

Linux中的用户、组和权限

一，Linux的安全模型

1.安全3A

Authentication(认证),Authorization(授权),Accounting(审计)(AAA)是用于对计算机资源的访问、策略执行、审计使用情况和提供服务账单所需信息等功能进行智能控制的基本组件的一个术语。大多数人认为这三个组合的过程对有效的网络管理和系统安全管理非常重要。

第一步，认证策略提供了辨识某个用户的方法，一般是在认证成功之前要求用户输入一个合法的用户名和有效的密码。认证的过程有赖于每个用户拥有获取访问权的唯一标准，AAA服务会拿该标准（密码）和数据库中的密码对比，如果匹配，则允许其访问计算机；否则，认证失败拒绝访问。

第二步，认证完成后，用户必须得到授权才能做特定的事情和处理相关任务。在登录某个系统后，用户可能会尝试运行相关的命令。授权的进程会决定用户是否有运行该命令的权利。简单说，授权就是实施策略的过程：即是确定允许用户使用哪种类型或质量的活动、资源或服务的过程。通常，授权发生在认证的上下文环境中。一旦你认证了某个用户也就意味着该用户也被授权了不同种类的访问和活动。

在AAA框架中最后的一项是审计，意思是需要监控和测量在访问的过程中的资源使用情况。身份认证、授权和审计服务通常由专用的AAA服务提供，AAA服务是执行这些功能的程序。

2.用户登录linux的背后发生了什么

二，Linux系统中用户和组及相关的文件

1.linux系统中的用户类型

- 一般linux用户分为管理员和普通用户，root用户为超级管理员 1，超级管理员默认名称为：root；其UID为：0 2，普通用户的UID：1-60000 系统自动分配；分为：系统用户和登录用户 系统用户：1-499（CentOS6），1-999（CentOS7）系统用户负责对守护进程获取资源进行权限分配 登录用户：500+，1000+（CentOS7）使用交互式登录

2.linux中的用户组

管理员组的组ID(GID)也为0，叫root组(即使你把其他用户加入root组，他任然是普通用户) 普通组分为系统组和普通组： 系统组：1-499, 1-999（CENTOS7） 普通组：500+, 1000+（CENTOS7）

Linux组的类别

用户的主要组(primary group)

用户必须属于一个且只有一个主组,组名同用户名,且仅包含一个用户,私有组

用户的附加组(supplementary group)

一个用户可以属于零个或多个辅助组

3.Linux用户和组的主要配置文件

- 用户和组的配置文件都位于/etc文件夹下

/etc/passwd: 保存用户及其属性信息(名称、UID、主组ID等)
/etc/group: 保存组及其属性信息
/etc/shadow: 保存用户密码及其相关属性
/etc/gshadow: 保存组密码及其相关属性

- passwd文件格式

passwd文件格式:

1:2:3:4:5:6:7 # 每个用户使用一行特定格式的文本记录
1:login name: 登录用名 (steve)
2:passwd: 密码 (x)
3:UID: 用户身份编号 (1000)
4:GID: 登录默认所在组编号 (1000)
5:GECOS: 用户全名或注释
6:home directory: 用户主目录 (/home/steve)
7:shell: 用户默认使用shell (/bin/bash)

- shadow文件格式

shadow文件格式

daemon*:18027:0:99999:7::: # 每个用户使用一行特定格式的文本记录
1:2:3:4:5:6:7:8:9
1:登录用名
2:用户密码:一般用sha512加密
3:从1970年1月1日起到密码最近一次被更改的时间
4:密码再过几天可以被变更 (0表示随时可被变更)
5:密码再过几天必须被变更 (99999表示永不过期)
6:密码过期前几天系统提醒用户 (默认为一周)
7:密码过期几天后帐号会被锁定
8:从1970年1月1日算起, 多少天后帐号失效
9:预留未用

- group文件格式

group文件格式

daemon:x:2:
1:2:3:4
1:群组名称: 就是群组名称
2:群组密码: 通常不需要设定, 密码是被记录在 /etc/gshadow
3:GID: 就是群组的 ID
4:以当前组为附加组的用户列表(分隔符为逗号)

- gshadow文件格式

gshadow文件格式

daemon:::

1:2:3:4

1:群组名称: 就是群的名称

2:群组密码:

3:组管理员列表: 组管理员的列表, 更改组密码和成员

4:以当前组为附加组的用户列表: 多个用户间用逗号分隔

三, Linux系统中用户和组的管理命令

1.相关文件操作

- **vipw & vigr** vipw, vigr - edit the password, group, shadow-password or shadow-group file

-g, --group

Edit group database.

-p, --passwd

Edit passwd database.

-s, --shadow

Edit shadow or gshadow database.

