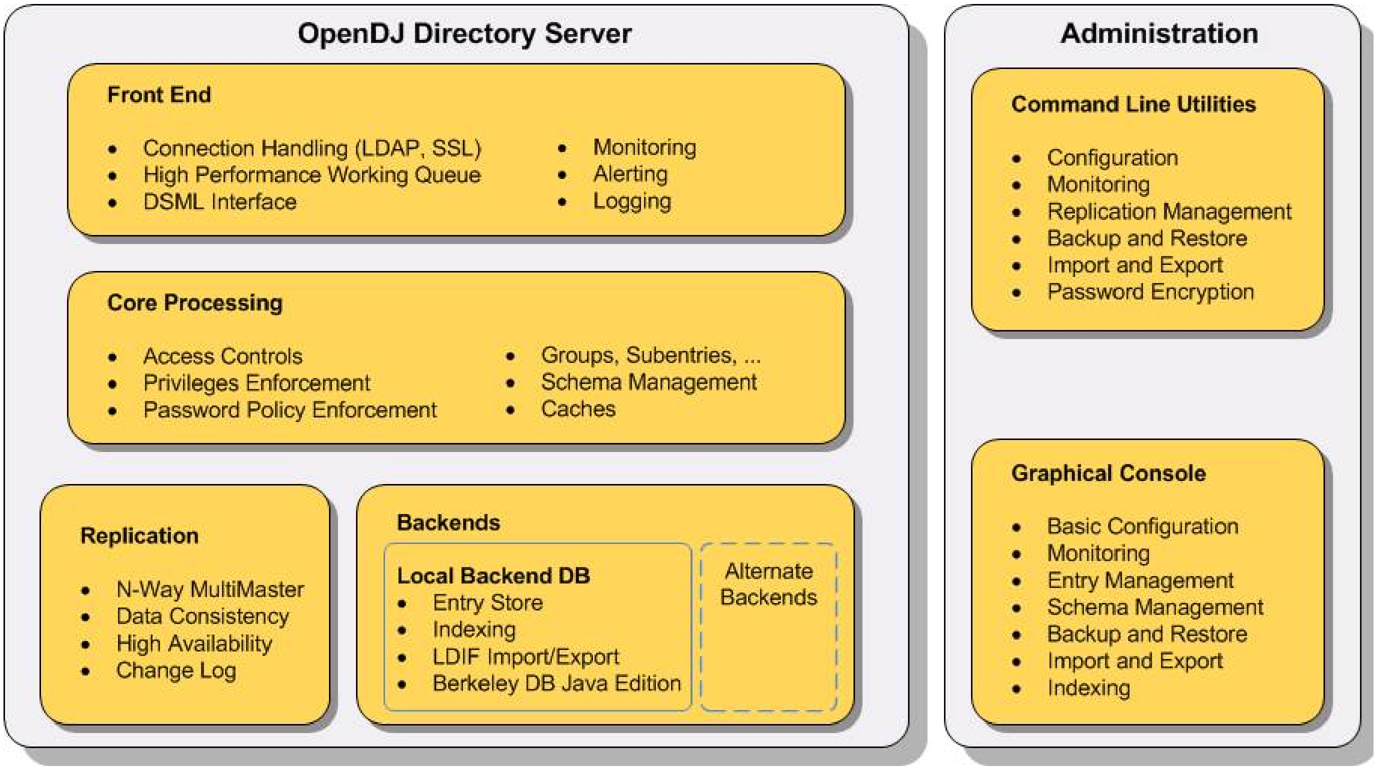
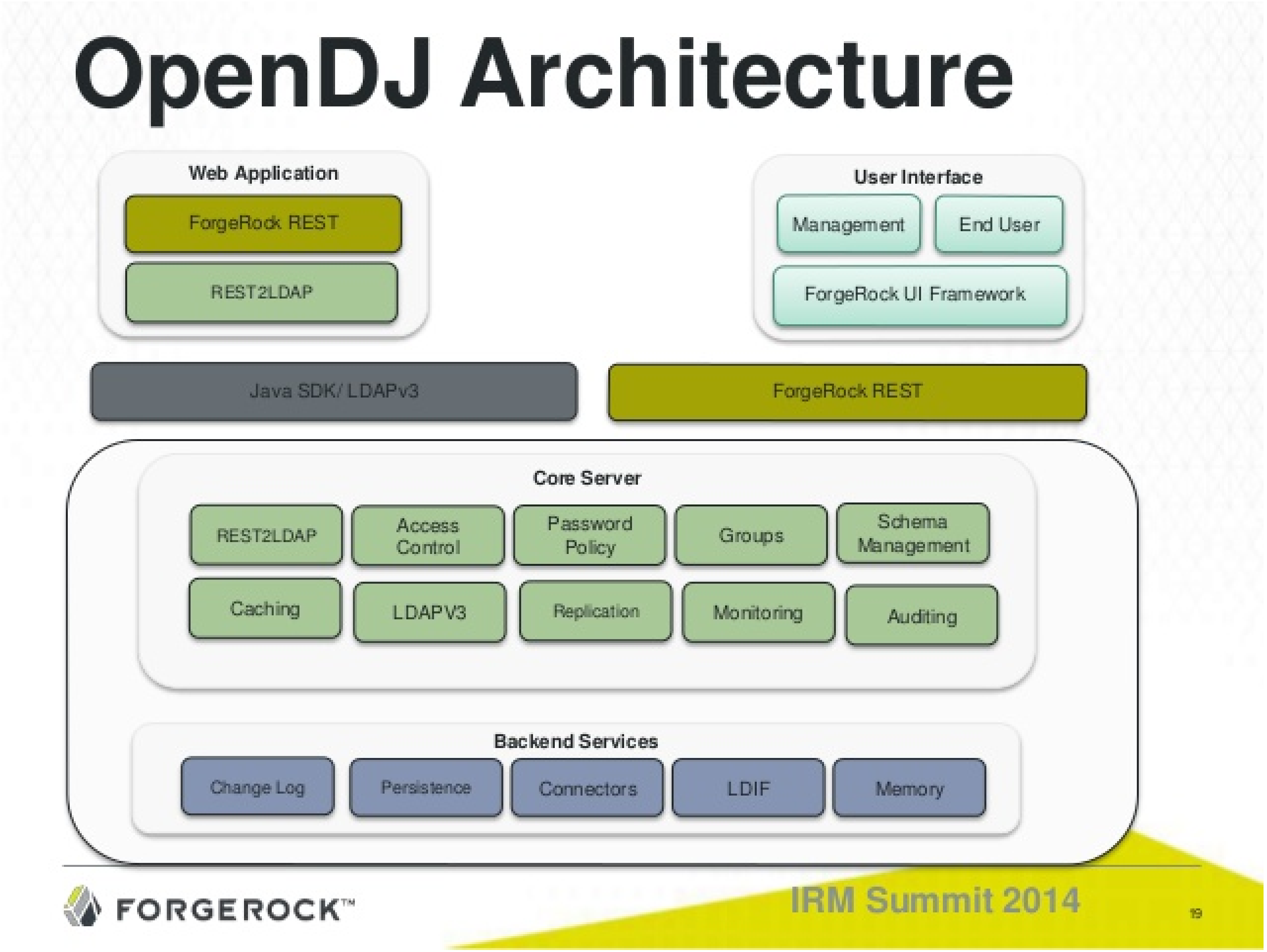
OpenDJ 2.6.0 Primary

