

Getting the most out of CA ACF2™ and CA Top Secret® with LDAP & DSI

Mitchell Rozonkiewicz

Product Owner, Product Management

8/22/2013



Abstract

Did you know that you can easily, and securely, access your mainframe security data and leverage it anywhere in the enterprise?

We'll review what is the CA LDAP Server and how to access the ESM data using it. We'll review a couple of ways that CA itself uses this server. And we'll cover the options to secure communication to the CA LDAP Server.

We'll briefly touch on the CA DSI Server. If more info is needed, we can hold a follow up presentation, or you can send me an email at rozmi02@ca.com.

What are we going to discuss

We are going to discuss:

- What is the CA LDAP Server?
- What can it do?
- What data can I access?
- Can I update this data?
- Can I use LDAP to send changes outbound?

- High level, what is the CA DSI Server?

What is the CA LDAP Server?

TCP/IP based server that provides inbound query & update access to data in the CA ACF2 and CA Top Secret security databases using the LDAP protocol.

Neither CA ACF2 nor CA Top Secret are X.500 directories, so you can't store just anything you want. You can access and maintain security objects only.

Since LDAP protocol is not a security protocol, there are some limitations to what an LDAP Server normally provides.

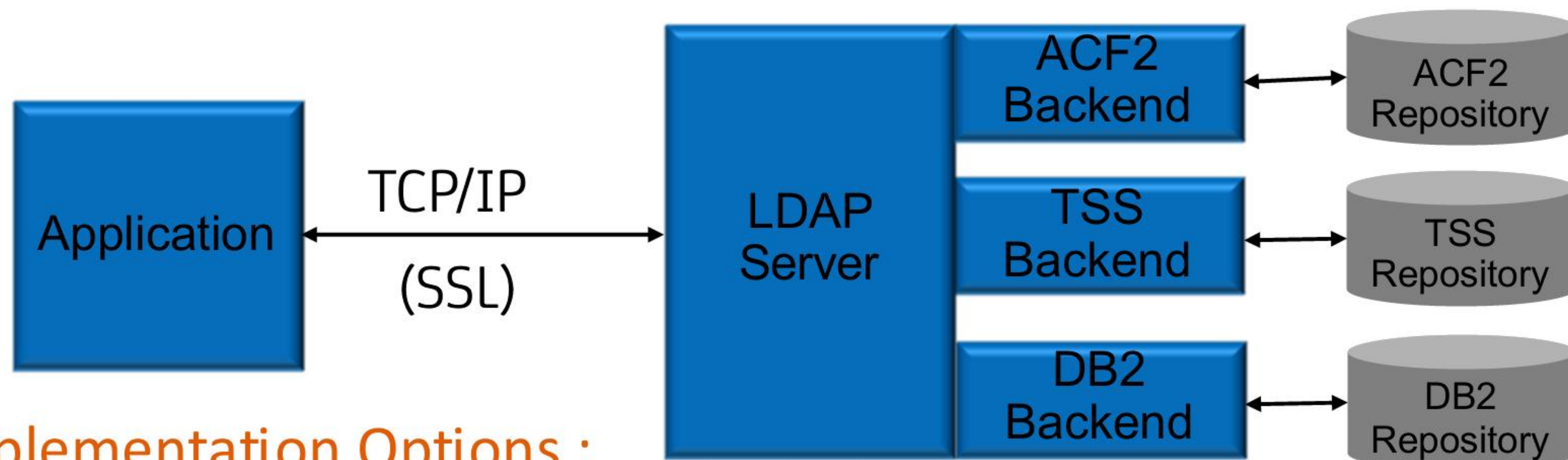
Object Class – Similar to a record layout, defines what fields (attributes) are required (must be provided) or allowed (may be provided) on the object

Attribute – Individual field in an Object Class. Defines the data type, case sensitive (yes/no) and single or multi-valued

Some types - Directory String, IA5 String, Integer, JPEG or DN

DIT – Directory Information Tree, this defines the hierarchy of object classes in the repository

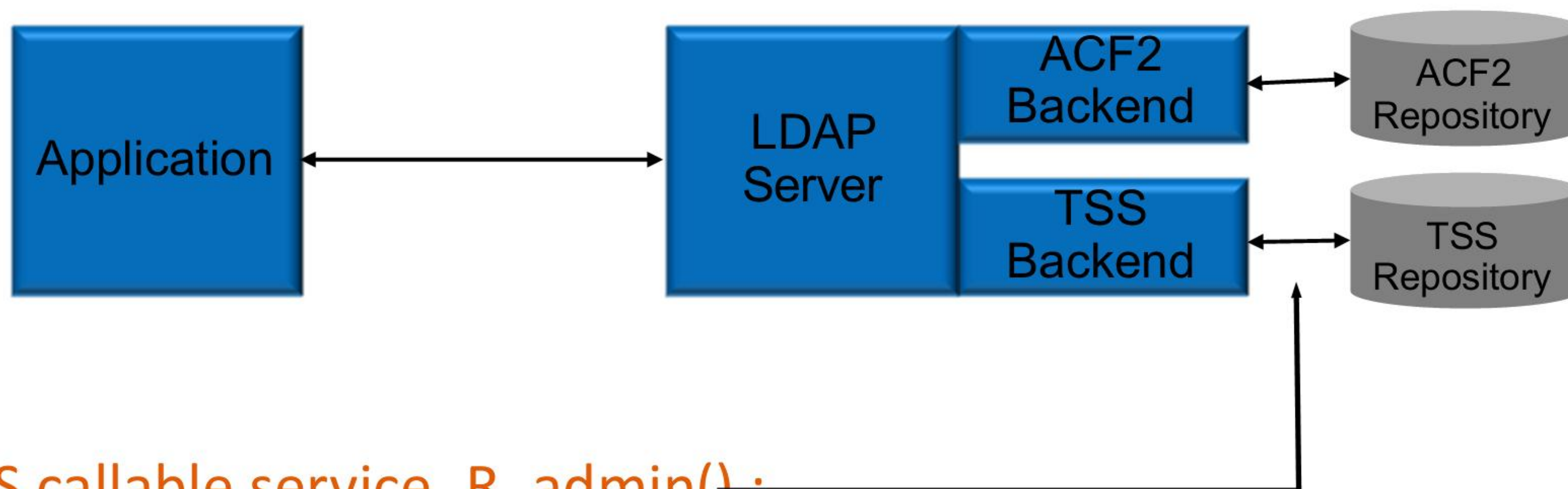
CA LDAP Server Architecture



Implementation Options :

- Just one interface (ACF2 or TSS) or both
 - Anything that uses LDAP protocol **
 - Configurable objects/search filters
- DB2 option for non-security objects
- Uses IBM System SSL
 - Hardware crypto/FIPS support

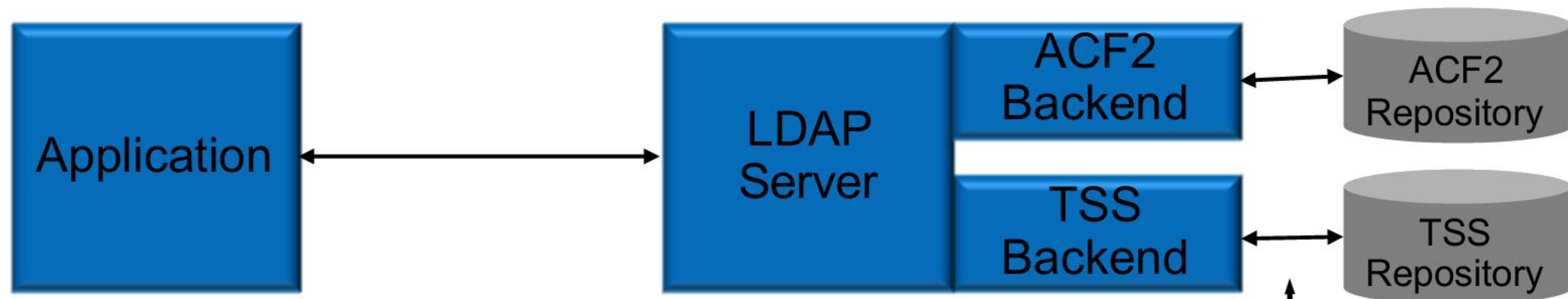
Interaction with the ESM



USS callable service, R_admin() :

- Gives command to CA ACF2 or CA Top Secret to execute
 - No different than issuing at a TSO prompt
 - ESM will determine if you are authorized (scoped)
- LDAP never has direct access to the security file
 - No copy of the data behind LDAP to maintain or sync

Limitations using LDAP



Callable service, `R_admin()` :

- Since LDAP issues a native command, limited to what the commands can do
- Can not issue a filter with AND, OR and NOT criteria to CA ACF2 or CA Top Secret

Ease of install and setup

— SMP/E Install

- A single install puts both servers into zFS
 - CA LDAP Server and CA DSI Server
- Configure and start the one (or both) that you need to use

— Sample Jobs

- Define STC id
- STC Procs

— MSM Support

- MSM Installable, Deployable and Configurable

Why use LDAP?

