

Operating System Security Hardening Guide for SAP HANA for SUSE Linux Enterprise Server 15 SP2 and later

SUSE Linux Enterprise Server for SAP Applications 15 SP2 and later

Soeren Schmidt, SAP Solution Architect (SUSE)
Markus Guertler, Senior Manager SAP Technology Team (SUSE)
Alexander Bergmann, Security Engineer (SUSE)

Operating System Security Hardening Guide for SAP HANA for SUSE Linux Enterprise Server 15 SP2 and later

Date: 2024-11-07

This document guides through various hardening methods for SUSE® Linux Enterprise Server for SAP Applications to run SAP HANA.

Disclaimer: Documents published as part of the SUSE Best Practices series have been contributed voluntarily by SUSE employees and third parties. They are meant to serve as examples of how particular actions can be performed. They have been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. SUSE cannot verify that actions described in these documents do what is claimed or whether actions described have unintended consequences. SUSE LLC, its affiliates, the authors, and the translators may not be held liable for possible errors or the consequences thereof.

Contents

- 1 Introduction 4
- 2 SAP HANA firewall 9
- 3 SUSE Remote Disk Encryption 16
- 4 Minimal operating system package selection 17
- 5 Security updates 19
- 6 Outlook 22
- 7 About the authors 22
- 8 Further information and references 22
- 9 Documentation updates 23
- 10 Legal notice 25
- 11 GNU Free Documentation License 26

1 Introduction

IT security is an essential topic for any organization. Newspapers report frequently about new IT security incidents such as hacked websites, successful Denial-of-Service attacks, or stolen user data like passwords, bank account numbers and other sensitive data.

In addition to the publicly reported attacks, there are also a large number of incidents that are not reported to the public. In particular, these cases are often related to espionage, where the affected party has no interest to report an incident. Security experts agree that, for protecting sensitive data, an organization must have a comprehensive security concept in place, taking all eventualities into account that can potentially lead into security risks. This starts with proper setup policies, like password and data protection policies for users and system administrators. It continues with a protected IT environment using for example firewalls, VPNs, and SSL in communication protocols. And it ends with hardened servers, intrusion detection systems, data encrypting and automated security reporting. Additionally, many organizations perform security audits on a regular basis to ensure a maximum of security in their IT environment.

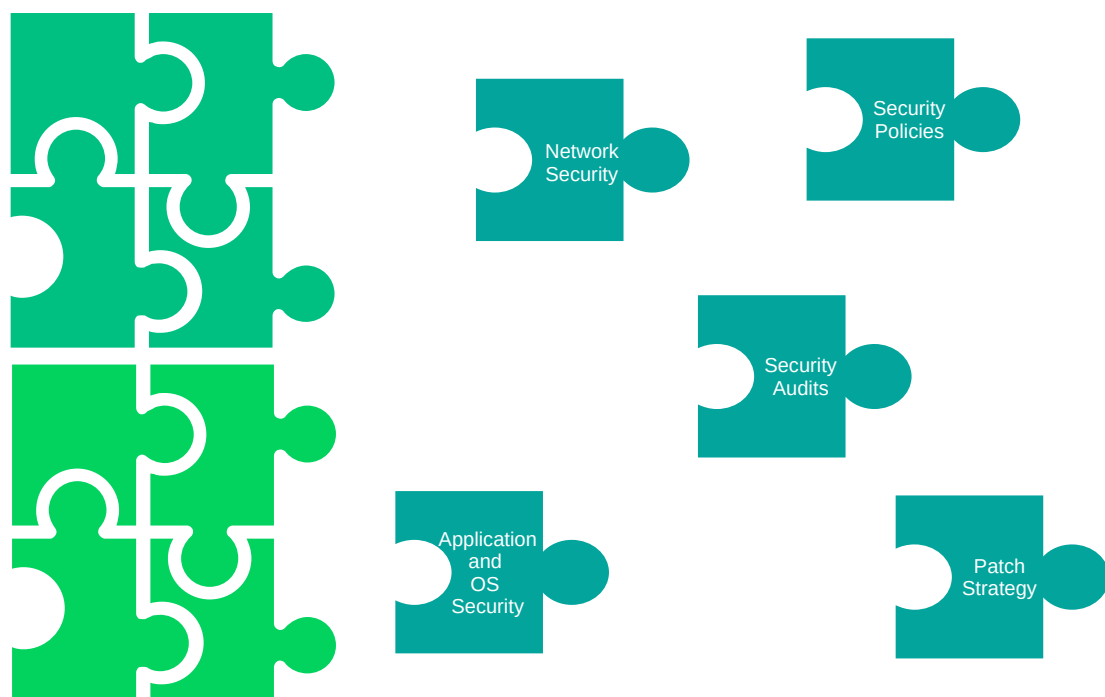


FIGURE 1: ELEMENTS OF A CORPORATE IT SECURITY

Comprehensive security concepts usually pay high attention to database systems, since databases belong to the most critical components in any IT environment. Database systems that potentially store sensitive data are by nature very popular targets for hackers and must therefore be protected. SAP HANA systems typically store business related information and are considered as being business critical. This is especially the case for ERP systems using SAP HANA. In addition, many other SAP applications using SAP HANA, like BW systems, may store sensitive data.

1.1 Security for SAP HANA

SAP takes the security topic very seriously. For SAP HANA, there is a comprehensive [SAP HANA Security Guide \(https://help.sap.com/doc/eec734dbb0fd1014a61590fcb5411390/2.0.05/en-US/SAP_HANA_Security_Guide_en.pdf\)](https://help.sap.com/doc/eec734dbb0fd1014a61590fcb5411390/2.0.05/en-US/SAP_HANA_Security_Guide_en.pdf) available. This guide describes in detail how to protect HANA from a database perspective. The guide also refers to security concepts for other connecting layers that are separate from the SAP HANA system, for example the network and storage layer. However, these topics are described only generically. There is no specific guidance on how to apply these recommendations on the operating system level.

