**相关说明：**首先自我介绍（运维的技术栈比较宽泛，这里最好突出下自己最擅长的技能，引导面试官对你最擅长的提问）

以下面试题答对2/3才可以推荐，在回答问题的时候注意考察沟通能力，如果回答不流畅就不用推荐了。

**1、LINUX系统软件安装和卸载的常见方法**

**答：**A.rpm包卸载：rpm -e XXX.rpm (如果想忽略依赖，可加上–nodeps)

B.yum remove xxx.rpm 这种方法非常不建议使用，卸载过程会将待卸载的软件包所依赖的软件包一并卸载掉，很容易造成系统缺少某些包而崩溃等问题

C.源码包卸载：cd命令进入编译后的软件目录，即安装时的目录，执行make uninstall命令即可；或者直接删除安装目录

**2、如何修改LINUX的IP地址、网关和主机名**

**答：**A、修改IP地址、网关：编辑/etc/sysconfig/network-scripts/ifcfg-eth0，修改里面IPADDR和GATEWAY内容，没有这两行，则添加即可，添加时确保BOOTPROTO=static，静态地址，如IPADDR=192.168.1.100   GATEWAY=192.168.1.1

B、修改主机名称：编辑/etc/sysconfig/network，修改里面的HOSTNAME内容，如设置主机名称为mysql，则：HOSTNAME=mysql即可；

**3、删除 /a/b下的所有文件及目录**

**答：**[root@Ant ~]# rm -rf /a/b/\*

**4、常用的网络管理工具（5种以上）/**查看网络配置相关信息的命令

**答：**Linux下有：ifconfig,ping,tracerroute,dig,nslookup……

Windows下有：ipcofnig(/all,/renew,/release),ping,tracert,nslookup……

**5、如何查看http的并发请求数与其TCP连接状态？**

**答：**netstat -n | awk ‘/^tcp/ {++b[$NF]}’ END {for(a in b) print a,b[a]}’

还有ulimit -n 查看linux系统打开最大的文件描述符，这里默认1024，不修改这里web服务器修改再大也没用。若要用就修改很几个办法，这里说其中一个：  
修改/etc/security/limits.conf  
\* soft nofile 10240  
\* hard nofile 10240  
重启后生效

**6、如何查看/var/log目录下的文件数？**

**答：**ls /var/log/ -1R | grep “-” | wc –l

**7、云计算中有哪些不同的层？**

**答：**云计算的不同层包括：

a）SaaS：软件即服务，它让用户可以直接访问云应用程序，不必在系统上安装任何东西。  
b）IaaS：基础设施即服务，它从硬件（比如内存和处理器速度等）等层面提供了基础设施。  
c）PaaS：平台即服务，它为开发人员提供了云应用程序平台。

**8、LVS有哪些负载均衡方式？**

**答：**分别是：VS/NAT、VS/TUN、VS/DR、

**9、MYSQL的GTID复制模式相较于传统的复制有什么区别？**

**答：**基于GTID的复制是从Mysql5.6开始支持的一种新的复制方式，此方式与传统基于日志的方式存在很大的差异，在原来的基于日志的复制中，从服务器连接到主服务器并告诉主服务器要从哪个二进制日志的偏移量开始执行增量同步，这时我们如果指定的日志偏移量不对，这与可能造成主从数据的不一致，而基于GTID的复制会避免。  
在基于GTID的复制中，首先从服务器会告诉主服务器已经在从服务器执行完了哪些事务的GTID值，然后主库会有把所有没有在从库上执行的事务，发送到从库上进行执行，并且使用GTID的复制可以保证同一个事务只在指定的从库上执行一次，这样可以避免由于偏移量的问题造成数据不一致。

**10.如果忘记mysql root密码怎么办？**

**答：**

关闭当前运行的mysqld服务程序：service mysqld stop（要先将mysqld添加为系统服务）  
2、 使用mysqld\_safe脚本以安全模式（不加载授权表）启动mysqld 服务  
/usr/local/mysql/bin/mysqld\_safe –skip-grant-table &  
3、 使用空密码的root用户登录数据库，重新设置ROOT用户的密码  
＃mysql -u root  
Mysql> Update mysql.user set password=password(‘新密码’) where user=’root’;  
Mysql> flush privileges;

