Troubleshooting

This page contains troubleshooting tips for scripters. Scripters can check various symptoms and attempt to eliminate problems with their setup or use of script before reporting problems to the camelot team.

Information for turning on Camelot logs is here.

SIP Trunk Troubleshooting

There are just some common troubleshooting tips I see on the camelot-support alias. Going through this checklist can many times solve the problem without involving Camelot support.

How to solve Common Camelot issues yourselves OR how to debug Camelot logs yourselves

- Enable Camelot logs which is explained in below section. Run your script. Go to Camelot logs directory. You can get the directory from Camelot Server console.
- grep for error logs in case you have not enabled error logs on Camelot server console
  grep -r "| error" ./camlog*
- See whether the error messages in logs are giving any clue by going through FAQs in this page. If not, send the complete logs to Camelot support mailer (camelot-support@cisco.com).

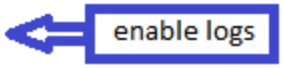
Enabling Logs

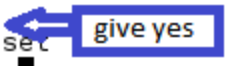
If you hit any Camelot issue, you will need to enable logs and try to identify the issue and solve it yourself with below FAQs, in case you are not able to solve ; send logs to send to camelot-support for us to analyze. Please enable logs as follows:

Enable logs from Camelot server console

```
logmask -moduleid * -level error -device console
logmask -moduleid * -level debug_5 -device file
yes
```

```
[camelot@cam-centos7-189 ~]$ camserv -vp 5000

Camelot Server Starting...

Version:          12.5.14.9.0.0
Build date:       Apr 30 2018
Build time:       22:06:36
OS:               Linux

Compatibility information:
  CUCM version:       10.5.1.10000-7
  CME version:        15.3
  CUP version:        10.5.1.10000-9
  CTMS version:       1.1.0
  EDGE version:       X8.2PreAlpha4
  NCS version:        1.0.0.0-163
  VAPI-EI version:    12.5.14.9.0.0


Skipping license verfification for this build...

Execution logs directory:
/var/camelot/logs/05000_20180504_113507

Setting core limit to unlimited (i.e.,4294967295)
Core limit is set already to unlimited

VAPI server listening on host 0.0.0.0, port 5000

(camserv)% logmask -moduleid * -level debug_5 -device file
Warning!
setting global logging may have severe impact on server performance under load
Apply settings? [yes|no]
yes
Log level set
(camserv)%
```





Enable logs on Camelot server running on docker containers and find current log directory

Find the container id of the container by running "docker ps" in docker host machine
Then get into Camelot server console by running "docker attach <container id>"
You will be taken into Camelot server console. Just give enter to see Camelot server console.
Give the logmask command and "yes" as explained in previous section.
Press **CTRL P Q** to detach from the container. **Don't do** exit or CTRL + C or CTRL + D, since exiting the console will stop the container.
If you want to know the log directory, just give "logdir" on Camelot server console.

Eg:

Tue Jul02 12:37:12pm camuser **docker ps**

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
6ec14401e27b	containers.cisco.com/ucsol/camelot-coc7:12.6.8.0.0.0	"camserv -vp 5000"	3 weeks ago	Up 3 weeks		camelot00_camelot-00_1
813aa630b045	containers.cisco.com/ucsol/camelot-coc7:12.6.3.0.0.0	"camserv -vp 5002"	2 months ago	Up 6 weeks		camelot02_camelot-02_1
8a24303b8bf1	containers.cisco.com/ucsol/camelot-coc7:12.0.18.0.23.0	"camserv -vp 5003"	3 months ago	Up 2 months		camelot03_camelot-03_1
d882b1b19801	containers.cisco.com/ucsol/camelot-coc7:12.6.3.0.0.0	"camserv -vp 5001"	3 months ago	Up 2 months		camelot01_camelot-01_1
3e388e2b4287	containers.cisco.com/ucsol/camelot-coc7:12.5.27.0.0.0	"camserv -vp 5004"	7 months ago	Up 2 months		camelot04_camelot-04_1

REMOTE-CAM3-F-6A - (/repo/camelot/logs/camelot-00/05000_20190607_050502)
Tue Jul02 12:38:22pm camuser **docker attach 6ec14401e27b**

(camserv)% **logmask -moduleid * -level debug_5 -device file**
Warning!
setting global logging may have severe impact on server performance under load
Apply settings? [yes|no]
yes
Log level set
(camserv)% **logdir**
/var/camelot/logs/05000_20190607_050502
(camserv)%
Press CTRL P Q

Enable logs from client side (from python script) and find current log directory

Sometimes you may not be able to get into Camelot Server console especially when your Camelot running in docker contaners.

