LINUX FOUNDATION

TRAINING

Managing User Accounts

A Linux Foundation Training Publication
www.training.linuxfoundation.org

Overview

Each user of a Linux system has an account, with various attributes that identify the user, allow a user to be a member of a group, have a password, set a specific shell on login, and grant ownership or execution permissions to run programs or edit files. Therefore, it is important to be familiar with managing users on a Linux system.

Key Ideas

useradd: the tool that is present on most Linux systems, which allows a privileged user to create new users and set various attributes for the new user

usermod: utility to modify existing user accounts

userdel: a utility to delete a user from a Linux system

passwd: a tool to set a password, lock an account, expire a password

chage: utility to change user password expiry information in /etc/shadow

/etc/passwd: file that contains user account information

/etc/shadow: file that contains encrypted user passwords

/etc/group: file that contains the group information for a user

Example Scenario

Create a new user with a corresponding named group as their primary group ID. Make some changes to the user, like setting a shell to use on login, change or set their password, alter their home directory, create an expiry date for their account, lock their account, and then delete the user.

Now Do It

1. Create a user ‘testuser’, making sure that their primary group has the same name as the user.
2. Add ‘testuser’ to the ‘adm’ group
3. Examine the /etc/group file and look at the ‘adm’ group to see that testuser is present
4. Examine /etc/shadow and look at the information for the testuser account
5. Set a password for the user

6. Reexamine /etc/shadow and notice the encrypted password for the testuser account
7. Change the testuser's home directory to /tmp/testuser
8. Change the testuser's shell to /bin/sh
9. Add an expiry date to the user's account using the usermod tool
10. Reexamine /etc/shadow and notice the last field, which is the number of days since Jan 1, 1970 until the date that the user's password expires
11. Verify the password expiry date using the chage utility
12. Check the testuser's password status using passwd utility
13. Lock the 'testuser' account
14. Examine the lock status for the testuser account using the passwd utility
15. Delete the testuser account
16. Shutdown the system.

If you remember nothing else...

useradd is the tool that is used to add an account to a Linux system. usermod can be used to change a user's groups or password lock. userdel is used to delete a user.

Answer Key

1. useradd -U testuser

2. usermod -G adm testuser

3. cat /etc/group | grep testuser
   or
   grep testuser /etc/group

4. grep testuser /etc/shadow

5. passwd testuser
   99999 in the fifth field of the output of this command indicates the password never expires.

6. grep testuser /etc/shadow

7. usermod --home /tmp/testuser testuser

8. usermod --shell /bin/sh testuser

9. usermod --expiredate 2030-01-01 testuser

10. passwd -S testuser

11. chage --list testuser

12. passwd -S testuser

13. passwd -l testuser

14. passwd -S testuser

15. userdel testuser

16. sudo shutdown -h now (Ubuntu)
    systemctl poweroff (CentOS / openSUSE)

LINUX FOUNDATION

Get Certified!

Get more information at http://training.linuxfoundation.org/certification/lfcs