**split分离解析**

分离解析概述

什么是分离系统

当收到客户机的DNS查询请求的时候

能够区分出客户机的来源地址

为不同类别的客户机提供不同的解析结果（IP地址）

根据客户端的不同，解析同一域名，得到的解析结果不同

目的：为客户端提供网络最近的服务器资源

典型适用场景

访问压力大的场景，购买CDN提供的内容分发系统

在全国各地/不同网络内部署大量镜像服务节点

针对不同的客户机就近提供服务器

BIND的view视图

根据源地址集合将客户机分类

不同客户机获得不同结果（待遇有差别）

注意：同一区域在多个视图内分别定义，其地址库文件相互独立，从而实现解析分离的结果；定义view视图后，不允许在view以外出现zone配置。

1. 由上到下依次匹配，匹配即停止
2. 使用view时，所有客户端必须中分类中
3. 所有的zone都必须在view中
4. 每一个view中的zone必须相同

view “联通” {

match-clients { 来源地址1;...;};

zone “12306.cn” IN {

地址库1;

};

};

view “铁通” {

match-clients { 来源地址1;...;};

zone “12306.cn” IN {

地址库1;

};

};

acl地址列表，简化match-clients

为大批量的客户机地址建立列表

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”

acl “liantong” {

IP地址1;IP地址2;...

网段1;网段2;...

};

acl “tietong” {

IP地址3;IP地址4;...

网段3;网段4;...

};

配置分离解析

案例需求及要点

环境及需求

权威DNS：svr7.tedu.cn 192.168.4.7

负责区域：tedu.cn

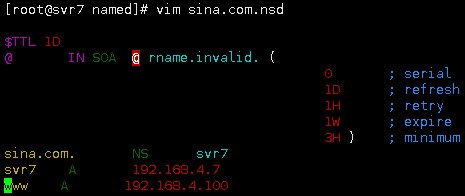
192.168.4.207、192.168.7.0/24---》192.168.4.100

