A MITEL
PRODUCT
GUIDE

OpenScape Voice

OpenScape Voice V10, Troubleshooting Guide

Service Documentation
01/2026

A31003-H80A0-S101-05-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 History of Changes

Issue	Date	Description
5	11/2025	Updated chapter Performance or Overload Issues on page 24.
4	03/2025	Added new chapters Basic troubleshooting on page 37 Centralized Call log issues with Unify Phone and Zoom PSI client on page 38 to cover issues with CLD integration
3	07/2024	Rebranding activities
2	11/2023	Updates on What to collect for all INCs and PRBs - Standard Package on page 7 Updates on Database (Solid) Issues on page 10 Updates on MLHG Issues on page 21 Updates on Failed Upgrade on page 30 New chapter CDM / CDAL issues on page 32
1	09/2023	Initial release

2 General Instructions

Before activating any tracing, first verify if tracing is already running on the system. If tracing is already running then coordinate with the system administrator to make sure there is no interference with other diagnostic activities.

It is important to always restore tracing to its original level, once done with diagnosing a specific issue.

To disable and restore original level of tracing you can:

- Login as *srx* user
- Navigate to *rtt_trace_scripts/ directory*
- Execute the following commands:

```
./hiq_all . off
./24_7_min
```

3 What to collect for all INCs and PRBs - Standard Package

The **Standard Package** should be included in all escalations and should contain:

- RapidStat in collect mode from both nodes
- RTTs with *24_7* or at least *24_7_min* tracing level enabled
- Scenario description, timestamp, Call IDs or UCE Context

NOTICE: If the problem is entirely reproducible and can be reproduced in a short period of time, it would be helpful to enable *hiq_all* instead of *24_7* or *24_7 min*, by using `./hiq_all .` command.

---

4 What to collect for all outage issues

This category addresses situations where a unknown problem causes the system to experience a outage situation which leaves users unable to place calls. This includes cases where several other symptoms are present, for example constant process restarts, system not accessible or slow system response.

In cases like this it is important to provide a comprehensive set of diagnostic data to allow for an overall system analysis. It is important to collect all the data before any attempt is made to recover the system via restart, etc.

- Collect **Standard Package**
- Collect TTUD and network or ethereal traces as described in section Network issues
- Likewise, in case of process lock ups, follow the instructions of Process Lock Ups section.
- If applicable, follow the instructions of System Does Not Answer SIP Requests section.
- Depending on your situation there might be additional symptoms present in your system, in which case it suggested to review the corresponding section and collect any applicable data.

5 What to collect for specific scenarios

5.1 Assistant Issues

- For Assistant issues enable *log4j_dsa.xml* before reproducing the scenario.

This can be done via **CMP** > **Maintenance** > **Monitoring** > **Tools & Utilities** > **Configuration Files**

- Login as *srx* on both nodes and enable the following extra RTT flag:

For both nodes:

```
cd rtt_trace_scripts
./soapserver_all
./submgtSchedule_all
```

When reproducing the scenario:

- Collect network traces from both nodes and also from CMP
- Collect **Standard Package**
- Collect *collect.sh*

5.2 CDR – Billing Issues

- The output of script *BillingScript* should be attached to the INC/PRB.

This is a shell script which collects debugging data for billing problems and can be run by *srx* user. It resides on the OpenScape Voice in */unisphere/srx3000/srx/bin/BillingScript* and is delivered as part of package *UNSPcdr*.

The output of the script is a file */tmp/BillingDebug.tar*. The script should be run for both nodes in case of a cluster system.

For FTP issues, script *UscFtpTest* should be used to check the FTP connection to primary and secondary billing servers. The script should be run separately on each node.

The script can be found in */unisphere/srx3000/srx/bin* folder and it can be run by *srx* user. Also, RTT trace shall be collected at the startup of the tool and while the *UscFtpTest* script is running:

```
oprtt_startup_ctl -a ADD_PROCESS
UscFtpTest:ALL_FACILITIES=-1
oprtt_read > ftpTest.txt
```

Besides *BillingScript* and *UscFtpTest*, additional data are needed:

log files from */log* folder, RtpDumpLog and CDRHandler RTT traces

Trace duration should be longer than the value configured in the *RTP ticket lifetime* value.

startCli and type `5 3 5` lifetime

RTT traces for CDR Handler should be collected by using following commands:

For node 1:

```
oprtt_ctl -p `pidof SrxCDRHandler01` OP_RTT_TRACE_ALL=-1
```

For node 2:

```
oprtt_ctl -p `pidof SrxCDRHandler02` OP_RTT_TRACE_ALL=-1
```

NOTICE: Check the FTP timeout value on billing server. The FTP timeout should be greater than the value configured in the RTP ticket lifetime parameter (*startCli* and type `5 3 5` lifetime) to avoid many loss of communication false alarms.

If there are issues with the conversion of CDRs (some CDRs have error extension) or CDRHandler cannot get the files from RTP, then RTT traces are needed from CDRHandler from both nodes (if the system is a cluster).

Please use RTT trace commands for CDR Handler above.

- Collect **Standard Package**

5.3 Call Park to Server Issues

- Collect **Standard Package**
- Collect OSV database backup export

5.4 CSTA Issues, including issues with OSCC

- Add *csta_all* flag to RTTs

Login as *srx* user execute on both nodes:

For node 1 and node 2:

```
>cd rtt_trace_scripts
./csta all
```

- Collect **Standard Package**

5.5 Database (Solid) Issues

- Collect **Standard Package**
- Collect **Database backup** (see Collect OSV Database Backup via SSH terminal).
- Add *submgtSchedule_all* and *soapServer_all* flags to RTTs
- Login as *srx* user execute on both nodes:

For node 1 and node 2:

```
cd rtt_trace_scripts
./submgtSchedule_all
./soapServer_all
```

- As the *srx* user, execute the command tools */unisphere/srx3000/callp/bin/tools*

This will show a menu on which you need to select item **83 System information - collects DB log files and data**. If requested enter the *root* password.

This will execute the utility that collects the database diagnostics. Once the diagnostics collection completes, you will be informed about the location of the generated files that you need to provide.

NOTICE: The database diagnostics can become very big, so they need to be removed from the system as soon as possible after they have been provided.

To remove database diagnostics from the system:

Login as *root* user and execute:

```
cd /var/RtpDb/log/supportinfo
rm -f support_*
```

5.6 Display and Number Modification

- Collect **Standard Package**
- Collect the *export_all* from CMP by:

Navigating to **Maintenance** > **Recovery** > **Export** > **OpenScape Voice**

Click *All configuration data*

Select *switch specific*

Select the name of your OSV switch

NOTICE: This process can take several minutes, depending on the size of the OSV database.

- Type `tools` at any directory to invoke the OpenScape tools and select option `8` for **ndal Memory Display**

Select **Yes** when prompted and provide the output.

5.7 Endpoint Audit Issues

Examples of Endpoint Audit Issues are loss of communication, inaccessible endpoint, missing or incorrect OPTIONS messages

- Collect network traces on both ends.

Endpoint (EP) audits are realized in the OSV through the interactions of several processes. This section is a consolidation of the tracing requirements for EP audit issues as well as some additional information to provide with a INC/PRB.

Information needed for EP audit issues

The majority of information needed can be found here, as it is common to all CQs.

In addition to this common information, the following information should be provided for EP audit issues:

- Is registration renewal enabled? (It should be enabled)
- Is the EP in question in inaccessible state?
- Are OPTIONS messages being sent to or received from the EP in question? (To see this, some sort of tracing is needed)

Tracing needed for EP audit issues

There are 7 processes which must be traced in order to provide the needed information to analyze EP audit issues. The required commands to enable tracing for these processes are shown below.

Since the process names are different, the information is provided for both nodes in the case of a duplex system.

