

**2019年8月28日**

[云计算基础篇]

[云计算基础篇](#_Toc1470445725) **[错误！未定义书签。](#_Toc1470445725)**

[第一部分 云计算系统管理 4](#_Toc245591253)

[1.Linux系统简介 4](#_Toc1252213876)

[2.Linux版本及应用 4](#_Toc534400988)

[3.Linux磁盘表示 4](#_Toc959481401)

[4.列出CPU处理器信息 4](#_Toc1653078169)

[5.检查内存大小、空闲情况 4](#_Toc1129999423)

[6.列出当前系统的主机名称 4](#_Toc1554927816)

[7.查看当前系统的版本 5](#_Toc946581698)

[8.目录和文件管理 5](#_Toc1994799438)

[9.管理用户和组 7](#_Toc1202177387)

[10.tar备份与恢复 9](#_Toc1424349315)

[11.cron计划任务 10](#_Toc238462652)

[12.教学环境介绍 11](#_Toc333294788)

[13.权限和归属 11](#_Toc932566323)

[14.附加权限(特殊权限) 13](#_Toc840686043)

[15.软件包管理 14](#_Toc790416870)

[16.Yum配置及使用,自动解决依赖关系安装软件 15](#_Toc1328231143)

[17.分区规划及使用 16](#_Toc753516719)

[18.LVM逻辑卷 17](#_Toc97293618)

[19.逻辑卷的扩展 18](#_Toc1078072162)

[20.查找文件 19](#_Toc1256698981)

[21.find扩展使用 20](#_Toc248938914)

[22.grep用法 20](#_Toc1048077667)

[23.NTP时间同步 21](#_Toc620433747)

[24.准备交换空间(虚拟内存) 21](#_Toc1510214846)

[25.补充内容:触发挂载(autofs) 22](#_Toc1943471299)

[第二部分 云计算应用管理 23](#_Toc1411127278)

[1.系统安全保护 23](#_Toc1191082889)

[2.alias别名设置 23](#_Toc2057303220)

[3.虚拟机server0:搭建Web服务器 23](#_Toc944703374)

[4.虚拟机server0:搭建FTP服务 24](#_Toc514044966)

[5.防火墙策略管理 24](#_Toc155410825)

[6.iSCSI网络磁盘 26](#_Toc49433602)

[7.数据库服务基础 27](#_Toc1048445954)

[8.NFS共享 30](#_Toc1114892227)

[9.HTTP服务基础 31](#_Toc1702511771)

[10.虚拟Web主机 32](#_Toc30961730)

[11.部署动态网站 35](#_Toc522336395)

[12.安全Web服务 36](#_Toc501609822)

[13.补充:Samba共享服务(Windows与Linux跨平台的共享) 37](#_Toc2025761168)

[14.设置网络参数 38](#_Toc1724513782)

[15.聚合连接(链路聚合 网卡绑定) 39](#_Toc1925959137)

[16.基础邮件服务 39](#_Toc116740173)

[17.parted分区工具,进行GPT分区模式 40](#_Toc2057808571)

[第三部分 系统&服务管理进阶 41](#_Toc711041812)

[1.构建新的教学环境 41](#_Toc957426216)

[2.目录结构 42](#_Toc700741793)

[3.制作快捷方式 制作连接(链接)文件 43](#_Toc2039272955)

[4.zip归档工具,跨平台的压缩格式 44](#_Toc1710942936)

[5.自定义Yum源 44](#_Toc798035411)

[6.vim编辑技巧 45](#_Toc969861469)

[7.源码编译安装 46](#_Toc820158269)

[8.手动图形安装虚拟机名为nsd01 46](#_Toc1046974325)

[9.虚拟机nsd01进行配置 47](#_Toc2017939136)

[10.安装虚拟化服务器平台 47](#_Toc1440592016)

[11.通过命令管理虚拟机 48](#_Toc409705523)

[12.一台KVM虚拟机的组成 48](#_Toc1813926788)

[13.在命令行手动制作一台虚拟机 49](#_Toc704235646)

[14.在命令行手动创建虚拟机 49](#_Toc1600788412)

[15.三合一:导出 修改 导入 50](#_Toc1723746360)

[16.DNS服务器的功能 51](#_Toc1648939021)

[17.构建基本DNS服务 51](#_Toc2114833379)

[18.多域名的DNS服务器,负责解析qq.com域名 52](#_Toc1879157185)

[19.特殊解析记录 53](#_Toc1698372623)

[20.DNS子域授权 54](#_Toc1015795685)

[21.缓存DNS,缓存解析结果,加快解析过程 55](#_Toc846565764)

[22.Split分离解析(视图解析) 56](#_Toc1253400747)

[23.RAID磁盘阵列 59](#_Toc1046757415)

[24.进程管理 60](#_Toc1368902160)

[25.日志管理 62](#_Toc1755010569)

[26.用户登录分析 63](#_Toc925034936)

[27.日志消息的优先级 63](#_Toc945932294)

[28.systemctl控制 64](#_Toc1533486058)

[29.DNS分离解析与Web结合 65](#_Toc1041775109)

[30.部署DHCP服务器 66](#_Toc856257217)

[31.网络装机概述 67](#_Toc97044222)

**云 计 算 基 础 篇**

**内容概述**:云计算系统管理、 云计算应用管理、系统&服务管理进阶

# **第一部分 云计算系统管理**

1.Linux系统简介

Linux是一种操作系统!

Unix/Linux发展史

UNIX诞生,1970-1-1

Linux的诞生:Linux之父,Linus Torwalds

– 1991年10月,发布0.02版(第一个公开版)内核

– 1994年03月,发布1.0版内核

– 内核版本号:主版本.次版本.修订号 4.10.123 用户------>内核------>硬件

2.Linux版本及应用

• 发行版的名称/版本由发行方决定

– Red Hat Enterprise Linux 5/6/7

– Suse Linux Enterprise 12

– Debian Linux 7.8

– Ubuntu Linux 14.10/15.04

3.Linux磁盘表示

hd,表示IDE设备

sd,表示SCSI设备

/dev/sda :表示SCSI设备,第一块

/dev/sdb :表示SCSI设备,第二块

/dev/sdc :表示SCSI设备,第三块

/dev/hdd :表示IDE设备,第四块

Linux系统中第三块SCSI硬盘如何表示? /dev/sdc

4.列出CPU处理器信息

[student@room9pc01 ~]$ lscpu #查看CPU的信息

CPU(s): 4

型号名称： Intel(R) Core(TM) i5-4430S CPU @ 2.70GHz

5.检查内存大小、空闲情况

[student@room9pc01 ~]$ cat /proc/meminfo

MemTotal: 16330736 kB

6.列出当前系统的主机名称

[root@svr7 桌面]# hostname #查看主机名称

[root@svr7 桌面]# hostname A.tedu.cn #临时设置主机名

[root@svr7 桌面]# exit #关闭当前的终端

root@A ~]# ifconfig eth0 #查看网卡IP地址信息

[root@A ~]# ifconfig eth0 192.168.1.1 #临时设置IP地址

7.查看当前系统的版本

[root@localhost ~]# cat /etc/redhat-release

CentOS Linux release 7.5.1804 (Core)

