# AIM

The provisioning directory is configured with no access controls: if you can BIND, you can modify anything. The only accounts available with access are the built-in accounts used by the Provisioning components (Servers) to update the Directory.

However it is useful to use other (shared) accounts to access the Provisioning Directory:

* Do NOT use the built-in accounts
* Use shared accounts whose password can be changed
* Use a read-only account for investigation
* Only use an account with modify access when appropriate

## HOW

Create 2 new accounts (these are shared accounts):

* DSAWrite
* DSAReadOnly

Change configuration of ALL provisioning DSAs or routers, so these now have access controls:

* Current built-in accounts (there are 2) still have access
* These 2 new accounts have appropriate access

## IMPACT on service

No services need to be stopped during this change. The time taken to re-initialise each service is very small.

# STEPS to enable access controls

## Summary

These are the steps:

* Step 1: Create 2 shared accounts – DSAReadOnly, DSAWrite
* Step 2: Copy new file to define access-controls to all DSA servers
* Step 3: Cause Directory servers to use the new configuration
* Step 4: Check access controls

## Step 1: Create 2 shared accounts

This is done ONLY ONCE:

* The accounts are in the “common” area, and so apply to all Provisioning Directories
* If using High Availability: multi-write will update all DSAs

|  |  |
| --- | --- |
| **Step** | **Details** |
| LDAP browser: Logon to imps-router | Using JXplorer (or similar)Connect as follows:* Host: <ip-address of server>
* Port: 20391
* Protocol: LDAP v3
* Level: User+Password
* User: eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb
* Password: as defined when installed
 |
| Prepare LDIF file | In Appendix is a sample LDIF file.Edit this (reset the passwords), and save locally (so the LDAPbrowser can find the file) |
| Import LDIF | This will create the 2 usersIn JXplorer this is done as follows: * MENU: LDIF – Import File
* Browse to and select the file you just saved
* Press OPEN
 |
| Check accounts exist | Expand the Tree (eTNamespaceName=CommonObjects,dc=etadb)The 2 new accounts will now exist: |

## Step 2: Copy new file to define access-controls to all DSA servers

This must be done an ALL appropriate servers:

* Those running the provisioning-directory DSAs
* Provisioning Servers, which are running the routers

|  |  |
| --- | --- |
| **Step** | **Details** |
| Save file on server | The file is given in the appendix. It is named impd.dxc.accessCopy the file to this path:<Directory-home>\dxserver\config\access |
| Rename files so new one is used | In folder <Directory-home>\dxserver\config\accessRename file: impd.dxcTo: impd.dxc.origCopy file: impd.dxc.accessAnd rename copy as: impd.dxc |

## Step 3: Cause Directory servers to use the new configuration

This must be done an ALL appropriate servers:

* Those running the provisioning-directory DSAs
* Provisioning Servers, which are running the routers

|  |  |
| --- | --- |
| **Step** | **Details** |
| Logon to server | RDP, using your sys account |
| Run init command | Run this command:dxserver init all NOTE: this will cause all DSAs on this server to read the (changed) config files and now apply the access controls.EXAMPLE: |

## Step 4: Check access controls

It may be enough to do this only on the Provisioning Servers (allowing router to implicitly check other servers).

However, it is safest to do this check on every DSA.

* Those running the provisioning-directory DSAs (4 DSAs on each)
* Provisioning Servers, which are running the routers

### Check built-in and new accounts work

|  |  |
| --- | --- |
| **Step** | **Details** |
| Open LDAP browser | Using JXplorer (or similar) |
| CHECK 1: built-in still works | Connect as follows:* Host: <ip-address of server>
* Port: <as defined for DSA service>
* Protocol: LDAP v3
* Level: User+Password
* User: eTDSAContainerName=DSAs,
	+ eTNamespaceName=CommonObjects,dc=etadb
* Password: as defined when installed

Perform tests (connect – read – update) |
| CHECK 2: DSAWrite works | Connect as follows:* Host: <ip-address of server>
* Port: <as defined for DSA service>
* Protocol: LDAP v3
* Level: User+Password
* User: eTDSAContainerName=DSAWrite,
	+ eTNamespaceName=CommonObjects,dc=etadb
* Password: as defined when installed

Perform tests (connect – read – update) |
| CHECK 3: DSAReadOnly works | Connect as follows:* Host: <ip-address of server>
* Port: <as defined for DSA service>
* Protocol: LDAP v3
* Level: User+Password
* User: eTDSAContainerName=DSAReadOnly,
	+ eTNamespaceName=CommonObjects,dc=etadb
* Password: as set on this user

Perform tests (connect – read – No able to update) |

### TESTS to be performed

These should be done against EVERY DSA on each appropriate server.

These are as follows:

|  |  |
| --- | --- |
| **Step** | **Details** |
| Connect test | Can connect – and then see Provisioning Directory data: example: |
| Read Test | Try reading the new accounts: Example: |
| Update Test | Try updating one of the new accounts:In this case:* Changed the description
* Press SUBMIT (update the LDAP)
* View account again – check change has been applied
 |
| Update Test (insufficient rights) | When using account DSAReadOnly and submitting an update, you should get this error: |

### Complete Set of Tests (When using High-Availability)

If using 4 Provisioning Servers and 4 Directory Servers: all these tests will be needed:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server****Type** | **DSA** | **Check 1****Built-in** | **Check 2****DSAReadOnly** | **Check3****DSAWrite** |
| Provisioning 1 | Router |  |  |  |
| Provisioning 2 | Router |  |  |  |
| Provisioning 3 | Router |  |  |  |
| Provisioning 4 | Router |  |  |  |
| Directory 1 | co |  |  |  |
|  | inc |  |  |  |
|  | main |  |  |  |
|  | notify |  |  |  |
| Directory 2 | co |  |  |  |
|  | inc |  |  |  |
|  | main |  |  |  |
|  | notify |  |  |  |
| Directory 3 | co |  |  |  |
|  | inc |  |  |  |
|  | main |  |  |  |
|  | notify |  |  |  |
| Directory 4 | co |  |  |  |
|  | inc |  |  |  |
|  | main |  |  |  |
|  | notify |  |  |  |

# Appendices

## Appendix: LDIF file for 2 new users

|  |
| --- |
| version: 1DN: eTDSAContainerName=DSAReadOnly,eTNamespaceName=CommonObjects,dc=etadbobjectClass: eTDSAContainereTDescription: Shared Account - Read Only access to DSAseTDSAContainerName: DSAReadOnlyuserPassword: changeitDN: eTDSAContainerName=DSAWrite,eTNamespaceName=CommonObjects,dc=etadbobjectClass: eTDSAContainereTDescription: Shared Account - Write access to DSAseTDSAContainerName: DSAWriteuserPassword: changeit |

##  Appendix: access file: impd.dxc.access

|  |
| --- |
| # CA Directory DXserver/config/access# static access controlsset access-controls = true;# dynamic access controlsset dynamic-access-control = false;#set super-user DSAs = {  user = <dc "etadb"><eTNamespaceName "CommonObjects"><eTDSAContainerName "DSAs">};set super-user DSAs = {  user = <dc "etadb"><dc "im"><eTNamespaceName "CommonObjects"><eTDSAContainerName "DSAs">};set super-user DSAWrite = {  user = <dc "etadb"><eTNamespaceName "CommonObjects"><eTDSAContainerName "DSAWrite">};set reg-user DSAReadOnly = {  user = <dc "etadb"><eTNamespaceName "CommonObjects"><eTDSAContainerName "DSAReadOnly"> subtree = <dc "etadb"> perms = read}; |