Configuring Superuser Privileges with sudo

WHAT?

Get familiar with the basics of `sudo` configuration and learn how to delegate superuser privileges with `sudo`.

WHY?

Some commands require administrator or `root` privileges. Using `sudo`, you can delegate the privileges to execute these commands to certain users or groups.

EFFORT

It takes you up to 20 minutes to read through this article. Writing your first `sudo` configuration rule only takes a few minutes, but establishing a functioning `sudo` configuration that works across your environment will take considerably longer, depending on the complexity of your setup.

GOAL

Understand the basic aspects of `sudo` configuration. Address common use cases for `sudo` configuration. Learn how to work with users, user groups and aliases in `sudo` setups. Familiarize yourself with `sudo` best practices and troubleshooting.

REQUIREMENTS

- Basic understanding of **sudo**.
- `root` privileges. For information on how to use **sudo** as a normal user, refer to https://documentation.suse.com/smart/systems-management/html/sudo-run-commands-as-superuser/index.html.
- The `sudo` package needs to be installed.

Publication Date: 20 May 2024

Contents

1 An introduction to **sudo** configuration

`sudo` provides a means to securely and efficiently delegate superuser privileges to specific users or groups.

Certain operations on a Linux system require `root` or administrator privileges. Home users who administer their own system do not have to delegate superuser privileges, because the administrator and the normal user are the same person in this scenario. But as soon as a system is part of a larger systems environment with multiple users, groups and hosts, it becomes vital to maintain control of who is allowed to do what and where. At the same time, it is important to provide all users and groups with the necessary privileges to carry out their tasks.

`sudo` is designed to help with this. It provides:

Enhanced system security

> `sudo` offers fine-grained control over users, groups, hosts and commands and thus increases system security by reducing the risk of malicious or accidental damage by an intruder or a system user.

Complete audit trail

> Whenever a user switches privileges, this appears in the system's log, and all operations carried out by this user with elevated privileges can be traced back to them.

A means to delegate `root`-specific tasks

> Using `sudo`, system administrators can enable single users or groups to carry out certain tasks without the need to enter the `root` password and switch to the `root` account.

Important: How to read this article

This article provides in-depth `sudo` configuration information. However, it does not provide any advice on how to build a comprehensive and secure `sudo` policy. Security-related policies are very complex and strongly depend on the environment they are created for.

2 Creating custom **sudo** configurations

Learn how to build a simple example custom `sudo` configuration and expand it step by step. Create groups and use aliases to keep your custom configuration lean and efficient.

Warning: Example configurations are for demonstration purposes only

The example rules outlined below are purely for demonstration purposes. Use them to understand the general syntax of `sudo` configuration files. Do not use them in real-world setups, because they do not reflect the complexity of these environments.

2.1 `sudo` configuration best practices

Before your start, here are a few ground rules for maintaining `sudo` configurations:

Always use `visudo` to edit `sudo` configuration files

Any changes to the `sudo` configuration should be done using the `visudo` command. `visudo` is a tailor-made tool that allows you to edit the `sudo` configuration files and runs basic syntax checks, making sure that the configuration remains intact and functional. A faulty `sudo` configuration can result in a user being locked out of their own system.

Always create custom configurations under `/etc/sudoers.d/`

Custom configurations must reside under `/etc/sudoers.d/` to be pulled in by `sudo`. Settings in the custom configuration files take precedence over the ones in the default configuration in `/etc/sudoers`.

Always mind the order in which configurations are read

To make sure the custom configurations are read in the correct order, prefix them with numbers. Use leading zeroes to establish the order in which the files are read. For example, `01_myfirstconfig` is parsed before `10_myotherconfig`. If a directive has been set in a file that is read before another file that contains conflicting information, the last-read directive is applied.

Always use descriptive file names

Use file names that hint at what the configuration file does. This helps you keep track of what your `sudo` setup is supposed to do.

Tip: **sudo** configuration and immutable file systems

An immutable file system is a file system that cannot be changed once it has been installed. It is accessed read-only. If the SUSE product you are using relies on an immutable file system, the **`sudo`** default configuration shipped with the product is installed under `/usr/etc/sudoers` and any pre-configured adjustments reside under `/usr/etc/sudoers.d/`.

