进程 1.程序：静态的代码，仅仅占用磁盘空间 2.进程：正在运行的代码，会占用CPU与内存 进程唯一标识编号：PID

RAID廉价冗余磁盘阵列：较小/低速的磁盘整合成一个大磁盘使用的一种存储技术

RAID 0,条带模式(2块硬盘) RAID 1,镜像模式 (2)RAID5,高性价比模式 (3)RAID6,高性价比/可靠模式(4)

日志管理：由系统服务rsyslog统一记录/管理

/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 记录邮件收发相关的消息

/var/log/secure(authpriv) 记录与访问限制相关的安全消息

内核及系统日志：由系统服务/etc/rsyslog.conf同一管理，格式相似

用户日志：记录用户登录及退出系统的事件

程序日志：由各种服务/程序独立管理，格式不统一

日志分析： 通用分析工具

– tail、tailf、less、grep等文本浏览/检索命令

– awk、sed等格式化过滤工具

Linux内核定义的日志事件紧急程度 1. 0~7 共8种优先级别 2.其数值越小,表示对应事件越紧急/重要（ERR 和 WARNING）

0 EMERG（emerg） （紧急） 会导致主机系统不可用的情况

1 ALERT(alert) （警告） 必须马上采取措施解决的问题

2 CRIT(crit) （严重） 比较严重的情况

3 ERR(err) （错误） 运行出现错误

4 WARNING(warning)（提醒） 可能会影响系统功能的事件

5 NOTICE(notice) （注意） 不会影响系统但值得注意

6 INFO(info) （信息） 一般信息

7 DEBUG(debug) （调试） 程序或系统调试信息等

systemctl控制：1.内核引导之后加载的第一个初始化进程(PID=1) 2. 负责掌控整个Linux的运行/服务资源组合

私有IP地址分类

• A类 10.0.0.0~10.255.255.255

• B类 172.16.0.0~172.31.255.255

• C类 192.168.0.0~192.168.255.255

数据包： 数据 源ip地址 目标IP地址 目标端口号

互联网常见协议：三次握手四次断开

传输层的协议：1.TCP（传输控制协议）：可靠的、面向连接的协议 传输效率低 （三次握手与四次断开）

syn ack，syn ack fin ack fin ack SYN请求连接 FIN请求断开 ACK同意

SSH FTP POP3 SMTP DNS HTTP Telnet

2.UDP（用户数据报协议）：不可靠的、无连接的服务 传输效率高 （小文件）

TFTP DNS NTP

DNS：递归用UDP协议 迭代用TCP协议

FTP：文件传输协议 默认端口号:21（和一个随机端口） TFTP：简单的文件 传输协议 默认端口号:69

ssh:加密远程管理 默认端口号:22 telnet:明文远程管理协议 默认端口号：23

SMTP：用户发邮件协议 默认端口号:25 DNS：域名解析协议 默认端口号:53

DHCP（动态IP协议）：udp 67（客户）和68（服务） redis:6379

pop3：用户收邮件协议 默认端口号:110 NTP：网络时间协议 默认段口号：123

imap：升级版用户收邮件协议 默认端口143 SNMP：网络管理协议 默认端口号:161

http：超文本传输协议 默认端口号:80 https：安全的超文本传输协议 默认端口号:443

iscsi：网络磁盘 默认端口号：3260 mariadb数据库服务器： 默认端口 3306

PHP ： 超文本预处理器 默认端口：9000 samba：137 138 139

tomcat：默认端口：8080 8009 ssl:8443 memcached:11211

ceph :6789

协议的端口可以有root改变，也可以具备多个端口

客户端访问服务端资源：

1.防火墙策略 1.1 区域 1.2区域服务

2.服务（软件）本身的访问控制

3.安全增强SELinux 3.1运行模式 3.三大策略

4.服务端本地目录的权限

请写出DNS常见的资源解析记录？

NS（名词服务器） A（主机） CNAME（别名）

作用域---->地址池---->租期----

网络装机PXE, – 预启动执行环境,在操作系统之前运行 – 可用于远程安装

部署 DHCP服务 1. 装软件包 dhcp• 配置文件 /etc/dhcp/dhcpd.conf • 起服务 dhcpd

一个网络中只能有一个DHCP服务器 yum provides \*/pxelinux.0 #查询仓库中那个软件包产生

字符模式：multi-user.target 图形模式：graphical.target

systemctl isolate graphical.target systemctl set-default graphical.target

systemd 一个更高效的系统&服务管理器– 开机服务并行启动,各系统服务间的精确依赖

2.tftp 3.syslinux 4.挂载 5.httpd 6.挂载 7.system-config-kickstart

虚拟Web主机 作用：一台服务器，提供多个不同的Web页面

区分方式

– 基于域名的虚拟主机

– 基于端口的虚拟主机

– 基于IP地址的虚拟主机

Web服务器提供的默认配置

– Listen:监听地址:端口(80)

