链滴

Linux 实战案列 - 服务器系统配置初始化

作者：heroinepn
原文链接：https://ld246.com/article/1680931027284
来源网站：链滴

服务器系统配置初始化

准备

- 设置时间地区并同步互联网时间
- 禁用Selinux安全机制
- 清空防火墙策略
- 显示历史命令的操作时间
- 禁止root远程登录
- 禁止定时任务发送邮件
- 设置最大打开文件数
- 减少物理交换分区Swap的使用
- 系统内核参数优化
- 安装系统性能分析工具

防止忘记命令的用法，以及shell练习

查看当前时间，分区 CST

```
date
```

编写 shell脚本 1.sh

```
ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/location
if !crontable -l |grep ntpate &>/dev/null;
```

```
  then(echo "* 1 * * ntpate time.window.com >/dev/null 2>&1";crontable -l) | crontable
fi

#ln [参数][源文件或目录][目标文件或目录]软连接

#如果系统中没有定时同步时间的任务，则执行后面的代码块。

#crontable -l ： 查看当前系统中所有的定时任务 #新的定时任务和原有的定时任务合并成一个任务表。 #crontable：将新的任务列表写入到crontab中，即将定时同步时间的任务添加到系统中。

#设置每天凌晨1点定时同步时间分　时　日　月　周　，ntpdate命令从time.window.com获取网时间，并将其设置为系统时间，并不输出任何信息

#2>&1 的意思是将标准错误输出（stderr）重定向到标准输出（stdout）。其中，2表示标准错误输，1表示标准输出。重定向操作符>后面没有指定文件名，

#表示将标准错误输出重定向到与标准输出相同的位置，即将错误信息输出到与正常信息相同的地方。

#这样做的目的是将所有输出信息都重定向到同一个文件或管道中，方便查看和处理。

#&m>file 意思是把 标准输出 和 标准错误输出 都重定向到文件file中

#n>&m表示使文件描述符n成为输出文件描述符m的副本。这样做的好处是，有的时候你查找文件的候很容易产生无用的信息,

#如:2> /dev/null的作用就是不显示标准错误输出；另外当你运行某些命令的时候,出错信息也许很重要便于你检查是哪出了毛病,如:2>&1

#&> 的意思是将标准输出和标准错误输出都重定向到同一个文件或管道中。

#其中，&表示将输出重定向符号后面的文件名或管道符号视为文件描述符，而不是普通的文件名。定向操作符>表示将标准输出重定向到指定文件或管道中，

#如果文件或管道不存在，则会创建文件或管道。因此，&>表示将标准输出和标准错误输出都重定向同一个文件或管道中。

#/dev/null是一个文件，这个文件比较特殊，所有传给它的东西它都丢弃掉。当程序在你所指定的时执行后，系统会发一封邮件给当前的用户，

#显示该程序执行的内容，若是你不希望收到这样的邮件，请在每一行空一格之后加上 > /dev/null 2>&1

#后续添加的 |crontable 的作用是将前面命令的标准输出作为输入传递给 crontab 命令，用于添加定任务。

#| 符号表示管道符号，用于连接两个命令，将前一个命令的标准输出作为后一个命令的标准输入设置同步时间追加到crontab。
```

禁用SeLinux

```
sed -i '/SELINUX/{s/permissive/disabled}' /etc/selinux/config

#禁用SeLinux sed -i 's/old/new' fill 匹配 SELINUX 新旧文件内容替换
```

关闭防火墙

```
if egrep "7.[0-9]" /etc/redhat-release &>/dev/null;then
   systemctl stop firewalld
   systemcttl diasble firewald
elif egrep "6.[0-9]" /etc/redhat-release &>          /dev/null;then
service iptables stop
```

```
chkconfig iptables off
fi
```

#禁用SeLinux sed -i 's/old/new' fill 匹配 SELINUX 新旧文件内容替换

chkconfig 命令用于检查，设置系统的各种服务。egrep: == grep -E 用于显示文件中符合条件的字符

检测当前系统的发行版版本号，如果是 CentOS 7.x 系列，则停止并禁用防火墙 firewalld，如果是 CentOS 6.x 系列，则停止并禁用防火墙 iptables。

显示历史时间

```
if !grep HISTTIMEFROMAT /etc/bashrc;then
   echo 'export HISTTIMEFROMAT="%F %T 'whoami' " ' >> /etc/bashrc
fi
```

#显示历史命令的操作时间 %F %T whoami 日期时间用户追加 export 命令用于设置或显示环境变量

SSH 超时关闭

```
if !grep "TMOUT=600" /etc/profile &>dev/null;then
   echo "export TMOUT=600 ">> /etc/profile
fi
```

#SSH超时关闭 检测是否设置环境变量超时没有添加值600 ， 无操作 10分钟后断开连接

禁止root 远程登录 ， 注意留有root权限的用户

```
sed -i 's/#PermitRootLogin yes/PErmitRootLogin no' /etc/ssh/ssh_config
```

插入， i 的后面可以接字串，而这些字串会在新的一行出现(目前的上一行修改文件)；

禁止定时任务发送邮件

```
sed -i 's/^MAILT0=rooot/MAILTo=""' /etc/crontab
```

#禁止定时任务发送不必要的邮件,设置收件人为空

设置最大打开文件数

```
if !grep "* soft nofile 65535" /etc/securoty/limits.conf &>/dev/null;then
cat >> /etc/secrity/limits.conf <<EOF
* soft nofile 65535
* hard nofile 65535
EOF
fi
```

#这段代码的作用是向 /etc/security/limits.conf 文件追加两行内容，即将所有用户的最大打开文件限制（nofile）设置为 65535。

#使用 cat 命令追加内容到 /etc/security/limits.conf 文件， <<EOR 表示使用 Here Document 方输入多行内容，结束符为 EOR。

#所有用户的软硬限制（soft）最大打开文件数限制为 65535。

#EOR：Here Document 结束符。

#文件追加两行内容，即将所有用户的最大打开文件数限制（nofile）设置为 65535。

系统内核优化

```
cat >> /etc/sysctl.conf << EOF
net.ipv4.tco_syncookies =1
net.ipv4.tcp_max_tw_buckets=20480
net.ipv4.tvp_max_syn_backlog=20480
net.core.netdev_max_backlog=262144
net.ipv4.tcp_fin_timout=20
EOF
```

- net.ipv4.tco_syncookies：启用TCP SYN cookies，用于防御SYN flood攻击。 - net.ipv4.tcp_max_tw_buckets：设置系统中允许保持TIME-WAT状态的最大数量。- net.ipv4.tcp_max_syn_backlog：设置TCP连接请求队列的最大长度。- net.core.netdev_max_backlog：设置网络接口收包队列的最大长度。- net.ipv4.tcp_fin_timeout：设置TCP连接的FIN-WAIT-2状态的等待时间。

减少SWAP的使用 改权重值

```
echo "0" >/proc/sys/vm/swappiness
```

安装系统性能分析工具

```
yum install gcc make autoconf vim sysstat net-toolsiostat iftop iotop lrzsz -y
```

安装脚本转换工具

```
yum install dos2unix -y

dos2unix 1.sh
```