Red Hat Enterprise Linux for SAP Solutions 9

SAP HANA での SELinux の使用

Last Updated: 2024-06-21

Red Hat Enterprise Linux for SAP Solutions 9 SAP HANA での SELinux の使用

法律上の通知

概要

SELinux を設定すると、システムのセキュリティーを強化できます。SELinux は強制アクセス制御 (MAC) の実装であり、追加のセキュリティー層を提供します。SELinux ポリシーは、ユーザーとプロセスがシステム上のファイルと対話する方法を定義します。特定の SELinux で制限されたユーザーにマッピングすることで、どのユーザーがどのアクションを実行できるかを制御できます。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメントにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。多様性を受け入れる用語に変更する取り組みの詳細は、Red Hat CTO である Chris Wright のメッセージ を参照してください。

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインしていることを確認してください。
2. こちらのリンク をクリックして、フィードバックをお寄せください。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
5. 今後の更新に関する通知を受け取りたい場合は、**Reporter** としてご自身が割り当てられていることを確認してください。
6. ダイアログの下部にある **Create** をクリックします。

第1章 SELINUX の概要

SELinux は、セキュリティーポリシーを適用し、ファイル、プロセス、ポートにラベルを使用し、不正なアクセス試行をログに記録することで、セキュリティーを強化します。

SELinux は RHEL 9 ではデフォルトで有効になっており、**enforcing** モードに設定されており、システムプロセスのセキュリティーポリシーは Red Hat によって管理されます。詳細は、RHEL での SELinux の状態とモードの変更 を参照してください。SAP Note 3108302 - SAP HANA DB: Recommended OS Settings for RHEL 9 を参照して、SELinux を**enforcing** モードおよび **unconfined** モードに設定して SAP によってテストされた HANA バージョンを確認できます。

Red Hat では、SAP HANA 上で実行する RHEL システムを設定するために、SELinux を **enforcing** モードで使用することを推奨しています。このドキュメントでは、実行する必要がある設定の変更を説明します。

SAP HANA システムのテスト中または実行中に SELinux 関連の問題が発生した場合、SAP は SELinux を無効にする権利を留保します。ただし、ほとんどの問題は、SELinux モードを **enforcing** から **permissive** に変更することで解決できます。利点は、問題を分析して解決する間もシステムが稼働し続けることです。

第2章 SAP HANA ディレクトリーを除外するように SELINUX を設定する

デフォルトでは、RHEL システムが SELinux を **enforcing** モードに設定して実行している場合、SELinux セキュリティーポリシーが定義されていないアプリケーションはすべて SELinux によってブロックされます。現在のところ、SAP は SAP HANA 向けの SELinux ポリシーを提供していません。SELinux が強制に設定されているときに SAP HANA 実行可能ファイルを実行するには、特定の SELinux ブール値を設定し、SAP HANA 関連ディレクトリーを SELinux 保護から除外する必要があります。**fapolicyd** フレームワークを使用して SAP HANA ソフトウェアを保護することもできます。詳細は、SAP HANA 実行可能ファイルのみを許可するように fapolicyd を設定する を参照してください。

前提条件

- SAP HANA がインストールされて停止されているか、まだインストールされていない。
- SELinux が利用可能であり、**enforcing** モードに設定されている。
- SAP HANA および関連ソフトウェアがインストールされているディレクトリー (通常は **/hana** および **/usr/sap**) が存在する。

手順

1. 次のコマンドを使用して、SELinux ブール値 **selinuxuser_execmod** を **1** に設定し、制限のない実行可能ファイルがテキストの再配置を必要とするライブラリー (SAP HANA など) を使用できるようにします。

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

2. 次のコマンドを使用して、SAP HANA が使用するディレクトリーとファイル (通常は **/hana** と **/usr/sap**) のラベルを変更し、SAP HANA を **unconfined** モードで実行できるようにします。

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

注記

上位ディレクトリーの下に新しく作成されたすべてのディレクトリーとファイルは SELinux ラベルを継承するため、この手順は SAP HANA のインストール前でもインストール後でも実行できます。

検証

- 次のコマンドを使用して、**/usr/bin** および **/hana** 内のファイルまたはディレクトリーのセキュリティーコンテキストを表示し、**/hana** の下のファイルまたはディレクトリーに **usr_t** ラベルがあることを確認します。

```
[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 SELINUX に関連する問題のトラブルシューティング

SELinux に関連する問題を診断するには、次のように **/var/log/audit/audit.log** ファイルを確認します。

1. Audit ログのクエリーには、**ausearch** ツールを使用します。アクセスの許可や不許可などの SELinux の決定は、アクセスベクターキャッシュ (AVC) にキャッシュされます。したがって、メッセージタイプパラメーターには **AVC** 値と **USER_AVC** 値を使用する必要があります。次に例を示します。

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

2. 一致するものがない場合は、Audit デーモンが実行しているかどうかを確認します。

3. 実行していない場合は、次の手順を実行します。

   a. 監査を再開します。

   b. 拒否されたシナリオを再実行します。

   c. 監査ログをもう一度確認してください。

   SELinux 関連の問題を解決する方法の詳細は、SELinux 関連の問題のトラブルシューティング を参照してください。

第4章 関連情報

- 環境 (クラウドプロバイダー、サードパーティーのユーザーツール、エージェント) に応じて、追加のマウントポイント (**/opt**、**/sapmnt**、**/trans**) の SELinux ラベルを変更する必要があります。