Managing Users & Groups

- Create, delete, and modify local user accounts
- Change passwords and adjust password aging for local user accounts
- Create, delete, and modify local groups and group memberships
- Configure superuser access

Introducing Default User Settings

When we create user without specifying or using any options with useradd command default user settings are applied to user account.

Default user settings are applied from below two files:

- /etc/default/useradd - Default values for user account creation
- /etc/login.defs - Defaults about shadow-utils components ,password aging controls, UIDs ,GIDs etc.

User account default values from /etc/default/useradd file

Variable/parameter	Description	Remarks(if any)
GROUP=100	Default primary group (users)	Applicable when '**USERGROUPS_ENAB** no' in **login.defs**
HOME=/home	Default base directory for user's home directory	**Applicable** when **'CREATE_HOME** yes' in **login.defs**
INACTIVE=-1	Account is not disabled after password expiry	
EXPIRE=	User account never expires	
SHELL=/bin/bash	Default shell for user	
SKEL=/etc/skel	Default skeleton directory	
CREATE_MAIL_SPOOL=yes	Create mail spool for user	Location of mail spool depends on setting in **login.defs** (MAIL_DIR or MAIL_FILE variable)

User account default values from /etc/login.defs file

Variable/parameter	Description	Remarks (if any)
MAIL_DIR /var/spool/mail	Default path where user's mail spool file is created	Depends on **CREATE_MAIL_SPOOL** variable in **useradd** file
UMASK 022	Used by **useradd** command to set mode on user's home directory when **HOME_MODE** variable is not set	
HOME_MODE 0700	Used by **useradd** command to set mode on user's home directory	
PASS_MAX_DAYS 99999	Maximum number of days password remains valid	
PASS_MIN_DAYS 0	Minimum password validity period	
PASS_WARN_AGE 7	Number of days warning given about password expiry day	
UID_MIN 1000 , **UID_MAX** 60000	Minimum and maximum value of automatic **uid** assignment	
GID_MIN 1000 , **GID_MAX** 60000	Minimum and maximum value of automatic **gid** assignment	
CREATE_HOME yes	By default, user's home directory is created	**HOME** variable in **useradd** file defines base directory for home directory
USERGROUPS_ENAB yes	Primary group with same name and **gid** is created as that of username and **uid**	If this is set to no, user is assigned group as per GROUP variable in **useradd** file
ENCRYPT_METHOD SHA512	Algorithm used to encrypt passwords	

Verifying Default User Settings

To understand default behavior, we will create test user (username : test ,password :password) with default user settings.

Then we will verify default user settings three files /etc/passwd ,/etc/shadow and /etc/group :

/etc/passwd - User account information

Field	1	2	3	4	5	6	7
Value	USERNAME :	X :	UID :	GID :	COMMENT:	HOME_DIR :	LOGIN_SHELL

/etc/shadow - Secure user account information , Information about password aging and account controls.

Field	1	2	3	4	5	6	7	8	9
Value	USERNAME :	ENCRYPT_PASS :	LAST_PASS_CHANGE :	PASS_MIN_DAYS(**0**) :	PASS_MAX_DAYS(**99999**) :	PASS_WARN_AGE(**7**):	INACTIVE(**-1**):	EXPIRE(**empty**) :	FOR_FUTURE_USE

/etc/group - Group account information

Field	1	2	3	4
Value	GROUP_NAME :	X :	GID :	USERS

Overriding Default User Settings

To override default user settings, we will use useradd, passwd and chage with different options.

Command	Action/Description
useradd	To create user account
passwd	To set **password** for user account
chage	To display/configure password aging and account controls
man useradd	To check manual page for **useradd**
man passwd	To check manual page for **passwd**
man chage	To check manual page for **chage**

- Configure System(system.example.com) to use UID_MIN and GID_MIN as 5000 by default.
  - Create one test user (username :test1) and verify that default selected UID is 5000=+.
  - Make user account password less.

Command	Action/Description
vim /etc/login.defs UID_MIN 5000 GID_MIN 5000 :wq	Configure **System** to use Minimum UserID and GroupID as 5000
useradd test1	Create **test1** user with default settings
more /etc/passwd | grep test1	Verify default **UID** assigned is 5000=+
passwd -u -f test1	To make user account password less
su - test1	Try user login as non-root(regular) user, user should be able to login without password

➢ Modify default password inactivity period (INACTIVE variable to 5) on System.