**11、如何查看Nginx进程？**

**答：**ps –A | grep nginx

**12、如何查看linux网卡实时流量？**

查看网络状态可以使用netstat、nmap等工具。若要查看实时的网络流量，监控TCP/IP连接等，则可以使用iftop。

**13、如何将A服务器上的文件夹传到到B服务器上？具体操作命令是什么？**

**答：**1.可以通过sftp、scp传输，具体操作如下：

scp –r /home/admin [root@1.1.1.1:/home/admin/test](mailto:root@1.1.1.1:/home/admin/test)

说明：

-r 表示传输文件夹，若不带参数只能传输单个文件

2.在被传输的服务器上配置sftp服务器，然后可以在传输端登录后选择性的传输。

**14、如何将linux下的/tmp/test目录打包成/home/test/test.zip**

**答：**具体操作：zip –r –q /home/test/test.zip /tmp/test

**更难的题**

**1.raid0 raid1 raid5 raid10 有什么区别，哪个更有优势，为什么？**

RAID，可以把硬盘整合成一个大磁盘，还可以在大磁盘上再分区，放数据  
还有一个大功能，多块盘放在一起可以有冗余（备份）  
RAID整合方式有很多，常用的：0 1 5 10

RAID 0，可以是一块盘和N个盘组合   
其优点读写快，是RAID中最好的  
缺点：没有冗余，一块坏了数据就全没有了

RAID 1，只能2块盘，盘的大小可以不一样，以小的为准  
10G+10G只有10G，另一个做备份。它有100%的冗余，缺点：浪费资源，成本高

RAID 5 ，3块盘，容量计算10\*（n-1）,损失一块盘  
特点，读写性能一般，读还好一点，写不好

冗余从好到坏：RAID1 RAID10 RAID 5 RAID0  
性能从好到坏：RAID0 RAID10 RAID5 RAID1  
成本从低到高：RAID0 RAID5 RAID1 RAID10

单台服务器：很重要盘不多，系统盘，RAID1  
数据库服务器：主库：RAID10 从库 RAID5RAID0（为了维护成本，RAID10）  
WEB服务器，如果没有太多的数据的话，RAID5,RAID0（单盘）  
有多台，监控、应用服务器，RAID0 RAID5

我们会根据数据的存储和访问的需求，去匹配对应的RAID级别

**2.HAproxy、LVS、Nginx、有什么区别？工作中如何选择？**

LVS： 是基于四层的转发  
HAproxy： 是基于四层和七层的转发，是专业的代理服务器  
Nginx： 是WEB服务器，缓存服务器，又是反向代理服务器，可以做七层的转发

区别： LVS由于是基于四层的转发所以只能做端口的转发  
而基于URL的、基于目录的这种转发LVS就做不了

工作选择：

HAproxy和Nginx由于可以做七层的转发，所以URL和目录的转发都可以做  
在很大并发量的时候我们就要选择LVS，像中小型公司的话并发量没那么大  
选择HAproxy或者Nginx足已，由于HAproxy由是专业的代理服务器  
配置简单，所以中小型企业推荐使用HAproxy

**3.什么是代理服务器？请描述下使用场景。**

能当替用户去访问公网，并且能把访问到的数据缓存到服务器本地，等用户下次再访问相同的资  
源的时候，代理服务器直接从本地回应给用户，当本地没有的时候，我代替你去访问公网，我接  
收你的请求，我先在我自已的本地缓存找，如果我本地缓存有，我直接从我本地的缓存里回复你  
如果我在我本地没有找到你要访问的缓存的数据，那么代理服务器就会代替你去访问公网.

