

MTAS Troubleshooting Guideline

MTAS

TROUBLESHOOTING

Copyright

© Ericsson AB 2016–2019. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Troubleshooting Procedure	3
2.1	Perform Node Health Check	3
2.2	Check Alarms	3
2.3	Counters and Key Performance Indicators (KPIs)	4
2.4	Verify Node Configuration	4
2.5	Troubleshooting SLA	5
3	Application Recovery Procedure	7
3.1	Diameter Interface	7
3.2	Small Restart	10
3.3	Recover H.248 Link	10
3.4	Sessions Hanging	11
3.5	Provisioning	12
4	Trouble Report	17





1 Introduction

This document describes how to perform the troubleshooting procedure in virtual Multimedia Telephony Application Server (MTAS).

1.1 Prerequisites

This section describes the prerequisites for this document.

It is assumed that users of this document are familiar with performing operations within the area for Operation and Maintenance (O&M) in general.

1.1.1 Documents

Before starting this procedure, ensure that the following documents are available:

- MTAS Health Check
- MTAS Alarm list
- Check Alarm Status
- Data Collection Guideline for MTAS
- Ericsson Command-Line Interface
- Performance Management Report File Format
- View Software Information
- MTAS Performance Indicators

1.1.2 Conditions

The following conditions must apply:

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress

Note: Certain troubleshooting activities can have an impact on the node performance. For example, tracing can be traffic disturbing and is not recommended without consulting Ericsson.





2 Troubleshooting Procedure

This section provides the workflow used when troubleshooting in MTAS.

The troubleshooting procedure involves checking:

- Node Health, see Section 2.1 Perform Node Health Check on page 3.
- Alarms, see Section 2.2 Check Alarms on page 3.
- Performance measurement counter logs and Key Performance Indicators (KPIs), see Section 2.3 Counters and Key Performance Indicators (KPIs) on page 4.
- Node configuration, see Section 2.4 Verify Node Configuration on page 4.

Identify the issue and resolve it according to the procedure described in each section. For more information on how to recover from the problem, see Section 3 on page 7.

Problems that cannot be solved by using this document must be reported to the next level of maintenance support, see Section 4 on page 17.

2.1 Perform Node Health Check

Health check provides an overview of node status and is an essential step in the troubleshooting procedure. Perform a node health check to gather information about the state of the node. For information on how to perform a health check, see [MTAS Health Check](#).

2.2 Check Alarms

Fault Management allows for detecting faults and malfunctions on the system and raising alarms accordingly. Based on the information stated in the alarm and the corresponding alarm Operating Instruction (OPI), actions can be taken to resolve or prevent failures. For more information, refer [Handling Alarms](#) and [MTAS Alarm List](#).

Do the following:

1. Check the alarm log, see [Check Alarm Status](#).
2. If any alarms exist, follow the relevant alarm OPI to solve the problem.



2.3 Counters and Key Performance Indicators (KPIs)

The performance measurement counter are generated by the MTAS and provide useful information when troubleshooting a problem.

To check the performance measurements counters:

1. Use the ECLI command `show-counters`. For more information about the command, see [Ericsson Command-Line Interface](#).
2. Active performance measurements counters for a Managed Object (MO) instance are displayed if the managed element supports displaying measurements through the ECLI.
3. The performance measurement counter logs are generated in 3GPP® compliant XML format and can be transferred outside the system for post processing. For more information about log file format, see [Performance Management Report File Format](#).

The performance measurement counters are used to get an indication of the network status and calculate some Key Performance Indicators (KPIs). The KPIs are defined on node (MTAS) and network level (IMS) and reflect the end-to-end performance. The information is used when judging in which domain and nodes the problem occurs. Check session accessibility and retainability KPIs. For more information on KPIs, see [MTAS Performance Indicators](#).

Alarms based on counter-thresholds can be defined to get an alarm when a counter exceeds a defined counter threshold. In case alarms based on counter-threshold are raised, do a node health check, see Section 2.1 Perform Node Health Check on page 3. For more information about threshold-based alarms, see [Performance Management](#).

