Red Hat Enterprise Linux for SAP Solutions 9

SAP HANA 的安全强化指南

Last Updated: 2024-05-04

法律通告

摘要

了解保护 Red Hat Enterprise Linux 服务器和工作站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

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 来提供反馈。https://issues.redhat.com/secure/CreateIssueDetails!init.jspa?pid=12330720&issuetype=3&components=12387093&priority=10200&summary=Doc&description=775&assignee=rh-ee-pmohta
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。