8.目录和文件管理

使用pwd、cd

pwd — Print Working Directory

– 用途:查看当前工作目录

cd — Change Directory

– 用途:切换工作目录

– 格式:cd [目标文件夹位置]

. 表示当前目录

.. 表示父目录

~:家目录

~user表示用户user的家目录

/root:管理员的家目录

/home:存放所有普通用户的家目录

• ls — List

– 格式:ls [选项]... [目录或文件名]

• 常用命令选项

– -l:以长格式显示,显示详细信息

– -A:包括名称以 . 开头的隐藏文档

– -d:显示目录本身(而不是内容)的属性

– -h:提供易读的容量单位(K、M等)

[root@1906 ~]# ls -lh /etc/passwd #显示文件的详细属性

[root@1906 ~]# ls -l /boot/ #显示目录内容详细属性

[root@1906 /]# ls -ld / #显示目录本身的详细属性

[root@1906 /]# ls -A /root #显示目录的所有内容,包括隐藏数据

使用通配符

• 针对不确定的文档名称,以特殊字符表示

– \*:任意多个任意字符

– ?:单个字符

[root@1906 /]# ls /dev/tty\* #显示tty开头的数据

[root@1906 /]# ls /etc/\*tab #以tab作为结尾的数据

[root@1906 /]# ls /etc/\*.conf #以.conf作为结尾的数据

[root@1906 /]# ls /dev/tty?

[root@1906 /]# ls /etc/??tab

• 针对不确定的文档名称,以特殊字符表示

– [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

[root@1906 /]# ls /dev/tty[3-8]

[root@1906 /]# ls /dev/tty{1,21,60}

[root@1906 /]# ls /dev/tty{1,3,5,7,9}

别名的定义:简化复杂的命令

• 查看已设置的别名

– alias [别名名称]

• 定义新的别名

– alias 别名名称= '实际执行的命令行'

• 取消已设置的别名

– unalias [别名名称]

[root@1906 /]# hostname

1906.tedu.cn

[root@1906 /]# alias hn='hostname' #定义别名

[root@1906 /]# alias #显示当前系统有效别名

[root@1906 /]# hn #运行hn执行成功

[root@1906 /]# unalias hn #删除别名

• mkdir — Make Directory

– 格式:mkdir [-p] [/路径/]目录名...

[root@1906 /]# mkdir -p /vod/movie/cartoon #-p表示连父目录一起创建

[root@1906 /]# ls /opt/

[root@1906 /]# ls -R /opt/aa #-R表示递归显示

查找文本内容

• 根据字符串模式提取文本行

– grep [选项] '匹配模式' 文本文件...

• 常用命令选项

– -v,取反匹配

– -i,忽略大小写

[root@1906 /]# grep -v root /etc/passwd #取反查找

[root@1906 /]# grep -i ROOT /etc/passwd #忽略大小写

– ^word 以字符串word开头

– word$ 以字符串word结尾

[root@1906 /]# grep ^root /etc/passwd #以root开头

[root@1906 /]# grep bash$ /etc/passwd #以bash结尾

rm 删除

• rm — Remove

– 格式:rm [选项]... 文件或目录...

• 常用命令选项

– -r、-f:递归删除(含目录)、强制删除

[root@1906 /]# rm -rf /opt/1.txt #强制删除所有

mv 移动/改名

• mv — Move

– 格式:mv [选项]... 原文件... 目标路径

[root@1906 /]# mv /opt/a.txt /opt/nsd

重命名:路径不变的移动

[root@1906 /]# mv /opt/nsd/ /opt/haha

cp 复制

• cp — Copy

– 格式:cp [选项]... 原文件... 目标路径

• 常用命令选项

– -r:递归,复制目录时必须有此选项

/etc:存放系统配置文件

/opt:用户可选择目录

[root@1906 /]# cp /etc/passwd /opt/

[root@1906 /]# cp -r /home /opt/

复制可以支持多个参数:永远把最后一个参数作为目标,其他的所有参数都作为源

]# cp -r /boot/ /etc/shadow /etc/resolv.conf /etc/hosts /opt/

复制经常与点连用: . 表示当前路径

[root@1906 network-scripts]# ls

复制出现重名:在本次操作临时取消别名

[root@1906 /]# \cp -r /boot/ /opt/ #本次操作临时取消别名

复制:可以重新命名,目标路径下数据

[root@1906 /]# cp /etc/passwd /opt/pa.txt

以下两次复制有何不同?

]# rm -rf /opt/\* #删除/opt目录下所有内容

]# cp -r /home/ /opt/test

#将/home目录复制到/opt目录下重命名为test

]# cp -r /home/ /opt/test

#将/home目录复制到/opt/test目录下

重定向输出操作:将前面的命令的输出,写入到文本文件

>:覆盖重定向

>>:追加重定向

管道操作 | :

将前面命令的输出,交由后面命令处理,作为后面命令的参数

显示/etc/passwd的8至12行内容

[root@1906 ~]# head -12 /etc/passwd

[root@1906 ~]# head -12 /etc/passwd | tail -5

9.管理用户和组

用户帐号: 1.登录系统 2.确认身份,实现权限控制

组:方便管理用户 唯一标识: UID GID

组分类: 基本组(私有组) 附加组(从属组) 一个用户至少属于一个组

添加用户

用户基本信息存放在 /etc/passwd文件(系统级配置文件)

[root@1906 ~]# head -1 /etc/passwd

root:x:0:0:root:/root:/bin/bash

用户名:密码占位符:UID:基本组GID:描述信息:家目录:解释器程序

使用 useradd 命令

– useradd [选项]... 用户名

• 常用命令选项

-u 用户id、-d 家目录路径、-s 登录解释器、-G 附加组

[root@1906 ~]# useradd -u 1500 nsd01 #创建用户指定UID

[root@1906 ~]# id nsd01

[root@1906 ~]# useradd nsd02

[root@1906 ~]# id nsd02 #查询nsd02用户基本的信息

[root@1906 ~]# ls /home/

]# useradd -d /opt/abc nsd05 #创建用户指定家目录

用户名:密码占位符:UID:基本组GID:描述信息:家目录:解释器程序

-s:指定解释器程序

/sbin/nologin:禁止用户登录系统

[root@1906 ~]# useradd -s /sbin/nologin nsd13

-G:指定附加组(从属组)

