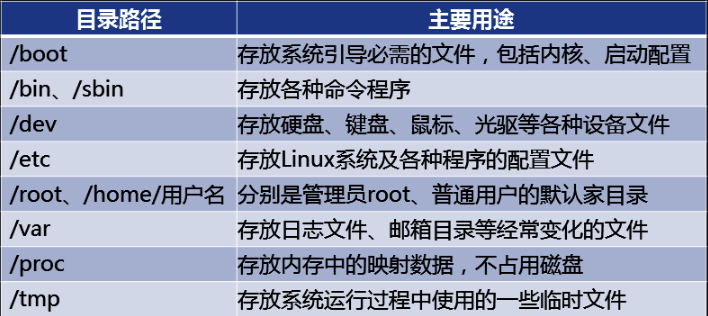
**0： 系统停机（关机）模式，系统默认运行级别不能设置为0，否则不能正常启动，一开机就自动关机。  
1：单用户模式，root权限，用于系统维护，禁止远程登陆，就像Windows下的安全模式登录。  
2：多用户模式，没有NFS网络支持。  
3：完整的多用户文本模式，有NFS，登陆后进入控制台命令行模式。  
4：系统未使用，保留一般不用，在一些特殊情况下可以用它来做一些事情。例如在笔记本电脑的电池用尽时，可以切换到这个模式来做一些设置。  
5：图形化模式，登陆后进入图形GUI模式或GNOME、KDE图形化界面，如X Window系统。  
6：重启模式，默认运行级别不能设为6，否则不能正常启动，就会一直开机重启开机重启。**