**4.请描述Tomcat：8005、8009、8080三个端口的含义？**

8005==》 关闭时使用

8009==》 为AJP端口，即容器使用，如Apache能通过AJP协议访问Tomcat的8009端口

8080==》 一般应用使用

**5.请详解Keepalived的工作原理和使用场景。**

在一个虚拟路由器中，只有作为MASTER的VRRP路由器会一直发送VRRP通告信息,  
BACKUP不会抢占MASTER，除非它的优先级更高。当MASTER不可用时(BACKUP收不到通告信息)  
多台BACKUP中优先级最高的这台会被抢占为MASTER。这种抢占是非常快速的(<1s)，以保证服务的连续性  
由于安全性考虑，VRRP包使用了加密协议进行加密。BACKUP不会发送通告信息，只会接收通告信息

**6.LVS三种模式的工作过程是什么？**

LVS 有三种负载均衡的模式，分别是VS/NAT（nat 模式） VS/DR(路由模式) VS/TUN（隧道模式）

一、NAT模式（VS-NAT）

原理：就是把客户端发来的数据包的IP头的目的地址，在负载均衡器上换成其中一台RS的IP地址

并发至此RS来处理,RS处理完后把数据交给负载均衡器,负载均衡器再把数据包原IP地址改为自己的IP

将目的地址改为客户端IP地址即可期间,无论是进来的流量,还是出去的流量,都必须经过负载均衡器

优点：集群中的物理服务器可以使用任何支持TCP/IP操作系统，只有负载均衡器需要一个合法的IP地址

缺点：扩展性有限。当服务器节点（普通PC服务器）增长过多时,负载均衡器将成为整个系统的瓶颈

因为所有的请求包和应答包的流向都经过负载均衡器。当服务器节点过多时

大量的数据包都交汇在负载均衡器那，速度就会变慢！

二、IP隧道模式（VS-TUN）

原理：首先要知道，互联网上的大多Internet服务的请求包很短小，而应答包通常很大

那么隧道模式就是，把客户端发来的数据包，封装一个新的IP头标记(仅目的IP)发给RS

RS收到后,先把数据包的头解开,还原数据包,处理后,直接返回给客户端,不需要再经过

负载均衡器。注意,由于RS需要对负载均衡器发过来的数据包进行还原,所以说必须支持

IPTUNNEL协议，所以,在RS的内核中,必须编译支持IPTUNNEL这个选项

优点：负载均衡器只负责将请求包分发给后端节点服务器，而RS将应答包直接发给用户

所以，减少了负载均衡器的大量数据流动，负载均衡器不再是系统的瓶颈，就能处理很巨大的请求量

这种方式，一台负载均衡器能够为很多RS进行分发。而且跑在公网上就能进行不同地域的分发。

缺点：隧道模式的RS节点需要合法IP，这种方式需要所有的服务器支持”IP Tunneling”

(IP Encapsulation)协议，服务器可能只局限在部分Linux系统上

三、直接路由模式（VS-DR）

原理：负载均衡器和RS都使用同一个IP对外服务但只有DR对ARP请求进行响应

所有RS对本身这个IP的ARP请求保持静默也就是说,网关会把对这个服务IP的请求全部定向给DR

而DR收到数据包后根据调度算法,找出对应的RS,把目的MAC地址改为RS的MAC（因为IP一致）

并将请求分发给这台RS这时RS收到这个数据包,处理完成之后，由于IP一致，可以直接将数据返给客户

则等于直接从客户端收到这个数据包无异,处理后直接返回给客户端

由于负载均衡器要对二层包头进行改换,所以负载均衡器和RS之间必须在一个广播域

也可以简单的理解为在同一台交换机上

优点：和TUN（隧道模式）一样，负载均衡器也只是分发请求，应答包通过单独的路由方法返回给客户端

与VS-TUN相比，VS-DR这种实现方式不需要隧道结构，因此可以使用大多数操作系统做为物理服务器。

缺点：（不能说缺点，只能说是不足）要求负载均衡器的网卡必须与物理网卡在一个物理段上。

**7.mysql如何减少主从复制延迟？**

mysql的innodb如何定位锁问题:

在使用 show engine innodb status检查引擎状态时，发现了死锁问题

在5.5中，information\_schema 库中增加了三个关于锁的表（MEMORY引擎）

innodb\_trx ## 当前运行的所有事务

innodb\_locks ## 当前出现的锁

innodb\_lock\_waits ## 锁等待的对应关系

mysql如何减少主从复制延迟:

如果延迟比较大，就先确认以下几个因素：

从库硬件比主库差，导致复制延迟

主从复制单线程，如果主库写并发太大，来不及传送到从库

就会导致延迟。更高版本的mysql可以支持多线程复制

慢SQL语句过多

网络延迟

master负载

主库读写压力大，导致复制延迟，架构的前端要加buffer及缓存层

slave负载

一般的做法是，使用多台slave来分摊读请求，再从这些slave中取一台专用的服务器

只作为备份用，不进行其他任何操作.另外， 2个可以减少延迟的参数:

–slave-net-timeout=seconds 单位为秒 默认设置为 3600秒

参数含义：当slave从主数据库读取log数据失败后，等待多久重新建立连接并获取数据

–master-connect-retry=seconds 单位为秒 默认设置为 60秒

参数含义：当重新建立主从连接时，如果连接建立失败，间隔多久后重试

通常配置以上2个参数可以减少网络问题导致的主从数据同步延迟

MySQL数据库主从同步延迟解决方案

最简单的减少slave同步延时的方案就是在架构上做优化，尽量让主库的DDL快速执行

还有就是主库是写，对数据安全性较高，比如sync\_binlog=1，innodb\_flush\_log\_at\_trx\_commit

= 1 之类的设置，而slave则不需要这么高的数据安全，完全可以讲sync\_binlog设置为0或者关闭binlog

innodb\_flushlog也可以设置为0来提高sql的执行效率。另外就是使用比主库更好的硬件设备作为slave

**8.如何重置mysql root密码？**

一、 在已知MYSQL数据库的ROOT用户密码的情况下，修改密码的方法：

1、 在SHELL环境下，使用mysqladmin命令设置：

mysqladmin –u root –p password “新密码” 回车后要求输入旧密码

2、 在mysql>环境中,使用update命令，直接更新mysql库user表的数据：

Update mysql.user set password=password(‘新密码’) where user=’root’;

flush privileges;

注意：mysql语句要以分号”；”结束

3、 在mysql>环境中，使用grant命令，修改root用户的授权权限。

grant all on . to root@’localhost’ identified by ‘新密码’；

二、 如查忘记了mysql数据库的ROOT用户的密码，又如何做呢？方法如下：

1、 关闭当前运行的mysqld服务程序：service mysqld stop（要先将mysqld添加为系统服务）

2、 使用mysqld\_safe脚本以安全模式（不加载授权表）启动mysqld 服务

/usr/local/mysql/bin/mysqld\_safe –skip-grant-table &

3、 使用空密码的root用户登录数据库，重新设置ROOT用户的密码

＃mysql -u root

Mysql> Update mysql.user set password=password(‘新密码’) where user=’root’;

Mysql> flush privileges;

**9.lvs/nginx/haproxy优缺点是什么？**

Nginx的优点是：  
1、工作在网络的7层之上，可以针对http应用做一些分流的策略，比如针对域名、目录结构  
它的正则规则比HAProxy更为强大和灵活，这也是它目前广泛流行的主要原因之一  
Nginx单凭这点可利用的场合就远多于LVS了。

2、Nginx对网络稳定性的依赖非常小，理论上能ping通就就能进行负载功能，这个也是它的优势之一  
相反LVS对网络稳定性依赖比较大，这点本人深有体会；

3、Nginx安装和配置比较简单，测试起来比较方便，它基本能把错误用日志打印出来  
LVS的配置、测试就要花比较长的时间了，LVS对网络依赖比较大。

4、可以承担高负载压力且稳定，在硬件不差的情况下一般能支撑几万次的并发量，负载度比LVS相对小些。

5、Nginx可以通过端口检测到服务器内部的故障，比如根据服务器处理网页返回的状态码、超时等等，并且会把返回错误的请求重新提交到另一个节点，不过其中缺点就是不支持url来检测。比如用户正在上传一个文件，而处理该上传的节点刚好在上传过程中出现故障，Nginx会把上传切到另一台服务器重新处理，而LVS就直接断掉了  
如果是上传一个很大的文件或者很重要的文件的话，用户可能会因此而不满。