Follow below steps to enable logs from python script

Go to Python shell in your client machine (where you run your scripts)

import camelot
serv = camelot.create_camelot_server('<Camelot Server IP>', <'Camelot Server Port'>)
serv.log_mask(moduleid="*",level="debug_5",device="file")

Eg:
camelot@cam-ubuntu-249:~$ python
Python 2.7.12 (default, Nov 12 2018, 14:36:49)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import camelot
serv = camelot.create_camelot_server('10.12.10.178', '5000')
>>> serv = camelot.create_camelot_server('10.12.10.178', '5000')
serv.log_mask(moduleid="*",level="debug_5",device="file")[2019-06-05 10:01:44,442] [camelot.protocol.tcp.camelot_connection] [INFO] Client Version: 12.6.7.0.0.0
>>> **serv.log_mask(moduleid="*",level="debug_5",device="file")**
'Log level set'
>>>**serv.log_dir()**
'/var/camelot/logs/06060_20190703_133827'

SHIFT LEFT Camelot docker logs directory can be accessed from Docker Hosts /repo/camelot/logs/ directory

Enable logs from client side (from tcl script)

Follow below steps to enable logs from tcl script
Go to tclsh shell in your client machine (where you run your scripts) and do
package require camelotvapiei
camelot::logmask "<Camelot Server Ip>" "<Camelot Server Port>" -moduleid * -level debug_5 -device file
Eg:
[root@cam-updm-5 ~]# tclsh
% package require camelotvapiei
12.6.8.0.0.0
% camelot::logmask 10.12.10.178 5000 -moduleid * -level debug_5 -device file
Log level set
%

Camelot Troubleshooting Session (Webex Recording)

Session-Camelot-Troubleshooting-Webex-Recording

Camelot endpoint fails to register to CUCM

- Check that the CUCM node ,the TFTP server and IDP server [**IP address as well as Hostname**] are pingable from the Camelot host server.
  If you have multiple network interfaces/IPs in your Camelot machines, make sure you ping to destination from the phone ip you have configured in your script.
  Eg : ping 10.12.10.99 -I 10.12.10.200 (provided 10.12.10.99 is CUCM IP and 10.12.10.200 is sip.phone.ip configured in your script)

- Check that the Camelot's machine IP address are pingable from the CUCM node and the TFTP server.
- If CUCM IP is pingable, not the hostname ; then add CUCM entry to /etc/hosts file of Camelot machine.
- From the Camelot machine, see if you can TFTP/HTTP get the configuration file for the phone that won't register. If you can't tftp the file, check that the phone is configured in CUCM and the config file is built on the TFTP server.
  wget <CCM IP>:6970/<MAC ADDRESS>.cnf.xml **"OR"** tftp <TFTP SERVER IP> -c get <MAC>.cnf.xml
  Eg :
  wget http://10.12.10.105:6970/SEPDAAADAAA6001.cnf.xml **"OR"** wget https://10.12.10.18:6972/JABBEREP1200001.cnf.xml --no-check-certificate **"OR"** tftp 10.12.10.105 -c get SEPDAAADAAA6001.cnf.xml
  If file download is expected to happen over secure port 6971 or 6972. Try getting the file over wget
  eg: wget https://10.12.10.18:6972/JABBEREP1200001.cnf.xml --no-check-certificate
- If you are hitting camelot error "invalid sip.line configuration", either tftp config file <MAC ADDRESS.cnf.xml> download would have failed OR directory number configuration might be missing in your CUCM Device configuration page
- If you are hitting socket error or connection error in connection logs, try to do telnet to CUCM's desired ports from Camelot machine and see whether the connections are successful. Common ports used (depending on endpoint type and security profile) are 5060, 5061, 6970, 6971, 6972, 8443
  eg: telnet 10.12.10.1 5060
- If you are hitting issues with Single SignOn (SSO). Please make sure your Camelot, Identity Provider (OpenAM / ADFS) and CUCM are synced to same NTP server.
  Also make sure tomcat/openam/adfs are running and respective ports are open. You can do telnet <openam IP> <port> from Camelot machine to check this. Similarly check the connectivity for ADFS ip and port
  For syncing ADFS Windows 2008 machine to NTP. Execute below steps in Command Prompt (opened with admin privileges)
  net stop w32time
  w32tm /config /syncfromflags:manual /manualpeerlist:"NTP IP"
  w32tm /config /reliable:yes
  net start w32time

