openEuler内核编程技术

实训指导书

第十章 第3讲

《内核安全模块之SELinux》

软件所制

**术语表**

|  |  |  |  |
| --- | --- | --- | --- |
| 英文 | 中文 | 含义 | 别名 |
|  |  |  |  |
|  |  |  |  |

第十章 第4讲 内核安全模块之SELinux

# 1 任务1：启用SELinux内核安全模块 (30min)

## 相关知识

**一、SELinux简介**

SELinux（Security Enhanced Linux）是由美国国家安全局（National Security Agency，NSA）贡献的一个Linux内核模块，主要用于Redhat及其衍生版本中，为整个系统提供更加健壮的安全服务。之所以开发这个模块，是因为NSA发现在系统的安全问题中，绝大多数问题并不是由于外部的攻击多么强大，更多的问题是由于所谓的内部员工的资源误用。

例如，在Apache中，默认的服务目录是/var/www/html，如果一个无经验的系统运维人员（糊涂蛋）在运维过程中，将其权限设置为777，那么所有的进程都可以在该目录中进行读写，这将造成极大的安全隐患。

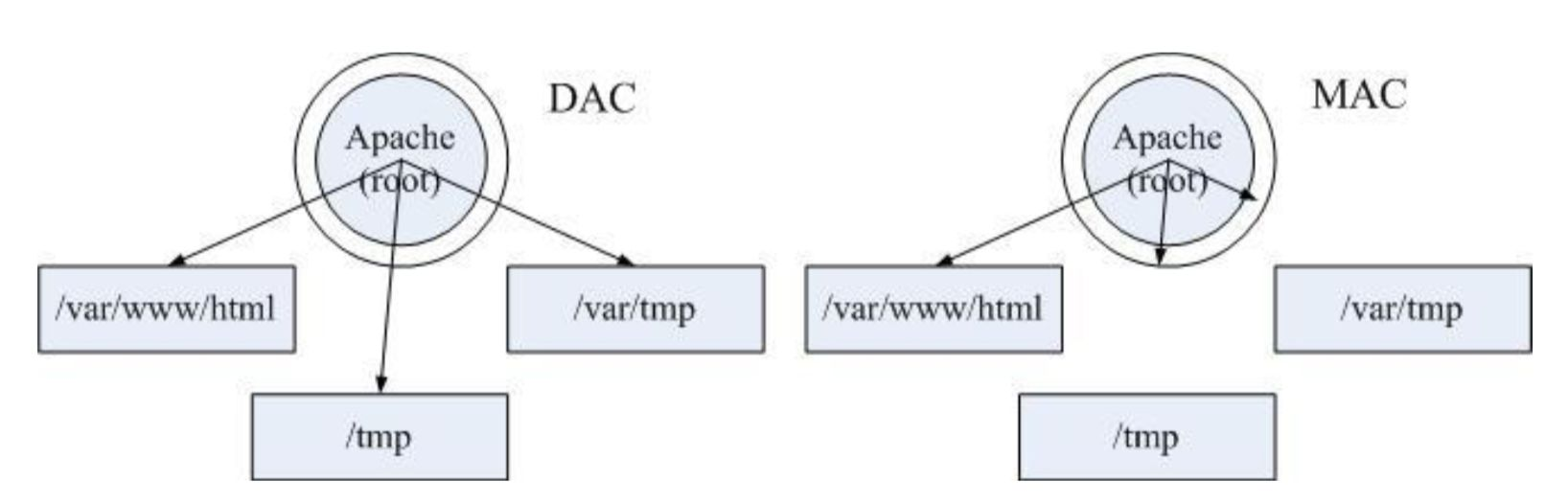
**1. MAC与DAC**

自主访问控制（Discretionary Access Control，DAC）：所谓DAC主要是指在没有启用SELinux的Linux系统中，系统会依据资源的rwx权限以及用户身份（进程所有者）来判断是否具有资源访问的权限。使用DAC的缺点在于：

* root具有最高权限：对于root用户而言，其具有系统最高的权限，因此各种rwx设置对于root用户而言形同虚设。
* 用户可以获取进程修改文件资源的访问权限：如果将某个资源的权限设置为777，那么该目录可以被任何用户读写操作

