



**TECNOLOGICO
DE MONTERREY®**

Novell eDirectory – Apple Open Directory integration through IDM

INTRODUCTION	3
OBJECTIVE	3
REQUIREMENTS	4
OPEN DIRECTORY CONFIGURATION	4
IDM CONFIGURATION	6
AFP CONFIGURATION	10

Introduction

First of all, we want to thank the support from the Novell engineer Jorge Puga on all the process of integration.

We were looking the best way to integrate our Open Enterprise Server 2 SP2 Linux Cluster environment with our Apple mac labs. We look for solutions like Kanaka, connecting directly every mac workstation to eDirectory (Simon Flood talk on Brainshare 2010) or trying to put every user identity from our edirectory to our OpenDirectory Server (Snow Leopard 10.6.3 Server)

We focus our efforts on the last options so here are the steps that we followed. I hope this can help you on some way.

If you have future improvements I hope you can send us information.

Manuel Salaiz - msalaiz@itesm.mx,

Leopoldo Márquez - leopoldo.marquez@itesm.mx

Objective

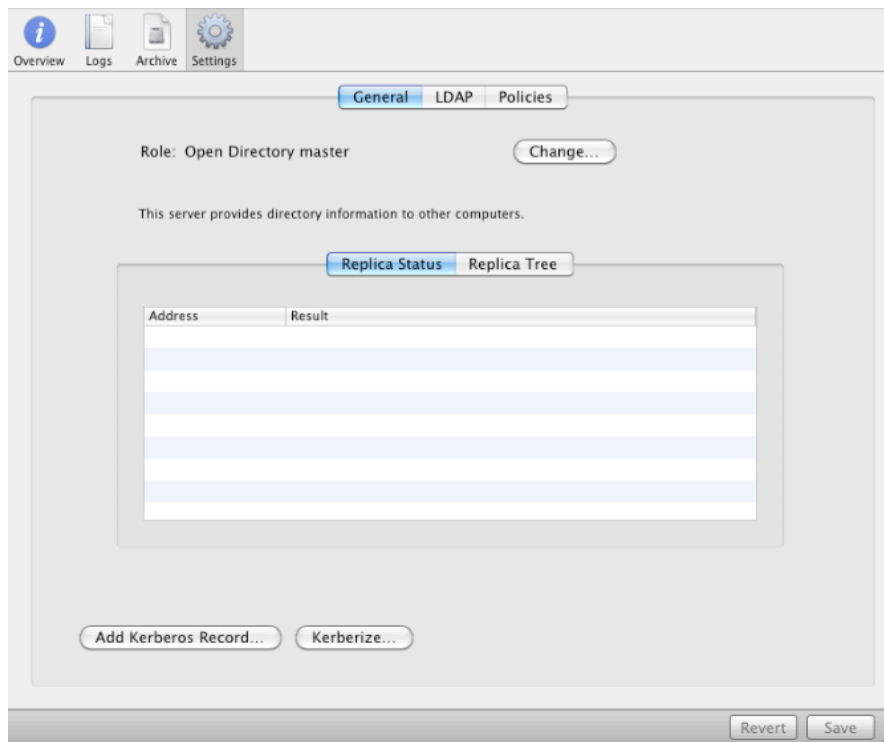
Generate user identities on a Open Directory Snow Leopard Server from a eDirectory 8.8. Our eDirectory is mounted on an Open Enterprise Server 2 SP2 Linux version. This identity synchronization was achieved through LDAP-IDM3_6_0-V4 driver

Requirements

- A Snow Leopard Server
- Open Directory Server configured as Open Directory Master
- A Open Enterprise Server 2 SP2, AFP pre-configured and working.
- eDirectory 8.8
- IDM 3.5.1 installed and configured on OES2 SP2

