

プレゼンストポロジに「不明」と表示されるIM&Pサービスのトラブルシューティング

内容

[概要](#)

[背景説明](#)

[問題](#)

[解決方法](#)

[必要なログ](#)

[ログの内容](#)

概要

このドキュメントでは、Instant Message and Presence(IM&P)サーバノードでサービスが[Unknown]と表示される場合の[Presence Topology]ページのトラブルシューティング方法について説明します。




















背景説明

[IM&P Administration] Webページ> [System] > [Presence Topology] に移動してサーバのヘルスステータスを確認すると、サーバが正しい状態ではないことに気付く場合があります。この場合、`utils service list`コマンドを使用してCommand Line Interface (CLI ; コマンドラインインターフェイス) でサービスが起動されているにもかかわらず、サーバでは赤い丸の中に白い十字が表示されます。

このドキュメントでは、これらのエラーがプレゼンストポロジWebページに表示される最も一般的な理由と、その修正方法について説明します。

問題

影響を受けるノードのいずれかでviewを選択すると、Webページに次のエラーが表示されます。サービスのステータスはunknownです。

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

ただし、IM&PサーバのCLIセキュアシェル(SSH)セッションにアクセスして次のコマンドを実行する場合は、次のようになります。utils service listで、これらのサービスがすべて実際には「STARTED」状態であることがわかります。

```

>> 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}

```

解決方法

GUIのエラーは、Tomcat証明書の問題に関連しています。確認する必要があるものは次のとおりです。

ステップ1：すべてのTomcatおよびTomcat-trust証明書が期限切れになっていないことを確認します。期限切れになっていない場合は、それらを再生成する必要があります。

ステップ2：サーバがCA署名付き証明書を使用する場合は、Tomcatチェーン全体が完了していることを検証する必要があります。つまり、中間証明書とルート証明書をTomcat-trustとしてアップロードする必要があります。

次に、Tomcatチェーンに存在しない証明書の例を示します。この場合、Tomcat証明書チェーンは次の2つの証明書だけで構成されます。ただし、[Root] > [Leaf]では、2つまたは3つ以上の中間証明書がチェーンを構築するシナリオがあります。

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	tenochtitlanCM-ria.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

この図の例では、Issuer:mexrus-TENOCHTITLAN-CAが証明書の欠落です。

必要なログ

[IM and Presence Serviceability] > [Trace] > [Trace Configuration] > [Server]に移動して次のものを選択します。[IM&P Publisher] > [Service Group] > [Database and Admin Services] > [Service:[Cisco IM and Presence Admin] > [Apply to all Nodes] > [Debug level:Debug > [Enable All Trace] チェックボックスをオンにして、保存します。

[IM and Presence Administration] > [System] > [Presence Topology] に移動し、不明なサービスの影響を受けるノードを選択し、タイムスタンプをメモします。

Cisco Real-Time Monitor Tool(RTMT)を開き、次のログを収集します。

- Cisco Syslog
- Cisco Tomcat
- Cisco Tomcatセキュリティ
- イベントビューアアプリケーションログ
- イベントビューアのシステムログ
- Cisco IM and Presence管理ログ

ログの内容

cupadmin*.logから

[プレゼントトポロジ(Presence Topology)] > [ノード(Node)]パネルにアクセスすると、

```
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]
```

証明書が検証されなかったため、例外が発生しました。

```
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)
```

トポロジのノードステータスを取得しようとする、次のようになります。

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証明書の発行者が見つからないため、例外が発生します。

```
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.
```

別のタイプの例外がcupadmin*.logトレースで見つかり、「Incorrect issuer for server cert」エラーが表示されます。

```
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.
```

この場合、IM&PはTomcatの発行者証明書を有効な発行者証明書として認識しません。これは、証明書の破損が原因で発生した可能性があります。次のオプションがあります。

- 両方に表示される情報を検証します。Tomcatおよび発行者証明書。
- 別の発行者証明書を取得し、IM&P信頼ストアにすでに存在する証明書と比較します。
- IM&Pから発行者証明書を削除し、再度アップロードします。
- Tomcat CA証明書を再生成します。

注：Cisco Bug ID [CSCvu78005](#)は、チェーン内の既存のCA証明書が置き換えられても、すべてのノードでTomcat RSA/ECDSAキーストアが更新されないことを意味します。

ステップ1：影響を受けるノードでutils diagnose testコマンドを実行します。

ステップ2：詳細については、Cisco Technical Assistance Center(TAC)にお問い合わせください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。