# Linux SELinux配置详解

简介：

SELinux 是基于Linux内核的轻质访问控制机制实现，它是由美国国家安全局开发的项目，旨在增强传统Linux操作系统的安全性。使用SELinux后，系统中的文件、目录、设备甚至端口都作为对象，而用户运行的进程则被当作主题，一个主题能不能访问对象。首先系统会检查传统的账户权限是否允许（DAC控制权限），如果传统的基于账户访问的权限允许，才会检查SELinux的强访问控制（MAC访问控制），SELinux依靠策略来决定是否允许主题访问目标对象。

## 一，SELinux配置文件

在CentOS 7 系统中部署SELinux非常简单，由于SELinux已经作为模块集成到内核中，默认SELinux已经处于激活状态。CentOS系统中SELinux全局配置文件为/etc/sysconfig/selinux。

**[root@centos7 ~]# vim /etc/sysconfig/selinux**

**# This file controls the state of SELinux on the system.**

**SELINUX=disabled**

**# enforcing - SELinux security policy is enforced.**

**# permissive - SELinux prints warnings instead of enforcing.**

**# disabled - No SELinux policy is loaded.**

**#SELINUX=enforcing**

**# SELINUXTYPE= can take one of three two values:**

**# targeted - Targeted processes are protected,**

**# minimum - Modification of targeted policy. Only selected processes are protected.**

**# mls - Multi Level Security protection.**

**SELINUXTYPE=targeted**

全局配置文件中除去以#符号开头的注释行，有效配置参数仅两行。

SELinux=enforcing为SELinux总开关，有效值可以是enforcing、permissive或disabled。

disabled 代表禁用SELinux功能，由于SELinux是内核模块功能，所以设置禁用，需要重启计算机。

permissive 代表警告模式，处于此状态下时，当主题程序视图访问无权限的资源时，SELinux会记录日志但不会拦截该访问，也就是最终访问时成功的，只是在SELinux日志中记录而已。

enforcing 代表强制开启，SELinux会拦截非法的资源访问并记录相关日志。

SELINUXTYPE=targeted设置项，用来设置SELinux类型。可以设置为targeted类型或者mls类型。

targeted 类型主要对系统中的服务进程进行访问控制。

mls 类型将对系统中的所有进程进行控制，启用mls后，用户执行简单的命令（如ls）都会报错。

使用setenforce可以临时在enforcing模式与permissive模式之间切换，切换会被立刻应用于当前系统，计算机重启后无效，永久修改模式需要修改配置文件。

**[root@centos7 ~]# setenforce 0 # 设置SELinux为permissive模式**

**[root@centos7 ~]# setenforce 1 # 设置SELinux为enforcing模式**

## 二，SELinux安全上下文

SELinux会为进程与文件添加安全信息标签，如：SELinux 用户、角色、类型以及可选的级别。当运行SELinux后所有这些信息都是访问控制的依据。

对于文件或文件夹，可以使用命令“ls -Z”查看上下文信息，而“ps aux -Z”则可以查看进程的安全上下文信息。

[root@centos7 ~]# ls -Z anaconda-ks.cfg

**-rw-------. root root system\_u:object\_r:admin\_home\_t:s0 anaconda-ks.cfg**

[root@centos7 ~]# ps aux -Z

SELinux的安全上下文包括

用户： 角色： 类型： 级别

每列具体描述如下：

1. SELinux用户

用户身份是通过SELinux策略授权特定角色集合的账户身份，每个系统账户都通过策略映射到一个SELinux用户。使用root身份运行 semanage login -l 命令查看系统账户与SELinux账户之间的映射关系。

[root@centos7 ~]#semanage login -l

登录名 SELinux 用户 MLS/MCS 范围 服务

\_\_default\_\_ unconfined\_u s0-s0:c0.c1023 \*

root unconfined\_u s0-s0:c0.c1023 \*

system\_u system\_u s0-s0:c0.c1023 \*

1. SELinux角色

SELinux部分采用基于角色的访问控制（RBAC）模型，而角色是RBAC的重要属性。SELinux账户被授予特定的角色，而角色被授予操控特定的域。角色是SELinux用户与域的媒介。

1. SELinux类型

SELinux类型是Type ENforcement的重要属性，类型定义了进程的域以及文件的类型。而SELinux策略规则定义了何种类型的主题可以访问其他何种类型的对象资源，仅当SELinux策略明确存在允许规则时，访问才可以被接受。

