Red Hat Enterprise Linux 8

SELinux の使用

Security-Enhanced Linux (SELinux) の基本設定および高度な設定

Last Updated: 2019-04-23

Red Hat Enterprise Linux 8 SELinux の使用

Security-Enhanced Linux (SELinux) の基本設定および高度な設定

法律上の通知

概要

本書は、ユーザーおよび管理者が利用できるように、SELinux の基礎および基本を紹介し、様々なサービスを設定および構成する実用的な作業を説明します。

目次

RED HAT ドキュメントへのフィードバック

ドキュメントの改善に関するご意見やご要望をお聞かせください。

- 特定の文章に簡単なコメントを記入する場合は、ドキュメントが Multi-page HTML 形式になっているのを確認してください。コメントを追加する部分を強調表示し、そのテキストの下に表示される **Add Feedback** ポップアップをクリックし、表示された手順に従ってください。
- より詳細なフィードバックを行う場合は、Bugzilla のチケットを作成します。
  1. Bugzilla の Web サイトにアクセスします。
  2. Component で **Documentation** を選択します。
  3. **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記入してください。
  4. **Submit Bug** をクリックします。

第1章 SELINUX の使用

1.1. SELINUX の概要

Security Enhanced Linux (SELinux) は、新たにシステムセキュリティーの層を提供します。SELinux は、基本的に **May <subject> do <action> to <object>?** の形式の問い (たとえば「**May a web server access files in users' home directories?** (Web サーバーは、ユーザーのホームディレクトリーのファイルにアクセスできますか?)」) に答えていきます。

ユーザー、グループ、およびその他のアクセス権に基づいた標準のアクセスポリシーは Discretionary Access Control (DAC) として知られており、システム管理者が、包括的で詳細なセキュリティーポリシー (たとえば、特定のアプリケーションではログファイルの表示だけを許可し、その他のアプリケーションでは、ログファイルに新しいデータを追加するのを許可するなど) を作成することはできません。

SELinux は、Mandatory Access Control (MAC) を実装します。それぞれのプロセスおよびシステムリソースには、**SELinux コンテキスト** と呼ばれる特別なセキュリティーラベルがあります。SELinux コンテキストは **SELinux ラベル** として参照されることがありますが、システムレベルの詳細を抽象化し、エンティティーのセキュリティープロパティーに焦点を当てた識別子です。これは、SELinux ポリシーでオプションを参照する一貫性のある方法を提供し、他の識別方法では解消できないあいまいさ (たとえば、ファイルがバインドマウントを利用したシステムで複数の有効なパスを持つことが可能) を排除します。

SELinux ポリシーは、プロセスが互いに対話する方法を定義する一連のルールにこのコンテキストを使用します。デフォルトでは、最初にルールが明示的にアクセスを許可し、その後ポリシーが任意の対話を許可します。

