SUSE

SUSE Best Practices

SAP

Operating System Security Hardening Guide for SAP HANA for SUSE Linux Enterprise Server 12

SUSE Linux Enterprise Server for SAP Applications 12
SAP HANA

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

SUSE

Operating System Security Hardening Guide for SAP HANA for SUSE Linux Enterprise Server 12

Date: 2024-11-14

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

Contents

1 Introduction

IT security is an essential topic for any organization. Newspapers report frequently about new IT security incidents like hacked websites, successful Denial-of-Service attacks, 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, 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.

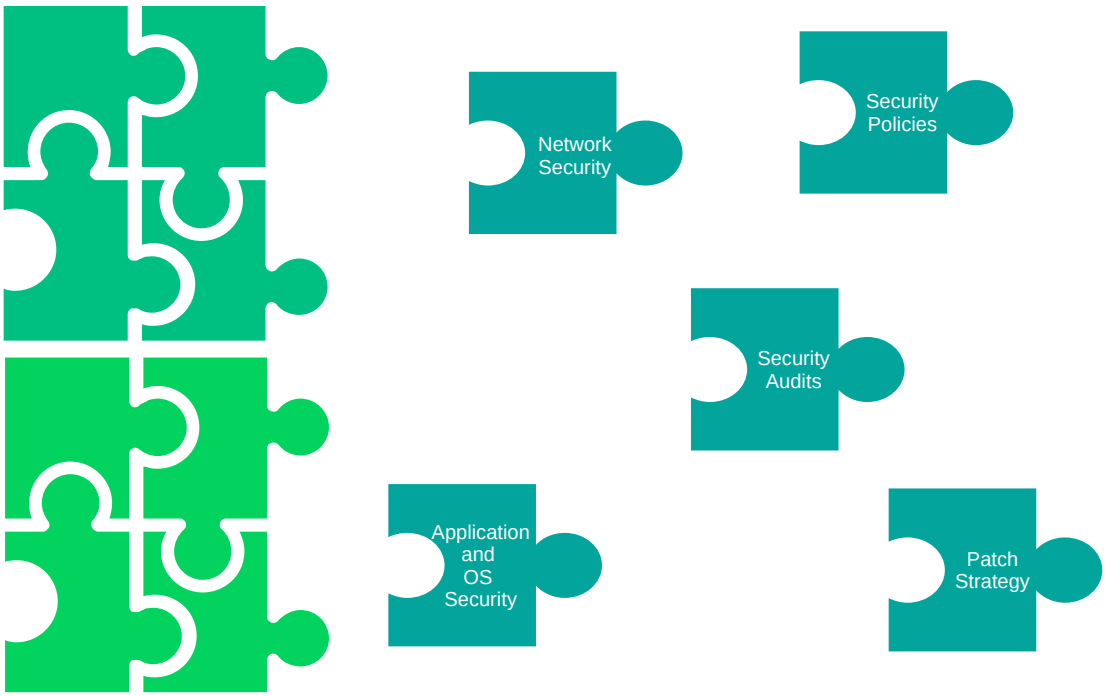

FIGURE 1: ELEMENTS OF A CORPORATE IT SECURITY

Comprehensive security concepts usually pay high attention to database systems, since databases belong to the most critical pieces 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 considered as being business critical. This is especially the case for ERP systems using SAP HANA. Also many other SAP applications using SAP HANA, like BW systems, may also 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) 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 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 on 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 the SUSE Linux Enterprise Server to protect systems from all kind of security incidents. This package consists of the following components:

Security certifications

SUSE Linux Enterprise Server 12 has been awarded many important security certifications, such as the FIPS (Federal Information Processing Standard) 140-2 validation or the Common Criteria Security EAL4+ certificate. For details please 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 over the whole product life cycle.

Documentation

SUSE has published a security guide that describes the security concepts and features of SUSE Linux Enterprise Server 12. This security guide provides generic security information valid for all workloads, not just for SAP HANA. For more detailed information, see https://www.suse.com/documentation/sles-12/singlehtml/book_hardening/book_hardening.html.

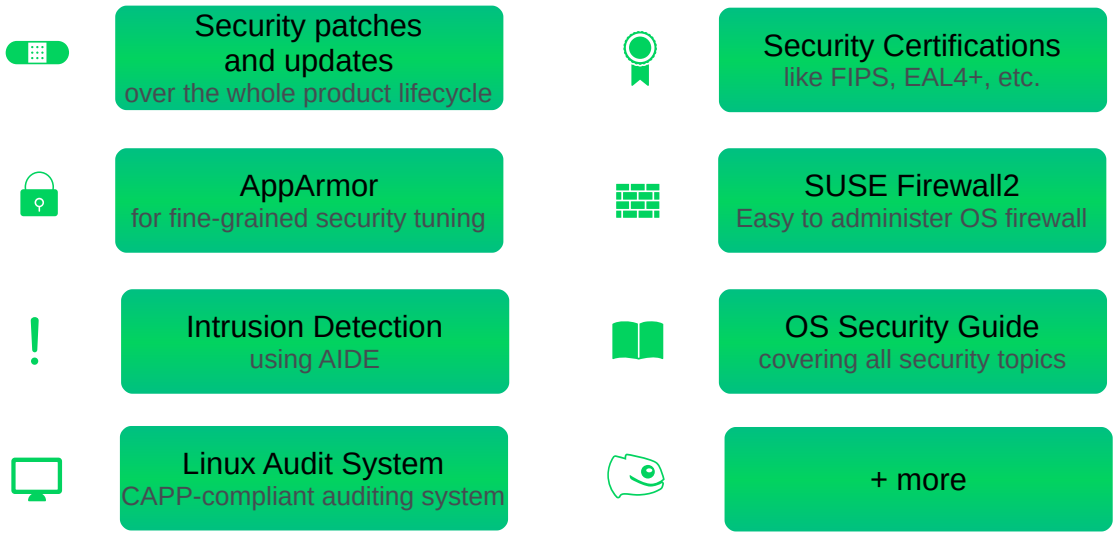

FIGURE 2: SECURITY COMPONENTS OF SUSE LINUX ENTERPRISE SERVER

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 12 running SAP HANA databases to fill the gap between the generic SUSE Linux Enterprise Server Security Guide, the SUSE Linux Enterprise Server Hardening Guide and the SAP HANA security guide. The SUSE Linux Enterprise Server Security Guide and Hardening Guide contain some of the recommenda-

tions found here, but also additional recommendations. Most of the recommendations can be applied to a 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 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 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 anb 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 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 12, like the security certifications and the constantly provided security updates and patches, SAP HANA can run in a very secure environment. This ensures that the implementation meets the security standards and corporate security concepts required by organizations of all sizes.

