



Red Hat Enterprise Linux Security Hardening Guide for SAP HANA

Version 2.0

SAP Alliance Team

Last Modified: Apr 2022

Contents

1. Overview of Security	3
2. About this document	3
3. Red Hat Enterprise Linux Security Hardening Settings for SAP HANA	4
3.1 Introduction	4
3.2 Minimal Required Installation Pattern and Package option	6
3.2.1 compat-sap-c++ (C++ compatibility runtime library for SAP applications)	8
3.2.2 libtool-ltdl	9
3.3 Disable unnecessary Network Services	9
3.3.1 Disable Telnet	10
3.4 Restrict sudo	11
3.5 Disabling root logins via SSH	12
3.6 Lock out a user to login after a set number of failed attempts	13
3.7 Network Bound Disk Encryption (NBDE)	16
3.8 fapolicyd	20
4. SAP HANA Network and Communication Security	22
4.1 Communication Channels	23
4.2 Network Security	23
4.3 SSL Configuration on the SAP HANA Server	25
4.4 Secure Operating System User- <sid>adm	26
5. SELinux	27
Enable SELinux in permissive mode	29
Enable SELinux in enforcing mode	30
Verification steps	32
5.4 How to create exceptions in SELinux	33

6. Security Updates	34
6.1 Planning and Configuring Security Updates and Patches	34
6.2 Updating and Installing Packages	35
6.3 Using the Security Features of Yum	35
7. Further Information and References	36

1. Overview of Security

Businesses today are faced with the almost insurmountable task of complying with a confusing array of laws and regulations relating to data privacy and security. These can come from a variety of sources: local, state, national, and even international lawmakers. Due to the increased reliance on powerful, networked computers to help run businesses and keep track of our personal information, entire industries have been formed around the practice of network and computer security. Enterprises have solicited the knowledge and skills of security experts to properly audit systems and tailor solutions to fit the operating requirements of their organization. Because most organizations are increasingly dynamic in nature, their workers are accessing critical company IT resources locally and remotely, hence the need for secure computing environments has become more pronounced.

IT Security is a general term that covers a wide area of computing and information processing. Industries that depend on computer systems and networks to conduct daily business transactions and access critical information regard their data as an important part of their overall assets. In some industries, the availability and trustworthiness of data can mean the difference between success and failure. Protecting corporate information is one of the most important topics. The main focus is to keep the systems secure, and stay on top of the compliance and regulatory requirements of today's digital world.

2. About this document

This guide provides instructions and practices on how to secure the Operating System RHEL 8 for running SAP HANA. The goal of this document is to increase security features on RHEL by minimizing the required packages, disabling unnecessary network services, secure user permissions, restrict sudo, SAP HANA Network and Communication Security as well as security updates. Red Hat Enterprise Linux provides many different settings and configurations to improve Operating Security according to the [Red Hat Enterprise Linux 8 Security Guide](#). This guide describes how to secure the required RHEL specifics for running SAP HANA, and describes the procedure needed at each step.

Outside of the security context, please always refer to the official SAP and Red Hat documents in order to properly configure the RHEL operating system. The list of the SAP HANA related documents can be found at: <https://wiki.scn.sap.com/wiki/x/rDK7Gg>

3. Red Hat Enterprise Linux Security Hardening Settings for SAP HANA

3.1 Introduction

OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware remote hackers. The hacker's target in most of the cases are Operating Systems. If the hacker has gained any access to the system with sufficient permissions and privileges, it is very easy for him or her to attack any application installed on the OS and even databases. Red Hat Enterprise Linux contains a lot of security driven configurations to protect the system from attacks, which can improve the overall durability of the operating system and its applications. These settings can be summarized in the following categories:

- Security Tips for Installation
- Keeping your system up-to-date
- Hardening your system with tools and services
- Using firewalls
- System Auditing
- Compliance and Vulnerability Scanning with OpenScap
- Federal Standards and Regulations

For more information please refer to the [Red Hat Enterprise Linux 8 Security Guide](#).

Operating System security is the process of ensuring OS integrity, confidentiality and availability, which SAP HANA database is running on.

Security Hardening for SAP HANA is the entry point for all information relating to the secure operation and configuration of SAP HANA. The following hardening settings are recommended for the improvement of the security for Red Hat Enterprise Linux Server upon a SAP HANA database. Security Hardening on the one hand brings the system to a more secure level, but on the other hand reduces administrative and system functionality. The goal is to have a more restrictive configured system, which will provide a better level of protection and a lower risk of attacks. 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 on how the users are using a system and how certain system administrative tasks are performed.

Note: before making any changes or editing the files according to the guide, It is recommended to execute all mentioned hardening settings and steps on a non-productive system. It is also recommended to back up the system, at least make a backup of the /etc directory. In addition to this, since the SAP HANA installations and versions, hardware and installed files differ from each testing scenario and environment in this guide, Red Hat cannot ensure that all settings work correctly as described in the guide or even have a negative effect on the functionality of the system.

For each hardening setting, the following details are provided:

- **Description.** Details and Info of each setting
- **Procedure.** How to configure a setting
- **Impacts.** Possible impacts for system administrators or users
- **Priority.** Low, Medium, High

