프레즌스 토폴로지에서 "알 수 없음"으로 표시된 IM&P 서비스 문제 해결

목차

소개

이 문서에서는 IM&P(Instant Message and Presence) 서버 노드에서 서비스를 알 수 없음으로 표시할 때 Presence Topology(프레즌스 토폴로지) 페이지의 문제를 해결하는 방법에 대해 설명합니다.

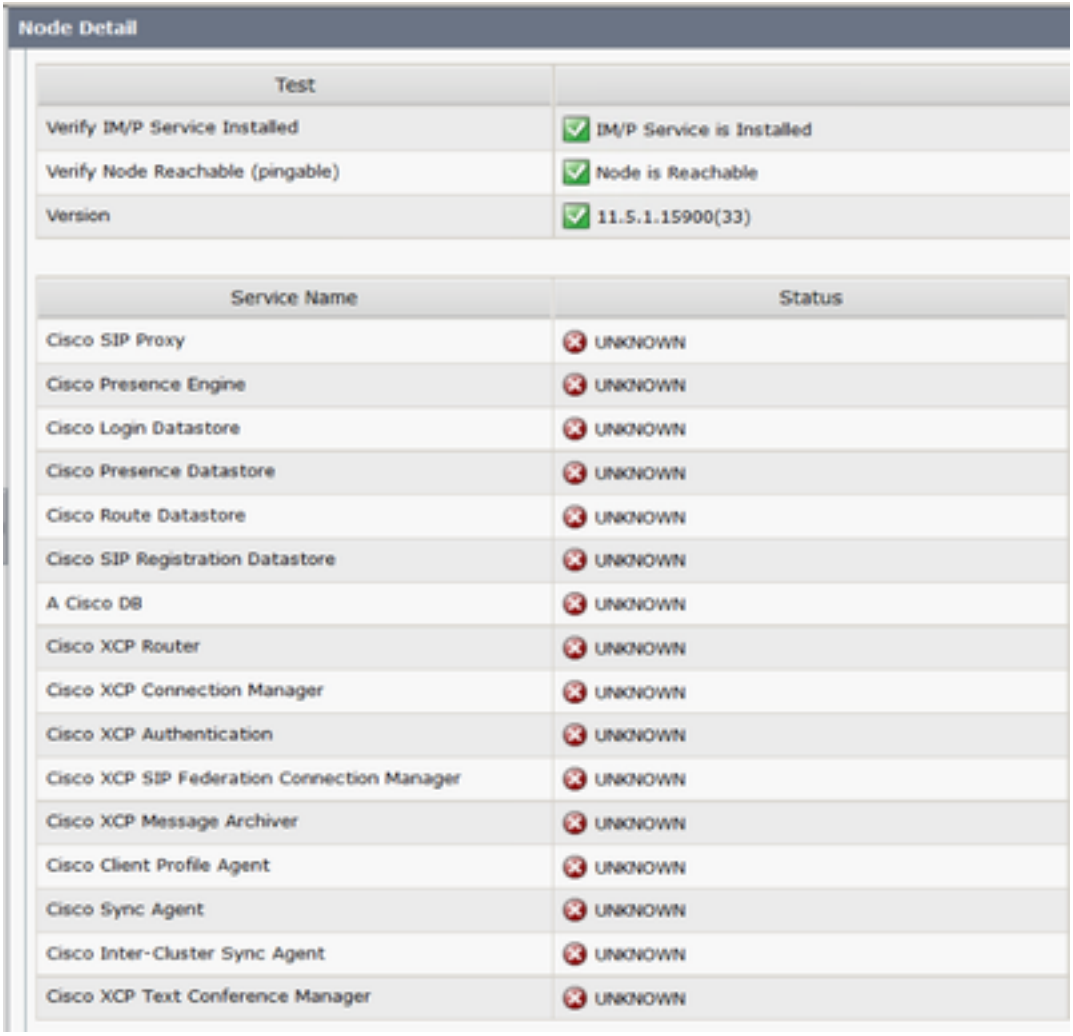
배경 정보

IM&P Administration 웹 페이지 > System > Presence Topology로 이동하여 서버의 상태를 확인할 때 서버가 올바른 상태가 아닐 수 있습니다. 이 경우, utils service list 명령을 통해 CLI(Command Line Interface)에 표시된 대로 서비스가 시작되더라도 서버에서 빨간색 원 안에 흰색 십자선이 **표시되어** 있습니다.

이 문서에서는 이러한 오류가 Presence Topology 웹 페이지에 표시되는 가장 일반적인 이유와 해결 방법에 대해 설명합니다.

문제

영향받는 노드 중 **하나**에서 보기를 선택하면 웹 페이지에서 다음 오류를 볼 수 있습니다. 서비스의 상태를 **알 수 없습니다**.