1. SElinux级别

级别MLS 和 MCS的属性，一个MLS方位是一对级别，书写格式为低级别-高级别，如果两个级别是一致的，也可以仅显示低级别，如，s0-s0与s0是一样的。

当我们使用passwd命令修改账户密码时，系统会运行/usr/bin/passwd程序，该程序运行在passwd-exec\_t域中，修改密码需要修改/etc/shadow文件，而该文件的类型为shadow\_t，SELinux默认的策略规则中允许运行在psswd\_t域中进程读写被标记为shadow\_t类型的文件。

## 三，SELinux排错

不管SELinuxc策略是允许还是拒绝资源的访问请求行为，都会记录日志，也就是AVC（Access Vector Cache）。所有SELinux拒绝的消息都会被记录进日志，根据系统中安装运行的服务进程不同，拒绝日志消息会被记录打怕不通的文件中。

进程与日志文件的关系：

日志文件 进程

/var/log/audit/audit.log auditd服务开启

/var/log/messages auditd服务关闭，rysylogd服务开启

/var/log/audit/audit.log ,/var/log/messages 安装setroubleshoot相关软件包

autitd与rsyslogd同时开启

若想恢复文件的安全上下文，可以使用命令“/sbin/restorecon -v 文件绝对路径”。

## 四，修改安全上下文

有多重方式可以修改与管理SELinux安全上下文，如：chcon、semanage、fcontext以及restorecon命令。

### 1，chcon命令

描述：修改文件SELinux安全上下文

用法：chcon [选项] [-u SELinux用户] [-r 角色] [-l 范围] [-t 类型] 文件

chcon [选项] --reference=参考文件 文件

选项：

-u 修改用户属性

-r 修改角色属性

-l 修改范围属性

-t 修改类型属性

示例：

1. 修改文件安全上下文

[root@centos7 ~]# cp --preserve=all /etc/passwd /root

# 复制文件（保留上下文信息）

[root@centos7 ~]# ls -Z /root/passwd

# 查看文件SELinux安全上下文

[root@centos7 ~]# chcon -t admin\_home\_t /root/passwd

# 修改文件安全上下文中的类型

[root@centos7 ~]# ls -Z /root/passwd

1. 修改目录上下文

[root@centos7 ~]# chcon -R -t admin\_home\_t /root/

# 递归修改目录安全上下文

1. 根据参考文件修改目标文件安全上下文

[root@centos7 ~]# chcon --reference=/etc/passwd /root/passwd

通过chcon修改的安全上下文并不是SELinux预设的安全上下文，当文件系统充值SELinux安全标签或使用restorecon命令充值指定目录的安全标签后，所有文件与目录的安全标签会被还原为系统的预设值，如果需要就该SELinux默认的预设安全上下文，需要使用semanage命令添加或修改。

### 2，semanage命令

描述：SELinux策略管理工具

用法：semanage fcontext [-S store] -{a|d|m|l|n|D} [-frst] file\_spec

选项：

-a,--add 添加预设安全上下文

-d,--delete 删除指定的预设安全上下文

-D,--deleteall 删除所有的预设自定义上下文

-m,--modify 修改指定的预设安全上下文

-l,--list 显示预设安全上下文

-n,--noheading 不显示头部信息

示例：

1. 查看SELinux策略默认的预设安全上下文信息，系统将列出策略中定义的所有目录与安全上下文信息。

[root@centos7 ~]# semanage fcontext -l

1. 修改策略，添加一条新的预设安全上下文信息

[root@centos7 ~]# semanage fcontext -a -t samba\_share\_t /test/test.txt

[root@centos7 ~]# mkdir /test; touch /test/test.txt

[root@centos7 ~]# ls -Z /test/test.txt

1. 使用restorecon命令，还原test.txt文件的安全上下文为预设值

[root@centos7 ~]# restorecon /test/test.txt

[root@centos7 ~]# ls -Z /test/test.txt

1. 递归设置目录的预设安全上下文

[root@centos7 ~]# semanage fcontext -a -t httpd\_sys\_content\_t "/site/www(/.\*)?"