Your own custom configurations are located under `/etc/sudoers.d/` and take precedence over anything that is provided in `/usr/etc/sudoers.d/`. The **`visudo`** command opens `/usr/etc/sudoers` and saves the changed file to `/etc/sudoers`, if there was no prior `sudoers` file. If there was already one, **`visudo`** opens and writes that one. The instance located under `/etc/` takes precedence over the one that is kept under `/usr/etc/`. This way, user-made configuration adjustments will not get broken upon updates.

2.2 Create a user-specific configuration file

Create a **`sudo`** configuration file that allows a normal user (`tux`) to use the **`useradd`** command with their own password instead of the `root` password.

EXAMPLE 1: CREATE A USER-SPECIFIC CONFIGURATION FILE

1. As system administrator (`root`), create a custom configuration file that holds the new user-specific directives by starting **`visudo`**. Use both numbering and a descriptive name:

```
#
visudo -f /etc/sudoers.d/02_usermanagement
```

2. Create a rule that allows `tux` to execute the **`/usr/sbin/useradd`** binary in the entire environment that this **`sudo`** configuration is applied to:

```
tux❶ ALL❷ = /usr/sbin/useradd❸
```

❶ Specify the user or group. List users by name or `#UID`, and groups by `%GROUPNAME`. If you have several items here, separate them with commas. To negate entries, use `!`.

❷ Specify one or several (separated by commas) hosts. Use (fully qualified) host names or IP addresses. Add `ALL` to enforce this setting globally across all hosts. Use `!` for negations.

❸ Specify one or several executables (separated by commas). When specifying them, make sure to mind the following rules:

`/usr/sbin/useradd`

Without any additional options added, this allows the execution of every possible `useradd` command.

`/usr/sbin/useradd -c`

If you explicitly specify an option, then that option is the only one that is allowed. Nothing else would be available to the user you specified above.

`/usr/sbin/useradd ""`

This would just let the user invoke a mere `useradd` without any option at all.

In the example above, you would want to either allow all options and subcommands or limit them to a few for security reasons, but forbidding a user to specify any option at all would be pointless in this context.

3. To let the user use their own password instead of the `root` password, add the following line:

```
Defaults:tux !targetpw
```

When active, this flag requires the user to enter the password of the target user, i.e. `root`. This flag is enabled by default on any SUSE Linux Micro system. Negate it using `!` to require the user to just enter their own password instead of the `root` password.

4. Save the configuration, leave the editor and open a second shell to test whether `sudo` honors your new configuration.

2.3 Create custom configurations by grouping items

Modify the configuration from *Example 1, “Create a user-specific configuration file”* so that a group of named users can run the `useradd` command without the need for the `root` password. Also, add the `usermod` and `userdel` to the list of commands available to this group.

EXAMPLE 2: CREATE CUSTOM CONFIGURATIONS BY GROUPING ITEMS

1. To modify the example configuration, open it as system administrator with `visudo`:

```
               #
```

```
visudo /etc/sudoers.d/02_usermanagement
```

2. Add more users to the rule in a comma-separated list:

```
tux, wilber ALL = /usr/sbin/useradd
```

3. To allow the listed users to execute a list of commands, specify the commands as a comma-separated list:

```
tux, wilber ALL = /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/userdel
```

4. To let the listed users use their own password instead of the `root` password, add the following line:

```
Defaults:tux, wilber !targetpw
```

   When active, this flag requires the listed users to enter the password of the target user, i.e. `root`. This flag is enabled by default on any SUSE Linux Micro system. Negate it using `!` to require the listed users to just enter their own password instead of the `root` password.

5. Save the configuration, leave the editor and open a second shell to test whether **`sudo`** honors your new configuration.

2.4 Simplify configurations by applying aliases

Use aliases to simplify your custom configuration from *Example 2, "Create custom configurations by grouping items"* even further. Grouping items helps to a certain extent, but using global aliases for users, commands and hosts is the most efficient way to keep a clean and lean **`sudo`** configuration.

Using aliases and groups instead of lists is a much better way to address changes in your setup. Should a user leave, just remove them from the global `User_Alias` declaration in your alias declaration file instead of scouring all the separate custom configuration files. The same procedure applies for any other type of alias (`Host_Alias`, `Cmnd_Alias` and `Runas_Alias`).

