· 五个用户的密码都是 redhat。

· 所有更改均应发生在 **/shares/cases** 目录及其文件中；请勿调整 **/shares** 目录。

1. **cases** 目录及其内容应属于 managers 组。新增至 **cases** 目录中的文件应自动属于 managers 组。现有文件的用户和组所有者应具有读取和写入权限，其他用户应没有任何权限。

> **注意**
> 提示：切勿使用 **setfacl**。

1.1. 以 student 用户身份登录 serverb。

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

1.2. 使用 **sudo -i** 命令，切换为 root 用户。student 用户的密码为 student。

```
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

1.3. 使用 **chgrp** 命令，以递归方式更新目录及其内容上的组所有权。

```
[root@serverb ~]# chgrp -R managers /shares/cases
```

1.4. 使用 **chmod** 命令更新目录上的 **set-GID** 标志。

```
[root@serverb ~]# chmod g+s /shares/cases
```

1.5. 使用 **chmod**，将所有现有文件的权限针对其所有者和组更新为 **rw**。

```
[root@serverb ~]# chmod 660 /shares/cases/*
```

2. 将 ACL 条目添加至 **cases** 目录（及其内容），以允许 contractors 组成员具有文件的读取/写入权限以及目录的执行权限。限制 contractor3 用户，使其只具有文件的读取权限和目录的执行权限。

2.1. 使用 **setfacl**，以递归方式更新现有 **cases** 目录及其内容。授予 contractors 组读取、写入及有条件的执行权限。

```
[root@serverb ~]# setfacl -Rm g:contractors:rwX /shares/cases
```

2.2. 使用 **setfacl**，以递归方式更新现有 **cases** 目录及其内容。授予 contractor3 用户读取及有条件的执行权限。

```
[root@serverb ~]# setfacl -Rm u:contractor3:rX /shares/cases
```

海量视频题库 myitpub.com QQ:5565462 www.52myit.com

3. 添加 ACL 条目，以确保 **cases** 目录中的任何新文件或目录均针对所有授权用户和组应用了正确的权限。

3.1. 使用 **setfacl**，为 contractors 组成员更新默认权限。默认权限为读取、写入和执行（即创建和访问适当子目录所需的权限）。

```
[root@serverb ~]# setfacl -m d:g:contractors:rwx /shares/cases
```

3.2. 使用 **setfacl**，为 contractor3 用户更新默认权限。默认权限为读取和执行（即访问适当子目录所需的权限）。

```
[root@serverb ~]# setfacl -m d:u:contractor3:rx /shares/cases
```

4. 验证您已正确更改了 ACL 和文件系统。

使用 **ls** 和 **getfacl** 检查 **/shares/cases** 上的设置。

以 student 用户身份，使用 **su - user** 先切换到 manager1，然后切换到 contractor1。验证您能够写入文件、读取文件、创建目录以及对新目录中的文件执行写入操作。使用 **ls** 检查新目录权限，并使用 **getfacl** 查看新目录的 ACL。

以 student 用户身份，使用 **su - contractor3** 切换用户。尝试写入一个文件（应会失败）并尝试创建新目录（应会失败）。作为 contractor3 用户，您应该能够读取 **cases** 目录中的 **shortlist.txt** 文件，并能够读取在由 manager1 或 contractor1 用户新建的任一目录中写入的“测试”文件。

4.1. 以 root 用户身份，使用 **ls** 检查 **cases** 目录及其内容。查找组所有权、目录和文件权限。组文件权限中的“**s**”表示已设置 **set-GID** 标志，而“**+**”则表示存在 ACL 条目。最后，退出 root 用户会话。

```
[root@serverb ~]# ls -ld /shares/cases
drwxrws---+ 2 root managers 46 Mar 29 00:40 /shares/cases
[root@serverb ~]# ls -l /shares/cases
total 8
-rw-rw----+ 1 root managers 44 Mar 29 00:33 backlog.txt
-rw-rw----+ 1 root managers 46 Mar 29 00:33 shortlist.txt
```

4.2. 使用 **getfacl** 并查看其输出。在标准和默认 ACL 中查找指定用户和指定组的条目。

```
[root@serverb ~]# getfacl /shares/cases
# file: shares/cases
# owner: root
# group: managers
# flags: -s-
user::rwx
user:contractor3:r-x
group::rwx
group:contractors:rwx
mask::rwx
other::---
default:user::rwx
default:user:contractor3:r-x
default:group::rwx
default:group:contractors:rwx
```

海量视频题库 myitpub.com QQ:556462
www.52myit.com