[root@1906 ~]# groupadd tedu #创建组tedu

[root@1906 ~]# useradd nsd15

[root@1906 ~]# id nsd15

[root@1906 ~]# useradd -G tedu nsd16 #创建用户指定附加组

[root@1906 ~]# id nsd16

设置登录密码

复杂密码: 3/4原则 字母 数字 大小写 特殊符号

• 使用 passwd 命令

[root@1906 ~]# useradd nsd17

[root@1906 ~]# passwd nsd17

更改用户 nsd17 的密码 。

新的 密码： #输入新的密码

重新输入新的 密码： #重新输入新的密码

passwd：所有的身份验证令牌已经成功更新

[root@1906 ~]# su - nsd17 #命令行临时切换身份

[nsd17@1906 ~]$ passwd

更改用户 nsd17 的密码 。

为 nsd17 更改 STRESS 密码。

（当前）UNIX 密码： #输入旧的密码

新的 密码：

重新输入新的 密码：

passwd：所有的身份验证令牌已经成功更新。

[nsd17@1906 ~]$ exit #回到root用户

非交互式设置密码

[root@1906 ~]# echo 123 | passwd --stdin nsd17

用户密码信息存放在 /etc/shadow 文件

[root@1906 ~]# grep nsd17 /etc/shadow

nsd17:$6$UJ1UmCDO$uxsebJRVxjfOTUngX3nfI21mYCrEYiiPZs6Q4FD5Op7kzEtF7f8

u49XSm8AVGqm6X4Ny/pULXIKngkDIo7pSS1:18079:0:99999:7:::

用户名:密码加密字符串:上一次修改密码的时间

上一次修改密码的时间:1970-1-1~2019-7-2 经历的天数

修改用户属性

• 使用 usermod 命令

– usermod [选项]... 用户名

• 常用命令选项

– -u 用户id、-d 家目录路径、-s 登录解释器 -G 附加组

[root@1906 ~]# useradd nsd19

[root@1906 ~]# grep nsd19 /etc/passwd

]# usermod -u 2500 -G tedu -s /sbin/nologin -d /mnt/abc nsd19

[root@1906 ~]# grep nsd19 /etc/passwd

[root@1906 ~]# id nsd19

删除用户

• 使用 userdel 命令

– userdel [-r] 用户名

-r:连同家目录一并删除

[root@1906 ~]# userdel nsd01

[root@1906 ~]# userdel -r nsd02 #连同家目录一同删除

管理组账号

添加组

组基本信息存放在 /etc/group文件

• 使用 groupadd 命令

– groupadd [-g 组ID] 组名

[root@1906 ~]# groupadd tarena

[root@1906 ~]# grep tarena /etc/group

tarena:x:2010:

组名:组的密码占位符:组GID:组成员列表

管理组成员

• 使用 gpasswd 命令

– gpasswd -a 用户名 组名

– gpasswd -d 用户名 组名

[root@1906 ~]# gpasswd -a natasha tarena

[root@1906 ~]# grep tarena /etc/group

[root@1906 ~]# gpasswd -d dc tarena

[root@1906 ~]# grep tarena /etc/group

删除组

• 使用 groupdel 命令

– groupdel 组名

案例1:配置用户和组账号

• 新建用户 alex,其用户ID为3456,密码是flectrag

[root@1906 ~]# useradd -u 3456 alex

[root@1906 ~]# echo flectrag | passwd --stdin alex

• 一个名为 adminuser 的组

[root@1906 ~]# groupadd adminuser

• 为 natasha 的用户其属于adminuser组,这个组是该用户的从属组

[root@1906 ~]# gpasswd -a natasha adminuser

[root@1906 ~]# id natasha

• 为 harry 的用户,其属于adminuser组,这个组是该用户的从属组

[root@1906 ~]# gpasswd -a harry adminuser

[root@1906 ~]# id harry

• 为 sarah的用户,其在系统中没有可交互的Shell

[root@1906 ~]# useradd -s /sbin/nologin sarah

• natasha 、harry、sarah 的密码都要设置为 flectrag

10.tar备份与恢复

1.整合分散的数据 2.减小空间占用

归档和压缩

• 归档的含义

– 将许多零散的文件整理为一个文件

– 文件总的大小基本不变

• 压缩的含义

– 按某种算法减小文件所占用空间的大小

– 恢复时按对应的逆向算法解压

常见的压缩格式及命令工具:

.gz ---> gzip .bz2 ---> bzip2 .xz ---> xz

• tar 集成备份工具

– -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):指定释放路径

制作tar包格式:

tar 选项 /路径/压缩包的名字 /路径/被压缩的源数据 .....

]# tar -zcf /opt/file.tar.gz /home/ /etc/passwd

]# tar -jcf /opt/abc.tar.bz2 /home/ /etc/passwd

]# tar -Jcf /opt/nsd.tar.xz /home/ /etc/passwd

解包格式:

tar 选项 /路径/压缩包的名字 释放的路径

]# tar -xf /opt/file.tar.gz -C /mnt/

案例2:创建一个备份包

使用 tar 工具完成以下备份任务:

– 创建一个名为 /root/backup.tar.bz2 的归档文件

11.cron计划任务

cron任务概述

• 用途:按照设置的时间间隔为用户反复执行某一项固定的系统任务

• 软件包:cronie、crontabs

• 系统服务:crond

• 日志文件:/var/log/cron

管理计划任务策略

• 使用 crontab 命令(不能自动创建目录,需要事先手动创建目录)

– 编辑:crontab -e [-u 用户名]

– 查看:crontab -l [-u 用户名]

– 清除:crontab -r [-u 用户名]

如何编写任务记录

• 配置格式可参考 /etc/crontab 文件

分 时 日 月 周 任务命令行(绝对路径)

\* \* \* \* \* #每分钟都执行

30 23 \* \* \* #每天晚上11:30

30 23 \* \* 5 #每周的周五晚上11:30

30 23 \* \* 1,3,5 #每周的周五,周一,周三 晚上11:30

30 23 \* \* 1-5 #每周的周一至周五 晚上11:30

1 \*/2 \* \* \* #每两个小时

分 时 日 月 周

1 8 1 \* 2 #每周的周二或每月的一号

\*: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 ...

利用root用户,每分钟记录当前系统时间,写入到/opt/time.txt

[root@1906 ~]# date #显示系统时间

[root@1906 ~]# date >> /opt/time.txt

[root@1906 ~]# cat /opt/time.txt

[root@1906 ~]# crontab -e

\* \* \* \* \* date >> /opt/time.txt

[root@1906 ~]# crontab -l -u root

\* \* \* \* \* date >> /opt/time.txt

12.教学环境介绍

• 每个学员机上有三台预先配置好的虚拟机

– server —— 作为练习用服务器

– desktop —— 作为练习用客户机

– classroom —— 提供网关/DNS/软件素材等资源

优先虚拟机classroom开机

真机上使用rht-vmctl辅助工具

]# rht-vmctl reset classroom //先重置资源服务器

]# rht-vmctl reset server

]# rht-vmctl reset desktop //再重置答题虚拟机

13.权限和归属

基本权限的类别

• 访问方式(权限)

– 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

对文本文件:

r: cat less head tail

w: vim > >>

x: Shell脚本

• 权限适用对象(归属)

– 所有者:拥有此文件/目录的用户-user u

– 所属组:拥有此文件/目录的组-group g

– 其他用户:除所有者、所属组以外的用户-other o

lisi lisi组 a.txt

查看权限

• 使用 ls -l 命令

– ls -ld 文件或目录...

