# Linux

# CPU

# top

* top：查看每个进程的情况
* 在top模式下，输入1：查看每个CPU的性能数据，注意观察是否有CPU100%占用率
* CPU参数含义：
  + 1)us过高表示Java应用程序消耗了大量CPU，需要定位是哪一个线程，并分析线程堆栈。
* 在top模式下，输入H：查看每个线程的性能信息
* 如果某个线程CPU利用率一直100%，则说明这个线程可能有死循环，也有可能是GC的问题。jstat命令可以查看GC情况，是不是产生了FullGC。
* 还可以把线程dump下来，看看是哪个线程、执行什么代码造成的CPU利用率高。
* jstack PID | grep ‘nid=十六进制线程id’ > /dir
* dump出来的线程ID（nid)是十六进制，TOP命令看到的线程ID是十进制的
  + 2)sy过高表示花费了更多时间进行线程切换。同样需要查看Java线程的状态。

# 文件IO 磁盘

# ls

* 显示文件夹下的文件详情，包括大小
* ls –al
* a表示all，包括隐藏文件

# stat（查看文件详情)

* stat filepath

# 软硬连接

* 软硬连接（inode这块，ln / ln -s)
* 硬链接 (hard link) 与软链接（又称符号链接，即 soft link 或 symbolic link)。链接为 Linux 系统解决了文件的共享使用，还带来了隐藏文件路径、增加权限安全及节省存储等好处。若一个 inode 号对应多个文件名，则称这些文件为硬链接。换言之，硬链接就是同一个文件使用了多个别名。硬链接可由命令 link 或 ln 创建。
* 软链接与硬链接不同，若文件用户数据块中存放的内容是另一文件的路径名的指向，则该文件就是软连接。软链接就是一个普通文件，只是数据块内容有点特殊。软链接有着自己的 inode 号以及用户数据块。
* ln -s source target

# 文本操作命令

* cat 由第一行开始显示内容，并将所有内容输出
* tac 从最后一行倒序显示内容，并将所有内容输出
* more 根据窗口大小，一页一页的显示文件内容
* less 和more类似，但其优点可以往前翻页，而且进行可以搜索字符
* head 只显示头几行
* tail 只显示最后几行
* sort、uniq
* sort 进行排序。
* $ sort [-fbMnrtuk] [file or stdin]
* -f ：忽略大小写
* -b ：忽略最前面的空格
* -M ：以月份的名字来排序，例如 JAN, DEC
* -n ：使用数字
* -r ：反向排序
* -u ：相当于 unique ，重复内容只出现一次
* -t ：分隔符，默认为tab
* -k ：指定排序的区间
* 范例：/etc/passwd 内容是以 : 来分隔的，以第三栏来排序。
* $ cat /etc/passwd | sort -t ':' -k 3
* root❌0:0:root:/root:/bin/bash
* dmtsai❌1000:1000:dmtsai:/home/dmtsai:/bin/bash
* alex❌1001:1002::/home/alex:/bin/bash
* arod❌1002:1003::/home/arod:/bin/bash
* uniq 可以将重复的数据只取一个。
* $ uniq [-ic]
* -i ：忽略大小写
* -c ：进行计数
* 使用cat命令可以显示文本文件内容,或 把几个文件内容附加到另一个文件中。
* 使用more命令可以分页显示文本文件的内容。
* 使用less命令可以回卷显示文本文件的内容。
* 使用head命令可以显示指定文件的前若干行文件内容。
* 使用tail命令可以查看文件的末尾数据。
* 使用sort命令可以对文件中的数据进行排序,并将结果显示在标准输出上。
* 使用uniq命令可以将文件内的重复行数据从输出文件中删除,只留下每条记录的唯一样本。
* 使用cut命令可以从文件的每行中显示出选定的字节、字符或字段。
* 使用comm命令可以比较两个已排过序的文件,并将其结果显示出来。
* 使用diff命令可以逐行比较两个文本文件,列出其不同之处。它比comm命令完成更复杂的检查。它对给出的文件进行系统的检查,并显示出两个文件中所有不同的行,不要求事先对文件进行排序。

# vim

* vi编辑器有3种基本工作模式,分别是命令行模式、插入模式和末行模式。
* 命令行模式控制屏幕光标的移动,字符、字或行的删除,移动、复制某区域及进入插入模式,或者到末行模式。
* 只有在插入模式下,才可以做文字输入,按“Esc”键可回到命令行模式。
* 末行模式将文件保存或退出vi编辑器,也可以设置编辑环境,如寻找字符串、列出行号等。
* 在指令列模式下，有以下命令用于离开或者存储文件。
* 命令 作用
* :w 写入磁盘
* :w! 当文件为只读时，强制写入磁盘。到底能不能写入，与用户对该文件的权限有关
* :q 离开
* :q! 强制离开不保存
* :wq 写入磁盘后离开
* :wq! 强制写入磁盘后离开

# 实时查看日志命令

* tail -f path
* -f 循环读取

# 系统日志

* /var/log/message 系统启动后的信息和错误日志，是Red Hat Linux中最常用的日志之一
* /var/log/secure 与安全相关的日志信息
* /var/log/maillog 与邮件相关的日志信息
* /var/log/cron 与定时任务相关的日志信息
* /var/log/spooler 与UUCP和news设备相关的日志信息
* /var/log/boot.log 守护进程启动和停止相关的日志消息
* /var/log/wtmp 该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件

# find

* 查找磁盘上最大的文件的命令
* find / -type f -size +10G
* 列出当前目录及子目录下所有文件和文件夹
* 在/home目录下查找以.txt结尾的文件名 find /home -name "\*.txt"
* 同上，但忽略大小写 find /home -iname "\*.txt"
* 当前目录及子目录下查找所有以.txt和.pdf结尾的文件 find . ( -name "*.txt" -o -name "*.pdf" ) 或 find . -name "*.txt" -o -name "*.pdf"
* 匹配文件路径或者文件 find /usr/ -path "*local*"
* 基于正则表达式匹配文件路径 find . -regex ".\*(.txt|.pdf)$"
* 同上，但忽略大小写 find . -iregex ".\*(.txt|.pdf)$"
* 找出/home下不是以.txt结尾的文件 find /home ! -name "\*.txt"
* 根据文件类型进行搜索find . -type 类型参数
* 类型参数列表：
* f 普通文件
* l 符号连接
* d 目录
* c 字符设备
* b 块设备
* s 套接字
* p Fifo
* 基于目录深度搜索
* 向下最大深度限制为3 find . -maxdepth 3 -type f
* 搜索出深度距离当前目录至少2个子目录的所有文件 find . -mindepth 2 -type f
* 根据文件时间戳进行搜索 find . -type f 时间戳
* UNIX/Linux文件系统每个文件都有三种时间戳：
* 访问时间（-atime/天，-amin/分钟)：用户最近一次访问时间。
* 修改时间（-mtime/天，-mmin/分钟)：文件最后一次修改时间。
* 变化时间（-ctime/天，-cmin/分钟)：文件数据元（例如权限等)最后一次修改时间。
* 搜索最近七天内被访问过的所有文件
* find . -type f -atime -7 搜索恰好在七天前被访问过的所有文件
* find . -type f -atime 7 搜索超过七天内被访问过的所有文件
* find . -type f -atime +7 搜索访问时间超过10分钟的所有文件
* find . -type f -amin +10 找出比file.log修改时间更长的所有文件
* find . -type f -newer file.log 根据文件大小进行匹配
* find . -type f -size 文件大小单元 文件大小单元：
* b —— 块（512字节)
* c —— 字节
* w —— 字（2字节)
* k —— 千字节
* M —— 兆字节
* G —— 吉字节
* 搜索大于10KB的文件find . -type f -size +10k
* 搜索小于10KB的文件find . -type f -size -10k
* 搜索等于10KB的文件find . -type f -size 10k
* 删除匹配文件
* 删除当前目录下所有.txt文件 find . -type f -name "\*.txt" -delete
* 根据文件权限/所有权进行匹配
* 当前目录下搜索出权限为777的文件 find . -type f -perm 777
* 找出当前目录下权限不是644的php文件 find . -type f -name "\*.php" ! -perm 644
* 找出当前目录用户tom拥有的所有文件 find . -type f -user tom
* 将当前目录下所有以“.txt”结尾的文件打印出来，再追问，除了“.txt”再加上“.abc”结尾的也打印出来。
* find . -name "\*.txt"

# grep

* 在文件内查找字符串
* grep “字符串” filename

# 文件权限

- r：可读(4)  
- w：可写(2)，对于目录来说表示可在目录中新建文件  
- x：可执行(1)，对于目录来说为可进入到该目录中

* -：表示无对应位上的权限
* 4代表读权限，2代表写权限，1代表执行权限
* 7=4+2+1,表示拥有可读可写可执行权限
* 5=4+1,表示拥有可读可执行权限，但是没有写权限
* 4 代表拥有可读权限
* 0 代表没有任何权限

# chmod 修改文件属性

* chmod 777 /home/berry
* chmod u+x /home/berry
* u 表示“用户（user)”，即文件或目录的所有者。
* g 表示“同组（group)用户”，即与文件属主有相同组ID的所有用户。
* o 表示“其他（others)用户”。
* a 表示“所有（all)用户”。它是系统默认值。

# chown 修改文件的属主与属组

* chown guest:guest a.txt
* chown -R guest /home/berry (把berry文件下的所有文件都改成guest这个组)

# chgrp 修改文件的所属的用户组

* chgrp -R guest /var/tmp/f.txt
* chgrp - R root /home/berry/file/a.txt

# iostat（查看各个设备的IO状态，查看磁盘读写性能)

* 直接输入iostat：
* tps是每秒的IO请求数，这是IO消耗情况值得关注的数字。
* Blk\_read/s是指每秒读取的块数量，通过块的大小是512字节
* Blk\_read是指总共读取的块数量
* iostat –x xvda 3 5 定时采样查看IO消耗情况
* 首先要关注的是CPU中的iowait%所占的百分比，当iowait占据主要的百分比时，就表示要关注IO方面的消耗状况了。

# pidstat（查看某个线程的IO状态)

* pidstat –d –t –p [pid] 1 100
* KB\_rd/s 表示每秒读取的KB数
* KB\_wd/s 表示每秒写入的KB数
* 通过pidstat直接找到文件IO操作多的线程，之后结合jstack找到对应的Java代码。

# cp/mv的区别

* 1、功能上的区别
* mv：用户可以使用该命令为文件或目录重命名或将文件由一个目录移入另一个目录中。
* cp: 该命令的功能是将给出的文件或目录拷贝到另一文件或目录中。
* 2、从inode角度来区分
* mv：会将存储于indoe索引节点上的文件元信息也移动到新文件中。
* cp : 只会复制文件数据，不会复制inode索引节点上的文件元信息。
* cp 的时候是真正意义上的内容copy，对于 inode 节点却是不会变化的。
* mv 的时候是把源文件直接删除了（inode 删除了)，新的文件其实已经不是以前的文件了，只是名字一样而已。

# 网络

# netstat（端口)

- 查看tcp连接数状态

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

- 统计8080端口上有多少个TCP连接，命令：

* netstat –nat | grep 8080 | wc –l

- TCP连接中有多少个连接状态是ESTABLISHED，命令：

* netstat –nat | grep 8080 | grep ESTABLISHED| wc -l

- TCP连接中有多少个连接状态是CLOSE\_WAIT

* netstat –nat | grep 8080 | grep CLOSE\_WAIT| wc -l

- TCP连接中有多少个连接状态是TIME\_WAIT

* netstat –nat | grep 8080 | grep TIME\_WAIT| wc -l  
  - 使用awk来完成统计信息，命令如下
* netstat –nat | grep 8080 | awk ‘{++S[$NF]} END {for (a in S) print a, S[a]}’

# sar

* sar –n FULL 1 2 执行后以1s为频率，总共输出两次网络IO的消耗情况。
* 输出信息包含三部分：网卡上成功的接包和发包的信息 网卡上失败的接包和发包信息 sockets上的统计信息（tcpsck、udpsck)
* 如需详细跟踪tcp/ip通信过程的信息，则可通过tcpdump来进行。

# tcpdump

* tcpdump [ -DenNqvX ] [ -c count ] [ -F file ] [ -i interface ] [ -r file ]
* [ -s snaplen ] [ -w file ] [ expression ]
* 抓包选项：
* -c：指定要抓取的包数量。注意，是最终要获取这么多个包。例如，指定"-c 10"将获取10个包，但可能已经处理了100个包，只不过只有10个包是满足条件的包。
* -i interface：指定tcpdump需要监听的端口。若未指定该选项，将从系统接口列表中搜寻编号最小的已配置好的接口(不包括loopback端口，要抓取loopback接口使用tcpdump -i lo)，
* ：一旦找到第一个符合条件的端口，搜寻马上结束。可以使用'any'关键字表示所有网络接口。
* -n：对地址以数字方式显式，否则显式为主机名，也就是说-n选项不做主机名解析。
* -nn：除了-n的作用外，还把端口显示为数值，否则显示端口服务名。
* -N：不打印出host的域名部分。例如tcpdump将会打印'nic'而不是'nic.ddn.mil'。
* -P：指定要抓取的包是流入还是流出的包。可以给定的值为"in"、"out"和"inout"，默认为"inout"。
* -s len：设置tcpdump的数据包抓取长度为len，如果不设置默认将会是65535字节。对于要抓取的数据包较大时，长度设置不够可能会产生包截断，若出现包截断，
* ：输出行中会出现"[|proto]"的标志(proto实际会显示为协议名)。但是抓取len越长，包的处理时间越长，并且会减少tcpdump可缓存的数据包的数量，
* ：从而会导致数据包的丢失，所以在能抓取我们想要的包的前提下，抓取长度越小越好。
* 输出选项：
* -e：输出的每行中都将包括数据链路层头部信息，例如源MAC和目标MAC。
* -q：快速打印输出。即打印很少的协议相关信息，从而输出行都比较简短。
* -X：输出包的头部数据，会以16进制和ASCII两种方式同时输出。
* -XX：输出包的头部数据，会以16进制和ASCII两种方式同时输出，更详细。
* -v：当分析和打印的时候，产生详细的输出。
* -vv：产生比-v更详细的输出。
* -vvv：产生比-vv更详细的输出。
* 其他功能性选项：
* -D：列出可用于抓包的接口。将会列出接口的数值编号和接口名，它们都可以用于"-i"后。
* -F：从文件中读取抓包的表达式。若使用该选项，则命令行中给定的其他表达式都将失效。
* -w：将抓包数据输出到文件中而不是标准输出。可以同时配合"-G time"选项使得输出文件每time秒就自动切换到另一个文件。可通过"-r"选项载入这些文件以进行分析和打印。
* -r：从给定的数据包文件中读取数据。使用"-"表示从标准输入中读取。
  + (1).默认启动
* tcpdump
* 默认情况下，直接启动tcpdump将监视第一个网络接口(非lo口)上所有流通的数据包。这样抓取的结果会非常多，滚动非常快。
  + (2).监视指定网络接口的数据包
* tcpdump -i eth1
* 如果不指定网卡，默认tcpdump只会监视第一个网络接口，如eth0。
  + (3).监视指定主机的数据包，例如所有进入或离开longshuai的数据包
* tcpdump host longshuai
  + (4).打印helios<-->hot或helios<-->ace之间通信的数据包
* tcpdump host helios and ( hot or ace )
  + (5).打印ace与任何其他主机之间通信的IP数据包,但不包括与helios之间的数据包
* tcpdump ip host ace and not helios
  + (6).截获主机hostname发送的所有数据
* tcpdump src host hostname
  + (7).监视所有发送到主机hostname的数据包
* tcpdump dst host hostname
  + (8).监视指定主机和端口的数据包
* tcpdump tcp port 22 and host hostname
  + (9).对本机的udp 123端口进行监视(123为ntp的服务端口)
* tcpdump udp port 123
* (10).监视指定网络的数据包，如本机与192.168网段通信的数据包，"-c 10"表示只抓取10个包
* tcpdump -c 10 net 192.168
  + (11).打印所有通过网关snup的ftp数据包(注意,表达式被单引号括起来了,这可以防止shell对其中的括号进行错误解析)
* shell> tcpdump 'gateway snup and (port ftp or ftp-data)'
  + (12).抓取ping包
* [root@server2 ~]# tcpdump -c 5 -nn -i eth0 icmp

# 内存

# vmstat、sar、top、pidstat等可以查看swap和物理内存的消耗情况。

* vmstat和sar共同的弱点是不能分析进程所占用的内存量。
* top可以查看进程所消耗的内存量，在top中看Java进程的内存包括了JVM已分配的内存加上JVM外的物理内存。
* pidstat也可以查看进程所消耗的内存量。
* pidstat –r –p [pid] [interval] [times]

# 进程

# ps –ef/-aux

* ps aux 和ps -ef
* 两者的输出结果差别不大，但展示风格不同。aux是BSD风格，-ef是System V风格。这是次要的区别，一个影响使用的区别是aux会截断command列，而-ef不会。当结合grep时这种区别会影响到结果。
* ps -ef 显示出的结果：
* 1.UID 用户ID
* 2.PID 进程ID
* 3.PPID 父进程ID
* 4.C CPU占用率
* 5.STIME 开始时间
* 6.TTY 开始此进程的TTY----终端设备
* 7.TIME 此进程运行的总时间
* 8.CMD 命令名

# lsof 进程打开的文件、端口

* lsof ［options］ filename
* -a：列出打开文件存在的进程；
* -c<进程名>：列出指定进程所打开的文件；
* -g：列出GID号进程详情；
* -d<文件号>：列出占用该文件号的进程；
* +d<目录>：列出目录下被打开的文件；
* +D<目录>：递归列出目录下被打开的文件；
* -n<目录>：列出使用NFS的文件；
* -i<条件>：列出符合条件的进程。（4、6、协议、:端口、 @ip )
* -p<进程号>：列出指定进程号所打开的文件；
* -u：列出UID号进程详情；
* -h：显示帮助信息；
* -v：显示版本信息。
* lsof输出各列信息的意义如下：
* COMMAND：进程的名称
* PID：进程标识符
* USER：进程所有者
* FD：文件描述符，应用程序通过文件描述符识别该文件。如cwd、txt等
* TYPE：文件类型，如DIR、REG等
* DEVICE：指定磁盘的名称
* SIZE：文件的大小
* NODE：索引节点（文件在磁盘上的标识)
* NAME：打开文件的确切名称
* cwd：表示current work dirctory，即：应用程序的当前工作目录，这是该应用程序启动的目录，除非它本身对这个目录进行更改
* txt：该类型的文件是程序代码，如应用程序二进制文件本身或共享库，如上列表中显示的 /sbin/init 程序
* lnn：library references (AIX);
* er：FD information error (see NAME column);
* jld：jail directory (FreeBSD);
* ltx：shared library text (code and data);
* mxx ：hex memory-mapped type number xx.
* m86：DOS Merge mapped file;
* mem：memory-mapped file;
* mmap：memory-mapped device;
* pd：parent directory;
* rtd：root directory;
* tr：kernel trace file (OpenBSD);
* v86 VP/ix mapped file;
* 0：表示标准输出
* 1：表示标准输入
* 2：表示标准错误

# kill

* 杀死进程

# 负载 Load Average

* 系统的load被定义为特定时间间隔内运行队列的平均线程数，如果一个线程满足以下条件，该线程就会处于运行队列中：   
  1.- 没有处于I/O等待状态。  
  2.- 没有主动进入等待状态，也就是没有调用wait操作；  
  3.- 没有被终止。
* 每个CPU的核都维护了一个运行队列，系统的load主要由运行队列来决定。load的值越大，也就意味着系统的CPU越繁忙，这样线程运行完以后等待操作系统分配下一个时间片段的时间也就越长。一般来说，只要每个CPU当前的活动线程数不大于3，我们认为它的负载是正常的，如果每个CPU的线程数大于5，则表示当前系统的负载已经非常高了，需要采取措施来减低系统的负载，以提高响应速度。
* 使用top命令查看，该值是三个浮点数，表示最近1分钟、5分钟、15分钟的运行队列平均进程数。

