Linux Audit Quick Start

SUSE Linux Enterprise 11 SP2

Linux audit allows you to comprehensively log and track access to files, directories, and resources of your system, as well as trace system calls. It enables you to monitor your system for application misbehavior or code malfunctions. By creating a sophisticated set of rules including file watches and system call auditing, you can make sure that any violation of your security policies is noted and properly addressed.

To set up Linux audit on your system, proceed as follows:

1 Stop the default audit daemon with the `rcauditd stop` command.

2 Adjust the system configuration for audit and enable audit.

3 Configure the audit daemon.

4 Determine which system components to audit and set up audit rules.

5 Optionally configure plugin applications you intend to use with the audit dispatcher.

6 Start the audit daemon after you have completed the configuration of the audit system using the `rcauditd start` command.

7 Determine which reports to run and configure these reports.

8 Analyze the audit logs and reports.

9 (Optional) Analyze individual system calls with autrace.

IMPORTANT: Users Entitled to Work with Audit

The audit tools, configuration files, and logs are only available to `root`. This protects audit from ordinary users of the system. To manipulate any aspect of audit, you must be logged in as `root`.

---

1 Enabling Audit

Your first task for enabling audit is to activate system call auditing, since system call auditing capabilities are needed even when you are only configuring plain file or directory watches:

Enabling System Call Auditing for One Session Only

Enable with `auditctl -e 1` and disable with `auditctl -e 0`. These settings
are valid for the current session only, and do not survive a reboot.

Enabling System Call Auditing Permanently

Permanently enable audit contexts for system calls by changing
`AUDITD_DISABLE_CONTEXTS` in `/etc/sysconfig/auditd` from `yes` to
`no`. To permanently disable audit contexts for system calls, revert this setting to
`yes`. This configuration will be applied with the next start of the audit daemon.

2 Configuring Audit

The configuration of the audit daemon is contained in the `/etc/audit/auditd`
`.conf` configuration file. The default settings as shipped with SUSE Linux Enterprise
should be sufficient for most setups.

```
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 4
disp_qos = lossy
dispatcher = /usr/sbin/audispd
name_format = NONE
#name = mydomain
max_log_file = 5
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
#tcp_listen_port =
tcp_listen_queue = 5
#tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
```

Most of the settings in this file apply the audit log files and how the logging is done.
The most important settings apply to the actions the daemon should take when encoun-
tering certain critical conditions or errors (system low on disk space, system out of disk

space, or disk error) and when to warn the administrator about these conditions. These actions are customizable and range from a mere warning in syslog to a complete halt of the system. For more information about `/etc/audit/auditd.conf`, refer to *The Linux Audit Framework* manual and the manual page of `auditd.conf` (`man 5 auditd.conf`).

3 Setting Up Audit Rules

Audit rules are used to specify which components of your system are audited. There are three basic types of audit rules:

- Basic audit system parameters

- File and directory watches

- System call audits

Before creating an audit rule set and before rolling it out to your system, carefully determine which components to audit. Extensive auditing causes a substantial logging load. Make sure that your system provides enough disk space to store large audit logs and test your audit rule set extensively before rolling it out to production.

Audit rules can either be passed to the audit system by the command line using `auditctl` or bundled into a rules file located under `/etc/audit/audit.rules` that is read during the start of the audit daemon:

```
# basic audit system parameters
-D
-b 8192
-f 1
-e 1

# some file and directory watches
-w /var/log/audit/
-w /etc/audit/auditd.conf -p rxwa
-w /etc/audit/audit.rules -p rxwa

-w /etc/passwd -p rwxa
-w /etc/sysconfig/

# an example system call rule
-a entry,always -S umask
```

The basic audit system parameters include a rule to delete any preexisting rules (-D) (to avoid clashes with the new rules), a rule that sets the number of outstanding audit buffers (-b), the failure flag (-f), and the enable flag (-e):

-b

> Depending on the audit load of your system, increase or decrease the number of outstanding audit buffers. If there are no more buffers left, the kernel checks the failure flag for action.

