

MTAS Logs

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016, 2018. 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 | Current Logs | 3 |
| 3 | Log Files | 5 |
| 3.1 | Syslog | 5 |
| 3.2 | vDicosApplog | 5 |
| 3.3 | Console Log | 5 |
| 3.4 | Additional vDicos Logs | 6 |
| 4 | Provisioning Log Files | 7 |
| 4.1 | Provisioning Access Logs | 7 |
| 4.2 | Provisioning Application Logs | 9 |
| 4.3 | Provisioning Catalina Log | 11 |
| 4.4 | Provisioning Catalina Out (Stack Traces) | 12 |
| 4.5 | Provisioning CAI3G Audit Log | 13 |





1 Introduction

This document describes the logs to be used for troubleshooting purposes by Ericsson service personnel in case of faults when MTAS is running in a virtual environment.

The operating system writes events used for troubleshooting the faults, as all programs do. The logs are stored as files on the System Controllers (SCs).

1.1 Prerequisites

This section describes the possible documents, tools, and required conditions before starting the data collection procedure.

It is expected that the reader has prior knowledge about telecommunication including knowledge about the MTAS and the virtualized environment. It is assumed that the reader is familiar with concepts, terminology, and abbreviations within these areas.

1.1.1 Tools

The following tools must be available before performing any procedure in this document:

- A workstation with SSH client.





2 Current Logs

Error information to be used for troubleshooting is found in the following logs:

- Syslog - Used by Linux standard “syslog”
- vDicosApplog - Used by the MTAS application
- Console logs - Used by vDicos and the MTAS application
- Provisioning logs - Used by the MTAS XDMS application





3 Log Files

Messages from all Payloads (PLs) are transferred to the System Controllers (SCs) for storage in respective log files.

When an error has occurred, the logs are compiled into an archive together with the error dump file by the `CrashCollector` to be sent to Ericsson for analysis. For more details, refer to [MTAS Error Dump](#).

3.1 Syslog

The syslog from each node (SCs and PLs) is stored in a file `/var/log/<node_name>/messages` respectively.

In addition to that, the syslog for SCs are also merged into the file `/var/log/messages`

Note: Based on log size, the directory, `/var/log/<node_name>/` can also contain rotated messages. `<integer>` file from the respective node. `/var/log/<node_name>/messages.1`: First rotated messages file from node.

3.2 vDicosApplog

For each application, vDicosApplog is stored in the directory `/cluster/storage/no-backup/coremw/var/log/saflog/MTASAppLogs/vdicos`

MTAS log files are stored with the following name template:

— `MTAS_<timestamp_start>.log`

Note: Based on log size, the directory, `/cluster/storage/no-backup/coremw/var/log/saflog/MTASAppLogs/vdicos` can also contain rotated `MTAS_<timestamp_start>_<timestamp_end>.log` files.

3.3 Console Log

The Console logs are stored in directory `/cluster/storage/no-backup/cdclsv/log/lpmsv`

The log of each vDicos instance (Virtual Machine (VM)) and processor is saved under the name of that specific VM instance and processor as follows:

— `vm<X>-<PL>-<Y>`

When a processor starts a new console log, based on log size, the previous log filename is overwritten with the following name format



vm<X>--<PL>--<Y>--<date>.<timestamp>.000.

The default size of these logs is 10 MB per VM.

The number of rotated files is limited to 1 by default.

3.4 Additional vDicos Logs

Additional vDicos log files are stored in the directory
/opt/cdc1sv/storage/log/

The log filenames created under this directory have the following template:

— <process_name>--<PL>--<Y>

When a processor starts a new console log, based on log size, the previous log filename is overwritten with the following name format
<process_name>--<PL>--<Y>--<date>.<timestamp>.000.

The default size of these logs is 10 MB per PL.

The number of rotated files is limited to 1 by default.



4 Provisioning Log Files

The provisioning access log present the received requests for normal provisioning and the cai3g audit log is generated when enabled by CM parameter `mtasXdmsCai3gLogging`. The provisioning application logs, catalina log and catalina out are filled if there are problems during provisioning

4.1 Provisioning Access Logs

The provisioning access logs contain one-line information per request to all MTAS XDMS interfaces. Each line contains information about the MTAS XDMS interface accessed.

