

Change Certificate Settings for LDAP TLS

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014, 2015. 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	Prerequisites	1
2	Procedure	3





1 Introduction

This document describes how to change the certificate settings for Lightweight Directory Access Protocol (LDAP) Transport Layer Security (TLS).

Authentication of the LDAP server and the Managed Element (ME), and encryption of the LDAP communication, are established by Public-Key Infrastructure (PKI) X.509 certificates.

The administrator needs to change the certificate settings for LDAP TLS because of a change in the certificate configuration and more specifically when a different ME node credential for LDAP TLS has to be used.

1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before using the procedure.

1.1.1 Conditions

The following conditions must apply:

- The user has the System Security Administrator role.
- The LDAP server is set up for TLS and has an X.509 certificate.
- The Uniform Resource Identifier (URI) configured to reach the server (that is, attribute `ldapIpAddress` in the `Ldap` managed object), is set as reference identity in the X.509 certificate of the LDAP server.
- The Managed Object (MO) for the node credential certificate for LDAP TLS is known.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Procedure

To change the node credential certificate settings for LDAP TLS:

1. Navigate to the *Ldap* MO, for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,UserManagement=1,LdapAuthenticationMethod=1,Ldap=1
```

2. Enter Config mode:

```
(Ldap=1) >configure
```

3. Set the reference to the applicable node credential certificate, for example:

```
(config-Ldap=1) >nodeCredential="ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, CertM=1, NodeCredential=1"
```

4. Commit the setting:

```
(config-Ldap=1) >commit
```

5. Verify the result:

```
(Ldap=1) >show
```

The following is an example output:

```
Ldap=1
  baseDn="dc=my-domain,dc=com"
  bindDn="cn=proxyaccount,dc=ericsson,dc=com"
  bindPassword="1:XUC+jE8QV05dG57Ouv7hWi1s/wa+uWi0"
  fallbackLdapIpAddress="192.0.2.11"
  ldapIpAddress="192.0.2.10"
  nodeCredential="ManagedElement=NODE06ST, SystemFunctions=1, =>
SecM=1, CertM=1, NodeCredential=1"
  profileFilter=ERICSSON_FILTER
  serverPort=636
  tlsMode=LDAPS
  trustCategory="ManagedElement=NODE06ST, SystemFunctions=1, =>
SecM=1, CertM=1, TrustCategory=aurora"
  userLabel="LDAP based login authentication"
  useTls=true
  useTlsFallback=true
[...]
```