tcp/ip

三次握手：syn,syn ack,ack 四次断开：fin,ack, fin ack , ack

四次断开需要保证用户已经传输完数据

ls pwd cd mv cp rm cat vim less man scp grep

find -type 类型(f文本文件、d目录、l快捷方式)-name -user -group -size +|- -iname -maxdepth mtime +|-

find .. .. -exec 处理命令 {} 路径 \;

基本权限：rwx--->chmod 设置文档归属： chown [R] 主:组 隐藏权限：lsattr、chattr

附加（特殊）权限：s新增的子文档，自动继承父目录的所属组s让使用者具有文件属主的身份及部分权限t阻止用户滥用写入

acl访问策略setfacl -m

tar -zPcf/-jPcf/-JPcf /路径/\*.tar.gz/bz2/xz /路径/源文件 /路径/源文件

tar -xPf /路径/tar包名字 -C /路径/指定释放位置

存储引擎，备份，授权，子查询（嵌套查循），匹配条件

awk工具：支持按列输出，内置变量

shell函数，可以避免代码重复，将大的工程分割成若干个小的功能模块，代码可读性更强

日志格式

awk '{ip[$1]++}END{for(i in ip){print ip[i],i}}' /var/log/httpd/access\_log | sort -nr---$1（列）可变

--without-模块名 禁用nginx不需要的模块

svn:代码管理，文档管理

nginx：添加server容器实现虚拟主机功能 动静分离 匹配用户地址栏 模块化 依赖包 系统检查和配置

添加启动用户 部署环境 配置 服务器池 实现 集群池属性 配置调度算法 设置调度规则

平滑升级 内存(硬盘) 运行内存 线程共享进程内存 认证提示符 密码文件

源码安装（5）---升级（5）----用户认证1（auth\_basic\_user\_file）.2（htpasswd）

----虚拟主机（添加server容器实现虚拟主机功能）----ssl 1（openssl）2（ssl.server容器）

-----LNMP1.2（~ \.php$）（fastcgi\_pass）---地址重写

rewrite ^/(.\*)$ http://www.tmooc.cn/$1；

mv /usr/local/nginx/sbin/nginx{,.bak}

参数 连通性 区域 结构 活跃 备份 虚拟

客户端访问速度慢：家用路由器，服务器并发量，对页面进行压缩处理，服务器内存缓存，数据存储位置

客户端输入域名---DNS解析---网络访问服务器ip（传输层）---网络层---数据链路层---服务器（物理层）-----nginx网页设置（并发量）

Memcached 是一个高性能的分布式内存对象缓存系统,用于动态Web应用以减轻数据库负载

mencache: session cookie

nginx: 用户认证，反向代理 LNMP

http: ssl(tls)

tomcat:java(openjdk)

实时同步：rsync+inotifywait工具（rsync -avz(n) --delete + inotifywait -rqm）

热备份路由选择协议（HSRP）：备份网关（数据走向） 优先级范围0～255，默认100 越大越优先

动态路由协议OSPF协议（开放式最短路径优先）OSPF区域

DHCP：动态主机配置协议

selinux布尔值：getsebool -a

安全上下文 chcon [-R] --reference=模板目录 新目录

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

vlan：虚拟局域网 物理设备上连接的不受物理位置限制的用户的一个逻辑组（非物理形式）（分割广播域）。

优点：1. 广播控制 2. 增加安全性 3. 提高带宽利用 4.降低延迟----4096

svi：交换虚拟接口（vlan接口）

trunk 中继链路（给不同vlan数据帧打上vlan标记（IEEE 802.1Q））

NAT（网络地址转换）的作用：优点 1.节省公有合法IP地址 2.处理地址重叠 3.安全性

缺点 1.延迟增大 2.配置和维护的复杂性

静态转换，端口多路复用PAT

acl：访问控制列表（标准1～99，拓展100～199）

STP（生成树协议）：生成树算法（基于vlan，1个vlan一个STP）.逻辑上断开环路,防止广播风暴的产生 2.备份线路

网桥优先级：取值范围:0 ~ 65535 网桥ID(BID)越小越优先

服务器：企业级+机架式2U+机柜42U+CPU+内存插槽+硬盘接口+raid卡+IBM（dell）

1U=1.75英寸=4.445厘米（通常1-2U）两台设备空1U左右

Yum软件包仓库，自动解决依赖关系 yum-config-manager --add

1.众多的软件包 2.仓库清单文件（repodata）3.构建Web服务或FTP服务传递数据

sed的用法：sed 选项 '/条件/指令' 文件.. ..

awk提取文本:awk 选项 ' BEGIN{指令} /条件/{指令} END{指令}' 文件

云计算：云中的计算机，云计算提供云服务，按需按量收费，节约成本。节约资源（用才给）

服务器：能够为其他计算机提供服务的更高级电脑

tcp/ip最广泛支持的通讯协议集合：支持跨网架，跨系统平台通信。表示一台计算机（节点的网络地址）（5类）

网关：不同网络通信关口（路由器或者防火墙/接入服务器） route -n

unix-->linux(linux torwalds)（基本哲学理念：一切皆文件）（red hat suse debian ubuntu）

centos：社区企业操作系统

内核：管理CPU（lscpu）/内存（cat /proc/meminfo） 驱动基本硬件，文件系统 ( + 外围软件 （uname -r）（

/boot/vmlinuz-\*）

硬盘：查看---分区（MBR，GPT）(刷新：partprobe)---格式化---挂载（mount -a）---使用(df -Th)

