SELinux

解释

本主题提供有关安全增强式 Linux 的基本信息。

原因

您想要了解 SELinux，以及如何在 SLE Micro 上配置它。

工作量

阅读时间大约为 40 分钟。

出版日期：2025 年 12 月 11 日

目录

1 关于 SELinux

SELinux 是作为附加的 Linux 安全解决方案开发的，它运用了 Linux 内核中的安全框架。其目的是实现更精细的安全策略，可以超越标准的自由访问控制 (DAC)，即传统的所有者/组/全局和读取/写入/执行文件权限控制。

SELinux 使用附加到对象（例如文件和网络套接字）的标签，并使用它们来做出访问决策。

SELinux 的默认操作是拒绝任何访问。SELinux 仅允许 SELinux 策略中明确允许的操作。另一项提高安全性的 SELinux 功能是，SELinux 允许严格限制进程，以至于进程无法访问同一系统上其他进程的文件。

SELinux 旨在增强而不是取代现有安全解决方案。例如，即使系统使用 SELinux，也仍会应用自由访问控制 (DAC)。如果 DAC 首先拒绝访问，则不会使用 SELinux，因为访问已由另一机制阻止。

2 获取 SELinux

通过 YaST 安装 SLE Micro 时默认会安装 SELinux，有时会将其安装为预构建映像的一部分。

如果您的系统上未安装 SELinux，请运行以下命令：

```
# transactional-update setup-selinux
```

该命令完成后，重引导您的系统。该命令将安装 SELinux 策略（如果尚未安装），设置 `enforcing` SELinux 模式并重构建 `initrd`。

3 SELinux 模式

SELinux 可在以下三种模式之一下运行：`disabled`、`permissive` 或 `enforcing`。

使用 `disabled` 模式意味着不应用 SELinux 策略中的规则，因而您的系统不受保护。因此我们不建议使用 `disabled` 模式。

在 `permissive` 模式下，SELinux 处于活动状态，将加载安全策略、标记文件系统，并记录拒绝访问错误项。但是，不会实施策略，因此实际上并未拒绝访问。

在 enforced 模式下，将应用安全策略。将拒绝未受策略明确允许的每种访问。

有关在 SELinux 模式之间切换的信息，请参见第 3.1 节 “更改 SELinux 模式”。

3.1 更改 SELinux 模式

可以暂时或永久切换 SELinux 模式。

3.1.1 暂时更改 SELinux 模式

要暂时将 SELinux 设置为 permissive 或 enforcing，请使用 **setenforce** 命令。

setenforce 命令的语法如下：

```
# setenforceMODE_ID
```

其中，MODE_ID 为 0（对于 permissive 模式）或 1（对于 enforced 模式）。

请记住，无法使用 **setenforce** 命令禁用 SELinux。

3.1.2 永久更改 SELinux 模式

要对 SELinux 模式执行更改，使其在重引导系统后仍会保留，请编辑 /etc/selinux/config 配置文件。在此文件中，还可以禁用系统上的 SELinux。但不建议执行此操作。如果 SELinux 可能会给您的系统造成问题，请切换到 permissive 模式并调试系统。

在文件 /etc/selinux/config 中，将 SELINUX 的值更改为 disabled、permissive 或 enforced，如下所示：

```
SELINUX=disabled
```

在该文件中所做的更改将在下次重引导后应用。

注意：从 disabled 模式切换后重新标记系统

如果您在系统上禁用 SELinux，然后又重新启用，请务必重新标记您的系统。如果您禁用 SELinux 并对文件系统执行更改，更改将不再反映在环境中（例如，新文件没有任何环境）。因此，需要使用 **restorecon** 命令、使用 `autorelabel` 引导参数或通过创建一个在下次引导时触发重新标记的文件，来重新标记您的系统。要创建该文件，请运行以下命令：

```
# touch /etc/selinux/.autorelabel
```

重引导后，文件 `/etc/selinux/.autorelabel` 将由另一个标志文件 `/etc/selinux/.relabelled` 替换，以防止在后续重引导时进行重新标记。

3.1.3 校验活动的 SELinux 模式

要校验模式，请运行以下命令：

```
# getenforce
```

该命令应返回 `permissive` 或 `enforced`，具体取决于提供的 `MODE_ID`。

3.2 校验 SELinux 是否正常运行

如果您正在执行配置更改，切换到宽松模式可能很有用。在此期间，用户可能会错误地标记文件，从而在切换回强制模式时导致出现问题。

要将系统恢复为受保护状态，请执行以下步骤：

1. 重置安全环境：

   ```
   > sudo restorecon -R /
   ```

2. 通过在 `/etc/selinux/config` 中设置 `SELINUX=enforcing` 切换到强制模式。

3. 重引导系统并再次登录。

4. 运行 **`sestatus -v`** 命令：该命令应返回如下所示的输出：

```
> sudosestatus -v
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:     requested(insecure)
Max kernel policy version:      33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_tty_device_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> \
                                system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
```

