Troubleshoot Jabber Login Problems

Contents

Introduction
Background Information
How to Collect Logs
Keywords to Search in Logs
Stages to Troubleshoot
Stage 1. CUCM Service Discovery
Stage 2. CUCM User Authentication
Stage 3. SOAP Login (IM and Presence Login)
Stage 4. XMPP Login (IM and Presence Login)
Mandatory Checks
How to Set Logs to DEBUG
Logs to Collect
Collect Logs from RTMT

Introduction

This document outlines the sequence of Cisco Jabber Login and how to troubleshoot when Jabber login fails while being in Internal/corporate Network.

Background Information

Jabber Login comprises of two stages namely Cisco Unified Communications Manager server (CUCM) Login and IM and Presence server (IMP) Login.
• CUCM Login involves Service discovery to identify the CUCM server to which Jabber should login.

• Jabber user Authentication with CUCM to retrieve the Service profile details which contains IMP server, Voicemail, Conferencing, CTI server details and also Device Configuration file for Phone services.

• Once CUCM Login is successful, Jabber will login to IMP server to authenticate and retrieve the contact list and other IM services.

• IMP Login has two stages namely SOAP Login which deals with User authentication and then XMPP Login which deals with XMPP session creation and Stream Management.

How to Collect Logs

Primarily, clear the cache on PC and collect the clean Jabber Problem Report (PRT). These are the steps to do the same

1. Sign out and exit the Jabber application.

2. Delete all the existing logs located at
3. Restart Jabber and recreate the problem by logging in.

4. Collect the Problem report (From Jabber Help menu, select Report a problem option to launch problem reporting tool and follow instructions).

**Keywords to Search in Logs**

- IMPStackCap::Login::OnLoginError
- ServiceDiscoveryHandlerResult

**Stages to Troubleshoot**

**Stage 1. CUCM Service Discovery**

**Error on screen**

Cannot find your services automatically. Click advanced settings to set up manually

**Cause**

This error is seen when _cisco-uds or _cuplogin SRV records are not configured in the DNS server

**What to check in Jabber log**

csf::dns::mapFromWindowsDNSResult

**Sample Log Snippet**

```
017-03-19 17:55:00,422 WARN  [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns] [csf::dns::mapFromWindowsDNSResult] - *-----* DNS query _cisco-uds._tcp.appslab.com. has failed: DNS name does not exist. (9003).
2017-03-19 17:55:00,438 WARN  [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns] [csf::dns::mapFromWindowsDNSResult] - *-----* DNS query _cuplogin._tcp.appslab.com. has failed: DNS name does not exist. (9003).
```

**Steps to Resolve**

Step 1. First start nslookup (on a windows client) start the command prompt and then enter `nslookup`.

Step 2. Next set the query type to SRV

`set type = SRV`

Step 3. After that insert the SRV record we need to check `_cisco-uds._tcp.example.com`

Step 4. This returns the DNS A records pointing to the CUCM servers. This is an example of the Successful _cisco-uds SRV record. If no records returned, contact your DNS Administrator to configure the SRV records.
Stage 2. CUCM User Authentication

Error on screen  Cause  What to check in Jabber log
Your username or password is not correct  This error is seen when the credentials entered is wrong or user is locked in CUCM/LDAP  "FAILED_UCM90_AUTHENTICATION"

Sample Log Snippet

2017-01-09 08:59:10,652 INFO [0x00001740] [vices\impl\DiscoveryHandlerImpl.cpp(460)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::evaluateServiceDiscoveryResult] - ServiceDiscoveryHandlerResult return code FAILED_UCM90_AUTHENTICATION

Steps to Resolve

Step 1. Ensure that the User you try to login as is configured as Enduser in CUCM by going to CUCM Administration -Enduser page.

Step 2. Verify if credentials are correct and user is active by logging into CUCM Self care Portal. This image refers to scenario where the LDAP is unable to authenticate the user either because the user is not a valid user or password supplied is incorrect.