MBR/msdos（fdisk分区工具）：小于2.2T gpt（parted）（gdisk分区工具）：只有主分区

lvm逻辑卷：将众多的物理卷( PV),组成卷组(VG)（PE）,再从卷组中划分出逻辑卷(LV) 可整合与扩容(须更新文件系统)

交换空间（swap）：当物理内存不够用时，使用磁盘空间来模拟内存。

（一定程度缓解内存不足----->交换分区(空闲分区充当交换空间)，交换文件（以文件模拟的设备充当交换空间））

RAID（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，提高效率或硬件级别的数据冗余

不同级别的功能特性各不相同。RAID0条带模式，并行写入提高效率 RAID1镜像模式，多份拷贝。RAID5：3块硬盘 RAID6：4块

虚拟软件：通过 软件模拟真实计算机的一类软件程序（可运行多个虚拟机）

用户账户：方便对用户的（权限）管理（ip 用户名） 组帐号：能批量高效的管理某一类用户

权限：用户类型ugo 基本权限rwx 附加权限sst 权限数值化 xxxx

归档：将众多零散的文件整理为一个文件，大小基本不变 （tar（rd）linux专用，zip可用于windows和linux）

压缩：按某种算法（熵编码和混合编码）减少文件所占空间大小，恢复时按对应逆向算法解压

源码编译安装：获得软件最新版，及时修复bug，软件功能可按需选择/定制，更多软件可供选择，适用各种平台

解压----./configure配置-----编译（make）-----安装（make install）

NTP网络时间协议/同步：NTP服务器为客户机提供标准时间，须保持沟通（chrony）

周期性cron任务：按照设定时间间隔为用户反复执行某一项固定任务。（crontabs）

LDAP网络用户认证：客户端软件包：sssd authconfig-gtk(tui) autofs--->家目录漫游：nfs 网络文件系统

shell脚本：提前设计可执行语句，用来完成特定任务的文件（须有执行权限）。交互式与非交互式

selinux：美国NSA国家安全局主导，一套增强linux系统安全的强制访问控制体系。集成到内核上的（3种模式）

聚合连接（链路聚合）：多网卡组建成的虚拟网卡（备份网卡，提高效率）

查看网络连接：nmcli connection show(down up) "连接名" 修改：nmcli connection modify "连接名" 参数...

samba共享：linux与windows跨平台共享（有共享帐号和密码）（samba）

pdbedit（a增L查x删）：管理（创建）samba共享账户

nfs：linux间的共享平台（nfs-utils）

iscsi网络磁盘：服务器提供磁盘空间，客户机连接并当成本地磁盘使用（backstore:后端存储 target：磁盘组

lun：逻辑单元）iqn 用来识别target磁盘组，也用来识别客户机身份

数据库mariadb：一批数据的集合,主流的数据库多用存放关系型（以二维表格记录大量实体的属性信息）表格数据（mariadb-server mariadb） 数据库管理系统DBMS：管理和操作数据库的大型软件平台

dns：将域名解析成对应的ip地址或将ip解析成对应域名（后者不常用）主配置文件，地址配置文件

特殊DNS解析：1.DNS轮询 2.配置多对一的泛域名解析 3.DNS子域授权（NS） 4.搭建并测试缓存DNS

split分离解析：能够区分客户机的来源地址，为不同类别客户机提供不同解析结果，针对不同客户提供就近服务

（CDN提供的内容分发服务）view视图 和 acl地址列表

web(apache)：基于B/S 架构的网页服务（http html） 主配置文件，调用文件，网页文件

虚拟主机：由一台服务器提供多个不同的Web站点（3种区分方式） 网页根目录运行身份：apache

安全web：https加密传输（mod\_ssl）及访问控制

静态网站的原始网页=浏览器访问到的网站 动态程序转后端模块处理（PHP网页 python网页，jsp网页...）

nginx(nginx):高性能的HTTP和反向代理服务 1.源码模块化下载可平滑升级 2.用户认证 3.虚拟主机 4.加密传输

5.LNMP动静分离 6.地址重写 7.反向代理---tcp/udp调度器

邮件：收发邮件，为用户提供电子邮箱存储空间

日志：记录系统，程序运行中发生的各种事件。通过查看日至，了解及排除故障。信息安全控制的依据

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

（5-system v 6-upstart） 7-systemd开机服务并行启动，各系统服务间精确依赖

PXE网络装机：预启动执行环境，再操作系统之前运行。规模化，自动化，远程实现

（配置DHCP服务，同时再配置文件中指定下一个服务器地址与网卡引导文件名称，TFTP，HTTP）

kickstart无人值守/自动应答：预先提供（配置）应答文件，定义好各种安装设置，免去交互过程，全自动安装，可添加post脚本

快捷键：补全命令:tab ctrl+l ctrl+c alt+. ctrl+u ctrl+z

文件：(un)alias(~/.bashrc) touch grep(-r -v -^ -$) > 2>错 &> >> 2>> &>>

目录：ls pwd cd cp mv mkdir mount（remount umount） find

其他：ssh scp reboot power crontab rpm (q ivh e) yum chmod(R)chown getfacl setfacl 管道|

