Operating System Security Hardening Guide for SAP HANA

Developed for SAP HANA Running on SUSE® Linux Enterprise Server

Guide

www.suse.com

Solution Guide

Server

SAP Partner

SUSE
We adapt. You succeed.

Table of Contents

page

Introduction

IT security is a very important topic in almost any organization. Newspapers report frequently about new IT security incidents like hacked websites, successful denial-of-service attacks and stolen user data like passwords, bank account numbers and other sensitive data.

Aside from the publicly reported attacks, a large number of incidents occur 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 to security risks. This starts with properly set up policies, like a password policy and data protection policies for users and system administrators; continues with a protected IT environment, using, for example, 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 to constantly guarantee maximum security in their IT environment.

Comprehensive security concepts usually pay a lot of attention to database systems, since databases are one of the most critical pieces in each IT environment. Database systems, which potentially store sensitive data, are naturally very popular targets for hackers. Therefore, they must be specially protected.

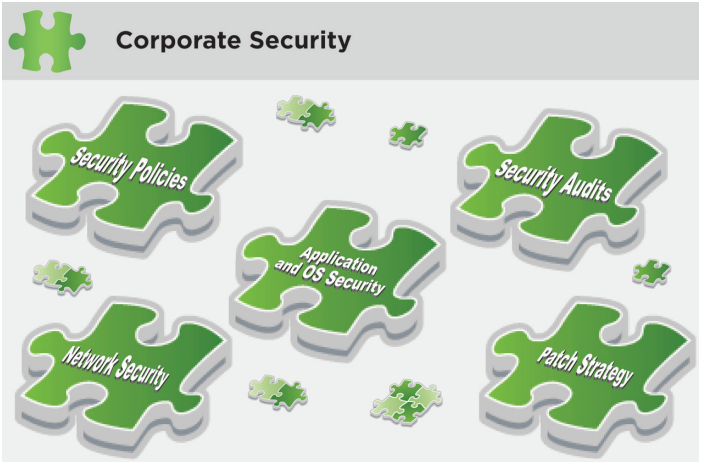

Figure 1. *Elements of corporate IT security*

The SAP HANA database typically stores business-related information, and often this information is critical. In particular, this is the case for ERP systems using SAP HANA as their database. Also many other SAP applications using SAP HANA, like business warehouse (BW) systems, may also store sensitive data in the database.

Security for SAP HANA

SAP pays a lot of high attention to the security. There is a comprehensive SAP HANA Security Guide available that describes in detail how to protect SAP HANA from a database perspective[1]. The guide also refers to security concepts for other connecting layers that are separate from the SAP HANA database: 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 (OS) level.

Security for SUSE® Linux Enterprise Server

At least as important as the security of the SAP HANA database is the security of the underlying operating system. Many hacker attacks are targeted at operating system and not directly at the database. Once a hacker has gained access and sufficient privileges, he or she can continue 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 kinds of security incidents. This package consists of the following components:

- **Security certifications.** *The SUSE Linux Enterprise 11 operating system achieved many important security certifications: Carrier Grade Linux (CGL) Registration, FIPS (Federal Information Processing Standard) 140-2 validation for OpenSSL and Common Criteria Security certification EAL4+.*
- **Security updates and patches.** *SUSE constantly provides security updates and patches for their SUSE Linux Enterprise OSs and guarantees the highest security standards over the entire product life cycle.*
- **Documentation.** *SUSE publishes a security guide that describes the security concepts and features of the SUSE Linux Enterprise Server 11 operating system (***www.suse.com/documentation/sles11/singlehtml/book_hardening/book_hardening.html***). This security guide provides generic security information valid for all workloads, not just for SAP HANA.*

1 **http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf**

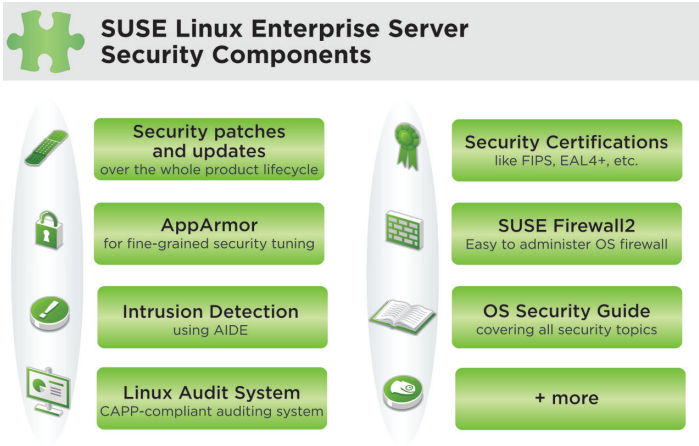

Figure 2. *Security components of SUSE Linux Enterprise Server*

About This Document

To further improve the security standard specifically for SAP HANA, SUSE developed this guide, dedicated to the security hardening of SUSE Linux Enterprise Server 11 running SAP HANA databases. It is meant to fill the gap between the generic SUSE Linux Enterprise Server Security Guide and the SAP HANA Security Guide. 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 with SAP in the SAP Linux Lab to provide the best compatibility with SAP HANA.

