

Introduction

This document describes an error you can receive when you set up a new CloudCenter Orchestrator (CCO) after the configuration of custom certificates on the CloudCenter Manager (CCM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Linux
- Certificates

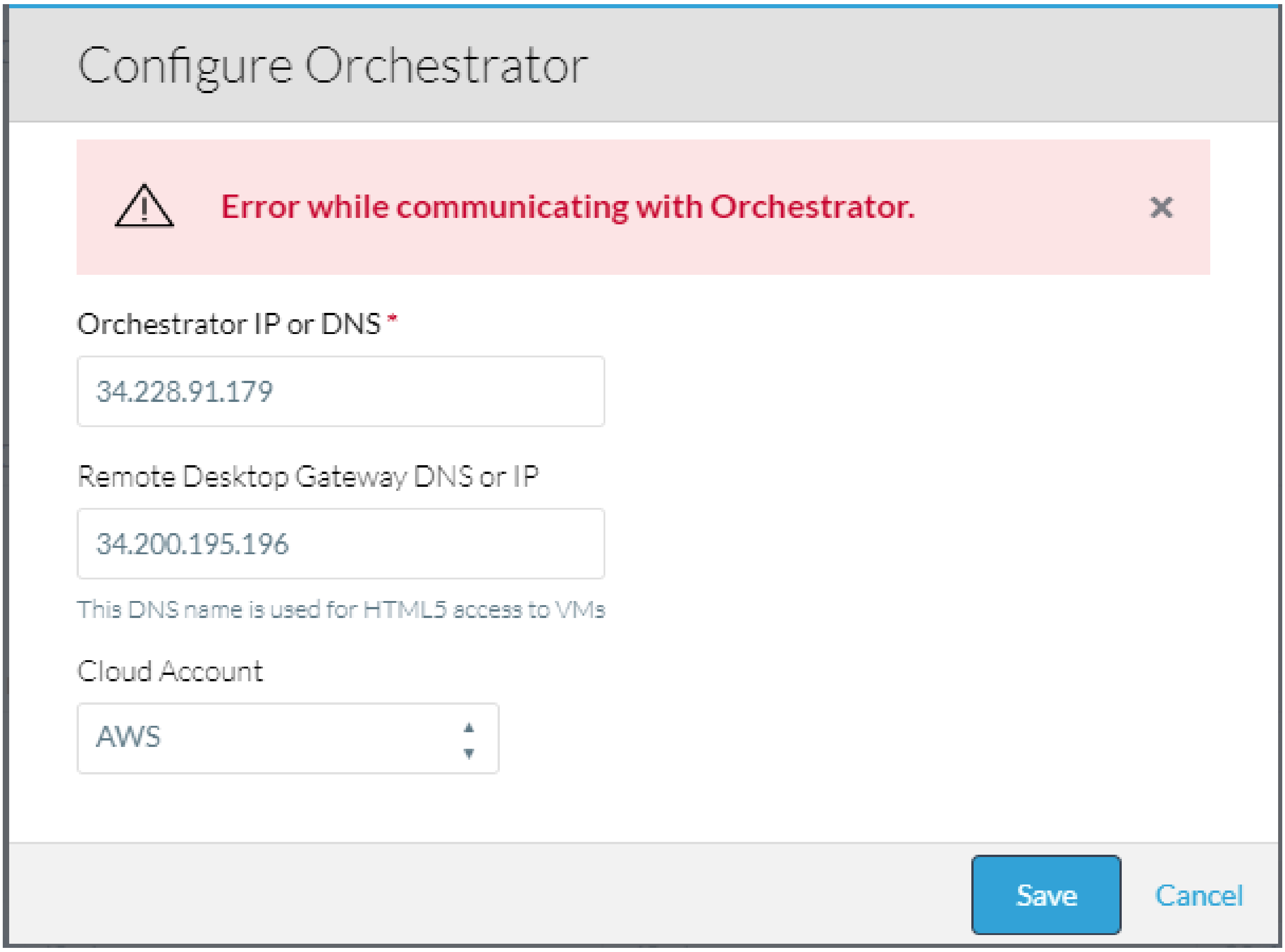
Components Used

The information in this document is based on 4.8.0+.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problem

When you configure the Orchestrator, you receive an error message "Error while communicating with Orchestrator." as shown in the image.