编辑：vim

文档：通配符\*?[]{} rm

mongodb(默认端口：27017)：分布式文件存储的数据库，为web应用提供可扩展的高性能数据存储解决方案

介于关系和非关系数据库之间的产品，存硬盘、格式不固定，json格式/csv格式

将数据存储为一个文档（类似json对象）,数据结构由键值对组成，一行就是一个文档

支持丰富的查询表达，可以设置任何属性的索引、副本集（集群[操作日志oplog]和主从同步）、支持分片

副本集实现方式：1.Master-Slave主从复制 2.Replica Sets副本集：故障自动切换，自动修复成员节点

Redis(默认端口6379):高性能（key/values）分布式内存(memory)数据库、支持数据持久化，定期保存到硬盘中

支持list、hash、set、zset数据类型及master-slave模式数据备份-----内存清除策略、内存管理部署

redis集群----部署管理主机（ruby脚本提供redis-trib.rb命令）---创建集群----访问集群要访问主库(分布式存储)---管理集群

redis主从服务（slaveof ）---哨兵服务:/etc/sentinel.conf----redis持久化RDB/AOF

RDBMS（关系型数据库)：按照预先设置的组织结构，将数据存储在物理介质上，数据之间可以做关联操作

NOSQL（非关系型数据库）：Redis、MongoDB、Memcached、

SQL：结构化查询语言

SQL键值 ： 普通索引（index） 主键（primary key） 外键（foreign key） 唯一索引（unique） 全文索引（fulltext）

类型：Brtee（二叉树算法） B+tree hash （标志：index普通索引：MUL primary key主键：PRI）

匹配条件，多表查询

完全备份mysqldump、binlog日志实现数据实时增量备份 第三方软件提供的innobackupex命令实现数据的增量备份与恢复

MYSQL存储引擎：myisam innodb memory

DB:数据库 DBMS：数据库管理系统 DBS（主机）：数据库系统（前两个结合）RDBMS：关系型数据库

图形化（浏览器）管理：phpMyAdmin（压缩包）

主从同步，结构模式，复制模式

支持数据读写分离服务（maxscale），实现数据库的高可用（MHA），提供数据分片服务（mycat）

mysql多实例：定义mysql.sock、错误日志 、pid文件、数据库目录、端口

mysql视图：视图不存放数据,只有结构没有数据，数据来自与查询的基表，基表和视图同步更新（算法（查询方式），检查范围）

mysql存储过程:一组为了完成特定功能的sql语句集

源码安装：1.下载依赖包 2.创建执行用户 3.tar解压，进入对应目录，系统检查及配置4.编译成二进制 5.安装到对应目录

平滑升级：1 3 4 src:存放源代码目录

添加server容器实现虚拟主机功能，https传输加密，用户认证，动静分离（LNMP）地址重写，反向七层代理，四层代理

优化：1.自定义错误页面2.查看并定义服务器状态信息3.优化nginx并发量4.优化数据包头（url）5.本地缓存

6.日志切割 7. 页面压缩 8.服务器内存缓存

tomcat+java(jdk ,jsp, servlet, jar war) /usr/local/tomcat/conf/server.xml

memcached(非关系型数据库)是高性能的分布式缓存对象服务器，用来集中缓存数据库查询结果，

减少数据库访问次数，以提高动态Web应用的响应速度cookie session

使用Varnish（CDN）加速Web访问加速、IP伪装 squid代理缓存软件

SVN版本控制工具：subversion是一个自由/开源的版本控制系统，允许你数据恢复到早期版本，

或者是检查数据修改的历史，允许你和别人协作文档并跟踪所做的修改git

VPN（虚拟专用网络）：在公用网络上建立专用私有网络，进行加密通讯，翻墙。

主流VPN技术：（（GRE：linux之间的）PPTP，L2TP+IPSec，SSL）

远程套件工具：pssh pscp+pssh pslurp pnuke

传统存储技术分类：

DAS直连式存储（台式机：主板上接硬盘，直连存储（SATA）需控制器参与）

NAS网络附加存储（内置好文件系统samba nfs fttp ftp..）

SAN存储区域网络（emc品牌）（块存储）FC光纤通道：速度最快

iscsi小型计算机系统接口(块存储)

NIC：网络接口卡（网卡）

iscsi:网络磁盘 multipath多路径环境

sysfs（内核动态识别硬件）----udev动态管理设备的方式-----动态写入到/dev/

udev 是Linux kernel设备管理器。它主要的功能是管理/dev目录底下的设备节点，是用来接替devfs及热插拔的功能

lvs：nat，dr，tun模式 LVS的IP负载均衡技术是通过IPVS模块实现的

高可用四层调度器：LVS(DR模式)+Keepalived（热备）（vrrp功能，防止单点故障）

keepalived作用：1.给电脑配浮动IP(vip) 2.自动配置lvs (为后台做健康检查)

vip：浮动IP：地址漂移 服务器配置VIP，防止地址冲突（/etc/sysctl.conf）

haproxy应用程序代理:（BigIP新网络协议框架）高可用型，负载均衡

ceph：分布式存储系统，并行写入，软件定义存储。多复本，默认3复本

OSDs：存储服务器【提供存储资源，设备越多性能越好，并行写入】

(可以给虚拟机做磁盘) --->块存储:RADOS块设备（RBD）--->KVM应用

Monitors（MON>=3(奇数)）:集群监控组件 client：客户端

MDSs（文件系统共享）：存放文件系统的(metedata data)