在使用了 SELinux 的操作系统中，决定一个资源是否能被访问的因素除了上述因素之外，还需要判断每一类进程是否拥有对某一类资源的访问权限。 这样一来，即使进程是以 root 身份运行的，也需要判断这个进程的类型以及允许访问的资源类型才能决定是否允许访问某个资源。进程的活动空间也可以被压缩到最小。 即使是以 root 身份运行的服务进程，一般也只能访问到它所需要的资源。即使程序出了漏洞，影响范围也只有在其允许访问的资源范围内。安全性大大增加。 这种权限管理机制的主体是进程，也称为强制访问控制（MAC）。 而 MAC 又细分为了两种方式，一种叫类别安全（MCS）模式，另一种叫多级安全（MLS）模式。简单而言，在DAC中控制的主体（subject）是用户，而MAC中控制的对象是进程。

这里引用一张图片来说明。



可以看到，在 DAC 模式下，只要相应目录有相应用户的权限，就可以被访问。而在 MAC 模式下，还要受进程允许访问目录范围的限制。

**2. SELinux的模式**

SELinux有三种模式：

* Enforceing：强制模式，SELinux启用
* Permissive：宽容模式，SELinux的安全策略不强制执行，但是会有相应的警告信息记录到日志文件中，一般用于SELinux的调试
* Disabled：关闭模式

要查看SELinux的运行状态，需要使用如下命令：

|  |
| --- |
| getenforce |

或者

|  |
| --- |
| sestatus |

使用sestatus命令除了可以查看当前SELinux的运行模式外，还能看到很多额外的信息。

修改SELinux的运行模式，主要有两种方法，一种是用命令行，另外一种是直接修改SELinux的配置文件。

命令行的方式只能为Enforce和Permissive的相互切换，不能进行关闭，其命令格式为：

|  |
| --- |
| setenforce [0|1] |

其中1为enforcing模式，0为permissive模式

要想关闭或者开启SELinux，只能修改SELinux的配置文件，其位置为/etc/selinux/config

打开该文件后，可以看到其中只有两行信息：

|  |
| --- |
| SELINUX=enforcing  SELINUXTYPE=targeted |

我们只要将SELINUX行设置为对应模式即可，需要注意的是如果从enforcing或permissive模式切换为disabled模式，或者反过来，则需要重启系统（从disabled模式修改为其他两种模式时，需要重启两次，因为要重新写入上下文信息）才能生效。在disabled模式下，无法使用setenforce命令。

**3. SELinux的策略**

系统中通常有大量的文件和进程，为了节省时间和开销，通常我们只是选择性地对某些进程进行管制。而哪些进程需要管制、要怎么管制是由政策决定的。一套政策里面有多个规则。部分规则可以按照需求启用或禁用（以下把该类型的规则称为布尔型规则）。规则是模块化、可扩展的。在安装新的应用程序时，应用程序可通过添加新的模块来添加规则。用户也可以手动地增减规则。

在openeuler系统中，有三套政策，分别是：

1. targeted：对大部分网络服务进程进行管制。这是系统默认使用的政策（下文均使用此政策）。
2. minimum：以 targeted 为基础，仅对选定的网络服务进程进行管制。一般不用。
3. mls：多级安全保护。对所有的进程进行管制。这是最严格的政策，配置难度非常大。一般不用，除非对安全性有极高的要求。

政策可以在/etc/selinux/config中设定。

**4. SELinux的安全上下文**

安全上下文是 SELinux 的核心。安全上下文可以分为「进程安全上下文」和「文件安全上下文」。一个「进程安全上下文」一般对应多个「文件安全上下文」，只有两者的安全上下文对应上了，进程才能访问文件。它们的对应关系由政策中的规则决定。文件安全上下文由文件创建的位置和创建文件的进程所决定。而且系统有一套默认值，用户也可以对默认值进行设定。需要注意的是，单纯的移动文件操作并不会改变文件的安全上下文。

安全上下文有四个字段，分别用冒号隔开。形如：system\_u:object\_r:admin\_home\_t:s0，含义如下：

* user：用户

相当于账户方面的身份识别，常见有几下几种类型

* + unconfined\_u：不受限的用户，该文件来自不受限的进程所产生的，一般来说，可以使用可登录账号来取得 bash，预设的 bash 环境是不受 SELinux 管制的，因为 bash 并不是什么特别的网络服务，因此在该 bash 进程所产生的文件，其身份识别大多就是该类型了。
  + system\_u：系统用户，基本上，如果是系统会软件本身所提供的文件，大多就是该类型，如果是用户通过 bash 自己建立的文件，大多则是不受限的 unconfined\_u 身份，如果是网络服务所产生的文件，或则是系统服务运行过程中所产生的文件，则大部分是 system\_u
* role：角色