6、Nginx不仅仅是一款优秀的负载均衡器/反向代理软件，它同时也是功能强大的Web应用服务器  
LNMP也是近几年非常流行的web架构，在高流量的环境中稳定性也很好。

7、Nginx现在作为Web反向加速缓存越来越成熟了，速度比传统的Squid服务器更快，可考虑用其作为反向代理加速器

8、Nginx可作为中层反向代理使用，这一层面Nginx基本上无对手，唯一可以对比Nginx的就只有lighttpd了  
不过lighttpd目前还没有做到Nginx完全的功能，配置也不那么清晰易读，社区资料也远远没Nginx活跃

9、Nginx也可作为静态网页和图片服务器，这方面的性能也无对手。还有Nginx社区非常活跃，第三方模块也很多

Nginx的缺点是：  
1、Nginx仅能支持http、https和Email协议，这样就在适用范围上面小些，这个是它的缺点  
2、对后端服务器的健康检查，只支持通过端口来检测，不支持通过url来检测  
不支持Session的直接保持，但能通过ip\_hash来解决

LVS：使用Linux内核集群实现一个高性能、高可用的负载均衡服务器  
它具有很好的可伸缩性（Scalability)、可靠性（Reliability)和可管理性（Manageability)

LVS的优点是：  
1、抗负载能力强、是工作在网络4层之上仅作分发之用，没有流量的产生  
这个特点也决定了它在负载均衡软件里的性能最强的，对内存和cpu资源消耗比较低

2、配置性比较低，这是一个缺点也是一个优点，因为没有可太多配置的东西  
所以并不需要太多接触，大大减少了人为出错的几率

3、工作稳定，因为其本身抗负载能力很强，自身有完整的双机热备方案  
如LVS+Keepalived，不过我们在项目实施中用得最多的还是LVS/DR+Keepalived

4、无流量，LVS只分发请求，而流量并不从它本身出去，这点保证了均衡器IO的性能不会收到大流量的影响。  
5、应用范围较广，因为LVS工作在4层，所以它几乎可对所有应用做负载均衡，包括http、数据库、在线聊天室等

LVS的缺点是：  
1、软件本身不支持正则表达式处理，不能做动静分离  
而现在许多网站在这方面都有较强的需求，这个是Nginx/HAProxy+Keepalived的优势所在  
2、如果是网站应用比较庞大的话，LVS/DR+Keepalived实施起来就比较复杂了  
特别后面有Windows Server的机器的话，如果实施及配置还有维护过程就比较复杂了  
相对而言，Nginx/HAProxy+Keepalived就简单多了。

HAProxy的特点是：  
1、HAProxy也是支持虚拟主机的。  
2、HAProxy的优点能够补充Nginx的一些缺点，比如支持Session的保持，Cookie的引导  
同时支持通过获取指定的url来检测后端服务器的状态

3、HAProxy跟LVS类似，本身就只是一款负载均衡软件  
单纯从效率上来讲HAProxy会比Nginx有更出色的负载均衡速度，在并发处理上也是优于Nginx的

4、HAProxy支持TCP协议的负载均衡转发，可以对MySQL读进行负载均衡  
对后端的MySQL节点进行检测和负载均衡，大家可以用LVS+Keepalived对MySQL主从做负载均衡

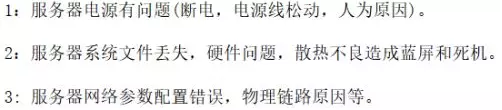
5、HAProxy负载均衡策略非常多，HAProxy的负载均衡算法现在具体有如下8种：  
①roundrobin，表示简单的轮询，这个不多说，这个是负载均衡基本都具备的；  
② static-rr，表示根据权重，建议关注；  
③leastconn，表示最少连接者先处理，建议关注；  
④ source，表示根据请求源IP，这个跟Nginx的IP\_hash机制类似  
我们用其作为解决session问题的一种方法，建议关注；  
⑤ri，表示根据请求的URI；  
⑥rl\_param，表示根据请求的URl参数’balance url\_param’ requires an URL parameter name；  
⑦hdr(name)，表示根据HTTP请求头来锁定每一次HTTP请求；  
⑧rdp-cookie(name)，表示根据据cookie(name)来锁定并哈希每一次TCP请求。