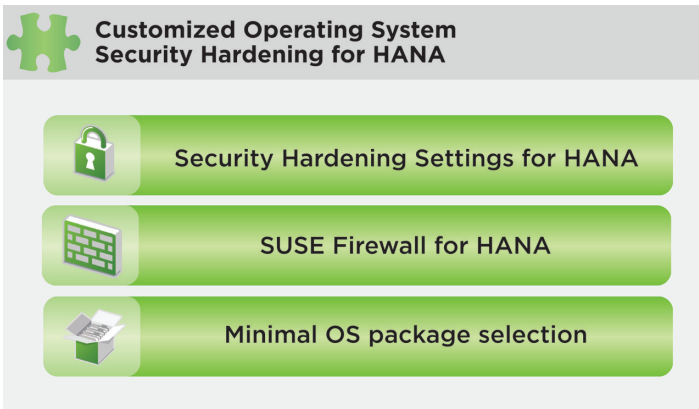

Figure 3. *The three main topics of OS security hardening for SAP HANA*

The guide provides detailed descriptions on the following topics:

- **Security hardening settings for SAP HANA systems.** *A Linux operating system provides many tweaks and settings to further improve OS security and security for hosted applications. To be able to fit certain application workloads, the default settings are not tuned for maximum security. This guide describes how to tune the OS for maximum security specifically when running SAP HANA. It also describes possible impacts, e.g., on system administration, and gives a prioritization for each setting.*
- **Local firewall for SAP HANA.** *SUSE developed a dedicated local firewall for SAP HANA systems. It improves the network security of a SAP HANA database by selectively opening network ports on external network interfaces that are needed either by SAP HANA and any 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 an RPM package and can be downloaded from the SUSE servers.*
- **Minimal package selection.** *The fewer OS packages an SAP HANAsystem has installed, the less possible security holes it might have. According to that principle, this guide describes which packages are absolutely necessary and which packages can be safely discarded. As a nice side effect, a minimized number of packages also reduces the number of updates and patches that have to be applied to a system.*
- **Security updates and patches.** *Open source software gets frequently reviewed and tested for security vulnerabilities. This is performed by open source developers, security engineers from the Open Source Community, security companies and, of course, by the bad guys. Once a vulnerability has been found and reported, it is published in security advisories. Usually it gets fixed very quickly. SUSE constantly provides security updates and patches for all supported packages on SUSE Linux Enterprise Server. This document explains which update and 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 that are relevant for the OS hardening of an SAP HANA system. Together with the other security features of SUSE Linux Enterprise Server 11, like the security certifications (CGL, FIPS, EAL4+) and the constantly provided security updates and patches, SAP HANA can run in a very secure environment, meeting the highest security standards and conforming with the corporate security concepts of organizations of all sizes.

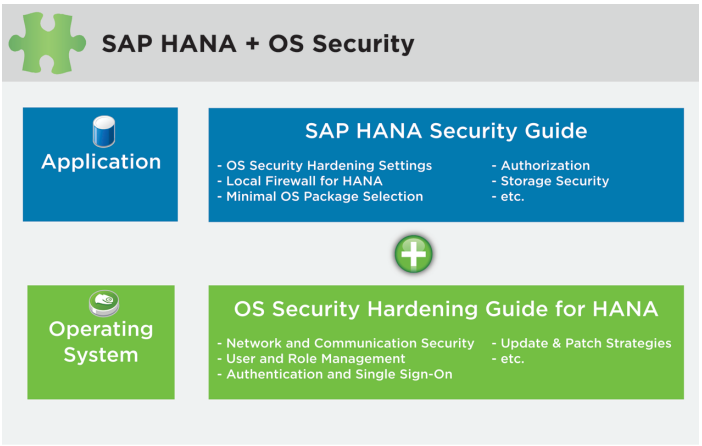

Figure 4. *SAP HANA + OS Security*

SUSE Linux Enterprise Security Hardening Settings for HANA

Introduction into the Linux Security Hardening

The SUSE Linux Enterprise Server already provides a high level of security in its 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 an impact on the comfort of the system administration and possibly also on users of the system. Therefore, the SUSE Linux Enterprise Server 11 standard security settings provide a good tradeoff between compatibility with all workloads, administrative comfort and a secure operating system.

SAP HANA is a 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 is to strengthen the security without affecting compatibility with SAP HANA.

Security hardening provides more security but, as a tradeoff, it reduces administrative comfort and system functionality. This is a fact that every system administrator should be aware of. However, a more restrictively 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 that 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 who is allowed to login, set password policy, etc.*
- **System access settings.** *Define which users are allowed to access the system locally and remotely using different login mechanisms (i.e., local logins via console ttys or remote logins via ssh)*
- **Network settings.** *Define how certain layers of the network stack behave, i.e., the IP layer or the TCP/UDP layer*
- **Service permissions.** *Define the permissions of certain system services, i.e., disabling the 'at' jobs*
- **File permissions.** *Define the file access rights of certain security-critical system files*
- **Logging and reporting.** *Changes the behavior of 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*

SUSE Linux Enterprise Server 11 provides a sophisticated YaST® module for many security settings. This YaST module can be started using the command

```
yast2 security
```

It provides configuration options for several security categories, like hardening settings, password strengthening settings and login settings.

However, hardening an SAP HANA system requires some additional settings that cannot be be configured using the YaST2 security module. Therefore, this guide does not describe how to configure certain settings via YaST. Instead, all hardening setting procedures here describe hardening via the Linux command line.

Hardening Settings for SAP HANA Systems

The following hardening settings are dedicated to improve the security of SUSE Linux Enterprise Server systems running an SAP HANA database. The settings have been developed according to the recommendations of a security audit that was performed on a SUSE Linux Enterprise Server standard installation running an SAP HANA database.