- **pwck**

pwck - verify integrity of password files

- **grpck**

grpck - verify integrity of group files

2.用户和组管理命令

用户管理命令

```
useradd usermod userdel
```

组帐号维护命令

```
groupadd groupmod groupdel
```

- useradd 创建用户

选项\用法	useradd [options] LOGIN
-u UID	指定用户UID
-o	配合-u 选项，不检查UID的唯一性，可创建不同用户名同UID的用户
-g GID	GID 指明用户所属基本组，可为组名，也可以GID
-c "COMMENT"	指定用户的注释信息
-d HOME_DIR	指定路径(不存在)为家目录
-s SHELL	指明用户的默认shell程序，可用列表在/etc/shells文件中
-G GROUP1[,GROUP2,...]	为用户指明附加组，组须事先存在
-N	不创建私用组做主组，使用users组做主组
-r	创建系统用户 CentOS 6: ID<500, CentOS 7: ID<1000
-m	创建家目录，用于系统用户
-M	不创建家目录，用于非系统用户
创建用户时默认值设定文件	/etc/default/useradd
显示或更改默认设置	useradd -D 显示目前的默认值
	useradd -D -s SHELL 改变新建用户的默认shell
	useradd -D -b BASE_DIR 改变新建用户的默认家目录
	useradd -D -g GROUP 改变新建用户的所属组
新建用户的相关文件和命令	
	/etc/default/useradd
	/etc/skel/*
	/etc/login.defs
newusers	使用passwd格式文件 批量创建用户
chpasswd	批量修改多个用户口令 每行的格式: username:passwd

- usermod 修改用户属性

参数\用法	usermod [OPTION] login
-u UID	指定新UID
-g GID	指定新主组
-G GROUP1[,GROUP2,...[,GROUPN]]	指定新附加组，原来的附加组将会被覆盖；若保留原有，则要同时使用-a选项
-s SHELL	新的默认SHELL
-c 'COMMENT'	新的注释信息
-d HOME	新家目录不会自动创建；若要创建新家目录并移动原家数据，同时使用-m选项
-l login_name	新的名字
-L	lock指定用户,即是在/etc/shadow 密码栏的增加感叹号!
-U	unlock指定用户,将 /etc/shadow 密码栏的!拿掉
-e YYYY-MM-DD	指明用户账号过期日期
-f INACTIVE	设定非活动期限


- userdel删除用户


选项\用法	userdel [OPTION]... Login
-f, --force	强制删除用户
-r, --remove	删除用户家目录和邮箱

- id命令查看用户相关的ID信息

选项\用法	id [OPTION]... [USER]
-u	显示UID
-g	显示GID
-G	显示用户所属的组的ID
-n	显示名称，需配合ugG使用

- su命令切换用户或以其他用户身份执行命令

选项\用法	 [user [args...]]
切换用户的方式	
su UserName	非登录式切换，即不会读取目标用户的配置文件，不改变当前工作目录

选项\用法	 [user [args...]]
su - UserName	登录式切换，会读取目标用户的配置文件，切换至家目录，完全切换
root使用su切换至其他用户无须密码；非root用户切换时需要密码	
换个身份执行命令	
 UserName -c 'COMMAND'	执行完命令还在当前用户下
选项：-l --login	
su -l UserName 相当于 su - UserName	

- 使用passwd命令设置密码

选项\用法	passwd [OPTIONS] UserName: 修改指定用户的密码
常用选项	
-d	删除指定用户密码
-l	锁定指定用户
-u	解锁指定用户
-e	强制用户下次登录修改密码
-f	强制操作
-n mindays	指定最短使用期限
-x maxdays	最大使用期限
-w warndays	提前多少天开始警告
-i inactivedays	非活动期限
--stdin	从标准输入接收用户密码
示例：echo "PASSWORD" passwd --stdin USERNAME	

- 用户相关的其它命令

chfn	指定个人信息
chsh	指定shell
finger	查看相关的注释信息

- 使用groupadd命令创建组

选项\用法	groupadd [OPTION]... group_name
-------	--

选项\用法	groupadd [OPTION]... group_name
-g GID	指明GID号；范围[GID_MIN, GID_MAX]
-r	创建系统组
CentOS 6: ID<500	
CentOS 7: ID<1000	

- 修改groupmod和删除组groupdel

选项\用法	groupmod [OPTION]... group
-n group_name	指定组的新名字
-g GID	新的GID
组删除: groupdel groupdel GROUP	

- gpasswd命令更改组密码

选项\用法	gpasswd [OPTION] GROUP
-a user	将user添加至指定组中
-d user	从指定组中移除用户user
-A user1,user2,...	设置有管理权限的用户列表
newgrp命令: 临时切换主组	
如果用户本不属于此组, 则需要组密码	

