SELinux

chcon -R -t（上下文类型） 将默认的主页路径改变，此时因为安全上下文不一致，selinux阻止服务启动，我们可以修改新的路劲安全上下文，让它和原服务一致，参数-R表示递归 -t表示类型，指明上下文的类型
chcon -R --reference=/var/lib/ /tmp/xx 对安全上下文不能熟练书写，可以通过引用参考的方式来生成，参数--referenc表示引用，这里的意思是引用/var/lib/这个目录的安全上下文给xx

Selinux布尔值

Audit2way
selinux NASA fedora，MAC（mandatory access control）强制访问控制，DAC（ Discretionary accesscontrol） 自主访问控制 0-day
selinux的控制策略不可见、策略的更改无需重启、可以从程序包括进程一直到目录的继承做完全的控制、控制范围包括文件系统、目录、文件、网卡、端口等等
安全上下文（Security context）：对特定的服务特定的进程限制用户特定的访问
身份、角色、类型
[root@hf /]# yum install setool* -y 安装selinux工具
[root@hf /]# vim /etc/sysconfig/selinux selinux的配置文件
selinux有三种模式，enforcing和perimissive和disabled，enforing是强制，最高级别，permissive是警告，不限制级别。disabled是关闭selinux ，只有这个模式设置后需要重启才能生效。
SELINUXTYPE有两种，一种是strict，一种是targeted。targeted是红帽默认使用的模式，这种模式限制级别主要是针对网络上的服务，本地限制很少。strict是美国国家安全局的标准，这种模式相对来说非常严格，完全性的限制。红帽的系统默认不支持这种模式。
[root@hf /]# getenforce 查看selinux当前的模式
[root@hf /]# setenforce 0
[root@hf /]# setenforce Permissive 改为警告模式
以上的修改都是临时有效。重启即失效
[root@hf /]# chcon -R --reference=/tmp/ /var/www/html/
改变目录的安全上下文，-R表示递归，--reference表示引用，这里的意思就是引用/tmp目录的安全上下文，将它的值赋予给apache的目录
[root@hf /]# restorecon /var/www/html/ -R 还原系统默认的安全上下文
除了安全上下文来控制目录和文件系统外，selinux还提供了布尔值来控制服务和进程
[root@hf booleans]# yum install setroubleshoot -y 安装selinux图形化警报工具
[root@hf booleans]# sealert -b 打开selinux的警告功能
[root@hf booleans]# getsebool -a 查看当前系统的布尔值
[root@hf booleans]# setsebool allow_ftpd_full_access on
[root@hf booleans]# setsebool allow_ftpd_full_access=0
以上两种输入都可以执行，结果是一样的。0表示关，1表示开。
命令行做的修改都是临时生效，如果希望永久更改布尔值，
[root@hf booleans]# setsebool -P allow_ftpd_full_access=0 参数-P表示写入配置，写入需要一些时间，不会立即生效。

[root@hf booleans]# yum whatprovides */system-config-selinux 查找什么软件包提供了这个命令，然后安装这个软件包，这个软件包是selinux的图形化管理工具

