Dépannage des services IM&P affichés comme « Inconnus » dans la topologie de présence

Contenu

Introduction

Ce document décrit comment dépanner la page Topologie de présence lorsqu'elle affiche les services comme Inconnus sur les noeuds du serveur de messagerie instantanée et de présence (IM&P).

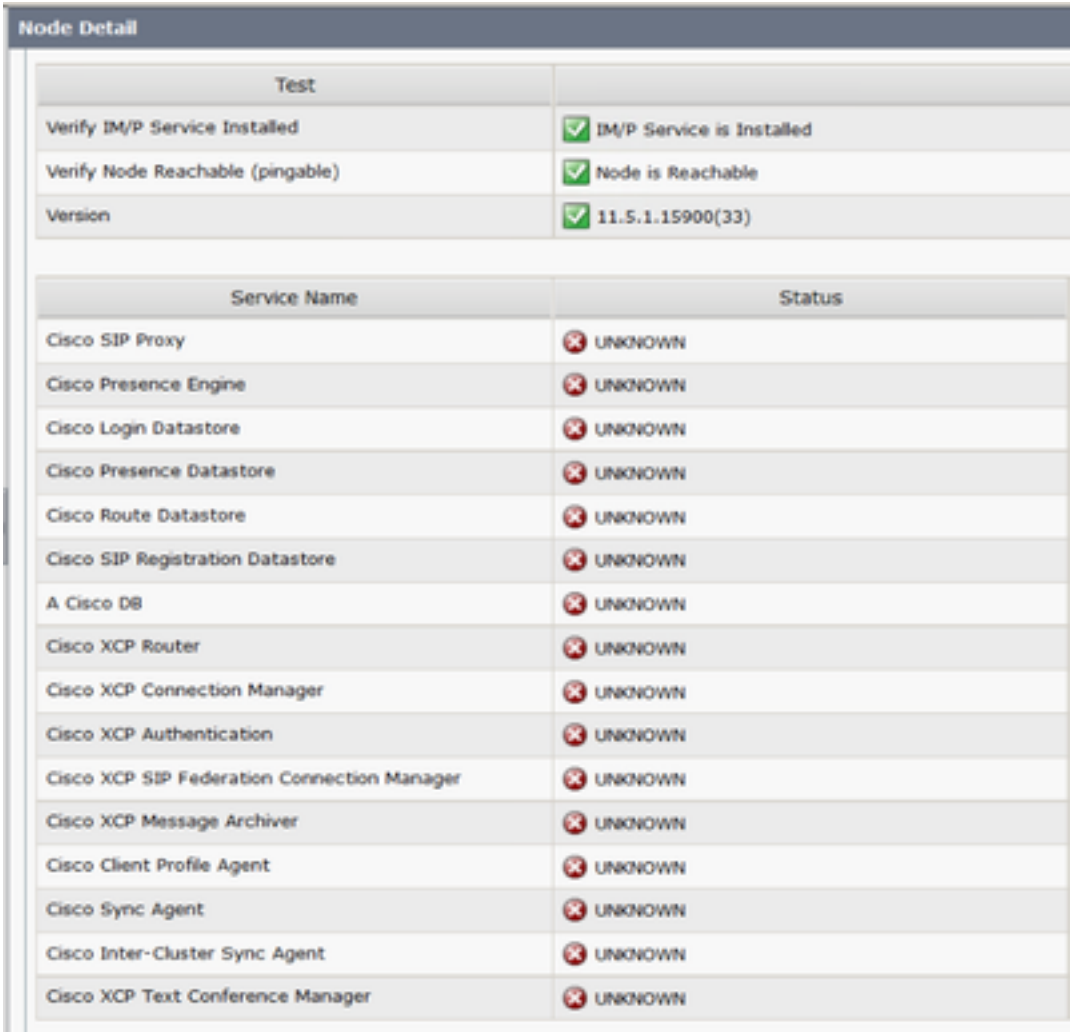
Informations générales

Lorsque vous accédez à la **page Web IM&P Administration > System > Presence Topology** pour vérifier l'état de santé du serveur, vous pouvez constater que le serveur n'est pas dans son état correct. Dans ce cas, le serveur affiche une croix blanche dans un cercle rouge, même si les services sont démarrés comme indiqué sur l'interface de ligne de commande (CLI) via la commande **utils service list**.

Ce document décrit les raisons les plus courantes pour lesquelles ces erreurs sont affichées sur la page Web Topologie de présence et comment les corriger.

