

Resuelva problemas el CVP que señala a servidor el estado inalcanzable en OAMP debido a la discordancia de la configuración de SSL

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Descripción de problemas](#)

[Análisis del registro](#)

[Procedimiento](#)

[Solución](#)

Introducción

Este documento describe cómo resolver problemas el estado inalcanzable (CVP) del servidor porta de la información de la Voz de cliente de Cisco en las operaciones y la consola de administración (OAMP) debido a una discrepancia de configuración de Secure Sockets Layer (SSL)

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración del CVP
- SSL

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CVP 11.0(1)
- CVP OAMP

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 su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Descripción de problemas

En un CVP deployment, el CVP que señala el servidor se agrega al CVP OAMP. En el CVP que señala el servidor, el **CVP CallServer de Cisco** del servicio está en el **estado de ejecución**. Sin embargo, el CVP que señala el servidor está en el estado **inalcanzable** en el CVP OAMP debido a una discordancia para la configuración de SSL.

Análisis del registro

Esto es un snippet de los registros OAMP recogidos del directorio del servidor **C:\Cisco\CVP\OAMP** OAMP.

```
843: 10.203.72.28: Nov 03 2017 03:12:43.803 -0700: %CVP_11_0_OAMP-3-  
OAMP_OMGR_JMX_CONNECTION_ERROR: Unable to establish JMX connector to URI  
service:jmx:rmi:///jndi/rmi://10.203.72.27:2099/jmxrmi: error during JRMP connection  
establishment; 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 [id:7513]
```

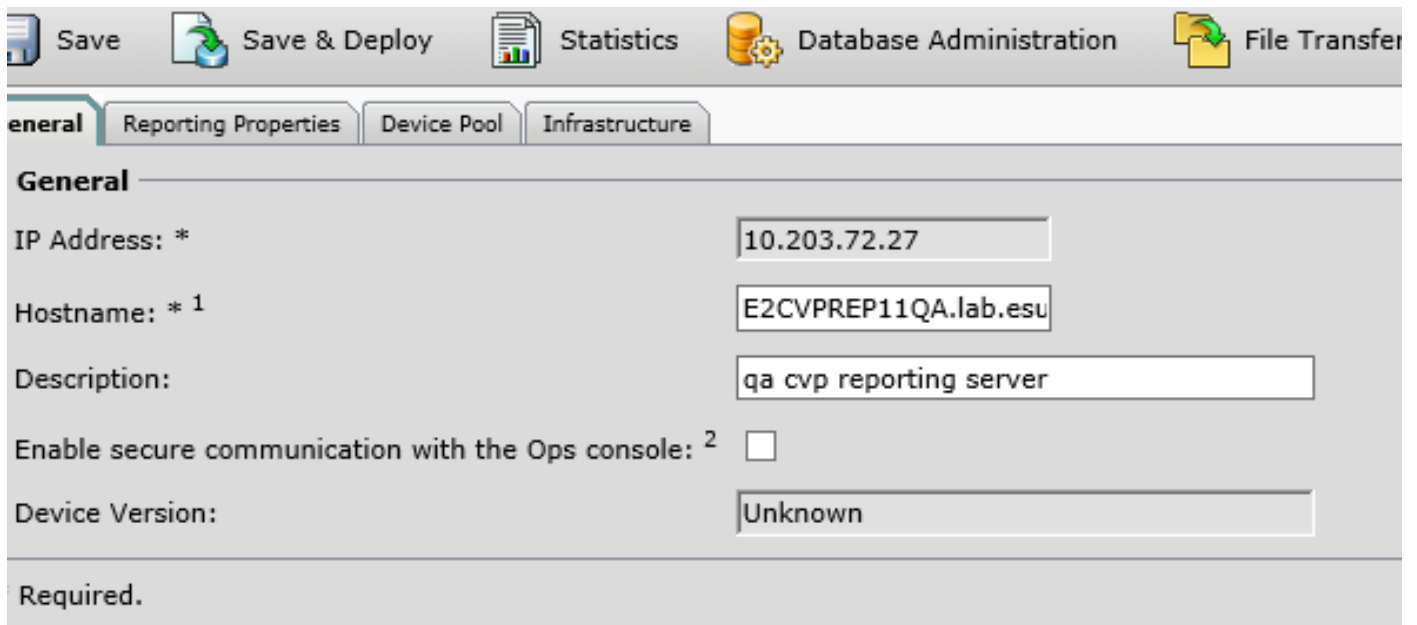
```
848: 10.203.72.28: Nov 03 2017 03:12:43.819 -0700: %CVP_11_0_OAMP-3-  
OAMP_OWEB_FORWARD_DEVICE_EXCEPTION_ERROR: An unexpected exception occurred during operation  
Save&Deploy (Device name: E2CVPREP11QA.lab.esurance.com | Managed address: 10.203.72.27 | Device  
type: Unified CVP Reporting Server): com.cisco.cvp.oamp.omgr.exception.MgmtException: JMX  
connection failed: uri=service:jmx:rmi:///jndi/rmi://10.203.72.27:2099/jmxrmi,rmiTimeout=10
```

Procedimiento

Paso 1. Marque que el SSL está fijado para verdad en el archivo orm_jmx.properties (el %CVP_HOME% \ conf \ orm_jmx.properties) en el CVP que señala el servidor.

```
Javax.net.debug = all  
  
com.sun.management.jmxremote.ssl.need.client.auth = false  
  
com.sun.management.jmxremote.authenticate = false  
  
com.sun.management.jmxremote.port = 2099  
  
com.sun.management.jmxremote.ssl = true
```

Paso 2. En OAMP, el control que habiliten comunicación segura con la consola del ops no se habilita en el CVP que señala el servidor, tal y como se muestra en de la imagen.



Solución

Paso 1. Pare el servicio del administrador de recursos de las operaciones (ORM) en el CVP que señala el servidor.

Paso 2. Edite el archivo del `%CVP_HOME%\conf\orm_jmx.properties` y cambie el valor `com.sun.management.jmxremote.sslproperty` de verdad a falso,

salve y cierre el archivo.

Paso 3. Comience el servicio ORM.

Paso 4. Navegue al OAMP, y edite el CVP respectivo que señala la Configuración del servidor para asegurarse de que el checkbox de la **Seguridad** en la **ficha general** está desmarcado. Entonces, **Save&Deploy** selecto.

Esto debe solucionar el problema y después de que 1 a 2 anote el OAMP debe reflejar el estado correcto del CVP que señala el servidor.