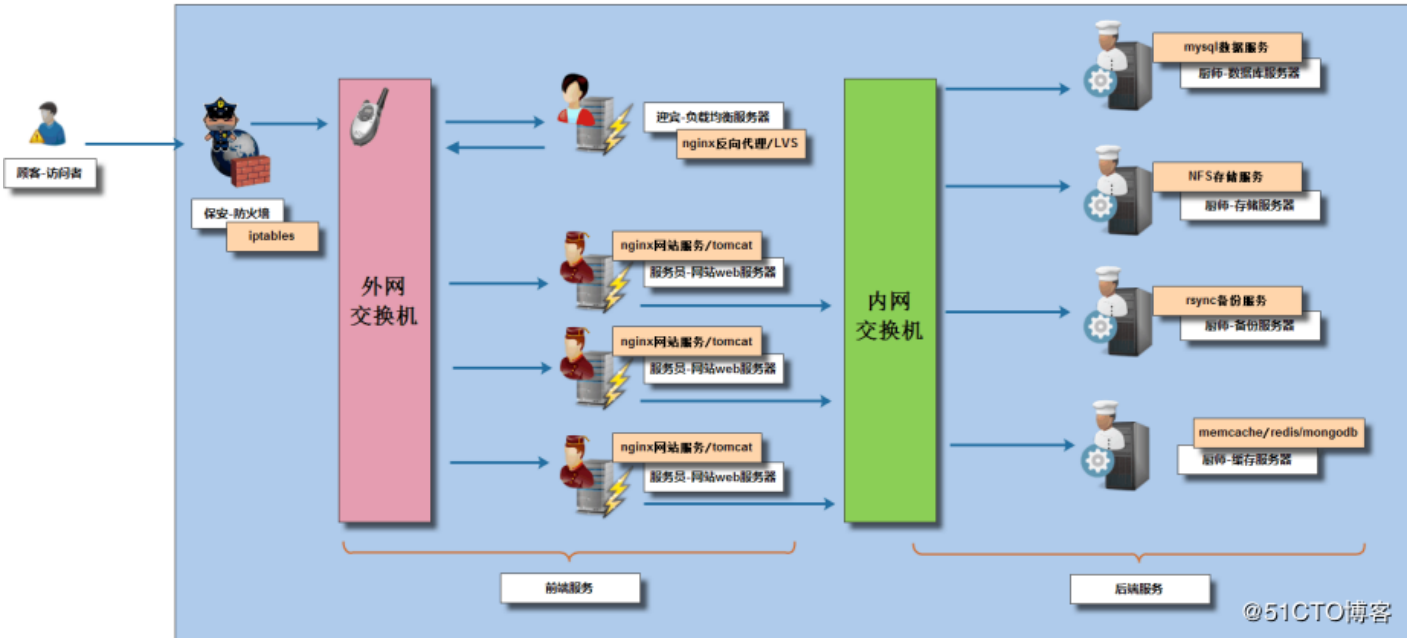
中小型公司架构集群部署经验

原创 GeorgeKai 2018-01-19 17:43:17 评论(1) 629人阅读

作者:Georgekai
归档：学习笔记
2018/1/19

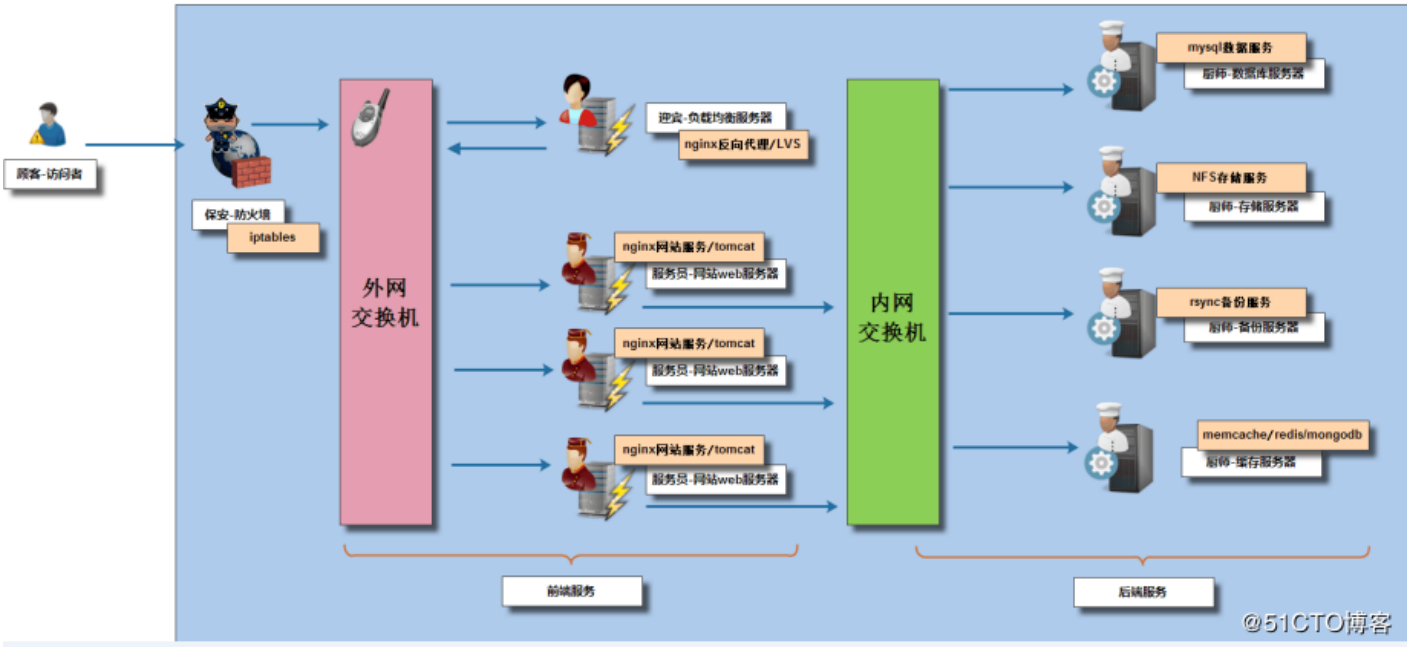
架构组成、架构部署
1.1 linux架构开场介绍
前段服务部分：（前段服务：负者负载均衡和web服务器）
顾客-访问者：访问网站架构的人员
保安-防火墙：主要提供系统架构的网络安全性
迎宾-负载均衡服务器：主要对访问请求进行调度处理（谁闲给闲，或挨个分配一部分）
服务员-网站web服务器：为访问者提供服务，做出相应处理（nginx或tomcat）
服务员-网站web服务器：为访问者提供服务，做出相应处理（nginx或tomcat）
服务员-网站web服务器：为访问者提供服务，做出相应处理（nginx或tomcat）

后端服务部分： （mysql和**NFS**和**rsync**和**memcache**）
厨师-数据库服务器：主要是用于存储字符串信息（mysql）
厨师-存储服务器：用于存储用户上传的图片、视频、音频、附件等数据（数据库服务器存储的内容不一样）（NFS存储服务）
厨师-备份服务器：对系统架构中，对重要数据信息进行备份存储（rsync备份）
厨师-缓存服务器：提供用户访问存储和读取快速响应，采用内存存储数据。
（会存储一份数据库服务器中的数据，用于用户优先访问提高访问速度，存放热 点数据）
（memcache和redis和mongodb）



1.2.1 异地备份方案：两地三中心

1.2.2 员工-运维人员：
秘密通道-VPN通道：（pptp vpn）
审计监控-跳板机：（shell / jumpserver）监控运维人员操作了哪些
监控-监控服务器：（zabbix）cpu、内存、磁盘、服务、网络等，可以实现电话、邮件、微信等报警通知。单击此处输入日期。
经理-批量管理服务器：（ssh+key+shell+ansible），对架构中所有服务器进行批量化操作



1.2.3 发现架构不足（完善架构）

1. 架构中的防火墙服务器可以部署多台，避免单点故障
2. 架构中负载均衡服务器也可以部署多台，避免单点故障（keeplived服务）
3. 架构中数据库服务器可以部署多台，实现主从架构，多个主多个从架构，避免单点故障
4. 架构中存储服务器可以部署多台
5. 架构中备份服务器可以部署多台
6. 架构中缓存服务器可以部署多台