通过该字段，可以知道这个资料是属于进程、文件资源还是代表使用者，一般的角色有：

* + object\_r：代表的是文件或目录等文件资源
  + system\_r：代表的是进程，不过一般使用者也会被指定为 system\_r
* type：类型，最重要

在预设的 targeted 政策中， identify 与 role 字段基本上是不重要的，而 type 是最重要的，基本上，一个主体进程能不能读取到这个文件资源，与类型字段有关，而类型字段在文件与进程的定义不相同：

* + type：在文件资源（object）上面称为类型（type）
  + domain：在主体进程（subject）则称为领域（domain）
* level: MLS安全级别，仅在MLS模式下起作用。

**5、SELinux 基本操作**

* **查询文件或目录的安全上下文**

命令基本用法

ls -Z <文件或目录>

用法举例

查询 /etc/hosts 的安全上下文。

ls -Z /etc/hosts

执行结果

-rw-r--r--. root root system\_u:object\_r:net\_conf\_t:s0 /etc/hosts

* **查询进程的安全上下文**

命令基本用法

ps auxZ | grep -v grep | grep <进程名>

用法举例

查询 Nginx 相关进程的安全上下文。

ps auxZ | grep -v grep | grep nginx

执行结果

system\_u:system\_r:httpd\_t:s0 root 7997 0.0 0.0 122784 2156 ? Ss 14:31 0:00 nginx: master process /usr/sbin/nginx

system\_u:system\_r:httpd\_t:s0 nginx 7998 0.0 0.0 125332 7560 ? S 14:31 0:00 nginx: worker process

* **手动修改文件或目录的安全上下文**

命令基本用法

chcon <选项> <文件或目录 1> [<文件或目录 2>...]



用法举例

修改 test 的安全上下文为 aaa\_u:bbb\_r:ccc\_t:s0。

chcon -u aaa\_u -r bbb\_r -t ccc\_t test

* **把文件或目录的安全上下文恢复到默认值**

命令基本用法

restorecon [选项] <文件或目录 1> [<文件或目录 2>...]



用法举例

添加一些网页文件到 Nginx 服务器的目录之后，为这些新文件设置正确的安全上下文。

restorecon -R /usr/share/nginx/html/

* **查询系统中的布尔型规则及其状态**

命令基本用法

getsebool -a

由于该命令要么查询所有规则，要么只查询一个规则，所以一般都是先查询所有规则然后用 grep 筛选。

用法举例

查询与 httpd 有关的布尔型规则。

getsebool -a | grep httpd

执行结果

httpd\_anon\_write --> off

httpd\_builtin\_scripting --> on

httpd\_can\_check\_spam --> off

httpd\_can\_connect\_ftp --> off

#

* **开关一个布尔型规则**

命令基本用法

setsebool [选项] <规则名称> <on|off>



用法举例

开启 httpd\_anon\_write 规则。

setsebool -P httpd\_anon\_write on

* **添加目录的默认安全上下文**

命令基本用法

（如果提示找不到命令的话请安装 `policycoreutils-python` 软件包，下同。）

semanage fcontext -a -t <文件安全上下文中的类型字段> "<目录（后面不加斜杠）>(/.\*)?"

注：目录或文件的默认安全上下文可以通过 semanage fcontext -l 命令配合 grep 过滤查看。

用法举例

为 Nginx 新增一个网站目录 /usr/share/nginx/html2 之后，需要为其设置与原目录相同的默认安全上下文。

semanage fcontext -a -t httpd\_sys\_content\_t "/usr/share/nginx/html2(/.\*)?"