CAI3G line format:

```
<TIME> <THREAD-ID> <CAI3G-SES-ID> <CAI3G-SEQ-ID>< USER> <METHOD> <SOAP ACTION>
<URL> <RESP CODE> [<OVERLOAD>] < ELAPSED TIME>
```

Ut line format:

```
<TIME> <THREAD-ID> <METHOD> <URL> <RESP CODE> [<OVERLOAD>] <ELAPSED TIME>
```

Detailed information:

| | |
|----------------|---|
| <TIME> | Log time stamp |
| <THREAD-ID> | Thread identity with entry address and port |
| <CAI3G-SES-ID> | CAI3G Session Identity |
| <CAI3G-SEQ-ID> | CAI3G Sequence Identity |
| <USER> | Public Identity user |
| <METHOD> | HTTP Request Method |
| <SOAP ACTION> | HTTP SOAP Action |
| <URL> | HTTP Request URL |
| <RESP CODE> | HTTP Response code |
| <OVERLOAD> | Optional field added only if "Retry-After" header is included in the response. The message is to be: (Overload) |
| <ELAPSED TIME> | Time (ms): it took to handle the request in MTAS . |

Note: The <USER> and <URL> may contain personal data. They are tagged with the appropriate privacy tags, for more information, refer to [MTAS Security Guide](#).



The access log is printed to the following directory on the PLs:
`/opt/mmas/appserver/traffic_instance<X>/logs/`

- Where <X> is the SU name of the PL (PL-3 for PL-3, and so on). For scaled-out nodes it is the instanceId, based on the node name during the scale-out operation

The access log file has a maximum size of 10 MB, when this size has been reached, a new archived file is created according to below rotation and retention policies. The total number of files can be up to 21, including one active access log file `localhost-access.log`, and up to 20 archived log files. The 20 archived log files consist of 10 active rotated log files and 10 oldest archived log files.

The Rotation Policy

The active access log file is renamed and compressed into an archived log file with name `localhost-access.log-<Date Time>-<next free number>.log.gz`. The <next free number> is the next integer to the current max index. If the current max index is already 10, the first archived file is deleted, and the other 9 files are renamed by changing the <index> to <index-1>, then a new archived file `localhost-access.log-<Data_Time>-10.log.gz` is created.

For example:

- If there are 5 archived files, the max index is 5, then on generating the new archive file, the <next free number> is 6, the file name is `localhost-access.log-<Data_Time>-6.log.gz`;
- If there are already 10 archived files, the max index is 10, then on generating the new archive file, the archive file with index 1 is deleted, the archive file with index 2 is renamed to `localhost-access.log-<Data_Time>-1.log.gz`, the archive file with index 3 is renamed to `localhost-access.log-<Data_Time>-2.log.gz`, and so on, then the new archive file is created and named with `localhost-access.log-<Date Time>-10.log.gz`

The Retention Policy

On generating new archive log file, the timestamp of the existing archive log files is checked and compared with the active access log file. For those log files which are 1 day older, only the last 10 files are kept, the older are deleted.

On the PLs, these access log files are not kept after a PL reload or instance restart.

On the SCs, the persistent access log files can be found in the following directory:

`/var/log/PL-<N>/mmas/appserver/traffic_instance<X>/localhost-access.log`

Where:

- <N> is the PL number, starting with 3 and increases by 1.
- <X> is the SU name of the PL (PL-3 for PL-3, and so on). For scaled-out nodes it is the instanceId, based on the node name during the scale-out operation



Below are the examples:

- Example of CAI3G content in access log file localhost-access.log:

```
2018-09-20 15:09:04,601 [http-apr-192.168.83.100-8095-exec-20] - POST CAI3G
#Login /axis2/services/CAI3G 200 12
2018-09-20 15:09:04,862 [http-apr-192.168.83.100-8095-exec-21] A192D168D83D1
00Z1474129481S1217P65537 87278078 <privIMPU>sip:abc@ericsson.com</privIMPU>
<privString>/axis2/services/CAI3G</privString> 200 254
2018-09-20 15:09:04,874 [http-apr-192.168.83.100-8095-exec-22] - POST CAI3G
Logout /axis2/services/CAI3G 200 5
```

- Example of Ut content in access log file localhost-access.log:

```
2018-09-20 13:25:46,269 [http-apr-127.0.0.1-8090-exec-5] - PUT <privString>
ervs.ngn.etsi.org/users/lars.magnus@ericsson.com/</privString> simservs.xml
```

- Example of Ut content with overload in access log file localhost-access.log:

```
2018-09-20 13:25:56,269 [http-apr-127.0.0.1-8090-exec-6] - PUT <privString>
ervs.ngn.etsi.org/users/lars.magnus@ericsson.com/</privString> simservs.xml
```

4.2

Provisioning Application Logs

The provisioning application logs contain information related to MTAS XDMS application processes.

