

LDAP Authentication

README FIRST

Instructions are for CentOS 5, Redhat 5, Redhat 4 only. If your operating system is not listed then STOP and proceed to the TESTING section at the end of this document.

1. Login to server and sudo su –
2. Run the Authconfig program with the following parameters based on your OS:

CentOS 5

```
authconfig --enableldap --enableldapauth --ldapserver=192.168.1.12 --  
ldapbasedn=dc=servers,dc=anx,dc=net --enablecache --enablelocauthorize  
-- enablemkhomedir --update
```

Redhat 5

```
authconfig --enableldap --enableldapauth --ldapserver=192.168.1.12 --  
ldapbasedn=dc=servers,dc=anx,dc=net --enablecache --enablelocauthorize  
-- enablemkhomedir --update
```

Edit /etc/ldap.conf

Locate the line below and comment it out:

```
nss_initgroups_ignoreusers root,ldap,named,avahi,haldaemon
```

Add the following line below:

```
nss_initgroups_ignoreusers  
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mail  
man,nscd,gdm
```

Redhat 4

```
authconfig --enableldap --enableldapauth --ldapserver=192.168.1.12 --  
ldapbasedn=dc=servers,dc=anx,dc=net --enablecache
```

3. Edit the `/etc/pam.d/sshd` config file, and add the following line to the end of the file

Redhat 5 or CentOS 5

```
account required pam_succeed_if.so user ingroup testgroup
```

Redhat 4

```
account required pam_succeed_if.so user ingroup testgroup
```

```
sessionrequired pam_mkhome.so skel=/etc/skel/ umask=0022
```

Each user will need to be in the LDAP group “testgroup” to be able to login to a server configured this way.

4. Configure LDAP for soft bind policy:

- a. Edit `/etc/ldap.conf`
- b. Locate “bind_policy” parameter.
- c. Change to “bind_policy soft”.

5. Setup completed. Users in the LDAP group testgroup are now able to log in to the server.

6. Open a second ssh window and verify LDAP authorization before logging off the first window.

TESTING

If your Operating system is different then the ones listed at the beginning of the document then you will want to test the above configuration and update this document for future use.

- 1) Configure using the instructions listed above.
- 2) You will need one user configured locally (referenced as local user)
- 3) You will need one user configured in LDAP that is in the "TESTGROUP" LDAP Group. (referenced as LDAP user)
- 4) Verify that the LDAP user can login to the system. If it is a new user verify that the home directories are created.
- 5) Verify that the LOCAL user can also log in to the system.
- 6) We will now disable LDAP to simulate a LDAP outage by changing the LDAP IP address in the `/etc/ldap.conf` to an IP that is unreachable.
 - a. Edit `/etc/ldap.conf` and change the LDAP server IP to an IP that is unused and reboot the test system.
 - b. Verify that the system boots in a normal time frame (5-10 min normally)
 - c. Verify the LDAP user cannot login.
 - d. Verify the LOCAL user can login.
- 7) Testing is completed.