设置系统主机名以及 Host 文件的相互解析

hostnamectl set-hostname k8s-master01

安装依赖包

yum install -y conntrack ntpdate ntp ipvsadm ipset jq iptables curl sysstat libseccomp wget vim net-tools git

设置防火墙为 Iptables 并设置空规则

systemctl stop firewalld && systemctl disable firewalld

yum -y install iptables-services && systemctl start iptables && systemctl enable iptables && iptables -F && service iptables save

关闭 SELINUX

swapoff -a && sed -i '/ swap / s/^\(.\*\)$/#\1/g' /etc/fstab

setenforce 0 && sed -i 's/^SELINUX=.\*/SELINUX=disabled/' /etc/selinux/config 调整内核参数，对于 K8S

cat > kubernetes.conf <<EOF

net.bridge.bridge-nf-call-iptables=1

net.bridge.bridge-nf-call-ip6tables=1

net.ipv4.ip\_forward=1

net.ipv4.tcp\_tw\_recycle=0

vm.swappiness=0 # 禁止使用 swap 空间，只有当系统 OOM 时才允许使用它

vm.overcommit\_memory=1 # 不检查物理内存是否够用

vm.panic\_on\_oom=0 # 开启 OOM

fs.inotify.max\_user\_instances=8192

fs.inotify.max\_user\_watches=1048576

fs.file-max=52706963

fs.nr\_open=52706963

net.ipv6.conf.all.disable\_ipv6=1

net.netfilter.nf\_conntrack\_max=2310720

EOF

cp kubernetes.conf /etc/sysctl.d/kubernetes.conf

sysctl -p /etc/sysctl.d/kubernetes.conf

调整系统时区

# 设置系统时区为 中国/上海

timedatectl set-timezone Asia/Shanghai

# 将当前的 UTC 时间写入硬件时钟

timedatectl set-local-rtc 0

# 重启依赖于系统时间的服务

systemctl restart rsyslog

systemctl restart crond

关闭系统不需要服务

systemctl stop postfix && systemctl disable postfix

设置 rsyslogd 和 systemd journald

mkdir /var/log/journal # 持久化保存日志的目录

mkdir /etc/systemd/journald.conf.d

cat > /etc/systemd/journald.conf.d/99-prophet.conf <<EOF

[Journal]

# 持久化保存到磁盘

Storage=persistent

# 压缩历史日志

Compress=yes

SyncIntervalSec=5m

RateLimitInterval=30s

RateLimitBurst=1000

# 最大占用空间 10G

SystemMaxUse=10G

# 单日志文件最大 200M

SystemMaxFileSize=200M

# 日志保存时间 2 周

MaxRetentionSec=2week

# 不将日志转发到 syslog

ForwardToSyslog=no

EOF

systemctl restart systemd-journald

升级系统内核为 4.44

CentOS 7.x 系统自带的 3.10.x 内核存在一些 Bugs，导致运行的 Docker、Kubernetes 不稳定，例如： rpm -Uvh http://www.elrepo.org/elrepo-release-7.0-3.el7.elrepo.noarch.rpm

rpm -Uvh http://www.elrepo.org/elrepo-release-7.0-3.el7.elrepo.noarch.rpm

# 安装完成后检查 /boot/grub2/grub.cfg 中对应内核 menuentry 中是否包含 initrd16 配置，如果没有，再安装 一次！

yum --enablerepo=elrepo-kernel install -y kernel-lt

# 设置开机从新内核启动

grub2-set-default "CentOS Linux (4.4.182-1.el7.elrepo.x86\_64) 7 (Core)"

# 重启后安装内核源文件

yum --enablerepo=elrepo-kernel install kernel-lt-devel-$(uname -r) kernel-lt-headers-$(uname -r) 关闭 NUMA

cp /etc/default/grub{,.bak}

vim /etc/default/grub # 在 GRUB\_CMDLINE\_LINUX 一行添加 `numa=off` 参数，如下所示： diff /etc/default/grub.bak /etc/default/grub

6c6

< GRUB\_CMDLINE\_LINUX="crashkernel=auto rd.lvm.lv=centos/root rhgb quiet"

---

> GRUB\_CMDLINE\_LINUX="crashkernel=auto rd.lvm.lv=centos/root rhgb quiet numa=off" cp /boot/grub2/grub.cfg{,.bak}

grub2-mkconfig -o /boot/grub2/grub.cfg