* **添加某类进程允许访问的端口**

命令基本用法

semanage port -a -t <服务类型> -p <协议> <端口号>

注：各种服务类型所允许的端口号可以通过 semanage port -l 命令配合 grep 过滤查看。

用法举例

为 Nginx 需要使用 10080 的端口用于 HTTP 服务。

semanage port -a -t http\_port\_t -p tcp 10080

## 任务描述

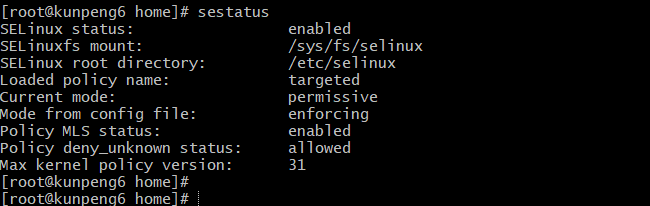
1. 安装SELinux,获取当前SELinux的状态并给出解释；
2. 切换SELinux 运行模式；
3. 检查用户、文件与文件夹、指定进程的安全上下文；

## 审核要求

1. 提交相关源码与过程截图。

## 参考答案

1. 鲲鹏服务器已经默认安装了SELinux，故不用自己另外安装。
2. 使用sestatus查看SELinux状态并给出解释



SELinux status: enabled # SELinux 是否启动

SELinuxfs mount: /sys/fs/selinux # SELinux 的相关文件数据挂载点

SELinux root directory: /etc/selinux # SELinux 的根目录所在

Loaded policy name: targeted # 当前的政策

Current mode: permissive # 当前模式

Mode from config file: enforcing # 目前配置文件内规范的 SELinux 模式

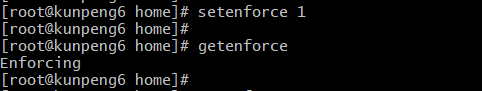
Policy MLS status: enabled # 是否含有 MLS 的模式机制