Security enhanced linux中文译为安全强化的linux。我们称为selinux，它是美国国家安全局联合NASA包括fedora社区等团体共同开发的一个Linux的安全子系统。
DAC（discretionary access control）自主访问控制就是根据文件的属性来实现读取写入的权限。Selinux使用的是MAC的控制方式。MAC全称是Mandatory Access Control（强制访问控制）
Selinux控制的程序，它最终的目标是针对这个程序可以读取的文档。
Selinx分为主体和客体。主体就是一个程序或者一个进程。客体是一个程序可以运行的文件的属性、可以是一个端口、可以是一组设备。
Selinux还要提供策略（policy），因为程序或者文件在系统中数量是非常庞大的，所有必须提供一个安全的机制策略来实现控制。这些机制策略会提供不同的规则来控制对程序或者文件的安全操作。Selinux在RHEL中的策略有target（主要提供针对网络服务的限制）、mls（rhel6中称为strict，提供完整的限制，非常非常严格，红帽不支持这种策略，这个策略来自美国国家安全）、minimum（RHEL7中提供的由target修订而来的策略，提供有选择的程序的保护）。
Selinux对服务或程序的控制通过安全上下文（Security context）。Selinux定义主体和客体的安全上下文必须一致才可以安全访问。可以通过命令ls -lZ查看文件或者目录的安全上下文。安全上下文由三段内容组成：身份、角色、类型。身份和我们的账号类似，角色一般有 object_r（代表文件或者目录）、system_r（代表的就是程序或者说服务），类型在红帽的target策略中是最重要的，target策略下的selinux基本都是通过类型来判断程序或者服务的访问的。分为文件级别的类型和程序基本的类型。
[root@server /]# yum install setools* -y //安装setool工具，它提供了selinux方面的很多查看工具
[root@server /]# ps -eZ //查看系统程序的selinux安全上下文
[root@server /]# vim /etc/selinux/config //查看selinux的主配置文件
Selinux有三种状态，第一个是enforcing，表示强制状态，这个状态下selinux会阻止一切非法操作。第二个状态时permissive状态，表示警告状态，这个状态下selinux对于非法操作会提出警告，但不会阻止。第三个状态时disabled状态，这个状态下selinux被关闭。
注意：如果设置为disabled状态，必须重启系统才能生效，而在RHEL7中，如果频繁改动selinux 的状态，系统会冻住我们操作的权限。
[root@server /]# sestatus //查看selinux当前的状态
如果我们需要修改selinux的启动状态，直接可以在/etc/selinux/config这个文件中修改
[root@server /]# getenforce //查看当前的selinux状态
[root@server /]# setenforce 1 //当当前的模式修改为enforcing模式，等同于setenforce enforcing命令，这个命令临时有效。如果希望状态修改永久生效，只能修改配置文件。
Selinux还提供额外的布尔值：
[root@server booleans]# ls /selinux/booleans/ //查看系统中selinux默认的布尔值，等同于命令seinfo -b
[root@server booleans]# getsebool -a //查看默认的布尔值的开关情况
[root@server booleans]# setsebool allow_ftpd_anon_write on //设置某一个布尔值开，临时生效
[root@server booleans]# setsebool -P allow_ftpd_anon_write=0 //设置某一个布尔值关，永久生效

验证selinux的阻止方式：
[root@server /]# yum install httpd* -y   //安装一个apache服务器
将默认的主页路径改变，此时因为安全上下文不一致，selinux会阻止apache服务启动。
[root@server /]# chcon -R -t httpd_sys_content_t /tmp/xx/   //修改主页新的路径的安全上下文，让它和apache服务一致。参数-R表示递归，-t表示type，指明安全上下文的类型
[root@server /]# chcon -R --reference=/var/lib/ /tmp/xx/   //如果对安全上下文并不能熟练书写，可以通过引用参考的方式来生成。选项--reference表示引用，这里的意思是引用/var/lib这个目录的安全上下文并赋予给/tmp/xx
[root@server /]# restorecon -R /var/www/html   //恢复默认的安全上下文，只能够针对网络服务来提供
安装图形化selinux管理工具：
[root@server booleans]# yum whatprovides */system-config-selinux   //查看哪个软件包提供的命令
[root@server booleans]# yum install policycoreutils-gui-2.0.83-19.39.el6.x86_64 -y   //安装图形化selinux工具
[root@server booleans]# system-config-selinux   //通过命令打开图形化selinux工具
安装selinux排除工具：
[root@server booleans]# yum install setroubleshoot -y   //安装selinux排除工具

SELinux端口安全测试
[root@test ~]# yum install httpd -y
[root@test ~]# systemctl status firewalld # 查看防火墙的状态
[root@test ~]# firewall-cmd --list-all # 列出当前的规则
[root@test ~]# firewall-cmd --add-service=http #临时允许访问本地的http服务
[root@test ~]# firewall-cmd --add-service=http --permanent # 永久允许访问本地的http服务

[root@test ~]# systemctl status firewalld
[root@test ~]# vim /etc/httpd/conf/httpd.conf # 修改端口号
Listen 888

[root@test ~]# getenforce

[root@test ~]# systemctl restart httpd
[root@test ~]# systemctl status httpd.service # 由于SELinux的原因，导致端口号不能修改
[root@test ~]# semanage port -l |grep 80 # 查看80端口对应的安全上下文信息
[root@test ~]# semanage port -a -t http_port_t -p tcp 888

[root@test ~]# firewall-cmd --add-port=888/tcp
[root@test ~]# firewall-cmd --add-port=888/tcp --per

[root@test ~]# cd /var/www/html/ # 网站的默认的根目录
[root@test html]# touch index.html
[root@test html]# vim index.html

客户端测试