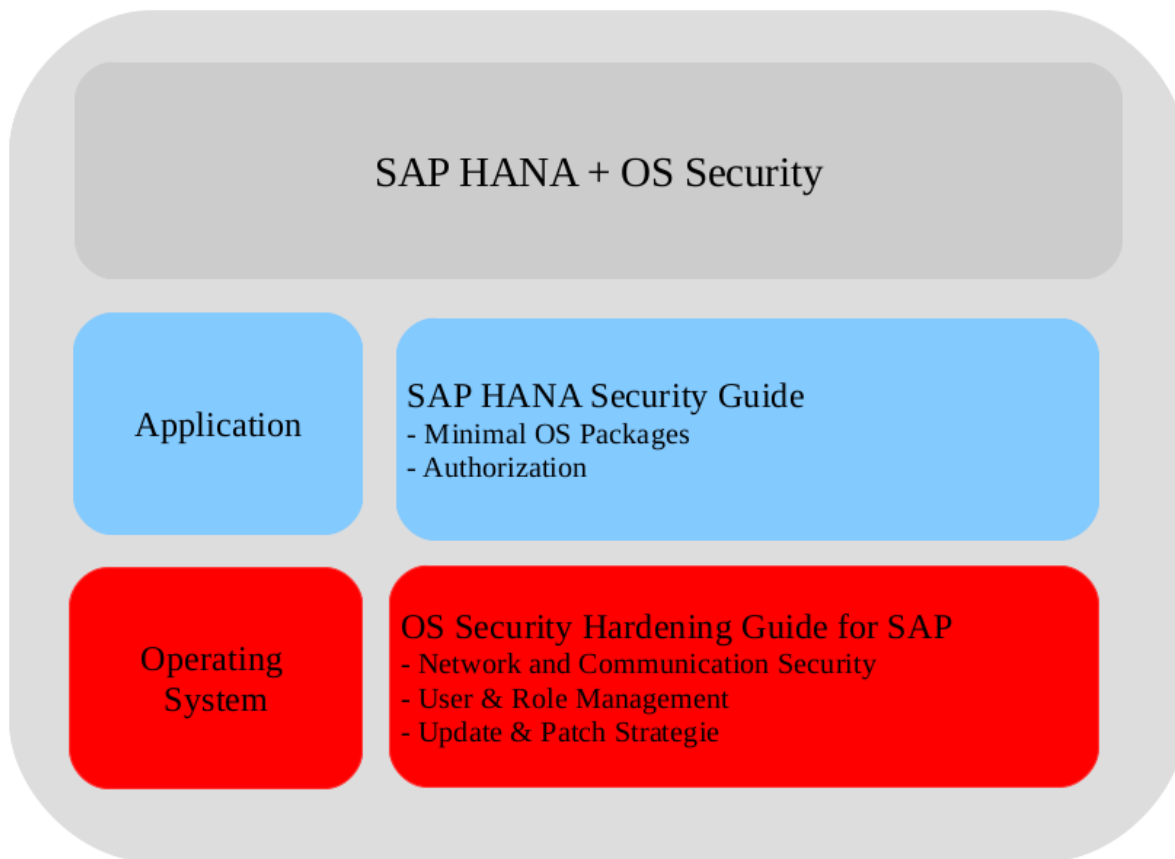


Figure 1. SAP HANA + OS Security

3.2 Minimal Required Installation Pattern and Package option

Description

This part of the guide explains which packages are necessary for running a standard SAP HANA on RHEL. By default, the Red Hat Enterprise Linux installation process loads a selection of software that is suitable for a system deployed as a basic server. It is best practice to install only the packages you will use because each piece of software on the computer could possibly contain a vulnerability. If you are installing from the DVD media, take the opportunity to select exactly what packages you want to install during the installation. During the RHEL installation, the user has most of the choices for the installation.

The **Package Installation Defaults** screen appears and details the default package set for the Red Hat Enterprise Linux installation. This screen varies depending on the version of Red Hat Enterprise Linux you are installing.

Note: If you Install Red Hat Enterprise Linux in text mode, you cannot make package selections. But if the installation of Red Hat Enterprise Linux is not in text mode, the installer automatically selects packages only from the base and core groups. These packages are sufficient to ensure that the system is operational at the end of the installation process, ready to install updates and new packages. To change and complete the installation, select the package installation, then use the **Add/Remove Software -> Minimal Install** to install the minimum on OS packages click the radio button on the option "Minimal".

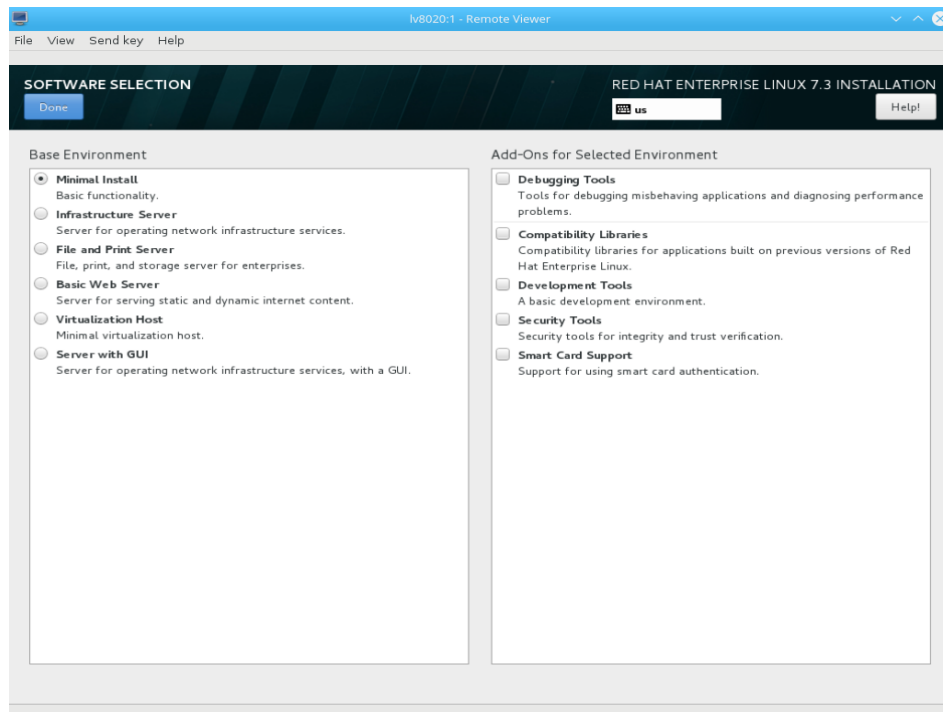


Figure 2. SOFTWARE SELECTION -Installation of RHEL

This option only provides the packages essential to run Red Hat Enterprise Linux. A minimal installation provides the basis for a single-purpose server or desktop appliance and maximizes performance and security on such an installation. For more information about installing the minimal install environment, see the [Software Selection](#) chapter of the [Red Hat Enterprise Linux 8 Installation Guide](#) and the Knowledgebase article [Installing SAP HANA DB with RHEL 8.4 using a Minimal Installation Environment](#).

Reducing the number of installed RPM packages to a minimum number of potentially files on the system improves the security of a system. A minimized number of packages also reduces the number of updates and patches that have to be applied to a system.