# AWK/SED

# awk

* awk是一个强大的文本分析工具，相对于grep的查找，sed的编辑，awk在其对数据分析并生成报告时，显得尤为强大。简单来说awk就是把文件逐行的读入，以空格为默认分隔符将每行切片，切开的部分再进行各种分析处理。
* awk '{pattern + action}' {filenames}
* 统计ip
* cat test.txt | awk '{print $2}' | sort | uniq -c | sort -n -r | head -n 1

# sed 编辑文本

* sed -e 's/foo/bar/' myfile
* 将 myfile 文件中每行第一次出现的foo用字符串bar替换，然后将该文件内容输出到标准输出
* sed -e 's/foo/bar/g' myfile
* g 使得 sed 对文件中所有符合的字符串都被替换
* sed -i 's/foo/bar/g' myfile
* 选项 i 使得 sed 修改文件
* sed -i 's/foo/bar/g' ./m\*
* 批量操作当前目录下以 m 开头的文件
* sed -i 's/foo/bar/g' grep foo -rl --include="m\*" ./
* ``括起来的grep命令，表示将grep命令的的结果作为操作文件
* grep 命令中，选项r表示查找所有子目录，l表示仅列出符合条件的文件名，用来传给sed命令做操作，--include="m\*" 表示仅查找 m 开头的文件

# 管道

* 管道是linux提供的一种常见的进程通信工具
* 管道中的数据只能读取一次
* 管道的实现并没有使用专门的数据结构，而是借助了文件系统的file结构和VFS的索引节点inode。通过将两个 file 结构指向同一个临时的 VFS 索引节点，而这个 VFS 索引节点又指向一个物理页面而实现的。

# IO模型

# mmap

* 零拷贝技术：让数据传输不需要经过user space 使用mmap
* mmap系统调用导致文件的内容通过DMA模块被复制到内核缓冲区中，该缓冲区之后与用户进程共享，这样就内核缓冲区与用户缓冲区之间的复制就不会发生。

# sendfile

* ssize*t sendfile(int out*fd, int in*fd, off*t \*offset, size\_t count);
* 参数特别注意的是：in\_fd必须是一个支持mmap函数的文件描述符，也就是说必须指向真实文件，不能使用socket描述符和管道。
* out\_fd必须是一个socket描述符。
* 由此可见sendfile几乎是专门为在网络上传输文件而设计的。
* Sendfile 函数在两个文件描述符之间直接传递数据(完全在内核中操作，传送)，从而避免了内核缓冲区数据和用户缓冲区数据之间的拷贝，操作效率很高，被称之为零拷贝。

# select poll（NIO)

* select poll epoll都是IO多路复用的实现方式！
* select系统调用的目的是：在一段指定时间内，监听用户感兴趣的文件描述符上的可读、可写和异常（异常不包括网络断开)事件。poll和select应该被归类为这样的系统调用，它们可以阻塞地同时探测一组支持非阻塞的IO设备，直至某一个设备触发了事件或者超过了指定的等待时间——也就是说它们的职责不是做IO，而是帮助调用者寻找当前就绪的设备。
* int select(int nfds, fd*set \*readfds, fd*set \*writefds, fd\_set \*exceptfds, struct timeval \*timeout);
* fd*set结构体是文件描述符集，该结构体实际上是一个整型数组，数组中的每个元素的每一位标记一个文件描述符。fd*set能容纳的文件描述符数量由FD*SETSIZE指定，一般情况下，FD*SETSIZE等于1024，这就限制了select能同时处理的文件描述符的总量。
  + 1)nfds参数指定被监听的文件描述符的总数。通常被设置为select监听的所有文件描述符中最大值加1；
  + 2)readfds、writefds、exceptfds分别指向可读、可写和异常等事件对应的文件描述符集合。这三个参数都是传入传出型参数，指的是在调用select之前，用户把关心的可读、可写、或异常的文件描述符通过FD\_SET函数分别添加进readfds、writefds、exceptfds文件描述符集，select将对这些文件描述符集中的文件描述符进行监听，如果有就绪文件描述符，select会重置readfds、writefds、exceptfds文件描述符集来通知应用程序哪些文件描述符就绪。这个特性将导致select函数返回后，再次调用select之前，必须重置我们关心的文件描述符，也就是三个文件描述符集已经不是我们之前传入 的了。
  + 3)timeout参数用来指定select函数的超时时间。
  + 1)如果指定timeout为NULL，select会永远等待下去，直到有一个文件描述符就绪，select返回；
  + 2)如果timeout的指定时间为0，select根本不等待，立即返回；
  + 3)如果指定一段固定时间，则在这一段时间内，如果有指定的文件描述符就绪，select函数返回，如果超过指定时间，select同样返回。
* select的几大缺点：
  + 1)每次调用select，都需要把fd集合从用户态拷贝到内核态，这个开销在fd很多时会很大
  + 2)每次调用select都需要在内核遍历传递进来的所有fd，这个开销在fd很多时也很大（不适合服务器，但客户端也可以使用)
  + 3)select支持的文件描述符数量太小了，默认是1024
* int poll(struct pollfd \*fds, nfds\_t nfds, int timeout);
* 与select非常类似，poll比select的好处就是没有描述符数量限制，select 有1024 的限制，描述符不能超过此值，poll不受限制。
* 此函数在系统调用select内部被使用，作用是把当前的文件指针挂到设备内部定义的等待
* 队列中。
* send不是立即发送数据，而是将数据放在本地网卡缓冲区中。

# epoll（NIO)

* select,poll还是在应用中轮询Socket，容易浪费；OS会自动轮询，通过epoll\_wait返回。
* epoll 与select和poll在使用和实现上有很大区别。首先，epoll使用一组函数来完成，而不是单独的一个函数；其次，epoll把用户关心的文件描述符上的事件放在内核里的一个事件表中，无须向select和poll那样每次调用都要重复传入文件描述符集合事件集。
* 系统调用：
* epoll*create 创建一个epoll对象，一般epollfd = epoll*create()
* epoll*ctl （epoll*add/epoll\_del的合体)，往epoll对象中增加/删除某一个流的某一个事件
* 比如
* epoll*ctl(epollfd, EPOLL*CTL\_ADD, socket, EPOLLIN);//注册缓冲区非空事件，即有数据流入
* epoll*ctl(epollfd, EPOLL*CTL\_DEL, socket, EPOLLOUT);//注册缓冲区非满事件，即流可以被写入
* epoll\_wait(epollfd,...)等待直到注册的事件发生
* （注：当对一个非阻塞流的读写发生缓冲区满或缓冲区空，write/read会返回-1，并设置errno=EAGAIN。而epoll只关心缓冲区非满和缓冲区非空事件)。
* 对于第一个缺点，epoll的解决方案在epoll*ctl函数中。每次注册新的事件到epoll句柄中时（在epoll*ctl中指定EPOLL*CTL*ADD)，会把所有的fd拷贝进内核，而不是在epoll\_wait的时候重复拷贝。epoll保证了每个fd在整个过程中只会拷贝一次。
* 对于第二个缺点，epoll的解决方案不像select或poll一样每次都把current轮流加入fd对应的设备等待队列中，而只在epoll*ctl时把current挂一遍（这一遍必不可少)并为每个fd指定一个回调函数，当设备就绪，唤醒等待队列上的等待者时，就会调用这个回调函数，而这个回调函数会把就绪的fd加入一个就绪链表。epoll*wait的工作实际上就是在这个就绪链表中查看有没有就绪的fd（利用schedule\_timeout()实现睡一会，判断一会的效果，和select实现中的第7步是类似的)。
* 对于第三个缺点，epoll没有这个限制，它所支持的FD上限是最大可以打开文件的数目，这个数字一般远大于2048,举个例子,在1GB内存的机器上大约是10万左右，具体数目可以cat /proc/sys/fs/file-max察看,一般来说这个数目和系统内存关系很大。
* 总结：
  + 1)select，poll实现需要自己不断轮询所有fd集合，直到设备就绪，期间可能要睡眠和唤醒多次交替。而epoll其实也需要调用epoll*wait不断轮询就绪链表，期间也可能多次睡眠和唤醒交替，但是它是设备就绪时，调用回调函数，把就绪fd放入就绪链表中，并唤醒在epoll*wait中进入睡眠的进程。虽然都要睡眠和交替，但是select和poll在“醒着”的时候要遍历整个fd集合，而epoll在“醒着”的时候只要判断一下就绪链表是否为空就行了，这节省了大量的CPU时间。这就是回调机制带来的性能提升。
  + 2)select，poll每次调用都要把fd集合从用户态往内核态拷贝一次，并且要把current往设备等待队列中挂一次，而epoll只要一次拷贝，而且把current往等待队列上挂也只挂一次（在epoll\_wait的开始，注意这里的等待队列并不是设备等待队列，只是一个epoll内部定义的等待队列)。这也能节省不少的开销。

## epoll原理

1.- epoll初始化时，会向内核注册一个文件系统，用于存储被监控的句柄文件，调用epoll*create时，会在这个文件系统中创建一个file节点。同时epoll会开辟自己的内核高速缓存区，以红黑树的结构保存句柄，以支持快速的查找、插入、删除。还会再建立一个list链表，用于存储准备就绪的事件。*  
*2.- 当执行epoll*ctl时，除了把socket句柄放到epoll文件系统里file对象对应的红黑树上之外，还会给内核中断处理程序注册一个回调函数，告诉内核，如果这个句柄的中断到了，就把它放到准备就绪list链表里。所以，当一个socket上有数据到了，内核在把网卡上的数据copy到内核中后，就把socket插入到就绪链表里。  
3.- 当epoll\_wait调用时，仅仅观察就绪链表里有没有数据，如果有数据就返回，否则就sleep，超时时立刻返回。

## 边缘触发模式ET（Edge*triggered)和水平触发模式LT（Level*triggered)

* Level*triggered(水平触发)：当被监控的文件描述符上有可读写事件发生时，epoll*wait()会通知处理程序去读写。如果这次没有把数据一次性全部读写完(如读写缓冲区太小)，那么下次调用 epoll\_wait()时，它还会通知你在上没读写完的文件描述符上继续读写，当然如果你一直不去读写，它会一直通知你！！！如果系统中有大量你不需要读写的就绪文件描述符，而它们每次都会返回，这样会大大降低处理程序检索自己关心的就绪文件描述符的效率！！！
* Edge*triggered(边缘触发)：当被监控的文件描述符上有可读写事件发生时，epoll*wait()会通知处理程序去读写。如果这次没有把数据全部读写完(如读写缓冲区太小)，那么下次调用epoll\_wait()时，它不会通知你，也就是它只会通知你一次，直到该文件描述符上出现第二次可读写事件才会通知你！！！这种模式比水平触发效率高，系统不会充斥大量你不关心的就绪文件描述符！！！

# IOCP（AIO)

* 微软在 Winsocket2 中引入了 IOCP（Input/Output Completion Port)模型。IOCP 是 Input/Output Completion Port（I/O 完成端口)的简称。简单的说，IOCP 是一种高性能的 I/O 模型，是一种应用程序使用线程池处理异步 I/O 请求的机制。Java7 中对 IOCP 有了很好的封装，程序员可以非常方便的时候经过封装的 channel 类来读写和传输数据。
* 不仅和epoll一样接收到Socket的事件，并且接收时OS已经完成了IO，不需要在应用层进行IO。
* 首先我们创建一个完成端口 CreateIOCompletionPort，然后再创建一个或多个工作线程，并指定它们到这个完成端口上去读取数据。再将远程连接的套接字句柄关联到这个完成端口。工作线程调用 getQueuedCompletionStatus 方法在关联到这个完成端口上的所有套接字上等待 I/O 的完成，再判断完成了什么类型的 I/O，然后接着发出 WSASend 和 WSARecv，并继续下一次循环阻塞在 getQueuedCompletionStatus。
* 具体的说，一个完成端口大概的处理流程包括：
* 创建一个完成端口；
* Port port = createIoCompletionPort(INVALID*HANDLE*VALUE, 0, 0, fixedThreadCount());
* 创建一个线程 ThreadA；
* ThreadA 线程循环调用 GetQueuedCompletionStatus 方法来得到 I/O 操作结果，这个方法是一个阻塞方法；
* While(true){
* getQueuedCompletionStatus(port, ioResult);
* }
* 主线程循环调用 accept 等待客户端连接上来；
* 主线程 accept 返回新连接建立以后，把这个新的套接字句柄用 CreateIoCompletionPort 关联到完成端口，然后发出一个异步的 Read 或者 Write 调用，因为是异步函数，Read/Write 会马上返回，实际的发送或者接收数据的操作由操作系统去做。
* if (handle != 0L) {
* createIoCompletionPort(handle, port, key, 0);
* }
* 主线程继续下一次循环，阻塞在 accept 这里等待客户端连接。
* 操作系统完成 Read 或者 Write 的操作，把结果发到完成端口。
* ThreadA 线程里的 GetQueuedCompletionStatus() 马上返回，并从完成端口取得刚完成的 Read/Write 的结果。
* 在 ThreadA 线程里对这些数据进行处理 ( 如果处理过程很耗时，需要新开线程处理 )，然后接着发出 Read/Write，并继续下一次循环阻塞在 GetQueuedCompletionStatus() 这里。

# 分区

# 磁盘的文件名

* Linux 中每个硬件都被当做一个文件。
* 常见磁盘的文件名：
* SCSI/SATA/USB 磁盘：/dev/sd[a-p]
* IDE 磁盘：/dev/hd[a-d]
* 其中文件名后面的序号的确定与磁盘插入的顺序有关，而与磁盘所插入的插槽位置无关。
* Linux系统使用字母和数字的组合来指代硬盘分区，Linux系统使用一种更加灵活的命名方案，该命名方案是基于文件的，文件名的格式为/dev/xxyN，
* /dev/：这是Linux系统下所有设备文件所在的目录名。
* xx：分区名的前两个字母表示分区所在设备的类型，通常是hd（IDE硬盘)或sd（SCSI硬盘)。
* y：这个字母表示分区所在的设备。
* N：最后的数字N代表分区。
* 挂载目录：
* Linux系统处理分区及磁盘存储的方法与Windows截然不同，Linux系统中的每一个分区都是构成支持一组文件和目录所必需的存储区的一部分。它是通过挂载来实现的，挂载是将分区关联到某一目录的过程，挂载分区使起始于这个指定目录（通称为挂载目录)的存储区能够被使用。

# 分区表

* 磁盘分区表主要有两种格式，一种是限制较多的 MBR 分区表，一种是较新且限制较少的 GPT 分区表。
  1. MBR
* MBR 中，第一个扇区最重要，里面有：主要开机记录（Master boot record, MBR)及分区表（partition table)，其中 MBR 占 446 bytes，partition table 占 64 bytes。
* 分区表只有 64 bytes，最多只能存储 4 个分区，这 4 个分区为主分区（Primary)和扩展分区（Extended)。其中扩展分区只有一个，它将其它空间用来记录分区表，可以记录更多的分区，因此通过扩展分区可以分出更多区分，这些分区称为逻辑分区。
* Linux 也把分区当成文件，分区文件的命名方式为：磁盘文件名+编号，例如 /dev/sda1。注意，逻辑分区的编号从 5 开始。
  1. GPT
* 不同的磁盘有不同的扇区大小，例如 512bytes 和最新磁盘的 4k。GPT 为了兼容所有磁盘，在定义扇区上使用逻辑区块地址（Logical Block Address, LBA)。
* GPT 第 1 个区块记录了 MBR，紧接着是 33 个区块记录分区信息，并把最后的 33 个区块用于对分区信息进行备份。
* GPT 没有扩展分区概念，都是主分区，最多可以分 128 个分区。

# 压缩

* tar 主选项+辅选项
* 备份/root/abc目录及其子目录下的全部文件,备份文件名为abc.tar。
* [root@PC-LINUX ~]# touch /root/abc/a /root/abc/b /root/abc/c
* //在/root/abc目录中创建/root/abc/a、/root/abc/b和/root/abc/c文件
* [root@PC-LINUX ~]# tar cvf abc.tar /root/abc
* 查看abc.tar备份文件的内容,并显示在显示器上。
* [root@PC-LINUX ~]# tar tvf abc.tar
* 将文件/root/abc/d添加到abc.tar包里面去。
* [root@PC-LINUX ~]# touch /root/abc/d
* [root@PC-LINUX ~]# tar rvf abc.tar /root/abc/d
* 更新原来tar包abc.tar中的文件/root/abc/d。
* [root@PC-LINUX ~]# tar uvf abc.tar /root/abc/d
* tar调用gzip
* 把/root/abc目录包括其子目录全部做备份文件,并进行压缩,文件名abc.tar.gz。
* [root@PC-LINUX ~]# tar zcvf abc.tar.gz /root/abc
* 查看压缩文件abc.tar.gz的内容,并显示在显示器上。
* [root@PC-LINUX ~]# tar ztvf abc.tar.gz
* 将压缩文件abc.tar.gz解压缩出来。
* [root@PC-LINUX ~]# tar zxvf abc.tar.gz
* tar调用bzip2
* 将目录/root/abc及该目录所有文件压缩成abc.tar.bz2文件。
* [root@PC-LINUX ~]# tar cjf abc.tar.bz2 /root/abc
* 查看压缩文件abc.tar.bz2的内容,并显示在显示器上。
* [root@PC-LINUX ~]# tar tjf abc.tar.bz2
* 将abc.tar.bz2文件解压缩。
* [root@PC-LINUX ~]# tar xjf abc.tar.bz2

# 其他

# 关机

* 1. 数据同步写入磁盘 sync
* 为了加快对磁盘上文件的读写速度，位于内存中的文件数据不会立即同步到磁盘上，因此关机之前需要先进行 sync 同步操作。
  1. shutdown

# /sbin/shutdown [-krhc] [时间] [警告讯息]

* -k ： 不会关机，只是发送警告讯息，通知所有在线的用户
* -r ： 将系统的服务停掉后就重新启动
* -h ： 将系统的服务停掉后就立即关机
* -c ： 取消已经在进行的 shutdown 指令内容
  1. 其它关机指令
* reboot、halt、poweroff。

# 运行等级

* 0：关机模式 1：单用户模式（可用于破解root密码) 2：无网络支持的多用户模式 3：有网络支持的多用户模式（文本模式，工作中最常用的模式) 4：保留，未使用 5：有网络支持的 X-windows 支持多用户模式（桌面) 6：重新引导系统，即重启

# BIOS

* BIOS 是开机的时候计算机执行的第一个程序，这个程序知道可以开机的磁盘，并读取磁盘第一个扇区的 MBR，由 MBR 执行其中的开机管理程序，这个开机管理程序的会加载操作系统的核心文件。
* MBR 中的开机管理程序提供以下功能：选单、载入核心文件以及转交其它开机管理程序。转交这个功能可以用来实现了多重引导，只需要将另一个操作系统的开机管理程序安装其它分区的启动扇区上，在启动 MBR 中的开机管理程序时，就可以选择启动当前的操作系统或者转交给其它开机管理程序从而启动另一个操作系统。

# 指令搜索顺序

* 1. 以绝对或相对路径来执行指令，例如 /bin/ls 或者 ./ls ；
  2. 由别名找到该指令来执行；
  3. 由 Bash 内建的指令来执行；
  4. 按 $PATH 变量指定的搜索路径的顺序找到第一个指令来执行。

# 数据流重定向

* 重定向有5种方式，分别是: 输出重定向、输入重定向、错误重定向、追加重定向以及同时实现输出和错误的重定向。
* 重定向就是使用文件代替标准输入、标准输出和标准错误输出。
* 标准输入 (stdin) ：代码为 0 ，使用 < 或 << ；
* 标准输出 (stdout) ：代码为 1 ，使用 > 或 >> ；
* 标准错误输出(stderr)：代码为 2 ，使用 2> 或 2>> ；
* 其中，有一个箭头的表示以覆盖的方式重定向，而有两个箭头的表示以追加的方式重定向。
* 可以将不需要的标准输出以及标准错误输出重定向到 /dev/null ，相当于扔进垃圾箱。
* 如果需要将标准输出以及标准错误输出同时重定向到一个文件，需要将某个输出转换为另一个输出，例如 2>&1 表示将标准错误输出转换为标准输出。
* $ find /home -name .bashrc > list 2>&1