1.2 Security for SUSE Linux Enterprise Server

The security of the underlying operating system is at least as important as the security of the SAP HANA database. Many hacker attacks target the operating system to gain access and sufficient privileges to attack the running database application. SUSE Linux Enterprise Server is the recommended and supported operating system for SAP HANA. SUSE has a long-running history in IT security for Linux operating systems. The company offers a comprehensive security package for SUSE Linux Enterprise Server to protect systems from all kind of security incidents. This package consists of the following components:

Security certifications

Both SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 15 have been awarded many important security certifications, such as the FIPS (Federal Information Processing Standard) 140-2 validation, or the Common Criteria EAL4+ certificate. For details visit <https://www.suse.com/support/security/certifications/>.

Security updates and patches

SUSE constantly provides security updates and patches for their SUSE Linux Enterprise operating systems and guarantees highest security standards during the entire product life cycle.

Documentation

SUSE has published a Hardening Guide and a Security Guide that describe the security concepts and features of SUSE Linux Enterprise Server 15. These guides provide generic security and hardening information valid for all workloads, not just for SAP HANA. For more details visit:

- <https://documentation.suse.com/sles/15-SP2/html/SLES-all/book-hardening.html> ↗
- <https://documentation.suse.com/sles/15-SP2/html/SLES-all/book-security.html> ↗

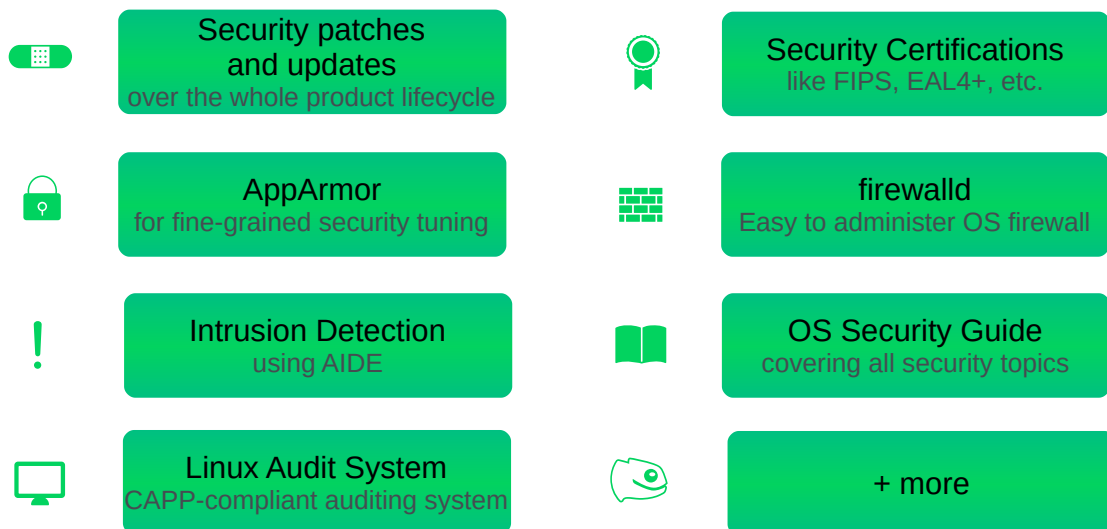


FIGURE 2: SECURITY COMPONENTS OF SUSE LINUX ENTERPRISE SERVER

1.3 About this document

To further improve the security level specifically for SAP HANA, SUSE provides the document at hand. It focuses on the security hardening of SUSE Linux Enterprise Server 15 running SAP HANA databases to fill the gap between the Security Guide for SUSE Linux Enterprise Server, the Hardening Guide for SUSE Linux Enterprise Server, and the SAP HANA Security Guide. The Hardening Guide for SUSE Linux Enterprise Server contains some of the recommendations found here, but also additional recommendations. Most of the recommendations can be applied to an SAP HANA installation after careful review and testing. SUSE collaborated with a large pilot customer to identify all relevant security settings and to avoid problems in real world scenarios. Also, SUSE and SAP are constantly cooperating in the SAP Linux Lab to provide the best compatibility with SAP HANA.



FIGURE 3: THE FIVE MAIN TOPICS OF THE OS SECURITY HARDENING FOR HANA

The guide at hand provides detailed descriptions on the following topics:

Security hardening settings for SAP HANA systems

The Linux operating system provides many tweaks and settings to further improve the operating system security and the security for the hosted applications. To be able to fit for certain application workloads, the default settings are not tuned for maximum security. This guide describes how to tune the operating system for maximum security when running SAP HANA specifically. In addition, it describes possible impacts, for example on system administration, and gives a prioritization of each setting.

Local firewall for SAP HANA

SUSE has developed a dedicated local firewall for SAP HANA systems to improve the network security of SAP HANA. This is done by only selectively opening network ports on external network interfaces that are really needed either by SAP HANA or other services. All remaining network ports are closed. The firewall has a broad range of features and is easy to configure. It is available as RPM package and can be downloaded from SUSE.

Remote Disk Encryption

Starting with SUSE Linux Enterprise Server for SAP Applications 12 SP2, SUSE introduced a new feature called **Remote Disk Encryption**. Classical Disk Encryption - available for years – always required a passphrase being entered during boot. That prevented its use in many setups because each boot needed a manual step. Remote Disk Encryption removes this manual step as it allows the encryption keys to be stored safely on a remote key server and to be automatically used during system boot.