– ServerName:本站点注册的DNS名称(空缺)

– DocumentRoot:网页根目录(/var/www/html）（文档 根）

– DirectoryIndex:起始页/首页文件名(index.html)

安全的Web服务器

Public Key Infrastructure,公钥基础设施

– 公钥:主要用来加密数据

– 私钥:主要用来解密数据(与相应的公钥匹配)

– 数字证书:证明拥有者的合法性/权威性(单位名称、有效期、公钥、颁发机构及签名、......)

– 数字证书授权中心:负责证书的申请/审核/颁发/鉴定/撤销等管理工作

邮件服务：1.安装 postfix软件 2.修改主配置文件/etc/postfix/main.cf

（myorigin，inet\_interfaces，mydestination）3.重起

发信操作1.mail -s '邮件标题' -r 发件人 收件人[@收件域]...

echo haha | mail -s 'test' -r yg xln

收信操作1.mail [-u 用户名]

系统安全保护Security-Enhanced Linux：增强Linux系统安全的强制访问控制体系

SELinux的运行模式 1. enforcing(强制)、permissive(宽松) 2. disabled(彻底禁用)---->12切换须重起

查看：getenforce 临时切换:setenforce 1|0 – 修改固定配置（固定切换）:/etc/selinux/config 文件

selinux布尔值: 查看 getsebool -a | grep httpd 修改 setsebool samba\_export\_all\_ro on

安全上下文 chcon [-R] --reference=模板目录 新目录 (ls -Zd semanage --man fcontext)

非默认端口的开放semanage port -a -t http\_port\_t -p tcp 8909(semanage port -l | grep http)

数据库服务基础：存放数据的仓库

一、部署mariadb数据库服务器，默认端口 3306 1.安装mariadb-server:提供服务端有关的系统程序

2.配置 /etc/my.cnf（skip-networking） 3.重起

二、数据库简单的使用：运行mysql 增 insert 删 delete 改 update 查select

1.mysqladmin [-u用户名] [-p[旧密码]] password '新密码'

2.show databases; 3.create database nsd1808; 4.drop database nsd1808;

5.mysql -u root -p123 nsd < users.sql 6.use nsd; 7.show tables; 8.select \* from base;

9.select \* from base where password='123'; 10. desc 表名 ##查询表结构

11.select count(\*) from base,location where base.name='Barbara' and (or)

location.city='Sunnyvale' and base.id=location.id;

12.grant select on nsd.\* to lisi@localhost identified by '123';

13.insert base values ('6','Barbara','123456');

14.delete from user where password=''; 15.flush privileges; #刷新数据所有策略

16.禁止监听,只服务于本机vim /etc/my.cnf --->[mysqld] skip-networking //跳过网络监听

17 exit

查看网卡名:nmcli connection show

添加以太网卡 : nmcli connection add type ethernet con-name eth1 ifname eth1

配置永久的IP地址、子网掩码、网关地址:nmcli connection modify 'System eth0' ipv4.method manual ipv4.addresses '172.25.0.110/24 172.25.0.254' connection.autoconnect yes

激活配置 nmcli connection up 'System eth0'

专用于查看链路聚合的命令 teamdctl team0 state

配置聚合连接(链路聚合) 查看网卡名： nmcli connection show

先添加连接# nmcli con add con-name 连接名 ifname 网卡名 type ethernet

1.创建虚拟网卡team0: nmcli connection add type team con-name team0 ifname team0

autoconnect yes config '{"runner": {"name": "activebackup"}}'

('{"runner": {"name": "activebackup"}}'------>参考 man teamd.conf-->/example)

2.添加成员:nmcli connection add type team-slave con-name team0-1 ifname eth1 master team0

nmcli connection add type team-slave con-name team0-2 ifname eth2 master team0

3. 为虚拟网卡team0配置IP地址 : 正常配置

4.激活配置nmcli connection up team0 (team0-1 team0-2)