Policy deny\_unknown status: allowed # 是否预设抵挡未知的主体进程

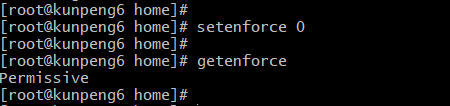
Max kernel policy version: 31

1. 切换SELinux 运行策略

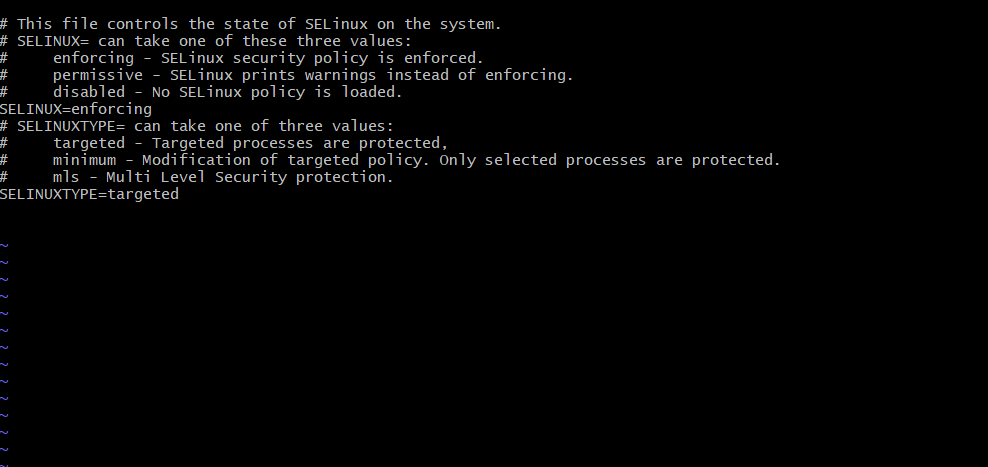
* 将SELinux的运行策略切换到Enforcing模式



* 将SELinux的运行策略切换到Permissive模式

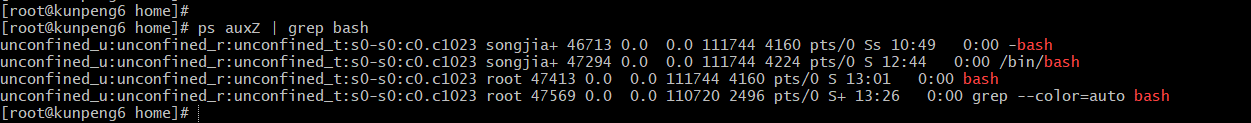


将SELinux的运行策略切换到Disabled需要修改 /etc/selinux/config文件，



需要注意的是修改上述配置文件之后，需要重新启动。

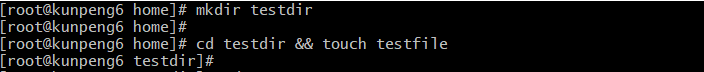
1. 检查指定进程的安全上下文

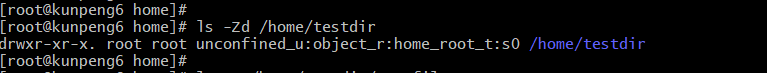


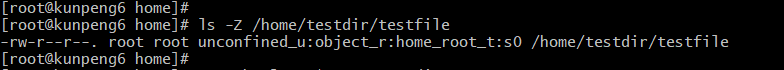
1. 检查文件与目录的安全上下文

执行下列操作：

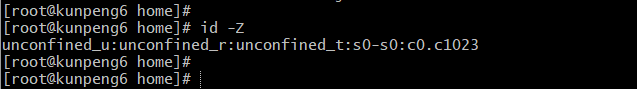
1. 在/home路径下创建testdir文件夹；
2. 进入testdir文件夹，并创建空文件testfile
3. 检查/home/testdir以及/home/testdir/testfile的安全上下文







1. 检查用户的安全上下文



# 2 任务2：使用Apache Web 服务器验证SELinux内核安全模块 (60min)

## 2.1 相关知识

Apache HTTP Server（简称Apache），是Apache软件基金会的一个开放源代码的网页服务器，可以在大多数电脑操作系统中运行，由于其具有的跨平台性和安全性，被广泛使用，是最流行的Web服务器端软件之一。

### 2.1.1 安装httpd服务

|  |
| --- |
| yum -y install httpd |

### 2.1.2 操作httpd服务 - 开机启动/重启/查看状态

|  |
| --- |
| systemctl start httpd #启动  systemctl stop httpd #停止  systemctl restart httpd #重启  systemctl enable httpd #开机启动  systemctl disable httpd #开机不启动  systemctl status httpd #检查httpd状态 |

有时服务器环境受限，比如在内网环境不能暴露端口从外网访问，用curl看html代码比较累，这时可以使用命令行浏览器来查看相关页面。Links浏览器，是一个带有ncurse界面的文本模式WEB浏览器，支持彩色，table渲染和后台下载，且包括菜单界面的浏览器，支持Frame框架。 我们可以通过外部的访问器来进行不同文件格式的浏览。 支持通过外部客户端使用mailto:和telnet:进行浏览。

