**Linux运维面试题**

1. **linux 下常用的DNS服务软件是什么，举出几种常用的DNS记录，如果域名abc.com**

**配置好了一台邮件服务器,IP 地址为202.106.0.20，我该如何做相关的解析？是否了解**

**bind 的智能解析，如果了解请简述一下其原理**

**答案：**

**1)常用的DNS 软件是bind**

**2)A 记录 地址记录**

**MX 记录 邮件交换记录**

**CNAME 记录 别名域记录**

**3)修改abc.com 域名的配置文件，增加以下记录**

**IN MX 10 mail.abc.com.**

**mail IN A 202.106.0.20**

**4)bind 根据请求解析客户端的IP 地址，做出不同的解析，其原理是在配置文件中，设定了**

**view，在每个view 都有客户端的IP 地址段，bind 服务器根据请求解析客户端的IP 地址，**

**匹配不同的view,再根据该view 的配置，到相应的配置文件进行查询，将结果返回给请求**

**的客户端。**

**2.如何用mysql 命令进行备份和恢复？以test 库为例，创建一个备份，并再用此备份**

**进行恢复。**

**mysqldump -u root -p test > test.sql**

**mysql -u root -p test < test.sql**

**//主要考对方msqldump > test.sql 和 mysql < test.sql**

**3.主机A和B 的网络是通的，最少列出五种传输文件的服务**

**nfs ,ftp,scp ,rsync,samba,http://**

**4.在Shell 环境下,如何查看远程Linux 系统运行了多少时间?**

**监控主机执行： ssh user@被监控主机ip "uptime"**

**5．系统中有用户user1 和user2，同属于users 组。在user1 用户目录下有一文件file1，**

**它拥有644 的权限，如果user2 用户想修改user1 用户目录下的file1 文件，应拥有 B 权**

**限。**

**A 744 B 664  C 646 D 746**

**6 如果想配置一台匿名ftp 服务器，应修改 C 文件。**

**A /etc/gateway**

**B /etc/ftpservers**

**C /etc/ftpusers**

**D /etc/inetd.conf**

**7. Samba 服务器的进程由B 两部分组成 。**

**A named 和sendmail**

**Bsmbd 和nmbd**

**C bootp 和dhcpd**

**D httpd 和squid**

**8. 要配置NFS 服务器，在服务器端主要配置 C 文件。**

**A /etc/rc.d/rc.inet1**

**B /etc/rc.d/rc.M**

**C /etc/exports**

**D /etc/rc.d/rc.S**

**9. 简述Linux 文件系统通过i 节点把文件的逻辑结构和物理结构转换的工作过程。**

**参考答案：**

**Linux 通过i 节点表将文件的逻辑结构和物理结构进行转换。**

**i 节点是一个64 字节长的表，表中包含了文件的相关信息，其中有文件的大小、文件所有**

**者、文件的存取许可方式以及文件的类型等重要信息。在i 节点表中最重要 的内容是磁盘地址表 。在磁盘地址表中有13 个块号，文件将以块号在磁盘地址表中出现的顺序依次读取相应的块。Linux 文件系统通过把i 节点和文件名进行 连接，当需要读取该文件时，文件系统在当前目录表中查找该文件名对应的项，由此得到该文件相对应的i 节点号，通过该 i 节点的磁盘地址表把分散存放的文件物 理块连接成文件的逻辑结构。**

**10.简述进程的启动、终止的方式以及如何进行进程的查看。**

**参考答案：**

**在Linux 中启动一个进程有手工启动和调度启动两种方式：**

**（1）手工启动**

**用户在输入端发出命令，直接启动一个进程的启动方式。可以分为：**

**①前台启动：直接在SHELL 中输入命令进行启动。**

**②后台启动：启动一个目前并不紧急的进程，如打印进程。**

**（2）调度启动**

**系统管理员根据系统资源和进程占用资源的情况，事先进行调度安排，指定任务运行的时间**

**和场合，到时候系统会自动完成该任务。**

**经常使用的进程调度命令为：at、batch、crontab。**

**11.简述DNS 进行域名解析的过程。**

**参考答案：**

**首先，客户端发出DNS 请求翻译IP 地址或主机名。DNS 服务器在收到客户机的请求后：**

**（1）检查DNS 服务器的缓存，若查到请求的地址或名字，即向客户机发出应答信息；**

**（2）若没有查到，则在数据库中查找，若查到请求的地址或名字，即向客户机发出应答信息；**

**（3）若没有查到，则将请求发给根域DNS 服务器，并依序从根域查找顶级域，由顶级查找二级域，二级域查找三级，直至找到要解析的地址或名字，即向客户机所在网络的DNS**

**服务器发出应答信息，DNS 服务器收到应答后现在缓存中存储，然后，将解析结果发给客户机。**

1. **若没有找到，则返回错误信息。**

**12.简述安装Slackware Linux 系统的过程。**

**参考答案：**

**（1）对硬盘重新分区。**

**（2）启动Linux 系统（用光盘、软盘等）。**

**（3）建立Linux 主分区和交换分区。**

**（4）用setup 命令安装Linux 系统。**

**（5）格式化Linux 主分区和交换分区**

**（6）安装Linux 软件包**

**（7）安装完毕，建立从硬盘启动Linux 系统的LILO 启动程序，或者制作一张启动Linux系统的软盘。重新启动Linux 系统。**

**13.什么是静态路由，其特点是什么？什么是动态路由，其特点是什么？**

**参考答案：**

**静态路由是由系统管理员设计与构建的路由表规定的路由。适用于网关数量有限的场合，且网络拓朴结构不经常变化的网络。其缺点是不能动态地适用网络状况的变化，当网络状况变化后必须由网络管理员修改路由表。**

**动态路由是由路由选择协议而动态构建的，路由协议之间通过交换各自所拥有的路由信息实时更新路由表的内容。动态路由可以自动 学习 网络的拓朴结构，并更新路由表。其缺点是路由广播更新信息将占据大量的网络带宽。**

**14.进程的查看和调度分别使用什么命令？**

**参考答案：**

**进程查看的命令是ps 和top。**

**进程调度的命令有at，crontab，batch，kill。**

**15.当文件系统受到破坏时，如何检查和修复系统？**

**参考答案：**

**成功修复文件系统的前提是要有两个以上的主文件系统，并保证在修复之前首先卸载将被修复的文件系统。**

**使用命令fsck 对受到破坏的文件系统进行修复。fsck 检查文件系统分为5 步，每一步检查系统不同部分的连接特性并对上一步进行验证和修改。在执行 fsck 命令时，检查首先从超级块开始，然后是分配的磁盘块、路径名、目录的连接性、链接数目以及空闲块链表、i-node。**

**16.什么是符号链接，什么是硬链接？符号链接与硬链接的区别是什么？**

**参考答案：**

**链接分硬链接和符号链接。符号链接可以建立对于文件和目录的链接。符号链接可以跨文件系统，即可以跨磁盘分区。符号链接的文件类型位是l，链接文件具有新的i 节点。硬链接不可以跨文件系统。它只能建立对文件的链接，硬链接的文件类型位是－，且硬链接文件的i 节点同被链接文件的i 节点相同。**

**17.在对linux 系统分区进行格式化时需要对磁盘簇（或i 节点密度）的大小进行选择，请**

**说明选择的原则。**

**参考答案：**

**磁盘簇（或i 节点密度）是文件系统调度文件的基本单元。磁盘簇的大小，直接影响系统调度磁盘空间效率。当磁盘分区较大时，磁盘簇也应选得大些；当分区较小时，磁盘簇应选得小些。通常使用经验值。**

**18.简述网络文件系统NFS，并说明其作用。**

**参考答案：**

**网络文件系统是应用层的一种应用服务，它主要应用于Linux 和Linux 系统、Linux 和Unix系统之间的文件或目录的共享。对于用户而言可以通过 NFS 方便的访问远地的文件系统，使之成为本地文件系统的一部分。采用NFS 之后省去了登录的过程，方便了用户访问系统资源。**

**19.Linux系统的开机启动顺序**

**加载BIOS–>读取MBR–>Boot Loader–>加载内核–>用户层init一句inittab文件来设定系统运行的等级(一般3或者5，3是多用户命令行，5是界面)–>init进程执行rc.syninit–>启动内核模块–>执行不同级别运行的脚本程序–>执行/etc/rc.d/rc.local(本地运行服务)–>执行/bin/login,就可以登录了。**

