Red Hat Enterprise Linux for SAP Solutions 9

Configuring fapolicyd to allow only SAP HANA executables

Last Updated: 2024-04-29

Legal Notice

Abstract

Configure this policy to secure the environment for running SAP HANA against local and remote intrusion, exploitation, and malicious activity.

Table of Contents

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 FAPOLICYD

The **fapolicyd** software framework controls the execution of applications based on a user-defined policy. This is one of the most efficient ways to prevent running untrusted and possibly malicious applications on the system. For more information, refer to Blocking and allowing applications by using fapolicyd in the Security hardening guide for RHEL 9.

NOTE

The procedures described below put all detected SAP HANA executables into **fapolicyd** trust files, which contain all names, sizes, and checksums of trusted files. SAP HANA binaries and shell scripts can only be executed if they are contained in the **fapolicyd** trust files. So, if you execute SAP HANA binaries or shell scripts that are not contained in the **fapolicyd** trust files, undesirable effects, including corruption or loss of data, could happen. You must carefully test all the steps and do proper verification on a non-production system first.

CHAPTER 2. PROTECTING SAP HANA INSTALLATION BY USING FAPOLICYD

You can perform the following steps to protect a SAP HANA installation:

- Installing the **fapolicyd** package.
- Setting the integrity checking to **SHA-256** hashes.
- Adding custom **fapolicyd** rules to protect shell scripts.
- Marking the SAP HANA files as trusted.
- Enabling the **fapolicyd** service.

2.1. INSTALLING THE FAPOLICYD PACKAGE

Procedure

- Install the **fapolicyd** package:

```
# dnf install fapolicyd
```

Verification

- Use the following command to verify that the **fapolicyd** service is installed but not currently running:

```
# systemctl status fapolicyd
● fapolicyd.service - File Access Policy Daemon
   Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor preset:
disabled)
   Active: inactive (dead) since Fri 2024-04-19 14:59:52 CEST; 1s ago
...
Apr 19 14:59:51 host01 fapolicyd[337927]: shutting down...
Apr 19 14:59:51 host01 systemd[1]: Stopping File Access Policy Daemon...
Apr 19 14:59:52 host01 systemd[1]: fapolicyd.service: Succeeded.
Apr 19 14:59:52 host01 systemd[1]: Stopped File Access Policy Daemon.
```

2.2. SETTING THE INTEGRITY CHECKING TO SHA-256 HASHES

By default, **fapolicyd** verifies the file names while deciding if an application has to be blocked from execution. You can modify this setting to **SHA-256** for a higher level of protection.

Prerequisites

- The **fapolicyd** package is installed on your system.

Procedure

1. Open the **/etc/fapolicyd/fapolicyd.conf** file in a text editor of your choice, for example:

```
# vi /etc/fapolicyd/fapolicyd.conf
```

2. Configure the integrity option and change the default value of **none** to **sha-256**:

```
integrity = sha-256
```

For the change to become effective, you need to restart the **fapolicyd** service. But you must not restart the **fapolicyd** now, as you have to make more changes to the **fapolicyd** configuration.

Verification

- Verify the correct entry:

```
# fapolicyd-cli --check-config
Daemon config is OK
```

The SAP HANA benchmark was tested on RHEL 9.2. While doing so, initially **fapolicyd** was disabled and then enabled to evaluate the performance implications of **fapolicyd**. To allow the tests to run, a total of 19,184 entries were added to the **fapolicyd** trust files. In 99% of the tests, the performance impact was 5% or less, with the vast majority of the tests experiencing a slowdown of 1-3%.

Please note that certain workloads may experience a higher performance penalty. Therefore, you must thoroughly evaluate performance within your specific environment to observe potential impacts accurately.

2.3. ADDING CUSTOM FAPOLICYD RULES TO PROTECT SHELL SCRIPTS

By default, **fapolicyd** blocks binary executable files and certain programs (e.g., Python) from being executed. To also protect shell scripts in the SAP HANA installation directories, you have to add new custom rules.

Prerequisites

- The **fapolicyd** package is installed on your system.

Procedure

1. Open the directory **/etc/fapolicyd/rules.d**.
2. Add a new file with a file name starting with 71 (proposed file name: **71-sap-shellscript.rules**) so the rule is placed between the rules of the files **70-trusted-lang.rules** and **72-shell.rules**, with the following content:

```
# Deny shell script execution and sourcing under SAP HANA directories

deny_audit perm=any all : ftype=text/x-shellscript dir=/hana/,/usr/sap/ trust=0
```

3. Set the ownership of the file to those of the other files in **/etc/fapolicyd/rules.d**:

```
# chown root:fapolicyd 71-sap-shellscript.rules
```

4. Use the following commands to confirm that new rules have been defined, and then load the new rules:

```
# fagenrules --check
/usr/sbin/fagenrules: Rules have changed and should be updated
# fagenrules --load
```

Verification

- Verify that the rules are updated:

```
# fagenrules --check
/usr/sbin/fagenrules: No change
```

2.4. MARKING THE SAP HANA FILES AS TRUSTED

Prerequisite

- The **fapolicyd** package is installed on your system.