  To sync any Linux machines to NTP. Either configure /etc/ntp.conf with your NTP server address as first entry (eg: server 10.12.10.100 iburst) OR
  stop ntpd service (service ntpd stop) and manually sync using ntpdate command (eg: ntpdate 10.12.10.100)
- If your **jabber endpoint registration is failing**, make sure you have called gen_cert_key api before inservice and also configured below parameters
  sip.phone.sso.clientid
  sip.phone.domain
  sip.phone.username
  sip.phone.password
- If you are getting **"Could not get proxy/registrar/ccm information"** in the Camelot logs then try to ping the your cucm hostname and if not able to ping please add an entry for it to /etc/hosts file OR correct your DNS.

SCCP endpoint fails to register to CUCM

- Sample shift left skinny script for reference (edit the values according to your setup, start camelot, paste the script in ipython console (in your tngpi machine). Check ep1.get_info() to check state
  sk_8945_shift_left.py
- Enable logs and see if you are hitting "Reg Reject Reason: Error: DB Config" in logs, then mostly you would have configured wrong devicetype (skinny.phone.devicetype)
  Go to our old userguid http://wwwin-vts.cisco.com/camelot/userguides/camelot_10_6_0_0_3_28/camelotguide.html and search for devicetype ; find the exact match and provide that value

Camelot endpoint fails to register to EDGE

- Make sure "Secure endpoints fail to register" section criteria is met (except it's not mandatory to put CUCM to mixed mode unless your endpoint is using secured profile)
- Add CamelotRoot.crt file from /usr/local/camelot/lib/certsigner/ under VCS-E's Trusted CA Certificate
- Check your DNS server is configured properly. It has entries for _collab-edge._tls for your domain
- Check DNS server entry in your Camelot machine is proper (/etc/resolv.conf)
  Example /etc/resolv.conf file
  /etc/resolv.conf
  search camelot.test
  nameserver 10.12.10.58
  search cisco.com
  nameserver 72.163.128.140
- It's observed that in CentOS 6 and CentOS 7 machines sometimes NetworkManager overwrites /etc/resolv.conf
  To disable that, run below commands as root
  For CentOS 6
  service NetworkManager stop
  chkconfig NetworkManager off
  For CentOS 7
  systemctl stop NetworkManager
  systemctl disable NetworkManager.service
- Check nslookup is returning edge server details on Camelot machine
  eg: Our domain is "camelot.test". Please use your domain name instead of camelot.test in below command

nslookup -type=srv _collab-edge._tls.camelot.test
Windows Server DNS configuration http://www.teradici.com/web-help/ter1401005/2.4/04_DeviceDiscovery/02_DNS_SRV.htm

- Make sure the device MAC is present in user page's associated devices.
- Also add the user to access group "Standard CCM End Users"
- If your VCS version is >= 8.10 , set sip.phone.tls1dot2 Camelot endpoint configuration as 2

Secure endpoints fail to register

- Make sure your CUCM is in mixed-mode (Check it from CUCM admin page -> System -> Enterprise Parameters -> Cluster Security mode : It should be 1). You can set CUCM 11.0 and above to mixed mode by ssh'ing to CUCM publisher as admin and executing command "utils ctl set-cluster mixed-mode"
- Check that the Camelot root certificate(/usr/local/camelot/lib/certsigner/CamelotRoot.crt from Camelot machine) is uploaded (Call Manager OS Administrator Security Certificate Management Upload Certificate Chain) as CallManager-trust Certificate from platform administration page. Restart "Cisco CallManager, Cisco Tftp, Cisco CTL Provider, Cisco Certificate Authority Proxy Function Services" from Serviceability web pages
- Make sure Camelot server time is in sync with CUCM [and VCS-E (edge)]. It should never be ahead of CUCM or Edge server time. So sync everything to same NTP server. To manually do ntp sync from Camelot, first disable ntpd service in your Camelot box as root using "stop ntpd service" in CEL 5 or CentOS 5 or CentOS 6 ; for CentOS 7 use "systemctl stop ntpd". Then sync with NTP server using "ntpdate <NTP Server IP>" eg: ntpdate 10.12.10.100. Run your test and check bad certificate error is not coming.
https://www.thegeekdiary.com/centos-rhel-how-to-configure-ntp-server-and-client/
- Old Camelot Root Certificate is getting **expired on 29-AUG-2016**. So if your secured endpoints are not registering,
EITHER upgrade to latest Camelot Version, and repeat step 1
OR unzip certsigner.zip and put the contents under /usr/local/camelot/lib/certsigner/ folder and repeat step 1.

