

Core Dump Generated Cloud Execution Environment

OPERATING INSTRUCTIONS

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

1	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	2
2.1	Actions for Solving the Alarm	3



Core Dump Generated



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

This is a primary alarm. The alarm is issued for both core and crash dumps.

The alarm is issued by the Managed Object (MO) `CoreDump`. The alarm is issued when a process fails. The memory content of the failed process is saved in a core dump. When the Linux kernel fails, the dump is called a “crash dump”.

The possible alarm causes and the corresponding fault reasons, fault locations, and impacts are described in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Core or crash dump is generated	The alarm is issued when a process fails.	The memory content of the failed process is saved in a core dump.	Dump file path <full_path_to_dump_file>	Dump file space is used. The user must delete the files, or else the new dumps are lost in case the disk space allocated for crash/core files is filled up.
		When the Linux kernel fails, the dump is called a crash dump.		

Note: An alarm can appear as a result of maintenance activity.

There is no `logrotate` on crash and core dumps.

If the alarm is not solved, the consequences are as follows:

- The user must delete the files, or else the new dumps are lost in case the disk space allocated for crash and core files is filled up.

The alarm attributes are listed in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	2031713



Attribute Name	Attribute Value
Managed Object Class	CoreDump
Managed Object Instance	Region=<name_of_the_region>, CeeFunction=1, Node=<hostname_of_the_node>, CoreDump=<name>
Specific Problem	Core Dump Generated
Event Type	other (1)
Probable Cause	m3100Indeterminate
Additional Text	Core dump file <full_path_to_dump_file> generated
Severity	MINOR (5)

Note: The root cause of the dump can be MAJOR, and the cause must be determined. The actual dump generation is a MINOR outcome.

1.2 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

1.2.1 Documents

The collection of the core and crash dumps is described in the *Data Collection Guideline*.

1.2.2 Tools

No tools are required.

1.2.3 Conditions

No conditions must be met before acting on the alarm.

2 Procedure

This section describes the procedure to follow when this alarm is active.



2.1 Actions for Solving the Alarm

Do the following:

1. Fetch the dump, according to the *Data Collection Guideline*.
2. Delete the dump.

Further actions are outside the scope of this instruction.

3. The job is completed.