# 静态链接库和动态链接库的区别

* 静态连接库就是把(lib)文件中用到的函数代码直接链接进目标程序，程序运行的时候不再需要其它的库文件；动态链接就是把调用的函数所在文件模块（DLL)和调用函数在文件中的位置等信息链接进目标程序，程序运行的时候再从DLL中寻找相应函数代码，因此需要相应DLL文件的支持。
* 静态链接库与动态链接库都是共享代码的方式，如果采用静态链接库，则无论你愿不愿意，lib 中的指令都全部被直接包含在最终生成的 EXE 文件中了。但是若使用 DLL，该 DLL 不必被包含在最终 EXE 文件中，EXE 文件执行时可以“动态”地引用和卸载这个与 EXE 独立的 DLL 文件。静态链接库和动态链接库的另外一个区别在于静态链接库中不能再包含其他的动态链接库或者静态库，而在动态链接库中还可以再包含其他的动态或静态链接库。动态库就是在需要调用其中的函数时，根据函数映射表找到该函数然后调入堆栈执行。如果在当前工程中有多处对dll文件中同一个函数的调用，那么执行时，这个函数只会留下一份拷贝。但是如果有多处对lib文件中同一个函数的调用，那么执行时，该函数将在当前程序的执行空间里留下多份拷贝，而且是一处调用就产生一份拷贝。

# 孤儿进程和僵死进程

## 孤儿进程

- 一个父进程退出，而它的一个或多个子进程还在运行，那么那些子进程将成为孤儿进程。孤儿进程将被 init 进程（进程号为 1)所收养，并由 init 进程对它们完成状态收集工作。由于孤儿进程会被 init 进程收养，所以孤儿进程不会对系统造成危害

## 僵尸进程

* 一个子进程的进程描述符在子进程退出时不会释放，只有当父进程通过 wait 或 waitpid 获取了子进程信息后才会释放。如果子进程退出，而父进程并没有调用 wait 或 waitpid，那么子进程的进程描述符仍然保存在系统中，这种进程称之为僵死进程。
* 僵死进程通过 ps 命令显示出来的状态为 Z。
* 系统所能使用的进程号是有限的，如果大量的产生僵死进程，将因为没有可用的进程号而导致系统不能产生新的进程。
* 要消灭系统中大量的僵死进程，只需要将其父进程杀死，此时所有的僵死进程就会变成孤儿进程，从而被 init 所收养，这样 init 就会释放所有的僵死进程所占有的资源，从而结束僵死进程。

# JDBC

* JDBC的桥接设计模式 jdbc的详细链接过程；底层源码；在Java中调用存储过程的方法
* 为什么要使用JDBC
* JDBC可以跨数据库平台
* 系统可以 小规模时使用MySQL 规模变大时使用Oracle
* 如果不需要改动API函数，就需要分层。
* ODBC统一与数据库的接口，ADO是.NET统一与数据库的接口
* JDBC是java与数据库统一的接口
* 但是注意JDBC还是要求将SQL语句插入到代码中，而SQL语句各数据库有所不同，所以不能完全实现移植。如果要实现完全的移植，需要使用Hibernate技术
* Hibernate将不同数据库微小的区别也屏蔽掉了
* EJB也实现了屏蔽数据库间微小的区别
* JDBC对于java的接口是一致，但对于不同数据库JDBC所用的类库是不同的，对于程序猿而言是透明的。
* JDBC编程步骤
* 先需要找JDBC的类库 java.sql
* Driver 驱动，用来提供给JDBC连接到数据库
* java并不知道使用的是哪种数据库，而java有一个管理数据库的管家DriverManager，它来管理使用哪种数据库的连接。
* 连接到某个数据库，需要先向DriverManager注册。然后通过DriverManager连接到数据库。
* 代码示例：
* import java.sql.\*;

public class TestJDBC {

public static void main(String []args){

* Connection conn = null;
* Statement stmt = null;
* ResultSet rs = null;
* try {
* Class.forName("com.mysql.jdbc.Driver");
* conn = DriverManager.getConnection("jdbc:mysql://localhost/mydata?user=root&password=130119");
* stmt = conn.createStatement();
* rs = stmt.executeQuery("select \* from emp");
* while(rs.next()){
* System.out.println(rs.getString("deptno"));
* }
* } catch (SQLException | InstantiationException | IllegalAccessException | ClassNotFoundException e) {
* e.printStackTrace();
* }finally{
* try{
* if(rs != null){
* rs.close();
* rs = null;
* }
* if(stmt != null ){
* stmt.close();
* stmt= null;
* }
* if(conn != null){
* conn.close();
* conn = null;
* }
* }catch(SQLException e){
* e.printStackTrace();
* }
* }
* }
* }
* 总结：JDBC连接流程  
  1.- 注册：驱动实例化 Class forName()  
  2.- 连接：获取连接 Connection DriverManager getConnection()  
  3.- 执行：通过连接执行SQL语句 Statement createStatement() executeQuery()  
  4.- 接收并输出：循环遍历取出数据 ResultSet next() getString()  
  5.- 关闭：close 先打开的后关闭 close()
* 除此之外，还需要抓Exception，并将关闭的代码放到finally里面
* 关闭前先判断是否为null，如果为null那么关闭时会出错
* 在close中也会抛Exception，也要写try catch

# JDBCUtils

* import java.io.IOException;
* import java.util.Properties;
* import java.sql.\*;

public final class JDBCUtils {

private static String driver;

private static String url;

private static String username;

private static String password;

private JDBCUtils() {

* }
* static {
* Properties props = new Properties();
* try {
* props.load(JDBCUtils.class.getClassLoader().getResourceAsStream(
* "dbinfo.properties"));
* driver = props.getProperty("driver");
* url = props.getProperty("url");
* username = props.getProperty("username");
* password = props.getProperty("password");
* } catch (IOException e) {
* throw new ExceptionInInitializerError(e);
* }
* try {
* Class.forName(driver);
* } catch (ClassNotFoundException e) {
* throw new ExceptionInInitializerError(e);
* }
* }

public static Connection getConn() {

* Connection conn = null;
* try {
* conn = DriverManager.getConnection(url, username, password);
* } catch (SQLException e) {
* e.printStackTrace();
* }
* return conn;
* }

public static void free(ResultSet rs, Statement stmt, Connection conn) {

* try {
* if (rs != null) {
* rs.close();
* rs = null;
* }
* } catch (SQLException e) {
* e.printStackTrace();
* } finally {
* try {
* if (stmt != null) {
* stmt.close();
* stmt = null;
* }
* } catch (SQLException e) {
* e.printStackTrace();
* } finally {
* try {
* if (conn != null) {
* conn.close();
* conn = null;
* }
* } catch (SQLException e) {
* e.printStackTrace();
* }
* }
* }
* }
* }
* 实际调用的代码：
* import java.sql.\*;

public class TestTemplate {

public static void main(String[] args) {

* read();
* }

public static void read(){

* Connection c = null;
* Statement stmt = null;
* ResultSet rs = null;
* try{
* c = JDBCUtils.getConn();
* stmt = c.createStatement();
* rs = stmt.executeQuery("select \* from dept");
* while(rs.next()){
* System.out.println(rs.getString("deptno"));
* }
* }catch(SQLException e){
* e.printStackTrace();
* }finally{
* JDBCUtils.free(rs, stmt, c);
* }
* }
* }
* 以下可以忽略
* 工具类可以采用单例模式

类中有一个静态私有的实例，有一个公开的静态的获取该实例的方法，其他方法是public但不是静态的

* 当其他的类要调用该工具类的方法时，先获取该类的实例，再调用其方法
* 还可以采用延迟加载，当第一次使用该类时new出实例；一开始是没有实例的成员变量的
* 以后使用该类就不会再new第二个实例了。
* 构造实例的成本很高时多采用该方法
* 还可以再完善，并发（多线程)控制时将new实例的部分加锁，避免出现两个实例
* 永远保持单个实例
* 这是双重检查
* DML增删改
* 注意sql语句不建议用\*，并且get获取值时不应该写1,2 ；写为字段名可读性更高
* 最好将sql语句中列出所需要的字段，全部取出效率较低
* 这是为了降低维护成本
* executeUpdate 返回值是int类型，是执行成功的影响行数
* 注意关闭执行DML语句的资源也可以使用封装的free方法，因为会判断是否为空，空即不关闭
* 注意与之前步骤不同，不需要ResultSet这个类，因为不需要接收结果集
* 示例模板（使用了JDBCUtils工具类)：
* import java.sql.\*;

public class TestTemplate {

public static void main(String []args){

* add();
* }

private static void add() {

* Connection c = null;
* Statement stmt = null;
* ResultSet rs = null;
* try{
* c = JDBCUtils.getConn();
* stmt = c.createStatement();
* String sql = "insert into dept2 values(14,'lala','china')";
* int result = stmt.executeUpdate(sql);
* System.out.println(result);
* }catch(SQLException e){
* e.printStackTrace();
* }finally{
* JDBCUtils.free(rs, stmt, c);
* }
* }
* }

# JDBC进阶

* SQL注入攻击指的是通过构建特殊的输入作为参数传入Web应用程序，而这些输入大都是SQL语法里的一些组合，通过执行SQL语句进而执行攻击者所要的操作，其主要原因是程序没有细致地过滤用户输入的数据，致使非法数据侵入系统。
* select \* from emp where ename = '' or 1 = 1;
* PreparedStatement类
* 是Statement接口的子接口
* 表示预编译的 SQL 语句的对象。
* SQL 语句（增改删DML)被预编译并存储在 PreparedStatement 对象中。然后可以使用此对象多次高效地执行该SQL语句。
* 与Statement不同的是通过preparedStatement方法来获得PreparedStatement对象。
* 参数：
* sql - 可能包含一个或多个 '?' IN 参数占位符的 SQL 语句
* 返回：
* 包含预编译 SQL 语句的新的默认 PreparedStatement 对象
* 不同于createStatement不需要参数，这个方法需要一个参数，即预编译的SQL语句，其插入的数据用？占位符表示
* PreparedStatement pstmt = conn.prepareStatement(“insert into dept values(?,?,?)”);
* 之后再使用pstmt来为这三个？赋值
* 使用的方法有：
* 这些方法的第一个参数都是表示第几个占位符
* 1表示第一个？
* 2表示第二个？
* pstmt.setInt(1,deptno);
* pstmt.setString(2,dname);
* pstmt.setString(3,loc);
* 另一个区别是executeUpdate方法不再需要参数传入。
* PreparedStatement类的好处是不必去考虑怎么才能拼凑出格式正确的SQL语句，而是调用方法就可以设置相应的值，十分方便；也易于修改占位符值。尽量使用；可以解决SQL注入问题（过滤掉特殊字符)（最大的优点)；同时效率同Statement相比较高（避免频繁SQL语句，是预编译)
* 可以执行查询和DML操作。
* 示例：
* import java.sql.\*;

public class TestTemplate {

public static void main(String []args){

- if(args.length != 3){

* System.out.println("Input Error!");
  + System.exit(-1);
* }
* int deptno =0 ;
* try{
* deptno = Integer.parseInt(args[0]);
* }catch(NumberFormatException e){
* e.printStackTrace();
* }
* String dname = args[1];
* String loc = args[2];
* Connection c = null;
* PreparedStatement pstmt = null;
* ResultSet rs = null;
* try{
* c = JDBCUtils.getConn();
* pstmt = c.prepareStatement("insert into dept2 values(?,?,?)");
* pstmt.setInt(1, deptno);
* pstmt.setString(2,dname);
* pstmt.setString(3,loc);
* pstmt.executeUpdate();
* }catch(SQLException e){
* e.printStackTrace();
* }finally{
* JDBCUtils.free(rs, pstmt, c);//这里仍可以执行，因为PreparedStatement是Statement的子类，而非超类
* }
* }
* }
* 在java中SQL语句测定时间的一种方法，在执行之前和执行之后的时间打印出来
* JDBC中最耗时间的是建立连接；使用的是Socket连接，三次握手机制
* 发送用户名密码
* 比发送执行SQL语句的时间要长得多
* 注意虽然PreparedStatement是Statement是子类，但是不能调用父类的executeQuery(sql);
* 会出错
* 因为该方法会直接将参数原始的sql语句传到数据库，而不管之前的填充sql语句的步骤
* 示例：
* import java.sql.\*;

public class TestTemplate {

public static void main(String []args){

* read("SMITH");
* }

private static void read(String name) {

* Connection c = null;
* PreparedStatement pstmt = null;
* ResultSet rs = null;
* try{
* String sql = "select \* from emp where ename = ?";
* c = JDBCUtils.getConn();
* pstmt = c.prepareStatement(sql);
* pstmt.setString(1,name);
* rs = pstmt.executeQuery();//如果这里加上sql，那么会报错
* while(rs.next()){
  + System.out.println(rs.getString(1));
* }
* }catch(SQLException e){
* e.printStackTrace();
* }finally{
* JDBCUtils.free(rs, pstmt, c);
* }
* }
* }
* 如何选择？ 一般带有参数的sql都使用PreparedStatement
* 如果没有条件或条件固定的可以使用Statement。 建议全部使用PreparedStatement
* CallableStatement(存储过程)
* 是PreparedStatement的子接口，是Statement的孙子接口。
* 用于执行 SQL 存储过程的接口。JDBC API 提供了一个存储过程 SQL 转义语法，该语法允许对所有 RDBMS 使用标准方式调用存储过程。此转义语法有一个包含结果参数的形式和一个不包含结果参数的形式。如果使用结果参数，则必须将其注册为 OUT 参数。其他参数可用于输入、输出或同时用于二者。参数是根据编号按顺序引用的，第一个参数的编号是 1。
* 继承自PreparedStatement
* Connection
* 可以创建一个CallableStatement对象
* 参数是sql语句
* sql语句是这样写的
* CollableStatement cs = null;
* cs = conn.prepareCall(“{call pro1(?,?)}”); //参数以？表示，之后赋值
* cs.setString(1,”SMITH”);
* cs.setIntFloat(2,456.7f);//f是表示float类型
* 第一个参数是1,2,3等 表示第一个、第二个、第三个？
* 第二个参数是所要设为的值
* 设置完后调用execute方法
* 注意如果在sql 中没有commit提交事务，那么java中无法访问数据库，处于阻塞状态
* 代码：

public static void main(String []args){

* Connection c = null;
* CallableStatement cs = null;
* try{
* c =JDBCUtils.getConn();
* cs = c.prepareCall("{call pro3(?,?)}");
* cs.setString(1, "SMITH");
* cs.setFloat(2, 7800f); //这个也可以是setString
* //注意oracle提供一种自动转换机制，如果该字段是数字类型，那么会自动将字符串转为数字
* cs.execute();
* 可以在SQL工具类中封装一个可以调用存储过程的方法
* 工具类中的成员变量均为静态变量，方法都是静态方法
* SQLHelper:

public static void callProcedure(String sql,String []parameters){

* Connection c= null;
* CallableStatement cs= null;
* ResultSet rs = null;
* //所有含有参数的sql语句都使用PreparedStatement，传入时还包括一个字符串数据
* 然后通过一个循环将参数使用setString将sql语句补充完毕
* 然后调用
* try{
* c =JDBCUtils.getConn();
* cs = c.prepareCall(sql);
* if(parameters != null && "".equals(parameters)){
* for(int i = 0; i< parameters.length ;i++){
* cs.setString(i+1,parameters[i]);
* }
* }
* cs.execute();
* }catch(SQLException e){
* e.printStackTrace();
* }finally{
* JDBCUtils.free(rs,cs,c);
* }
* }
* 调用此方法的代码：
* 带返回值参数的存储过程
* 分页查询
* 存储过程代码：
* create or replace procedure paged\_query
* (v*in*table in varchar2,v*in*record*per*page in number, v*in*now*page in number,v*in\_col varchar2,
* v*out*records out number,v*out*pages out number, v*out*result out p1.my\_cursor) is
* v\_start number;
* v\_end number;
* v\_sql varchar2(2000);
* v*sql*get\_record varchar2(300);
* begin
  + v*start := 1+v*in*record*per*page\*( v*in*now*page-1) ;
* v*end := 1+ v*in*record*per*page \* v*in*now*page;
* v*sql*get*record := 'select count(\*) from '||v*in\_table;
* execute immediate v*sql*get*record into v*out\_records;
* if mod(v*out*records,v*in*record*per*page) = 0 then
* v*out*pages := v*out*records / v*in*record*per*page;
* else
* v*out*pages := v*out*records / v*in*record*per*page + 1;
* end if;
* v\_sql := 'select t2.\* from (select t1.\* ,rownum rn from
* (select \* from '||v*in*table||' order by '||v*in*col||') t1
* where rownum <= '||v\_end||'
* ) t2
* where rn >= '||v\_start;
* open v*out*result for v\_sql;
* end;
* /
* 使用CallableStatement来接收Connection的prepareCall方法，得到statement
* 传入的是含有等同于参数个数的sql语句
* String sql = “{call pro1(?,?)}”;
* 然后set方法设置每个？所对应的值；注意数值类型也可以用setString
* oracle会自动转为相应的数值类型
* 与不含输出参数的过程的第一个不同是还需要调用这个方法registerOutParameter
* 注册输出参数的类型
* 注意不同数据库，参数类型也是不同的
* 第一个参数是给第n个？赋值；第二个参数是对应的返回值的类型
* 对oracle而言是oracle.jdbc.OracleTypes.某个类型
* 最后execute
* 第二个不同是还需要再取出返回值
* get…数据类型(n)
* 比如getString(第几个？的返回值);
* 如果返回的是结果集（游标)，那么需要使用结果集来接收游标变量
* oracle.jdbc.OracleTypes.CURSOR
* 取出返回值的集合
* 方法是getObject 将游标视为一个对象
* 接收的是ResltSet结果集（需要将Object类型强制转为ResultSet)
* ResultSet实际上就是游标
* 之后就可以使用next和get…来获取值了
* java调用代码:
* try {
* c = JDBCUtils.getConn();
* cs = c.prepareCall("{call paged\_query(?,?,?,?,?,?,?)}");
* int page = 2;
* cs.setString(1, "emp");
* cs.setString(2,"5");
* cs.setString(3,""+page);
* cs.setString(4, "sal");
* cs.registerOutParameter(5, oracle.jdbc.OracleTypes.NUMBER);
* //每个返回的变量都需要注册
* cs.registerOutParameter(6, oracle.jdbc.OracleTypes.NUMBER);
* cs.registerOutParameter(7, oracle.jdbc.OracleTypes.CURSOR);
* cs.execute();
  + String recordCount = cs.getString(5);
  + String pageCount = cs.getString(6);
* System.out.println("共有"+recordCount+"条记录");
* //执行完后需要逐个取出返回值
* System.out.println("共有"+pageCount+"页");
* System.out.println("第"+page+"页:");
  + rs = (ResultSet)cs.getObject(7);
* while(rs.next()){
  + System.out.println(rs.getString(1)+","+rs.getString(2));
* }catch ……略
* getGeneratedKeys产生主键
* 用于拿出插入的记录的主键
* getGeneratedKeys(获取主键)
* API介绍：
* Connection:
* prepareStatement
* PreparedStatement prepareStatement(String sql,
* int autoGeneratedKeys)
* throws SQLException
* 创建一个默认 PreparedStatement 对象，该对象能获取自动生成的键。给定常量告知驱动程序是否可以获取自动生成的键。如果 SQL 语句不是一条 INSERT 语句，或者 SQL 语句能够返回自动生成的键（这类语句的列表是特定于供应商的)，则忽略此参数。
* 该SQL语句是插入语句，可以立刻获得插入记录的主键
* 第二个参数是Statement中的常量
* PreparedStatement:
* ResultSet getGeneratedKeys() throws SQLException
* 获取由于执行此 Statement 对象而创建的所有自动生成的键。如果此 Statement 对象没有生成任何键，则返回空的 ResultSet 对象。
* 注：如果未指定表示自动生成键的列，则 JDBC 驱动程序实现将确定最能表示自动生成键的列。
* 返回：包含通过执行此 Statement 对象自动生成的键的 ResultSet 对象
* 执行的是insert语句，返回的是ResultSet
* ResultSet 可能是多个主键（组合主键)，所以需要ResultSet
* 代码：

