6.Manage users and groups

1. **Create, delete, and modify local user accounts**

To create a local user account (here **user**), type:

# useradd **user**

Note: a group with the same name is automatically created.

To create a local user account (here **user**) with given **UID** and **GID**, type:

# useradd -u UID -g GID **user**

To create a local user account (here **user**) with a secondary group (here **team**), type:

# useradd -G **team user**

To create a local user account (here **user**) without login access (useful for Samba configuration), type:

# useradd -s /sbin/nologin **user**

To delete a local user account (here **user**) with removal of the user’s home directory and the user’s mail spool (-r), type:

# userdel -r **user**

Note: the associated group is automatically removed.

To change the name of a user account (here from **user** to **usr**), type:

# usermod -l **usr** **user**

1. **Change passwords and adjust password aging for local user accounts**

To assign a password to a user account (here **user**), type:

# passwd **user**

To set an expiration date to a local user account (here **user**), type:

# chage -E YYYY-MM-DD **user**

“chage -d 0 username” requires the user to change his password immediately after logon, which is a quite a nice feature.

To check the result, type:

# chage -l **user**

1. **Create, delete, and modify local groups and group memberships**

To create a group without any associated user (here **grp**), type:

# groupadd **grp**

To create a group without any associated user (here**grp**) with a given **GID**, type:

# groupadd -g GID **grp**

To change the name of a group (here from **grp** to **gr**), type:

# groupmod -n gr **grp**

To remove a group without any associated user (here **grp**), type:

# groupdel **grp**

To change the **GID** of a group (here **grp**), type:

# groupmod -g GID **grp**

To add a secondary group (here **grp**) to a user account (here **user**), type:

# usermod -aG **grp user**

**or:**

# gpasswd -a **user grp**

To remove a user (here **user**) from a secondary group (here **grp**), type:

# gpasswd -d **user grp**

Note: This doesn’t work on the primary group.

To get the list of the members of a given group (here **mail**), type:

# **groupmems -g mail -l**

postfix

1. **Configure a system to use an existing authentication service for user and group information**

## **LDAP Server Configuration**

In order to test a **LDAP** client configuration, you will need to [configure a LDAP directory service](https://www.certdepot.net/rhel7-configure-ldap-directory-service-user-connection/).  
The **LDAP** server is called **instructor.example.com** in this procedure.

## **LDAP Client Configuration**

As the **authconfig-tui** is deprecated, to configure the **LDAP** client side, there are two available options: **nslcd** and **sssd**.  
In this tutorial, the **nslcd** option will be used, see the [authconfig tutorial](https://www.certdepot.net/ldap-client-configuration-authconfig/) for the **sssd** option.

Install the following packages:

# **yum install -y openldap-clients nss-pam-ldapd**

Note: Just to mention that **Sander van Vugt** advises to install the **Directory Client** group package: **# yum group install “Directory Client”**

Then, type:

# **authconfig --enableforcelegacy --update**

# **authconfig --enableldap --enableldapauth --ldapserver="instructor.example.com" \**

**--ldapbasedn="dc=example,dc=com" --update**

Note1: According to your requirements, you can need to specify the **–enablemkhomedir** option after the installation of the **oddjob-mkhomedir** package. The option creates a local user home directory at the first connection if none exists.  
Note2: Type **# authconfig –help | grep ldap** to remember the necessary options.

Put the **LDAP** server certificate into the **/etc/openldap/cacerts** directory:

# **scp root@instructor.example.com:/etc/openldap/certs/cert.pem \**

**/etc/openldap/cacerts/cert.pem**

Apply the correct **SELinux** context to the certificate:

# **restorecon /etc/openldap/cacerts/cert.pem**

Activate the **TLS** option:

# **authconfig --enableldaptls --update**

Test the configuration:

# **getent passwd ldapuser02**

ldapuser02:\*:1001:1001:ldapuser02:/home/guests/ldapuser02:/bin/bash

## **NFS Server Configuration**

To get the home directory mounted, you need to [configure a NFS server](https://www.certdepot.net/rhel7-provide-nfs-network-shares-specific-clients/).  
The **NFS** server is called **instructor.example.com** in the procedure.  
Note: It’s not required to have the **LDAP** server and the **NFS** server on the same machine, it’s only easier.

## **Automounter Client Configuration**

Install the following packages:

# **yum install -y autofs nfs-utils**

Create a new indirect **/etc/auto.guests** map and paste the following line:

**\* -rw,nfs4 instructor.example.com:/home/guests/&**

Add the following line at the beginning of the **/etc/auto.master** file:

**/home/guests /etc/auto.guests**

Start the **Automounter** daemon and enable it at boot:

# **systemctl enable autofs && systemctl start autofs**

Test the configuration:

# **su - ldapuser02**

## **Additional Resources**

**Ralph Nyberg** offers an interesting video about [configuring LDAP authentication (20min/2015)](https://www.youtube.com/watch?v=uqd51i8X3Yk).  
The [ForumSystems website](https://www.forumsys.com/) provides a free [online LDAP test server](https://www.forumsys.com/en/tutorials/integration-how-to/ldap/online-ldap-test-server/).