LDAP is a standard way of encoding a request, add, modify, delete, search

Applications that support LDAP protocol can interact *IF* the application can support multiple schema's. Why? Every repository is different.

- MS AD, RACF, even ACF2 is different from TSS
- AD – uniPwd, RACF, ACF2, TSS - userPassword

Failover – Supply multiple URLs, LDAP protocol will try each until one works

How might I use CA LDAP Server

Onboarding

- Whatever your process is to add/change/remove an employee, many Identity Management systems support the LDAP protocol. Integrate to CA ACF2 and CA Top Secret with the process by automating it. Free up your admins for architecture work.
- CA's own distributed security products integrate to the mainframe using the LDAP Server
 - Identity Minder, Cloud Minder, Access Control, EEM
- Authentication of user ids/password using a single repository

How might I use CA LDAP Server

Chorus

- When you view users in the Chorus Investigator, you can go into edit mode
- After making changes in the Investigator, the changes create an LDAP modify or delete
- The currently logged in Chorus user is logged into the LDAP Server, then a modify or delete is sent to LDAP to perform the needed change

What can I access in CA ACF2 and CA Top Secret

Virtually everything - Users, Permissions, Control options

ACF2 – Lids, Rules, GSO, CPF, Shift, Scope, etc

TSS – Acids (all types), NDT, FDT, RDT, Permissions

Not accessible in CA ACF2:

- Digital Certificates
- Compiler User Profile Records

Not accessible in CA Top Secret:

- Digital Certificates

CA LDAP Server Product Guide documents the DIT

What LDAP operations are supported?

All operations are supported:

Bind/unbind – Equivalent to a TSO Login/Logout

Add – Maps to ACF2 INSERT and TSS CREATE/ADMIN

Delete – Maps to ACF2 and TSS DELETE

Modify – Maps to ACF2 CHANGE and TSS REPLACE/REMOVE/DEADMIN

Modrdn – Maps to TSS MOVE ** TSS ONLY

Search – Maps to ACF2 and TSS LIST

Notice all operations are inbound to the ESM

CA LDAP Server can not be used to send outbound LDAP operations, we'll come back to this later

Does the CA LDAP Server support user defined fields added to the ESMs?

- Absolutely
- CA LDAP Server queries the security product for version and fields (attributes) during initialization
- Based on the version, dynamically define attributes and object classes
- Walks the ACF2 FDR and TSS FDT to get all user defined fields and adds them to the acf2lid or tssacid object

NOTE: After adding a new field, just restart LDAP to recognize it

How do I determine what schema is defined?

You query for the 'schema'. To get all data syntax, matching rules, attributes and object classes you'd issue:

— ldapsearch -D cn=USERID -w PASSWORD -H
ldap://HOSTNAME_or_IP:PORT -s base -b cn=subschema +

For just attributes:

— ldapsearch -D cn=USERID -w PASSWORD -H
ldap://HOSTNAME_or_IP:PORT -s base -b cn=subschema
attributeTypes

Continued on next page

How do I determine what schema is defined? (cont.)

For just objects:

- `ldapsearch -D cn=USERID -w PASSWORD -H
ldap://HOSTNAME_or_IP:PORT -s base -b cn=subschema
objectClasses`

How do I determine the configuration?

You can query for the 'suffix' and other configuration information like you did the 'schema'. To get all ACF2 configuration data, you'd issue:

```
— ldapsearch -D cn=USERID -w PASSWORD -H  
  ldap://HOSTNAME_or_IP:PORT -s one -b cn=config  
  olcBackend=caacf2_utf
```

How does this help?

Using LDAP configuration info

Some of the info returned is:

olcSuffix: host=xe42_im,o=ca,c=us	← Required for all operations
acfEnableRefresh: TRUE	← F ACF2,REFRESH will be issued
acfCreateAlias: Relate Catalog	← When user add, a catalog alias will be created
acfDeleteAlias: TRUE	← When user deleted, catalog alias will be deleted
acfEnableRefreshXref: TRUE	← F ACF2,REFRESH will be issued
acfSecAuth: VGID,XE41,XE42	← Secondary Auth Ids that LDAP can retrieve
acfHostNamingMode: im	← The naming mode (z/OS or Identity Manager)

Using the suffix

Now that you have the suffix, get details about the host

— `ldapsearch -D cn=USERID -w PASSWORD -H
ldap://HOSTNAME_or_IP:PORT -s base -b SUFFIX_HERE`

dn: host=xe42_im,o=ca,c=us

securityType: ACF2

secVersion: 15.0

secMode: ABORT

secDateFormat: MM/DD/YY

secLogonInvalidCount: 3

Continued on next page

Using the suffix (cont.)

secPswdMinLength: 3

secPreventUserIdAsPswd: NO

acf2PswdChgByUser: NO

acf2RequireNumericChar: NO

secPswdChkAllNumeric: NO

secPswdRepeatingChars: 2

secPswdChkReserved: NO

secRequireNationalChar: NO

acf2MixedCaseVowels: YES

secExpireWarningDays: 10

acf2UIDstring: COMPANY,SITE,LEVEL,PROJECT,LID,GROUP

Reset a user password

Create an LDIF file:

dn: acf2lid=**TEST**,acf2admingrp=lids,host=xe42,o=ca,c=us

replace: userPassword

userPassword: newval

Issue modify command:

— ldapmodify -D cn=**USERID** -w **PASSWORD** -H
ldap://**HOSTNAME_or_IP:PORT** -f **FILE_NAME**

This is a command line example, could have been issued programmatically as well

Top Secret Specific Extension

TSS commands allow a comment:

```
TSS REP(acid) TSOPROC(newval) /* Ticket CR:1923432
```

CA LDAP Server has a control (**1.3.6.1.4.1.791.2.3.6.2.5.1**) that supports adding a comment to Add, Modify, Delete operations

