

CSCF SIP Request Timed Out

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 SIP Request Timed Out	2



CSCF SIP Request Timed Out



1 Alarm Description

This threshold alarm CSCF SIP Request Timed Out indicates that there is a communication failure to a SIP server.

The alarm is associated to the Performance Management counter sipStatsReqTimeout. The counter sipStatsReqTimeout is stepped every time a SIP request times out without having received a response.

The alarm is raised when the number of sipStatsReqTimeouts 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=151, and thresholdLow=3. This means that when the counter value is 151 or higher, the alarm is raised when the Granularity Period is ended. The alarm is ceased when the counter sipStatsReqTimeout has reached a value of 3 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=<n ode_name>, SystemFunctions=1, Pm=1, PmJob=CscfSipClientThreshhold, MeasurementReader=sipStatsReqTimeoutMeasReader, PmThresholdMonitoring=sipStatsReqTimeout.

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.

Table 1 CSCF SIP Request Timed Out Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
The PM counter sipStatsReqTimeout has reached or exceeded its configured upper threshold value.	The number of received SIP communication failure errors has reached or exceeded the configured threshold.	Peer entity communication problems (SIP Request time out) to manage SIP messages.	Peer protocol communication problems between SIP servers.	Connection problems on CSCF SIP traffic interfaces causing communication issues with destination SIP servers.

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



Table 2 CSCF SIP Request Timed Out Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	6684689
Managed Object Class	MeasurementReader
Managed Object Instance	ManagedElement=<node_name>,SystemFunctions=1, Pm=1, PmJob=CscfSipClientThreshold,MeasurementReader=sipStatsReqTimeoutMeasReader
Specific Problem	CSCF SIP Request Timed Out
Event Type	communication (2)
Probable Cause	x733CommunicationsProtocolError (305)
Additional Text	-
Perceived Severity	minor (5)

2 Procedure

2.1 Handle Alarm CSCF SIP Request Timed Out

Prerequisites

— This instruction references the following documents:

- Performance Management
- Managed Object Model (MOM)

— 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 the details of the issued alarm to get the affected subsystems and the detailed specific cause.

It is possible to get the `sipStatsReqTimeout` counter keyed on specific IP addresses. To achieve this, configure the suspected IP addresses into the configuration parameter `cscfSipPMKey`. This tells the amount of transaction time-out per configured IP address.

It is also possible to get additional information by enabling the function “monitoring” by setting `cscfMonitorEnabled` to **true**. Because of transaction time-out for the blacklisted destinations, the alarm `CSCF, SIP Monitored Interface Unreachable` is raised. Information about source and destination transport addresses is then provided.

2. Find and remove any connection problems on the CSCF SIP traffic interfaces, if possible.

The alarm ceases when the communication with the destination works.

3. Adjust the thresholds for raising and ceasing the alarm to suit the specific IMS network.

4. Has the alarm ceased?

Yes: Proceed with Step 6.

No: Continue with the next step.

5. If the alarm is not ceased, consult the next level of maintenance support.

Further actions are outside the scope of this instruction.

6. Job is completed.