Running commands as superuser with sudo

Certain commands on SUSE Linux cannot be executed by the normal user but require administrator privileges. For administrative purposes, you can log in as `root` by using the **`sudo`** command to gain `root` privileges.

This article gives you an overview of the basic concepts of **`sudo`** and the most common use cases and commands that you need to run **`sudo`**. You will also learn how to configure the `sudoers` file and to troubleshoot.

WHAT

Learn about the basic concepts of **`sudo`** and how to use it as a normal user or system administrator.

WHY

Certain commands require administrator or `root` privileges. To log in as `root`, you can use the **`sudo`** command.

EFFORT

It takes you up to 20 minutes to read through this article. If you have a specific question, you can jump directly to the respective chapter.

GOAL

Understanding the basic concepts of **`sudo`** and how to use it. Running commands with **`sudo`** for certain use cases. Configuring the `sudoers` file and troubleshooting **`sudo`**.

REQUIREMENTS

- Basic understanding of `sudo`.
- `root` or `sudo` privileges. For more information, refer to *Section 1, “Basic concepts of* ***sudo****”*.
- The `sudo` package needs to be installed. This package is available on SUSE Linux by default.

Publication Date: 23 May 2023

Contents

1 Basic concepts of **sudo**

1.1 What is **sudo**?

sudo is an abbreviation for “super user do.” It is a Linux command that you can use to execute programs as a root user. **sudo** gives you elevated privileges when you want to run important commands. The root user is the Linux superuser and the equivalent to the administrator who has maximum permissions to do anything to the system. As a normal user on Linux, you have reduced permissions. For example, you cannot write to system directories. For security reasons, the normal user is separate from the root user. You must have root privileges to run commands which can only be executed by the root. The following options to log in as root are available:

- **su**: allows you to run a command as root but requires you to know the root password.
- **sudo**: allows you to run a command as root. Based on the configuration, the command does not require the root password.

Note: root vs. **sudo**

For security reasons and to avoid mistakes, it is not recommended to log in as root. With **sudo** you can log in as a normal user and execute commands with elevated privileges.

The **sudo** package is installed by on all SUSE Linux distributions by default.

2 Difference between **sudo** and **su**

Learn the difference between **sudo** and **su** commands.

You can execute single commands as root or another user, based on your settings in the /etc/sudoers file. The sudoers files are files that Linux administrators use to allocate system rights to the system users. This allows the administrator to control who does what. If you want to securely execute a command as a root user, you must always use the **sudo** command. The main difference between **sudo** and **su** commands is that **su** elevates privileges only during the shell session while **sudo** elevates privileges only for the specific command that you execute.

3 **sudo** configuration basics

Learn about the basic `sudoers` configuration settings before you start editing or creating your own **`sudo`** configuration files.

3.1 Basic `sudoers` configuration syntax

The `sudoers` configuration files contain two types of options: strings and flags. While strings can contain any value, flags can be turned either ON or OFF. The most important syntax constructs for `sudoers` configuration files are as follows:

```
# Everything on a line after # is ignored❶
Defaults !insults # Disable the insults flag❷
Defaults env_keep += "DISPLAY HOME" # Add DISPLAY and HOME to env_keep❸
tux ALL = NOPASSWD: /usr/bin/frobnicate, PASSWD: /usr/bin/journalctl❹
```

❶ There are two exceptions: `#include` and `#includedir` are regular commands.

❷ Remove the `!` character to set the desired flag to ON.

❸ Specify a list of environment variables that should be kept when `env_reset` is enabled.

❹ A complex rule that states that the user `tux` requires a password to run **`/usr/bin/journalctl`** and does not require one to run **`/usr/bin/frobnicate`** on all hosts.