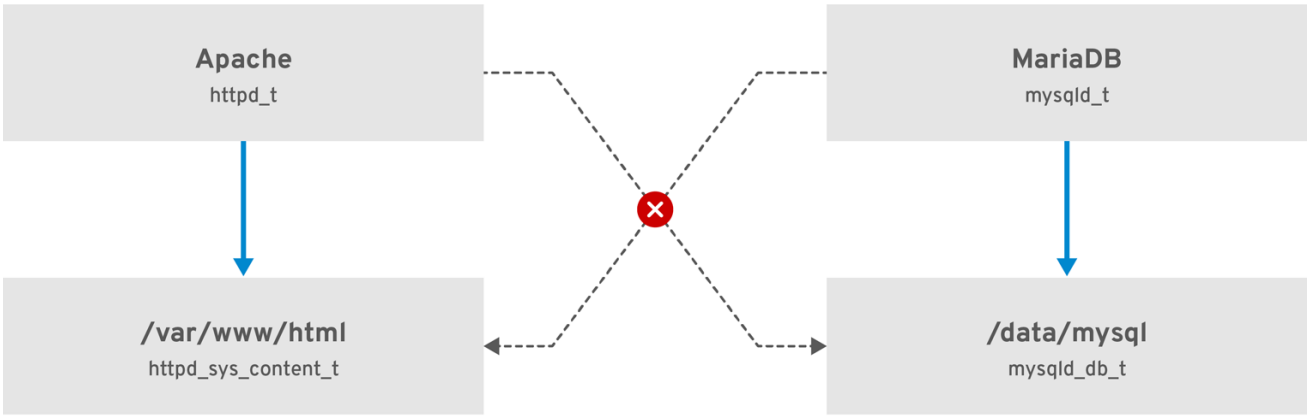
注記

SELinux ポリシールールが DAC ルールの後に確認されている点に注意してください。DAC ルールが最初にアクセスを拒否する場合、SELinux ポリシールールは使用されません。これは、従来の DAC ルールがそのアクセスを拒否する場合は、SELinux 拒否がログに記録されないということを示しています。

SELinux コンテキストには、複数のフィールド (ユーザー、ロール、タイプ、セキュリティーレベル) があります。SELinux ポリシーではおそらく SELinux のタイプ情報が最も重要です。プロセスとシステムリソースとの間で許可される対話を定義する最も一般的なポリシールールが、完全な SELinux コンテキストではなく、SELinux のタイプを使用するためです。SELinux のタイプは、通常 **_t** で終わります。たとえば、Web サーバーのタイプ名は **httpd_t** です。**/var/www/html/** にあるファイルとディレクトリーのタイプコンテキストは、通常 **httpd_sys_content_t** です。**/tmp** および **/var/tmp/** にあるファイルおよびディレクトリーに対するタイプコンテクストは、通常 **tmp_t** です。Web サーバーポートのタイプコンテキストは **http_port_t** です。

たとえば、Apache (**httpd_t** として実行する Web サーバープロセス) を許可するポリシールールがあります。このルールでは、通常 **/var/www/html/** にあるコンテキストを持つファイルおよびディレクトリーと、その他の Web サーバーディレクトリー (**httpd_sys_content_t**) へのアクセスを許可します。通常、**/tmp** および **/var/tmp/** に含まれるファイルのポリシーには、許可ルールがありません。SELinux を使用すれば、Apache が危険にさらされ、悪意のあるスクリプトがアクセスを得た場合でも、**/tmp** ディレクトリーにアクセスすることはできなくなります。

図1.1 SELinux は、httpd_t として実行している Apache プロセスが /var/www/html/ ディレクトリーにアクセスするのは許可しますが、同じ Apache プロセスが /data/mysql/ ディレクトリーにアクセスするのは拒否します。これは、httpd_t タイプコンテキストと mysqld_db_t タイプコンテキストに許可ルールがないのが原因です。一方、mysqld_t として実行する MariaDB プロセスは /data/mysql/ ディレクトリーにアクセスできますが、SELinux により、mysqld_t タイプを持つプロセスが、httpd_sys_content_t とラベルが付いた /var/www/html/ ディレクトリーにアクセスするのは拒否されます。



関連資料
SELinux の基本概念の詳細は、次のドキュメントを参照してください。

- man ページの **`selinux(8)`**
- The SELinux Coloring Book
- SELinux for Mere Mortals
- SELinux Wiki FAQ
- The SELinux Notebook