```
default:mask::rwx
default:other::---

[root@serverb ~]# exit
logout
```

4.3. 切换到 manager1 用户并执行以下操作。检查您是否获得预期的访问行为。

```
[student@serverb ~]$ su - manager1
Password: redhat
[manager1@serverb ~]$ cd /shares/cases
[manager1@serverb cases]$ echo hello > manager1.txt
[manager1@serverb cases]$ cat shortlist.txt
###Shortlist of Clients to call###TEMPLATE###
[manager1@serverb cases]$ mkdir manager1.dir
[manager1@serverb cases]$ echo hello > manager1.dir/test.txt
[manager1@serverb cases]$ ls -ld manager1.dir
drwxrws---+ 2 manager1 managers 22 Mar 29 00:59 manager1.dir
[manager1@serverb cases]$ ls -l manager1.dir
total 4
-rw-rw----+ 1 manager1 managers 6 Mar 29 00:59 test.txt
[manager1@serverb cases]$ getfacl manager1.dir
# file: manager1.dir/
# owner: manager1
# group: managers
# flags: -s-
user::rwx
user:contractor3:r-x
group::rwx
group:contractors:rwx
mask::rwx
other::---
default:user::rwx
default:user:contractor3:r-x
default:group::rwx
default:group:contractors:rwx
default:mask::rwx
default:other::---

[manager1@serverb cases]$ exit
logout
```

4.4. 切换到 contractor1 用户并执行以下操作。检查您是否获得预期的访问行为。

```
[student@serverb ~]$ su - contractor1
Password: redhat
[contractor1@serverb ~]$ cd /shares/cases
[contractor1@serverb cases]$ echo hello > manager1.txt
[contractor1@serverb cases]$ cat shortlist.txt
###Shortlist of Clients to call###TEMPLATE###
[contractor1@serverb cases]$ mkdir contractor1.dir
[contractor1@serverb cases]$ echo hello > contractor1.dir/test.txt
[contractor1@serverb cases]$ ls -ld contractor1.dir
drwxrws---+ 2 contractor1 managers 22 Mar 29 01:05 contractor1.dir
```

海量视频题库 myitpub.com QQ:5565462 www.52myit.com

```
[contractor1@serverb cases]$ ls -l contractor1.dir
total 4
-rw-rw----+ 1 contractor1 managers 6 Mar 29 01:07 test.txt
[manager1@serverb cases]$ getfacl contractor1.dir
# file: contractor1.dir/
# owner: contractor1
# group: managers
# flags: -s-
user::rwx
user:contractor3:r-x
group::rwx
group:contractors:rwx
mask::rwx
other::---
default:user::rwx
default:user:contractor3:r-x
default:group::rwx
default:group:contractors:rwx
default:mask::rwx
default:other::---

[contractor1@serverb cases]$ exit
logout
```

4.5. 切换到 contractor3 用户并执行以下操作。检查您是否获得预期的访问行为。

```
[student@serverb ~]# su - contractor3
Password: redhat
[contractor3@serverb ~]# cd /shares/cases
[contractor3@serverb cases]# echo hello > contractor3.txt
-bash: contractor3.txt: Permission denied
[contractor3@serverb cases]# cat shortlist.txt
###Shortlist of Clients to call###TEMPLATE###
[contractor3@serverb cases]# mkdir contractor3.dir
mkdir: cannot create directory 'contractor3.dir': Permission denied
[contractor3@serverb cases]# cat manager1.dir/test.txt
hello
[contractor3@serverb cases]# cat contractor1.dir/test.txt
hello
[contractor3@serverb cases]# exit
logout
[student@serverb ~]#
```

4.6. 从 serverb 注销

```
[student@serverb ~]# exit
logout
Connection to serverb closed.
[student@workstation ~]$
```

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

注意
上述这组测试是您可用来执行以检查访问权限是否正确的其中一些测试。您应根据自己的环境来设计合适的访问权限验证测试。

评估

在 workstation 上，运行 **lab acl-review grade** 命令来确认是否成功完成本练习。

```
[student@workstation ~]$ lab acl-review grade
```

完成

在 workstation 上，运行 **lab acl-review finish** 命令来完成本练习。