SAP HANA is an in-memory, column-oriented, relational database management system, will be delivered in different versions and having many additional components available that are not part of the standard installation. Therefore it is not simple to follow the OS minimum required packages in a Linux system. Generally for a SAP HANA system the OS minimum required packages is impossible because it has to consider all eventualities of certain SAP HANA installations, including different configurations, versions, add-on, etc. Therefore, the current approach to a minimal package selection is an option of Red Hat Linux Enterprise Server installation. The strategy and idea is to use the RHEL “Minimal” installation option and optionally add some additional required packages after the installation, if they are required for running a SAP HANA on RHEL.

Red Hat has tested a minimal installation environment when it comes to SAP HANA on RHEL, The environment used for testing was a RHEL 8.4 system with minimal install selected.

From there ansible scripts installed the required packages that are needed when setting up a HANA DB, and other ansible scripts installed the required SAP system roles that are also needed for setting up HANA DB.

For a more streamlined installation of SAP HANA the roles “[sap-preconfigure](#)” and “[sap-hana-preconfigure](#)” can be used.

Lastly, for testing the minimal install environment we tested if the RHEL 8.4 system could run SAP HANA validation test suite which is SAP’s method of verifying if a system is able to run and process a HANA DB.

The results of running SAP HANA validation test suite showed us that a RHEL 8.4 system is stable when set up with the minimal amount of packages.

To install a Standard SAP HANA Database on RHEL with “Minimal” installation option, you need to install the following additional packages on the system:

- compat-sap-c++
- libtool-ltdl

3.2.1 compat-sap-c++ (C++ compatibility runtime library for SAP applications)

The compat-sap-c++ packages carry runtime compatibility libraries needed for the SAP HANA system. These libraries are installed independently of the standard runtime

libraries provided by RHEL. It contains the libstdc++ shared library, named sap-compat-c++.so.

3.2.2 libtool-ltdl

The libtool-ltdl package contains the GNU Libtool Dynamic Module Loader, a library that provides a consistent, portable interface which simplifies the process of using dynamic modules. These runtime libraries needed by programs that link directly to the system-installed ltdl libraries are not needed by software built using the rest of the GNU Autotools (including GNU Autoconf and GNU Automake).

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

For more information on recommended OS settings including the packages, please refer to [SAP Note 2235581](#), and the [additional packages for installing SAP HANA](#).

Impact

Depending on your Installation environment of different versions of HANA, It is probably required to install more additional RHEL packages.

Priority

Medium

3.3 Disable unnecessary Network Services

Description

Many services under Red Hat Enterprise Linux 8 are network services. If a network service is running on a machine, then a server application (called a daemon) is listening for connections on one or more network ports. Each of these services should be treated as a potential avenue of attack.

Network services can pose many risks for Linux systems. Some of the primary issues are: DoS, DDos, Script Vulnerability Attacks, Buffer Overflow Attacks. Potentially, any network service is insecure. This is why turning off unused network services is so important. Exploits for services are routinely revealed and patched, making it very important to regularly update packages associated with any service. Some network protocols are inherently more insecure than others. These include any services that:

- *Transmit Usernames and Password Over a Network Unencrypted* - Many older protocols, such as Telnet and FTP, do not encrypt the authentication session and should be avoided whenever possible.
- *Transmit Sensitive Data Over a Network Unencrypted* - Many protocols transmit data over the network unencrypted. These protocols include Telnet, FTP, rlogin, HTTP and SMTP. Many network file systems, such as NFS and SMB, also transmit information over the network encrypted. It is the user's responsibility when using these protocols to limit what type of data is transmitted.

To secure a RHEL system from attacks via insecure Network Services, It is recommended to turn off the unused network services. Examples of inherently insecure services include *vsftpd*, *telnet*, *rlogin*, and *rsh* in favor of *ssh*. For more information about securing the network services, refer to the following KBA [Securing Hardening](#).

3.3.1 Disable Telnet

Description

Telnet is an unsecured network protocol service that facilitates remote login to a server via network connection. This is a legacy remote access protocol that does not support encryption, thus allowing hackers or crackers to sniff and obtain this information easily, for example the login username and password for Telnet. It is a good practice to disable telnet, especially on web servers which are reachable from the Internet, and replace it with a secure remote access protocol such as SSH.

By default telnet listens for incoming messages on port 23, and sends outgoing messages to port 23.

Procedure for disabling the telnet service on the server

To disable telnet:

```
#systemctl stop telnet.socket
#systemctl disable telnet.socket
[root@localhost ~]# systemctl status telnet.socket
• telnet.socket - Telnet Server Activation Socket
  Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:telnetd(8)
  Listen: [::]:23 (Stream)
  Accepted: 0; Connected: 0
Apr 04 15:12:15 localhost systemd[1]: Listening on Telnet Server Activation Socket.
Apr 04 15:12:15 localhost systemd[1]: Starting Telnet Server Activation Socket.
Apr 04 15:30:14 localhost systemd[1]: Closed Telnet Server Activation Socket.
Apr 04 15:30:14 localhost systemd[1]: Stopping Telnet Server Activation Socket.
```

To enable telnet again, refer to the following [How to enable the Telnet service.](#)

Impact

The user can not have access to the machine via telnet network services.

Priority

High

3.4 Restrict sudo

Description

The **sudo** command offers a mechanism for providing trusted users with administrative access to a system without sharing the password of the **root** user. When users given access via this mechanism precede an administrative command with **sudo** they are prompted to enter their own password. Once authenticated, and assuming the command is permitted, the administrative command is executed as if run by the root user. Like the command **su**, **sudo** asks for the root password by default. However, unlike **su**, **sudo** remembers the password and allows further command to be executed as root without asking again for the password, therefore, **sudo** should be enabled for selected users only, i.e., admin users.

