Solucionar problemas de servicios de IM&P mostrados como "desconocidos" en la topología de presencia

Contenido

Introducción

Este documento describe cómo resolver problemas de la página Topología de presencia cuando muestra los servicios como Desconocido en los nodos del servidor de Mensajería instantánea y presencia (IM&P).

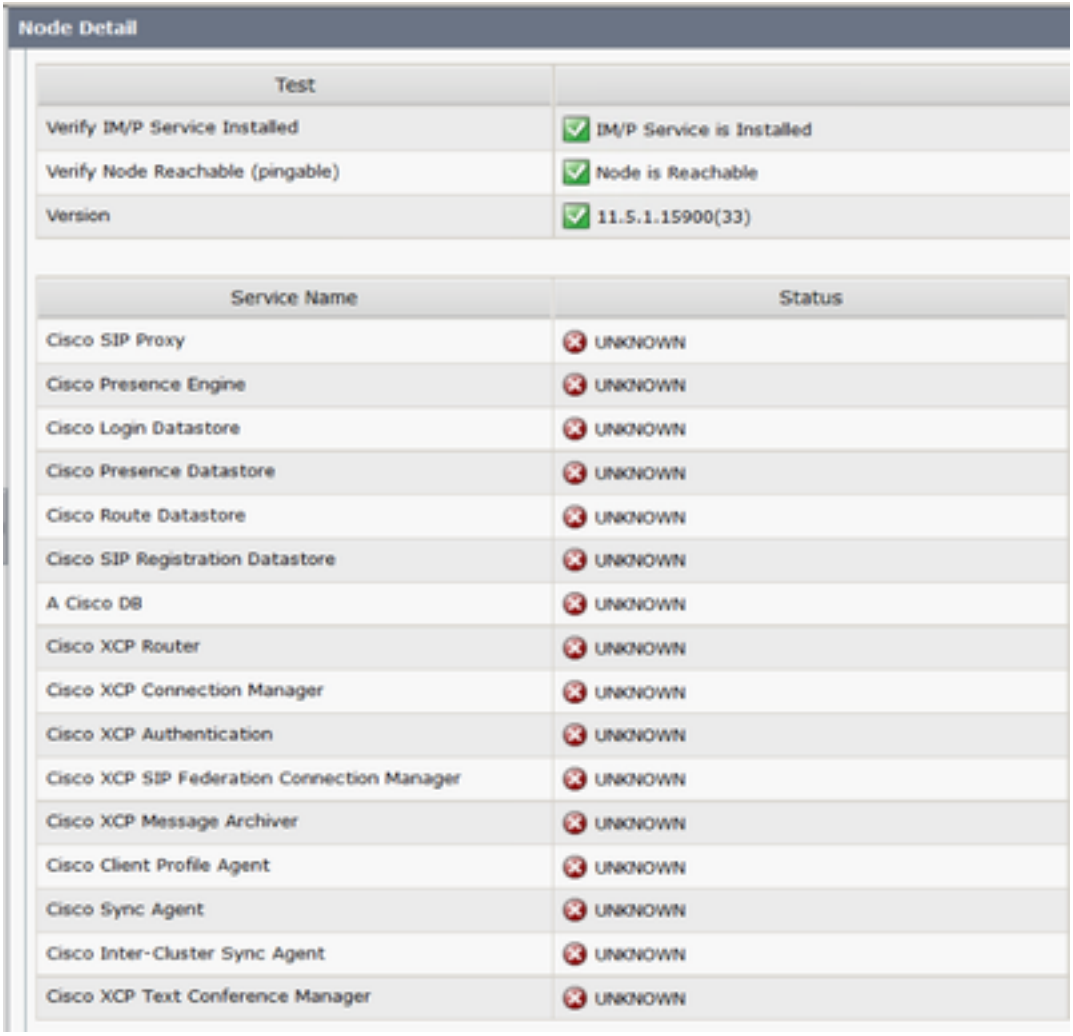
Antecedentes

Cuando navega a la **página Web de IM&P Administration > System > Presence Topology** para verificar el estado del servidor, puede encontrar que el servidor no está en su estado correcto. En este caso, el servidor muestra una cruz blanca dentro de un círculo rojo, aunque los servicios se inicien como se muestra en la interfaz de línea de comandos (CLI) mediante el comando **utils service list**.