Command	Action/Description
useradd -D	To display **useradd** defaults
useradd -D -f 5	To modify default password inactivity period **(INACTIVE=5)** to 5
useradd -D	To verify results

- Create a user with username lisa with password access.
  - Use UID 6000 for this user.
  - User should have non-interactive shell

Command	Action/Description
useradd -u 6000 -s /sbin/nologin lisa	To create user with **UID 6000** and **non-interactive** login shell
passwd lisa	To set the password for user **lisa**
more /etc/passwd | grep lisa	To verify user account information
more /etc/group | grep lisa	To verify Group information

- Create a user with username riya with home directory /riya/private and set password access.
  - At first login, she should be forced to change her password.
  - Password should be set to expire every 30 days.

Command	**Action/Description**
useradd -d /riya/private riya	To create user with non-default home directory **/riya/private**
passwd riya	To set the password for user **riya**
chage riya	To set the maximum password age and password change after first login
more /etc/passwd	To verifying user account information
more /etc/shadow	To verify configured password aging controls, account controls etc
more /etc/group	To verify group(s) related information

- Create a group named redhat and assign this group to user lisa as secondary group.
  - GID 5555 should be used.

Command	Action/Description
groupadd -g 5555 redhat	To Create group **redhat** with **GID 5555**
usermod -aG redhat lisa	To assign **redhat** group to user **lisa** as supplementary group
more /etc/group	To verify group related information

- Create user with username harry and set password as access.
  - Account should expire on 31st Dec current year (2023).
  - Password should expire every 70 days.
  -Set password expiry warning to 4 days.

Command	Action/Description
useradd harry	To create user with username, **harry** with default settings
passwd harry	To set the password for user **harry**
chage harry	To set the **maximum password age** ,**password expiry warning** and **account expiration** date
passwd -S harry	To check password status information
more /etc/shadow | grep harry	Verifying configured password aging controls and account controls

- Create the directory /dir and set the group and user ownership to redhat and lisa respectively.
  - Give read only access to group redhat and rwx access to lisa. ..

Command	**Action/Description**
mkdir /dir	To create directory **/dir**
chown lisa:redhat /dir	To set user and group ownership
ls -ld /dir	To verify permissions

- Configure System (system.example.com) as IPA client to use LDAP services configured on IPA Server with Free IPA Server solution.
  - Use user admin and password password to enroll System.
  - ldap users should be able to login on System.

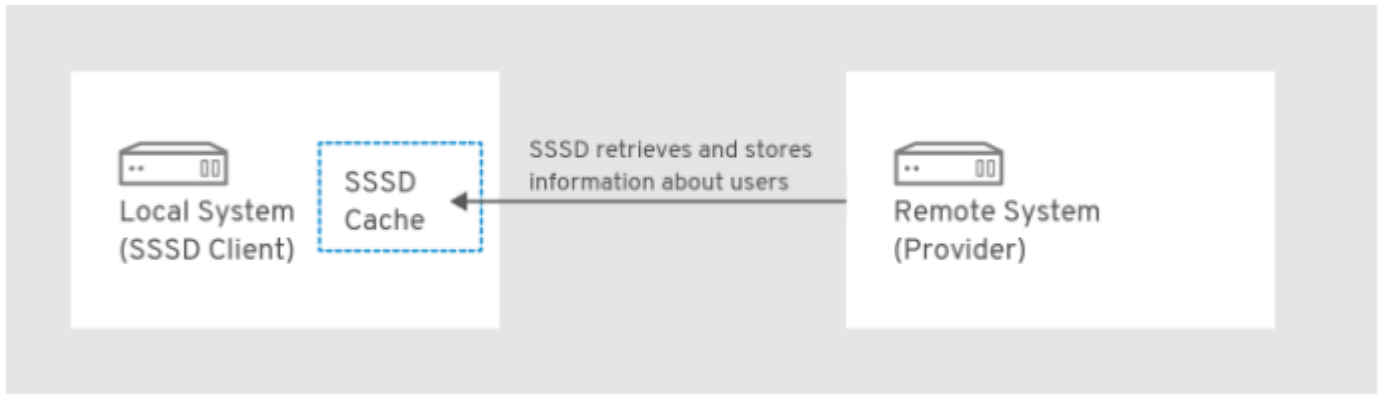
Command	**Action/Description**
dnf install ipa-client	To install package for ipa client
ipa-client-install	Configuring System as **IPA Client**
su - ldap	Verify **ldap** user login

How SSSD works ?