- groupmems更改和groups查看组成员

选项\用法	groupmems [options] [action]
options:	
-g, --group groupname	更改为指定组 (只有root)
actions:	
-a, --add username	指定用户加入组
-d, --delete username	从组中删除用户
-p, --purge	从组中清除所有成员
-l, --list	显示组成员列表
groups [OPTION].[USERNAME]... 查看用户所属组列表	

- 练习

题目	解答
创建用户gentoo，附加组为bin和root，默认shell为/bin/csh，注释信息为"Gentoo Distribution"	useradd -G bin,root -s /bin/csh -c "Gentoo Distribution" gentoo
创建下面的用户、组和组成员关系	
名字为webs 的组	groupadd webs
用户nginx，使用webs 作为附加组	useradd -G webs nginx
用户varnish，使用webs 作为附加组	useradd -G webs varnish
用户mysql，不可交互登录系统，且不是webs的成员，nginx，varnish，mysql密码都是magedu	
useradd mysql -s /bin/nologin	
	cat > passwd <<EOF
	nginx:magedu
	varnish:magedu
	mysql:magedu
	EOF
	echo passwd chpasswd

四，Linux系统中文件权限管理

1.文件属性及命令

- 文件属性



- 文件属性操作命令

chown	设置文件的所有者
-------	----------

chgrp 设置文件的属组信息

- 使用chown/chgrp修改文件的属主和属组

选项/用法	chown [OPTION]... [OWNER][:[GROUP]] FILE...
chown OWNER file	改变文件属主
chown OWNER:GROUP	同时改变属主和属组
chown :GROUP	只改变属组，冒号也可用 . 替换
	-R: 递归
chown [OPTION]... --reference=RFILE FILE...	继承文件的属主属组
修改文件的属组：chgrp	
	chgrp [OPTION]... GROUP FILE...
	chgrp [OPTION]... --reference=RFILE FILE...
	-R 递归

2.文件的权限

- 文件的权限主要针对三类对象进行定义

owner	属主， u
group	属组， g
other	其他， o

- 每个文件针对每类访问者都定义了三种权限

r	Readable
w	Writable
x	eXcutable

- 每种权限所对应的具体允许行为

文件	
r	可使用文件查看类工具获取其内容
w	可修改其内容
x	可以把此文件提请内核启动为一个进程
目录	

文件

r	可以使用ls查看此目录中文件列表
w	可在此目录中创建文件，也可删除此目录中的文件
x	可以使用ls -l查看此目录中文件元数据（须配合r），可以cd进入此目录
X	只给目录x权限，不给文件x权限

- 使用touch修改文件权限

选项/用法

chmod [OPTION]... OCTAL-MODE FILE...	
	-R: 递归修改权限
chmod [OPTION]... MODE[,MODE]... FILE...	
	MODE: 修改一类用户的所有权限
	u= g= o= ug= a= u,g=
修改一类用户某位或某些位权限	
	u+ u- g+ g- o+ o- a+ a- + -
chmod [OPTION]... --reference=RFILE FILE...	
	参考RFILE文件的权限，将FILE的修改为同RFILE

- 权限设置示例

```
chgrp market files
chown root:admins testfile
chmod u+wx,g-r,o=rx file
chmod -R g+rwX /pat/to/dir
chmod 600 file
chown steve file1
```

- 使用umask来规定新创建的文件和目录的默认权限

新建文件的默认权=666-umask	如果所得结果某位存在执行（奇数）权限，则将其权限+1
新建目录的默认权限=777-umask	
非特权用户umask是 002	
root的umask 是 022	
umask	默认查看当前shell环境的umask

umask #	设定umask
	示例: umask 002
	umask u=rw,g=r,o=
umask -S 模式方式显示	
umask -p 输出可被调用	
配置文件: 全局设置: /etc/bashrc 用户设置: ~/.bashrc	
<ul style="list-style-type: none"> 练习 	
当用户docker对/testdir 目录无执行权限时, 意味着无法做哪些操作?	docker不能新建、重命名或删除文件, 不能追加目录内文件内容, 不能转到该目录
当用户mongodb对/testdir 目录无读权限时, 意味着无法做哪些操作?	
当用户redis 对/testdir 目录无写权限时, 该目录下的只读文件file1是否可修改和删除?	不可以
当用户zabbix对/testdir 目录有写和执行权限时, 该目录下的只读文件file1是否可修改和删除?	只读文件只可以读, 不可以修改, 因为对目录有执行权限, 所有可以删除文件
复制/etc/fstab文件到/var/tmp下, 设置文件所有者为tomcat读写权限, 所属组为apps组有读写权限, 其他人无权限	cp /etc/fstab /var/tmp--> chown tomcat:apps /var/tmp--> chmod 660 /var/tmp/fstab
误删除了用户git的家目录, 请重建并恢复该用户家目录及相应的权限属性	cp -a /etc/skel/ /home/git/ --> chown -R git:git /home/git/-->chmod -R 700 /home/git