Procedure of restrict sudo for normal users

- Run the **chgrp** command to set the wheel group as the owner for the **/usr/bin/sudo** and **/usr/bin/su** command

```
chgrp wheel /usr/bin/sudo /usr/bin/su
```

- Use the **chmod** command to ensure that only root user and the wheel group can execute the **sudo** and **su** command

```
chmod 7770 /usr/bin/sudo /usr/bin/su
```

- Run the **visudo** to edit the **/etc/sudoers** file. This file defines the policies applied to the **sudo** command.

```
#visudo
```

- Ensure that in the **/etc/sudoers** file there is 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>
```

The user added to the wheel group, should be logged out and login to the system again, so that the new group membership applied.

Impact

The above procedure prohibits sudo command for all users, other than the ones that are members of the group wheel. Note that the su command is still available for other users.

Priority

High

3.5 Disabling root logins via SSH

Description

By default the root access is enabled for the outside world. It's not secure to have ssh root access enabled for unauthorized users. So, it's better to have another account that you regularly use and then switch to root user by using 'su - ' command when necessary. Before disable root logins, an administrative user should be added that can ssh into the server and become root with su. To prevent root logins via the SSH protocol, edit the SSH daemon's configuration file, **/etc/ssh/sshd_config**, add a line in the Authentication section of the file that says `PermitRootLogin no`. This line may already exist and be commented out. In this case, remove the "#".

Procedure

```
#Authentication
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Restart the SSH server:

```
#Service sshd restart
```

Impact

Root cannot login to the system remotely anymore. Users first are needed to login to the system and then user "su" or sudo" to get the root access when they are using ssh to login to the system.

Priority

High

3.6 Lock out a user to login after a set number of failed attempts

Description

Locking out a user to login after a certain number of failed login attempts prevents users from logging and is one of the security configurations on RHEL. Red Hat Enterprise Linux provides this mechanism via the PAM system. Pluggable Authentication Module (PAM) comes with the pam_tally login counter module. Pam_tally has the capability to maintain attempted access count, reset counters on successful logins and also lock out users with multiple failed login attempts. In the authentication phase of /etc/pam.d/system-auth and /etc/pam.d/password-auth files the pam_tally deny parameter can be used to restrict the number of failed login attempts. The user account will be locked out once the login attempts exceed the deny tally value.

For **Red Hat Enterprise Linux 8**, **pam_tally2** has been replaced by **pam_faillock**.

In Red Hat Enterprise Linux 8, the **pam_faillock** PAM module allows system administrators to lock out user accounts after a specified number of failed attempts. Limiting user login attempts mainly as a security measure that aims to prevent possible brute force attacks targeted to obtain a user's account password.

With the **pam_faillock** module, failed login attempts are stored in a separate file for each user in the **/var/run/faillock** directory.

Follow these steps to configure account locking:

Procedure

Manually editing `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` is not recommended. Use `authselect` to enable/disable `pam_faillock`

Enable/Disable faillock

To enable faillock:

```
# authselect enable-feature with-faillock
```

To disable faillock:

```
# authselect disable-feature with-faillock
```

Configure faillock

faillock options should be stored in `/etc/security/faillock.conf`:

```
deny=4
unlock_time=1200
silent
```

Note: `/etc/security/faillock.conf` is available from `pam-1.3.1-8.el8`.

Using the faillock command

To reset/view authentication failure records use commands like the following:

To display authentication failure records for username:

```
# faillock --user username
```

To reset authentication failure records for username:

```
# faillock --user username --reset
```

SSHD configuration adjustment

If pam_faillock.so is not working as expected, the following changes may have to be made to SSHD's configuration:

```
# vi /etc/ssh/sshd_config
ChallengeResponseAuthentication yes
PasswordAuthentication no
```

Then restart the sshd service in order for these configuration changes to take effect:

```
# systemctl restart sshd
```

Additional Notes

The sequence of the lines in the files (/etc/pam.d/system-auth and /etc/pam.d/password-auth) are important and any change in sequence may result in the locking of all user accounts including root user when you are using even_deny_root option.

The pam_faillock module supports temporary locking of user accounts in the event of multiple failed authentication attempts. This new module improves functionality over the existing pam_tally2 module, as it also allows temporary locking when the authentication attempts are done over a screensaver.

The pam_faillock module now also supports persistent locking via errata release RHBA-2016-2314.

In RHEL8, we do not recommend you make modifications directly in PAM global files system-auth and password-auth available under the /etc/pam.d/ directory.

To configure pam_faillock to lock ONLY local user accounts and skip network accounts such as IPA/AD/LDAP from being locked modify PAM files as mentioned in this article: [How to set up account lockout policy using pam_faillock when system is an LDAP/IPA/AD client](#)

For more info please refer to [pam faillock and how to use it in Red Hat Enterprise Linux](#)

Impact

The password for RHEL system users have to be set according to the [Defining Password Policies](#). After the user has a certain failed attempt to login to the system, the user will be locked and is not able to login to the RHEL system.

Priority

Medium

3.7 Network Bound Disk Encryption (NBDE)

Description

When it comes to the encryption of hard drives on physical and virtual machines, Red Hat has a collection of technologies that enable the unlocking of encrypted root and secondary volumes of these hard drives. This technology is known as Policy-Based Decryption (PBD). PBD has a variety of unlocking mechanisms such as user passwords, a Trusted Platform Module (TPM) device, a PKCS #11 device that is connected to a system, a smart card, or a special network server.

The Network Bound Disc Encryption (NBDE) is a subcategory of PBD that allows binding encrypted volumes to a special network server. The current implementation of the NBDE includes a Clevis pin for the Tang server and the Tang server itself.

Procedure

To install Clevis and its pins on a system with an encrypted volume:

```
# yum install clevis
```

To decrypt data, use a `clevis decrypt` command and provide a cipher text in the JSON Web Encryption (JWE) format, for example:

```
$ clevis decrypt < secret.jwe
```

Use the following steps to configure unlocking of LUKS-encrypted volumes with NBDE.

To automatically unlock an existing LUKS-encrypted volume, install the `clevis-luks` subpackage:

```
# yum install clevis-luks
```

Identify the LUKS-encrypted volume for PBD. In the following example, the block device is referred as `/dev/sda2`:

```
# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                                8:0  0  12G  0 disk
├─sda1                             8:1  0   1G  0 part  /boot
├─sda2                             8:2  0  11G  0 part
│   └─luks-40e20552-2ade-4954-9d56-565aa7994fb6 253:0  0  11G  0 crypt
│       ├─rhel-root                 253:0  0   9.8G  0 lvm  /
│       └─rhel-swap                 253:1  0   1.2G  0 lvm  [SWAP]
```

Bind the volume to a Tang server using the `clevis luks bind` command:

```
# clevis luks bind -d /dev/sda2 tang '{"url":"http://tang.srv"}'
```

The advertisement contains the following signing keys:

```
_OsIkOT-E2l6qjfdDiwVmidoZjA
```

```
Do you wish to trust these keys? [ynYN] y
You are about to initialize a LUKS device for metadata storage.
Attempting to initialize it may result in data loss if data was
already written into the LUKS header gap in a different format.
A backup is advised before initialization is performed.
```

```
Do you wish to initialize /dev/sda2? [yn] y
Enter existing LUKS password:
```

This command performs four steps:

1. Creates a new key with the same entropy as the LUKS master key.

2. Encrypts the new key with Clevis.
3. Stores the Clevis JWE object in the LUKS2 header token or uses LUKSMeta if the non-default LUKS1 header is used.
4. Enables the new key for use with LUKS.