High Level Diagrams





OpenDJ Architecture

Web Application

ForgeRock REST

REST2LDAP

User Interface

Management

End User

ForgeRock UI Framework

Java SDK/ LDAPv3

ForgeRock REST

Core Server

REST2LDAP

Access Control

Password Policy

Groups

Schema Management

Caching

LDAPV3

Replication

Monitoring

Auditing

Backend Services

Change Log

Persistence

Connectors

LDIF

Memory

FORGEROCK™

IRM Summit 2014

19

DNS

OpenDJ replication requires that you use fully qualified domain names, such as opendj.example.com so we'll use,

opendj1.krypton.com and www.opendj1.krypton.com

Subsequent server instances with replication will increment the number for example

opendj2.krypton.com and www.opendj2.krypton.com

Ensure that your dns entries are in your host file,

```
127.0.0.1   localhost

127.0.1.1   opendj1
127.0.1.1   www.opendj1.krypton.com
127.0.1.1   opendj1.krypton.com
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

This is the hosts file from Ubuntu 14.x.

Setup Java

Java 8 is not supported with this version so use Java 7.

Make OpenDJ truly zero footprint and specify the exact version of Java to run via the systems configuration file. Will use a Java environment variable to run OpenDJ.

When you try to run the setup,

```
cd /opt/opendj

./setup --cli
Please set OPENDS_JAVA_HOME to the root of a Java 6 update 10 (or higher)
installation or edit the java.properties file and then run the
dsjavaproperties script to specify the Java version to be used.
```

Install Java

Forget about using editing the java.properties. Instead, first install JRE per the Zero Footprint Java on Ubuntu instructions using serveradmin. The only slight change is that we will move the JRE into the following folder using a root enabled account,

```
sudo mv /home/serveradmin/java/ /opt/java-forgerock/
sudo chown -R serveradmin:staff /opt/java-forgerock/
sudo chmod -R 750 /opt/java-forgerock/
```

I thought about using oracle **server** jre edition, but given certificate things, it's best to use the most popular and tested which is standard jre.

Configure Java Environment Path

We set the environment variable for serveradmin by editing the profile for the account running opendj. In this case, serveradmin,