```
[student@workstation ~]$ lab acl-review finish
```

本实验到此结束。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

总结

在本章中，您学到了：

- ACL 提供对文件和目录的细化访问控制。
- **getfacl** 命令显示文件或目录的 ACL。
- **setfacl** 命令设置、修改和删除文件及目录上的默认和标准 ACL。
- 使用默认 ACL 来控制新文件和目录的权限。
- 红帽企业 Linux 使用 systemd 和 udev 向设备、文件夹和文件应用预定义的 ACL。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

章 5

管理 SELINUX 安全性

目标

使用 SELinux 保护和管理服务器的安全性。

培训目标

- 介绍 SELinux 如何保护资源以及如何选择执行模式。
- 配置文件的 SELinux 上下文，以控制进程如何与该文件进行交互。
- 配置 SELinux 布尔值，从而允许针对不同的访问需求更改运行时策略。
- 调查 SELinux 日志消息并对 SELinux AVC 拒绝问题进行故障排除。

章节

- 更改 SELinux 到强制模式（及引导式练习）
- 控制 SELinux 文件上下文（及引导式练习）
- 使用布尔值调整 SELinux 策略（及引导式练习）
- 调查和解决 SELinux 问题（及引导式练习）

实验

管理 SELinux 安全性

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

更改 SELINUX 到强制模式（及引导式练习）

培训目标

学完本节后，您应能够：

- 解释 SELinux 如何保护资源。
- 更改系统的当前 SELinux 模式。
- 设置系统的默认 SELinux 模式。

SELINUX 如何保护资源

SELinux 在 Linux 中具有重要的安全用途，它可以允许或拒绝访问文件及其他资源，且精准度相比用户权限要大幅提高。

文件权限控制了哪些用户或用户组可以访问哪些特定文件。但是，被授予对特定文件的读取或写入权限的用户可以按用户选择的任何方式使用该文件，即使这种使用方式并不是文件本该采用的方式。

例如，对于文件的写入权限而言，结构化数据文件是否应当设计为只能使用特定的程序写入，但其他编辑器仍可以打开和修改此文件，而这可能会导致损坏？

文件权限并不能阻止此类不合要求的访问。它们未设计为控制如何使用文件，而仅仅是控制谁可以读取、写入或运行文件。

SELinux 由应用开发人员定义的若干组策略组成，这些策略准确声明了对于应用使用的每个二进制可执行文件、配置文件和数据文件，哪些操作和访问权限是恰当且被允许的。这被称为目标政策，因为会编写一个策略以涵盖单个应用的活动。策略声明了各个程序、文件和网络端口上放置的预定义标签。

为什么使用 SECURITY ENHANCED LINUX?

并非所有安全问题都可以提前预测。SELinux 实施了一组可以防止一个应用程序的弱点影响其他应用或基础系统的访问规则。SELinux 提供了一个额外的安全层，此外还增加了一层复杂结构，这令该子系统的新用户感到烦恼。学习使用 SELinux 可能会需要一些时间，但执行政策意味着系统某一部分的弱点不会扩散到其他部分。如果 SELinux 在特定的子系统上运行不佳，则可以关闭该特定服务的执行，直至找到潜在问题的解决方案。

SELinux 有三种模式：

- 强制：SELinux 强制执行访问控制规则。计算机通常在该模式下运行。
- 许可：SELinux 处于活动状态，但并不强制执行访问控制规则，而是记录违反规则的警告。该模式主要用于测试和故障排除。
- 禁用：SELinux 完全关闭 - 不拒绝任何 SELinux 违规，甚至不予记录。不建议禁用 SELinux!

SELINUX 安全的基本概念

Security Enhanced Linux (SELinux) 是一个额外的系统安全层。SELinux 的主要目标是防止已遭泄露的系统服务访问用户数据。大多数 Linux 管理员都熟悉标准的用户/组/其他权限安全模型。这种基于

海量视频题库 myitpub.com QQ:5565462 www.52myit.com

用户和组的模型称为自由决定的访问控制。SELinux 提供另一层安全，它基于对象并由更加复杂的规则控制，称为强制访问控制。

要允许远程匿名访问 Web 服务器，必须打开防火墙端口。不过，这也让恶意人员有机会通过安全漏洞侵入系统。如果他们成功入侵了 Web 服务器进程，就可以获得进程的权限。具体来说，就是 apache 用户和 apache 组的权限。该用户和组对文档根目录 **/var/www/html** 具有读取权限。它还可以访问 **/tmp** 和 **/var/tmp**，以及全局可写的其他任何文件和目录。

SELinux 是用于确定哪个进程可以访问哪些文件、目录和端口的一组安全规则。每个文件、进程、目录和端口都具有专门的安全标签，称为 SELinux 上下文。上下文是一个名称，SELinux 策略使用它来确定某个进程能否访问文件、目录或端口。除非显式规则授予访问权限，否则，在默认情况下，策略不允许任何交互。如果没有允许规则，则不允许访问。

SELinux 标签具有多种上下文：用户、角色、类型和敏感度。目标策略（即红帽企业 Linux 中启用的默认策略）会根据第三个上下文（即类型上下文）来制定自己的规则。类型上下文名称通常以 **_t** 结尾。

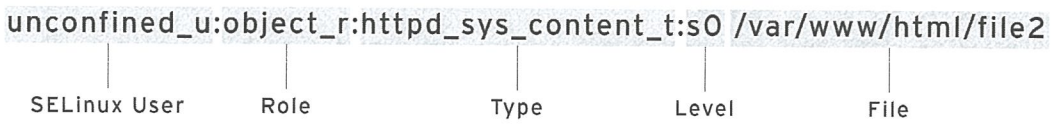

图 5.1: SELinux 文件上下文

Web 服务器的类型上下文是 **httpd_t**。通常位于 **/var/www/html** 中的文件和目录的类型上下文是 **httpd_sys_content_t**。通常位于 **/tmp** 和 **/var/tmp** 中的文件和目录上下文是 **tmp_t**。Web 服务器端口的类型上下文是 **http_port_t**。

Apache 具有类型上下文 **httpd_t**。有一个策略规则允许 Apache 访问具有 **httpd_sys_content_t** 类型上下文的文件和目录。默认情况下，在 **/var/www/html** 和其他 Web 服务器目录中找到的文件具有 **httpd_sys_content_t** 类型上下文。策略中没有允许规则适用于通常位于 **/tmp** 和 **/var/tmp** 中的文件，因此不允许访问。在启用 SELinux 的情况下，破坏了 Web 服务器进程的恶意用户将无法访问 **/tmp** 目录。

MariaDB 服务器具有类型上下文 **mysqld_t**。默认情况下，在 **/data/mysql** 中找到的文件具有 **mysqld_db_t** 类型上下文。该类型上下文允许 MariaDB 访问这些文件，但禁止其他服务（如 Apache Web 服务）访问。

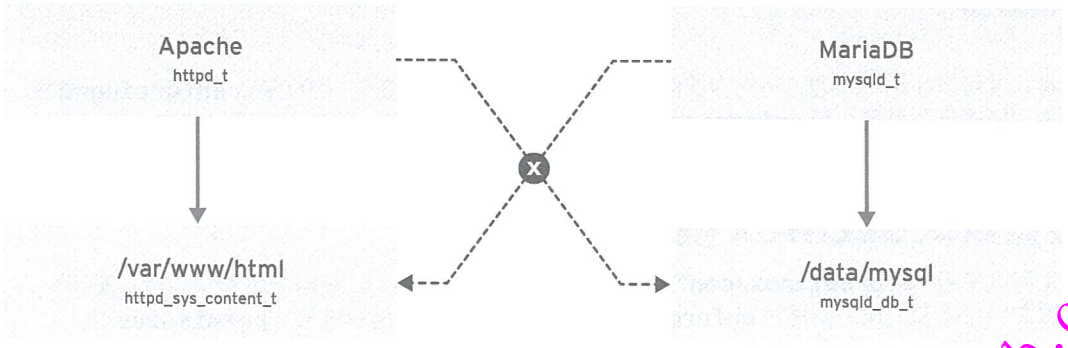

图 5.2: SELinux 访问

许多处理文件的命令都使用 **-Z** 选项来显示或设置 SELinux 上下文。例如，**ps**、**ls**、**cp** 和 **mkdir** 都使用 **-Z** 选项显示或设置 SELinux 上下文。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