**20.Apache 服务器的配置文件httpd.conf 中有很多内容，请解释如下配置项：**

**（1）MaxKeepAliveRequests 200 （2）UserDir public\_html**

**（3）DefaultType text/plain （4）AddLanguare en.en**

**（5）DocumentRoot“/usr/local/httpd/htdocs”**

**（6）AddType application/x-httpd-php.php.php.php4**

**参考答案:**

**（1）允许每次连接的最大请求数目，此为200；（2）设定用户放置网页的目录；**

**（3）设置服务器对于不认识的文件类型的预设格式；**

**（4）设置可传送语言的文件给浏览器；（5）该目录为Apache 放置网页的地方；**

**（ 6）服务器选择使用php4。**

**21.某Linux 主机的/etc/rc.d/rc.inet1 文件中有如下语句，请修正错误，并解释其内容。**

**/etc/rc.d/rc.inet1：**

**……**

**ROUTE add –net default gw 192.168.0.101 netmask 255.255.0.0 metric 1**

**ROUTE add –net 192.168.1.0 gw 192.168.0.250 netmask 255.255.0.0 metric 1**

**参考答案:**

**修正错误:**

**（1）ROUTE 应改为小写：route；（2）netmask 255.255.0.0 应改为:netmask**

**255.255.255.0；**

**（3）缺省路由的子网掩码应改为:netmask 0.0.0.0；**

**（4）缺省路由必须在最后设定,否则其后的路由将无效。**

**解释内容:**

**（1）route：建立静态路由表的命令；（2）add：增加一条新路由；**

**（3）-net 192.168.1.0：到达一个目标网络的网络地址；**

**（4）default：建立一条缺省路由；（5）gw 192.168.0.101：网关地址；**

**（6）metric 1：到达目标网络经过的 路由器 数（跳数）。**

**22.试解释apache 服务器以下配置的含义：**

**（1）port 1080 （2）UserDir userdoc**

**（3）DocumentRoot “/home/htdocs”**

**（4）;**

**Options Indexes FollowSymLinks**

**AllowOverride None**

**Order deny,allow**

**deny from all**

**allow from 192.168.1.5**

**;**

**（5）Server Type Standlone**

**考答案：**

**Apache 服务器配置行含义如下：**

**（1）将apache 服务器的端口号设定为1080；**

**（2）设定用户网页目录为userdoc；**

**（3）设定apache 服务器的网页根目录:/home/htdocs；**

**（4）在此apache 服务器上设定一个目录/home/htdocs/inside，且此目录只允许IP 地**

**址为192.168.1.5 的主机访问；**

**（5）定义apache 服务器以独立进程的方式运行。**

**23.简述使用ftp 进行文件传输时的两种登录方式？它们的区别是什么？常用的ftp 文件传**

**输命令是什么？**

**参考答案：**

**（1）ftp 有两种登录方式：匿名登录和授权登录。使用匿名登录时，用户名为：anonymous，**

**密码为：任何合法email 地址；使用授权登录时，用户名为用户在远程系统中的用户帐号，**

**密码为用户在远程系统中的用户密码。**

**区别：使用匿名登录只能访问ftp 目录下的资源，默认配置下只能下载；而授权登录访问的**

**权限大于匿名登录，且上载、下载均可。**

**（2）ftp 文件传输有两种文件传输模式：ASCII 模式和binary 模式。ASCII 模式用来传**

**输文本文件，其他文件的传输使用binary 模式。**

**（3）常用的ftp 文件传输命令为：bin、asc、put、get、mput、mget、prompt、bye**

**24.用Shell 编程，判断一文件是不是字符设备文件，如果是将其拷贝到 /dev 目录下。**

**参考程序：**

**#!/bin/sh**

**FILENAME=**

**echo “Input file name：”**

**read FILENAME**

**if [ -c "$FILENAME" ]**

**then**

**cp $FILENAME /dev**

**fi**

**25.某系统管理员需每天做一定的重复工作，请按照下列要求，编制一个解决 方案 ：**

**（1）在下午4 :50 删除/abc 目录下的全部子目录和全部文件；**

**（2）从早8:00～下午6:00 每小时读取/xyz 目录下x1 文件中每行第一个域的全部数据**

**加入到/backup 目录下的bak01.txt 文件内；**

**（3）每逢星期一下午5:50 将/data 目录下的所有目录和文件归档并压缩为文件：**

**backup.tar.gz；**

**（4）在下午5:55 将IDE 接口的CD-ROM 卸载（假设：CD-ROM 的设备名为hdc）；**

**（5）在早晨8:00 前开机后启动。**

**参考答案:**

**解决方案：**

**（1）用vi 创建编辑一个名为prgx 的crontab 文件；**

**prgx 文件的内容：**

**50 16 \* \* \* rm -r /abc/\***

**（2）、0 8-18/1 \* \* \* cut -f1 /xyz/x1 >;>; /backup/bak01.txt**

**（3）、50 17 \* \* \* tar zcvf backup.tar.gz /data**

**（4）、55 17 \* \* \* umount /dev/hdc**

**（5）、由超级用户登录，用crontab 执行 prgx 文件中的内容：**

**root@xxx:#crontab prgx；在每日早晨8:00 之前开机后即可自动启动crontab。**

**26.有一普通用户想在每周日凌晨零点零分定期备份/user/backup 到/tmp 目录下，该用**

**户应如何做？**

**参考答案：（1）第一种方法：**

**用户应使用crontab –e 命令创建crontab 文件。格式如下：**

**0 0 \* \* sun cp –r /user/backup /tmp**

1. **Linux设备中字符设备与块设备有什么主要的区别？请分别列举一些实际的设备说出它们是属于哪一类设备。**

**参考答案：**

**字符设备：字符设备是个能够像字节流（类似文件）一样被访问的设备，由字符设备驱动程序来实现这种特性。字符设备驱动程序通常至少实现open,close,read和write系统调用。字符终端、串口、鼠标、键盘、摄像头、声卡和显卡等就是典型的字符设备。**

**块设备：和字符设备类似，块设备也是通过/dev目录下的文件系统节点来访问。块设备上能够容纳文件系统，如：u盘，SD卡，磁盘等。 字符设备和块设备的区别仅仅在于内核内部管理数据的方式，也就是内核及驱动程序之间的软件接口，而这些不同对用户来讲是透明的。**

1. **挑出来一个与众不同的来. HP-UX AIX OSX Slackware Solaris**

**答 : Slackware。 HP-UX, AIX, OSX, Solaris 分别是由 HP, IBM, APPLE, Oracle 开发的，并且都是UNIX的变种. Slackware 则是一个Linux操作系统**

**29.Linux 不会感染病毒吗？**

**答 : 当然会! 这个地球上不存在不会感染病毒的操作系统。但是Linux以迄今为止病毒数量少而著称，是的，甚至比UNIX还要少。Linux榜上有名的病毒只有60-100个，而且没有一个病毒在传播蔓延。Unix粗略估计有85-120个。**