-f

> The failure flag controls the kernel's reaction to critical errors. Possible values are 0 (silent), 1 (printk, print a failure message), and 2 (panic, bring the system down—no clean shutdown and risk of data loss or corruption).

-e

> If set to 1, this enables audit and audit contexts for system calls. Setting it to 2 does the same, but also locks down the configuration. Set to 0, audit is disabled. This flag is used to enable or disable audit temporarily.

File system watches can be added whenever you want to track files or directories for unauthorized access. Typical examples would include watching the audit configuration and logs and user and security databases. Use permission filtering to focus on those system calls requesting the permissions in which you are interested:

```
-w /etc/audit/audit.rules -p rxwa
```

The -p flag enables permission filtering. This example has permission filtering turned on for read, write, execute, and attribute change permissions.

Note the following limitations to file system watches:

- Directory watches produce less verbose logs than exact file watches. When in need of detailed file-related records, enable separate file watches for all files of interest.

- Pathname globbing of any kind is not supported by audit. Always use the exact pathnames.

- Auditing can only be performed on existing files. Any files added while the audit daemon is already running are ignored until the audit rule set is updated to watch the new files.

Assigning keys to your audit rules helps you to identify any records related to this rule in the logs. An example rule plus key:

```
-w /var/log/audit/ -k LOG_audit
```

The `-k` option attaches a text string to any event that is recorded in the logs due to this rule. Using the `ausearch` log analyzer, you can easily filter for any events related to this particular rule.

A sample system call audit rule could look like the following:

```
-a entry,always -S umask
```

This adds the rule to the system call entry list (`-a`) and logs an event whenever this system call is used (`entry,always`). The `-S` option precedes the actual system call, `umask` in this example. Using `-F`, you could add optional filtering to this rule. For more information about audit rules, refer to *The Linux Audit Framework* and the manual page of `auditctl` (`auditctl(8)`).

4 Generating Reports

Every audit event is recorded in the audit log, `/var/log/audit/audit.log`. To avoid having to read the raw audit log, configure custom audit reports with aureport and run them regularly. Use the aureport tool to create various types of reports filtering for different fields of the audit records in the log. The output of any `aureport` command is printed in column format and can easily be piped to other commands for further processing. Because the aureport commands are scriptable, you can easily create custom report scripts to run at certain intervals to gather the audit information for you.

`aureport --summary`
> Run this report to get a rough overview of the current audit statistics (events, logins, processes, etc.). To get detailed information about any of the event categories listed, run individual reports for the event type.

`aureport --success`
> Run this report to get statistics of successful events on your system. This report includes the same event categories as the summary report. To get detailed information for a particular event type, run the individual report adding the `--success`

option to filter for successful events of this type, for example, `aureport -f --success` to display all successful file-related events.

`aureport --failed`
Run this report to get statistics of failed events on your system. This report includes the same event categories as the summary report. To get detailed information for a particular event type, run the individual report adding the `--failed` option to filter for failed events of this type, such as `aureport -f --failed` to display all failed file-related events.

`aureport -l`
Run this command to generate a numbered list of all login-related events. The report includes date, time, audit ID, host and terminal used, as well as name of the executable, success or failure of the attempt, and an event ID.

`aureport -p`
Run this report to generate a numbered list of all process-related events. This command generates a numbered list of all process events including date, time, process ID, name of the executable, system call, audit ID, and event number.

`aureport -f`
Run this report to generate a numbered list of all file-related events. This command generates a numbered list of all process events including date, time, process ID, name of the executable, system call, audit ID and event number.

`aureport -u`
Run this report to find out which users are running what executables on your system. This command generates a numbered list of all user-related events including date, time, audit ID, terminal used, host, name of the executable, and an event ID.

Use the `-ts` and `-te` (for start time and end time) options with any of the above commands to limit your reports to a certain time frame. Use the `-i` option with any of these commands to transform numeric entities to human-readable text. The following command creates a file report for the time between 8 am and 5:30 pm on the current day and converts numeric entries to text.

```
aureport -ts 8:00 -te 17:30 -f -i
```

5 Analyzing Audit Log Files and Reports

While aureport helps you generate custom reports focusing on a certain area, ausearch helps you find the detailed log entry of individual events:

`ausearch -a` *`audit_event_id`*
> Run this search to view all records carrying a particular audit event ID. Each audit event message is logged, along with a message ID consisting of a UNIX epoch time stamp plus a unique event ID, separated by a colon. All events that are logged from one application's system call have the same event ID. For example, use `ausearch -a 1234` to display all audit events carrying this audit event ID. As one application's system call may trigger several events to be logged, you are likely to retrieve more than one record from the log.