以 d 开头为目录

以 - 开头为文本文件

以 l 开头为快捷方式

• 使用 chmod 命令

– chmod [-R] 归属关系+-=权限类别 文档...

[-R]:递归设置权限

[root@server0 ~]# chmod g+w /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod ugo=rwx /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod u=rwx,g=rx,o=rx /nsd01

[root@server0 ~]# mkdir -p /opt/aa/bb/cc #递归创建

[root@server0 ~]# chmod -R o=--- /opt/aa #递归设置

Linux判定一个用户拥有的权限 匹配及停止

1.判断用户的身份 所有者>所属组>其他人

2.查看相应权限位的权限

1.严老师可以进入 1.所有人不可以进入

2.所有人不可以进入 2. 严老师可以进入

Permission denied :权限不足

目录的r权限:能够 ls 浏览此目录内容

目录的w权限:能够执行rm/mv/cp/mkdir/touch更改目录内容的操作

目录的x权限:能够 cd 切换到此目录

以root用户新建/nsddir目录，在此目录下新建readme.txt文件

并进一步完成下列操作

1）使用户lisi能够在此目录下创建子目录 su - lisi

chmod o+w /nsddir/

2）使用户lisi不能够在此目录下创建子目录

chmod o-w /nsddir/

3）使用户lisi能够修改readme.txt文件内容

chmod o+w /nsddir/readme.txt

4）调整此目录的权限，使所有用户都不能cd进入此目录

chmod u-x,g-x,o-x /nsddir/

5）为此目录及其下所有文档设置权限 rwxr-x---

chmod -R u=rwx,g=rx,o=--- /nsddir/

　　　-R：递归设置权限，目录下及目录下所有

设置文档归属

• 使用 chown 命令

– chown [-R] 属主 文档...

– chown [-R] :属组 文档...

– chown [-R] 属主:属组 文档...

[root@server0 ~]# mkdir /nsd03

[root@server0 ~]# ls -ld /nsd03

[root@server0 ~]# groupadd tedu

[root@server0 ~]# chown lisi:tedu /nsd03

[root@server0 ~]# ls -ld /nsd03

利用root用户新建/nsd06目录，并进一步完成下列操作

1）将属主设为gelin01，属组设为tarena组

[root@server0 /]# useradd gelin01

[root@server0 /]# useradd gelin02

[root@server0 /]# groupadd tarena

[root@server0 /]# chown gelin01:tarena /nsd06

2）使用户gelin01对此目录具有rwx权限

除属主与属组之外的人，对此目录无任何权限

[root@server0 /]# chmod o=--- /nsd06

3）使用户gelin02能进入、查看此目录内容

[root@server0 /]# gpasswd -a gelin02 tarena

4）将gelin01加入tarena组, 将nsd06目录的权限设为rw-r-x---

再测试gelin01用户能否进入此目录

[root@server0 /]# gpasswd -a gelin01 tarena

[root@server0 /]# chmod u=rw,g=rx /nsd06

设置权限,让lisi用户可以读取/etc/shadow文件内容,有几种办法?

1.利用其他人:chmod o+r /etc/shadow

2.利用所属组:chown :lisi /etc/shadow chmod g+r /etc/shadow

3.利用所有者: chown lisi /etc/shadow chmod u+r /etc/shadow

4.利用ACL策略 setfacl -m u:lisi:r /etc/shadow

14.附加权限(特殊权限)

Set GID

• 附加在属组的 x 位上

– 属组的权限标识会变为 s

– 适用于目录,Set GID可以使目录下新增的文档自动设

置与父目录相同的属组

– 自动继承父目录所属组身份

[root@server0 ~]# chmod g+s /nsd08/ #设置Set GID

[root@server0 ~]# ls -ld /nsd08/

财务: caiwu组

/nsd09/20190703.txt

[root@server0 ~]# chown :caiwu /nsd09

[root@server0 ~]# chmod g+s /nsd09

Set UID

• 附加在属主的 x 位上

– 属主的权限标识会变为 s

– 适用于可执行文件,Set UID可以让使用者具有文件属主的身份及部分权限

[root@server0 ~]# cp /usr/bin/mkdir /usr/bin/hahadir

[root@server0 ~]# chmod u+s /usr/bin/hahadir

Sticky Bit

• 附加在其他人的 x 位上

– 其他人的权限标识会变为 t

– 适用于开放 w 权限的目录,可以阻止用户滥用 w 写入

权限(禁止操作别人的文档)

[root@server0 ~]# chmod o+t /public

[root@server0 ~]# ls -ld /public

acl访问控制列表

acl策略的作用

• 文档归属的局限性

– 任何人只属于三种角色:属主、属组、其他人

– 无法实现更精细的控制

• acl访问策略

– 能够对个别用户、个别组设置独立的权限

– 大多数挂载的EXT3/4、XFS文件系统默认已支持

[root@server0 ~]# setfacl -m u:lisi:rx /nsd11

[root@server0 ~]# getfacl /nsd11 #专用于查看ACL策略

使用 getfacl、setfacl 命令

– getfacl 文档...

– setfacl [-R] -m u:用户名:权限类别 文档...

– setfacl [-R] -m g:组名:权限类别 文档...

– setfacl [-R] -x u:用户名 文档... #删除指定ACL

– setfacl [-R] -b 文档... #清除所有ACL

]# setfacl -m u:genlin01:rwx /nsd14

]# setfacl -m u:genlin02:--- /nsd14 #设置无任何权限

]# getfacl /nsd14

]# setfacl -x u:genlin02 /nsd14 #删除指定ACL策略

]# getfacl /nsd14

]# setfacl -x u:genlin01 /nsd14 #删除指定ACL策略

]# getfacl /nsd14

]# setfacl -b /nsd14 #清除所有的ACL策略

]# getfacl /nsd14

15.软件包管理

下载软件包

• 使用wget下载工具

– wget 软件包的URL网址

– wget 软件包的URL网址 -O(大写) /目录路径/新文件名

真机的浏览器: Ctrl + f 当前页面查找 vsftpd

http://classroom.example.com/content/rhel7.0/x86\_64/dvd/Packages/

• RPM Package Manager,RPM包管理器

– rpm -q 软件名...

