

对在线状态拓扑中显示为“未知”的IM&P服务进行故障排除

目录

[简介](#)

[背景信息](#)

[问题](#)

[解决方案](#)

[所需日志](#)

[日志中的预期](#)

简介

本文档介绍当“在线状态拓扑”页在即时消息和在线状态(IM&P)服务器节点上将服务显示为“未知”时，如何排除故障。




















背景信息

导航到IM&P Administration web page > System > Presence Topology以验证服务器的运行状况时，可能会遇到服务器未处于正确的状态。在这种情况下，服务器在红色圆圈内显示一个白十字，即使服务是通过`utils service list`命令在命令行界面(CLI)上所示启动的。

本文档介绍这些错误显示在在线状态拓扑网页上的最常见原因以及如何修复它们。

问题

当您在受影响的节点上选择**view**时，您可以在网页上看到以下错误：服务的状态是**unknown**：

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

但是，如果您访问IM&P服务器的CLI安全外壳(SSH)会话并运行命令：**utils service list**，您会看到所有这些服务实际上都处于“STARTED”状态。

```

>> 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}

```

解决方案

GUI上的错误与Tomcat证书问题相关联。以下是需要验证的内容：

步骤1.确保所有Tomcat和Tomcat-trust证书均未过期，否则，需要重新生成这些证书。

步骤2.如果服务器使用CA签名的证书，则需要验证整个Tomcat链是否完整。这意味着中间证书和根证书需要作为Tomcat-trust上传。

以下是Tomcat链中缺少证书的示例。在这种情况下，Tomcat证书链仅包含两个证书：但是，根>枝叶，存在超过2个或3个中间证书构建链的情况。

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

在图像示例中，颁发者：mexrus-TENOCHTITLAN-CA缺少证书。

所需日志

导航到IM and Presence Serviceability > Trace > Trace Configuration > Server以选择：IM&P Publisher > Service Group > Database and Admin Services > Service:Cisco IM and Presence Admin > Apply to all Nodes > Debug level:Debug > Check the Enable All Trace Checkbox > Save。

导航到IM and Presence Administration > System > Presence Topology > 选择受未知服务影响的节点，并记下时间戳。

打开思科实时监控工具(RTMT)并收集以下日志：

- 思科系统日志
- Cisco Tomcat
- 思科Tomcat安全
- 事件查看器应用程序日志
- 事件查看器系统日志
- 思科即时消息和在线状态管理员日志

日志中的预期

从cupadmin*.log

当您访问Presence Topology > Node面板时。

```
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]
```

由于未验证证书，因此收到异常。

```
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)
```

尝试检索拓扑的节点状态时：

```
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
```

由于Tomcat证书的颁发者缺失，导致异常。

```
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.
```

在cupadmin*.log跟踪中还可以发现另一种异常，其中显示错误“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.
```

在这种情况下，IM&P无法将Tomcat的颁发者证书识别为有效的颁发者证书，这可能是由于证书损坏导致的。此处的选项包括：

- 验证以下两种上提供的信息：Tomcat和Issuer证书。
- 获取另一个颁发者证书，并将其与IM&P信任库中已存在的证书进行比较。
- 从IM&P中删除颁发者证书并重新上传。
- 重新生成Tomcat CA证书。

注意：请注意Cisco Bug ID [CSCvu78005](#)，该漏洞是指Tomcat RSA/ECDSA Keystore's not update in all nodes when the existing CA certificate in the chain is replaced.

步骤1.在受影响的节点上运行**utils diagnose test**命令。

步骤2.联系思科技术支持中心(TAC)获取进一步帮助。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。