Procedure

1. Install the SAP HANA software if not already done.
2. Use the following commands to add all the SAP HANA files to the **fapolicyd** trust database. We recommend using a separate trust file for each directory tree, for example, **hana** and **usr_sap**:

```
# fapolicyd-cli --file add /hana --trust-file hana
# fapolicyd-cli --file add /usr/sap --trust-file usr_sap
```

   This creates two files, named **hana** and **usr_sap**, in the directory **/etc/fapolicyd/trust.d**, which contains entries for all files under **/hana** and **/usr/sap**.

3. For an SAP HANA installation on a freshly installed RHEL system, the SAP HANA installer creates the directories **/hana** and **/usr/sap**, so we can trust that all the files in these directories are valid SAP files.
   In any other case, there might be files in those directories that the SAP HANA installer has not created.

   Therefore, you should carefully verify that all the files in the trust files **/etc/fapolicyd/trust.d/hana** and **/etc/fapolicyd/trust.d/usr_sap** are valid SAP files. One of the possible ways is explained below:

   i. Perform a fresh SAP HANA installation on another freshly installed RHEL system.

   ii. Repeat step 2 on that system.

   iii. Compare the resulting trust files of both systems.

2.5. ENABLING THE FAPOLICYD SERVICE

Prerequisites

- The **fapolicyd** package is installed and not currently running on your system.
- You have completed all the previous steps.

Procedure

- Enable and start the **fapolicyd** service:

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

The **fapolicyd** service now protects the SAP HANA system. Scripts and binaries in **/hana** or **/usr/sap** that are not in the **fapolicyd** trust files are blocked, and non-root users cannot execute these files.

Verification

1. Verify that the **fapolicyd** service is up and running:

```
# systemctl status fapolicyd
● fapolicyd.service - File Access Policy Daemon
    Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; preset: disabled)
    Active: active (running) since Thu 2024-03-14 16:38:32 IST; 18h ago
...
Mar 14 16:38:33 host01 fapolicyd[579216]: Trust database checks OK
Mar 14 16:38:33 host01 fapolicyd[579216]: Starting to listen for events
```

2. Verify that the non-root users, including the SAP HANA administrator user (example: **h70adm**), cannot execute any new scripts and binary programs in **/hana** and **/usr/sap**:

```
# cp -pi /usr/bin/date /hana/
# su - h70adm
h70adm@host01:/usr/sap/H70/HDB35> /hana/date
-sh: /hana/date: Operation not permitted
h70adm@host01:/usr/sap/H70/HDB35> cat > try-to-start-me.sh
#!/bin/bash
echo "I will not execute."
<ctrl>d
h70adm@host01:/usr/sap/H70/HDB35> chmod u+x try-to-start-me.sh
h70adm@host01:/usr/sap/H70/HDB35> ./try-to-start-me.sh
-sh: ./try-to-start-me.sh: Operation not permitted
h70adm@host01:/usr/sap/H70/HDB35> rm try-to-start-me.sh
h70adm@host01:/usr/sap/H70/HDB35> exit
# rm /hana/date
rm: remove regular file '/hana/date'? y
```

CHAPTER 3. RECREATING THE FAPOLICYD TRUST FILES WHEN UPDATING SAP HANA

Prerequisites

- The **fapolicyd** package is installed on your system.
- You have verified that there are no new executables in the SAP HANA software directories, so you do not accidentally add software from unknown sources. For more information, refer to Marking the SAP HANA files as trusted .

Procedure

1. Stop **fapolicyd** before performing the SAP HANA software update:

```
# systemctl stop fapolicyd
```

2. Create a backup of the existing **fapolicyd** trust files **/etc/fapolicyd/trust.d/hana** and **/etc/fapolicyd/trust.d/usr_sap**, and then remove these files.
3. Perform the SAP HANA software update.
4. Repeat procedure section's step 2 of Marking the SAP HANA files as trusted , to recreate the **fapolicyd** trust files for SAP HANA.
5. Start **fapolicyd**:

```
# systemctl start fapolicyd
```

CHAPTER 4. TROUBLESHOOTING ISSUES RELATED TO FAPOLICYD

For diagnosing issues related to **fapolicyd**, you can:

- check the file **/var/log/fapolicyd-access.log** for **fapolicyd** access statistics, and/or,
- run **fapolicyd** in debug mode.

For more information on diagnosing **fapolicyd** related issues, refer to Troubleshooting problems related to fapolicyd.

CHAPTER 5. ADDITIONAL INFORMATION

- After adding more files to the **fapolicyd** trust file, use the following command to update the **fapolicyd** database:

```
# fapolicyd-cli --update
```

- After removing entries from the **fapolicyd** trust file, you have to restart **fapolicyd** instead:

```
# systemctl restart fapolicyd
```