1.2. SELINUX を実行する利点

SELinux は、次のような利点を提供します。

- プロセスとファイルにはすべてラベルが付いています。SELinux ポリシーで、プロセスがファイルと対話する方法と、プロセスが互いに対話する方法が定義されます。アクセスは、それを特別に許可する SELinux ポリシールールが存在する場合に限り許可されます。
- 詳細なアクセス制御。SELinux のアクセスは、ユーザーの裁量と、Linux のユーザー ID およびグループ ID に基づいて制御される従来の UNIX アクセス権だけでなく、SELinux のユーザー、ロール、タイプ、(および必要に応じてセキュリティーレベル) などの、入手可能なすべての情報に基づいて決定されます。
- SELinux ポリシーは管理者により定義され、システム全体に適用されます。
- 権限昇格攻撃に対する軽減策が向上。プロセスはドメインで実行するため、互いに分離しています。SELinux ポリシールールは、プロセスがどのようにファイルやその他のプロセスにアクセスするかを定義します。プロセスへのアクセスが不正に行われても、攻撃者は、そのプロセスの通常の機能と、そのプロセスがアクセスするように設定されているファイルにしかアクセスできません。たとえば、Apache HTTP Server へのアクセスが不正に行われても、そのアク

セスを許可する特別な SELinux ポリシールールが追加されたり、設定された場合を除き、ユーザーのホームディレクトリーにあるファイルを読み込むプロセスを攻撃者が利用することはできません。

- SELinux は、データの機密性と完全性、並びに信頼されていない入力からの保護プロセスを強化するのに使用できます。

ただし、SELinux は以下の機能とは異なります。

- ウイルス対策ソフトウェア
- パスワード、ファイアウォールなどのセキュリティーシステムの代替
- 一体型のセキュリティーソリューション

SELinux は、既存のセキュリティーソリューションを強化するために作られており、代わりに使用されるものではありません。SELinux を実行している場合でも、ソフトウェアを最新の状態にする、推測が困難なパスワードを使用する、ファイアウォールを使用するなど、優れたセキュリティー対策を続けることが重要です。

1.3. SELINUX の例

以下の例は、SELinux がどのようにセキュリティーを向上するかを説明します。

- デフォルトのアクションは「拒否」です。アクセスを許可する SELinux のポリシールール (ファイルを開くプロセスなど) が存在しない場合は、アクセスが拒否されます。
- SELinux は、Linux ユーザーに制限をかけられます。SELinux ポリシーには、制限がかけられた SELinux ユーザーが多数含まれます。Linux ユーザーを、制限がかけられた SELinux ユーザーにマッピングして、SELinux ユーザーに適用されているセキュリティールールおよびメカニズムを利用できます。たとえば Linux ユーザーを、SELinux の **user_u** にマッピングすると、その Linux ユーザーは、(許可が設定されていない限り) **sudo** や **su** などの setuid (set user ID) アプリケーションを実行したり、そのユーザーのホームディレクトリーにある (害を及ぼす可能性がある) ファイルやアプリケーションを実行したりできなくなります。
- プロセスとデータの分離を向上。プロセスは自身のドメインで実行するため、その他のプロセスが使用するファイルにアクセスしたり、他のプロセスからアクセスされることはありません。たとえば、SELinux を実行している場合に、(許可が設定されていない限り) 攻撃者は Samba サーバーを危険にさらすことはできず、その Samba サーバーを攻撃ベクトルとして使用して、その他のプロセス (MariaDB など) が使用するファイルの読み書きを行うことはできません。
- SELinux は、設定ミスによるダメージを軽減します。Domain Name System (DNS) サーバーはゾーン転送として知られている機能で、互いの間で頻繁に情報を複製します。攻撃者は、ゾーン転送を使用して、虚偽の情報で DNS サーバーを更新できます。Red Hat Enterprise Linux で Berkeley Internet Name Domain (BIND) を DNS サーバーとして実行すると、ゾーン転送を実行できるサーバーを管理者が制限し忘れた場合でも、BIND **named** デーモンと、その他のプロセスによるゾーン転送を利用してゾーンファイル [1] が更新されるのを、デフォルトの SELinux ポリシーにより防くことができます。

1.4. SELINUX のアーキテクチャーおよびパッケージ

SELinux は、Linux カーネルに組み込まれる Linux セキュリティーモジュール (LSM) です。カーネルの SELinux サブシステムは、管理者が制御し、システムの起動時に読み込まれるセキュリティーポリシーにより動作します。システムにおけるセキュリティー関連の、カーネルレベルのアクセス操作はすべて

