



# Operating System Security Hardening Guide for SAP HANA for SUSE® Linux Enterprise Server 15

---



# Operating System Security Hardening Guide for SAP HANA for SUSE® Linux Enterprise Server 15

Publication Date: 10/26/2018

SUSE LLC  
10 Canal Park Drive  
Suite 200  
Cambridge MA 02141  
USA

<https://www.suse.com/documentation> 

# Contents

- 1 Introduction 1**
  - 1.1 Security for SAP HANA 2
  - 1.2 Security for SUSE Linux Enterprise Server 2
  - 1.3 About this Document 3
  
- 2 SUSE Linux Enterprise Security Hardening Settings for HANA 7**
  - 2.1 Introduction into the Linux Security Hardening 7
  - 2.2 Hardening Settings for SAP HANA systems 8
    - Prohibit login as root via ssh 9 • Install SUSE security checker 10 • Configure mail forwarding for root user 11 • Forwarding of syslog files to a central syslog server 12 • Disable Ctrl-Alt-Del 13 • Implement `cron.allow` 14 • Implement `at.allow` 14 • Restrict sudo for normal users 15 • Adjust default `umask` 16 • Modify login definitions according to corporate security policies 17 • Set default inactive time to 1 day 18 • Set up password failure counts for users 19 • Setup password strengthening for user accounts according to corporate policies 19 • Configure user remote login restriction 20 • Set up password for rescue mode 21 • Adjust `sysctl` variables to improve network security 21 • Allow `root` login only via the first local console (`tty1`) 24 • Change home directory permissions from 775 to 700 25 • Modify permissions on certain system files 25
  
- 3 SAP HANA Firewall 28**
  - 3.1 SAP HANA Network Communication 28
  - 3.2 Local Firewall for SAP HANA 29
  - 3.3 Installation 32
  - 3.4 Configuration 32

3.5	Services	33
	Service Definitions	33 • Predefined Services 33 • Userdefined Services 34
3.6	Testing & Activation	34
<b>4</b>	<b>SUSE Remote Disk Encryption</b>	<b>36</b>
<b>5</b>	<b>Minimal OS Package Selection</b>	<b>37</b>
5.1	Background	37
5.2	Required Installation Patterns and Packages	37
<b>6</b>	<b>Security Updates</b>	<b>39</b>
6.1	Security Updates for SUSE Linux Enterprise Server 15	39
6.2	SUSE Linux Enterprise Server Update Channels	39
6.3	Update & Patch Strategies	40
	Installation of all new updates & patches on a regular basis	40 • Installation of all new updates & patches during maintenance windows 41 • Selective installation of new updates & patches (e.g. security updates only) 41 • Not updating 42
<b>7</b>	<b>Outlook</b>	<b>43</b>
<b>8</b>	<b>About the Authors</b>	<b>44</b>
<b>9</b>	<b>Further Information &amp; References</b>	<b>45</b>
<b>A</b>	<b>Documentation Updates</b>	<b>46</b>
<b>B</b>	<b>Copyright Information</b>	<b>47</b>

# 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 properly setup policies, like a password policy and data protection policies for users and system administrators, continues with a protected IT environment using i.e. firewalls, VPNs, SSL in communication protocols and ends with hardened servers, intrusion detection systems, data encrypting and automated security reporting. Additionally, many organizations perform security audits on a regular basis in order to ensure a maximum of security in their IT environment.

