Impossibile trovare un percorso di certificazione valido per la destinazione richiesta quando si aggiunge CCO

Sommario

Introduzione

Questo documento descrive un errore che è possibile ricevere quando si configura un nuovo CloudCenter Orchestrator (CCO) dopo la configurazione dei certificati personalizzati su CloudCenter Manager (CCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Linux
- Certificati

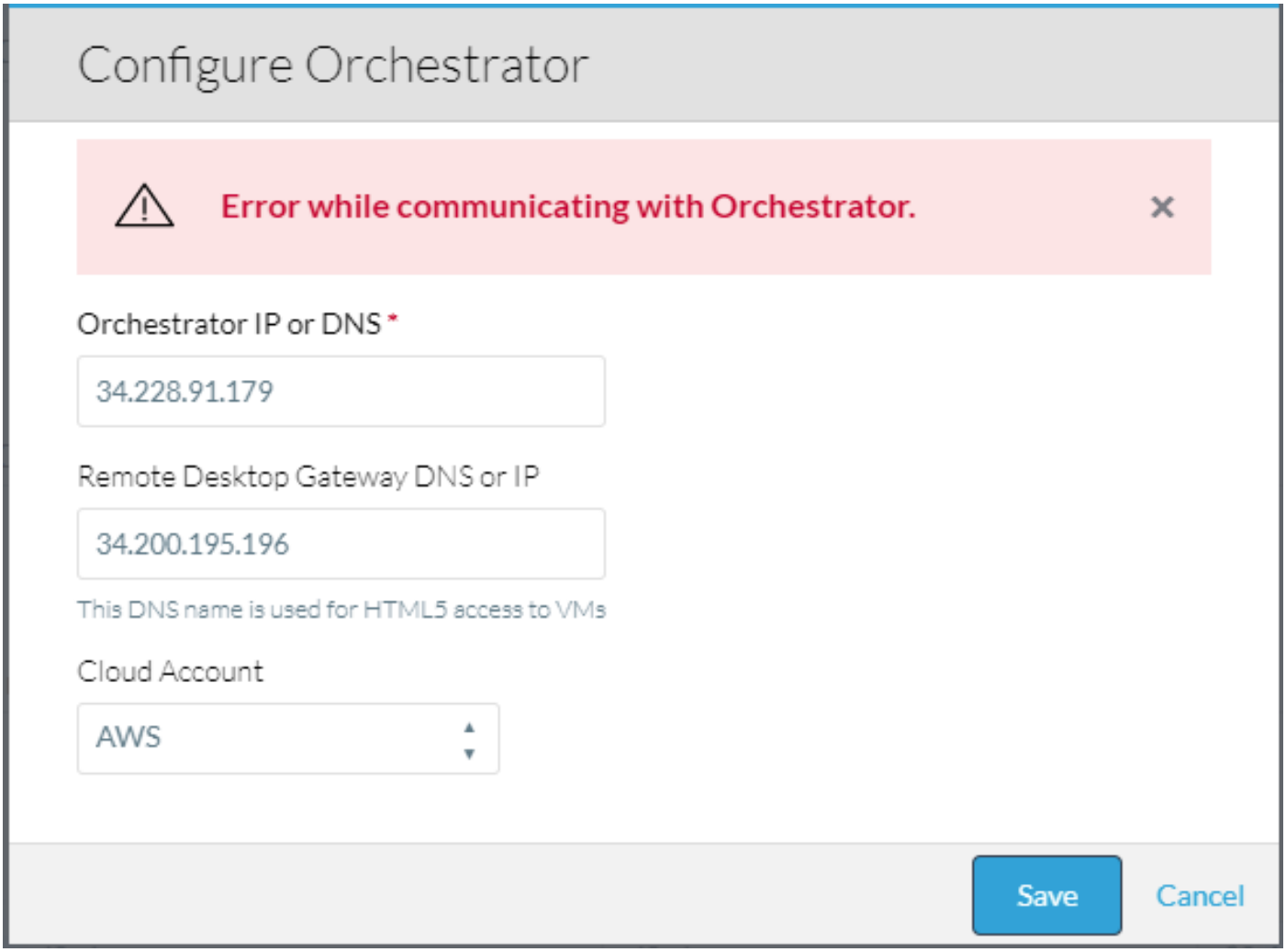
Componenti usati

Le informazioni di questo documento si basano sulla versione 4.8.0+.

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

Quando si configura Orchestrator, viene visualizzato il messaggio di errore "Errore durante la comunicazione con Orchestrator". come mostrato nell'immagine.



