Fehlerbehebung bei IM&P-Services, die in der Presence-Topologie als "Unbekannt" angezeigt werden

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung auf der Seite "Presence Topology" (Anwesenheitstopologie) beschrieben, wenn die Services auf den IM&P-Serverknoten (Instant Message und Presence) als "Unbekannt" angezeigt werden.

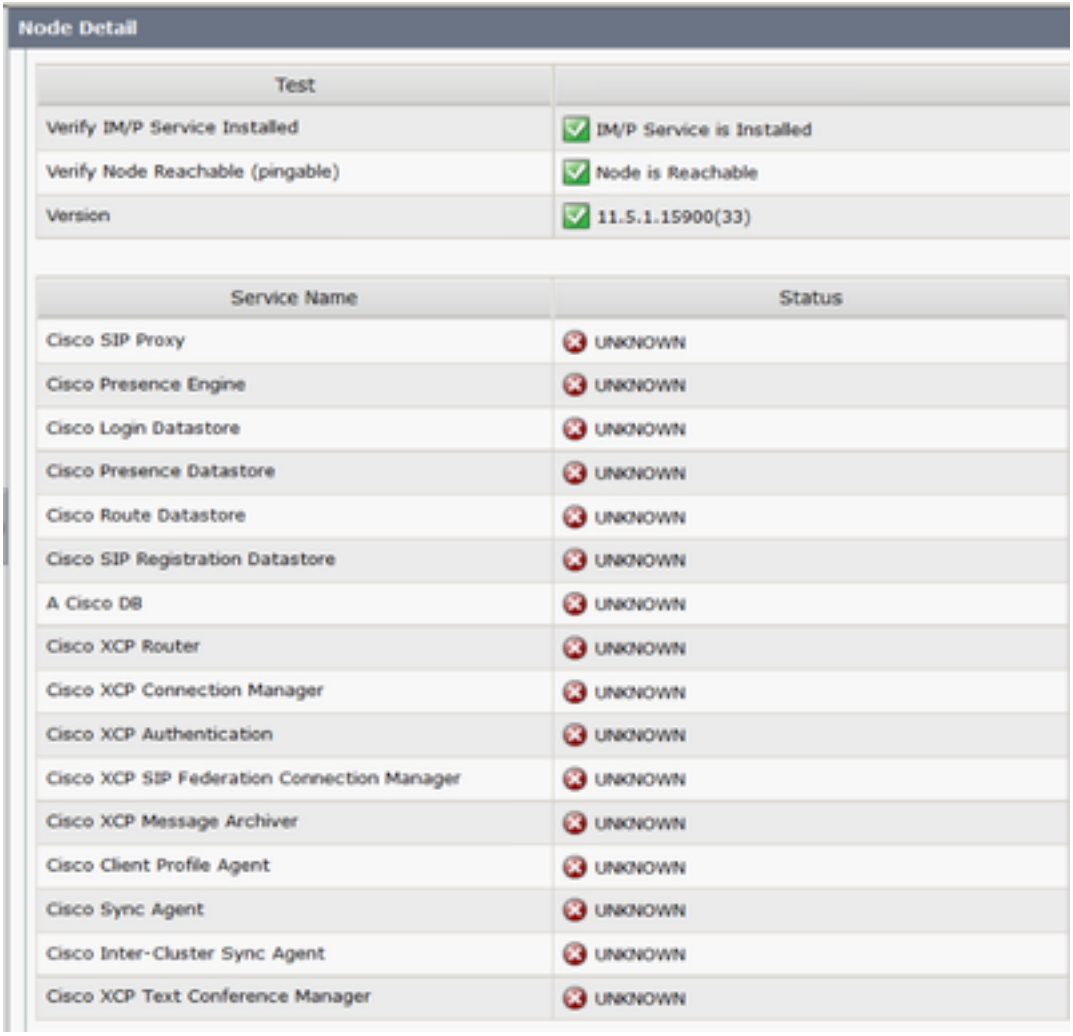
Hintergrundinformationen

Wenn Sie zur **Webseite IM&P-Administration > System > Presence Topology (System > Presence-Topologie)** navigieren, um den Zustand des Servers zu überprüfen, kann es sein, dass sich der Server nicht im richtigen Zustand befindet. In diesem Fall zeigt der Server ein weißes Kreuz innerhalb eines roten Kreises an, obwohl die Dienste gestartet werden, wie in der Befehlszeilenschnittstelle (CLI) über den Befehl **utils service list** angegeben.

In diesem Dokument werden die häufigsten Ursachen für die Anzeige dieser Fehler auf der Website Presence Topology (Präsenztopologie) beschrieben. Außerdem wird beschrieben, wie diese behoben werden können.