其他地址----》1.2.3.4

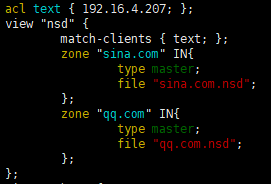
基本配置步骤

1. 建立2份地址库文件

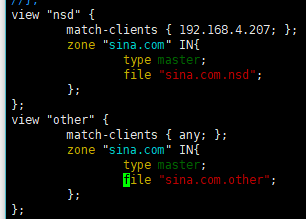




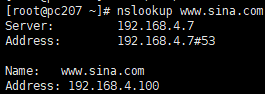
1. 针对来源地址定义acl列表

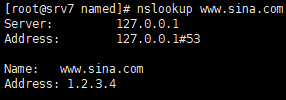


1. 配置2个view，调用不同的地址库

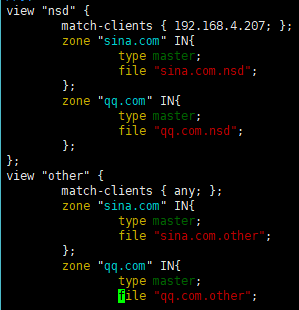


1. 重启named服务
2. 测试分离结果





多区域的分离解析



**RAID磁盘阵列**

RAID磁盘阵列

RAID阵列概述

廉价冗余磁盘阵列RAID，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

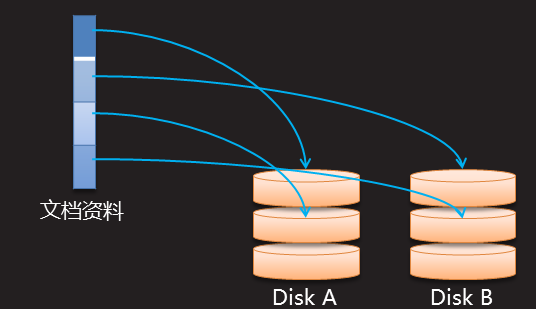
RAID0/1/10

RAID0，条带模式

同一文档分散存放中不同磁盘

并行写入以提高效率

至少由两块磁盘组成

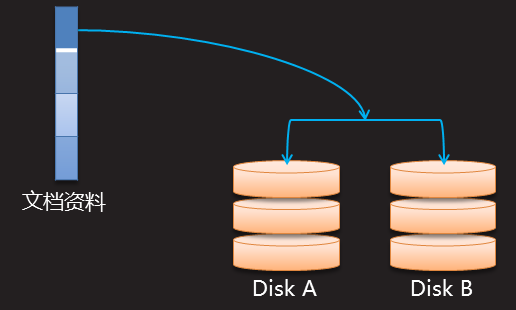


RAID1，镜像模式

一个文档复制成多份，分别写入不同磁盘

多份拷贝提高可靠性，效率无提升

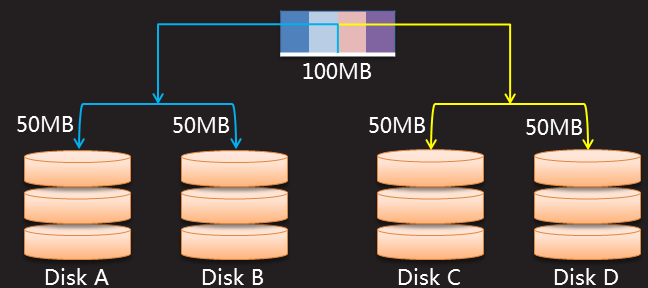
有完全备份



RAID0+1/RAID1+0

整合前两者的优势

并行存取提升效率、镜像写入提高可靠性

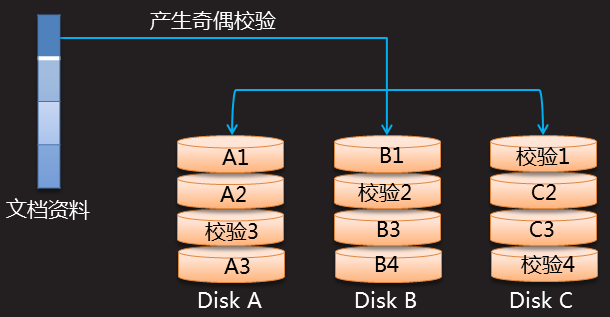


RAID5/6

RAID5，高性价比模式

相当于RAID0和RAID1的折中方案

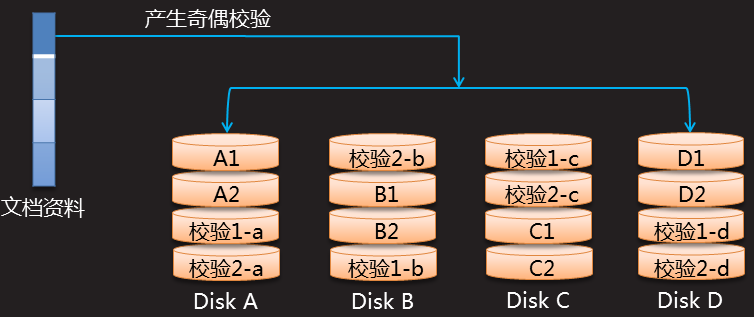
需要至少一块磁盘的容量来存放校验数据



RAID6，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

需要至少两块磁盘的容量来存放校验数据



RAID各级别特点对比

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 对比项 | RAID0 | RAID1 | RAID10 | RAID5 | RAID6 |
| 磁盘数 | ≥2 | ≥2 | ≥4 | ≥3 | ≥4 |
| 存储利用率 | 100% | ≤50% | ≤50% | n-1/n | n-2/n |
| 校验盘 | 无 | 无 | 无 | 1 | 2 |
| 容错性 | 无 | 有 | 有 | 有 | 有 |
| IO性能 | 高 | 低 | 种 | 较高 | 较高 |

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

**进程管理**

**程序：动态的代码，占用的是CPU 内存**

**进程：静态的代码，占用的是磁盘空间**

**唯一标识：PID**

**父进程与子进程：树形结构，一个父进程多个子进程，父进程消亡，子进程也不会存在，systemd是所有进程的父进程**

查看进程

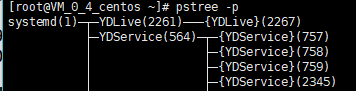
查看进程树pstree

格式：pstree [选项] [PID或用户名]

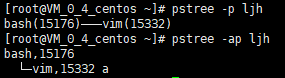
常用选项：

-a：显示完整的命令行

-p：列出对应PID编号









查看进程快照ps

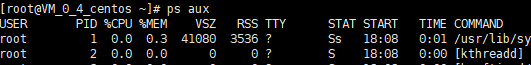
格式：ps [选项]...

常用选项：

aux：显示当前终端所有进程（a）、当前用户在所有终端下的进程（x），以用户格式输出（u）

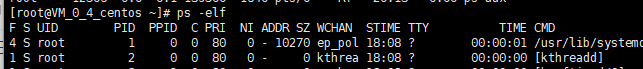
-elf：显示系统内所有进程（-e）、以长格式输出（-l）信息、包括最完整的进程信息（-f）

列出当前终端正在运行的所有进程：



用户 进程ID CPU占用率 内存占用率 占用的虚拟内存 占用的固定内存 终端 状态 起始时间 CPU时间 程序指令

列出系统正在运行的所有进程



PPID：父进程的PID号 PRI/NI：进程优先级，数值越小优先级越高

进程动态排名top交互式工具

格式：top [-d 刷新秒数] [-U 用户名]





