Linux server - Manage user and Groups and working with file systems

---

1. **What is default uid for root user ?**
    - the default user ID (UID) for the root user is typically 0.

2. **What is default uid for system user ?**
    - system users typically have low UID values. The specific range of UIDs reserved for system users can vary, but it's common for system users to have UIDs in the range from 0 to 999.

3. **What is the uid for normal users ?**
    - the User IDs (UIDs) for regular or normal users start at 1000 and go upwards. This is a common convention to avoid conflicts with system users, which usually have UIDs in the lower range (e.g., 0-999) as mentioned earlier.

4. **How to add comment in user file?**
    - In Linux, you can add comments to configuration files and scripts using the # symbol.

5. **From " /etc/passwd " which information will we gather ?**
    - Username: The first field is the username, which is used for logging into the system.
    - Password Placeholder: The second field used to contain the password hash, but in modern systems, it is often replaced with an 'x' or '*' character. The actual password hash is stored in the /etc/shadow file for security reasons.
    - User ID (UID): The third field is the user's unique numerical identifier, known as the User ID (UID). It is used by the system to identify users.
    - Group ID (GID): The fourth field is the primary group's numerical identifier, known as the Group ID (GID). It specifies the user's primary group.
    - User Information: The fifth field is a comment or additional information about the user, typically the user's full name and other details.
    - Home Directory: The sixth field specifies the user's home directory, where they will be placed after logging in.
    - Login Shell: The seventh field specifies the user's default shell, which is the command interpreter they will use after logging in.

Linux server - Manage user and Groups and working with file systems

---

6. **From " /etc/shadow " which information will we gather ?**
    - Username: The first field is the username, matching the user from the /etc/passwd file.
    - Password Hash: The second field contains the encrypted password hash for the user. This hash is used to authenticate the user during login.
    - Last Password Change: The third field records the date of the last password change for the user. It is typically represented in days since the Unix epoch (January 1, 1970).
    - Minimum Password Age: The fourth field specifies the minimum number of days a user must keep a password before they can change it.
    - Maximum Password Age: The fifth field indicates the maximum number of days a password is valid before it must be changed.
    - Password Warning Period: The sixth field is the number of days before the password expires when the user is warned about it.
    - Password Inactivity Period: The seventh field is the number of days after the password has expired during which the account remains active. After this period, the account is locked.
    - Account Expiry Date: The eighth field represents the date when the account will be disabled, given in days since the Unix epoch.
    - Reserved Field: The ninth field is typically reserved for future use and is not currently used.
    - Additional Information: The tenth field may contain additional information or comments about the user.

7. **From " /etc/group " which information will we gather ?**
    - Group Name: The first field is the name of the group, which is used to identify the group.
    - Password Placeholder: The second field used to contain the group's password hash, but in modern systems, it is often replaced with an 'x' or '*' character. The actual password hash is stored in the /etc/gshadow file for security reasons.
    - Group ID (GID): The third field is the unique numerical identifier for the group, known as the Group ID (GID). It is used by the system to identify groups.
    - Group Members: The fourth field lists the usernames of users who are members of the group. Multiple usernames are separated by commas.

Linux server - Manage user and Groups and working with file systems

---

8. **From " /etc/gshadow " which information will we gather ?**
    - Group Name: The first field is the name of the group, matching the group name in the /etc/group file.
    - Password Hash: The second field contains the encrypted password hash for the group. This hash is used for security purposes, but it's rarely used for group authentication.
    - Group Administrators: The third field lists the usernames of users who are designated as group administrators. These users have the authority to manage the group, adding or removing members.
    - Group Members: The fourth field specifies the group members. It can include usernames of users who are part of the group.

9. **What is the meaning of + and – in file permission?**
    - "+" (Plus): The plus symbol (+) is used to add or grant permissions to a file or directory. You can specify which permissions you want to add for a specific user or group. For example, you can use +r to add read permission, +w to add write permission, and +x to add execute permission.
    - "-" (Minus): The minus symbol (-) is used to remove or revoke permissions from a file or directory. You can specify which permissions you want to remove for a specific user or group. For example, you can use -r to remove read permission, -w to remove write permission, and -x to remove execute permission.

10. **What is " r " " w " ' x " in file permission?**
    - "r" (Read): The "r" permission allows a user or process to read the contents of a file. For directories, it allows listing the files and subdirectories within the directory.
    - "w" (Write): The "w" permission allows a user or process to modify or write to a file. For directories, it allows creating, deleting, and renaming files and subdirectories within the directory.
    - "x" (Execute): The "x" permission allows a user or process to execute or run a file if it's a program or script. For directories, it allows accessing the contents of the directory, provided the user has permission to access the specific files within.

Linux server - Manage user and Groups and working with file systems

---

11. What is “ 4 “ “ 2 “ “1” in files permission?

- 4 (Read Permission): This digit represents the read permission. When it's present, it's assigned a value of 4. Read permission allows a user to view the contents of a file or list the contents of a directory.
- 2 (Write Permission): This digit represents the write permission and is assigned a value of 2. Write permission allows a user to modify or delete a file (or its contents) or create and delete files in a directory.
- 1 (Execute Permission): This digit represents the execute permission and is assigned a value of 1. Execute permission allows a user to run a program or script or enter a directory.

12.What is the use of umask?

- umask is a command and a concept in Unix-like operating systems that is used to set default file permission bits for newly created files and directories. The term "umask" stands for "user file creation mask," and it acts as a protective mask that specifies which permissions are turned off by default when a new file or directory is created.

13. What is default root permission for directory?

- The default root (superuser) permission for directories in most Unix-like operating systems, including Linux, is typically set to 755 (rwxr-xr-x). This means:
- The owner (root) has read, write, and execute permissions (7).
- The group and others have read and execute permissions (5).