For each hardening setting, the following details are provided:

- **Description.** *Details of each setting*
- **Procedure.** *How to apply a 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 security engineer can decide if the loss of administrative comfort is worth the gain in security. This depends heavily on how the users are using a system and how certain system administrative tasks are performed.

The prioritization can be used to determine which settings have to be applied for certain security requirements. High-priority settings should be applied when possible, whereas low priority settings can be treated as optional.

Disclaimer: *We strongly recommend executing all described hardening settings on a non-productive (i.e., a DEV or QA) system first. We also recommend* ***backing up the system****, or at least the /etc directory, before making any changes. Furthermore, we recommend testing the functionality of the SAP HANA database, all HANA applications and all other applications and services after applying these settings. Since SAP HANA installations and versions, use-cases, hardware and installed services likely differ from our testing scenario, we can not guarantee that all settings work correctly or even 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 be made only within a maintenance window that leaves enough time for a proper system functionality test and a restore of the system (or of the /etc directory).

Hardening Settings Overview

Prohibit login as root via ssh

Description

By default, the user "root" is allowed to remotely log in via ssh. This has two disadvantages. First, root logins are logged, but cannot be associated with a particular user. This is especially a disadvantage if more than one system administrator makes changes on the system. Second, 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.conf and set parameter

```
PermitRootLogin no
```

Impact

Root no longer can be used to login remotely, so that users are required to use "su" or "sudo" to gain root access when using ssh.

Priority: high

Install SUSE security checker

Description

The SUSE security checker performs certain security checks on a regular basis and generates reports. These records are printed to cron, which usually forwards its output via email to root.

Procedure

Install package seccheck

```
zypper in seccheck
```

Impact

Daily reports via email to the root user. Requires a properly set-up email forwarding.

Priority: medium

Configure 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. The forwarding destination can be, e.g., a dedicated email account for the collection of system mails.

Procedure

- Install YaST2-mail add-ons.

```
zypper in yast2-mail yast2-mail-plugins

Start yast: yast mail.
```

- Choose "stdard" configuration.
- Enter the address of the internal mail gateway and configure authentication if required.
- Do NOT enable "accept external SMTP connections."
- Enter the email address for forwarding root emails (typically, a dedicated system mail collection account).
- Save settings.

- Test settings with

```
mail root

subject: test
test
.
```

- Verify with the command mailq if the email has been delivered.

Impact
Requires an accessible SMTP server; requires somebody who regularly checks the mails of the "root" user.

Priority: high

Configure 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.

Forwarding of syslog files to a central syslog server

Description
Logfiles should be forwarded from an SAP HANA node to a central syslog server. This prevents syslog files from being manipulated by an attacker and allows administrators to have a central view of the syslog files.

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

On the target server (running SUSE Linux Enterprise Server)

- Edit /etc/syslog-ng/syslog-ng.conf.
- Un-comment the following line in the "source" section of the configuration file:

```
udp(ip("0.0.0.0") port(514));
```

- Restart syslog-ng using the command

```
rcsyslog restart
```

On the SAP HANA node

- Edit /etc/syslog-ng/syslog-ng.conf.
- Add the following lines and replace <logserver> with the IP or hostname of a valid syslog server:

```
#
# Enable this and adopt IP to send log messages to
a log server.
#

destination logserver { udp("<remote syslogserver
hostname or IP>" port(514)); };
log { source(src); destination(logserver); };
```

- Restart syslog-ng using the command

```
rcsyslog restart
```

- 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

Modify /etc/inittab and comment out ctrl+alt+del trap

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

Procedure

- Un-comment the following line from the file /etc/inittab

```
ca::ctrlaltdel:/sbin/shutdown -r -t 4 now
```

- Reload the content of the inittab using the command

```
cnit q
```

Impact
A system reboot can no longer be performed via a local keyboard or a remote management session. This can be irritating for system administrators, but also helps to prevent accidental reboots.

Priority: medium

Implement cron.allow

Description
The cron.allow file specifies a whitelist of users who are allowed to execute cronjobs via the Linux cron system. Per default no user should be allowed to create cronjobs.

Procedure
Create an empty file /etc/cron.allow using the command

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

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

Impact
SAP HANA users (<sid>adm) and other users are no longer allowed to create their own cronjobs.

Priority: low

Implement at.allow

Description
The at.allow files specify a whitelist of users who are allowed to execute "at" jobs (scheduled one-time running jobs) via the Linux at job execution system. Per default no user should be allowed to create "at" jobs.

Procedure
Create an empty file /etc/at.allow using the command

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

Impact
The UNIX functionality of one-time jobs gets disabled.

Priority: medium

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 and 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 be enabled for selected users only, i.e., admin users.

Procedure
- Edit file /etc/sudoers.
- Comment out the line

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

- Comment in this line

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

- Add all system administrator users to the group wheel by editing the file */etc/group*

```
wheel:x:10:<user names of sysadmin users>
```

Impact
Prohibits sudo command functionality for all users other than the ones who are members of the group wheel. Be aware that the su command is still available for other users.

Priority: high

Adjust default umask

Description
The umask specifies the default XOR-masking for access rights for newly created files. We recommend changing this value to 077.

This will force newly created files and directories to not be read/write/execute enabled for group and world users.

Procedure

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

```
UMASK 077
```

Impact

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

Remarks

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

Priority: high

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.