Step 3. If this issue is seen for all users you need to verify if the LDAP syncronisation and LDAP...
Authentication settings on **CUCM Administration -System > LDAP** is correct.

<table>
<thead>
<tr>
<th>Error on screen</th>
<th>Cause</th>
<th>What to check in Jabber log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot communicate with the server</td>
<td>Jabber is unable to resolve/reach the CUCM FQDN/HOSTNAME that it received during the Service discovery</td>
<td>&quot;FAILED_UCM90_CONNECTION&quot;</td>
</tr>
</tbody>
</table>

**Sample Log Snippet**

```
2017-08-28 12:04:00.282 INFO [0x00004290] [vices\impl\DiscoveryHandlerImpl.cpp(452)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::evaluateServiceDiscoveryResult] - ServiceDiscoveryHandlerResult return code FAILED_UCM90_CONNECTION
```

**Steps to Resolve**

1. **Test if you are able to open this URL in the browser on the PC** `https://<CUCM IP/FQDN>:8443/cucm-uds/version`
   
   **Unsuccessful**
   
   **Successful**

2. **If the response is unsuccessful, please verify if DNS is configured correctly to resolve them and also if no Network Elements like Firewall/ASA is blocking port 8443.**

3. **This URL must be tested for all CUCM Servers in the cluster. In order to know the list of Servers, navigate to **CUCM Administration -System > Server.****

<table>
<thead>
<tr>
<th>Error on screen</th>
<th>Cause</th>
<th>What to check in Jabber log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot communicate with the server</td>
<td>This error is seen when the userid entered in Jabber doesn't match with userid configured in CUCM</td>
<td>&quot;FAILED_USER_LOOKUP&quot;</td>
</tr>
</tbody>
</table>
Sample Log Snippet

2016-08-18 13:14:49,943 INFO [0x000036e4] [vices\impl\DiscoveryHandlerImpl.cpp(367)] [service-discovery] [DiscoveryHandlerImpl::evaluateServiceDiscoveryResult] - ServiceDiscoveryHandlerResult return code FAILED_USER_LOOKUP

Steps to Resolve

Step 1. Test if you are able to open this URL in the browser on the PC https://CUCM:8443/cucm-uds/clusterUser?username=<userid>

Step 2. Check if the userid that is being entered in Jabber matches the userid in CUCM End user page.

Tip: Jabber has UPN discovery enabled by default and hence get the userid prepopulated from LDAP UPN field. Check if UPN is same as configured in CUCM, if you need to disable UPN discovery ,set UPN_DISCOVERY_ENABLED=false during installation

Stage 3. SOAP Login (IM and Presence Login)

<table>
<thead>
<tr>
<th>Error on screen</th>
<th>Cause</th>
<th>What to check in Jabber log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your username or password is not correct</td>
<td>This error is caused due to user Authentication failure</td>
<td>&quot;LERR_CUP_AUTH&quot;</td>
</tr>
</tbody>
</table>

Sample Log Snippet

2017-01-14 15:55:09,615 INFO [0x00000dc0] [s\adapters\imp\components\Login.cpp(99)] [imp.service] [IMPStackCap::Login::OnLoginError] -  ****************************************************************
2017-01-14 15:55:09,615 INFO [0x00000dc0] [s\adapters\imp\components\Login.cpp(100)] [imp.service] [IMPStackCap::Login::OnLoginError] - OnLoginError: (data=0) LERR_CUP_AUTH <12>:
201-01-14 15:55:09,615 INFO [0x00000dc0] [s\adapters\imp\components\Login.cpp(101)] [imp.service] [IMPStackCap::Login::OnLoginError] -  ****************************************************************

Steps to Resolve

Step 1. Check if user is assigned to a Presence Node and there are no duplicates for the user (IM and presence Administration > Diagnostics > System troubleshooter).