SELinux により傍受され、読み込んだセキュリティーポリシーのコンテキストに従って検討されます。読み込んだポリシーが操作を許可すると、その操作は継続します。許可しないと、その操作はブロックされ、プロセスがエラーを受け取ります。

アクセスの許可、拒否などの SELinux の結果はキャッシュされます。このキャッシュは、アクセスベクトルキャッシュ (AVC) として知られています。このようにキャッシュされた結果を使用すると、必要なチェックの量が減るため、SELinux ポリシーのパフォーマンスが向上します。DAC ルールがアクセスを拒否した場合は、SELinux ポリシールールが適用されないことに注意してください。未加工の監査メッセージのログは、行頭に **type=AVC** 文字列が追加されて、**/var/log/audit/audit.log** に記録されます。

Red Hat Enterprise Linux 8 では、システムサービスは **systemd** デーモンにより制御されます。すべてのサービスの開始および停止は **systemd** が行い、ユーザーとプロセスは、**systemctl** を介して **systemd** とやりとりします。**systemd** デーモンは、SELinux ポリシーを調べ、呼び出しているプロセスのラベルと、呼び出し元が管理するユニットファイルのラベルを確認してから、呼び出し元のアクセスを許可するかどうかを SELinux に確認します。このアプローチにより、システムサービスの開始や停止などの、重要なシステム機能へのアクセス制御が強化されます。

また、**systemd** デーモンは SELinux Access Manager としても起動し、**systemctl** を実行するプロセス、または **systemd** に **D-Bus** メッセージを送信したプロセスのラベルを取得します。その後、プロセスが設定したユニットファイルのラベルをデーモンが検索します。そして、プロセスのラベルと、ユニットファイルのラベルの間のアクセスを SELinux ポリシーが許可する場合は、**systemd** がカーネルから情報を取得します。これは、不正アクセスされたアプリケーションが、特定のサービスについて **systemd**とやりとりする必要があるかどうかを、SELinux で設定できることを示しています。ポリシーの作成者は、このような詳細な制御を使用して、管理者を制御することもできます。

重要

SELinux ラベリングが誤っているために問題が発生するのを回避するには、**systemctl start** コマンドを使用してサービスを開始するようにしてください。

Red Hat Enterprise Linux 8 では、SELinux を操作する以下のパッケージが提供されます。

- ポリシー - **selinux-policy-targeted**、**selinux-policy-mls**
- ツール - **policycoreutils**、**policycoreutils-gui**、**libselinux-utils**、**policycoreutils-python-utils**、**setools-console**, **checkpolicy**

1.5. SELINUX の状態およびモード

SELinux は、3 つあるモード (Disabled、Permissive、または Enforcing) のいずれかで実行できます。

Disabled モードを使用することは推奨されません。システムは、SELinux ポリシーの強制を回避するだけでなく、ファイルなどの任意の永続オブジェクトにラベルを付けなくなり、将来的に SELinux を有効にすることが難しくなります。

Permissive モードでは、システムは、読み込んだセキュリティーポリシーを SELinux が強制しているように振る舞い、オブジェクトのラベリングや、ログにアクセスを拒否したエントリーを出力しますが、実際に操作を拒否しているわけではありません。Permissive モードは、実稼働システムで使用することは推奨されませんが、SELinux ポリシーの開発やデバッグには役に立ちます。

Enforcing モードは、デフォルトのモードで、推奨される動作モードです。SELinux は、Enforcing モードでは正常に動作し、読み込んだセキュリティーポリシーをシステム全体に強制します。

Enforcing モードと Permissive モードとの間を切り替えるには **setenforce** ユーティリティーを使用

してください。**setenforce** で行った変更は、システムを再起動すると元に戻ります。Enforcing モードに変更するには、Linux の root 権限で、**setenforce 1** コマンドを実行します。Permissive モードに変更するには、**setenforce 0** コマンドを実行します。**getenforce** ユーティリティーを使用して、現在の SELinux モードを表示します。

```
# getenforce
Enforcing
```

```
# setenforce 0
# getenforce
Permissive
```

```
# setenforce 1
# getenforce
Enforcing
```