2.4 Verify Node Configuration

To verify that the node is correctly configured:

1. Verify that the MTAS is activated.
2. Verify that used services are enabled. For more information, see [MTAS VNF Management Guide](#) and [MTAS Service Management Guide](#).
3. Verify that all required licenses are installed. For more information about the licenses, see [MTAS Licenses](#).
4. Verify that the Diameter links are correctly configured and working.

For more information, see the following documents:

- [MTAS Charging Management Guide](#)
- [MTAS Media Control Management Guide](#)



- MTAS Subscriber Data Management Guide
 - MTAS XDMS Management Guide
 - 5. Verify that the Ericsson Media Resource Function Processor (MRFP) links are correctly configured and working. For more information, see [MTAS Media Control Management Guide](#).
 - 6. Verify that the MTAS SIP interfaces are correctly configured and working. For more information, see [MTAS SIP Management Guide](#).
 - 7. Verify the state of VIP ports. For more information, see [Virtual IP Address Management](#).
 - 8. Verify that Number Normalization is correctly configured. For more information, see [MTAS Number Normalization Management Guide](#) and [Managed Object Model \(MOM\)](#).
 - 9. Verify that SS7 is correctly configured. For more information, see the [MTAS SS7 Management Guide](#) and [Signaling Manager User Guide](#).
- Note:** Contact the next level of maintenance support if there is a problem with SS7 configuration.
10. If any of the listed conditions and features are incorrectly configured or in a faulty state, corrective actions are required. If the problem still cannot be solved, contact the next level of maintenance support, see Section 4 on page 17.

2.5 Troubleshooting SLA

This section describes Service Level Agreement (SLA) trouble cases and how to resolve them.

The following SLA trouble cases exist:

- CpuSteal Verdict FAIL
- Network Verdict FAIL
- VM Unreachable VERIFY

2.5.1 CpuSteal Verdict FAIL

The CpuSteal verdict is **FAIL** when the CpuSteal is > 1% for any VM, or core of VM.

CPU overcommit is not acceptable. Run one VM on the host or if multiple Virtual Machines run on the same compute host, use CPU pinning.

Contact the cloud service provider to verify if the problem is caused by the cloud. If not, consult the next level of maintenance support.



2.5.2 Network Verdict FAIL

VM Network verdict is **FAIL** when packet loss is $> 0.1\%$ for any Interface of VM.

The following reasons can result in a packet loss:

- Network function entities that are present along the packet path which is provided by the Infrastructure Network Service or by external IP networks such as vNIC, vSwitch, vRouter, firewall, or backbone site router.
- Congestion
- Link faults
- Poor connectivity

Contact the cloud service provider to verify if the problem is caused by the cloud. If not, consult the next level of maintenance support.

2.5.3 VM Unreachable Verdict is VERIFY

The verdict is VERIFY when any of the following conditions are fulfilled:

- Any VM outage is observed. This verdict can be ignored when the reboot has been performed manually.
- If any VM has left the cluster and not joined, check if any SCALE-IN operation for the corresponding PL has been performed in an hour. If SCALE-IN operation has been performed, the issue can be ignored.

Contact the cloud service provider to verify if the problem is caused by the cloud. If not, consult the next level of maintenance support.



3 Application Recovery Procedure

3.1 Diameter Interface

This section describes the Diameter interface trouble cases and how to solve them.

The following Diameter error situations are described:

- The Diameter interface is down
- Link inactivity
- IP network failure
- Check Diameter link status

3.1.1 Diameter Interface Is Down

One or more of the Diameter interfaces are down.

Symptoms

Either of the following Diameter interfaces are down:

- Rf
- Ro
- Sh
- Dh

Locate and Confirm the Fault

The possible causes are:

- Home Subscriber Server (HSS) is down
- Subscriber Location Function (SLF) is down
- Charging Server (CS) is down
- Communication Details Server (CDS) is down
- Network issues
- Format error of Capabilities-Exchange-Request (CER) or Capabilities-Exchange-Answer (CEA) messages



- Coding error or missing Attribute-Value Pairs (AVP). This error occurs if a vendor defined, mandatory AVP is received, but not defined on the receiving node.

If any Diameter interface is down:

1. Wait for an automatic reconnection.
2. If a connection is not established, disable the neighbor node and enable it again. For more information, see [Diameter Management](#).
3. If a connection is still not established, consult the next level of maintenance support.