Adjust the settings according to your corporate security policies.

Procedure

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

```
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 his or her 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 Security Guide section: "3.31. Enabling Password Aging."

Impact

Some login.defs settings, like the password expiration time, reject users who try 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

Set default inactive time to one 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 setting the timeout to one day.

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 one day. We recommend using "screen" to detach sessions before logging out. Screen sessions are not terminated and can be re-attached whenever required.

Priority: medium

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 generally do not recommend using password failure counts because they can be misused for denial-of-service attacks on certain user accounts.

If your corporate policy requires setting up password failure counts for users, please refer to the SUSE Linux Enterprise Security Guide, section: "3.33.3. Locking User Accounts after Too Many Login Failures."

Set 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 passwords that are too simple and too short. In some cases, it is required to configure a strengthened password exactly according to a corporate password policy. This is possible when changing the PAM password authentication settings in the file */etc/pam.d/common-password*.

Procedure
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.

Example:

```
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 the user a maximum of three 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 number of other characters such as '_, !, %'
- A new password must differ by at least five characters from the old password

More information on the password strengthening options can be found in the pam_cracklib manpage.

```
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 no longer login after their passwords have expired.

Priority: medium

Configure user login restriction

Description
Utilize access.conf to deny access to the system for the root account and any other user accounts, except to a number of whitelisted user accounts. The whitelisted accounts are only able to login from a certain IP subnet.

Procedure
- Activate pam_access.so.
- Edit file */etc/pam.d/common-auth-pc*.

```
auth required pam_access.so
```

See man access.conf for configuration details.

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
```

Impact
Only whitelisted users coming from the specified IP subnet are allowed to login. Root login is prohibited.

Priority: medium

Set up password for single user mode

Description
The root password is needed in single user mode to access the system. On SUSE Linux Enterprise Server operating systems no change has to be made.

Adjust sysctl variables

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. The sysctl variables are defined in the file */etc/sysctl.conf*. The corresponding kernel parameters can be looked up in the /proc filesystem, in the subdirectory /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 making all changes in the sysctl.conf 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 directs the answer packet to a different outgoing interface according to the routing table, this packet is discarded.

The setting prevents certain kind of IP spoofing attacks, i.e., those used for DoS 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., 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 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
```

Prevents hijacking of routing path by only allowing redirects from gateways known in the routing table.

```
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, i.e., 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. Exceeding the queue, 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 databases 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. Because SAP HANA databases 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

Allow "root" login only via the first local console (tty1)

Description
The TTYs 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 six different consoles, which can be switched via the key combinations Alt+F1—Alt+F6. This setting restricts the access 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
Comment out or remove all tty's in file */etc/securetty* except for tty1.

Impact
It is no longer possible to open multiple login sessions via local KVM sessions or remote management sessions. This may reduce the administrative comfort when working locally on a system.

Priority: low

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 be accessible only by their 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 $(ls /home); do echo "Changing rights for
directory $a"; chmod 700 /home/$a; done
```

Impact
System users are no longer allowed to access other users' home directories. An exception is made for <sid>adm users with their home directories in /usr/sap/<sid>/home.

Priority: medium

Make access rights 700 the default of a home directory when adding a new user

Description

The UMASK setting in /etc/login.defs should be set to 077, so that files and directories are only accessible by the owner *(see also Adjust default umask on page 8)*. This also includes newly created home directories, i.e., with the adduser command.

Modify permissions on certain system files

Description

Many system files are group- or world-readable by default. Especially 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 their security.

SUSE provides the tool chkstat to check and set file permissions of certain files, which are defined in one of the following configuration files:

- permissions.local
- permissions.easy
- permissions.paranoid
- permissions.secure

The permissions.local file is dedicated to user-defined file permissions.

Procedure

For SAP HANA systems we recommend to using the permissions.easy pattern plus some additional file permissions that will be stored in the permissions.local pattern.

First, 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:root        0400
/etc/inittab                  root:root        0400
/etc/syslog-ng/syslog-ng.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.weeky               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:tty         0600
# /var/log/wtmp               root:tty         0600
```

Then, install the patterns permissions.secure and permission.local in the right order.

```
chkstat --set permissions.secure
chkstat --set permissions.local
```

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

Priority: medium

SAP HANA Firewall

SAP HANA Network Communication

The SAP HANA Security Guide (section 4.2 "Network Security") 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 database is connected by 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). The physical interfaces can also be virtual interfaces.

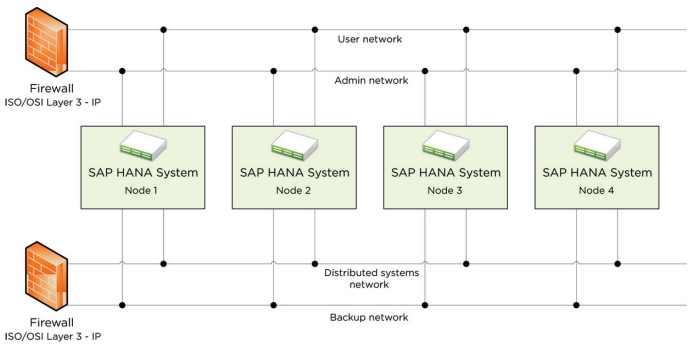

Figure 5. *Example of an SAP HANA network diagram with external firewalls*

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 an SAP HANA network that is required for communicating 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.