USEFUL FLAGS AND OPTIONS

`targetpw`

If set, **`sudo`** prompts for the user password specified in the `-u` option or the `root` password, if `-u` is not used. The default is ON.

```
Defaults targetpw # Turn targetpw flag ON
```

`rootpw`

If set, **`sudo`** prompts for the `root` password. The default is OFF.

```
Defaults !rootpw # Turn rootpw flag OFF
```

`env_reset`

If set, **`sudo`** constructs a minimal environment with `TERM`, `PATH`, `HOME`, `MAIL`, `SHELL`, `LOGNAME`, `USER`, `USERNAME`, and `SUDO_*`. Additionally, variables listed in `env_keep` are imported from the calling environment. The default is ON.

```
Defaults env_reset # Turn env_reset flag ON
```

`env_keep`

The list of environment variables to keep when the `env_reset` flag is ON.

```
# Set env_keep to contain EDITOR and PROMPT
Defaults env_keep = "EDITOR PROMPT"
Defaults env_keep += "JRE_HOME" # Add JRE_HOME
Defaults env_keep -= "JRE_HOME" # Remove JRE_HOME
```

`env_delete`

The list of environment variables to remove when the `env_reset` flag is OFF.

```
# Set env_delete to contain EDITOR and PROMPT
Defaults env_delete = "EDITOR PROMPT"
Defaults env_delete += "JRE_HOME" # Add JRE_HOME
Defaults env_delete -= "JRE_HOME" # Remove JRE_HOME
```

3.2 Basic sudoers rules

Each rule follows the following scheme (`[]` marks optional parts):

```
#Who      Where         As whom      Tag                  What
User_List Host_List = [(User_List)] [NOPASSWD:|PASSWD:] Cmnd_List
```

SUDOERS RULE SYNTAX

`User_List`

One or several (separated by comma) identifiers: either a user name, a group in the format `%GROUPNAME`, or a user ID in the format `#UID`. Negation can be specified with the `!` prefix.

`Host_List`

One or several (separated by comma) identifiers: either a (fully qualified) host name or an IP address. Negation can be specified with the `!` prefix. `ALL` is a common choice for `Host_List`.

`NOPASSWD:|PASSWD:`

The user is not prompted for a password when running commands matching `Cmd_List` after `NOPASSWD:`.

`PASSWD:` is the default. It only needs to be specified when both `PASSWD:` and `NOPASSWD:` are on the same line:

```
tux ALL = PASSWD: /usr/bin/foo, NOPASSWD: /usr/bin/bar
```

`Cmnd_List`

One or several (separated by comma) specifiers: a path to an executable, followed by an optional allowed argument.

```
/usr/bin/foo     # Anything allowed
/usr/bin/foo bar # Only "/usr/bin/foo bar" allowed
/usr/bin/foo ""  # No arguments allowed
```

`ALL` can be used as `User_List`, `Host_List` and `Cmnd_List`.

3.3 Simplify sudoers using aliases

Administrators can avoid having to maintain a set of repetitive and individual rules by introducing aliases to group items. Their syntax is the same as the syntax of the rules. The following types of aliases are supported:

`User_Alias`

A list of user names

`Runas_Alias`

A group of users by UID

`Host_Alias`

A list of host names

`Cmnd_Alias`

A list of commands and directories, and aliases

Think of aliases as named lists of users, groups, commands and hosts. To illustrate the power of aliases, take this example:

```
Host_Alias    WEBSERVERS = www1, www2, www3❶
User_Alias    ADMINS = tux, wilber, suzanne❷
Cmnd_Alias    REBOOT = /sbin/halt, /sbin/reboot, /sbin/poweroff❸
ADMINS WEBSERVERS = REBOOT❹
```

❶ The three servers are grouped into one Host_Alias `WEBSERVERS`. You can use (fully qualified) host names or IP addresses.

❷ Similar to the hosts grouped above, group users or even groups of users (like `%wheel`) are listed here. Negation is achieved with the `!` prefix, as usual.

3. Specifies a group of commands that are used in the same context.
4. All aliases are wrapped into a single rule stating that all users specified by the `User_Alias` can execute the group of commands specified under `Cmnd_Alias` on all hosts named in `Host_Alias`.

In summary, aliases help administrators to keep `sudoers` lean and manageable (and therefore secure). If, for example, one of the users has left the company, you can delete this person's name from the `User_Alias` statement and any system group they belonged to just once instead of having to search for all rules including this particular user.