3.1.2 Link Inactivity

A connection to a Diameter peer is broken owing to link inactivity.

Symptoms

There is no response to the watchdog messages.

Locate and Confirm the Fault

If link inactivity occurs:

1. Check if the other Diameter node is operational by contacting the system administrator of the neighbor node, and wait for an automatic reconnection.
2. If a connection is not established, disable the neighbor node and enable it again. For more information, see [Diameter Management](#).
3. If a connection is still not established, consult the next level of maintenance support.

3.1.3 IP Network Failure

A connection to a Diameter peer is broken owing to IP Network failure.

Symptom

There is an IP Network or socket failure, or a malformed message.

Locate and Confirm the Fault

If an IP Network failure occurs:

1. Wait for automatic reconnection.
2. If a connection is not established, disable the neighbor node and enable it again. For more information, see [Diameter Management](#).



3. If a connection is still not established, consult the next level of maintenance support.

3.1.4 Check Diameter Link Status

A Diameter link is broken.

Symptom

The Diameter link has incorrect status in the ECLI.

Locate and Confirm the Fault

To check that all Diameter links are operational:

1. Run the following command in the ECLI:
 > **configure**
2. In the output:
 (config)>**ManagedElement=1,MtasFunction=MtasFunction,MtasSupport
 Functions=0,DIA-CFG-Application=DIA,DIA-CFG-StackContainer=MTAS
 _SH,DIA-CFG-PeerNodeContainer.peerNodeContainerId=MTAS_SH**
3. Go through each DIA-CFG-NeighbourNode=...\..MTAS_SH and
 verify that the value of the attribute linkStatus is Up for each
 DIA-CFG-Conn=MTAS_SH\...\23conn...
4. To get back to the config prompt, insert the following command four times:
 >..
5. Insert:
 (config)>**ManagedElement=1,MtasFunction=MtasFunction,MtasSupport
 Functions=0,DIA-CFG-Application=DIA,DIA-CFG-StackContainer=MTAS
 _SH,DIA-CFG-PeerNodeContainer.peerNodeContainerId=MTAS**
6. Go through each DIA-CFG-NeighbourNode=...\..MTAS and
 verify that the value of the attribute linkStatus is Up for each
 DIA-CFG-Conn=MTAS\...\23conn..
7. To get back to the config prompt, insert the following command four times:
 >..
8. Insert:
 (config)>**ManagedElement=1,MtasFunction=MtasFunction,MtasSupport
 Functions=0,DIA-CFG-Application=DIA,DIA-CFG-StackContainer=MTAS
 XDMS,DIA-CFG-PeerNodeContainer.peerNodeContainerId=MTASXDMS**
9. Go through each DIA-CFG-NeighbourNode=...\..MTASXDMS and
 verify that the value of the attribute linkStatus is Up for each
 DIA-CFG-Conn=MTASXDMS\...\23conn..

If each one of the linkStatus is Up, the Diameter link is operational, as required.



If any of the `linkStatus` is not Up, some instance of the Diameter link is down and the next level of maintenance support must be consulted.

3.2 Small Restart

The small restart is used to restart all static processes and terminate all dynamic processes. All data is kept in the database and stable sessions are not affected during the small restart. It is used to restart the MTAS SW without doing a cluster reboot.

To do a small restart:

1. Run the following command in the ECLI:

```
>ManagedElement=1,MtasFunction=MtasFunction,mtasFunctionSmallRestart
```

2. A small restart is performed.

3.3 Recover H.248 Link

This procedure describes how to resolve H.248 links that are failing after, for example, an upgrade.

Note: This applies only if internal Media Resource Function Controller (MRFC) is used.

If the H.248 link does not work:

1. Perform a small restart, see Section 3.2 Small Restart on page 10.
2. If the small restart does not resolve the problem, deactivate and activate the MRFP with the failing H.248 link.