Red Hat Enterprise Linux では、システムを Enforcing モードで実行している場合に、個々のドメインを Permissive モードに設定できます。たとえば、**httpd_t** ドメインを Permissive に設定するには、以下を行います。

```
# semanage permissive -a httpd_t
```

[1] IP アドレスマッピングへのホスト名など、DNS サーバーが使用する情報が含まれるテキストファイル。

第2章 SELINUX の状態およびモードの変更

2.1. SELINUX の状態およびモードの永続的変更

「SELinux の状態およびモード」 にあるように、SELinux は有効にも無効にもできます。有効にした場合の SELinux のモードには、Enforcing および Permissive の 2 つがあります。

getenforce コマンド、または **sestatus** コマンドを使用して、SELinux が実行しているモードを確認できます。**getenforce** コマンドは、**Enforcing**、**Permissive**、または **Disabled** を返します。

sestatus コマンドは SELinux の状態と、使用されている SELinux ポリシーを返します。

```
$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      31
```

注記

Permissive モードで SELinux を実行すると、ユーザーやプロセスにより、さまざまなファイルシステムオブジェクトのラベルが間違って設定される可能性があります。SELinux が無効になっている間に作成されたファイルシステムのオブジェクトには、ラベルが追加されません。したがって、SELinux では、ファイルシステムオブジェクトのラベルが正しいことが必要になるため、Enforcing モードに変更したときに問題が発生します。Disabled 状態から Permissive モードまたは Enforcing モードに変更すると、ファイルシステムのラベルが自動的に再設定されます。

2.2. SELINUX の有効化

SELinux が有効になっている場合は、Enforcing モードまたは Permissive モードのいずれかで実行できます。以下のセクションでは、これらのモードに変更する方法を説明します。

SELinux が無効になっていたシステムで SELinux を有効にする際に、システムが起動できない、プロセスが失敗するなどの問題を回避するには、この手順に従ってください。

1. SELinux を Permissive モードで有効にします。詳細は 「Permissive モードへの変更」 を参照してください。
2. システムを再起動します。
3. SELinux の拒否メッセージをチェックします。
4. 拒否がない場合は、Enforcing モードに切り替えます。詳細は 「Enforcing モードへの変更」 を参照してください。

Enforcing モードで SELinux を使用してカスタムアプリケーションを実行するには、次のいずれかのシナリオを選択してください。

- **unconfined_service_t** ドメインでアプリケーションを実行します。
- アプリケーションに新しいポリシーを記述します。詳細は、ナレッジベースアーティクル「Writing Custom SELinux Policy」 を参照してください。

モードの一時的な変更は 「SELinux の状態およびモード」 で説明されています。

2.2.1. Permissive モードへの変更

SELinux を Permissive モードで実行していると、SELinux ポリシーは強制されません。システムは動作し続け、SELinux がオペレーションを拒否せず AVC メッセージをログに記録できるため、このログを使用して、トラブルシューティングやデバッグ、そして SELinux ポリシーの改善に使用できます。この場合、各 AVC は一度だけログに記録されます。

モードを Permissive へ永続的に変更するには、以下の手順に従ってください。

1. 以下のように **/etc/selinux/config** ファイルを編集します。

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

2. システムを再起動します。

```
# reboot
```

2.2.2. Enforcing モードへの変更

SELinux を Enforcing モードで実行している場合は、SELinux ポリシーが強制され、SELinux ポリシールールに基づいてアクセスが拒否されます。Red Hat Enterprise Linux では、システムに SELinux を最初にインストールした時に、Enforcing モードがデフォルトで有効になります。

前提条件
selinux-policy-targeted、**libselinux-utils**、および **policycoreutils** の各パッケージがインストールされている。