5. 如果系统工作不正常，请检查 `/var/log/audit/audit.log` 中的日志文件。
   有关详细信息，请参考 SELinux 查错 (https://documentation.suse.com/smart-supported.html)↗。

4 SELinux 安全环境

安全环境是指派给文件或进程的一系列信息。它由 SELinux 用户、角色、类型、级别和类别组成。此信息用于做出访问控制决策。

SELINUX 环境字段

SELinux 用户

策略中定义的身份，已根据特定的一组角色和特定的**级别**范围为其授权。每个 Linux 用户只会映射到一个 SELinux 用户。但是，一个 SELinux 用户可以拥有多个角色。

SELinux 不使用 Linux 在 `/etc/passwd` 中维护的用户帐户列表，而是使用自身的数据库和映射。按照惯例，身份名称以 `_u` 为后缀，例如：`user_u`。

如果创建了新的 Linux 帐户但未为该帐户指派 SELinux 用户，则会使用默认的 SELinux 用户。默认值通常为 `unconfined_u`。有关更改默认值的过程，请参见第 7.5.2 节 “`semanage login` 命令”。

角色

定义可为用户授予的一组权限。角色定义了指派到此角色的用户可以访问哪些**类型**。按照惯例，角色名称以 `_r` 为后缀，例如：`system_r`。

类型

类型传达了有关特定文件和进程如何交互的信息。进程由具有具体 SELinux 类型的文件组成，它无法访问此类型之外的文件。按照惯例，类型名称以 `_t` 为后缀，例如：`var_t`。

级别

一个可选属性，用于指定多级别安全性中的许可级别范围。

类别

一个可选属性，用于为进程、文件和用户添加类别。然后用户可以访问具有相同类别的文件。

下面是 SELinux 环境的示例：

```
allow user_t bin_t:file {read execute gettattr};
```

此示例规则规定，允许环境类型为 `user_t` 的用户（此用户称为源对象）使用权限 `read`、`execute` 和 `getattr`，来访问环境类型为 `bin_t` 的类**文件**（目标）的对象。

5 SELinux 策略概览

策略是 SELinux 中的关键组件。SELinux 策略定义了规则，这些规则指定哪些对象可以访问系统上的哪些文件、目录、端口和进程。为此，需为所有这些对象定义一个安全环境。

SELinux 策略包含巨量的规则。为使其更易于管理，通常会将策略分割成多个模块。这样，管理员便可为不同的系统组件打开或关闭保护。

为系统编译策略时，您可以选择使用模块化策略或单体式策略，如果选择后者，将使用一个巨型策略来保护系统上的一切组件。我们强烈建议使用模块化策略而不是单体式策略。模块化策略要容易管理得多。

SLE Micro 随附了 `targeted` SELinux 策略。

5.1 使用 SELinux 模块

作为管理员，您可以开启或关闭模块。如果您只想禁用 SELinux 策略的某个部分，并且不希望在关闭 SELinux 保护的情况下运行特定的服务，则此功能可能很有用。

要查看正在使用的所有 SELinux 策略模块，请运行以下命令：

```
semodule -l
```

获取要关闭的模块名称后，运行以下命令：

```
> sudo semodule -d MODULENAME
```

要打开策略模块，请运行以下命令：

```
> sudo semodule -e MODULENAME
```

5.2 为容器创建策略

SLE Micro 附带的某个策略在默认情况下不允许容器访问容器数据之外的文件。另一方面，它允许进行各种网络访问。通常，容器是使用绑定挂载点创建的，应该能够访问 `/home` 或 `/var` 等其他目录。您可能希望能够允许访问这些目录，或者相反，您希望即使系统上使用了 SELinux，也仅限容器访问某些端口。在这种情况下，需要创建新的策略规则来启用或禁用访问。SLE Micro 为此提供了 Udica 工具。

以下过程说明如何为容器创建自定义策略：

1. 确保 SELinux 处于强制模式。有关细节，请参见第 3.1 节 “更改 SELinux 模式”。
2. 使用以下参数启动容器：

   ```
   # podman run -v /home:/home:rw -v /var/:/var/:rw -p 21:21 -it sle15 bash
   ```

   容器使用默认策略运行，该策略不允许访问挂载点，但不限制其他端口。
3. 您可以退出容器。
4. 获取容器 ID：

   ```
   # podman ps -a

   CONTAINER ID  IMAGE
                         COMMAND     CREATED        STATUS            PORTS
              NAMES
   e59f9d0f86f2  registry.opensuse.org/devel/bci/tumbleweed/containerfile/
   opensuse/bci/ruby:latest  /bin/bash   8 minutes ago  Up 8 seconds ago
    0.0.0.0:21->21/tcp  zen_ramanujan
   ```
5. 创建一个 JSON 文件，供 Udica 用来为容器创建自定义策略：

