SELINUX

SELinux

Security Enhanced Linux 安全强化的 Linux

作用

强制限制某些操作，属于权限的一种

思考：到目前为止学过的 linux 中的权限？

u\g\o r\w\x ssid\sgid\stid acl attr

配置文件

/etc/selinux/config

```
[#15#root@rhel6 ~]#ll /etc/selinux/config
-rw-r--r--. 1 root root 458 Jul 2 2015 /etc/selinux/config
[#16#root@rhel6 ~]#ll /etc/sysconfig/selinux
lrwxrwxrwx. 1 root root 17 Jul 2 2015 /etc/sysconfig/selinux -> ../selinux/config
[#17#root@rhel6 ~]#cat /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values: 【三种状态】
# enforcing - SELinux security policy is enforced. 【打开 selinux ，并强制限制】
# permissive - SELinux prints warnings instead of enforcing. 【打开 selinux ，不限制操作 ，但会警告】
# disabled - No SELinux policy is loaded. 【关闭 selinux 】
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values: 【两种类型】
# targeted - Targeted processes are protected, 【针对网络服务较多 ，针对主机较少】
# mls - Multi Level Security protection. 【全方位的控制】
SELINUXTYPE=targeted
```

重启电脑后生效，并永久生效

相关指令

- 查看当前 selinux 状态的命令 : getenforce/sestatus
- 设置 selinux 状态 (临时生效): setenforce [Enforcing | Permissive | 1 | 0]

```
[#12#root@rhel6 ~]#getenforce
Enforcing
[#13#root@rhel6 ~]#sestatus
SELinux status:
enabled
SELinuxfs mount:
/selinux
Current mode:
enforcing
Mode from config file:
enforcing
Policy version:
28
Policy from config file:
targeted
[root@rhel7 ~]# setenforce 0
[root@rhel7 ~]# getenforce
Permissive
[root@rhel7 ~]# sestatus
SELinux status:
enabled
SELinuxfs mount:
/sys/fs/selinux
SELinux root directory:
/etc/selinux
Loaded policy name:
targeted
Current mode:
permissive
Mode from config file:
enforcing
Policy MLS status:
enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28
[root@rhel7 ~]# which getenforce
/usr/sbin/getenforce
[root@rhel7 ~]# rpm -qf /usr/sbin/getenforce
libselinux-utils-2.2.2-6.el7.x86_64
[root@rhel7 ~]# rpm -ql libselinux-utils|head
/usr/sbin/avcstat
/usr/sbin/getenforce
/usr/sbin/getsebool
/usr/sbin/matchpathcon
/usr/sbin/selinuxconlist
/usr/sbin/selinuxdefcon
/usr/sbin/selinuxenabled
/usr/sbin/selinuxexeccon
/usr/sbin/setenforce
/usr/share/man/man5/booleans.5.gz
[root@rhel7 ~]# which sestatus
/usr/sbin/sestatus

[root@rhel7 ~]# rpm -qf /usr/sbin/sestatuspolicycoreutils-2.2.5-11.el7.x86_64
```

```
[root@rhel7 ~]# rpm -ql policycoreutils|head
/etc/sestatus.conf
/usr/bin/secon
/usr/sbin/fixfiles
/usr/sbin/genhomedircon
/usr/sbin/load_policy
/usr/sbin/restorecon
/usr/sbin/semodule
/usr/sbin/sestatus
/usr/sbin/setfiles
/usr/sbin/setsebool
```

操作限制的实现方法

1. 通过 bool 值来进行操作的限制

- 1>getsebool -a <== 显示主机中所有的布尔值
- 2>setsebool [-PV] boolean value | bool1=val1 bool2=val2 ...

1. 通过安全上下文

```
[#19#root@rhel6 ~]#ls -Z
-rw-------. root root system_u:object_r:admin_home_t:s0 anaconda-ks.cfg
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Desktop
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Documents
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Downloads
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 index.php3?stat=26
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log.syslog
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Music
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Pictures
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Public
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 root@172.25.0.10
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Templates
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Videos
```

安全上下文主要用冒号分为三个字段：

Identify:role:type

身份识别：角色：类型1.5 selinux 所需要的服务

setroubleshoot

```
[#40#root@rhel6 ~]#yum install -y setroubleshoot
[#42#root@rhel6 ~]#rpm -ql setroubleshoot-server|head
/etc/audisp/plugins.d/sedispatch.conf
/etc/dbus-1/system.d/org.fedoraproject.SetroubleshootFixit.conf
/etc/dbus-1/system.d/org.fedoraproject.Setroubleshootd.conf
/etc/logrotate.d/setroubleshoot
/etc/setroubleshoot
/etc/setroubleshoot/setroubleshoot.conf

/usr/bin/sealert
```

setroubleshot 将 selinux 相关的错误信息和解决方法记录在 /var/log/messages 日志中。`cat /var/log/messages | grep setroubleshoot`

auditd

- auditd --> 将 selinux 相关的信息记录在 /var/log/audit/audit.log 日志中,非常详细。
- sealert -a /var/log/audit/audit.log

selinux-policy-devel

el6 上没有该软件

```
[root@rhel7 ~]# yum list|grep selinux-policy-devel
selinux-policy-devel.noarch 3.12.1-153.el7 server

[#64#root@rhel6 ~]#yum list|grep selinux-policy-devel
This system is not registered to Red Hat Subscription Management. You can use subscription-
manager
to register.
```

`man` 关键词 `_selinux` 查找和关键字相关的 `selinux` 限制具体内容，包括什么打开什么布尔值，需要设置怎样的安全上下文。