

Tearing down the Local Kerberos (LKDC) Centre on Leopard Server



January 2009

Tearing down the Local KDC (LKDC) on the Open Directory infrastructure:	3
<i>For the Master ODM:</i>	3
Setting up the Open Directory Child Server	4
Binding without tearing down the Open Directory Master	5
To test if its working:	7

Tearing down the Local KDC (LKDC) on the Open Directory infrastructure:

For the Master ODM:

Demote the server to stand alone as root from the command line:

```
# slapconfig -destroyldapserver
```

Alternatively, this can be done from Server Admin --> Open Directory

```
# rm -rf /private/var/db/krb5kdc
# mkdir -m 700 /private/var/db/krb5kdc
# rm -rf /etc/krb5.keytab
# rm -rf /Library/Preferences/edu.mit.kerberos
# rm -rf /Library/Preferences/com.apple.AppleFileServer.plist
```

On the local Default node, remove the following entries (if they exist) on the server to be the master ODM:

```
# dscl
# cd /Local/Default/Config
# delete Kerberos:SERVER.REALM.CA
# quit
```

Then run (all on 1 line):

```
# slapconfig -createldapmasterandadmin diradmin "Directory
Administrator" 1000 dc=server,dc=realm,dc=ca
SERVER.REALM.CA
```

Alternatively, you can run this from the Server Admin --> Open Directory and change the role from Stand Alone to Open Directory Master and fill out the same information. Running it from the command line just gives you explicit output of the setup process and you can find any issues that pop up as opposed to getting it all the way through and learning that the Kerberos didn't start up properly.

The above will setup the Kerberos environment and the Open Directory (LDAP) services as well as kerberize all services and the base users on the system (root / diradmin / vpn auth)

There is no longer a requirement to enter in the Child Servers SERVER NAME into the computers tab within Workgroup Manager as we did in the past with 10.4 and earlier.

Setting up the Open Directory Child Server

```
# rm -rf /private/var/db/krb5kdc
# mkdir -m 700 /private/var/db/krb5kdc
# rm -rf /etc/krb5.keytab
# rm -rf /Library/Preferences/edu.mit.kerberos
# rm -rf /Library/Preferences/
com.apple.AppleFileServer.plist
```

In Directory Utility, remove any servers listed in the Search Policy in the Search Base from "custom" change both the Authentication and the Contacts back to Automatic

```
# sudo killall DirectoryService
# dscl
# cd /Local/Default/Config
# delete Kerberos:SERVER.REALM.CA
# sync <--Optional
# sync <--Optional
# shutdown -r now
```

Launch Server Admin, click on Services for the child server and add in Open Directory

- Click on the "Change" button, and select "Connected to a Directory Server"
- Click on Open Directory Utility and use Directory Utility to connect to the remote server:
- Click on the "+" button and type in the name of your OD Master (server.realm.ca)
- Once configured (you generally don't need to worry about authenticated binding) click on the OK button.

Under the authentication and contacts tab in Directory Utility, the search should be set to Custom Path and the server should be in the list.

You can now quit the Directory Access Application

- Click on the "Join Kerberos Button" and you will be prompted for the Directory Administrators (or another admin with the ability to join the Kerberos domain) and password.

Once the server adds in the keys and principals, the information Join Kerberos button will disappear after you refresh Server Admin.

You can also join this from the command line with the following command (all one line):

```
# sso_util configure -r SERVER.REALM.CA -a diradmin -p ****
-f /LDAPv3/server.realm.ca -v 1 all
```

If you go back to the Open Directory Master, and issue the following command as root:

```
# kadmin.local
```

and then

```
> listprincs
```

You will get the output of your principals from the KDC and you should see something along these lines:

```
kadmin/admin@SERVER.REALM.CA  
kadmin/changepw@SERVER.REALM.CA  
kadmin/history@SERVER.REALM.CA  
kadmin/SERVER.REALM.CA@SERVER.REALM.CA  
krbtgt/SERVER.REALM.CA@SERVER.REALM.CA  
ldap/server1.realm.ca@SERVER.REALM.CA  
ldap/server.realm.ca@SERVER.REALM.CA
```

Binding without tearing down the Open Directory Master

If you already have a pre-existing Mac OS X Server Open Directory installation that you don't wish to destroy, you can still setup the child server to properly authenticate with Kerberos authentication.

