Red Hat Enterprise Linux for SAP Solutions 9

配置 fapolicyd 以只允许 SAP HANA 可执行文件

Last Updated: 2024-04-30

Red Hat Enterprise Linux for SAP Solutions 9 配置 fapolicyd 以只允许 SAP HANA 可执行文件

法律通告

摘要

配置此策略，以保护运行 SAP HANA 环境免受本地和远程入侵、利用和恶意活动的环境。

目录

使开源包含更多 3

对红帽文档提供反馈 4

第 1 章 FAPOLICYD 简介 5

第 2 章 使用 FAPOLICYD 保护 SAP HANA 安装 6
2.1. 安装 FAPOLICYD 软件包 6
2.2. 将完整性检查设置为 SHA-256 哈希 6
2.3. 添加自定义 FAPOLICYD 规则来保护 SHELL 脚本 7
2.4. 将 SAP HANA 文件标记为可信 8
2.5. 启用 FAPOLICYD 服务 8

第 3 章 更新 SAP HANA 时重新创建 FAPOLICYD 信任文件 10

第 4 章 故障排除与 FAPOLICYD 相关的问题 11

第 5 章 附加信息 12

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 FAPOLICYD 简介

fapolicyd 软件框架根据用户定义的策略来控制应用程序的执行。这是防止在系统上运行不受信任的和可能具有恶意的应用程序的最有效的方法之一。如需更多信息，请参阅 RHEL 9 安全强化 指南中的使用 fapolicyd 来阻止和 允许应用程序。

注意

下面的步骤将所有检测到的 SAP HANA 可执行文件放入 **fapolicyd** 信任文件中，其中包含可信文件的所有名称、大小和校验和。SAP HANA 二进制文件和 shell 脚本只能在 **fapolicyd** 信任文件中包含时才执行。因此，如果您执行不包含在 **fapolicyd** 信任文件中的 SAP HANA 二进制文件或 shell 脚本，则可能会出现不必要的影响，包括损坏或数据丢失。您必须仔细测试所有步骤，并首先在非生产环境的系统上进行正确的验证。

第 2 章 使用 FAPOLICYD 保护 SAP HANA 安装

您可以执行以下步骤来保护 SAP HANA 安装：

- 安装 **fapolicyd** 软件包。
- 将完整性检查设置为 **SHA-256** 哈希。
- 添加自定义 **fapolicyd** 规则来保护 shell 脚本。
- 将 SAP HANA 文件标记为可信。
- 启用 **fapolicyd** 服务。

2.1. 安装 FAPOLICYD 软件包

流程

- 安装 **fapolicyd** 软件包：

```
# dnf install fapolicyd
```

验证

- 使用以下命令验证 **fapolicyd** 服务是否已安装，但当前没有运行：

```
# systemctl status fapolicyd
● fapolicyd.service - File Access Policy Daemon
   Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor preset:
disabled)
   Active: inactive (dead) since Fri 2024-04-19 14:59:52 CEST; 1s ago
...
Apr 19 14:59:51 host01 fapolicyd[337927]: shutting down...
Apr 19 14:59:51 host01 systemd[1]: Stopping File Access Policy Daemon...
Apr 19 14:59:52 host01 systemd[1]: fapolicyd.service: Succeeded.
Apr 19 14:59:52 host01 systemd[1]: Stopped File Access Policy Daemon.
```

2.2. 将完整性检查设置为 SHA-256 哈希

默认情况下，**fapolicyd** 会在决定应用程序是否被阻止执行时验证文件名。您可以为更高级别的保护将此设置修改为 **SHA-256**。

先决条件

- **fapolicyd** 软件包已安装在您的系统中。

流程

1. 在您选择的文本编辑器中打开 **/etc/fapolicyd/fapolicyd.conf** 文件，例如：

```
# vi /etc/fapolicyd/fapolicyd.conf
```

2. 配置 integrity 选项，将默认值 **none** 改为 **sha-256** ：

```
integrity = sha-256
```

要使更改生效，您需要重启 **fapolicyd** 服务。但您不得现在重启 **fapolicyd**，因为您必须对 **fapolicyd** 配置进行更多更改。

验证

- 验证正确的条目：

```
# fapolicyd-cli --check-config
Daemon config is OK
```

SAP HANA 基准在 RHEL 9.2 上进行了测试。在这样做时，最初禁用了 **fapolicyd**，然后启用来评估 **fapolicyd** 的性能影响。要允许测试运行，总计 19,184 条目被添加到 **fapolicyd** 信任文件中。在 99% 的测试中，性能影响为 5% 或更少，因为大多数测试都遇到了缓慢的 1-3% 的测试。

请注意，某些工作负载可能会遇到更高的性能损失。因此，您必须完全评估特定环境中的性能，才能准确观察潜在的影响。

2.3. 添加自定义 FAPOLICYD 规则来保护 SHELL 脚本

默认情况下，**fapolicyd** 会阻止二进制可执行文件和某些程序（如 Python）被执行。为了保护 SAP HANA 安装目录中的 shell 脚本，您必须添加新的自定义规则。

先决条件

- **fapolicyd** 软件包已安装在您的系统中。

流程

1. 打开目录 **/etc/fapolicyd/rules.d**。
2. 添加一个以 71 开头的文件名（带文件名 **71-sap-shellscript.rules**）的新文件，以便规则放置在文件 **70-trusted-lang.rules** 和 **72-shell.rules** 的规则之间，其内容如下：

```
# Deny shell script execution and sourcing under SAP HANA directories

deny_audit perm=any all : ftype=text/x-shellscript dir=/hana/,/usr/sap/ trust=0
```