The binding procedure assumes that there is at least one free LUKS password slot. The `clevis luks bind` command takes one of the slots.

The volume can now be unlocked with your existing password as well as with the Clevis policy.

To enable the early boot system to process the disk binding, use the `dracut` tool on an already installed system:

```
# yum install clevis-dracut
```

In Red Hat Enterprise Linux 8, Clevis produces a generic `initrd` (initial ramdisk) without host-specific configuration options and does not automatically add parameters such as `rd.neednet=1` to the kernel command line. If your configuration relies on a Tang pin that requires network during early boot, use the `--hostonly-cmdline` argument and `dracut` adds `rd.neednet=1` when it detects a Tang binding:

```
# dracut -fv --regenerate-all --hostonly-cmdline
```

Alternatively, create a `.conf` file in the `/etc/dracut.conf.d/`, and add the `hostonly_cmdline=yes` option to the file, for example:

```
# echo "hostonly_cmdline=yes" > /etc/dracut.conf.d/clevis.conf
```

You can also ensure that networking for a Tang pin is available during early boot by using the `grubby` tool on the system where Clevis is installed:

```
# grubby --update-kernel=ALL --args="rd.neednet=1"
```

Then you can use dracut without `--hostonly-cmdline`:

```
# dracut -fv --regenerate-all
```

Verification

To verify that the Clevis JWE object is successfully placed in a LUKS header, use the `clevis luks list` command:

```
# clevis luks list -d /dev/sda2
1: tang '{"url":"http://tang.srv:port"}'
```

For more info please refer to [Configuring Automated Unlocking of Encrypted Volumes Using Policy-based Decryption](#) and [Setting Up a RHEL System with NBDE and Installing SAP HANA DB with RHEL](#)

Impact

Our recommendation for customers is to use Network Bound Encryption as it allows for additional security when it comes to protecting the information on the servers that are running Red Hat Linux and it enables an easier process of unlocking encrypted systems.

Conclusion

Red Hat has tested an environment for NBDE with a RHEL 8.2 system with encryption enabled on all available drives.

From there ansible scripts installed the required packages that are needed when setting up a HANA DB, and other ansible scripts installed the required SAP system roles that are also needed for setting up HANA DB.

Afterwards, clevis was set up on the test RHEL 8.2 machine, and this machine was binded to a testing tang server to allow for automatic unlocking of the encrypted drives.

For a more streamlined installation of SAP HANA the roles “sap-preconfigure” and “sap-hana-preconfigure” can be used.

Lastly, for testing network bound disk encryption we tested if the RHEL 8.2 system could run SAP HANA validation test suite which is SAP’s method of verifying if a system is able to run and process a HANA DB.

The results of running SAP HANA validation test suite showed us that a RHEL 8.2 system is stable when set up with Network Bound Disk Encryption and is able to be unlocked with a tang server. With the SAP HANA validation test suite we were able to run all tests, with no issues.

Priority

Medium

3.8 fapolicyd

Description

The *fapolicyd* framework introduces the concept of trust. An application is trusted when it is properly installed by the system package manager, and therefore it is registered in the system RPM database. The *fapolicyd* daemon uses the RPM database as a list of trusted binaries and scripts. The *fapolicyd* RPM plugin registers any system update that is handled by either the YUM package manager or the RPM Package Manager. The plugin notifies the *fapolicyd* daemon about changes in this database. Other ways of adding applications require the creation of custom rules and restarting the *fapolicyd* service.

Procedure

1. Install the *fapolicyd* package:

```
# yum install fapolicyd
```

2. Enable and start the *fapolicyd* service:

```
# systemctl enable --now fapolicyd
```

Verification

1. Verify that the *fapolicyd* service is running correctly:

```
# systemctl status fapolicyd
fapolicyd.service - File Access Policy Daemon
Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor p>
Active: active (running) since Tue 2019-10-15 18:02:35 CEST; 55s ago
Process: 8818 ExecStart=/usr/sbin/fapolicyd (code=exited, status=0/SUCCESS)
Main PID: 8819 (fapolicyd)
Tasks: 4 (limit: 11500)
Memory: 78.2M
CGroup: /system.slice/fapolicyd.service
└─8819 /usr/sbin/fapolicyd

Oct 15 18:02:35 localhost.localdomain systemd[1]: Starting File Access Policy D>
Oct 15 18:02:35 localhost.localdomain fapolicyd[8819]: Initialization of the da>
Oct 15 18:02:35 localhost.localdomain fapolicyd[8819]: Reading RPMDB into memory
Oct 15 18:02:35 localhost.localdomain systemd[1]: Started File Access Policy Da>
Oct 15 18:02:36 localhost.localdomain fapolicyd[8819]: Creating database
```

2. Log in as a user without root privileges, and check that *fapolicyd* is working, for example:

```
$ cp /bin/ls /tmp
$ /tmp/ls
bash: /tmp/ls: Operation not permitted
```

Impact

The environment used for testing was a RHEL 8.4 system with `fapolicyd` enabled on the machine.

From there ansible scripts installed the required packages that are needed when setting up a HANA DB, and other ansible scripts installed the required SAP system roles that are also needed for setting up HANA DB.

Afterwards, the installed files on the machines were marked as trusted in the `fapolicyd` policy on the RHEL 8.4 machine. The machine then had the `fapolicyd` database updated and `fapolicyd` was then restarted to update the database.

For a more streamlined installation of SAP HANA the roles "[sap-preconfigure](#)" and "[sap-hana-preconfigure](#)" can be used.

Lastly, for testing `fapolicyd` we tested if the RHEL 8.4 system could run SAP HANA validation test suite which is SAP's method of verifying if a system is able to run and process a HANA DB.

The results of running SAP HANA validation test suite showed us that a RHEL 8.4 system is stable when set up with `fapolicyd`. And once the SAP HANA files are added to the trusted `fapolicyd.trust` file, we see no issues when it comes to running the SAP HANA validation test suite.