public static void add() {

* Connection c = null;
* PreparedStatement ps = null;
* ResultSet rs = null;
* String sql = "insert into UserTable(user*name,user*password) values(?,?)";
* try {
* c = JDBCUtils.getConn();
* ps = c.prepareStatement(sql, Statement.RETURN*GENERATED*KEYS);
* ps.setString(1, "wulitaotao");
* ps.setString(2, "666");
* ps.executeUpdate();
* rs = ps.getGeneratedKeys();
* if(rs.next()){
  + System.out.println(“刚插入记录的id为”+rs.getInt(1));
* }
* } catch (SQLException e) {
* e.printStackTrace();
* } finally{
* JDBCUtils.free(rs,ps,c);
* }
* }
* 实际作用是如果数据库的表是自动主键，那么插入之后是不知道id的。只能从数据库中根据其他的唯一键来找到这条记录再取出主键
* 而这种方式可以在插入之后立刻得到主键，然后取出赋给对象，ok
* 优化UserDAOJDBCImpl中的addUser方法
* try {
* c = JDBCUtils.getConn();
* String sql = "insert into UserTable(user*name,user*password,user\_birthday)
* values(?,?,?)";
* pstmt = c.prepareStatement(sql,Statement.RETURN*GENERATED*KEYS);
* pstmt.setString(1, user.getUsername());
* pstmt.setString(2, user.getPassword());
* pstmt.setDate(3, new java.sql.Date(user.getBirthday().getTime()));
* pstmt.executeUpdate();
* rs = pstmt.getGeneratedKeys();
* if(rs.next()){
  + user.setId(rs.getInt(1));
* }
* } catch (SQLException e) {
* throw new DAOException(e.getMessage(),e);
* } finally {
* JDBCUtils.free(rs, pstmt, c);
* }
* 批处理Batch
* 可以一次执行多条SQL语句，调用Statement接口的addBatch方法
* 不必建立多次的连接（建立连接成本很高)，只建立一次连接就可以执行多条语句
* 将给定的 SQL 命令添加到此 Statement 对象的当前命令列表中。通过调用方法 executeBatch 可以批量执行此列表中的命令。
* 参数：
* sql - 通常此参数为 SQL INSERT 或 UPDATE 语句
* 执行语句时调用
* 将一批命令提交给数据库来执行
* 如果全部命令执行成功，则返回更新计数组成的数组。返回数组的 int 元素的排序对应于批中的命令，批中的命令根据被添加到批中的顺序排序。
* 返回：
* 包含批中每个命令的一个元素的更新计数所组成的数组。数组的元素根据将命令添加到批中的顺序排序。
* 批处理适用于Statement，当然适用于其子类PreparedStatement
* 示例1 Statement：
* import java.sql.\*;

public class JDBC {

public static void main(String []args){

* Connection c = null;
* Statement stmt = null;
* ResultSet rs = null;
* try{
* c = JDBCUtils.getConn();
* stmt = c.createStatement();
* stmt.addBatch("insert into dept2 values(88,'aaa','aaa')");
* stmt.addBatch("insert into dept2 values(89,'aaa','aaa')");
* stmt.addBatch("insert into dept2 values(90,'aaa','aaa')");
* stmt.executeBatch();
* }catch(SQLException e){
* e.printStackTrace();
* }finally{
* JDBCUtils.free(rs,stmt,c);
* }
* }
* }
* 示例2 PreparedStatement：
* import java.sql.\*;

public class JDBC {

public static void main(String []args){

* Connection c = null;
* PreparedStatement pstmt = null;
* ResultSet rs = null;
* try{
* c = JDBCUtils.getConn();
* pstmt = c.prepareStatement("insert into
* UserTable(user*name,user*password,user\_birthday) values(?,?,?)");
* for(int i = 0 ; i<100;i++){//一次性插入100条记录
  + pstmt.setString(1, "user"+i+1);
* pstmt.setString(2, "111");
* pstmt.setDate(3, new Date(System.currentTimeMillis()));
* pstmt.addBatch();
* //设置完一条记录添加一次，然后重新设置下一条记录 字段的值
* }
* int []id = pstmt.executeBatch();//返回值全部是1
* for(int i:id){
* System.out.println(i);
* }
* }catch(SQLException e){
* e.printStackTrace();
* }finally{
* JDBCUtils.free(rs,pstmt,c);
* }
* }
* }
* addBatch(sql) 也是存在的，可以将sql语句传入
* 如果记录太多可能会内存溢出
* 事务处理
* 在java程序中将多个DML语句视为一个事务，统一提交和回滚
* 注意java中事务是自动提交的，也就是执行一条DML语句就commit一下
* 需要我们去设置不自动提交事务，由自己来设定事务
* Connection有一个方法setAutoCommit
* 参数为true or false
* 当想提交时，执行Connection的commit方法
* 在执行commit方法之前的DML语句都还未提交，当执行commit方法时将之前的DML语句视为一个事务，整体地执行
* 当事务执行过程中出现异常，可以在catch到exception后回滚
* 可以Connection的rollback方法，有重载的方法，可以无参数，对应sql中的rollback；
* rollback方法可以有参数，是保存点，回滚到这个保存点

public static void testSavepoint() throws Exception{

* Connection c = null;
* Statement stmt = null;
* ResultSet rs = null;
* String sql1 = "update emp2 set sal = sal - 800 where empno = 7369";
* String sql2 = "update emp2 set sal = sal - 800 where empno = 7369";
* try {
* c = JDBCUtils.getConn();
* c.setAutoCommit(false);
* stmt = c.createStatement();
  + stmt.executeUpdate(sql1);
* int i = 8/0; //故意制造出一些错误
  + stmt.executeUpdate(sql2);
* c.commit();
* c.setAutoCommit(true);//恢复现场
* }catch (Exception e) { //捕捉到任何异常，立刻返回到初始状态
* //不能只写SQLException，应该是所有异常，否则ArithmeticException就捕捉不到了，捕捉不到也就无法执行catch块中的代码了
* if(c != null) //如果没有建立连接那么没有必要去rollback
* c.rollback();
* c.setAutoCommit(true);//无论如何都应该恢复现场
* throw e;//交给上一级去处理
* } finally{
* JDBCUtils.free(rs,stmt,c);
* }
* }
* }
* 设置保存点:
* 假如在执行了第一条sql之后设置保存点，如果在执行第二条sql时出错，回滚到第一条sql之后
* Connection:

public static void testSavepoint() throws SQLException {

* Connection c = null;
* Statement stmt = null;
* ResultSet rs = null;
* Savepoint sp = null;
* String sql1 = "update emp2 set sal = sal - 800 where empno = 7369";
* String sql2 = "update emp2 set sal = sal - 800 where empno = 7369";
* String sql3 = "select sal from emp2 where empno = 7369";
* try {
* c = JDBCUtils.getConn();
* c.setAutoCommit(false);
* stmt = c.createStatement();
  + stmt.executeUpdate(sql1);
* sp = c.setSavepoint();
  + rs = stmt.executeQuery(sql3);
* int sal = 0;
* if(rs.next())
* sal = rs.getInt("sal");
* if(sal < 1000)
* throw new RuntimeException("工资过低!");
* //自己new一个异常，以便于与SQLException区分开来
  + stmt.executeUpdate(sql2);
* c.commit();
* c.setAutoCommit(true);//恢复现场
* }catch (RuntimeException e) {
* if(c != null && sp != null){
* c.rollback(sp);
* //如果工资减去800之后小于1000，那么不再减少，保留第一次的结果
* }
* c.setAutoCommit(true);
* throw e;
* } catch (SQLException e) {
* if(c != null){
* c.rollback();
* c.setAutoCommit(true);
* }
* throw e;
* } finally{
* JDBCUtils.free(rs,stmt,c);
* }
* }
* JTA类似指挥官，第一阶段给所有数据库发送一个准备提交的请求，如果有数据库提出要回滚，那么JTA会通知其他数据库，一起回滚
* 如果没有数据库没有提出要回滚，那么第二阶段JTA发送提交的命令

# JDBC桥接模式源码分析（以MySQL为例)

# Class.forName

* Class.forName("com.mysql.jdbc.Driver");
* Driver#static{}
* 注册MySQL的Driver

public class Driver extends NonRegisteringDriver implements java.sql.Driver {  
 // ~ Static fields/initializers  
 // ---------------------------------------------  
  
 //  
 // Register ourselves with the DriverManager  
 //  
 static {  
 try {  
 java.sql.DriverManager.registerDriver(new Driver());  
 } catch (SQLException E) {  
 throw new RuntimeException("Can't register driver!");  
 }  
 }

* }
* DriverManager#registerDriver

public static synchronized void registerDriver(java.sql.Driver driver)  
 throws SQLException {  
  
 registerDriver(driver, null);  
}

public static synchronized void registerDriver(java.sql.Driver driver,  
 DriverAction da)  
 throws SQLException {  
  
 /\* Register the driver if it has not already been added to our list \*/  
 if(driver != null) {  
 registeredDrivers.addIfAbsent(new DriverInfo(driver, da));  
 } else {  
 // This is for compatibility with the original DriverManager  
 throw new NullPointerException();  
 }  
  
 println("registerDriver: " + driver);  
  
}

* DriverManager#getConnection

public static Connection getConnection(String url)  
 throws SQLException {  
  
 java.util.Properties info = new java.util.Properties();  
 return (getConnection(url, info, Reflection.getCallerClass()));  
}

private static Connection getConnection(  
 String url, java.util.Properties info, Class<?> caller) throws SQLException {  
 /\*  
 \* When callerCl is null, we should check the application's  
 \* (which is invoking this class indirectly)  
 \* classloader, so that the JDBC driver class outside rt.jar  
 \* can be loaded from here.  
 \*/  
 ClassLoader callerCL = caller != null ? caller.getClassLoader() : null;  
 synchronized(DriverManager.class) {  
 // synchronize loading of the correct classloader.  
 if (callerCL == null) {  
 callerCL = Thread.currentThread().getContextClassLoader();  
 }  
 }  
  
 if(url == null) {  
 throw new SQLException("The url cannot be null", "08001");  
 }  
  
 println("DriverManager.getConnection(\"" + url + "\")");  
  
 // Walk through the loaded registeredDrivers attempting to make a connection.  
 // Remember the first exception that gets raised so we can reraise it.  
 SQLException reason = null;  
  
 for(DriverInfo aDriver : registeredDrivers) {  
 // If the caller does not have permission to load the driver then  
 // skip it.  
 if(isDriverAllowed(aDriver.driver, callerCL)) {  
 try {  
 println(" trying " + aDriver.driver.getClass().getName());  
 Connection con = aDriver.driver.connect(url, info);  
 if (con != null) {  
 // Success!  
 println("getConnection returning " + aDriver.driver.getClass().getName());  
 return (con);  
 }  
 } catch (SQLException ex) {  
 if (reason == null) {  
 reason = ex;  
 }  
 }  
  
 } else {  
 println(" skipping: " + aDriver.getClass().getName());  
 }  
  
 }  
  
 // if we got here nobody could connect.  
 if (reason != null) {  
 println("getConnection failed: " + reason);  
 throw reason;  
 }  
  
 println("getConnection: no suitable driver found for "+ url);  
 throw new SQLException("No suitable driver found for "+ url, "08001");  
}

* Driver#connect

public java.sql.Connection connect(String url, Properties info)  
 throws SQLException {  
 if (url != null) {  
 if (StringUtils.startsWithIgnoreCase(url, LOADBALANCE\_URL\_PREFIX)) {  
 return connectLoadBalanced(url, info);  
 } else if (StringUtils.startsWithIgnoreCase(url,  
 REPLICATION\_URL\_PREFIX)) {  
 return connectReplicationConnection(url, info);  
 }  
 }  
  
 Properties props = null;  
  
 if ((props = parseURL(url, info)) == null) {  
 return null;  
 }  
  
 if (!"1".equals(props.getProperty(NUM\_HOSTS\_PROPERTY\_KEY))) {  
 return connectFailover(url, info);  
 }  
   
 try {  
 Connection newConn = com.mysql.jdbc.ConnectionImpl.getInstance(  
 host(props), port(props), props, database(props), url);  
   
 return newConn;  
 } catch (SQLException sqlEx) {  
 // Don't wrap SQLExceptions, throw  
 // them un-changed.  
 throw sqlEx;  
 } catch (Exception ex) {  
 SQLException sqlEx = SQLError.createSQLException(Messages  
 .getString("NonRegisteringDriver.17") //$NON-NLS-1$  
 + ex.toString()  
 + Messages.getString("NonRegisteringDriver.18"), //$NON-NLS-1$  
 SQLError.SQL\_STATE\_UNABLE\_TO\_CONNECT\_TO\_DATASOURCE, null);  
   
 sqlEx.initCause(ex);  
   
 throw sqlEx;  
 }  
}

# 总结

* 有了抽象部分——JDBC的API，有了具体实现部分——驱动程序，那么它们如何连接起来呢？就是如何桥接呢？
* 就是前面提到的DriverManager来把它们桥接起来，从某个侧面来看，DriverManager在这里起到了类似于简单工厂的功能，基于JDBC的应用程序需要使用JDBC的API，如何得到呢？就通过DriverManager来获取相应的对象。
* JDBC的这种架构，把抽象和具体分离开来，从而使得抽象和具体部分都可以独立扩展。对于应用程序而言，只要选用不同的驱动，就可以让程序操作不同的数据库，而无需更改应用程序，从而实现在不同的数据库上移植；对于驱动程序而言，为数据库实现不同的驱动程序，并不会影响应用程序。而且，JDBC的这种架构，还合理的划分了应用程序开发人员和驱动程序开发人员的边界。
* Class.forName是用MySql还是Oracle，这个Driver一定会实现接口java.sql.Driver，然后通过DriverManager.registerDriver(new Driver());使DriverManager类持有一个Driver，是否可以把DriverManager当成桥，当成桥连接中的抽象类？然后持有一个接口Driver，至于是MySql还是Oracle，不关心，坐等传参。因为DriverManager持有的是一个Driver接口，你传过来什么，我就得到什么的实例化，然后我再通过getConnection用你的实例，去调用你自己的方法connect，去获得Connection的一个实例。

# 安全

# XSS攻击

# 原理

* 跨站脚本攻击（Cross-Site Scripting, XSS)：主要是指在用户浏览器内运行了JavaScript 脚本。比如富文本编辑器，如果不过滤用户输入的数据直接显示用户输入的HTML内容的话，就会有可能运行恶意的 JavaScript 脚本，导致页面结构错乱，Cookies 信息被窃取等问题。
* XSS 的原理是恶意攻击者往 Web 页面里插入恶意可执行网页脚本代码，当用户浏览该页之时，嵌入其中 Web 里面的脚本代码会被执行，从而可以达到攻击者盗取用户信息或其他侵犯用户安全隐私的目的。
* 常见的XSS攻击类型有两种，一种是反射型，一种是持久型。

## 反射型

* 攻击者诱使用户点击一个嵌入恶意脚本的链接，达到工具的目的。
* 比如新浪微博中，攻击者发布的微博中含有一个恶意脚本的URL（URL中包含脚本的链接)，用户点击该URL，脚本会自动关注攻击者的新浪微博ID，发布含有恶意脚本URL的微博，攻击就被扩散了。
* 现实中，攻击者可以采用XSS攻击，偷取用户Cookie、密码等重要数据，进而伪造交易、盗窃用户财产、窃取情报。

## 持久型

* 黑客提交含有恶意脚本的请求，保存在被攻击的Web站点的数据库中，用户浏览网页时，恶意脚本被包含在正常页面中，达到攻击的目的。此种攻击经常使用在论坛、博客等Web应用中。

# 预防

* Web 页面渲染的所有内容或者渲染的数据都必须来自于服务端。
* 后端在入库前应该选择不相信任何前端数据，将所有的字段统一进行转义处理。
* 后端在输出给前端数据统一进行转义处理。
* 前端在渲染页面 DOM 的时候应该选择不相信任何后端数据，任何字段都需要做转义处理。

## 消毒

* XSS攻击者一般都是在请求中嵌入恶意脚本达到攻击的目的，这些脚本是一般在用户输入中不常用的，如果进行过滤和消毒处理，即对某些HTML危险字符转义，如”>”转义为”>”，就可以防止大部分的攻击。为了避免对不必要的内容错误转义，如”3<5”中的”<”需要进行文本匹配后再转义，如”<img src=”这样上下文中的”<”才转义。

## HttpOnly

* 浏览器禁止页面JavaScript访问带有HttpOnly属性的Cookie。

# SQL注入

# 原理

* 针对 Web 应用使用的数据库，通过运行非法的SQL而产生的攻击。

# 预防

* 所有的查询语句建议使用数据库提供的参数化查询接口，使用SQL预编译和参数绑定。
* 在应用发布之前建议使用专业的 SQL 注入检测工具进行检测。

# CSRF攻击

# 原理

* CSRF（Cross-site request forgery)跨站请求伪造，利用跨站请求，在用户不知情的情况下，以用户的身份伪造请求，其核心是利用了浏览器Cookie或者Session，盗取用户身份。
* 下面是CSRF的常见特性：
* 依靠用户标识危害网站
* 利用网站对用户标识的信任，欺骗用户的浏览器发送HTTP请求给目标站点
* 攻击者可以盗用你的登陆信息，以你的身份模拟发送各种请求。攻击者只要借助少许的社会工程学的诡计，例如通过 QQ 等聊天软件发送的链接(有些还伪装成短域名，用户无法分辨)，攻击者就能迫使 Web 应用的用户去执行攻击者预设的操作。例如，当用户登录网络银行去查看其存款余额，在他没有退出时，就点击了一个 QQ 好友发来的链接，那么该用户银行帐户中的资金就有可能被转移到攻击者指定的帐户中。
* 所以遇到 CSRF 攻击时，将对终端用户的数据和操作指令构成严重的威胁。当受攻击的终端用户具有管理员帐户的时候，CSRF 攻击将危及整个 Web 应用程序。

# 预防

* 防御手段主要是识别请求者身份。
* 1、重要数据交互采用POST进行接收，当然是用POST也不是万能的，伪造一个form表单即可破解
* 2、使用验证码，只要是涉及到数据交互就先进行验证码验证，这个方法可以完全解决CSRF。但是出于用户体验考虑，网站不能给所有的操作都加上验证码。因此验证码只能作为一种辅助手段，不能作为主要解决方案。
* 3、验证HTTP Referer字段，该字段记录了此次HTTP请求的来源地址，最常见的应用是图片防盗链。PHP中可以采用APache URL重写规则进行防御，可参考：http://www.cnblogs.com/phpstudy2015-6/p/6715892.html（但是这个也是可以绕过的)
* 4、为每个表单添加令牌token并验证（推荐)
* （可以使用cookie或者session进行构造。当然这个token仅仅只是针对CSRF攻击，在这前提需要解决好XSS攻击，否则这里也将会是白忙一场【XSS可以偷取客户端的cookie】)
* 可以为每一个表单生成一个随机数秘钥，并在服务器端建立一个拦截器来验证这个token，如果请求中没有token或者token内容不正确，则认为可能是CSRF攻击而拒绝该请求。
  1. 用户访问某个表单页面。
  2. 服务端生成一个Token，放在用户的Session中，或者浏览器的Cookie中。【这里已经不考虑XSS攻击】
  3. 在页面表单附带上Token参数。
  4. 用户提交请求后， 服务端验证表单中的Token是否与用户Session（或Cookies)中的Token一致，一致为合法请求，不是则非法请求。

# DDoS 攻击

# 原理

* DDoS 又叫分布式拒绝服务，全称 Distributed Denial of Service，其原理就是利用大量的请求造成资源过载，导致服务不可用。
* TCP的半连接