Deactivate the MRFP

To deactivate the MRFP with the failing H.248 link:

1. From the ECLI, navigate to the `MtasMrfpNode` MO to be deactivated:

```
>configure
(config)>ManagedElement=1,MtasFunction.applicationName=MtasFunction,MtasMediaFramework.mtasMediaFramework=0,MtasMrf.mtasMrf=0,MtasMpController.mtasMpController=0
```

2. Set the `mtasMrfpNodeAdministrativeState` attribute to Shuttingdown.
3. Commit the change:

```
(config)>commit
```



4. Wait until the network is free from traffic sessions, that is, typically more than five times the normal holding time for a session. See call statistics for a suitable time.
5. Set the `mtasMrfpNodeAdministrativeState` attribute to **Locked**.

Activate the MRFP

To activate the MRFP:

1. From the ECLI, navigate to the `MtasMrfpNode` MO to be activated:

```
>configure
(config)>ManagedElement=1,MtasFunction.applicationName=MtasFunction,MtasMediaFramework.mtasMediaFramework=0,MtasMrf.mtasMrf=0,MtasMpController.mtasMpController=0
```

2. Set the `mtasMrfpNodeAdministrativeState` attribute to **Unlocked**.
3. Commit the change:

```
(config)>commit
```

For more information on activating and deactivating the MRFP, see [MTAS Media Control Management Guide](#).

If the MRFP traffic still does not recover, contact the next level of maintenance support.

3.4 Sessions Hanging

If an MTAS node experiences problems of hanging sessions, which prevents a subscriber from establishing new sessions, the CM attribute `mtasFunctionMaxNumberOfSessionsAction` is used to clear the hangings.

When an action is taken as a result of configuration, the session-related information including the event history, is printed to the Proc-logs.

When the number of sessions are equal to the CM attribute `mtasFunctionMaxNumberOfSessions`, the following setting decides the action to be taken:

- 0: Reject new communication attempts
- 1: Gracefully terminate all sessions of the subscriber that exceed the maximum duration limit defined by the CM attribute `mtasFunctionMaxSessionDuration`
- 2: Forcibly terminate all system resources allocated by the subscriber, that is, Capsule Abortion



- 3: Perform continuous removal of sessions exceeding the maximum duration limit defined by `mtasFunctionMaxSessionDuration`, at each communication attempt to or from the subscriber

In addition, reject the new communication attempt when exceeding the maximum number of simultaneous sessions of a served subscriber defined by `mtasFunctionMaxNumberOfSessions`.

Two more options exist for the clean-up mechanism:

- The presence of `MtasSystemConstantSC ID 2` suppresses the continuous removal of non-stable sessions at application process serialization, hence all sessions are serialized without considering their state.
- The presence of `MtasSystemConstantSC ID 3` suppresses the printout of session debug information to log when an action is taken as a consequence of the configuration of the CM attribute `mtasFunctionMaxNumberOfSessionsAction`.

3.5 Provisioning

3.5.1 Manual Health Check

3.5.1.1 Check the `XdmsLinuxServer` and `XdmsDiameterDistributor` Server

In an MTAS node, there are two processes for MTAS XDMS:

- `XdmsLinuxServer`, used to check the access of CAI3G request and tracing.
- `XdmsDiameterDistributor`, used for fetching CM parameters, pushing PM counters, Number Normalization, storing document over Sh, Charging, DTM and so on.

To check the readiness of the two processes:

1. Log on to the Controller as user `root` using Secure Shell (SSH):

```
ssh root@<OAM VIP>
```

2. Log on to the payload, where X is the payload number:

```
ssh PL-X
```

3. Check the `XdmsLinuxServer`:

```
telnet localhost 12112
```

The following is the expected output:

```
Connected to localhost
```




Connection is established. If not, reload the specific MTAS XDMS Linux® processor by reloading related area.

4. Check the XdmsDiameterDistributor:

```
telnet localhost 12113
```

The following is the expected output:

```
Connected to localhost
```

Connection is established. If not, reload the specific MTAS XDMS Linux processor by reloading related area.

5. Repeat Step 1 to Step 4 for all MTAS XDMS processors.

3.5.1.2

Check the XDMS (CAI3G and Ut) Ports

There are ports for different interfaces, which can be checked.