Questo errore si verifica quando si controlla il log osmosix su CCM.

```
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
```

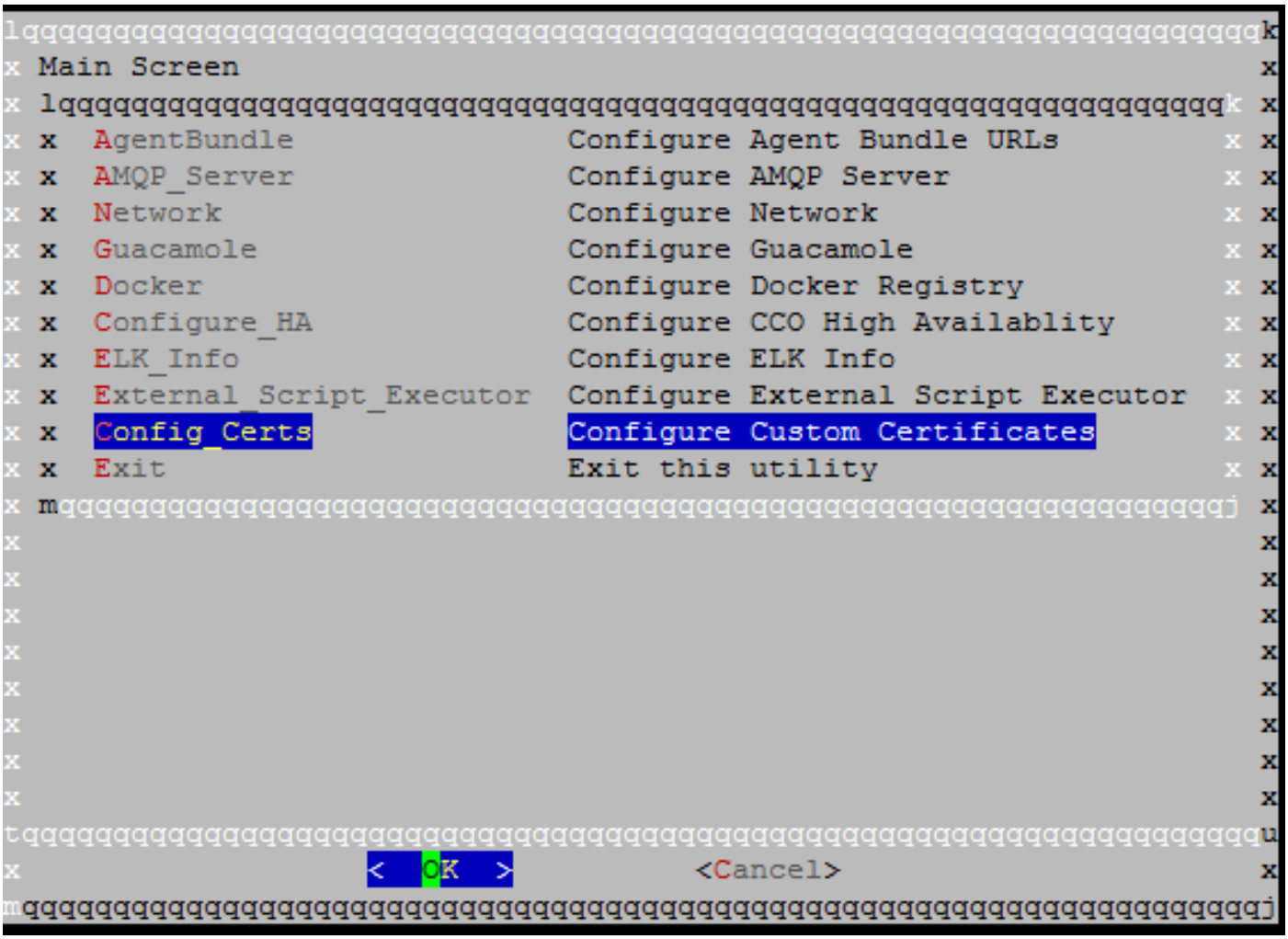
Soluzione

Ciò è causato da una mancata corrispondenza tra il CCO e il CCM.

Se i certificati nel modulo CCM sono stati creati utilizzando la Configurazione guidata CCM, eseguire i passaggi seguenti:

Passaggio 1. Copiare la cartella **certs.zip** creata nella directory**/tmp** di CCM in CCO e accedere alla configurazione guidata CCO disponibile in **/usr/local/cliqr/bin/cco_config_wizard.sh**.

Passaggio 2. Selezionare **Config_Certs** come mostrato nell'immagine.



Passaggio 3. Digitare il percorso della cartella certs.zip.

In questo modo i certificati pertinenti vengono copiati automaticamente e il file necessario viene aggiornato in modo da farvi riferimento.

Se il certificato CCM è stato creato manualmente, effettuare le seguenti operazioni:

Passaggio 1. Copiare il certificato, la chiave e il certificato dell'autorità di certificazione nel CCO e inserirli nella directory **/usr/local/tomcat/conf/ssl/**.

Passaggio 2. Aggiornare **/usr/local/tomcat/conf/server.xml**.

- Individuare la sezione che inizia con **<Connector port="8443" maxHttpHeaderSize="8192"** .
- Aggiornare **SSLCertificateFile**, **SSLCertificateKeyFile** e **SSLCACertificateFile** in modo che puntino ai nuovi file copiati, come mostrato nell'immagine.

```
<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" />
```

Passaggio 3. Per riavviare il server, eseguire il comando **service tomcat stop**, quindi **service tomcat start**.

La connettività tra CCM e CCO deve ora essere possibile.