Minimal package selection

The fewer operating system packages an SAP HANA system has installed, the less possible security holes it should have. Following that principle, this guide describes which packages are absolutely necessary and which packages can be safely discarded. As a positive side effect, a minimized number of packages also reduces the number of updates and patches that have to be applied to a system.

Security updates & patches

Open source software is frequently reviewed and tested for security vulnerabilities by open source developers, security engineers from the open source community, security companies and, of course, by the hackers. When a vulnerability has been found and reported, it is published in security advisories and usually gets fixed very quickly. SUSE constantly provides security updates and patches for all supported packages on SUSE Linux Enterprise

Server. This chapter explains which update and patch strategies are the best. It also details how to configure SUSE Linux Enterprise Server to frequently receive all relevant security updates.

In short, this guide covers all important topics in detail that are relevant for the operating system hardening of an SAP HANA system. Combining them with the other security features of SUSE Linux Enterprise Server 15, like the security certifications and the constantly provided security updates and patches, SAP HANA can run in a highly secure environment. This ensures that the implementation meets the security standards and corporate security concepts required by organizations of all sizes.

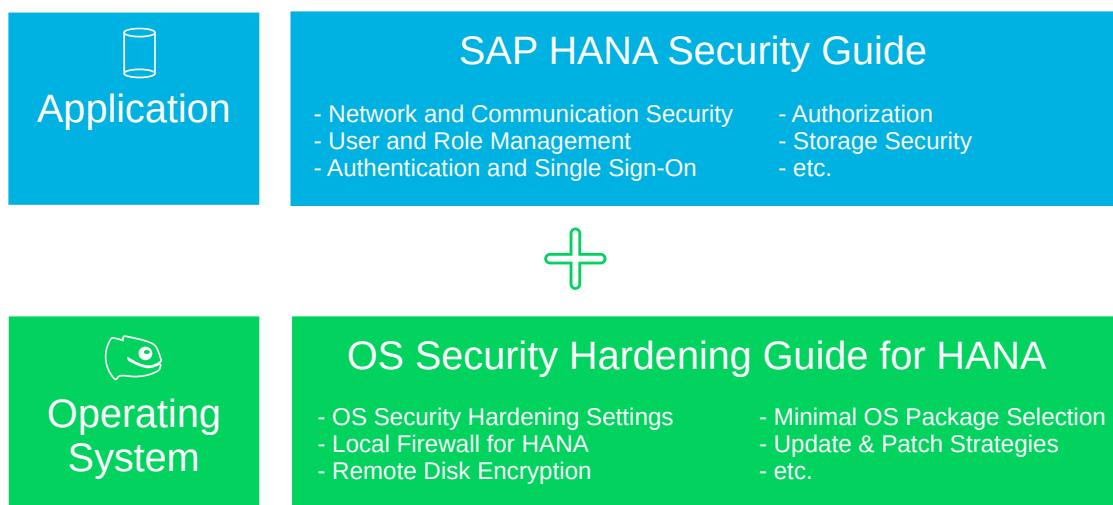


FIGURE 4: SAP HANA AND OPERATING SYSTEM SECURITY

2 SAP HANA firewall

2.1 SAP HANA network communication



Note

The SAP HANA firewall currently only includes rules for IPv4.

The section "Network Security" of the SAP HANA Security Guide (<https://help.sap.com>) recommends that different components of the SAP HANA database should operate in different network zones. Also, the network communication should be restrictively filtered to follow a minimal communication approach.

In practice, this results in segmenting the network communication of certain SAP HANA components into multiple dedicated IP networks (ISO/OSI Layer 3). The SAP HANA system is connected with exactly one interface to each IP network. Typically, these interfaces are logical bonding interfaces that include two or more physical interfaces for redundancy. The physical interfaces are connected to separated Ethernet network segments (ISO/OSI Layer 2).