4 Maintaining **sudo** configuration files

The integrity of your system's **`sudo`** configuration is very important. Errors in these files can compromise your entire system. The **`visudo`** command provides a safe and secure way for an administrator to edit the **`sudo`** configuration.

Tip: Separate custom configurations from the main **sudo** policy file

The main policy configuration file for **`sudo`** is `/etc/sudoers`. This file is supplied by the system packages, and changes made to it may break updates. Therefore, create separate configuration files holding your custom settings under the `/etc/sudoers.d/` directory. These are pulled in by default by a directive in `/etc/sudoers`.

Settings in the custom configuration files under the `/etc/sudoers.d/` directory always take precedence over the same settings made in the global configuration file `/etc/sudoers`. The global configuration is read and applied first and the custom one after that.

4.1 Editing **sudo** configuration files with **visudo**

While it is possible to edit **`sudo`** configuration files with any editing tool, it is best practice to use **`visudo`** for this task. **`visudo`** provides a basic set of safety measures to make sure you do not lock yourself out of your system due to a broken **`sudo`** configuration. It checks for parse errors, provides basic integrity checks and locks the configuration file against simultaneous edits, either by someone else or you in another session. If you tried editing a locked configuration file, **`visudo`** would tell you to try again later.

By default, **`visudo`** uses **`vi`** as the underlying editor. To change this to, for example, **`nano`**, set the `EDITOR` environment variable:

```
> sudo EDITOR=/usr/bin/nano visudo -f /etc/sudoers.d/NAME
```

4.2 Creating custom sudo configuration files

To create a custom configuration file in the `/etc/sudoers.d/` directory, run **`visudo`** with the `-f` option and provide the name of your new configuration file:

```
> sudo visudo -f /etc/sudoers.d/01_custom_configuration
```

When naming your custom configuration files, remember the following general rules:

Use descriptive file names

Use file names that hint at what the configuration file does.

Do not use `~` and `.` in the file names

`sudo` interprets configuration file names containing `.` as provided or created by the package management rather than the system administrator and ignores them. The same applies to files that end in `~`. These are interpreted as being copies locked by an editing tool.

Make sure the configuration files are read in the correct order

The order in which any custom files under `/etc/sudoers.d/` are parsed determines how directives are carried out. If you have set one directive in a file parsed early in the process and the same one in another file that is parsed later, **`sudo`** processes the last read version. To determine the order in which your custom configurations are read, add numbering to your configuration files and use a consistent number of leading zeroes. For example, `01_myfirstconfig` is parsed before `10_myotherconfig`.

4.3 Checking sudo configurations with visudo

`visudo` performs a number of built-in checks to ensure your system's integrity.

A basic syntax check is run when you edit a **sudo** configuration file. In this example, the edit introduced an error:

```
> sudo visudo -f /etc/sudoers.d/01_test
[sudo] password for root:
visudo: /etc/sudoers.d/01_test:1:17: unknown defaults entry "insult"❶
What now?
Options are:
  (e)dit sudoers file again❷
  e(x)it without saving changes to sudoers file❸
  (Q)uit and save changes to sudoers file (DANGER!)❹

What now? e
```

❶ An error has been spotted. The file name, the line number and the type of error are given.

❷ Open the file in editing mode again and fix the error. If this option is selected, the file opens in edit mode again and the line containing the error is highlighted.

❸ Exit without applying the most recent change.

❹ Apply the changes and exit. This results in a malfunctioning or broken **sudo** configuration.

To run a check of your entire **sudo** configuration, run:

```
> sudo visudo -c
/etc/sudoers: parsed OK
/etc/sudoers.d/01_test: parsed OK
/etc/sudoers.d/02_test: parsed OK
/etc/sudoers.d/03_test: parsed OK
```

This tells you that all of your configuration files are syntactically correct and gives you the order in which the configurations are parsed. This information is needed in case you notice unexpected behavior of **sudo** which can simply be caused by directives being applied in the wrong order or overriding each other. If the configuration contains an error, **visudo** reports the file name, line number and error description of the affected file (see above).

4.4 For more information

For more information on `visudo`, refer to **man 8 visudo**.