`ausearch -ul` *`login_id`*
> Run this search to view records associated with a particular login user ID. It displays any records related to the user login ID specified, provided that user had been able to log in successfully. For example, use `ausearch -ul root` to list all processes owned by the given login user ID.

`ausearch -k` *`key`*
> Run this search to find records that contain a certain key assigned in the audit rule set. For example, use `ausearch -k CFG_etc` to display any records containing the `CFG_etc` key.

`ausearch -m` *`message_type`*
> Run this search to find records related to a particular message type. Examples of valid message types include `PATH`, `SYSCALL`, `USER_LOGIN`. Invoking `ausearch -m` without a message type displays a list of all message types.

`ausearch -f` *`filename`*
> Run this search to find records containing a certain filename. For example, run `ausearch -f /foo/bar` for all records related to the `/foo/bar` file. Using the filename alone would work as well, but using relative paths would not.

```
ausearch -p process_id
```
> Run this to search for records related to a certain process ID. For example, use `ausearch -p 13368` to search for all records related to this process ID.

Use the `-ts` and `-te` (start time and end time) options with any of these commands to limit your reports to a certain time frame. Use the `-i` option with any of these to transform numeric entities to human readable text. The following command searches for any file event related to `audit.log` that took place any time between 8 am and 5:30 pm on the current day and converts numeric entries to text.

```
ausearch -ts 8:00 -te 17:30 -f audit.log -i
```

6 Analyzing Individual System Calls

Perform dedicated audits of individual processes using the autrace command. autrace works similarly to the strace command, but gathers slightly different information. The output of autrace is written to `/var/log/audit/audit.log` and does not look any different from the standard audit log entries.

When performing an autrace on a process, make sure that any audit rules are purged from the queue to avoid having these rules clash with the ones that autrace adds. Delete the audit rules with the `auditctl -D` command.

```
autrace /usr/bin/less /etc/sysconfig/auditd

Waiting to execute: /usr/bin/less
Cleaning up...
No rules
Trace complete. You can locate the records
with 'ausearch -i -p 7642'
```

Always use the full path to the executable with autrace. After the trace is complete, autrace provides you with the event ID of the trace, so you can analyze the entire data trail with ausearch. To restore the audit system to use the audit rule set again, just restart the audit daemon by calling `rcauditd restart`.

7 Audit Tool Set

`auditctl`
>   Controls the audit system. Check the audit daemon's status and rule set, delete rules, or create new ones.

`aureport`
>   Create various types of reports from the audit daemon logs.

`ausearch`
>   Create custom queries to search the audit daemon logs.

`autrace`
>   Add audit rules to trace a process. Similar to `strace`.

`rcauditd`
>   Controls the audit init script.

8 Files

`/etc/audit/auditd.conf`
>   Contains configuration options specific to the audit daemon, such as log file location, log rotation, maximum size of the log file, and various actions to be taken when the system starts to run low on disk space.

`/etc/sysconfig/auditd`
>   Controls configuration aspects of auditd that are not covered in `/etc/audit/auditd.conf`, such as the locale to use with audit, the use of audit contexts with system calls, and if rules and watches should be deleted on shutdown of the system.

`/etc/audit/audit.rules`
>   Controls the rules auditd processes to track system calls and file and directory access.

`/var/log/audit/audit.log`
>   The audit log file.

9 For More Information

For a more detailed introduction to the Linux audit framework, refer to the *The Linux Audit Framework* manual that is available at `http://www.suse.com/documentation/sles11/http://www.suse.com/documentation/sled11/`.

10 Legal Notice

GNU Free Documentation License

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.

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.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, 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.

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.

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.

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".

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.

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.

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.

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.

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

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
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.