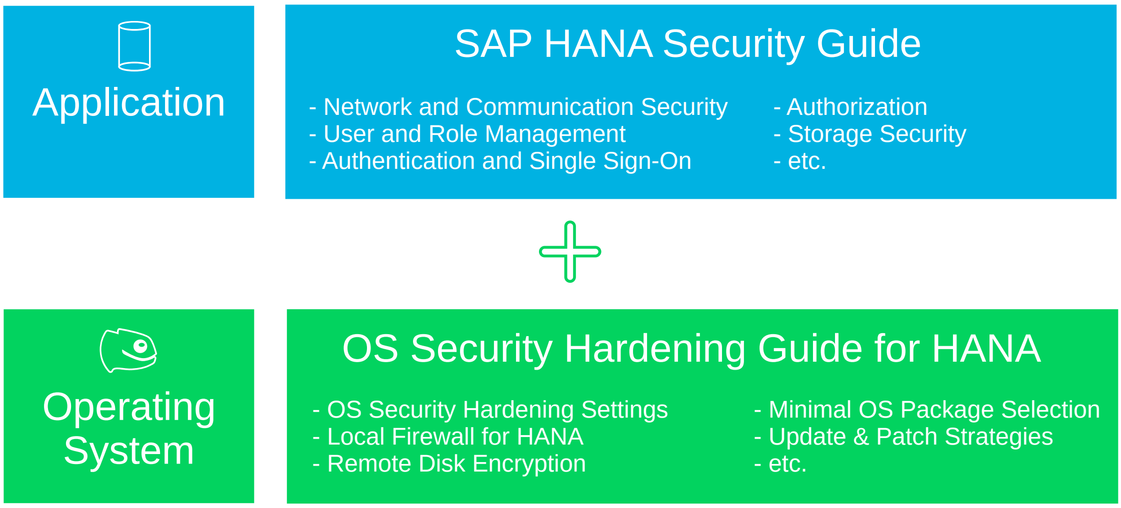

FIGURE 4: SAP HANA AND OPERATING SYSTEM SECURITY

2 SUSE Linux Enterprise security hardening settings for HANA

Introduction to Linux security hardening ~~~~~~~~~~~~~~~~~~ SUSE Linux Enterprise Server already provides a high level of security with the standard installation. However, the standard security settings are generic, because they have to fit to all possible Linux server workloads. Also, many security settings have impacts on the comfort of the system administration and possibly also for the users of the system. Therefore, the SUSE Linux Enterprise Server 12 standard security settings provide a good tradeoff between compatibility to all workloads, administrative comfort and a secure operatingsSystem.

SAP HANA is a very special workload with clearly defined requirements. For such a workload, it is possible to have a more restrictive security configuration compared to the standard configuration. The goal of this guide is to strengthen the security without affecting the compatibility with SAP HANA.

While security hardening results in more security, it usually comes with the drawback of less administrative comfort and system functionality. This is a fact that every System Administrator should be aware off. However, a more restrictive configured system also provides a better level of protection and a lower risk of successful attacks. In many cases company security policies, guidelines or security audits force very high security standards, which automatically result in

more restrictive configured systems. The Linux Operating System has many tweaks and settings that can improve the overall security of the Operating System and its applications. These settings can be summarized in the following categories:

Authentication settings

Define for example who is allowed to login, password policy, etc.

System access settings

Defines which users are allowed to access the system locally and remotely using different login mechanisms (e.g. local logins via console ttys or remote logins via ssh)

Network settings

Define how certain layers of the network stack behave, for example the IP layer, or the TCP/UDP layer

Service permissions

Define the permissions of certain system service, for example disabling of 'at' jobs

File permissions

Define the file access rights of certain security-critical system files

Logging & reporting

Change the behavior of the system logging, syslog forwarding to a central syslog server, automatic creation of reports (i.e. security reports) and forwarding of security relevant information via email

2.1 Hardening settings for SAP HANA systems

Important

The measures in this chapter are described for the x86 architecture (x86 and AMD64/ Intel 64), but apply for the POWER architecture as well. Because of the differences in the hardware, it might be necessary to adapt them (different device names, etc.)
Also, the graphical user interface is not covered. Running a GUI on a secure server should be avoided.

The following hardening settings improve the security of SUSE Linux Enterprise Server systems running SAP HANA database. These settings are based on the recommendations of a security audit, which was performed on a SUSE Linux Enterprise Server standard installation, running SAP HANA database.

Note

Read the SUSE Linux Enterprise Server Security Guide and the SUSE Linux Enterprise Server Hardening Guide for additional measures (see https://documentation.suse.com/). (Choose "SUSE Linux Enterprise Server" instead of "SUSE Linux Enterprise Server for SAP Applications".

For each setting the following details are provided:

- Description: Details of the setting
- Procedure: How to apply the setting
- Impacts: Possible impacts for system administrators or users
- Priority: High, Medium, Low

Based on the impact of a particular setting, a system administrator or a security engineer can decide if the lost of administrative comfort is worth the gain in security.

The prioritization can be used to help decide which settings should be applied to meet security requirements. High priority settings should be applied when possible, whereas low priority settings can be treated as optional.

IMPORTANT: Disclaimer: We strongly recommend to execute all described hardening settings on a non-productive (such as a DEV or QA) system first. We also recommend to **backup the system** before doing any changes. If btrfs/snapper is being used, creating a snapshot of the root file system is advised. Furthermore, we recommend to test the functionality of SAP HANA and all related applications and services after applying the settings. Since SAP HANA installations, use cases, hardware and installed services are likely to be different from the test audit. it cannot be guaranteed that all settings work correctly. It even cannot be completely excluded that they potentially have a negative impact on the functionality of the system.

If it is not possible to test the settings on a non-productive system, the changes should only be made within a maintenance window. The maintenance window should provide enough time for a proper system functionality test, or for restoring the system if necessary.

2.1.1 Installing SUSE security checker

Description

The SUSE security checker (`seccheck`) performs certain security checks, executed via cron jobs, on a regular basis, and generates reports. These records are usually forwarded via email to root. More details about `seccheck` can be found in **/usr/share/doc/packages/seccheck/README** or at https://www.suse.com/documentation/sles-12/single-html/book_hardening/book_hardening.html#sec.sec_prot.general.seccheck.

Important

The password check is not done because the password-cracking software tool `john` is not available on SUSE Linux Enterprise Server. The check would fail silently.

Procedure

Install package `seccheck`:

```
zypper in seccheck
```

Impact

- Daily and weekly reports via email to the root user.
- Requires a properly setup email forwarding.

Priority

Medium

2.1.2 Configuring mail forwarding for root user

Description

To receive information about the security relevant changes and incidents, it is strongly recommended to enable mail forwarding for the user root to a dedicated email account for the collection of system mails.

Procedure

1. Install 'Yast2-mail':

```
zypper in yast2-mail
```

2. Start the 'YaST' mail module:

```
yast mail
```

3. Choose 'Permanent' as connection type
4. Enter address of internal mail gateway and configure authentication if required
5. Do **NOT** enable 'accept external SMTP connections'
6. Enter email address to forward root emails (typically a dedicated system mail collection account)
7. Save settings
8. Test settings with

```
mail root

subject: test
test
.
```

9. Verify with the command `mailq` if the email has been delivered.

Impact

- Requires an accessible SMTP server.
- Requires somebody that regularly checks the mails of the 'root' user.

Priority

High

2.1.3 Configuring `hosts.allow` and `hosts.deny` according to local network setup

Description

The files `hosts.allow` and `hosts.deny` allow or respectively deny access for certain services and applications. We recommend **not** to set access control in these files and to use the local SAP HANA firewall instead. The SAP HANA firewall, based on iptables, allows a much more fine-grained access control, higher security and better logging mechanisms. Only few applications still support these files. To verify if a binary does so, check if 'libwrap' is used:

```
ldd <path_to_binary> | grep libwrap
```

2.1.4 Forwarding syslog files to a central syslog server

Description

Log files should be forwarded from an SAP HANA node to a central **syslog** server. This prevents syslog files from being manipulated by an attacker. In addition, it allows administrators to have a central view on the syslog files.