```
[root@host ~]# ps axZ
LABEL                              PID TTY      STAT   TIME COMMAND
system_u:system_r:init_t:s0          1 ?        Ss     0:09 /usr/lib/systemd/...
system_u:system_r:kernel_t:s0        2 ?        S      0:00 [kthreadd]
system_u:system_r:kernel_t:s0        3 ?        S      0:00 [ksoftirqd/0]
...output omitted...
[root@host ~]# systemctl start httpd
[root@host ~]# ps -ZC httpd
LABEL                              PID TTY          TIME CMD
system_u:system_r:httpd_t:s0      1608 ?        00:00:05 httpd
system_u:system_r:httpd_t:s0      1609 ?        00:00:00 httpd
...output omitted...
[root@host ~]# ls -Z /home
drwx------. root    root    system_u:object_r:lost_found_t:s0 lost+found
drwx------. student student unconfined_u:object_r:user_home_dir_t:s0 student
drwx------. visitor visitor unconfined_u:object_r:user_home_dir_t:s0 visitor
[root@host ~]# ls -Z /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
```

更改当前的 SELINUX 模式

SELinux 子系统提供了显示和更改模式的工具。要确定当前的 SELinux 模式，请运行 **getenforce** 命令。要将 SELinux 设置为其他模式，请使用 **setenforce** 命令：

```
[user@host ~]# getenforce
Enforcing
[user@host ~]# setenforce
usage:  setenforce [ Enforcing | Permissive | 1 | 0 ]
[user@host ~]# setenforce 0
[user@host ~]# getenforce
Permissive
[user@host ~]# setenforce Enforcing
[user@host ~]# getenforce
Enforcing
```

或者，您可以在启动时通过将向内核传递参数来设置 SELinux 模式：内核参数 **enforcing=0** 将以许可模式启动系统；值 **enforcing=1** 则设置强制模式。此外，您还可以通过传递内核参数 **selinux=0** 来彻底禁用 SELinux。值 **selinux=1** 将启用 SELinux。

设置默认 SELINUX 模式

您也可以使用 **/etc/selinux/config** 文件来持久配置 SELinux。在以下示例中（默认配置），配置文件会将 SELinux 设置为 **enforcing**。注释中还显示了其他有效值：**permissive** 和 **disabled**。

```
# 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.
```

海量视频题库 myitpub.com QQ:556462 www.52myit.com

```
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes
#               are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

