in DNS:

--------

FL -- hostname => IP

RL -- IP => hostname

In general a host is addressed with domain:

-------------------------------------------

for example server11.veecube.com

server11 => host\_name

veecube.com => domain\_name

LDAP:

-----

Lightweight directory access protocol

example for a directory : Telephone directory

what is the difference between RDBMS and LDAP\_DB:

-------------------------------------------------

For example in banking sector (oracle, sql or any RDBMS) :

1) transcaction are stored in DB

2) Storing is a write operation

3) Writing is slower than reading

LDAP DB is optimized for read operation:

----------------------------------------

1) Used mainly for Authentication purposes

expressing a DNS entry in LDAP Format:

--------------------------------------

cn=common\_name (unique\_name, leaf\_object)

dc=domain\_component (for example the domain names in DNS)

so the former example server11.veecube.com can be expressed:

cn=server11,ou=hosts,dc=veecube,dc=com

another example:

----------------

phosur@veecube.com

cn=phosur,ou=people,dc=veecube,dc=com

where ou is organisational unit, it is a branch/dept

RPM has Openldap packages:

--------------------------

for server side:

openldap-servers

openldap-clients

nss-pam-ldapd

ldap fuctions on the port:389

where ldaps has the port:636

for client side:

openldap-clients

nss-pam-ldapd

configuration directory:

------------------------

/etc/openldap

DB directory:

-------------

/var/lib/ldap

server service/daemon name:

---------------------------

slapd

client service:

---------------

nscd/nslcd

or

sssd

main configuration file for the server side:

--------------------------------------------

/etc/openldap/slapd.conf

db directory: /var/lib/ldap

###create slappasswd

###copy the encrypted passwd

vi /etc/slapd.conf

###make all the schemas available

allow bind\_v2 ### to allow ldap version 2 also

#referral ldap://root.openldap.org ### means if any other server is in sync

with this openldap, can be referred here

pidfile /var/run/openldap/slapd.pid ###has the running process id

argsfile /var/run/openldap/slapd.args ###has the cli arg of slapd

modulepath /usr/lib64/openldap ###as the machine is 64 bit the lib are in 64 bit path

#moduleload to load the required modules

TLSCA --- used only for ldaps

###don't change database config

###don't change database monitor

database bdb ### berckely db

##change the suffix and rootdn

### paste the slappasswd in front of

root pw {SSHA}dVeRF0L5JBa+SjAxyLz5jJ4WUqXoEHg1

directory /var/lib/ldap ### default directory for DB

default conf clearence:

------------------------

rm -rf /etc/openldap/slapd.d/\*

rm -rf /var/lib/ldap/\*

cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

generate new conf from slapd.conf:

----------------------------------

slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d

change permission & ownership:

------------------------------

chmod -R 750 /etc/openldap/slapd.d

chmod -R 700 /var/lib/ldap

chown -R ldap. /etc/openldap/slapd.d

chown -R ldap. /var/lib/ldap

systemctl start slapd

==================================================================

client side configuration:

--------------------------

yum install openldap-clients nss-pam-ldapd authconfig

authconfig-tui

####please clear the \* on life side

#### enable the \* for ldap authentication on the right side

#### then next

ldap://192.168.1.116:3890

dc=veecube00,dc=com

####then next

vi /etc/nsswitch.conf

passwd files ldap

shadow files ldap

group files ldap

netgroup files ldap

###save & exit

authconfig --enablemkhomedir --updateall

verify:

-------

getent passwd

su - phosur

(automatically create homedir for the fist login)

pwd

whoami

Migration tools:

----------------

yum install migrationtools

cd /usr/share/migrationtools/

###change the domain name in migrate\_common.ph

sed -i 's/padl/veecube/g' migrate\_common.ph

##migrating base:

-----------------

./migrate\_base.pl >>/tmp/base.ldif

ldapadd -x -h 192.168.1.126 -D "cn=Manager,dc=veecube,dc=com" -W -f /tmp/base.ldif

-x without certificates

-h host

-D "to specify who am i"

-f file

-W passwd auth

adding a group:

---------------

groupadd ldapuser

adding users:

-------------

usermod -g ldapuser ldapuser1

useradd -g ldapuser ldapuser2

passwd ldapuser1

passwd ldapuser2

filtering the group entry:

--------------------------

grep ldapuser: /etc/group >/tmp/grp

filtering the user entry:

-------------------------

grep ldapuser1: /etc/passwd >/tmp/usr

migrating group entry to ldif:

------------------------------

./migrate\_group.pl /tmp/grp >>/tmp/grp.ldif

migrating user entries to ldif:

-------------------------------

./migrate\_passwd.pl /tmp/usr >>/tmp/usr.ldif

Import the ldif:

----------------

ldapadd -x -h 192.168.1.126 -D "cn=Manager,dc=veecube,dc=com" -W -f /tmp/grp.ldif

ldapadd -x -h 192.168.1.126 -D "cn=Manager,dc=veecube,dc=com" -W -f /tmp/usr.ldif

ACL access control list:

------------------------