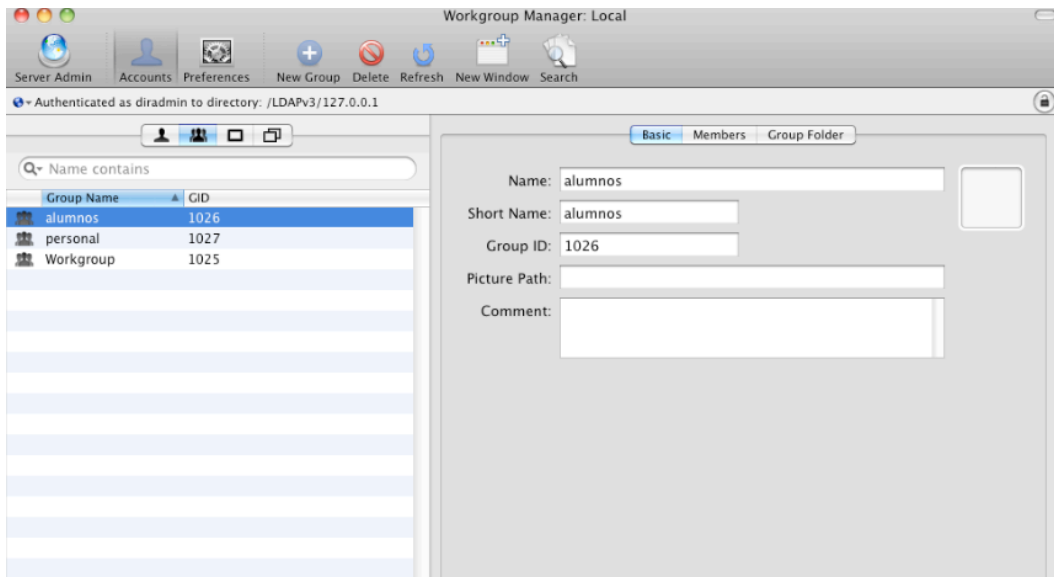
Open Directory Configuration

1. Generate a open directory master directory



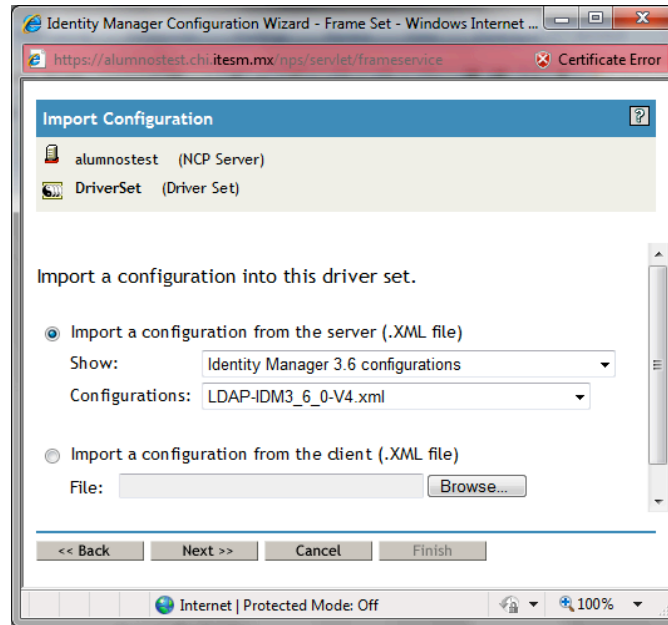
ITESM Campus Chihuahua

2. Generate groups on Open Directory so you can control access to workstation by profiles. We generate a group for students (alumnos) and other for teachers and staff (personal).