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

그러나 IM&P 서버의 CLI SSH(Secure Shell) 세션에 액세스하여 다음 명령을 실행하면 **유틸리티 서비스 목록**에서 모든 서비스가 실제로 "시작됨" 상태임을 확인할 수 있습니다.

```
>> 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]
```

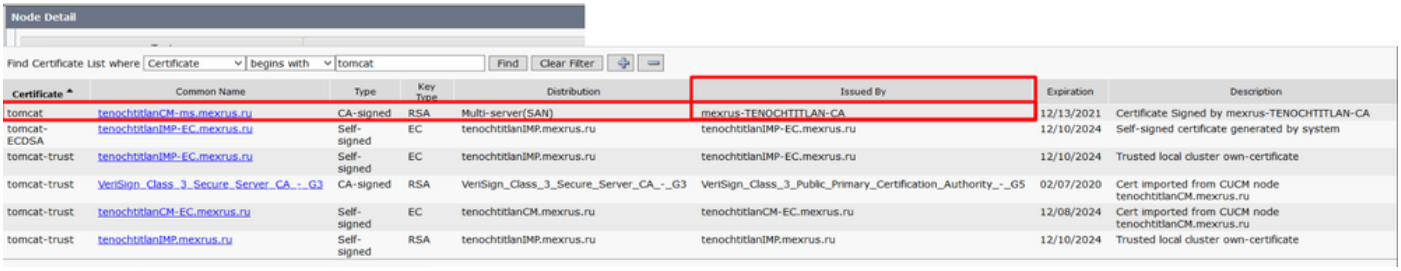
솔루션

GUI의 오류는 Tomcat 인증서 문제와 관련이 있습니다. 다음은 확인이 필요한 사항입니다.

1단계. 모든 Tomcat 및 **Tomcat-trust 인증서**가 만료되지 않았는지 확인합니다. 만료되지 않은 경우 인증서를 다시 생성해야 합니다.

2단계. 서버에서 CA 서명 인증서를 사용하는 경우 전체 Tomcat 체인이 완료되었는지 검증해야 합니다. 즉, 중간 인증서와 루트 인증서를 Tomcat-trust로 업로드해야 합니다.

다음은 Tomcat 체인에 누락된 인증서의 예입니다. 이 경우 Tomcat 인증서 체인은 두 개의 인증서로만 구성됩니다. 그러나 Root(루트) > Leaf(리프)에서는 2개 또는 3개 이상의 중간 인증서가 체인을 작성하는 경우가 있습니다.


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

이 그림에서 Issuer(발급자)는 **mexrus-TENOCHTITLAN-CA**가 누락된 인증서입니다.

필수 로그

IM and Presence Serviceability(**IM and Presence 서비스 가용성) > Trace(추적) > Trace Configuration(추적 컨피그레이션) > Server(**서버)로 이동하여 다음을 선택합니다. **IM&P 게시자 > 서비스 그룹 > 데이터베이스 및 관리 서비스 >** 서비스: **Cisco IM and Presence Admin(Cisco IM and Presence 관리) >** Apply to all Nodes(모든 노드에 적용) > Debug level(디버그 레벨): **Debug**(디버그) > Enable **All Trace(모든 추적 활성화) 확인란** > Save(**저장)를 선택합니다.**

IM and Presence Administration(IM and Presence 관리) > System(시스템) > Presence Topology(프레즌스 토폴로지) > Select the node that affected by the unknown services(알 수 없는 서비스의 영향을 받는 노드를 선택하고 타임스탬프를 기록합니다.

Cisco RTMT(Real-Time Monitor Tool)를 열고 다음 로그를 수집합니다.

- Cisco Syslog
- Cisco Tomcat
- Cisco Tomcat 보안
- 이벤트 뷰어 애플리케이션 로그
- 이벤트 뷰어 시스템 로그
- Cisco IM and Presence Admin 로그

로그에서 예상되는 사항

cupadmin*.log에서

Presence Topology(프레즌스 토폴로지) **> Node(노드) 패널에 액세스할** 때

```
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]
```

인증서가 확인되지 않았기 때문에 예외가 발생했습니다.

```
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)
```

토폴로지에 대한 노드 상태를 검색하려고 하면

```
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
```

Tomcat 인증서의 발급자가 누락되어 예외가 발생했습니다.

```
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.
```

"Incorrect issuer for server cert(서버 인증서의 발급자 오류)" 오류가 표시되는 cupadmin*.log 추적에서 또 다른 유형의 예외를 찾을 수 있습니다.

```
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.
```

이 경우 IM&P는 Tomcat에 대한 발급자 인증서를 유효한 발급자 인증서로 인식하지 않습니다. 이는 대부분 인증서가 손상되어 발생한 것일 수 있습니다. **다음 옵션을 사용할 수 있습니다.**

- 다음 두 항목에 표시된 정보를 확인합니다. Tomcat 및 발급자 인증서
- 다른 발급자 인증서를 가져와 IM&P Trust Store에 이미 있는 인증서와 비교합니다.
- IM&P에서 발급자 인증서를 삭제하고 다시 업로드합니다.
- Tomcat CA- 인증서를 다시 생성합니다.

  참고: Cisco 버그 ID CSCvu78005에 유의하십시오. 즉, Tomcat RSA/ECDSA 키 저장소의 는 체인의 기존 CA 인증서가 교체될 때 모든 노드에서 업데이트되지 않습니다.

1단계. 영향을 받는 **노드**에서 utils **diagnose test** 명령을 실행합니다.

2단계. 자세한 내용은 Cisco TAC(Technical Assistance Center)에 문의하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.