Step 2. Check if the High Availability (HA) state is Normal and no Failover has occured. If you have tried assigning user during abnormal HA state, Users are not assigned to any IMP node and login fails and now you need to recover the HA state first and re-assign the user.

Step 3. Ensure that the credentials are valid.

1. In case of LDAP user, verify if user is able to login to CUCM Selfcare portal.

2. If ccmenduser page login fails, check the LDAP Authentication settings in CUCM and also
verify the same settings are replicated to IMP

run sql select * from ldapauthentication
run sql select * from ldapauthenticationhost

3. Check if the account is not locked in LDAP

4. If user was recently enabled for Presence, restart Cisco Sync Agent service on IMP Publisher.

Step 4. Check the server is having a high TOMCAT CPU consumption

- show process load
- utils diagnose test

Step 5. Set these services log to DEBUG and then recreate the Login issue and collect the logs

- Client Profile Agent
- Cisco Tomcat
- Event Viewer-Application Log
- Event Viewer-System Log

Error on screen | Cause | What to check in Jabber log
---|---|---
Cannot communicate with the server | This error is caused due to Issues with IMDB or TCP connectivity to IMP | "LERR_CUP_UNREACHABLE" or "LERR_CUP_TIMEOUT"

Sample Log Snippet

```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLoginError] - ************************************************
2017-11-08 16:03:20,051 INFO [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLoginError] - OnLoginError: LERR_CUP_UNREACHABLE
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLoginError] - ************************************************
```

Steps to Resolve

Step 1. Check if IMP FQDN/Hostnames are resolvable from client PC.

Step 2. Check if you can open this URL in browser https://<IMP SERVER FQDN/IP>:8443/EPASSoap/service/v105

Successful
Unsuccessful

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<error>This is a SOAP service. Send a POST request!</error>
**HTTP Status 404 - /EPASSoap/serviceV105**

- **type:** Status report
- **message:** /EPASSoap/serviceV105
- **description:** The requested resource is not available.

---

Step 3. Verify that firewall/VPN is not blocking the connectivity to IMP server (Port 8443, 5222)

Step 4. Verify if this service runs in IMP server: Cisco Client profile Agent

Step 5. Set these services log to DEBUG, recreate the Login issue and then collect the logs if above steps doesn't resolve the problem.

- Cisco XCP Router
- Cisco XCP connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent

**Tip:** If the problem persists for only one user, you can try to unassign and re-assign the user for presence in CUCM. If it's a system wide problem, collect the logs and check the services status.

---

**Error on screen**

Cannot communicate with the server

**Cause**

Usually this error is caused due to Issues with IMDB

**What to check in Jabber log**

"LERR_CUP_INTERNAL_ERROR"

---

**Sample Log Snippet**

```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)]
[IMPServices] [CSFUnified::IMPSockCap::Login::OnLoginError] - 
************************************************
2017-11-08 16:03:20,051 INFO [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)]
[IMPServices] [CSFUnified::IMPSockCap::Login::OnLoginError] - OnLoginError: 
LERR_CUP_INTERNAL_ERROR
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)]
[IMPServices] [CSFUnified::IMPSockCap::Login::OnLoginError] - 
************************************************
```

---

**Steps to Resolve**

Step 1. Perform [Mandatory checks](#)

Step 2. Verify if following services are running in IMP server

- Cisco XCP Router
- Cisco XCP connection Manager
Step 3. Check if this Field notice is applicable

Field Notice: FN - 64267 - Cisco Unified Communications Manager IM & Presence causes Cisco Jabber login failures - Software Upgrade Recommended

Step 4. Set these services log to DEBUG, recreate the Login issue and then collect the logs if above steps doesn't resolve the problem.

- Cisco XCP Router
- Cisco XCP connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Cisco Presence Login Datastore
- Event Viewer-Application Log
- Event Viewer-System Log

Step 5. Reboot the cluster to recover the situation.