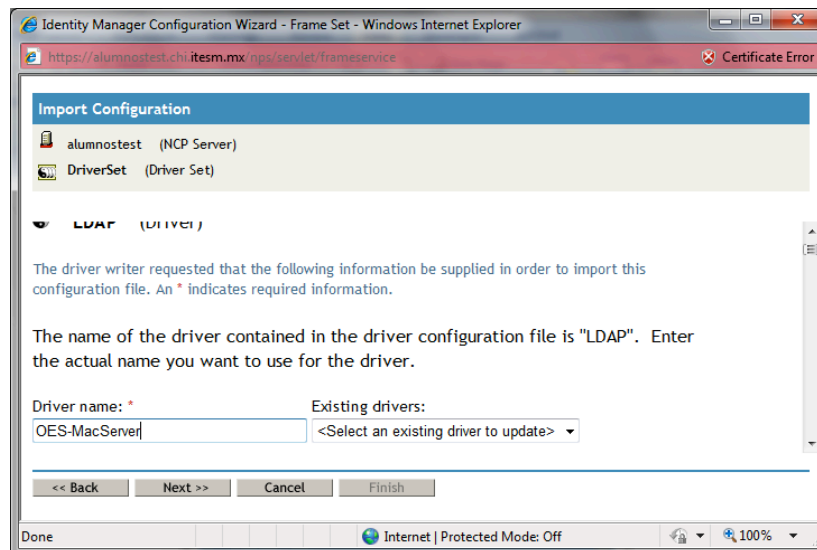


IDM Configuration

1. Generate and configure LDAP-IDM3_6_0-V4 drivers available on IDM installation.



2. Define the initial configuration for our driver set

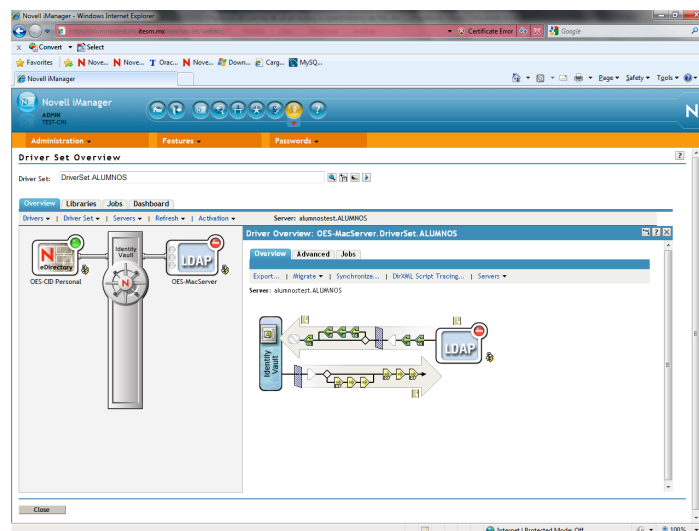


ITESM Campus Chihuahua

Some important features that you have to consider on this configuration are:

- Subscriber Channel Placement Type:** Specify the desired form of placement for the Subscriber channel. Select Flat to place objects strictly within the base container. Select Mirrored to place objects hierarchically within the base container. This is used to determine the Subscriber channel Placement policies.
- Connected LDAP Server Base DN:** Specify the container where user objects reside in the LDAP Directory. If you are using a flat Placement rule, this is the container where the users are placed. If you are using a mirrored Placement rule, this is the root container.
- Publisher Channel Placement Type:** Specify the desired form of placement for the Publisher channel. Select Flat to place objects strictly within the base container. Select Mirrored to place objects hierarchically within the base container. This is used to determine the Publisher channel Placement policies.
- Driver is Local/Remote:** Do you want this driver to run locally, or remotely with the Remote Loader service?
- LDAP Authentication DN:** Enter the DN of the LDAP account the driver will use for authentication. Example
uid=useradmin,cn=users,dc=nameserver,dc=chi,dc=itesm,dc=mx
- LDAP Authentication Password:** Enter the password for the LDAP authentication account.
- LDAP Server:** Enter the hostname:port or IP address:port of the LDAP server. Typical ports are 389 for standard LDAP and 636 for LDAP over SSL. [###.###.###.###:port]