**10.统计ip访问情况，要求分析nginx访问日志，找出访问页面数量在前十位的ip，请使用具体命令描述？**

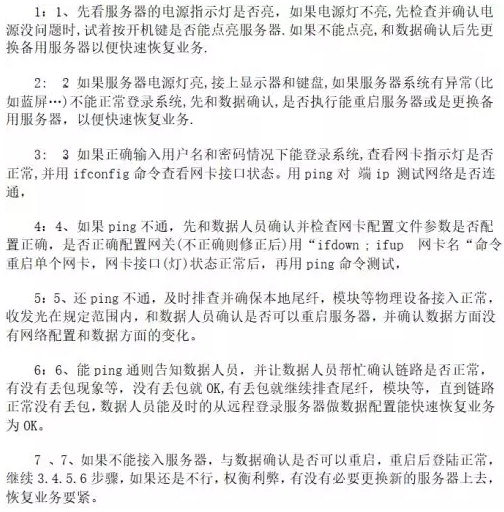
cat access.log | awk ‘{print $1}’ | uniq -c | sort -rn | head -10

**11.服务器开不了机怎么解决一步步的排查？**

A、造成服务器故障的原因可能有以下几点：



B、如何排查服务器故障的处理步骤如下：



**12.Linux系统中病毒怎么解决？**

1）最简单有效的方法就是重装系统  
2）要查的话就是找到病毒文件然后删除  
中毒之后一般机器cpu、内存使用率会比较高  
机器向外发包等异常情况，排查方法简单介绍下

top 命令找到cpu使用率最高的进程  
一般病毒文件命名都比较乱，可以用 ps aux 找到病毒文件位置   
rm -f 命令删除病毒文件  
检查计划任务、开机启动项和病毒文件目录有无其他可以文件等

3）由于即使删除病毒文件不排除有潜伏病毒，所以最好是把机器备份数据之后重装一下

**13.请详解TCP/IP的七层模型**

应用层 (Application)：

网络服务与最终用户的一个接口。

协议有：HTTP FTP TFTP SMTP SNMP DNS TELNET HTTPS POP3 DHCP

表示层（Presentation Layer）：

数据的表示、安全、压缩。（在五层模型里面已经合并到了应用层）

格式有，JPEG、ASCll、DECOIC、加密格式等

会话层（Session Layer）：

建立、管理、终止会话。（在五层模型里面已经合并到了应用层）

对应主机进程，指本地主机与远程主机正在进行的会话

传输层 (Transport)：

定义传输数据的协议端口号，以及流控和差错校验。

协议有：TCP UDP，数据包一旦离开网卡即进入网络传输层

网络层 (Network)：

进行逻辑地址寻址，实现不同网络之间的路径选择。

协议有：ICMP IGMP IP（IPV4 IPV6） ARP RARP

数据链路层 (Link)：

建立逻辑连接、进行硬件地址寻址、差错校验等功能。（由底层网络定义协议）

将比特组合成字节进而组合成帧，用MAC地址访问介质，错误发现但不能纠正

物理层（Physical Layer）：

是计算机网络OSI模型中最低的一层

物理层规定:为传输数据所需要的物理链路创建、维持、拆除

而提供具有机械的，电子的，功能的和规范的特性

简单的说，物理层确保原始的数据可在各种物理媒体上传输。局域网与广域网皆属第1、2层

物理层是OSI的第一层，它虽然处于最底层，却是整个开放系统的基础

物理层为设备之间的数据通信提供传输媒体及互连设备，为数据传输提供可靠的环境

如果您想要用尽量少的词来记住这个第一层，那就是“信号和介质”