5 Running a command prefaced with **sudo**

On Linux, certain commands require elevated privileges. Learn how a normal user can run any command as `root` by prefacing the command with **`sudo`**.

The execution of certain commands requires `root` privileges. The `root` account is a special account with unlimited privileges. Any user with access to the `root` password can gain this privileges and accidentally or maliciously break the system. Therefore it is not recommended to log in as `root`. A safer approach is logging in as a normal user and running the command prefaced with **`sudo`** to gain `root` privileges. This way, you also need to share the `root` credentials.

As a normal user, you can run any command as `root` by prefacing the command with **`sudo`**. After successful authentication with the `root` password, the command is executed with elevated privileges. The elevated privileges persist for a certain period of time, so you do not need to provide the `root` password again when running another **`sudo`**. The following example shows how to execute a command prefaced with **`sudo`**.

PROCEDURE 1: RUNNING A COMMAND PREFACED WITH **sudo**

1. To show the content of the `sudoers` file, enter the following command:

   ```
   > sudo cat /etc/sudoers
   ```

2. You are prompted to enter the `root` password. Note that the password is not shown during input, either as clear text or as masking characters.

   ```
   password for root:
   ```

3. After successful authentication, the `sudoers` file is displayed.
   If you do not have the required **`sudo`** privileges or you run the command not prefaced with **`sudo`**, the following message returns:

   ```
   cat: /etc/sudoers: Permission denied
   ```

You have run your first **`sudo`** command.

6 Starting a shell with `root` privileges

Start a shell with permanent `root` privileges by using the **`sudo -s`** or **`sudo -i`** command. With both commands, you are prompted for the `root` password only once.

6.1 Introduction

Having to enter **`sudo`** every time you want to run a command as `root` can become tedious. Instead, you can use one of the built-in mechanisms to start a shell with permanent `root` privileges. For this, there are two command options available:

- **`sudo -s`** launches the shell with the environment of the current user and offers a few privilege control measures. To run this command, you have to enter the `root` password.
- **`sudo -i`** starts the shell as an interactive login shell with a clean environment. To run this command, you must enter your user password. With this method, it is not needed to share the `root` credentials.

With both commands, the shell is started with a new environment, and you are logged in as superuser. Any subsequent command that is executed within that shell is run with elevated privileges without having to enter the password again. This environment is terminated when you close the shell, and you must enter the password again for another **`sudo`** command.

6.2 Starting a shell with **`sudo -s`**

The **`sudo -s`** command launches an interactive non-login shell. After successful authentication with the `root` password, all subsequent commands are executed with elevated privileges.

The `SHELL` environment variable or the user's default shell specifies which shell opens. If this variable is empty, the shell defined in the `/etc/passwd` is picked up.

By default, the **`sudo -s`** command runs from the directory of the previous user because the target user inherits the environment of the previous user. The command is also logged in your history.

To start a shell with permanently elevated privileges, enter the following command:

```
tux:~ > sudo -s
root's password:
```

```
root:/home/tux # exit
tux:~ >
```

The prompt changes from `>` to `#`.

You have started a shell with permanently elevated privileges. All subsequent commands are executed without prompting for the password again.

6.3 Starting a shell with **sudo -i**

The **`sudo -i`** is similar to the **`sudo -s`** command-line option but launches an interactive login shell. When using the **`sudo -s`** command, the target user inherits the environment of the previous user. You can prevent it by using the **`sudo -i`** command, where the target user gets a clean environment and starts at their own `$HOME` directory.

To run a command with **`sudo -i`**, enter the following:

```
tux:~ > sudo -i
root's password:
root:~ # exit
tux:~ >
```

You have started a shell with permanently elevated privileges, and the command is logged in your history. All subsequent commands are executed without prompting for the password again.

7 Changing the **sudo** password prompt time-out

Learn how to change the time-out settings to execute commands that require `root` privileges without being prompted for the `root` password for each command.

When running a command prefaced with **`sudo`** for the first time, you are prompted for the `root` password. This password remains valid for a certain period. Once it is expired, the user is prompted for the password again. To extend or shorten the time-out when executing commands that require `root` privileges, make the following changes to your **`sudo`** configuration file.

