Red Hat Enterprise Linux for SAP Solutions 9

Using SELinux for SAP HANA

Last Updated: 2024-04-30

Legal Notice

Abstract

Configuring SELinux helps you enhance your system’s security. SELinux is an implementation of Mandatory Access Control (MAC), and provides an additional layer of security. The SELinux policy defines how users and processes can interact with the files on the system. You can control which users can perform which actions by mapping them to specific SELinux confined users.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE 3

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION 4

CHAPTER 1. INTRODUCTION TO SELINUX 5

CHAPTER 2. CONFIGURING SELINUX TO EXCLUDE SAP HANA DIRECTORIES 6

CHAPTER 3. TROUBLESHOOTING ISSUES RELATED TO SELINUX 7

CHAPTER 4. ADDITIONAL INFORMATION 8

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code and documentation. We are beginning with these four terms: master, slave, blacklist, and whitelist. Due to the enormity of this endeavor, these changes will be gradually implemented over upcoming releases. For more details on making our language more inclusive, see our CTO Chris Wright's message.

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Let us know how we can improve it.

Submitting feedback through Jira (account required)

1. Make sure you are logged in to the Jira website.
2. Provide feedback by clicking on this link.
3. Enter a descriptive title in the **Summary** field.
4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
5. If you want to be notified about future updates, please make sure you are assigned as **Reporter**.
6. Click **Create** at the bottom of the dialogue.

CHAPTER 1. INTRODUCTION TO SELINUX

SELinux provides enhanced security by enforcing security policies, using labels for files, processes and ports, and logging unauthorized access attempts.

SELinux is enabled and set to **enforcing** mode on RHEL 9 by default and security policies for system processes are maintained by Red Hat. For more information, refer to Changing SELinux states and modes on RHEL. You can refer to SAP Note 3108302 - SAP HANA DB: Recommended OS Settings for RHEL 9, to know which HANA versions have been tested by SAP with SELinux set to **enforcing** and **unconfined** mode.

Red Hat recommends that you use SELinux in **enforcing** mode to configure your RHEL systems running on SAP HANA. This document describes the necessary configuration changes that you must make.

In case you come across SELinux related issues while testing or running your SAP HANA system, SAP reserves the right to disable SELinux. However, most of the problems can be solved by changing SELinux mode from **enforcing** to **permissive**. The advantage is that your system is still operating while you analyze and solve the problem.

CHAPTER 2. CONFIGURING SELINUX TO EXCLUDE SAP HANA DIRECTORIES

By default, any application for which no SELinux security policy has been defined is blocked by SELinux if your RHEL system is running with SELinux set to **enforcing** mode. As of today, SAP does not provide SELinux policies for SAP HANA. For running SAP HANA executables while SELinux is set to enforcing, a certain SELinux boolean has to be set, and the SAP HANA related directories have to be excluded from SELinux protection. You can also use the **fapolicyd** framework to protect your SAP HANA software. For more information, refer to the Configuring fapolicyd to allow only SAP HANA executables document.

Prerequisites

- SAP HANA is installed and stopped, or not yet installed.
- SELinux is available and set to **enforcing** mode.
- The directories in which SAP HANA and related software are installed (typically /**hana** and /**usr**/**sap**) exist.

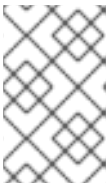
Procedure

1. Use the following command to set the SELinux boolean **selinuxuser_execmod** to **1**, allowing unconfined executables to use libraries that require text relocation (such as SAP HANA):

```
# setsebool -P selinuxuser_execmod 1
```

2. Use the following commands to relabel the directories and files used by SAP HANA (typically /**hana** and /**usr**/**sap**) so that SAP HANA can be run in **unconfined** mode:

```
# semanage fcontext -a -t usr_t '/hana(/.)?'*
# semanage fcontext -a -t usr_t '/usr/sap(/.)?'*
# restorecon -Rv '/hana'
# restorecon -Rv '/usr/sap'
```



NOTE

You can perform this step before or after installing SAP HANA, as all newly created directories and files below the upper level directories inherit the SELinux labels.

Verification

- Use the following command to show the security context of a file or directory in /**usr**/**bin** and in /**hana**, confirming that the file or directory under /**hana** has the **usr_t** label:

```
[root@host01 ~]# ls -lZ /usr/bin/ls
-rwxr-xr-x. 1 root root system_u:object_r:bin_t:s0 143296 Jan  6  2023 /usr/bin/ls
[root@host01 ~]# ls -lZd /hana/shared
drwxr-xr-x. 3 root root system_u:object_r:usr_t:s0 17 Apr 18 23:03 /hana/shared
```

CHAPTER 3. TROUBLESHOOTING ISSUES RELATED TO SELINUX

For diagnosing issues related to SELinux, you can check the file **/var/log/audit/audit.log**, as follows:

1. To query Audit logs, use the **ausearch** tool. SELinux decisions, such as allowing or disallowing access, are cached in the Access Vector Cache (AVC). Therefore, you should 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 boot
   ```

2. If there are no matches, check if the Audit daemon is running.

3. If it is not running, then perform the following steps:

   a. Restart the audit.

   b. Re-run the denied scenario.

   c. Check the Audit log again.

   For more information about solving SELinux related issues, see Troubleshooting problems related to SELinux.

CHAPTER 4. ADDITIONAL INFORMATION

- Depending on your environment (cloud providers, third party user tools, and agents), you should change SELinux labels on additional mount points (/**opt**, /**sapmnt**, and /**trans**).