切换真实网卡 ：ifconfig eth1 down

删除team0（team0-1）配置： nmcli connection delete team0（team0-1）

TCP/IP是最广泛支持的通信协议集合：32个二进制位.表示为4个十进制数,以 . 隔开

– 包括大量Internet应用中的标准协议

– 支持跨网络架构、跨操作系统平台的通信

作用:用来标识一个计算机

私有IP地址分类

A类 10.0.0.0~10.255.255.255

B类 172.16.0.0~172.31.255.255

C类 192.168.0.0~192.168.255.255

分类：A类:1 ~ 127 /8 网+主+主+主

– B类:128 ~ 191 /16 网+网+主+主

– C类:192 ~ 223 /24 网+网+网+主

– D类:224 ~ 239 组播

– E类:240 ~ 254 科研专用

子网掩码：区分IP地址的网络位与主机位，用二进制的1表示网络位，用二进制的0表示主机位

什么是网关（跨网络通信时，会用到网关）

1.从一个网络连接到另一个网络的“关口” 2.通常是一台路由器,或者防火墙/接入服务器

完整Linux系统：Linux内核 + 各种应用软件

Linux是一种操作系统!! 操作系统:一堆软件的集合

Linux系统内核作用： 操控所有计算机硬件

通配符:\*:任意多个任意字符 ?:单个字符

[a-z]:多个字符或连续范围中的一个,若无则忽略 – {a,min,xy}:多组不同的字符串,全匹配

磁盘分类：hd,表示IDE设备 sd,表示SCSI设备 vd,表示虚拟化设备

zip归档工具,跨平台的压缩工具

归档+压缩操作: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]

tar备份与恢复 归档及压缩：1.零散的文件归成一个 2.占用硬盘空间变小

制作归档及压缩 格式：tar 选项 /路径/tar包名字 /路径/源文件 /路径/源文件(zcf jcf Jcf)

解包 格式：tar 选项 /路径/tar包名字 /路径/释放的位置(xf C)

查看 （tf）

-c:创建归档 -x:释放归档 -f:指定归档文件名称 -z、-j、-J:调用 .gz、.bz2、.xz 格式的工具进行处理

-t:显示归档中的文件清单 -C（大写）:指定释放位置 -P（大写）绝对路径释放/压缩

配置永久的IP地址、子网掩码、网关地址:nmcli connection modify 'System eth0' ipv4.method manual ipv4.addresses '172.25.0.110/24 172.25.0.254'（网关 ipv4.gateway (7.2以上) ipv4.dns） connection.autoconnect yes

激活配置 nmcli connection up 'System eth0'

cron周期性计划任务：1.软件包:cronie、crontabs 2.系统服务:crond 3.日志文件:/var/log/crond

\*:匹配范围内任意时间 ,:分隔多个不连续的时间点 -:指定连续时间范围 /n:指定时间频率,每n

crontab （-e-r-l）（加减查） -u root （分时日月周 任务命令行）

3-5 3,5 \*/3 ##日期设置

Shell脚本：脚本：一个可以运行文件，可以实现某种功能

一般组成：1.#! 环境声明(以下的代码有那个程序进行翻译) 2.# 注释文本 3.可执行代码

read : -p ：屏幕的提示信息

1.产生交互

2.记录用户在键盘上的输入

3.将记录的信息赋值给变量

变量：重复使用，多变环境。变量名=变量值(1.引用变量值:$变量名2.查看变量值:echo $变量名、 echo ${变量名})

种类：1.环境变量：变量名一般都大写，系统定义完成用户直接使用 USER：当前用户名 PATH：存储命令程序的路径

2.位置变量:由系统定义完成，用户直接使用,非交互式（$1 $2 ${1} ${2}...）

3.预定义变量:由系统定义完成，用户直接使用($#输入变量个数 $\*输出所有位置变量的值 $? 退出状态值0和非0)

4.自定义变量:用户自主设置、修改及使用

常用的测试选项

检查文档状态

-e:文档存在为真 -d:文档存在,且为目录才为真 -f:文档存在,且为文件才为真

-r:文档存在,且具备读取权限才为真 -w:文档存在,且具备写入权限才为真-x:文档存在,且具备执行权限才为真

比较整数大小

-gt：大于 -ge：大于等于 -eq：等于 -ne：不等于 -lt：小于 -le：小于等于

字符串比对

==:两个字符串相等为真 !=:两个字符串不相等为真

if多分支处理

if [条件测试1];then

命令序列xx

elif [条件测试2];then

命令序列yy

elif [条件测试3];then

命令序列cc

......

