

CSCF, SIP Monitored Interface Unreachable

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	3
2.1	Handle Alarm CSCF, SIP Monitored Interface Unreachable	3



CSCF, SIP Monitored Interface Unreachable



1 Alarm Description

The alarm `CSCF, SIP Monitored Interface Unreachable` is raised for every monitored interface that becomes blacklisted because it is unreachable. If an interface is blacklisted because of receiving a SIP 503 response, the alarm is raised in case the configuration parameter `cscfAlarmOnSIP503Behavior` is enabled. If the alarm is raised for a blacklisted interface and the reason for blacklisting on that interface is changed, the alarm is ceased and raised again with the new reason for blacklisting.

A SIP response can cease the alarm. Ceasing of the alarm depends on the value of the configuration parameter `cscfAlarmOnSIP503Behavior` as follows:

- If the configuration parameter is disabled, the alarm is ceased on any SIP response to the SIP OPTIONS from the blacklisted destination.
- If the configuration parameter is enabled, the alarm is ceased on any SIP response to the SIP OPTIONS other than a SIP 503 from the blacklisted destination.

The alarm is also ceased when the monitoring is disabled or the maximum monitoring time (24 hours) expires.



Table 1 CSCF, SIP Monitored Interface Unreachable Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
A SIP network interface has become blacklisted.	The SIP monitoring is enabled and a SIP network interface has become blacklisted.	<p>A SIP network interface has been blacklisted because of the following reasons:</p> <ul style="list-style-type: none">• Transaction time-out• ICMP failure• Fatal transport failure• SIP 503 response	The Additional Text in the alarm gives both the source and target destination together with a reason for the problem. The typical fault location is at the blacklisted destination, but can also be because of signalling network problems or routing configuration.	A blacklisted destination is normally not used by regular traffic and possible alternative destinations are chosen. ⁽¹⁾ When no alternative destinations are available, traffic is rejected or the blacklisting is bypassed depending on configuration. A blacklisted destination is monitored by periodically sending SIP OPTIONS and either prolonging the blacklisting or taking the destination back into service when it is available for service again.

(1) There is a risk that alternative destinations also become overloaded.

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

Table 2 CSCF, SIP Monitored Interface Unreachable Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	6684704
Managed Object Class	CscfMonitoredInterfaceClass
Managed Object Instance	ManagedElement=<node_name>, CscfFunction=1, CSCF-Application=CSCF, CscfMonitoredInterfaceGroupClass=0, CscfMonitoredInterfaceClass=<source transport address>-<destination transport address>



Attribute Name	Attribute Value
Specific Problem	CSCF, SIP Monitored Interface Unreachable
Event Type	processingErrorAlarm (4)
Probable Cause	x733CommunicationsSubsystemFailure (306)
Additional Text	Format: It is not possible to reach <protocol>:<IP-address>:<port> from <protocol>:<IP-address>:<port> due to <reason>. ⁽¹⁾⁽²⁾
Perceived Severity	major (4)

(1) <reason> can have one of the following values: transaction timeout, transport error, or service unavailable

(2) Example: It is not possible to reach Udp : 192 . 168 . 10 . 50 : 5555 from Udp : 192 . 168 . 10 . 202 : 7025 due to service unavailable

2 Procedure

2.1 Handle Alarm CSCF, SIP Monitored Interface Unreachable

Prerequisites

- This instruction references the following documents:
 - CSCF Configuration Management
 - Managed Object Model (MOM)
- No tools are required.
- The following condition must apply:
 - The alarm is raised.

Steps

1. Is a network reconfiguration planned concerning the blacklisted destination?

Yes: Ignore this alarm until the reconfiguration has been completed and proceed with Step 9.

No: Continue with the next step.



This information can be found at the maintenance center.

2. Are there general transient problems with the signaling network or the neighbor destinations?

Yes: Consider adjusting the configurable blacklisting thresholds, refer to *CSCF Configuration Management*.

No: Continue with the next step.

3. Find the indicated reason in the Additional Text alarm attribute.

Note: The source and destination addresses of the unreachable interface can also be found in the Additional Information alarm attribute.

4. Is the reason service unavailable?

Yes: Consider increasing the values of the blacklisting thresholds `cscfBlacklistingSip503WithRetryAfterThreshold` and `cscfBlacklistingSip503WithoutRetryAfterThreshold`

The blacklisted destination is reachable on SIP application level but can be temporarily overloaded or having some other local problems that most likely cannot be cured otherwise from the CSCF.

No: Continue with the next step.

5. Is the CSCF application supposed to raise an alarm when a destination is blacklisted because of a received SIP 503 response?

Yes: Continue with the next step.

No: Set `cscfAlarmOnSIP503Behavior` to 0.

6. Perform all the following actions:

- Make sure that the destination address is correct.
- Make sure that the network cables operate correctly.
- Make sure that the destination host is operational.
- Make sure that the firewall settings and routing tables are configured correctly.

For more information about the configuration management parameters, refer to *Managed Object Model (MOM)* and *CSCF Configuration Management*.

7. Has the alarm ceased?

Yes: Proceed with Step 9.

No: Continue with the next step.



8. If the alarm is not ceased, consult the next level of maintenance support.
Further actions are outside the scope of this instruction.
9. Job is completed.