To check the MTAS XDMS (CAI3G and Ut) ports:

1. Log on to the Controller as user root using Secure Shell (SSH):

```
ssh root@<OAM VIP>
```

2. Log on to the payload, where X is the payload number:

```
ssh PL-X
```

3. Check that the ports 8090, 8095, and 8096 are open and listening:

```
netstat -a | egrep 8090\|8095\|8096
```

The following is the expected output:

```
Tcp 0 0 10.64.65.39:8090 *:* LISTEN
Tcp 0 0 10.64.65.39:8095 *:* LISTEN
Tcp 0 0 10.64.65.39:8096 *:* LISTEN
```

For more information, see Section Interface Accesses in MTAS XDMS Management Guide.

If any of the mentioned ports are missing, Tomcat is not started correctly, see Section 3.5.2 Restart Tomcat on page 14.

If the ports are not visible after the restart, search for the string Wrong VIP configuration in the syslog. Depending on the message, take relevant actions.

4. Use telnet to CAI3G port 8095:

```
telnet <ip> 8095
```



Connection is established.

<ip> is cai3g-vip4/cai3g-vip6

5. Use telnet to Ut port 8090/8096:

```
telnet <ip> 8090
telnet <ip> 8096
```

Connection is established.

<ip> is ut-vip4/ut-vip6

The following is an output example:

Connected to 10.64.65.39.

If connection is not established for the specific processor, see Section 3.5.2 Restart Tomcat on page 14. After the restart is finished, perform Step 4 to Step 5.

6. Log out from the payload.
7. To ensure that the VIPs are working, perform Step 2 to Step 5 from the shell in which the node is accessible.

If telnet is successful from the MTAS XDMS Linux processor but fails in Step 7, correct the VIP configuration.

3.5.2 Restart Tomcat

If Tomcat needs to be restarted, it must be done on all the MTAS XDMS Linux processors.

To restart Tomcat:

1. Log on to the Controller as user root using Secure Shell (SSH):

```
ssh root@<OAM VIP>
```

2. Log on to the payload, where X is the payload number:

```
ssh PL-X
```

3. Get the pid for Java:

```
ps -ef | grep java
```

4. Stop Tomcat:

```
kill -9 <pid>
```

Note: Tomcat starts automatically.



5. Perform Step 1 to Step 4 on all the payloads.

3.5.3 Order of Services and Elements in XML Document in CAI3G Interface

The order of services and elements in the XML document is important in CAI3G. For more information on the correct order, see Section Information Model in MTAS CAI3G Interface.

The following is an example of a received error if the order of services or elements is incorrect:

```
<reasonText>
  Private: error: cvc-complex-type.2.4a:
    Expected elements '
      user-common-data@http://schemas.ericsson.com/mtas/⇒
mmtel/cai3g ...
    instead of '
      calling-name-identity-presentation@http://⇒
schemas.ericsson.com/mtas/mmtel/cai3g ...
    ...
</reasonText>
```

3.5.4 Generate Stack Traces for MTAS XDMS

The stack trace is generated to check what is ongoing in the Java parts of the MTAS XDMS.

To generate the stack trace:

1. Log on to the Controller as user root using Secure Shell (SSH):

```
ssh root@<OAM VIP>
```

2. Log on to the payload, where X is the payload number:

```
ssh PL-X
```

3. Get the pid for Java:

```
ps -ef | grep java
```

4. Generate the stack trace of the status:

```
kill -3 <pid>
```





4 Trouble Report

Problems identified that cannot be solved by using this document must be reported to the next level of maintenance support. This is to result in a Customer Service Report (CSR).

The procedure for collecting data for the next level of maintenance support is described as follows:

1. Collect the data from the day and time of the event. Use the full profile when data is collected. For more information on how to collect information, see [Data Collection Guideline for MTAS](#).
2. Provide a severity statement expressing how the customer and its subscriber are effected by the problem. Indicate if a temporary work-around exists.
3. Check and provide the software version and level. For information on how to check MTAS software version, see [View Software Information](#).
4. Send a Customer Service Request (CSR) to the local Ericsson support organization or a Trouble Report (TR) for internal Ericsson use.
5. For problems still ongoing or when repeated tracing can be used to get more information for the troubleshooting process, contact the next level of maintenance support that can perform tracing.