Sudo

是[linux系统](https://baike.baidu.com/item/linux%E7%B3%BB%E7%BB%9F/1732935" \t "_blank)管理指令，是允许[系统管理员](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E7%AE%A1%E7%90%86%E5%91%98/1503845)让普通用户执行一些或者全部的root命令的一个工具，如halt，reboot，su等等。这样不仅减少了root用户的登录 和管理时间，同样也提高了安全性。

===================================================================

在sudo于1980年前后被写出之前，一般用户管理系统的方式是利用[su](https://baike.baidu.com/item/su" \t "_blank)切换为超级用户。但是使用su的缺点之一在于必须要先告知超级用户的密码。

sudo使一般用户不需要知道超级用户的密码即可获得权限。首先超级用户将普通用户的名字、可以执行的特定命令、按照哪种用户或用户组的身份执行等信息，登记在特殊的文件中（通常是/etc/sudoers），即完成对该用户的授权（此时该用户称为“sudoer”）；在一般用户需要取得特殊权限时，其可在命令前加上“sudo”，此时sudo将会询问该用户自己的密码（以确认终端机前的是该用户本人），回答后系统即会将该命令的进程以超级用户的权限运行。之后的一段时间内（默认为5分钟，可在/etc/sudoers自定义），使用sudo不需要再次输入密码。

由于不需要超级用户的密码，部分Unix系统甚至利用sudo使一般用户取代超级用户作为管理帐号，

特性：

sudo能够限制用户只在某台[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)上运行某些命令。

sudo提供了丰富的日志，详细地记录了每个用户干了什么。它能够将日志传到中心主机或者日志服务器。

sudo使用[时间戳](https://baike.baidu.com/item/%E6%97%B6%E9%97%B4%E6%88%B3" \t "_blank)文件来执行类似的“检票”系统。当用户调用sudo并且输入它的密码时，用户获得了一张存活期为5分钟的票（这个值可以在编译的时候改变）。

sudo的配置文件是sudoers文件，它允许系统管理员集中的管理用户的使用权限和使用的主机。它所存放的位置默认是在/etc/sudoers，属性必须为0440。

===========================================================

配置：/etc/sudoers

用户或组 主机列表=(提权身份) [NOPASSWD]:命令列表

注意事项：命令需要写绝对路径，对组授权需要在组名称前面加%。

===================================================================

关于权限： 特殊权限：

普通用户不能使用：安装软件/卸载软件/查看分区/创建分区、删除分区、系统目录、如（/etc/ /opt/）读写权限

Sudo常见参数

|  |  |
| --- | --- |
| -V | 显示版本编号 |
| -h | 会显示版本编号及指令的使用方式说明 |
| -l | 显示出自己（执行 sudo 的使用者）的权限 |
| -v | 因为 sudo 在第一次执行时或是在 N 分钟内没有执行（N 预设为五）会问密码，这个参数是重新做一次确认，如果超过 N 分钟，也会问密码 |
| -k | 将会强迫使用者在下一次执行 sudo 时问密码（不论有没有超过 N 分钟） |
| -b | 将要执行的指令放在背景执行 |
| -p | prompt 可以更改问密码的提示语，其中 %u 会代换为使用者的帐号名称， %h 会显示主机名称 |
| -u | username/#uid 不加此参数，代表要以 root 的身份执行指令，而加了此参数，可以以 username 的身份执行指令（#uid 为该 username 的使用者号码） |
| -s | 执行环境变数中的 SHELL 所指定的 shell ，或是 /etc/passwd 里所指定的 shell |
| -H | 将环境变数中的 HOME （家目录）指定为要变更身份的使用者家目录（如不加 -u 参数就是系统管理者 root ） |
| command | 要以系统管理者身份（或以 -u 更改为其他人）执行的指令 |

===================================================================

Ansible：/etc/anaible/Ansible.cfg配置文件：

remote\_user = alice                #以什么用户远程被管理主机（被管理端主机的用户名）

[privilege\_escalation]

become = true                    #alice没有特权，是否需要切换用户提升权限

become\_method = sudo                #如何切换用户（比如用su就可以切换用户，这里是sudo）

become\_user = root                #切换成什么用户（把alice提权为root账户）

become\_ask\_pass = no                #执行sudo命令提权时是否需要输入密码

启动ansible： 需要再拷贝秘钥到被控制端主机的alice

===================================================================