else

命令序列zz

fi

for循环结构：循环:让计算机重复执行一个操作 造数：{起始数值..结束数值}

for 变量名 in 值列表

do

命令序列

done

防火墙： 隔离作用 系统服务:firewalld 管理工具:firewall-cmd、firewall-config（图形化）

根据所在的网络场所区分,预设保护规则集：1.public:仅允许访问本机的ssh、ping、dhcp服务

2.trusted:允许任何访问 3.block:阻塞任何来访请求，明确拒绝 4.drop:丢弃任何来访的数据包，直接丢弃

查看（修改）默认区域：firewall-cmd --get（set）-default-zone（=public）

重新加载防火墙配置：firewall-cmd --reload

列出 public区域中规则：firewall-cmd --zone=public --list-all

临时（永久）添加服务：firewall-cmd （--permanent） --zone=public --add-service=http

单独拒绝172.25.0.10访问：firewall-cmd --permanent --zone=block --add-source=172.25.0.10

实现本机的端口映射：访问两个地址可以看到相同的页面：

firewall-cmd --permanent --zone=trusted --add-forward-port=port=5423:proto=tcp:toport=80

IPv4地址：32个二进制组成,利用点分隔,用4个十进制数表示

IPv6地址：128个二进制组成,利用冒号分隔8部分, 最终每一部分利用4个16进制数表示

每段内连续的前置 0 可省略、连续的多个 : 可简化为 ::

Cobbler装机平台 1.配置cobbler vim /etc/cobbler/settings

2.配置cobbler的dhcp vim /etc/cobbler/dhcp.template

3.绝对路径解压 tar -P

cobbler import --path=挂载点 --name=导入系统命名（随意起） ####导入安装镜像数据

cobbler导入的镜像放在：/var/www/cobbler/ks\_mirror

网络自动装机PXE：DHCP服务器 装软件包 dhcp ---起服务 dhcpd ---配置文件 /etc/dhcp/dhcpd.conf

（next-server 192.168.4.7;#指定下一个服务器地址 filename "pxelinux.0";})

tftp：简单的文件传输协议69 安装软件包tftp-server tftp服务 提供默认共享路径：/var/lib/tftpboot/

3.下载syslinux (cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot/)

4.挂载 （cp /mnt/isolinux/isolinux.cfg /var/lib/tftpboot/pxelinux.cfg/default)

（1.vmlinuz 2.initrd.img 3.vesamenu.c32 4.splash.png---->启动内核，驱动程序，图形模块，背景图）

5.安装httpd 6.挂载（软件包共享）

7.安装图形的工具(system-config-kickstart) --> 无人值守安装，生成应答文件-->指定ks.cfg（/var/www/html）

DT是数据处理技术

DB数据库

数据包： 数据 源ip地址 目标IP地址 目标端口号

互联网常见协议：SNMP：网络管理协议 默认端口号:161

http：超文本传输协议 默认端口号:80 https：安全的超文本传输协议 默认端口号:443

FTP：文件传输协议 默认端口号:21 DNS：域名解析协议 默认端口号:53

SMTP：用户发邮件协议 默认端口号:25 pop3：用户收邮件协议 默认端口号:110

telnet：运程管理协议 默认端口号:23 TFTP：简单的文件传输协议 默认端口号:69

协议的端口可以有root改变，也可以具备多个端口

客户端访问服务端资源：

1.防火墙策略 1.1 区域 1.2区域服务

2.服务（软件）本身的访问控制

3.安全增强SELinux 3.1运行模式 3.2布尔值

4.服务端本地目录的权限

黑色：文件文档 蓝色：目录 红色：压缩包

绿色：可运行程序 青色：快捷方式

/ 根目录：所有的数据都是放在此目录下（Linux系统的起点）

/opt 存放外载软件包或程序

/var/www/html/index.html(vim):网页文件默认存放路径

/var/ftp:默认共享数据路径

/etc/selinux/config :SELinux固定配置文件

/dev 存放与设备相关资料

/home：存放所有普通用户的家目录

/root 管理员的家目录

/proc:所占用的空间不是硬盘，而是内存

/var：存放经常变化的数据（/var/log：存放日志文件）

/dev/null:黑洞设备,专用于收集无用的信息