RGW:对象存储

cdph脚本软件：ceph-deploy

ceph文件系统MDSs（额外MDS主机存储元数据）

文件系统：

（1）inode区域：索引节点（描述信息）=metedata（元数据，数据的数据）

（2）block区域

finaldate：数据恢复 （误删千万别进行写操作，给文件名加入delete标签）

磁盘碎片：碎片整理

ceph对象存储（额外RGM主机提供一个web）radosgw(rgw)

启动RGW服务----->api（API）ceph提前准备好的函数

VNC (Virtual Network Console)是虚拟网络控制台的缩写

GPL:通用公共许可证

GUI:图形用户界面（Graphical User Interface)

cat /etc/rc.local | sed 's/.//4'

awk -F: '$3>=10 && $3<=20{print $1":"$3}' /etc/passwd

awk '{ip[$1]++} END{for(i in ip) {print i,ip[i]}}' /var/log/httpd/access\_log | sort -nr---$1（列）可变

从数据库比主数据库性能要好：备份 读访问多

Shell是在Linux内核与用户之间的解释器程序，通常指的是bash，负责向内核翻译及传达用户/程序指令

arp欺骗：数据链路层，攻击者大量发出伪造的arp响应，使受攻击的计算机记录错误的mac地址

安全：chage改变账户有效期 passwd锁定密码 隐藏tty登陆信息/etc/issue(本地)

修改文件属性：chmod、chown、setfacl、chattr +i

优化：noexec noatime

提权：su sudo（需授权visudo）+命令

组授权（%wheel）添加一个普通用户，为禁用root登陆做铺垫

提高SSH服务安全: /etc/ssh/sshd\_config

常见防护：改端口、用户限制、禁root和空密码登陆、认证次数、

黑白名单、更改验证方式（密钥）防火墙

数据加密、aide做入侵检测、NMAP扫描 -n（-sS、-sP ）

抓包信息存文件上：tcpdump -A -i eth0 -w abc.bao

审计（系统）的目的是基于事先配置的规则生成日志，记录可能发生在系统上的事件

审计不会为系统提供额外的安全保护，但她会发现并记录违反安全策略的人及其对应的行为

开源：jumpserver---1.堡垒机（调板机） 2.安全审计（图形）

自带：audit审计系统（audit）配置文件：/etc/audit/auditd.conf

使用diff和patch工具打补丁

diff -Nura 原文档 新文档 > \*.patch

patch -pN < 补丁包(\*.patch)

iptables [-t 表名] 选项 [链名] [条件 条件..] [-j 目标操作]

-p 协议名称 s 源地址 -i 接收数据的网卡 -o 发送数据的网卡

-p 协议名称 --dport 目标端口号(必须指定协议)

扩展规则mac multiport iprange

iptables -t nat -I POSTROUTING -s 192.168.4.0/24（私有ip） -j SNAT --to-source 176.130.2.192（公网ip）

磁盘阵列：raid卡 由很多价格较便宜的磁盘，组合成一个容量巨大的磁盘组

主板BIOS即基本输入输出系统

下载大白菜（软件）插入U盘制作U盘启动调用镜像-----备份好的完整系统

IDC机房：存放服务器的地方

TCP（传输控制协议）和IP（网际协议）：互联网的基础通信架构。它常被通称为TCP/IP协议族

TCP/IP提供点对点的链接机制，将数据应该如何封装、定址、传输、路由以及在目的地如何接收，都加以标准化。

nginx工作原理：Nginx由内核和模块组成，其中，内核的设计非常微小和简洁，完成的工作也非常简单，仅仅通过查找配置文件将客户端请求映射到一个location block（location是Nginx配置中的一个指令，用于URL匹配），而在这个location中所配置的每个指令将会启动不同的模块去完成相应的工作

CGI全称是“通用网关接口

NFS网络文件系统共享(Linux与Linux平台之间) 所需软件包:nfs-utils 系统服务:nfs-server

搭建基本的NFS共享 服务端：1.安装软件包nfs-utils 2.创建目录及文件

3.修改主配置文件 /etc/exports（/abc ##文件夹路径 \*(ro) ##客户机地址(权限)）（exportfs -r可以重新加载）(no\_root\_squash)

4.重起服务nfs-server

客户端：修改配置文件：1.查看对方挂载：showmount -e serverX

2.vim /etc/fstab（172.25.0.11:/abc /mnt/nsd01 nfs defaults,\_netdev 0 0）

2.mount -a df -h

安全的NFS：服务端 1.装包nfs-utils 2.创建共享目录 2.下载密钥并改名（wget -O /etc/krb5.keytab）

4.配置：vim /etc/exports（/protected 172.25.X.0/24(rw,sec=krb5p)） 5.重起nfs-secure-server nfs-server