1.3 架构部署

1.3.1 环境规划（统一规划）

1. 服务器主机名称与主机IP地址规划

❑ 服务器规划表：

服务器规划/形象比喻	数量	作用说明
负载均衡服务器 类似酒店迎宾	两台	对访问网站的流量进行分流，减少流量对某台服务器的压力
web 服务器 类似酒店服务员	三台	处理用户页面访问请求（Nginx）
NFS 存储(兼职批量管理)	一台	存储图片、附件、头像等静态数据
备份服务器(Rsync)	一台	对全网服务器数据，进行实时与定时备份
数据库服务器(MySQL)	一台	对动态变化数据进行存储(文本内容)
管理服务器	一台	1、作为 yum 仓库服务器，提供全网服务器的软件下载 2、跳板机、操作审计 3、vpn(pptp) 4、监控(zabbix) 5、兼职批量分发和管理（ssh key+ansible+saltstack）
说明：总计需要服务器 9 台，完成本次项目		

@51CTO博客

注：如主机配置较差可mysql和rsync可以为一台　web 可以设置二台，　NFS和批量管理为一台

2. 主机IP规划表：

❑ 主机 IP 规划表：

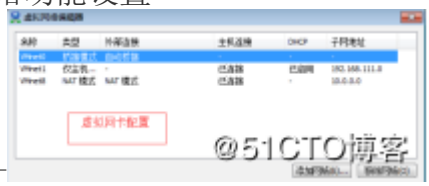
服务器说明	外网 IP(NAT)	内网 IP(LAN 区段)	主机名称规划
A1-nginx 负载服务器 01	10.0.0.5/24	172.16.1.5/24	lb01
A2-nginx 负载服务器 02	10.0.0.6/24	172.16.1.6/24	lb02
B1-nginx web 服务器	10.0.0.7/24	172.16.1.7/24	web01
B2-nginx web 服务器	10.0.0.8/24	172.16.1.8/24	web02
B3-nginx web 服务器	10.0.0.9/24	172.16.1.9/24	web03
C3-mysql 数据库服务器	10.0.0.51/24 (生产环境不设置)	172.16.1.51/24	db01
C1-NFS 存储服务器	10.0.0.31/24 (生产环境不设置)	172.16.1.31/24	nfs01
C2-rsync 备份服务器	10.0.0.41/24 (生产环境不设置)	172.16.1.41/24	backup
X-管理服务器	10.0.0.61/24 (生产环境不设置)	172.16.1.61/24	m01

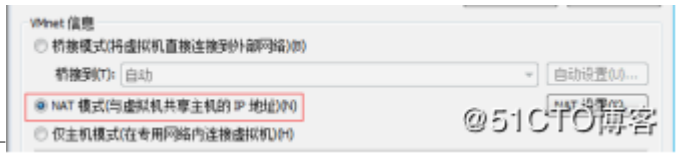
@51CTO博客

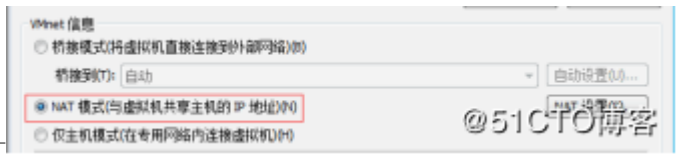
3. 服务器目录规划
/server/scripts
/server/tools
/application