– rpm -ivh 软件名-版本信息.rpm...

– rpm -e 软件名...

[root@server0 ~]# rpm -q vsftpd #查询软件是否安装

未安装软件包 vsftpd

[root@server0 ~]# rpm -q firefox

firefox-24.5.0-1.el7.x86\_64

]# rpm -ivh /root/vsftpd-3.0.2-9.el7.x86\_64.rpm

[root@server0 ~]# rpm -q vsftpd

[root@server0 ~]# rpm -e vsftpd #卸载软件

[root@server0 ~]# rpm -q vsftpd

]# rpm -ivh /root/vsftpd-3.0.2-9.el7.x86\_64.rpm

]# rpm -ql vsftpd #查询已安装的软件,安装了那些内容

[root@server0 ~]# rpm --import /root/RPM-GPG-KEY-redhat-release

[root@server0 ~]# rpm -e vsftpd

[root@server0 ~]# rpm -q vsftpd

未安装软件包 vsftpd

[root@server0 ~]# rpm -i /root/vsftpd-3.0.2-9.el7.x86\_64.rpm

###########################################################

常见的提示:

]# rpm -ivh /root/bind-chroot-9.9.4-14.el7.x86\_64.rpm

错误：依赖检测失败：

bind = 32:9.9.4-14.el7 被 bind-chroot-32:9.9.4-14.el7.x86\_64 需要

16.Yum配置及使用,自动解决依赖关系安装软件

服务:自动解决依赖关系安装软件

服务端: 1.众多的软件包 2.仓库数据文件 3.构建Web服务或FTP服务

光盘内容中

总结:构建Web服务或FTP服务,共享光盘所有内容

虚拟机classroom构建Web服务,共享光盘所有内容

客户端: 虚拟机server 书写一个配置文件,指定服务端位置

– /etc/yum.repos.d/\*.repo

错误的文件会影响正确配置文件

[root@server0 ~]# rm -rf /etc/yum.repos.d/\*

[root@server0 ~]# vim /etc/yum.repos.d/dc.repo

[haha] #仓库标识,随意写不能有特殊字符

name=rhel7.0 xixi hehe #仓库描述信息

baseurl=http://classroom.example.com/content/rhel7.0/x86\_64/dvd/ #指定服务端位置

enabled=1 #是否启用本文件配置

gpgcheck=0 #是否检测红帽签名信息

[root@server0 ~]# yum repolist #显示仓库信息

[root@server0 ~]# yum -y install sssd

[root@server0 ~]# yum -y install httpd

yum的使用

[root@server0 ~]# yum info 软件名

[root@server0 ~]# yum info vsftpd #查询软件介绍信息

[root@server0 ~]# yum remove 软件名

[root@server0 ~]# yum remove httpd #卸载软件

清空Yum的缓存

[root@server0 ~]# yum clean all

已加载插件：langpacks

正在清理软件源： haha

Cleaning up everything

[root@server0 ~]# yum repolist

案例2:升级Linux内核

1.下载新的内核软件包

[root@server0~]#wget http://classroom.example.com/content/rhel7.0/x86\_64/errata/Packages/kernel-3.10.0-123.1.2.el7.x86\_64.rpm

[root@server0 ~]# ls

[root@server0 ~]# uname -r

3.10.0-123.el7.x86\_64

[root@server0 ~]# rpm -ivh /root/kernel-3.10.0-123.1.2.el7.x86\_64.rpm

[root@server0 ~]# reboot

17.分区规划及使用

扇区默认大小 512字节

容量单位: EB

1EB=1024\*1024TB

一块硬盘的“艺术”之旅

• 识别硬盘 => 分区规划 => 格式化 => 挂载使用

毛坯楼层 => 打隔断 => 装修 =>入驻

一 识别硬盘

sd:SCSI设备 hd:IDE设备 vd:虚拟设备

[root@server0 ~]# lsblk #查看当前系统所有的硬盘信息

NAME SIZE TYPE MOUNTPOINT

vda 10G disk

└─vda1 10G part /

vdb 10G disk

二 分区规划

• MBR/msdos 分区模式

– 1~4个主分区,或者 3个主分区+1个扩展分区(n个逻辑分区)

– 最大支持容量为 2.2TB 的磁盘

– 扩展分区不能格式化

/dev/sda1:第一块SCSI硬盘,第一个主分区

/dev/sda5:第一块SCSI硬盘,第1个逻辑分区

• 修改硬盘的分区表,分出两个主分区,大小都为2G

[root@server0 ~]# fdisk /dev/vdb

n 创建新的分区--->回车--->回车-->回车--->在last结束时 +2G

p 查看分区表

n 创建新的分区--->回车---->回车--->回车--->在last结束时 +2G

d 删除分区

w 保存并退出

[root@server0 ~]# lsblk

[root@server0 ~]# ls /dev/vdb[1-2]

三 格式化 :赋予空间文件系统的过程

文件系统:存储数据的规则

Windows: NTFS FAT

Linux: ext4(RHEL6) xfs(RHEL7)

[root@server0 ~]# mkfs.ext4 /dev/vdb1 #格式化为ext4

[root@server0 ~]# blkid /dev/vdb1 #查看文件系统类型

[root@server0 ~]# mkfs.xfs /dev/vdb2 #格式化为xfs

[root@server0 ~]# blkid /dev/vdb2 #查看文件系统类型

四 挂载使用

[root@server0 ~]# mkdir /mypart1

[root@server0 ~]# mount /dev/vdb1 /mypart1

[root@server0 ~]# df -h #正在挂载的设备使用情况

[root@server0 ~]# df -h

五 开机自动挂载 /etc/fstab

[root@server0 ~]# vim /etc/fstab

设备路径 挂载点 类型 参数 备份标记 检测顺序

/dev/vdb1 /mypart1 ext4 defaults 0 0

[root@server0 ~]# umount /mypart2

[root@server0 ~]# df -h

[root@server0 ~]# mount -a

检测/etc/fstab开机自动挂载配置文件,格式是否正确

检测/etc/fstab中,书写完成,但当前没有挂载的设备,进行挂载

[root@server0 ~]# df -h

综合分区:

最终实现3个主分区均为2G 划分扩展分区,划分2个逻辑分区均为1G

1.识别硬盘 lsblk

2.分区规划 fdisk

3.分区表刷新 partprobe

4.格式化 mkfs.ext4 mkfs.xfs blkid

5.挂载使用 mount df -h

6.开机自动挂载 /etc/fstab mount -a

18.LVM逻辑卷

综合分区:

图形添加一块100G硬盘,划分3个主分区,一个扩展分区,三个逻辑分区

[root@server0 ~]# lsblk

[root@server0 ~]# fdisk /dev/vdc

[root@server0 ~]# lsblk

LVM逻辑卷

1.整合分散的空间(分区或整个磁盘)

