

# Incapaz de encontrar o caminho de certificação válido ao alvo pedido quando você adicionar o CCO

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução](#)

## Introdução

Este documento descreve um erro que você pode receber quando você estabelece um Orchestrator novo de CloudCenter (CCO) após a configuração de Certificados feitos sob encomenda no gerente de CloudCenter (CCM).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Linux
- Certificados

### Componentes Utilizados

A informação neste documento é baseada em 4.8.0+.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Problema

Quando você configura o Orchestrator, você recebe um Mensagem de Erro “erro ao se comunicar com o Orchestrator.” segundo as indicações da imagem.

## 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

Save

Cancel

Quando você revê o fazer login do osmosix o CCM este erro esta 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.ValidatorException: 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.ValidatorException: 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
```

## Solução

Isto é causado por uma má combinação do certificado entre o CCO e o CCM.



```
<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" />
```

Etapa 3. A fim reiniciar o server, execute a **parada de TomCat** do comando service, seguida pelo **começo de TomCat** do serviço.

A Conectividade entre o CCM e o CCO deve agora ser possível.