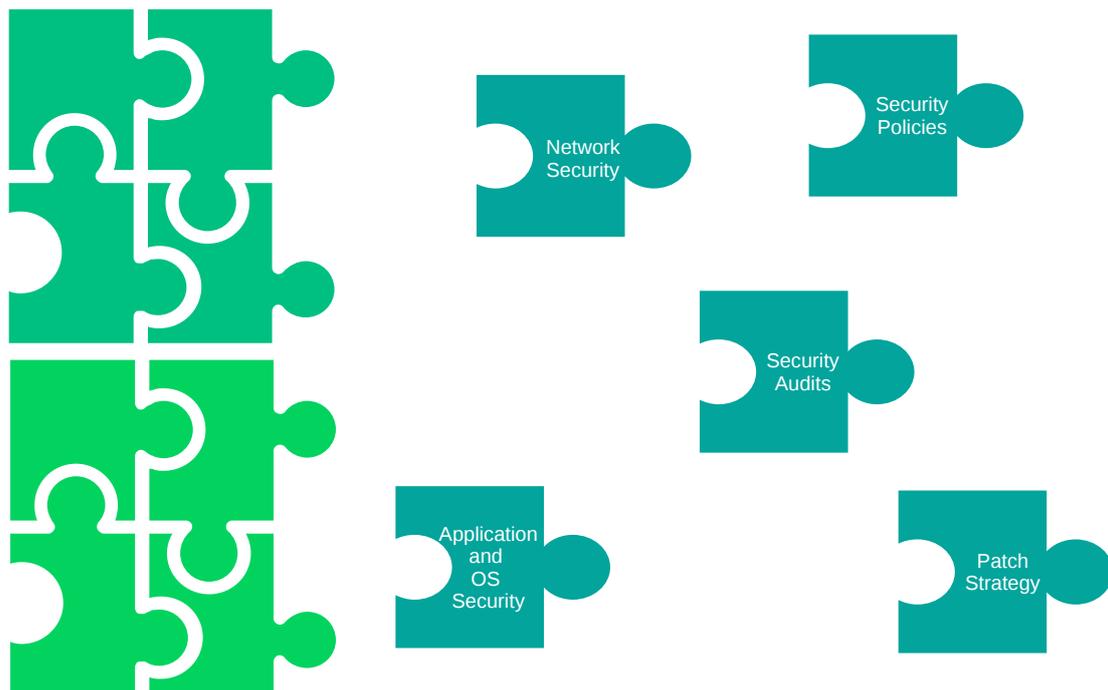


FIGURE 1.1: ELEMENTS OF A CORPORATE IT SECURITY

Comprehensive security concepts usually pay high attention to database systems, since databases belong to one of 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 in particular 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 itself takes the security topic very seriously. For SAP HANA, there is a comprehensive security guide available, that describes in detail how to protect HANA from a database perspective ([http://help.sap.com/hana/SAP\\_HANA\\_Security\\_Guide\\_en.pdf](http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf)). 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 and 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 in order 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 and 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 12 Operating System achieved many important security certifications, like the FIPS (Federal Information Processing Standard) 140-2 validation or the Common Criteria Security certification EAL4+. Currently we are in the process of achieving the same for SUSE Linux Enterprise 15. For details please visit: <https://www.suse.com/support/security/certifications/>.

## Security updates and patches

SUSE constantly provides security updates and patches for their SLES Operating Systems and guarantees highest security standards over the whole product life cycle.

## Documentation

SUSE published a security guide, that describes the security concepts and features of the SUSE Linux Enterprise Server 15 Operating System. ([https://www.suse.com/documentation/sles-15/singlehtml/book\\_hardening/book\\_hardening.html](https://www.suse.com/documentation/sles-15/singlehtml/book_hardening/book_hardening.html)). The SLES security guide provides generic security information valid for all workloads, not just for SAP HANA.

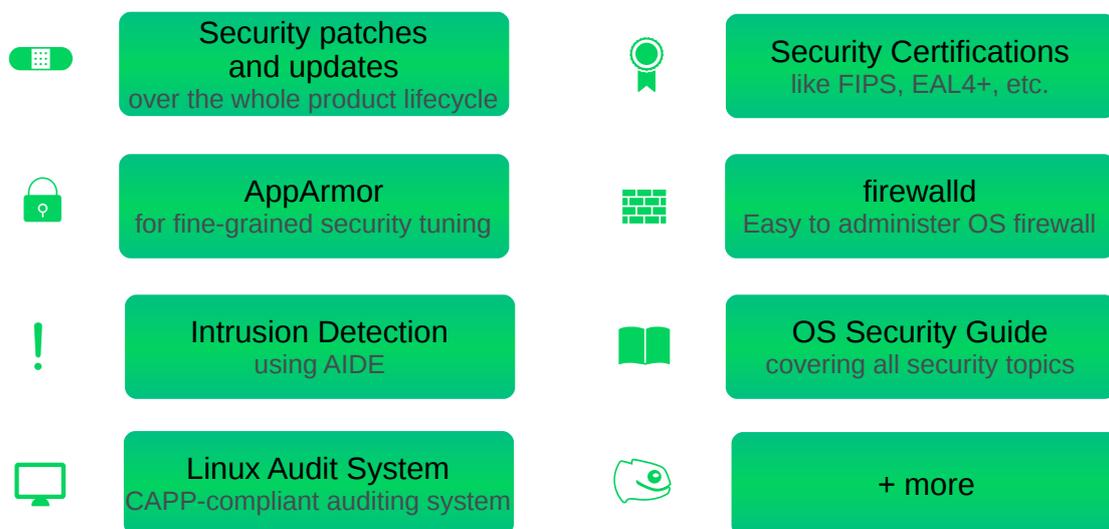


FIGURE 1.2: SECURITY COMPONENTS OF SUSE LINUX ENTERPRISE SERVER

## 1.3 About this Document

In order to further improve the security level specifically for SAP HANA, SUSE provides this guide, dedicated to the security hardening of SUSE Linux Enterprise Server 15 running SAP HANA databases to fill the gap between the generic SLES Security Guide, the SLES Security and Hardening Guide and the SAP HANA security guide. The SLES Security and Hardening Guide contains some of the recommendations found here and also additional ones. Most of the recommendations there can also applied to a SAP HANA installation after careful review

and testing. SUSE worked together with a large pilot customer to identify all relevant security settings and to avoid problems in real world scenarios. Also, SUSE works constantly together with SAP in the SAP Linux Lab in order to provide the best compatibility with SAP HANA.



**FIGURE 1.3: 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 OS security and the security for the hosted applications. In order 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 OS for maximum security when running SAP HANA specifically, as well as describing possible impacts, e.g. on system administration and gives a prioritization of each setting.

