Risoluzione dei problemi relativi ai servizi IM&P visualizzati come "Sconosciuti" nella topologia della presenza

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alla pagina Topologia presenza quando i servizi vengono visualizzati come Sconosciuto nei nodi del server Instant Message e Presence (IM&P).

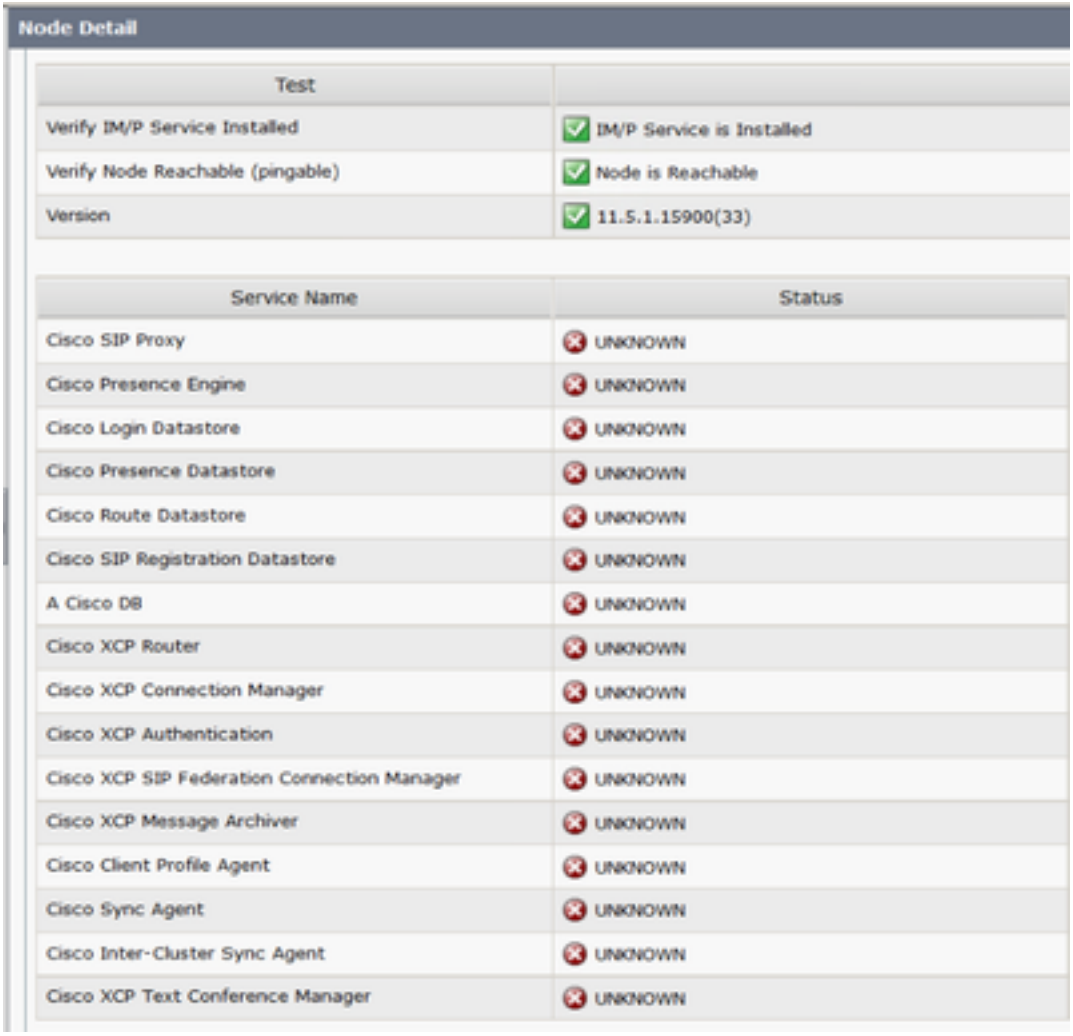
Premesse

Quando si passa alla **pagina Web di amministrazione di IM&P > Sistema > Topologia presenza** per verificare lo stato di integrità del server, è possibile che il server non si trovi nello stato corretto. In questo caso, il server visualizza una croce bianca all'interno di un cerchio rosso, anche se i servizi vengono avviati come mostrato nell'interfaccia della riga di comando (CLI) tramite il comando **utils service list**.

Questo documento descrive i motivi più comuni per cui questi errori vengono visualizzati nella pagina Web Topologia di presenza e come correggerli.

