链滴

1.CentOS7 装机初始化配置

作者：jianwi

原文链接：https://ld246.com/article/1537862106453

来源网站：链滴

Swap分区

1、使用dd命令创建一个swap交换文件

if(输入文件，input file)；
of(输出文件，output file)；
bs(数据块大小，block size)同时读入/输出的块字节大小为1024个字节即1KB；
count(数据块数量)单位M表示1024 * 1024，K表示1024，因此4GB=4M * 1KB。

```
dd if=/dev/zero of=/swap bs=1024 count=4M
```

2、对交换文件格式化并转换为swap分区

```
mkswap /swap
```

3、挂载并激活分区

```
swapon /swap
```

4、修改swap分区权限

```
chmod -R 0600 /swap
```

5、防止重启后swap分区变成0，修改/etc/fstab文件

```
# 目标文件
TARGET_FILE='/etc/fstab'
# 待追加的行字符串
TMP_STR='\/swap swap swap default 0 0'
# sed删除相同行
SED_DEL_CMD="sed -i '/^"$TMP_STR"\$/d' $TARGET_FILE"
# sed追加行
SED_APPEND_CMD="sed -i '\$a"$TMP_STR"' $TARGET_FILE"
# 执行
echo $SED_DEL_CMD' && '$SED_APPEND_CMD | bash
```

6、系统使用swap分区的依赖值（进阶配置）

```
cat /proc/sys/vm/swappiness
# 系统默认的swappiness值为30
sysctl vm.swappiness=10
# 使永久生效
TARGET_FILE='/etc/sysctl.conf'
TMP_STR='vm.swappiness = 10'
SED_DEL_CMD="sed -i '/^"$TMP_STR"\$/d' $TARGET_FILE"
SED_APPEND_CMD="sed -i '\$a"$TMP_STR"' $TARGET_FILE"
echo $SED_DEL_CMD' && '$SED_APPEND_CMD | bash
```

6、删除swap分区

```
swapoff /swap && rm -rf /swap
# 删除swap分区开机自动挂载策略
sed -i '/^\/swap swap swap default 0 0$/d' /etc/fstab
```

系统升级

```
yum install
# 添加EPEL(企业级Linux的一组高质量额外软件包)yum源
yum install -y epel-release
# 软件升级
yum -y update && yum -y upgrade
yum clean all && yum makecache
# 安装让程序后台运行的伪终端工具screen
yum install -y screen
# 安装守护进程工具
yum install -y daemonize
```

主机名

```
# 设置主机名并使永久生效
hostnamectl set-hostname domain.com
```

SSH配置

1、修改ssh默认端口，允许公钥登录

```
# 修改`/etc/ssh/sshd_config`的`#Port 22`为`Port 60022`
sed -i '/^Port [0-9]\+$/d' /etc/ssh/sshd_config
sed -i '/^#Port 22$/aPort 60022' /etc/ssh/sshd_config
# 开启公钥登录
sed -i '/^PubkeyAuthentication yes$/d' /etc/ssh/sshd_config
sed -i '/^#PubkeyAuthentication yes$/aPubkeyAuthentication yes' /etc/ssh/sshd_config
# 重启sshd
systemctl restart sshd
```

2、配置ssh免密登录

- 免登录其实是在本机生成两把锁，一把所谓的公钥是放到要登录的那台服务器上的，即公钥放在客端。
- 被登录的服务器上会有一个公钥文件，叫authorized_keys。如果被登录的服务器有多个客户端要上来，就会把每个密钥存成一行。
- 客户端发送到服务器端的密钥文件一定要放到登录用户主目录的 ~/.ssh这个隐藏目录下，如gues用户则在/home/guest/.ssh/下。
- 如果直接将authorized_keys的文件从客户端通过ssh-copy-id方式发送到服务器端，会覆盖原来的件，对其他用户有影响，所以发送时要进行改名后合并，

```
# 生成rsa公私钥
```

```
ssh-keygen
# 查看ssh
ls -al ~/.ssh/
```

- authorized_keys：存放远程免密登录的公钥,主要通过这个文件记录多台机器的公钥
- id_rsa：生成的私钥文件
- id_rsa.pub：生成的公钥文件
- know_hosts：已知的主机公钥清单

```
# 发送公钥到免密服务器上
ssh-copy-id -i root@server.com
# 如果ssh端口不为22，则需指定端口
ssh-copy-id -i -p 60022 root@server.com
```

防火墙配置

```
# 开启ssh端口，http服务，https服务
systemctl start firewalld
firewall-cmd --zone=public --add-port=60022/tcp --permanent
firewall-cmd --zone=public --remove-service=ssh --permanent
firewall-cmd --zone=public --add-service=http --permanent
firewall-cmd --zone=public --add-service=https --permanent
systemctl restart firewalld
systemctl enable firewalld
```

dns配置

```
nmcli connection show
nmcli con mod eth0 ipv4.dns "223.5.5.5  8.8.8.8"
systemctl restart network
```