CentOS6安装配置规范

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 日期 | 版本 | 内容 | 主要修订人 | 备注 |
| 2017-08-28 | 0.1 | 初稿 | 黄金强 |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. 本文档针对CentOS6.x系列操作系统
2. 安装方式以最小化安装
3. 分区规划

|  |  |  |
| --- | --- | --- |
| 分区 | 大小(单位MB) | 用途 |
| /boot | 512 | 引导分区 |
| Swap | 一般为物理内存2倍, 最大不超过4096, 对于分析类系统环境可适合加大 | 交换分区 |
| / | 51200 | 根分区 |
| /data | 剩余磁盘空间 | 数据分区 |

4. 初始化配置规范

(1). 禁用selinux

shell# vi /etc/selinux/config

把SELINUX=enforcing

修改为SELINUX=disabled

shell# setenforce 0

(2). 网络配置ip和dns

shell# vi /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0 #网卡名称

ONBOOT=yes #开机激活网卡

BOOTPROTO=static #静态

IPADDR=192.168.0.212 #ip地址

NETMASK=255.255.0.0 #子网掩码

GATEWAY=192.168.0.1 #网关

shell# /etc/init.d/network restart

shell# vi /etc/resolv.conf

nameserver ip1

nameserver ip2

options timeout:1 rotate

(3). 安装软件包

shell# yum -y install wget make gcc gcc-c++ automake autoconf openssl openssl-devel vim-enhanced \

patch ncurses libtool zlib zlib-devel bc nc lsof sysstat iproute telnet mtr\

ncurses-devel ntpdate openssh-clients

(4). 配置主机名

shell# vi /etc/sysconfig/network

NETWORKING=yes

HOSTNAME=vm6 #主机名

(5). 配置时区

shell# \cp /usr/share/zoneinfo/Asia/Shanghai /etc/localtime

shell# vi /etc/sysconfig/clock

ZONE="Asia/Shanghai"

UTC=false

shell# echo "00 00 \* \* \* /usr/sbin/ntpdate 0.pool.ntp.org > /dev/null 2>&1"|crontab

(6). 禁用control-alt-delete

shell# mv /etc/init/control-alt-delete.conf /etc/init/control-alt-delete.conf.default

(7). 禁用ipv6

shell# echo "options ipv6 disable=1" >> /etc/modprobe.d/dist.conf

(8). 磁盘IO性能优化

shell# sed -i '/ext.\*defaults /s/defaults/&,noatime,nodiratime/' /etc/fstab

(9). 服务启动最小化

for i in $(chkconfig --list|awk '{print $1}');do chkconfig $i off;done

for i in auditd crond iptables network rsyslog sshd udev-post;do chkconfig $i on;done

(10). 打开最大文件句柄和进程数

vi /etc/security/limits.d/90-nproc.conf

\* soft nproc unlimited

vi /etc/security/limits.conf

\* soft nproc 100000

\* hard nproc 100000

\* soft nofile 100000

\* hard nofile 100000

(11). 内核参数优化

shell# vi /etc/sysctl.conf

#swap

vm.swappiness = 5 #当物理内存使用率剩余此值时就尽可能使用swap

vm.dirty\_ratio = 10 #文件系统刷新脏页达内存使用百分比时刷新脏页到磁盘

vm.dirty\_background\_ratio = 10 #当写缓冲使用到内存的百分比时触发后台脏页刷新到磁盘

net.ipv4.ip\_local\_port\_range = 4096 65000 #向外可使用应用程序端口范围

net.ipv4.tcp\_fin\_timeout = 2 #表示如果套接字由本端要求关闭，保持在FIN-WAIT-2状态的时间，默认值是60秒。

net.ipv4.tcp\_syncookies = 1 #当有大量SYN包，等待队列溢出时，就会启用Cookies来处理，可防范少量SYN攻击，默认是1，开启

net.ipv4.tcp\_tw\_reuse = 1 #1是开启复用，允许将TIME\_WAIT sockets重新用于新的TCP连接，默认是0，表示关闭

net.ipv4.tcp\_tw\_recycle = 1 #开启TCP连接中TIME\_WAIT sockets的快速回收，默认是0关闭

net.ipv4.tcp\_max\_tw\_buckets = 5000 #系统同时保持TIME\_WAIT套接字的最大数量，如果超出这个数字，TIME\_WATI套接字将立刻被清除并打印警告信息，默认180000

net.ipv4.tcp\_max\_syn\_backlog = 4096 #进入SYN队列的最大长度，默认是1024，加大队列长度可容纳更多的等待连接

net.core.netdev\_max\_backlog = 10240 #网络接口接受数据包的队列，允许送到队列的数据包最大设备队列，默认值1000

net.core.somaxconn = 2048 #调节系统同时发起的tcp连接数，默认值128

net.core.wmem\_default = 4096000 #发送缓存区大小的缺省值

net.core.rmem\_default = 4096000 #接受套接字缓冲区大小的缺省值（以字节为单位）

net.core.rmem\_max = 4096000 #最大接收缓冲区大小的最大值

net.core.wmem\_max = 4096000 #发送缓冲区大小的最大值

net.ipv4.tcp\_syn\_retries = 2 #SYN握手重试次数，当超过这个数，此连接就会从syn\_backlog中删除

net.ipv4.tcp\_synack\_retries = 2 #SYN-ACK握手状态重试次数

net.ipv4.tcp\_max\_orphans = 3276800 #系统中最多有多少个TCP套接字不被关联到任何一个用户文件句柄上，如果超出这个数字，孤儿连接将立即复位并打印警告信息

net.ipv4.tcp\_mem = 94500000 915000000 927000000

(12). 创建普通用户

shell# groupadd -g 2000 shenqi

shell# useradd -g 2000 -u 2000 shenqi

shell# echo 'shenqi#ML@1688' | passwd --stdin shenqi

(13). ssh配置

shell# vi /etc/ssh/sshd\_config

Port 4365

PermitRootLogin no

PermitEmptyPasswords no

# GSSAPIAuthentication yes

# GSSAPICleanupCredentials yes

UseDNS no

(14). 防火墙策略

shell# vi /etc/sysconfig/iptables

-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

-A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 4365 -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT

-A INPUT -j REJECT --reject-with icmp-host-prohibited

-A FORWARD -j REJECT --reject-with icmp-host-prohibited