Red Hat Enterprise Linux for SAP Solutions 9

为 SAP HANA 使用 SELinux

Last Updated: 2024-05-01

法律通告

摘要

配置 SELinux 可帮助您增强系统的安全性。SELinux 是一种强制访问控制(MAC)的实现，它提供额外的安全层。SELinux 策略定义了用户和进程如何与系统上的文件进行交互。您可以通过将用户映射到特定的 SELinux 受限用户来控制哪些用户可以执行哪些操作。

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 SELINUX 简介

SELinux 通过强制安全策略提供增强安全性，使用文件、进程和端口的标签以及日志记录未经授权的访问尝试。

默认情况下，SELinux 在 RHEL 9 上启用并设置为 **enforcing** 模式，红帽会维护系统进程的安全策略。如需更多信息，请参阅 更改 RHEL 上的 SELinux 状态和模式 。您可以参考 SAP Note 3108302 - SAP HANA DB：推荐 RHEL 9 的建议操作系统设置，以了解 SAP 已测试哪个 HANA 版本，并将 SELinux 设置为 **enforcing** 和 **unconfined** 模式。

红帽建议您在 **enforcing** 模式下使用 SELinux 来配置在 SAP HANA 上运行的 RHEL 系统。本文档描述了您必须进行的必要配置更改。

如果您在测试或运行 SAP HANA 系统时遇到与 SELinux 相关的问题，SAP 保留禁用 SELinux 的权利。但是，大多数问题可以通过将 SELinux 模式从 **enforcing** 模式更改为 **permissive** 来解决。这样做的好处是，在分析和解决问题的同时，您的系统仍然正常运行。

第 2 章 配置 SELINUX 以排除 SAP HANA 目录

默认情况下，如果您的 RHEL 系统运行时，没有定义 SELinux 安全策略的任何应用程序都会被 SELinux 阻止。**目前，SAP 不会为 SAP HANA 提供 SELinux 策略。对于在 SELinux 设置为 enforcing 时运行 SAP HANA 可执行文件，必须设置特定的 SELinux 布尔值，并且 SAP HANA 相关目录必须从 SELinux 保护中排除。您还可以使用 fapolicyd 框架来保护 SAP HANA 软件。如需更多信息，请参阅配置 fapolicyd 以只允许 SAP HANA 可执行文件 文档。**

先决条件

- **SAP HANA 已安装并停止，或尚未安装。**
- **SELinux 可用，并设置为 enforcing 模式。**
- **安装了 SAP HANA 及相关软件的目录（通常是 /hana 和 /usr/sap）。**

流程

1. **使用以下命令，将 SELinux 布尔值 selinuxuser_execmod 设置为 1，允许无限制的可执行文件使用需要文本重定位的库（如 SAP HANA）：**

```
# setsebool -P selinuxuser_execmod 1
```

2. **使用以下命令重新标记 SAP HANA 使用的目录和文件（通常为 /hana 和 /usr/sap），以便 SAP HANA 可以在未限制模式下运行：**

```
# semanage fcontext -a -t usr_t '/hana(/.)?'*
# semanage fcontext -a -t usr_t '/usr/sap(/.)?'*
# restorecon -Rv '/hana'
# restorecon -Rv '/usr/sap'
```

注意

您可以在安装 SAP HANA 之前或之后执行此步骤，因为上一级目录下所有新创建的目录和文件都继承 SELinux 标签。

验证

- **使用以下命令显示 /usr/bin 和 /hana 下的文件或目录的安全上下文，确认 /hana 下的文件或目录具有 usr_t 标签：**

```
[root@host01 ~]# ls -lZ /usr/bin/ls
-rwxr-xr-x. 1 root root system_u:object_r:bin_t:s0 143296 Jan  6  2023 /usr/bin/ls
[root@host01 ~]# ls -lZd /hana/shared
drwxr-xr-x. 3 root root system_u:object_r:usr_t:s0 17 Apr 18 23:03 /hana/shared
```

第 3 章 故障排除与 SELINUX 相关的问题

要诊断与 SELinux 相关的问题，您可以检查文件 /var/log/audit/audit.log，如下所示：

1. **要查询审计日志，请使用 ausearch 工具。SELinux 决策（如允许或禁止访问）会在 Access Vector Cache (AVC)中缓存。因此，您应该将 AVC 和 USER_AVC 值用于 message type 参数，例如：**

```
# ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts boot
```

2. **如果没有匹配项，请检查 audit 守护进程是否正在运行。**

3. **如果它没有运行，请执行以下步骤：**

   a. **重新启动审计。**

   b. **重新运行拒绝的场景。**

   c. **再次检查审计日志。**

有关解决 SELinux 相关问题的更多信息，请参阅 SELinux 故障排除。

第 4 章 附加信息

- 根据您的环境（云供应商、第三方用户工具和代理），您应该在附加挂载点(/opt、/sapmnt 和 /trans)上更改 SELinux 标签。