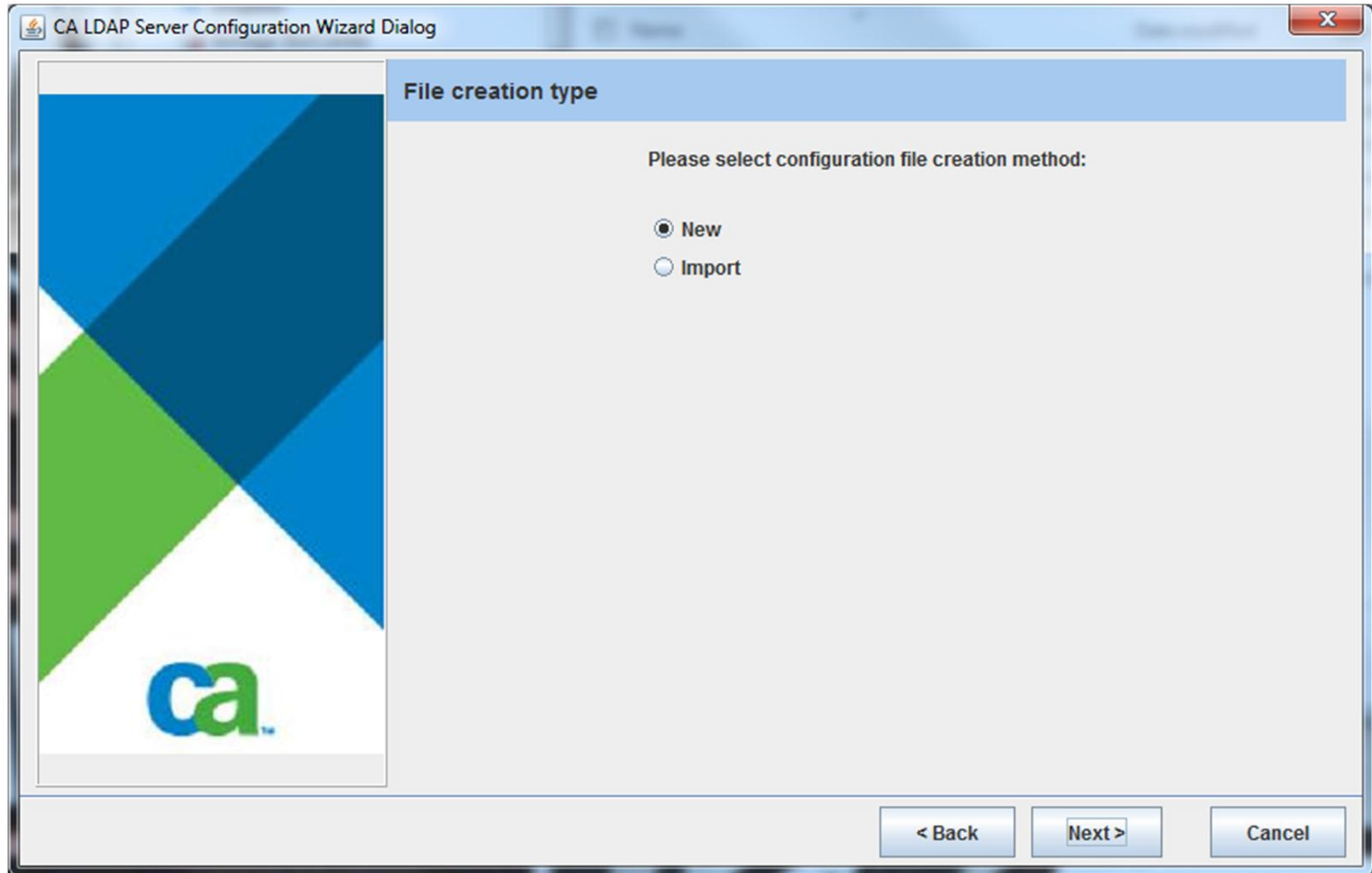
LDAP Configuration Wizard

There are many LDAP Server configuration options

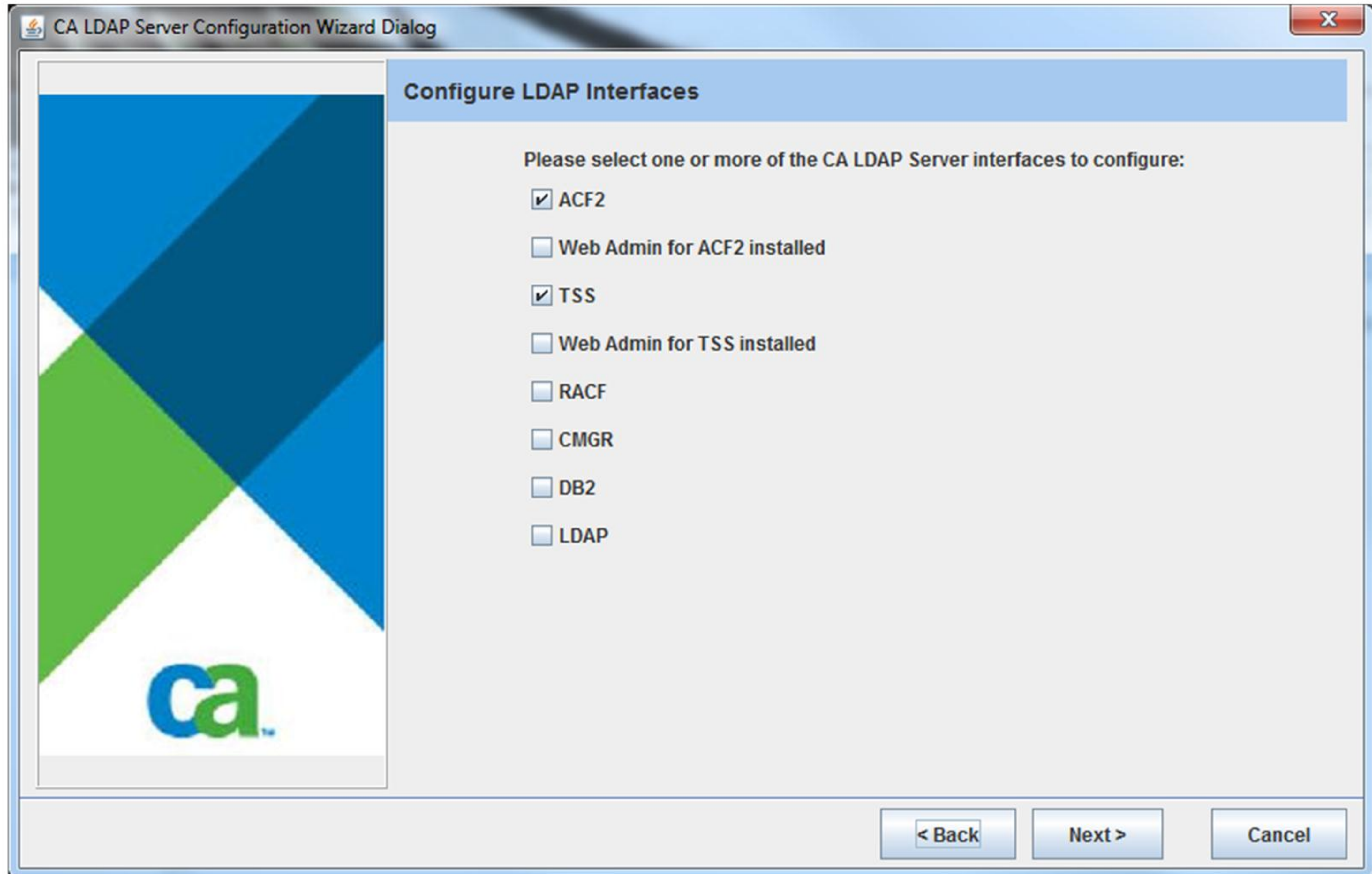
Some are mutually exclusive, some global, some are specific to a backend, some are for a specific security file instance

To aid in the setup of the server, as well as migration from older releases to the current r15, we have a configuration wizard

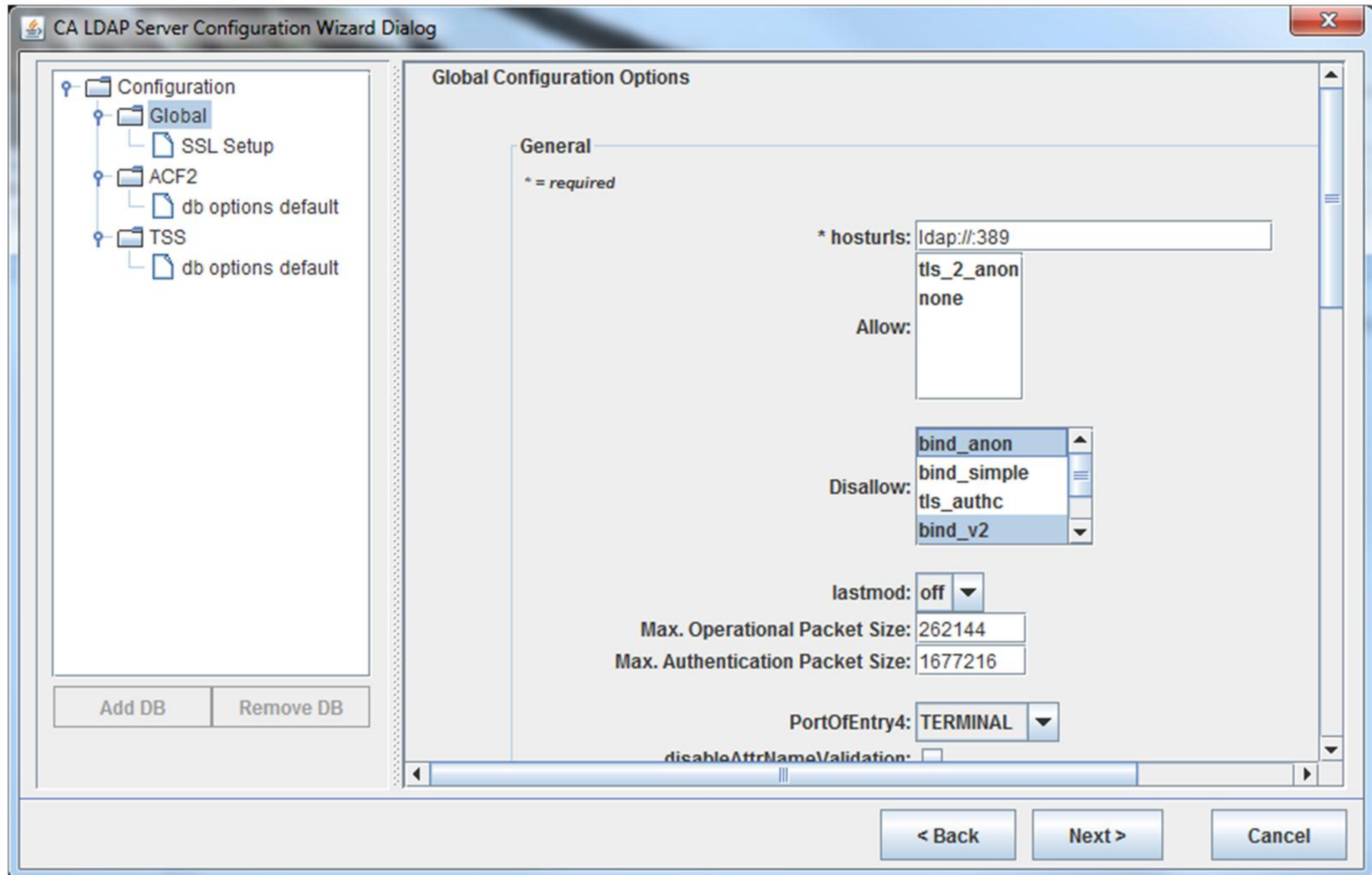
Configuration Wizard – New or Import



Configuration Wizard – Which backend?



