

# CSCF Degraded HSS Redundancy

## 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Alarm Description	1
1.2	Prerequisites	3
<b>2</b>	<b>Procedure</b>	<b>5</b>





# 1 Introduction

This instruction concerns alarm handling.

## 1.1 Alarm Description

The Call Session Control Function (CSCF) quarantines a Home Session Server (HSS) when it detects that the HSS is unavailable. An HSS is quarantined only when there are multiple HSS nodes in the network. If the HSS becomes unavailable, and is not the last HSS in the list, it is put in quarantine, an alarm is issued, and a failover to the next HSS in the list takes place. An HSS in quarantine is never used.

**Note:** This only applies when monolithic HSS setup is deployed, that is, not when using HSS-FE and Centralized User Database (CUDB).

The alarm indicates the HSS host identity (FQDN) that has been put in quarantine.

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
HSS Redundancy has been compromised.	CSCF has determined that at least one HSS has become unavailable and put in quarantine.	The HSS is unavailable and therefore put into quarantine, which has caused the alarm to be raised.	The attribute <code>cscfHssInQuarantineEntry</code> is placed in the MOC <code>CscfHssQuarantine</code> , which represents an HSS currently placed in quarantine. It is only possible to remove an entry, not to add an entry, or to change an existing entry. Removing an entry from the list leads to the HSS being used immediately.	If the HSS becomes unavailable, and is not the last HSS in the list, it is put in quarantine, an alarm is issued, and a failover to the next HSS in the list takes place. An HSS in quarantine is never used.

**Note:** The 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	6684690
Managed Object Class	CscfHssQuarantine
Managed Object Instance	ManagedElement=<node_name>, CscfFunction=1, CSCF-Application=CSCF, CscfHssQuarantine=0
Specific Problem	CSCF Degraded HSS Redundancy
Event Type	qualityOfServiceAlarm (3)



Attribute Name	Attribute Value
Probable Cause	x736OutOfService (414)
Additional Text	Check connection to the HSS, Cscf HssInQuarantineEntry=<HSS host identity (FQDN)>
Perceived Severity	critical (3)

## 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:

- *Managed Object Model (MOM)*
- *vDicos, Diameter Link Failure*

### 1.2.2 Tools

No tools are required.

### 1.2.3 Conditions

Before starting this procedure, ensure that the following conditions are met:

- It must be possible to communicate with the HSS, therefore the alarm `vDicos, Diameter Link Failure` must not be raised for the HSS that is to be taken out of quarantine.
- All users must be deregistered in the HSS.
- The HSS that is to be taken out of quarantine must have the same provisioning status as the HSS that is handling the traffic.



**Note:** Taking an HSS out of quarantine has consequences. A failover to another HSS could be disturbing for already registered users if the registration information is not synchronized between the HSSs (the HSS loses all registration information at failover). The loss of registration information in the HSS leads to registration state inconsistencies between the CSCF and the HSS; already registered users will be in state **registered** in CSCF, but **not registered** in the HSS. When an HSS is taken out of quarantine, the same consequences for registered users as at a failover occurs. In other words, a fallback is as disturbing as a failover.





## 2 Procedure

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

The alarm is automatically cleared when the HSS is removed from quarantine. This can be done in the following ways:

### Manual Removal from Quarantine:

**Note:** Check that the quarantined HSS is operating normally and that the Diameter links between the CSCF and the HSS are up. The HSS can be removed manually from quarantine if these conditions are met.

1. Every HSS in quarantine is presented in the Operation & Maintenance (O&M) interface as an entry in a quarantine list. The name of the entry is `cscfHssInQuarantineEntry`.

An HSS is removed from quarantine by removing the corresponding list entry.

2. Setting `cscfHssQuarantineEnabled` from **true** to **false** removes any HSS from the quarantined list and clear its associated alarm.

### Automatic Removal from Quarantine:

3. The CSCF supports automatic removal of an HSS from quarantine at a configurable time of day. For example, if the time is configured to "02:00", all quarantined HSSs are removed from quarantine when the clock strikes 2 am. The O&M parameter is called `cscfAutoRemoveHssFromQuarantineTime`.

If no time is set, which is also the default setting, the automatic removal is disabled.

For more information about configuration management parameters, refer to *Managed Object Model (MOM)*.

4. If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction.
5. Job is completed.