   ```
   # podman inspect e59f9d0f86f2 >OUTPUT_JSON_FILE
   ```

   例如，将 OUTPUT_JSON_FILE 替换为 container.json。
6. 运行 Udica 以根据容器参数生成策略：

   ```
   # udica -jOUTPUT_JSON_FILECUSTOM_CONTAINER_POLICY
   ```

   例如：

   ```
   # udica -j container.json custom_policy
   ```
7. 根据提供的说明，运行以下命令来加载策略模块：

   ```
   # semodule -i custom_policy.cil /usr/share/udica/templates/
   {base_container.cil,net_container.cil,home_container.cil}
   ```

8. 使用 `--security-opt` 选项通过新策略模块运行容器，如下所示：

```
# podman run --security-opt label=type:custom_policy.process -v /home:/
home:rw -v /var/:/var/:rw -p 21:21 -it sle15 bash
```

6 SELinux 布尔值

SELinux 布尔值支持灵活的策略管理方法。例如，使用布尔值可以在一台服务器上禁用特定策略，同时使该策略在另一台服务器上保持活动状态。换句话说，可将布尔值理解为策略规则的开关。您无需更改特定的策略，而可以将其关闭。在策略代码中，布尔值称为**可调参数**。由于布尔值包含在策略中，因此在加载策略后即可供使用。

对布尔值所做的更改可以是永久性的，也可以是暂时性的（保留到会话结束为止）。

使用 SELinux 提供的工具可以列出和查看细节，或更改布尔值的状态。有关细节，请参见以下几节。

6.1 使用布尔值

6.1.1 列出布尔值

可以使用 **`getsebool`** 或 **`semanage`** 命令列出当前定义的布尔值。要列出当前定义的所有布尔值及其状态，请运行以下命令：

```
# getsebool -a

abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
...
```

要获取有关特定布尔值的更多细节，可如下所示使用 **`semanage`** 命令：

```
# semanage boolean -l
```

```
SELinux boolean                State   Default     Description

abrt_anon_write                (off   ,  off)       Allow abrt to anon write
abrt_handle_event              (off   ,  off)       Allow abrt to handle event
abrt_upload_watch_anon_write   (on    ,   on)       Allow abrt to upload watch
 anon write
```

要获取单个布尔值的状态，可使用以下命令：

```
# getseboolBOOLEAN_NAME
```

或者，可以对 **semanage boolean** 输出使用 **grep** 命令：

```
# semanage boolean -l | grepBOOLEAN_NAME
```

6.1.2 切换布尔值

setsebool 和 **semanage** 命令可用于切换布尔值。可以永久或暂时（保留到会话结束为止）更改布尔状态。要暂时更改布尔值，请运行以下命令：

```
# setseboolBOOLEAN_NAMEBOOLEAN_VALUE
```

其中 BOOLEAN_VALUE 为 on 或 off。

要永久更改布尔值，请运行以下两个命令之一：

```
# setsebool -PBOOLEAN_NAMEBOOLEAN_VALUE
```

或者，使用 **semanage** 命令：

```
# semanage boolean -m --BOOLEAN_VALUEBOOLEAN_NAME
```

其中 BOOLEAN_VALUE 为 on 或 off。

一个布尔值可以启用或禁用多个策略规则。要查看哪些布尔值启用或禁用了哪些策略规则，请使用 **sedispol** 工具，它可以分析策略文件：

```
# sedispol /etc/selinux/targeted/policy/policy.32
```

由于策略规则通常很大，我们建议通过选择 f 并指定文件名来设置输出文件。指定文件名后，按 6。然后您可以检查该文件。

7 用于管理 SELinux 的工具

SLE Micro 提供了用于管理系统上的 SELinux 的工具。如果您的系统上未安装下述工具，请运行以下命令安装这些工具：

```
# transactional-update pkg install policycoreutils-python-utils
```

安装成功后，重引导系统。

7.1 使用 Z 选项

安装并配置 SELinux 后，可将 `-Z` 用于 **`ls`**、**`id`** 或 **`ps`** 等普通命令。使用此选项可以显示文件或进程的安全环境。例如，使用 **`ls`** 命令：

```
> ls -Z /etc/shadow

        system_u:object_r:shadow_t:s0 /etc/shadow
```

7.2 chcon 命令

命令名称 **`chcon`** 代表更改环境。该命令可将文件的整个安全环境更改为 CLI 中提供的值，或者可以更改环境的某些部分。或者，您可以提供某个文件作为参考。

要更改文件的整个安全环境，命令语法如下：

```
# chconSECURITY_CONTEXTFILENAME
```

其中：

- `SECURITY_CONTEXT` 的格式为：`SELinux_USER:ROLE:TYPE:LEVEL:CATEGORY`。例如，环境可能是：**system_u:object_r:httpd_config_t:s0**。
- `FILENAME` 是要更改其环境的文件的路径。

