SU / SUDO

Most Linux users will be faced with sudo and su at least once in their lives. Because of their comparable syntax and overlapping functions, it is often complicated for new users to differentiate between them.The commands sudo and su are among the most widespread and effective in Linux. By deterring unpredictable things in your network, you can deter performance and safety issues in your network.The two methods of gaining root privileges are sudo and su. As a result, each functions distinctly and uses a distinct default configuration counting on the Linux distribution.With sudo, a user with the appropriate permissions can manage commands as root with administrative rights. By using the command su, a user can manage commands with the rights of another user. This permits us to exchange accounts without having to log out of the existing session. The difference between sudo and su is that sudo enables limited credentials and su enables limitless credentials.

The "sudo" command

Employing sudo offers you the capability to run commands as root. It may not be essential to utilize the root password relying on the setup. A log is held for every command managed with su.

In technical terms, **sudo** is an acronym for **SuperUser & Do** or **Switch User & DO**, which is required to access restricted files and commit operations. In order to prevent sensitive files from being altered, Linux restricts access to specific parts of the system by default.

When executed as root, sudo elevate privileges, enabling users to perform sensitive tasks without logging into the root account. By default, the Ubuntu Linux configuration doesn't include a root account.

The end-user must devise a root account password manually by running the sudo command. The use of sudo is typically one of the most efficient ways to protect the computer from being used as a tool for exploitation.

The root privilege is required each time a user attempts to install, remove, or change any component of the software. Once a user enters a login password for granting system-based permissions, the Sudo command permits them to attain such permissions for any certain command they expect to perform.

The "su" command

Implying su (also known as a substitute or switch user), you can accomplish commands with the privileges of another user, by default root.

During a current login session, su is the most opportunely way to switch to the administrative account. In situations where the root user cannot log in via ssh or the GUI display manager, this can be particularly helpful.

su ensures you have the root password when running a command as root. The output of all commands accomplished with su is not logged.

Switching from one account to another is done with the Ubuntu Linux command su. A password request will be made to the user from whom the switch is being made.

At the time of installing the Linux operating system, the SuperUser (su) - usually called root in Unix-like systems is created as the first user. Each Linux system user has a User ID, also called a UID in Linux which is their unique identifier.

Due to the way Linux recognizes users, the root has an ID of 0, meaning that it is the first user. All Linux files can be created, modified, executed, and deleted by the Superuser on any Linux system.