Note: Do not grant unlimited passwordless access to `root` privileges

For security reasons you should not give unlimited access to `root` privileges. Instead, set a reasonable time-out to prevent misuse of the `root` account by any intruder.

PROCEDURE 2: CHANGING THE TIME-OUT FOR **sudo** PASSWORD PROMPTS

1. Create a new `sudo` configuration file for the timestamp configuration with:

   ```
   sudo visudo --f=/etc/sudoers.d/timestamp_timeout
   ```

   After successful authentication with the `root` password, the file is opened.
   For more information on how to edit the `sudo` configuration file, refer to *Section 4, "Maintaining* ***sudo*** *configuration files"*.

2. Enable editing and add the line `timestamp_timeout=`. Enter a value for the timestamp. For example, to shorten the time-out to three minutes, enter:

   ```
   timestamp_timeout=3
   ```

   If the timestamp is set to zero, you are prompted for the `root` password for every execution of a `sudo` command.

3. Save the changes and close the file.

You have created a `sudo` configuration file and shortened the time-out setting for the execution of `sudo` commands.

8 Managing the `wheel` user group for **sudo** privileges

Members of the user group `wheel` have access to the `root` account and can receive unlimited privileges. Learn how to add a user to the `wheel` group.

The user group `wheel` is available on all SUSE Linux systems by default. The group settings are managed in the `sudoers` file, and the members of this group can run all commands with `sudo`. We recommend creating user groups for any administrative tasks where the users require elevated privileges instead of granting `sudo` access to individual users.

Note: Create specific user groups

Carefully think about adding users to a user group because not all users need full administrator privileges, for example, privileges for installing software. You can create specific user groups with only the required privileges and then assign certain users to such a group. For example, create a dedicated group for all users that install and manage software packages. If you are using the `wheel` user group, do not grant all `root` privileges to it. We recommend restricting **`sudo`** access to certain directories or files.

PROCEDURE 3: ADDING A USER TO THE `wheel` GROUP

1. Verify that the `wheel` group exists:

   ```
   > getent group wheel
   ```

   This returns, for example:

   ```
   wheel:x:476:
   ```

   If the previous command returned no result, install the `system-group-wheel` package that creates the `wheel` group:

   ```
   > sudo zypper install system-group-wheel
   ```

2. To add a user account to the `wheel` group, run the following command:

   ```
   > sudo usermod -a -G wheel USERNAME
   ```

   Enter the `root` password.

3. Log out and log in again from the terminal or close the current session to enable the change. Verify that the change was successful by running the following command:

   ```
   groups USERNAME
   ```

   This returns:

   ```
   USERNAME : users wheel
   ```

You have added a user account to the `wheel` user group.

9 Common `sudo` commands

By adding `sudo` before any command, you can run commands with elevated permissions. You can also run commands as another user and use their environment variables. Using `sudo` helps you accomplish system administration tasks without logging in as `root`.

9.1 Examples of `sudo` commands

This section provides examples of common commands that often require administrative privileges.

Run the last command with `sudo`

To repeat the last command as an administrator, run `sudo !!` and enter the password. For example, a user without administrative privileges cannot create a directory under the `/etc/` directory. To create it, run `sudo !!`.

```
> mkdir /etc/test/
mkdir: cannot create directory ‘/etc/test/’: Permission denied

> sudo !!
sudo mkdir /etc/test/
[sudo] password for root:

> ls -alrt /etc  | grep test
drwxr-xr-x 1 root root        0 Apr 20 12:48 test
```

Manage packages using `sudo` and `zypper`

To run package management commands as an administrator, add `sudo` before the command in the following format:

```
> sudo zypper [--GLOBAL-OPTIONS] <COMMAND> [--COMMAND-OPTIONS] [ARGUMENTS]
```

For example, to install the Docker CE containerization platform from its official package repository, run the following commands with `sudo`:

```
> sudo zypper addrepo https://download.docker.com/linux/suse/docker-ce

> sudo zypper refresh
> sudo zypper search docker-ce

> sudo zypper install docker-ce

> sudo systemctl enable docker

> sudo systemctl start docker
```