Configure Orchestrator

Error while communicating with Orchestrator.

Orchestrator IP or DNS *

34.228.91.179

Remote Desktop Gateway DNS or IP

34.200.195.196

This DNS name is used for HTML5 access to VMs

Cloud Account

AWS

When you review the osmosix log on the CCM this error is present.

```
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
```

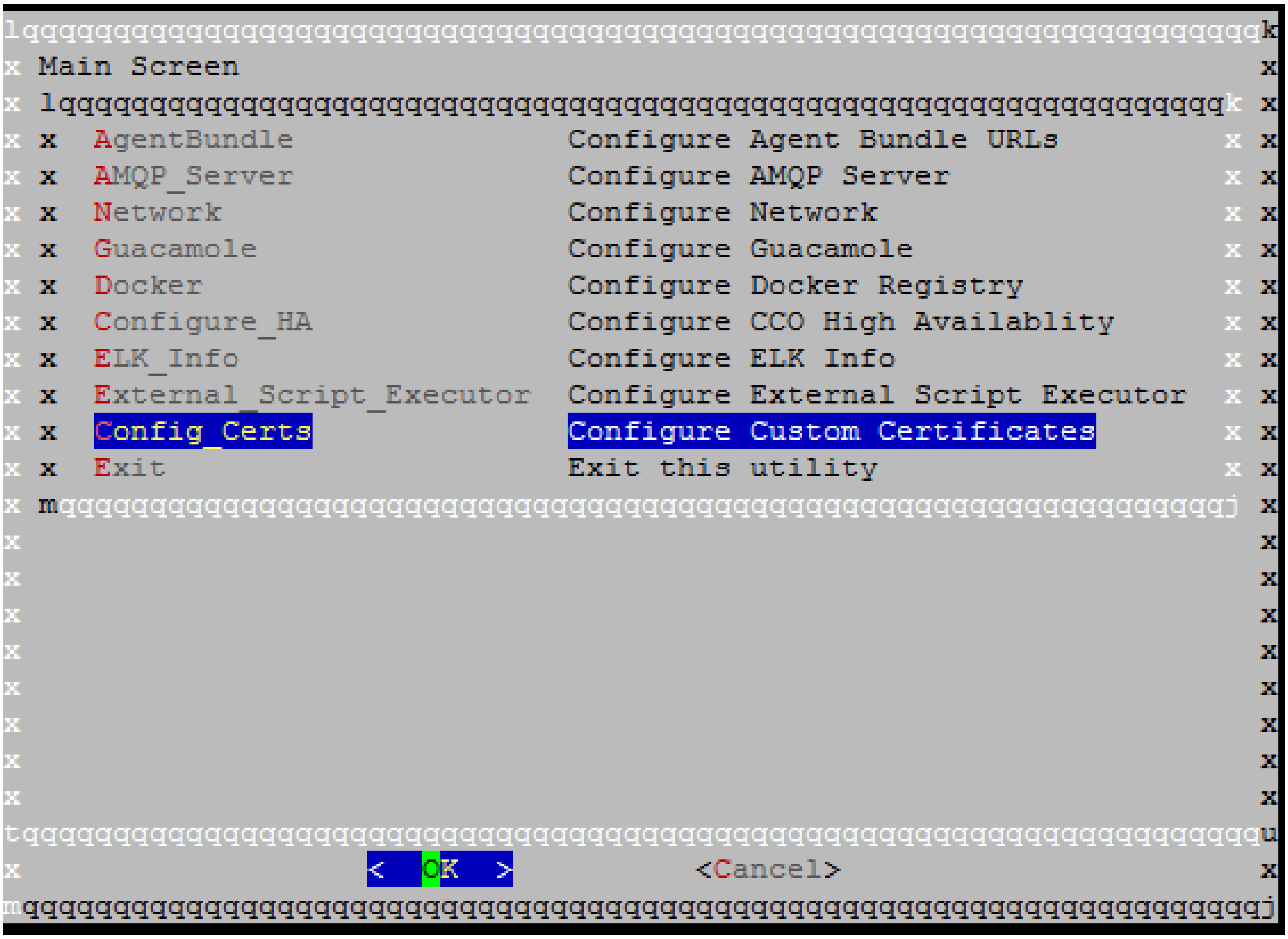
Solution

This is caused by a certificate mismatch between the CCO and the CCM.