手順
SELinux が無効の場合は、以下の手順に従って、再度 Enforcing モードに変更してください。

1. 以下のように **/etc/selinux/config** ファイルを編集します。

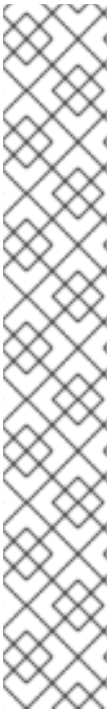
```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
```

```
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

2. システムを再起動します。

```
# reboot
```

次回の起動時に、SELinux はシステム内のファイルおよびディレクトリーのラベルを再設定し、SELinux が無効になっている間に作成したファイルおよびディレクトリーに SELinux コンテキストを追加します。



注記

Enforcing モードに変更したあと、SELinux ポリシーが間違っていたか設定されていなかったため、SELinux が一部のアクションを拒否する場合があります。SELinux が拒否するアクションを表示するには、root で以下のコマンドを実行します。

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

setroubleshoot-server パッケージがインストールされている場合は、次のコマンドも使用できます。

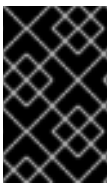
```
# grep "SELinux is preventing" /var/log/messages
```

SELinux が有効で、Audit デーモン (**auditd**) がシステムで実行していない場合は、**dmesg** コマンドの出力で SELinux メッセージを検索します。

```
# dmesg | grep -i -e selinux -e type=1400
```

2.3. SELINUX の無効化

SELinux が無効になっていると、SELinux ポリシーは読み込まれません。SELinux が強制されないと、AVC メッセージがログに記録されません。したがって、「Benefits of SELinux」 に記載されている、SELinux を実行することで得られる利点はすべて失われます。



重要

Red Hat は、SELinux を永続的に無効にする代わりに、Permissive モードを使用することを強く推奨します。Permissive モードに関する詳細は 「Permissive モードへの変更」 を参照してください。

SELinux を永続的に無効にするには、以下の手順に従ってください。

1. **/etc/selinux/config** ファイルに **SELINUX=disabled** を設定します。

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
```

```
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

2. システムを再起動します。再起動したら、**getenforce** コマンドが **Disabled** を返すことを確認します。

```
$ getenforce
Disabled
```

2.4. システムの起動時に SELINUX モードの変更

システムの起動時に、SELinux の実行方法を変更するカーネルパラメーターを設定できます。

enforcing=0

このパラメータを設定すると、マシンを起動する際に、Permissive モードで起動します。これは、問題のトラブルシューティングを行うときに便利です。ファイルシステムの破損がひどい場合は、Permissive モードを使用することが、問題を検出するための唯一の選択肢となるかもしれません。また、Permissive モードでは、ラベルの作成が適切に行われます。このモードで作成した AVC メッセージは、Enforcing モードと同じになるとは限りません。Permissive モードでは、最初の拒否が報告されますが、Enforcing モードでは、ディレクトリーの読み込みが拒否される場合もあり、アプリケーションも停止します。Permissive モードでは、表示される AVC メッセージは同じですが、アプリケーションは、ディレクトリー内のファイルを読み続け、拒否が発生するたびに AVC を取得します。

selinux=0

このパラメーターにより、カーネルは、SELinux インフラストラクチャーのどの部分も読み込まないようになります。init スクリプトは、システムが **selinux=0** パラメーターで起動してるのを認識し、**/.autorelabel** ファイルのタイムスタンプを変更します。これにより、次回 SELinux を有効にしてシステムを起動する際にシステムのラベルが自動的に再設定されます。

重要

Red Hat では、**selinux=0** パラメーターを使用することは推奨されません。システムをデバッグする場合は、Permissive モードを使用することが推奨されます。

autorelabel=1

このパラメーターにより、システムで、以下のコマンドと同様の再ラベルが強制的に行われます。

```
# touch /.autorelabel
# reboot
```

ラベルが間違っているオブジェクトがファイルシステムに大量に含まれる場合は、自動再ラベルプロセスを成功させるために、Permissive モードで起動する必要があります。