### 2.1.3 Links的安装与使用

|  |
| --- |
| yum install links #安装Links  links URL #使用Links访问指定网站 |

## 2.2 任务描述

1. 安装并启动httpd、links；

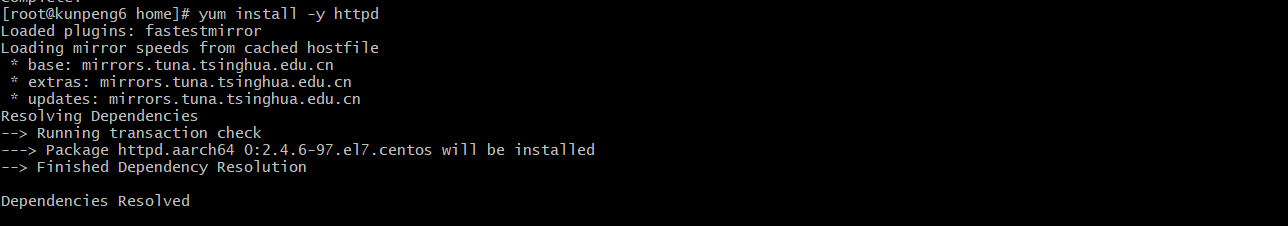
2. 使用httpd、links验证SELinux；

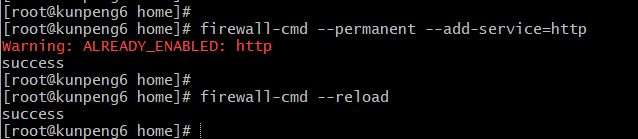
## 2.3 审核要求

1. 提交相关源码与过程截图。

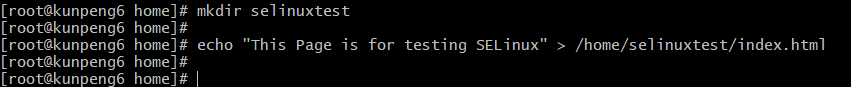
## 2.4 参考答案

（1）安装httpd服务，设置防火墙允许http服务

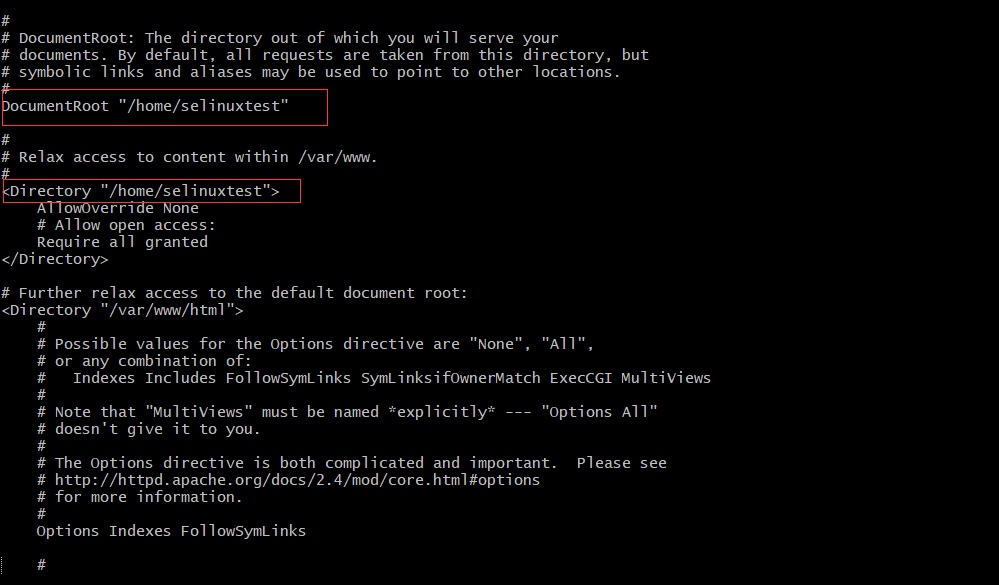




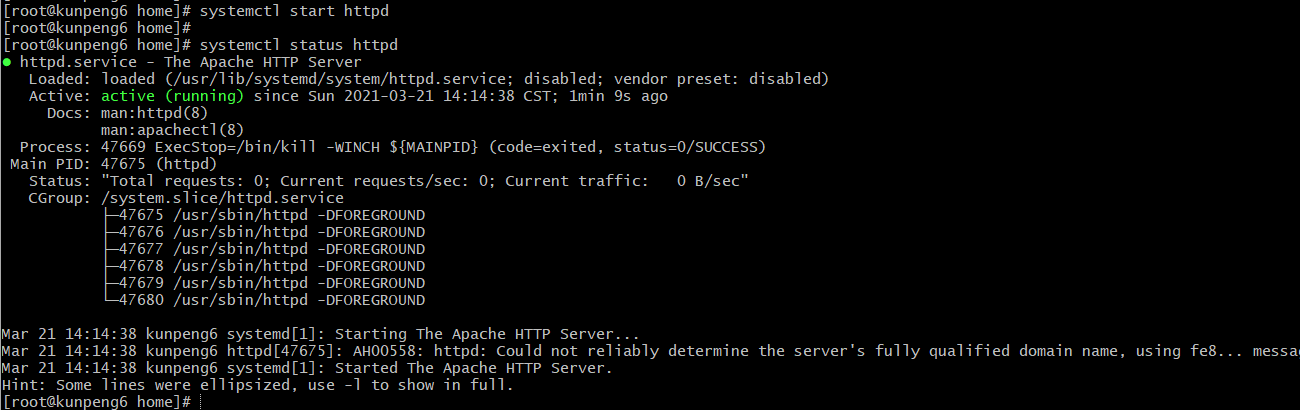
（2）将网站数据目录修改为/home/selinuxtest目录，并创建首页文件