Conclusion

To properly enforce rules on your machine it is recommended to enable *fapolicyd* on your machine after the installation of RHEL. When it comes to enabling `fapolicyd`, Red Hat's recommendation is to enable `fapolicyd` on RHEL 8.4 and higher systems as it has not been tested on earlier versions

Priority

Medium

4. SAP HANA Network and Communication Security

Description

Several mechanisms are possible for securing network communication in the SAP HANA landscape. SAP HANA supported encrypted communication for network

communication channels. [SAP HANA security guide](#) recommends using encrypted channels in all cases where the network isn't protected by other security measures against attacks such as eavesdropping, for example, when the network is accessed from public networks. Alternatively, one should use virtual private network (VPN) tunnels to transfer encrypted information.

4.1 Communication Channels

The network communication channels used by SAP HANA can be categorized into those used for database clients connecting to SAP HANA and those used for internal database communication. SAP recommends using encrypted communication channels where possible.

To support the different SAP HANA scenarios and set-up, SAP HANA has different types of network communication channels:

- Channels used for external access to SAP HANA functionality by end-user clients, administration clients, application servers, and for data provisioning through SQL or HTTP.
- Channels used for SAP HANA internal communication within the database, between hosts in multiple-host systems, and between systems in system-replication scenarios.

The connection between SAP HANA and external components and applications come under these categories:

- Connections for administrative purposes
- Connections for data provisioning
- Connections from database clients that access the SQL/MDX interface for the SAP HANA database
- Connections from HTTP/S Clients
- Outbound connections

4.2 Network Security

To integrate SAP HANA securely into the network environment, several general recommendations apply.

The components of an SAP HANA landscape communicate through different network communication channels. It is recommended security practice to have a well-defined network topology to control and limit network access to SAP HANA to only those communication channels for the scenario, and to apply appropriate security measures,

such as encryption, where necessary. This can be achieved through different means, such as separate network zones, network firewalls, and through the configuration options provided by SAP HANA (for example, encryption). The exact setup depends on your environment, your implementation scenario, and your requirements and policies.

It is recommended in the [SAP HANA Security Guide](#) to protect internal communication further by applying additional mechanisms. This may include filtering access to the relevant ports and channels by applying additional protection at the network level for example: VPN, IPsec. In Red Hat Enterprise Linux 8, a *Virtual Private Network (VPN)* can be configured using the IPsec tunneling protocol which is supported by the **Libreswan** application. **Libreswan** is a fork of the **Openswan** application and examples in documentation should be interchangeable. The **NetworkManager IPsec** plug-in is called **NetworkManager-libreswan**. Users of GNOME shell should install the **NetworkManager-libreswan-gnome** package, which **libreswan-gnome** package is only available from the Optional channel. Please refer to [Enabling Supplement and Optional Repositories](#).

Libreswan is an open-source, user-space **IPsec** implementation available in Red Hat Enterprise Linux 8. **Libreswan** interfaces with the Linux kernel using netlink to transfer the encryption keys. Packet encryption and decryption happen in the Linux kernel.

IMPORTANT: IKE/IPsec, implemented by **Libreswan**, is the only VPN technology recommended for use in Red Hat Enterprise Linux 8. Do not use any other VPN technology without understanding the risks of doing so.

Procedure

To install and check that Libreswan, is installed issue the following command as root:

```
#yum install libreswan
#yum info libreswan
```

After a new installation of Libreswan the NSS database should be initialized as part of the install process. However, should you need to start a new database, first remove the old database and then, to initialize a new NSS database, run as follows:

```
#rm /etc/ipsec.d/*db
#ipsec initnss
Initializing NSS database
See 'man pluto' if you want to protect the NSS database with a password
```

If you do not want to use a password for NSS, just press Enter twice prompted for the password. If you do enter a password then you will have to re-enter it every time **Libreswan** is started, such as every time the system is booted.

To start the ipsec daemon provided by Libreawman and to confirm that the daemon is now running, issue the following command as root:

```
#systemctl start ipsec
#systemctl status ipsec
ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec
Loaded: loaded (/usr/lib/systemd/system/ipsec.service; disabled)
Active: active (running) since Wed 2018-02-21 12:14:12 CET; 2 days ago
```

To ensure that Libreswan will start when the system starts, run the '**systemctl enable ipsec**' as root. For more information about Libreswan and Security VPN, please refer to [Chapter 4. Configuring a VPN with IPsec](#) of the RHEL 8 Security Guide.

4.3 SSL Configuration on the SAP HANA Server

To use the Transport Layer Secure (TLS) /Secure Socket Layer (SSL) protocol to secure communication between the SAP HANA database and clients that access the SQL interface of the database, TLS/SSL must be configured on both the server and client.

Before configuring TLS/SSL on the SAP HANA server, please check beforehand if the SAP Cryptographic Library CommonCryptoLib (SAPCRYPTOLIB) is available on the server. CommonCryptoLib (libsapcrypto.so) is installed by default as part of SAP HANA installation at \$DIR_EXECUTABLE.

If you are using trust and key stores located in the file system instead of in the database, OpenSSL is also supported. The OpenSSL library is installed by default as part of the RHEL installation. However, it is recommended that you migrate to CommonCryptoLib after an upgrade to Support Package Stack. For more information, see [SAP Note 2093286](#).

OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them. The OpenSSL program is a command line tool for using the various cryptography functions of OpenSSL's crypto library from the shell. It can be used for

- o Creation and management of private keys, public keys and parameters

- o Public key cryptographic operations
- o Creation of X.509 certificates, CSRs and CRLs
- o Calculation of Message Digests
- o Encryption and Decryption with Ciphers
- o SSL/TLS Client and Server Tests
- o Handling of S/MIME signed or encrypted mail
- o Timestamp requests, generation and verification

OpenSSL is one of the packages that the user has to install on RHEL 8 for SAP HANA as a dependency for SAP HANA. To install the OpenSSL, please execute the required commands as following:

```
[root@lv8020 ~]# yum install openssl
Loaded plugins: product-id, rhnplugin, search-disabled-repos
This system is receiving updates from RHN Classic or Red Hat Satellite.
Resolving Dependencies
--> Running transaction check
---> Package openssl.x86_64 1:1.0.2k-8.el7 will be installed
--> Finished Dependency Resolution
```

Dependencies Resolved

=====				
=====				
Package	Arch	Version	Repository	Size
=====				
=====				
Installing:openssl k	x86_64	1:1.0.2k-8.el7	rhel-x86_64-server-8.0.eus	492

Transaction Summary

=====

Install 1 Package

Total download size: 492 k
Installed size: 826 k
Is this ok [y/d/N]:

4.4 Secure Operating System User- <sid>adm

Description

<sid>adm user (where <sid> is the ID of the SAP HANA system) is not a database user but a user at the operating system user level and is also referred to as the operating system administrator. For instance the <sid>adm user is created during the installation

process with super user privileges. All platform services of the SAP HANA system (the application server included) run using this OS user. Therefore, <sid>adm is not limited in any way and needs to be handled with special care. This operating system user has unlimited access to all local resources related to SAP systems.

