爱维 Linux 公开课

线上 Linux 服务器优化经验

主讲人：南非蚂蚁

课程安排

- 系统安装分区经验
- 如何最小化安装系统
- 修改 ip 地址、网关、主机名、DNS 等
- 关闭 selinux，清空 iptables，设置线上环境的 iptables demo
- 添加普通用户并进行 sudo 授权管理
- 更新 yum 源及必要软件安装
- 设置自动更新服务器时间 NTP 服务
- 精简开机自启动服务
- 删除不必要的系统用户和群组
- 部署监控客户端软件（ganglia-gmond/zabbix agent）
- 变更默认的 ssh 服务端口，禁止 root 用户远程连接
- 调整文件描述符大小
- 内核参数优化

一、系统安装和分区经验

1、磁盘 RAID 经验

系统盘：raid1

数据盘：raid5/raid1/raid10

2、Linux 版本选择之我见

推荐版本：Centos5.8/6.5 x86_64 对应 RHEL5.8/6.5

3、Linux 分区经验

系统分区和数据分区分离原则

LVM 是否需要

多分区原则（/、/boot、/var、/usr、/data）

4、 swap 使用建议

大内存服务器是否还需要 swap？

线上服务器 swap 设置建议

阿里云真的不需要 swap 吗？

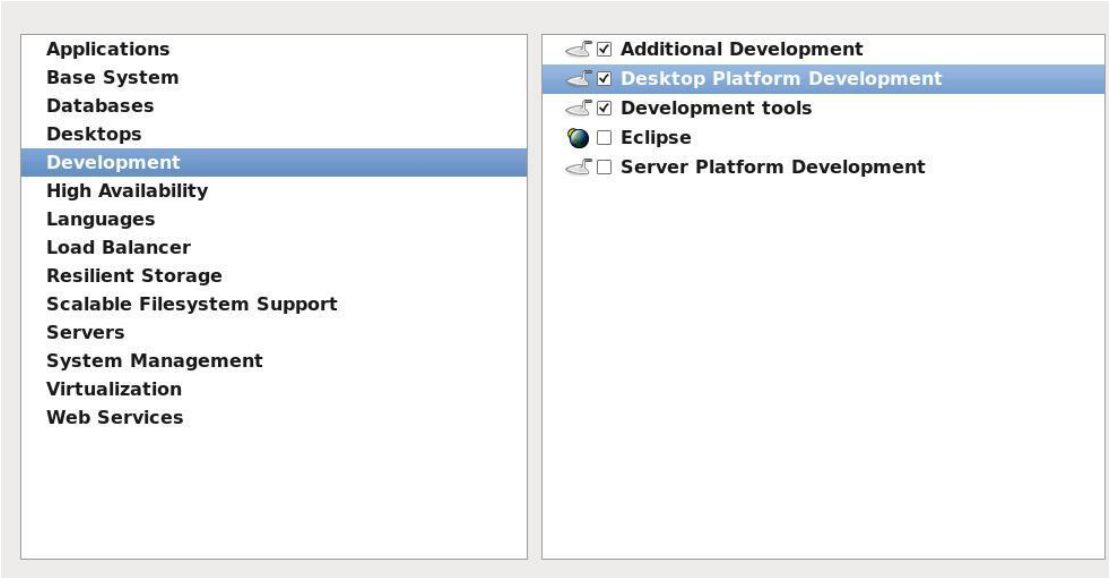
5、软件安装建议

精简安装策略：

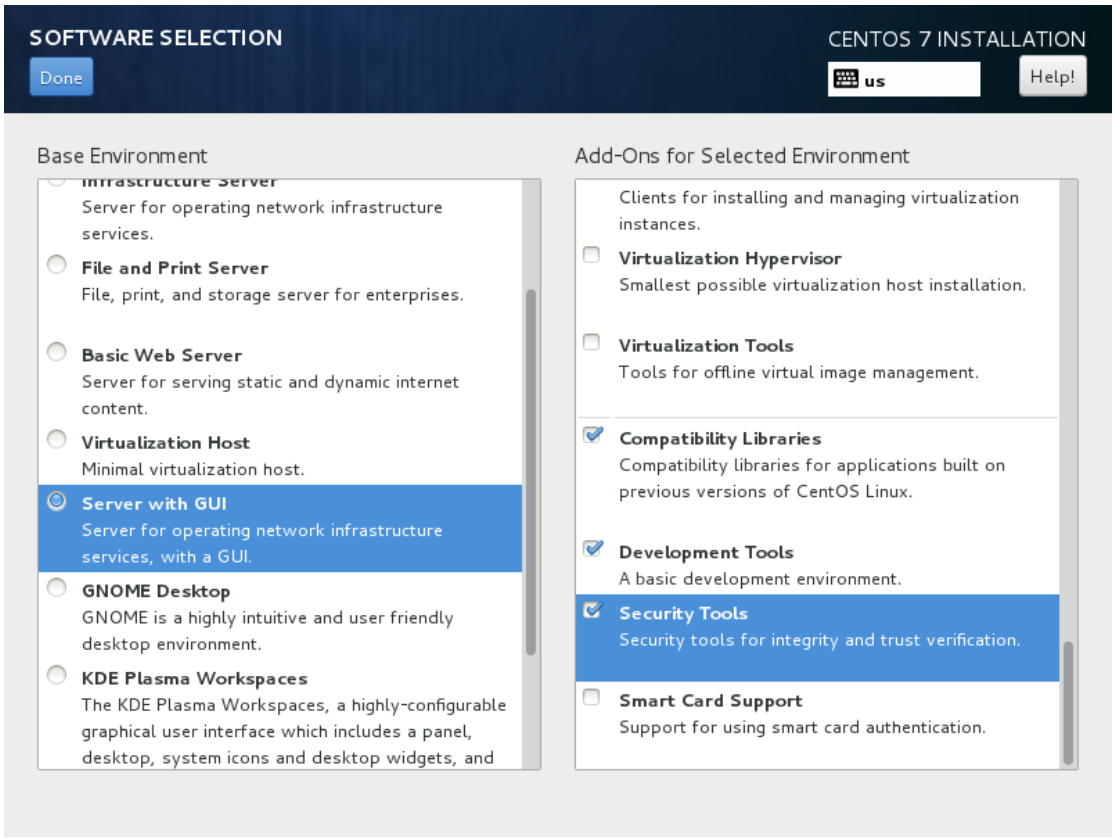
1、仅安装需要的，按需安装、不用不装

2、开发包、基本网络包、基本应用包

Centos6.x 下的设置：



Centos7.x 下的软件包选择：



二、服务器网络配置

1、服务器 IP 地址配置

/etc/sysconfig/network-scripts/ifcfg-eth0/1/2....

重启网卡命令：

service network restart 或者 /etc/init.d/network restart

2、网关/主机名配置

/etc/sysconfig/network

3、DNS 配置

/etc/resolv.conf

4、HOSTS 文件配置

/etc/hosts

三、网络安全配置

1、Selinux 配置（如何关闭 selinux）

cat /etc/selinux/config

SELINUX 的状态：

enforcing 开启状态
permissive 提醒的状态
disabled 关闭状态

命令行关闭：setenforce 0

2、iptables 配置

/etc/sysconfig/iptables

推荐配置：

```
iptables -P INPUT ACCEPT
iptables -F

iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 1.1.1.1 -p tcp -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 2.2.2.2 -p tcp -m tcp --dport 22 -j ACCEPT
iptables -A INPUT -i eth1 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,ACK FIN -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags PSH,ACK PSH -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags ACK,URG URG -j DROP

iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
```

查看 iptables 策略：

iptables –L –n

四、系统登录安全与 SSH 配置

1、授权用户登录与 sudo 设定

/etc/sudoers 文件

<user list> <host list> = <operator list> <tag list> <command list>

常见配置：

iiveylinux　　ALL=(ALL)　　NOPASSWD: ALL

2、ssh 安全登录经验

备份：cp /etc/ssh/sshd_config sshd_config_bak（运维必备守则）

vi /etc/ssh/sshd_config

#SSH 链接默认端口

#不使用 DNS 反查，可提高 ssh 连接速度

UseDNS no

#关闭 GSSAPI 验证，可提高 ssh 连接速度

GSSAPIAuthentication no

#禁止 root 账号登陆

PermitRootLogin no

五、更新 yum 源以及软件版本

1、常用的几个 yum 源

epel 源：https://fedoraproject.org/wiki/EPEL

repoforge 源：http://repoforge.org/use/

rpm –ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm

2、升级系统内核以及更新软件

清空 yum 缓存
yum clean all
生存缓存
yum makecache
开始更新系统以及内核
yum upgrade
必备软件
yum install ntpdate wget -y

六、调整服务器时间 NTP 设置

1、通过 crontab 设置时间同步

推荐时间服务器：ntp.sjtu.edu.cn
/usr/sbin/ntpdate ntp.sjtu.edu.cn >> /var/log/ntp.log 2>&1; /sbin/hwclock –w

2、架设 ntp server

关注两个文件：
/etc/ntp/ntpserver.conf
/etc/ntp.conf

七、系统资源调优

1、关注 ulimit 命令

ulimit –n（最大打开文件数）

常见案例日志：java.net.SocketException: Too many open files

相关配置文件：

/etc/security/limits.conf

/etc/security/limits.d/90-nproc.conf（centos6.x 版本）

```
*          soft    nofile          65536
*          hard    nofile          65536
```

ulimit -u（最大用户数）

```
*          soft    nproc       65536
root       soft    nproc       unlimited
```

2、系统内核参数调优

常见案例日志：kernel: ip_conntrack: table full, dropping packet

ip_conntrack_max 参数

/proc/sys/net/ipv4/netfilter/ip_conntrack_max 或者

/proc/sys/net/ipv4/ip_conntrack_max (centos5.x)