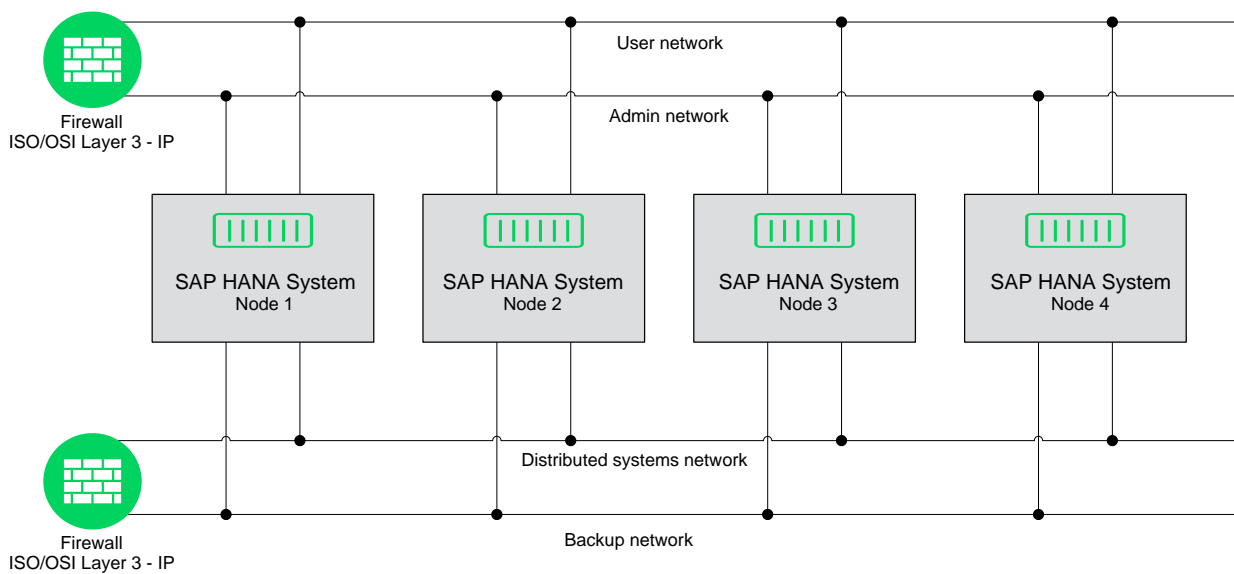


FIGURE 5: EXAMPLE OF A SAP HANA NETWORK DIAGRAM WITH EXTERNAL FIREWALLS

All SAP HANA networks should be either isolated (this means distributed system networks), or if they require communication from other networks (this means user communication), they should be behind an external firewall. This external firewall should only allow traffic for a SAP HANA network that is required for the communication with the SAP HANA services that are listening on this network.

In some cases an external firewall cannot be provided, or certain networks are shared between many servers but not just SAP HANA database systems. In these case, a local running firewall can take over some of the functionalities of an external firewall.

2.2 Local firewall for SAP HANA

The security of an SAP HANA database can be further improved by configuring a locally running firewall. This firewall should only allow network communication on ports where HANA services or other required system services are listening. Communication to all other ports should be dropped and optionally be logged. This complies with the “minimal communication approach” suggested in the SAP HANA Security Guide.

SUSE developed a dedicated local firewall for SAP HANA, based on Linux [iptables](#). This firewall takes all requirements from typical SAP HANA systems into account.

The firewall provides the following features:

- Predefined SAP HANA services definitions (according to the SAP HANA Master Guide)
- Protection of multiple SAP HANA instances running on one server
- Interface / service mappings for an unlimited number of interfaces
- Possibility to directly use service definitions from `/etc/services`
- Option to restrict access to services to certain source networks
- Simulating option that prints the [iptables](#) commands to the console instead of executing them (What if...)

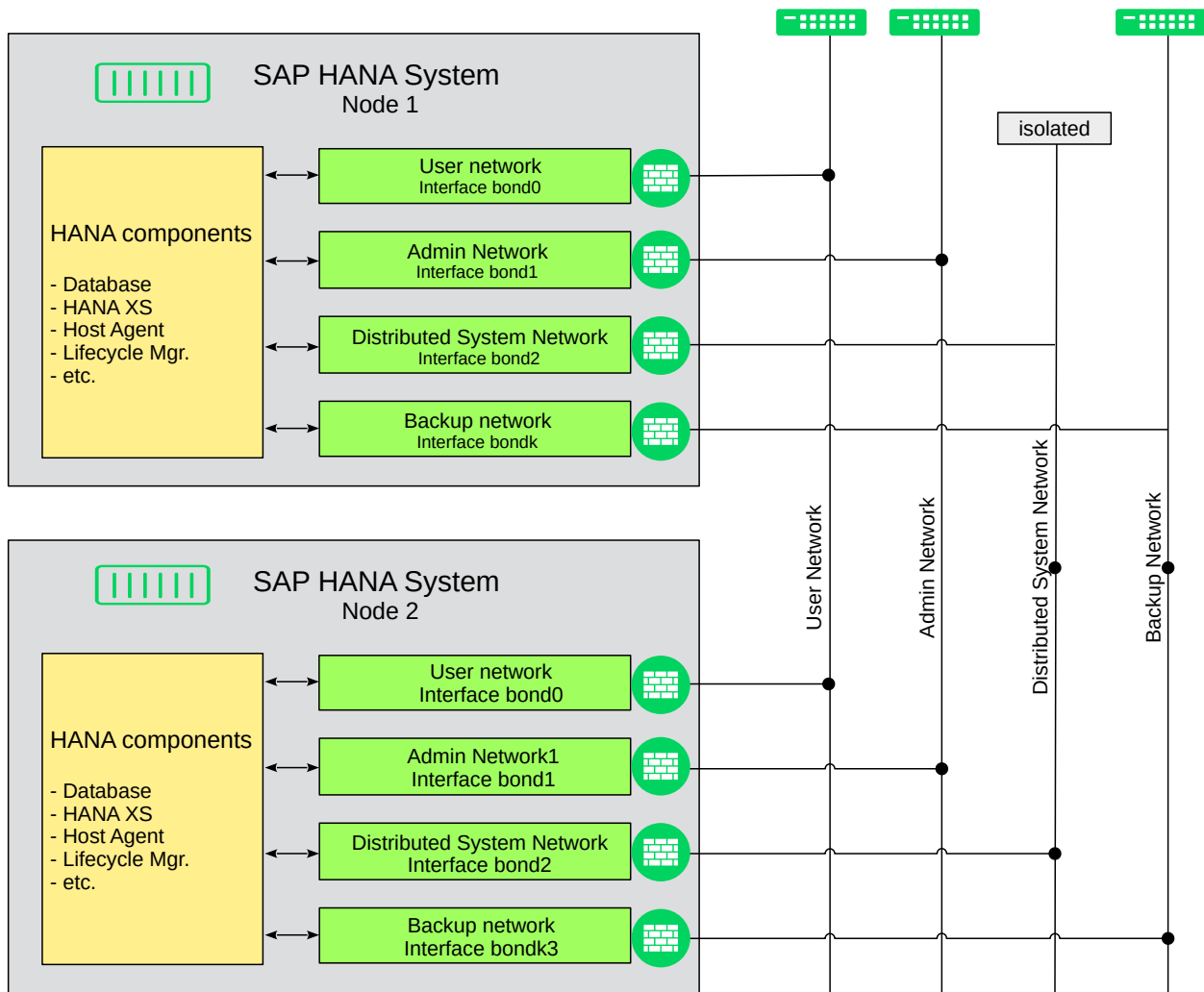


FIGURE 6: EXAMPLE OF A SAP HANA FIREWALL NETWORK DIAGRAM

Not every scenario requires having a dedicated local firewall on the SAP HANA servers. For example, if all SAP HANA networks are behind a properly configured external firewall, a local firewall is not necessarily required.

