Es konnte kein gültiger Zertifizierungspfad für das angeforderte Ziel gefunden werden, wenn Sie CCO hinzufügen.

Inhalt

Einführung

In diesem Dokument wird ein Fehler beschrieben, der nach der Konfiguration benutzerdefinierter Zertifikate im CloudCenter Manager (CCM) beim Einrichten eines neuen CloudCenter Orchestrator (CCO) angezeigt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Linux
- Zertifikate

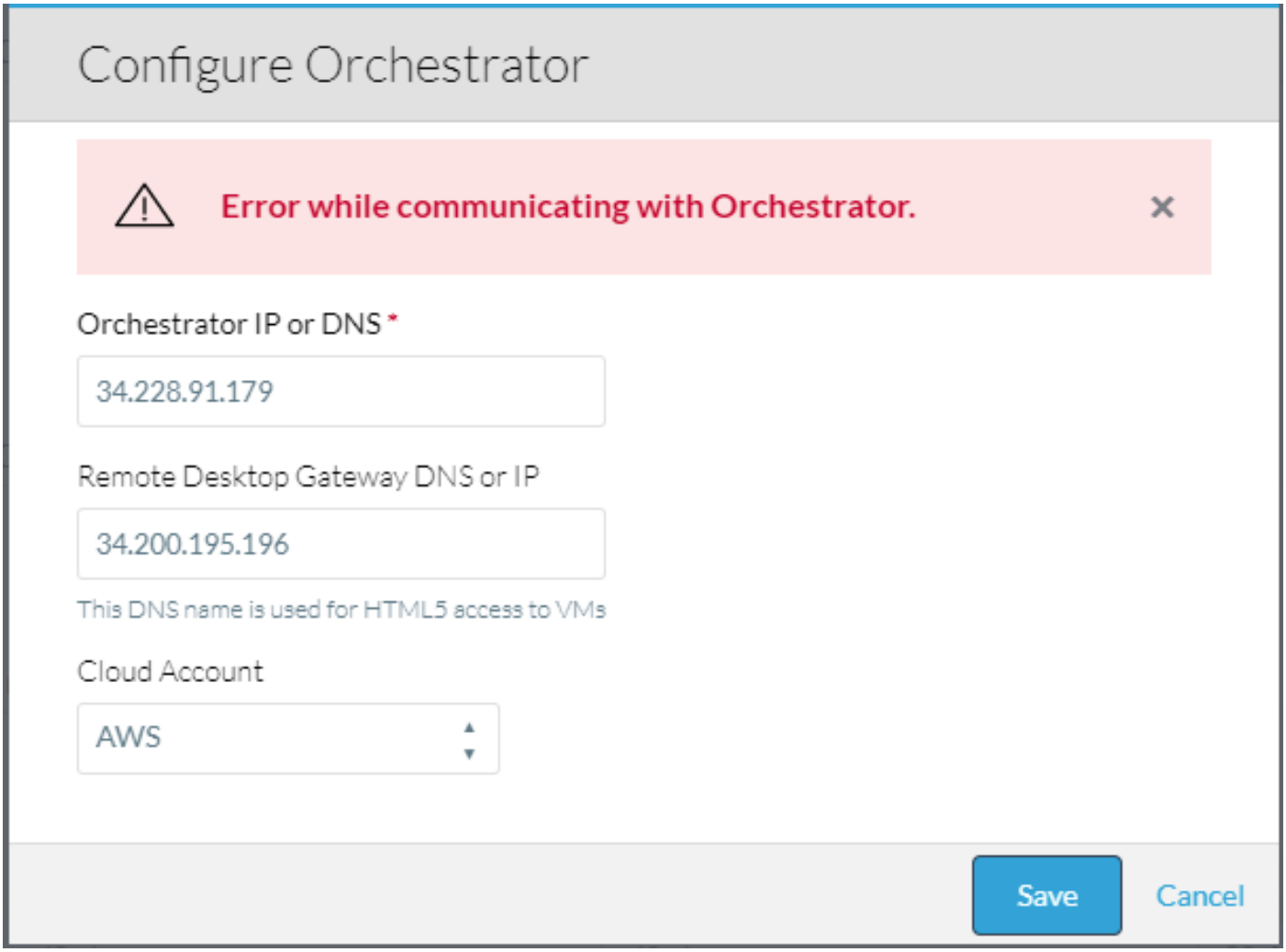
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Version 4.8.0+.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Wenn Sie den Orchestrator konfigurieren, erhalten Sie die Fehlermeldung "Fehler bei der Kommunikation mit dem Orchestrator". wie im Bild gezeigt.



