

操作练习题：

任意虚拟机即可操作（准备1台虚拟机，如 web1），下面我们假设你的虚拟机主机名为 web1：

实验准备工作（前奏）：

使用 root 给虚拟机创建普通账户 alice，设置密码为 654321

```
# useradd alice
```

```
# echo 654321 | passwd --stdin alice
```

提问：

- 1) 使用 alice 用户登录系统可以安装软件包吗？
- 2) 使用 alice 用户登录系统可以创建用户吗？
- 3) 使用 alice 用户登录系统可以启动、关闭服务吗？

答案：（管理员 root 使用 su - alice 切换用户测试一下便可知晓）

```
# su - alice
```

```
$ systemctl restart crond          #重启计划任务服务会失败
```

```
$ useradd nb                        #创建用户会失败
```

```
$ yum -y reinstall vim              #重装 vim 会失败
```

那么问题来了，如何让普通用户也可以做管理员的操作呢？

实验验证真理（序曲）：

- 1) 管理员 root 修改/etc/sudoers 文件（这是一个神奇的文件，后面安全课程还会再讲）

注意是管理员 root 操作：

```
# vim /etc/sudoers                #打开这个文件，在文件最后一行手动添加如下一行内容
```

```
alice web1=(root) ALL              #让 alice 用户组 web1 这台电脑上可以以 root 的身份执行所有命令
```

```
:wq!                                #该文件为只读文件，需要 root 强制保存退出
```

- 2) 普通用户 alice 再次测试一下，看看能不能装包、启服务、建用户

```
# su - alice                        #先切换为普通用户 alice
```

```
$ useradd nb                        #创建用户会失败
```

```
$ systemctl restart crond          #重启服务会失败
```

什么情况？修改刚才的神奇文件(sudoers)没用吗？戏法失败了吗？玩砸了吗？

等等... ..

```
$ sudo useradd nb                  #会提示输入 alice 的密码，正确输入 alice 密码后成功
```

```
$ sudo restart crond              #成功
```

```
$ exit                             #退出普通用户，回到 root
```

结论：正常执行命令就是以普通用户的身份执行命令，sudo 后面加命令就是以 root 身份执行命令

晋级操作（高潮）：

管理员 root 再次修改 /etc/sudoers 文件，将之前添加的一行内容适当修改如下：

```
# vim /etc/sudoers
```

```
alice web1=(root) NOPASSWD: ALL
```

```
:wq! #该文件为只读文件，需要 root 强制保存退出
```

普通用户 alice 再次测试一下：

```
# su - alice #先切换为普通用户 alice
```

```
$ sudo useradd dachui #不用输入任何密码就可以创建账户（神奇吗）
```

```
$ sudo -i #普通用户不需要任何密码，直接切换为 root（惊不惊喜，意不意外）
```

结论：su 可以切换用户，sudo 也可以切换用户!!!

普通用户 sudo -i 切换 root 后就可以为所欲为了!!!

但是，前提条件是管理员需要修改 sudoers 文件，允许你这么干!!!

附加尝试（尾声）：

1) 管理员 root 再次修改 /etc/sudoers 文件，将之前添加的一行内容适当修改如下：

```
# vim /etc/sudoers
```

```
alice client=(root) NOPASSWD: ALL
```

```
:wq! #该文件为只读文件，需要 root 强制保存退出
```

假设你是在 web1 主机上做实验，主机名叫 web1.

这里故意将 sudoers 配置文件第二列改的和主机名不一致!!!

看看 alice 是否还可以为所欲为呢？

2) 管理员 root 再次修改 /etc/sudoers 文件，将之前添加的一行内容适当修改如下：

```
# vim /etc/sudoers
```

```
alice ALL=(root) NOPASSWD: ALL
```

```
:wq! #该文件为只读文件，需要 root 强制保存退出
```

假设你是在 web1 主机上做实验，主机名叫 web1.

这里故意将 sudoers 配置文件第二列改为 ALL!!!

看看 alice 是否还可以为所欲为呢？

3) 管理员 root 再次修改 /etc/sudoers 文件，将之前添加的一行内容适当修改如下：

```
# vim /etc/sudoers
```

```
alice ALL=(ALL) NOPASSWD: ALL
```

```
:wq! #该文件为只读文件，需要 root 强制保存退出
```

这里故意将 sudoers 配置文件第二列和第三列改为 ALL!!!

看看 alice 是否还可以为所欲为呢？

总结语法：用户 主机名=(提权的用户) NOPASSWD: 命令

授权什么人，在什么主机，以什么人的身份，执行什么命令