Problema

Quando si sceglie **visualizza** in uno dei nodi interessati, è possibile visualizzare nella pagina Web gli errori seguenti: lo stato dei servizi è **sconosciuto**:



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

Tuttavia, se si accede alla sessione CLI Secure Shell (SSH) del server IM&P ed si esegue il comando: **utils service list**, tutti questi servizi sono in realtà nello stato "STARTED".

```
>> 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]
```

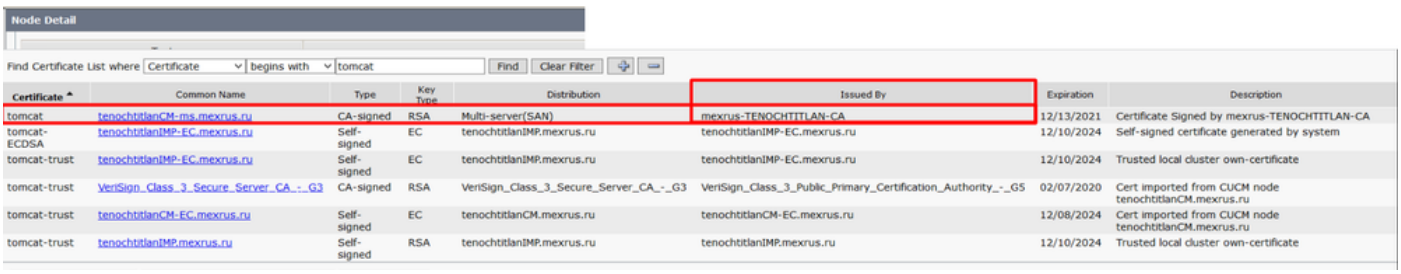
Soluzione

L'errore sulla GUI è associato a un problema di certificato Tomcat. Di seguito sono riportati gli elementi da verificare:

Passaggio 1. Verificare che tutti i certificati **Tomcat** e **Tomcat-trust** non siano scaduti. In caso contrario, sarà necessario rigenerarli.

Passaggio 2. Se il server utilizza certificati con firma CA, è necessario verificare che l'intera catena Tomcat sia stata completata. Ciò significa che i certificati intermedi e radice devono essere caricati come Tomcat-trust.

Di seguito è riportato un esempio di certificato mancante nella catena Tomcat. In questo caso, la catena di certificati Tomcat è costituita solo da due certificati: Radice > Foglia, tuttavia, esistono scenari in cui la catena viene creata da più di 2 o 3 certificati intermedi.


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

Nell'esempio di immagine, l'autorità emittente: **mexrus-TENOCHTITLAN-CA** è il certificato mancante.

Registri necessari

Passare a **IM e Presence Serviceability > Trace > Trace Configuration >** Server per selezionare: **IM&P Publisher > Gruppo di servizi > Servizi di database e amministrazione >** Servizio: **Cisco IM e Presence Admin** > Applica a tutti i nodi > Livello di debug: **Debug** > Selezionare la casella di controllo **Abilita tutte le tracce** > **Salva.**

Passare a **Amministrazione messaggistica immediata e presenza > Sistema > Topologia presenza >** Scegliere il nodo interessato dai servizi sconosciuti e annotare l'indicatore orario.

Aprire lo strumento Cisco Real-Time Monitor Tool (RTMT) e raccogliere i seguenti log:

- Cisco Syslog
- Cisco Tomcat
- Cisco Tomcat Security
- Registri applicazioni Visualizzatore eventi
- Registri di sistema del Visualizzatore eventi
- Log di Cisco IM e Presence Admin

Cosa aspettarsi nei log

Dal file cupadmin*.log

Quando accedete al **pannello Topologia presenza > 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]
```

Eccezione ricevuta. Impossibile verificare un certificato.

```
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 si tenta di recuperare lo stato del nodo per la 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
```

Eccezione causata dall'emittente mancante del certificato 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.
```

Nelle tracce di cupadmin*.log è possibile trovare un altro tipo di eccezione. Viene visualizzato il messaggio di errore "Emittente errata per certificato server":

```
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 questo caso, IM&P non riconosce il certificato dell'autorità emittente per Tomcat come certificato dell'autorità emittente valido, probabilmente a causa di un certificato danneggiato. Le **opzioni disponibili sono:**

- Convalidare le informazioni presentate su: Certificati Tomcat e autorità emittente.
- Ottenere un altro certificato dell'autorità di certificazione e confrontarlo con quello già presente nell'archivio di protezione di IM&P.
- Eliminare il certificato dell'autorità di certificazione dalla messaggistica immediata e caricarlo di nuovo.
- Rigenerare il certificato CA Tomcat.

> **Nota:** Tenere presente che l'ID bug Cisco CSCvu78005, che fa riferimento al keystore Tomcat RSA/ECDSA, non viene aggiornato in tutti i nodi quando si sostituisce il certificato CA esistente nella catena.

Passaggio 1. Eseguire il comando **utils diagnostse test** sul nodo interessato.

Passaggio 2. Per ulteriore assistenza, contattare il Technical Assistance Center (TAC) di Cisco.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).