Being the owner of all OS processes, this administrative user is very powerful from a security perspective. For this reason, It is strongly recommended that the user limit the number of people with <sid>adm credentials as far as possible.

The initial password is specified during installation by your hardware partner or certified administrator. After handover, It is important that you change this password. A system administrator can do this at the operating system level. It is also possible as part of a system rename with SAP HANA lifecycle manager.

Priority

High

5. SELinux

5.1 Description

SELinux is enabled by default on RHEL 8 systems. The goal of this chapter is to re-enable SELinux on RHEL 8 systems running SAP HANA where SELinux was previously disabled.

SELinux can run in one of three modes: disabled, permissive, or enforcing. Red Hat's suggestion is to set SELinux to enforcing as it allows for a more secure system.

When enabled, SELinux has two modes: enforcing and permissive. Use the `getenforce` or `sestatus` commands to check the status of SELinux. The `getenforce` command returns Enforcing, Permissive, or Disabled. The `sestatus` command returns the SELinux status and the SELinux policy being used:

```
[localhost@linux ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:        enforcing
```

```
Policy MLS status:      enabled
Policy deny_unknown status:  allowed
Max kernel policy version: 30
```

5.2 Benefits of SELinux

SELinux provides the following benefits:

- All processes and files are labeled. SELinux policy rules define how processes interact with files, as well as how processes interact with each other. Access is only allowed if an SELinux policy rule exists that specifically allows it.
- Fine-grained access control. Stepping beyond traditional UNIX permissions that are controlled at user discretion and based on Linux user and group IDs, SELinux access decisions are based on all available information, such as an SELinux user, role, type, and, optionally, a security level.
- SELinux policy is administratively-defined and enforced system-wide.
- Improved mitigation for privilege escalation attacks. Processes run in domains, and are therefore separated from each other. SELinux policy rules define how processes access files and other processes. If a process is compromised, the attacker only has access to the normal functions of that process, and to files the process has been configured to have access to. For example, if the Apache HTTP Server is compromised, an attacker cannot use that process to read files in user home directories, unless a specific SELinux policy rule was added or configured to allow such access.
- SELinux can be used to enforce data confidentiality and integrity, as well as protecting processes from untrusted inputs.
- SELinux is an implementation of the Mandatory Access Control mechanism.

5.3 Procedure

When SELinux is running in enforcing mode, it enforces the SELinux policy and denies access based on SELinux policy rules. In Red Hat Enterprise Linux, enforcing mode is enabled by default when the system was initially installed with SELinux. One way of changing the SELinux mode permanently to either Enforcing or Permissive is to edit the `/etc/sysconfig/selinux` file and set `SELINUX` parameters value to either enforcing or permissive.

```
[localhost@linux ~]$ ls -l /etc/sysconfig/selinux
lrwxrwxrwx. 1 root root 17 Nov 15 2016 /etc/sysconfig/selinux -> ../selinux/config

[localhost@linux ~]$ cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are
protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

For checking the SELinux mode, use the `getenforce` command, as in the following example:

```
# getenforce
Enforcing
```

When you enable SELinux on systems that previously had it disabled, to avoid problems, such as systems unable to boot or process failures, follow this procedure:

Enable SELinux in permissive mode

Edit the `/etc/sysconfig/selinux` file and set SELINUX parameters value to permissive.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Relabel whole filesystem to fix SELinux labels on the filesystem:

```
# fixfiles onboot
```

Restart your system:

```
# reboot
```

After the system restarts, confirm that the `getenforce` command returns Permissive:

```
$ getenforce
Permissive
```

If the system boots in permissive mode and there are no SELinux denials, please continue with the next section, Enable SELinux in enforcing mode.

Enable SELinux in enforcing mode

Edit the `/etc/sysconfig/selinux` file and set SELINUX parameters value to permissive

```
# This file controls the state of SELinux on the system.
```

```
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Restart your system:

```
# reboot
```

After the system restarts, confirm that the `getenforce` command returns enforcing:

```
$ getenforce
Enforcing
```

How to read and understand log files

How to check for SELinux denial messages

When your software is blocked by SELinux, the `/var/log/audit/audit.log` file is the first place to check for more information about a denial. To query Audit logs, use the `ausearch` tool. Because the SELinux decisions, such as allowing or disallowing access, are cached and this cache is known as the Access Vector Cache (AVC), use the AVC and `USER_AVC` values for the message type parameter, for example:

```
# ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts recent

Or

# ausearch -m AVC -ts boot
```


If there are no matches, check if the Audit daemon is running. If it does not, repeat the denied scenario after you start auditd and check the Audit log again.

If there are no denials, switch to enforcing mode.

```
# setenforce 1
```

Another way of changing the SELinux mode permanently to either of Enforcing or Permissive is – to edit the /etc/sysconfig/selinux file and set SELINUX parameters value to either enforcing or permissive:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Then restart the machine:

```
# reboot
```

Verification steps

After the system restarts, confirm that the getenforce command returns Enforcing:

```
$ getenforce
Enforcing
```

SAP Hana processes should run in unconfined_t SELinux policy. You can verify it by running:

```
$ ps -efZ | grep unconfined_t
```

5.4 How to create exceptions in SELinux

Please refer to this [link](#) for instructions on how to create exceptions in SELinux.
If you need to disable SELinux

Changing the SELinux mode from Enforcing to Disabled immediately on a running system is not possible.