**30.ps aux 中的VSZ代表什么意思，RSS代表什么意思**

**VSZ:虚拟内存集,进程占用的虚拟内存空间**

**RSS:物理内存集,进程战用实际物理内存空间**

**31.某/etc/fstab 文件中的某行如下：**

**/dev/had5 /mnt/dosdata msdos defaults,usrquota 1 2**

**请解释其含义。**

**参考答案:**

**（1）第一列：将被加载的文件系统名；（2）第二列：该文件系统的安装点；**

**（3）第三列：文件系统的类型；（4）第四列：设置参数；**

**（5）第五列：供备份程序确定上次备份距现在的天数；**

**（6）第六列：在系统引导时检测文件系统的顺序。**

**32.怎么把脚本添加到系统服务里，即用service来调用**

**在脚本里加入Shell**

**#!/bin/bash**

**# chkconfig: 345 85 15**

**# description: httpd**

**然后保存**

**chkconfig httpd –add 创建系统服务**

**现在就可以使用service 来 start or restart**

**33.写一个脚本，实现判断192.168.1.0/24网络里，当前在线的IP有哪些，能ping通则认为在线**

****

**#!/bin/bash**

**for ip in `seq 1 255`**

**do**

**{**

**ping -c 1 192.168.1.$ip > /dev/null 2>&1**

**if [ $? -eq 0 ]; then**

**echo 192.168.1.$ip UP**

**else**

**echo 192.168.1.$ip DOWN**

**fi**

**}&**

**done**

****

**出题随机脚本。**

**#!/bin/bash**

**touch ./temp**

**>temp**

**while [ `sort temp | uniq | wc -l` != 10 ]**

**do**

**echo `expr $RANDOM % 33 + 1` >> temp**

**done**

**sort temp | uniq**

**rm temp**

**安全检测及防护**

**1 LINUX系统安全加固应该从哪些方面入手？**

**目录：**

**1.BIOS**

**2.SSH安全**

**3.禁用telnet**

**4.禁用代码编译**

**5.ProFTP**

**6.TCPwrappers**

**7.创建一个SU组**

**8.root通知**

**9.history安全**

**10.欢迎信息**

**11.禁用所有特殊账户**

**12.chmod危险文件**

**13.指定允许root登陆的TTY设备**

**14.选择一个安全的密码**

**15.检查Rootkit**

**16.安装补丁**

**17.隐藏Apache信息**

**18.隐藏php信息**

**19.关闭不使用的服务**

**20.检测监听中的端口**

**21.关闭打开的端口和服务**

**22.删除不用的rpm包**

**23.禁用危险的php函数**

**24.安装配置防火墙**

**25.安装和配置BFD**

**26.内核加固(sysctl.conf)**

**27.更改SSH端口**

**28./tmp /var/tmp,/dev/shm分区安全**

**29.PHP IDS**

**2 LINUX系统安全加固应该从哪些方面入手？请列举一二详细的方法。**

**略。该题为随机题。**

**3. 写一个shell脚本来得到当前的日期，时间，用户名和当前工作目录。**

**答案 : 输出用户名，当前日期和时间，以及当前工作目录的命令就是logname，date，who i am和pwd。**

**现在，创建一个名为userstats.sh文件，将下面的代码添加到它。**

**复制代码 代码如下:**

**#!/bin/bash**

**echo "Hello, $LOGNAME"**

**echo "Current date is `date`"**

**echo "User is `who i am`"**

**echo "Current directory `pwd`"**

**给它添加执行权限，并且执行他。**

**复制代码 代码如下:**

**# chmod 755 userstats.sh**

**# ./userstats.sh**

**样例输出**

**复制代码 代码如下:**

**Hello, avi**

**Current date is Sat Jun 7 13:05:29 IST 2016**

**User is avi pts/0 2016-06-07 11:59 (:0)**

**Current directory /home/avi/Desktop**

**4.写一个shell脚本，进行两个数字的相加，如果没有输入参数就输出错误信息和一行使用说明**

**答案 : 下面是简单的shell脚本以及描述，如果没有命令行参数，它会抛出错误与如何使用脚本的说明。**

**再创建一个名为twonumbers.sh文件和下面的内容添加到文件里。**

**复制代码 代码如下:**

**#!/bin/bash**

**# The Shebang**

**if [ $# -ne 2 ]**

**# If two Inputs are not received from Standard Input**

**then**

**# then execute the below statements**

**echo "Usage - $0 x y"**

**# print on standard output, how-to use the script (Usage - ./1.sh x y )**

**echo " Where x and y are two nos for which I will print sum"**

**# print on standard output, “Where x and y are two nos for which I will print sum ”**

**exit 1**

**# Leave shell in Error Stage and before the task was successfully carried out.**

**fi**

**# End of the if Statement.**

**echo "Sum of $1 and $2 is `expr $1 + $2`"**

**# If the above condition was false and user Entered two numbers as a command Line Argument,**

**it will show the sum of the entered numbers.**

**给他添加可执行权限，并且执行。**

**复制代码 代码如下:**

**# chmod 755 two-numbers.sh**

**情形一: 未输入两个数字作为命令行参数运行脚本，你将得到下面的输出。**

**样例输出**

**复制代码 代码如下:**

**# ./two-numbers.sh**

**Usage - ./two-numbers.sh x y**

**Where x and y are two nos for which I will print sum**

**情形二: 当数字存在时，你会得到如图所示的结果。**

**复制代码 代码如下:**

**$ ./two-numbers.sh 4 5**

**Sum of 4 and 5 is 9**

**因此，上述shell脚本满足了问题的要求。**

**5.你需要打印一个给定的数字的反序，如输入10572，输出27501，如果没有输入数据，应该抛出错误和使用脚本说明。在此之前，告诉我你需要在这里使用的算法。**

**算法**

**1.输入的数字为n**

**2.赋值 rev=0, sd=0 (反向和单个数字设置为0)**

**3.n % 10, 将得到最左边的数字**

**4.反向数字可以用这个方法生成 rev \* 10 + sd**

**5.对输入数字进行右位移操作（除以10）**

**6.如果n > 0, 进入第三步，否则进行第七步**

**7.输出rev**

**现在，创建一个名为`numbers.sh`文件，并添加以下代码。**

**复制代码 代码如下:**

**#!/bin/bash**

**if [ $# -ne 1 ]**

**then**

**echo "Usage: $0 number"**

**echo " I will find reverse of given number"**

**echo " For eg. $0 0123, I will print 3210"**

**exit 1**

**fi**

**n=$1**

**rev=0**

**sd=0**

**while [ $n -gt 0 ]**

**do**

**sd=`expr $n % 10`**

**rev=`expr $rev \\* 10 + $sd`**

**n=`expr $n / 10`**

**done**

**echo "Reverse number is $rev"**

**授予对文件的执行权限，并运行如下所示的脚本。**

**复制代码 代码如下:**

**# chmod 755 numbers.h**

**情形一: 当输入不包含命令行参数，你将得到下面的输出**

**样例输出**

**复制代码 代码如下:**

**./numbers.sh**

**Usage: ./numbers.sh number**

**I will find reverse of given number**

**For eg. ./2.sh 123, I will print 321**

**情形二: 正常输入**

**复制代码 代码如下:**

**$ ./numbers.sh 10572**

**Reverse number is 27501**

**上面的脚本非常完美，输出正是我们需要的。**

**6. 你应该直接用终端，而不是依靠任何shell脚本来进行实数计算。你会怎么做（比如实数7.56+2.453）？**

**答案 : 我们需要用如下所述的特殊方式使用bc命令。将7.56+2.453作为输入通过管道进入bc中。**

**复制代码 代码如下:**

**$ echo 7.56 + 2.453 | bc**

**10.013**

**7. 根据 web 日志或者或者网络连接数，监控当某个 IP 并发连接数或者短时内 PV 达到 100 ，即调用防火墙命令封掉对应的 IP ，监控频率每隔 3 分钟。防火墙命令为： iptables -I INPUT -s 10.0.1.10 -j DROP 。**

**netstat -na| grep EST| awk -F "[ :]+" '{print $6}' | sort | uniq -c >> /tmp/a .log**

**while true**

**do**

**grep EST a.log| awk -F '[ :]+' '{print $6}' | sort | uniq -c > /tmp/tmp .log**

**exec < /tmp/tmp .log**

**while read line**

**do**

**ip=` echo $line| awk "{print $2}" `**

**count=` echo $line| awk "{print $1}" `**

**if [ $count -gt 100 ] && [ `iptables -L -n| grep $ip| wc -l` -lt 1 ]**

**then**

**iptables -I INPUT -s $ip -j DROP //-I 将其封杀在iptables显示在第一条**

**echo "$line is dropped" >> /tmp/dropip .log**

**fi**

**done**

**sleep 180**

**done**

**8.** **TCP\_wrappers工作原理**

**1. 当有请求从远程到达本机的时候**

**首先检查/etc/hosts.allow**

**如有匹配的，就默认允许访问,跳过 /etc/hosts.deny这个文件**

**没有匹配的,就去匹配/etc/hosts.deny 文件,如果有匹配的，那么就拒绝这个访问**

**2. 如果在这两个文件中，都没有匹配到，默认是允许访问的**

**9.** **详述 iptales 工作流程以及规则过滤顺序？**

**iptables过滤的规则顺序是由上至下，若出现相同的匹配规则则遵循由上至下的顺序**

**10. iptables 的几个表以及每个表对应链的作用，对应企业应用场景？**

**filter：INPUT 作用:for packets destined to local sockets**

**FORWARD 作用：for packets being routed through the box**

**OUTPUT 作用：for locally-generated packets**

**nat：PREROUTING 作用：for altering packets as soon as they come in**

**OUTPUT 作用：for altering locally-gener- ated packets before routing**

**POSTROUTING 作用：for altering packets as they are about to go out**

**mangle ：PRE-ROUTING (for altering incoming packets before rout-ing) and**

**OUTPUT (for altering locally-generated pack-ets before routing).**

**INPUT (forpackets coming into the box itself),**

**FORWARD (foraltering packets being routed through the box), and**

**POSTROUTING (for altering packets as they are about to go out).**

**11.** **禁止来自 10.0.0.188 ip 地址访问 80 端口的请求**

**iptables -A INPUT -p tcp --dport 80 -j DROP**

**12.如何使在命令行执行的 iptables 规则永久生效？**

**/etc/init.d/iptables save**

**13.** **实现把访问 10.0.0.3:80 的请求转到 172.16.1.17:80**

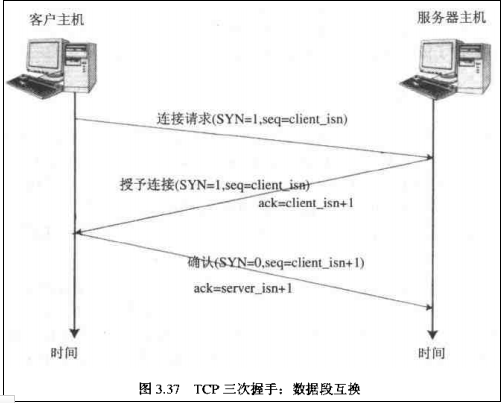
**iptables -t nat -A PREROUTING -d 10.0.0.3 -p tcp --dport 80 -j DNAT --to-destination 172.16.1.6:80**

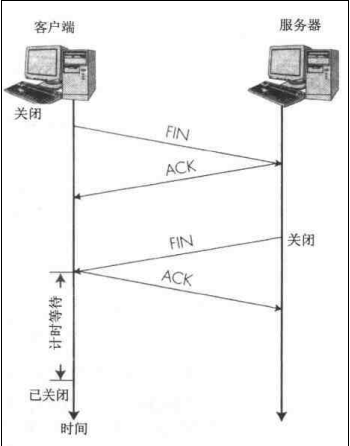
**14 、实现 172.16.1.0/24 段所有主机通过 124.32.54.26 外网 IP 共享上网。**

**iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j SNAT --to-source 124.32.54.26**

**iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j MASQUERADE**

**15.描述 tcp 3 次握手及四次断开过程？**

****

****

**16.** 详细描述 HTTP 工作原理？

**1 ) 地址解析**

**2）封装HTTP请求数据包**

**3）封装成TCP包，建立TCP连接 （ TCP的三次握手 ）**

**4）客户机发送请求命令**

**5）服务器响应**

**6）服务器关闭TCP连接**

**17.** **请描述 iptables 的常见生产应用场景。**

**端口映射**

**企业应用场景：**

**1） 把访问外网IP及端口的请求映射到内网某个服务器及端口（企业内部）；**

**2） 硬件防火墙，把访问LVS/nginx外网VIP及80端口的请求映射到IDC 负载均衡服务器内部IP及端口上（IDC机房的操作） ；**

**局域网共享上网**

**iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 120.43.61.124**

**18. 企业 WEB 应用较大并发场景如何优化 iptables?**

**net.nf\_conntrack\_max = 25000000**

**net.netfilter.nf\_conntrack\_max = 25000000**

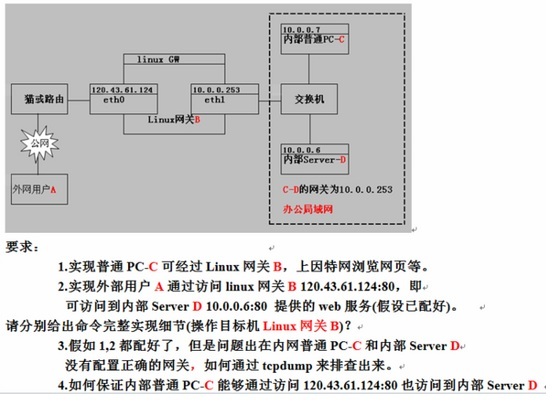
**net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 180**

**net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120**

**net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60**

**net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120**

**19. 如图编写iptables**



iptables -t nat -A POSTROUTING -s 10.0.0.253 -j SNAT -o eth0 --to-source 120.43.61.124

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

tcpdump ip host 10.0.0.253 and 10.0.0.6 或 tcpdump ip host 10.0.0.253 and 10.0.0.7

iptables -t nat -A PREROUTING -d 120.43.61.124 -p tcp --dport 80 -j DNAT --to-destination 172.16.1.6:80

**20.** **什么是代理服务器？代理服务器在计算机网络中有什么用途？**

**答 : 代理服务器是指那些作为客户端和资源提供商或服务器之间的中间件的物理机或者应用程序。客户端从代理服务器中寻找文件、页面或者是数据，而且代理服务器能处理客户端与服务器之间所有复杂事务，从而满足客户端的生成的需求。**

**代理服务器是WWW（万维网）的支柱，它们其中大部分都是Web代理。一台代理服务器能处理客户端与服务器之间的复杂通信事务。此外，它在网络上提供的是匿名信息（LCTT 译注：指浏览者的 IP、浏览器信息等被隐藏），这就意味着你的身份和浏览痕迹都是安全的。代理可以去配置允许哪些网站的客户能看到，哪些网站被屏蔽了。**

**21.** **Squid是什么?**

**答 : Squid是一个在GNU/GPL协议下发布的既可作为代理服务器，同时也可作为Web缓存守护进程的应用软件。Squid主要是支持像HTTP和FTP那样的协议，但是对其它的协议比如HTTPS，SSL,TLS等同样也能支持。其特点是Web缓存守护进程通过从经常上访问的网站里缓存Web和DNS数据，从而让上网速度更快。Squid支持所有的主流平台，包括Linux，UNIX，微软公司的Windows和苹果公司的Mac。**

**22.** **Squid的默认端口是什么？怎么去修改它的操作端口？**

**回答 : Squid运行时的默认端口是3128。我们可以通过编辑它的配置文件来把它的默认端口修改成未被用户使用的端口，路径是 /etc/squid/squid.conf**

**23.** **你的公司管理层要求你通过Squid代理服务器屏蔽掉一些域名，你怎么做？**

**答 : 屏蔽域名是一个在配置文件中实现的功能模块。我们只需要执行一个小的手动配置即可，建议如下。**

**a. 在 ‘/etc/squid’ 目录下创建一个名为 ‘blacklist’ 的文件。**

**# touch /etc/squid/blacklist**

**b. 用nano编辑器打开这个文件。**

**# nano /etc/squid/blacklist**

**c. 以每行一个域名的方式将想要屏蔽的域名写进这个文件里。**

**.facebook.com**

**.twitter.com**

**.gmail.com**

**.yahoo.com**

**...**

**d. 保存退出，然后从 ‘/etc/squid/squid.conf’ 打开Squid配置文件。**

**# nano /etc/squid/squid.conf**

**e. 在配置文件中添加如下行。**

**acl BLACKLIST dstdom\_regex -i “/etc/squid/blacklist”**

**http\_access deny blacklist**

**f. 保存配置文件并退出，重启Squid服务让其生效。**

**# service squid restart**

**24.** **在Squid中什么是媒体范围限制（Media Range Limitation）和部分下载？**

**答 : 媒体范围限制是Squid的一种特殊的功能，它只从服务器中获取所需要的数据而不是整个文件。这个功能很好的实现了用户在各种视频流媒体网站如YouTube和Metacafe看视频时，可以点击视频中的进度条来选择进度，因此整个视频不用全部都加载，除了一些需要的部分。**

**25.** **什么是Squid的反向代理？**

**反向代理是Squid的一个功能，这个功能被用来加快最终用户的上网速度。下面用缩写 ‘RS’ 的表示包含了资源的原服务器，而代理服务器则称作 ‘PS’ 。初次访问时，它会从RS得到其提供的数据，并将其副本按照配置好的时间存储在PS上。这样的话每次从PS上请求的数据就相当于就是从原服务器上获取的。这样就会减轻网络拥堵，减少CPU使用率，降低网络资源的利用率，从而缓解原来实际服务器的负载压力。但是RS统计不了总流量的数据，因为PS分担了部分原服务器的任务。‘X-Forwarded-For HTTP’ 信息能用于记录下通过HTTP代理或负载均衡方式连接到RS的客户端最原始的IP地址。**

**26.** **你有一台工作中的机器可以访问代理服务器，如果想要限制你的孩子的访问时间，你会怎么去设置那个场景？**

**答：把允许访问的时间设置成晚上4点到7点三个小时，跨度为星期一到星期五。**

**27.** **Squid存储的数据是什么文件格式？**

**答 : Squid存储的数据是UFS文件格式的。UFS是一种老的，使用比较广泛的Squid存储格式**

**28.** **构建及使用漏洞评估系统**

**安装OpenVAS所需各软件包，启动各组件服务**

**访问gsad服务提供的Web界面程序**

**添加并执行扫描任务，查看扫描报告**

**29.你使用过监控软件吗？说说其特点**

**使用nagios 对服务器进行监控，其特点可实时实现手机短信、电子邮件、MSN、飞信报警。使用cacti 对流量进行监控。**

1. **cacti有哪些组件，工作原理是什么？**

**1. cacti是用php语言实现的一个软件，它的主要功能是用snmp服务获取数据，然后用rrdtool储存和更新数据，当用户需要查看数据的时候用rrdtool生成图表呈现给用户。因此，snmp和rrdtool是cacti的关键。Snmp关系着数据的收集，rrdtool关系着数据存储和图表的生成。**

**2. Mysql配合PHP程序存储一些变量数据并对变量数据进行调用，如：主机名、主机ip、snmp团体名、端口号、模板信息等变量**

**3. snmp抓到数据不是存储在mysql中，而是存在rrdtool生成的rrd文件中（在cacti根目录的rra文件夹下）。rrdtool对数据的更新和存储就是对rrd文件的处理，rrd文件是大小固定的档案文件（RoundRobinArchive），它能够存储的数据笔数在创建时就已经定义。**

1. **zabbix能做哪些监控？**

**硬件监控：Zabbix IPMI Interface**

**系统监控：Zabbix Agent Interface**

**Java监控：Zabbix JMX Interface**

**网络设备监控：Zabbix SNMP Interface**

**应用服务监控：Zabbix Agent UserParameter**

**MySQL数据库监控：percona-monitoring-plulgins**

**URL监控：Zabbix Web 监控**

**31.** **开源网管工具 Cacti，Nagios,Zabbix 比较**

**首先 Cacti 是一个用 rrdtool 来画图的网络监控系统, 通常一说到网络管理, 大家首先想到的经常是 mrtg, 但是 mrtg 画的图比较简单而且且难看, rrdtool 虽然画图本领一流, 画出来的图也漂亮, 但是毕竟是一个画图工具, 不像 mrtg 那样本身还集成了数据收集功能. Cacti 则是集成了各种数据收集功能,然后用 rrdtool 画出监控图形. 其本身界面比起同类系统要漂亮不少. 推荐所有有监控需求的人都去研究一下。**

**Cacti 和 Nagios 是不同功用的系统, Nagios 适合监视大量服务器计算环境，重点并不在于图形化的监控, 其集成了很多功能，例如报警,都是 cacti 没有或者很弱的. Cacti 主要用途还是用来收集历史数据和画图, 所以界面比 Nagios 漂亮很多.**