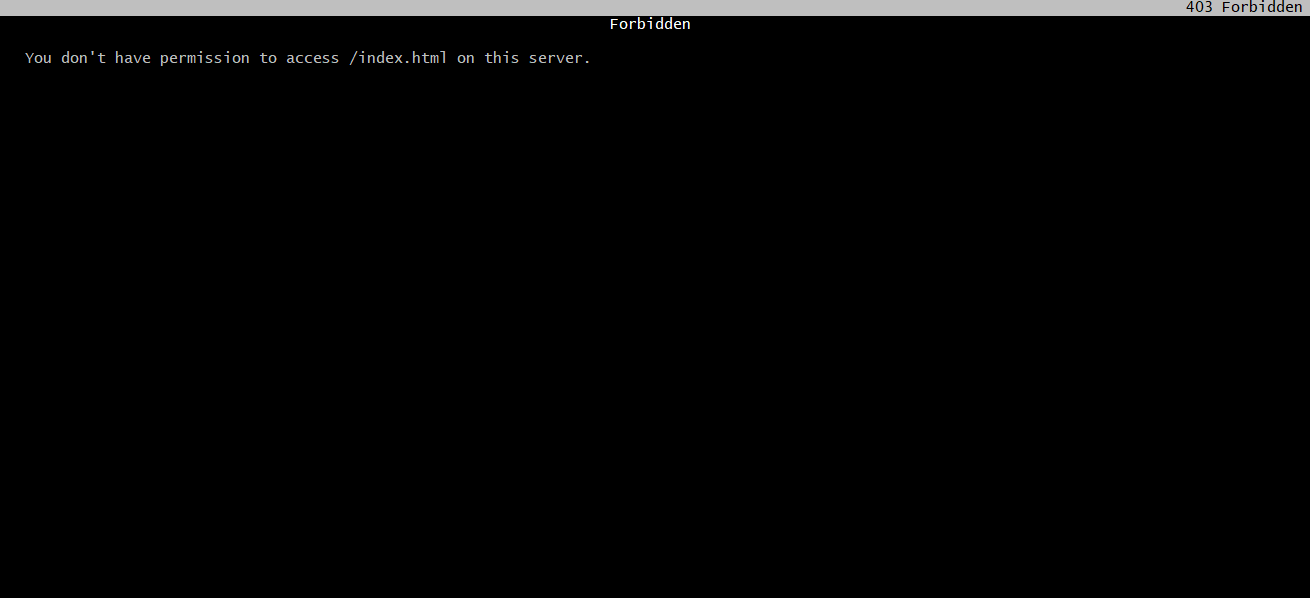
（3）修改httpd服务的配置文件



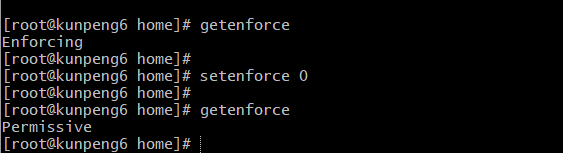
（4）启动httpd服务，并验证效果



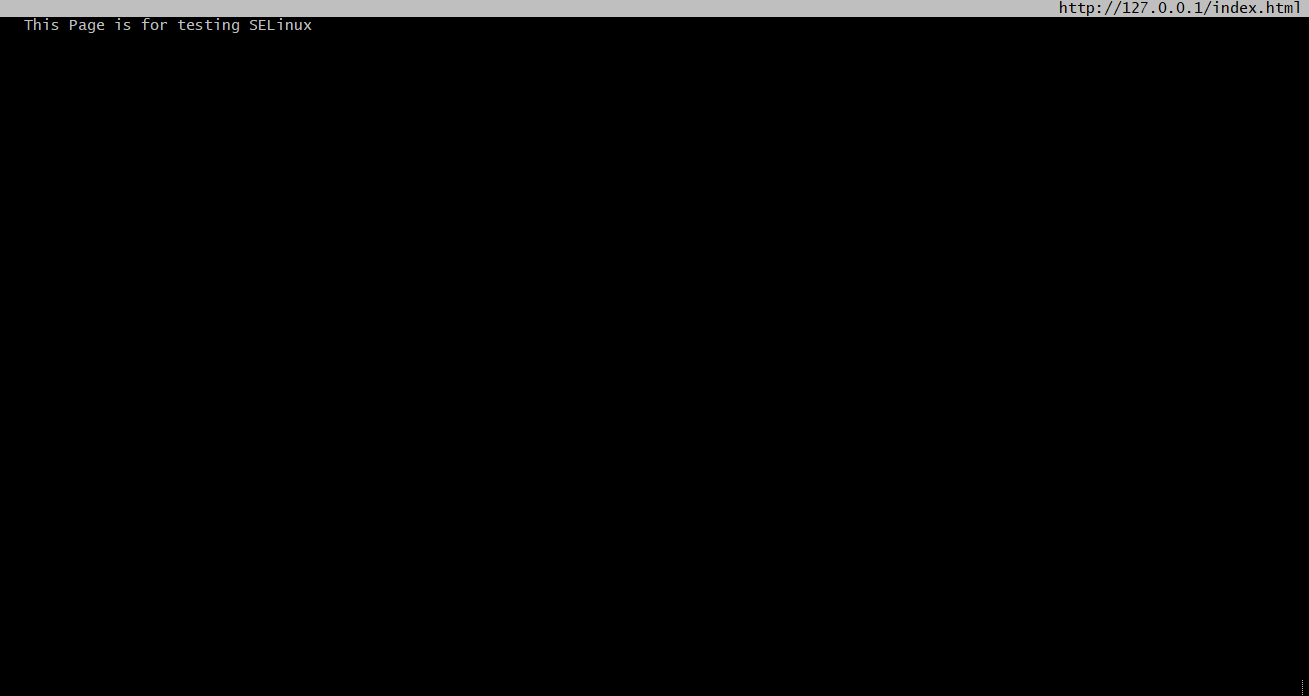




（5）修改selinux运行状态，重新验证效果

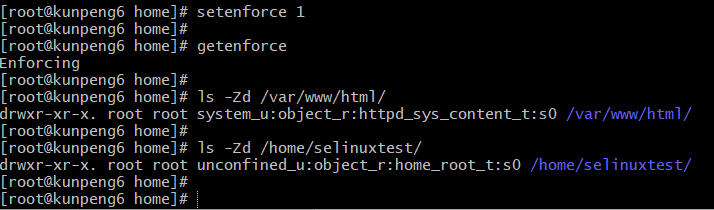






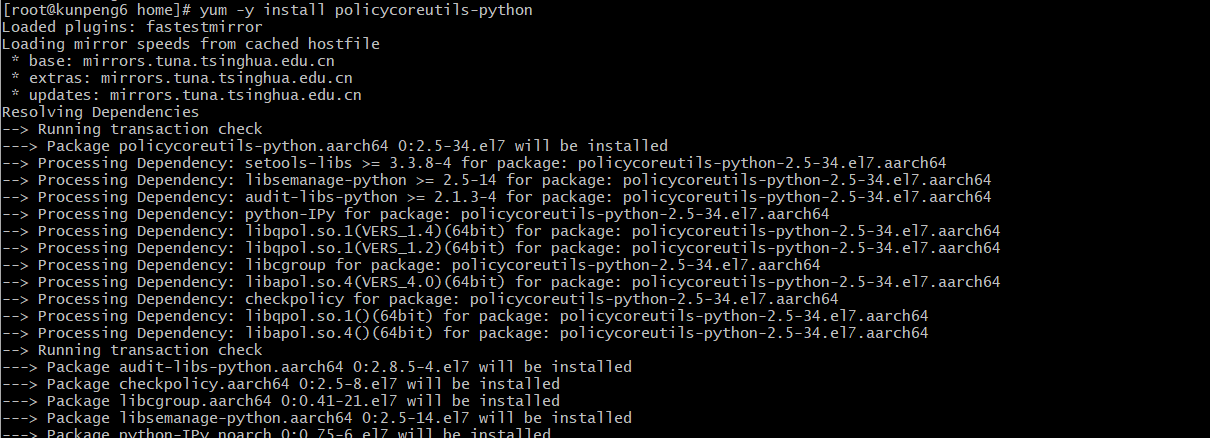
（6）修改selinux运行状态，通过修改文件安全上下文的方式访问网页

我们把httpd服务的网站数据默认保存目录修改为/home/selinuxtest，这显然违反了selinux的监管原则，/home目录是用来存放普通用户的家目录数据的，而现在httpd服务却要去获取普通用户家目录中的数据，selinux自然是不允许了。我们现在把selinux服务恢复到强制启用安全策略模式，然后修改selinux的安全上下文即可。

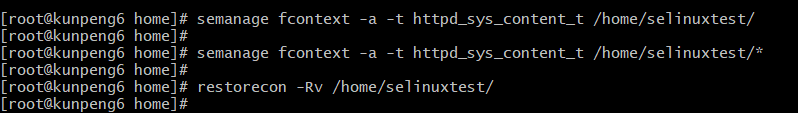


selinux安全上下文是由用户段、角色段和类型段等多个信息项组成的，用户段system\_u表示系统进程的身份，角色段object\_r表示文件目录的角色，类型段httpd\_sys\_content\_t表示网站服务的系统文件。我们可以通过将/home/selinuxtest目录的安全上下文修改为跟原始网站目录一样就行了。

首先安装所需命令软件包policycoreutils-python



然后将/home/selinuxtest目录添加一条安全上下文



查看selinux状态



重新访问网页