Configuration Wizard – Global Options



The image shows a screenshot of the 'CA LDAP Server Configuration Wizard Dialog' window. The title bar reads 'CA LDAP Server Configuration Wizard Dialog'. On the left is a tree view with the following structure:

- Configuration
 - Global (selected)
 - SSL Setup
- ACF2
 - db options default
- TSS
 - db options default

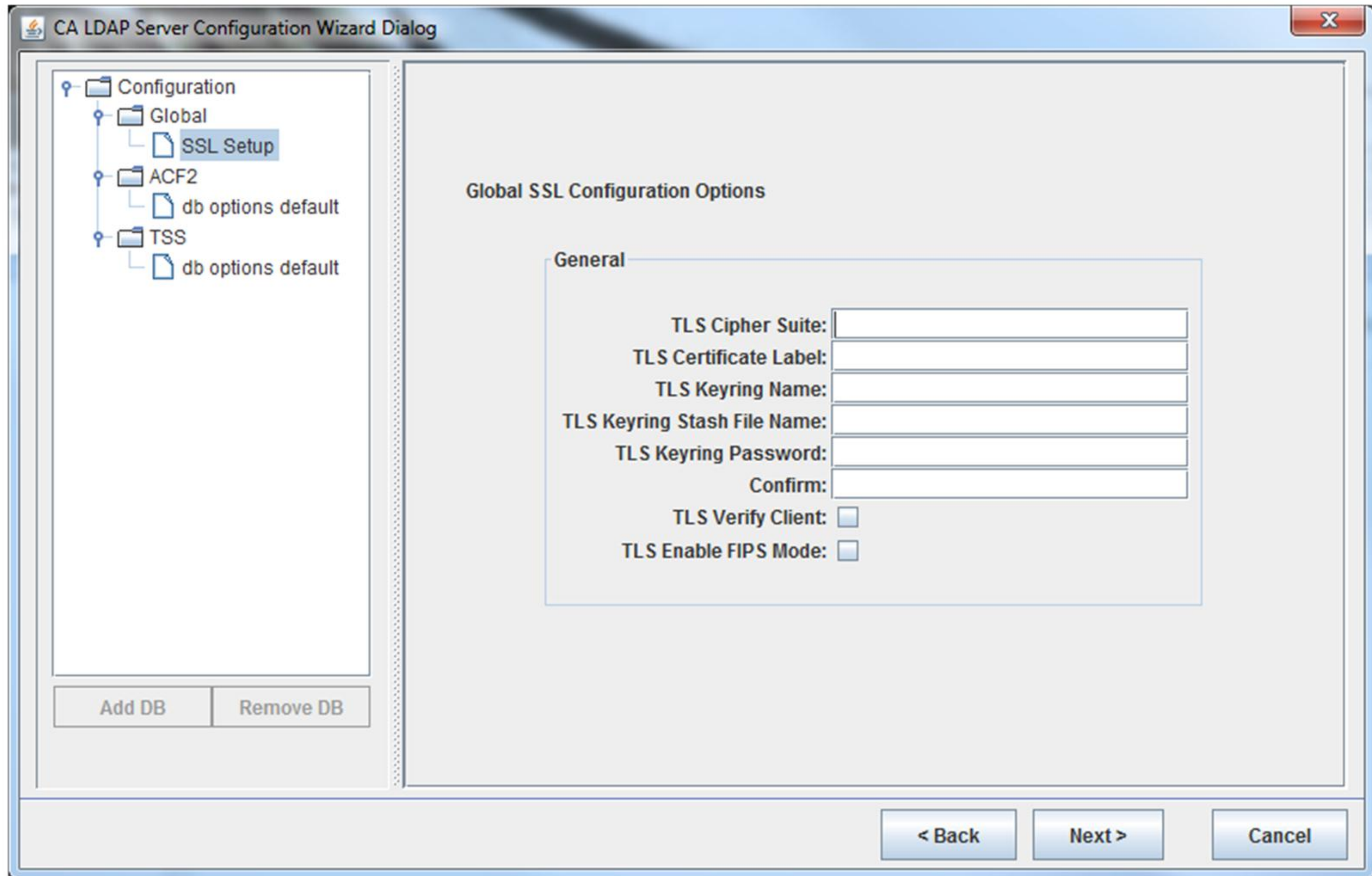
At the bottom of the tree view are two buttons: 'Add DB' and 'Remove DB'.

The main area is titled 'Global Configuration Options' and contains a 'General' tab. A note below the tab says '* = required'. The configuration options are as follows:

- * hosturls: ldap://:389
- Allow: (empty list)
- Disallow: (list containing bind_anon, bind_simple, tls_authc, bind_v2)
- lastmod: off
- Max. Operational Packet Size: 262144
- Max. Authentication Packet Size: 1677216
- PortOfEntry4: TERMINAL
- disableAttrNameValidation: ☐

At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Configuration Wizard – SSL Options



The image shows a screenshot of the 'CA LDAP Server Configuration Wizard Dialog'. The window title is 'CA LDAP Server Configuration Wizard Dialog'. On the left, there is a tree view showing the configuration structure: 'Configuration' (folder), 'Global' (folder), 'SSL Setup' (file, selected), 'ACF2' (folder), 'db options default' (file), 'TSS' (folder), and 'db options default' (file). Below the tree view are two buttons: 'Add DB' and 'Remove DB'. The main area of the dialog is titled 'Global SSL Configuration Options'. Inside this area, there is a section titled 'General' which contains the following fields and options:

- TLS Cipher Suite: [text input field]
- TLS Certificate Label: [text input field]
- TLS Keyring Name: [text input field]
- TLS Keyring Stash File Name: [text input field]
- TLS Keyring Password: [text input field]
- Confirm: [text input field]
- TLS Verify Client: ☐
- TLS Enable FIPS Mode: ☐

At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Configuration Wizard – All ACF2 Instance Options

The image shows a screenshot of the 'CA LDAP Server Configuration Wizard Dialog'. The window title is 'CA LDAP Server Configuration Wizard Dialog'. On the left, there is a tree view showing the configuration structure: 'Configuration' (folder), 'Global' (folder), 'SSL Setup' (file), 'ACF2' (folder), 'db options default' (file), 'TSS' (folder), and 'db options default' (file). The 'ACF2' folder is selected. Below the tree view are two buttons: 'Add DB' and 'Remove DB'. The main area of the dialog is titled 'ACF2 Global Settings'. Inside this area, there is a 'General' tab. Below the tab, there is a note '* = required'. The settings are as follows: 'UFN Override:' with an empty text box; 'Disable LID UFN Mapping:' with an unchecked checkbox; 'Disable User Def:' with an unchecked checkbox; 'Enable Refresh:' with a checked checkbox; 'Enable Refresh XREF:' with an unchecked checkbox; and 'Disable Segments:' with an unchecked checkbox. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

CA LDAP Server Configuration Wizard Dialog

Configuration

- Global
 - SSL Setup
- ACF2
 - db options default
- TSS
 - db options default

Add DB Remove DB

ACF2 Global Settings

General

* = required

UFN Override:

Disable LID UFN Mapping: ☐

Disable User Def: ☐

Enable Refresh: ☒

Enable Refresh XREF: ☐

Disable Segments: ☐

< Back Next > Cancel

Configuration Wizard – ACF2 Database Specific Options

The screenshot shows the 'CA LDAP Server Configuration Wizard Dialog' window. On the left is a tree view with the following structure:

- Configuration
 - Global
 - SSL Setup
 - ACF2
 - db options default (selected)
 - TSS
 - db options default

At the bottom of the tree view are two buttons: 'Add DB' and 'Remove DB'.