En este documento se describen las razones más comunes por las que se muestran estos errores en la página web de topología de presencia y cómo corregirlos.

Problema

Cuando elige **view** en uno de los nodos afectados, puede ver estos errores en la página web: el estado de los servicios es **desconocido**:



Node Detail

Test	
Verify IM/P Service Installed	IM/P Service is Installed
Verify Node Reachable (pingable)	Node is Reachable
Version	11.5.1.15900(33)

Service Name	Status
Cisco SIP Proxy	UNKNOWN
Cisco Presence Engine	UNKNOWN
Cisco Login Datastore	UNKNOWN
Cisco Presence Datastore	UNKNOWN
Cisco Route Datastore	UNKNOWN
Cisco SIP Registration Datastore	UNKNOWN
A Cisco DB	UNKNOWN
Cisco XCP Router	UNKNOWN
Cisco XCP Connection Manager	UNKNOWN
Cisco XCP Authentication	UNKNOWN
Cisco XCP SIP Federation Connection Manager	UNKNOWN
Cisco XCP Message Archiver	UNKNOWN
Cisco Client Profile Agent	UNKNOWN
Cisco Sync Agent	UNKNOWN
Cisco Inter-Cluster Sync Agent	UNKNOWN
Cisco XCP Text Conference Manager	UNKNOWN

Sin embargo, si accede a la sesión Secure Shell (SSH) de CLI del servidor IM&P y ejecuta el comando: **utils service list**, verá que todos esos servicios están en realidad en el estado "INICIADO".

```
>> Return code = 0
A Cisco DB[STARTED]
A Cisco DB Replicator[STARTED]
Cisco AMC Service[STARTED]
Cisco AXL Web Service[STARTED]
Cisco Audit Event Service[STARTED]
Cisco Bulk Provisioning Service[STARTED]
Cisco CDP[STARTED]
Cisco CDP Agent[STARTED]
Cisco CallManager Serviceability[STARTED]
Cisco CallManager Serviceability RTMT[STARTED]
Cisco Certificate Expiry Monitor[STARTED]
Cisco Client Profile Agent[STARTED]
Cisco Config Agent[STARTED]
Cisco DRF Local[STARTED]
Cisco Database Layer Monitor[STARTED]
Cisco IM and Presence Admin[STARTED]
Cisco IM and Presence Data Monitor[STARTED]
Cisco Intercluster Sync Agent[STARTED]
Cisco Log Partition Monitoring Tool[STARTED]
Cisco Login Datastore[STARTED]
Cisco Management Agent Service[STARTED]
Cisco OAM Agent[STARTED]
Cisco Presence Datastore[STARTED]
Cisco Presence Engine[STARTED]
Cisco RCC Device Selection Service[STARTED]
Cisco RIS Data Collector[STARTED]
Cisco RTMT Reporter Servlet[STARTED]
Cisco Route Datastore[STARTED]
Cisco SIP Proxy[STARTED]
Cisco SIP Registration Datastore[STARTED]
Cisco Server Recovery Manager[STARTED]
Cisco Sync Agent[STARTED]
Cisco Syslog Agent[STARTED]
Cisco Tomcat[STARTED]
Cisco Tomcat Stats Servlet[STARTED]
Cisco Trace Collection Service[STARTED]
Cisco Trace Collection Servlet[STARTED]
Cisco XCP Authentication Service[STARTED]
Cisco XCP Config Manager[STARTED]
Cisco XCP Connection Manager[STARTED]
Cisco XCP Message Archiver[STARTED]
Cisco XCP Router[STARTED]
```