3. 将文件的所有权设置为 **/etc/fapolicyd/rules.d** 中其他文件的所有权：

```
# chown root:fapolicyd 71-sap-shellscript.rules
```

4. 使用以下命令确认定义了新规则，然后载入新规则：

```
# fagenrules --check
/usr/sbin/fagenrules: Rules have changed and should be updated
# fagenrules --load
```

验证

- 验证规则是否已更新：

```
# fagenrules --check
/usr/sbin/fagenrules: No change
```

2.4. 将 SAP HANA 文件标记为可信

前提条件

- **fapolicyd** 软件包已安装在您的系统中。

流程

1. 安装 SAP HANA 软件（如果尚未完成）。
2. 使用以下命令将所有 SAP HANA 文件添加到 **fapolicyd** 信任数据库。我们建议为每个目录树使用单独的信任文件，如 **hana** 和 **usr_sap** ：

```
# fapolicyd-cli --file add /hana --trust-file hana
# fapolicyd-cli --file add /usr/sap --trust-file usr_sap
```

这会在 **/etc/fapolicyd/trust.d** 目录中创建两个名为 **hana** 和 **usr_sap** 的文件，其中包含 **/hana** 和 **/usr/sap** 下所有文件的条目。

3. 对于新安装的 RHEL 系统上的 SAP HANA 安装，SAP HANA 安装程序会创建目录 **/hana** 和 **/usr/sap**，因此我们可以信任这些目录中的所有文件都是有效的 SAP 文件。
在任何其他情况下，这些目录中可能存在 SAP HANA 安装程序尚未创建的文件。

   因此，您应该仔细验证信任文件 **/etc/fapolicyd/trust.d/hana** 和 **/etc/fapolicyd/trust.d/usr_sap** 中的所有文件都是有效的 SAP 文件。以下是可能的方法之一：

   i. 在另一个新安装的 RHEL 系统上执行全新的 SAP HANA 安装。

   ii. 在该系统上重复步骤 2。

   iii. 比较两个系统生成的信任文件。

2.5. 启用 FAPOLICYD 服务

先决条件

- **fapolicyd** 软件包已安装，且当前没有在您的系统中运行。
- 您已完成了所有前面的步骤。

流程

- 启用并启动 **fapolicyd** 服务：

```
# systemctl enable --now fapolicyd
```

fapolicyd 服务现在保护 SAP HANA 系统。不在 **fapolicyd** 信任文件中的 **/hana** 或 **/usr/sap** 中的脚本和二进制文件会被阻止，非 root 用户无法执行这些文件。

验证

1. 验证 **fapolicyd** 服务是否正在运行：

```
# systemctl status fapolicyd
● fapolicyd.service - File Access Policy Daemon
    Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; preset: disabled)
    Active: active (running) since Thu 2024-03-14 16:38:32 IST; 18h ago
...
Mar 14 16:38:33 host01 fapolicyd[579216]: Trust database checks OK
Mar 14 16:38:33 host01 fapolicyd[579216]: Starting to listen for events
```

2. 验证非 root 用户，包括 SAP HANA 管理员用户（例如： **h70adm**），无法在 **/hana** 和 **/usr/sap** 中执行任何新脚本和二进制程序：

```
# cp -pi /usr/bin/date /hana/
# su - h70adm
h70adm@host01:/usr/sap/H70/HDB35> /hana/date
-sh: /hana/date: Operation not permitted
h70adm@host01:/usr/sap/H70/HDB35> cat > try-to-start-me.sh
#!/bin/bash
echo "I will not execute."
<ctrl>d
h70adm@host01:/usr/sap/H70/HDB35> chmod u+x try-to-start-me.sh
h70adm@host01:/usr/sap/H70/HDB35> ./try-to-start-me.sh
-sh: ./try-to-start-me.sh: Operation not permitted
h70adm@host01:/usr/sap/H70/HDB35> rm try-to-start-me.sh
h70adm@host01:/usr/sap/H70/HDB35> exit
# rm /hana/date
rm: remove regular file '/hana/date'? y
```

第 3 章 更新 SAP HANA 时重新创建 FAPOLICYD 信任文件

先决条件

- **fapolicyd** 软件包已安装在您的系统中。
- 您已确认 SAP HANA 软件目录中没有新的可执行文件，因此您不会意外地添加来自未知来源的软件。如需更多信息，请参阅将 SAP HANA 文件标记为可信。

流程

1. 在执行 SAP HANA 软件更新前，停止 **fapolicyd** ：

```
# systemctl stop fapolicyd
```

2. 创建现有 **fapolicyd** 信任文件 **/etc/fapolicyd/trust.d/hana** 和 **/etc/fapolicyd/trust.d/usr_sap** 的备份，然后删除这些文件。
3. 执行 SAP HANA 软件更新。
4. 重复步骤部分的第 2 步，将 SAP HANA 文件标记为可信，以便为 SAP HANA 重新创建 **fapolicyd** 信任文件。
5. 启动 **fapolicyd** ：

```
# systemctl start fapolicyd
```

第 4 章 故障排除与 FAPOLICYD 相关的问题

要诊断与 **fapolicyd** 相关的问题，您可以：

- 检查文件 **/var/log/fapolicyd-access.log** 以了解 **fapolicyd** 访问统计信息和/或
- 在 debug 模式下运行 **fapolicyd**。

有关诊断 **fapolicyd** 相关问题的更多信息，请参阅与 fapolicyd 相关的故障排除问题。

第 5 章 附加信息

- 在 **fapolicyd** 信任文件中添加更多文件后，使用以下命令更新 **fapolicyd** 数据库：

```
# fapolicyd-cli --update
```

- 从 **fapolicyd** 信任文件中删除条目后，您必须重启 **fapolicyd** ：

```
# systemctl restart fapolicyd
```