However, in some cases it helps to improve the network security. It can even improve network debugging capabilities (→ logging of dropped packets). The most common cases for running a local firewall are:

- when an external firewall is not available to protect non-isolated SAP HANA networks from other networks (e.g. user network).
- when an external firewall can not be configured restrictively enough to only allow network communication for particular SAP HANA ports for certain SAP HANA networks.

- when an external firewall provides not enough security zones.
- when a protected network contains many different servers, such as non-SAP servers, in the same network.

There are several other reasons why a local firewall could make sense. For example, a local firewall prevents unwanted services or daemons listening TCP or UDP ports and receiving connections. That is because all not specifically allowed network ports are blocked by default. Also, unauthorized network traffic received on blocked ports can be logged. This allows to easily identify unwanted connection attempts. Last but not least, a local firewall can be a set requirement by corporate security policies or security audits.

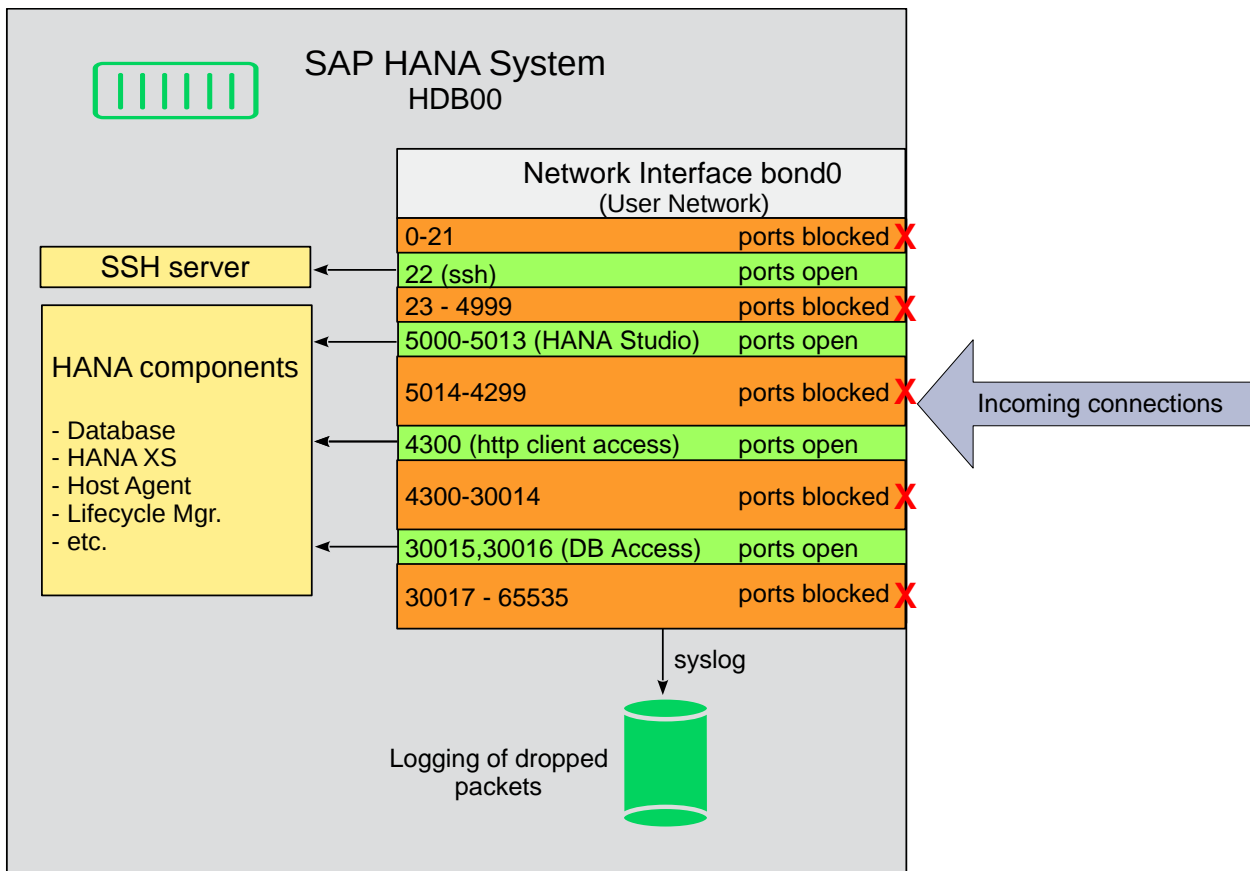


FIGURE 7: EXAMPLE OF A SAP HANA FIREWALL NETWORK TRAFFIC FLOW (PORTS ARE EXEMPLARY)

2.3 Installation

The SAP HANA firewall is available from the repositories for SUSE Linux Enterprise Server for SAP Applications 15 and extends `firewalld` by adding rulesets.

```
zypper install HANA-Firewall
```

The package installs the following files:

<u>/usr/sbin/hana-firewall</u>	Firewall executable. A usage description can be printed with the command: <u>/usr/sbin/hana-firewall --help</u>
<u>/etc/hana-firewall/</u>	Main configuration file
<u>/etc/sysconfig/hana-firewall</u>	Directory for HANA services and user defined services
<u>/usr/share/man/man8/hana-firewall-1.8.gz</u>	Man page for the HANA firewall

2.4 Configuration

With SUSE Linux Enterprise Server 15, firewalld replaces SUSE Firewall2, and HANA-Firewall is now an integral part. To get familiar with firewalld, refer to the SUSE Linux Enterprise Server 15 Security Guide, section 18.4 "firewalld" at https://www.suse.com/documentation/sles-15/singlehtml/book_security/book_security.html#sec.security.firewall.firewalld.