要根据作为参考提供的文件设置安全环境，请如下所示运行 **`chcon`**：

```
# chcon --reference=REFERENCE_FILEFILENAME
```

其中：

- REFERENCE_FILE 是要用作参考的文件的路径。
- FILENAME 是要更改其环境的文件的路径。

或者，可以仅更改安全环境的某个部分。**chcon** 命令的一般语法如下：

```
# chconCONTEXT_OPTIONCONTEXT_PARTFILENAME
```

选项和参数的含义如下：

- 根据环境部分，CONTEXT_OPTION 可为下列其中一项：

  -u，表示 --user

  表示根据提供的文件更改 SELinux 用户环境：

  ```
  # chcon -u system_u logind.conf
  ```

  -r，表示 --role

  仅更改所提供文件的环境中的角色部分：

  ```
  # chcon -r object_r logind.conf
  ```

  -t，表示 --type

  仅更改所提供文件的环境中的类型部分：

  ```
  # chcon -t etc_t logind.conf
  ```

  -l，表示 --range

  仅更改安全环境的范围部分：

  ```
  # chcon -l s0 logind.conf
  ```

- CONTEXT_PART 是要设置的安全环境的特定值。
- FILENAME 是要更改其环境的文件的路径。

注意：对符号链接使用 chcon

默认情况下，当您更改符号链接的安全环境时，链接目标的环境将会更改，而符号链接环境则**不会**更改。要强制 **chcon** 更改符号链接而不是链接目标的环境，请如下所示使用 `--no-dereference` 选项：

```
# chcon --no-dereference -u system_u -t etc_t network.conf
```

可以使用 recursive 选项更改目录中所有文件的环境：

```
# chcon --recursive  system_u:object_r:httpd_config_t:s0 conf.d
```

7.3 getenforce 和 setenforce 命令

getenforce 命令返回当前的 SELinux 模式：`Enforcing`、`Permissive` 或 `Disabled`。

```
# getenforce

Permissive
```

setenforce 命令暂时将 SELinux 模式更改为强制或宽松。无法使用此命令禁用 SELinux。请记住，更改只能保留到下次重引导为止。要永久更改状态，请按照第 3.1 节 “更改 SELinux 模式”中的说明操作。

```
# setenforceMODE_ID
```

其中，`MODE_ID` 为 `0`（对于 `permissive` 模式）或 `1`（对于 `enforced` 模式）。

7.4 fixfiles 脚本

使用该脚本可对安全环境执行以下任务：

- 检查环境是否正确
- 更改任何错误的文件环境标签
- 在添加新策略后重新标记您的系统

该脚本的语法如下：

```
# fixfiles [OPTIONS] ARGUMENT
```

其中：

- OPTIONS 可为下列其中一项：

  `-l LOGFILE`
  : 将输出保存到提供的文件

  `-o OUTPUT_FILE`
  : 将文件环境与默认环境不同的所有文件的名称保存到提供的输出文件

  `-F`
  : 强制重置环境。

- ARGUMENT 可为下列其中一项：

  check
  : 显示错误标签的先前和当前文件环境，但不执行任何更改

  relabel
  : 根据当前加载的策略重新标记错误的文件环境

  restore
  : 将错误的文件环境恢复为默认值

  verify
  : 列出具有错误文件环境标签的所有文件，但不执行任何更改

7.5 semanage 命令

semanage 命令可用于配置策略的各个部分，而无需从源开始重新编译策略。使用该命令可执行以下任务：

- 使用 boolean 参数管理布尔值。有关布尔值的细节，请参见第 6.1 节 “使用布尔值”。
- 使用 fcontext 参数调整文件的环境

- 使用 `login` 参数管理用户映射
- 使用 `user` 参数管理 SELinux 用户
- 使用 `module` 参数管理 SELinux 策略模块

一般命令语法如下：

```
# semanageARGUMENTOPTIONS [OBJECT_NAME]
```

其中：

- `ARGUMENT` 为下列其中一项：**`login`**、**`user`**、**`fcontext`**、**`boolean`**、**`module`**。
- `OPTIONS` 取决于提供的 `ARGUMENT`。通用选项中介绍了通用选项。
- 根据提供的 `ARGUMENT`，`OBJECT_NAME` 可为登录名、模块名、文件名或 SELinux 用户。

