Add and delete users

Welcome back! In this video, we are going to discuss adding and deleting users.
This is related to the concept of authentication.
Authentication is the process of a user proving that they are who they say they are in the system.

Just like in a physical building, not all users should be allowed in.
Not all users should get access to the system.
But we also want to make sure everyone who should have access to the system has it.
That's why we need to add users.
New users can be new to the organization or new to a group.
This could be related to a change in organizational structure or simply a directive from management to move someone.

And also, when users leave the organization, they need to be deleted.
They should no longer have access to any part of the system.
Or if they simply changed groups, they should be deleted from groups that they are no longer a part of.

Now that we've sorted out why it's important to add and delete users, let's discuss a different type of user, the root user.
A root user, or superuser, is a user with elevated privileges to modify the system.
Regular users have limitations, where the root does not.

Individuals who need to perform specific tasks can be temporarily added as root users.
Root users can create, modify, or delete any file and run any program.
Only root users or accounts with root privileges can add new users. So you may be wondering how you become a superuser.
Well, one way is logging in as the root user, but running commands as the root user is considered to be bad practice when using Linux.

Why is running commands as a root user potentially problematic?
The first problem with logging in as root is the security risks.
Malicious actors will try to breach the root account.
Since it's the most powerful account, to stay safe, the root account should have logins disabled.
Another problem is that it's very easy to make irreversible mistakes.

It's very easy to type the wrong command in the CLI, and if you're running as the root user, you run a higher risk of making an irreversible mistake, such as permanently deleting a directory.
Finally, there's the concern of accountability.
In a multi-user environment like Linux, there are many users.
If a user is running as root, there is no way to track who exactly ran a command.
One solution to help solve this problem is sudo.

sudo is a command that temporarily grants elevated permissions to specific users.
This provides more of a controlled approach compared to root, which runs every command with root privileges.
sudo solves lots of problems associated with running as root.

sudo comes from super-user-do and lets you execute commands as an elevated user without having to sign in and out of another account.
Running sudo will prompt you to enter the password for the user you're currently logged in as.
Not all users on a system can become a superuser.
Users must be granted sudo access through a configuration file called the sudoers file.

Now that we've learned about sudo, let's learn how we can use it with another command to add users.
This command is useradd.
useradd adds a user to the system.
Only root or users with sudo privileges can use a useradd command.
Let's look at a specific example in which we need to add a user.
We'll imagine a new representative is joining the sales department and will be given the username of salesrep7.
We're tasked with adding them to the system.

Let's try adding the new user.
First, we need to use the sudo command, followed by the useradd command, and then last, the username we want to add, in this case, salesrep7.
This command doesn't display anything on the screen.
But since we get a new Bash cursor and not an error message, we can feel confident that the command worked successfully.
If it didn't, an error message would have appeared.
Sometimes an error has to do with something simple like misspelling useradd.
Or, it might be because we didn't have sudo privileges.

Now let's learn how to do the opposite.
Let's learn how to delete a user with userdel.
userdel deletes a user from the system.
Similarly, we need root permissions that we'll access through sudo to use userdel.
Let's go back to our example of the user we added.
Let's imagine two months later, the sales representative that we just added to the system leaves the company.
That user should no longer have access to the system. Let's delete that user from the system.

Again, the sudo command is used first, then we add the userdel command.
Last, we add the name of the user we want to delete.
Again, we know it ran successfully because there is a new Bash cursor and not an error message.

Now, we've covered how to add and delete users and how these actions require sudo.
When using sudo, we have to use our best judgment.

These special privileges must be used responsibly to ensure a secure system.

Revision #1
Created 7 July 2023 11:42:10 by naruzkurai
Updated 7 July 2023 11:44:13 by naruzkurai