Important

Before setting up the SAP HANA firewall, you first need to configure firewalld for all non-SAP related services like SSH.

To configure the SAP HANA firewall, follow the respective instructions detailed in the SUSE Linux Enterprise Server for SAP Applications Guide, section [Configuring HANA-Firewall](https://www.suse.com/documentation/sles-for-sap-15/singlehtml/book_s4s/book_s4s.html#sec.s4s.configure.firewall-hana) (https://www.suse.com/documentation/sles-for-sap-15/singlehtml/book_s4s/book_s4s.html#sec.s4s.configure.firewall-hana).



Tip

It is recommended to use the YaST HANA-Firewall module. There is no simple way to do this on the command line.

2.5 Services

2.5.1 Service definitions

A service is a named definition of TCP or UDP ports used by a specific network service. Common services are defined in `/etc/services`. For an easier configuration of the firewall, additional services are provided by the package, or can even be created manually. The HANA Firewall service definitions are stored in the directory `/etc/hana-firewall/`. Each file defines one service and allows to define a list of ports or port ranges for TCP and UDP.

2.5.2 Predefined services

The SAP HANA Administrators Guide and the SAP HANA Security Guide describe all services and the required TCP/UDP ports that SAP HANA uses. These services can also be found in the tabular overview "TCP/IP Ports of All SAP Products" at <https://help.sap.com/viewer/ports>. Most of these services are available as predefined services in the HANA-Firewall module:

TABLE 1: LIST OF SHIPPED SAP HANA SERVICE DEFINITIONS (HANA-FIREWALL 1.1.5)

Service Name	Description
<u>HANA cockpit</u>	More information may be found in the SAP knowledge base article 2389709.
<u>HANA database client access</u>	Provide access to system database and all tenant databases.
<u>HANA data provisioning</u>	Event streaming via SQLDBC (ODBC/JDBC) protocol.
<u>HANA HTTP client access</u>	Allow web browser access to HANA.
<u>HANA distributed systems</u>	Internal network communication for multi-host (distributed) installation.
<u>HANA system replication</u>	Internal network communication for system replication for both single and multi container setup.

Service Name	Description
<u>HANA studio lifecycle manager</u>	Allow connection to HANA lifecycle manager via host agent.
<u>Software provisioning manager</u>	The port 4237 will allow web browsers to access software provisioning web UI remotely.
<u>HANA special support</u>	The ports should be used in rare technical support scenarios. See HANA administration guide for more details.

2.5.3 User-defined services

To create a new service, run:

```
hana-firewall define-new-hana-service
```

Follow the instructions on the screen. After the service has been created, you have to generate the XML files:

```
hana-firewall generate-firewalld-services
```

Now the service should appear in the YaST HANA-Firewall module and can be assigned.

Testing and activation ~~~~~ After the firewall has been configured, it should carefully be tested. After that, make sure that the firewall is started on system boot automatically:

```
systemctl enable firewalld.service
```



Warning

Ensure there is no other non-SUSE firewall enabled that might start automatically.

3 SUSE Remote Disk Encryption

All data processed by SAP HANA can contain sensitive information that need to be protected. Depending on the version the data volume, redoing log files or database backups can be encrypted by the SAP HANA itself. For details consult the SAP HANA Security Guide at <https://help.sap.com>.

If the internal encryption of SAP HANA should not or cannot be used, you can encrypt directories containing sensitive data via Remote Disk Encrypting available in SUSE Linux Enterprise Server for SAP Applications. When using the internal encryption, the various encryption keys are stored on disk in the SSFS which is located by default in `<home-of-sidadm>/hdb/<host-identity>/SSFS_HDB.DAT`. The SSFS itself is encrypted with the SSFS master key, normally located in `$DIR_GLOBAL/hdb/security/ssfs/`, which is protected only by file permissions. To protect this key or the SSFS Remote Disk Encrypting can help to reach higher security. It will not store any key of SAP HANA directly, but can encrypt the part of the file system where the keys are located.

SUSE Remote Disk Encryption uses block devices as an encrypted container for arbitrary directories. It allows to store the encryption keys safely on a remote key server. To mount the device, the host contacts the key server on a TLS secured connection to retrieve the necessary keys automatically to unlock the data. Clearly the key server should be a dedicated, security-hardened, and protected system, since anyone with access to this system can retrieve the keys and decrypt the data.

The setup of client and server is described in more detail in the SUSE Linux Enterprise Server for SAP Applications guide, section 10 Encrypting Directories Using `cryptctl` at <https://www.suse.com/documentation/sles-for-sap-15/>.

4 Minimal operating system package selection

4.1 Background

A typical Linux installation has many files that are potentially security-relevant. This is especially true for binary files and executables. Also, every running service might potentially be vulnerable to a local or remote attack. Therefore it is recommended to have as less files (binaries, executables, configuration files) as possible installed and as few services as possible running.