通用选项

`-a`、`--add`
: 添加提供的对象

`-h`、`--help`
: 列显命令帮助

--extract
: 显示用于更改系统（布尔值、文件环境等）的命令。

`-l`、`--list`
: 列出所有对象。

`-m`、`--modify`
: 修改提供的对象

`-n`、`--noheading`
: 通过省略标题来修改列出操作的输出。

`-s`、`--seuser`
: 指定 SELinux 用户。

其他选项与特定的 **semanage** 命令相关，已在相应章节中予以介绍。

7.5.1 semanage fcontext 命令

使用 **semanage fcontext** 命令可执行以下任务：

- 查询文件环境定义
- 添加文件的环境
- 添加您自己的规则

使用 **semanage fcontext** 命令对文件环境执行更改后不需要修改或重新编译策略。

除了通用选项中所述的通用选项外，**semanage fcontext** 命令还接受以下选项：

`-e`、`--equal`

该选项可让您使用提供的路径环境来标记其他目录（提供的目标路径）中的文件。例如，您希望将 `/home` 具有的同一环境指派给另一个主目录 `/export/home`。如果使用此选项，则需要提供源路径和目标路径：

```
# semanage fcontext -a -e /home /export/home
```

`-f`、`--ftype`

指定文件类型。使用以下值之一：

- `a` - 所有文件，这也是默认值
- `b` - 块设备
- `c` - 字符设备
- `d` - 目录
- `f` - 常规文件
- `l` - 符号链接
- `p` - 命名管道
- `s` - 套接字

7.5.2 `semanage login` 命令

使用 **`semanage login`** 可执行以下任务：

- 将 Linux 用户映射到特定的 SELinux 用户。例如，要将 Linux 用户 **tux** 映射到 `sysadm_u`，请运行以下命令：

  ```
  # semanage login -a -s sysadm_u tux
  ```

- 将一组 Linux 用户映射到特定的 SELinux 用户。例如，要将 **writers** 组的用户映射到 `user_u`，请运行以下命令

  ```
  # semanage login -a -s user_u %writers
  ```

  然后，该组将列在 **`semanage login -l`** 的输出中（以 % 字符为前缀）。
  请记住，用户组应该是主组，因为将 SELinux 用户映射到补充组可能会导致不兼容的映射。

  ```
  # semanage login -m -s staff_u %writers
  ```

- 在特定 SELinux MLS/MCS 安全范围内映射 Linux 用户。
- 修改已创建的映射。为此，只需将前面命令中的 `-a` 选项替换为 `-m` 即可。
- 为新的 Linux 用户设置默认的 SELinux 用户。默认的 SELinux 用户通常是 `unconfined_u`。要将值更改为 `staff_u`，请运行以下命令：

  ```
  # semanage login -m -s staff_u __default__
  ```

7.5.3 `semanage boolean` 命令

`semanage boolean` 命令用于控制 SELinux 策略中的布尔值。

命令摘要如下：

```
semanage boolean [-h] [-n]  [ --extract |
       --deleteall | --list [-C] | --modify ( --on | --off | -1 | -0 ) boolean ]
```

除了通用选项之外，还可使用以下特定于 **`semanage boolean`** 命令的选项：

--list -C
: 显示在本地对布尔值所做修改的列表。

-m --on |-1
: 打开提供的布尔值。

-m --off | -0
: 关闭提供的布尔值。

-D、--deleteall
: 删除在本地对布尔值所做的修改。

该命令的最常见用途是打开或关闭特定的布尔值。例如，要打开 `authlogin_yubikey` 布尔值，请运行：

```
# semanage boolean -m on authlogin_yubikey
```

7.5.4 `semanage user` 命令

`semanage user` 命令控制 SELinux 用户、角色和 MLS/MCS 级别之间的映射。

除了通用选项中所述的通用选项外，**`semanage use`** 命令还接受以下选项：

-R [ROLES]、--roles [ROLES]
: SELinux 角色列表。可将多个角色括在双引号中并用空格分隔，或者可以多次使用 `-R`。

使用此命令可执行以下任务：

- 运行以下命令列出 SELinux 用户与角色的映射：

  ```
  # semanage user -l
  ```

- 更改指派给 `user_u` SELinux 用户的角色：

  ```
  # semanage user -m -R "system_r unconfined_r user_r"
  ```

- 为 `admin_u` 指派角色 `staff_r` 和类别 `s0`：

```
# semanage user -a -R "staff_r -r s0 admin_u
```

- 例如，创建角色为 `staff_r` 的新 SELinux 用户 `admin_u`。您还需要使用 `-P` 为此用户定义标记前缀：

```
# semanage user -a -R "staff_r" -P admin admin_u
```

7.5.5 `semanage module` 命令

`semanage module` 命令可以安装、去除、禁用或启用 SELinux 策略模块。

除了通用选项中所述的通用选项外，**`semanage fcontext`** 命令还接受以下选项：

`-d`、`--disable`

要禁用提供的 SELinux 策略模块，请运行以下命令：

```
# semanage module --disable MODULE_NAME
```

`-e`、`--enable`

要启用提供的 SELinux 策略模块，请运行以下命令：

```
# semanage module --enable MODULE_NAME
```

7.6 `sestatus` 命令

`sestatus` 获取运行 SELinux 的系统的状态。

该命令的一般语法如下所示：

```
sestatus [OPTION]
```

如果不结合任何选项和参数运行该命令，它将输出以下信息：

```
# 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:      requested (insecure)
Max kernel policy version:       33
```