第一行：系统时间；系统运行了多长时间；正在登陆用户数量（有几个终端远程登陆）；平均值（CPU负载量平均值）：1分钟，5分钟，15分钟

第二行：进程数量；正在运行的数量；睡眠的进程；停止进程；僵尸进程（占资源）

第三行CPU：us用户占用资源百分比；sy系统内核占用资源百分比；ni运行已调整优先级的用户占用资源百分比；id空闲CPU百分比；wa用于等待IO完成占用资源百分比；hi处理硬件终端占用资源百分比；si处理软中断所占用的资源；st；这个虚拟机被hypervistor偷取所占用的资源（这行数据均为CPU数据并以百分比格式显示，例如“97.1id”意味着有97.1%处于空闲）

第四行（内存）：共有多少内存；剩余；用了；作为内核缓存的内存量

第五行（缓存）：共有多少缓存；剩余；用了；已被提前加载的内存量

top交互操作指令

?：查看帮助（列出可用的按键指令）

1. M：根据%CPU、%MEM降序排列

T：根据消耗进程的TIME降序排列

k：杀死指定的进程

q：退出程序

检索进程pgrep（包含就算）

格式：pgrep [选项]... 查询条件

常用选项

-l：输出进程名，而不仅仅是PID



-U：检索指定用户进程



-t：检索指定终端的进程



-x：精确匹配完整的进程名



控制进程

进程的前后台调度

前台启动：输入正常命令行，运行期间占用当前终端

后台启动：在命令行末尾添加“&”符号，不占用当前终端

ctrl+z组合键：挂起当前进程（暂停并转入后台）

jobs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（默认为最近1个任务 后面可以接任务序号）

bg命令：激活后台被挂起任务（默认为最近1个任务 后面可以接任务序号）

杀死进程

干掉进程的不同方法

ctrl+c，中断当前命令程序

kill [-9] PID...、kill [-9] %后台任务编号（只能杀死一个进程）

killall [-9] 进程名（杀死多个进程）

pkill 查找文件（包含就算，误杀几率较高）

-9代表强制杀，不加-9进程自己衰亡

killall -9 -u 用户名 杀死该用户开启的所有进程

**日志管理**

日志概述

日志的功能

系统和程序的“日记本”

记录系统、程序运行中发生的各种事件

通过查看日志，了解及排除故障

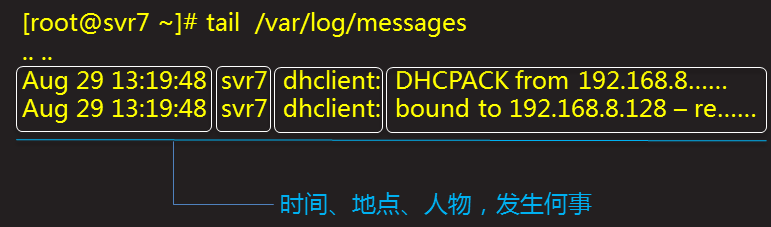
信息安全控制的“依据”

内核及系统日志

由系统服务rsyslog统一记录/管理

日志系统采用文本格式

主要记录事件发生的时间、主机、进程、内容



常见的日志文件

|  |  |
| --- | --- |
| 日志文件 | 主要用途 |
| /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信息 |
| /var/log/cron | 记录与cron计划任务相关的消息 |
| /var/log/maillog | 记录邮件收发相关的消息 |
| /var/log/secure | 记录与访问限制相关的安全信息 |

用户日志文件

由登录程序负责记录/管理

日志消息采用二进制格式

记录登录用户的时间、来源、执行的命令等信息

|  |  |
| --- | --- |
| 日志文件 | 主要用途 |
| /var/log/lastlog | 记录最近的用户登录事件 |
| /var/log/wtmp | 记录成功的用户登录/注销事件 |
| /var/log/btmp | 记录失败的用户登录事件 |
| /var/run/utmp | 记录当前登录的每个用户的相关信息 |

日志分析

查看文本日志消息

通过分析工具

tail、tailf（实时跟踪日志信息）、less、grep等文本浏览/检索内容

awk、sed等格式化过滤工具

专用分析工具

webmin系统管理套件

webalizer、awstats等日志统计套件

用户登录分析

user、who、w命令

查看已登录的用户信息，详细度不同

last（最近登录成功）、lastb（最近登录失败）命令

查看最近登录成功/失败的用户信息

日志消息的优先级

linux内核定义的时间紧急程度

分为0-7共8种优先级别

0 EMERG（紧急） 会导致主机系统不可用的情况

1 ALTER（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时间

5 NOTICE（注意） 不会影响系统但值得注意

6 INFO（信息） 一般信息

7 DEBUG（调试） 程序或系统调试信息等

其数值越小，表示对应时间越紧急/重要

使用journalctl工具

提取由systemd-journal服务搜集的日志

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 消息条数

journalctl --since=”yyyy-mm-dd HH:MM:SS” --until=”yyyy-mm-dd HH:MM:SS”