Red Hat Enterprise Linux for SAP Solutions 9

Security hardening guide for SAP HANA

Last Updated: 2024-05-02

Legal Notice

Abstract

Learn the processes and practices for securing Red Hat Enterprise Linux servers and workstations against local and remote intrusion, exploitation, and malicious activity. The documentation contains approaches and practices to secure Red Hat Enterprise Linux servers applicable for various scenarios, including SAP HANA and other SAP applications.

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. SECURITY HARDENING SETTINGS FOR SAP HANA

You should consider the following before applying the approaches and practices to SAP HANA and SAP application systems:

- You can install SAP HANA or SAP NetWeaver software and relevant packages with the help of RHEL System Roles for SAP. For more information, refer to Red Hat Enterprise Linux System Roles for SAP and Installing the Minimum Amount of Packages Required .
- You should implement the recommended settings and steps on a non-production system before making any changes or editing the files according to the Security Hardening guide. It is recommended that you backup the system. You must at least make a backup of the **/etc** directory.
- If you follow the steps described in Blocking and allowing applications by using fapolicyd , you must also perform the steps described in the Configuring fapolicyd to allow only SAP HANA executables document.
- If you follow the steps described in Using SELinux for RHEL, you must also perform the steps described in Using SELinux for SAP HANA.
- To enhance users' management and access to the RHEL for SAP Solution system, you can configure secure remote communication, sudo access, and set password policy and complexity. For more information, refer to the following:
  - Using secure communications between two systems with OpenSSH
  - Managing sudo access
  - What is pam_faillock and how to use it in Red Hat Enterprise Linux 8 & 9?
  - Set Password Policy & Complexity for RHEL 8 & 9 via pam_pwhistory, pam_pwquality & pam_faillock

  To keep your Red Hat Enterprise Linux for SAP Solutions systems secured against newly discovered threats and vulnerabilities, refer to Managing and monitoring security updates.