For setting the SELinux mode to Disabled permanently, use the following command and reboot the server:

```
# sed -i 's/\(SELINUX=enforcing\|SELINUX=permissive\)/SELINUX=disabled/g'  
/etc/selinux/config
```

This will configure the `/etc/selinux/config` file so that any SELINUX parameter setting other than disabled will be changed to disabled. The SELinux configuration change will only become effective after a system reboot. Note the different spelling in file `/etc/selinux/config` vs. in the `getenforce`/`setenforce` usage and outputs: All characters of the SELINUX value in file `/etc/selinux/config` are in lowercase, whereas the SELINUX value in the mentioned commands is capitalized.

Please note: Unless noted otherwise, all changes mentioned above require root access on operating system level. It is recommended to reboot the system after the changes have been applied. Future implementations might lead to changes of these recommendations.

Conclusion

To properly enforce rules on your machine it is recommended to enable SELinux on your machine after the installation of RHEL. When it comes to enabling SELinux, Red Hat's

recommendation is to enable enforcing on RHEL 8.2 and higher systems as it has not been tested on earlier versions. If a system is having issues with SELinux denials, our recommendation is to set SELinux into permissive mode and then view the SELinux logs to see what processes are being denied, if these processes are processes that should be allowed then an exception should then be created.

Priority

High

6. Security Updates

6.1 Planning and Configuring Security Updates and Patches

Description

As security vulnerabilities are discovered, the affected software must be updated in order to limit any potential security risk. If the software is part of the package within an Red Hat Enterprise Linux distribution that is currently supported, Red Hat, Inc is committed to releasing updated packages that fix the vulnerability as soon as possible. Often, announcements about a given security exploit are accompanied with a patch (or source code) that fixes the problem. This patch is then applied to the Red Hat Enterprise Linux package and tested and released as an erratum update. However, if an announcement does not include a patch, Red Hat developers first work with the maintainer of the software to fix the problem. Once the problem is fixed, the package is tested and released as an erratum update. If an errata update is released for software used on your system like SAP HANA, It is highly recommended to update the affected packages as soon as possible to minimize the amount of time the system is potentially vulnerable. If a security patch impacts SAP HANA operation, SAP will publish an SAP note where this face is stated. To install and configure the SAP HANA on RHEL please refer to the [SAP Note 2009879](#).

All software contains bugs. Often, these bugs can result in a vulnerability that can expose your system to malicious users. Packages that have not been updated are a common cause of computer intrusions. Implement a plan for installing security patches in a timely manner to quickly eliminate discovered vulnerabilities, so they cannot be exploited. Test security updates when they become available and schedule them for installation. Additional controls need to be used to protect the system during the time between the release of the update and its installation on the system. These controls

depend on the exact vulnerability, but may include additional firewall rules, the use of external firewalls, or changes in software settings.

Bugs in supported packages are fixed using the errata mechanism. An erratum consists of one or more RPM packages accompanied by a brief explanation of the problem that the particular erratum deals with. All errata are distributed to customers with active subscriptions through the Red Hat Subscription Management service. Errata that address security issues are called Red Hat Security Advisories

6.2 Updating and Installing Packages

When updating software on a system, It is important to download from a trusted source. An attacker can easily rebuild a package with the same version number as the one that is supposed to fix the problem but with a different security exploit and release It on the Internet. If this happens, using security measures such as verifying files against the original RPM does not detect the exploit. Thus, It is very important to only download RPMs from trusted sources, such as from Red Hat, Inc and check the signature of the packages to verify its integrity.

Red Hat offers ways to find information on errata updates:

1. Using Red Hat Network
2. Using the [Red Hat Errata Website](#)

Red Hat Enterprise Linux consistently provides security updates and patches, so that SAP HANA can run in a very secure environment, and the highest security standards.

Note: Beginning with the Red Hat Enterprise Linux product line, updated packages can be downloaded only from Red Hat Network. Although the Red Hat Errata website contains updated information, it does not contain the actual packages for download.

6.3 Using the Security Features of Yum

Description

The **Yum** packages manager includes several security-related features that can be used to search, list, display, and install security errata. These features also make It possible to use **Yum** to install nothing but security updates.

To check for security- related updates available for the system, enter the following command as **root**:

Procedure

```
# yum check-update --security
Loaded plugins: product-id, rhnplugin, search-disabled-repos
This system is receiving updates from RHN Classic or Red Hat Satellite.
--> pcp-pmda-postfix-3.11.3-4.el7.x86_64 from rhel-x86_64-server-8.0.eus excluded
(updateinfo)
--> fence-agents-bladecenter-4.0.11-27.el7.x86_64 from rhel-x86_64-server-8.0.eus
excluded (updateinfo)
--> 10:libcacard-1.5.3-105.el7.x86_64 from rhel-x86_64-server-8.0.eus excluded
(updateinfo)
...
No packages needed for security; 0 packages available
Security: kernel-3.10.0-693.17.1.el7.x86_64 is an installed security update
Security: kernel-3.10.0-693.el7.x86_64 is the currently running version
```

Note: the above command runs in a non-interactive mode, so it can be used in scripts for automated checking whether there are any updates available. The command returns an exit value of 100 when there are any security updates available and 0 when there are not. On encountering an error, it returns 1.

Use the following command to only install security-related updates:

```
# yum update --security
Loaded plugins: product-id, rhnplugin, search-disabled-repos
This system is receiving updates from RHN Classic or Red Hat Satellite.
No packages needed for security; 0 packages available
No packages marked for update
```

7. Further Information and References

- Enabling SELinux with SAP HANA DB
<https://access.redhat.com/articles/5946171>
- Security hardening - Red Hat Enterprise Linux 8
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_harden/index
- Configuring basic system settings - Red Hat Enterprise Linux 8
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/index
- Configuring sudo Access

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/managing-sudo-access-configuring-basic-system-settings

- SELINUX

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/index

- SAP HANA Security Guide

<https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.02/en-US>

- Package manifest - Red Hat Enterprise Linux 8

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/package_manifest/index

- Chapter 24. Changing and resetting the root password

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/changing-and-resetting-the-root-password-from-the-command-line_configuring-basic-system-settings

- Chapter 51. Using and configuring firewalld

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/using-and-configuring-firewalld_configuring-and-managing-networking

- How to set the idle-timeout in Linux

<https://www.redhat.com/archives/rhl-list/2005-May/msg04387.html>

- What is pam_faillock and how to use it in Red Hat Enterprise Linux?

<https://access.redhat.com/solutions/62949>