2.空间的可以扩大

– 零散空闲存储 ---- 整合的虚拟磁盘 ---- 虚拟的分区

物理卷(pv) Physical Volume

卷组(vg) Volume Group

逻辑卷(lv) Logical Volume

将众多的物理卷,整合成卷组,再从卷组中划分逻辑卷

LVM管理工具集

功能 物理卷管理 卷组管理 逻辑卷管理

Scan 扫描 pvscan vgscan lvscan

Create 创建 pvcreate vgcreate lvcreate

Display 显示 pvdisplay vgdisplay lvdisplay

Remove 删除 pvremove vgremove lvremove

Extend 扩展 / vgextend lvextend

一 制作逻辑卷

successfully(成功)

1.制作卷组

命令格式: vgcreate 卷组名 设备路径

]# vgcreate systemvg /dev/vdb /dev/vdc1

]# vgs #查看卷组信息

]# pvs #查看物理卷信息

2.创建逻辑卷

命令格式:lvcreate -L 大小 -n 逻辑卷名称 基于卷组名

]# lvcreate -L 16G -n vo systemvg

]# lvs #查看逻辑卷信息

]# vgs

]# ls /dev/systemvg/vo #查看逻辑卷设备文件

]# ls -l /dev/systemvg/vo

3.逻辑卷的使用

]# mkfs.xfs /dev/systemvg/vo #格式化文件系统

]# blkid /dev/systemvg/vo #查看文件系统

]# vim /etc/fstab

/dev/systemvg/vo /mylv xfs defaults 0 0

]# mkdir /mylv

]# mount -a #测试是否书写正确

]# df -h #显示正在挂载设备的使用情况

19.逻辑卷的扩展

一 卷组有足够的剩余空间

1.扩展空间

[root@server0 ~]# lvs

[root@server0 ~]# vgs

[root@server0 ~]# lvextend -L 18G /dev/systemvg/vo

[root@server0 ~]# lvs

2.文件系统的扩展

扩展ext4文件系统: resize2fs

扩展xfs文件系统: xfs\_growfs

[root@server0 ~]# df -h

[root@server0 ~]# xfs\_growfs /dev/systemvg/vo

[root@server0 ~]# df -h

二 卷组没有足够的剩余空间

1.扩展卷组空间

]# vgextend systemvg /dev/vdc2 /dev/vdc3

]# vgs

2.扩展逻辑卷空间

[root@server0 ~]# lvs

[root@server0 ~]# vgs

[root@server0 ~]# lvextend -L 25G /dev/systemvg/vo

[root@server0 ~]# lvs

3.文件系统的扩展

[root@server0 ~]# df -h

[root@server0 ~]# xfs\_growfs /dev/systemvg/vo

[root@server0 ~]# df -h

了解:逻辑卷也可以做缩小 首先缩小文件系统,在缩减空间

ext4支持缩小 xfs不支持缩小

补充内容: 卷组划分空间的单位 PE 默认 1PE=4MB

[root@server0 ~]# vgdisplay systemvg #显示卷组详细信息

PE Size 4.00 MiB

创建一个逻辑卷名为lvredhat,大小为250M

]# vgchange -s 1M systemvg

]# vgdisplay systemvg

]# lvcreate -L 250M -n lvtest systemvg

]# lvs

修改PE的大小为1M

创建一个逻辑卷为500个PE组成

逻辑卷名为lvtest

-l:PE的个数

]# vgchange -s 1M systemvg #修改PE的大小

]# vgdisplay systemvg #查看卷组详细信息,PE的大小

]# lvcreate -l 500 -n lvtest systemvg

]# lvs

逻辑卷的删除:

首先删除逻辑卷,然后在删除卷组(基于该卷组没有任何的逻辑卷)

[root@server0 ~]# lvremove /dev/systemvg/lvredhat

Do you really want to remove active logical volume lvredhat? [y/n]: y

Logical volume "lvredhat" successfully removed

[root@server0 ~]# lvs

[root@server0 ~]# lvremove /dev/systemvg/vo

Logical volume systemvg/vo contains a filesystem in use.

[root@server0 ~]# umount /mylv/

[root@server0 ~]# lvremove /dev/systemvg/vo

Do you really want to remove active logical volume vo? [y/n]: y

Logical volume "vo" successfully removed

[root@server0 ~]# lvs

[root@server0 ~]# vgs

VG #PV #LV #SN Attr VSize VFree

systemvg 4 0 0 wz--n- 39.98g 39.98g

[root@server0 ~]# vgremove systemvg

Volume group "systemvg" successfully removed

[root@server0 ~]# vgs

20.查找文件

• 根据预设的条件递归查找对应的文件

– find [目录] [条件1] [-a|-o] [条件2] ...

– 常用条件表示:

-type 类型(f文件、d目录、l快捷方式)

-name '文档名称'

[root@server0 ~]# find /boot/ -type d #目录查找

[root@server0 ~]# find /boot/ -type f #文件查找

[root@server0 ~]# find /boot/ -type l #快捷方式查找

[root@server0 ~]# find /etc/ -name 'passwd' #文档名称查找

[root@server0 ~]# find /etc/ -name '\*tab'

[root@server0 ~]# find /etc/ -name '\*tab\*'

[root@server0 ~]# find /etc/ -name '\*.conf'

]# find /root/ -name 'nsd\*' -a -type f

]# find /root/ -name 'nsd\*' -type f

]# find /root/ -name 'nsd\*' -type d

-size +或-文件大小(k、M、G)

-user 用户名 #按照数据的所有者进行查找

[root@server0 ~]# find /boot/ -size +10M #大于10M的

[root@server0 ~]# find /boot/ -size -10M

[root@server0 ~]# find /boot/ -size +300k

/proc:不占用磁盘空间,占用内存空间

[root@server0 ~]# find / -user student

[root@server0 ~]# find /home -user student

-mtime 根据文件修改时间

-mtime +10 #10天之前的数据

-mtime -10 #最近10天之内的数据

[root@server0 ~]# find /root/ -mtime +1000

[root@server0 ~]# find /root/ -mtime +10

[root@server0 ~]# find /root/ -mtime -2

三个月以前:

[root@server0 ~]# find /root/ -mtime +90

21.find扩展使用

• 使用find命令的 -exec 操作

– find .. .. -exec 处理命令 {} \;

– 优势:以 {} 代替每一个结果,逐个处理,遇 \; 结束

]# find /boot/ -size +10M

]# find /boot/ -size +10M -exec cp {} /opt \;

]# find /root/ -name 'nsd\*' -exec rm -rf {} \;

案例4:查找并处理文件

• 使用find命令完成以下任务

– 找出所有用户 student 拥有的文件

– 把它们拷贝到 /root/findfiles/ 文件夹中

]# find / -user student -type f -exec cp {} /root/findfiles/ \;