**Nagios和Cacit都是比较老牌的开源网管软件；OpenNMS是稍微点出现的项目，它集成了前两者的部分优点，界面是Java的界面，后台的自动发现机制非常的方便。Zenoss是一个比较年轻的项目，所谓长江后浪推前浪，它是纯Python语言编写的一个软件，架构非常的不错，而其界面做的非常好，面向对象编程的理念处处可见。从根上可以看出它们的主要编程语言各有不同，这也决定了它们的特点和发展方向的不同.**

1. **你对现在运维工程师的理解和以及对其工作的认识**

**你是如何看待运维的**

**大部分朋友认为，在互联网公司中linux系统运维的工作就是安装系统，部署服务处理紧急故障，为公司开发人员及其它部门提供支持。同时负责内外网的网络稳定**

**没错，上面的工作的确是运维的一部分工作，但并不是全部，或者说是中小公司低级的运维劳动。**

**​作为运维人员除了上面的角色外，运维人员还是管理、制度、规范、流程的制定和推行、监督角色。**

**​运维的核心是运维思想，非运维技术本身（如部署服务等，这是部分朋友的误区）**

**上百台以上的服务器的规模如果没有好的管理流程、规范、制度策略，是无法协调工作的。上千台、上万台更是如此。运维流程、运维规范、运维制度、自动化、智能化、批量部署、批量管理、网站架构优化、监控预警、流量及日志分析统计、成本控制（注意字眼是控制，不是节省）才是真正的运维人员需要做的。如何推进并完善上面的工作，提升工作效率，提升团队以一当十的战斗力才是最核心的内容。**

**​运维的宗旨：7\*24小时网络稳定、用户体验良好（用户包括内部的员工、外部的网站用户）所以，我们做什么都不要离开运维的宗旨，否则，你的工作都可能是徒劳的无用功（起码和目标没直接对接）。**

**​有经验的运维人员会先思考在动作，经验不足的运维人员会先做，遇到问题在思考，这是完全不同的层次和境界。**

**​试想盖一座大楼如果先盖好在思考，那还能盖好么？所以，请别轻易说你精通什么什么服务，会多少多少软件，那只是几块砖头、几袋水泥、几根钢筋而已。盖好大楼，这些仅仅是基本的元素，运维同样是如此！**

1. **如何快速，大规模的部署服务器系统，当服务器应用需求不同时，如桌面服务器，web服务器，SQL服务器，文件的类型和数量各不相同，那么他们的分区大小的应该如何规划。**

**答：linux快速部署，可以使用PXE+Kickstart实现。常见的分区在掌握其功能和推荐配置后，再根据业务的需求不同适当的调整大小，但这一点就是**仁者见仁智者见智了。

**常见的分区有/boot：一般设置100M~200M**

**/根分区，未指定的全部空间。/home用户目录，一个用户可以给100M左右。/var可变数据通常2~3G。SWAP分区，通常设置内存的2倍，/bin和/sbin是命令文件默认即可。**

**常见的服务有：普通桌面用户，boot200M,home50G，SWAP4G，剩下的全是/。**

**web服务器，boot500M，tmp2G，var2G，usr10G，剩下的是/**

**总结的特点如下：分区方案关键点：**

**——大数据库一般要加大/usr挂载点**

**——多用户、下载类、多存储文件等要加大/home挂载点**

**——文件小，用户多要注意/tmp和/var挂载点大小**

**34.常用的web服务器nginx的优化方法。**

**大多数的Nginx安装指南都告诉我。经过安装，修改这里或那里的几行配置，好了，就已经有了一个Web服务器了。而且，在大多数情况下，一个常规安装的nginx对你的网站来说已经能很好地工作了。然而，如果你真的想挤压出Nginx的性能，你必须更深入一些。我将解释Nginx的那些设置可以微调，以优化处理大量客户端时的性能。需要注意一点，这不是一个全面的微调指南。这是一个简单的预览——那些可以通过微调来提高性能设置的概述。你的情况可能不同。**

**1 基本的 (优化过的)配置**

**我们将修改的唯一文件是nginx.conf，其中包含Nginx不同模块的所有设置。你应该能够在服务器的/etc/nginx目录中找到nginx.conf。首先，我们将谈论一些全局设置，然后按文件中的模块挨个来，谈一下哪些设置能够让你在大量客户端访问时拥有良好的性能，为什么它们会提高性能。本文的结尾有一个完整的配置文件。**

**高层的配置**

**nginx.conf文件中，Nginx中有少数的几个高级配置在模块部分之上。**

**user和pid应该按默认设置 - 我们不会更改这些内容，因为更改与否没有什么不同。**

**worker\_processes 定义了nginx对外提供web服务时的worker进程数。最优值取决于许多因素，包括（但不限于）CPU核的数量、存储数据的硬盘数量及负载模式。不能确定的时候，将其设置为可用的CPU内核数将是一个好的开始（设置为“auto”将尝试自动检测它）。**

**worker\_rlimit\_nofile 更改worker进程的最大打开文件数限制。如果没设置的话，这个值为操作系统的限制。设置后你的操作系统和Nginx可以处理比“ulimit -a”更多的文件，所以把这个值设高，这样nginx就不会有“too many open files”问题了。**

**2 Events模块**

**worker\_connections 设置可由一个worker进程同时打开的最大连接数。如果设置了上面提到的worker\_rlimit\_nofile，我们可以将这个值设得很高。**

**记住，最大客户数也由系统的可用socket连接数限制（~ 64K），所以设置不切实际的高没什么好处。**

**multi\_accept 告诉nginx收到一个新连接通知后接受尽可能多的连接。**

**use 设置用于复用客户端线程的轮询方法。如果你使用Linux 2.6+，你应该使用epoll。如果你使用\*BSD，你应该使用kqueue。**

**（值得注意的是如果你不知道Nginx该使用哪种轮询方法的话，它会选择一个最适合你操作系统的）**

**3 HTTP 模块**

**HTTP模块控制着nginx http处理的所有核心特性。因为这里只有很少的配置，所以我们只节选配置的一小部分。所有这些设置都应该在http模块中，甚至你不会特别的注意到这段设置。**

**access\_log 设置nginx是否将存储访问日志。关闭这个选项可以让读取磁盘IO操作更快(aka,YOLO)**

**error\_log 告诉nginx只能记录严重的错误：**

**keepalive\_timeout 给客户端分配keep-alive链接超时时间。服务器将在这个超时时间过后关闭链接。我们将它设置低些可以让ngnix持续工作的时间更长。**

**等等**

**35.**[**rsync的几种优化应用方案**](http://blog.csdn.net/onlyforcloud/article/details/46971101)**？（详细抽查其中某一项）**

**答：为了解决文件增多导致rsync变慢的问题，方案是很多的。1、使源目录保存较少文件，2、使用/dev/shm内存分区3、使用推送方式4、仅用一台作同步比较5、使用inotify　6、双路同步**

**1、使源目录保存较少文件**

**这是一个传统优化办法，因为rsync虽然是同步所有文件，但和同步最近更新的文件是一个道理，因此将源**[**服务器**](http://server.chinaitlab.com/)**上的目录删除，仅仅保持最近更新的文件，文件数量就变得不但很少，而且是稳定的，随着时间推移，这数量也不会涨得很快。但这样做有个缺点，就是rsync不能使用删除模式，如果有文件要删除，可以将其弄成空文件，假如有更严格要求，可以另一个程序来删除。**

**2、使用/dev/shm内存分区**

**在源目录保持较少文件的前提下，将文件不存在硬盘上而放入内存，就可以避免系统IO带来的问题，但是这个内存分区在系统reboot后会丢掉所有数据，虽然并不常常需要reboot，但是其中的风险也需要计算清楚。**

**3、使用推送方式**

**因为性能问题是出现在rsync的客户端，用生产**[**服务器**](http://server.chinaitlab.com/)**抓取源服务器的话，性能问题就会出现在生产服务器上，这当然不很妥当。假如在生产服务器上使用 rsync daemon，源服务器执行rsync命令将文件推送到生产服务器上，性能问题就转移到了源服务器上，这在一定程度可以保证生产服务器的稳定性。**

**4、仅用一台作同步比较**

**假如源服务器的文件要被同步到很多台生产服务器，那么会出现rsync并发。可以分析到这些生产服务器在同一时刻文件是一致的，因此每台机都和源服务器做一次比较就是浪费的。这时可以让源服务器和生产服务器同步一次，并且使用-v参数打印出log，其它生产服务器通过同步这个log记录的文件就可以避免数次比较过程。**

**5、使用inotify**

**inotify就不是rsync了，inotify是一个守护进程，它可以监控到文件目录下的文件变动情况，根据其输出然后用rsync做文件传输，就可以减掉文件比较这个环节。inotify使用并不复杂，对文件变更情况的监控是实时的，也不消耗很多性能。**

**6、双路同步**

**以上均是对rsync性能方面做优化，但是优化也会带来问题。在3、4、5号方案中，假如生产服务器有一台机器因为负载或其它问题reboot了，在 reboot过程中同步就失败了，这部分失败的文件假如没有其它处理，就永远不会再同步到生产服务器上。这时可以使用多一路rsync来处理，譬如使用 inotify，做到了实时同步，然后再每小时进行一次完整的rsync同步。这样就可以保证有很高的同步速度，又能使丢失文件的风险控制在一小时之内。**

