

# Emergency Recovery Procedure for MTAS

## MTAS

---

### EMERGENCY RECOVERY

**Copyright**

© Ericsson AB 2016. 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Prerequisites	1
<b>2</b>	<b>Related Information</b>	<b>3</b>
<b>3</b>	<b>Emergency Procedures</b>	<b>5</b>
3.1	Localize Fault	5





# 1 Introduction

This document describes the emergency recovery procedure for the MTAS node.

## Scope

Only MTAS-related recovery actions are included. The root cause can sometimes be inside the system, but troubleshooting outside MTAS is out of the scope for this procedure.

The recovery actions are intended for critical situations with an apparent disturbance in traffic handling. It is also applicable for situations where an important redundant function is lost (no single point of failure safe any more). Since this document is a recovery instruction, the affected systems are assumed to have been in a fully working state before the problems started. Therefore no troubleshooting steps that are related to faulty configuration or wrong software or hardware versions are explained.

Often, the critical situation has been caused by some kind of manual activity ongoing at the site. This is often some kind of upgrade or other maintenance tasks. For such situations the fallback, or recovery procedures belonging to that particular activity (often delivered together with the upgrade), is to be tried first when problems occur. If that does not help, this recovery procedure can be tried.

If there are alarms raised from the system, the procedures for solving the cause of the alarms are also to be tried before this recovery procedure is consulted. Such documentation is a part of the Customer Product Information (CPI) stored in the Active Library Explorer. Also, the *MTAS Troubleshooting Guideline* is to be consulted before this recovery procedure is considered.

## Target Groups

This instruction is intended to be used by experienced support engineers within first and Second Line Support when facing an urgent situation on the MTAS nodes that handle live traffic.

## 1.1 Prerequisites

This document is intended for readers who have administrative privileges to the system. The system administrator performing tasks on an MTAS must be familiar with the following:

- Unix®



- MTAS system knowledge (nodes, components, and so on)
- IMS network
- Diameter protocol
- Application-layer protocols (SIP, H.248, HTTP, and so on)
- Internet Protocol (IP) based networks

It is assumed that the system administrator has root access to all relevant machines on which the different MTAS nodes are hosted. Furthermore, the system administrator must know the IP addresses of these machines, and have access to all other relevant information about them.

Finally, it is also recommended that system administrators are familiar with other documentation for the MTAS system (or at least have access to the document set for further reference).



## 2 Related Information

Trademark information, typographic conventions, definition, and explanation of acronyms and terminology can be found in the following documents:

- *Glossary of Terms and Acronyms*
- *Trademark Information*
- *Typographic Conventions*







## 3 Emergency Procedures

The procedures presented in this section describe the various scenarios used to find and resolve faults that can cause an MTAS outage.

**Note:** Do **not** perform the following activities in the event of system failure unless otherwise stated.

- Altering databases
- Modifying anything other than configuration. Before modifying the configuration, always make a backup copy of the original configuration file.
- Introducing any additional changes (deltas)
- Powering off or rebooting
- Altering the network level
- Changing any system passwords

### 3.1 Localize Fault

To localize the fault and resolve the problem in the node:

1. If the problem started in connection to an upgrade, roll back to the last working release, that is, the one not causing any problems.
2. Find out what procedures were performed before the failure, what Correction Packages (CPs) or Emergency Packages (EPs) were added, and what files were modified.
3. Check the node health by following the guidelines in *MTAS Health Check*.
4. If any unexpected alarms are found, follow the instructions in the relevant alarm Operating Instruction (OPI) to solve the problem causing the alarm.

The alarm has a corresponding OPI title in the document library for each installation.

5. Retrieve the following log files on the System Controller (SC) processor and examine them:
  - `/var/log/<node-name>/messages`
  - `/cluster/storage/no-backup/coremw/var/log/saflog/MTASAppLogs/vdicos/MTAS_<timestamp>`



- `/opt/cdclsv/storage/log/<process_name>-<log_source><-instance_id><-timestamp>`
6. Examine the following files stored in the `/cluster/storage/no-backup/com-apr9010443/PerformanceManagementReportFiles` default counters directory:
    - PlatformMeasures
    - MTAS
    - SignallingMeasures
    - oamProvisioningCounter
  7. Run basic checks of the SCs.
    - Check if the file system is full on the SCs:  
  
`% df -k`  
  
If the disk is full on the SCs, clean up unnecessary files
    - Check for memory consuming processes on the SCs:  
  
`% top`
  8. If the problem still exists, contact the next level of maintenance support providing all the relevant information and log files.