**linux目录结构**

****

**权限的数值表示**

**基本权限 ：r=4, w=2 , x=1**

**附加权限 ：SUID= 4 , SGID=2 , Sticky Bit=1**

**采用数值形式设置权限**

**Chmod [-R] nnn 文档**

**Chmod [-R] xnnn 文档**

**历史命令**

**History 查看历史命令列表**

**History -c 清空历史命令 !n 执行历史命令中的第n条历史命令**

**!str 执行最近一次以str开头的历史命令 调整历史命令的数量 /etc/profile HISTSIZE=1000 默认记录1000条**

**统计文件的占用空间**

**- du 【选项】...[目录或者文件]。。。**

**- s 只统计每个参数所占用的总空间大小**

**-h 提供易读容量单位**

**- ln 创建软连接**

**----软连接---> 原始文档-----> i节点 --> 文档数据**

**- ln -s 原始文件或者目录 软连接文件**

**若原始文件或者目录被删除，连接文件将失效 软连接可以存放不同的分区/文件系统**

**-----硬连接 ---> 节点 ----> 文档数据**

**-ln 原始文件 硬连接文件**

**若原始文件被删除，连接文件仍可用 硬连接与原始文件必须在同一分区/文件系统**

**归档压缩**

**Zip [-r ] 备份文件.zip 被归档的文档**

**释放归档+解压操作**

**Unzip 备份文件.zip [-d目标文件夹]**

**Yum仓库特点 镜像挂载格式 iso9660**

**Packages/ //存放.rpm软件包**

**Isopodata/ // 光盘引导数据**

**-RPM-GPG-KEY-redhat-release //签名校验密钥**

**Repodata /仓库档案数据**

**- fileists.xml.gz //软件包的文件安装清单**

**- primary.xml.gz //软件包的基本/主要信息**

**- other.xml.gz //软件包的其它信息**

**- repomd.xml //提供.xml.gz 下载和校验信息**

**第三方rpm 需额外创建repodata档案**

**Createrepo 文件路径**

**VIM编辑技巧**

**光标跳转**

****

**复制/粘贴/删除**

****

**查找/撤销/保存**

****

**末行模式操作**

**保存/退出/文件操作**

****

**字符串替换**

****

**开关参数的控制**

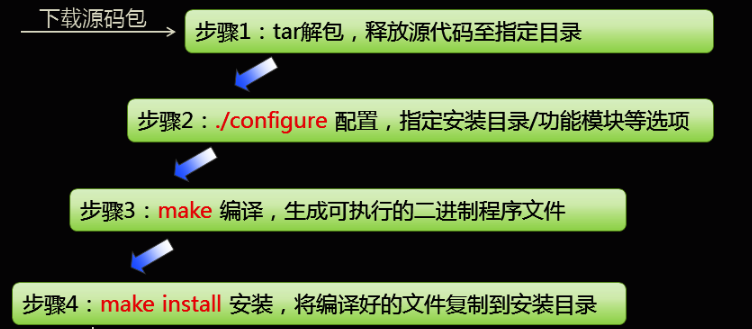
****

**源码编译安装**

**需要gcc gcc-c++ make等编译工具**

**获得软件的最新版本 及时修复bug 适用于各种平台 软件功能按需选择**

**基本的实现过程**

****

**#inotifywait -mrq /opt & 监控**

**systemd**

**一个更高校的系统&服务管理器**

**开机服务并行启动 各系统服务间的精确依赖**

**列出活动的系统服务 systemctl -t service**

**列出所有系统服务 systemctl -t service --all**

**列出可用运行 systemctl -t target**

**DNS 解析的作用 协议 TCP/UDP 53**

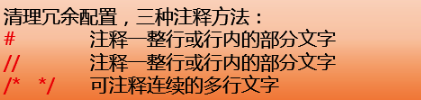
**系统服务 named 运行时的虚拟根环境 ：/var/named/chroot**

**主配置文件 /etc/named.conf**

**地址文件默认位置/var/named**

**检查配置语法错误 : named-checkconf [配置文件] #无错误无输出**

**全局配置部分 设置监听地址/端口 地址库存放位置**

****

**区域配置部分**

**定义DNS区域。类型 地址文件路径**

**地址库文件**

**NS 域名服务器记录 A 地址记录 仅用于正相解析区域**

**检查语法配置 named-checkzone 区域名 配置文件**

**正相解析 ：根据注册的域名查找对应的IP地址**

**反向解析 ： 根据IP地址查找对应的注册域名**

**DNS储存了网络中的 IP 地址与对应主机的信息，邮件路由信息和其他网络应用方面的信息，用户通过询问解决库（解决库发送询问并对DNS回应进行说明）在 DNS 上查询信息。DNS是网络分层里的应用层协议**

**DNS劫持**

**解决办法可以手动修改本地DNS域名服务器地址，首选DNS服务器：114.114.114.114，是国内第一个、全球第三个开放的DNS服务地址，又称114DNS，或8.8.8.8（google提供的DNS服务器）等，然后修改宽带密码，路由器密码，主机密码。**