## Local firewall for SAP HANA

SUSE developed a dedicated local firewall for SAP HANA systems to improve the network security of SAP HANA, 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 SLES 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, when prevented its use in many setups because each boot needed a manual step. Remote Disk Encryption removes this manual step by allowing the encryption keys to be stored safely on a remote key server and be automatically used during system boot.

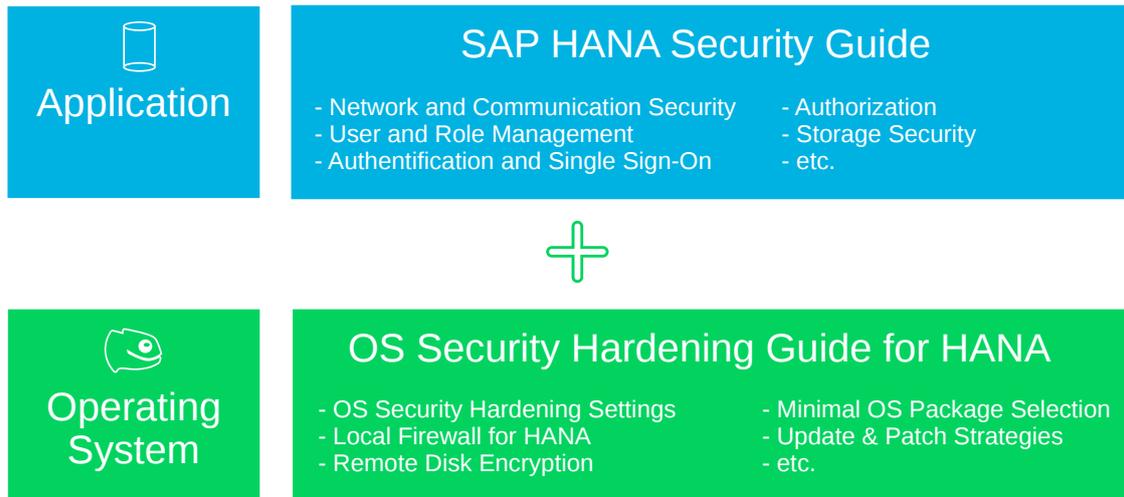
## Minimal package selection

The fewer OS packages a 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. Once a vulnerability has been found and reported, they are published in security advisories which usually get fixed very quickly. SUSE constantly provides security updates & patches for all supported packages on SUSE Linux Enterprise Server. This chapter explains, which update & patch strategies are the best and how to configure a SUSE Linux Enterprise Server to frequently receive all relevant security updates.

All in all, this guide covers all important topics in detail, relevant for the OS hardening of a SAP HANA system. Together 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 very secure environment, meeting the security standards and corporate security concepts required by organizations of all sizes.



**FIGURE 1.4: SAP HANA + OS SECURITY**

## 2 SUSE Linux Enterprise Security Hardening Settings for HANA

### 2.1 Introduction into the Linux Security Hardening

The 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 Operating System.

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. It is the goal of this guide to strengthen the security without affecting the compatibility with SAP HANA.

While security hardening results in more security it has a tradeoff of less administrative comfort and system functionality. This is a fact that every System Administrator should be aware of. 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 i.e. 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**

Defines, how certain layers of the network stack behave, e.g. the IP layer, or the TCP/UDP layer

### Service permissions

Defines the permissions of certain system service, e.g. disabling of *at* jobs

### File permissions

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

### Logging & reporting

Changes 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

## 2.2 Hardening Settings for SAP HANA systems

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

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 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 (i.e. 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 as well as all related applications and services after applying the settings. Since SAP HANA installations, use-cases, hardware and installed services likely to be different from the test audit, it cannot be guaranteed that all settings work correctly or even have a potentially 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, that leaves enough time for a proper system functionality test and to restore a system if necessary.

## 2.2.1 Prohibit login as root via ssh

### Description

By default, the user *root* is allowed to remotely login via ssh. This has two disadvantages:

- Firstly, root logins are logged, but cannot be associated with a particular user. This is especially a disadvantage, if there are more than one System Administrators that do changes on the system.
- Secondly, a stolen root password allows an attacker to login directly to the system. Instead of logging in as a normal user first, then doing `su` or a `sudo`, an attacker just requires the root password.

### Procedure

Edit `/etc/ssh/sshd_config` and set parameter:

```
PermitRootLogin no
```

After the change a restart of the sshd service is required:

```
systemctl restart sshd.service
```

### Impact

Root is not allowed to login remotely anymore, which require users to use `su` or `sudo` to gain root access when using ssh.



## Tip

It is also possible to allow a root login only with key authentication. Please read the man page of `sshd_config` for different `PermitRootLogin` values.

