



Red Hat Enterprise Linux for SAP Solutions 9

Security hardening guide for SAP HANA

Legal Notice

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

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	3
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	4
CHAPTER 1. SECURITY HARDENING SETTINGS FOR SAP HANA	5

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](#).