**36.请你自我介绍一下**

**这是面试题最常见的，也是最容易得分的题，反而也是各位学员的短板。所以现在要求大家从现在开始就要准备好一段陈述，每天对着镜子说一遍，直到无论什么时候你也能脱口而出。除非面试官有特殊要求，否则一定要围绕应聘职位展开。​**

**37.你对薪资的要求？**

**要记着谈到钱的时候，谁先出价谁就输了**

**所以你不要回答，你可以说，“这个问题实在太难回答了”你能告诉我这个职位咱们公司的薪水范围吗.**

**大多数​面试官会给你说一下，告诉你答案，如果没有，那可能与具体的职位有关，他们也会给你一个范围。**

**提示：如果你对薪酬的要求太低，那在别人看来就是贬低自己的能力，如果 你对薪酬要的过高，那又显得你分量过重，公司受用不起。基本上，只要公司开始招聘就一定有个基本预算​，所以与你要多少没有关系，这个时候你要注意，一般情况下，面试官第一次提高的工资就是预算的一个最高值或者一个较高值，除非你对自己特别有自信，这个时候你可以一刀切，我非30K以上才能上班，那你可以直接说就可以了，要不然就不要主动出价、**

**但是有的时候，面试官非让你出价，说个具体的数目，这个时候，切记不要说一个范围，比如5000-8000，那一定会给你5K的。按照最少的给你，所以你要尽可能的说一个准确的值比如8K**

**​比较优秀的回答：我现在的工资是6000，我期望能拿到8K，我很少参加面试，所以对薪资水平并不太了解，如果贵公司认为我配不上我提的待遇要求，那你可以给我降低待遇要求，如果能在您收下供职，我会把我现在的能力显示给您看，也把我的学习能力展示给您，我以前在公司都用加薪肯定了我的能力，我也相信靠自己的努力公司会给我更多的回报。**

**38.你对加班的看法？**

**提示：实际上公司问这个问题，并不证明一定要加班，只是想测试下你是否愿意为公司做贡献**

**回答提示：**

**IT技术是我的爱好，我喜欢挑战，加班能增长我的个人经验，就算早回家我也是泡在电脑前研究技术。我以前的公司也都是加班的，我觉IT公司加班其实很正常的，当然我也会​提高工作效率，减少不必要的加班**

**39.未来五年到十年你要干什么，你的职业规划什么。**

**提示：成为高级架构师，懂运维开发，在面试官面前要表现出自己想干好当前的工作，而不要说职业规划是当运维总监。​**

**40.你以前在公司每天工作都做什么**

**到公司​首先看流量，机房的流量，cdn的流量，然后看报警，然后看邮件，定时任务的备份正不正常，有没有意外，白天是搭建环境，该配置，处理开发的需求，下午上线，分组，把代码推到服务器上去，有时间的话就做什么，像跳板机，等等，如果有内网的活比如员工上不liao网了，也负责。**

**41. apache工作模式**

**工作模式即：MPM又称Apache多道处理模式**

**追求稳定性用prefork模式，追求性能用event模式**

**1、Prefork**

**Apache启动时预先创建一些子进程等待连接请求，子进程只有一个线程，同一时间一个进程只能处理一个请求。**

**优点：成熟稳定，兼容所有新老模块，不需要担心线程安全的问题**

**（其中一个进程出错不影响其他进程，用于政府网站的访问量不大，不要求性能）**

**缺点：占用更多的系统资源，消耗更多的内存，效率低**

**2、Worker**

**多线程和多进程的混合模式，预先创建子进程（数量比较少），然后每个子进程创建多个线程，线程通常会共享父进程的内存空间**

**优点：有效节约了服务器资源，尤其是内存资源**

**缺点：稳定性差（一个线程出错，影响其他线程）**

**3、Event**

**解决了keep-alive长期占用的线程问题的worker，需要Linux2.6+内核**

**优点：解决长期占用线程的问题，节约资源（尤其是内存资源）**

**缺点：稳定性差（线程与线程直接的影响依然存在）**

**42. Apache与PHP是如何交互的**

**1、php-module（系统默认的方法）**

**(1)把php直接编译成Apache的一个模块（当Apache处理动态页面的时候，直接调用这个PHP模块来处理）**

**Yum安装的可以查看vim /etc/httpd/conf.d/php.conf**

**2、CGI&FCGI(PHP-FPM)**

**PHP以独立的服务模式工作，Apache转发php请求给php进程**

**CGI：通用网关接口，是一种协议**

**FCGI：快速的通用网关接口**

**PHP进程名：PHP-FPM**

**注：在这种模式下PHP是一个单独的服务，PHP与Apache进程相互通讯用FCGI协议，Apache只处理静态页面，接到动态页面请求，直接转给PHP进程处理，处理完生成静态页面返给Apache。**

**43.php调优工作**

**1、配置文件:**

**pm.max\_children = 50 （最大处理客户端多少并发连接请求）**

**pm.start\_servers = 20 （启动时开启多少个进程）**

**pm.min\_spare\_servers = 10 （最小空闲进程）**

**pm.max\_spare\_servers = 30 （最大空闲进程）**

**10+30不能超过50**

1. **LAMP 平台****调优（****apache+****php+mysql）**

**MySQL 调优：1。替换有问题的硬件。2.对 MySQL 进程的设置进行调优。3.对查询进行优化**

**php调优:**利用缓存模块（如Memcache）或者模板系统(如Smarty)进行缓存处理。我们可以缓存数据库结果和提取页面结果的方式来提升网站性能

迫使php强行在缓冲区填满之前把数据响应给用户，这样就会让你的网站看起来更快一些

当你写php类的时候，你可以直接操作对象属性，这样能帮助你节省时间和提升你的脚本性能。而不是那种让人感到幼稚可笑的setters和getters

没有原因不要copy变量以及 避免循环做SQL操作,

**apache调优：**无限大的拼命增加VU的数量，

**偏执的用一定的数据量的VU，**

**合理的制定系统最大用户、并发用户，**

**影响和评估性能的几个关键指标如吞吐量，吞吐率，** **事务，TPS，点击率，平均相应时间等**

**合理的性能测试如VU数量的增加，** **吐吞量的变化，** **平均响应时间，** **内存监控，CPU Load，**

1. **LVS HARPOXY** **NGINX 反向代理优缺点比较。(**<http://www.ha97.com/5646.html>**)**

**Nginx的优点是**

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

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

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

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

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

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

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

**Nginx的缺点是：**

Nginx仅能支持http、[**https**](http://www.ha97.com/tag/https)和Email协议，这样就在适用范围上面小些

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

**LVS的优点是：**

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，对内存和cpu资源消耗比较低

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

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

应用范围比较广，因为LVS工作在4层，所以它几乎可以对所有应用做负载均衡

**LVS的缺点是：**

软件本身不支持正则表达式处理，不能做动静分离

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**](http://www.ha97.com/tag/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

**HAProxy的特点是：**

HAProxy也是支持虚拟主机的。

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

HAProxy支持TCP协议的负载均衡转发，可以对MySQL读进行负载均衡

1. **负载均衡算法有哪些？他们的区别是什么？**

我们知道，负载均衡器在负载均衡设备中的作用是至关重要的，它起着承上启下的作用。一方面接收用户的网络请求，一方面把请求按照某种算法转接到特定的应用服务器中，实现负载均衡。所以，负载均衡器中的算法是至关重要的。大多数负载均衡设备实现了以下多种算法。  
**轮询调度**  
 轮询调度(Round Robin Scheduling)算法就是以轮询的方式依次将请求调度到不同的服务器，即每次调度执行i = (i + 1) mod n，并选出第i台服务器。算法的优点是其简洁性，它无需记录当前所有连接的状态，所以它是一种无状态调度。  
　在实际实现过程中，一般会为每台服务器设定一个权重值，这就是权重轮询调度算法。  
**最小连接调度(Least-Connection Scheduling)** 最小连接调度(Least-Connection Scheduling)算法是把新的连接请求分配到当前连接数最小的服务器。最小连接调度是一种动态调度算法，它通过服务器当前所活跃的连接数来估计服务器的负载情况。  
 在实际实现过程中，一般会为每台服务器设定一个权重值，这就是加权最小连接调度(Weighted Least-Connection Scheduling)  
**基于局部性的最少链接(LBLC)** 基于局部性的最少链接调度(Locality-Based Least Connections Scheduling，以下简称为LBLC)算法是针对请求报文的目标IP地址的负载均衡调度，目前主要用于Cache集群系统，因为在Cache集群中客户请求报文的目标IP地址是变化的。  
 LBLC调度算法先根据请求的目标IP地址找出该目标IP地址最近使用的服务器，若该服务器是可用的且没有超载，将请求发送到该服务器; 若服务器不存在，或服务器超载或有服务器处于其一半的工作负载，则用“最少链接”的原则选出一个可用的服务器，将请求发送到该服务器。  
**带复制的基于局部性最少链接(LBLCR)**  
 带复制的基于局部性最少链接调度(Locality-Based Least Connections with Replication Scheduling，以下简称为LBLCR)算法也是针对目标IP地址的负载均衡，目前主要用于Cache集群系统。它与LBLC算法的不同之处是它要维护从一个目标IP地址到一组服务器的映射，而LBLC算法维护从一个目标IP地址到一台服务器的映射。  
 LBLCR调度算法将“热门”站点映射到一组Cache服务器(服务器集合)，当该“热门”站点的请求负载增加时，会增加集合里的Cache服务器，来处理不断增长的负载; 当该“热门”站点的请求负载降低时，会减少集合里的Cache服务器数目。这样，该“热门”站点的映像不太可能出现在所有的Cache服务器上，从而提供Cache集群系统的使用效率。  
**目标地址散列调度(Destination Hashing Scheduling)** 目标地址散列调度(Destination Hashing Scheduling)算法是针对目标IP地址的负载均衡，但它是一种静态映射算法，通过一个散列(Hash)函数将一个目标IP地址映射到一台服务器。  
 目标地址散列调度算法先根据请求的目标IP地址，作为散列键(Hash Key)从静态分配的散列表找出对应的服务器，若该服务器是可用的且未超载，将请求发送到该服务器，否则返回空。  
**源地址散列调度(Source Hashing Scheduling)** 和目标地址散列调度类似，唯一的区别是按照源地址为散列函数的散列键。  
 在实际应用中，源地址散列调度和目标地址散列调度可以结合使用在防火墙集群中，它们可以保证整个系统的唯一出入口