Local Firewall for SAP HANA

The security of an 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 system services are listening. Communication to all other ports should be dropped and optionally be logged. This complies with the "minimal communication approach" suggested in the SAP HANA Security Guide.

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

The firewall provides the following features:

- *Predefined SAP HANA services definitions (according to the SAP HANA Master Guide)*
- *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*
- *Option to log dropped packets to a firewall logfile*
- *Simulate option, which prints the iptable commands to the console instead of executing them (what if...)*

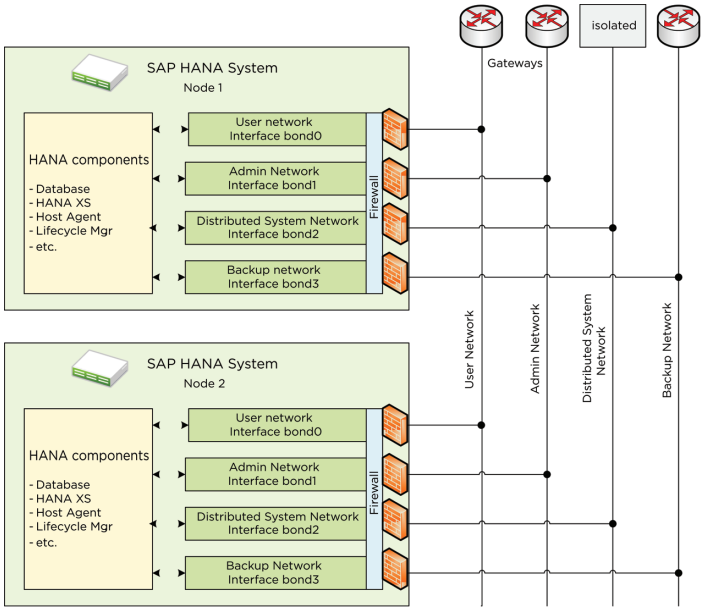

Figure 6. *Example of an SAP HANA Firewall Network Diagram*

Not every SAP scenario requires 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 that protects non-isolated SAP HANA networks from other networks (i.e., user networks) is not available.*
- *When an external firewall cannot be configured to be sufficiently restrictive enough to only allow network communication for particular SAP HANA ports for certain SAP HANA networks*
- *When an external firewall does not provide enough security zones (i.e., Internal, External, DMZ are not sufficient for all SAP HANA networks in some cases)*
- *When a protected network contains many different servers, i.e., non-SAP servers in the same network*

There are also other circumstances when a local firewall could makes sense. For example, a local firewall prevents unwanted services or deamons from listening on TCP or UDP ports and receiving connections. This occurs because all not specifically allowed network ports are blocked by default. Also, unauthorized network traffic received on blocked ports can be logged. This allows easy identification of unwanted connection attempts. Last but not least, a local firewall can be a set requirement of corporate security policies or security audits.

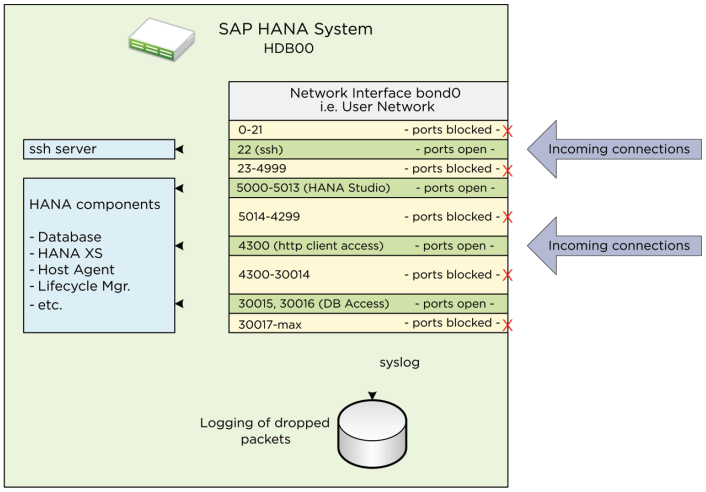

Figure 7. *Example of an SAP HANA firewall network traffic flow*

Download and Installation

The SAP HANA firewall is available as an RPM package. The base URL of the package is: **http://download.opensuse.org/repositories/home:/abergmann:/HANA**

Note: *It is possible that this location will change in the future. Please check for later versions of this document if this download location is no longer available.*

Before installing the SAP HANA firewall, we recommend de-installing the SuSEFirewall2 package first. It is not possible to run both firewalls in parallel. You de-install the SuSEFirewall2 using the commands:

```
# Stop possibly running SUSE Firewall
rcSuSEfirewall2 stop
# Remove the SuSEFirewall2 package
zypper rm SuSEFirewall2
```

The SAP HANA Firewall package can be either downloaded and installed manually or added to the respective package repository, to the list of update repositories and then using YaST or zypper for the installation. The latter method requires the system to have direct access to the Internet.

```
# Manually download & installation of the package
wget http://download.opensuse.org/repositories/
home:/abergmann:/HANA/SLE_11_SP3/noarch/HANA-
Firewall-1.0-0.2.1.noarch.rpm
zypper install HANA-Firewall-1.0-0.2.1.noarch.rpm
# Adding the HANA firewall update repository and
install via zypper
zypper addrepo -f 'http://download.opensuse.org/
repositories/home:/abergmann:/HANA/SLE_11_SP3/'
HANA-Tools
zypper refresh -s
zypper install HANA-Firewall
```

The package has an intended conflict with the SuSEFirewall2 package. When installing the SAP HANA firewall package without having removed the SuSEFirewall2 package first, you get an installation conflict warning with several options for a resolution. In this case, choose to de-install the SuSEFirewall2 package and to install the SAP HANA firewall package.