22.grep用法

显示文件的有效信息(去除注释行,去除空行)

]# grep -v ^# /etc/login.defs

]# grep -v ^# /etc/login.defs | grep -v ^$

]# grep -v ^# /etc/login.defs | grep -v ^$ > /opt/1.txt

]# less /opt/1.txt

在Linux大多数配置文件中,以#开头的行为注释行

^$ : 匹配空行

23.NTP时间同步

查看修改系统时间:

[root@server0 ~]# date

[root@server0 ~]# date -s '年-月-日 时:分:秒'

[root@server0 ~]# date -s '2008-10-1 12:10:1'

2008年 10月 01日 星期三 12:10:01 CST

NTP网络时间协议

• Network Time Protocol

– NTP服务器为客户机提供标准时间

– NTP客户机需要与NTP服务器保持沟通

NTP服务器:虚拟机classroom提供标准时间

NTP客户机:虚拟机server同步时间

1.安装chrony客户端软件,寻找时间服务器

[root@server0 ~]# yum -y install chrony

[root@server0 ~]# rpm -q chrony

chrony-1.29.1-1.el7.x86\_64

2.修改配置文件

[root@server0 ~]# vim /etc/chrony.conf

#server 0.rhel.pool.ntp.org iburst

#server 1.rhel.pool.ntp.org iburst

#server 2.rhel.pool.ntp.org iburst

server classroom.example.com iburst #指定服务端

3.重启程序(重启服务)

daemon 英 [ˈdiːmən] 美 [ˈdiːmən](古希腊神话中的)半神半人精灵

]# systemctl restart chronyd #重启程序

]# systemctl enable chronyd #设置开机自启动

4.测试验证:

[root@server0 ~]# date -s '2000-10-1'

2000年 10月 01日 星期日 00:00:00 CST

[root@server0 ~]# systemctl restart chronyd

[root@server0 ~]# date

2000年 10月 01日 星期日 00:00:13 CST

[root@server0 ~]# date

2019年 07月 05日 星期五 16:21:59 CST

24.准备交换空间(虚拟内存)

缓解真实物理内存的压力

• 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

一 利用fdisk进行分区,划分两个主分区分别为2G

[root@server0 ~]# fdisk /dev/vdb

[root@server0 ~]# lsblk

二 格式化为交换文件系统

[root@server0 ~]# mkswap /dev/vdb1 #专业格式化交换文件系统

[root@server0 ~]# blkid /dev/vdb1 #查看文件系统类型

三 启用交换分区

[root@server0 ~]# swapon /dev/vdb1 #启用交换分区

[root@server0 ~]# swapon -s #查看交换空间的成员信息

[root@server0 ~]# swapoff /dev/vdb1 #停用交换分区

[root@server0 ~]# swapon -s

四 开机自动启用交换分区

[root@server0 ~]# vim /etc/fstab

/dev/vdb1 swap swap defaults 0 0

[root@server0 ~]# swapoff /dev/vdb1

[root@server0 ~]# swapon -s

[root@server0 ~]# swapon -a #专门检测/etc/fstab交换分区

[root@server0 ~]# swapon -s

25.补充内容:触发挂载(autofs)

准备工作:在划分一个2G的主分区

[root@server0 ~]# fdisk /dev/vdb

[root@server0 ~]# partprobe #刷新分区表

[root@server0 ~]# lsblk

[root@server0 ~]# mkfs.xfs /dev/vdb3 #格式化文件系统

[root@server0 ~]# blkid /dev/vdb3

1.安装触发挂载的软件包

[root@server0 ~]# yum -y install autofs

2.重启autofs程序

[root@server0 ~]# systemctl restart autofs

[root@server0 ~]# systemctl enable autofs

3.完成对/dev/vdb3触发挂载的配置

最终实现:访问路径/nsd/dc 挂载设备/dev/vdb3 到/nsd/dc

主配置文件:定义监控目录/etc/auto.master

格式:监控目录路径 挂载配置文件路径

挂载配置文件:定义挂载点目录与设备

cd -fstype=iso9660,ro,nosuid,nodev :/dev/cdrom

挂载点目录 -fstype=文件系统 :挂载设备

[root@server0 /]# mkdir /nsd #必须手动创建监控目录

[root@server0 /]# vim /etc/auto.master

/nsd /etc/test

格式:监控目录路径 挂载配置文件路径

[root@server0 /]# cp /etc/auto.misc /etc/test

[root@server0 /]# vim /etc/test #修改挂载配置文件

dc -fstype=xfs :/dev/vdb3

格式: 挂载点目录 -fstype=文件系统 :挂载设备

[root@server0 /]# systemctl restart autofs

[root@server0 /]# systemctl status autofs #查看服务状态

[root@server0 /]# ls /nsd/dc

[root@server0 /]# df -h

# 第二部分 云计算应用管理

1.系统安全保护

SELinux安全机制

• Security-Enhanced Linux

– 美国NSA国家安全局主导开发,一套增强Linux系统安

全的强制访问控制体系

– 集成到Linux内核(2.6及以上)中运行

– RHEL7基于SELinux体系针对用户、进程、目录和文件

提供了预设的保护策略,以及管理工具

SELinux的运行模式

– enforcing(强制)、permissive(宽松)

– disabled(彻底禁用)

任何模式切换成disabled模式,都要经历重启

切换运行模式

– 临时切换:setenforce 1|0

– 固定配置:/etc/selinux/config 文件

虚拟机server0

[root@server0 ~]# getenforce #查看当前的状态

[root@server0 ~]# setenforce 0 #临时修改为宽松模式

[root@server0 ~]# getenforce

[root@server0 ~]# vim /etc/selinux/config

SELinux=permissive

启用selinux:source /etc/selinux/config

2.alias别名设置

• 查看已设置的别名

– alias [别名名称]

• 定义新的别名

– alias 别名名称= '实际执行的命令行'

• 取消已设置的别名

– unalias [别名名称]

• 影响指定用户的 bash 解释环境

– ~/.bashrc,每次开启 bash 终端时生效

• 影响所有用户的 bash 解释环境

– /etc/bashrc,每次开启 bash 终端时生效

[root@server0 ~]# vim /root/.bashrc

alias hello='echo hello'

[root@server0 ~]# vim /home/student/.bashrc

alias hi='echo hi'

新开一个终端验证

3.虚拟机server0:搭建Web服务器

Web服务:提供网页内容

实现Web服务的软件: httpd Nginx Tomcat

实现Web通信的协议: http(超文本传输协议)

1.安装httpd软件

[root@server0 ~]# yum -y install httpd

2.重启程序(重启服务)

