**Module 18**

**Linux server - Manage user and Groups and**

**working with file systems**

**Assignment Level Basic**

1. **What is default uid for root user ?**

* The user ID (UID) '0' is reserved for default root account. Root is the superuser account in Linux. It is a user account for administrative purposes, and typically has the highest access rights on the system. Configuring UID as '0' for other user account grants them root-level privileges.

1. **What is default uid for system user ?**

* A unique identifier (UID) is a numeric or alphanumeric string that is associated with a single entity within a given system. UIDs make it possible to address that entity, so that it can be accessed and interacted with.

1. **What is the uid for normal users ?**

* Although UID numbers 0 through 99 are reserved, you can add a user with one of these numbers. However, do not use 0 through 99 for regular user accounts. By definition, root always has UID 0, daemon has UID 1, and pseudo-user bin has UID 2.

1. **How to add comment in user file?**

* Select Review > New Comment. Type what you want. Click elsewhere in the document when you are done.

1. **From “ /etc/passwd “ which information will we gather ?**

* The/etc/passwd file is a plain text file with information for all user accounts. It includes a list of user accounts on the system, as well as details such as user ID, group ID, home directory, and default shell.

1. **From “ /etc/shadow “ which information will we gather ?**

* The /etc/shadow file provides an enhanced authentication mechanism for Linux systems by tightening access at the account level. This text file stores actual passwords in hashed format, along with additional information related to these passwords.

1. **From “ /etc/group “ which information will we gather ?**

* The /etc/group file in Linux and UNIX-like operating systems is a text file that defines the groups to which users belong.

1. **From “ /etc/gshadow “ which information will we gather ?**

* The /etc/gshadow file in Linux systems contains secure group account information. It’s readable only by the root user and includes details that provide an additional layer of security for group passwords.

1. **What is the meaning of + and – in file permission?**

* In the context of file permissions in Linux, the + and - symbols have specific meanings:
* The + symbol is used to **add** specified permissions to a file or directory. For example, using chmod g+w filename would add write permission to the group class for the file named filename.
* The - symbol is used to **remove** specified permissions from a file or directory. For example, chmod o-r filename would remove read permission from the others class for the file named filename.

**10.What is “ r “ “ w ” ‘ x “ in file permission**

|  |  |
| --- | --- |
| * **Value** | * **Meaning** |
| * - | * Flag is not set. |
| * r | * File is readable. |
| * w | * File is writable. For directories, files may be created or removed. |
| * x | * File is executable. For directories, files may be listed. |

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

* Each octal digit is the sum of 4 if read permission is granted, 2 if write permission is granted and 1 if execute permission is granted.

**12.What is the use of umask?**

* The umask (UNIX shorthand for "user file-creation mode mask") is a four-digit octal number that UNIX uses to determine the file permission for newly created files. Every process has its own umask, inherited from its parent process.

**13.What is default root permission for directory?**

* Default permissions for the root directory ('/') are typically set to 0755 (drwxr-xr-x), allowing the owner (root) to read, write, and execute, while other users can read and execute but not write.

**Assignment Level Intermediate**

1. **How to assign another new home directory for new user?**

* **useradd: create home AND another directory for user**
* useradd -m -d /home/<username> <username>
* mkdir /ssd/<username>
* change the directory permissions.

1. **Command to check group membership of any user**

* Enter the PowerShell cmdlet Get-ADPrincipalGroupMembership. This cmdlet shows the AD groups that a specified user, computer, group, or service account is a member. A global catalog is necessary for this command to perform a group search.

1. **What happened if I use “ su – “ command ?**

* The su command in Linux lets you switch to another user's account or execute commands as a different user. It's useful for administrative tasks that require elevated privileges. su is also used to test commands with different user permissions to ensure the system requires authentication for user switches.

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

* userdel -r: Whenever we are deleting a user using this option then the files in the user's home directory will be removed along with the home directory itself and the user's mail spool. All the files located in other file systems will have to be searched for and deleted manually.

1. **How to add new user without home directory ?**

* Open the Ubuntu Terminal by pressing CTRL+ALT+T.
* Insert the following command to create a user: sudo useradd -M abir. OR, sudo useradd --no-create-home abir. EXPLANATION. sudo: Grants administrative privileges. useradd: Adds a new user. ...
* Press the ENTER key after providing the password.