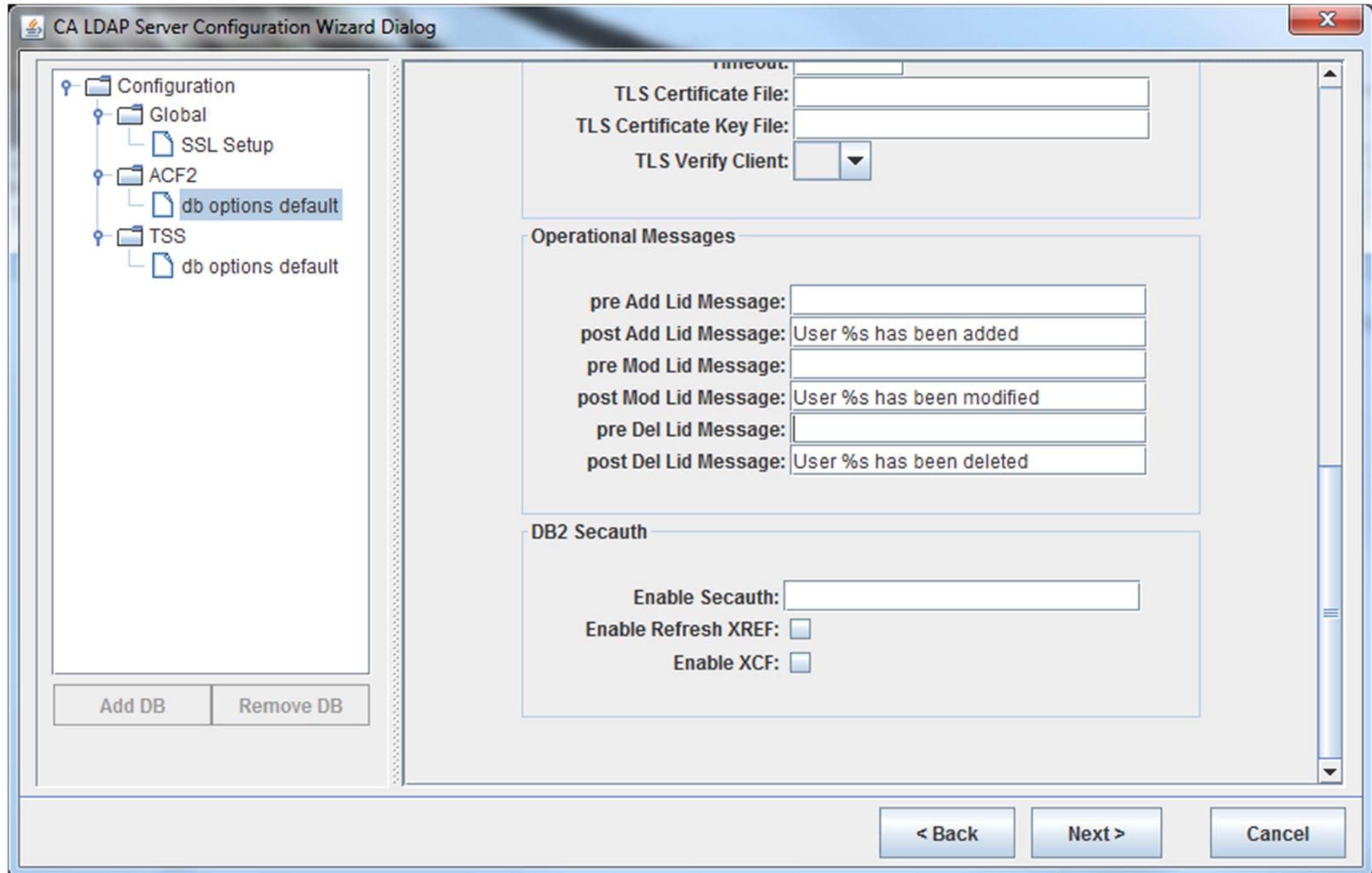
The main area is titled 'ACF2 Instance Settings' and contains a 'General' tab. Below the tab is a note: '* = required'. The settings are as follows:

- * Suffix:
- Naming Mode: (dropdown menu)
- Host UFN Override:
- Rule Cache Count:
- Enable groups:
- Create Alias:
- Disable Segments: ☐
- Enable Refresh: ☒
- Delete Alias: ☐
- Disable LID Details: ☐
- Disable Rule Details: ☐
- Disable OMVS Details: ☐

At the bottom of the main area is a section for 'Remote DSI Parm's' with an empty text box.

At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Configuration Wizard – Console Messages for Automation



The image shows a screenshot of the 'CA LDAP Server Configuration Wizard Dialog'. The dialog has a tree view on the left with the following structure:

- Configuration
 - Global
 - SSL Setup
 - ACF2
 - db options default
 - TSS
 - db options default

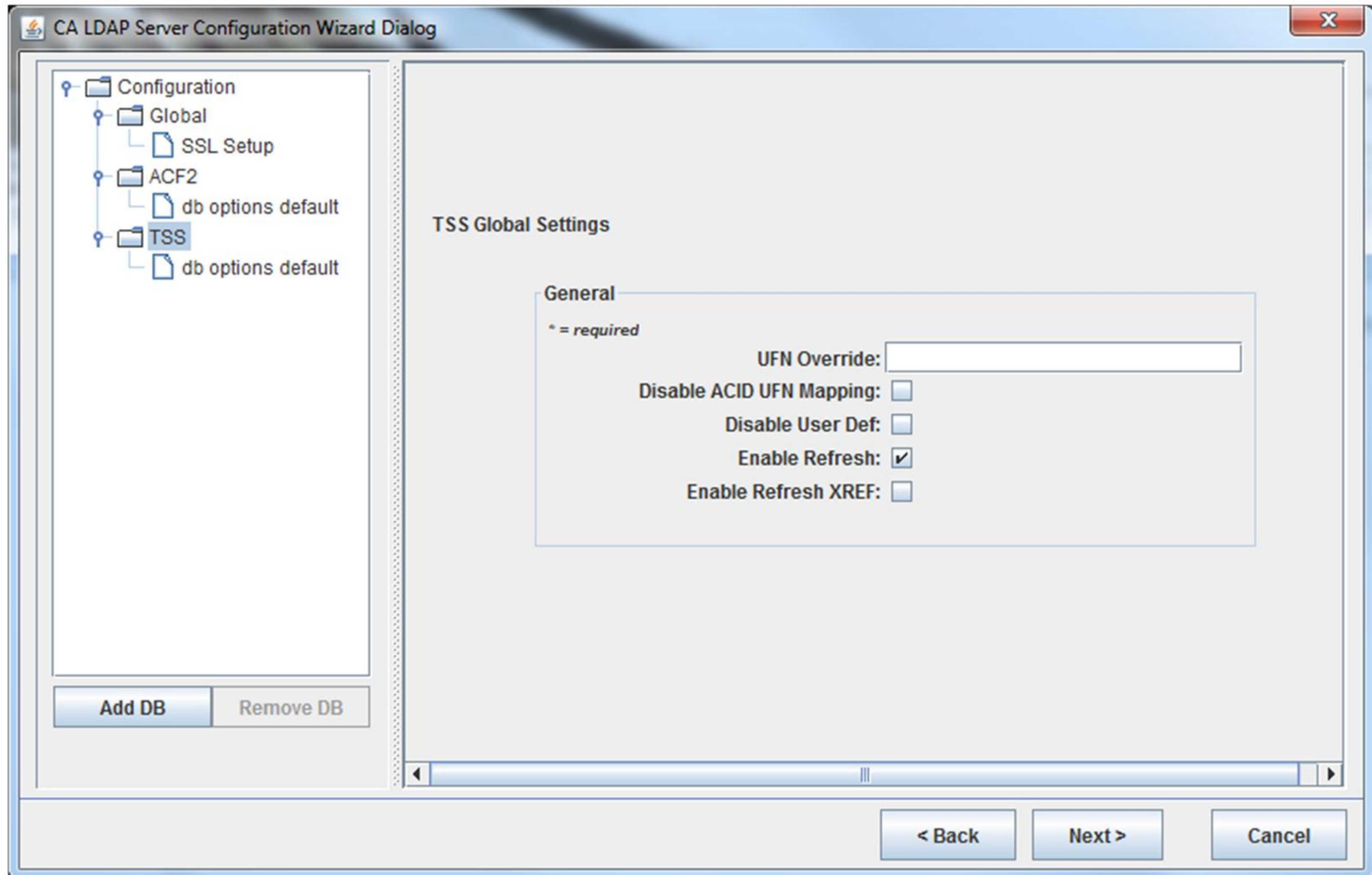
At the bottom of the tree view are two buttons: 'Add DB' and 'Remove DB'.