Wenn Sie das Osmoseprotokoll im CCM überprüfen, tritt dieser Fehler auf.

```
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
```

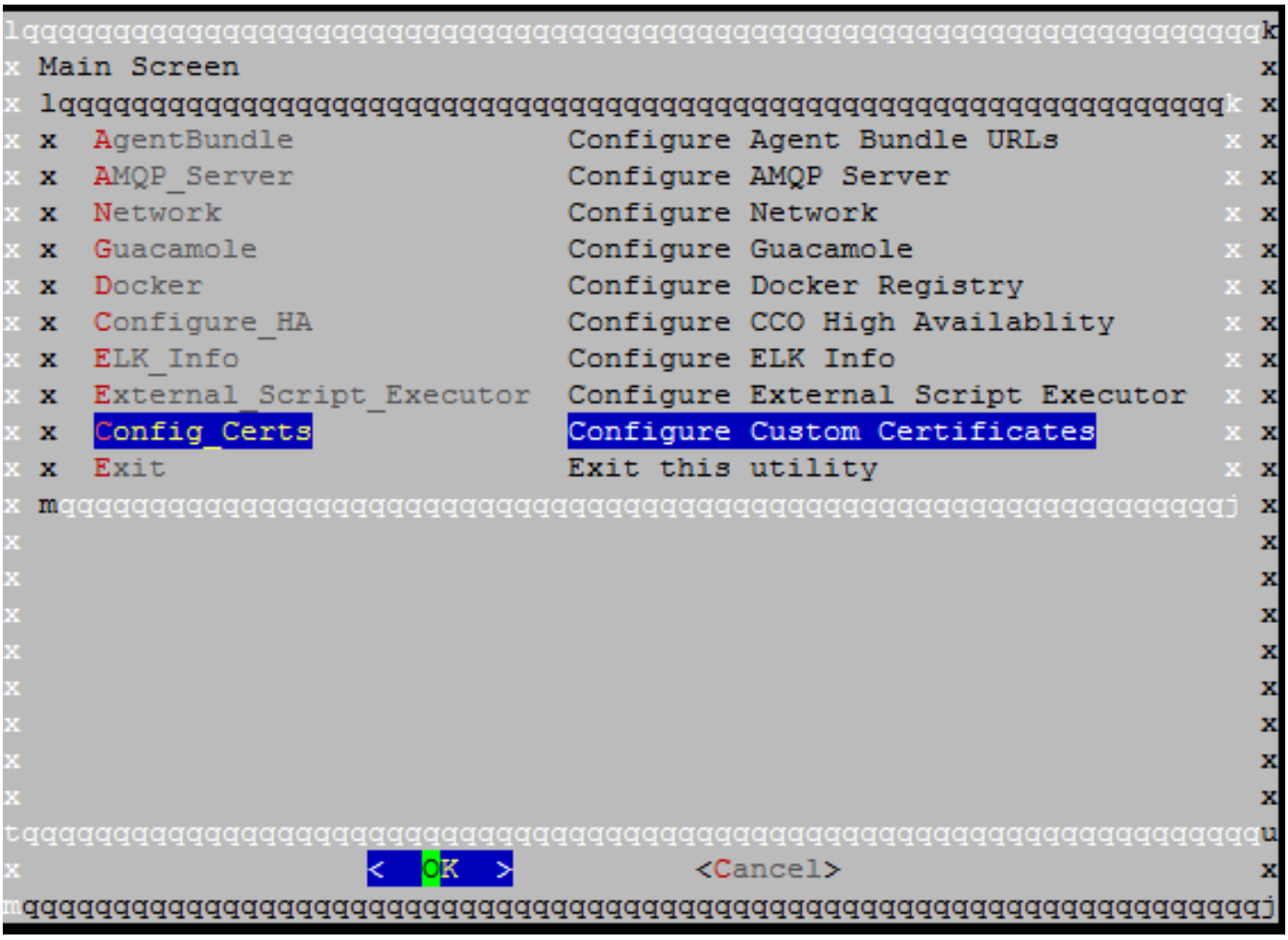
Lösung

Dies ist auf eine Zertifikatungleichheit zwischen CCO und CCM zurückzuführen.

Wenn die Zertifikate im CCM mithilfe des CCM-Konfigurationsassistenten erstellt wurden, führen Sie die folgenden Schritte aus:

Schritt 1: Kopieren Sie den Ordner **certs.zip**, der im Verzeichnis**/tmp** des CCM erstellt wurde, in das CCO-Verzeichnis, und geben Sie den CCO-Konfigurationsassistenten ein, der sich unter **/usr/local/cliqr/bin/cco_config_wizard.sh** befindet.

Schritt 2: Wählen Sie **Config_Certs** wie im Bild gezeigt aus.



Schritt 3: Geben Sie den Pfad zum Ordner certs.zip ein.

Damit werden automatisch die entsprechenden Zertifikate kopiert und die notwendige Datei aktualisiert, um auf sie zu verweisen.

Wenn Sie das CCM-Zertifikat manuell erstellt haben, führen Sie die folgenden Schritte aus:

Schritt 1: Kopieren Sie das Zertifikat, den Schlüssel und das Zertifikat der Zertifizierungsstelle in das CCO und platzieren Sie es im **/usr/local/tomcat/conf/ssl/**verzeichnis.

Schritt 2: Aktualisieren Sie **/usr/local/tomcat/conf/server.xml**.

- Suchen Sie nach dem Abschnitt, der mit **<Connector port="8443" maxHttpHeaderSize="8192"** beginnt.
- Aktualisieren Sie die **Datei SSLCertificateFile**, **SSLCertificateKeyFile** und **SSLCACertificateFile**, um auf die neuen Dateien zu zeigen, die Sie wie im Bild kopiert haben.

```
<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" />
```

Schritt 3: Um den Server neu zu starten, führen Sie den Befehl **service tomcat stop aus**, gefolgt von **service tomcat start**.

Eine Verbindung zwischen CCM und CCO muss jetzt möglich sein.