1. **Command to assign account expiry to the user ?**

* The useradd command supports the -e or –expiredate option to set an expiration date for the user. Notably, there's no output by default and useradd creates a user with the specified expiration date. Also, we can notice that the expiration date is in the YYYY-MM-DD format.

1. **Command to add a new group …**

* Create and modify groups. To add a group in Linux, use the groupadd command: $ sudo groupadd demo. ...
* Change the group ID. You can change the group ID of any group with the groupmod command and the --gid or -g option: $ sudo groupmod -g 1011 demo1. ...
* Rename a group. ...
* Add and remove users from a group. ...
* Delete a group.

1. **What is default root permission for file?**

* Default permissions for the root directory ('/') are typically set to 0755 (drwxr-xr-x), allowing the owner (root) to read, write, and execute, while other users can read and execute but not write.

1. **What is the default umask for root?**

* For root user the default value is 0022, and for the local users it's 0002. However you can always change it to whatever value or permissions you want

**10.What is the default umask for student?**

* Default octal umask is 022 for root and 002 for standard users, in most Linux distros.

**11.Which command is used to set user ownership?**

* The chown command changes the owner of the file or directory specified by the File or Directory parameter to the user specified by the Owner parameter.

**Assignment Level Advance**

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

* If a user is already created and you just want to add that user to a group: Use the command usermod -Gmanagement “name of user”

1. **What is the difference between “ usermod -G “ and “ usermod -aG “**

* Difference between "usermod -aG" and "usermod -G" options in linux? In summary, the conversation discusses the differences between the "usermod -aG" and "usermod -G" options on CentOS 7, with the former adding a user to a secondary group and the latter replacing all secondary groups with a new one

1. **What is the meaning of “ -1 “ in password state information?**

* 0 : Password can be changed, but does not have to be changed. 1 : Password is initial and must be changed. 2 : Password has expired and must be changed. 3 : Password must be changed because it no longer meets the new rules.

1. **Which command tis used to remove the password of any user?**

* The quick way to remove/delete a user password is to pass --delete option to the passwd command

1. **What is the use of “ gpasswd “ ?**

* The gpasswd command allows you to edit a group's password, members, and administrators. It is used to edit both the /etc/group and /etc/gshadow files. If you use the command without any options, it will prompt for a new password for the group.

1. **Command to change password policy**

* The easiest way to configure a password policy is to by using the dsconfig command to manage the existing password policies and to modify the password policy properties. The following examples use dsconfig to modify various properties of the password policy.

1. **What is use of “ sudo “**

* Sudo is a command-line utility for Unix and Unix-based operating systems such as Linux and macOS. The utility provides an efficient way to temporarily grant users or user groups privileged access to system resources so that they can run commands that they cannot run under their regular accounts.

1. **Command to reset virtual machine**

* **Select VM Power > Reset to display the Run Power Control window.**
* Run Power Control: Verify the VM you want to reset, then select Next. ...
* Scheduling: Select when you want the reset job to run, then select Next.
* Notifications: Optionally enter a notifier, then select Next.

1. **How to change user and group ownership on same time**

* OWNER[:GROUP] – gives an option to change ownership for a user, a group, or both at the same time. ...
* FILE(s) – here users can list the files or directories that they want to change ownership for.

**10.Command to change user permission on directory**

* The chmod command enables you to change the permissions on a file. You must be superuser or the owner of a file or directory to change its permissions.

**11.List of special permission in Linux 7.0 is……**

|  |  |  |
| --- | --- | --- |
| * **Permission** | * **Alphabetical Notation** | * **Binary Notation** |
| * write | * -w- | * 010 |
| * execute | * --x | * 001 |
| * read, write | * rw- | * 110 |
| * read, execute | * r-x | * 101 |

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

* Using the command chmod u+s /user/bin/vim on a Unix-like operating system would set the **setuid** (Set User ID) permission on the vim executable. This means that when any user executes the vim program, it will run with the file owner’s permissions, rather than the permissions of the user who launched it.
* chmod: Command to change file system permissions.
* u+s: Sets the setuid bit.
* /user/bin/vim: The path to the vim executable (usually it’s /usr/bin/vim

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

* Short: "s" means set. Long: As applied to a file, chmod g+s is used for setgid. That is, if the file is executable and has the group-s bit set, it will run with its group set to match the group-ownership of the file.