EXAMPLE 3: SIMPLIFY CONFIGURATIONS BY APPLYING ALIASES

1. Create a new file to hold your global alias definitions:

```
#
visudo /etc/sudoers.d/01_aliases
```

2. Add the following line to create the `TEAMLEADERS` alias:

   ```
   User_Alias    TEAMLEADERS = tux, wilber
   ```

3. Add the following line to create the `USERMANAGEMENT` alias:

   ```
   Cmnd_Alias    USERMANAGEMENT = /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/
   userdel
   ```

4. Save your changes and exit **`visudo`**.

5. As system administrator, start **`visudo`** to edit the example configuration file:

   ```
   #
   visudo -f /etc/sudoers.d/02_usermanagement
   ```

6. Delete the previous rule and replace it with the following rule that uses the aliases you have just defined above:

   ```
   TEAMLEADERS ALL = USERMANAGEMENT
   ```

7. To let all the users defined by `User_Alias` use their own password instead of the `root` password, add the following line:

   ```
   Defaults:TEAMLEADERS !targetpw
   ```

8. Save the configuration, leave the editor and open a second shell to test whether **`sudo`** honors your new configuration.

Note: For more information

Find a more detailed description of the **`sudo`** configuration syntax in *Section 7, “**sudo** configuration reference”* and refer to the man page of **`sudo`**.

3 Changing the **sudo** password prompt timeout

Learn how to change the timeout 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 timeout when executing commands that require `root` privileges, make the following changes to your `sudo` configuration file.

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

For security reasons, do not give unlimited access to `root` privileges. Instead, set a reasonable timeout to prevent misuse of the `root` account by any intruder.

PROCEDURE 1: CHANGING THE TIMEOUT FOR **sudo** PASSWORD PROMPTS

1. As system administrator, create a new `sudo` configuration file for the timestamp configuration with:

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

   After successful authentication with the `root` password, the file is opened.

2. Enable editing and add the line `timestamp_timeout=`. Enter a value for the timestamp. For example, to shorten the timeout 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 timeout setting for the execution of `sudo` commands.

4 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.

4.1 Difference between `sudo -s` and `sudo -i`

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, enter the `root` password.
- `sudo -i` starts the shell as an interactive login shell with a clean environment. To run this command, you enter the `root` password.

With both commands, the shell is started with a new environment, and you are logged in as `root`. 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.

4.2 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
[sudo] password for root:
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.

4.3 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
[sudo] password for root:
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.

5 sudo best practices

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

Thoroughly test and audit your `sudo` configurations

To build a truly efficient and secure `sudo` configuration framework, establish a routine of regular testing and auditing. Identify possible loopholes and deal with them. Do not let convenience trump security.

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`.

Limit the `sudo` timeout

For security reasons, do not give unlimited access to `root` privileges. Instead, set a reasonable timeout instead to prevent misuse of the `root` account by any intruder. For more information, refer to *Section 3, “Changing the* **sudo** *password prompt timeout”*.

Use the **visudo** command

Use the **visudo** command to safely edit the `/etc/sudoers` file, because 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. Besides the basic syntax check, you can also run **visudo -c** to check whether your entire framework of **sudo** configuration is parsed in the right order and without an error.

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 an example `%admingrp` group to execute all commands:

```
%admingrp ALL = (ALL) ALL
```

Restrict the path for binaries

With the `secure_path` directive, restrict the areas where users can execute commands. The following example is the default setting that ships with SUSE Linux Micro.

```
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
```

6 Troubleshooting

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

6.1 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. If they do, rename them.

6.2 Custom directives conflict

The order in which the configuration files are read determines when a **`sudo`** configuration directive is applied. 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 using **`visudo -c`**. Adjust the order, if necessary.

6.3 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`**.

7 **sudo** configuration reference

This section provides a basic **`sudo`** configuration reference that helps you understand and maintain both default and custom **`sudo`** configurations.

7.1 `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 ignored ❶
Defaults !insults # Disable the insults flag ❷
Defaults env_keep += "DISPLAY HOME" # Add DISPLAY and HOME to env_keep3
tux ALL = NOPASSWD: /usr/bin/frobnicate, PASSWD: /usr/bin/journalctl4
```

1. There are two exceptions: `#include` and `#includedir` are regular commands. The more current version does not use the `#` anymore. Instead, include directives are now preceded by `@`. The `#` notation is still supported for backward compatibility reasons.
2. Remove the `!` character to set the desired flag to ON.
3. Specify a list of environment variables that should be kept when `env_reset` is enabled.
4. 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
```

7.2 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 identifiers (separated by commas): 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 identifiers (separated by commas): 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 specifiers (separated by commas): 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`.

7.3 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.

❸ Specifies a group of commands that are used in the same context.

❹ 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.

8 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 https://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.