You do not need to add **sudo** before **zypper** commands that do not modify the system, or provide privileged access to information. For example, you can list the repositories for the installed software packages on your system without using **sudo**:

```
> zypper lr
```

Manage system services using sudo and systemctl

In systems that use **systemd** for managing services, you can use the **systemctl** with **sudo**. For example, to restart the Apache Web Server service, run the following command:

```
> sudo systemctl restart apache2
```

You do not need to add **sudo** before **systemctl** commands that do not modify the system, or provide privileged access to information. For example, you can display the status of Network Manager without using **sudo**:

```
> systemctl status NetworkManager
● NetworkManager.service - Network Manager
     Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vendor
 preset: disabled)
    Drop-In: /usr/lib/systemd/system/NetworkManager.service.d
             └─NetworkManager-ovs.conf
     Active: active (running) since DAY YYYY-MM-DD HH:MM:SS TIMEZONE; 1h 21min ago
       Docs: man:NetworkManager(8)
   Main PID: 1548 (NetworkManager)
      Tasks: 8 (limit: 4915)
     CGroup: /system.slice/NetworkManager.service
             ├─ 1548 /usr/sbin/NetworkManager --no-daemon
             ├─ 4304 /sbin/dhclient -d -q -sf /usr/lib/nm-dhcp-helper -
pf /run/NetworkManager/dhclient-wlan0.pid -lf /var/lib/NetworkManager/
dhclient-2acc1c75-018d-4909-b71
             ├─ 6379 /usr/lib/nm-openconnect-service --bus-name
 org.freedesktop.NetworkManager.openconnect.Connection_5
             └─ 6423 /usr/sbin/openconnect --servercert
 sha256:2ec361fcd88ce28ffb2b2f22a3431df49be0210a6f538893707f1041f05e42b3 --syslog --
cookie-on-stdin --script /usr/lib
```

Modify a user account using `sudo` and `usermod`

To run the **`usermod`** command for modifying user accounts, use the following format:

```
> sudo usermod [OPTION] USERNAME
```

For example, to set the number of days to `30` for permanently disabling the user account `tux` after password expiry, run the following command:

```
> sudo usermod --inactive 30 tux
```

Modify file and directory ownership using `sudo` and `chown`

To change file and directory ownerships from the current owner to a new owner, use the following format:

```
> sudo chown [OPTION] [OWNER:[GROUP]] FILE
```

For example, to give `tux` the ownership of files and subdirectories in the `/home/test/tux-files` directory, run the following command:

```
> sudo chown tux /home/test/tux-files/ --recursive
```

You can test the change in ownership by running the following command:

```
> ls -alrt /home/test/tux-files/ --recursive
```

Run a command as another user using `sudo -s`

Instead of using the **`su`** command for switching to a different user and then running commands, you can use the **`sudo -s`** command. A shell run by the **`sudo -s`** command inherits the environment of the current user. The **`sudo -s`** command also offers a few privilege control measures.

To run a command as a different user, use the following format:

```
> sudo -s -u USERNAME COMMAND
```

By default, the command runs from the directory of the previous user, because the target user inherits the environment of the previous user.

For example, to recursively list the files and subdirectories of the `/home/test/tux-files/` directory as the target user `tux`, run the following command:

```
> sudo -s -u tux ls -alrt /home/test/tux-files/ --recursive
```

When you use the **`sudo -s`** approach for running a command as a different user, the command is logged in your history.

Run a command as another user with a clean environment using `sudo -i`

When using the `sudo -s` command, the target user inherits the environment of the previous user. You can prevent it by using the `sudo -i` command, where the target user gets a clean environment and starts at their own `$HOME` directory.
To run a command as a different user with a clean environment, use the following format:

```
> sudo -i -u USERNAME COMMAND
```

The `sudo -i` command runs the shell as an interactive login shell of the target user. As a result, there are shell startup scripts such as `.profile` and `.bash_profile` files.
For example, to list the files and subdirectories of the `/home/test/tux-files/` directory as `tux`, run the following command:

```
> sudo -i -u tux ls -alrt /home/test/tux-files/
```

When you use the `sudo -i` approach for running a command as a different user, the command is logged in your history.