The System Security Services Daemon (SSSD) is a system service that allows you to access remote directories and authentication mechanisms. You can connect a local system, an SSSD client, to an external back-end system, a provider which in our case is IPA Server which uses LDAP directory for directory service.

- It connects the client to a remote provider to retrieve identity and authentication information.
- It uses the obtained authentication information to create a local cache (**var/lib/sss/db**) of users and credentials on the client.

Users on the local system are then able to authenticate using the user accounts stored in the remote provider. SSSD does not create user accounts on the local system.



autofs - Mounting file systems on demand

autofs service is used to mount the filesystems on demand which means filesystem gets mounted automatically when it is accessed and unmounted when it is not used.

When we mount filesystem through fstab file, it remains mounted no matter if filesystem is accessed or not and system has to allocate dedicated resources to keep the mounted system in place. So, this is not good practice specially for infrequently accessed filesystems because it can cause performance issues when there are multiple such filesystems.

autofs can mount NFS,SMB,CIFS and local filesystems. We will use **autofs** to mount LDAP user's home directories which are exported as NFS filesystems on IPA Server.

autofs configuration files :

1. **The master map file (/etc/auto.master)** : This is the primary default configuration file used by **autofs** and contains mount points controlled by **autofs** . There are two types of mounts (maps) :

   Indirect mount : Base path is specified in master map and key (relative path) in map-file
   Direct mount : Full path is specified in map-file .Master map contains **/-** .

   Example entry for Indirect map in **auto.master** file :

Base path	map-file	options
/home/ldapuser	/etc/auto.ldap	-rw

2. **Map-file** : Map-files configures properties of individual mount points.
   Example entry for Indirect map in **map file** :

key	options	location
ldap	-fstype=nfs4	ipaserver.example.com:/home/ldapuser/ldap

- Configure system.example.com to automount home directory of LDAP user ldap when logged in.
  - Home directory of LDAP user is /home/ldapuser/ldap.
  - Home directory is exported by ipaserver.example.com as NFS export .
  - LDAP user should get his home directory when logged in.

Command	**Action/Description**
dnf install autofs	To install packages required for **autofs**
systemctl start autofs	To start **autofs** service
systemctl enable autofs	Configuring to start service at boot
vim /etc/auto.master /home/ldapuser /etc/auto.ldap :wq	To define master automounter map
vim /etc/auto.ldap ldap ipaserver.example.com:/home/ldapuser/ldap :wq	
systemctl restart autofs	Restart **autofs** service
su - ldap	Switch user to **ldap**
pwd	Current directory should be ldap user's home directory

- Configure system.example.com to automount home directories of LDAP users ldap1 and ldap2.
  - Home directories of LDAP users ldap1 and ldap2 are /ldap/home/ldap1 and /ldap/home/ldap2 respectively.
  - Home directories are shared by ipaserver.example.com through NFS export.
  - LDAP user should get his home directory when logged in.

Command	**Action/Description**
dnf install autofs	Installing **autofs**
systemctl start autofs	Starting **autofs** service
systemctl enable autofs	Configuring **autofs** to start at boot
vim /etc/auto.master /ldap/home /etc/auto.ldap12 :wq	To define base location for home directory
vim /etc/auto.ldap12 * ipaserver.example.com:/ldap/home/& :wq	
systemctl restart autofs	Restarting **autofs** service
su - ldap1	Switch user to **ldap1**
pwd	Current directory should be home directory of **/ldap/home/ldap1**

- Create user (username)maria on System with default user settings.
  - Delete user maria from system.example.com.
  - User's home directory and mailbox should also be deleted

Command	Action/Description
useradd maria	To create user **maria** with default user settings
userdel -r maria	To delete user **maria** ,also home directory and mail spool
userdel --help	To check help for **userdel**

➢ Configure superuser access for user (username) harry to enable him to use root privileges with sudo.
- Create a user with username testuser using sudo.

Command	**Action/Description**
more /etc/sudoers	To verify line "**%wheel ALL=(ALL) ALL"** is not commented
usermod -aG wheel harry	To add user, **harry** to wheel group
sudo whoami	To verify access
sudo useradd testuser	To create user using **sudo**