Below are the supported provisioning interfaces and the corresponding application log names used by the MTAS XDMS log system.

| Provisioning Interface | Application Log | Application Log Max Size | Application Archived |
|------------------------|---------------------|--------------------------|--|
| CAI3G | xdms.axis2.log | 10 MB | xdms.axis2.log-<Date_Time>.log.gz |
| Ut/XCAP | xdms.mtasxdms.log | 10 MB | xdms.mtasxdms.log-<Date_Time>.log.gz |
| GenSSC | xdms.mtasgenssc.log | 5 MB | xdms.mtasgenssc.log-<Date_Time>.log.gz |
| CAI3G for SIP Trunk | xdms.mtasstas.log | 10 MB | xdms.mtasstas.log-<Date_Time>.log.gz |

— Where <Date_Time> is in the format of Month-Day-Year. <Index> is from 1 to 10

The provisioning application logs contain FATAL and ERROR logs on processing provisioning events. When more log information than level FATAL and ERROR is needed, detailed logging can be activated (on at least level 37) for `ims.mtas.xdms.*`. For more information about AppTrace, refer to [MTAS AppTrace](#)



Each line in the application logs has below format:

CAI3G line format

```
<TIME> <LOG LEVEL> <THREAD-ID> <AppTrace DOMAIN>
[<SESSION>, <SEQ NUM>, <USER>]
- <LOG CONTENT>
```

Ut line format

```
<TIME> <LOG LEVEL> <THREAD-ID> <AppTrace DOMAIN>
[<ADDRESS>, <XCAP APP>, <USER>]
- <LOG CONTENT>
```

GenSSC line format

```
<TIME> <LOG LEVEL> <THREAD-ID> <AppTrace DOMAIN> [<ADDRESS>]
- <LOG CONTENT>
```

| | |
|-------------------|---|
| <TIME> | Log time stamp |
| <LOG LEVEL> | Log severe level |
| <THREAD-ID> | Thread identity with entry address and port |
| <AppTrace DOMAIN> | Tracing Domain |
| <SESSION> | CAI3G Session Identity |
| <SEQ NUM> | CAI3G Sequence Identity |
| <ADDRESS> | IP Address where XCAP message received |
| <XCAP APP> | simservs for normal Ut/XCAP request; xcap-caps for XCAP Capabilities request |
| <USER> | Public Identity user* |
| <LOG CONTENT> | Log Details |

Note: The <ADDRESS> and <USER> may contain personal data. They are tagged with the appropriate privacy tags, for more information, refer to [MTAS Security Guide](#).

The provisioning applications log is printed to the following directory on the PLs: /opt/mmas/appserver/traffic_instance<X>/logs/

- Where <X> is the SU name of the PL (PL-3 for PL-3, and so on). For scaled-out nodes it is the instanceId, based on the node name during the scale-out operation

The application logs have the same log rotation and retention policies as access log, for more information, see Provisioning Log Files.

On the PLs, the provisioning application log files are not kept after a reload or instance restart.



On the SCs, the persistent application log files can be found in the following directory:

```
/var/log/PL-<N>/mmas/appserver/traffic_instance<X>/<Application
Log Name>.log
```

Where:

- <N> is the PL number, starting with 3 and increases by 1
- <X> is the SU name of the PL (PL-3 for PL-3, and so on). For scaled-out nodes it is the instanceId, based on the node name during the scale-out operation

The following are examples:

- Example of CAI3G application log string:

```
2018-09-15 10:10:01,260 [http-apr-127.0.0.1-8095-exec-8]DEBUG mtas.xdms.xdms
cai3g A192D168D83D100Z1441384753S516P65537 1688257881 - Document pre-edit =>
```

- Example of Ut/XCAP application log string:

```
2018-09-15 10:07:07,879 [http-apr-127.0.0.1-8090-exec-2]DEBUG mtas.xdms.xdms
validation <privIpAddress>127.0.0.1</privIpAddress> simservs <privIMPU>sip:u
```

- Example of GenSSC application log string:

```
2018-12-13T12:07:51,928 DEBUG [http-apr-8094-exec-5] ims.mtas.xdms.genssc [1
<privString><report version="1" id="default" xmlns="http://uri.etsi.org/ngn/
  <response>201 Created</response>
  <job>put</job>
  <value type="simple">video</value>
</report></privString>
```

4.3 Provisioning Catalina Log

The provisioning Catalina log files now record the runtime processes events, the provisioning application logs are recorded in the different application logs files per each interface, See section Section 4 on page 7.

