



# Red Hat Enterprise Linux for SAP Solutions 9

SAP HANA 的安全强化指南





## 法律通告

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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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.

## 摘要

了解保护 Red Hat Enterprise Linux 服务器和 workstation 免受本地和远程入侵、利用和恶意活动的流程和实践。文档包含保护适用于各种场景的 Red Hat Enterprise Linux 服务器的方法和实践，包括 SAP HANA 和其他 SAP 应用程序。

---

## 目录

使开源包含更多 .....	3
对红帽文档提供反馈 .....	4
第1章 SAP HANA 的安全强化设置 .....	5



## 使开源包含更多

红帽承诺替换我们的代码和文档中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于这一努力的精力，这些更改将在即将发布的版本中逐渐实施。[有关让我们的语言更加包含的更多详情，请参阅我们的CTO Chris Wright 信息。](#)

## 对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

### 通过 Jira 提交反馈（需要帐户）

1. 确保您已登录到 [JIRA](#) 网站。
2. 通过单击此[链接](https://issues.redhat.com/secure/CreateInfoDetails!init.jspx?pid=12330720&issuetype=3&components=12387093&priority=10200&summary=Doc&description=775&assignee=rh-ee-pmohta) 来提供反馈。
3. 在 **Summary** 字段中输入描述性标题。
4. 在 **Description** 字段中输入您对改进的建议。包括文档相关部分的链接。
5. 如果要通知将来的更新，请确保已分配为 **Reporter**。
6. 点对话框底部的 **Create**。



# 第1章 SAP HANA 的安全强化设置

在将方法和实践应用到 SAP HANA 和 SAP 应用程序系统之前，您应该考虑以下问题：

- 您可以通过 SAP 的 RHEL 系统角色安装 SAP HANA 或 SAP NetWeaver 软件和相关软件包。如需更多信息，请参阅 [用于 SAP 的 Red Hat Enterprise Linux 系统角色](#) 并安装所需的最少软件包。
- 您应该在非生产环境的系统上实施推荐的设置和步骤，然后根据 [安全强化](#) 指南进行任何更改或编辑文件。建议您备份系统。您必须至少备份 `/etc` 目录。
- 如果您遵循 [使用 fapolicyd 阻止和允许应用程序](#) 中描述的步骤，还必须执行 [配置 fapolicyd 中描述的步骤](#)，以只允许 SAP HANA 可执行文件 文档。
- 如果您遵循为 RHEL [使用 SELinux](#) 中描述的步骤，还必须执行为 SAP HANA [使用 SELinux](#) 中所述的步骤。
- 为增强用户的对 RHEL for SAP 解决方案系统的管理和访问，您可以配置安全远程通信、sudo 访问和设置密码策略和复杂性。如需更多信息，请参阅以下：
  - [使用 OpenSSH 的两个系统间使用安全通讯](#)
  - [管理 sudo 访问](#)
  - [什么是 pam\\_faillock 以及如何在 Red Hat Enterprise Linux 8 和 9 中使用它？](#)
  - [通过 pam\\_pwhistory、pam\\_pwhistory、pam\\_pwquality 和 pam\\_faillock 为 RHEL 8 和 9 设置密码策略和复杂性](#)

要保护您的 Red Hat Enterprise Linux for SAP Solutions 系统免受新发现的威胁和漏洞，请参阅 [管理和监控安全更新](#)。