What you need to do is tear down the local KDC system on the server and delete the Kerberos Client records on the local default search node.

Then, setup the server again as Connected to Directory Service through Server Admin and then once that is done, reconfigure the Directory Utility on the child server to authenticate against the Open Directory Master server and then join Kerberos.

Follow these steps:

- 1.) Remove the server from the Open Directory Network and turn it back to stand alone
- 2.) From the terminal:

```
# dscl
# cd /Local/Default/Config
# delete Kerberos:SERVER.REALM.CA
```

- 3.) Launch Directory Utility and remove the ODM from the search and contact fields and set back to automatic.

- 4.) From the terminal:

```
# killall DirectoryService
# rm -rf /Library/Preferences/edu.mit.Kerberos
# rm -rf /etc/krb5.keytab
# rm -rf /var/db/krb5kdc
# mkdir -m 700 /var/db/krb5kdc
```

- 5.) In Server Admin, choose Open Directory and then change it from a stand alone server to "Connected to a Directory Server" This sets up the following:

```
# slapconfig -setclient
# slapconfig -setmacosxodpolicy
```

- 6.) In Server Admin, click on the Open Directory Utility... Button

- 7.) In the Directory Utility application, connect to your remote server either from the File --> Connect or "Option + K" command

- 8.) In the server, type in the remote Server DNS or IP address, and local admin username and password

- 9.) In the Directory Servers Option, click on the "+" button and fill out the information for your remote ODM Server. server.realm.ca

Optional: If prompted to bind to your server, and your environment requires this, enter in the user name and password of a network administrator who has rights to bind the child server into the Open Directory Environment.

This sets up the search path and contacts to browse not only the local users and groups on the child server, but also the network directory server (server.realm.ca)

- 10.) With that portion done, you are now free to join the server via Kerberos. Click on the Join Kerberos button. From the pop down menu, you should have ONLY the main

Open Directory Network (SERVER.REALM.CA) and not the Local KDC (LKDC:SHA1.1A9FC49F1E499BFD1AF68001C454977B1A8F0BD2)

Enter in the username and password of a user who has rights to join the server into the environment. By default this would be the user “diradmin” with the password you set at time of creation of the Open Directory Master.

The above interaction does the following from the command line:

```
# sso_util configure -r SERVER.REALM.CA -a diradmin -p ****  
-f /LDAPv3/server.realm.ca -v 1 all
```

This builds and populates and `/etc/krb5.keytab` file from the main Open Directory master.

If you now click on the refresh button on your Open Directory Section within Server Admin, the “Join Kerberos” button should now be gone.

Congratulations, you have joined your child server to Open Directory successfully with a single Network based Kerberos Realm, for Single Sign-On Authentication.

If you want to test the Kerberos and ensure that all the keys were properly entered on the child server, do the following on your child server:

```
# sudo ktutil  
> read_kt /etc/krb5.keytab  
> list
```

You should get a whole list of all server servers and principals for the server.

To test if its working:

Change your AFP settings in Server Admin to only allow Kerberos Authentication
Launch the Kerberos App [/System/Library/Core Services/Kerberos](#) (on the master).

Click new and obtain a network users name and password (diradmin should work)
Once you have a Kerberos ticket, in the Finder, choose to connect to the child server you just joined into the network. You should automatically get an AFP ticket for the child server and have the list of available share points which you can access. You can see the tickets in the Kerberos App which you currently have or from the command line.

To obtain a ticket:

```
# kinit diradmin < -- Or another network user
Please enter the password for : diradmin@SERVER.REALM.CA
# klist
Kerberos 5 ticket cache: 'API:Initial default ccache'
Default principal: diradmin@SERVER.REALM.CA

Valid Starting      Expires              Service Principal
01/30/09 10:01:21   01/30/09 20:01:21   krbtgt/
SERVER.REALM.CA@SERVER.REALM.CA
renew until 02/06/09 10:01:21
```

You now have a Kerberos ticket from the master. Now in the finder, connect to the child server you just setup, and once you mount a share point, go back and again issue the following command: klist

You should now see the following:

```
01/30/09 09:51:01   01/30/09 19:50:51
afpserver/server1.realm.ca@ SERVER.REALM.CA
renew until 02/06/09 09:50:51
```