Stage 4. XMPP Login (IM and Presence Login)

<table>
<thead>
<tr>
<th>Error on screen</th>
<th>Cause</th>
<th>What to check in Jabber log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot communicate with the server</td>
<td>Commonly seen when Jabber cannot create a session and bind itself in IMP server</td>
<td>LERR_JABBER_AUTH &lt;17&gt;: Authentication error with server e.g. resource bind, TLS, create session or SASL error</td>
</tr>
</tbody>
</table>

Sample Log Snippet

```
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(127)] [IMPServices] [OnLoginError] - ****************************************************************
2017-10-27 10:56:47,396 INFO [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(128)] [IMPServices] [OnLoginError] - OnLoginError: LERR_JABBER_AUTH <17>: Authentication error with server e.g. resource bind, TLS, create session or SASL error
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(129)] [IMPServices] [OnLoginError] - ****************************************************************
```

Steps to Resolve

Step 1. Check if the cup-xmpp Certificates are valid.

Step 2. Check if the Port 5222 is open.

Step 3. Set the following services log to DEBUG and then recreate the Login issue and collect the logs before step 4 if Root cause to be identified as Reboot of the server is the only fix known so far

- Cisco XCP Router
- Cisco XCP connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Application Log
Step 4. Reboot the server to resolve the issue.

**Error on screen**  
Cannot communicate with the server

**Cause**  
Seen when IMP is not resolvable or reachable due to Network problems like firewall

**What to check in Jabber log**  
"LERR_JABBER_UNREACHABLE"

**Sample Log Snippet**

```
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components\Login.cpp(96)]
[imp.service] [IMPStackCap::Login::OnLoginError] -
****************************************************************
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components\Login.cpp(97)]
[imp.service] [IMPStackCap::Login::OnLoginError] - OnLoginError: (data=0)
LERR_JABBER_UNREACHABLE <16>:
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components\Login.cpp(98)]
[imp.service] [IMPStackCap::Login::OnLoginError] -
****************************************************************
```

**Steps to Resolve**

Step 1. Check if IMP FQDN/Hostnames are resolvable.

Step 2. Verify that firewall/VPN is not blocking the connectivity to IMP server (Port 8443, 5222).

Step 3. Verify if these services are running in IMP server and restart them once.

- Cisco XCP Router
- Cisco XCP connection Manager
- Cisco XCP Authentication Service

Step 4. Perform **Mandatory checks**.

Step 5. Set these services log to DEBUG, recreate the Login issue and then collect the logs if above steps don't resolve the problem.

- Cisco XCP Router
- Cisco XCP connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Application Log
- Event Viewer-System Log

Step 6. In case of all users experiencing the same error, a server Reboot can be done for quick recovery.

**Mandatory Checks**

Step 1. Check if user is assigned to a Presence Node (navigate to **IM and Presence Administration > System > Topology**) and there are no duplicates for the user (navigate to **IM and Presence Administration > Diagnostics > System troubleshooter**)
Step 2. If High Availability is enabled, navigate to **CUCM Administration > Server > Presence Redundancy Group** and check if they are in Normal state. This is the image of how Normal state looks. For more information about High Availability can be found [here](#).

**Abnormal State**

**Normal State**

Step 3. Check High Availability Replication status.

1. `utils dbreplication runtimestate`

   ```
   DB Version: ccm10_5_1_13900_2
   Repltimeout set to: 300s
   PROCESS option set to: 1
   Cluster Detailed View from IMPSUB-1051SU3 (2 Servers):
   ```

   ```
   TABLE: DB/REC/ REPL. Replication Group ID
   ID 3 (NULL) 3 (NULL)
   7 (NULL) 7 (NULL)
   ```