Problème

Lorsque vous choisissez **view** sur l'un des noeuds affectés, vous pouvez voir ces erreurs sur la page Web : l'état des services est **inconnu** :



Cependant, si vous accédez à la session CLI Secure Shell (SSH) du serveur IM&P et exécutez la commande : **jusqu'à la liste des services**, vous voyez que tous ces services sont en fait à l'état "DÉMARRÉ".

```
>> 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]
```

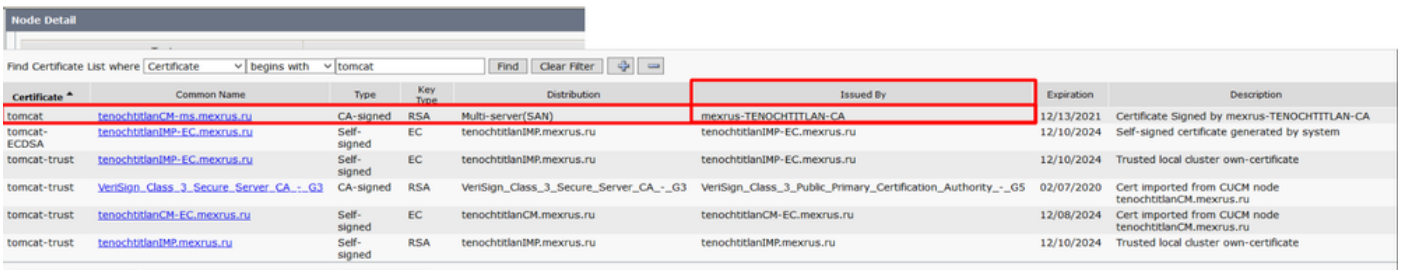
Solution

L'erreur sur l'interface utilisateur graphique est associée à un problème de certificat Tomcat. Voici ce qui doit être vérifié :

Étape 1. Assurez-vous que tous vos certificats **Tomcat** et **Tomcat-trust** n'ont pas expiré, sinon ils doivent être régénérés.

Étape 2. Si votre serveur utilise des certificats signés par une autorité de certification, vous devez vérifier que toute la chaîne Tomcat est terminée. Cela signifie que les certificats intermédiaires et racine doivent être téléchargés en tant que Tomcat-trust.

Voici un exemple de certificat manquant dans la chaîne Tomcat. Dans ce cas, la chaîne de certificats Tomcat se compose uniquement de deux certificats : Root > Leaf, cependant, il existe des scénarios où plus de 2 ou 3 certificats intermédiaires construisent la chaîne.


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

Dans l'exemple d'image, l'émetteur : **mexrus-TENOCHTITLAN-CA** est le certificat manquant.

Journaux requis

Accédez à **IM and Presence Serviceability > Trace > Trace Configuration >** Server pour sélectionner : **IM&P Publisher > Service Group > Database and Admin Services >** Service : **Cisco IM and Presence Admin >** Apply to all Nodes **>** Debug level : **Debug >** Cochez la case **Enable All Trace > Save.**

Accédez à **IM and Presence Administration > System > Presence Topology >** Choisissez le noeud qui est affecté par les services inconnus, et notez l'horodatage.

Ouvrez l'outil Cisco Real-Time Monitor Tool (RTMT) et collectez les journaux suivants :

- Cisco Syslog
- Cisco Tomcat
- Sécurité Cisco Tomcat
- Journaux des applications Observateur d'événements
- Journaux système de l'Observateur
- Journaux d'administration Cisco IM et Presence

Àquoi s'attendre dans les journaux

Àpartir du fichier cupadmin*.log

Lorsque vous accédez au **panneau Topologie de présence > Noeud.**

```
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]
```

Une exception a été reçue car un certificat n'a pas été vérifié.

```
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)
```

Lorsque vous tentez de récupérer l'état du noeud pour la topologie :

```
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
```

Une exception est provoquée en raison de l'émetteur manquant du certificat 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.
```

Un autre type d'exception se trouve sur les traces cupadmin*.log, qui affichent l'erreur "Émetteur incorrect pour certificat de serveur" :

```
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.
```

Dans ce cas, l'IM&P ne reconnaît pas le certificat d'émetteur du Tomcat comme un certificat d'émetteur valide, ce qui est probablement dû à un certificat endommagé. Les **options sont les suivantes :**

- Validez les informations présentées sur les deux éléments suivants : Certificats Tomcat et émetteur.
- Procurez-vous un autre certificat d'émetteur et comparez-le à celui qui figure déjà sur la boutique IM&P Trust.
- Supprimez le certificat de l'émetteur du MI&P et téléchargez-le à nouveau.
- Régénérez le certificat CA Tomcat.

> **Note**: Notez que le bogue Cisco portant l'ID CSCvu78005, qui fait référence au Keystore RSA/ECDSA Tomcat, ne se met pas à jour dans tous les noeuds lorsque le certificat CA existant dans la chaîne est remplacé.

Étape 1. Exécutez la commande **utils diagnose test** sur le noeud affecté.

Étape 2. Contactez le Centre d'assistance technique Cisco (TAC) pour obtenir de l'aide.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.