Jabber on-prem endpoints fail to register

- Make sure Camelot root certificate(/usr/local/camelot/lib/certsigner/CamelotRoot.crt from Camelot machine) is uploaded (Call Manager OS Administrator Security Certificate Management Upload Certificate Chain) as CallManager-trust Certificate from platform administration page. Restart "Cisco CallManager, Cisco Tftp, Cisco CTL Provider, Cisco Certificate Authority Proxy Function Services" from Serviceability web pages
Jabber uses secure connection to 6972 port of CUCM for downloading config files. That's why we've to do the above step.
- Make sure CUCM and Camelot are synced to same NTP server.
https://www.thegeekdiary.com/centos-rhel-how-to-configure-ntp-server-and-client/

To update the Root certificates on UCM nodes:

1. Login to OS Administration on UCM Pub and go to Security Management
2. Login to OS Administration on any other UCM Subscriber node and go to Security Management
3. Find Camelot certificate on both nodes. Search "Camelot" by Common Name
4. Open and delete the old certificate from Pub
5. Wait a few minutes (the deletion process will keep spinning)
6. Verify the certificate is gone from the Sub (automatically)
7. Upload the new certificate with "CallManager trust" on Pub
8. Wait for a few minutes
9. Verify the new certificate is now also present on the Sub
10. Register the Camelot endpoints (no need to restart CUCM services or reboot nodes)

Jabber / Jabber Mobile imp/xmpp login failure due to "Invalid AUTH_TYPE"

- If you are using CUCM/CUP versions 12.0+ , make sure you are setting below parameters explicitly to override the default value "10.0.0.0"
"cupc.user.clientversion":"12.0.0.0"

Registering new SIP phone models using Camelot

- Previously Camelot used to map each phone model using config parameter 'sip.phone.deviceid' (search deviceid in userguide)
- Now for the new models you can configure the model number (which real phone sends in REGISTER message) using '**sip.phone.modelnumber**' parameter
- Additionally you can also configure the **'sip.protocol.reguseragenthdr**' parameter in case you want Camelot to add that value in User-agent header
- if deviceid and modelnumber is configured, then the priority will be given to modelnumber.
- Some examples for modelnumber values for different phone models are given below
DX 650 : 647, SX 20 : 626, EX 60 : 604, EX 90 : 584, 7861 : 623
- Some examples for reguseragenthdr
DX 650 : Cisco-CP-DX650/9.3.1, EX 60 : SX 20 : TANDBERG/520, EX 60 : TANDBERG/518 (TE6.0.1.47c1258), EX 90 : TANDBERG/519 (TC7.0.0 Beta4)

Finding blobs to use with enable_auto_script command checkprompt

- Use Camelot's enable_auto_record feature to record the incoming traffic as rtp file.
- rtp file is located at /var/camelot_<version with underscore>/recordings/ directory
- Open that file in any Hex Editor (eg: HxD in windows)
- Copy the complete Hex content to another Text Editor (like notepad++ in Windows)
- Find and replace all " " (spaces) with "" (null)
- Select some part of the hex values, check whether it's repeating in the same file multiple times. (assumption : most of the announcements will be played in loop)
- If its repeating, the use that as blob with checkprompt command.

TNGpi troubleshooting

Feedback state received for call with ID, which TNG is not tracking

Condition

When our test is running it seems to have failed:

```
[device.Camelot] ERROR [<Camelot SIPTRUNK1 at CAMSIPTRUNK1>] Feedback
state 'ringing' received for call with ID '0xf043b200', which TNG is not
tracking!
'get_call_state' returned 'incoming' in 1.0 seconds

[device.Camelot] ERROR [<Camelot SIPTRUNK1 at CAMSIPTRUNK1>] Feedback
state 'connected' received for call with ID '0xf043b200', which TNG is not
tracking!
```

Resolution

These error messages are noise and do not cause a script to fail. This error log comes because Camelot state changes happens outside of TNGpi's state machine and TNGpi feels these are not expected changes, since Camelot calls Camelot APIs directly.

To suppress these messages in the logs, suppress TNGpi state tracking in your script by calling ep.feedback.stop_listening() once endpoint is created.