Each line contains information about the runtime information in below format:

```
<TIME> <LOG LEVEL> <LOG SOURCE> <LOG CONTENT>
```

```
<TIME>                                Log time stamp
```

```
<LOG LEVEL>                           Log severe level
```



| | |
|---------------|-------------------------------|
| <LOG SOURCE> | The source generating the log |
| <LOG CONTENT> | Log Details |

The Catalina log is printed to the following directory on the PLs:
`/opt/mmas/appserver/traffic_instance<X>/logs/`

- Where <X> is the SU name of the PL (PL-3 for PL-3, and so on). For scaled-out nodes it is the instanceId, based on the node name during the scale-out operation

The Catalina log file has a maximum size of 10 MB, when this size has been reached, a new file is created. The total number of files can be up to 11, named `catalina.log`, `catalina.log.1`, and so on. The `catalina.log` is the active log file and it is renamed with the next free number when the size of the file is reached, for example `catalina.log.2`. When the total number of these files are reached, the first, `catalina.log.1`, is overwritten.

On the PLs, the Catalina log files are not kept after a reload or instance restart.

On the SCs, the persistent Catalina log files can be found in the following directory:

`/var/log/PL-<N>/mmas/appserver/traffic_instance<X>/catalina.log`

Where:

- <N> is the PL number, starting with 3 and increases by 1.
- <X> is the SU name of the PL (PL-3 for PL-3, and so on). For scaled-out nodes it is the instanceId, based on the node name during the scale-out operation

The following are examples of a Catalina string:

```
10-Nov-2018 17:02:18.715 INFO [com.ericsson.mmas.monitoring.MonitoringManager.i
10-Nov-2018 17:02:18.716 INFO [com.ericsson.mmas.lifecycle.services.MonitoringL
10-Nov-2018 17:02:18.717 INFO [com.ericsson.mmas.lifecycle.LifecycleServicesMar
10-Nov-2018 17:02:18.718 INFO [com.ericsson.mmas.lifecycle.LifecycleServicesMar
10-Nov-2018 17:02:18.719 INFO [com.ericsson.mmas.tomcat.lifecycle.MmasLifecycle
10-Nov-2018 17:02:18.719 INFO [org.apache.catalina.startup.Catalina.start] (mai
```

4.4 Provisioning Catalina Out (Stack Traces)

The Provisioning Catalina Out file contains runtime stack trace information related to MTAS XDMS processes. The Catalina Out file is one and has no limit on size.

An example of information that can be found in Catalina Out file is the generation of stack trace. The generation of stack traces for MTAS XDMS needs to be manually initiated, see MTAS Troubleshooting Guideline Section Generate Stack Traces for MTAS XDMS.



The Catalina Out file is printed to the following directory on the PLs:
/opt/mmas/appserver/traffic_instance<X>/logs/catalina.out

Where <X> is the SU name of the PL (PL-3 for PL-3, and so on). For scaled-out nodes it is the instanceId, based on the node name during the scale-out operation

The log file is not kept after a reload.

4.5 Provisioning CAI3G Audit Log

The CAI3G log information contains received MTAS XDMS CAI3G messages and corresponding responses.

The format of each log entry is shown below:

<TIME> <SAF COMPONENT> "<METHOD> <FROM HOST><MESSAGE>

| | |
|-----------------|--|
| <TIME> | Log time stamp |
| <SAF COMPONENT> | The SAF component where the CAI3G message is processed |
| <METHOD> | The CAI3G method (Login/Logout/Get/Create/Set/Delete) |
| <FROM HOST> | The client IP address |
| <MESSAGE> | The CAI3G XML message containing request and response |

The CAI3G log information is stored in AuditLog_<date>_<time>.log and is located in /cluster/storage/no-backup/coremw/var/log/saflog/MMASAuditLogs/.

To enable cai3g.log, the CM attribute mtasXdmsCai3gLogging must be set, refer to Managed Object Model (MOM).

An example of CAI3G audit log:

```
12:00:57 2018-12-07 IN safComp=traffic-mmas.instance,safSu=SC-1,safSg=NWA,safApp=ERIC-mmas.tomcat.traffic "Login 192.168.83.254<?xml version='1.0' encoding='utf-8'?><soapenv:Envelope xmlns:soapenv='http://schemas.xmlsoap.org/soap/envelope/'><soapenv:Body><cai3g:Login xmlns:cai3g='http://schemas.ericsson.com/cai3g1.2/'><cai3g:userId>John_Doe</cai3g:userId><cai3g:pwd>***</cai3g:pwd></cai3g:Login></soapenv:Body></soapenv:Envelope><?xml version='1.0' encoding='utf-8'?><soapenv:Envelope xmlns:soapenv='http://schemas.xmlsoap.org/soap/envelope/'><soapenv:Body><LoginResponse xmlns='http://schemas.ericsson.com/cai3g1.2/'><sessionId>A192D168D83D100Z1544001788S1P65537</sessionId><baseSequenceId>2129633216</baseSequenceId></LoginResponse></soapenv:Body></soapenv:Envelope>"
```