Problem

Wenn Sie **Ansicht** auf einem der betroffenen Knoten auswählen, werden auf der Webseite folgende Fehler angezeigt: Der Status der Dienste ist **unbekannt**:



Wenn Sie jedoch auf die CLI Secure Shell (SSH)-Sitzung des IM&P-Servers zugreifen und den folgenden Befehl ausführen: **utils service list**, sehen Sie, dass alle diese Dienste tatsächlich den Status "STARTED" aufweisen.

```
>> 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]
```

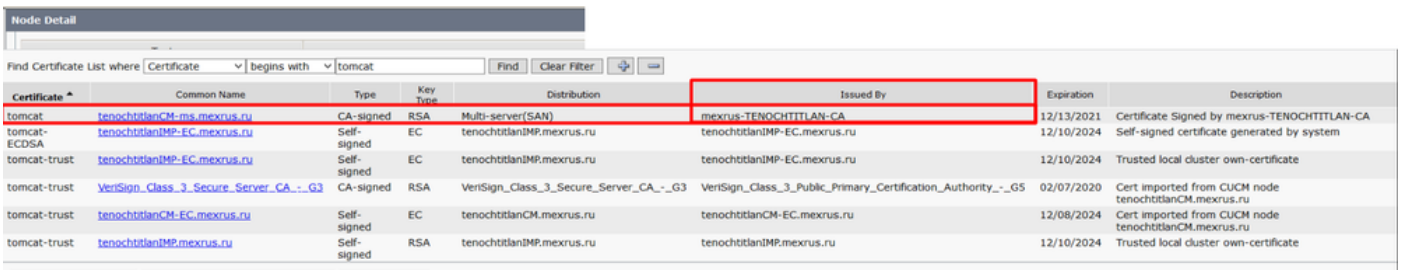
Lösung

Der Fehler in der GUI ist mit einem Tomcat-Zertifikatsproblem verknüpft. Dies sind die zu überprüfenden Punkte:

Schritt 1: Stellen Sie sicher, dass alle Ihre **Tomcat**- und **Tomcat-trust**-Zertifikate nicht abgelaufen sind, da sie andernfalls regeneriert werden müssen.

Schritt 2: Wenn Ihr Server CA-signierte Zertifikate verwendet, müssen Sie überprüfen, ob die gesamte Tomcat-Kette abgeschlossen ist. Das bedeutet, dass die Intermediate und Root-Zertifikate als Tomcat-trust hochgeladen werden müssen.

Hier ist ein Beispiel für ein fehlendes Zertifikat in der Tomcat-Kette. In diesem Fall besteht die Tomcat-Zertifikatskette nur aus zwei Zertifikaten: Root > Leaf gibt es jedoch Szenarien, in denen mehr als 2 oder 3 Zwischenzertifikate die Kette bilden.


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

Im Bildbeispiel führt der Aussteller Folgendes aus: **mexrus-TENOCHTITLAN-CA** fehlt das Zertifikat.

Erforderliche Protokolle

Navigieren Sie zu **IM and Presence Serviceability > Trace > Trace Configuration >** Server, um Folgendes auszuwählen: **IM&P Publisher > Service Group > Database and Admin Services >** Service: **Cisco IM und Presence Admin** > Auf alle Knoten anwenden > Debugging-Stufe: **Debuggen** > Aktivieren Sie das Kontrollkästchen **Alle Ablaufverfolgungen aktivieren > Speichern.**

Navigieren Sie zu **IM und Presence-Verwaltung > System > Presence-Topologie >** Wählen Sie den Knoten aus, der von den unbekannten Diensten betroffen ist, und notieren Sie sich den Zeitstempel.

Öffnen Sie das Cisco Real-Time Monitor Tool (RTMT), und sammeln Sie die folgenden Protokolle:

- Cisco Syslog
- Cisco Tomcat
- Cisco Tomcat-Sicherheit
- Ereignisanzeige - Anwendungsprotokolle
- Ereignisanzeige - Systemprotokolle
- Cisco IM- und Presence Admin-Protokolle

Details zu den Protokollen

Aus cupadmin*.log

Wenn Sie auf den **Bereich Presence Topology > Node (Anwesenheitstopologie > Knoten) zugreifen**

```
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]
```

Eine Ausnahme wurde empfangen, da ein Zertifikat nicht verifiziert wurde.

```
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)
```

Wenn Sie versuchen, den Knotenstatus für die Topologie abzurufen:

```
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
```

Eine Ausnahme wird durch den fehlenden Aussteller des Tomcat-Zertifikats verursacht.

```
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.
```

Eine weitere Art von Ausnahme finden Sie in den cupadmin*.log-Ablaufverfolgungen, die den Fehler "Falscher Aussteller für Serverzertifikat" anzeigen:

```
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.
```

In diesem Fall erkennt der IM&P das Ausstellerzertifikat für den Tomcat nicht als gültiges Ausstellerzertifikat an, was höchstwahrscheinlich auf ein beschädigtes Zertifikat zurückzuführen ist. Die **folgenden Optionen stehen zur Verfügung:**

- Validieren Sie die Informationen zu beiden: Tomcat und Ausstellerzertifikate.
- Holen Sie sich ein weiteres Ausstellerzertifikat, und vergleichen Sie es mit dem Zertifikat, das bereits im IM&P Trust Store vorhanden ist.
- Löschen Sie das Ausstellerzertifikat aus dem IM&P, und laden Sie es erneut hoch.
- Regenerieren Sie das Tomcat CA-Zertifikat.

  Anmerkung: Beachten Sie die Cisco Bug-ID CSCvu78005, die sich auf den Tomcat RSA/ECDSA-Schlüsselspeicher bezieht, der nicht in allen Knoten aktualisiert wird, wenn das vorhandene CA-Zertifikat in der Kette ersetzt wird.

Schritt 1: Führen Sie den Befehl **utils diagnose test** auf dem betroffenen Knoten aus.

Schritt 2: Wenden Sie sich für weitere Unterstützung an das Cisco Technical Assistance Center (TAC).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.