Procedure

This procedure explains a basic syslog forwarding setup. For a more sophisticated setup, consult the **RSyslog** manual at https://www.rsyslog.com/doc/master/index.html#manual.

On the target syslog server (running SUSE Linux Enterprise Server 12)

1. Edit `/etc/rsyslog.d/remote.conf`
2. Uncomment the following lines in the 'UDP Syslog server' or 'TCP Syslog Server' block of the configuration file and enter the IP address and port of the interface 'rsyslogd' shall listen:
   TCP example

   ```
   $ModLoad imtcp.so
   $UDPServerAddress <ip>
   $InputTCPServerRun <port>
   ```

   UDP example

   ```
   $ModLoad imudp.so
   ```

```
$UDPServerAddress <ip>
$UDPServerRun <port>
```

3. Restart `rsyslog`:

```
systemctl restart rsyslog.service
```

On the SAP HANA node

1. Edit `/etc/rsyslog.d/remote.conf`
2. Uncomment the appropriate line (TCP or UDP) and replace 'remote-host' with the address of the central log server:
   TCP example

```
# Remote Logging using TCP for reliable delivery
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @@remote-host
```

   UDP example

```
# Remote Logging using UDP
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @remote-host
```

3. Restart `rsyslog`:

```
systemctl restart rsyslog.service
```

4. Verify the proper function of the syslog forwarding using the command:

```
logger "hello world"
```

   The log message “hello world” should now appear on the central syslog server.

Impact

- Requires a central syslog server.

Priority

Medium

2.1.5 Disabling `ctrl-alt-del`

Description

Prevent reboot of a system via serial console and/or external keyboard

Procedure

Create the following symlink:

```
ln -s /dev/null /etc/systemd/system/ctrl-alt-del.target
```

Impact

- A system reboot can not be performed via a local keyboard or a remote-management session anymore.
- This can be irritating for system administrators, but it also helps to prevent accidental reboots.

Priority

Medium

2.1.6 Implementing `cron.allow`

Description: The `cron.allow` file specifies a whitelist of users that are allowed to execute jobs via the cron system. The file does not exist by default. This means every user (except those listed in cron.deny) can create cron jobs.

Procedure

Create an empty file `/etc/cron.allow` to prevent a user from creating cron jobs:

```
touch /etc/cron.allow
```

Info

Location of user crontabs: `/var/spool/cron/tabs`

Impact

- SAP HANA users ('<sid>adm') and other users are not allowed anymore to create their own cronjobs.

Priority

Low

2.1.7 Implementing `at.allow`

Description

The `at.allow` file specifies a whitelist of users that are allowed to execute scheduled one-time running jobs, so-called 'at' jobs, via the 'at' job execution system. This file does not exist by default. This means that every user (except those listed in `at.deny`) can create 'at' jobs.

Procedure

Create an empty file `/etc/at.allow` to prevent a user from creating 'at' jobs:

```
touch /etc/at.allow
```

Impact

- The functionality of one-time 'at' jobs gets disabled.

Priority

Medium

Restricting `sudo` for general users Description:: The `sudo` command allows users to execute commands in the context of another user, typically the root user. The `sudo` configuration consists of a ruleset that defines the mappings between commands to execute, their allowed source and target users and groups. The configuration is stored in the file `/etc/sudoers`. Like the command `su`, `sudo` asks for the root password by default. However, unlike `su`, `sudo` remembers the password and allows further commands to be executed as root without asking again for the password for five minutes. Therefore, sudo should only be enabled for selected users, such as **admin** users.

Procedure

1. Edit file `/etc/sudoers`, for example by executing `visudo`
2. Comment out the line to:

```
#ALL ALL=(ALL) ALL # WARNING! Only use this together with 'Defaults targetpw'!
```

3. Uncomment this line to:

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

4. Add all system administrator users to the group wheel:

```
usermod -aG wheel <admin_user>
```

> **Important**
>
> The user added to the wheel group has to log out and log in again to get the new group membership applied.

> **Tip**
>
> If `sudo` asks for the password of the target user instead of the user invoking `sudo`, uncomment (default) the line `Defaults targetpw # ask for the password of the target user i.e. root`. For more details, read the man page of `sudoers`.

Impact

- Prohibits `sudo` command functionality for all users, other than the ones that are members of the group 'wheel'.
- Note that the `su` command is still available for other users.

Priority

High

Adjusting default `umask` ^^^^^^^ Description:: The command `umask` specifies the default XOR-masking for access rights for newly created files. We recommend to change this value to 077. This will force newly created files and directories to be not read/write/execute enabled for groups and other users.

Procedure

Edit file `/etc/login.defs` and change the umask value:

```
UMASK 077
```

Tip

The PAM module `pam_umask.so` (in `/etc/pam.d/common-session`) applies the UMASK setting made in `/etc/login.defs`. Refer to the respective man page for alternatives.

Impact

- Newly created files and directories are not read-, write- and executable by users other than the creating user.

Remarks

To take changes into effect, a logout / re-login of all user sessions is required.

Priority

High

2.1.8 Modifying login definitions according to corporate security policies

Description

The file `/etc/login.defs` describes the login settings for users, such as password expiration times password aging), number of allowed login retries, `umask` settings, etc. It does not provide options to set the password policy. All changes apply only to newly created accounts! To change existing accounts, use the `passwd` and `chage` commands. Adjust the settings according to your corporate security policies.

Procedure

Edit file `/etc/login.defs` and make changes according to your policies.

```
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   14
```

This example sets default password expiration values for all newly created users:

- Password expires after 90 days
- Warns 14 days before the password expires
- Allows a user to change the password only every seven days

The `chage` command prints information about the current password expiration state for a particular user.

```
chage -l <user name>
```

Remark

It is also to possible to specify password expiration times and similar settings on a per-user basis using the `useradd` command. More information about password aging can be found in the SUSE Linux Enterprise Server 15 Hardening Guide, section 2.27 Enabling Password Aging.

Impact

- Some `login.defs` settings, like the password expiration time, reject users to login after their passwords have expired. These settings require system administrators to inform their users about the password expiration times.
- Users are required to actively change their passwords from time to time.

Priority

Medium

2.1.9 Setting up password failure counts for users

Description

Password failure counts prevent users from logging in after a defined number of failed login attempts. SUSE Linux Enterprise Server provides this mechanism via the PAM system. We do not recommend to use password failure counts, as they can be misused for denial-of-service attacks of certain user accounts. If your corporate policy requires to setup password failure counts for users, refer to the SUSE Linux Enterprise Server 12 Hardening Guide, section 2.29.3 Locking User Accounts After Too Many Login Failures.

2.1.10 Setting up password strengthening for user accounts according to corporate policies

Description

The default password policy for user accounts on a default SUSE Linux Enterprise Server system is already quite strong. For example, a password cracking library is used to prevent too simple and too short passwords. In some cases, it is required to configure the password strengthening exactly according to a corporate password policy. This is possible by changing the PAM password authentication settings in the file `/etc/pam.d/common-password`. Use the `pam-config` utility to modify the PAM password strengthening settings. The changes are reflected in the file `/etc/pam.d/common-password`. Change the settings according to your requirements.

```
pam-config --add \
--cracklib-retry=3 \
--cracklib-minlen=8 \
--cracklib-lcredit=-1 \
--cracklib-ucredit=-1 \
--cracklib-dcredit=-1 \
--cracklib-ocredit=0 \
--cracklib-difok=5
```

This example configures the password strengthening according to the following rules:

- Ask user up to a maximum number of three times to enter a new valid password
- Minimum of eight characters
- At least one uppercase alpha character
- At least one lowercase alpha character
- At least one number
- An unlimited amount of special characters, such as `_, !, %`
  A new password must differ by at least five characters from the old password. More information on password strengthening options can be found in the man page `man pam_cracklib`.