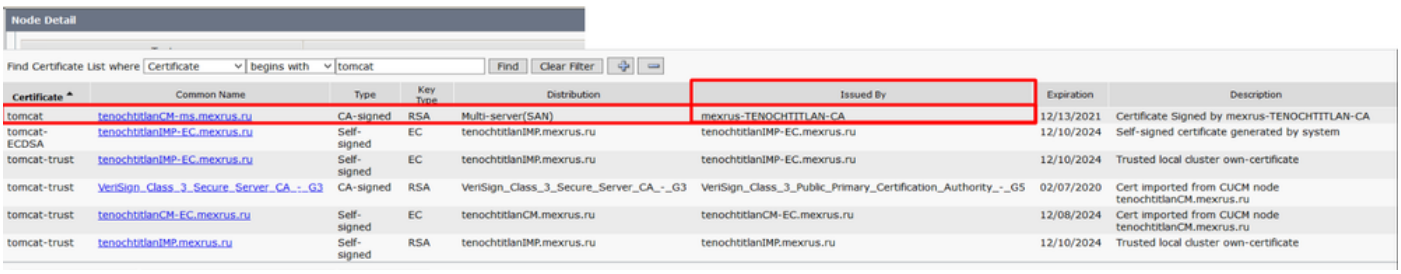
Solución

El error en la GUI está asociado con un problema de certificado de Tomcat. Esto es lo que se requiere verificar:

Paso 1. Asegúrese de que todos sus certificados **Tomcat** y **Tomcat-trust** no hayan caducado; de lo contrario, es necesario volver a generarlos.

Paso 2. Si su servidor utiliza certificados firmados por CA, debe validar que la cadena Tomcat completa está completa. Esto significa que los certificados intermedios y raíz deben cargarse como Tomcat-trust.

Este es un ejemplo de certificado faltante en la cadena Tomcat. En este caso, la cadena de certificados de Tomcat consta de solo dos certificados: Raíz > Hoja, sin embargo, hay escenarios donde más de 2 o 3 certificados intermedios construyen la cadena.


Node Detail

Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	tenochtitlanCM-ms.mexrus.ru	CA-signed	RSA	Multi-server(SAN)	mexrus-TENOCHTITLAN-CA	12/13/2021	Certificate Signed by mexrus-TENOCHTITLAN-CA
tomcat-ECDSA	tenochtitlanIMP-EC.mexrus.ru	Self-signed	EC	tenochtitlanIMP.mexrus.ru	tenochtitlanIMP-EC.mexrus.ru	12/10/2024	Self-signed certificate generated by system
tomcat-trust	tenochtitlanIMP-EC.mexrus.ru	Self-signed	EC	tenochtitlanIMP.mexrus.ru	tenochtitlanIMP-EC.mexrus.ru	12/10/2024	Trusted local cluster own-certificate
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	CA-signed	RSA	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/07/2020	Cert imported from CUCM node tenochtitlanCM.mexrus.ru
tomcat-trust	tenochtitlanCM-EC.mexrus.ru	Self-signed	EC	tenochtitlanCM.mexrus.ru	tenochtitlanCM-EC.mexrus.ru	12/08/2024	Cert imported from CUCM node tenochtitlanCM.mexrus.ru
tomcat-trust	tenochtitlanIMP.mexrus.ru	Self-signed	RSA	tenochtitlanIMP.mexrus.ru	tenochtitlanIMP.mexrus.ru	12/10/2024	Trusted local cluster own-certificate

En el ejemplo de la imagen, el emisor: **mexrus-TENOCHTITLAN-CA** falta el certificado.

Registros necesarios

Vaya a **IM and Presence Serviceability > Trace > Trace Configuration >** Server para seleccionar: **IM&P Publisher > Service Group > Database and Admin Services >** Service: **Cisco IM and Presence Admin** > Apply to all Nodes > Debug level: **Debug** > Marque la casilla de verificación **Enable All Trace > Save.**

Navegue hasta **IM and Presence Administration > System > Presence Topology >** Elija el nodo que se ve afectado por los servicios desconocidos y observe la marca de tiempo.

Abra la herramienta Cisco Real-Time Monitor Tool (RTMT) y recopile estos registros:

- Syslog de Cisco
- Tomcat de Cisco
- Seguridad Tomcat de Cisco
- Registros de aplicación del Visor de eventos
- Registros del sistema del visor de eventos
- Registros del administrador de Cisco IM and Presence

Qué se puede esperar de los registros

Desde cupadmin*.log

Cuando acceda al **panel Topología de presencia > Nodo.**

```
2021-01-23 17:54:57,036 DEBUG [Thread-137] logging.IMPCommonLogger - IMPSocketFactory: Create
socket called with host tenochtitlanIMP.mexrus.ru and port 8443
2021-01-23 17:54:57,040 DEBUG [Thread-137] logging.IMPCommonLogger - Enabled protocols:
[TLSv1.1, TLSv1, TLSv1.2]
```