If the certificates on the CCM were created with the use of the CCM configuration wizard perform these steps:

Step 1. Copy the **certs.zip** folder that was made in the**/tmp** directory of the CCM to the CCO and enter the CCO configuration wizard located at **/usr/local/cliqr/bin/cco_config_wizard.sh**.

Step 2. Select **Config_Certs** as shown in the image.



```
Main Screen
   AgentBundle               Configure Agent Bundle URLs
   AMQP_Server               Configure AMQP Server
   Network                   Configure Network
   Guacamole                 Configure Guacamole
   Docker                    Configure Docker Registry
   Configure_HA              Configure CCO High Availablity
   ELK_Info                  Configure ELK Info
   External_Script_Executor  Configure External Script Executor
   Config_Certs              Configure Custom Certificates
   Exit                      Exit this utility

                    <  OK  >          <Cancel>
```

Step 3. Type in the path to the certs.zip folder.

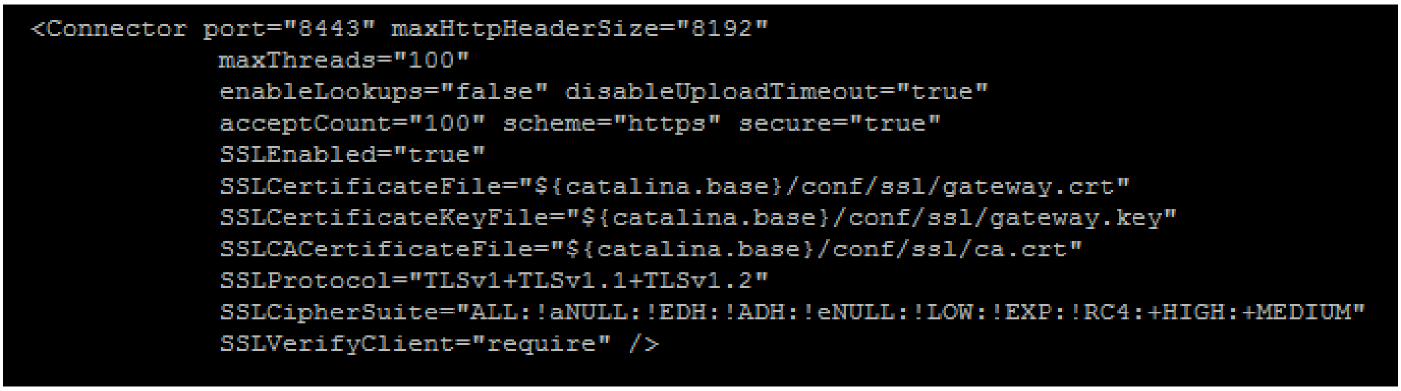
This automatically copies the relevant certificates and update the necessary file to point to them.

If you have manually created the CCM certificate then perform these steps:

Step 1. Copy the CCM's certificate, key, and the certificate authority's certificate to the CCO and place them in the **/usr/local/tomcat/conf/ssl/** directory.

Step 2. Update **/usr/local/tomcat/conf/server.xml**.

- Locate the section that starts with **<Connector port="8443" maxHttpHeaderSize="8192"** .
- Update the **SSLCertificateFile**, **SSLCertificateKeyFile**, and **SSLCACertificateFile** to point to the new files you copied over as shown in the 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" />
```

Step 3. In order to restart the server, run the command **service tomcat stop**, followed by **service tomcat start**.

Connectivity between the CCM and CCO must now be possible.