Chapter 3
Config of LDAP

1. Explore current auth environment

a. connect to system

b. less /etc/nsswitch.conf (this file will be updated to use LDAP)

2. Setup LDAP Environment

a. Install 'openldap2*' RPMs

b. Requires 'db42' RPM - Berkeley DB

Note: Use package manager (yum) to auto-resolve dependencies

c. Explore 'openldap2*' RPMs - rpm -qa | grep -i ldap

d. rpm -ql openldap2

- /etc/init.d/ldap - run-script (start|stop|restart|reload) - LDAP server
- /etc/init.d/slurpd - run-script for the replication daemon
- /etc/openldap/schema - top-level schema container
- /etc/openldap/slapd.conf - LDAP server config. file
- /usr/sbin/slap* - offline admin commands
- /var/lib/ldap - DB container

e. rpm -ql openldap2-client - contains client utilities(Online)

- /etc/openldap/ldap.conf - primary config file for LDAP online clients
- /usr/bin/ldap* - key LDAP online clients

###Key Online Management Utilities###

- /usr/bin/ldapadd - used to add objects to DIT
- /usr/bin/ldapcompare - used to compare
- /usr/bin/ldapdelete - used to delete
- /usr/bin/ldapexop - export
- /usr/bin/ldapmodify - modify|add|delete
- /usr/bin/ldapmodrdn - modifies relative DN

- /usr/bin/ldappasswd - changes one's password
- /usr/bin/ldapsearch - used to search the Directory Information Tree (DIT)
- /usr/bin/ldapwhoami - used to return the current user

f. Explore and configure /etc/openldap/* environment

g. Update /etc/openldap/slapd.conf

Update: suffix "dc=my-domain,dc=com"

TO: suffix "dc=raja,dc=internal"

###Super-User Info###

#rootdn "cn=Manager,dc=my-domain,dc=com"

rootdn "cn=Manager,dc=raja,dc=internal"

#rootpw secret

rootpw abc123

lappasswd

New password:

Re-enter new password:

{SSHA}XtKwb5TGK0YIaHTaHxN8yAITiQTXPQwx

Note: 'Manager' from "cn=Manager,dc=raja,dc=internal" is case-insensitive

h. Ensure that PAM and NSS support is installed

Use 'yum' to install the 2 packages

Execution:

rpm -qa| grep pam_ldap

pam_ldap-185-11.el6.i686

if not response ----> echo $?

rpm -qa| grep nss

nss-util-3.16.2.3-2.el6_6.i686

nss-sysinit-3.16.2.3-3.el6_6.i686

nss-softokn-freebl-devel-3.14.3-18.el6_6.i686

globus-openssl-module-4.6-1.el6.i686

nss-tools-3.16.2.3-3.el6_6.i686

openssh-askpass-5.3p1-104.el6_6.1.i686

nss_db-2.2.3-0.5.pre1.el6_5.1.i686

nss-3.16.2.3-3.el6_6.i686

nss-util-devel-3.16.2.3-2.el6_6.i686

mod_dnssd-0.6-2.el6.i686

nss-softokn-freebl-3.14.3-18.el6_6.i686

nss_compat_ossl-0.9.6-1.el6.i686

nss-devel-3.16.2.3-3.el6_6.i686

mod_nss-1.0.8-21.el6.i686

nss-devel-3.16.2.3-3.el6_6.i686

mod_nss-1.0.8-21.el6.i686

openssl-1.0.1e-30.el6_6.4.i686

globus-gsi-openssl-error-3.5-1.el6.i686

openssh-5.3p1-104.el6_6.1.i686

nss-pam-ldapd-0.7.5-18.2.el6_4.i686

openssh-clients-5.3p1-84.1.el6.i686

krb5-pkinit-openssl-1.10.3-33.el6.i686

nss-softokn-devel-3.14.3-18.el6_6.i686

python-nss-0.13-1.el6.i686

openssh-server-5.3p1-84.1.el6.i686

openssl098e-0.9.8e-18.el6_5.2.i686

nss-softokn-3.14.3-18.el6_6.i686

openssl-devel-1.0.1e-30.el6_6.4.i686

nss-mdns-0.10-8.el6.i686

rpm -ql nss_ldap

package nss_ldap is not installed

root@linuxcent Desktop]# yum install nss-pam-ldapd.i686

rpm -qa | grep nss-pam-ldapd

nss-pam-ldapd-0.7.5-18.2.el6_4.i686

rpm -qa| grep nss | grep ldap

nss_ldap-253-52.el5_11.2

nss_ldap-253-37.el5

i. Ensure that LDAP clients are properly configured

j. Start LDAP server - /sbin/service ldap start

Execution:

ps -ef | grep ldap

ldap 17487 1 0 01:45 ? 00:00:00 /usr/sbin/slapd -h ldap:/// -u ldap

vim /etc/openldap/slapd.conf

pidfile /var/run/openldap/slapd.pid

argsfile /var/run/openldap/slapd.args

[root@linuxcent ldap]# cat /var/run/openldap/slapd.pid

17487

[root@linuxcent ldap]# cat /var/run/openldap/slapd.args

/usr/sbin/slapd -h ldap:/// -u ldap

netstat -ntlp | grep 389

tcp 0 0 0.0.0.0:389 0.0.0.0:*
LISTEN 17487/slapd

tcp 0 0 :::389

###Search the DIT###

Two ways to search:

1. 'ldapsearch' - included with openldap2-client* RPM
2. LDAP Browser GUI

###LDAPSEARCH###

ldapsearch -x -b "dc=raja,dc=internal" "(objectclass=*)" - performs anonymous search for any object in the DIT

- -x --bypass encrypted authentication
- -b --base dn
- "dc=raja,dc=internal" --base suffix
- "(objectclass=*)" --generic search

###LDAP BROWSER###

YaST -> Network Services -> LDAP Browser in SUSE

http://jxplorer.org/downloads/users.html

https://www.netiq.com/communities/cool-solutions/cool_tools/gawors-excellent-ldap-browsereditor-v282/

Authenticate using: rootDN (Administrator DN)