系统在启动时会读取此文件并如文中所示配置 SELinux。内核参数（**selinux=0|1** 和 **enforcing=0|1**）将覆盖此配置。

参考文献

getenforce(8)、**setenforce**(8) 和 **selinux_config**(5) man page

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

指导练习

更改 SELINUX 强制模式

在本实验中，您将练习暂时性管理以及持久性管理 SELinux 模式。

成果

您应能够查看和设置当前的 SELinux 模式。

在你开始之前

在 workstation 上，以 student 用户身份并使用密码 student 进行登录。

在 workstation 上，运行 **lab selinux-opsmode start** 命令。此命令将运行一个起始脚本，它将确定 servera 计算机是否可从网络访问。

```
[student@workstation ~]$ lab selinux-opsmode start
```

1. 使用 **ssh** 命令，以 student 用户身份登录 servera。系统已配置为使用 SSH 密钥来进行身份验证，因此不需要提供密码。

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

2. 使用 **sudo -i** 命令，切换为 root 用户。student 用户的密码为 student。

```
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

3. 将默认 SELinux 模式更改为许可模式，并重新启动。

3.1. 使用 **getenforce** 命令，验证 servera 是否处于强制模式。

```
[root@servera ~]# getenforce
Enforcing
```

3.2. 使用 **vim** 命令打开 **/etc/selinux/config** 配置文件。将 SELINUX 参数从 enforcing 更改为 permissive。

```
[root@servera ~]# vim /etc/selinux/config
```

3.3. 使用 **grep** 命令，确认 SELINUX 参数是否设置为 permissive。

海量视频题库 myitpub.com QQ:556462
www.52myit.com

```
[root@servera ~]# grep '^SELINUX' /etc/selinux/config
SELINUX=permissive
SELINUXTYPE=targeted
```

3.4. 使用 **systemctl reboot** 命令来重启 servera。

```
[root@servera ~]# systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@workstation ~]$
```

4. 重启 servera 需要几分钟的时间。几分钟后，以 student 用户身份登录 servera。使用 sudo -i 命令变为 **root** 用户。使用 **getenforce** 命令显示当前的 SELinux 模式。

4.1. 从 workstation，使用 **ssh** 命令以 student 用户身份登录 servera。

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

4.2. 使用 sudo -i 命令变为 **root** 用户。

```
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

4.3. 使用 **getenforce** 命令显示当前的 SELinux 模式。

```
[root@servera ~]# getenforce
Permissive
```

5. 在 **/etc/selinux/config** 文件中，将 SELinux 的默认模式更改为强制模式。此更改仅在下次重启时生效。

5.1. 使用 **vim** 命令打开 **/etc/selinux/config** 配置文件。将 SELINUX 恢复为 enforcing 模式。

```
[root@servera ~]# vim /etc/selinux/config
```

5.2. 使用 **grep** 命令，确认 SELINUX 参数是否设置为 enforcing。

```
[root@servera ~]# grep '^SELINUX' /etc/selinux/config
SELINUX=enforcing
SELINUXTYPE=targeted
```

6. 使用 **setenforce** 命令，在不重启的情况下将当前 SELinux 模式设置为 enforcing。使用 **getenforce** 命令，确认模式已设置为 enforcing。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

```
[root@servera ~]# setenforce 1
[root@servera ~]# getenforce
Enforcing
```

▶ **7.** 从 servera 退出。

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

完成

在 workstation 上，运行 **lab selinux-opsmode finish** 脚本来完成本练习。

```
[student@workstation ~]$ lab selinux-opsmode finish
```

本引导式练习到此结束。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

控制 SELINUX 文件上下文

培训目标

学完本节后，您应能够：

- 使用 **semanage fcontext** 命令，管理决定了文件和目录默认上下文的 SELinux 策略规则。
- 使用 **restorecon** 命令，将 SELinux 策略所定义的上下文应用到文件和目录。

初始 SELINUX 上下文

在运行 SELinux 的系统上，所有进程和文件都会有相应的标签。标签代表了与安全有关的信息，称为 SELinux 上下文。

新文件通常从父目录继承其 SELinux 上下文，从而确保它们具有适当的上下文。

但是，有两种不同的方式可能会破坏该继承过程。首先，如果您在与最终目标位置不同的位置创建文件，然后移动文件，则该文件将具有创建它时所在目录的 SELinux 上下文，而不是目标目录的 SELinux 上下文。其次，如果是复制一个保留 SELinux 上下文的文件（正如使用 **cp -a** 命令），则 SELinux 上下文将反映原始文件的位置。

以下示例演示了继承关系及存在的缺陷。以 **/tmp** 中创建的这两个文件为例，一个移动到 **/var/www/html**，另一个复制到同一目录中。请注意文件的 SELinux 上下文。移动到 **/var/www/html** 目录的文件保留了 **/tmp** 目录的文件上下文。复制到 **/var/www/html** 目录中的文件则继承了 **/var/www/html** 目录的 SELinux 上下文。

ls -Z 命令显示文件的 SELinux 上下文。请注意文件的标签。

```
[root@host ~]# ls -Z /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/
index.html
```

ls -Zd 命令显示目录的 SELinux 上下文：

```
[root@host ~]# ls -Zd /var/www/html/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html/
```