Impact

- The passwords for system users have to be set according to the defined policies.
- The root user is allowed to overrule the password policy.
- When setting password expiration times, users can not login anymore after their passwords have expired.

Priority

Medium

2.1.11 Configuring user remote login restriction

Description

Utilize `access.conf` to control remote access to the system for the root and any other user accounts. The configured accounts are restricted to log in from a certain IP subnet via SSH.

Procedure

1. Edit file `/etc/pam.d/sshd` and append:

   ```
   auth required pam_access.so
   ```

   See `man access.conf` for configuration details.

2. Edit file `/etc/security/access.conf` (see `man access.conf` for configuration details):

   ```
   + : <sid>adm : <network/netmask>
   + : sapadm : <network/netmask>
   + : <admin user> : <network/netmask>
   - : ALL : ALL
   ```

Warning

Do not use the `pam-config` utility here. It only supports `pam_access` as global module. The configuration above is not suitable to be used globally for all services and can cause a denial of access for the entire system!

Impact

- Only whitelisted users coming from the specified IP subnet are allowed to login via SSH.
- Remote root login is prohibited.

Priority

Medium

2.1.12 Setting up password for rescue mode

Description

The root password is needed in rescue mode (rescue.target) to access the system. On SUSE Linux Enterprise operating systems no change has to be made.

2.1.13 Adjusting `sysctl` variables to improve network security

Note

This section only covers settings for IPv4. There are similar IPv6 parameters available if required.

Description

`sysctl` (system control) variables change certain kernel parameters that influence the behavior of different parts of the operating system, such as the Linux network stack. These kernel parameters can be looked up in the proc file system, in `/proc/sys/`. Many kernel parameters can be directly changed by echo'ing a value into a parameter file. However, these changes are not persisted and are lost after a system reboot. Therefore we recommend to make all changes in the `sysctl` configuration file.

Procedure

Edit the `/etc/sysctl.conf` file and set or change the following variables:

```
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
```

This setting enables the reverse path filter in strict mode. The setting ensures that the answers to incoming IP packets are always sent out via the interface where the packet has been received. If the system would direct the answer packet to a different outgoing interface according to the routing table, this packet would be discarded. The setting prevents certain kind of IP spoofing attacks, such as those used for DDoS attacks.

```
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_source_route = 0
```

This setting disables the acceptance of packets with the SRR option set in the IPv4 packet header. Packets that use “Source Routing” are rejected. This prevents IP packet redirection, such as a redirection to a host behind a firewall, that is not directly reachable.

```
net.ipv4.tcp_syncookies = 1
```

The TCP SYN Cookie Protection is enabled by default. A 'SYN Attack' is a denial of service attack that consumes all the resources on a machine. Any server that is connected to a network is potentially subject to this attack.

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

ICMP echo requests (ping) can be sent to a broadcast address to scan a network for existing hosts / IPs or to perform a ICMP flood within a network segment. This setting ignores `icmp` echo packets, sent to a broadcast address.

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

This setting avoids filling up log files with unnecessary error messages coming from invalid responses to broadcast frames. See RFC 1122 'Requirements for Internal Hosts - Communication Layers' for more information.

```
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
```

Accepting "secure" ICMP redirects (from those gateways listed as default gateways) has few legitimate uses. It should be disabled unless it is absolutely required.

```
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
```

This disables the acceptance of ICMP redirect messages. These messages are usually sent by gateways to inform a host about a better route to an outside network. These redirects can be misused, for example for man-in-the-middle attacks.

```
net.ipv4.tcp_max_syn_backlog = 4096
```

The TCP SYN backlog defines the number of SYN packets that are queued for further processing. When the queue limit is exceeded, all new incoming syn-packets are dropped. This improves the protection against TCP SYN flood attacks.

```
net.ipv4.ip_forward = 0
```

IP forwarding is the IP routing functionality of a Linux system. SAP HANA systems should never act as routers. Therefore IP forwarding is disabled.

```
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```

IP redirects should only be sent by routers / gateways. As SAP HANA systems do not act as gateways, redirects are disabled.

Impact

- This changes the behavior of the IP network stack, which might cause some network problems or performance issues with certain network setups and devices (such as firewalls) in some rare cases.

Priority

High

2.1.14 Changing home directory permissions from 755 to 700

Description

By default, home directories of users are accessible (read, execute) by all other users on the system. As this is a potential information leak, home directories should only be accessible by their owners. SAP HANA system users ('<sid>adm') have their home directories in the directories `/usr/sap/<sid>/home/`. As this directory structure is in the domain of SAP, we do not describe any changes here.

Procedure

The following commands will set the permissions to 700 (directory only accessible for the user) for all home directories in `/home`:

```
chmod 755 /home
```

```
for a in /home/*; do echo "Changing rights for directory $a"; chmod 700 ”$a”; done
```

Impact

- System users are not allowed anymore to access other users home directories.
- An exception is made to '<sid>adm' users with their home directories in `/usr/sap/<sid>/home`.

Priority

Medium

2.1.15 Modifying permissions on certain system files

Description

Many system files are group- or world-readable by default. For those files that carry sensitive information, this can be a security risk. Changing the file permissions of these files to more restrictive values increases the security. SUSE provides the tool `chkstat` to check and set file permissions of certain files that are defined in one of the following configuration files:

```
permissions.local
permissions.easy
permissions.paranoid
permissions.secure
```

The `permissions.local` file is dedicated for user-defined file permissions.

Procedure

For SAP HANA systems we recommend to use the `permissions.easy` pattern plus some additional file permissions that will be stored in the `permissions.local` pattern.
First set the permissions in the correct order in `/etc/sysconfig/security`:

```
...
PERMISSION_SECURITY="easy local"
...
```

Then add the following permission settings to the file `/etc/permissions.local`:

```
#
```

```
# HANA Security Hardening
#
/etc/at.allow                   root:root       0400
/etc/bash.bashrc                root:root       0444
/etc/csh.cshrc                  root:root       0444
/etc/csh.login                  root:root       0444
/etc/shadow                     root:shadow     0440
/etc/rsyslog.conf               root:root       0400
/etc/crontab                    root:root       0400
/etc/cron.d                     root:root       0700
/etc/cron.hourly                root:root       0700
/etc/cron.daily                 root:root       0700
/etc/cron.weekly                root:root       0700
/etc/cron.monthly               root:root       0700
/etc/login.defs                 root:root       0400
/etc/security/access.conf       root:root       0400
/etc/sysctl.conf                root:root       0400
/etc/X11/xdm/Xservers           root:root       0444
/root                           root:root       0700
/root/.cshrc                    root:root       0400
/var/log/boot.log               root:root       0640
/var/log/sa                     root:root       0770
#
# Changing permissions of utmp files would cause the commands
# w, who and last not to work anymore for non-root users
#
# Uncomment these lines, if you are really sure about that
/var/run/utmp                   root:utmp       0600
/var/log/wtmp                   root:utmp       0600
```

Now apply the permissions:

```
chkstat --system --set
```

Impact

- Some system administration tasks that require access to files mentioned above and that are usually performed as normal system user have to be performed as root user.

Priority

Medium

3 SAP HANA firewall

3.1 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).

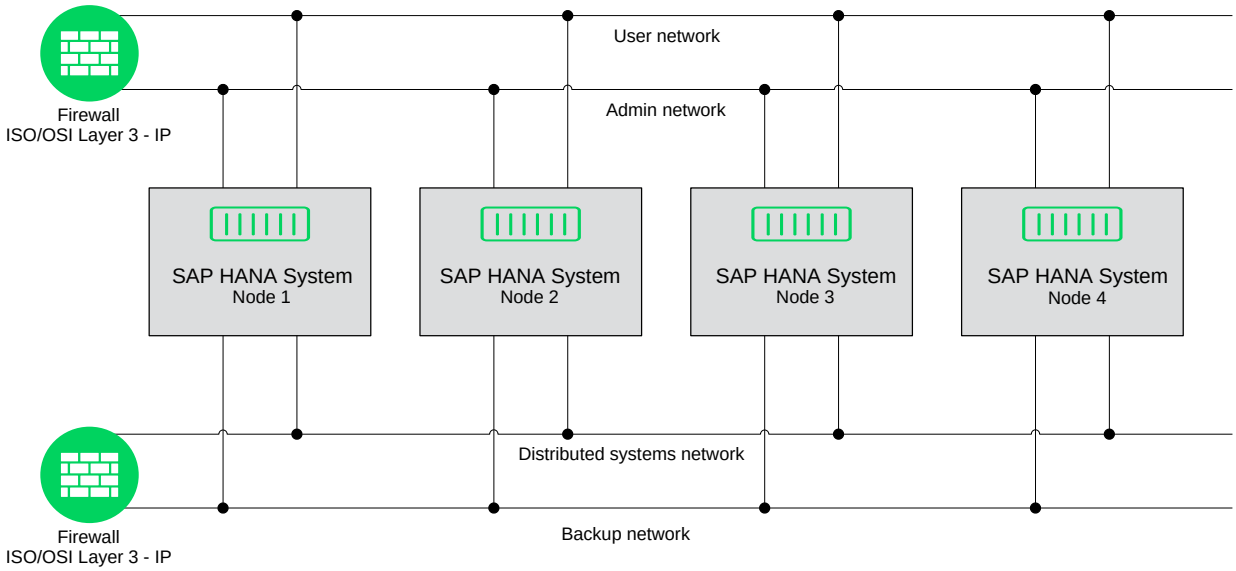

FIGURE 5: EXAMPLE OF A SAP HANA NETWORK DIAGRAM WITH EXTERNAL FIREWALLS

All SAP HANA networks should be either isolated (that means distributed system networks), or if they require communication from other networks (that means user communication), they should be behind an external firewall. This external firewall should only allow traffic for an 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 not just SAP HANA database systems. In this case, a local running firewall can take over some of the functionality of an external firewall.

3.2 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 has 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
- Access to services can be restricted to certain source networks
- Option to log dropped packets to a firewall log file
- Simulating option that prints the `iptables` commands to the console instead of executing them (What if…)

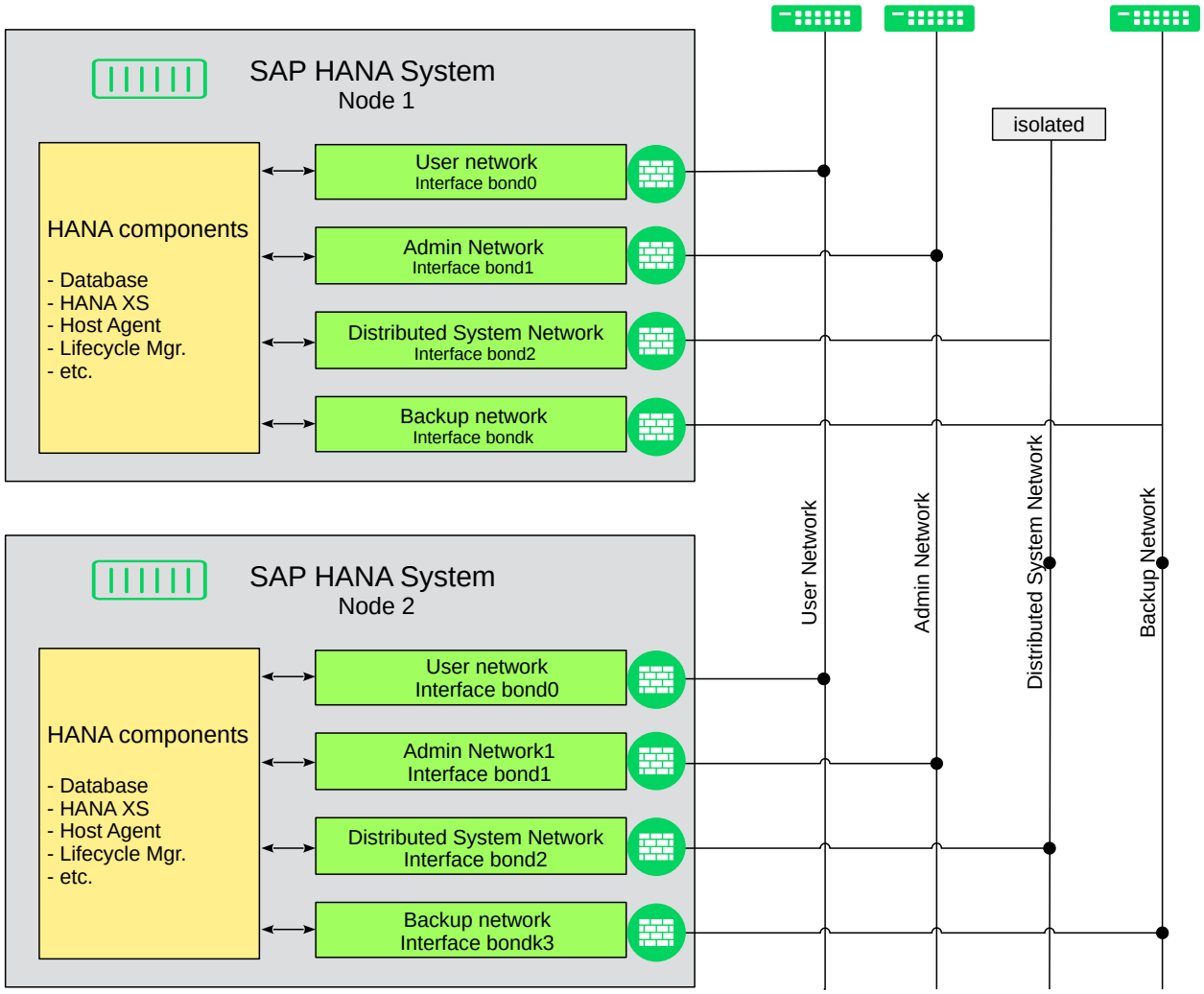

FIGURE 6: EXAMPLE OF A SAP HANA FIREWALL NETWORK DIAGRAM

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, when a local running firewall makes sense, are:

- when an external firewall that protects non-isolated SAP HANA networks from other networks (for example user network) is not available.
- when an external firewall cannot be configured restrictively enough, to only allow network communication for particular SAP HANA ports for certain SAP HANA networks.

- when an external firewall provides too less security zones.
- when a protected network contains many different servers, that means non-SAP servers, in the same network.

There are several other reasons why a local firewall could makes 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.

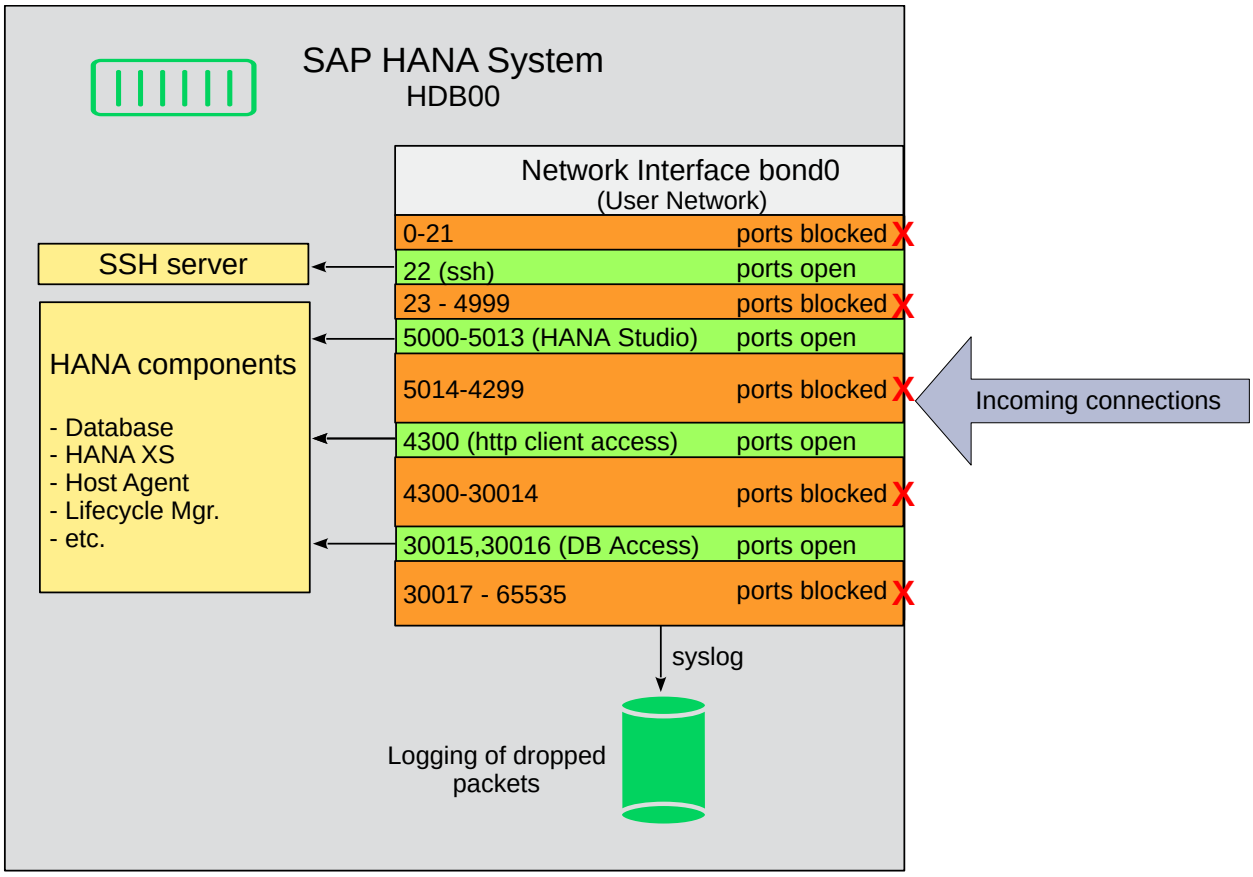

FIGURE 7: EXAMPLE OF A SAP HANA FIREWALL NETWORK TRAFFIC FLOW (PORTS ARE EXEMPLARY)

3.3 Installation

The SAP HANA firewall is available in the repositories for SUSE Linux Enterprise Server for SAP Applications 12. It extends the SuSEFirewall2 configuration by adding rulesets.