After all this process you will have a new LDAP driver on a driver set



ITESM Campus Chihuahua

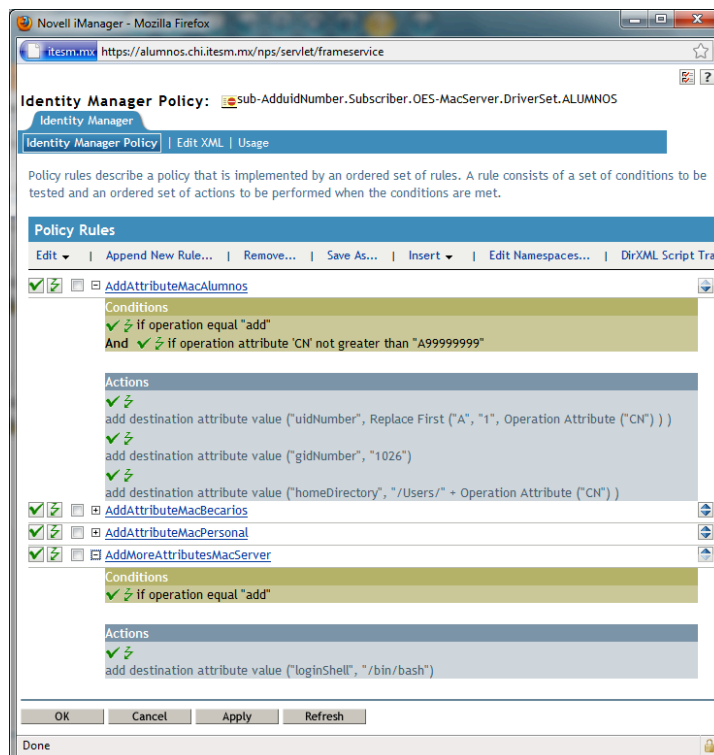
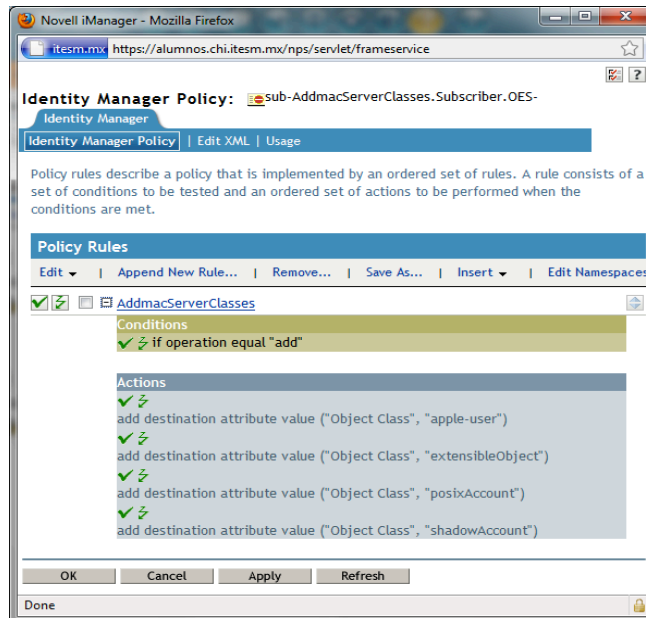
Now we need to do some additional adjustments to our driver to ensure that we are generating classes and attributes required on Mac users, so workstation can authenticate on the Open Directory

If we observe our users objects on OpenDirectory through a LDAP Browser we can see classes and attributes that are really important, so we need to generate them:

- **homeDirectory** (We put */Users/ID*). This value is really important because it generate a users home directly on each workstation they login.
- **loginShell**: It could be any shell that mac uses like */bin/bash, /bin/sh, /bin/ksh...*
- **uidNumber**. We decide to put *1+student-id* or *2+teacher-id*. But you can use any uid, just be careful that you don't put the same id for two user objects.
- **gidNumber**. Put the id explained before for each group you generate on Open Directory configuration. On this document Alumnos = 1026 and Personal = 1027
- **class Apple-user**. Just generate the class as is shown on the next image
- **class extensibleObject**: Just generate the class as is shown on the next image
- **class posixAccount**: Just generate the class as is shown on the next image
- **class shadowAccount**: Just generate the class as is shown on the next image

ITESM Campus Chihuahua

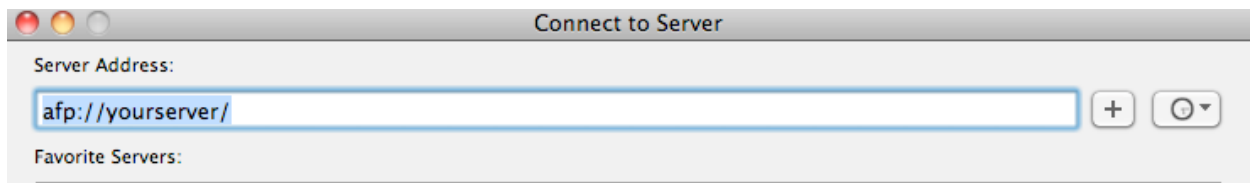
To add these classes and attributes that we mentioned before, we generate one or more policies on the subscriber channel specifically on “creation policies” of our driver, as it is shown on the next figure:



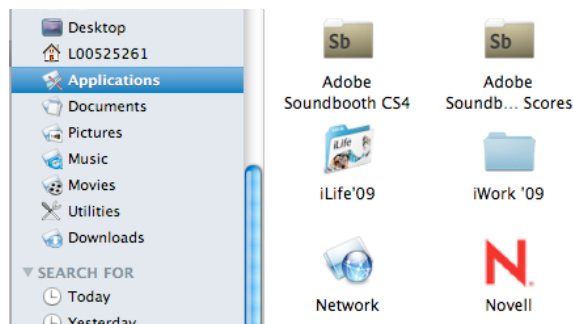
AFP Configuration

If you want to Mac users map their Novell home directories, you must configure your home users volumes on your OES2 SP2 server to support AFP connections. To do that you need:

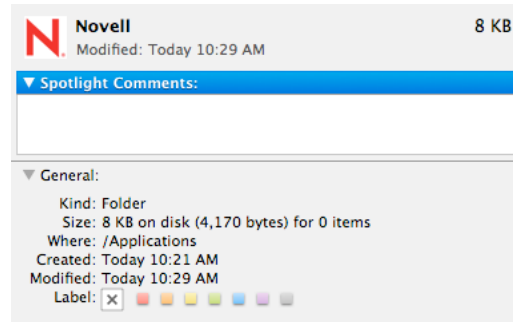
1. Install and configure AFP service on your OES 2 SP2 Servers where the users home are. (http://www.novell.com/documentation/oes2/file_afp_lx/?page=/documentation/oes2/file_afp_lx/data/accym3.html-accym3)
2. Be sure that users can connect to a OES2 SP2 Servers through AFP protocol (afp://yourserver/)



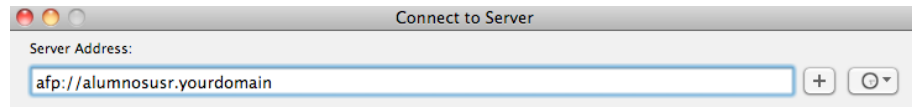
3. Create a easy way for users to connect to their home directories, to do that, we create a application folder on each mac workstation, that contained a alias that point to their home directory accessed by AFP. Here the steps we follow:
 - a. Create a folder called Novell on applications for every mac workstation (change the icon to something users can recognize)



ITESM Campus Chihuahua



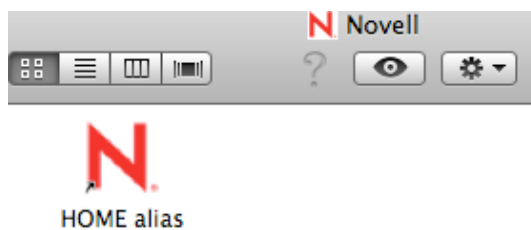
- b. On that folder create an Alias that point to the afp home directory on OES2SP2. To do that you can connect to your afp home directory volume as admin and generate the alias and copy that alias to your mac workstation.



After we connect to the home users (admin account)

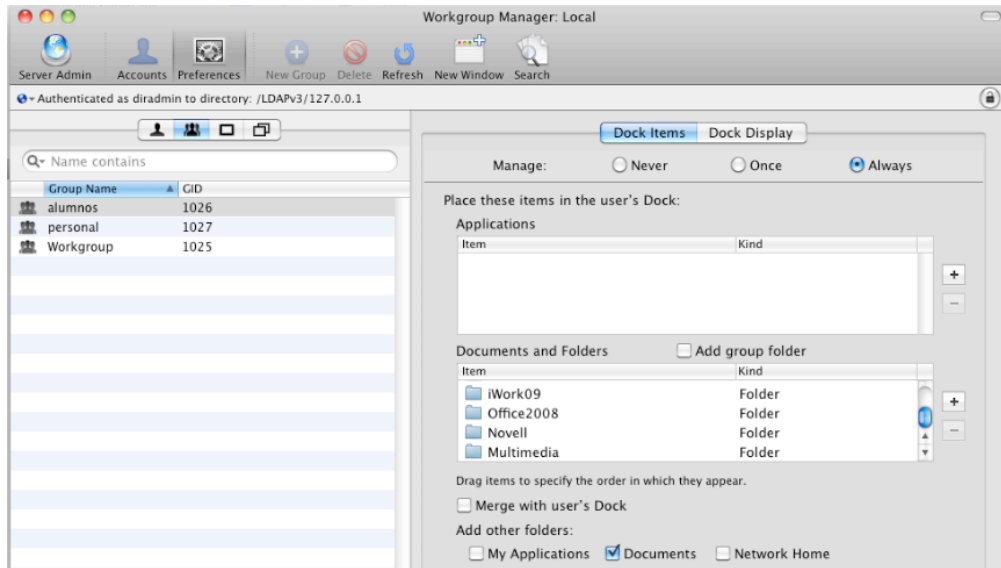


Copy that alias to the Novell Application Folder that we created before.



ITESM Campus Chihuahua

- c. After we generate a afp home directory alias, we just modify the docking for all students group through our open directory server (Workgroup Manager), so the docking it is the same for everyone.



And the docking look like this after the user login to the mac server