[root@centos7 ~]# mkdir -p /site/www/{web1,web2}

[root@centos7 ~]# touch /site/www/{web1,web2}/index.php

[root@centos7 ~]# ls -RZ /site/www

[root@centos7 ~]# restorecon -R /site/

1. 删除预设安全上下文

[root@centos7 ~]# semanage fcontext -d /test/test.txt

1. 检查预设SELinux安全上下文

[root@centos7 ~]# matchpathcon /site/www/

## 五，查看与修改布尔值

SELinux布尔值可以实时被修改。

getsebool是用来查看SELinux布尔值的命令，用法比较简单，-a选项用来查看所有的布尔值。显示数据中左侧为关键词，右侧为开关，on代表开，off代表关。

除了getsebool命令外，还可以使用semanage boolean -l 命令，该命令的输出结果与getsebool命令相比，输出信息多了默认状态与当前状态以及相关描述信息。

修改SELinux布尔值状态也非常检点，使用setsebool name X 即可实现。

其中,name是布尔值名称，X代表on或off。

默认setsebool命令修改的布尔值参数会立即生效，但计算机重启后会被还原，如果希望永久修改，需要使用-p参数。

[root@centos7 ~]# setsebool ftp\_home\_dir on

[root@centos7 ~]# setsebool -p ftp\_home\_dir on

小知识：

实际应用中，建议管理员先将SELinux模式调整我permissive模式，经过大量的测试后，再实际部署带生产环境。在部署SELinux环境的过程中，遇到问题可以参考各种日志文件，另外，CentOS7 系统中还提供了专门的SELinux帮助文档，这些帮助文件多数以\_selinux结尾。使用man -k key命令可以帮助我们查看某个关键词相关的帮助手册。但前提是系统已经使用makewhatis创建了whatis数据库。

[root@centos7 ~]# makewhatis # 生成whatis数据库

[root@centos7 ~]# man -k selinux # 查找selinux相关帮助

[root@centos7 ~]# man -k selinux | grep ftp # 查找与ftp相关的SELInux帮助

1. httpd相关SELinux安全策略

1，布尔值

SELinux策略是可定制的，SELinux针对httpd的策略非常灵活，大量的布尔值可以帮助管理员快速维护与管理相关策略，实现安全快捷的访问策略。

允许httpd脚本或模块通过网络连接数据库：

[root@centos7 ~]# setsebool -P httpd\_can\_net-work\_connect\_db 1

允许httpd支持CGI程序：

[root@centos7 ~]# setsebool -P httpd\_enable\_cgi 1

允许httpd访问cifs文件系统资源：

[root@centos7 ~]# setsebool -P httpd\_usr\_cifs 1

允许Apache使用mod\_auto\_pam模块：

[root@centos7 ~]# setsebool -P allow\_httpd\_mod\_auth\_pam 1

允许httpd访问NFS文件系统资源：

[root@centos7 ~]# setsebool -P httpd\_use\_nfs 1

允许httpd守护进程发送电子邮件：

[root@centos7 ~]# setsebool -P httpd\_can\_sendmail 1

允许httpd连接网络memcache服务器：

[root@centos7 ~]# setsebool -P httpd\_can\_network\_memcache 1

2，安全上下文

如果希望多个进程域（如，Apache、FTP、rsync等）共享相同的文件，我们可以设置文件安全上下文为public\_content\_t 或者 public\_content\_rw\_t，这些安全上下文允许上面提到的所有服务进程域读文件内容，如果修改为可以读写，则需要public\_content\_rw\_t的类型标签。

[root@centos7 ~]# semanage fcontext -a -t public\_content\_t "/var/httpd(/.\*)?"

[root@centos7 ~]# restorecon -F -R -v /var/httpd

通过添加public\_content\_rw\_t类型标签，允许httpd可读可写/var/web目录及子目录。

注意，该设置需要开启布尔值allow\_httpd\_anon\_write:

[root@centos7 ~]# semanage fcontext -a -t public\_content\_rw\_t "/var/web(/.\*)?"

[root@centos7 ~]# restorecon -F -R -v /var/httpd/incoming

具体的文件与目录资源的安全上下文描述信息：

文件与目录描述 安全上下文类型标签

/var/cache 缓存目录资源 httpd\_cache\_t

Apache配置 httpd\_config\_t

作为CVS内容的文件资源 httpd\_cvs\_content\_t

Apache 日志文件资源 httpd\_log\_t

httpd 代理内容资源 httpd\_squid\_content\_t

httpd系统资源 httpd\_sys\_content\_t

可读写httpd系统资源 httpd\_sys\_rw\_content\_t

1. FTP相关的SELinux安全策略

1，布尔值

允许ftp对用户家目录中的数据：

[root@centos7 ~]# setsebool -P ftp\_home\_dir 1

允许本地账号登陆ftp可以读写文件系统中的所有文件：

[root@centos7 ~]# setsebool -P allow\_ftpd\_full\_access 1

允许ftp连接数据库：

[root@centos7 ~]# setsebool -P ftpd\_connect\_db 1

允许ftp共性cifs文件系统：

[root@centos7 ~]# setsebool -P allow\_ftpd\_use\_cifs 1

允许ftp共享NFS文件系统：

[root@centos7 ~]# setsebool -P allow\_ftpd\_use\_nfs 1

2，安全上下文

添加预设的SELinux安全上下文的类型属性，允许ftp读取/var/ftp目录：

[root@centos7 ~]# semanage fxontext -a -t public\_content\_t "/var/ftp(/.\*)?"