### Priority

high

## 2.2.2 Install SUSE security checker

### Description

The SUSE security checker performs certain security checks on a regular basis (executed via cron jobs) and generates reports. These records are usually forwarded via email to root. More details about `seccheck` can be found in </usr/share/doc/packages/sec-check/README> or [https://www.suse.com/documentation/sles-15/singlehtml/book\\_hardening/book\\_hardening.html#sec.sec\\_prot.general.seccheck](https://www.suse.com/documentation/sles-15/singlehtml/book_hardening/book_hardening.html#sec.sec_prot.general.seccheck).



## Important

The password check is not done because the tool `john` is not available on SLES. The check will 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

## 2.2.3 Configure mail forwarding for root user

### Description

In order 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 as outgoing mail server 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

## 2.2.4 Forwarding of syslog files to a central syslog server

### Description

Logfiles should be forwarded from a SAP HANA node to central syslog server. This prevents syslog files from being manipulated by an attacker as well as allowing administrators to have a central view on the syslog files.

### Procedure

This procedure explains a basic syslog forwarding setup. For a more sophisticated setup please consult the rsyslog manual.

#### On the target syslog server (running SLES12)

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

## 2.2.5 Disable 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 also helps to prevent accidentally reboots.

## Priority

medium

## 2.2.6 Implement `cron.allow`

Description: The `cron.allow` file specifies a whitelist of users, that are allowed to execute jobs via the Linux cron system. Per default the file does not exist, so 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

## 2.2.7 Implement `at.allow`

### Description

The `at.allow` files specifies a whitelist of users, that are allowed to execute `at` jobs (scheduled one-time running jobs) via the Linux `at` job execution system. Per default the file does not exist, so 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 Linux functionality of one-time jobs gets disabled.

## Priority

medium

## 2.2.8 Restrict sudo for normal 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 rule-set, 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 5 minutes. Therefore sudo should only be enabled for selected users only, i.e. admin users.

### Procedure

1. Edit file `/etc/sudoers`, e.g. 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 logout and login again to get the new group membership applied.



## Tip

If `sudo` shall ask 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 please 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`. Be aware, that the `su` command is still available for other users.

### Priority

high

## 2.2.9 Adjust default umask

### Description

The `umask` specifies the default XOR-masking for access rights for newly created files. This setting. We recommend to change this value to `077`. This will force newly created files and directories to be not read/write/execute enabled for group 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`. Please read its man page for alternatives.

### Impact

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

### Remarks

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

## Priority

high

## 2.2.10 Modify 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 new created accounts! To change existing accounts please 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 new creates users:

- password expires after 90 days
- warns 14 days before the password expires
- allows a user to change his password only every 7 days

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

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

### Remark

It is also 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 Security and Hardening Guide*, section: 2.26. *Enabling Password Aging*.

## Impact

Some `login.defs` settings, like the password expiration time, rejects users to login after their passwords have expired. These settings require System Administrators to inform their users about the password expiration times and users are required to actively change their passwords from time to time.

## Priority

medium

## 2.2.11 Set default inactive time to 1 day

### Description

By default, there is no timeout for inactive user sessions. This setting specifies in seconds, when an interactive user session is being terminated. We recommend to set the timeout to one day. The package `seccheck` (see above) provides a similar feature, called *autologout*.

### Procedure

Create the file `/etc/profile.d/timeout.sh` with the following content:

```
# /etc/profile.d/timeout.sh for SuSE Linux
#
# Timeout in seconds till the bash session is terminated
# in case of inactivity.
# 24h = 86400 sec
TMOUT=86400
```

## Impact

Long running user sessions are terminated after 1 day. We recommend to use *screen* in order detach sessions before logging out. Screen sessions are not terminated and can be re-attached whenever it is required.



### Warning

The login shell of the user has to evaluate the `TMOUT` variable, which is the case for the *bash*. Please verify this for all used login shells.

Priority: medium

## 2.2.12 Set 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, please refer to the *SUSE Linux Enterprise Server Security and Hardening Guide*, section: 2.28.3. *Locking User Accounts After Too Many Login Failures*

## 2.2.13 Setup 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-ucrcdit=-1 \  
--cracklib-dcredit=-1 \  
--cracklib-ocredit=0 \  
--cracklib-difok=5
```

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

- Ask the user to a maximum number of 3 times to enter a new valid password a minimum of eight characters total.
- at least one uppercase alpha character

- at least one lowercase alpha character
- at least one number
- an unlimited amount of other characters, like `_`, `!`, `%`

A new password must differ by at least with 5 characters from the old password More information on password strengthening options, can be found in the [pam\\_cracklib](#) manpage. `man pam_cracklib`

### Impact

The password 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 password have expired.

### Priority

Medium

## 2.2.14 Configure user remote login restriction

### Description

Utilize [access.conf](#) to control remoter access to the system for the root and any other user accounts. The configured accounts are restricted to login 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
```

## Caution

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 deny complete access to the system!

### Impact

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

### Priority

medium

## 2.2.15 Set up password for rescue mode

### Description

The root password is needed in rescue mode (`rescue.target`) to access the system. On SLES Operating Systems no change has to be made.