Display the current `sudo` settings using `sudo -V`

As a `root` user, you can display the current `sudo` settings for the entire system using the following commands:

```
> su -

> sudo -V
```

The output of the `sudo -V` command is lengthy, but contains information that is useful for system administrators. For example, the sample output below contains information about the time-outs and retry limits for `sudo` passwords.

```
...
Authentication timestamp timeout: 5.0 minutes
Password prompt timeout: 5.0 minutes
Number of tries to enter a password: 3
...
```

10 Troubleshooting

Learn how to debug and troubleshoot `sudo` configuration issues.

10.1 Custom configurations under `/etc/sudoers.d/` are ignored

The `#includedir` directive in `/etc/sudoers` ignores files that end with the `~` character or contain the `.` character. This is to avoid issues with configuration files provided by the package manager (containing `.`), or with an editor's temporary or backup files (ending in `~`). Make sure that the names of your custom configuration files neither contain nor end in these characters and rename them, if they do.

10.2 Custom directives conflict

The time when a **`sudo`** configuration directive is applied is determined by the order in which the respective configuration file is read. Directives in a file located under `/etc/sudoers.d/` take precedence over the same directives in `/etc/sudoers`. If custom directives stated in `/etc/sudoers.d/` do not work, check the order in which the files are read and fix it, if necessary.

To check the order in which the configurations are parsed, use the **`visudo -c`** command.

10.3 Locked out due to broken **sudo** configuration

If you have accidentally broken your system's **`sudo`** configuration and locked yourself out of **`sudo`**, use **`su -`** and the `root` password to start a root shell. Run **`visudo -c`** to check for errors and then fix them using **`visudo`**.

11 **sudo** best practices

Learn about some of the best practices of **`sudo`** to control system access and enable users to be productive.

Keep custom **`sudo`** configurations in separate files

The main policy configuration file for **`sudo`** is `/etc/sudoers`. This file is supplied by the system packages, and changes made to it may break updates. Therefore, create separate configuration files holding your custom settings under the `/etc/sudoers.d/` directory. These are pulled in by default by a directive in `/etc/sudoers`. For more information, refer to *Section 4.2, “Creating custom **sudo** configuration files”*.

Limit the `sudo` time-out

For security reasons you should not give unlimited access to `root` privileges. Instead, set a reasonable time-out instead to prevent misuse of the `root` account by any intruder. For more information, refer to *Section 7, "Changing the* **`sudo`** *password prompt time-out"*.

Use the `visudo` command

Use the **`visudo`** command to safely edit the `/etc/sudoers` file, as it checks the syntax of the file before saving the changes. This is a preventive way to correct any errors that can break the system. For more information, refer to *Section 4.1, "Editing* **`sudo`** *configuration files with* **`visudo`***"*

Manage users in groups rather than individually

Keep your **`sudo`** configuration as lean and manageable as possible. Manage users by adding them to groups and then granting privileges to these groups rather than to the individuals. This allows you to add or remove users by simply changing the group settings instead of having to look for the user across your configuration.

An example rule that allows all users in the `%wheel` group to execute all commands:

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

Limit access to `sudo` users

A good practice is to configure **`sudo`** to enable users to execute specific commands as required. For example, if there is a user or a group of users who need to install software, but do not need to perform any other task that requires elevated privileges, let your settings reflect that. The following rule allows tux to use any kind of software installation utility on SUSE Linux.

```
tux ALL = (ALL) PASSWD : /usr/bin/zypper, /usr/bin/rpm, /usr/bin/yast /usr/bin/yast2
```

Restrict the path for binaries

Restrict the areas where users can execute commands using the `secure_path` directive. The following example is the default setting that ships with SUSE Linux.

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

Keep `sudo` logging transparent

`sudo` logs to the standard log file where its log entries may easily get overlooked. Add the following rule to your configuration to specify a dedicated **`sudo`** log file.

```
Defaults logfile=/var/log/sudo.log
```

12 Legal Notice

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

A GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/ ↗.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.