Se recibió una excepción porque no se verificó un certificado.

```
2021-01-23 17:54:57,087 ERROR [Thread-137] services.ServiceUtil - Got an exception setting up
the HTTPS connection.
javax.net.ssl.SSLException: Certificate not verified.
at com.rsa.sslj.x.aH.b(Unknown Source)
at com.rsa.sslj.x.aH.a(Unknown Source)
at com.rsa.sslj.x.aH.a(Unknown Source)
at com.rsa.sslj.x.ap.c(Unknown Source)
at com.rsa.sslj.x.ap.a(Unknown Source)
at com.rsa.sslj.x.ap.j(Unknown Source)
at com.rsa.sslj.x.ap.i(Unknown Source)
at com.rsa.sslj.x.ap.h(Unknown Source)
at com.rsa.sslj.x.aS.startHandshake(Unknown Source)
at com.cisco.cup.services.ServiceUtil.init(ServiceUtil.java:118)
at com.cisco.cup.services.ServiceUtil.getServiceInfo(ServiceUtil.java:197)
at com.cisco.cup.services.ServiceUtil.getServiceInfo(ServiceUtil.java:182)
```

Cuando intenta recuperar el estado del nodo para la topología:

```
at
```

```
com.cisco.cup.admin.actions.TopologyNodeStatusAction$ServiceRunner.run(TopologyNodeStatusAction.
java:358)
at java.lang.Thread.run(Thread.java:748)
Caused by: com.rsa.sslj.x.aK: Certificate not verified.
at com.rsa.sslj.x.bg.a(Unknown Source)
at com.rsa.sslj.x.bg.a(Unknown Source)
at com.rsa.sslj.x.bg.a(Unknown Source)
... 13 more
```

Se ha producido una excepción debido a que falta el emisor del certificado Tomcat.

```
Caused by: java.security.cert.CertificateException: Issuer for signed certificate
[CN=tenochtitlanCM-ms.mexrus.ru,OU=Collab,O=Cisco,L=Mexico,ST=Mexico City,C=MX] not found:
CN=mexrus-TENOCHTITLAN-CA,DC=mexrus,DC=ru
at com.cisco.cup.security.TLSTrustManager.checkServerTrusted(TLSTrustManager.java:309)
at com.rsa.sslj.x.aE.a(Unknown Source)
... 16 more

2021-01-23 17:54:57,087 DEBUG [Thread-137] actions.TopologyNodeStatusAction$ServiceRunner -
Retrieved service status for node tenochtitlanIMP.mexrus.ru
2021-01-23 17:54:57,088 DEBUG [http-bio-443-exec-8] actions.TopologyNodeStatusAction -
[Topology] VerifyNodeServices - Complete.
```

Se puede encontrar otro tipo de excepción en los seguimientos de cupadmin*.log, que muestran el error "Emisor incorrecto para certificado de servidor":

```
Caused by: java.security.cert.CertificateException: Incorrect issuer for server cert
               at
com.cisco.cup.security.TLSTrustManager.checkServerTrusted(TLSTrustManager.java:226)
               at com.rsa.sslj.x.aE.a(Unknown Source)
               ... 16 more
2017-10-14 09:04:01,667 ERROR [Thread-125] services.ServiceUtil - Failed to retrieve service
status. Reason: Certificate not verified.
javax.net.ssl.SSLException: Certificate not verified.
```

En este caso, IM&P no reconoce el certificado de emisor para Tomcat como un certificado de emisor válido, lo que probablemente se deba a un certificado dañado. Las **opciones son:**

- Valide la información presentada en: Tomcat y certificados de emisor.
- Obtenga otro certificado de emisor y compárelo con el que ya se encuentra en IM&P Trust Store.
- Elimine el certificado del emisor del IM&P y cárguelo de nuevo.
- Regenere el certificado CA- de Tomcat.

> **Nota:** Tenga en cuenta que el Id. de bug Cisco CSCvu78005, que se refiere a que el Almacén de Llaves Tomcat RSA/ECDSA no se actualiza en todos los nodos cuando se reemplaza el certificado de CA existente en la cadena.

Paso 1. Ejecute el comando **utils diagnose test** en el nodo afectado.

Paso 2. Póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) para obtener más ayuda.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).