**Task: 1**

1. **Find details about current logged-in user.**

* To find details about the current logged-in user on a Windows system, you can use several methods. Here are a few options:
* **Task Manager**:
* Press Ctrl+Shift+Esc to open Task Manager.
* [Switch to the ‘Users’ tab to see the list of currently logged-in users and their status](https://www.thewindowsclub.com/how-to-find-all-signed-in-users-in-windows)[1](https://www.thewindowsclub.com/how-to-find-all-signed-in-users-in-windows).
* **Command Prompt**:
* Open Command Prompt by searching for cmd in the Taskbar search box.
* Type the command query user to list all signed-in users. [The USERNAME column will display the names, and an arrow (>) will indicate the current user](https://www.thewindowsclub.com/how-to-find-all-signed-in-users-in-windows)

1. **Show all processes on terminal**

* To list all running processes, you can use the following command: ps -A or ps -e Both commands will provide you with a list of currently running processes along with their relevant details, such as process ID (PID), terminal, CPU usage, and more.

1. **Create primary group**

* When you create a user on Linux using the useradd command, a group with the same name as the username is also created, and the user is added as the group's sole member. This group is the user's primary group.

1. **Create supplementary group**

* The groupadd command can be used with multiple options to create a supplementary group for user accounts, or a system user group. Creates a system group using a GID from the default system group's range (1-999), or as given in the /etc/login. defs file.

1. **Find groups details and list on terminal P6. Find user details and list on terminal.**

* To find group details and list them on a terminal in Windows, you can use the net localgroup command. Here’s how you can do it:
* Open **Command Prompt** or **Windows PowerShell**.
* Type the following command and press Enter:
* net localgroup
* This will list all local groups on the system.

1. **Use “sudo”**

* Sudo is a command-line utility for Unix and Unix-based operating systems such as Linux and macOS. The utility provides an efficient way to temporarily grant users or user groups privileged access to system resources so that they can run commands that they cannot run under their regular accounts.

1. **View the last 5 lines of the “ /var/log/messages “**

* The tail command is probably one of the single most handy tools you have at your disposal for the viewing of log files. What tail does is output the last part of files. So, if you issue the command tail /var/log/syslog, it will print out only the last few lines of the syslog file.

1. **Add a new user with name “ NuPuR “**

* To add a new user named “NuPuR” on a Windows system, you can use the Command Prompt with administrative privileges.
* Open the **Start** menu, type cmd, right-click on **Command Prompt**, and select **Run as administrator**.
* In the Command Prompt, type the following command and press **Enter**:
* net user NuPuR /add
* This will create a new user account with the username “NuPuR”.

1. **Remove this user and user’s home directory**

* To remove a user, type: $ sudo userdel <user\_name>
* Delete a user in other root directory (cd into the /path/to/dir1/ and then remove it) : $ sudo userdel --root </path/to/dir1/> <user\_name>
* Remove a user along with the home directory and mail spool: $ sudo userdel --remove <user\_name>

**10.Create new supplementary group name is “ whEEL “**

* To create a new supplementary group named “whEEL” on a Windows system, you can use PowerShell with administrative privileges. Here’s how you can do it:
* Open the **Start** menu, type PowerShell, right-click on **Windows PowerShell**, and select **Run as administrator**.
* In the PowerShell window, type the following command and press **Enter**:
* New-LocalGroup -Name "whEEL"
* This will create a new local group named “whEEL”.

**11.Create a new user with name “ ELviS “**

* To create a new user named “ELviS” on a Windows system, you can use the Command Prompt with administrative privileges. Here’s how you can do it:
* Open the **Start** menu, type cmd, right-click on **Command Prompt**, and select **Run as administrator**.
* In the Command Prompt, type the following command and press **Enter**:
* net user ELviS /add
* This will create a new user account with the username “ELviS”.

**12.Add / Append a user to a supplementary group**

* We can use option -a in addition to -G. The argument -a stands for ‐‐append, which means we're adding the user to supplementary groups in addition to the ones they already belong to. Now, the user will be added to the listed groups but also kept in the ones it already belonged to.

**13.Restrict / Lock login access for “ ELviS “ user**

* To restrict or lock login access for the user “ELviS” on a Windows system, you can use the following method:
* Open **Command Prompt** as an administrator.
* To disable the account, type the following command and press **Enter**:
* net user ELviS /active:no
* This will disable the account “ELviS”, effectively preventing login access.