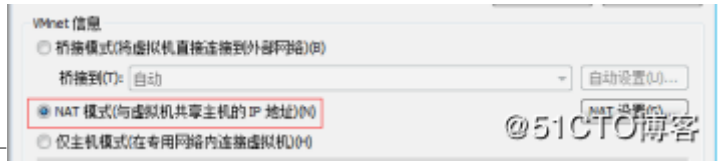
1.3.2 配置模板主机

1. 配置网络环境：
1）网卡的网段信息
2）网卡的网关信息
3）其他相关虚拟网络功能设置——

虚拟网络编辑器—— 

VMnet8—— 

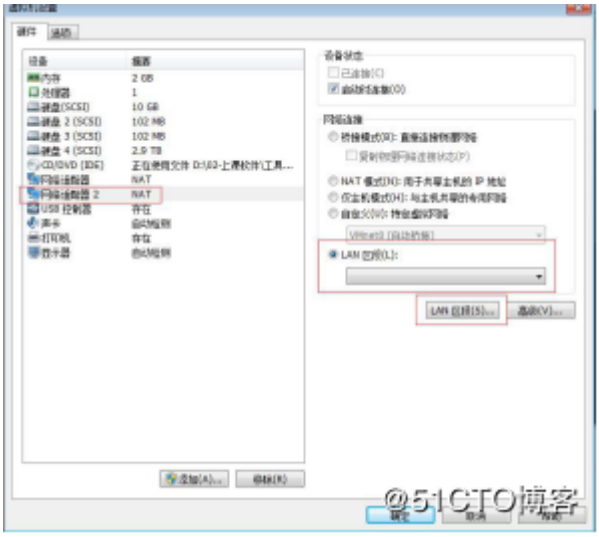
NAT模式—— 

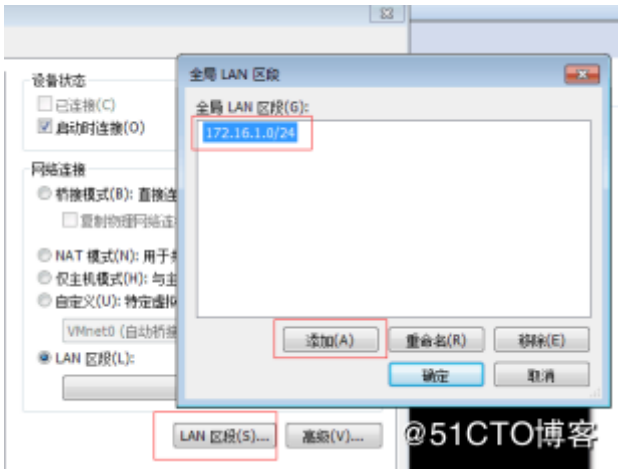
不应用DHCP服务—— 

NAT设置为10.0.0.254—— 

2. 添加虚拟网卡：

1）添加出一块新的虚拟网卡，网卡名为：eth1

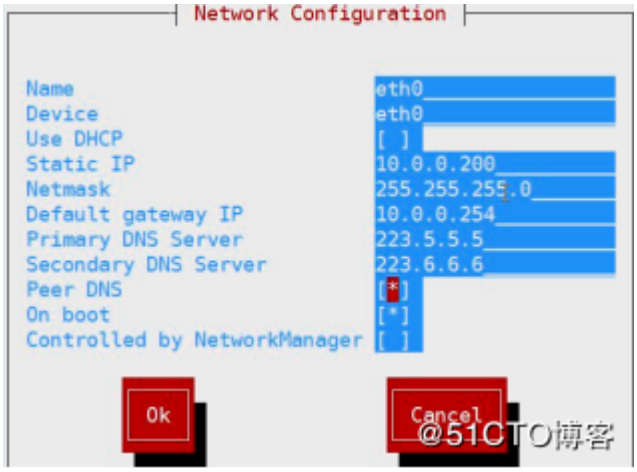




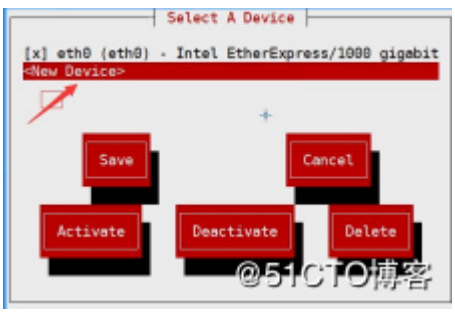
注：LAN区段定义一个内部网络环境，只要在同一个LAN区段即可相互通信

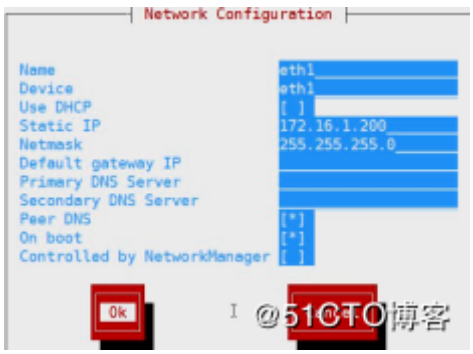
3. 开启模板主机，进行网卡地址信息配置

1）第一块网卡：eth0网络地址配置情况



2）第二块网卡：eth1网络地址配置情况



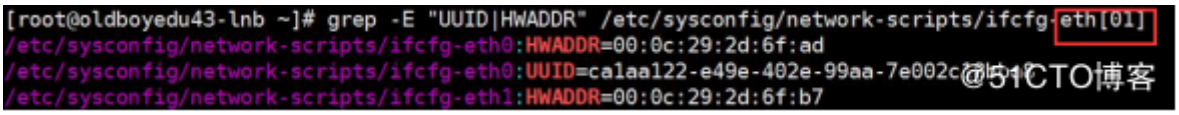


保存并退出，重启网卡服务！

4. 为虚拟主机克隆，做好环境准备（一清空，两删除）

1）两删除：删除网卡里面UUID信息，删除网卡里面mac地址信息

同时查看俩块网卡的UUID和HWADDR信息：



删除查看网卡的UUID和HWADDR信息：sed -ri '/UUID|HWADDR/d' /etc/sysconfig/network-scripts/ifcfg-eth[01]

2）一清空：清空一个网络规则配置文件

```
1. >/etc/udev/rules.d/70-persistent-net.rules
2. echo '>/etc/udev/rules.d/70-persistent-net.rules' >> /etc/rc.local
```

5. 对模板机进行基本系统优化

1）hosts文件配置 （内网地址对应的主机名）

```
\cp /etc/hosts{,.bak}
cat >/etc/hosts<<EOF
127.0.0.1   localhost localhost.localdomain localhost4
localhost4.localdomain4
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6
172.16.1.5      lb01
172.16.1.6      lb02
172.16.1.7      web01
172.16.1.8      web02
172.16.1.9      web03
172.16.1.51     db01 db01.etiantian.org
172.16.1.31     nfs01
172.16.1.41     backup
172.16.1.61     m01
EOF
```

2）更改yum源

```
1.下载yum源
wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-6.repo
wget -O /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-6.repo
PS：yum repolist 列出yum源信息；讲解什么是epel源
2.查看是否下载成功
ls /etc/yum.repos.d/
```

3）关闭SElinux

```
临时关闭：setenforce 0
永久关闭：vim /etc/sysconfig/selinux
  SELINXU=disabled
  sed -i.bak 's/SELINUX=enforcing/SELINUX=disabled/' /etc/selinux/config
          grep SELINUX=disabled /etc/selinux/config
```

4）关闭iptables

```
/etc/init.d/iptables stop
        /etc/init.d/iptables stop
        chkconfig iptables off
```

5）精简开机自启动服务

```
export.UTF-8
        chkconfig|egrep -v "crond|sshd|network|rsyslog|sysstat"|awk '{print
"chkconfig",$1,"off"}'|bash
        chkconfig --list|grep 3:on
```

6）提权george用户可以sudo

```
        useradd oldboy
        echo 123456|passwd --stdin oldboy
        \cp /etc/sudoers /etc/sudoers.ori
```

```
echo "oldboy  ALL=(ALL) NOPASSWD: ALL " >>/etc/sudoers
tail -1 /etc/sudoers
visudo -c
```

7）英文字符集

```
cp /etc/sysconfig/i18n /etc/sysconfig/i18n.ori
echo 'LANG="en_US.UTF-8"'  >/etc/sysconfig/i18n
source /etc/sysconfig/i18n
echo $LANG
```

8）时间同步

```
echo '#time sync by lidao at 2017-03-08' >>/var/spool/cron/root
echo '*/5 * * * * /usr/sbin/ntpdate pool.ntp.org >/dev/null 2>&1' >>/var/spool/cron/root
crontab -l
```

9）加大文件描述符

永久修改打开文件数量：`echo '*  -  nofile  65535  ' >>/etc/security/limits.conf`

```
tail -1 /etc/security/limits.conf
```