## 2.2.16 Adjust 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, i.e. the Linux network stack. These kernel parameters can be looked up in the `proc` filesystem, 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

Create a configuration file ([man 5 sysctl.d](#) for details) in `/etc/sysctl.d/` and set 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 settings prevents certain kind of IP spoofing attacks, i.e. 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 i.e. 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 in order 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 settings avoids filling up logfiles 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
```

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 e.g. 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. Once 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 and 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

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

## 2.2.17 Allow *root* login only via the first local console (tty1)

### Description

The TTY's provide system access via the console, typically a connected keyboard via a KVM switch or a remote management card (ILO, DRAC, etc). By default, Linux offers 6 different consoles, that can be switched via the key-combinations Alt + F1 - Alt + F6. This setting restricts the access only via a single console (tty1). This access method is only meant for emergency access to the system and should never be used for general system administration tasks.

### Procedure

1. Ensure that /etc/pam.d/login contains the *pam\_securetty* module in the *auth* block:

```
auth    requisite    pam_nologin.so
auth [user_unknown=ignore success=ok ignore=ignore auth_err=die default=bad]
    pam_securetty.so
auth    include      common-auth
```

2. Comment out or remove all tty's in the file /etc/securetty except of tty1.

```
#
# This file contains the device names of tty lines (one per line,
# without leading /dev/) on which root is allowed to login.
#
tty1
```

### Impact

It is not possible to open multiple login-sessions via local KVM sessions or remote-management sessions anymore. This might reduce the administrative comfort, when working locally on a system.

### Priority

low