# 预防

- 网络架构上做好优化，采用负载均衡分流。  
- 确保服务器的系统文件是最新的版本，并及时更新系统补丁。  
- 添加抗 DDos 设备，进行流量清洗。  
- 限制同时打开的 SYN 半连接数目，缩短 SYN 半连接的 Timeout 时间。  
- 限制单 IP 请求频率。  
- 防火墙等防护设置禁止 ICMP 包等。  
- 严格限制对外开放的服务器的向外访问。  
- 运行端口映射程序或端口扫描程序，要认真检查特权端口和非特权端口。  
- 关闭不必要的服务。  
- 认真检查网络设备和主机/服务器系统的日志。只要日志出现漏洞或是时间变更,那这台机器就可能遭到了攻击。  
- 限制在防火墙外与网络文件共享。这样会给黑客截取系统文件的机会，主机的信息暴露给黑客，无疑是给了对方入侵的机会。

# 加密算法

* 什么是对称加密，什么是非对称加密，知道的加密算法有哪些
* BCrypt算法
* 对称加密在加密和解密的过程中，使用相同的密钥；而非对称加密在加密过程中使用公钥进行加密，使用私钥进行解密。

# 对称加密

* 所谓常规密钥密码体制，即加密密钥与解密密钥是相同的密码体制。这种加密系统又称为对称密钥系统。
* 对称加密算法有：DES、AES等。
* DES 的保密性仅取决于对密钥的保密，而算法是公开的。尽管人们在破译 DES 方面取得了许多进展，但至今仍未能找到比穷举搜索密钥更有效的方法。
* DES 是世界上第一个公认的实用密码算法标准，它曾对密码学的发展做出了重大贡献。
* 目前较为严重的问题是 DES 的密钥的长度。
* 现在已经设计出来搜索 DES 密钥的专用芯片。
* 对称加密的加密和解密需要使用相同的密钥，所以需要解决密钥配送问题。

# 非对称加密

* 公钥密码体制使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。
* 公钥密码体制的产生主要是因为两个方面的原因，一是由于常规密钥密码体制的密钥分配问题，另一是由于对数字签名的需求。
* 现有最著名的公钥密码体制是RSA 体制，它基于数论中大数分解问题的体制，由美国三位科学家 Rivest, Shamir 和 Adleman 于 1976 年提出并在 1978 年正式发表。
* 可以用公钥加密，私钥解密；也可以用私钥加密、公钥解密。
* 若密钥能够实现安全交换，那么有可能会考虑仅使用公开密钥加密来通信。但是公开密钥加密与共享密钥加密相比，其处理速度要慢。
* 任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量
* 在这方面，公钥密码体制并不比传统加密体制更加优越
* 由于目前公钥加密算法的开销较大，在可见的将来还不会放弃传统的加密方法
* 公钥需要密钥分配协议，具体的分配过程并不比采用传统加密方法时更简单

# 消息摘要/单向散列

* 单向散列函数也称为消息摘要函数（message digest function)，哈希函数，适用于检查消息完整性的加密技术。
* 单向散列函数有一个输入和一个输出，其中输入称为信息，输出称为散列值。单向散列函数可以根据消息的内容计算出散列值，篡改后的信息的散列值计算结果会不一样，所以散列值可以被用来检查消息的完整性 。
* 常见消息摘要技术：MD5、SHA-1、SHA-256
* CRC、MD5、SHA1都是通过对数据进行计算，来生成一个校验值，该校验值用来校验数据的完整性。
* 不同点：
  1. 算法不同。CRC采用多项式除法，MD5和SHA1使用的是替换、轮转等方法；
  2. 校验值的长度不同。CRC校验位的长度跟其多项式有关系，一般为16位或32位；MD5是16个字节（128位)；SHA1是20个字节（160位)；
  3. 校验值的称呼不同。CRC一般叫做CRC值；MD5和SHA1一般叫做哈希值（Hash)或散列值；
  4. 安全性不同。这里的安全性是指检错的能力，即数据的错误能通过校验位检测出来。CRC的安全性跟多项式有很大关系，相对于MD5和SHA1要弱很多；MD5的安全性很高，不过大概在04年的时候被山东大学的王小云破解了；SHA1的安全性最高（现在SHA-256安全性比较高)。
  5. 效率不同，CRC的计算效率很高；MD5和SHA1比较慢。
  6. 用途不同。CRC一般用作通信数据的校验；MD5和SHA1用于安全（Security)领域，比如文件校验、数字签名等。

# 密码

* 利用单向散列加密的特性，可以进行密码加密保存，即用户注册时输入的密码不直接保存到数据库，而是对密码进行单向散列加密，将密文存入数据库，用户登录时，进行密码验证，同样计算得到输入密码的密文，并和数据库中的密文比较，如果一致，则密码验证成功。
* 这样保存在数据库中的是用户输入的密码的密文，而且不可逆地计算得到密码的明文，因此即使数据库被拖库（指网站遭到入侵后，黑客窃取其数据库)，也不会泄露用户的密码信息。
* 虽然不能通过算法将单向散列密文反算得到明文，但是由于人们设置密码具有一定的模式吗，因此通过彩虹表（建立一个 源数据与加密数据之间对应的hash表。这样在获得加密数据后通过比较，查询或者一定的运算，可以快速定位源数据)等手段可以进行猜测式破解。
* 为了加强单向散列计算的安全性，还会给散列算法加点盐，salt相当于加密的密钥，增加破解的难度。盐一般都是跟hash一起保存在数据库里，或者作为hash字符串的一部分。salt是由系统随机生成的，并且只有系统知道。这样，即便两个用户使用了同一个密码，由于系统为它们生成的salt值不同，他们的散列值也是不同的。

# 算法介绍

* sha比md5更安全一些，sha比md5哈希碰撞的概率更小一些。
* 到目前为止，我们已经了解如何为密码生成安全的 Hash 值以及通过利用 salt 来加强它的安全性。但今天的问题是，硬件的速度已经远远超过任何使用字典或彩虹表进行的暴力攻击，并且任何密码都能被破解，只是使用时间多少的问题。
* 为了解决这个问题，主要想法是尽可能降低暴力攻击速度来保证最小化的损失。我们下一个算法同样是基于这个概念。目标是使 Hash 函数足够慢以妨碍攻击，并对用户来说仍然非常快且不会感到有明显的延时。
* 要达到这个目的通常是使用某些 CPU 密集型算法来实现，比如 PBKDF2, Bcrypt 或 Scrypt 。这些算法采用 work factor(也称之为 security factor)或迭代次数作为参数来确定 Hash 函数将变的有多慢，并且随着日后计算能力的提高，可以逐步增大 work factor 来使之与计算能力达到平衡。
* bcrypt是单向的，而且经过salt和cost的处理，使其受rainbow攻击破解的概率大大降低，同时破解的难度也提升不少。
* 因为bcrypt采用了一系列各种不同的Blowfish加密算法，并引入了一个work factor，这个工作因子可以让你决定这个算法的代价有多大。因为这些，这个算法不会因为计算机CPU处理速度变快了，而导致算法的时间会缩短了。因为，你可以增加work factor来把其性能降下来。

# 数字签名

* 别人不能冒充我的签名（不可伪造)，我也不能否认上面的签名是我的（不可抵赖)。
* 数字签名又是靠什么保证不可伪造和不可抵赖两个特性呢？
* 答案是利用公钥加密系统。
* RSA既可以用公钥加密然后私钥解密，也可以用私钥加密然后公钥解密（对称性)。
* 因为RSA中的每一个公钥都有唯一的私钥与之对应，任一公钥只能解开对应私钥加密的内容。换句话说，其它私钥加密的内容，这个公钥是解不开的。
* 这样，如果你生成了一对RSA密钥，你把公钥公布出去，并告诉全世界人这个公钥是你的。之后你只要在发送的消息，比如“123456”，后面加上用私钥加密过的密文，其他人拿公钥解密，看解密得到的内容是不是“123456”就可以知道这个“123456”是不是你发的。
* 其他人因为没有对应的私钥，所以没法生成公钥可以解密的密文，所以是不可伪造的。
* 又因为公钥对应的私钥只有一个，所以只要能成功解密，那么发消息的一定是你，不会是其他人，所以是不可抵赖的。
* 由于直接对原消息进行签名有安全性问题，而且原消息往往比较大，直接使用RSA算法进行签名速度会比较慢，所以我们一般对消息计算其摘要（使用SHA-256等安全的摘要算法)，然后对摘要进行签名。只要使用的摘要算法是安全的（MD5、SHA-1已经不安全了)，那么这种方式的数字签名就是安全的。
* 一个具体的RSA签名过程如下：
* 小明对外发布公钥，并声明对应的私钥在自己手上
* 小明对消息M计算摘要，得到摘要D
* 小明使用私钥对D进行签名，得到签名S
* 将M和S一起发送出去
* 验证过程如下：
* 接收者首先对M使用跟小明一样的摘要算法计算摘要，得到D
* 使用小明公钥对S进行解签，得到D’
* 如果D和D’相同，那么证明M确实是小明发出的，并且没有被篡改过。
* 报文鉴别——接收者能够核实发送者对报文的签名
* 报文的完整性——发送者事后不能抵赖对报文的签名
* 不可否认——接收者不能伪造对报文的签名

# 密钥管理

* 对称密码的密钥、非对称加密的私钥、salt等都需要保证不被泄露。
* 改善密钥安全性的方式有两种：
  + 1)把密钥和算法放在一个单独的服务器上，对外提供加密和解密服务，应用系统通过调用这个服务实现数据的加解密。容易成为应用瓶颈，系统性能开销较高。
  + 2)将加解密算法放到应用系统中，密钥放在独立服务器中。实际存储时，密钥被切分成薯片，加密后分别保存在不同存储介质中，兼顾密钥安全性的同时又改善了性能。

# HTTP

# HTTP概述

* HTTP（hypertext transport protocol)，即超文本传输协议。这个协议详细规定了浏览器和万维网服务器之间互相通信的规则。
* HTTP就是一个通信规则，通信规则规定了客户端发送给服务器的内容格式，也规定了服务器发送给客户端的内容格式。其实我们要学习的就是这个两个格式！客户端发送给服务器的格式叫“请求协议”；服务器发送给客户端的格式叫“响应协议”。

# 请求协议

* 请求协议的格式如下：  
  请求首行； 包括请求类型,要访问的资源以及所使用的HTTP版本.  
  请求头信息；  
  空行； \r\n DOS/Windows:’\r\n’ UNIX/Linux:’\n’ Mac:’\r’  
  请求体。
* 浏览器发送给服务器的内容就这个格式的，如果不是这个格式服务器将无法解读！在HTTP协议中，请求有很多请求方法，其中最为常用的就是GET和POST。不同的请求方法之间的区别，后面会一点一点的介绍。

# GET请求

* 打开IE，在访问hello项目的index.jsp之间打开HttpWatch，并点击“Record”按钮。然后访问index.jsp页面。查看请求内容如下：

GET /hello/index.jsp HTTP/1.1  
Host: localhost  
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Language: zh-cn,zh;q=0.5  
Accept-Encoding: gzip, deflate  
Accept-Charset: GB2312,utf-8;q=0.7,\*;q=0.7  
Connection: keep-alive  
Cookie: JSESSIONID=369766FDF6220F7803433C0B2DE36D98

- GET /hello/index.jsp HTTP/1.1：GET请求，请求服务器路径为/hello/index.jsp，协议为1.1；  
- Host:localhost：请求的主机名为localhost；  
- User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0：与浏览器和OS相关的信息。有些网站会显示用户的系统版本和浏览器版本信息，这都是通过获取User-Agent头信息而来的；  


Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8：告诉服务器，当前客户端可以接收的文档类型，其实这里包含了\*/\*，就表示什么都可以接收；

- Accept-Language: zh-cn,zh;q=0.5：当前客户端支持的语言，可以在浏览器的工具选项中找到语言相关信息；  
- Accept-Encoding: gzip, deflate：支持的压缩格式。数据在网络上传递时，可能服务器会把数据压缩后再发送；  
- Accept-Charset: GB2312,utf-8;q=0.7,\*;q=0.7：客户端支持的编码；  
- Connection: keep-alive：客户端支持的链接方式，保持一段时间链接，默认为3000ms；（无状态的)  
- Cookie: JSESSIONID=369766FDF6220F7803433C0B2DE36D98：因为不是第一次访问这个地址，所以会在请求中把上一次服务器响应中发送过来的Cookie在请求中一并发送去过

# POST请求

* 为了演示POST请求，我们需要修改index.jsp页面，即添加一个表单：
* 打开HttpWatch，输入hello后点击提交，查看请求内容如下：  
  POST /hello/index.jsp HTTP/1.1  
  Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */*  
  Referer: http://localhost:8080/hello/index.jsp  
  Accept-Language: zh-cn,en-US;q=0.5  
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)  
  Content-Type: application/x-www-form-urlencoded  
  Accept-Encoding: gzip, deflate  
  Host: localhost:8080  
  Content-Length: 13  
  Connection: Keep-Alive  
  Cache-Control: no-cache  
  Cookie: JSESSIONID=E365D980343B9307023A1D271CC48E7D

keyword=hello

* POST请求是可以有体的，而GET请求不能有请求体。  
  - Referer: http://localhost:8080/hello/index.jsp：请求来自哪个页面，例如你在百度上点击链接到了这里，那么Referer:http://www.baidu.com；如果你是在浏览器的地址栏中直接输入的地址，那么就没有Referer这个请求头了；  
  - Content-Type: application/x-www-form-urlencoded：表单的数据类型，说明会使用url格式编码数据；url编码的数据都是以“%”为前缀，后面跟随两位的16进制，例如“传智”这两个字使用UTF-8的url编码用为“%E4%BC%A0%E6%99%BA”；  
  - Content-Length:13：请求体的长度，这里表示13个字节。  
  - keyword=hello：请求体内容！hello是在表单中输入的数据，keyword是表单字段的名字。
* Referer请求头是比较有用的一个请求头，它可以用来做统计工作，也可以用来做防盗链。
* 统计工作：我公司网站在百度上做了广告，但不知道在百度上做广告对我们网站的访问量是否有影响，那么可以对每个请求中的Referer进行分析，如果Referer为百度的很多，那么说明用户都是通过百度找到我们公司网站的。
* 防盗链：我公司网站上有一个下载链接，而其他网站盗链了这个地址，例如在我网站上的index.html页面中有一个链接，点击即可下载JDK7.0，但有某个人的微博中盗链了这个资源，它也有一个链接指向我们网站的JDK7.0，也就是说登录它的微博，点击链接就可以从我网站上下载JDK7.0，这导致我们网站的广告没有看，但下载的却是我网站的资源。这时可以使用Referer进行防盗链，在资源被下载之前，我们对Referer进行判断，如果请求来自本网站，那么允许下载，如果非本网站，先跳转到本网站看广告，然后再允许下载。

# GET和POST请求的区别

* 幂等意味着对同一URL的多个请求应该返回同样的结果。
  + 1)前者将请求参数放在URL中，文本格式；后者将请求参数放在请求体中，可以是文本、二进制等格式
  + 2)前者语义上是从服务器获取资源，安全（无副作用)、幂等、可缓存；后者语义上是向服务器提交资源，不安全（有副作用)、不幂等、不可缓存
  + 3)前者的URL是明文传输，会保存在浏览器历史记录中，安全性不足，可能会受到CSRF攻击；后者较为安全（但是如果没有加密的话，都是可以明文获取的)

# 其他请求方法

* GET（SELECT)：从服务器取出资源（一项或多项)。
* POST（CREATE)：在服务器新建一个资源。
* PUT（UPDATE)：在服务器更新资源（客户端提供改变后的完整资源，数据输入必须与由 GET 接收的数据表示保持一致)。
* PATCH（UPDATE)：在服务器更新资源（客户端提供改变的属性)。
* DELETE（DELETE)：从服务器删除资源。
* HEAD：获取资源的元数据。
* OPTIONS：1、获取服务器支持的HTTP请求方法
* 2、用来检查服务器的性能

# 响应内容

* 响应协议的格式如下：  
  响应首行；由HTTP协议版本号， 状态码， 状态消息 三部分组成。  
  响应头信息；  
  空行；  
  响应体。
* 响应内容是由服务器发送给浏览器的内容，浏览器会根据响应内容来显示。  
  HTTP/1.1 200 OK  
  Server: Apache-Coyote/1.1  
  Content-Type: text/html;charset=UTF-8  
  Content-Length: 724  
  Set-Cookie: JSESSIONID=C97E2B4C55553EAB46079A4F263435A4; Path=/hello  
  Date: Wed, 25 Sep 2012 04:15:03 GMT

<title>My JSP 'index.jsp' starting page</title>  
<meta http-equiv="pragma" content="no-cache">  
<meta http-equiv="cache-control" content="no-cache">  
<meta http-equiv="expires" content="0">   
<meta http-equiv="keywords" content="keyword1,keyword2,keyword3">  
<meta http-equiv="description" content="This is my page">  
<!--  
<link rel="stylesheet" type="text/css" href="styles.css">  
-->

- HTTP/1.1 200 OK：响应协议为HTTP1.1，状态码为200，表示请求成功，OK是对状态码的解释；  
- Server: Apache-Coyote/1.1：服务器的版本信息；  
- Content-Type: text/html;charset=UTF-8：响应体使用的编码为UTF-8；  
- Content-Length: 724：响应体为724字节；  
- Set-Cookie: JSESSIONID=C97E2B4C55553EAB46079A4F263435A4; Path=/hello：响应给客户端的Cookie；  
- Date: Wed, 25 Sep 2012 04:15:03 GMT：响应的时间，这可能会有8小时的时区差；

# 响应码

* 响应头对浏览器来说很重要，它说明了响应的真正含义。例如200表示响应成功了，302表示重定向，这说明浏览器需要再发一个新的请求。
* 2xx表示成功，3xx表示重定向，4xx表示客户端出错，5xx表示服务器出错。  
  - 200：请求成功，浏览器会把响应体内容（通常是html)显示在浏览器中；  
  - 404：请求的资源没有找到，说明客户端错误的请求了不存在的资源；  
  - 500：请求资源找到了，但服务器内部出现了错误；  
  - 302：重定向，当响应码为302时，表示服务器要求浏览器重新再发一个请求，服务器会发送一个响应头Location，它指定了新请求的URL地址；  
  - 304：（缓存)

## 301&302

* 301 Move Permanently
* 302 Found
* 301是永久性重定向。当网站需要改版时，多域名指向同一个页面时，为了不让网站被降低和分散权重，就需要使用301重定向来实现，同时在搜索引擎索引库中彻底废弃掉原先的老地址。
* 302是临时性重定向，搜索引擎会抓取新的内容而保留旧的网址。因为服务器返回302代码，搜索引擎认为新的网址只是暂时的，不会传递权重。

# 其他响应头

* 告诉浏览器不要缓存的响应头：  
  - Expires: -1；（过期时间，-1表示马上过期)  
  - Cache-Control: no-cache；（不缓存)  
  - Pragma: no-cache；（不缓存)
* 自动刷新响应头，浏览器会在3秒之后请求http://www.baidu.com：  
  - Refresh: 3;url=http://www.baidu.com

# HTML中指定响应头

* 在HTMl页面中可以使用来指定响应头，例如在index.html页面中给出，表示浏览器只会显示index.html页面3秒，然后自动跳转到http://www.itcast.cn。

# 缓存

# 强缓存与协商缓存

* 浏览器HTTP缓存可以分为强缓存和协商缓存。强缓存和协商缓存最大也是最根本的区别是：强缓存命中的话不会发请求到服务器（比如chrome中的200 from memory cache)，协商缓存一定会发请求到服务器，通过资源的请求首部字段验证资源是否命中协商缓存，如果协商缓存命中，服务器会将这个请求返回，但是不会返回这个资源的实体，而是通知客户端可以从缓存中加载这个资源（304 not modified)。