[root@centos7 ~]# restorecon -F -R -v /var/ftp

添加预设的SELinux安装上下文的类型属性，允许ftp读写/var/ftp目录：

[root@centos7 ~]# semanage fcontext -a -t public \_content\_rw\_t "/var/ftp(/.\*)?"

[root@centos7 ~]# restorecon -F -R -v /var/ftp

1. MYSQL相关的SELinux安全策略

1，布尔值

允许用户连接mysql服务器：

[root@centos7 ~]# setsebool -P allow\_user\_mysql\_connect 1

允许mysqld服务连接所有的端口号：

[root@centos7 ~]# setsebool -P mysql\_connect\_any 1

2，安全上下文

文件与目录描述 安全上下文类型标签

mysql数据库文件 mysqld\_db\_t

存储在/etc/目录下的mysql文件 mysqld\_etc\_t

控制mysql程序仅在mysqld\_t域中运行 mysqld\_exec\_t

控制mysql程序仅在mysqld\_initrc\_t域中运行 mysqld\_initrc\_exec\_t

ftp在/tmp目录下生成的临时文件 ftpd\_tmp\_t

控制mysql程序仅在mysqld\_safe\_t域中运行 mysqld\_safe\_exec\_t

mysql存储在/tmp目录下的临时文件 mysqld\_tmp\_t

mysql存储在/var/run目录下的文件 mysqld\_var\_run\_t

1. NFS相关的SELinux安全策略

1，布尔值

允许ftp服务器使用NFS文件系统共享：

[root@centos7 ~]# setsebool -P allow\_ftpd\_use\_nfs 1

允许Git京城访问NFS文件系统：

[root@centos7 ~]# setsebool -P git\_system\_use\_nfs 1

允许qemu使用NFS文件系统：

[root@centos7 ~]# setsebool -P qemu\_use\_nfs 1

允许rsync服务器共享NFS文件系统：

[root@centos7 ~]# setsebool -P rsync\_use\_nfs 1

允许Cobbler访问NFS文件系统：

[root@centos7 ~]# setsebool -P cobbler\_use\_nfs 1

2，安全上下文

文件与目录描述 安全上下文类型标签

nfs数据文件 nfs\_t

控制NFS程序仅在nfsd\_t域中运行 nfsd\_exec\_t

控制NFS程序仅在nfsd\_initrc\_exec\_t域中运行 nfsd\_initrc\_exec\_t

设置文件为只读NFS文件 nfsd\_ro\_t

设置文件为可读可写NFS文件 nfsd\_rw\_t

1. Smaba相关的SELinux安全策略

1，布尔值

允许samba作为域控制添加账户和修改密码：

[root@centos7 ~]# setsebool -P samba\_domain\_controller 1

允许samba以只读方式共享任意文件或目录：

[root@centos7 ~]# setsebool -P samba\_export\_all\_ro 1

允许samba以可读可写方式共享任意文件或目录：

[root@centos7 ~]# setsebool -P samba\_export\_all\_rw 1

开启samba家目录：

[root@centos7 ~]# setsebool -P use\_samba\_home\_dirs 1

允许smabe共享账户家目录：

[root@centos7 ~]# setsebool -P samba\_enable\_home\_dirs 1

2，安全上下文

文件与目录描述 安全上下文类型标签

samba存储在/etc/目录下的文件 samba\_etc\_t

samba存储在/tmp/目录下的文件 samba\_net\_tmp\_t

samba存储在/var/目录下的文件 samba\_var\_t

samba密码文件 samba\_secrets\_t

samba共享文件 samba\_share\_t

samba日志文件 samba\_log\_t

控制samba程序仅在samba\_initrc\_t域中运行 samba\_initrc\_exec\_t

控制samba程序仅在samba\_net\_t域中运行 samba\_net\_exec\_t