**DNS轮询 基于DNS的站点负载均衡**

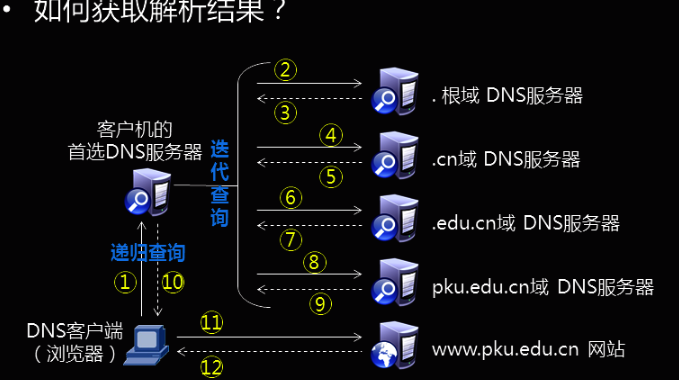
**一个域名对应多个不同的IP地址 每个IP提供镜像服务内容**

**子域授权的作用**

**适用于同一个DNS组织**

**父域子域的解析工作由不同的DNS服务器负责 父DNS服务器应该有为子域迭代的能力**

**DNS工作的查询方式**

****

**递归查询时默认开启的 可以设置recursion yes 明确启用 禁止递归 recursion no**

**验证迭代查询**

**Dig @DNS服务器 目标地址**

**缓存DNS 不需要管理任何DNS区域 但是能够替客户机查询 而且通过缓存、复用查询结果来加快速度 典型应用 ISP服务商 企业局域网**

**主要适用环境 互联网出口带宽较低的企业局域网 ISP服务商的公共DNS服务器**

**解析记录来源**

**方式1 全局转发**

**将请求转发给指定的公共DNS 请求递归服务**

**方式2： 根域迭代**

**依次向根、一级、二级。。。。。域的DNS服务器迭代**

**Split分离解析**

**当收到客户机的DNS查询请求的时候**

**- 能够区分客户机的来源地址**

**- 为不同类别的客户机提供不同的解析结果**

**BIND的view**

**根据源地址集合将客户机分类 不同客户机获得不同的结果（待遇有差别）**

**1 同一个区域在多个私视图内分别定义，其地址库相互独立，从而实现解析结果的分离**

**2 定义view视图后，不允许在view以外出现zone配置**

**Acl地址列表**

**为大批量的客户机建立列表**

**--- 调用时指定列表名即可 ，列表名any可匹配任意地址**

**--- 根据view调用的顺序 “匹配即停止”**

**RAID磁盘阵列**

**廉价冗余磁盘阵列**

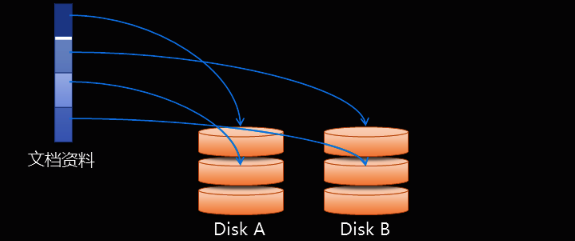
**- 通过硬件/软件技术 将多个较小/低速的磁盘整合成一个大磁盘**

**- 阵列的价值： 提升I/O效率、硬件级别的数据冗余**

**- 不同 RAID级别的功能、特性各不相同**

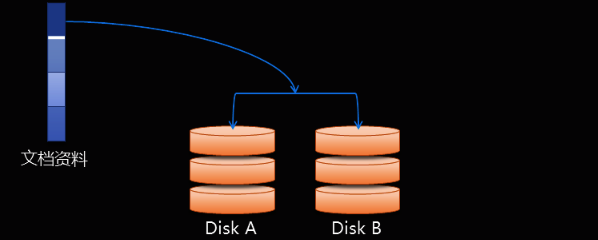
**RAID 0 条带模式**

**同一文档分散存放在不同的磁盘 并行写入以提高效率 至少需要两块磁盘**

****

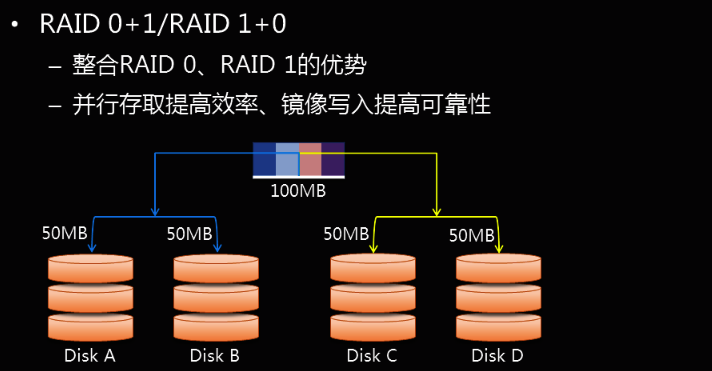
**RAID 1 镜像模式**

**一个文档复制成多份，分别写入不同磁盘 可靠性提高 效率无提升 至少需要两块磁盘**

****

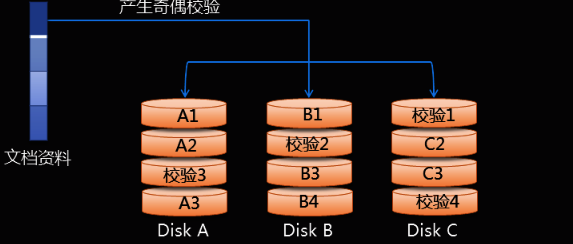
**RAID 0+1 / RAID 1+0**

**整合RAID 0、RAID 1的优势 并行存取提高效率、镜像写入提高可靠性 至少需要四块磁盘**

****

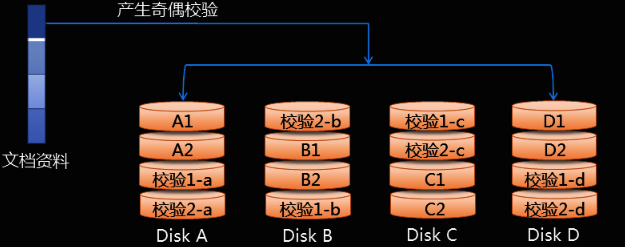