```
zypper install HANA-Firewall
```

The package installs the following files:

`/usr/sbin/hana-firewall`	Firewall executable. A usage description can be printed with the command: `/usr/sbin/hana-firewall --help`
`/usr/lib/systemd/system/hana-firewall.service`	Systemd service file for HANA firewall
`/etc/sysconfig/hana-firewall`	Main configuration file
`/usr/sbin/rchana-firewall`	compatibility link to start the service via `rchana-firewall`
`/etc/hana-firewall.d`	Directory for HANA services and user defined services
`/usr/share/man/man8/hana-firewall.8.gz`	Man page for the HANA firewall

3.4 Configuration

The configuration can be done:

- by the YaST SAP HANA Firewall module (`yast hanafirewall`) or
- on the command line with `hana-firewall`

Section 9.2 Configuring HANA-Firewall (https://documentation.suse.com/sles-sap/12-SP4/single-html/SLES4SAP-guide/#sec-s4s-configure-firewall-hana) of the SUSE Linux Enterprise Server for SAP Applications Guide describes the SAP HANA-Firewall YaST module and lists some advice regarding multi-tenant HANA databases.

3.4.1 Prerequisites

Make sure, that you have no non-SUSE local firewall running or which starts automatically after a reboot.

3.4.2 Quick configuration guide

This quick configuration guide provides a small setup procedure for a simple SAP HANA firewall setup without using YaST.

1. Open the configuration file `/etc/sysconfig/hana-firewall`.
2. Add all installed SAP HANA systems and instances to the parameter `HANA_SYSTEMS` as a space separated list. Use the format `<sid><instance-nr>`, that is 'HDB00'.
3. Edit the network interface / service mappings using the `INTERFACE_<n>` and the `INTERFACE_<n>_SERVICES` parameters. `INTERFACE_<n>_SERVICES` has to list all services that should be opened on a particular interface as a space separated list.
   Here is an example:

   ```
   # Interface eth0
   INTERFACE_0="eth0"
   # Enable all HANA services for all HANA instances + ssh service on eth0
   INTERFACE_0_SERVICES="HANA_* ssh"
   ```

   If you have multiple network interfaces, configure the `INTERFACE_<n>` and `INTERFACE_<n>_SERVICES` parameters for each interface
4. Save the configuration.
5. Now you can test the firewall. The sub-command 'dry-run' displays a list of the resulting iptables rules, 'apply' will activate these rules and 'status' reports the current status:

   ```
   hana-firewall dry-run
   hana-firewall apply
   hana-firewall status
   ```
6. If everything is working correctly, edit the file `` `/etc/sysconfig/hana-firewall `` again and set the global parameter.

   ```
   OPEN_ALL_SSH="no"
   ```
7. Make sure that you have the SSH service configured on at least one interface. Otherwise you might not be able to login anymore.
8. Apply the changed configuration using the command:

   ```
   hana-firewall apply
   ```
9. Make sure that the firewall gets started on bootup.