该命令接受以下选项：

-b

显示系统上布尔值的状态

-v

显示 `/etc/sestatus.conf` 文件中列出的文件和进程的安全环境。

8 法律声明

A GNU 自由文档许可证

0. 导言

此许可证的目的是赋予手册、教科书或其他功能性的和有用的文档以“自由”：即保证每个人都有复制和再分发此类文档的有效自由，无论是否进行修改，也无论将其用于商业或非商业用途。其次，此许可证为作者和出版者保留了因工作获得声誉但不视为对他人所做修改负责的方式。

本许可证是一种“非盈利版权”，这意味着从该文档衍生的作品也必须是以同一方式自由的。它补充了 GNU 通用公共许可证（为自由软件设计的非盈利版权许可证）。

我们设计此许可证旨在将其用于免费软件的手册，因为免费软件需要自由文档：免费程序所附手册应具有与软件本身同样的自由。但是此许可证不限于软件手册；它可以用于任何文本作品，无论主题如何或它是否作为印刷书籍出版。建议本许可证主要用于目的是指导或参考的作品。

1. 适用性和定义

此许可证适用的对象：由版权所有者在其中明确声明可按照此许可证条款以任何媒体分发的任何手册和其他作品。此类声明授予在此处所述的条款和条件下使用该作品的全球无限期无版权许可证。下述“文档”指任何此类手册或作品。任何公众成员都是一个被许可人，以下称为“您”。如果您以需要版权法许可的任何方式复制、修改或分发该作品，则表示您接受该许可证。

该文档的“修改版本”表示包含该文档或其一部分（或者逐字复制或者有修改和/或翻译为另一语言）的任何作品。

“次要章节”是该文档的命名附录或扉页章节，专门讲述该文档的出版者或作者与该文档整个主题（或相关问题）的关系，不包含与整个主题相关的内容。（因此，如果该文档是数学课本的一部分，则辅助部分可能不说明任何数学问题。）这种关系可以是与主题或相关问题的历史联系，或与它们相关的法律、商业、哲学、伦理或政治地位。

在该文档基于此许可证项发布的声明中，“固定章节”是将其标题指定为固定章节标题的一些辅助章节。如果一个章节不适用上述辅助章节的定义，则不允许将其指定为固定章节。该文档可能不包含固定章节。如果该文档不标识任何固定章节，则表示没有固定章节。

在该文档基于此许可证项发布的声明中，“封页文本”是作为封面文本或封底文本列出的简短文本段落。封面文本最多 5 个单词，封底文本最多 25 个单词。

文档的“透明”副本是一个机器可读的副本，使用公众可以得到其规范的格式表达，这样的副本适合于使用通用文本编辑器、（对于像素构成的图像）通用绘图程序、（对于绘制的图形）广泛使用的绘画编辑器直接修改文档，也适用于输入到文本格式处理程序或自动翻译成各种适于适用于输入到文本格式处理程序的格式。一个用其他透明文件格式表示的副本，如果该格式的标记（或缺少标记）已经构成了对读者的后续修改的障碍，那么就是不透明的。表示实质性数量的文本的图像格式都是不透明的。不“透明”的副本称为“不透明”。

适于作为透明副本的格式的示例有：没有标记的纯 ASCII 文本、Texinfo 输入格式、LaTeX 输入格式、使用公共可用 DTD 的 SGML 或 XML，符合标准的简单 HTML、可以人为修改的 PostScript 或 PDF。透明图像格式的示例有 PNG、XCF 和 JPG。不透明的格式包括：仅可以被私有版权的字处理软件使用的私有版权格式、所用的 DTD 和/或处理工具不是广泛可用的的 SGML 或 XML、机器生成的 HTML、一些字处理器生成的只用于输出目的的 PostScript 或 PDF。

对于印刷书籍，“扉页”就是扉页本身以及随后的一些用于补充的页，显然本许可资料需要出现在扉页上。对于那些没有扉页的作品形式，“扉页”代表接近作品最突出标题的、在文本正文之前的文本。

“命名为 XYZ”的章节表示文档的一个特定的子单元，其标题就是 XYZ 或在括号中包含 XYZ 且后跟 XYZ 的其他语言翻译文本。（这里 XYZ 代表下面提及的特定章节名称，比如“致谢”、“题献”、“签名”或“历史”。）要在修改文档时对这类章节“保留标题”就是依据此定义保持这样一个“命名为 XYZ”的章节。