```
cd ~
vi .profile
```

At the the following to the end of the file,

```
export OPENDJ_JAVA_HOME=/opt/java-forgerock
export OPENDS_JAVA_HOME=/opt/java-forgerock
```

There is still a need for OPENDS environment. Variable. Looks like since 2.4.5 this was somewhat fixed (ie OPEN**DJ** is now being used), but some parts of the code are still using OPEN**DS** so you need both. Report this when I have time.

Command Line Setup

Do everything as the user that will be running OpenDJ. In our tutorial we will use **serveradmin** unless otherwise indicated,

OpenDJ Download and Prep

First grab the software and unzip,

```
wget http://download.forgerock.org/downloads/opendj/2.4.5/OpenDJ-2.4.5.zip
unzip OpenDJ-2.4.5.zip
```

Setup folder using a **root** capable user,

```
sudo mv /home/serveradmin/opendj/ /opt/
cd /opt
sudo chown -R serveradmin:staff ./opendj/
sudo chmod -R 750 ./opendj/
```

Now with 5.0 LXC, you can easily setup multiple machines (instead of using just one machine) to try out replication so I have dropped the opendj1 folder name convention from previous tutorials. Uniformity also makes it easier to compare instances too.

Start the Setup

Run the command line setup using the opendj dedicated account,

```
cd /opt/opendj
./setup --cli
```

Unless otherwise indicated select the default option,

```
What would you like to use as the initial root user DN for the Directory
Server? [cn=Directory Manager]:
Please provide the password to use for the initial root user:
Please re-enter the password for confirmation:
```

Make sure to use a complex password for the initial root user. We'll use the standard T&R password on "Directory Manager".

```
Provide the fully-qualified directory server host name that will be used
when
generating self-signed certificates for LDAP SSL/StartTLS, the
administration
connector, and replication [ldap1]: ldap1.krpton.com
```

This will be name of the first server. Second server increment by one. Note you **must** use a fully quantified name. If it is not registered in your DNS then you may use hosts file instead.

```
On which port would you like the Directory Server to accept connections
from
LDAP clients? [1389]:
On which port would you like the Administration Connector to accept
connections? [4444]:
```

For LDAP client port, unless you are running with root privileges you cannot use ports 1 through 1024. So rather than use 389, use 1389.

Use the default 4444 port for Administration Connector.

```
Do you want to create base DNs in the server? (yes / no) [yes]:
Provide the base DN for the directory data: [dc=example,dc=com]:
cd=krypton,dc=com
Options for populating the database:
    1)  Only create the base entry
    2)  Leave the database empty
    3)  Import data from an LDIF file
    4)  Load automatically-generated sample data
Enter choice [1]: 4
```

Do you want to create base DNs in the server, select yes if you have a real DNS or use host entries on the server and client.

```
Enter choice [1]: 4
Please specify the number of user entries to generate: [2000]: 20
```

Generate some sample data if you are learning. Otherwise hit enter to default to "1) Only create the base entry".

```
Do you want to enable SSL? (yes / no) [no]:
Do you want to enable Start TLS? (yes / no) [no]:
Do you want to start the server when the configuration is completed? (yes /
no) [yes]: no
```

I select no to start the server because I like to we can run the status command even if the server is off and verify the configuration.

```
Setup Summary
=============
LDAP Listener Port:            1389
Administration Connector Port: 4444
LDAP Secure Access:            disabled
Root User DN:                  cn=Directory Manager
Directory Data:                Create New Base DN cd=krypton,dc=com.
Base DN Data: Import Automatically-Generated Data (20 Entries)
Do not start Server when the configuration is completed


What would you like to do?
    1)  Set up the server with the parameters above
    2)  Provide the setup parameters again
    3)  Print equivalent non-interactive command-line
    4)  Cancel and exit
Enter choice [1]: 3
Equivalent non-interactive command-line to setup server:
/opt/opendj/setup \
          --cli \
          --baseDN cd=krypton,dc=com \
          --sampleData 20 \
          --ldapPort 1389 \
          --adminConnectorPort 4444 \
          --rootUserDN cn=Directory\ Manager \
          --rootUserPassword ****** \
          --doNotStart \
          --no-prompt \
          --noPropertiesFile
```

Since we will be setting up a secondary system for replication export and save the options for later. Note it looks like a bug as the hostname parameter (ldap1.krypton.com) is not outputted here.

```
What would you like to do?
    1)  Set up the server with the parameters above
    2)  Provide the setup parameters again
    3)  Print equivalent non-interactive command-line
    4)  Cancel and exit
Enter choice [1]:

See /tmp/opendj-setup-8737651315284839293.log for a detailed log of this
operation.


Configuring Directory Server ..... Done.
Importing Automatically-Generated Data (20 Entries) ..................
Done.