SUSE Linux Enterprise Server provides an RPM package for each logical component, like a Linux application, a service or a library. An RPM package groups all files, including executables, other binaries, configuration files and documentation files, that belong to this particular component. The most common packages are grouped by use cases as 'Installation Patterns'. These patterns can be selected during the operating system installation or later via YaST to easily get an installation that fits the requirements of a particular use case, for example for an SAP server with development tools.

Reducing the number of installed RPM packages to a minimum lowers the amount of potentially vulnerable files on the system. This significantly improves the overall security of a system. Furthermore, a low number of installed packages reduces the number of required (security) updates and patches that have to be applied to the system on a regular basis. SAP HANA is a very complex application, shipped in different versions, and having many additional components, which makes it hard to choose the minimal list of packages.

4.2 Required installation patterns and packages

The required software for SAP HANA is described in 'SUSE Linux Enterprise Server 15.x for SAP Applications Configuration Guide for SAP HANA' attached to SAP note '1944799 - SAP HANA Guidelines for SLES Operating System Installation' and lists the necessary patterns.

The recommendation is to install the system with the role "Minimal" (pattern "Base System"). Then add the patterns "Enhanced Base System" (which pulls in the patterns "AppArmor", "Software Management" and "YaST System Administration") and "SAP Application Server Base". The pattern "X Window System" should be installed only if needed. This results in a total amount of 746 packages, or 941 package if "X Window System" has been installed.

For SSL support, the SAPCRYPTOLIB (SAP package) and the SAR archiver tool should be installed in addition.

In some rare cases, the support might ask for the installation of additional packages. Therefore, we generally recommend to have SUSE Linux Enterprise Server update repositories configured on your HANA system to be able to quickly install new packages.

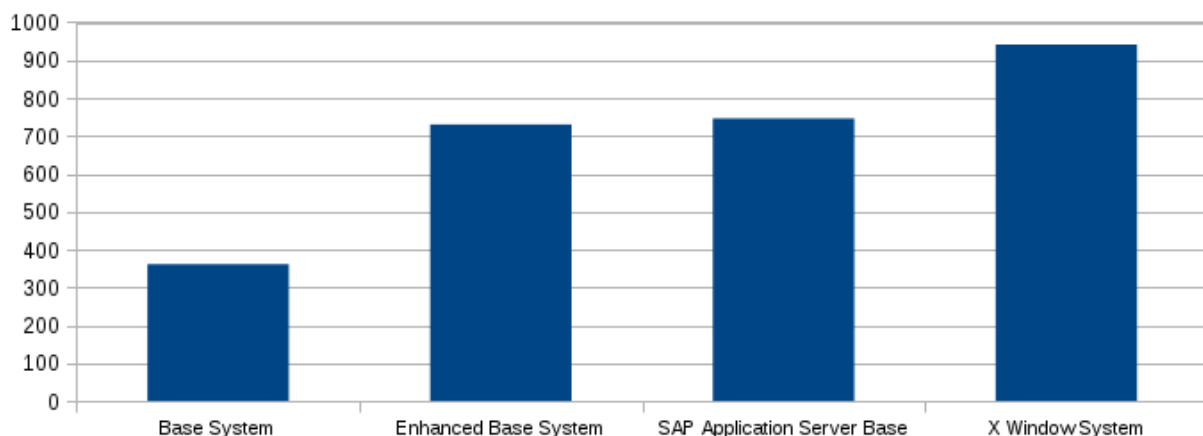


FIGURE 8: COMPARISON OF THE AMOUNT OF INSTALLED PACKAGES BETWEEN CERTAIN PACKAGE SELECTIONS

5 Security updates

5.1 Security updates for SUSE Linux Enterprise Server 15

No different from commercial software, open source software is tested by hackers and security experts for vulnerabilities. Also, it can contain programming errors. These facts may result in security risks. As soon as newly found security vulnerabilities are reported, for example on security mailing-lists or by security advisories, the affected code usually gets fixed quickly – sometimes even within hours. This is usually done either by the authors of the affected application, by security experts in the community, or by the Linux distributors.

For SUSE Linux Enterprise Server, the resulting security patches are quickly incorporated into the corresponding software package and published as security updates through our update channels. As soon as they are available there, they can be downloaded by all SUSE Linux Enterprise Server customers, and should be applied immediately.

5.2 SUSE Linux Enterprise Server update channels

To receive security updates (and other updated packages) on SAP HANA systems, the SUSE update channels must be configured properly. Usually SAP HANA systems do not have direct access to the Internet. This requires an update proxy between the corporate network and the Internet. Thus SUSE provides the Subscription Management Tool (SMT) or Repository Mirroring Tool (RMT), or SUSE Manager.

To verify that your HANA system has been configured properly to receive updates, check if it has been registered to the SUSE update channels:

```
zypper lr
```

This command lists the available software repositories of a SUSE Linux Enterprise Server instance. The output should show the update channels for all enabled modules of the particular Service Pack.

There are many ways to install new patches and also to selectively install just the security updates. The most common way to install only security updates is to execute the following commands:

```
zypper ref # Refreshes the update sources
zypper patch -g security # Install security patches only
```

5.3 Update and patch strategies

In many cases, organizations have corporate policies in place that describe requirements regarding updates and patches for their Linux servers.

The following overview describes some of the most common update and patch strategies, and their advantages and disadvantages.

5.3.1 Installing all new updates and patches on a regular basis

Description

This strategy promotes the installation of new updates and patches for example once a day or once per week, either manually by a system administrator or using automatic update tools like YOU (YaST Online Update) or SUSE Manager. Since SUSE does not implement any new features between Service Packs, the installation of updates and patches (including security updates) is usually uncritical for a system. However, in some rare cases, updates might cause problems and can compromise the stability of a system.

Advantages

The System is always up-to-date and latest security updates are applied quickly. This makes a system very secure.