14. How to assign another new home directory for new user?

- Create the New User: You can create a new user using the useradd or adduser command.
- Set the User's Password: Use the passwd command to set a password for the new user:
- Modify User Information (Optional): If you need to add more user information, such as the full name, you can use the usermod .
- Change Home Directory Permissions (If Necessary): If the new home directory is not owned by the new user, you may need to change the.

Linux server - Manage user and Groups and working with file systems

---

15.Command to check group membership of any user

- To check the group membership of any user in a Unix-like operating system, you can use the groups or id command followed by the username of the user you want to check.

16.What happened if I use " su – " command ?

- The su - command is used in Unix-like operating systems, including Linux, to switch to another user account, typically the superuser or root, and acquire that user's environment, including their home directory and settings. The hyphen or dash (-) after su signifies that you want to start a new login session as the specified user.

17.Which command is used to delete any user with its home directory?

- To delete a user along with their home directory in a Unix-like operating system, you can use the userdel command with the -r option.

18. How to add new user without home directory ?

- To add a new user without creating a home directory in a Unix-like operating system, you can use the useradd command with the --no-create-home option.

19.Command to assign account expiry to the user ?

- To assign an account expiry date to a user in a Unix-like operating system, you can use the chage command. The chage command allows you to configure various user account aging and password policy settings, including setting an account expiry date.
- Here's the command to set an account expiry date for a user:
- sudo chage -E YYYY-MM-DD username

20. Command to add a new group …

- sudo groupadd newgroupname

21.What is default root permission for file?

- The default root (superuser) permission for files in most Unix-like operating systems, including Linux, is typically set to 644 (rw-r--r--). This means:
- The owner (root) has read and write permissions (6).
- The group and others have read-only permissions (4).

Linux server - Manage user and Groups and working with file systems

---

22.What is the default umask for root?

- The default umask value for the root user in Unix-like operating systems is typically set to 022. The umask value determines the default permissions assigned to newly created files and directories.

23. Which command is used to set user ownership?

- To set user ownership of a file or directory in a Unix-like operating system, you can use the chown (short for "change owner") command. The chown command allows you to change the owner of a file or directory to a specific user.

24. Which command is used to set group ownership?

- To set the group ownership of a file or directory in a Unix-like operating system, you can use the chown (short for "change owner") command, just like you would for changing the user ownership.

25. I have on user with the name of KAMAL, Now, I want to add this user in the group name Which command will used?

- sudo usermod -aG N KAMAL

26. What is the difference between " usermod -G " and " usermod -aG ".

- The usermod command is used to modify user account properties in Unix-like operating systems, including Linux. Both -G and -aG options are used to manage a user's group membership, but they work differently:
- usermod -G (Change Primary Group):
- When you use usermod -G newgroup username, you are changing the user's primary group to "newgroup."
- This command replaces the user's primary group with the specified group and removes them from their previous primary group. The user will no longer be a member of their previous primary group.
- usermod -aG (Append to Groups):
- When you use usermod -aG newgroup username, you are adding the user to the "newgroup" in addition to their existing group memberships.
- This command appends the user to the specified group, allowing them to be a member of multiple groups simultaneously.

Linux server - Manage user and Groups and working with file systems

---

27. What is the meaning of " -1 " in password state information?

- the password state information field in the /etc/shadow file typically contains a variety of flags and settings that control user password attributes and policies. The -1 value in this field typically indicates that the password is disabled, effectively preventing the user from logging in with a password.

28. Which command is used to remove the password of any user?

- sudo passwd -d username

29. What is the use of " gpasswd " ?

- The gpasswd command is used in Unix-like operating systems to manage group passwords and group membership. It allows system administrators and group owners to set and change the password for a particular group.

30. Command to change password policy.

- The command to change password policies in a Unix-like operating system largely depends on the specific system and the password policy framework in use. Commonly, you'll configure password policies through the Pluggable Authentication Module (PAM) system, which is used on many Linux distributions.

31.What is use of " sudo "

- The sudo command, which stands for "superuser do" or "switch user do," is a fundamental utility in Unix-like operating systems, including Linux. It is used to execute commands with superuser or root privileges, allowing authorized users to perform administrative tasks and system management safely.

32.Command to reset virtual machine.

- The command to reset a virtual machine can depend on the virtualization software you're using. I'll provide instructions for a common virtualization software, VMware, and another for VirtualBox.
- For VMware (using VMware Workstation or VMware Player):
- Open the VMware Workstation or VMware Player application.
- Make sure the virtual machine you want to reset is powered off.
- Right-click on the virtual machine in the VMware interface.
- Select "Power" from the context menu.
- Choose "Reset."

Linux server - Manage user and Groups and working with file systems

---

33. How to change user and group ownership on same time.

- sudo chown new_owner:new_group file_or_directory

34.Command to change user permission on directory

- chmod u[+|-|=][permissions] directory

35. List of special permission in Linux 7.0 is……

- here is a list of the special permissions in Linux:
- Set User ID (SUID)
- Set Group ID (SGID)
- Sticky Bit

36. What happened if i used this command…?[#chmod u+s /user/bin/vim]

- The command chmod u+s /usr/bin/vim sets the Set User ID (SUID) permission on the vim executable located in the /usr/bin directory. When you set the SUID permission on an executable file, it means that when any user runs the file, it will temporarily execute with the permissions of the file's owner.

37. What happened if i used this command…. [#chmod g+s /data]

- The command chmod g+s /data sets the Set Group ID (SGID) permission on the /data directory. When you set the SGID permission on a directory.