

CSCF, UDP SIP Load Regulation Rejection

Call Session Control Function

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	5





1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm `CSCF, UDP SIP Load Regulation Rejection` is raised when Session Initiation Protocol (SIP) messages received on User Diagram Protocol (UDP) are rejected because of load regulation.

The alarm is associated to the Performance Management (PM) counter `sipStatsUdpCongestions`. The counter `sipStatsUdpCongestions` is stepped for every rejected SIP message received on UDP, because of load regulation.

The alarm is raised when the number of `sipStatsUdpCongestions` has reached or exceeded its configured `thresholdHigh` within the time period configured by `thresholdRateOfVariation` and `granularityPeriod`.

The alarm is automatically ceased when it reaches or goes below the configured `thresholdLow` value.

The default values related to this alarm are: `thresholdRateOfVariation=PER_GP`, `granularityPeriod=FIVE_MIN`, `thresholdHigh=1` and `thresholdLow=0`. This means that when the counter value is 1 or higher, the alarm is raised when the granularity period is ended. The alarm is ceased when the counter `sipStatsUdpCongestions` has reached a value of 0 at the end of a granularity period.

Note: The thresholds for raising and ceasing this alarm are configurable. The default distinguished name for the thresholds is `ManagedElement=<node_name>`, `SystemFunctions=1`, `Pm=1`, `PmJob= CscfSipServerThreshold`, `MeasurementReader=sipStatsUdpCongestions`, `PmThresholdMonitoring=sipStatsUdpCongestions`.

It is not possible to change threshold values once they have been set. To change a threshold, first the `PmThresholdMonitoring` instance must be deleted and recreated with required `thresholdHigh` and `thresholdLow`.

For more information, refer to *Performance Management*.

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
The PM counter sipStatsUdpCongestions has exceeded its configured upper threshold value.	The number of rejected SIP messages because of load regulation has exceeded the configured threshold.	A received SIP message is rejected because of load regulation.	The processing resource has exceeded its configured maximum limit (for example: CPU load, memory load).	Incoming traffic is rejected with SIP 503 including a Retry-After header, with the risk of becoming blacklisted by neighboring nodes.

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

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	66846716
Managed Object Class	MeasurementReader
Managed Object Instance	ManagedElement=<node_name>, SystemFunctions=1, Pm=1, PmJob=CscfSipServerThreshold, MeasurementReader=sipStatsUdpCongestionsMeasReader
Specific Problem	CSCF, UDP SIP Load Regulation Rejection
Event Type	ProcessingErrorAlarm (4)
Probable Cause	x733CpuCyclesLimitExceeded (310)
Additional Text	sipStatsUdpCongestions, rejected SIP messages due to load regulation
Perceived Severity	minor (5)

1.2 Prerequisites

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



1.2.1 Documents

The following are suggested reference documents:

- *Performance Management*
- *LPM, Load Regulation Limit Passed*
- *LOTC Memory Usage*
- *CSCF Health Check*
- *Data Collection Guideline for CSCF*

1.2.2 Tools

No tools are required.

1.2.3 Conditions

No conditions.





2 Procedure

Note: If the reason for the alarm has disappeared after the granularity period, the alarm automatically ceases.

Do the following:

1. Check for other alarms regarding memory and CPU use and, if applicable, follow the procedures in those Operating Instructions.
 - *LPM, Load Regulation Limit Passed*
 - *LOTC Memory Usage*
2. Check if the alarm can be related to a transient situation. This can be, for example, that abnormal amount of traffic is received because of a failover scenario, failing hardware, abnormal communication burst compared to network dimensioning, or because of some maintenance activity like system upgrade. If so, the alarm automatically ceases when traffic is back to normal, or maintenance is concluded. If this alarm occurs frequently, it may be needed to check traffic models and redimension of the CSCF. To get an overview of the CSCF, do a Health Check and check the amount of SIP traffic and resource use.
3. The alarm depends on the status of load regulation on the node, so both the thresholds for raising and ceasing the alarm may have to be adjusted to suit the specific IMS network, refer to *CSCF Health Check*.
4. Confirm that the alarm has ceased. If the alarm remains, perform data collection, refer to *Data Collection Guideline for CSCF*, and consult next level of maintenance support. Further actions are outside the scope of this instruction.
5. Job is completed.