09 February, 2023 by **Ashley**

How to Edit Sudoers File in Linux

Linux operating systems set up the first user as an admin by default and grant it access to sudo and reasonable defaults. While the Sudoers file provides instructions to the system on handling the sudo command, the sudo command enables non-root users to execute other Linux commands that typically require superuser access. But sometimes they may encounter the sudo command not found error.

In this article, you will learn How to Edit Sudoers File and Manage Sudo Command in Linux. Join us to review the way you can edit the file if you want to limit what users can run as sudo, grant new users access to sudo,

or revoke a user's permission.

When you completed the initial server setup of your favorite distribution after buying Linux VPS, log in to your server as a non-root user and move on to learn how to obtain root privileges correctly.

Table of Contents

What is Sudoers File?

previously, you have learned what Sudo is exactly. Super-user rights are granted to a special user called root. There are no restrictions on this administrator account that apply to regular users. There are various ways for users to run commands with super-user or root access. The sudo prefix is not required by default for the root user. They already get every benefit that is possible. The sudo prefix must be added to the useradd command if a non-root user wants to add another user:

```
sudo useradd operavps
```

As you guess, the user will see a *Permission denied output* if they don't use the sudo prefix.

However, it is possible to configure other users as well as to run the sudo command. So, you need to edit sudoers to do this. While sudoers error might lock out all users on your distribution, you are recommended to follow this guide to have a safe and certain source.

Sudoers Syntax

Let's explore different forms and guidelines for editing sudoers:

- root ALL=(ALL:ALL) ALL: this line indicates that the root user has unrestricted access to the system and can execute any command.

- %admin ALL=(ALL) ALL: The % symbol designates a group. Anyone with an admin group membership has root user rights.
- %sudo ALL=(ALL:ALL) ALL: Each member of the sudo group has the ability to execute any command.

Also, the line of #includedir /etc/sudoers.d, says that we can link the file sudoers.d here and add configurations to it.

Tutorial Edit Sudoers File and Manage Sudo Command in Linux

As a Linux user, you might by default have sudo access and be an admin. But if not, you need to make changes. Let's go through this guide and learn how to use sudo and change sudoers file.

Visudo Command

The `sudo` command is configured through a file located at `/etc/sudoers`. The **`visudo`** command at a terminal is used to edit the Sudoers file. Press **Ctrl + Alt + T** on the keyboard to launch a terminal window, or look for a terminal in the program menu, to access the Sudoers file for editing. Log in to the terminal using the root account once it is open and ready to use.

To use `visudo` command, you must make root login possible. It is crucial to use the visudo command when editing the `/etc/sudoers` file since erroneous syntax can result in a damaged system that prevents you from obtaining elevated privileges. The visudo command opens a text editor as usual, but before saving, it checks the file's syntax. This keeps `sudo` activities from being halted by configuration issues, which might be the only way for you to gain root access.

While `visudo` opens the file with the `vi` text editor, Ubuntu configures

visudo to use the `nano` text editor. However, you can run the following command to change it back to `vi`.

```
sudo update-alternatives --config editor
```

Execute the following command to view the `/etc/sudoers` file after setting up `visudo`:

```
sudo visudo
```

How to Edit Sudoers File in Linux

You can use the command below to edit `/etc/sudoers` file:

```
sudo visudo -f /etc/sudoers
```

It is advised to edit the sudoers file with visudo. Visudo performs the necessary syntactic checks and ensures that only one user at a time can edit sudoers. You can use the grep tool to determine whether users are members of the sudo group:

```
grep 'sudo' /etc/group
```

In this way, the user names will be listed as a result of this. Using the **adduser** command on the command line, we can add a user named bill to the sudo group as follows:

```
adduser bill sudo
```

The username bill will be visible if we run the grep command to examine who is a member of the group. Simply add someone to sudo to grant them root access. Run the following command to remove a user from sudo:

```
deluser bill sudo
```

Bill will be removed from the sudo group via the deluser command. Acts requiring sudo privileges can no longer be carried out by the user bill.

How to Grant a User Sudo Privileges

Giving a new user general sudo access is the most frequent task users attempt when handling sudo rights. If you wish to grant a user account full administrative access to the system, this is helpful. Adding the user in question to the general purpose administration group is the simplest way to accomplish this on a system that has one set up.

```
sudo usermod -aG sudo username
```

Also, you can use the command below too. However, both of them will achieve the same result.

```
sudo gpasswd -a username sudo
```

How to Give Specific Privileges Using Sudoers File

To let bill run only specific kinds of commands with sudo privileges, you need to create a configuration file in **/etc/sudoers.d/** called networking. So, to create the file, type:

```
sudo visudo -f /etc/sudoers.d/networking
```

Then, add the following text to the file:

```
Cmnd_Alias CAPTURE = /usr/sbin/tcpdump
Cmnd_Alias SERVERS = /usr/sbin apache2ctl, /usr/bin/htpass
Cmnd_Alias NETALL = CAPTURE, SERVERS
%netadmin ALL=NETALL
```

Next, run the following command:

```
addgroup netadmin
```

To add user bill to the netadmin group, type:

```
sudo adduser bill netadmin
```

In this way, the user bill will run the **tcpdump** command along with other networking-related commands.