**14.你常用的Nginx模块，具体做什么？**

rewrite模块，实现重写功能

access模块：来源控制

ssl模块：安全加密

ngx\_http\_gzip\_module：网络传输压缩模块

ngx\_http\_proxy\_module 模块实现代理

ngx\_http\_upstream\_module模块实现定义后端服务器列表

ngx\_cache\_purge实现缓存清除功能

**15.用tcpdump嗅探80端口的访问看看谁最高？**

tcpdump -i eth0 -tnn dst port 80 -c 1000 | awk -F”.” ‘{print $1″.”$2″.”$3″.”$4}’| sort | uniq -c | sort -nr |head -20

**16.已知Apache服务的访问日志按天记录在服务器本地目录/app/logs下，由于磁盘空间紧张现在要求只能保留最近7天的访问日志！请问如何解决？ 请给出解决方法或配置或处理命令？**

创建文件脚本：

!/bin/bash

for n in seq 14  
do   
date -s “11/0$n/14”  
touch access\_www\_(date +%F).log  
done

解决方法：

pwd/application/logs

ll

-rw-r–r–. 1 root root 0 Jan 1 00:00 access\_www\_2015-01-01.log  
-rw-r–r–. 1 root root 0 Jan 2 00:00 access\_www\_2015-01-02.log  
-rw-r–r–. 1 root root 0 Jan 3 00:00 access\_www\_2015-01-03.log  
-rw-r–r–. 1 root root 0 Jan 4 00:00 access\_www\_2015-01-04.log  
-rw-r–r–. 1 root root 0 Jan 5 00:00 access\_www\_2015-01-05.log  
-rw-r–r–. 1 root root 0 Jan 6 00:00 access\_www\_2015-01-06.log  
-rw-r–r–. 1 root root 0 Jan 7 00:00 access\_www\_2015-01-07.log  
-rw-r–r–. 1 root root 0 Jan 8 00:00 access\_www\_2015-01-08.log  
-rw-r–r–. 1 root root 0 Jan 9 00:00 access\_www\_2015-01-09.log  
-rw-r–r–. 1 root root 0 Jan 10 00:00 access\_www\_2015-01-10.log  
-rw-r–r–. 1 root root 0 Jan 11 00:00 access\_www\_2015-01-11.log  
-rw-r–r–. 1 root root 0 Jan 12 00:00 access\_www\_2015-01-12.log  
-rw-r–r–. 1 root root 0 Jan 13 00:00 access\_www\_2015-01-13.log  
-rw-r–r–. 1 root root 0 Jan 14 00:00 access\_www\_2015-01-14.log

find /application/logs/ -type f -mtime +7 -name “\*.log”|xargs rm –f

也可以使用-exec rm -f {} ;进行删除

-rw-r–r–. 1 root root 0 Jan 7 00:00 access\_www\_2015-01-07.log  
-rw-r–r–. 1 root root 0 Jan 8 00:00 access\_www\_2015-01-08.log  
-rw-r–r–. 1 root root 0 Jan 9 00:00 access\_www\_2015-01-09.log  
-rw-r–r–. 1 root root 0 Jan 10 00:00 access\_www\_2015-01-10.log  
-rw-r–r–. 1 root root 0 Jan 11 00:00 access\_www\_2015-01-11.log  
-rw-r–r–. 1 root root 0 Jan 12 00:00 access\_www\_2015-01-12.log  
-rw-r–r–. 1 root root 0 Jan 13 00:00 access\_www\_2015-01-13.log  
-rw-r–r–. 1 root root 0 Jan 14 00:00 access\_www\_2015-01-14.log

**17.查看http的并发请求数与其TCP连接状态？**

netstat -n | awk ‘/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}’

还有ulimit -n 查看linux系统打开最大的文件描述符，这里默认1024  
不修改这里web服务器修改再大也没用，若要用就修改很几个办法，这里说其中一个：  
修改/etc/security/limits.conf

soft nofile 10240

hard nofile 10240  
重启后生效