1. **web压力测试工具有哪些？**

**http\_load：程序非常小，解压后也不到100K ，http\_load以并行复用的方式运行，用以**[**测试**](http://lib.csdn.net/base/softwaretest)**web服务器的吞吐量与负载。 但是它不同于大多数压力测试工具，它可以以一个单一的进程运行，一般不会把客户机搞死。   
还可以测试HTTPS类的网站请求**

**webbench：webbench是**[**Linux**](http://lib.csdn.net/base/linux)**下的一个网站压力测试工具，最多可以模拟3万个并发连接去测试网站的负载能力。**

**ab：ab是apache自带的一款功能强大的测试工具。 安装了apache一般就自带了**

**Siege：一款开源的压力测试工具，可以根据配置对一个WEB站点进行多用户的并发访问，记录每个用户所有请求过程的相应时间，并在一定数量的并发访问下重复进行**

**.**[**Web Polygraph**](http://www.web-polygraph.org/)**– Web Polygraph这个软件也是一个用于测试WEB性能的工具，这个工具是很多公司的标准测试工具，包括微软在分析其软件性能的时候，也是使用这个工具做为基准工具的。**

[**OpenSTA**](http://www.oschina.net/p/opensta)**– OpenSTA是一个免费的、开放源代码的web性能测试工具，能录制功能非常强大的脚本过程，执行性能测试**

1. **主流****X86服务器厂商，三种服务器，主基本参数**

**戴尔，联想等**

**戴尔 PowerEdge R430，￥1.58万，机架式1U，CPU类型 Intel 至强E5-2600 v3 ， 标配CPU数量 2颗 ，内存类型 DDR4 ，内存容量 32GB ， 最大内存容量 384GB， 硬盘接口类型 SAS ，标配硬盘容量 6TB**

**热插拔盘位 非热插拔**

**戴尔 PowerEdge R730XD， ￥10.5万， 机架式2U， CPU型号 Xeon E5-2620 v3 ， 标配CPU数量 2颗 ，内存类型 RDIMM ，内存容量 32GB ， 硬盘接口类型 SAS ， 标配硬盘容量 7200GB ， 热插拔盘位 支持热插拔**

**戴尔 PowerEdge R930，￥27.54万， 机架式4U， CPU型号 Xeon E7-4820 v3 ，标配CPU数量 4颗 ，内存类型 RDIMMs ，内存容量 128GB ，硬盘接口类型 SAS ， 标配硬盘容量 900GB ，热插拔盘位 支持热插拔**

**ThinkServer RD450 ：机架式： 2U，CPU型号： Xeon E5-2609 v3，标配CPU数量： 1颗，内存类型： DDR4，内存容量： 4GB，硬盘接口类型： SAS，标配硬盘容量： 1TB**

**ThinkServer RD450 R710： 机架式： 2U，CPU型号： Xeon E5-2620 v3，标配CPU数量： 1颗，内存类型： DDR4，内存容量： 16GB，硬盘接口类型： SATA，标配硬盘容量： 2TB**

**ThinkServer TS250 S6100/1TO： 塔式： 4U，CPU型号： 酷睿i3 6100，标配CPU数量： 1颗，内存类型： DDR4，内存容量： 4GB，硬盘接口类型： SATA，标配硬盘容量： 1TB**

1. **市场上的****硬件负载均衡产品有哪些？主要参数是什么？价格？**

**F5 BIG-IP负载均衡器（LTM），深信服 梭子鱼等**

F5 BIG-IP LTM 1600 ￥**15.38万**

**设备类型:负载均衡器**

**硬件配置处理器：单CPU，基本内存：4GB，硬盘：500GB，端口：4个千兆端口，2个可选千兆光纤端口**

**性能应用概述：全面的负载均衡，应用状态监控，高可用性和交易保障，广域流量管理器，链路控制器等**

深信服AD-1600 参考报价：￥11.8

**设备类型：应用交付网关 ，硬件配置吞吐性能：700 Mbps，网口配置：6个千兆电口，尺寸：标准1U，电源：单电源**

**性能应用概述：包含链路负载均衡、服务器负载均衡、全局负载均衡、商业智能分析功能，以及缓存、压缩、SSL卸载、TCP连接复用等优化特性。支持单边加速功能，提高低质量网络环境下远端用户的访问速度**

梭子鱼BBFI430 ￥46.3万

**设备类型：链路负载均衡**

**硬件配置迷你1U机架,3个WAN口**

**性能应用概述：最大吞吐量为65M。支持链路均衡、链路健康检查、链路Failover、流量聚合、网络防火墙、本地DHCP和DNS、基于Web的流量统计、SNMP、自动链路配置、带宽管理和QoS**

**50.市场上的****存储服务器产品有哪些？主要参数是什么？价格？**

**浪潮英信NF8465M3是一款采用英特尔® E7 v2处理器技术的中高端四路服务器，搭配4路处理器，60颗计算核心，120个计算线程，最大支持2TB内存容量，满足海量内存需求，同时还可支持Flash Dimms、卡式PCIe SSD、2.5寸 SATA SSD，高性能12G SAS RAID控制器支持1、2、4GB缓存，而E7 v2计算平台最佳性价比设计更是让这款机器拥有均衡优异的性能表现。目前该款服务器在商家深博服务器中心处售34500元**

**灵活存储 DELL R730XD：戴尔PowerEdge R730是一款标配的高性能服务器，其采用2U机架式架构，配有Intel 至强E5-2600 v4系列高性能处理器，内存方面采用的是DDR4 16GB内存。戴尔 PowerEdge R730(配置：至强2603V4, 16G,2\*300G SAS)能最大限度地提高基于服务器的存储灵活性和性能。R730提供可选的服务器内混合存储配置，可提供12个SATA固态硬盘的超大容量，从而实现存储利用率、性能和成本的最佳平衡。目前该款产品在商家广州天翱处售11500元，**

**51.市场上的服务器产品有哪些？主要参数是什么？价格？**

**戴尔 PowerEdge R430，￥1.58万， 机架式1U，CPU类型 Intel 至强E5-2600 v3， 标配CPU数量 2颗 ， 内存类型 DDR4 ，内存容量 32GB ， 最大内存容量 384GB， 硬盘接口类型 SAS ， 标配硬盘容量 6TB ， 热插拔盘位 非热插拔**

**戴尔 PowerEdge R730XD，￥10.5万，机架式2U，CPU型号 X eon E5-2620 v3 ，标配CPU数量 2颗 ，内存类型 RDIMM ，内存容量 32GB ，硬盘接口类型 SAS ，标配硬盘容量 7200GB ，热插拔盘位 支持热插拔**

**戴尔 PowerEdge R930，￥27.54万，机架式4U， CPU型号 Xeon E7-4820 v3 ，标配CPU数量 4颗 ，内存类型 RDIMMs ，内存容量 128GB ，硬盘接口类型 SAS ， 标配硬盘容量 900GB ，热插拔盘位 支持热插拔**

**52. 开发监控http服务脚本。调动keepalive.在****HTTP服务故障时，能触发keepalived状态切换。**

**#!/bin/bash  
netstat -anpt | grep 80 &> /dev/null  
if [  $? -ne 0   ]  
then  
service keepalived stop &> /dev/null  
echo "http服务异常"  
fi**

**53. 高可用群集由哪些？keepalived是如何实现的。**

**RoseHA、Rose MirrorHA, RoseHA（Multi-node）, RoseStor Fundation , Red Hat**

**NEC ExpressCluster , Newstart HA, Newstart Mirror HA , Moebius, Double-Take**

**MSCS , Fujitsu PRIMECLUSTER , Landercluster**

keepalived是集群管理中保证集群高可用的一个服务软件，其功能类似于[heartbeat](https://github.com/chenzhiwei/linux/tree/master/heartbeat)