五, Linux系统中的特殊权限

1.linux中有三种特殊权限

SUID	SGUI	Sticky
用于可执行文件	用于可执行文件和目录	目录设置Sticky 位, 只有文件的所有者或root可以删除该文件

2.SUID权限用于可执行文件上

任何一个可执行程序文件能不能启动为进程: 取决发起者对程序文件是否拥有执行权限

启动为进程之后, 其进程的属主为原程序文件的属主

SUID只对二进制可执行程序有效 ;SUID设置在目录上无意义

权限设定

`chmod u+s FILE...`

`chmod u-s FILE...`

3.SGID权限用于可执行文件上

任何一个可执行程序文件能不能启动为进程：取决发起者对程序文件是否拥有执行权限

启动为进程之后，其进程的属组为原程序文件的属组

权限设定：

`chmod g+s FILE...`

`chmod g-s FILE...`

4.SGID权限用于目录，用来创建一个协作目录

默认情况下，用户创建文件时，其属组为此用户所属的主组

一旦某目录被设定了SGID，则对此目录有写权限的用户在此目录中创建的文件

所属的组为此目录的属组;通常用于创建一个协作目录

权限设定：

`chmod g+s DIR...`

`chmod g-s DIR...`

5.Sticky位 权限

具有写权限的目录通常用户可以删除该目录中的任何文件，无论该文件的权限或拥有权

在目录设置Sticky 位，只有文件的所有者或root可以删除该文件

sticky 设置在文件上无意义

权限设定：

`chmod o+t DIR...`

`chmod o-t DIR...`

例如：

`ls -ld /tmp`

drwxrwxrwt 12 root root 4096 Nov 2 15:44 /tmp

- 用数字表示特殊权限

特殊权限数字法

SUID SGID STICKY

000 0

001 1

010 2

011 3

100 4

101 5

110 6

111 7

chmod 4777 /tmp/a.txt

6.特殊权限位映射

SUID: user,占据属主的执行权限位	
s	属主拥有x权限
S	属主没有x权限
SGID group,占据属组的执行权限位	
s	group拥有x权限
S	group没有x权限
Sticky other,占据other的执行权限位	
t	other拥有x权限
T	other没有x权限 v

7.设置文件特定属性

chattr +i file	不能删除，改名，更改
chattr +a file	只能追加内容
lsattr file	显示特定属性

六，Linux文件系统的FACL

FACL全称为：文件访问控制列表

FACL全称为：文件访问控制列表

ACL: Access Control List	用于实现灵活的权限管理
除了文件的所有者，所属组和其它人，可以对更多的用户设置权限	
	CentOS7 默认创建的xfs和ext4文件系统具有ACL功能
	CentOS7 之前版本，默认手工创建的ext4文件系统无ACL功能,需手动增加
	<code>tune2fs -o acl /dev/sdb1</code>
	<code>mount -o acl /dev/sdb1 /mnt/test</code>
ACL生效顺序：所有者-->自定义用户-->所属组 自定义组-->其他人	
<ul style="list-style-type: none"> • **为多用户或者组的文件和目录赋予访问权限rwx** 	
<code>mount -o acl /directory</code>	开启facl功能
<code>getfacl file directory</code>	
<code>setfacl -m u:wang:rwx file directory</code>	
<code>setfacl -m g:admins:rw file directory</code>	
<code>setfacl -x u:wang file directory</code>	
<code>setfacl -b file1</code>	清除所有ACL权限
<code>getfacl file1 setfacl --set-file=- file2</code> 复制file1的acl权限给file2	
<p>mask只影响除所有者和other的之外的人和组的最大权限</p> <p>mask需要与用户的权限进行逻辑与运算后，才能变成有限的权限(Effective Permission)</p> <p>用户或组的设置必须存在于mask权限设定范围内才会生效</p> <p><code>setfacl -m mask::rx file</code></p> <p>--set选项会把原有的ACL项都删除，用新的替代，需要注意的是是一定要包含UGO的设置，不能象-m一样只是添加ACL就可以</p> <p>示例：</p> <p><code>setfacl --set u::rw,u:wang:rw,g::r,o::- file1</code></p>	
<ul style="list-style-type: none"> • 备份和恢复ACL 	
主要的文件操作命令cp和mv都支持ACL，只是cp命令需要加上-p 参数。但是tar等常见的备份工具是不会保留目录和文件的ACL信息	
<code>getfacl -R /tmp/dir1 > acl.txt</code>	
<code>setfacl -R -b /tmp/dir1</code>	

```
setfacl -R --set-file=acl.txt /tmp/dir1
```

```
setfacl --restore acl.txt
```

```
getfacl -R /tmp/dir1
```