

CSCF, DNS Server Unavailable

Call Session Control Function

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2017, 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	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	5



CSCF, DNS Server Unavailable



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm `CSCF, DNS Server Unavailable` is raised when one or more Domain Name System (DNS) servers that are configured in the Call Session Control Function (CSCF) are unavailable.

The DNS servers that are configured in the CSCF are constantly monitored by sending dummy messages according to [RFC6761](#). The CSCF needs the DNS servers to route SIP messages. If all DNS servers become unavailable, the CSCF cannot route SIP messages correctly.

The CSCF allows the possibility to configure a subset of the configured DNS servers for specific types of DNS lookups and queries. Ensure that at least one DNS server per lookup type is available. If all DNS servers for a certain lookup type are not available, the CSCF cannot route all SIP messages correctly. Perceived Severity is set to critical only when all DNS servers are unavailable, regardless of whether a certain lookup type is used or not.

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
CSCF DNS server is unavailable.	A major alarm is raised when one or more configured DNS servers are unavailable. At least one DNS server is available.	The DNS server is not responding.	Incorrect CSCF configuration data, DNS server, or IP connectivity.	Redundancy of DNS servers is reduced. The CSCF is possibly not able to route SIP messages, if dedicated lookup types are used.
	A critical alarm is raised when all configured DNS servers are unavailable.	The DNS server is not responding.	Incorrect CSCF configuration data, DNS server, or IP connectivity.	The CSCF is not able to route SIP messages.

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
Minor Type	6684721
Managed Object Class	DNS-Application
Managed Object Instance	ManagedElement=<node_name>, C scfFunction=1, DNS-Applicati on=DNS
Specific Problem	CSCF, DNS Server Unavailable
Event Type	communicationAlarm(2)
Probable Cause	x733CommunicationsSubsystemFai lure (306)
Additional Text	The following DNS server(s) are unavailable: <comma separated list of IP addresses> ⁽¹⁾
Perceived Severity	Major (4) or critical (3) ⁽²⁾

(1) Example: The following DNS server(s) are unavailable: 10.11.12.13, 13.12.11.10.

(2) If all configured DNS servers in the CSCF are unavailable, Perceived Severity is set to critical. Otherwise, it is set to major.

1.2 Prerequisites

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

1.2.1 Documents

This procedure references the following documents:

- *CSCF Configuration Management*
- *Data Collection Guideline for CSCF*
- *Managed Object Model (MOM)*
- Site-specific documentation describing IP infrastructure and IP Numbering Plan

1.2.2 Tools

No tools are required.



1.2.3

Conditions

No conditions.



CSCF, DNS Server Unavailable



2 Procedure

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

Do the following:

1. Log on to ECLI:

```
ssh -A <username>@<OAM IP> -p <port>
```

2. Verify that the DNS server addresses specified by the `dnsServerEntry` attribute and the local bind address specified by the `dnsLocalAddress` attribute are correct and write down the local bind address. For example:

```
> show -v ManagedElement=1,CscfFunction=1,DNS-Application=DNS
```

```
applicationName="DNS"
dnsCacheSize=20000 <default>
dnsExpiredCacheBehavior=REMOVED <default>
dnsLocalAddress
    "10.11.12.13"
dnsRetransmissionTimer=10 <default>
dnsServerEntry <default>
    "0:13.12.11.10"
```

3. Is the CSCF configured correctly?

Yes: Proceed with Step 5.

No: Continue with the next step.

4. Correct the CSCF configuration according to the site-specific IP plan. For more information on CSCF configuration, refer to *CSCF Configuration Management*

5. Is the alarm cleared?

Yes: Proceed with Step 13.

No: Continue with the next step.

6. Use commands `ping` and `traceroute` to check the IP connectivity between the CSCF and the unavailable DNS server. The IP address is written down in Step 2. Further instructions on using the tools are outside the scope of this document.

Note: `sudo` or root privileges are required for running `traceroute`.



7. Resolve any problems with IP connectivity, if found. Further instructions on solving IP connectivity, for example correcting routing tables in routers, are outside the scope of this document.
8. Is the alarm cleared?

Yes: Proceed with Step 13.

No: Continue with the next step.
9. Troubleshoot the unavailable DNS server to make sure that the DNS application is running and is correctly configured. Further instructions on troubleshooting the DNS server are outside the scope of this document.
10. Is the alarm cleared?

Yes: Proceed with Step 13.

No: Continue with the next step.
11. Perform data collection, refer to *Data Collection Guideline for CSCF*.
12. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
13. Job is completed.