The main area of the dialog is divided into three sections:

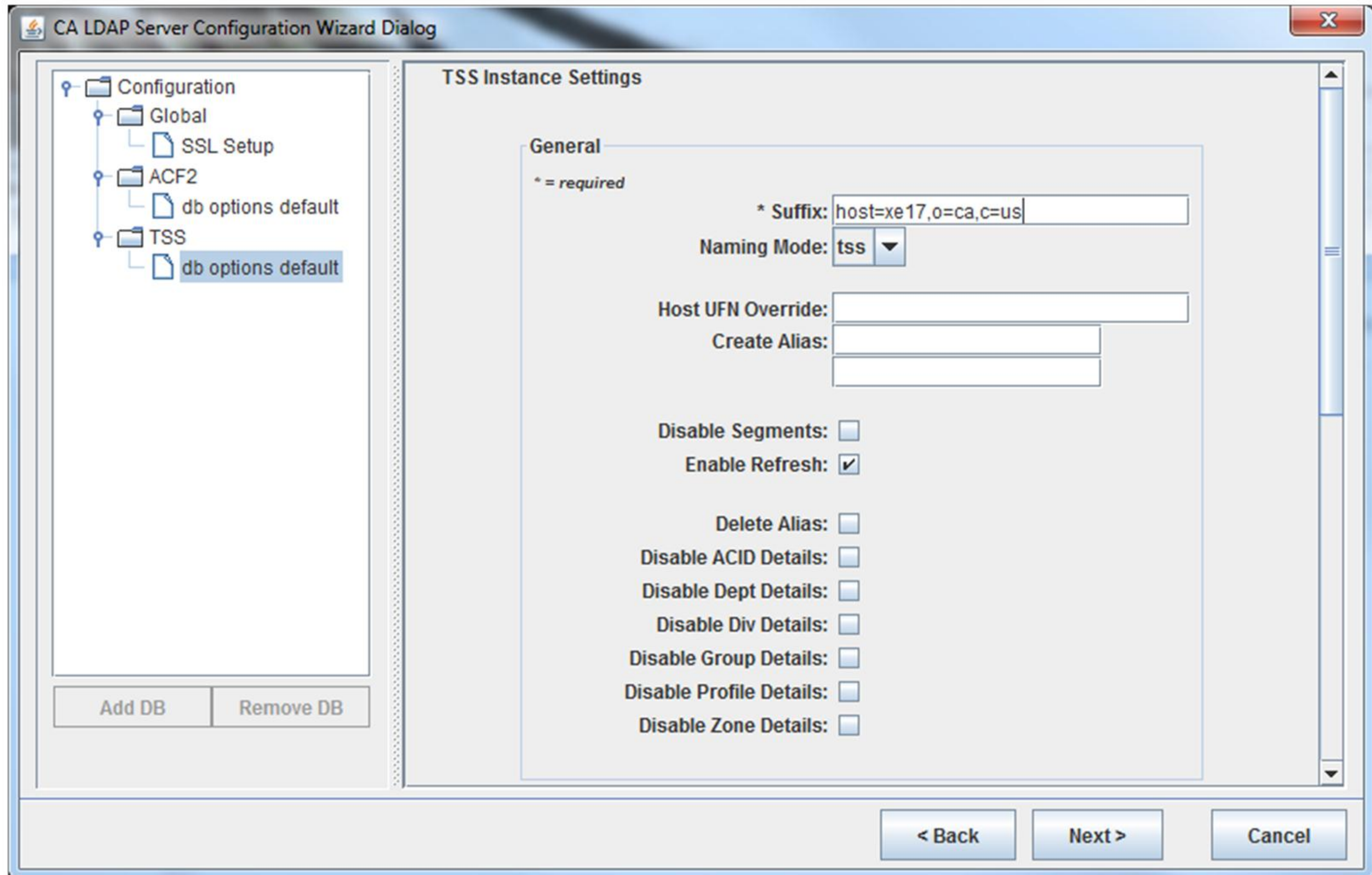
- Timeout:** A text input field.
- TLS Certificate File:** A text input field.
- TLS Certificate Key File:** A text input field.
- TLS Verify Client:** A dropdown menu.
- Operational Messages:**
 - pre Add Lid Message:** A text input field.
 - post Add Lid Message:** A text input field containing 'User %s has been added'.
 - pre Mod Lid Message:** A text input field.
 - post Mod Lid Message:** A text input field containing 'User %s has been modified'.
 - pre Del Lid Message:** A text input field.
 - post Del Lid Message:** A text input field containing 'User %s has been deleted'.
- DB2 Secauth:**
 - Enable Secauth:** A text input field.
 - Enable Refresh XREF:** A checkbox.
 - Enable XCF:** A checkbox.

At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Configuration Wizard – All TSS Instance Options



Configuration Wizard – TSS Database Specific Options



The image shows a screenshot of the 'CA LDAP Server Configuration Wizard Dialog' window. The window has a title bar with a close button. On the left is a tree view showing the configuration structure: 'Configuration' (folder), 'Global' (folder), 'SSL Setup' (file), 'ACF2' (folder), 'db options default' (file), 'TSS' (folder), and 'db options default' (file). The 'TSS' folder is selected. Below the tree are 'Add DB' and 'Remove DB' buttons. The main area is titled 'TSS Instance Settings' and contains a 'General' tab. Below the tab is a note '* = required'. The settings include: '* Suffix:' with a text box containing 'host=xe17,o=ca,c=us'; 'Naming Mode:' with a dropdown menu set to 'tss'; 'Host UFN Override:' with a text box; 'Create Alias:' with two stacked text boxes; 'Disable Segments:' with an unchecked checkbox; 'Enable Refresh:' with a checked checkbox; 'Delete Alias:' with an unchecked checkbox; 'Disable ACID Details:' with an unchecked checkbox; 'Disable Dept Details:' with an unchecked checkbox; 'Disable Div Details:' with an unchecked checkbox; 'Disable Group Details:' with an unchecked checkbox; 'Disable Profile Details:' with an unchecked checkbox; and 'Disable Zone Details:' with an unchecked checkbox. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

CA LDAP Server Configuration Wizard Dialog

Configuration

- Global
 - SSL Setup
- ACF2
 - db options default
- TSS
 - db options default

Add DB Remove DB

TSS Instance Settings

General

* = required

* Suffix: host=xe17,o=ca,c=us

Naming Mode: tss

Host UFN Override:

Create Alias:

Disable Segments: ☐

Enable Refresh: ☒

Delete Alias: ☐

Disable ACID Details: ☐

Disable Dept Details: ☐

Disable Div Details: ☐

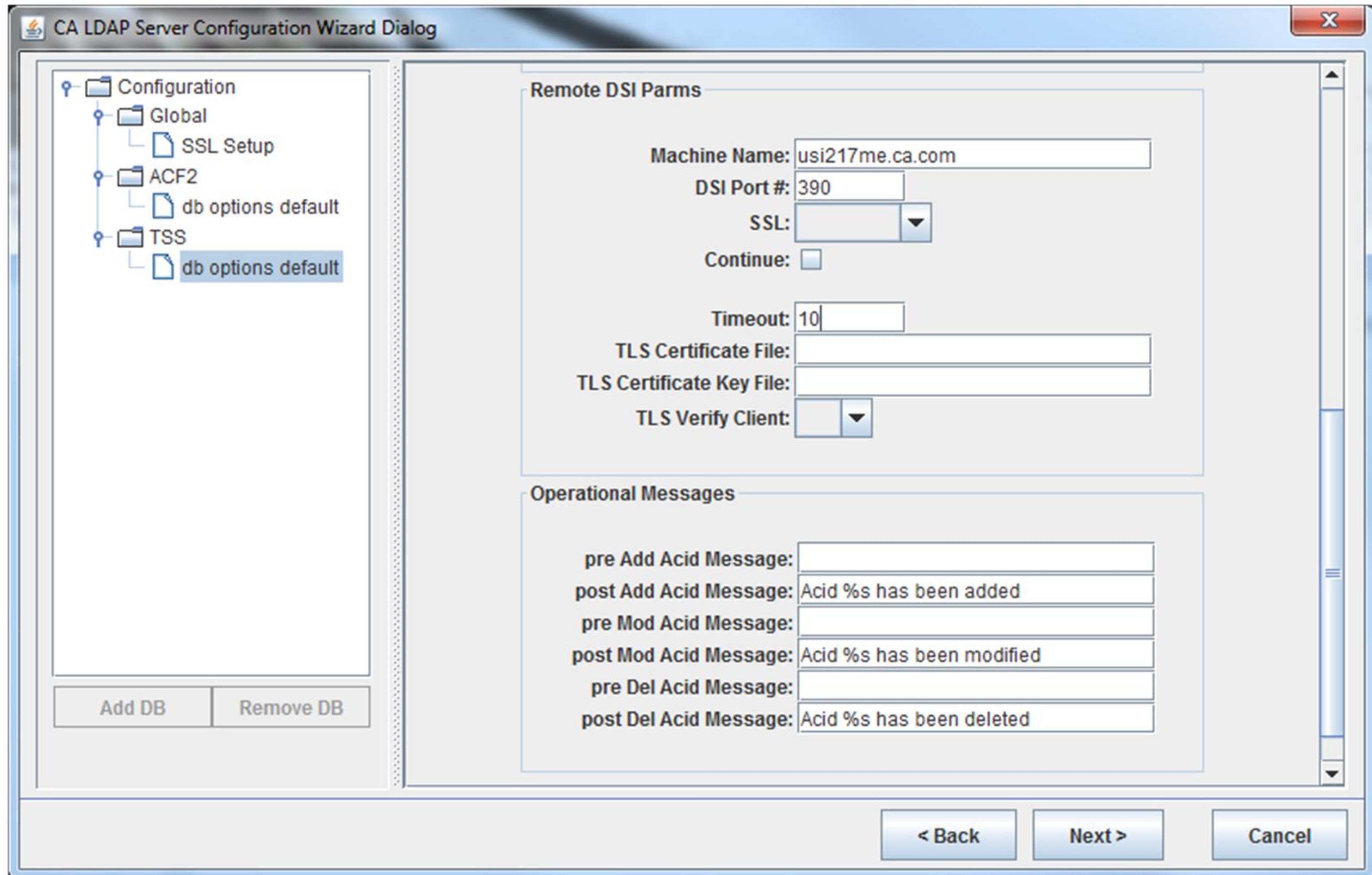
Disable Group Details: ☐

Disable Profile Details: ☐

Disable Zone Details: ☐

< Back Next > Cancel

Configuration Wizard – Console Messages for Automation



The image shows a screenshot of the 'CA LDAP Server Configuration Wizard Dialog'. The dialog has a title bar with a close button. On the left is a tree view under 'Configuration' with folders 'Global', 'ACF2', and 'TSS'. Under 'Global' is 'SSL Setup'. Under 'ACF2' is 'db options default'. Under 'TSS' is 'db options default', which is currently selected. At the bottom of the left pane are 'Add DB' and 'Remove DB' buttons. The main area is divided into two sections: 'Remote DSI Params' and 'Operational Messages'. The 'Remote DSI Params' section contains fields for 'Machine Name' (usi217me.ca.com), 'DSI Port #' (390), 'SSL' (a dropdown menu), 'Continue' (checkbox), 'Timeout' (10), 'TLS Certificate File', 'TLS Certificate Key File', and 'TLS Verify Client' (a dropdown menu). The 'Operational Messages' section contains six text input fields for messages: 'pre Add Acid Message', 'post Add Acid Message' (Acid %s has been added), 'pre Mod Acid Message', 'post Mod Acid Message' (Acid %s has been modified), 'pre Del Acid Message', and 'post Del Acid Message' (Acid %s has been deleted). At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

CA LDAP Server Configuration Wizard Dialog

Configuration

- Global
 - SSL Setup
- ACF2
 - db options default
- TSS
 - db options default

Add DB Remove DB

Remote DSI Params

Machine Name: usi217me.ca.com

DSI Port #: 390

SSL: [dropdown]

Continue: ☐

Timeout: 10

TLS Certificate File: [text box]

TLS Certificate Key File: [text box]

TLS Verify Client: [dropdown]

Operational Messages

pre Add Acid Message: [text box]

post Add Acid Message: Acid %s has been added

pre Mod Acid Message: [text box]

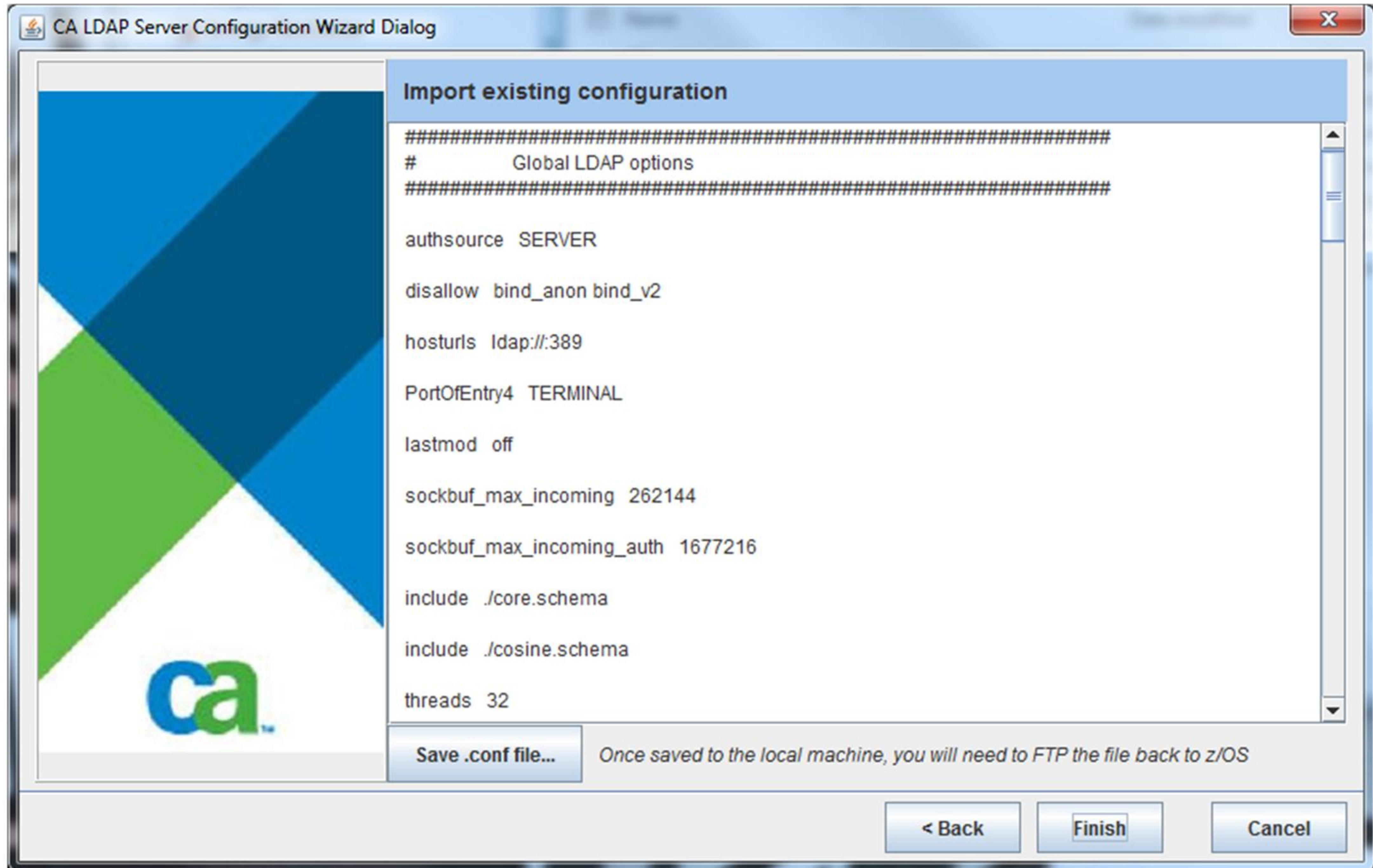
post Mod Acid Message: Acid %s has been modified

pre Del Acid Message: [text box]

post Del Acid Message: Acid %s has been deleted

< Back Next > Cancel

Configuration Wizard – Generated configuration file



CA LDAP Server console interface

- Several modify commands
 - BACKEND – Display backend specific info
 - DATABASE – Display database specific info
 - SET – Change some values while LDAP is running
 - STATUS – Displays setup info and APAR levels

CA LDAP Server console interface (cont.)

- F LDAPR15,STATUS
- Shows which ports are active, debug level, if SSL is configured, which backends are loaded/active as well as other info
- r15.1 now shows level of code running (High APAR #), as well as max region size and amount currently used

CA LDAP Server console interface (cont.)

- F LDAPR15,SET,DEBUG,0
 - Turn trace off
- F LDAPR15,SET,DEBUG,ALL
 - Turn on all tracing
- F LDAPR15,SET,DEBUG,ALL,-PACKETS,-BER
 - Turn on all tracing, excluding TCP/IP packets and BER packets
 - Gives a good level of tracing for CA support (no packet tracing)

What is CA DSI Server

I said in the opening that the LDAP protocol is not a security protocol and it has some limitations

- Login – Only allow rc=0, 49
- RACROUTE VERIFY can return 41 combinations of SAF, RACF and Reason codes

We designed to allow integration and access to the details that the LDAP protocol doesn't support

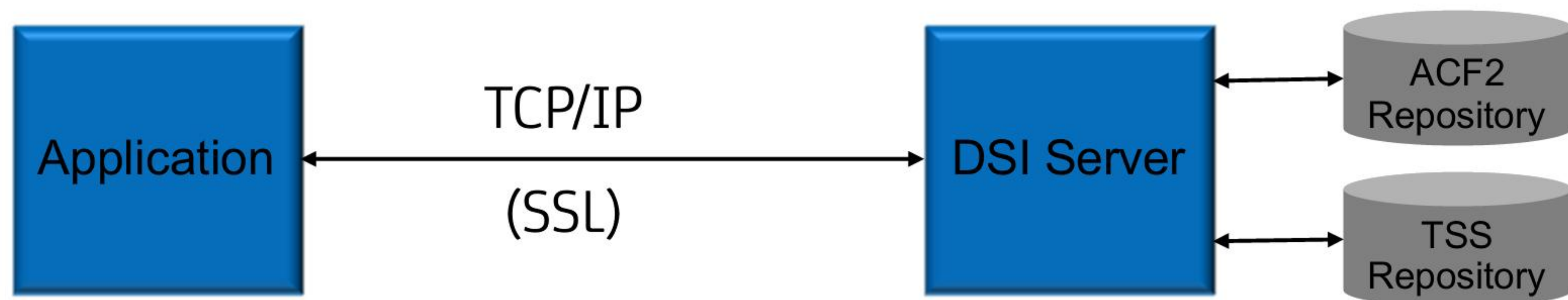
What is CA DSI Server (cont.)