This information can be copied directly to the command-line on the OSV and the user must be logged on as *srx* in order to execute them:

For node 1:

```
oprtt_ctl -p `pidof sipsm11` SIP=ERROR,INFO
oprtt_ctl -p `pidof XdmRegistrar1` XDM=-1
oprtt_ctl -p `pidof prmgr11` OP_RTT_TRACE_ALL=-1
```

For node 2:

```
oprtt_ctl -p `pidof sipsm21` SIP=ERROR,INFO
oprtt_ctl -p `pidof XdmRegistrar2` XDM=-1
oprtt_ctl -p `pidof prmgr21` OP_RTT_TRACE_ALL=-1
```

- Collect **Standard Package**

5.8 Feature Status – Call forwarding, Message Waiting and Do not Disturb

- When suspecting issues with the status information for CF, MWI and DND, collect traces for the Feature Status Notification (FSN) process and the SMDI (*smdiMgr1*) process:

Enter the following commands on each OSV node from the OSV RTT scripts directory:

```
/unisphere/srx3000/srx/rtt_trace_scripts
./hiq_all fsn
./hiq_all smdiMgr
```

When the traces have been collected, turn off this specific tracing on each OSV node by entering the following commands from the OSV RTT scripts directory:

```
/unisphere/srx3000/srx/rtt_trace_scripts
./hiq_all fsn off
./hiq_all smdiMgr off
```

Collect **Standard Package**

5.9 Internal Resource Manager (IRM) Issues

IRM is mainly responsible for monitoring the BW usage within BW limited links and disallow calls when the maximum capacity of the link is reached, to ensure that the quality of the existing calls is not degraded.

IRM interacts with SIP/ UCE and due to its participation in every single call scenario, it belongs to the processes for which traces should be collected and presented in all INCs/PRBs relevant to call processing (in addition to the traces needed for all INCs/PRBs, as described in Collect RTT Traces Without Trace Manager) section.

- To activate IRM traces, use the following commands:

For node 1:

```
oprtt_ctl -p 'pidof irm1' OP_RTT_TRACE_ALL=-1
```

For node 2:

```
prtt_ctl -p 'pidof irm2' OP_RTT_TRACE_ALL=-1
```

An automated script has been added to the switches that performs the above functionality. To invoke the script type the following:

```
./irm_all
```

- Collect **Standard Package**

5.10 Licensing Issues

- Login on both OSV nodes as *srx* and enable via SSH the following extra flag by executing:

```
oprtt_ctl LICENSING=-1
```

- Import OSV Licenses as described in *OpenScape Voice V10, Service Manual: Installation and Upgrades, Installation Guide.*
- Provide the license files for both nodes.
- As *root*, execute the following command via SSH on both nodes:

```
cd /opt/unisphere/srx3000/cla/bin/
```

```
./get_ali -f /opt/unisphere/srx3000/cla_inst/backup/
OSCVoice_V10.alf
```

- Provide the output of the above commands.
- Collect **Standard Package**

5.11 OpenScape Mobile (OSMO) Issues

If the scenario involves login failures in mixed mode (user has UC and OSMO configured), collect the OSV SOAP traces in addition to the UC traces.

- Login as *srx*
- Activate SOAP traces with:

```
cd rtt_trace_scripts
./soapServer_all
```

- Collect **Standard Package**

5.12 Port Display Manager (PDM) Issues

PDM is the process that handles requests from users (Cli, Assistant) to retrieve and display SIP or MGCP endpoint information.

To obtain the appropriate information regarding a problem with PDM, the trace flags of PDM need to be activated.

- Login as *srx* and execute:

```
cd rtt_trace_scripts
. /pdm_all
```

In some special cases, process startup information might be needed.

To obtain startup information for PDM the appropriate trace flags need to be added to the startup list.

- To do so you need to enter the following command:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS pdm1:ALL_FACILITIES=-1
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS pdm2:ALL_FACILITIES=-1
```

- Collect **Standard Package**

5.13 Prevention & Recovery Manager (PRM) Issues

PRM is the process that deals with audits (SIP endpoint audits and Media Server audits).

To obtain the appropriate information regarding a problem with audits, the trace flags of PRM need to be activated.

- Login as *srx* and execute:

```
cd rtt_trace_scripts
./prm_all
```

In some special cases process startup information might be needed. To obtain startup information for PRM the appropriate trace flags need to be added to the startup list.

- To do so you need to enter the following command:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS prmgr11:ALL_FACILITIES=-1
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS prmgr21:ALL_FACILITIES=-1
```

- Collect **Standard Package**

5.14 Retailer and Subscriber System (RSS)

The *rsstest* tool can be used in order to dump RSS's shared memory data to a text file.

- Login as *srx* and execute:

```
rsstest -l rssdump -p
```

By default the output file will be in *~srx/RssSharedMemory.txt*

- Collect the *RssSharedMemory.txt*
- Collect database backup from OSV terminal
- Collect **Standard Package**

5.15 SDM/SDAL Issues

- Login on both OSV nodes as *srx* and enable via SSH the following extra flag by executing:

```
oprtt_ctl SDAL=-1
```

```
oprtt_ctl SDM=-1
```

If the problem is between the SDAL and DB interface, activate the following facilities(*):

```
oprtt_ctl SDAL=-1
```

```
oprtt_ctl SDM=-1
```

```
oprtt_ctl DBSQLLAYER=-1
```

(*) If the issue is caused at startup, then the traces shall be activated before starting up RTP.

In order to do that, execute the following command instead:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS Sdm1:ALL_FACILITIES=-1
```

For node 2 (Sdm2):

```
oprtt_startup_ctl -a ADD_PROCESS Sdm1:ALL_FACILITIES=-1
```

- Collect **Standard Package**
- Type `tools` at any directory to invoke the OpenScape tools and type `34` for **sdalMemDisplay**

The SDAL data stored in the shared memory tables are exported to the text file:

/unisphere/srx3000/callp/etc/sdal/sdalInit.result.txt

Select the above file and attach it to any INC/PRB opened against SDAL. The file contains a result section, for each of the selected components.

5.16 Silent Monitoring / Continuous Silent Monitoring (SILM) or Executive Busy Override

- Login on both OSV nodes as *srx* and enable via SSH the following extra flag by executing:

```
oprtt_ctl CCM=-1
oprtt_ctl SDM=-1
```

- Collect **Standard Package**

5.17 SIP Endpoint Registration Issues

If this issues occur when the system is up and running

For node 1:

- Login as *srx*:
- Activate XDM RTT facility for XDM processes:

```
oprtt_ctl -p `pidof Xdm1` XDM=-1
oprtt_ctl -p `pidof XdmDispatcher1` XDM=-1
oprtt_ctl -p `pidof XdmRegistrar1` XDM=-1
oprtt_ctl -p `pidof XdmDbRegistrar1` XDM=-1
```

- Activate SIPREG RTT facility for SIPRegistrar processes:

```
oprtt_ctl -p `pidof sipRegistrar11` SIPREG=-1
oprtt_ctl -p `pidof sipRegistrar22` SIPREG=-1
```

- Collect RTT traces in binary format:

```
oprtt_read -c >n1_tracefilename.raw
```

For node 2:

- Login as *srx*:
- Activate XDM RTT facility for XDM processes:

```
oprtt_ctl -p `pidof Xdm2` XDM=-1
oprtt_ctl -p `pidof XdmDispatcher2` XDM=-1
oprtt_ctl -p `pidof XdmRegistrar2` XDM=-1
oprtt_ctl -p `pidof XdmDbRegistrar2` XDM=-1
```

- Activate SIPREG RTT facility for SIPRegistrar processes:

```
oprtt_ctl -p `pidof sipRegistrar21` SIPREG=-1
oprtt_ctl -p `pidof sipRegistrar12` SIPREG=-1
```

- Collect RTT traces in binary format:

```
oprtt_read -c > n2_tracefilename.raw
```

If the issue occurs during system startup

If the issue is caused/reproduced at start-up, traces should be activated before starting up RTP. To do so execute the following commands:

For node 1:

- Login as *srx*:
- Activate XDM RTT facility for XDM processes:

```
oprtt_startup_ctl -a ADD_PROCESS Xdm1:XDM=-1
oprtt_startup_ctl -a ADD_PROCESS XdmDispatcher1:XDM=-1
oprtt_startup_ctl -a ADD_PROCESS XdmRegistrar1:XDM=-1
oprtt_startup_ctl -a ADD_PROCESS XdmDbRegistrar1:XDM=-1
```

- Activate SIPREG RTT facility for SIPRegistrar processes:

```
oprtt_startup_ctl -a ADD_PROCESS sipRegistrar11:SIPREG=-1
oprtt_startup_ctl -a ADD_PROCESS sipRegistrar22:SIPREG=-1
```

- Collect RTT traces in binary format:

```
oprtt_read -c > n1_tracefilename.raw
```

For node 2:

- Login as *srx*
- Activate XDM RTT facility for XDM processes:

```
oprtt_startup_ctl -a ADD_PROCESS Xdm2:XDM=-1
oprtt_startup_ctl -a ADD_PROCESS XdmDispatcher2:XDM=-1
oprtt_startup_ctl -a ADD_PROCESS XdmRegistrar2:XDM=-1
oprtt_startup_ctl -a ADD_PROCESS XdmDbRegistrar2:XDM=-1
```

- Activate SIPREG RTT facility for SIPRegistrar processes:

```
oprtt_startup_ctl -a ADD_PROCESS sipRegistrar21:SIPREG=-1
oprtt_startup_ctl -a ADD_PROCESS sipRegistrar12:SIPREG=-1
```

- Collect RTT traces in binary format:

```
oprtt_read -c > n2_tracefilename.raw
```

- For both nodes execute the following:

```
rm /unisphere/srx3000/callp/etc/xdm/XdmShmInit.result.txt
```

Type `tools` at any directory to invoke the OpenScape tools and type `33` for **XdmShmDisplay**.

The result of the above command is located in */unisphere/srx3000/callp/etc/xdm/XdmShmInit.result.txt* and should also be provided when opening an INC/PRB from both nodes.

For both nodes execute the following commands:

```
rm /unisphere/srx3000/callp/etc/xla/xlaInit.result.txt /
unisphere/srx3000/callp/bin/xlaMemDisplay
```

Answer `y` to all prompts or hit ENTER

The result of the above command is located in the paths below and should also be provided when opening an INC/PRB from both nodes

/unisphere/srx3000/callp/etc/xla/xlaInit.result.txt

/unisphere/srx3000/callp/etc/xla/xlaInit.registrationInfo.txt

- Collect **Standard Package**

5.18 SIP – HUNG SIP Calls

- Login as *srx* user, run the following commands and attach the files to the INC/PRB:

```
sipsmdump -c > sipsmdump.contexts.txt
```

```
sipsmdump -d > sipsmdump.dialogs.txt
```

This will show the existing contexts and dialogs in SIP shared memory.

Contexts older than 24 hours are candidates for hung calls.

- Collect **Standard Package**

5.19 SNMP Alarm Troubleshooting

- Provide */etc/snmp/snmpd.conf*
- Execute the following CLI expert mode command and provide the output:

You can obtain this information from **startCli** menu:

Type `98` for *Expert Mode*, then type the following command:

```
EvtGetSnmpEventFilters
```

- Provide the value of RTP Parameter *Rtp/Adm/eventMgmt/impl/snmp/sendGenericTrap*

You can obtain this information from **startCli** menu by typing `112` for **getParameterInfo**.

5.20 SOAP Issues

- Login as *srx* on both nodes and enable the following extra RTT flag:

For both nodes execute the following commands:

```
cd rtt_trace_scripts
```

```
./soapserver_all
```

- Reproduce the scenario
- Collect network traces on both nodes and also from CMP
- Collect screenshots showing the error on CMP.
- Collect OSV Database Backup (as described in Collect OSV Database Backup via SSH section).

- Collect **Standard Package**

  soapExport

  If the provisioning problem has to do with exporting provisioned data, RTT traces of the *soapExport* should be captured and attached on the INC/PRB.

  To perform such action follow the steps of the section, except a different script, that is:
  Activation of RTT traces as the process starts up:

  ```
  ./soapExport_all -s
  ```

  This deactivates the RTT traces as the process starts up:

  ```
  ./soapExport_all -s off
  ```

  Note that when tracing the soapExport process and especially when this is initiated via the OSV Assistant GUI, soapExport RTT traces should be collected from both nodes.

  soapMassProv

  The file that was attempted to be imported, along with the output log are the mandatory pieces of information that should be attached to INC/PRB.

  soapMassProv RTT traces might also be requested by development. To capture those, the steps are the same as the ones described in X section, except a different script, that is:

  Activation of RTT traces

  ```
  ./soapMassProv_all -s
  ```

  Deactivation of RTT traces:
  ```
  ./soapMassProv_all off
  ```

5.21 SOAP/Assistant collective information regarding E/A Cockpit issues

- For Assistant problems enable *log4j_dsa.xml* before reproducing the scenario.

This can be done via **CMP** > **Maintenance** > **Monitoring** > **Tools & Utilities** > **Configuration Files**.

- Login as *srx* user and on both nodes enable the following extra RTT flag:

For both nodes:

```
cd rtt_trace_scripts
```

```
./soapserver_all
```

- When reproducing the scenario execute the command below:

```
tshark -i any -w /software/test.pcap port 5060
```

- Collect **Standard Package**
- Collect *collect.sh*

5.22 TLS – Any scenario that involves TLS devices

- If a network issue is suspected, collect TTUD and network (ethereal, t-shark) traces when running the scenario.

TTUD Traces

Switch on TTUD trace:

```
oprtt_ctl TTUD=-1 TTUD_NET=-1
```

When tracing is finished, switch off TTUD trace:

```
oprtt_ctl TTUD=0 TTUD_NET=0
```

- Collect network traces from both ends
- Collect **Standard Package**

5.23 Translation / Routing Issues During Call Processing

- For both nodes execute the following commands:

```
rm /unisphere/srx3000/callp/etc/xla/xlaInit.result.txt
```

```
/unisphere/srx3000/callp/bin/xlaMemDisplay
```

Answer **y** to all prompts or hit `ENTER`

- The results of the above command are located at the paths below and should also be provided when opening an INC/PRB from both nodes.

/unisphere/srx3000/callp/etc/xla/xlaInit.result.txt

/unisphere/srx3000/callp/etc/xla/xlaInit.registrationInfo.txt

- Login as *srx* user and enable the following extra RTT flag by executing:

```
oprtt_ctl XLA=-1
```

- Collect **Standard Package**

NOTICE: Once finished, you can disable this flag by executing `oprtt_ctl XLA=0`

5.24 Translation / Routing Issues During Provisioning or Startup

- Activate the following facilities(*):

```
oprtt_ctl -p 'process_list' XLA=-1 XDM=-1 DBSQLLAYER=-1
NDM=-1
```

where *process_list* is the comma separated list of pids for the following processes.

For node 1:

soapServer, Xdm1, Cli

For node 2:

soapServer, Xdm2, Cli

(*) If the issue is caused at startup, then the traces shall be activated before starting up RTP.

To do so execute the following command instead:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS
Xdm1:XLA=-1,XDM=-1,DBSQLLAYER=-1
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS
Xdm1:XLA=-1,XDM=-1,DBSQLLAYER=-1
```

- Collect the *export_all* from CMP by:

Navigating to **Maintenance** > **Recovery** > **Export** > **OpenScape Voice**

Select **All configuration data**

Select **switch specific**

Select the name of your OpenScape Voice switch

- Collect **Standard Package**

5.25 MLHG Issues

For issues concerning MLHG or an MLHG call please activate also the MLHG process traces.