文档可能在文档遵照此许可证的声明后面包含免责声明。这些免责声明应作为参考信息包含在此许可证中，但是只能将其视作免责声明：这些免责声明暗指的任何其他含义均无效，且对此许可证的含义不产生任何影响。

2. 逐字复制

您可以用任何媒体复制并分发文档，无论是出于商业还是非商业目的，只要保证此许可证、版权声明和声称此许可证应用于文档的声明都完整地、无任何附加条件地存在于所有副本中。不能使用任何技术手段阻碍或控制您制作或发布的副本的阅读或再次复制。不过您可以在副本交易中得到报酬。如果发布足够多的副本，则您必须遵循下面第三节中的条件。

您也可以在如上的条件下出租副本和向公众放映副本。

3. 大量复制

如果您出版的文档印刷版副本（或是有印制封页的其他媒体副本）多于 100 份，而文档的许可证声明中要求有封页文本，则您必须将它清晰地置于封页之上，封面文本在封面上，封底文本在封底上。封面和封底上还必须标明您是这些副本的出版者。封面必须同等显著地完整展现标题的所有文字。您可以在封页上加入其他资料。改动仅限于封页的复制，只要保持文档的标题不变并满足这些条件，可以在其他方面被视为逐字复制。

如果需要加上的文本对于封面或封底过多，无法明显地表示，您应该在封页上列出前面的（在合理的前提下尽量多），把其他的放在邻近的页面上。

如果您出版或分发了超过 100 份文档的不透明副本，则必须在每个不透明副本中包含一份计算机可读的透明副本，或是在每个不透明副本中给出一个计算机网络地址，通过这个地址，网络公共用户可以使用标准网络协议下载文档的无任何附加资料的完整透明副本。如果您选择后者，则必须在开始大量分发非透明副本的时候采用相当谨慎的步骤，保证透明副本在其所给出的位置在（直接或通过代理和零售商）分发最后一次该版本的非透明副本的时间之后一年之内始终是有效的。

在重新大量发布副本之前，请您（但不是必须）与文档的作者联系，以便他们可以有机会向您提供文档的更新版本。

4. 修改

在上述第 2、3 节的条件下，您可以复制和分发文档的修改版本，前提是严格按照此许可证发布修改后的文档，将修改版本用作文档，从而允许任何拥有此修改版副本的人执行分发或修改。另外，在修改版中，您需要做到如下几点：

A. 用于与文档以及以前各个版本（如果有，应该列在文档的“历史”章节中）显著不同的扉页（和封页，如果有）。如果那个版本的原始发行者允许的话，您可以使用和以前版本相同的标题。

B. 与作者一样，在扉页上列出承担修改版本中的修改的作者责任的一个或多个人或实体和至少五个文档的原作者（如果原作者不足五个就全部列出），除非他们免除了您的这个责任。

C. 与原来的发行者一样，在扉页上列出修改版的发行者的姓名。

D. 保持该文档的全部版权声明不变。

E. 在与其他版权声明邻近的位置加入恰当的针对您的修改的版权声明。

F. 在紧接着版权声明的位置加入许可声明，按照下面附录中给出的形式，以本许可证给公众授于是用修订版本的权利。

G. 保持原文档的许可声明中的全部不可变章节、封面文字和封底文字的声明不变。

H. 包含一份未作任何修改的本协议的副本。

I. 保持命名为“历史”的章节不变，保持它的标题不变，并在其中加入一项，至少声明扉页上的已修改版本的标题、年份、新作者和出版者。如果文档中没有命名为“历史”章节，则请新建它，并加入一项以声明原文档扉页上所列的标题、年份、作者与出版者，再在其后加入如上所说的描述修改版本的项。

J. 如果文档中有用于公共用户访问的文档透明副本的网址，则保持网址不变，并同样提供它所基于的以前文档版本的网址。这些网址可以放在“历史”章节。您可以不给出那些在原文档发行之前已经发行至少四年的版本给出的网址，或者该版本的发行者授权不列出网址。

K. 对于任何命名为“致谢”或“题献”的章节，保持其标题不变，并保持其全部内容以及对每位贡献者致谢和/或题献的语气不变。

L. 保持文档的所有固定章节不变，不改变它们的标题和内容。章节的编号或相当的内容不被认为是章节标题的一部分。

M. 删除命名为“签名”的章节。这样的章节不可以被包含在修改后的版本中。

N. 不要把任何现有章节重命名为“签名”或与任何不可变章节相冲突的标题。

O. 保持任何免责声明不变。

如果修改版本加入了新的符合次要章节定义的引言或附录章节，并且不含有从原文档中复制的内容，您可以选择将其标记为固定。如果需要这样做，则将它们的标题加入修改版本许可声明的不可变章节列表之中。这些标题必须和其他章节的标题相区分。