请注意，**/var/www/html/index.html** 与父目录 **/var/www/html/** 具有相同的标签。现在，在 **/var/www/html** 目录之外创建文件并注意它们的文件上下文：

```
[root@host ~]# touch /tmp/file1 /tmp/file2
[root@host ~]# ls -Z /tmp/file*
unconfined_u:object_r:user_tmp_t:s0 /tmp/file1
unconfined_u:object_r:user_tmp_t:s0 /tmp/file2
```

将其中一个文件移动到 **/var/www/html** 目录，复制另一个文件，同时注意每个文件的标签：

海量视频题库 myitpub.com QQ:556462
www.52myit.com

```
[root@host ~]# mv /tmp/file1 /var/www/html/
[root@host ~]# cp /tmp/file2 /var/www/html/
```

```
[root@host ~]# ls -Z /var/www/html/file*
unconfined_u:object_r:user_tmp_t:s0 /var/www/html/file1
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2
```

移动的文件保留了自己的原始标签，而复制的文件则继承了 **/var/www/html** 目录的标签。**unconfined_u:** 代表用户，**object_r:** 代表角色，**s0** 代表级别。敏感度级别 0 为最低级别。

更改文件的 SELINUX 上下文

用于更改文件 SELinux 上下文的命令包括：**semanage fcontext**、**restorecon** 和 **chcon**。

为文件设置 SELinux 上下文的首选方法是使用 **semanage fcontext** 命令来声明文件的默认标签，然后使用 **restorecon** 命令将该上下文应用于文件。这样可确保标签符合预期，即便在对文件系统完全重新标记之后也是如此。

chcon 命令更改 SELinux 上下文。**chcon** 设置存储在文件系统中的文件安全上下文。它对于测试和实验很有用。但是，它不会将上下文更改保存到 SELinux 上下文数据库中。当 **restorecon** 命令运行时，**chcon** 命令所做的更改也同样无法保留。此外，如果对整个文件系统进行重新标记，则使用 **chcon** 更改过的文件的 SELinux 上下文将恢复。

以下屏幕显示正在创建的目录。该目录的类型值为 **default_t**。

```
[root@host ~]# mkdir /virtual
[root@host ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual
```

chcon 命令更改 **/virtual** 目录的文件上下文：类型值更改为 **httpd_sys_content_t**。

```
[root@host ~]# chcon -t httpd_sys_content_t /virtual
[root@host ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:httpd_sys_content_t:s0 /virtual
```

运行 **restorecon** 命令，类型值恢复为 **default_t** 的值。请注意 **Relabeled** 消息。

```
[root@host ~]# restorecon -v /virtual
Relabeled /virtual from unconfined_u:object_r:httpd_sys_content_t:s0 to
 unconfined_u:object_r:default_t:s0
[root@host ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual
```

定义 SELINUX 默认文件上下文规则

semanage fcontext 命令可显示和修改 **restorecon** 用来设置默认文件上下文的规则。它使用扩展正则表达式来指定路径和文件名。**fcontext** 规则中最常用的扩展正则表达式是 **(/.*)?**，表示“可选择匹配后跟任何数量字符的 /”。它将会匹配在表达式前面列出的目录并递归地匹配该目录中的所有内容。

海量视频题库 mvpub.com QQ:556462
www.52mvp.com

基本文件上下文操作

下表可作为 **semanage fcontext** 选项的参考，用于添加、删除或列出 SELinux 文件上下文。

semanage fcontext 命令

选项	描述
-a, --add	添加指定对象类型的记录
-d, --delete	删除指定对象类型的记录
-l, --list	列出指定对象类型的记录

为了确保您拥有管理 SELinux 上下文的工具，请根据需要安装 **policycoreutil** 软件包和 **policycoreutil-python** 软件包。这两个软件包中分别包含 **restorecon** 命令和 **semanage** 命令。

为了确保目录中的所有文件都具有正确的文件上下文，请先运行 **semanage fcontext -l**，再运行 **restorecon** 命令。在以下示例中，请注意在运行 **semanage** 和 **restorecon** 命令前后每个文件的文件上下文。

```
[root@host ~]# ls -Z /var/www/html/file*
unconfined_u:object_r:user_tmp_t:s0 /var/www/html/file1
 unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2


[root@host ~]# semanage fcontext -l
...output omitted...
/var/www(/.*)?       all files    system_u:object_r:httpd_sys_content_t:s0
...output omitted...


[root@host; ~]# restorecon -Rv /var/www/
Relabeled /var/www/html/file1 from unconfined_u:object_r:user_tmp_t:s0 to
 unconfined_u:object_r:httpd_sys_content_t:s0
[root@host ~]# ls -Z /var/www/html/file*
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file1
 unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/file2
```

