

CSCF, SIP Monitored Interface Unreachable

Call Session Control Function

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016, 2017. 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	3
2	Procedure	5
2.1	Analyze the Alarm	5
2.2	Actions to Clear the Alarm	5



CSCF, SIP Monitored Interface Unreachable



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm `CSCF, SIP Monitored Interface Unreachable` is issued 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.

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
A SIP network interface has become blacklisted.	The SIP monitoring is enabled and a SIP network interface has become blacklisted.	A SIP network interface has been blacklisted because of the following reasons: <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: 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



Attribute Name	Attribute Value
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>
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

1.2 Prerequisites

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

1.2.1 Documents

This instruction references the following document:

- *CSCF Configuration Management*
- *Managed Object Model (MOM)*

1.2.2 Tools

No tools are required.



1.2.3

Conditions

No conditions.



2 Procedure

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

2.1 Analyze the Alarm

Do the following at the maintenance center:

1. Check if there is a network reconfiguration planned concerning the blacklisted destination. If so, ignore this alarm until the reconfiguration has been completed.
2. If there are general transient problems with signaling network or neighbor destinations, consider adjusting the configurable blacklisting thresholds, refer to *CSCF Configuration Management*.

2.2 Actions to Clear the Alarm

Do the following:

1. Check the indicated reason in the `Additional Text` of the alarm.

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

2. If the reason is “service unavailable”, the blacklisted destination is reachable on SIP application level but can be temporarily overloaded or having some other local problems. It is mostly likely nothing that can be done in the CSCF raising the alarm other than consider increasing the values of the blacklisting thresholds `cscfBlacklistingSip503WithRetryAfterThreshold` and `cscfBlacklistingSip503WithoutRetryAfterThreshold`.
3. If the CSCF application is not supposed to raise an alarm when a destination is blacklisted because of a received SIP 503 response, disable it by setting `cscfAlarmOnSIP503Behavior=0`.
4. To identify the problem, try the following:
 - Check that the destination address is correct.
 - Check network cables.
 - Check that the destination host is operational.
 - Check firewall settings and routing tables.



5. Take the necessary actions to correct the discovered faults. For more information about the configuration management parameters, refer to *Managed Object Model (MOM)* and *CSCF Configuration Management*.
6. Confirm that the alarm has ceased. If the alarm is still present or reoccurs, consult the next level of maintenance support. Further actions are outside the scope of this instruction.
7. Job is completed.