**14.Create a new user name “ LiNuX without home directory**

* Open the Ubuntu Terminal by pressing CTRL+ALT+T.
* Insert the following command to create a user: sudo useradd -M abir. OR, sudo useradd --no-create-home abir. EXPLANATION. sudo: Grants administrative privileges. useradd: Adds a new user. ...
* Press the ENTER key after providing the password.

**15.Create a new user name “ RedHat “ with new home directory “**

* To create a new user named “RedHat” with a new home directory on a Windows system, you can use PowerShell with administrative privileges. Here’s how you can do it:
* Open the **Start** menu, type PowerShell, right-click on **Windows PowerShell**, and select **Run as administrator**.
* To create the new user “RedHat”, type the following command and press **Enter**:
* New-LocalUser -Name "RedHat" -Password (Read-Host -AsSecureString "Enter Password")
* This will prompt you to enter a password for the new user.

**16./etc/HatRed**

* It seems like you’re referring to a directory path, but ./etc/HatRed does not appear to be a standard directory or command. If you’re trying to access the /etc directory on a Unix-like system, which is used for system configuration files, the correct path would be /etc.
* However, “HatRed” does not correspond to any known system command or directory. If “HatRed” is intended to be a custom script or directory, you would need to ensure that it exists within the etc directory and has the appropriate permissions set to be accessed or executed.

**17.Create a new user with two(2) days expiry**

* We can create a new user using the built-in useradd command. The useradd command supports the -e or –expiredate option to set an expiration date for the user. Notably, there's no output by default and useradd creates a user with the specified expiration date.

**18.Remove password for “ ELviS “ user**

* Their language of Khuzdul is a secret that they don't share with outsiders, so writing it on a public door wouldn't have been allowed. As such, the choice to have Moria's password be in Elvish both reflects the friendship between the two peoples and Dwarven culture.

**19.Check user password policy for “ LiNuX “ user**

* To check the password policy for a specific user in Windows, you would typically use the Local Security Policy editor or Active Directory tools, depending on whether your system is part of a domain. However, since you mentioned “LiNuX” which could imply a Unix-like system, I’ll provide instructions for both Windows and Unix-like systems.
* **For Windows:**
* Open the **Local Security Policy** editor by pressing Windows key + R, typing secpol.msc, and pressing **Enter**.
* Navigate to **Account Policies** > **Password Policy**.

**Task :2**

* 1. **Login from “LiNuX” user**
* Username and user ID (UID)
* Password.
* Primary group name and group ID (GID)
* Secondary group names and group IDs.
* Location of the home directory.
* Preferred shell.

**2. Create new directory on desktop name is "FoLdEr”**

* Use the keyboard shortcut Ctrl + Shift + N to create a new desktop folder.

**3. Change group ownership from LiNuX to root on “FoLdEr” directory**

* The `chgrp` command in Linux is used to change the group ownership of a file or directory. All files in Linux belong to an owner and a group. You can set the owner by using “chown” command, and the group by the “chgrp” command.

**4. Create new file on /etc/ with name “ FiLe”**

* To create a new file named “FiLe” in the /etc directory on a Unix-like system, you would typically use the touch command. However, since /etc is a system directory that requires administrative privileges to modify, you’ll need to use sudo to perform the operation. Here’s how you can do it:
* sudo touch /etc/FiLe
* This command will prompt you for your password. After entering it, the file “FiLe” will be created in the /etc directory. [Remember that modifying system directories can affect your system’s configuration, so be sure to only make changes if you’re certain of the implications](https://www.wikihow.com/Create-a-File-in-a-Directory-in-Linux)

**5. Check permissions of above file**

* Open File Explorer.
* Locate the desired file. ...
* Right click on the file and go to Properties.
* Choose the Security Tab at the top to view current permissions.
* To edit permissions for certain users, select Edit.
* To add an account, select Add.

**6. Login from “student” user**

* Student Portal is the common phrase used to describe a secure web based platform used by institutions which allows students to login to their respective websites to access the educational materials, services and resources.

**7. Create new directory on students home with name “file1”**

* To create a new directory named “file1” in the home directory of a user named “students” on a Unix-like system, you can use the mkdir command.
* Open the terminal.
* Use the cd command to navigate to the “students” home directory. If “students” is the username, the home directory is typically /home/students.
* Run the following command:
* mkdir file1
* This will create a directory named “file1” inside the “students” home directory.

