Solucionar problemas de serviços IM&P exibidos como "Desconhecidos" na topologia de presença

Contents

Introduction

Este documento descreve como solucionar problemas da página Topologia de Presença quando ela mostra os serviços como Desconhecido nos nós do servidor de Mensagem Instantânea e Presença (IM&P).

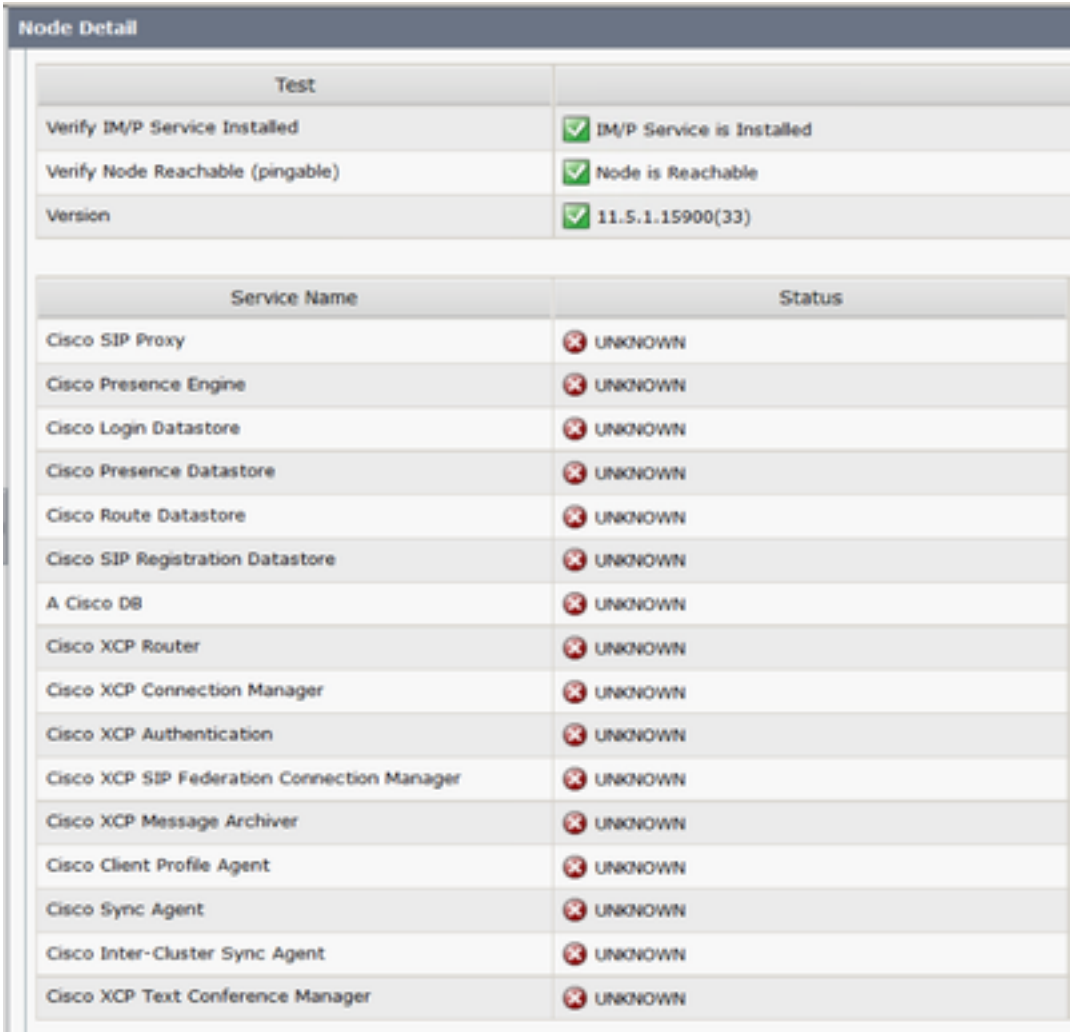
Informações de Apoio

Quando você navega até a **página da Web Administração de IM&P > Sistema > Topologia de Presença** para verificar o status de integridade do servidor, pode perceber que o servidor não está em seu estado correto. Nesse caso, o servidor mostra uma cruz branca dentro de um círculo vermelho, mesmo que os serviços sejam iniciados como mostrado na Interface de Linha de Comando (CLI) através do comando **utils service list**.

Este documento descreve os motivos mais comuns pelos quais esses erros são exibidos na página da Web Topologia de presença e como corrigi-los.