## 2.2.18 Change home directory permissions from 775 to 700

### Description

By default, home directories of users are accessible (read, execute) by any other user in the system. As this is a potential security leak, home directories should only be accessible by its owner. 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

## 2.2.19 Modify 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 only includes rules for IPv4 at the moment.

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 in order 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).

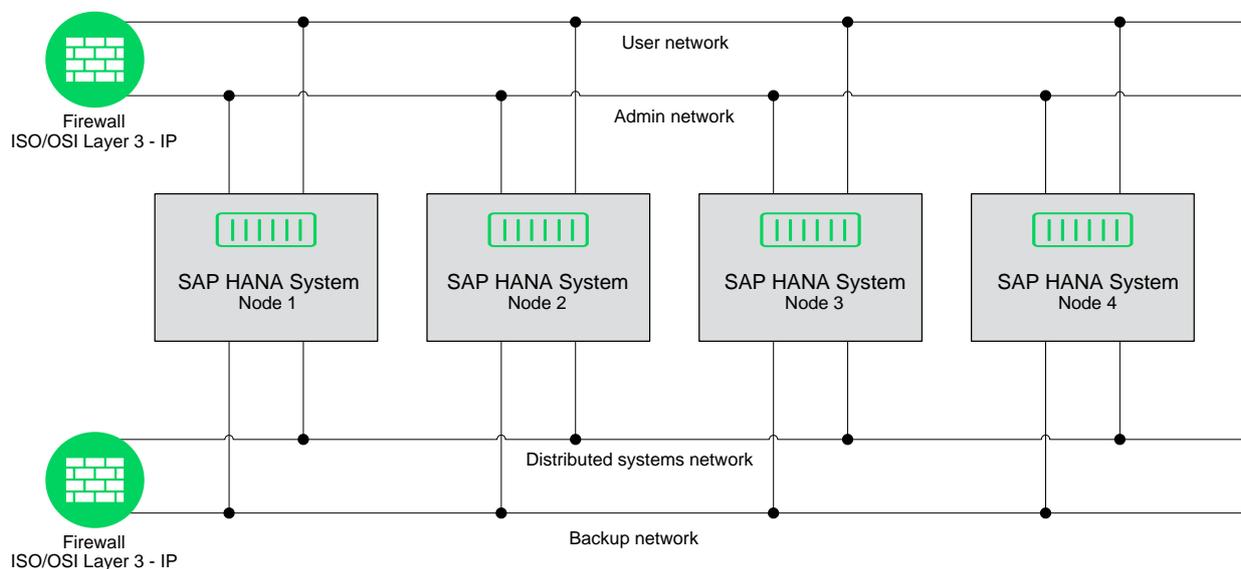


FIGURE 3.1: EXAMPLE OF A SAP HANA NETWORK DIAGRAM WITH EXTERNAL FIREWALLS

All SAP HANA networks should be either isolated (i.e. distributed system networks), or if they require communication from other networks (i.e. 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 not just SAP HANA database systems. In this case, a local running firewall can takeover some of the functionality of an external firewall.

## 3.2 Local Firewall for SAP HANA

The security of a SAP HANA database can be further improved by configuring a local 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: CHECK THIS LIST!!!!!!!!!!!!!!!!!!!! \* Predefined SAP HANA services definitions (according to the SAP HANA Master Guide) \* Able to protect 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

- Simulate option, that prints the iptables commands to the console instead of executing them (What if...)

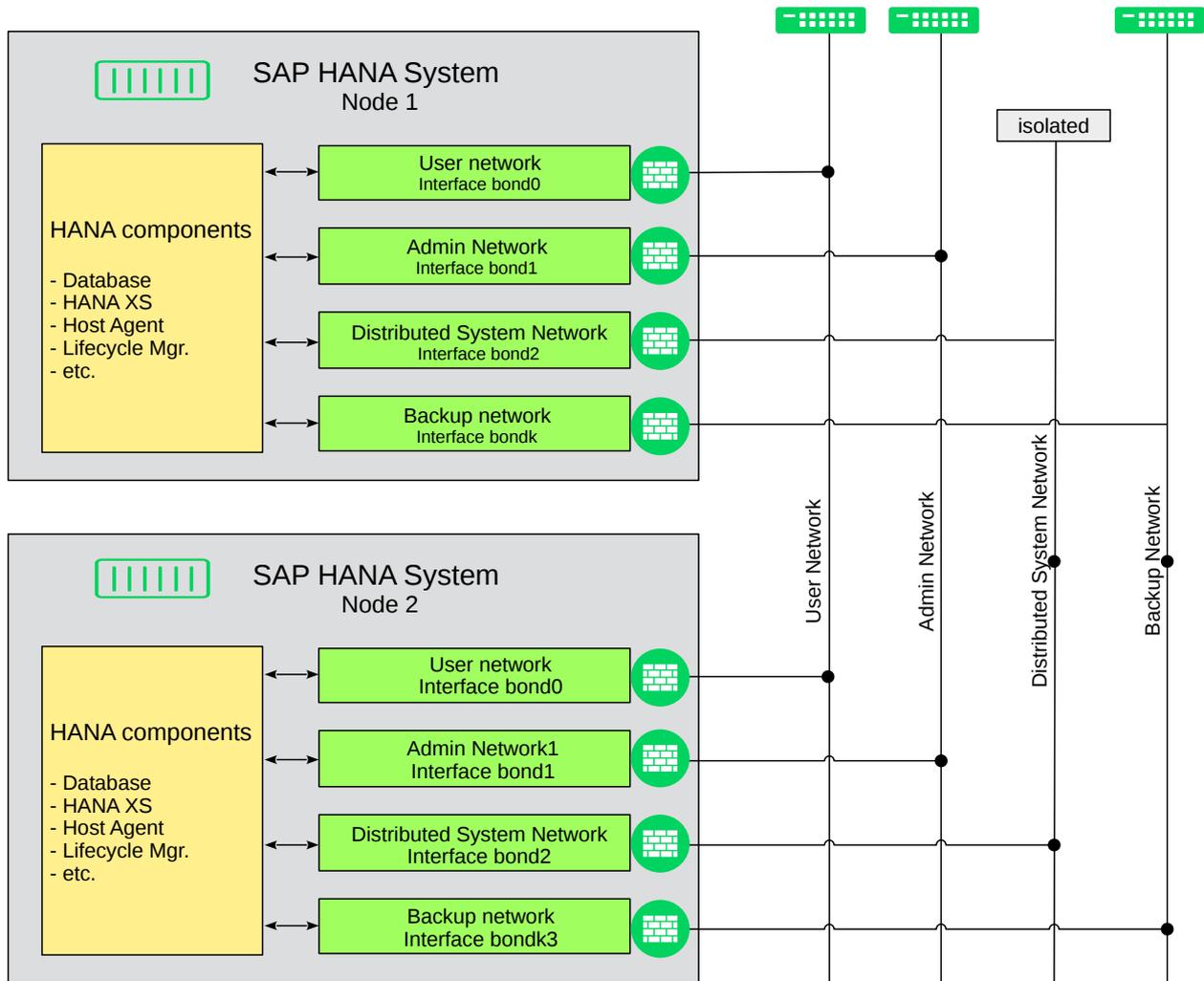


FIGURE 3.2: EXAMPLE OF A SAP HANA FIREWALL NETWORK DIAGRAM

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 and 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 is not available, that protects non-isolated SAP HANA networks from other networks (e.g. user network)
- when an external firewall can not be configured restrictive enough, to only allow network communication for particular SAP HANA ports for certain SAP HANA networks
- when an external firewall provides to less security zones
- when a protected network contains many different servers, i.e. non-SAP servers in the same network

There are also other reasons, when 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.

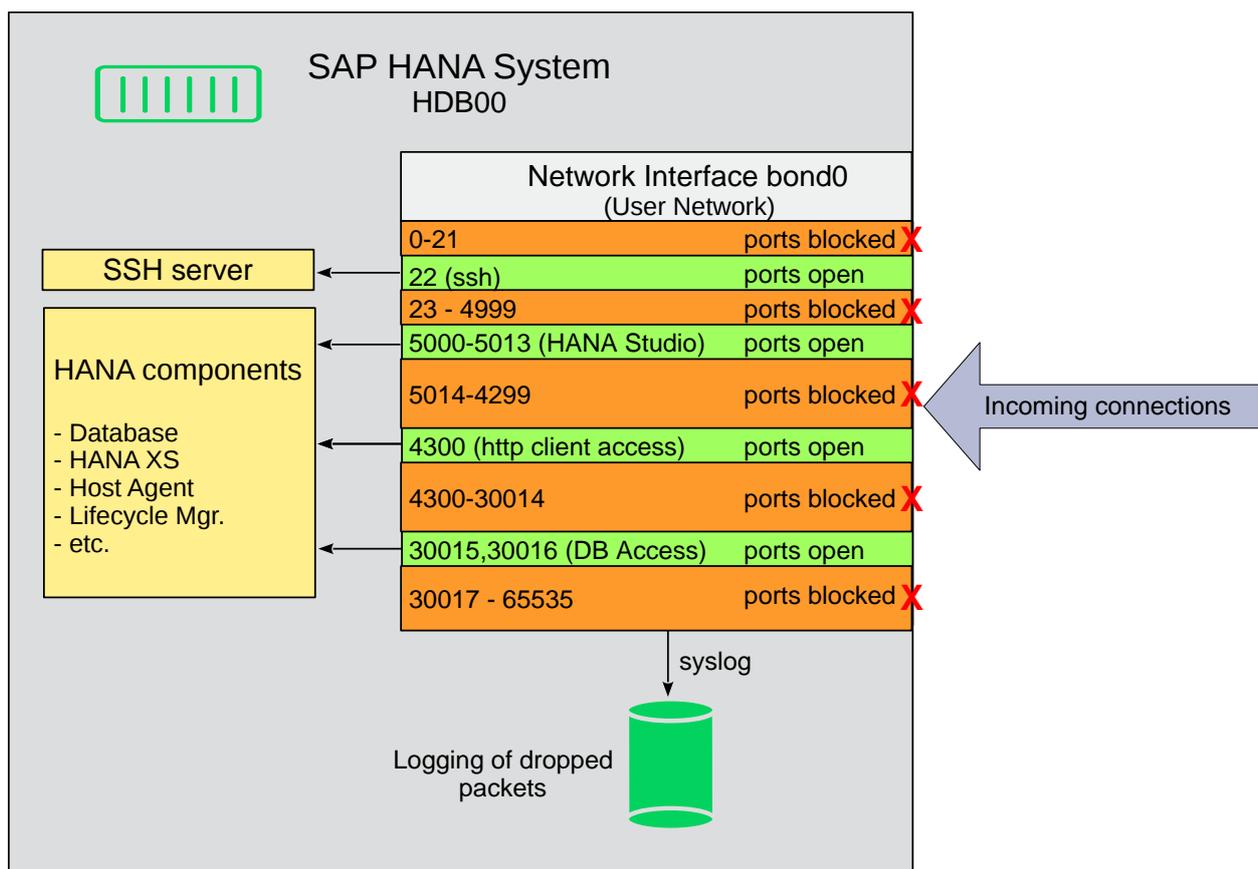


FIGURE 3.3: EXAMPLE OF A SAP HANA FIREWALL NETWORK TRAFFIC FLOW (PORTS ARE EXEMPLARY)

## 3.3 Installation

The SAP HANA firewall is available in the repositories for SLES 15 for SAP Applications and extends firewalld by adding rule sets.