**RAID5 高性价比模式**

**相当于RAID0和RAID1的折中方案 需要至少一块磁盘的容量来存放校验数据 至少需要三块磁盘**

****

**RAID 6 高性价比/可靠模式**

**相当于扩展的RAID5阵列 提供2份独立校验方案 至少需要两块磁盘的容量来存放校验数据 至少需要四块磁盘**

****

**RAID各级别特点对比**

****

**RAID阵列实现方式**

**硬RAID：由RAID控制卡管理阵列**

**-主板 ->阵列卡 ->磁盘 ->操作系统 ->数据**

**软RAID ： 由操作系统来管理阵列**

**-主板 -> 磁盘 -> 操作系统 -> RAID软件 -> 数据**

**进程**

**查看进程树pstree[选项] [PID或用户名] -a 显示完整的命令行 -p 列出对应的PID编号**

**查看进程快照 ps [选项]**

**- aux ： 显示当前终端进程(a) 当前用户在所有终端下的进程（x）以用户格式输出(u)**

**-elf : 显示系统内所有进程(-e) 以长格式输出(-l) 信息、包括最完整的进程信息(-f)**

**Ps aux 列出正在运行的所有进程**

**2018-11-27 15-26-37 的屏幕截图**

**Ps -elf 列出正在运行的所有进程**

**2018-11-27 15-26-55 的屏幕截图**

**进程动态排名**

**Top 交互式工具**

**Top [-d 刷新秒数] [-U 用户名]**

**Top 交互操作指令**

**-? 查看帮助（列出可用的按键） - T 根据进程消耗的TIME降序排列**

**- P、M 根据%CPU、%MEM降序排列 -k 杀死指定的进程 -q ： 退出top程序**

**Pgrep 『选项』 ....查询条件**

**-l 输出进程名 而不仅仅是 PID -U 检索指定用户的进程**

**-t 检索指定终端的进程 -x 精确匹配完整的进程名**

**在命令行的末尾添加 & 不占用当前终端**

**Jobs [-l]命令 查看后台任务列表**

**Fg 命令 将后台任务恢复到前台运行 bg激活后台被挂起的任务**

**日志的功能**

**记录系统、程序运行中发生的各种事件 通过日志、了解及排除故障 信息安全控制的依据**

**由系统服务rsyslog统一记录/管理**

**- 日志消息采用文本格式 -主要记录事件发生的时间、主机 进程 内容**

**常见的日志文件**

**/var/log/messages 记录内核消息、各种服务的公共消息**

**/var/log/dmesg 记录系统启动过程的各种消息**

**/var/log/cron 记录与cron计划任务相关的消息**

**/var/log/maillog 记录邮件收发的相关消息**

**/var/log/secure 记录访问限制相关的安全消息**

**用户日志**

**由登陆的程序负责记录/管理**

**-日志消息采用二进制格式 -记录登陆用户的时间 来源 执行的命令等信息**

**/var/log/lastlog 记录最近的用户登陆事件**

**/var/log/wtmp 记录成功的用户登陆/注销事件**

**/var/log/btmp 记录失败的用户登陆事件**

**/var/log/utmp 记录当前登陆的每个用户的相关消息**

**查看文本日志消息**

**专用分析工具 Webmin系统管理套件 Wsbalizer AWStats 等日志统计套件**

**用户登陆分析**

**Users who w 查看已登陆的用户信息 详细度不同**

**Last lastb 查看最近的登陆成功/失败的用户信息 last -数字**