**Keepalived工作原理：**

**keepalived是以VRRP协议为实现基础的，VRRP即虚拟路由冗余协议。**

**虚拟路由冗余协议，可以认为是实现路由器高可用的协议，即将N台提供相同功能的路由器组成一个路由器组，这个组里面有一个master和多个backup，master上面有一个对外提供服务的vip， master会发组播，当backup收不到vrrp包时就认为master宕掉了，这时就需要根据VRRP的优先级来选举一个backup当master。这样的话就可以保证路由器的高可用了。**

**keepalived主要有三个模块，分别是core、check和vrrp。core模块为keepalived的核心，负责主进程的启动、维护以及全局配置文件的加载和解析。check负责健康检查，包括常见的各种**

**54. 阅读****heartbeat的配置过程。**

<https://my.oschina.net/tianjiangwei/blog/225341>

**55.** **keepalived和heartbeat的优缺点，适用哪些场合?**

**Keepalived使用的vrrp协议方式，虚拟路由冗余协议 简称VRRP)；**

**Heartbeat是基于主机或网络的服务的高可用方式；**

**keepalived的目的是模拟路由器的双机**

**heartbeat的目的是用户service的双机**

**lvs的高可用建议用keepavlived**

**业务的高可用用heartbeat**

**56：网络的几种存储方式：****DAS、NAS、SAN、ISCSI的区别？**

**DAS：直连于主机服务器的一种存储方式，（硬盘存储）。  
NAS：网络存储设备，（ftp，nfs，smb）性价比高，提供对象级存储。  
SAN：利用高速网络连接（gbit ethernet 千兆以太网）连接专业主机服务器的存储方式，对**速率，冗余性**要求高。位于主机群的后端，提供块级存储，无需文件系统  
ISCSI: 利用普通的数据网来传输ISCSI数据实现和SAN相似的功能可以大大的降低成本，同时提高系统的灵活性。SCSI就是这样一种技术，它利用普通的TCP/IP网来传输本来用存储区域网来传输的SCSI数据块.随着千兆网的普及，万兆网也逐渐的进入主流，使ISCSI的速度相对SAN来说并没有太大的劣势**

**67：常见的****RAID有哪些方式？特点分别是什么？**

**RAID0 无差错控制的带区组**

**分成数据块保存在不同驱动器上，数据吞吐量提高，驱动器的负载也比较均衡。不需要计算校验码，实现容易。**

**RAID2 带海明码校验**

**与RAID3相似，都是将数据条块化分布于不同硬盘上，条块单位为位或字节。 使用一定的编码技术提供错误检索及恢复。它可以在数据发生错误的情况下将错误校正，以保证输出的正确。数据传送速率相当高**

**RAID3带奇偶校验码的并行传送**

**校验码与RAID2不同，访问数据时一次处理一个带区，可以提高读取和写入速度，像RAID0一样来存放数据，但速度没RAID0快。校验码在写入数据时产生并保存在另一个磁盘上。需要实现时用户必须要有三个以上的驱动器，写入/读出速率都很高。因校验位较少，所以计算时间相对较少**

**RAID4 带奇偶校验码的独立磁盘结构**

**RAID4与RAID3很象，不同的是，它对数据的访问是按数据块进行的**

**RAID5 分布式奇偶校验的独立磁盘结构**

**奇偶校验码存在于所有磁盘上，提高了可靠性，允许单个磁盘出错。读出效率很高，写入效率一般，块式的集体访问效率不错。提供了冗余性，磁盘空间利用率较高，读写速度较快1倍。**

**RAID6 带有两种分布存储的奇偶校验码的独立磁盘结构**

**是对RAID5的扩展，主要用于要求 数据绝对不能出错的场合。由于引入了第二种奇偶校验值，所以需要X+2个磁盘，同时对控制器的设计变得十分复杂，用于计算奇偶校验值和验证数据正确性所花费的时间比较多，造成了不必须的负载。除军队没有人用得起这种东西**

**RAID7 优化的高速数据传送磁盘结构**

**RAID7中所有I/O传送均是同步进行的，可以分别控制，这样提高了系统的并行怀，提高系统访问数据的速度；允许使用SNMP协议进行**

**68.数据库本身设计上考虑到了加速查询问题，有一些基本概念，如（主键，索引，外键，触发器）是什么意思呢？**

**主键：**

**能够唯一标识表中某一行的属性或属性组。一个表只能有一个主键，但可以有多个候选索引。主键常常与外键构成参照完整性约束，防止出现数据不一致。主键可以保证记录的唯一和主键域非空,数据库管理系统对于主键自动生成唯一索引，所以主键也是一个特殊的索引。**

**索引：**

**是用来快速地寻找那些具有特定值的记录。主要是为了检索的方便，是为了加快访问速度， 按一定的规则创建的，一般起到排序作用。**

**外键：**

**是用于建立和加强两个表数据之间的链接的一列或多列。外键约束主要用来维护两个表之间数据的一致性。简言之，表的外键就是另一表的主键，外键将两表联系起来。一般情况下，要删除一张表中的主键必须首先要确保其它表中的没有相同外键（即该表中的主键没有一个外键和它相关联）。**

**触发器：**

**触发器是一种与表操作有关的数据库对象，当触发器所在表上出现指定事件时，将调用该对象，即表的操作事件触发表上的触发器的执行。**

69.**既然数据库可以通过二进制日志来执行数据复制，那么可不可以通过二进制日志进行数据库备份和还原呢？**

**在my.cnf中的mysqld下 添加**

**log-bin=mysql-bin**

**binlog\_format=mixed**

**重启服务后便可以看到新增的日志文件了**

**日志位置**

**>>如果没有指定文件名,则Mysql使用hostname-bin文件.**

**>>如果指定了相对路径,则假定该路径相对于数据目录**

**>>Mysql在文件名后添加了数字索引.所以该文件最后的形式为filename.number**

**一个例子：**

**log-bin=”D:/mysql/log/binlog” 那么，在该文件夹下就会有文件D:/mysql/log/binlog.000001等**

**1.清除binlog**

**PURGE {MASTER | BINARY} LOGS TO ‘log\_name' //log\_name不会被清除**

**PURGE {MASTER | BINARY} LOGS BEFORE ‘date' //date不会被清除**

**例如**

**mysql> purge master logs to ‘binlog.000004′;**

**mysql> purge master logs before '2009-09-22 00:00:00′;**

**删除之前所有的binlog，并重新生成新的binlog**

**2.记录到二进制日志知的内容配置**

**binlog-do-db=sales 只记录sales库**

**binlog-ignore-db=sales 除sales库不记录，其他都记**

**3.二进制日志不准确的处理**

**mysqldump --databases repltest --flush-logs --opt repltest>q:/repltest\_full\_01.sql**

**上面这句话可以在备份的同时刷新日志，生成新的日志，这样新日志里面的内容相当于这次备份之后的增量部分，可以用这种方式来实现mysql的**

**恢复**

**/usr/local/mysql/bin/mysqlbinlog bin.000001 |mysql -u root -p**

**70.如果mysql群集中的主机不能满足业务需求量呢？如何新增数据库服务器呢？思路是什么？**

**首先需要关注数据库**

**HTML静态化**

**图片服务器分离**

**图片服务器分离**

**网站架构和网站开发中的缓存**

**nginx分流**

**镜像是大型网站常采用的提高性能和数据安全性的方式**

**负载均衡将是大型网站解决高负荷访问和大量并发请求采用的终极解决办法**

**硬件四层交换**

**软件四层交换**

**71.mysql如何优化？**

**在Join表的时候使用相当类型的例，并将其索引**

**为搜索字段建索引**

**避免 SELECT \***

**永远为每张表设置一个ID**

**使用 ENUM 而不是 VARCHAR**

**尽可能的使用 NOT NULL**

**无缓冲的查询**

**固定长度的表会更快**

**垂直分割**

**越小的列会越快**

**72.mysql中间件有哪些？区别？**

**mysql-proxy是官方提供的mysql中间件产品可以实现负载平衡，读写分离，failover等，但其不支持大数据量的分库分表且性能较差。下面介绍几款能代替其的mysql开源中间件产品以及区别**

**Atlas , cabar , TDDL**

**Atlas功能特性**

**1.主库宕机不影响读**

**2.通过管理接口，简化管理工作，DB的上下线对应用完全透明，同时可以手动上下线。**

**3.自己实现读写分离**

**4.自己实现分表**

**5.之前官方主要功能逻辑由使用lua脚本编写，效率低，Atlas用C改写，QPS提高，latency降低。**

**6.安全方面的提升**

**7.平滑重启**

**cabar优点总结：**

**1.数据和访问从集中式改变为分布：**

**2.解决连接数过大的问题。**

**3.对业务代码侵入性少。**

**4.提供数据节点的failover,HA：**

**TDDL主要优点：**

**1.数据库主备和动态切换**

**2.带权重的读写分离**

**3.单线程读重试**

**4.集中式数据源信息管理和动态变更**

**5.剥离的稳定jboss数据源**

**6.支持mysql和oracle数据库**

**73.什么是PV.UV？**

**PV是基于访客数的浏览量，即网页访问数**

**UV，即独立访客数。**

**指访问某个站点或点击某条新闻的不同访客人数。**

**一日内访问某个网站或者网页的不同用户数量。**

**同一个用户对一个网站或者一个网页的多次访问记为贡献一个uv。**