# 控制强缓存的字段按优先级介绍

1.- Pragma Pragma是HTTP/1.1之前版本遗留的通用首部字段，仅作为于HTTP/1.0的向后兼容而使用。虽然它是一个通用首部，但是它在响应报文中时的行为没有规范，依赖于浏览器的实现。RFC中该字段只有no-cache一个可选值，会通知浏览器不直接使用缓存，要求向服务器发请求校验新鲜度。因为它优先级最高，当存在时一定不会命中强缓存。  
2.- Cache-Control Cache-Control是一个通用首部字段，也是HTTP/1.1控制浏览器缓存的主流字段。和浏览器缓存相关的是如下几个响应指令：  
指令 参数 说明  
private 无 表明响应只能被单个用户缓存，不能作为共享缓存（即代理服务器不能缓存它)  
public 可省略 表明响应可以被任何对象（包括：发送请求的客户端，代理服务器，等等)缓存  
no-cache 可省略 缓存前必需确认其有效性  
no-store 无 不缓存请求或响应的任何内容  
max-age=[s] 必需 响应的最大值  
- max-age（单位为s)设置缓存的存在时间，相对于发送请求的时间。只有响应报文首部设置Cache-Control为非0的max-age或者设置了大于请求日期的Expires（下文会讲)才有可能命中强缓存。当满足这个条件，同时响应报文首部中Cache-Control不存在no-cache、no-store且请求报文首部不存在Pragma字段，才会真正命中强缓存。   
- no-cache 表示请求必须先与服务器确认缓存的有效性，如果有效才能使用缓存（协商缓存)，无论是响应报文首部还是请求报文首部出现这个字段均一定不会命中强缓存。Chrome硬性重新加载（Command+shift+R)会在请求的首部加上Pragma：no-cache和Cache-Control：no-cache。  
- no-store 表示禁止浏览器以及所有中间缓存存储任何版本的返回响应，一定不会出现强缓存和协商缓存，适合个人隐私数据或者经济类数据。  


public 表明响应可以被浏览器、CDN等等缓存。



private 响应只作为私有的缓存，不能被CDN等缓存。如果要求HTTP认证，响应会自动设置为private。

3.- Expires Expires是一个响应首部字段，它指定了一个日期/时间，在这个时间/日期之前，HTTP缓存被认为是有效的。无效的日期比如0，表示这个资源已经过期了。如果同时设置了Cache-Control响应首部字段的max-age，则Expires会被忽略。它也是HTTP/1.1之前版本遗留的通用首部字段，仅作为于HTTP/1.0的向后兼容而使用。

# 控制协商缓存的字段

1.- Last-Modified/If-Modified-Since If-Modified-Since是一个请求首部字段，并且只能用在GET或者HEAD请求中。Last-Modified是一个响应首部字段，包含服务器认定的资源作出修改的日期及时间。当带着If-Modified-Since头访问服务器请求资源时，服务器会检查Last-Modified，如果Last-Modified的时间早于或等于If-Modified-Since则会返回一个不带主体的304响应，否则将重新返回资源。

* If-Modified-Since: , :: GMT Last-Modified: , :: GMT  
  2.- ETag/If-None-Match ETag是一个响应首部字段，它是根据实体内容生成的一段hash字符串，标识资源的状态，由服务端产生。If-None-Match是一个条件式的请求首部。如果请求资源时在请求首部加上这个字段，值为之前服务器端返回的资源上的ETag，则当且仅当服务器上没有任何资源的ETag属性值与这个首部中列出的时候，服务器才会返回带有所请求资源实体的200响应，否则服务器会返回不带实体的304响应。ETag优先级比Last-Modified高，同时存在时会以ETag为准。
* 因为ETag的特性，所以相较于Last-Modified有一些优势：
  1. 某些情况下服务器无法获取资源的最后修改时间
  2. 资源的最后修改时间变了但是内容没变，使用ETag可以正确缓存
  3. 如果资源修改非常频繁，在秒以下的时间进行修改，Last-Modified只能精确到秒

# 协商缓存细节

* 当用户第一次请求index.html时，服务器会添加一个名为Last-Modified响应头，这个头说明了index.html的最后修改时间，浏览器会把index.html内容，以及最后响应时间缓存下来。当用户第二次请求index.html时，在请求中包含一个名为If-Modified-Since请求头，它的值就是第一次请求时服务器通过Last-Modified响应头发送给浏览器的值，即index.html最后的修改时间，If-Modified-Since请求头就是在告诉服务器，我这里浏览器缓存的index.html最后修改时间是这个，您看看现在的index.html最后修改时间是不是这个，如果还是，那么您就不用再响应这个index.html内容了，我会把缓存的内容直接显示出来。而服务器端会获取If-Modified-Since值，与index.html的当前最后修改时间比对，如果相同，服务器会发响应码304，表示index.html与浏览器上次缓存的相同，无需再次发送，浏览器可以显示自己的缓存页面，如果比对不同，那么说明index.html已经做了修改，服务器会响应200。（只有html等静态资源可以做缓存，动态资源不做缓存)
* 响应头：  
  - Last-Modified：最后的修改时间；
* 请求头：  
  - If-Modified-Since：把上次请求的index.html的最后修改时间还给服务器；
* 状态码：304，比较If-Modified-Since的时间与文件真实的时间一样时，服务器会响应304，而且不会有响应正文，表示浏览器缓存的就是最新版本！

# 幂等性（并非是HTTP的问题，而是服务器API设计问题)

* 幂等性是http层面的问题吗，还是服务器要处理和解决的内容？
* 对HTTP协议的使用实际上存在着两种不同的方式：一种是RESTful的，它把HTTP当成应用层协议，比较忠实地遵守了HTTP协议的各种规定；另一种是SOA的，它并没有完全把HTTP当成应用层协议，而是把HTTP协议作为了传输层协议，然后在HTTP之上建立了自己的应用层协议。这里所讨论的HTTP幂等性主要针对RESTful风格的，但幂等性并不属于特定的协议，它是分布式系统的一种特性；所以，不论是SOA还是RESTful的Web API设计都应该考虑幂等性。下面将介绍HTTP GET、DELETE、PUT、POST四种主要方法的语义和幂等性。
* HTTP GET方法用于获取资源，不应有副作用，所以是幂等的。
* 比如：GET http://www.bank.com/account/123456，不会改变资源的状态，不论调用一次还是N次都没有副作用。请注意，这里强调的是一次和N次具有相同的副作用，而不是每次GET的结果相同。GET http://www.news.com/latest-news这个HTTP请求可能会每次得到不同的结果，但它本身并没有产生任何副作用，因而是满足幂等性的。
* HTTP DELETE方法用于删除资源，有副作用，但它应该满足幂等性。
* 比如：DELETE http://www.forum.com/article/4231，调用一次和N次对系统产生的副作用是相同的，即删掉id为4231的帖子；因此，调用者可以多次调用或刷新页面而不必担心引起错误。
* 比较容易混淆的是HTTP POST和PUT。POST和PUT的区别容易被简单地误认为“POST表示创建资源，PUT表示更新资源”；而实际上，二者均可用于创建资源，更为本质的差别是在幂等性方面。在HTTP规范中对POST和PUT是这样定义的：POST所对应的URI并非创建的资源本身，而是资源的接收者。比如：POST http://www.forum.com/articles的语义是在http://www.forum.com/articles下创建一篇帖子，HTTP响应中应包含帖子的创建状态以及帖子的URI。两次相同的POST请求会在服务器端创建两份资源，它们具有不同的URI；所以，POST方法不具备幂等性。而PUT所对应的URI是要创建或更新的资源本身。比如：PUT http://www.forum/articles/4231的语义是创建或更新ID为4231的帖子。对同一URI进行多次PUT的副作用和一次PUT是相同的；因此，PUT方法具有幂等性。

# 无状态

* 客户端和服务器在某次会话中产生的数据，从而【无状态】就意味着，这些数据不会被保留；协议对于事务处理没有记忆能力，服务器不知道客户端是什么状态。但是通过增加cookie和session机制，现在的网络请求其实是有状态的。在没有状态的http协议下，服务器也一定会保留你每次网络请求对数据的修改，但这跟保留每次访问的数据是不一样的，保留的只是会话产生的结果，而没有保留会话。
* 与之相对的是TCP，TCP是有状态的，因为每一条消息的seq和ack（还有一堆滑动窗口，拥塞的控制参数，等)都和前面消息相关。
* HTTP并不会在内存里保留前次请求相关的任何状态，仅仅以协议逻辑（打包解包)存在，所以是它无状态的。
* 无状态的设计会加强透明度(visibility)，稳定度(reliability)和伸缩度(scalability)。提高透明度是因为系统无需通过请求内容以外的信息判断请求的完整内容；提高稳定度是指在部分失败的情况下，减轻了恢复的难度；提高伸缩度的原因是无需储存请求间的状态使服务器端可以很快释放资源并简化实现。
* 优点在于解放了服务器，每一次请求“点到为止”不会造成不必要连接占用，缺点在于每次请求会传输大量重复的内容信息。

# 跨域 CORS 跨域资源共享

* 之所以会跨域，是因为受到了同源策略的限制，同源策略要求源相同才能正常进行通信，即协议、域名、端口号都完全一致。
* 同源策略具体限制些什么呢？
  1. 不能向工作在不同源的的服务请求数据（client to server)这里有个问题之前也困扰了我很久，就是为什么home.com加载的cdn.home.com/index.js可以向home.com发请求而不会跨域呢？其实home.com加载的JS是工作在home.com的，它的源不是提供JS的cdn，所以这个时候是没有跨域的问题的，并且script标签能够加载非同源的资源，不受同源策略的影响。
  2. 无法获取不同源的document/cookie等BOM和DOM，可以说任何有关另外一个源的信息都无法得到 （client to client)。
* 跨域最常用的方法，应当属CORS，如下图所示：
* 只要浏览器检测到响应头带上了CORS，并且允许的源包括了本网站，那么就不会拦截请求响应。
* CORS把请求分为两种，一种是简单请求，另一种是需要触发预检请求，这两者是相对的，怎样才算“不简单”？只要属于下面的其中一种就不是简单请求：
  + （1)使用了除GET/POST/HEAD之外的请求方式，如PUT/DELETE
  + （2)使用了除Content-Type/Accept等几个常用的http头这个时候就认为需要先发个预检请求

# 简单请求

* 对于简单请求，浏览器直接发出CORS请求。具体来说，就是在头信息之中，增加一个Origin字段。
* 下面是一个例子，浏览器发现这次跨源AJAX请求是简单请求，就自动在头信息之中，添加一个Origin字段。
* GET /cors HTTP/1.1
* Origin: http://api.bob.com
* Host: api.alice.com
* Accept-Language: en-US
* Connection: keep-alive
* User-Agent: Mozilla/5.0...
* 上面的头信息中，Origin字段用来说明，本次请求来自哪个源（协议 + 域名 + 端口)。服务器根据这个值，决定是否同意这次请求。
* 如果Origin指定的源，不在许可范围内，服务器会返回一个正常的HTTP回应。浏览器发现，这个回应的头信息没有包含Access-Control-Allow-Origin字段（详见下文)，就知道出错了，从而抛出一个错误，被XMLHttpRequest的onerror回调函数捕获。注意，这种错误无法通过状态码识别，因为HTTP回应的状态码有可能是200。
* 如果Origin指定的域名在许可范围内，服务器返回的响应，会多出几个头信息字段。
* Access-Control-Allow-Origin: http://api.bob.com
* Access-Control-Allow-Credentials: true
* Access-Control-Expose-Headers: FooBar
* Content-Type: text/html; charset=utf-8
* 上面的头信息之中，有三个与CORS请求相关的字段，都以Access-Control-开头。
  + （1)Access-Control-Allow-Origin
* 该字段是必须的。它的值要么是请求时Origin字段的值，要么是一个\*，表示接受任意域名的请求。
  + （2)Access-Control-Allow-Credentials
* 该字段可选。它的值是一个布尔值，表示是否允许发送Cookie。默认情况下，Cookie不包括在CORS请求之中。设为true，即表示服务器明确许可，Cookie可以包含在请求中，一起发给服务器。这个值也只能设为true，如果服务器不要浏览器发送Cookie，删除该字段即可。
  + （3)Access-Control-Expose-Headers
* 该字段可选。CORS请求时，XMLHttpRequest对象的getResponseHeader()方法只能拿到6个基本字段：Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragma。如果想拿到其他字段，就必须在Access-Control-Expose-Headers里面指定。上面的例子指定，getResponseHeader('FooBar')可以返回FooBar字段的值。

# 非简单请求

* 简单请求是那种对服务器有特殊要求的请求，比如请求方法是PUT或DELETE，或者Content-Type字段的类型是application/json。
* 非简单请求的CORS请求，会在正式通信之前，增加一次HTTP查询请求，称为"预检"请求（preflight)。
* 浏览器先询问服务器，当前网页所在的域名是否在服务器的许可名单之中，以及可以使用哪些HTTP动词和头信息字段。只有得到肯定答复，浏览器才会发出正式XMLHttpRequest请求，否则就报错。
* "预检"请求用的请求方法是OPTIONS，表示这个请求是用来询问的。头信息里面，关键字段是Origin，表示请求来自哪个源。
* 除了Origin字段，"预检"请求的头信息包括两个特殊字段。
  + （1)Access-Control-Request-Method
* 该字段是必须的，用来列出浏览器的CORS请求会用到哪些HTTP方法
  + （2)Access-Control-Request-Headers
* 该字段是一个逗号分隔的字符串，指定浏览器CORS请求会额外发送的头信息字段
* 服务器收到"预检"请求以后，检查了Origin、Access-Control-Request-Method和Access-Control-Request-Headers字段以后，确认允许跨源请求，就可以做出回应。
* 如果浏览器否定了"预检"请求，会返回一个正常的HTTP回应，但是没有任何CORS相关的头信息字段。这时，浏览器就会认定，服务器不同意预检请求，因此触发一个错误，被XMLHttpRequest对象的onerror回调函数捕获。
* 一旦服务器通过了"预检"请求，以后每次浏览器正常的CORS请求，就都跟简单请求一样，会有一个Origin头信息字段。服务器的回应，也都会有一个Access-Control-Allow-Origin头信息字段。
* CORS与JSONP的使用目的相同，但是比JSONP更强大。
* JSONP只支持GET请求，CORS支持所有类型的HTTP请求。JSONP的优势在于支持老式浏览器，以及可以向不支持CORS的网站请求数据。

# 长轮询与短轮询

* 短轮询相信大家都不难理解，比如你现在要做一个电商中商品详情的页面，这个详情界面中有一个字段是库存量（相信这个大家都不陌生，随便打开淘宝或者京东都能找到这种页面)。而这个库存量需要实时的变化，保持和服务器里实际的库存一致。
* 这个时候，你会怎么做？
* 最简单的一种方式，就是你用JS写个死循环，不停的去请求服务器中的库存量是多少，然后刷新到这个页面当中，这其实就是所谓的短轮询。
* 这种方式有明显的坏处，那就是你很浪费服务器和客户端的资源。客户端还好点，现在PC机配置高了，你不停的请求还不至于把用户的电脑整死，但是服务器就很蛋疼了。如果有1000个人停留在某个商品详情页面，那就是说会有1000个客户端不停的去请求服务器获取库存量，这显然是不合理的。
* 那怎么办呢？
* 长轮询这个时候就出现了，其实长轮询和短轮询最大的区别是，短轮询去服务端查询的时候，不管库存量有没有变化，服务器就立即返回结果了。而长轮询则不是，在长轮询中，服务器如果检测到库存量没有变化的话，将会把当前请求挂起一段时间（这个时间也叫作超时时间，一般是几十秒,Object.wait)。在这个时间里，服务器会去检测库存量有没有变化，检测到变化就立即返回（Object.notify)，否则就一直等到超时为止。
* 而对于客户端来说，不管是长轮询还是短轮询，客户端的动作都是一样的，就是不停的去请求，不同的是服务端，短轮询情况下服务端每次请求不管有没有变化都会立即返回结果，而长轮询情况下，如果有变化才会立即返回结果，而没有变化的话，则不会再立即给客户端返回结果，直到超时为止。
* 这样一来，客户端的请求次数将会大量减少（这也就意味着节省了网络流量，毕竟每次发请求，都会占用客户端的上传流量和服务端的下载流量)，而且也解决了服务端一直疲于接受请求的窘境。
* 但是长轮询也是有坏处的，因为把请求挂起同样会导致资源的浪费，假设还是1000个人停留在某个商品详情页面，那就很有可能服务器这边挂着1000个线程，在不停检测库存量，这依然是有问题的。
* 因此，从这里可以看出，不管是长轮询还是短轮询，都不太适用于客户端数量太多的情况，因为每个服务器所能承载的TCP连接数是有上限的，这种轮询很容易把连接数顶满。

# 长连接与短连接

* HTTP的短连接和长连接；长连接与短连接的区别（LVS是通过长连接作负载均衡)
* HTTP的长连接和短连接本质上是TCP长连接和短连接。
* 在HTTP/1.0中，默认使用的是短连接。也就是说，浏览器和服务器每进行一次HTTP操作，就建立一次连接，但任务结束就中断连接。
* 但从 HTTP/1.1起，默认使用长连接，用以保持连接特性。使用长连接的HTTP协议，会在响应头有加入这行代码：Connection:keep-alive。
* 在使用长连接的情况下，当一个网页打开完成后，客户端和服务器之间用于传输HTTP数据的 TCP连接不会关闭，如果客户端再次访问这个服务器上的网页，会继续使用这一条已经建立的连接。Keep-Alive不会永久保持连接，它有一个保持时间，可以在不同的服务器软件（如Apache)中设定这个时间。实现长连接要客户端和服务端都支持长连接。
* 长连接可以省去较多的TCP建立和关闭的操作，减少浪费，节约时间。对于频繁请求资源的客户来说，较适用长连接。不过这里存在一个问题，存活功能的探测周期太长，还有就是它只是探测TCP连接的存活，属于比较斯文的做法，遇到恶意的连接时，保活功能就不够使了。在长连接的应用场景下，client端一般不会主动关闭它们之间的连接，Client与server之间的连接如果一直不关闭的话，会存在一个问题，随着客户端连接越来越多，server早晚有扛不住的时候，这时候server端需要采取一些策略，如关闭一些长时间没有读写事件发生的连接，这样可以避免一些恶意连接导致server端服务受损。
* 短连接对于服务器来说管理较为简单，存在的连接都是有用的连接，不需要额外的控制手段。但如果客户请求频繁，将在TCP的建立和关闭操作上浪费时间和带宽。

# URL

* url有最大长度限制，就问长度有限制是get的原因还是url的原因，为什么长度会有限制，是http数据包的头的字段原因还是内容字段的原因
* 是GET的原因，长度受到服务器和客户端的限制。
* URL编解码
* Url的编码格式采用的是ASCII码，而不是Unicode，这也就是说你不能在Url中包含任何非ASCII字符，例如中文。
  + Url中只允许包含英文字母（a-zA-Z)、数字（0-9)、-\_.~4个特殊字符以及所有保留字符；
* RFC3986中指定了以下字符为保留字符：! \* ' ( ) ; : @ & = + $ , / ? # [ ]
* Url编码通常也被称为百分号编码（Url Encoding，also known as percent-encoding)，是因为它的编码方式非常简单，使用%百分号加上两位的十六进制字符。

# URI&URL

* URL（Uniform ResourceLocator)统一资源定位符，是专门为标识网络上的资源位置而设计的一种编址方式。URL一般由3个部分组成：
* 应用层协议
* 主机IP地址或域名
* 资源所在路径/文件名
* 统一资源标识符（Uniform Resource Identifier，或URI)是一个用于标识某一互联网资源名称的字符串。
* URI ：Uniform Resource Identifier，统一资源标识符；
* URL：Uniform Resource Locator，统一资源定位符；
* URN：Uniform ResourceName，统一资源名称。
* 其中，URL,URN是URI的子集。
* URL是一种具体的URI，它不仅唯一标识资源，而且还提供了定位该资源的信息。URI是一种语义上的抽象概念，可以是绝对的，也可以是相对的，而URL则必须提供足够的信息来定位。