以下示例显示了如何使用 **semanage** 为新目录添加上下文。

```
[root@host ~]# mkdir /virtual
[root@host ~]# touch /virtual/index.html
[root@host ~]# ls -Zd /virtual/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual/
```

海量视频题库 myitpub.com QQ:556462
www.52myit.com

```
[root@host ~]# ls -Z /virtual/
-rw-r--r--. root root unconfined_u:object_r:default_t:s0 index.html
[root@host ~]# semanage fcontext -a -t httpd_sys_content_t '/virtual(/.*)?'
[root@host ~]# restorecon -RFvv /virtual
[root@host ~]# ls -Zd /virtual/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /virtual/
[root@host ~]# ls -Z /virtual/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 index.html
```

参考文献

chcon(1)、**restorecon**(8)、**semanage**(8) 和 **semanage-fcontext**(8) man page

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

指导练习

控制 SELINUX 文件上下文

在本实验中，您将对一个目录及其内容的 SELinux 上下文进行持久更改。

成果

您应能够配置 Apache HTTP 服务器，以便从非标准文档根目录发布 Web 内容。

在你开始之前

在 workstation 上，以 student 用户身份并使用密码 student 进行登录。

在 workstation 上，运行 **lab selinux-filecontexts start** 命令。此命令将运行一个起始脚本，它将确定 servera 计算机是否可从网络访问。此外，它还将安装 **httpd** 服务并配置 servera 的防火墙，以允许进行 HTTP 连接。

```
[student@workstation ~]$ lab selinux-filecontexts start
```

1. 使用 **ssh** 命令，以 student 用户身份登录 servera。系统已配置为使用 SSH 密钥来进行身份验证，因此不需要提供密码。

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

2. 使用 **sudo -i** 命令，切换为 root 用户。student 用户的密码为 student。

```
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

3. 配置 Apache 的站点目录，不使用默认的根目录。

3.1. 使用 **mkdir** 命令，新建文档根目录 **/custom**。

```
[root@servera ~]# mkdir /custom
```

3.2. 使用 **echo** 命令，在 **/custom** 文档根目录中创建 **index.html** 文件。

```
[root@servera ~]# echo 'This is SERVERA.' > /custom/index.html
```

3.3. 配置 Apache 使用新的文档根目录位置。需要将 Apache 配置文件 **/etc/httpd/conf/httpd.conf** 中两次出现的 **/var/www/html** 替换为 **/custom**。

海量视频题库 mvitpub.com QQ:556462
www.52mvit.com

```
[root@servera ~]# vim /etc/httpd/conf/httpd.conf
[root@servera ~]# grep custom /etc/httpd/conf/httpd.conf
DocumentRoot "/custom"
<Directory "/custom">
```

4. 启动并启用 Apache Web 服务，确认该服务正在运行。

4.1. 使用 **systemctl** 命令启动并启用 Apache Web 服务。

```
[root@servera ~]# systemctl enable --now httpd
```

4.2. 使用 **systemctl** 命令确认服务处于运行状态。

```
[root@servera ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset:
 disabled)
   Active: active (running) since Mon 2019-03-25 19:16:48 CET; 15h ago
     Docs: man:httpd.service(8)
 Main PID: 6565 (httpd)
   Status: "Total requests: 16; Idle/Busy workers 100/0;Requests/sec: 0.000285;
 Bytes served/sec:   0 B/sec"
   Tasks: 213 (limit: 11406)
   Memory: 37.3M
   CGroup: /system.slice/httpd.service
           ├─6565 /usr/sbin/httpd -DFOREGROUND
           ├─6566 /usr/sbin/httpd -DFOREGROUND
           ├─6567 /usr/sbin/httpd -DFOREGROUND
           ├─6568 /usr/sbin/httpd -DFOREGROUND
           └─6569 /usr/sbin/httpd -DFOREGROUND

Mar 25 19:16:48 servera.lab.example.com systemd[1]: Starting The Apache HTTP
 Server...
Mar 25 19:16:48 servera.lab.example.com httpd[6565]: Server configured, listening
 on: port 80
Mar 25 19:16:48 servera.lab.example.com systemd[1]: Started The Apache HTTP
 Server.
```

5. 在 workstation 上打开 Web 浏览器，并尝试查看 http://servera/index.html。您将会收到一条错误消息，提示您不具有访问该文件的权限。

6. 要想授予对 servera 上的 **index.html** 文件的访问权限，必须配置 SELinux。定义一条 SELinux 文件上下文规则，以便将 **/custom** 目录及目录中所有文件的上下文类型设置为 **httpd_sys_content_t**。

```
[root@servera ~]# semanage fcontext -a -t httpd_sys_content_t '/custom(/.*)?'
```

7. 使用 **restorecon** 命令更改文件上下文。

海量视频题库 myitpub.com QQ:556462
www.52myit.com