```
zypper install HANA-Firewall
```

The package installs the following files:

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

## 3.4 Configuration

With SLES 15 firewalld replaces SUSE Firewall2 and HANA-Firewall is now an integral part. To get familiar with firewalld please read the chapter "firewalld" in the SLES 15 Security Guide ([https://www.suse.com/documentation/sles-15/singlehtml/book\\_security/book\\_security.html#sec.security.firewall.firewalld](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, first you have to configure firewalld for all non-SAP related services, like SSH.

For configuring the HANA Firewall please follow the instructions in chapter *Configuring HANA-Firewall* in the *SLES for SAP Applications Guide* ([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 commandline.

## 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 even can 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.

### 3.5.2 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 (They also can be found in the tabular overview "TCP/IP Ports of All SAP Products": <https://help.sap.com/viewer/ports>). Most of these services are available as predefined services in the HANA firewall:

TABLE 3.1: LIST OF SHIPPED SAP HANA SERVICE DEFINITIONS (HANA-FIREWALL 1.1.5)

Service Name	Description
<u><a href="#">HANA cockpit</a></u>	More information may be found in the SAP knowledge base article 2389709.
<u><a href="#">HANA database client access</a></u>	Provide access to system database and all tenant databases.
<u><a href="#">HANA data provisioning</a></u>	Event streaming via SQLDBC (ODBC/JDBC) protocol.
<u><a href="#">HANA HTTP client access</a></u>	Allow web browser access to HANA.

Service Name	Description
<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.
<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.

### 3.5.3 Userdefined Services

To create a new service, run

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

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

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

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

## 3.6 Testing & Activation

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

