

CSCF, TCP SIP Load Regulation Rejection

Call Session Control Function

OPERATING INSTRUCTIONS

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	Alarm Description	1
2	Procedure	2
2.1	Handle Alarm CSCF, TCP SIP Load Regulation Rejection	2





1 Alarm Description

The alarm CSCF, TCP SIP Load Regulation Rejection is raised when Session Initiation Protocol (SIP) messages received on Transmission Control Protocol (TCP) are rejected because of load regulation.

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

The alarm is raised when the number of sipStatsTcpCongestions 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 sipStatsTcpCongestions 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=sipStatsTcpCongestions, PmThresholdMonitoring=sipStatsTcpCongestions.

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 the required thresholdHigh and thresholdLow values.

For more information, refer to [Performance Management](#).



Table 1 CSCF, TCP SIP Load Regulation Rejection Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
The PM counter sipStatsTcpCongestions has reached or exceeded its configured upper threshold value.	The number of rejected SIP messages because of load regulation has reached or exceeded the configured threshold.	A received SIP message is rejected because of load regulation.	The processing resource has reached or 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: This alarm can appear as a result of maintenance activity.

Table 2 CSCF, TCP SIP Load Regulation Rejection Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	66846715
Managed Object Class	MeasurementReader
Managed Object Instance	ManagedElement=<node_name>,SystemFunctions=1, Pm=1, PmJob=CscfSipServerThreshold, MeasurementReader=sipStatsTcpCongestionsMeasReader
Specific Problem	CSCF, TCP SIP Load Regulation Rejection
Event Type	ProcessingErrorAlarm (4)
Probable Cause	x733CpuCyclesLimitExceeded (310)
Additional Text	sipStatsTcpCongestions, rejected SIP messages due to load regulation
Perceived Severity	minor (5)

2 Procedure

2.1 Handle Alarm CSCF, TCP SIP Load Regulation Rejection

Prerequisites



- This instruction references the following 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

- No tools are required.

- The following condition must apply:

- The alarm is raised.

Steps

Note: If the reason for the alarm has disappeared after the Granularity Period, the alarm automatically ceases.

1. Check for other alarms regarding memory and CPU use and, if applicable, follow the procedures in those Operating Instructions. Refer to the following:

- LPM, Load Regulation Limit Passed
- LOTC Memory Usage

2. Is the alarm 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.

Yes: The alarm automatically ceases when traffic is back to normal, or maintenance is concluded. Proceed with Step 7.

No: Continue with the next step.

3. If this alarm occurs frequently, check traffic models and redimension of the CSCF.

To get an overview of the CSCF, do a Health Check and make sure that there are no problems regarding the amount of SIP traffic and resource use, refer to [CSCF Health Check](#).

4. Adjust the values of `thresholdHigh` and `thresholdLow` in `sipStatsTcpCongestions` to suit the specific IMS network.



5. Has the alarm ceased?

Yes: Proceed with Step 7.

No: Continue with the next step.

6. 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.

7. Job is completed.