马哥教育
最专业的Linux培训机构

SELinux

http://www.magedu.com

本章内容

- SELinux概念
- 启用SELinux
- 管理文件安全标签
- 管理端口标签
- 管理SELinux布尔值开关
- 管理日志
- 查看SELinux帮助

SELinux介绍

- SELinux：Secure Enhanced Linux， 是美国国家安全局(NSA=The National Security Agency)和SCC(Secure Computing Corporation)开发的 Linux的一个强制访问控制的安全模块。2000年以GNU GPL发布，Linux内核2.6版本后集成在内核中
- DAC：Discretionary Access Control自由访问控制
- MAC：Mandatory Access Control 强制访问控制
  - DAC环境下进程是无束缚的
  - MAC环境下策略的规则决定控制的严格程度
  - MAC环境下进程可以被限制的
  - 策略被用来定义被限制的进程能够使用那些资源（文件和端口）
  - 默认情况下，没有被明确允许的行为将被拒绝

SELinux工作类型

- SELinux有四种工作类型：
- strict：centos5,每个进程都受到selinux的控制
- targeted：用来保护常见的网络服务,仅有限进程受到selinux控制，只监控容易被入侵的进程，rhel4只保护13个服务，rhel5保护88个服务
- minimum：centos7,修改过的targeted，只对选择的网络服务
- mls:提供MLS（多级安全）机制的安全性
- minimum和mls稳定性不足，未加以应用

SELinux安全上下文

- 传统Linux，一切皆文件，由用户，组，权限控制访问
- 在SELinux中，一切皆对象（object），由存放在inode的扩展属性域的安全元素所控制其访问
- 所有文件和端口资源和进程都具备安全标签：安全上下文（security context）
- 安全上下文有五个元素组成：
  - user:role:type:sensitivity:category
  - user_u:object_r:tmp_t:s0:c0
- 实际上下文：存放在文件系统中，ls -Z;ps -Z
- 期望(默认)上下文：存放在二进制的SELinux策略库（映射目录和期望安全上下文）中

```
semanage fcontext -l
```

五个安全元素

- User:指示登录系统的用户类型,如root，user_u,system_u，多数本地进程都属于自由（unconfined）进程
- Role:定义文件，进程和用户的用途：文件:object_r，进程和用户：system_r
- Type:指定数据类型，规则中定义何种进程类型访问何种文件Target策略基于type实现,多服务共用：public_content_t
- Sensitivity:限制访问的需要，由组织定义的分层安全级别，如unclassified， secret,top,secret，一个对象有且只有一个sensitivity,分0-15级，s0最低,Target策略默认使用s0
- Category：对于特定组织划分不分层的分类，如FBI Secret，NSA secret，一个对象可以有多个categroy， c0-c1023共1024个分类， Target 策略不使用category

SELinux策略

- 对象(object)：所有可以读取的对象，包括文件、目录和进程，端口等
- 主体：进程称为主体(subject)
- SELinux中对所有的文件都赋予一个type的文件类型标签，对于所有的进程也赋予各自的一个 domain的标签。domain标签能够执行的操作由安全策略里定义。
- 当一个subject试图访问一个object，Kernel中的策略执行服务器将检查AVC (访问矢量缓存Access Vector Cache)，在AVC中，subject和object的权限被缓存(cached)，查找“应用+文件”的安全环境。然后根据查询结果允许或拒绝访问
- 安全策略：定义主体读取对象的规则数据库，规则中记录了哪个类型的主体使用哪个方法读取哪一个对象是允许还是拒绝的，并且定义了哪种行为是充许或拒绝

设置SELinux

- 配置SELinux：
  - SELinux是否启用
  - 给文件重新打安全标签
  - 给端口设置安全标签
  - 设定某些操作的布尔型开关
  - SELinux的日志管理
- SELinux的状态：
  - enforcing：强制，每个受限的进程都必然受限
  - permissive：允许，每个受限的进程违规操作不会被禁止，但会被记录于审计日志
  - disabled：禁用

配置SELinux

- 相关命令：

  getenforce：获取selinux当前状态

  sestatus ：查看selinux状态

  setenforce 0|1

    0：设置为permissive

    1：设置为enforcing

- 配置文件：

  /boot/grub/grub.conf

    使用selinux=0禁用SELinux

  /etc/sysconfig/selinux

  /etc/selinux/config

  SELINUX={disabled|enforcing|permissive}

修改SELinux安全标签

- 给文件重新打安全标签：

  chcon [OPTION]... [-u USER] [-r ROLE] [-t TYPE] FILE...

  chcon [OPTION]... --reference=RFILE FILE...

  -R：递归打标；

- 恢复目录或文件默认的安全上下文：

  restorecon [-R] /path/to/somewhere

默认安全上下文查询与修改

- semanage 来自 policycoreutils-python包
- 查看默认的安全上下文

```
semanage fcontext -l
```

- 添加安全上下文

```
semanage fcontext  -a -t httpd_sys_content_t '/testdir(/.*)?'
restorecon -Rv /testdir
```

- 删除安全上下文

```
semanage fcontext  -d -t httpd_sys_content_t '/testdir(/.*)?'
```

Selinux端口标签

- 查看端口标签

  semanage port -l

- 添加端口

  semanage port -a -t *port_label* -p *tcp|udp PORT*

  semanage port -a -t http_port_t -p tcp 9527

- 删除端口

  semanage port -d -t *port_label* -p *tcp|udp PORT*

  semanage port -d -t http_port_t -p tcp 9527

- 修改现有端口为新标签

  semanage port -m -t *port_label* -p *tcp|udp PORT*

  semanage port -m -t http_port_t -p tcp 9527

SELinux布尔值

- 布尔型规则：
  - getsebool
  - setsebool
- 查看bool命令：
  - getsebool [-a] [boolean]
  - semanage boolean -l
  - semanage boolean -l -C 查看修改过的布尔值
- 设置bool值命令：
  - setsebool [-P] boolean value（on,off）
  - setsebool [-P] Boolean=value（0，1）

SELinux日志管理

- yum install setroublesshoot*（重启生效）

将错误的信息写入/var/log/message

- grep setroubleshoot /var/log/messages
- sealert -l UUID

查看安全事件日志说明

- sealert -a /var/log/audit/audit.log

扫描并分析日志

SELinux帮助

- yum -y install selinux-policy-devel（centos7）
- yum -y install selinux-policy-doc （centos6）
- mandb | makewhatis
- man -k _selinux

练习

- 1、启用SELinux策略并安装httpd服务，改变网站的默认主目录为/website,添加SELinux文件标签规则，使网站可访问
- 2、修改上述网站的http端口为9527，增加SELinux端口标签，使网站可访问
- 3、启用相关的SELinux布尔值，使上述网站的用户student的家目录可通过http访问

关于马哥教育

- 博客：http://mageedu.blog.51cto.com
- 主页：http://www.magedu.com
- QQ：1661815153，113228115
- QQ群：203585050，279599283

马哥教育
最专业的Linux培训机构

Thank You!