How to Remove Users from the Sudoers File

You can remove users from sudo access without modifying the Sudoers file if you added sudo access using the “wheel” group or the “sudo” group. Open a terminal instead, then enter the following commands.

```
su
usermod -G wheel username
```

OR

```
su
usermod -G sudo username
```

Set Up Custom Rules

Let’s create some new rules now that we are familiar with the file’s general syntax.

Create Aliases

Since grouping items with multiple “aliases” will make organizing the

sudoers file easier, we can create three different user groups that share members. For example:

/etc/sudoers

```
. . .
User_Alias              GROUPONE = abby, brent, carl
User_Alias              GROUPTWO = brent, doris, eric,
User_Alias              GROUPTHREE = doris, felicia, grant
. . .
```

Names of groups must begin with a capital letter. Then, by establishing a rule similar to the following, we may permit members of `GROUPTWO` to change the `apt` database:

/etc/sudoers

```
. . .
GROUPTWO        ALL = /usr/bin/apt-get update
. . .
```

As mentioned above, sudo runs as the root user by default if we don't select a user or group to run as. By establishing a "command alias" and applying it in a rule for `GROUPTHREE` , we may permit members of `GROUPTHREE` to shut down and restart the computer:

/etc/sudoers

```
. . .
Cmnd_Alias              POWER = /sbin/shutdown, /sbin/halt
GROUPTHREE      ALL = POWER
. . .
```

We create a command alias called `POWER` that includes instructions for rebooting and powering off the computer. Then we give these commands to the members of `GROUPTTHREE` . Additionally, "Run as" aliases can be made to take the place of the rule's section that designates the user for

the command to be executed as:

/etc/sudoers

```
. . .
Runas_Alias              WEB = www-data, apache
GROUPONE         ALL = (WEB) ALL
. . .
```

Anyone who belongs to `GROUPONE` will be able to run commands under the `www-data` user or the `apache` user thanks to this. Just remember that if there is a dispute between two rules, the later rule will take precedence.

3 Methods to Obtain Root Privileges

There are three fundamental ways to obtain root privileges, ranging in complexity:

1. Logging In As Root.
2. Using `su` to Become Root.
3. Using `sudo` to Execute Commands as Root.

Let's see what these three ways of obtaining root privileges are.

Logging In As Root:

Directly logging into your server as the root user is the quickest and easiest way to gain root access. Enter `root` as your username and the root password when prompted if you're logging into a local machine. In your SSH connection string, put the root user before the IP address or domain name if you're using SSH to log in:

```
ssh root@server_domain_or_ip
```

Enter the root password when requested if the root user's SSH keys have

not been configured.

Using su to Become Root

Direct root logins are typically not advised because it is simple to start using the system for purposes other than administration, which is risky. The following method makes it possible for you to take on the role of the root user whenever you need to. The su command, which stands for "substitute user," can be used to accomplish this. To get root privileges, type:

```
su
```

When you are asked for the root user's password, a root shell session will be launched for you. After completing the actions that call for root access, type the following to return to your default shell:

```
exit
```

Using sudo to Execute Commands as Root

The sudo command is the last method of gaining root access that we'll cover. Without having to create a new shell, you can run one-off commands as root with the sudo command. It is carried out as follows:

```
sudo command_to_execute
```

The sudo command, in contrast to su, will ask for the current user's password rather than the root password.

Increase Sudo Security

Increase sudo security if you care about security. Fortunately, you can increase your Sudo security by turning on the use_pty option. This

feature makes sure that sudo runs in a sandbox, making it more difficult for malware to exploit. Locate a section of the Sudoers file that has the line “Defaults” to enable this feature. Next, hit Enter to add a new line. The use_pty feature can then be enabled by adding the following code.

```
Defaults use_pty
```

Press **Ctrl + O** when you are done with editing.

How to solve adding the user to the group in CentOS?

If it does not work immediately, edit the **/etc/sudoers** file to uncomment the group name:

```
sudo visudo
```

/etc/sudoers

```
. . .
%wheel ALL=(ALL) ALL
. . .
```

How to Limit root User?

Users with root access can make unrestricted changes to the system. Since there are no limitations on the privileges that can be used once root access has been given, you may need to limit root users. You can choose to utilize the sudo tool, which will grant trusted users with restricted root access. To do this, you can configure sudo to allow access to only some, but not all commands. Take care with this as sometimes this may allow shell access. It is possible to limit root user with AppArmor. Encrypting data will also prevent even the root from accessing

it.

As another solution, you can remove users from the group sudo using the command `deluser user sudo` if you don't want them to be able to use root commands.

How to Edit sudoers File Without root?

Super-user privileges are granted to a special user called root. There are no restrictions on this administrator account that apply to regular users. There are numerous ways for users to run commands with super-user or root access.