2. `run pe sql ttlogin select count(*) from typesysreplication`

   ```
   admin:run pe sql ttlogin select count(*) from typesysreplication
   sqlRv(t) sqlstmt(select count(*) from typesysreplication;)
   ***result set start***
   count(0), success(t)
   ***result set end***
   ```

   or

   ```
   utils imdb_replication status ( 10.5.2 SU2a and above)
   ```

**How to Set Logs to DEBUG**

Step 1 Choose **Navigation > Unified serviceability > Trace > Configuration**.
Step 2 From the Server drop-down list, choose the server (i.e. IMP node) that is running the service for which you want to configure trace and then, click **Go**.
Step 3 From the Service Group drop-down list box, choose the service group for the service that you want to configure trace; then, click **Go**.
Step 4 From the Service drop-down list box, choose the service for which you want to configure trace; then, click **Go**.
Step 5 Check box **Apply to All Nodes** and select the trace level to **DEBUG**.
Step 6 To save your trace parameters configuration, click the **Save** button.

For more information of setting trace levels refer [Cisco Unified Serviceability Administration Guide](#).
### Trace Configuration

**Status:**
- Ready

**Select Server, Service Group and Service**

<table>
<thead>
<tr>
<th>Server*</th>
<th>192.168.100.85--CUCM IM and Presence</th>
<th>Go</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Group*</td>
<td>IM and Presence Services</td>
<td>Go</td>
</tr>
<tr>
<td>Service*</td>
<td>Cisco XCP Connection Manager (Active)</td>
<td>Go</td>
</tr>
</tbody>
</table>

- Apply to All Nodes

- Trace On

**Trace Filter Settings**

- Debug Trace Level: Debug
- Enable All Trace

**Trace Output Settings**

- Maximum No. of Files*: 250
- Maximum File Size (MB)*: 2
Trace Configuration

Status:
Ready

Select Server, Service Group and Service

Server*: 192.168.100.85--CUCM IM and Presence  Go
Service Group*: IM and Presence Services  Go
Service*: Cisco Client Profile Agent (Active)  Go

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level: Debug
Enable All Trace

Trace Output Settings

Maximum No. of Files*: 250
Maximum File Size (MB)*: 1
Trace Configuration

**Status:**
- Ready

**Select Server, Service Group and Service**
- Server: 192.168.100.85--CUCM IM and Presence
- Service Group: IM and Presence Services
- Service: Cisco Login Datastore (Active)
- Apply to All Nodes: checked
- Trace On: checked

**Trace Filter Settings**
- Debug Trace Level: Debug
- Enable All Trace: checked

**Trace Output Settings**
- Maximum No. of Files: 250
- Maximum File Size (MB): 1
### Trace Configuration

**Status:**
- Ready

#### Select Server, Service Group and Service

<table>
<thead>
<tr>
<th>Server*</th>
<th>192.168.100.85--CUCM IM and Presence</th>
<th>Go</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Group*</td>
<td>IM and Presence Services</td>
<td>Go</td>
</tr>
<tr>
<td>Service*</td>
<td>Cisco XCP Authentication Service (Active)</td>
<td>Go</td>
</tr>
</tbody>
</table>

- Apply to All Nodes

- Trace On

#### Trace Filter Settings

<table>
<thead>
<tr>
<th>Debug Trace Level</th>
<th>Debug</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Enable All Trace

#### Trace Output Settings

- Maximum No. of Files* | 250 |
- Maximum File Size (MB)* | 2 |
Logs to Collect

RTMT  Admin CLI
Cisco Client Profile Agent  file get activelog tomcat/logs/epassoap/log4j/*
Cisco Login Datastore  file get activelog epas/trace/imdb/sdi/ttlogin/
Cisco Tomcat Security Logs  file get activelog tomcat/logs/security/log4j/*
Cisco XCP Authentication Service  file get activelog epas/trace/xcp/log/auth*
Cisco XCP Connection Manager  file get activelog epas/trace/xcp/log/client-cm-1*.log
Cisco XCP Router  file get activelog epas/trace/xcp/log/rtr-jsm-1
Event Viewer-Application Log  file get activelog syslog/CiscoSyslog*
Event Viewer-System Log  file get activelog syslog/messages*

Collect Logs from RTMT