Problema

Ao escolher **exibir** em um dos nós afetados, você pode ver estes erros na página da Web: o status dos serviços é **desconhecido**:



No entanto, se você acessar a sessão Secure Shell (SSH) do CLI do Servidor IM&P e executar o comando: **lista de serviços do utils**, você verá que todos esses serviços estão realmente no 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]
```

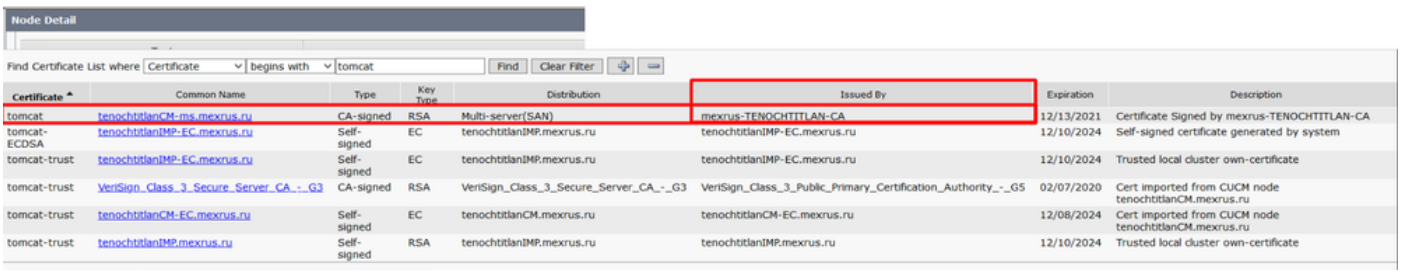
Solução

O erro na GUI está associado a um problema de certificado do Tomcat. Veja o que precisa ser verificado:

Etapa 1. Certifique-se de que todos os certificados **Tomcat** e **Tomcat-trust** não tenham expirado, caso contrário, eles precisam ser regenerados.

Etapa 2. Se o servidor usar certificados com assinatura CA, você precisará validar se toda a cadeia Tomcat está completa. Isso significa que os intermediários e os certificados raiz devem ser carregados como Tomcat-trust.

Aqui está um exemplo de um certificado ausente na cadeia Tomcat. Nesse caso, a cadeia de certificados do Tomcat consiste em apenas dois certificados: Raiz > Folha, no entanto, há cenários em que mais de 2 ou 3 certificados intermediários criam a cadeia.



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

No exemplo da imagem, o Emissor: **mexrus-TENOCHTITLAN-CA** está faltando o certificado.

Logs necessários

Navegue para **Serviço de IM e Presença > Rastrear > Rastrear Configuração >** Servidor para selecionar: **Editor do IM&P > Grupo de Serviços > Serviços de Banco de Dados e Administração >** Serviço: **Cisco IM and Presence Admin** > Aplicar a todos os nós > Nível de depuração: **Debug** > Check the **Enable All Trace** Checkbox > **Save.**

Navegue para **Administração de IM e Presença > Sistema > Topologia de Presença >** Escolha o nó afetado pelos serviços desconhecidos e observe o carimbo de data/hora.

Abra a Cisco Real-Time Monitor Tool (RTMT) e reúna estes registros:

- Cisco Syslog
- Cisco Tomcat
- Segurança Cisco Tomcat
- Logs do aplicativo Visualizador de Eventos
- Logs do sistema do Visualizador de Eventos
- Registros do Cisco IM e do Presence Admin

O que esperar nos registros

Do arquivo cupadmin*.log

Quando você acessa o **painel Topologia de presença > Nó.**

```
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]
```

Exceção recebida porque um certificado não foi verificado.

```
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)
```

Quando você tentar recuperar o Status do Nó para a topologia:

```
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
```

Uma exceção foi causada devido à ausência do emissor do 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.
```

Outro tipo de exceção pode ser encontrado nos rastreamentos do cupadmin*.log, que exibem o erro "Incorrect issuer for server cert":

```
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.
```

Nesse caso, o IM&P não reconhece o certificado do emissor do Tomcat como um certificado válido do emissor, que provavelmente foi causado devido a um certificado corrompido. As **opções aqui são:**

- Valide as informações apresentadas em ambos: Certificados do Tomcat e do emissor.
- Obtenha outro certificado do emissor e compare-o com o que já está no Repositório Confiável de IM&P.
- Excluir o certificado do emissor do IM&P e carregá-lo novamente.
- Gere novamente o certificado CA- do Tomcat.

> **Note**: Esteja ciente do bug da Cisco Id CSCvu78005, que se refere ao Tomcat RSA/ECDSA Keystore não é atualizado em todos os nós quando o certificado CA existente na cadeia é substituído.

Etapa 1. Execute o comando **utils diagnose test** no nó afetado.

Etapa 2. Entre em contato com o Cisco Technical Assistance Center (TAC) para obter assistência.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.