

I-CSCF, LDAP Server Communication Failure

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

1	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3





1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm `I-CSCF, LDAP Server Communication Failure` is issued for communication failure to the LDAP server (for example, time-out or permanent transport failure). The alarm is raised on a per LDAP server basis, that is, one alarm is issued per unavailable LDAP server.

The alarm is ceased when one of the following events occur:

- The LDAP server is up and the next LDAP BIND is established.
- The unreachable LDAP server is removed from the list of LDAP servers used by the system.

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
Communication failure between the I-CSCF and the LDAP server.	The I-CSCF is unable to communicate with the LDAP server because of communications error.	Communication failure to the LDAP server because of time-out or permanent transport failures.	Various communication failure responses from LDAP servers cause this alarm to be raised due to triggers from the <code>icscfDuisLdapFailure</code> counter.	If the LDAP server is unreachable, it is removed from the list of LDAP servers used by the I-CSCF. If there are no LDAP servers available, the DUIS feature is not available.

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	6684705
Managed Object Class	LdapServerEntry
Managed Object Instance	ManagedElement=<node_name>,CscfFunction=1,LdapClientApplication=LdapClientApplication,LdapClientUserGroup=0,LdapClientUser=CscfDuaR,LdapServerEntry=<ldap_url>
Specific Problem	I-CSCF, LDAP Server Communication Failure
Event Type	communicationsAlarm (2)
Probable Cause	x733CommunicationsSubsystemFailure (306)
Additional Text	Check the counter <code>icscfDuisLdapFailure</code> for the possible cause of communication failure
Perceived Severity	major (4)

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:

- *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.

Do the following:

1. If the Dynamic User Identity Support (DUI) feature in the I-CSCF is not supposed to be used, disable it by setting `icscfDynamicUserIdentitySupportEnabled = false`.

Note: Disabling DUI after receiving the alarm does not clear the alarm.
2. Find the failed LDAP server identity from the `ldapServerEntryId` attribute of the Managed Object Instance.
3. To identify the problem, do the following:
 - Check the counter `icscfDuisLdapFailure` for the possible cause of communication failure. The DUI LDAP error code indicates the cause of the LDAP request failure. For more information about the `icscfDuisLdapFailure` counter and a complete list of possible errors, refer to *Managed Object Model (MOM)*.
 - Check that the destination address is configured correctly.
 - Check that the LDAP server is operational.
 - Check firewall settings and routing tables.
 - If the server is down and is not used any more, the server must be removed from the configured list of LDAP servers.
4. Take the necessary actions to correct the discovered faults.
5. Confirm that the alarm has ceased. If the alarm has not ceased, consult the next level of maintenance support. Further actions are outside the scope of this instruction.
6. Job is completed.