```
[root@servera ~]# restorecon -Rv /custom
Relabeled /custom from unconfined_u:object_r:default_t:s0 to
 unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /custom/index.html from unconfined_u:object_r:default_t:s0 to
 unconfined_u:object_r:httpd_sys_content_t:s0
```

8. 再次尝试查看 `http://servera/index.html`。您应当看到显示的消息 **This is SERVERA**。

9. 从 `servera` 退出。

```
[root@servera ~]# exit
logout
[student@servera ~]$ exit
logout
Connection to servera closed.
[student@workstation ~]$
```

完成

在 `workstation` 上，运行 **`lab selinux-filecontexts finish`** 脚本来完成本练习。

```
[student@workstation ~]$ lab selinux-filecontexts finish
```

本引导式练习到此结束。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

使用布尔值调整 SELINUX 策略

培训目标

学完本节后，您应能够：

- 使用 **setsebool** 激活/停用 SELinux 策略规则。
- 使用 **semanage boolean -l** 命令来管理 SELinux 布尔值的持久值。
- 查阅以 **_selinux** 结尾的 man page，寻找有关 SELinux 布尔值的有用信息。

SELINUX 布尔值

SELinux 布尔值是可更改 SELinux 策略行为的参数。SELinux 布尔值是可以启用或禁用的规则。安全管理员可以使用 SELinux 布尔值来有选择地调整策略。

selinux-policy-doc 软件包附带的 SELinux man page 中介绍了可用布尔值的用途。使用 **man -k '_selinux'** 命令可以列出这些 man page。

用于管理 SELinux 布尔值的命令包括：**getsebool** - 列出布尔值及其状态；**setsebool** - 修改布尔值；**setsebool -P** - 更改 SELinux 策略以使修改持久保留。**semanage boolean -l** 将报告布尔值是否为持久值，并提供该布尔值的简短描述。

非特权用户可以运行 **getsebool** 命令，但只有超级用户才能运行 **semanage boolean -l** 和 **setsebool -P**。

```
[user@host ~]$ getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
...output omitted...
[user@host ~]$ getsebool httpd_enable_homedirs
httpd_enable_homedirs --> off
```

```
[user@host ~]$ setsebool httpd_enable_homedirs on
Could not change active booleans. Please try as root: Permission denied
[user@host ~]$ sudo setsebool httpd_enable_homedirs on
[user@host ~]$ sudo semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (on   ,  off)  Allow httpd to enable homedirs
[user@host ~]$ getsebool httpd_enable_homedirs
httpd_enable_homedirs --> on
```

-P 选项可将所有待定值写入策略，使其在重启后持久保留。在下例中，请注意括号中的值：二者现在都设为 **on**。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

```
[user@host ~]$ setsebool -P httpd_enable_homedirs on
[user@host ~]$ sudo semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (on   ,   on)  Allow httpd to enable homedirs
```

要列出当前状态与默认状态不同的布尔值，请运行 **semanage boolean -l -C**。

```
[user@host ~]$ sudo semanage boolean -l -C
SELinux boolean                State  Default Description

cron_can_relabel               (off   ,   on)  Allow cron to can relabel
```

参考文献

booleans(8)、**getsebool**(8)、**setsebool**(8)、**semanage**(8)、**semanage-boolean**(8) man page

海量视频题库 myitpub.com QQ:556546 2
www.52myit.com

指导练习

使用布尔值调整 SELINUX 策略

Apache 可以发布在用户主目录中托管的 Web 内容，但是 SELinux 默认阻止此操作。在本练习中，您将对允许 Apache 访问用户主目录的 SELinux 布尔值进行确定和更改。

成果

您应能够配置 Apache，以便从用户的主目录发布 Web 内容。

在你开始之前

在 workstation 上，以 student 用户身份并使用密码 student 进行登录。

在 workstation 上，运行 **lab selinux-booleans start** 命令。此命令将运行一个起始脚本，它将确定 servera 计算机是否可从网络访问。此外，它还将安装 httpd 服务并配置 servera 的防火墙，以允许进行 HTTP 连接。

```
[student@workstation ~]$ lab selinux-booleans start
```

1. 使用 **ssh** 命令，以 student 用户身份登录 servera。系统已配置为使用 SSH 密钥来进行身份验证，因此不需要提供密码。

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

2. 使用 **sudo -i** 命令，切换为 root 用户。student 用户的密码为 student。

```
[student@servera ~]$ sudo -i
[sudo] password for student: student
[root@servera ~]#
```

3. 要启用允许用户从其主目录发布 Web 内容的 Apache 功能，必须编辑 **/etc/httpd/conf.d/userdir.conf** 配置文件。注释掉将 **UserDir** 设为 **disabled** 的行并取消注释将 **UserDir** 设为 **public_html** 的行。

```
[root@servera ~]# vim /etc/httpd/conf.d/userdir.conf
#UserDir disabled
UserDir public_html
```

4. 使用 **grep** 命令确认更改。

海量视频题库 myitpub.com QQ:3565462
www.52myit.com