To activate MLHG traces:

For node 1:

```
oprtt_ctl -p `pidof MLHG11` OP_RTT_TRACE_ALL=-1
```

For node 2:

```
oprtt_ctl -p `pidof MLHG21` OP_RTT_TRACE_ALL=-1
```

- For issues involving MLHG, please also collect the MLHG Shared Memory snapshot in addition to the RTT traces:

```
/unisphere/srx3000/srx > mlhgprint
```

This command will create the file *mlhgSharedMemory.txt* in the current directory.

Attach that file to the INC/PRB.

NOTICE: If the problem consists execute `mlhgprint` before and after the scenario.

- Collect **Standard Package**
- Also, perform the following and provide the output file:

```
cd /unisphere/srx3000/srx/dbscripts/repair
./check_mlhg.sh
```

6 What to collect for more specific platform and system scenarios - Specific Issue Package

6.1 Backup

- Collect **Standard Package**

6.2 EZ-IP ifgui update mode (easy-IP)

- Collect **Standard Package**
- A complete log of all actions performed by service personnel prior to and during the *node.cfg* update
- Any screenshot on the Windows or Linux PC hosting the *ifgui* that shows the produced error message
- The directory ifgui from the user's home directory:

If run from a Windows PC this is the directory *C:\Documents and Settings \<username>\ifgui*.

If run from a Linux PC, this is the directory *~<username>/ifgui*.

- The directory */opt/unisphere/srx3000/ifw* from both nodes:

Execute as *root* for each node:

```
tar -C /opt/unisphere/srx3000 -zhcf ifw.tar.gz ifw
```

Collect and send the file *ifw.tar.gz* from each node.

- The directory */etc*

Execute as *root* for each node:

```
tar -C / -zhcf etc.tar.gz /etc
```

- Collect and send the file *etc.tar.gz* from each node.

6.3 Linux Kernel Audit (Audit)

- Collect **Standard Package**

Collect the following:

- Output of `ls -l of /software/securityLogs`
- Output of `ls -l of /var/log`
- Copy of `/var/tmp/SrxSecEvtReactor.log`
- Copy of `/etc/audit/audit.rules`
- Output of `rcauditd status`
- Output of `auditctl -s`

6.4 NCPE

- Collect **Standard Package**
- Screenshot of the erroneous panel
- Screenshot of CHECK panel (Expert Mode – Ctrl + E)
- NCPE (or Offline Wizard) version
- Platform (Windows/Linux)
- Java version

6.5 Network Issues

If a network issue is suspected, collect TTUD and network (ethereal, t-shark) traces when running the scenario.

TTUD Traces

Switch on TTUD trace on both nodes:

```
oprtt_ctl TTUD=-1 TTUD_NET=-1
```

- Collect **Standard Package**

When tracing is finished, switch off TTUD trace on both nodes:

```
oprtt_ctl TTUD=0 TTUD_NET=0
```

TTUD Startup Issues

Enable the following extra RTT flag:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS ttud1:ALL_FACILITIES=-1
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS ttud2:ALL_FACILITIES=-1
```

To disable the flag:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS ttud1:ALL_FACILITIES=0
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS ttud2:ALL_FACILITIES=0
```

6.6 Operational Measurement Management (OMM)

The Operational Measurement Management is a statistic tool that provides traffic usage data upon the OpenScape Voice for various figures.

- To retrieve RTP tracers please run the following commands:

For node 1:

```
oprtt_ctl -p `pidof OMM1` OP_RTT_TRACE_ALL=-1
```

For node 2:

```
oprtt_ctl -p `pidof OMM2` OP_RTT_TRACE_ALL=-1
```

For retrieving RTT startup tracers:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS OMM1:ALL_FACILITIES=-1
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS OMM2:ALL_FACILITIES=-1
```

- Collect **Standard Package**

6.7 Packet Filter Rule (Firewall) Issues

If the OSV is not in state 4, please provide the following file:

/unisphere/srx3000/callp/etc/sec/FILT_START.txt

From one node:

Output from expert mode CLI command:

```
startCli -x -l sysad
PktFltrRulesQuery ""
```

- Collect **Standard Package**

6.8 Performance or Overload Issues

You can collect performance statistics and minimize trace impacts during load runs to avoid performance or overload issues.

These procedures help identify the root causes of degraded system performance, prevent excessive resource consumption, and ensure stable service operation during high-load conditions.

6.8.1 Collecting Performance Statistics

You can collect performance statistics via the **bg_monitor** collection tool.

If the OSV server experiences performance degradation resulting in service impact, the **bg_monitor** performance statistics collection tool will continuously sample data from the following utilities: *vmstat*, *top*, *mpstat*, *iostat* and *iotop*.

The collected statistics are rotated and compressed **hourly** to prevent the server's storage from filling up.

By default, data from the last six hours is retained, and older files are automatically deleted.

A minimum of **200 MB** of free disk space is required to store these statistics.

If this requirement is not met, the user will be prompted to select another disk partition with sufficient available space.

bg_monitor help menu

Run the utility as root by executing the following command:

```
cd ~srx/../callp/bin/

./bg_monitor -h

Write performance statistics from the following tools:

vmstat, top, mpstat, iostat and iotop

Syntax: bg_monitor [-d <output_dir>] [-i <sec>] [-r
<hours>] [-h] [stop]

-d: directory where to save the output (default: current
directory)

-i: sampling period (default: 3 sec.)

-r: the number of rotated logs to keep (default: 6).
Normally, logs are rotated on a hourly base.

-h: print this help

stop: terminate bg_monitor. It should be used before
harvesting the collected statistics.
```

Basic execution steps:

1) Run the utility as root by executing the following command:

```
cd ~srx/../callp/bin/

./bg_monitor -d [directory where to save the output] -r
[the number of rotated logs to keep, (default: 6 hours)]
```

For example:

```
cd ~srx/../callp/bin/

./bg_monitor -d /software/data -r 10
```

NOTICE: The specified directory must exist before executing the script.

2) Once started, the utility runs in the background as a daemonized process, allowing the user to safely log off the system.

3) Finally, After the issue symptoms occur, and within the log retention time frame, stop the utility before collecting the data:

```
cd ~srx/../callp/bin/

./bg_monitor stop
```

4) Collect and transfer outside of the OSV Server the data collected under the specified directory.

6.8.2 Minimizing Trace Impact During Load Runs

The critical part is to use the minimum amount of trace flags during the load run to prevent the traces from overloading the system and causing *503* errors.

Before proceeding to the trace flags:

Do not capture the traces by hand (by running *oprtt_read* in the command line). This will create a huge trace file that is hard to work with. Instead, use *TraceManager*.

Try the load run with these trace flags first (the following line is important as it will turn off all flags before adding only what is needed):

```
/unisphere/srx3000/srx/rtt_trace_scripts/hiq_all . off
```

For node 1:

```
oprtt_ctl -p `pidof ttudProc1` OP_RTT_MSG=MSG_EXT
```

For node 2:

```
oprtt_ctl -p `pidof ttudProc2` OP_RTT_MSG=MSG_EXT
oprtt_ctl SIP=ERROR,INFO
oprtt_ctl CSTA_TRACE=ERROR,INFO
oprtt_ctl UCE=-1
oprtt_ctl SVC=-1
```

The first line ensures all flags are off. The other lines activate minimal tracing for SIP, UCE and CSTA.

If SIP SM is sending 503 error codes with the trace flags above, it may indicate the trace itself is overloading the system.

To exclude that from the possible causes, switch to bare minimum tracing:

```
/unisphere/srx3000/srx/rtt_trace_scripts/hiq_all . off
oprtt_ctl -p `pidof ttudProc1` OP_RTT_MSG=MSG_EXT
```

If node 2 is also being used for the load run:

```
/unisphere/srx3000/srx/rtt_trace_scripts/hiq_all . off
oprtt_ctl -p `pidof ttudProc2` OP_RTT_MSG=MSG_EXT
```

Run the load again. If 503 errors are still present, collect the traces and the other pieces of information listed in this section.

6.9 Cluster Issues

- Collect **Standard Package**
- Collect network traces from cluster interface on both ends.

6.10 Process Lock Ups

Two symptoms are an indication of a process lock up. Processes are not crashing (there are no new stack dump files in the system), but the system is either:

1) Not responding to the devices or
2) Running very slowly (responds to the devices after several seconds)

For those cases please collect the output of the **top** command and force the generation of a stack dump for the process that is using CPU the most and/or the processes involved in the scenario.

How to collect the output of top command

Use the top command to find out what process is using the CPU the most:

```
top -b -n 5 > /software/top_output.txt
```

Let the process finish (go back to the command line prompt) and attach the file to the INC/PRB.

For which processes is the stack dump needed

As a general rule, collect the stack dump for the first five processes listed on top. Also collect the stack dump for UCE and all the signaling managers involved in the scenario.

Use the `ps -ax | grep <process name>` command to find the process id (Pid).

For example `ps -ax | grep -i sipsm` results ***2432*** *X Sl 0:03 sipsm11 -i 11 -n 1 -a sipsm_G1 -r ucerr*

The following table shows the usage of "process names", to find specific processes in the system.

Use that text in the grep command inside single quotes, as shown in the example above.

Process	node A	node B
uce	uce[1/2]	uce[3/4]
sipsm	sipsm[11/22]	sipsm[12/21]

How to force the generation of a stack dump of a process

Find out the the process ID and force a stack dump with:

```
gstack <pid> > /software/gstack_output.txt
```

Attach the file to the INC/PRB.

6.11 Pstacks, Process Crashes, System Restarts or System Malfunctions

- Collect **Standard Package**
- Collect the last two minutes of RTT leading to the *pstack* (to the first pstack, if several pstacks were created).

Please transfer the RapidStat data first, then the RTT files, so the investigations can start as soon as possible.

6.12 Rapidstat

In case of issues with RapidStat please provide the output from the debug mode:

```
cd ~srx/bin
```

```
./RapidStat -d -b -R 2>&1 | tee -a /software/
RapidStat_debug.out
```

Send the file */software/RapidStat_debug.out*

If Rapidstat cannot be ran at all, when opening a INC/PRB, also provide the output of *trace8k* by executing as *srx* user:

```
cd ~srx/bin/
./trace8k
```

6.13 Rolling Upgrade

- Provide RapidStat in collect mode

6.14 Resilient Telco Platform (RTP)

In case of issues with Resilient Telco Platform processes:

- Provide Rapidstat in collect mode

As user *srx* on each OSV node run:

```
RtpDiagSnap -p 40
```

This results in RTP diagnostic data to be written to */unisphere/srx3000/srx/40/log/DIAG/*.

After *RtpDiagSnap* command completes for each node, collect a tar of */unisphere/srx3000/srx/40* as *root* user by executing:

```
tar cvfz /software/rtp-40-diag.tgz /unisphere/srx3000/
srx/40
```

For each node, send */software/rtp-40-diag.tgz*

NOTICE: If the local node's RTP state was 2 (solid not running) prior to executing *RtpDiagSnap* command, the node's RTP state will change and remain at state 3 (solid running).

6.15 SMUCOM Channel

Enable the following extra RTT flag by executing as *srx* user the following:

For node 1:

```
./hiq_all smucom1
```

For node 2:

```
./hiq_all smucom2
```

- Collect **Standard Package**

Afterward you can disable the extra flag by executing as *srx* user the following commands:

For node 1:

```
./hiq_all smucom1 off
```

For node 2:

```
./hiq_all smucom2 off
```

- As root user, display TCP network connections from both nodes at the time where the issue occurs and store in a file by entering:

```
netstat -tap > netstatX.txt
```

where X is the node ID and its values can be 1 or 2.

- As root user, display PFRs from both nodes at the time where the issue occurs and store in a file by entering:

```
iptables -vnL > iptablesX.txt
```

where X is the node ID and its values can be 1 or 2.

- Collect network traces from both nodes for all interfaces at the time where the issue occurs.

6.16 Simple Network Time Protocol (SNTP) Troubleshooting

- Provide the following files from both nodes:

```
/etc/ntp.conf
```

```
/etc/ntp.conf.cluster
```

```
/var/ntp/ntp.log
```

```
/var/lib/ntp/drift/ntp.drift
```

- On both nodes, provide the results for the following commands:

```
ntpq -pn
```

- From one node:

Output from expert mode CLI command:

```
startCli -x -l sysad
```

Type `98` for *Expert Mode* and execute the following commands:

```
openlog filename.txt
```

```
PktFltrRulesQuery ""
```

```
closelog
```

Output is stored in */unisphere/srx3000/srx/*

- Collect **Standard Package**
- Trace from each node and send the file */tmp/ntp.cap*

```
tshark -i any -f "port 123" -w /tmp/ntp.pcap
```

Press Ctrl + C for the trace to end when the packets are collected.

6.17 Failed Upgrade

In most cases when an error occurs during the image upgrade process, the fallback to the source release is initiated automatically and data is collected automatically for analysis of the error. In case an automatic fallback is not initiated by the system, the user can initiate the fallback manually and you need to provide the following data prior to falling back.

Specify the source software version, the target image and the toolkit version.

Run `upgrade8k -collect` on node 1.

This command will collect data from both nodes and places them in a single compressed file named *data-<clusterName>.tar.gz*, in the */log* directory of node 1.

NOTICE: Please check the file */log/prepare8k.log* for clues about the failure. Information regarding the timing of the upgrade is available on node 1 in file */repository/upgrade8k-timing*.

Run `RapidStat -b -c` on node 1 and provide the output files.

Additionally, extra files from fallback partition are needed, such as a screenshot if the system freezes.

1) Determine the fallback partition:

As root run `cd ~srx/bin`

followed by `./sync8k -d`

See if the fallback partition (the one which contains the target version) it is either primary or secondary (here specified as <partition> in further context.

2) On node 1 as root, run the following:

```
cd /software
```

```
tar -cvf extraLogs.tar /img/logimg/<partition> /img/
softwareimg/<partition>/AuditLogs /img/softwareimg/
<partition>/changeLogs /img/varimg/<partition>/log/mess*
```

```
tar -cvf extraDBData.tar /img/homeimg/<partition>/
solid/RtpSolid* /img/homeimg/<partition>/solid/RtpDb/
solid.db /img/varimg/<partition>/RtpDb/solmsg*
```

```
tar -cvf extraData.tar /img/varimg/<partition>/RtpDb/
dba.secrets /img/rootimg/etc/hosts /img/rootimg/etc/
hiq8000/node.cfg
```

```
gzip extraLogs.tar
```

```
gzip extraDBData.tar
```

3) Provide the following:

extraLogs.tar.gz

extraDBData.tar.gz

extraData.tar

6.18 Softswitch Patching Tool (SPT)

- Provide Rapidstat in collect mode

6.19 System Does Not Answer SIP Requests

- Collect TTUD and network (ethereal, t-shark) traces when running the scenario.

TTUD Traces

Switch on TTUD trace on both nodes:

```
oprtt_ctl TTUD=-1 TTUD_NET=-1
```

- Collect **Standard Package**

When tracing is finished, switch off TTUD trace on both nodes:

```
oprtt_ctl TTUD=0 TTUD_NET=0
```

TTUD Startup Issues

Enable the following extra RTT flag:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS ttud1:ALL_FACILITIES=-1
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS ttud2:ALL_FACILITIES=-1
```

To disable the flag:

For node 1:

```
oprtt_startup_ctl -a ADD_PROCESS ttud1:ALL_FACILITIES=0
```

For node 2:

```
oprtt_startup_ctl -a ADD_PROCESS ttud2:ALL_FACILITIES=0
```

6.20 Virtualization

For any virtualization errors provide the following:

- Screenshot of both of the VM servers **Virtual Machine Properties - Hardware Tab**, which can be obtained by clicking **Edit Virtual Machine Settings**.
- Screenshot of the ESXi virtual switch configuration which can be obtained by clicking the **ESXi server IP** in *vSpehere Client* and then choosing the **Configuration** tab and **Networking** in the hardware box.
- For both servers, provide the mapping of the physical connections made from ethernet ports behind the server to the network switch or to the partner server.

6.21 CDM / CDAL issues

Login as *srx* user:

- Find pids

```
ps -ef | grep -i cdm
```

On node 1:

```
oprtt_ctl -p <pid cmd1> OP_RTT_TRACE_ALL=-1 (needed for
sure CDAL=-1 DBSQLLAYER=-1)
```

`oprtt_ctl -lo` (just to see if traces are OK)

If yes, run:

```
oprtt_read > /software/cdm1_trace.txt
```

On node 2:

```
ps -ef | grep -i cdm
```

```
oprtt_ctl -p <pid cmd2> OP_RTT_TRACE_ALL=-1 (needed for
sure CDAL=-1 DBSQLLAYER=-1)
```

```
oprtt_ctl -lo (just to see if traces are O.K.)
```

If yes, run :

```
oprtt_read > /software/cdm2_trace.txt
```

- Also, provide contents from certain DB tables

```
for mytable in CERTIFICATE_REVOCATION_LIST_T CERTIFICATE_T
CLIENT_CERTIFICATE_T DISTINGUISHED_NAME_T;do /opt/solid/
bin/solexp -x pwdfile:/var/RtpDb/dba.secrets "tcp 16760"
dba $mytable;done
```

- Provide **.ctr* and **.dat* files
- Collect **Standard package**

7 How-Tos

7.1 Rapidstat

RapidStat provides a means to check OpenScape Voice (OSV) system health status, as this is represented by various health indicators. It applies to all OSV deployments and configurations.

It is typically executed at regular intervals via *Cron* jobs and also utilized before maintenance activities (to ensure a healthy system prior to maintenance) or after them (to verify nothing has been affected negatively by the maintenance).

RapidStat has two modes of operation:

Status display Mode and *Data Collection Mode*.

Status Display Mode: In this mode, RapidStat generates a system health report for on-the-spot analysis. A summary of Warnings and Errors found is appended to the end of the report as a summary, and a Minor Alarm is generated to alert the relevant Network Operations Center (NOC). This is the most typical operational mode.

Rapidstat in Status Display Mode can be executed via SSH terminal as root by typing:

```
cd ~srx/bin
./Rapidstat -s
```

If you want to display the RapidStat info from the other node too without opening a new terminal you can add *-b* flag at the command, for example `./Rapidstat -s -b`

Data Collection Mode: In this mode, RapidStat collects multiple log files and other debugging data and prepares a file that can be collected with FTP or SFTP to the interested parties (e.g. GVS or Development) for further analysis.

Rapidstat in Data Collection Mode can be executed on each node separately or executed on one node and automatic collect logs from the other node too.

In order to collect RapidStat from both nodes execute only on node 1 via SSH terminal as *root* the following :

```
cd ~srx/bin/
./RapidStat -c -b
```

In order to collect Rapidstat only from one node 2 execute via SSH terminal as *root* the following :

```
cd ~srx/bin/
./RapidStat -c
```

When prompt appears to collect logs from the other node, press the letter `N` and then `ENTER`

7.2 Determine RTT Trace Levels

How to determine which RTT trace levels (24_7, 24_7_min, 24_7_extern) are running from SSH terminal

Login to each node via SSH and switch user to *srx* by typing :

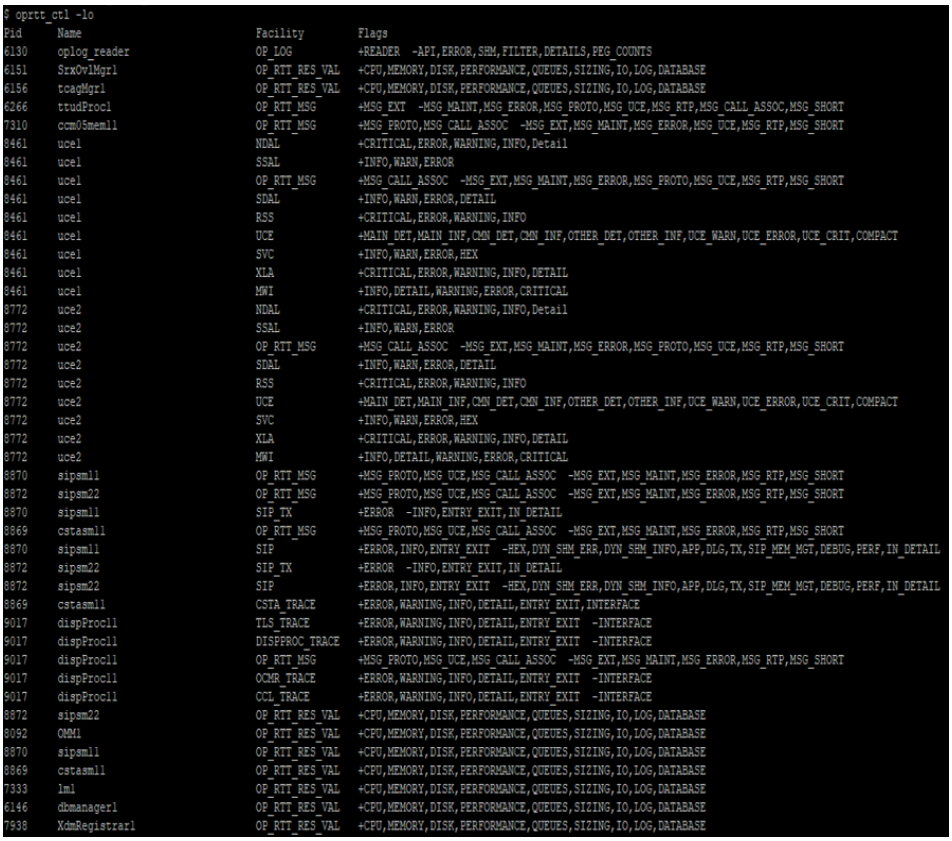
```
su - srx
```

Next execute :

```
oprtt_ctl -lo
```

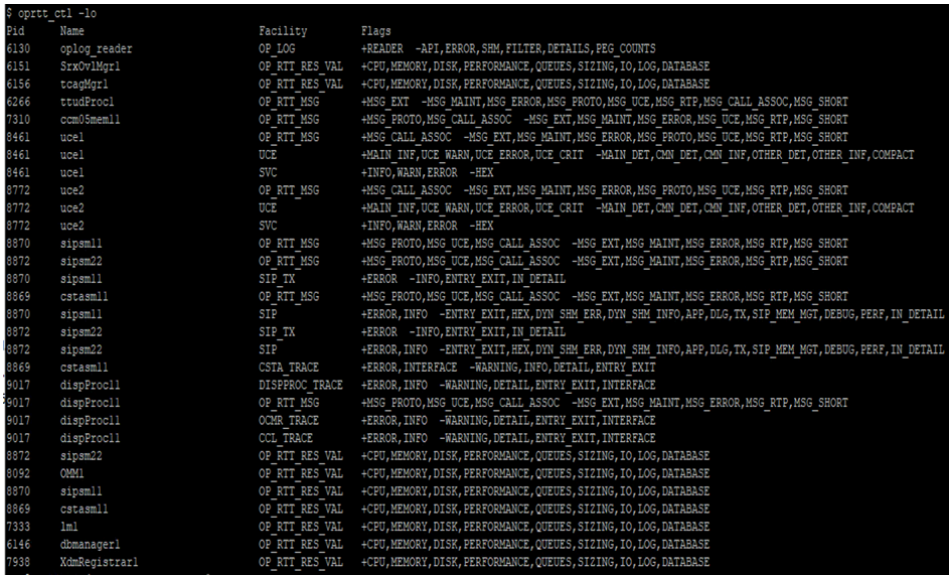
Below you can see the output of the command for each trace level:

24_7 - see the image below



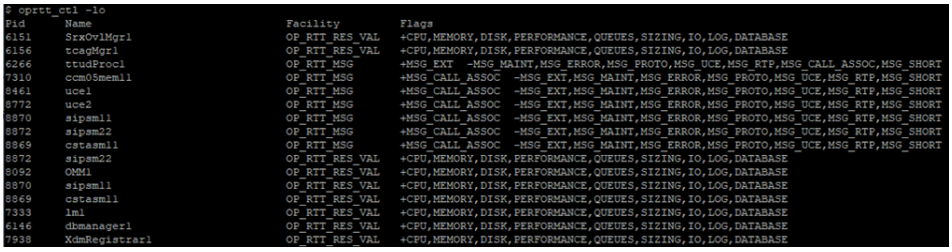
```
$ oprtt_ctl -lo
Pid     Name                    Facility        Flags
6130    oplog_reader            OP_LOG          +READER  -API,ERROR,SHM,FILTER,DETAILS,PEG_COUNTS
6151    SrxOvlMgr1              OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6156    tcagMgr1                OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6266    ttudProc1               OP_RTT_MSG      +MSG_EXT  -MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_CALL_ASSOC,MSG_SHORT
7310    ccm05mem11              OP_RTT_MSG      +MSG_PROTO,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_UCE,MSG_RTP,MSG_SHORT
8461    uce1                    NDAL            +CRITICAL,ERROR,WARNING,INFO,Detail
8461    uce1                    SSAL            +INFO,WARN,ERROR
8461    uce1                    OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8461    uce1                    SDAL            +INFO,WARN,ERROR,DETAIL
8461    uce1                    RSS             +CRITICAL,ERROR,WARNING,INFO
8461    uce1                    UCE             +MAIN_DET,MAIN_INF,CMN_DET,CMN_INF,OTHER_DET,OTHER_INF,UCE_WARN,UCE_ERROR,UCE_CRIT,COMPACT
8461    uce1                    SVC             +INFO,WARN,ERROR,HEX
8461    uce1                    XLA             +CRITICAL,ERROR,WARNING,INFO,DETAIL
8461    uce1                    MWI             +INFO,DETAIL,WARNING,ERROR,CRITICAL
8772    uce2                    NDAL            +CRITICAL,ERROR,WARNING,INFO,Detail
8772    uce2                    SSAL            +INFO,WARN,ERROR
8772    uce2                    OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8772    uce2                    SDAL            +INFO,WARN,ERROR,DETAIL
8772    uce2                    RSS             +CRITICAL,ERROR,WARNING,INFO
8772    uce2                    UCE             +MAIN_DET,MAIN_INF,CMN_DET,CMN_INF,OTHER_DET,OTHER_INF,UCE_WARN,UCE_ERROR,UCE_CRIT,COMPACT
8772    uce2                    SVC             +INFO,WARN,ERROR,HEX
8772    uce2                    XLA             +CRITICAL,ERROR,WARNING,INFO,DETAIL
8772    uce2                    MWI             +INFO,DETAIL,WARNING,ERROR,CRITICAL
8870    sipsm11                 OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
8872    sipsm22                 OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
8870    sipsm11                 SIP_TX          +ERROR  -INFO,ENTRY_EXIT,IN_DETAIL
8869    cstasm11                OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
8870    sipsm11                 SIP             +ERROR,INFO,ENTRY_EXIT  -HEX,DYN_SHM_ERR,DYN_SHM_INFO,APP,DLG,TX,SIP_MEM_MGT,DEBUG,PERF,IN_DETAIL
8872    sipsm22                 SIP_TX          +ERROR  -INFO,ENTRY_EXIT,IN_DETAIL
8872    sipsm22                 SIP             +ERROR,INFO,ENTRY_EXIT  -HEX,DYN_SHM_ERR,DYN_SHM_INFO,APP,DLG,TX,SIP_MEM_MGT,DEBUG,PERF,IN_DETAIL
8869    cstasm11                CSTA_TRACE      +ERROR,WARNING,INFO,DETAIL,ENTRY_EXIT,INTERFACE
9017    dispProc11              TLS_TRACE       +ERROR,WARNING,INFO,DETAIL,ENTRY_EXIT  -INTERFACE
9017    dispProc11              DISPPROC_TRACE  +ERROR,WARNING,INFO,DETAIL,ENTRY_EXIT  -INTERFACE
9017    dispProc11              OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
9017    dispProc11              OCMR_TRACE      +ERROR,WARNING,INFO,DETAIL,ENTRY_EXIT  -INTERFACE
9017    dispProc11              CCL_TRACE       +ERROR,WARNING,INFO,DETAIL,ENTRY_EXIT  -INTERFACE
8872    sipsm22                 OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8092    OMM1                    OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8870    sipsm11                 OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8869    cstasm11                OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
7333    lm1                     OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6146    dbmanager1              OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
7938    XdmRegistrar1           OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
```

24_7 min - see the image below



```
$ oprtt_ctl -lo
Pid     Name                    Facility        Flags
6130    oplog_reader            OP_LOG          +READER  -API,ERROR,SHM,FILTER,DETAILS,PEG_COUNTS
6151    SrxOvlMgr1              OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6156    tcagMgr1                OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6266    ttudProc1               OP_RTT_MSG      +MSG_EXT  -MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_CALL_ASSOC,MSG_SHORT
7310    ccm05meml1              OP_RTT_MSG      +MSG_PROTO,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_UCE,MSG_RTP,MSG_SHORT
8461    uce1                    OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8461    uce1                    UCE             +MAIN_INF,UCE_WARN,UCE_ERROR,UCE_CRIT  -MAIN_DET,CMN_DET,CMN_INF,OTHER_DET,OTHER_INF,COMPACT
8461    uce1                    SVC             +INFO,WARN,ERROR  -HEX
8772    uce2                    OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8772    uce2                    UCE             +MAIN_INF,UCE_WARN,UCE_ERROR,UCE_CRIT  -MAIN_DET,CMN_DET,CMN_INF,OTHER_DET,OTHER_INF,COMPACT
8772    uce2                    SVC             +INFO,WARN,ERROR  -HEX
8870    sipsml1                 OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
8872    sipsm22                 OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
8870    sipsml1                 SIP_TX          +ERROR  -INFO,ENTRY_EXIT,IN_DETAIL
8869    cstasml1                OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
8870    sipsml1                 SIP             +ERROR,INFO  -ENTRY_EXIT,HEX,DYN_SHM_ERR,DYN_SHM_INFO,APP,DLG,TX,SIP_MEM_MGT,DEBUG,PERF,IN_DETAIL
8872    sipsm22                 SIP_TX          +ERROR  -INFO,ENTRY_EXIT,IN_DETAIL
8872    sipsm22                 SIP             +ERROR,INFO  -ENTRY_EXIT,HEX,DYN_SHM_ERR,DYN_SHM_INFO,APP,DLG,TX,SIP_MEM_MGT,DEBUG,PERF,IN_DETAIL
8869    cstasml1                CSTA_TRACE      +ERROR,INTERFACE  -WARNING,INFO,DETAIL,ENTRY_EXIT
9017    dispProc11              DISPPROC_TRACE  +ERROR,INFO  -WARNING,DETAIL,ENTRY_EXIT,INTERFACE
9017    dispProc11              OP_RTT_MSG      +MSG_PROTO,MSG_UCE,MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_RTP,MSG_SHORT
9017    dispProc11              OCMR_TRACE      +ERROR,INFO  -WARNING,DETAIL,ENTRY_EXIT,INTERFACE
9017    dispProc11              CCL_TRACE       +ERROR,INFO  -WARNING,DETAIL,ENTRY_EXIT,INTERFACE
8872    sipsm22                 OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8092    OMM1                    OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8870    sipsml1                 OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8869    cstasml1                OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
7333    lm1                     OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6146    dbmanager1              OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
7938    XdmRegistrar1           OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
```