客户端 1.查看对方挂载：showmount -e serverX 2.创建挂载点 3.下载密钥并改名（wget -O /etc/krb5.keytab）

4.重起服务：nfs-secure

5.配置：vim /etc/fstab（serverX.example.com:/protected /mnt/nfssecure nfs sec=krb5p,\_netdev 0 0）

6.mount -a

[root@svr7 /]# vim /root/rsync.sh

#!/bin/bash

while inotifywait -rqq /opt

do

rsync -az --delete /opt/ root@192.168.4.207:/opt/

done

Cobbler装机平台,不同版本的多系统的安装-----防火墙 与selinux

搭建cobbler:1.解压 2.配置（cobbler） vim /etc/cobbler/settings

next\_server: 192.168.4.168 #设置下一个服务器还为本机

server: 192.168.4.168 #设置本机为cobbler服务器

manage\_dhcp: 1 #设置cobbler管理dhcp服务

pxe\_just\_once: 1 #防止客户端重复安装操作系统

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

:%s /旧/新/g #全文替换

:%s /192.168.1/192.168.4/g #全文替换

5 次替换，共 4 行

4.绝对路径解压cobbler\_boot.tar.gz #众多的引导文件 #

tar -xPf /Cobbler/cobbler\_boot.tar.gz #绝对路径释放

5.启动相关服务重起并开机自动重起（cobblerd，httpd，tftp，rsyncd）

6.同步刷新cobbler配置：cobbler sync #检测配置是否正确（COMPLETE）

7.cobbler应用：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

cobbler list 查询镜像系统

删除 ：cobbler profile remove --name=CentOS7-x86\_64 # #删除菜单信息

cobbler distro remove --name=CentOS7-x86\_64 # #删除镜像信息

自定义应答文件：开头注释行删除

system-config-kickstart #生成ks文件 存放位置：/var/lib/cobbler/kickstarts/

修改kickstart文件：cobbler profile edit --name=CentOS7.4-A --kickstart=/var/lib/cobbler/

kickstarts/自定义.cfg

cobbler profile report

cobbler sync #同步配置

网络自动装机PXE yum provides \*/pxelinux.0 #查询仓库中那个软件包产生

1.http----->将镜像挂载到\*/html/rh7dvd/ system-config-kickstart

2.dhcp----->PXE引导服务器位于 next-server 192.168.4.7 filename 引导文件 pxelinux.0

3.tftp-server(tftp)--->图形支持：vesamenu.c32（镜像） 背景图片：splash.png（镜像）

syslinux---->pxelinux.0(yum provides \*/pxelinux.0)--->tftpboot

4.tftp-server(tftp)--->rhel7-->内核vmlinuz、初始化文件initrd.img（镜像isolinux）

5.tftp-server(tftp)--->pxelinux.cfg---->default(<----镜像/isolinux.cfg)

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

1.安装dhcp软件包 2.配置vim /etc/dhcp/dhcpd.conf(：r /usr/share/doc/dhcp\*/dhcpd.conf.example)

subnet 192.168.4.0 netmask 255.255.255.0 { #分配的网段

range 192.168.4.100 192.168.4.200; #分配IP范围

option domain-name-servers 192.168.4.7; #DNS服务器

option routers 192.168.4.254; #网关地址

default-lease-time 600;

max-lease-time 7200;

next-server 192.168.4.7; #指定下一个服务器地址

filename "pxelinux.0"; } #指定网卡引导文件名称

3.重起

二、搭建tftp服务

1.安装软件包tftp-server 2.重起tftp服务（简单的文件传输协议69 默认共享路径：/var/lib/tftpboot/）

部署pxelinux.0文件 1.下载syslinux 2.cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot/

部署菜单文件 1.挂载 2.cp /mnt/isolinux/isolinux.cfg /var/lib/tftpboot/pxelinux.cfg/default

部署图形的模块vesamenu.c32 及背景图片splash.png

部署启动内核vmlinuz 与驱动程序 initrd.img

三、修改菜单文件 vim /var/lib/tftpboot/pxelinux.cfg/default

开启行号

1 default vesamenu.c32 #默认加载图形的模块

2 timeout 600 #读秒时间 1/10

10 menu background splash.png #指定背景图片

11 menu title NSD1808 PXE Server ！ #菜单显示的标题

61 label linux

62 menu label Install RHEL7.4 #选项内容

63 menu default #读秒结束后默认选择

64 kernel vmlinuz #加载内核

65 append initrd=initrd.img #加载驱动 ks=http://192.168.4.7/ks.cfg #指定ks应答文件

四、搭建httpd服务（ mount /dev/cdrom /var/www/html/rhel7）

五、实现无人值守安装，生成应答文件 1.安装一个图形的工具(system-config-kickstart)

2.运行（必须要求Yum仓库标识 [development]）

六、共享ks应答文件 （cp /root/ks.cfg /var/www/html/）(YUM源，源ID设为 development)

DNS服务器的功能 将域名解析成ip地址 – 正向解析 反向解析 完全合格主机名（FQDN）ServerName www.nb.com

软件包：bind与bind-chroot – 运行时的虚拟根环境:/var/named/chroot/ #牢笼政策

– 系统服务:named – 默认端口: 53

分离解析概述：1.能够区分客户机的来源地址 2.不同的客户端解析同一个域名时，解析结果不同

3.为客户端提供最近的资源

检查配置语法：named-checkconf /etc/named.conf[配置文件]

named-checkzone tedu.cn tedu.cn.zone [区域名][配置文件]