```
systemctl enable firewalld.service
```



## Warning

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

## 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, redo log files or database backups can be encrypted by the SAP HANA itself. For details consult the SAP HANA Security Guide (<https://help.sap.com> ↗).

If the internal encryption of SAP HANA shall or can not be used, you can encrypt directories containing sensitive data via Remote Disk Encrypting available in "SLES 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, the keys are located.

SUSE Remote Disk Encryption uses block devices as an encrypted container for arbitrary directories and 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 could retrieve the keys and decrypt the data.

The "SLES for SAP Applications" guide describes the setup of client and server in chapter "Encrypting Directories Using cryptctl" (<https://www.suse.com/documentation/sles-for-sap-15/> ↗) in detail.

## 5 Minimal OS Package Selection

### 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 a RPM package for each logical component, like an Linux application, a service or a library. A 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 OS installation or later via YaST in order easily get an installation that fits the requirements of a particular use-case, e.g. SAP server with development tools.

Reducing the number of installed RPM packages to a minimum, lowers the amount potentially vulnerable files on the system and therefore 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.

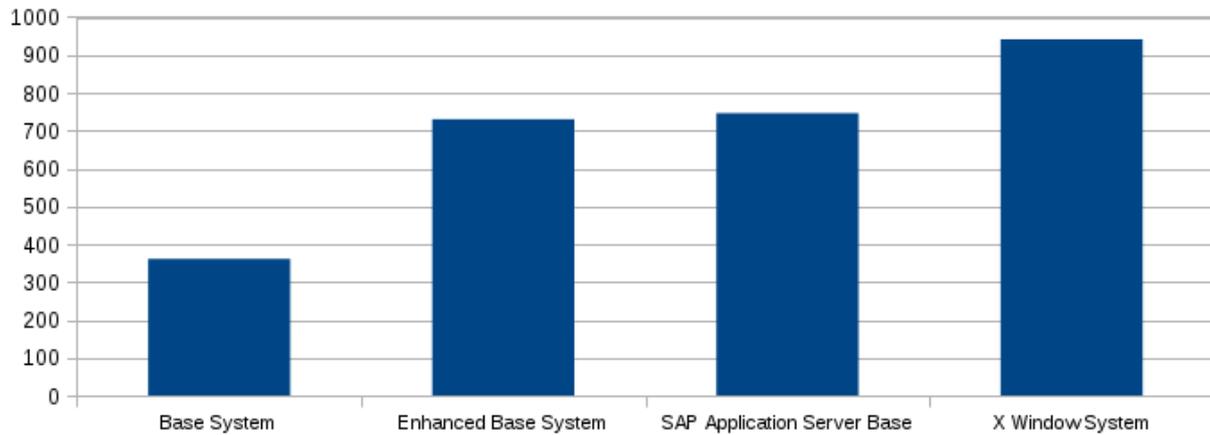
### 5.2 Required Installation Patterns and Packages

**INSTALLATION GUIDE FOR SLES 15 DOES NOT EXIST YET!!** 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 XXXXXXXX - *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") and add the patterns "Enhanced Base System" (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, 941 if "X Window System" has been installed.

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

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



**FIGURE 5.1: COMPARISON OF THE AMOUNT OF INSTALLED PACKAGES BETWEEN CERTAIN PACKAGE SELECTIONS**

## 6 Security Updates

### 6.1 Security Updates for SUSE Linux Enterprise Server 15

As with commercial software, open source software is also frequently tested by hackers and security experts for vulnerabilities – and can contain programming errors what may result in security risks. Many vulnerabilities in the last years became own names and found there way to the world press.

As soon as newly found security vulnerabilities are reported, e.g. on security mailing-lists or by security advisories, the affected code get fixed quickly – sometimes within hours. This is performed 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 arrive there, they are available for all SUSE Linux Enterprise Server customers and should be applied regularly.

### 6.2 SUSE Linux Enterprise Server Update Channels

In order to be able to receive security updates (and other updated packages) on SAP HANA systems, the SUSE update channels must properly be configured. Usually SAP HANA systems do not have direct access to the Internet. This requires a update proxy between the corporate network and the Internet, like our SUSE SMT/RMT server or a SUSE Manager instance.

To verify, if your HANA system has been properly configured 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
```

## 6.3 Update & Patch Strategies

In many cases, organizations have corporate policies in place, that describe requirements on updating and patching of Linux servers.

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

### 6.3.1 Installation of all new updates & 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 Installation of all new updates & 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.

## 6.3.3 Selective installation of new updates & patches (e.g. security updates only)

### Description

A selective installation of patches and updates, e.g. 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*.

### 6.3.4 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 in the SAP Linux Lab), Sören Schmidt (Architect in the SAP Linux Lab) and Alexander Bergmann (Software Security Engineer in the SUSE Maintenance & Security team).

## 9 Further Information & References

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

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

**SAP NOTE "1944799 - SAP HANA Guidelines for SLES Operating System Installation" ABOVE IS NOT THE ONE FOR 15 --> CHANGE AS SOON THE NOTE IS READY**

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

# A Documentation Updates

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

## B Copyright Information

Copyright © 2018 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](#).

For SUSE trademarks, see Trademark and Service Mark list <http://www.suse.com/company/legal/> Linux\* is a registered trademark of Linus Torvalds. All other third party trademarks are the property of their respective owners. A trademark symbol (®, ™ etc.) denotes a SUSE trademark; an asterisk (\*) denotes a third party trademark.

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