# HTTPS

# HTTP缺点

- 明文传输，内容可能会被窃听  
- 不验证通信方的身份，因此有可能遭遇伪装  
- 无法证明报文的完整性，所以有可能已遭篡改

* HTTP+加密+认证+完整性保护=HTTPS
* 用SSL将通信的报文主体内容进行加密，使用SSL建立http的安全通信线路，SSL处于http与TCP通信之间，这样的SSL与HTTP组合被称为HTTPS。
* HTTPS 采用对称加密和非对称加密两者并用的混合加密机制
* HTTPS 公钥能用公钥解吗？在客户端抓包，看到的是加密的还是没加密 是没加密的
* https ssl tcp三者关系，其中哪些用到了对称加密，哪些用到了非对称加密，非对称加密密钥是如何实现的
* 加密的私钥和公钥各自如何分配（客户端拿公钥，服务器拿私钥)
* 客户端是如何认证服务器的真实身份，详细说明一下过程，包括公钥如何申请，哪一层加密哪一层解密
* 怎么攻击https
* TLS改进，如果session ticket被偷听到会怎样，如何防止中间人攻击

# SSL/TLS

* SSL（Secure Socket Layer安全套接字层)
* TLS（Transport Layer Security)
* SSL发展到3.0版本后改成了TLS。
* TLS主要提供三个基本服务  
  - 加密  
  - 身份验证  
  - 消息完整性校验
* 通常，HTTP 直接和 TCP 通信。当使用 SSL 时，则演变成先和 SSL 通信，再由 SSL 和 TCP 通信了。用 SSL 建立安全通信线路之后，就可以在这条线路上进行 HTTP 通信了。
* SSL 是独立于 HTTP 的协议，所以不光是 HTTP 协议，其他运行在应用层的 SMTP 和 Telnet 等协议均可配合 SSL 协议使用。可以说 SSL 是当今世界上应用最为广泛的网络安全技术。
* 虽然使用 HTTP 协议无法确定通信方，但如果使用 SSL 则可以。SSL 不仅提供加密处理，而且还使用了一种被称为证书的手段，可用于确定双方身份。
* 证书由值得信任的第三方机构颁发，用以证明服务器和客户端是实际存在的。另外，伪造证书从技术角度来说是异常困难的一件事。所以只要能够确认通信方(服务器或客户端)持有的证书，即可判断通信方的真实意图。

# 中间人攻击

* mim 就是man in the middle，中间人攻击正常情况下浏览器与服务器在TLS连接下内容是加密的，第三方即使可以嗅探到所有的数据，也不能解密。中间人可以与你建立连接，然后中间人再与服务器建立连接，转发你们之间的内容。这时候中间人就获得了明文的信息。
* 有什么危害？你与服务器的通信被第三方解密、查看、修改。如何防范？如果确定是否被攻击？在访问https连接的时候，查看一下服务器提供的证书是不是正确的。除非入侵并取得服务器的证书私钥，否则中间人是不能完全伪装成服务器的样子的。
* 数字证书可以保证服务器发来的公钥是真的来自服务器的

# 服务器保证其提供的公钥的正确性——数字证书

* 公钥是由数字证书认证机构(CA，Certificate Authority)和其相关机关颁发的公开密钥证书。
* 数字证书认证机构处于客户端与服务器双方都可信赖的第三方机构的立场上。服务器会将这份由数字证书认证机构颁发的公钥证书发送给客户端，以进行公开密钥加密方式通信。公钥证书也可叫做数字证书或直接称为证书。
* 接到证书的客户端可使用数字证书认证机构的公开密钥，对那张证书上的数字签名进行验证，一旦验证通过，客户端便可明确两件事：
* 认证服务器的公开密钥的是真实有效的数字证书认证机构
* 服务器的公开密钥是值得信赖的
* 此处认证机关的公开密钥必须安全地转交给客户端。使用通信方式时，如何安全转交是一件很困难的事，因此，多数浏览器开发商发布版本时，会事先在内部植入常用认证机关的公开密钥。

# 过程

*  客户端发起HTTPS请求 这个没什么好说的，就是用户在浏览器里输入一个HTTPS网址，然后连接到服务端的443端口。
*  服务端的配置 采用HTTPS协议的服务器必须要有一套数字证书，可以自己制作，也可以向组织申请。区别就是自己颁发的证书需要客户端验证通过，才可以继续访问，而使用受信任的公司申请的证书则不会弹出提示页面。这套证书其实就是一对公钥和私钥。
*  传送证书 这个证书其实就是公钥，只是包含了很多信息，如证书的颁发机构，过期时间等等。
*  客户端解析证书 这部分工作是由客户端的SSL/TLS来完成的，首先会验证公钥是否有效，比如颁发机构，过期时间等等，如果发现异常，则会弹出一个警示框，提示证书存在的问题。如果证书没有问题，那么就生成一个随机值。然后用证书（也就是公钥)对这个随机值进行加密。
*  传送加密信息 这部分传送的是用证书加密后的随机值，目的是让服务端得到这个随机值，以后客户端和服务端的通信就可以通过这个随机值来进行加密解密了。
*  服务端解密信息 服务端用私钥解密后，得到了客户端传过来的随机值，然后把内容通过该随机值（密钥)进行对称加密，将信息和私钥通过某种算法混合在一起，这样除非知道私钥，不然无法获取内容，而正好客户端和服务端都知道这个私钥，所以只要加密算法够复杂，私钥够复杂，数据就够安全。
*  传输加密后的信息 这部分信息就是服务端用私钥加密后的信息，可以在客户端用随机值解密还原。
*  客户端解密信息 客户端用之前生产的私钥解密服务端传过来的信息，于是获取了解密后的内容。整个过程第三方即使监听到了数据，也束手无策。
* 客户端获得服务器的公钥的过程是基于非对称加密实现的（数字证书)
* 而之后客户端和服务器之间的数据交换是基于对称加密实现的。

# 更具体的过程

*  客户端通过发送 Client Hello 报文开始 SSL 通信。报文中包含客户端支持的 SSL 的指定版本、加密组件(Cipher Suite)列表(所使用的加密算法及密钥长度等)
*  服务器可进行 SSL 通信时，会以 Server Hello 报文作为应答。和客户端一样，在报文中包含 SSL 版本以及加密组件。服务器的加密组件内容是从接收 到的客户端加密组件内筛选出来的。
*  之后服务器发送 Certificate 报文。报文中包含公开密钥证书。
*  最后服务器发送 Server Hello Done 报文通知客户端，最初阶段的 SSL 握手协商部分结束。
*  SSL 第一次握手结束之后，客户端以 Client Key Exchange 报文作为回应。报文中包含通信加密中使用的一种被称为 Pre-master secret 的随机密码串。该 报文已用步骤 3 中的公开密钥进行加密。
*  接着客户端继续发送 Change Cipher Spec 报文。该报文会提示服务器，在此报文之后的通信会采用 Pre-master secret 密钥加密。
*  客户端发送 Finished 报文。该报文包含连接至今全部报文的整体校验值。这次握手协商是否能够成功，要以服务器是否能够正确解密该报文作为判定标准。
*  服务器同样发送 Change Cipher Spec 报文。
*  服务器同样发送 Finished 报文。
*  服务器和客户端的 Finished 报文交换完毕之后，SSL 连接就算建立完成。当然，通信会受到 SSL 的保护。从此处开始进行应用层协议的通信，即发 送 HTTP 请求。
*  应用层协议通信，即发送 HTTP 响应。
*  最后由客户端断开连接。断开连接时，发送 close\_notify 报文。

# WebSocket

* web浏览器和web服务器之间全双工通信标准。
* 优点是，直接发送数据，不用等待客户端请求，一直保持连接状态，且首部信息量少，通信量减少。

# HTTP 2.0

# 二进制分帧

* 在应用层(HTTP2.0)和传输层(TCP or UDP)之间增加一个二进制分帧层。
* 在二进制分帧层上， HTTP 2.0 会将所有传输的信息分割为更小的消息和帧,并对它们采用二进制格式的编码。Frame 由 Frame Header 和 Frame Payload 两部分组成。不论是原来的 HTTP Header 还是 HTTP Body，在 HTTP/2 中，都将这些数据存储到 Frame Payload，组成一个个 Frame，再发送响应/请求。通过 Frame Header 中的 Type 区分这个 Frame 的类型。由此可见语义并没有太大变化，而是数据的格式变成二进制的 Frame。
* HTTP 2.0 通信都在一个连接上完成，这个连接可以承载任意数量的双向数据流。相应地，每个数据流以消息的形式发送，而消息由一或多个帧组成，这些帧可以乱序发送，然后再根据每个帧首部的流标识符重新组装。

# 首部压缩

* HTTP 2.0 在客户端和服务器端使用“首部表”来跟踪和存储之前发送的键-值对，对于相同的数据，不再通过每次请求和响应发送;通信期间几乎不会改变的通用键-值对(用户代理、可接受的媒体类型,等等)只需发送一次。事实上,如果请求中不包含首部(例如对同一资源的轮询请求),那么 首部开销就是零字节。此时所有首部都自动使用之前请求发送的首部。
* 如果首部发生变化了，那么只需要发送变化了数据在Headers帧里面，新增或修改的首部帧会被追加到“首部表”。首部表在 HTTP 2.0 的连接存续期内始终存在,由客户端和服务器共同渐进地更新 。
* HTTP/2 使用了专门为首部压缩而设计的 HPACK 算法。

# 服务器推送

* HTTP 2.0 新增的一个强大的新功能，就是服务器可以对一个客户端请求发送多个响应。换句话说，服务器除了对最初请求的响应外，还可以额外向客户端推送资源，而无需客户端明确地请求。
* 当浏览器请求一个html，服务器其实大概知道你是接下来要请求资源了，而不需要等待浏览器得到html后解析页面再发送资源请求。我们常用的内嵌图片也可以理解为一种强制的服务器推送：我请求html，却内嵌了张图。
* 有了HTTP2.0的服务器推送，HTTP1.x时代的内嵌资源的优化手段也变得没有意义了。而且使用服务器推送的资源的方式更加高效，因为客户端还可以缓存起来，甚至可以由不同的页面共享（依旧遵循同源策略)。当然，浏览器是可以决绝服务器推送的资源的。

# 多路复用

* 多路复用允许同时通过单一的HTTP/2连接发起多重的请求-响应信息。
* 每个 Frame Header 都有一个 Stream ID 就是被用于实现该特性。每次请求/响应使用不同的 Stream ID。就像同一个 TCP 链接上的数据包通过 IP:PORT来区分出数据包去往哪里一样。通过 Stream ID 标识，所有的请求和响应都可以欢快的同时跑在一条 TCP 链接上了。

# SOA

* Web Service也叫XML Web Service WebService是一种可以接收从Internet或者Intranet上的其它系统中传递过来的请求，轻量级的独立的通讯技术。是通过SOAP在Web上提供的软件服务，使用WSDL文件进行说明，并通过UDDI进行注册。
* SOA是一种架构风格，包括两个方面的内容：
  + 1)抽象出服务，这些服务满足离散、松耦合、可复用、自治、无状态等特征；
  + 2)服务可以灵活地组装和编排，满足流程整合和业务变化的需要
* WebService是SOA的一种实现技术，跨语言，跨平台，提供了标准的服务定义、服务注册、服务接入和访问的方式。使用了XML、SOAP、WSDL、UDDI等技术。

# SOA三角操作模型

- 1)三种角色

* 服务提供者：发布自己的服务，并且对服务请求进行响应
* 服务请求者：利用服务注册中心查找所需要的服务，然后使用该服务
* 服务注册中心：注册已经发布的服务，对其进行分类，并提供搜索服务
  + 2)三个操作：
* 发布：为了使服务可访问，需要发布服务描述以使服务使用者可以发现它
* 查找：服务请求者查询服务注册中心来找到满足其要求的服务
* 绑定：检索到服务描述后，服务请求者继续根据服务描述中的信息调用服务

# XML

* XML：(Extensible Markup Language)扩展型可标记语言。面向短期的临时数据处理、面向万维网络，是Soap的基础。

# SOAP

* SOAP：(Simple Object Access Protocol)简单对象传输协议。是XML Web Service 的通信协议。当用户通过UDDI找到你的WSDL描述文档后，他通过可以SOAP调用你建立的Web服务中的一个或多个操作。SOAP是XML文档形式的调用方法的规范，它可以支持不同的底层接口，像HTTP(S)或者SMTP。
* SOAP=RPC+HTTP+XML：采用HTTP作为底层通讯协议；RPC作为一致性的调用途径，ＸＭＬ作为数据传送的格式，允许服务提供者和服务客户经过防火墙在INTERNET进行通讯交互。
* 简单对象传输协议，是轻量级的、简单的、基于XML的用于交换数据的协议。
* SOAP本质上是一个 XML文档，包含以下元素：
  + 1)Envelope元素：必需元素，根元素，标识此XML文档为一条SOAP消息
* 可以包含命名空间和声明额外的属性
  + 2)Header元素：可选元素，有关SOAP消息的应用程序专用消息
  + 3)Body元素：必需元素，包含所有的请求和响应信息
  + 4)Fault元素：可选元素，提供有关在处理此消息所发生错误的信息
* SOAP处理模型：
  + 1)用XML打包请求
  + 2)将请求发送给服务器
  + 3)服务器接收到请求，解码XML，处理请求，以XML格式返回响应
* SOAP并不假定传输数据的下层协议，因此必须设计为能在各种协议上运行。即使绝大多数SOAP是运行在HTTP上，使用URI标识服务，SOAP也仅仅使用POST方法发送请求，用一个唯一的URI标识服务的入口。
* 使用 HTTP 协议的 SOAP，由于其设计原则上并不像 REST 那样强调与 Web 的工作方式相一致，所以，基于 SOAP 应用很难充分发挥 HTTP 本身的缓存能力。
* HTTP是其通信协议/传输协议，SOAP是其应用协议

# WSDL

* WSDL：(Web Services Description Language) WSDL 文件是一个 XML 文档，用于说明一组 SOAP 消息以及如何交换这些消息。大多数情况下由软件自动生成和使用。
* 网络服务描述语言，是基于XML的，用于描述网络服务、服务定位和服务提供的操作的协议。

# UDDI

* UDDI (Universal Description, Discovery, and Integration) 是一个主要针对Web服务供应商和使用者的新项目。在用户能够调用Web服务之前，必须确定这个服务内包含哪些商务方法，找到被调用的接口定义，还要在服务端来编制软件，UDDI是一种根据描述文档来引导系统查找相应服务的机制。UDDI利用SOAP消息机制（标准的XML/HTTP)来发布，编辑，浏览以及查找注册信息。它采用XML格式来封装各种不同类型的数据，并且发送到注册中心或者由注册中心来返回需要的数据。
* 统一描述、发现、集成协议，提供基于网络服务的注册和发现机制

# REST

* SOAP协议属于复杂的、重量级的协议，当前随着Web2.0的兴起，表述性状态转移（Representational State Transfer，REST)逐步成为一个流行的架构风格。REST是一种轻量级的Web Service架构风格，其实现和操作比SOAP和XML-RPC更为简洁，可以完全通过HTTP协议实现，还可以利用缓存Cache来提高响应速度，性能、效率和易用性上都优于SOAP协议。REST架构对资源的操作包括获取、创建、修改和删除资源的操作正好对应HTTP协议提供的GET、POST、PUT和DELETE方法，这种针对网络应用的设计和开发方式，可以降低开发的复杂性，提高系统的可伸缩性。REST架构尤其适用于完全无状态的CRUD（Create、Read、Update、Delete，创建、读取、更新、删除)操作。
* REST简单而直观，把HTTP协议利用到了极限，在这种思想指导下，它甚至用HTTP请求的头信息来指明资源的表示形式（如果一个资源有多种形式的话，例如人类友善的页面还是机器可读的数据？)，用HTTP的错误机制来返回访问资源的错误。由此带来的直接好处是构建的成本减少了，例如用URI定位每一个资源可以利用通用成熟的技术，而不用再在服务器端开发一套资源访问机制。又如只需简单配置服务器就能规定资源的访问权限，例如通过禁止非GET访问把资源设成只读。
* 1．面向资源的接口设计
* 所有的接口设计都是针对资源来设计的，也就很类似于我们的面向对象和面向过程的设计区别，只不过现在将网络上的操作实体都作为资源来看待，同时URI的设计也是体现了对于资源的定位设计。后面会提到有一些网站的API设计说是REST设计，其实是RPC-REST的混合体，并非是REST的思想。
* 2．抽象操作为基础的CRUD
* 这点很简单，Http中的get,put,post,delete分别对应了read,update,create,delete四种操作，如果仅仅是作为对于资源的操作，抽象成为这四种已经足够了，但是对于现在的一些复杂的业务服务接口设计，可能这样的抽象未必能够满足。其实这也在后面的几个网站的API设计中暴露了这样的问题，如果要完全按照REST的思想来设计，那么适用的环境将会有限制，而非放之四海皆准的。
* 3．Http是应用协议而非传输协议
* 这点在后面各大网站的API分析中有很明显的体现，其实有些网站已经走到了SOAP的老路上，说是REST的理念设计，其实是作了一套私有的SOAP协议，因此称之为REST风格的自定义SOAP协议。
* 4．无状态，自包含
* 这点其实不仅仅是对于REST来说的，作为接口设计都需要能够做到这点，也是作为可扩展和高效性的最基本的保证，就算是使用SOAP的WebService也是一样。

# Git

# git init

* 在本地新建一个repo,进入一个项目目录,执行git init,会初始化一个repo,并在当前文件夹下创建一个.git文件夹.

# git clone

* 获取一个url对应的远程Git repo, 创建一个local copy.
* 一般的格式是git clone [url].
* clone下来的repo会以url最后一个斜线后面的名称命名,创建一个文件夹,如果想要指定特定的名称,可以git clone [url] newname指定.

# git status

* 查询repo的状态.
* git status -s: -s表示short, -s的输出标记会有两列,第一列是对staging区域而言,第二列是对working目录而言.

# git log

* show commit history of a branch.
* git log --oneline --number: 每条log只显示一行,显示number条.
* git log --oneline --graph:可以图形化地表示出分支合并历史.
* git log branchname可以显示特定分支的log.
* git log --oneline branch1 ^branch2,可以查看在分支1,却不在分支2中的提交.^表示排除这个分支(Window下可能要给^branch2加上引号).
* git log --decorate会显示出tag信息.
* git log --author=[author name] 可以指定作者的提交历史.
* git log --since --before --until --after 根据提交时间筛选log.
* --no-merges可以将merge的commits排除在外.
* git log --grep 根据commit信息过滤log: git log --grep=keywords
* 默认情况下, git log --grep --author是OR的关系,即满足一条即被返回,如果你想让它们是AND的关系,可以加上--all-match的option.
* git log -S: filter by introduced diff.
* 比如: git log -SmethodName (注意S和后面的词之间没有等号分隔).
* git log -p: show patch introduced at each commit.
* 每一个提交都是一个快照(snapshot),Git会把每次提交的diff计算出来,作为一个patch显示给你看.
* 另一种方法是git show [SHA].
* git log --stat: show diffstat of changes introduced at each commit.
* 同样是用来看改动的相对信息的,--stat比-p的输出更简单一些.

# git add

* 在提交之前,Git有一个暂存区(staging area),可以放入新添加的文件或者加入新的改动. commit时提交的改动是上一次加入到staging area中的改动,而不是我们disk上的改动.
* git add .
* 会递归地添加当前工作目录中的所有文件.

# git diff

* 不加参数的git diff:
* show diff of unstaged changes.
* 此命令比较的是工作目录中当前文件和暂存区域快照之间的差异,也就是修改之后还没有暂存起来的变化内容.
* 若要看已经暂存起来的文件和上次提交时的快照之间的差异,可以用:
* git diff --cached 命令.
* show diff of staged changes.
* (Git 1.6.1 及更高版本还允许使用 git diff --staged，效果是相同的).
* git diff HEAD
* show diff of all staged or unstated changes.
* 也即比较woking directory和上次提交之间所有的改动.
* 如果想看自从某个版本之后都改动了什么,可以用:
* git diff [version tag]
* 跟log命令一样,diff也可以加上--stat参数来简化输出.
* git diff [branchA] [branchB]可以用来比较两个分支.
* 它实际上会返回一个由A到B的patch,不是我们想要的结果.
* 一般我们想要的结果是两个分支分开以后各自的改动都是什么,是由命令:
* git diff [branchA]…[branchB]给出的.
* 实际上它是:git diff $(git merge-base [branchA] [branchB]) [branchB]的结果.