/proc/sys/net/netfilter/nf_conntrack_max(centos6.x)

在/etc/sysctl.conf 加入

net.ipv4.netfilter.ip_conntrack_max = 655360(centos5.x)

net.nf_conntrack_max = 100000(centos6.x)

swappiness 参数

表示使用 swap 的概率，此值越大，表示使用 swap 的概率越大。推荐配置如下：

查看目前配置：cat /proc/sys/vm/swappiness

添加如下内容到/etc/sysctl.conf

vm.swappiness=10

表示当内存使用率超过（100-10）90%时，才开始使用 swap。

我们线上 web 服务器配置参考（每天 3 亿的量）

```
net.ipv4.conf.lo.arp_ignore = 1
net.ipv4.conf.lo.arp_announce = 2
net.ipv4.conf.all.arp_ignore = 1
net.ipv4.conf.all.arp_announce = 2
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_fin_timeout = 10

net.ipv4.tcp_max_syn_backlog = 20000
net.core.netdev_max_backlog =  32768
net.core.somaxconn = 32768

net.core.wmem_default = 8388608
net.core.rmem_default = 8388608
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216

net.ipv4.tcp_timestamps = 0
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 2
net.ipv4.tcp_syncookies = 1

net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_tw_reuse = 1

net.ipv4.tcp_mem = 94500000 915000000 927000000
net.ipv4.tcp_max_orphans = 3276800

net.ipv4.tcp_fin_timeout = 10
net.ipv4.tcp_keepalive_time = 120
net.ipv4.ip_local_port_range = 1024  65535
net.ipv4.tcp_max_tw_buckets = 80000
net.ipv4.tcp_keepalive_time = 120
net.ipv4.tcp_keepalive_intvl = 15
net.ipv4.tcp_keepalive_probes = 5

net.ipv4.conf.lo.arp_ignore = 1
net.ipv4.conf.lo.arp_announce = 2
net.ipv4.conf.all.arp_ignore = 1
net.ipv4.conf.all.arp_announce = 2
```

net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_fin_timeout = 10

net.ipv4.tcp_max_syn_backlog = 20000
net.core.netdev_max_backlog = 32768
net.core.somaxconn = 32768

net.core.wmem_default = 8388608
net.core.rmem_default = 8388608
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216

net.ipv4.tcp_timestamps = 0
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 2

net.ipv4.tcp_mem = 94500000 915000000 927000000
net.ipv4.tcp_max_orphans = 3276800

net.ipv4.ip_local_port_range = 1024 65535
net.ipv4.tcp_max_tw_buckets = 500000
net.ipv4.tcp_keepalive_time = 60
net.ipv4.tcp_keepalive_intvl = 15
net.ipv4.tcp_keepalive_probes = 5
net.nf_conntrack_max = 2097152

八、精简系统服务和开机进程

1、线上服务器建议开启的服务

crond，network，syslog，sshd、iptables、udev-post、sysstat

快捷开启方法：

先关闭所有

for serv in `chkconfig --list|grep 3:on|awk '{print $1}'`;do chkconfig --level 3 $serv off;done

然后开启需要的服务：

for serv in `crond network syslog sshd iptables udev-post sysstat`;do chkconfig --level 3 $serv on;done

2、可删除的系统用户和组

#删除不必要的用户

```
userdel adm
userdel lp
userdel sync
userdel shutdown
userdel halt
userdel news
userdel uucp
userdel video
userdel games
userdel gopher
userdel ftp
```

#删除不必要的群组

```
groupdel adm
groupdel lp
groupdel news
groupdel uucp
groupdel games
groupdel dip
```

下期公开课预告

主题：Linux 服务器调优经验

内容：

1、系统性能问题讨论

2、影响 Linux 性能的因素

3、系统性能分析工具

4、系统性能分析标准

5、性能调优思路与技巧分享

参与方式：

加入 Linux 运维专家（134896298），然后关注群公告，每周会定期进行公开课技术分享，具体开课时间会进行提前通知，欢迎大家届时参加，参与方式：群（134896298）应用中群视频直播！

广而告之

开班介绍

爱维 Linux，专注 Linux 运维实战教育，我们开设了两个班级：

- 高薪运维入门提高班　详情：http://www.iivey.com/666-2
- 高薪运维实战提升班　详情：http://www.iivey.com/archives/66

授课模式

课程汇聚了以**南非蚂蚁**领衔的行业顶尖技术专家 10 年一线工作经验和培训心得，课程由浅入深，循序渐进，能够帮助学员们系统学习 Linux 一线经验，并迅速掌握 Linux 的各种应用技能。

我们的授课方法：

理论结合实际+实战技巧+经验分享+实时互动+专业学习教材

开课时间

入门提高班将在 3 月 12 开课，而实战提高班将在 5 月份开课，5 个月的授课时间，现在入门提高班接受报名，有意向的朋友可通过如下方式联系我们：

QQ：397824870（蚂蚁老师） 3335603751（章老师） 1218761836（王老师）

微信：ixdba8