```
systemctl enable hana-firewall.service
```

3.4.3 Detailed configuration

For a more comprehensive configuration you can use the YaST HANA Firewall module. This is described in detail in the SUSE Linux Enterprise Server for SAP Application 12 Guide. As an alternative, editing `/etc/sysconfig/hana-firewall` is shown here.

3.4.3.1 'Global Parameters' section

List of HANA systems and instance numbers

This setting contains a list of HANA systems and instance numbers in a space separated list. The format is '<SID><INSTANCE NR>', this means 'HDB00'. Based on these values, the firewall automatically creates ports and port-ranges for the HANA firewall services mentioned below.
Example:

```
HANA_SYSTEMS="HDB00"
```

Open SSH on all devices

Opens the SSH (secure shell) port on all interfaces. This is useful for testing purposes, to avoid accidentally locking out of admin users. In the final firewall configuration, SSH should only be enabled for selected interfaces, and the global setting should be turned off.
Example:

```
OPEN_ALL_SSH="yes"
```

Warning

Open the SSH port on all interfaces should be done only temporarily during testing. In the final configuration `OPEN_ALL_SSH` should be set to "no".

3.4.3.2 'Interfaces' section

`INTERFACE` and `INTERFACE SERVICES` parameters map services to network interfaces. `INTERFACE` parameters have to be in the format `INTERFACE_<0-n>` and contain names of valid network interfaces, like 'eth0' or 'bond0'. `INTERFACE SERVICES` parameters have to be in the format `INTERFACE_<0-n>_SERVICES` and contain one or more service names in a comma-separated list.

Service names can be all services defined in directory `/etc/hana-firewall.d` and all service names from `/etc/services`. A special HANA service is called `HANA_*`, which includes all SAP HANA services.

Detailed service descriptions can be found in the appropriate service definition files in the directory `/etc/hana-firewall.d` or in this document section 'Predefined Services'. All service names can be optionally prepended by a network or host definition in the format `:<network>[/<cidr netmask>]`.

Examples:

```
INTERFACE_0="eth0"
INTERFACE_0_SERVICES="HANA_* ssh"

INTERFACE_1="bond1"
INTERFACE_1_SERVICES="smtp ssh:10.0.0.0/24 ntp:10.10.10.1 HANA_HTTP_CLIENT_ACCESS"

INTERFACE_2="eth0:1"
INTERFACE_2_SERVICES="HANA_SYSTEM_REPLICATION HANA_DISTRIBUTED_SYSTEMS HANA_SAP_SUPPORT"
```

3.5 Services

3.5.1 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 SAP HANA firewall service definitions are stored in the directory `/etc/hana-firewall.d`. Each file (in capital letters) defines one service. The service name equals the file name and can immediately be used in the 'Interfaces' section of the main configuration. Each service file currently requires two parameters (TCP, UDP) that specify the TCP and UDP ports and/or port-ranges. Ports and port ranges have to be entered as a space-separated list. Port ranges are defined in the format: `<start port>:<end port>`, that is `10000:20000`.

Examples:

```
TCP=”22”
UDP=””
```

```
TCP="10050:10054 111 2049"
UDP="10050:10054 111 2049"
```

To create a new user defined service, use the script `create_new_service`:

```
cd /etc/hana-firewall.d
./create_new_service
```

Then follow the instructions on the screen. After the service has been created, it can immediately be used.

3.5.2 Predefined services

3.5.2.1 HANA 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.

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

Service Name	Description
`HANA_DATABASE_CLIENT`	Open ports for Application servers that use SAP HANA as a database
`HANA_DATA_PROVISIONING`	This connection is used for event streaming. The protocol is SQLDBC (ODBC/JDBC).
`HANA_HTTP_CLIENT_ACCESS`	Open ports for web browser client access to SAP HANA

Service Name	Description
HANA_SAP_SUPPORT	The connection is not active by default because it is required only in certain support cases. To find out how to open a support connection, see the 'SAP HANA Administration Guide'
HANA_DISTRIBUTED_SYSTEMS	Distributed scenarios: Internal network communication takes place between the hosts of a distributed system on one site. Certified SAP HANA hosts contain a separate network interface card that is configured as part of a private network, using separate IP addresses and ports.
HANA_STUDIO	The connection to the instance agent acts as an administrative channel for low-level access to the SAP HANA instance to allow features such as starting or stopping of the SAP HANA database. The protocol used for this connection is SQLDBC (ODBC/JDBC).
HANA_STUDIO_LIFECYCLE_ MANAGER	This is the connection to SAP HANA lifecycle manager via SAP Host Agent. For more information about SAP HANA lifecycle manager, see 'SAP HANA Update and Configuration Guide'. The protocol used for this connection is SQLDBC (ODBC/JDBC).
HANA_SYSTEM_REPLICATION	Distributed scenarios: Internal network communication takes place between the hosts of a distributed system on one site. Certified SAP HANA hosts contain a separate network interface card that is configured as part of a private network, using separate IP addresses and ports.

Service Name	Description
`HANA_HIGH_AVAILABILITY`	Several communication ports used by SUSE HA solution

3.5.2.2 User services

Currently there is only one predefined user service for a local running NFS server.

TABLE 2: LIST OF SHIPPED USER SERVICE DEFINITIONS (HANA-FIREWALL 1.1.5)

Service Name	Description
`NFS_SERVER`	To allow access to an NFS server, you have also to set fixed ports for certain NFS services in `/etc/sysconfig/nfs`. NFS usually uses random port numbers, which leads into difficulties when having restrictive firewalls enabled.

3.6 Testing and activation

3.6.1 Testing the firewall

After the firewall has been properly configured, it should carefully be tested. First, you should simulate the start with the 'dry-run' option. This option just prints the `iptables` commands to STDOUT without actually executing the `iptables` commands.

```
hana-firewall dry-run
```

If you are satisfied with the rules, you can activate the firewall using the command:

```
hana-firewall apply
```

Note

If there is an error in your configuration, you will get a detailed description of what went wrong.

Now the firewall can be tested.

Important

After making any changes in the configuration, you always have to apply the new rules.

Important

Do not forget to set the global parameter `OPEN_ALL_SSH` to 'no' and to configure the SSH service for the appropriate interfaces.

3.6.2 Enabling the firewall

To start the firewall on system boot automatically, enable the HANA-Firewall service:

```
systemctl enable hana-firewall.service
```

Make sure that there is no other non-SUSE firewall enabled that starts automatically.

Important

Since SUSE Linux Enterprise Server 12, HANA-Firewall is part of SuSEfirewall2. It will start automatically, no matter whether the SuSEfirewall2 service is enabled or not. Also, note that the resulting `iptables` rules are a combination from **BOTH** HANA firewall and SuSEfirewall2!

4 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 SAP HANA itself. For details consult the SAP HANA Security Guide (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. 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. From there, it retrieves the necessary keys automatically to unlock the data. The key server should by any means be a dedicated security-hardened and protected system, since anyone with access to this system can retrieve the keys and decrypt the data.

The SUSE Linux Enterprise Server for SAP Applications guide describes the setup of client and server in section 10 Encrypting Directories Using cryptctl (https://documentation.suse.com/sles-sap/12-SP4/single-html/SLES4SAP-guide/#cha-s4s-configure-cryptctl).

5 Minimal operating system package election

5.1 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) installed and as few services running as possible.

SUSE Linux Enterprise Server provides an RPM package for each logical component, like an 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. Installation patterns help to easily get an installation that fits the requirements of a particular use case, for example an SAP server with development tools.

Reducing the number of installed RPM packages to a minimum lowers the amount 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. It is shipped in different versions and offers many additional components. This makes it difficult to follow the concept of installing only a minimal set of packages. Therefore, the current approach to minimal package selection is to use the SUSE Linux Enterprise Server installation patterns 'Base System' + 'Minimal System' and optionally add 'SAP HANA Server Base'. Depending on the actual setup, further packages might be required.

5.2 Required installation patterns and packages

The required software for SAP HANA is described in 'SUSE Linux Enterprise Server 12.x for SAP Applications Configuration Guide for SAP HANA' attached to SAP note '1944799 - SAP HANA Guidelines for SLES Operating System Installation'.

The document lists the necessary patterns and additional software packages.

It is strongly recommended to install at least the following two patterns:

- 'Base System' (adds 'YaST2 configuration packages' as a dependency)
- 'Minimal System (Appliances)'

This results in a total amount of approximately 880 packages, compared to 1700 packages of a standard installation.

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

In some rare cases, you might need to install additional packages, for example to get support in certain scenarios. We generally recommend to have SUSE Linux Enterprise Server update repositories configured on your HANA system to be able to quickly install new packages.

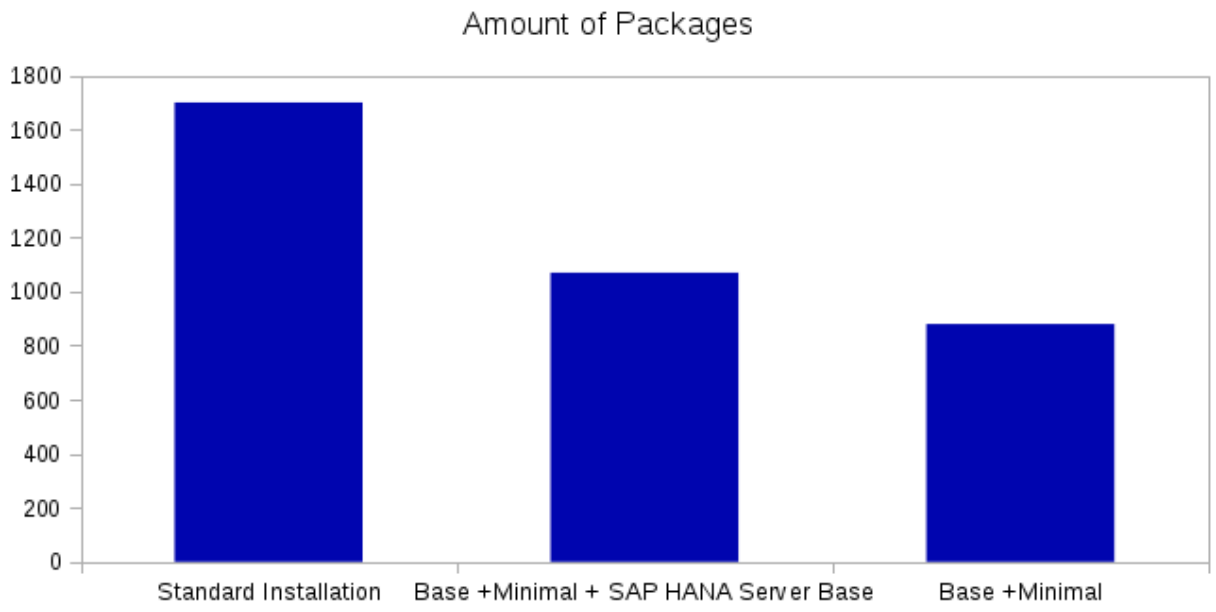

FIGURE 8: COMPARISON OF THE AMOUNT OF INSTALLED PACKAGES BETWEEN CERTAIN PACKAGE SELECTIONS

Tip

If you want to enable X11 forwarding for remote ssh connections (`ssh -X` or `ssh -Y`), the additional package xauth is required. X11 forwarding via ssh is useful for example when using the graphical HANA installer.

6 Security updates

6.1 Security updates for SUSE Linux Enterprise Server 12

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 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 regularly.

6.2 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 provides the Subscription Management Tool (SMT) 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 channel for the particular Service Pack of SUSE Linux Enterprise Server 12. On SUSE Linux Enterprise Server for SAP Applications 12, the update channels for the Service Pack of SUSE Linux Enterprise Server for SAP Applications and for the High Availability Extension should be available.

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

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

6.3 Update and patch strategies

In many cases, organizations have corporate polices 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.

6.3.1 Installing all new updates and patches on a regular basis

Description

Installation of new updates and patches, e.g. once a day or once a 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, updates & patches (incl. security updates) are usually harmless for a system. However, in some rare cases, updates might cause problems and can compromise the stability of a system.

Advantages

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 & patches might cause problems. Also some updates (e.g. kernel) require a reboot.

Recommendation

Good strategy for all non-productive HANA systems, but not for systems that are in production.

6.3.2 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 long time frames in between (e.g. 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 normal maintenance windows.

Selectively installing new updates and patches ^^ Description:: A selective installation of patches and updates, for example 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 with SUSE Manager.

Advantages

Mostly up-to-date system 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 (e.g. cve number, category, severity) cannot be used.

Recommendation

Probably the best update strategy, but also the most complicated one.

> **Tip**
>
> An important issue with updates is in most cases 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 'SLES Administration Guide, chapter: Live Patching the Linux Kernel Using kGraf'.

6.3.3 Not updating

Description

A system is not registered to the SUSE update channels and no updates are applied Advantages: None

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 as well as on the requirements on 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, i.e. using YOU (YaST Online Update), on a regular basis.

7 Outlook

Even though, this guide already covers most security hardening topics, we are planning to do further improvements. Also, later versions of SAP HANA might have changed or new requirements on the hardening settings, the firewall or the minimal package selection. 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 in the resource library on the SUSE website.

8 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).

9 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-12/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 12: Installation notes	SAP note 1984787

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

10 Documentation updates

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

v1.3

- Removal of the following chapters (moved to the general SLES "Hardening Guide":
  - "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"
- Add comment about x86/Power and GUI on top of "SUSE Linux Enterprise Security Hardening Settings for HANA"

v1.2

- minor typos corrected
- in section "Install SUSE security checker": Note that `john` is not available on SLES.
- in section "Adjust sysctl variables to improve network security": Explanation for setting net.ipv4.conf.default.secure_redirects and net.ipv4.conf.all.secure_redirects corrected
- in section "Restrict sudo for normal users" tip for using `Default targetpw` corrected
- in section "Adjust default umask": tip about `pam_umask.so` added

- in section "Set up password for single user mode": renamed single user mode more correctly to resuce mode
- in "Adjust sysctl variables to improve network security": now recommends creating a file in `/etc/sysctl.d/` instead of changing `/etc/sysctl.conf`
- in section "Modify permissions on certain system files": correct some errors in permissions and usage
- in "SUSE Linux Enterprise Server Update Channels": reference to unavailable document 'SUSE Linux Enterprise Server Maintenance made simple' in resource-library removed
- in "Further Information & References": link to SUSE security site corrected
- in "Outlook": Link to Resource Library removed because place for documentation is under rework
- in "SAP HANA Firewall":
  - port lists removed because they are often subject of change
  - command `hana-firewall` is now spelled correctly
  - wrong path `/etc/sysconfig/firewall.d` was replaced with `/etc/firewall.d`
  - table of installed files has been corrected
  - detailed configuration now bases on editing of `/etc/sysconfig/hana-firewall` and not existing logging variable has been removed
  - use of `yast sysconfig` has been removed
  - minor changes in text due to changes above

11 Legal notice

12 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 noncommercially. 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 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.