• 主配置文件: /etc/named.conf #设置本服务器负责解析的域名

options {

directory "/var/named"; ##地址文件的默认位置 13

recursion no; ##关闭递归查询 29

};

acl test { 192.168.4.207; 192.168.7.0/24; 192.168.10.1; };

view "nsd" {

match-clients { test; };

zone "tedu.cn" IN { ---->51

type master;

file "tedu.cn.zone";

};

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

};

view "other" {

match-clients { any; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.other";

};

zone "qq.com" IN {

type master;

file "qq.com.other";

};

};

• 地址库文件: /var/named/tedu.cn.zone #主机名与IP地址的对应关系 复制的时候机的cp -p

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

qq.com. NS sur7

bj.qq.com. NS pc207

sur7 A 192.168.4.7

pc207 A 192.168.4.207

www A 1.1.1.1

tts CNAME www

主机映射记录文件/etc/hosts(起到DNS解析的功能) 只为本机提供解析功能

搭建DNS服务器: 1.递归解析 （递归查询是默认开启的，也可以设置 recursion yes; 来明确启用） 2.迭代解析

服务端： 1.安装 2.修改主配置文件/etc/named.conf 3.建立地址库文件/var/named/ 4.重起named服务

（1.搭建多区域的DNS 2.特殊的解析记录（轮询） 3.泛域名解析（最后一条记录 \*） 4.解析记录的别名 CNAME

5.有规律的泛域名解析 $GENERATE 1-50 pc$ A 192.168.20.$ 6.DNS子域授权）

缓存DNS服务器,缓存加速 方式1:全局转发 2:根域迭代

1.有DNS服务器 2.修改DNS主配置文件，指定缓存DNS服务器配置 （/etc/named.conf）

options {

directory "/var/named";

forwarders { 192.168.1.1; };

};

客户端：1.vim /etc/resolv.conf (nameserver 192.168.1.1) 2.nslookup www.bj.qq.com 192.168.4.7

搭建基本Web服务：BS架构 默认端口号80 防火墙trusted 检查语法:httpd -t

服务端:1.安装httpd(Apache)软件包 2.创建默认目录与文件/index.html

3.创建设置调用配置文件：/etc/httpd/conf.d/\*.conf

<virtualhost \*:80> #本机所有IP启用虚拟Web

servername www.qq.com #此站点的DNS名称

documentroot /webapp #此站点的网页根目录

wsgiscriptalias / /var/www/nsd01/webinfo.wsgi ##网页跳转

</virtualhost>

listen 8909 ## 主机侦听在端口8909

<virtualhost \*:8909>

servername www.163.com

documentroot /var/www/nsd02

directoryindex index ##起始页/首页文件名

</virtualhost>

4.创建设置权限目录：/etc/httpd/conf.d/\*.conf

<Directory /var/www/myweb/private>

Require ip 172.25.0.11(not ip 10.252.46.165)（all granted）(all denied)

</Directory>

5.使用自定义根目录：chcon [-R] --reference=模板目录 新目录 6.重起httpd服务

部署动态网站：1.安装mod\_wsgi软件包,专用于翻译Python代码页面

2.设置动态网站（调用配置文件）：WsgiScriptAlias / /var/www/nsd02/webinfo.wsgi 3.重起

修改主机侦听端口8909：1.修改调用配置文件Listen 8909 <VirtualHost \*:8909>

2.selinux非默认端口的开放：查semanage port -l | grep http #查

semanage port -a -t http\_port\_t -p tcp 8909 #改 -a:添加 -t：类型 -p：协议

3.重起并验证 ：firefox webapp0.example.com:8909

安全的Web服务器

服务端：1.安装支持安全https的软件mod\_ssl

2.部署网站证书（营业执照）（1） cd /etc/pki/tls/certs （2）wget 路径/server0.crt

3.部署根证书（公安局信息）（1） cd /etc/pki/tls/certs （2）wget 路径/example-ca.crt

4.部署私钥（用于解密） （1）cd /etc/pki/tls/private/ （2）wget 路径/server0.key

5.修改配置文件：vim /etc/httpd/conf.d/ssl.conf 修改100行 107行 122行（59行及60行）

6.书写一个网站用于测试 DocumentRoot "/var/www/html" 7.重起httpd服务

客户端 ：firefox https://www0.example.com

搭建FTP服务:文件数据传输

服务端 1.安装软件包vsftpd 2.重起vsftpd服务(默认共享数据路径：/var/ftp)

sed -i 's/^#anon/anon/' /etc/vsftpd/vsftpd.conf

匿名上传 #anon\_upload\_enable=YES

#anon\_mkdir\_write\_enable=YES

chmod 777 /var/ftp/pub

客户端 本机测试 firefox ftp://172.25.0.11

Yum软件包仓库，自动解决依赖关系

1.众多的软件包 2.仓库清单文件（repodata）3.构建Web服务或FTP服务传递数据

yum服务端：将镜像文件挂载到/var/ftp下，本机测试，开机自动重起

客户端配置文件：/etc/yum.repos.d/\*.repo（[] name baseurl enabled gpgcheck）

(clean all repolist -y install -y reinstall remove)