临时修改打开文件数量：`ulimit -n 65535`

`ulimit -a  ---检查默认打开文件数`

`open files  (-n) 1024`

注：文件描述符：一个服务默认可以打开的文件数量

```
[root@oldboyedu43-lnb yum.repos.d]# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 7332
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
```

@51CTO博客

10）内核优化

```
cat >>/etc/sysctl.conf<<EOF
net.ipv4.tcp_fin_timeout = 2
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_keepalive_time = 600
net.ipv4.ip_local_port_range = 4000    65000
net.ipv4.tcp_max_syn_backlog = 16384
net.ipv4.tcp_max_tw_buckets = 36000
net.ipv4.route.gc_timeout = 100
net.ipv4.tcp_syn_retries = 1
net.ipv4.tcp_synack_retries = 1
net.core.somaxconn = 16384
net.core.netdev_max_backlog = 16384
net.ipv4.tcp_max_orphans = 16384
#以下参数是对iptables防火墙的优化，防火墙不开会提示，可以忽略不理。
net.nf_conntrack_max = 25000000
net.netfilter.nf_conntrack_max = 25000000
net.netfilter.nf_conntrack_tcp_timeout_established = 180
net.netfilter.nf_conntrack_tcp_timeout_time_wait = 120
net.netfilter.nf_conntrack_tcp_timeout_close_wait = 60
net.netfilter.nf_conntrack_tcp_timeout_fin_wait = 120
EOF
#使配置文件生效：sysctl -p
```

11）安装其他小软件

实现linux和windows上传和下载软件：

```
yum install lrzsz nmap tree dos2unix nc telnet sl -y
```

12）ssh连接速度慢优化

```
sed -i.bak 's@#UseDNS yes@UseDNS no@g;s@^GSSAPIAuthentication yes@GSSAPIAuthentication no@g'
 /etc/ssh/sshd_config
```

重新加载sshd配置文件： /etc/init.d/sshd reload

13）创建目录环境

```
mkdir /server/{scripts,tools} /application -p
```

14）重启网卡确认配置是否正确

5. 进行虚拟主机克隆

1）关闭虚拟模板机，做一个模板机快照

内存：512M 硬盘：10G

2）进行虚拟主机克隆

链接克隆：

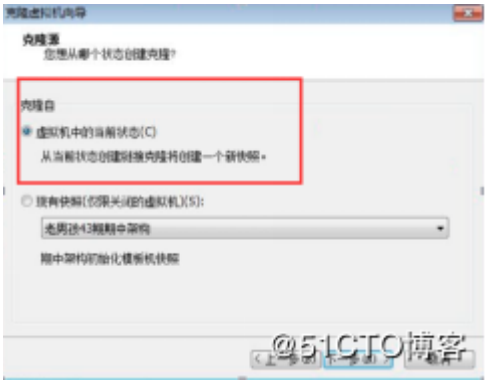
缺点：模板机（母体）没有了，所有链接克隆主机也会消失

优点：克隆效率高，占用系统资源少

完整克隆：

缺点：克隆效率低，占用系统资源多

优点：克隆主机更加安全，互相独立



第一台虚拟主机名：rsync-backup（按顺序往下排）

虚拟机位置：最好找一个专用位置存放期中架构虚拟机

6. 对克隆后的虚拟主机进行网络配置（修改IP地址和主机名）

注：当多个虚拟主机克隆完毕后，要一台一台开启，进行网 络配置，否则会造成网络地址冲突

开启一台克隆主机：

1）修改IP地址

```
sed 's#200#41#g' /etc/sysconfig/network-scripts/ifcfg-eth[01] -i
egrep '41'  /etc/sysconfig/network-scripts/ifcfg-eth[01] -i
```

2）修改主机名

```
hostsname backup
sed 's#georgekai#backup#g' /etc/sysconfig/network
```

3）查看hosts文件是否修改成功（9个IP对应的主机名）

4）重启网络服务

```
service network restart
```

5）xshell中重新连接，并设置好会话标签名称

小伙伴们可以关注我的微信公众号：linux运维菜鸟之旅

关注“中国电信天津网厅”公众号，首次绑定可免费领2G流量，为你的学习提供流量！

版权声明：原创作品，如需转载，请注明出处。否则将追究法律责任