To see basic server configuration status and configuration you can launch
/opt/opendj/bin/status
```

All should go well.

Verify Configuration with Server Status

You can verify things are good before starting,

```
cd /opt/opendj/bin
 ./status
./status
          --- Server Status ---
Server Run Status:        Stopped
Open Connections:         <not available> (*)
          --- Server Details ---
Host Name:                ldap1
Administrative Users:     cn=Directory Manager
Installation Path:        /opt/opendj
Version:                  OpenDJ 2.6.0
Java Version:             <not available> (*)
Administration Connector: Port 4444 (LDAPS)
          --- Connection Handlers ---
Address:Port : Protocol : State
-------------:----------:---------
--           : LDIF     : Disabled
0.0.0.0:161  : SNMP     : Disabled
0.0.0.0:636  : LDAPS    : Disabled
0.0.0.0:1389 : LDAP     : Enabled
0.0.0.0:1689 : JMX      : Disabled
0.0.0.0:8080 : HTTP     : Disabled
          --- Data Sources ---
Base DN:     cd=krypton,dc=com
Backend ID:  userRoot
Entries:     <not available> (*)
Replication:
* Information only available if server is running and you provide valid
authentication information when launching the status command.
```

OpenDJ follows most Unix convention and everything is self contained in the one directory.

Start and Stop

As a reference,

```
cd /opt/opendj/bin
./start-ds

cd /opt/opendj/bin
./stop-ds

# I think this is verbose mode but not finding docs on it
./start-ds -s
```

Start the server,

```
cd /opt/opendj/bin
./start-ds
[13/Jul/2015:00:08:30 -0400] category=EXTENSIONS severity=NOTICE
msgID=1507899 msg=Loaded extension from file
'/opt/opendj/lib/extensions/snmp-mib2605.jar' (build 2.6.0, revision 9086)
[13/Jul/2015:00:08:31 -0400] category=CORE severity=NOTICE msgID=458886
msg=OpenDJ 2.6.0 (build 20130626200626Z, R9086) starting up
[13/Jul/2015:00:08:38 -0400] category=RUNTIME_INFORMATION severity=NOTICE
msgID=20381717 msg=Installation Directory:  /opt/opendj
[13/Jul/2015:00:08:38 -0400] category=RUNTIME_INFORMATION severity=NOTICE
msgID=20381719 msg=Instance Directory:      /opt/opendj
[13/Jul/2015:00:08:38 -0400] category=RUNTIME_INFORMATION severity=NOTICE
msgID=20381713 msg=JVM Information: 1.7.0_79-b15 by Oracle Corporation,
64-bit architecture, 496697344 bytes heap size
[13/Jul/2015:00:08:38 -0400] category=RUNTIME_INFORMATION severity=NOTICE
msgID=20381714 msg=JVM Host: ldap1, running Linux 3.13.0-57-generic amd64,
2048925696 bytes physical memory size, number of processors available 1
[13/Jul/2015:00:08:38 -0400] category=RUNTIME_INFORMATION severity=NOTICE
msgID=20381715 msg=JVM Arguments: "-Dorg.opends.server.scriptName=start-ds"
[13/Jul/2015:00:08:40 -0400] category=JEB severity=NOTICE msgID=8847402
msg=The database backend userRoot containing 22 entries has started
[13/Jul/2015:00:08:42 -0400] category=EXTENSIONS severity=NOTICE
msgID=1507549 msg=DIGEST-MD5 SASL mechanism using a server fully qualified
domain name of: ldap1.krpton.com
[13/Jul/2015:00:08:43 -0400] category=PROTOCOL severity=NOTICE
msgID=2556180 msg=Started listening for new connections on Administration
Connector 0.0.0.0 port 4444
[13/Jul/2015:00:08:43 -0400] category=PROTOCOL severity=NOTICE
msgID=2556180 msg=Started listening for new connections on LDAP Connection
Handler 0.0.0.0 port 1389
[13/Jul/2015:00:08:43 -0400] category=CORE severity=NOTICE msgID=458887
msg=The Directory Server has started successfully
[13/Jul/2015:00:08:43 -0400] category=CORE severity=NOTICE msgID=458891
msg=The Directory Server has sent an alert notification generated by class
org.opends.server.core.DirectoryServer (alert type
org.opends.server.DirectoryServerStarted, alert ID 458887):  The Directory
Server has started successfully
```

(Talk about next steps and links here...).

References

Not bad but not good manual setup - http://opendj.forgerock.org/docs.html

https://bugster.forgerock.org/jira/browse/OPENDJ-330

Install Guide - http://opendj.forgerock.org/opendj-server/doc/bootstrap/install-guide/

Replication - http://ludopoitou.com/2011/05/10/opendj-quick-replication-setup/

replication -