24_7 extern - see the image below



```
$ oprtt_ctl -lo
Pid     Name                    Facility        Flags
6151    SrxOvlMgr1              OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6156    tcagMgr1                OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6266    ttudProc1               OP_RTT_MSG      +MSG_EXT  -MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_CALL_ASSOC,MSG_SHORT
7310    ccm05meml1              OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8461    uce1                    OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8772    uce2                    OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8870    sipsml1                 OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8872    sipsm22                 OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8869    cstasml1                OP_RTT_MSG      +MSG_CALL_ASSOC  -MSG_EXT,MSG_MAINT,MSG_ERROR,MSG_PROTO,MSG_UCE,MSG_RTP,MSG_SHORT
8872    sipsm22                 OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8092    OMM1                    OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8870    sipsml1                 OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
8869    cstasml1                OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
7333    lm1                     OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
6146    dbmanager1              OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
7938    XdmRegistrar1           OP_RTT_RES_VAL  +CPU,MEMORY,DISK,PERFORMANCE,QUEUES,SIZING,IO,LOG,DATABASE
```

7.3 Disable All RTT Levels

If you need to disable all RTT trace levels, execute the following command via SSH as *srx* user on each node:

```
oprtt_ctl OP_RTT_TRACE_ALL=0
```

7.4 Collect OSV Database Backup via SSH terminal

Execute only on node 1

- Login via SSH, switch user to *srx* and execute:

```
startConsole
```

```
createJob backup.job
```

Once you get a job ID you should wait for a couple of minutes.

getJob <job-id>

When you see **DONE** just type `Exit`

When you see **ERROR** check the log files using the `createJob` command

Provide the exported file which is located under */opt/unisphere/srx3000/mmgr/backup/backup_all.tar.gz*.

7.5 Collect RTT Traces Without Trace Manager

- Login as *srx* on both OSV nodes via SSH terminal
- Enable the required tracers in RTTs
- Start capturing RTTs by executing the following command on both nodes:

```
oprtt_read -c > /software/tracefilename.raw
```

- After reproducing the scenario press CTRL+C to stop capturing packets.

7.6 Collect Network Traces from OSV nodes

- To capture all network packets execute the following as *root* user:

```
tshark -i any -w /software/test.pcap
```

After reproducing the scenario press CTRL+C to stop capturing packets.

- To capture packets coming to specific port (i.e. 5060) execute the following as root:

```
tshark -i any -w /software/test.pcap port 5060
```

After reproducing the scenario press CTRL + C to stop capturing packets.

8 CloudLink Integration

8.1 Basic troubleshooting

Check warnings

The CloudLink Daemon (CLD) performs checks to detect common environmental problems (e.g., connectivity, and system time).

Any warning displayed in the CloudLink daemon's user interface should be addressed first.

INFO: The daemon's user interface is accessible via CMP.

Include logs and configuration

For OpenScape Voice type the command:
`cld-getlogs`

to create a tarball in the local directory. This tarball contains important logs, configuration files, and a copy of the latest inventory report.

The above command works for other platforms (OpenScape CMP, OpenScape SBC, OpenScape 4000) as well.

Since the CLD on OSV is controlled by the CMP web server, you should also include logs from Common Management Platform (CMP).

Check Logs for Errors

You can check the CloudLink daemon logs for error messages. If these errors are caused by environmental issues you may find valuable information.

The CloudLink Daemon (CLD) logs can be found under */var/log/cld/**

and using the following command:
`grep level=ERROR /var/log/cld/*.log`

Networking

The network connection can be checked by running *curl* command on the daemon's host system.

for example, to check with a PROXY connection on a daemon’s host system.

```
curl -v --proxy http://<proxy-ip>:<proxy-port> https://
download.mitel.io/cld/linux/amd64/current.json
```

Also check the proxy configuration file, and that the *HTTPS_PROXY* and *NO_PROXY* values are correct.

System time

Some tokens used by the CLD are only valid for a short time for security reasons. The validation of these tokes may fail if the system time is not correct.

In that case, check your Network Time Protocol (NTP). Using local time zones is supported and should not create any issues.

Restart the CloudLink daemon

Restart the CLD using the following command:

```
systemctl restart cld
```

8.2 Centralized Call log issues with Unify Phone and Zoom PSI client

OpenScape Voice supports a centralized call log service for WebRTC clients, like Unify Phone and Zoom PSI clients.

The call log events for Zoom PSI are routed via the CloudLink Container for CSTA Proxy.

The responsible process for sending Call Log Event (CLE) messages is *dispProc*. For any call log issues, it is recommended to enable the following flags, on top of *24_7.*

RTT traces for dispProc can be collected using the following commands, as srx user:

For node 1:

```
oprtt_ctl -p `pidof dispProc11`  OP_RTT_TRACE_ALL=-1
```

For node 2:

```
oprtt_ctl -p `pidof dispProc12`  OP_RTT_TRACE_ALL=-1
```

In case the Centralized Call Logs are not working for a user, it is necessary to provide the output of *cstasmdump*, using the following command, as srx user:

```
cstasmdump > cstasmdump.output
```

For any call log issues with Zoom PSI client, it is helpful to collect logs from CloudLink Container for CSTA Proxy, using the following commands as root user:

```
docker cp cloudlink:/opt/micloud-link/src/log/. /var/log/
micloud_logs/
```

```
docker cp cloudlink:/opt/CstaProxy/log/. /var/log/
cstaproxy_log/
```

Please collect all logs under: */var/log/micloud_logs/* and */var/log/cstaproxy_log/*

8.2.1 Centralized Call log issues with Zoom PSI client

For issues specific to Zoom PSI consult Mitel Phone System Integration (PSI) with Zoom, Troubleshooting Guide.

8.3 Call-related issues

For issues related to calls, collect the following:

- RTT (24_7 or 24_7_min)
- SBC SIP traces
- RapidStat level 5 traces

8.4 Non call-related issues

For issues non related to calls, only Centralized Call Log is supported (see chapter Centralized Call log issues with Unify Phone.

For similar issues you can also refer to the following documents:

- *OpenScape SBC Troubleshooting Guide*
- *Mitel Phone System Integration (PSI) with Zoom, Troubleshooting Guide*

8.5 CloudLink Gateway logs

CloudLink Gateway (CLGWY) logs can be downloaded using the CloudLink Platform.

- Login to CloudLink Platform.
- Navigate to **System Inventory** > **Applications** > **CloudLink Gateways Manage** > **Download Logs**.