**日志消息的优先级**

**Linux内核定义的事件紧急程度**

**分为0~7共八种优先级别 其数值越小，表示对应事件越紧急重要**

**0 EMERG(紧急) 会导致主机系统不可用的情况**

**1 ALERT (警告) 必须马上采取措施解决的问题**

**2 CRIT (严重) 比较严重的情况**

**3 ERR (错误) 运行出现错误**

**4 WARNING (提醒) 可能会影响系统功能的事件**

**5 NOTICE (注意) 不会影响系统但是值得注意**

**6 INFO (信息) 一般信息**

**7 DEBUG (调试) 程序或系统调试信息等**

**使用journalctl工具**

**提取由systemd-journal服务收集的日志 - 主要包括内核/系统日志 服务日志**

**常见用法**

**- Journalctl | grep 关键词 -journalctl -u 服务名 [-p 优先级]**

**- journalctl -n 信息条数**

**- journalctl --since=”yyyy-mm-dd hh:mm:ss” --until=”yyyy-mm-dd hh:mm:ss” 圈定时间范围查看**

**Rsync 远程同步 支持本地复制或者与其它SSH。Rsync主机同步**

**- rsync [选项] 源目录 目标目录**

**同步与复制的差异**

**复制：完全拷贝源到目标 同步：增量拷贝,只传输变化过的数据**

**本地同步**

**- rsync [选项..] 本地目录1 本地目录2 //同步整个文件夹**

**- rsync [选项..] 本地目录1 本地目录2 // 只同步目录下的数据**

**Rsync操作选项**

**-n 测试同步过程，不做实际修改 --delete 删除目标文件夹内多于的文档**

**-a 归档模式 相当于-rlptgoD -v 显示详细操作信息**

**-r 递归包括目录子目录及所有文件 -z 传输过程中启用压缩解压**

**-l 保留符号连接文件**

**-p -t 保留文件的权限 时间标记**

**-o -g 保留文件的属主属组标记**

**-D 保留设备文件及其它特殊文件**

**列出ssh服务资源 rsync user@host:远程目录/**

**与远程的SSH目录保持同步**

**下行： rsync [...] user@host:远程目录 本地目录**

**上行： rsync [...] 本地目录 user@host:远程目录**

**同步的实时性**

**按照固定周期定期同步**

**-时间间隔不好固定 同步不及时或资源浪费 -实时性较差**

**Linux 内核的inotify机制**

**-提供事件响应式的文件系统通知机制 安装inotify-tools控制工具可用**

**基本用法 -inotifywait [选项] 目标文件夹**

**-m 持续监控(捕获一个事件后不退出) -r 递归监控 包括子目录和文件**

**-q 减少屏幕输出信息 -e 指定监控的modify move create delete attrib 事件**

**当文档出现监视事件时 会立即给出相应提示**

**利用while循环来反复检查单次监控结果**

**While inotifywait监控操作**

**do**

**需要执行的rsync同步操作**

**Done**