1.baseurl=ftp://192.168.4.254/rhel7

2.baseurl=http://classroom.example.com/content/rhel7.0/x86\_64/dvd/

自定义yum仓库

1.具备互联网下载的包，真机传递tools.tar.gz到虚拟机A

scp /root/桌面/tools.tar.gz root@192.168.4.7:/root

2.虚拟机A解tar包

3.运行createrepo生成仓库数据文件# createrepo /tools/other/

4.书写客户端配置文件 baseurl=file:///tools/other（指定本机）

源码编译安装：（需要删除直接删除目录下）步骤1: 安装gcc与make 步骤2: tar解包,释放源代码至指定目录

步骤3: （1）cd /inotify-tools-3.13/（2）./configure --prefix=/opt/myrpm #指定安装位置

作用（1）配置,指定安装目录/功能模块等选项 （2） 作用：检测本机是否安装gcc

步骤4: make 编译,生成可执行的二进制程序文件 步骤5 make install 安装,将编译好的文件复制到安装目录

zip归档工具,跨平台的压缩工具（1）归档+压缩操作– zip [-r] 备份文件.zip 被归档的文档...

（2） 释放归档+解压操作– unzip 备份文件.zip [-d 目标文件夹]

硬盘：扇区的大小为512字节 1PB=1000TB 1EB=1000PB

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

1.识别硬盘lsblk 2.分区规划(fdisk -l /dev/vdb ：查看分区模式MBR/msdos最大2.2TB 或者 GPT最大到18EB)

fdisk /dev/vdb d删除 n新增 p查找 q不保存退出 w保存退出 刷新分区表：partprobe

3.格式化：mkfs.xfs /dev/vdb3 查看文件系统（格式化）：blkid /dev/vdb3

4.开机自动挂载：vim /etc/fstab

设备路径 挂载点 类型 参数 备份标记 检测顺序（可手动挂载）

检查及自动挂载：mount -a 查看已挂载磁盘分区信息：df -Th

parted /dev/vdb "mktable gpt" "mkpart" "ext2" "ext2" "0G" "1G"

parted大容量分区，专用于gpt分区方案

parted /dev/vdb #编辑 mklabel(mktable) gpt #指定分区模式为GPT print #查看分区表

mkpart #划分分区 忽略/Ignore/放弃/Cancel? Ignore #输入i选择忽略 unit GB # 使用GB作为显示单位

交换空间：以空闲分区充当的交换空间，相当于虚拟内存,当物理内存不够用时,使用磁盘空间来模拟内存，在一定程度上缓解内存不足的问题

mkswap /dev/vdb1 #格式化交换文件系统 swapon（swapoff ） /dev/vdb1 #启用（停用）的命令

swapon -s #查看交换空间的成员

开机自启：vim /etc/fstab （/dev/vdb1 swap swap defaults 0 0）

swapon -a #检测书写是否正确 swapon -s

LVM逻辑卷的管理: 将众多的物理卷( PV),组成卷组(VG),再从卷组中划分出逻辑卷(LV)

作用：1.可以整合分散的空间 2.容量大小可以扩大------------------>查看：pvs vgs（vgdisplay） lvs(can)

1.直接创建卷组:vgcreate 卷组的名 设备路径1 设备路径2 .......

2.通过卷组划分逻辑卷:lvcreate -n 逻辑卷名 -L 逻辑卷大小(300M)) 卷组名

3.格式化：mkfs.ext4 设备路径（blkid）

4.开机自动挂载： vim /etc/fstab 设备路径 挂载点 类型 参数 备份标记 检测顺序

检查及自动挂载：mount -a 查看已挂载磁盘分区信息：df -h(挂载点)

逻辑卷的扩展:1.扩展卷组vgextend 卷组名 设备路径 2.扩展空间的大小：lvextend -L（l） 大小(300M) 设备路径

3.扩展文件系统的大小 resize2fs 设备路径（扩展ext4文件系统） xfs\_growfs:扩展xfs文件系统

卷组划分空间的单位：PE（默认4M） 1.查看卷组PE大小 vgdisplay systemvg

2.修改方式 卷组存在：vgchange -s PE大小 卷组名---创建卷组时，可以通过-s选项指定PE的大小

创建卷组的时候设置PE大小：vgcreate -s PE大小 卷组名 设备路径

逻辑卷的删除：先卸载 逻辑卷（lvremove）--->卷组(vgremove)-------> 物理卷(pvremove)

Samba服务基础，Linux与Windows跨平台的共享 （协议:SMB(TCP 139 用户验证)、CIFS(TCP 445 传输数据)

Samba用户： 专用来访问共享文件夹的用户 1.采用独立设置的密码 2.需要提前建立同名的系统用户(可以不设密码）

搭建Samba共享：服务端 1.安装软件包samba（系统服务:smb）

2.创建samba共享帐号及目录/文件（useradd pdbedit -（a增L查x删））（/sbin/nologin）

3.SELinux布尔值ro（服务功能的开关on 或 off）加-P选项才能实现永久设置（查getsebool -a 改setsebool）及本地目录

4.修改配置文件/etc/samba/smb.conf （[common] #共享名 path = /common #共享实际路径）(注意空格) 5.重起smb服务

