1 什么是SELinux

SELinux（Security Enhanced Linux 加强的安全linux）是基于MAC（Mandatory Access Control）演变而来，他的特性之一是**最小权限集合**，也就是让一个进程运行，且在程序正常运行的前提下所能运行的最小权限集合中。**SELinux已经成为内核的一部分。**

2 SELinux的实现方式

SELinux通过定义许多的策略（policy）来控制一个进程运行后处于哪个domain中，这个domain包含哪些文件，对这些文件能够做出哪些操作。一个进程的权限不仅依赖于这个进程所携带的用户身份，还取决于SELinux的策略。

File Type

What actions？

Process domain

object

action

subject

3 SELinux类型

1 Strict mode：严格类型，所有的进程都受其控制

2 Targeted mode：目标类型，只控制部分进程。红帽所应用的模式，像httpd samba vsftpd 等都受selinux控制。

4 selinux的配置文件

**1 /etc/sysconfig/selinux** 开启或者关闭selinux，设定selinux的类型

2 /etc/selinux/targeted/plicy/ 策略设置。

5 如何查看每个文件或者每个进程的selinux特性？

查看文件安全上下文：ls -Z

User identity : Role(类似于组) : type(文件安全上下文类型)

查看进程domain：ps -Z | -auxZ

6 如何设置selinux？

1 selinux运行时有两种状态enforcing（违规操作会被拒绝，并记录到/var/log/audit/audit.log）和permissive（不拒绝，只记录）

2 setenforce 0或者1（关闭或者开启selinux）

3 echo 0 > /selinux/enforce (因为selinux属于内核，所以红帽在/下创建了一个selinux目录的伪文件系统来方便用户与selinux交互)关闭selinux。

4 chcon 修改文件的安全上下文类型

5 boolean 布尔值（0/1）

Getsebool -a 查看所有进程的布尔开关，通过调整这些开关可以改变某些进程的部分策略。

6 restorecon 恢复文件或者目录的默认的安全上下文

7 semanage 管理selinux。