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.
/etc/init.d/hana_firewall	SysVinit start/stop script. A usage description can be printed when calling the script without any argument.
/etc/sysconfig/hana_firewall	Main configuration file
/etc/sysconfig/hana_firewall.d	Directory for SAP HANA services and user-defined services
/etc/sysconfig/hana_firewall.d/create_new_service.pl	Little helper script to create a new SAP HANA service
/etc/sysconfig/hana_firewall.d/*	Definition files for SAP HANA services and user defined services

Configuration

PREREQUISITES

Make sure that you have no other local firewall running and that there is no other firewall that starts automatically after a reboot. Check, i.e. with the following commands:

```
# Check for enabled firewalls in SysVinit
chkconfig -a |grep -i firewall
# Check for possibly running firewall
iptables -L
```

QUICK CONFIGURATION GUIDE

This quick configuration guide provides a small setup procedure for a simple SAP HANA Firewall setup.

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>, i.e., HDB00.
3. Edit the network interface / service mappings using the INTERFACE_<n> and the INTERFACE_<n>_SERVICES parameters.

1. If you have only one network interface (named eth0), just make the following configuration and continue with the next step:

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

2. If you have multiple network interfaces, configure an INTERFACE_<n> and INTERFACE_<n>_SERVICES parameter for each interface.
3. Add the predefined SAP HANA services and all other services (i.e., ssh) that should be opened on a particular interface as a space separated list.

4. Save the hana_firewall configuration.
5. Test the firewall using the commands:

```
hana_firewall --simulate start
hana_firewall start
hana_firewall show
```

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 may no longer be able to login.
8. Restart the firewall using the command:

```
hana_firewall restart
```

9. Make sure that the firewall gets started on bootup.

```
chkconfig hana_firewall on
```

DETAILED CONFIGURATION INSTRUCTIONS

The configuration of the SAP HANA firewall is stored in the file /etc/sysconfig/hana_firewall. It can be edited manually, i.e., using vi or via the YaST2 Sysconfig editor.

```
yast2 sysconfig
```

The configuration is divided into two categories: Global Parameters and Interfaces. In the Global Parameters section, parameters like the installed SAP HANA systems/instances are configured. In the Interfaces section, the network interface / service mappings are defined.

Global Parameters Section

List of SAP HANA systems and instance numbers

Description:
This setting contains a list of SAP HANA systems and instance numbers in a space separated list. The format is <SID><INSTNACE NR>, i.e., HNA00. Based on these values, the firewall automatically creates ports and port ranges for the SAP HANA firewall services mentioned below.

Example:

```
HANA_SYSTEMS="HNA00"
```

Open SSH on all devices

Description:
Opens the ssh (secure shell) port on all interfaces. This is useful for testing purposes to avoid accidentally locking out admin users. In the firewall configuration, ssh should be enabled only for one interface. This global setting should be TURNED OFF in the final configuration!

Example:

```
OPEN_ALL_SSH="yes"
```

Log dropped packets to syslog

Description:
Enabling this option causes the SAP HANA firewall to log dropped packets to syslog in /var/log/firewall. In order to prevent syslog storms, it limits the number of logged packets to five packets / minute, with a burst rate of ten packets.

This option can be useful to identify attacks and portscans, but it also helps to identify valid remote connection attempts that require additional ports opened in the firewall.

Example:

```
ENABLE_LOGGING="yes"
```

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, such as 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/sysconfig/hana_firewall.d

as well as all service names from /etc/services.

A special SAP HANA service called HANA_* includes all SAP HANA services.

Detailed service descriptions can be found in the appropriate service definition files in the directory /etc/sysconfig/hana_firewall.d or in the document section Predefined Services on this page.

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"
```

Services

SERVICE DEFINITIONS

Services can either be service names from the file /etc/services or they can be defined as SAP HANA firewall services.

The SAP HANA firewall service definitions are stored in the directory /etc/sysconfig/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>, i.e., 10000:20000/

EXAMPLES:

```
TCP="22"
UDP=""
```

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

To create a new user defined service, you can use the script create_new_service.pl:

```
cd /etc/sysconfig/hana_firewall.d
./create_new_service.pl
```

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

PREDEFINED SERVICES

SAP HANA Services

The SAP HANA Master Guide describes all services and the required TCP/UDP ports that SAP HANA uses. All of these services are available as predefined services in the SAP HANA firewall.

Here is a list and a short description of all SAP HANA services. For more information please consult the SAP HANA Master Guide, section: "2. The SAP HANA Network."

Most SAP HANA services select port numbers dependent on the Instance Number of a SAP HANA system. The firewall automatically expands all in the main configuration defined SAP HANA Instance Numbers to the correct port numbers.

Service Name	Description *(for more information, please consult the SAP HANA Master Guide)*	Ports *(xx = Instance nr, xy = Instance nr + 1)*
HANA_DATABASE_CLIENT	Open ports for application servers that use SAP HANA as a database	TCP="3xx15 3xx16"
HANA_DATA_PROVISIONING	This connection is used for event streaming. The protocol is SQLDBC (ODBC/JDBC).	TCP="3xx15 3xx17"
HANA_HTTP_CLIENT_ACCESS	Open ports for web browser client access to SAP HANA	TCP="80xx 43xx"
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	TCP="3xx09"
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.	TCP="3xx00 3xx01 3xx02 3xx03 3xx04 3xx05 3xx07 3xx10 3xx40:3xx99"
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).	TCP="5xx13 5xx14"
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).d	TCP="1128 1129"
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.	TCP="3xy01 3xy02 3xy03 3xy04 3xy05 3xy07 3xy40:3xy99"
HANA_*	Special service that includes all SAP HANA services	

USER SERVICES

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

Service Name	Description	Ports
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. MOUNTD_PORT="10050" STATD_PORT="10051" LOCKD_TCPPORT="10052" LOCKD_UDPPORT="10052" RQUOTAD_PORT="10053" STATD_OUTGOING_PORT="10054"	TCP="10050:10054 10050:10054 111 111 2049 2049" UDP="10050:10054 10050:10054 111 111 2049 2049"

Testing and Activation

TESTING THE FIREWALL

After the firewall has been properly configured, it should carefully be tested. To perform the basic tasks you can run the SysVinit script /etc/init.d/hana_firewall. However, we recommend using the SAP HANA firewall executable /usr/bin/hana_firewall directly for testing.

First, you should simulate the start with the "--simulate" option. This option just prints the iptables commands to STDOUT instead of actually executing the iptable commands.

```
hana_firewall --simulate start
```

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

```
hana_firewall start
```

Note: *If you have an error in your configuration, you will get a detailed description of what went wrong.*

After the firewall is started without errors, you can list all installed iptables rules using the command

```
hana_firewall show
```

After you have made any changes in the configuration, you must restart the firewall:

```
hana_firewall restart
```

If you are finally satisfied with your firewall ruleset, you might want to turn the global parameter "OPEN_ALL_SSH" to "no" in the firewall configuration file. Make sure that you have configured the ssh service for at least one interface.

ENABLING THE FIREWALL

To start the firewall on system boot automatically, you have to enable the firewall service in SysVinit, i.e., using the command:

```
chkconfig hana_firewall on
```

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

Minimal OS Package Selection

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 against a local or remote attack. Therefore, it is recommended to have as few 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, such as a Linux application, a service or a library. A RPM package groups all files that belong to this particular component, including executables, other binaries, configuration files and documentation files. The most common packages are grouped by use cases as "Installation Patterns." These patterns can be selected i.e., during the OS installation or later via YaST, in order to easily get an installation that fits the requirements of a particular use case, e.g., an SAP server with development tools.

Reducing the number of installed RPM packages to a minimum lowers the number of potentially vulnerable files on the system and, therefore, significantly improves the overall security of a system. Furthermore, a small 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 available that are not part of the standard installation. This makes it difficult to follow a JeOS approach. JeOS stands for "Just enough Operating System" and defines the bottom-up approach when installing a Linux system. It means that the initial OS installation is based on a minimal set of packages, and additional packages are only added if they are absolutely necessary. For an SAP HANA system the JeOS approach is impossible because it has to consider all eventualities of certain SAP HANA installations, including different configurations, versions, add-ons, etc. The probability that this approach leads to missing packages that cause incompatibilities would be too high.

Therefore, the current approach to a minimal package selection is a middle ground between a SUSE Linux Enterprise Server standard installation and a JeOS installation. The strategy is to use the SUSE Linux Enterprise Server installation patterns "Base System" + "Minimal System" and optionally to add some additional packages required when contacting the support.

Required Installation Patterns and Packages

The minimal OS package installation for SAP HANA that is supported by SAP is described in SAP note "#1855805—Recommended SLES 11 packages for HANA support on OS level."

It is strongly recommended to install at least these two patterns:

- *Base System*
- *Minimal System (Appliances)*

This results in a total number of around 550 packages, compared to 1200 packages in a standard installation.

In case of a support inquiry, the support might ask to install some additional packages. These packages are listed in the following table:

bing	A Point-to-Point Bandwidth Measurement Tool
bonnie	File System Benchmark
cairo	Vector Graphics Library
findutils-locate	Tool for Locating Files
graphviz	Graph Visualization Tools
iptraf	TCP/IP Network Monitor
krb5-32bit	MIT Kerberos5 Implementation—Libraries
krb5-client	MIT Kerberos5 Implementation—Client Programs
nfs-client	Support Utilities for NFS
sensors	Hardware health Monitoring for Linux

Some of these packages have additional dependencies, i.e., to some X11 libraries, which results in a total number around 750 packages. It is recommended to install these additional packages during the OS installation by default.

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

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

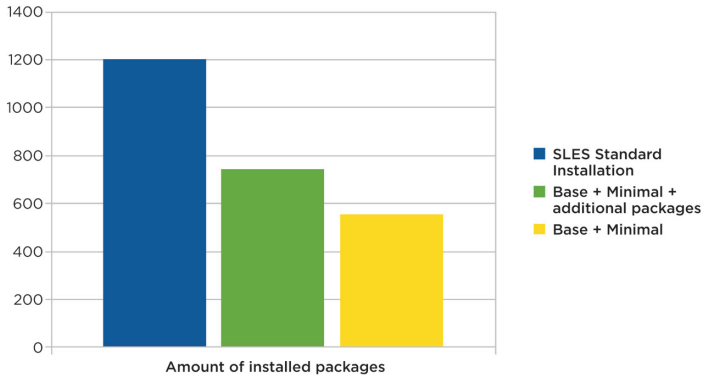

Figure 8. *Comparison of the number of installed packages between certain package selections*

Hint: *If you want to enable X11 forwarding for remote ssh connections ("ssh -X" or "ssh -Y"), the additional package xorg-x11-xauth is required. X11 forwarding via ssh is useful, e.g.,when using the graphical SAP HANA installer.*

Security Updates

Security Updates for SUSE Linux Enterprise Server 11

As any other commercial software, open source software is frequently tested by hackers and security experts for vulnerabilities—and often they are successful. Also open source software contains programming errors, and some of them lead into security leaks. Probably the most common programming error that often leads to a vulnerability is buffer overflow. It allows an attacker to overwrite protected memory areas with his or her own code. One of the most famous buffer overflow vulnerabilities in the last years was found in the OpenSSL library. It is well known as the "heart bleed bug." SUSE Linux Enterprise Server 11 was, luckily, not affected by this vulnerability.

As soon as newly found security vulnerabilities are reported, i.e., 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.

SUSE Linux Enterprise Server Update Channels

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

To verify that your SAP HANA system has been properly configured to receive security updates and also has been registered to the SUSE update channels, the following command can be used:

```
zypper lr
```

This command listens to the available software repositories of a SUSE Linux Enterprise Server instance. The output should show the update channel "SLE11-SP3-Updates" for a SUSE Linux Enterprise Server 11 SP3 system. On SUSE Linux Enterprise Server for SAP Applications 11 SP3 systems, the channels "SLE11-SP3-SAP-Updates" and "SLES11-SP3-SAP-Updates" should also be present.

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
```

More information on how to properly configure SAP HANA systems to receive updates can be found in the document "SUSE Linux Enterprise Server Maintenance Made Simple" available in our resource library[2].

Update and Patch Strategies

In many cases, organizations have corporate polices in place that describe requirements on updating and patching Linux servers. In most cases, they also take security measures into consideration, e.g., keeping the timeframes between maintenance windows short.

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

INSTALLATION OF ALL NEW UPDATES AND PATCHES ON A REGULAR BASIS

Description: Installation of new updates and patches, for example, 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 and patches (including 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 and patches might cause problems.

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

INSTALLATION OF ALL NEW UPDATES AND PATCHES DURING MAINTENANCE WINDOWS

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

Advantages: Problematic updates will not put a productive SAP HANA system in danger.

2 **www.suse.com/de-de/products/sles-for-sap/resource-library/**

Disadvantages: Since maintenance windows usually have long timeframes 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.

SELECTIVE INSTALLATION OF NEW UPDATES AND PATCHES (I.E., SECURITY UPDATES ONLY)

Description: A selective installation of patches and updates, i.e., security updates only, further reduces the probability of installing problematic updates. Most times, this strategy is combined with updating systems on a regular basis. The selective installation of packages can be performed using zypper (see example in section "SUSE Linux Enterprise Server Update Channels") or with SUSE Manager. All remaining package updates (i.e., updates with bugxfixes) should also be installed from time to time, i.e. during maintenance windows.

Advantages: Mostly up-to-date system with (almost) all security patches installed

Disadvantages: All packages, that are not in the custom selection (i.e. packages, belonging to the security category) are not installed immediately

Recommendation: Probably the best update strategy

NOT UPDATING AN SAP HANA SYSTEM

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 that you subscribe to the SUSE update channels and 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 and patching policies / guidelines as well as on the requirements for a particular SAP HANA system. For important SAP HANA systems (e.g., productive ERP databases), 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.

Outlook

Even though this guide already covers most security hardening topics, we are planning 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. We plan to incorporate these new requirements as soon as they occur.

The following list gives you an idea of some of the planned enhancements that might come with future versions of this document:

- **Hardening settings:** *Provide additional hardening settings and hardening setting patterns for different SAP HANA installation and use cases*
- **Firewall:** *Improvements in the firewall configuration, e.g., automatic detection of installed SAP HANA database systems*
- **Minimal package selection:** *Further reduce the number of required packages for an SAP HANA installation*

We recommend checking for updated versions of this document from time to time in the resource library on the SUSE website[3].

About the Authors

This document has been developed by Markus Guertler, who is working as Architect & Technical Manager SAP in the SAP Linux Lab, and Alexander Bergmann, who is working as Software Security Engineer in the SUSE Maintenance & Security team.

3 **www.suse.com/products/sles-for-sap/resource-library/**

Further Information and References

The following table gives an overview about sources for further information on topics discussed in this guide:

SUSE Security Portal	**www.suse.com/security**
SUSE Linux Enterprise Server Security Guide	**www.suse.com/documentation/sles11/singlehtml/book_security/book_security.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**
Recommended SLES 11 packages for HANA support on OS level	SAP note #1855805
SUSE Linux Enterprise Server 11 Installation Notes	SAP note #1310037

If you have any questions, comments or feedback on this document, please do not hesitate to contact us at the following email address: **saphana@suse.com**

Contact your local SUSE Solutions Provider, or call SUSE at:

1 800 796 3700 U.S./Canada
1 801 861 4500 Worldwide

SUSE
Maxfeldstrasse 5
90409 Nuremberg
Germany

www.suse.com

SAP Partner

SUSE
We adapt. You succeed.