客户端：1.安装软件cifs-utils（samba-client：smbclient -L serverX -U 用户名） 2.开机自动挂载 （/etc/fstab）

//172.25.0.11/common /mnt/nsd cifs defaults,user=harry,pass=123,\_netdev 0 0

读写：服务端：1234

5.[devops] path = /devops write list = chihiro workgroup = STAFF hosts allow = 172.25.0.0/24(注意空格)

6 7.rw 8.修改本地目录权限

多用户Samba共享:SMB客户端的 multiuser 挂载技术

客户端：添加挂载参数 – multiuser – sec=ntlmssp

cifscreds add -u 共享用户名 服务器地址

ISCSI网络磁盘： 服务器提供磁盘空间,客户机连接并当成本地磁盘使用 默认端口：3260

backstore,后端存储 target,磁盘组 lun,逻辑单元

IQN名字规范：iqn.yyyy-mm.倒序域名:自定义标识 作用：1.用来识别 target磁盘组,2.用来识别客户机身份

服务端 一、划分新的分区

二、部署iSCSI共享存储 1.安装软件targetcli 2.运行targetcli可以再交互式界面

A:创建与命名后端存储 backstores/block create name=nsd dev=/dev/vdb1（以下皆可用ls查询）

B:创建target,磁盘组iscsi/ create iqn.2018-09.com.example:server0

C:lun,逻辑单元

iscsi/iqn.2018-09.com.example:server0/tpg1/ luns create /backstores/block/nsd

D:配置访问控制，设置访问服务时，客户端声称的名字iscsi/iqn.2018-09.com.example:server0/tpg1/ acls create iqn.2018-09.com.example:desktop0

E:客户端访问本机的IP地址及端口

iscsi/iqn.2018-09.com.example:server0/tpg1/ portals create 172.25.0.11 3260-->exit退出

三、重起服务target

客户端：1.安装所需软件包iscsi-initiator-utils 2.修改配置文件/etc/iscsi/initiatorname.iscsi

InitiatorName=iqn.2018-09.com.example:desktop0

3.需重启服务 iscsid（刷新iqn）--

自起vim /var/lib/iscsi/nodes/iqn.2016-02.com.example\:server0/\*/default--->node.conn[0].startup = automatic

4.发现服务端共享存储 参考# man iscsiadm 搜索全文 /example

iscsiadm --mode discoverydb --type sendtargets --portal 172.25.0.11 --discover

5.本机识别服务端共享：重起服务iscsi

用户帐号作用： 1. 访问控制的设置，不同的用户具备不同权限 2. 提高安全可靠性

useradd usermod(u d s g G从属组) userdel(r)（管理员0 系统程序用户1-999 普通用户1000）

组帐号作用：方便管理用户帐号 所有用户至少属于一个组 基本组 附加组

groupadd groupmod(n g) grouddel gpasswd(a d)

修改密码：passwd – passwd [用户名]+++++++++++++++++

切换用户身份：su - 用户

非交互式设置用户密码 echo '密码' | passwd --stdin 用户名

存放的是用户的基本信息 /etc/passwd

组基本信息存放在 /etc/group

用户密码信息存放在 /etc/shadow

权限：基本权限：访问方式(权限) 以 - 开头：代表文本文件 以 d 开头：代表目录 以 l 开头：快捷方式

读取:允许查看内容-read r – 写入:允许修改内容-write w – 可执行:允许运行和切换-execute x

权限适用对象：所有者-user:u 所属组-group:g 其他用户-other: o a=ugo

设置基本权限：chmod [-R] 归属关系（ugo）+-=权限类别（rwx-） 文档...

设置文档归属：chown [-R] 属主:属组 文档..

附加权限(特殊权限):Set GID(属组x位上标识为s)Set UID 属主的x位标识为s Sticky Bit 其他人的x位标识为t

acl权限： 能够对个别用户、个别组设置独立的权限 查看：getfacl 文档...

setfacl [-R]：递归设置ACL权限 -m u:用户名:权限类别 文档... -m g:组名:权限类别 文档...

– setfacl -x u:用户名 文档... #删除指定的ACL -b 文档... #删除所有的ACL

权限的数值化 – 基本权限:r = 4,w = 2,x = 1

– 附加权限:SUID = 4,SGID = 2,Sticky Bit = 1（粘滞位）（tmp）

root创建目录默认755权限 umask 权限掩码0022 （改umask 077）

LDAP网络用户认证，达到用户的集中管理

客户端：软件包：sssd authconfig-tui (配置完重起) autofs（+nfs）:/dev/ ##本地挂载

1.下载autofs 2.vim /etc/auto.master /home/guests /etc/guests.rule

3.vim /etc/guests.rule \* -rw classroom.example.com:/home/guests/& 4.重起

NTP网络时间协议：1.NTP服务器为客户机提供标准时间 2.NTP客户机需要与NTP服务器保持沟通

客户端 1.安装chrony软件包

2.修改程序主配置文件，指定服务端位置（/etc/chrony.conf） 3.重起程序（chronyd）4.验证-->重起

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）

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 --zone=block --3add-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=public --add-forward-port=port=5423:proto=tcp:toport=80