CA mainframe security team designed, so it uses a proprietary protocol, but it provides access to the details that LDAP can't

To ease it's use, we supply SDKs for both C and Java

- Support for 32bit and 64 bit OS's
 - Windows
 - Linux Intel and System z
 - AIX
 - HP-UX (PARISC and Itanium(64bit only))
 - Solaris (SPARC and Intel)
 - System z

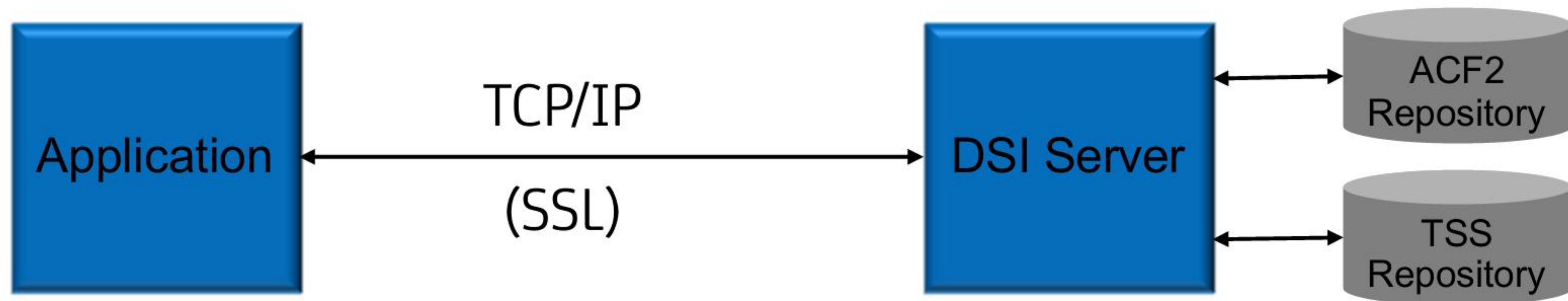
CA DSI Architecture



Implementation Options :

- Single server, single configuration, either ESM
 - Uses several callable services based on what's needed
- Uses IBM System SSL
 - Hardware crypto/FIPS support

Interaction with the ESM



- Like LDAP, never has direct access to the security file
 - Uses several callable services based on function invoked
 - No copy of the data to maintain or sync
 - ESM will determine if you are authorized (scoped)

How might I use CA DSI Server

How does CA use?

- CA Mainframe Software Manager (MSM) uses an embedded DSI Server to perform all authentication and authorizations
 - MSM menus of available options are built using Resource Check API
- CA Chorus (all roles) use an embedded DSI Server to perform all authentication and authorizations
 - Validate what functional roles the logged in user is permitted to access

Available functionality

PASSCHK

- Performs user ID and password authentication to the ESM
- Can change password as well
- Support Password and Pass Phrase

RESCHECK

- Performs a resource authorization check to the ESM

XEQCMD

- Issues any 'native' command to the ESM as if at a TSO prompt

Available functionality (cont.)

Key ring manipulation

- Delete ring - Deletes a key ring
- New ring - Creates a new key ring.
- Purge ring - Removes all certificates from an existing key ring

Digital Certificate

- Dataput – Add cert to database and connect to keyring
- Dataremove - Removes a certificate from a key ring.
 - You can also indicate that the certificate should be removed from the database.

Available functionality (cont.)

Map user id

- Maps a *long* user name to a *short* name or a *short* name to a *long* name using the SNAME, UNAME and LINUXNAM records

GETVER

- Gets the product name and version of the ESM that is currently running

Available functionality (cont.)

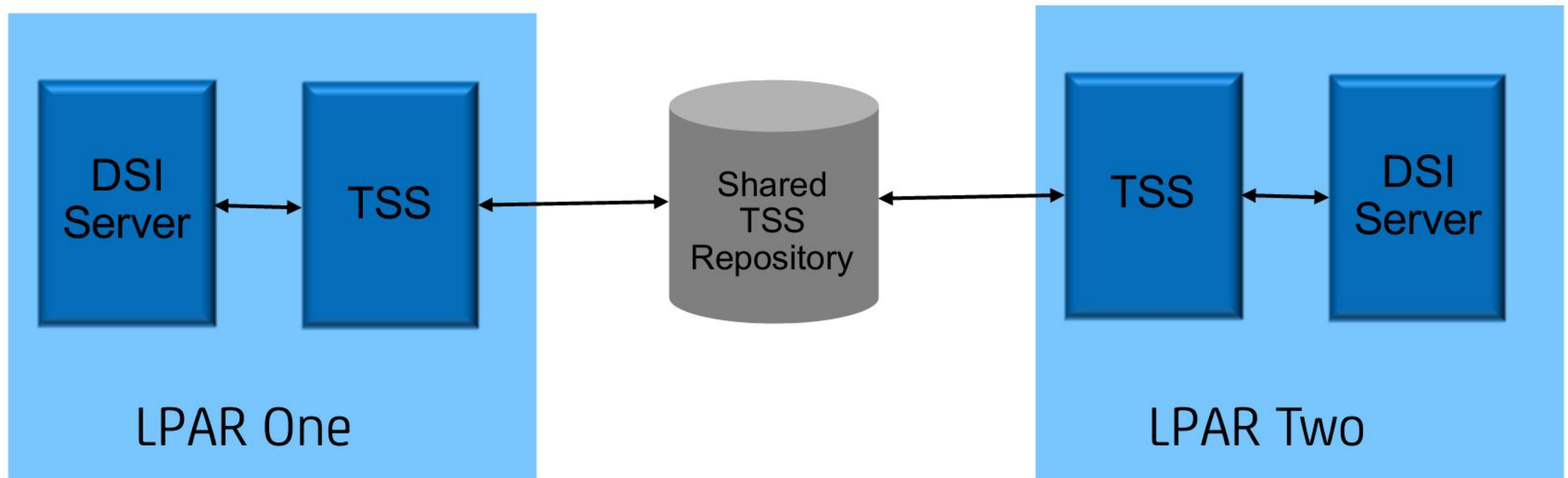
WTO

- Write a string to the system console

CERT2UID

- Maps a digital certificate to a user ID

CA DSI Architecture – Failover support



SDK implements failover :

- If you have a shared security file, setup DSI on each LPAR
- In application, define all hosts in the sequence you want the connection attempted, used in sequence

What is LDS?

LDS stands for LDAP Directory Services

- Had a client who wanted to push password changes to another product that could interface to the mainframe

Earlier I mentioned that CA LDAP Server provided inbound operations, this provides outbound changes

What do I define?

Create a LDAPNODE definition

ACF2 – INS LDAP.nodename

TSS – ADDTO(NDT) LDAPNODE(nodename)

Allows you to define what operations to send

Insert, Change, Delete – Each can be configured on/off

What do I define? (cont.)

When we discussed LDAP, I mentioned applications need to support multiple schemas

The key to LDS functionality is what we refer to as the XREF records

XREF allows the configuration (mapping) of CA ACF2 and CA Top Secret base fields to the remote LDAP Server attribute names

set control(lds)

insert ldap.cpu2 active insert delete pswdasis objclass(acf2lid)
url('ldap://ca.ldap.server:389') userdns('acf2lid=%L, host=cpu2,
o=cai, c=usa') admin dn('acf2lid=admin') adm pswd(password)
xref(name/Name)

- TSS ADD(NDT) LDAPNODE(testnode) ADMDN('cn=USER1, o=CAI, c=USA') ADMPSWD(password) USERDNS('o=CAI, ou=TSS Team, c=USA') URL(ldap://ca.ldap.server:389) XREF(ACIDNAME,ldap_attr_name1)

Can I with LDS?

Can I send authentication off platform?

No. LDS is designed to send Add, Modify and Delete commands outbound

Will I loose commands if the remote node is down?

No, if Journaling is configured and enabled. All commands hardened to disk, then read and sent.

Can I sync passwords changes to Active Directory

Yes.

Q&A ~ Open Discussion

agility
made possible™