Disadvantages

In some rare cases, updates and patches might cause problems. Also, some updates (for example kernel updates) require a reboot.

Recommendation

This is a good strategy for all non-productive HANA systems, but not for systems that are in production.

5.3.2 Installing all new updates and patches during maintenance windows

Description

This strategy is very similar to the last one, but it ensures that a SAP HANA system is out of production or tagged with a limited availability during the update cycle. This is a very commonly used strategy for systems running large databases.

Advantages

Problematic updates will not put a productive SAP HANA system into danger.

Disadvantages

Since maintenance windows usually have longer time frames in between (for example once a month), systems might not be up-to-date from a security perspective.

Recommendation

This is only a good strategy if important security updates are installed outside of the usual maintenance windows.

5.3.3 Selectively installing new updates and patches

Description

A selective installation of patches and updates, for example of security updates only, further reduces the probability of installing problematic updates. This strategy is frequently combined with updating systems on a regular basis. The selective installation of packages can be performed using zypper, YaST or SUSE Manager.

Advantages

The system is mostly up-to-date with (almost) all security patches installed.

Disadvantages

Selecting packages has to be done manually and creates recurring effort, if one of the filters provided by zypper (for example cve number, category, severity) cannot be used.

Recommendation

This is probably the best update strategy, but also the most complicated one.



Tip

An important issue with updates in most cases is the reboot and the involved downtime. Some kernel updates are shipped as live patches and do not require a reboot anymore. More details can be found in the SUSE Linux Enterprise Server 15 Administration Guide, section 8 Live Kernel Patching with KLP.

5.3.4 Not updating

Description

A system is not registered to the SUSE update channels and no updates are applied.

Advantages: This has only disadvantages.

Disadvantages

Constantly increasing number of known security vulnerabilities make the system an ideal target for hacker attacks.


Recommendation

We strongly recommend to subscribe to the SUSE update channels and to install at least security-updates on a regular basis.

Which update strategy fits best for the SAP HANA systems in an organization heavily depends on the corporate updating & patching policies / guidelines. It also depends on the requirements of a particular SAP HANA system. For important SAP HANA systems, a more conservative update strategy should be chosen. For test systems, updates might even be applied automatically, for example by using YOU (YaST Online Update), on a regular basis.

6 Outlook

Even though this guide already covers most security hardening topics, we are planning to provide further improvements. Also, later versions of SAP HANA might have changed, or new requirements regarding the hardening settings, the firewall or the minimal package selection might apply in future. It is planned to incorporate these new requirements as soon as they occur.

We recommend to check for updated versions of this document from time to time at the SUSE documentation pages at <https://documentation.suse.com> .

7 About the authors

This document has been developed by Markus Guertler (Architect & Technical Manager, SAP Linux Lab), Soeren Schmidt (Solutions Architect, SAP Linux Lab) and Alexander Bergmann (Software Security Engineer, SUSE Maintenance & Security team).

8 Further information and references

The following table provides an overview of sources for further information regarding the discussed topics in this guide.

SUSE Security Portal	http://www.suse.com/security ↗
SUSE Linux Enterprise Server Security Guide	https://www.suse.com/documentation/sles-15/singlehtml/book_hardening/book_hardening.html ↗
SAP HANA Security Guide	http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf ↗
SAP HANA Master Guide	http://help.sap.com/hana/SAP_HANA_Master_Guide_en.pdf ↗
SAP HANA Guidelines for SLES Operating System Installation	SAP note 1944799
SUSE Linux Enterprise Server 15: Installation Note	SAP note 2578899

If you have any questions, comments or feedback on this document, do not hesitate to contact us under the email address [saphana@suse.de \(mailto:saphana@suse.de\)](mailto:saphana@suse.de) ↗.

9 Documentation updates

This chapter lists content changes for this document since its first release.

v1.3

- Removed the entire chapter "SUSE Linux Enterprise Security Hardening Settings for HANA" which content became part of the "Security and Hardening Guide" (15 SP3 and onwards). Also changed the title to reflect this.

v1.2

- Removed the following chapters (content was moved to the official Hardening Guide for SUSE Linux Enterprise Server):
 - "Allow root login only via the first local console (tty1)"
 - "Prohibit login as root via ssh"
 - "2.2.11 Set default inactive time to 1"
- Added comment about x86/Power and GUI on top of "SUSE Linux Enterprise Security Hardening Settings for HANA"

v1.1

- Removed obsolete comment about SAP Note 1944799 in "Further Information & References"
- Reworked "Set default inactive time to 1 day"
- Added comment about x86/Power and GUI on top of "SUSE Linux Enterprise Security Hardening Settings for HANA"
- Added missing SAP Note 1944799

10 Legal notice

Copyright © 2006–2024 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled "GNU Free Documentation License".

SUSE, the SUSE logo and YaST are registered trademarks of SUSE LLC in the United States and other countries. For SUSE trademarks, see <https://www.suse.com/company/legal/>.

Linux is a registered trademark of Linus Torvalds. All other names or trademarks mentioned in this document may be trademarks or registered trademarks of their respective owners.

Documents published as part of the SUSE Best Practices series have been contributed voluntarily by SUSE employees and third parties. They are meant to serve as examples of how particular actions can be performed. They have been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. SUSE cannot verify that actions described in these documents do what is claimed or whether actions described have unintended consequences. SUSE LLC, its affiliates, the authors, and the translators may not be held liable for possible errors or the consequences thereof.

Below we draw your attention to the license under which the articles are published.

11 GNU Free Documentation License

Copyright © 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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 noncommercially. Secondly, 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 in order 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 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.

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.