# git commit

* 提交已经被add进来的改动.
* git commit -m “the commit message"
* git commit -a 会先把所有已经track的文件的改动add进来,然后提交(有点像svn的一次提交,不用先暂存). 对于没有track的文件,还是需要git add一下.
* git commit --amend 增补提交. 会使用与当前提交节点相同的父节点进行一次新的提交,旧的提交将会被取消.

# git reset

* undo changes and commits.
* 这里的HEAD关键字指的是当前分支最末梢最新的一个提交.也就是版本库中该分支上的最新版本.
* git reset HEAD: unstage files from index and reset pointer to HEAD
* 这个命令用来把不小心add进去的文件从staged状态取出来,可以单独针对某一个文件操作: git reset HEAD - - filename, 这个- - 也可以不加.
* git reset --soft
* move HEAD to specific commit reference, index and staging are untouched.
* git reset --hard
* unstage files AND undo any changes in the working directory since last commit.
* 使用git reset —hard HEAD进行reset,即上次提交之后,所有staged的改动和工作目录的改动都会消失,还原到上次提交的状态.
* 这里的HEAD可以被写成任何一次提交的SHA-1.
* 不带soft和hard参数的git reset,实际上带的是默认参数mixed.
* 总结:
* git reset --mixed id,是将git的HEAD变了(也就是提交记录变了),但文件并没有改变，(也就是working tree并没有改变). 取消了commit和add的内容.
* git reset --soft id. 实际上，是git reset –mixed id 后,又做了一次git add.即取消了commit的内容.
* git reset --hard id.是将git的HEAD变了,文件也变了.
* 按改动范围排序如下:
* soft (commit) < mixed (commit + add) < hard (commit + add + local working)

# git revert

* 反转撤销提交.只要把出错的提交(commit)的名字(reference)作为参数传给命令就可以了.
* git revert HEAD: 撤销最近的一个提交.
* git revert会创建一个反向的新提交,可以通过参数-n来告诉Git先不要提交.

# git rm

* git rm file: 从staging区移除文件,同时也移除出工作目录.
* git rm --cached: 从staging区移除文件,但留在工作目录中.
* git rm --cached从功能上等同于git reset HEAD,清除了缓存区,但不动工作目录树.

# git clean

* git clean是从工作目录中移除没有track的文件.
* 通常的参数是git clean -df:
* -d表示同时移除目录,-f表示force,因为在git的配置文件中, clean.requireForce=true,如果不加-f,clean将会拒绝执行.

# git mv

* git rm - - cached orig; mv orig new; git add new

# git stash

* 把当前的改动压入一个栈.
* git stash将会把当前目录和index中的所有改动(但不包括未track的文件)压入一个栈,然后留给你一个clean的工作状态,即处于上一次最新提交处.
* git stash list会显示这个栈的list.
* git stash apply:取出stash中的上一个项目(stash@{0}),并且应用于当前的工作目录.
* 也可以指定别的项目,比如git stash apply stash@{1}.
* 如果你在应用stash中项目的同时想要删除它,可以用git stash pop
* 删除stash中的项目:
* git stash drop: 删除上一个,也可指定参数删除指定的一个项目.
* git stash clear: 删除所有项目.

# git branch

* git branch可以用来列出分支,创建分支和删除分支.
* git branch -v可以看见每一个分支的最后一次提交.
* git branch: 列出本地所有分支,当前分支会被星号标示出.
* git branch (branchname): 创建一个新的分支(当你用这种方式创建分支的时候,分支是基于你的上一次提交建立的).
* git branch -d (branchname): 删除一个分支.
* 删除remote的分支:
* git push (remote-name) :(branch-name): delete a remote branch.
* 这个是因为完整的命令形式是:
* git push remote-name local-branch:remote-branch
* 而这里local-branch的部分为空,就意味着删除了remote-branch

# git checkout

* git checkout (branchname)
* 切换到一个分支.
* git checkout -b (branchname): 创建并切换到新的分支.
* 这个命令是将git branch newbranch和git checkout newbranch合在一起的结果.
* checkout还有另一个作用:替换本地改动:
* git checkout --
* 此命令会使用HEAD中的最新内容替换掉你的工作目录中的文件.已添加到暂存区的改动以及新文件都不会受到影响.
* 注意:git checkout filename会删除该文件中所有没有暂存和提交的改动,这个操作是不可逆的.

# git merge

* 把一个分支merge进当前的分支.
* git merge [alias]/[branch]
* 把远程分支merge到当前分支.
* 如果出现冲突,需要手动修改,可以用git mergetool.
* 解决冲突的时候可以用到git diff,解决完之后用git add添加,即表示冲突已经被resolved.

# git tag

* tag a point in history as import.
* 会在一个提交上建立永久性的书签,通常是发布一个release版本或者ship了什么东西之后加tag.
* 比如: git tag v1.0
* git tag -a v1.0, -a参数会允许你添加一些信息,即make an annotated tag.
* 当你运行git tag -a命令的时候,Git会打开一个编辑器让你输入tag信息.
* 我们可以利用commit SHA来给一个过去的提交打tag:
* git tag -a v0.9 XXXX
* push的时候是不包含tag的,如果想包含,可以在push时加上--tags参数.
* fetch的时候,branch HEAD可以reach的tags是自动被fetch下来的, tags that aren’t reachable from branch heads will be skipped.如果想确保所有的tags都被包含进来,需要加上--tags选项.

# git remote

* list, add and delete remote repository aliases.
* 因为不需要每次都用完整的url,所以Git为每一个remote repo的url都建立一个别名,然后用git remote来管理这个list.
* git remote: 列出remote aliases.
* 如果你clone一个project,Git会自动将原来的url添加进来,别名就叫做:origin.
* git remote -v:可以看见每一个别名对应的实际url.
* git remote add [alias] [url]: 添加一个新的remote repo.
* git remote rm [alias]: 删除一个存在的remote alias.
* git remote rename [old-alias] [new-alias]: 重命名.
* git remote set-url [alias] [url]:更新url. 可以加上—push和fetch参数,为同一个别名set不同的存取地址.

# git fetch

* download new branches and data from a remote repository.
* 可以git fetch [alias]取某一个远程repo,也可以git fetch --all取到全部repo
* fetch将会取到所有你本地没有的数据,所有取下来的分支可以被叫做remote branches,它们和本地分支一样(可以看diff,log等,也可以merge到其他分支),但是Git不允许你checkout到它们.

# git pull

* fetch from a remote repo and try to merge into the current branch.
* pull == fetch + merge FETCH\_HEAD
* git pull会首先执行git fetch,然后执行git merge,把取来的分支的head merge到当前分支.这个merge操作会产生一个新的commit.
* 如果使用--rebase参数,它会执行git rebase来取代原来的git merge.

# git rebase

* --rebase不会产生合并的提交,它会将本地的所有提交临时保存为补丁(patch),放在”.git/rebase”目录中,然后将当前分支更新到最新的分支,最后把保存的补丁应用到分支上。本地的所有提交记录会被丢弃。
* rebase的过程中,也许会出现冲突,Git会停止rebase并让你解决冲突,在解决完冲突之后,用git add去更新这些内容,然后无需执行commit,只需要:
* git rebase --continue就会继续打余下的补丁.
* git rebase --abort将会终止rebase,当前分支将会回到rebase之前的状态.

# git push

* push your new branches and data to a remote repository.
* git push [alias] [branch]
* 将会把当前分支merge到alias上的[branch]分支.如果分支已经存在,将会更新,如果不存在,将会添加这个分支.
* 如果有多个人向同一个remote repo push代码, Git会首先在你试图push的分支上运行git log,检查它的历史中是否能看到server上的branch现在的tip,如果本地历史中不能看到server的tip,说明本地的代码不是最新的,Git会拒绝你的push,让你先fetch,merge,之后再push,这样就保证了所有人的改动都会被考虑进来.

# git reflog

* git reflog是对reflog进行管理的命令,reflog是git用来记录引用变化的一种机制,比如记录分支的变化或者是HEAD引用的变化.
* 当git reflog不指定引用的时候,默认列出HEAD的reflog.
* HEAD@{0}代表HEAD当前的值,HEAD@{3}代表HEAD在3次变化之前的值.
* git会将变化记录到HEAD对应的reflog文件中,其路径为.git/logs/HEAD, 分支的reflog文件都放在.git/logs/refs目录下的子目录中.

# AJAX

# 1、AJAX概述

# 1.1 什么是AJAX

* AJAX（Asynchronous Javascript And XML)翻译成中文就是“异步Javascript和XML”。即使用Javascript语言与服务器进行异步交互，传输的数据为XML（当然，传输的数据不只是XML)。
* AJAX还有一个最大的特点就是，当服务器响应时，不用刷新整个浏览器页面，而是可以局部刷新。这一特点给用户的感受是在不知不觉中完成请求和响应过程。  
  - 与服务器异步交互；  
  - 浏览器页面局部刷新；

# 1.2. 同步交互与异步交互

- 同步交互：客户端发出一个请求后，需要等待服务器响应结束后，才能发出第二个请求；  
- 异步交互：客户端发出一个请求后，无需等待服务器响应结束，就可以发出第二个请求。

# 1.3. AJAX常见应用情景

* 当我们在百度中输入一个“传”字后，会马上出现一个下拉列表！列表中显示的是包含“传”字的10个关键字。
* 其实这里就使用了AJAX技术！当文件框发生了输入变化时，浏览器会使用AJAX技术向服务器发送一个请求，查询包含“传”字的前10个关键字，然后服务器会把查询到的结果响应给浏览器，最后浏览器把这10个关键字显示在下拉列表中。  
  - 整个过程中页面没有刷新，只是刷新页面中的局部位置而已！  
  - 当请求发出后，浏览器还可以进行其他操作，无需等待服务器的响应！
* 当输入用户名后，把光标移动到其他表单项上时，浏览器会使用AJAX技术向服务器发出请求，服务器会查询名为zhangSan的用户是否存在，最终服务器返回true表示名为zhangSan的用户已经存在了，浏览器在得到结果后显示“用户名已被注册！”。  
  - 整个过程中页面没有刷新，只是局部刷新了；  
  - 在请求发出后，浏览器不用等待服务器响应结果就可以进行其他操作；

# 1.4 AJAX的优缺点

* 优点：  
  - AJAX使用Javascript技术向服务器发送异步请求；  
  - AJAX无须刷新整个页面；  
  - 因为服务器响应内容不再是整个页面，而是页面中的局部，所以AJAX性能高；
* 缺点：  
  - AJAX并不适合所有场景，很多时候还是要使用同步交互；  
  - AJAX虽然提高了用户体验，但无形中向服务器发送的请求次数增多了，导致服务器压力增大；  
  - 因为AJAX是在浏览器中使用Javascript技术完成的，所以还需要处理浏览器兼容性问题；

# 2、AJAX技术

# 2.1 AJAX第一例（发送GET请求)

## 2.1.1 准备工作

* 因为AJAX也需要请求服务器，异步请求也是请求服务器，所以我们需要先写好服务器端代码，即编写一个Servlet！
* 这里，Servlet很简单，只需要输出“Hello AJAX!”。  
  public class AServlet extends HttpServlet {  
  public void doGet(HttpServletRequest request, HttpServletResponse response)  
   throws ServletException, IOException {  
   System.out.println("Hello AJAX!");  
   response.getWriter().print("Hello AJAX!");  
  }  
  }

## 2.1.2 AJAX核心（XMLHttpRequest)

* 其实AJAX就是在Javascript中多添加了一个对象：XMLHttpRequest对象。所有的异步交互都是使用XMLHttpRequest对象完成的。也就是说，我们只需要学习一个Javascript的新对象即可。
* 注意，各个浏览器对XMLHttpRequest的支持也是不同的！大多数浏览器都支持DOM2规范，都可以使用：var xmlHttp = new XMLHttpRequest()来创建对象
* 为了处理浏览器兼容问题，给出下面方法来创建XMLHttpRequest对象：  
  function createXMLHttpRequest() {  
   var xmlHttp;  
   // 适用于大多数浏览器，以及IE7和IE更高版本  
   try{  
   xmlHttp = new XMLHttpRequest();  
   } catch (e) {  
   // 适用于IE6  
   try {  
   xmlHttp = new ActiveXObject("Msxml2.XMLHTTP");  
   } catch (e) {  
   // 适用于IE5.5，以及IE更早版本  
   try{  
   xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");  
   } catch (e){}  
   }  
   }   
   return xmlHttp;  
  }

## 2.1.3 打开与服务器的连接（open方法)

* 当得到XMLHttpRequest对象后，就可以调用该对象的open()方法打开与服务器的连接了。open()方法的参数如下：
* open(method, url, async)：  
  - method：请求方式，通常为GET或POST；  
  - url：请求的服务器地址，例如：/ajaxdemo1/AServlet，若为GET请求，还可以在URL后追加参数；  
  - async：这个参数可以不给，默认值为true，表示异步请求；
* var xmlHttp = createXMLHttpRequest();  
  xmlHttp.open("GET", "/ajaxdemo1/AServlet", true);

## 2.1.4 发送请求

* 当使用open打开连接后，就可以调用XMLHttpRequest对象的send()方法发送请求了。send()方法的参数为POST请求参数，即对应HTTP协议的请求体内容，若是GET请求，需要在URL后连接参数。
* 注意：若没有参数，需要给出null为参数！若不给出null为参数，可能会导致FireFox浏览器不能正常发送请求！  
  xmlHttp.send(null);

## 2.1.5 接收服务器响应

* 当请求发送出去后，服务器端Servlet就开始执行了，但服务器端的响应还没有接收到。接下来我们来接收服务器的响应。
* XMLHttpRequest对象有一个onreadystatechange事件，它会在XMLHttpRequest对象的状态发生变化时被调用。下面介绍一下XMLHttpRequest对象的5种状态：  
  - 0：初始化未完成状态，只是创建了XMLHttpRequest对象，还未调用open()方法；  
  - 1：请求已开始，open()方法已调用，但还没调用send()方法；  
  - 2：请求发送完成状态，send()方法已调用；  
  - 3：开始读取服务器响应；  
  - 4：读取服务器响应结束。
* onreadystatechange事件会在状态为1、2、3、4时引发。
* 下面代码会被执行四次！对应XMLHttpRequest的四种状态！  
   xmlHttp.onreadystatechange = function() {  
   alert('hello');  
   };
* 但通常我们只关心最后一种状态，即读取服务器响应结束时，客户端才会做出改变。我们可以通过XMLHttpRequest对象的readyState属性来得到XMLHttpRequest对象的状态。  
  xmlHttp.onreadystatechange = function() {  
   if(xmlHttp.readyState == 4) {  
   alert('hello');   
   }  
   };
* 其实我们还要关心服务器响应的状态码是否为200，其服务器响应为404，或500，那么就表示请求失败了。我们可以通过XMLHttpRequest对象的status属性得到服务器的状态码。
* 最后，我们还需要获取到服务器响应的内容，可以通过XMLHttpRequest对象的responseText得到服务器响应内容。
* responsXML是xml格式的文本，是document对象  
  xmlHttp.onreadystatechange = function() {  
   if(xmlHttp.readyState == 4 && xmlHttp.status == 200) {  
   alert(xmlHttp.responseText);   
   }  
   };

## 2.1.6 AJAX第一例小结

- 创建XMLHttpRequest对象；  
- 调用open()方法打开与服务器的连接；  
- 调用send()方法发送请求；  
- 为XMLHttpRequest对象指定onreadystatechange事件函数，这个函数会在XMLHttpRequest的1、2、3、4，四种状态时被调用；

* XMLHttpRequest对象的5种状态：  
  - 0：初始化未完成状态，只是创建了XMLHttpRequest对象，还未调用open()方法；  
  - 1：请求已开始，open()方法已调用，但还没调用send()方法；  
  - 2：请求发送完成状态，send()方法已调用；  
  - 3：开始读取服务器响应；  
  - 4：读取服务器响应结束。
* 通常我们只关心4状态。
* XMLHttpRequest对象的status属性表示服务器状态码，它只有在readyState为4时才能获取到。
* XMLHttpRequest对象的responseText属性表示服务器响应内容，它只有在readyState为4时才能获取到！
* var xmlHttp = new XMLHttpRequest();
* xmlHttp.open("GET", "/AJAX/AServlet");
* xmlHttp.send(null);
* xmlHttp.onreadystatechange = function(){
* if(xmlHttp.readyState == 4 && xmlHttp.status == 200){
* var h1 = document.getElementById("h1");
* h1.innerHTML = xmlHttp.responseText;
* }
* }

public class AServlet extends HttpServlet {

public void doGet(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {

* response.setContentType("text/html;charset=utf-8");
* response.getWriter().print("hehe");
* }
* }

# 2.2 AJAX第二例（发送POST请求)

## 2.2.1 发送POST请求注意事项

* POST请求必须设置ContentType请求头的值为application/x-www.form-encoded。表单的enctype默认值就是为application/x-www.form-encoded！因为默认值就是这个，所以大家可能会忽略这个值！当设置了的enctype=” application/x-www.form-encoded”时，等同与设置了Cotnent-Type请求头。
* 但在使用AJAX发送请求时，就没有默认值了，这需要我们自己来设置请求头：  
  xmlHttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
* 当没有设置Content-Type请求头为application/x-www-form-urlencoded时，Web容器会忽略请求体的内容。所以，在使用AJAX发送POST请求时，需要设置这一请求头，然后使用send()方法来设置请求体内容。  
  xmlHttp.send("b=B");
* 这时Servlet就可以获取到这个参数！！！
* AServlet  
  public void doPost(HttpServletRequest request, HttpServletResponse response)  
   throws ServletException, IOException {  
   System.out.println(request.getParameter("b"));  
   System.out.println("Hello AJAX!");  
   response.getWriter().print("Hello AJAX!");  
  }
* ajax2.jsp

function send() {  
 var xmlHttp = createXMLHttpRequest();  
 xmlHttp.onreadystatechange = function() {  
 if(xmlHttp.readyState == 4 && xmlHttp.status == 200) {  
 var div = document.getElementById("div1");  
 div.innerHTML = xmlHttp.responseText;  
 }  
 };  
 xmlHttp.open("POST", "/ajaxdemo1/AServlet?", true);  
 xmlHttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");  
 xmlHttp.send("b=B");  
}

测试

# 2.3 AJAX第三例（用户名是否已被注册)

## 2.3.1 功能介绍

* 在注册表单中，当用户填写了用户名后，把光标移开后，会自动向服务器发送异步请求。服务器返回true或false，返回true表示这个用户名已经被注册过，返回false表示没有注册过。
* 客户端得到服务器返回的结果后，确定是否在用户名文本框后显示“用户名已被注册”的错误信息！

## 2.3.2 案例分析

- regist.jsp页面中给出注册表单；  
- 在username表单字段中添加onblur事件，调用send()方法；  
- send()方法获取username表单字段的内容，向服务器发送异步请求，参数为username；  
- RegistServlet：获取username参数，判断是否为“itcast”，如果是响应true，否则响应false；

## 2.3.3 代码

* regist.jsp
* RegistServlet.java  
  public void doGet(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {  
   String username = request.getParameter("username");  
   System.out.println(username);  
   if(username.equals("admin")){  
   response.getWriter().print(false);  
   }else{  
   response.getWriter().print(true);  
   }  
  }

# 前端

* HTML的DOM对象说几个，Document的对象和方法  
  document.body 返回元素 1  
  document.cookie 返回或设置与当前文档相关的cookie 1  
  document.domain 返回当前文档的服务器域名 1  
  document.referrer 返回连接至当前文档的文档连接 1  
  document.title 返回当前文档的元素 1  
  document.URL 返回当前文档的完整URL 1