

Configure TLS for LDAP

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	Description	1
2	Procedure	1
2.1	Configure TLS for LDAP	1





1 Description

This instruction describes how to configure Transport Layer Security (TLS) between LDAP Server and the Management Element (ME).

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

TLS connection uses the system-wide TLS cipher suite configured in the managed object *Tls* refer to *Configure TLS Ciphers*.

2 Procedure

2.1 Configure TLS for LDAP

Prerequisites

- This instruction references the following document:
 - *Configure TLS Ciphers*
- No tools are required.
- 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 x.509 certificate that the LDAP server sends to the ME to set up TLS is constructed properly: The `subjectAltName` (or `subject`) field in the certificate contains the Uniform Resource Identifier (URI), which is configured in the ME to reach the LDAP server. That is, the attribute `ldapIpAddress` in *Ldap* Managed Object (MO).
 - The MO for the node credential certificate for LDAP TLS is known.
 - The MO for the trust category for LDAP TLS is known.
 - An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



Steps

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 *ldapIpAddress* to the IP address of the remote LDAP server, for example:

```
(config-Ldap=1) >ldapIpAddress="192.168.0.10"
```

4. Optionally, set the *fallbackLdapIpAddress* to be used when the primary LDAP server is down, for example:

```
(config-Ldap=1) >fallbackLdapIpAddress="192.168.0.11"
```

5. Configure the *baseDn* from where the LDAP server starts to search for users, for example:

```
(config-Ldap=1) >baseDn="dc=my-domain,dc=com"
```

6. If LDAP server is listening to a non-default port, then the *serverPort* must be set, for example:

```
(config-Ldap=1) >serverPort=1000
```

7. Enable TLS:

```
(config-Ldap=1) >useTls=true
```

8. Optionally, configure the *tlsMode* attribute, for example:

```
(config-Ldap=1) >tlsMode=LDAPS
```

9. Set the reference to the applicable trust category, for example:

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

10. Optionally, 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"
```

Note: It is mandatory to set the reference to the applicable node credential certificate if LDAP server requires a certificate for TLS.

11. Commit the setting:



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

12. Verify the result:

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

The following is an example output:

```
Ldap=1
  baseDn="dc=my-domain,dc=com"
  fallbackLdapIpAddress="192.0.2.11"
  ldapIpAddress="192.0.2.10"
  nodeCredential="ManagedElement=NODE06ST, =>
SystemFunctions=1,SecM=1,CertM=1,NodeCredential=1"
  serverPort=1000
  tlsMode=LDAPS
  trustCategory="ManagedElement=NODE06ST, =>
SystemFunctions=1,SecM=1,CertM=1,TrustCategory=1"
  userLabel="LDAP based login authentication"
  useTls=true
  [...]
```

Note: If attribute `useTls` in `Ldap` MO is set to `true`, then either one of the following conditions must be met:

- Only `trustCategory` is set
- Both `nodeCredential` and `trustCategory` are set

If these conditions are not met, depending on the configuration one of the following error messages is reported to NBI during `commit` or `validate` operation:

- Error: neither `nodeCredential` nor `trustCategory` is available
- Error: `trustCategory` is not available