您可以加入一个命名为“签名”的章节，只要它只包含对您的修改版本由不同的各方给出的签名，例如书评或是声明文本已经被一个组织认定为一个标准的权威定义。

您可以加入一个最多 5 个字的段落作为封面文本和一个最多 25 个字的段落作为封底文本，将它们加入修改版本的封页文本列表末端。一个实体只可以添加（或编排）一段封面和一段封底文本。如果原文档已经为该封页（封面或封底）包含了封页文本，由您或您所代表的实体先前加入或排列的文本，不能再新加入一个，但您可以在原来的发行者的明确许可下替换掉原来的那个。

作者和发行者不能通过本许可证授权公众使用他们的名字推荐或暗示认可任何一个修改版本。

5. 组合文档

遵照第 4 节所说的修改版本的规定，您以将文档和其他文档合并并以本许可证发布，只要您在合并结果中包含原文档的所有不可变章节，对它们不加以任何改动，并在合并结果的许可声明中将它们全部列为不可变章节，而且维持原作者的免责声明不变。

合并作品仅需要包含一份此许可证，多个相同的固定章节可以由一个副本取代。如果有多个名称相同但内容不同的固定章节，通过在章节名称后面的括号中加上原作者或出版者的姓名（如果已知）来加以区别，或者使用唯一编号加以区别。并对合并作品许可声明中的固定章节列表中的章节标题做相同的调整。

在合并过程中，必须合并不同原始文档中任何命名为“历史”的章节，从而形成新的命名为“历史”的章节；类似地，还要合并命名为“致谢”和“题献”的章节。必须删除所有命名为“签名”的章节。

6. 文档的合集

您可以制作一个文档和其他文档的合集，在本许可证下发布，并在合集中将不同文档中的多个本许可证的副本以一个单独的副本来代替，只要您在文档的其他方面遵循本许可证的逐字复制的条款即可。

您可以从一个这样的合集中提取一个单独的文档，并将它在本许可证下单独发布，只要您想这个提取出的文档中加入一份本许可证的副本，并在文档的其他方面遵循本许可证的逐字复制的原则。

7. 独立作品的聚合体

将文档或其派生品以及其他独立和无关文档或作品编撰在一个储存卷中或分发媒体上，这称为文档的“聚合体”，前提是编撰成品的著作权对其使用者的法律权限的限制未超出各个独立作品的许可范围。当基于此许可证发布的文档包含在一个聚合体中时，此许可证不适用于聚合体中的本非该文档派生作品的其他作品。

如果第 3 节中的封页文本要求适用于这些文档的副本，则若文档在聚合体中所占的比重小于全作品的一半，文档的封页文本可以放置在聚合体内包含文档部分的封页上，或是电子文档中的等效部分。否则，它必须位于整个聚合体的印刷的封页上。

8. 翻译

翻译被视为一种修改，因此您可以根据第 4 节的条款分发文档的翻译。将固定章节替换为翻译内容需要经得其版权所有者的特别许可，但除了这些固定章节的原始版本之外，您还可以包含一部分或所有固定章节的翻译。您可以包含一个此许可证以及所有许可证声明和免责声明的翻译版本，前提是同时包含它们的原始英文版本。当翻译版本和英文版发生冲突的时候，原始版本有效。

如果在文档中有命名为“致谢”、“题献”或“历史”的章节，保持标题（第 1 节）的要求（第 4 节）恰恰需要更换实际的标题。

9. 终止

除非此许可证中有明确规定，否则您不能对该文档进行复制、修改、分授许可或分发。在此许可证规定外对该文档所进行的任何复制、修改、分授许可或分发都是无效的，并且将自动终止您在此许可证下所拥有的权利。但是，对于在此许可证的规定下从您这里获得副本或权利的各方，只要其完全遵守此许可证的规定，其许可证将不会被终止。

10. 本许可的未来修订版本

自由软件基金会有时会发布 GNU 自由文档许可证的新的修订版版本。这些新版本的主旨和精神与当前版本是一致的，但在解决新问题的具体细节方面可能有所不同。请参见 https://www.gnu.org/copyleft/。

许可证的每个版本都有一个不同的版本号。如果文档指定了适用于它的此许可证“或任何后续版本”的特定带编号版本，则您可以选择遵从指定版本或自由软件基金会发布的任何随后版本（非草稿）的条款和条件。如果文档没有指定此许可证的版本号，您可以选择自由软件基金会发布的任何许可证版本（非草稿）。

附录：如何针对您的文档使用此许可证

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

如果您有固定章节、封面文本和封底文本，请将“with...Texts”部分替换为：

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

如果有不可变章节而没有封页文本，或这三种内容（不可变章节、封面文本、封底文本）的任何其他组合，请合并这两个备选项以适应您的情况。

如果您的文档包含不一般的程序代码示例，建议同时选择自由软件许可证（如 GNU 通用公共许可证）发布这些示例，以允许它们可以用于自由软件。