In the text editor of your choice, open the **/etc/sudoers** file.

```
Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/

root ALL=(ALL:ALL) ALL

%admin ALL=(ALL) ALL
%sudo ALL=(ALL:ALL) ALL

#includedir /etc/sudoers.d
```

FAQ

− I cannot log into root with the su command

Enable root login by running sudo -s, followed by passwd.

+ Why adding a user to the Sudoers file is dangerous?

+ which is a special group that provides its members with the ability to run the su and sudo commands?

+ how to exit sudoers file?

+ how to edit /etc/sudoers file in ubuntu?

+ what are the steps of editing sudoers file redhat?

Conclusion

In this article, you learned How to Edit Sudoers File and Manage Sudo Command in Linux. Understanding the sudo command and the sudoers file is essential if you're working with multiple users. With this knowledge, you should be able to read and alter the sudoers file and understand the different ways you can gain root access.

If you encounter any problems, please do not hesitate to contact us. Our technical support team will try their best to solve your problems.

← Previous

SSH "Connection Refused"

Next →

What is Load Average in Linux?

Leave a Reply

Your email address will not be published. Required fields are

marked.

Message *

Your comment will improve the progress of both of us ...

Name *

John Alphabet

Email *

john.alphabet@example

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Mari_Gh20

Publish in June 25, 2023 at 8:58 am

Reply

How do i modify sudoers file to add a user?

Ashley

Publish in June 26, 2023 at 11:56 am

Reply

You can either create a group that has access to sudo and then add the user to it, or you can directly edit the file using the visudo command. The

`username ALL= (ALL) NOPASSWD: ALL` line must be added at the end of the file when the visudo command opens it in the vi editor. This will grant the user sudo access without requiring a password. You can use the adduser command to create a new user.

Rosemah_K20

Publish in June 25, 2023 at 8:48 am

Reply

how to edit sudoers list in Linux

Ashley

Publish in June 25, 2023 at 1:14 pm

Reply

Press Ctrl + Alt + T to open a terminal and use the command `sudo visudo` to edit the sudoers file. Then, to add, change, or delete users and groups who have access to sudo, use the visudo syntax. Visudo will check for syntax mistakes and forbid concurrent editing.

Rufqa

Publish in June 25, 2023 at 7:15 am

Reply

where is sudoers file location in linux?

Ashley

Reply

Publish in June 26, 2023 at 5:45 am

The `/etc/sudoers` directory contains the sudoers file. It is a plain text file that lists the guidelines for the rights that a user may get by using the `sudo` command.

Zumar

Reply

Publish in June 25, 2023 at 7:14 am

how to add user to sudoers file?

Ashley

Reply

Publish in June 26, 2023 at 2:19 am

You have two options for adding a user to the sudoers file: either make a group that has access to sudo and include the user in that group, or manually modify the file using the visudo command. You must add a line at the end of the file that reads `username ALL=(ALL) NOPASSWD: ALL` after using the visudo command to open the file in the vi editor. The user will then have sudo access without a password. The adduser command1 can be used to create a new user.

Vikram2020

Publish in June 25, 2023 at 7:13 am

Reply

what do you enter at the command prompt to edit /etc/sudoers file?

Ashley

Publish in June 25, 2023 at 3:36 pm

Reply

The `/etc/sudoers` file can be edited with the `visudo` command. It is advised to use `visudo` to edit the sudoers file since it guarantees that only one user may edit sudoers at once and offers essential syntax checks12. Make changes to the `/etc/sudoers` file using the command: `sudo visudo -f /etc/sudoers`

Taseen

Publish in June 25, 2023 at 7:12 am

Reply

User is not in the sudoers file CentOS 7. how to solve this problem?

Ashley

Publish in June 25, 2023 at 1:12 pm

Reply

When a user is not a member of the sudo group, is not granted sudo access, or the sudoers file cannot be read,

the error message "User is not in the sudoers file" appears. You can fix this problem by giving the user sudo rights and adding them to the sudo group. The command `adduser username sudo` can be used to add a user to the sudo group.

search

Helpful

Let us know if you liked the post. That's the only way we can improve

Yes 0

No 0

Linux VPS

Pay for what you need with our scalable Linux VPS plans.

Get Linux VPS Now

OPERAVPS

As an advocate of environmental sustainability, OperaVPS is more than just a VPS provider. With their commitment to eco-friendly practices, OperaVPS delivers reliable hosting solutions while minimizing their environmental impact. Experience top-notch hosting services combined with a strong focus on environmental support at OperaVPS.

Product and Solution

VPS Server

Buy RDP

Linux VPS

Windows VPS

Windows 11 VPS

Debian VPS

More

Customer care

Knowledge Base

Contact Us

Submit Ticket

Terms and Conditions

Telephone: +44 74 1835 1231
Report abuse: abuse[at]operavps.com

UK: 47 Wharf Rd, London, N1 7GS

Turkey: 19 Mayis Mah, Saadet Hanim Sk 9, NO. 9/13 Istanbul 34363 COC Number: 0483-0785-6810-0001

SAFE AND SECURE PAYMENT