Rocky Enterprise Linux 9.2 Manual Pages on command 'sudo_root.8'

C:\>man sudo_root.8

sudo_root(8) System Manager's Manual sudo_root(8)

NAME

sudo_root - How to run administrative commands

SYNOPSIS

sudo command

sudo -i

INTRODUCTION

By default, the password for the user "root" (the system administrator) is locked. This means you cannot login as root or use su. Instead, the installer will set up sudo to allow the user that is created during install to run all administrative commands.

This means that in the terminal you can use sudo for commands that require root privileges. All programs in the menu will use a graphical sudo to prompt for a password. When sudo asks for a password, it needs your password, this means that a root password is not needed.

To run a command which requires root privileges in a terminal, simply prepend sudo in front of it. To get an interactive root shell, use sudo -i.

ALLOWING OTHER USERS TO RUN SUDO

By default, only the user who installed the system is permitted to run sudo. To add more administrators, i. e. users who can run sudo, you have to add these users to the group 'sudo' by doing one of the following steps:

* In a shell, do

sudo adduser username sudo

* Use the graphical "Users & Groups" program in the "System settings" menu to add the new user to the sudo group.

BENEFITS OF USING SUDO

The benefits of leaving root disabled by default include the following:

* Users do not have to remember an extra password, which they are likely to forget.
* The installer is able to ask fewer questions.
* It avoids the "I can do anything" interactive login by default - you will be prompted for a password before major changes can happen, which should make you think about the consequences of what you are doing.
* Sudo adds a log entry of the command(s) run (in /var/log/auth.log).
* Every attacker trying to brute-force their way into your box will know it has an account named root and will try that first. What they do not know is what the usernames of your other users are.
* Allows easy transfer for admin rights, in a short term or long term period, by adding and removing users from the sudo group, while not compromising the root account.
* sudo can be set up with a much more fine-grained security policy.
* On systems with more than one administrator using sudo avoids sharing a password amongst them.

DOWNSIDES OF USING SUDO

Although for desktops the benefits of using sudo are great, there are possible is? sues which need to be noted:

* Redirecting the output of commands run with sudo can be confusing at first. For instance consider

  sudo ls > /root/somefile

  will not work since it is the shell that tries to write to that file. You can use

  ls | sudo tee /root/somefile

  to get the behaviour you want.
* In a lot of office environments the ONLY local user on a system is root. All other users are imported using NSS techniques such as nss-ldap. To setup a work? station, or fix it, in the case of a network failure where nss-ldap is broken, root is required. This tends to leave the system unusable. An extra local user,

or an enabled root password is needed here.

GOING BACK TO A TRADITIONAL ROOT ACCOUNT

This is not recommended!

To enable the root account (i.e. set a password) use:

```
sudo passwd root
```

Afterwards, edit the sudo configuration with sudo visudo and comment out the line

```
%sudo  ALL=(ALL) ALL
```

to disable sudo access to members of the sudo group.

SEE ALSO

sudo(8), https://wiki.ubuntu.com/RootSudo