**8. Remove read and write permission for group and other on above file “file1”**

* To remove read and write permissions for the group and others on the file “file1”, you can use the chmod command on a Unix-like system. Here’s the command you would use:
* chmod go-rw file1
* This command will modify the permissions of “file1” so that:
* Group members (g) will not have read (r) or write (w) permissions.
* Others (o) will also not have read (r) or write (w) permissions.

1. **Add execute permission for everyone on“file2”**

* To add world read and execute permission to a file using the symbolic mode you would type chmod o+rx [filename]. To remove world read permission from a file you would type chmod o-r [filename].

**10.Set Read,write,execute for USER**

* To change directory permissions for everyone, use “u” for users, “g” for group, “o” for others, and “ugo” or “a” (for all). chmod ugo+rwx foldername to give read, write, and execute to everyone. chmod a=r foldername to give only read permission for everyone.

**11.Set Read and execute for GROUP**

* chmod 777 foldername will give read, write, and execute permissions for everyone. chmod 700 foldername will give read, write, and execute permissions for the user only. chmod 327 foldername will give write and execute (3) permission for the user, w (2) for the group, and read, write, and execute for the users.

**12.Set No permission for other on “Directory1”**

* To set no permissions for others on a directory named “Directory1” on a Unix-like system, you can use the chmod command with the appropriate permissions setting. Here’s the command you would use:
* chmod o-rwx Directory1
* This command will remove read (r), write (w), and execute (x) permissions for others (o) on “Directory1”. [Ensure that you have the necessary permissions to modify the directory’s permissions and that you’re in the correct directory or provide](https://linuxize.com/post/chmod-command-in-linux/)

**13.Create new group name “ateam” , And add two new user in this group “andy” and “alice”, set password is “password”**

* Select the team you want to add members to. Click the “…” (more options) button beside the team name and choose “Add member” from the drop-down menu. A pop-up window will appear. Here, enter the names or email addresses of the members you wish to add.

**14.Login from root and root home directory**

* Try cd /root . ~ is normally just a shorthand for the home directory, so if you are the regular user person then cd ~ is the same as cd /home/person . To start in interactive session as root, which is treated as a login shell. This will set the HOME environment variable appropriately.

**15.Create a new directory in “/home” name is “ateam-text”**

* To create a new directory named “ateam-text” in the /home directory on a Unix-like system, you can use the mkdir command. Here’s how you can do it:
* Open the terminal.
* Type the following command and press **Enter**:
* sudo mkdir /home/ateam-text
* This command will create a new directory named “ateam-text” in the /home directory. [You’ll need to use sudo because /home is typically a system directory that requires administrative privileges to modify](https://linuxize.com/post/how-to-create-directories-in-linux-with-the-mkdir-command/)

**16.Change the group ownership of the ateam-text directory to “ateam”.**

* ext” to the group “ateam” on a Unix-like system, you can use the chgrp command. Here’s how you can do it:
* Open the terminal.
* Type the following command and press **Enter**:
* sudo chgrp ateam /home/ateam-text
* This command will change the group ownership of the “ateam-text” directory to the group “ateam”. [You’ll need to use sudo because changing group ownership is a privileged operation1](https://linuxize.com/post/chgrp-command-in-linux/).
* Make sure that the group “ateam” exists on your system before running this command. You can check existing groups with the getent group command. If the group does not exist, you can create it using the groupadd command before assigning it to the directory.

**17.Ensure the permission of ateam-text allows group members to create**

* To ensure that the group members of “ateam” can create files and directories within the “ateam-text” directory, you need to set the appropriate group permissions and also set the setgid bit on the directory. Here’s how you can do it:
* Open the terminal.
* Type the following commands and press **Enter**:
* sudo chmod g+rwxs /home/ateam-text
* sudo setfacl -d -m g:ateam:rwx /home/ateam-text
* The first command chmod g+rwxs sets the read, write, and execute permissions for the group, and the s sets the setgid bit. This means that new files and directories created within “ateam-text” will inherit the group ownership from the parent directory.
* The second command setfacl -d -m g:ateam:rwx sets a default Access Control List (ACL) for the group “ateam”, giving them read, write, and execute permissions on new files and directories created within “ateam-text”.