[root@server0 ~]# systemctl restart httpd

3.本机测试访问

[root@server0 ~]# firefox 172.25.0.11

4.书写自己的页面文件

默认存放路径:/var/www/html

默认首页文件名称:index.html

[root@server0 ~]# vim /var/www/html/index.html

<marquee><font color=red><h1>NSD1906 haha

滚动 字体颜色 标题字体

[root@server0 ~]# firefox 172.25.0.11

4.虚拟机server0:搭建FTP服务

FTP服务:传输数据

FTP协议:文件传输协议

实现FTP服务软件:vsftpd

默认共享路径:/var/ftp

1.安装vsftpd软件

[root@server0 ~]# yum -y install vsftpd

2.重启程序(重启服务)

[root@server0 ~]# systemctl restart vsftpd

[root@server0 ~]# firefox <ftp://172.25.0.11>

5.防火墙策略管理

作用: 隔离 众多的策略,允许出站,严格控制入站

硬件防火墙

软件防火墙

firewalld服务基础

• 系统服务:firewalld

• 管理工具:firewall-cmd、firewall-config

预设安全区域

• 根据所在的网络场所区分,预设保护规则集

– public:仅允许访问本机的ssh dhcp ping服务

– trusted:允许任何访问

– block:阻塞任何来访请求(明确拒绝,有回应客户端)

– drop:丢弃任何来访的数据包(没有回应,节省服务端资源)

根据数据包的源IP地址

数据包: 源IP地址 目标IP地址 数据

防火墙判定原则:

1.查看数据包的源IP地址,然后查看自己所有的区域,那个区域中有该源IP地址的规则,则进入该区域

2.进入默认区域(public)

防火墙默认区域的修改

虚拟机server:

]# firewall-cmd --get-default-zone #查看默认区域

虚拟机desktop:

]# ping 172.25.0.11 #可以通信,有回应

虚拟机server:

]# firewall-cmd --set-default-zone=block #修改默认区域

]# firewall-cmd --get-default-zone

虚拟机desktop:

]# ping 172.25.0.11 #不可以通信,有回应

虚拟机server:

]# firewall-cmd --set-default-zone=drop

]# firewall-cmd --get-default-zone

虚拟机desktop:

]# ping 172.25.0.11 #不可以通信,没有回应

互联网常见的协议:

http:超文本传输协议 默认端口:80

https:安全的超文本传输协议 默认端口:443

DNS:域名解析协议 默认端口:53

FTP:文件传输协议 默认端口:21

tftp:简单的文件传输协议 默认端口:69

telnet:远程管理协议(明文传输) 默认端口:23

ssh:远程管理协议(加密传输) 默认端口:22

SMTP:邮件协议(用户发邮件) 默认端口:25

pop3:邮件协议(用户收邮件) 默认端口:110

snmp:简单的网络管理协议 默认端口:161

防火墙区域添加允许的协议

虚拟机server

]# firewall-cmd --set-default-zone=public #修改默认区域

]# firewall-cmd --zone=public --list-all #查看区域规则

]# firewall-cmd --zone=public --add-service=ftp #添加协议

]# firewall-cmd --zone=public --add-service=http

]# firewall-cmd --zone=public --list-all

虚拟机desktop

[root@desktop0 ~]# firefox 172.25.0.11 #访问成功

[root@desktop0 ~]# firefox ftp://172.25.0.11 #访问成功

#防火墙规则的永久设置

– 永久(permanent)

]# firewall-cmd --reload #重新加载防火墙所有配置

]# firewall-cmd --zone=public --list-all

]# firewall-cmd --permanent --zone=public --add-service=http #永久添加协议

]# firewall-cmd --permanent --zone=public --add-service=ftp

单独拒绝虚拟机desktop访问

虚拟机server:将虚拟机desktop的IP地址写入block

]# firewall-cmd --zone=block --add-source=172.25.0.10 #添加IP到防火墙规则

]# firewall-cmd --zone=block --list-all

虚拟机desktop:

]# firefox 172.25.0.11 #访问失败

]# firefox ftp://172.25.0.11 #访问失败

真机:

]# firefox 172.25.0.11 #可以进行访问

]# firefox ftp://172.25.0.11 #可以进行访问

虚拟机server: 删除规则

]# firewall-cmd --zone=block --remove-source=172.25.0.10 #将IP从防火墙规则中删除

虚拟机desktop:

]# firefox 172.25.0.11 #可以进行访问

]# firefox ftp://172.25.0.11 #可以进行访问

端口: 协议或程序或服务的编号

利用root可以改变端口,而且一个程序可以具备多个端口

监听端口

实现本机的端口映射

• 本地应用的端口重定向(端口1 --> 端口2)

客户端访问: firefox 172.25.0.11:5423--->172.25.0.11:80

虚拟机server:

]# firewall-cmd --permanent --zone=public

--add-forward-port=port=5423:proto=tcp:toport=80

]# firewall-cmd --reload

]# firewall-cmd --zone=public --list-all

虚拟机desktop:

[root@desktop0 ~]# firefox 172.25.0.11:5423

6.iSCSI网络磁盘

• Internet SCSI,网际SCSI接口 默认端口:3260

– 一种基于C/S架构的虚拟磁盘技术

– 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

– 对应到服务端提供实际存储空间的设备,需要起一个管理名称

• target,磁盘组

– 是客户端的访问目标,作为一个框架,由多个lun组成

• lun,逻辑单元

– 每一个lun需要关联到某一个后端存储设备,在客户端

会视为一块虚拟硬盘

• ISCSI Qualified Name 名称规范(iqn)

– iqn.yyyy-mm.倒序域名:自定义标识

– 用来识别 target 磁盘组,也用来识别客户机身份

一 修改防火墙默认区域

虚拟机server

]# firewall-cmd --set-default-zone=trusted

虚拟机desktop

]# firewall-cmd --set-default-zone=trusted

二 划分一个5G的主分区

[root@server0 ~]# fdisk /dev/vdb

[root@server0 ~]# lsblk

虚拟机server服务端:

1.安装软件包targetcli

[root@server0 ~]# yum -y install targetcli

2.运行targetcli命令进行配置

[root@server0 ~]# targetcli

/> ls #查看相关配置

1)建立后端存储backstore,后端存储

/> backstores/block create name=nsd dev=/dev/vdb1

2)建立target磁盘组

/> iscsi/ create iqn.2019-07.com.example:server

3)进行lun关联

/> iscsi/iqn.2019-07.com.example:server/tpg1/luns create /backstores/block/nsd

4)设置访问控制,客户端声称的名字,符合iqn名称规范

/> iscsi/iqn.2019-07.com.example:server/tpg1/acls create iqn.2019-07.com.example:desktop

5)设置监听的IP地址

/> iscsi/iqn.2019-07.com.example:server/tpg1/portals create ip\_address=172.25.0.11

三 重启服务(重启程序)

[root@server0 ~]# systemctl restart target

[root@server0 ~]# systemctl enable target #设置为开机自启

虚拟机desktop

1.安装软件包(客户端软件)

• 所需软件包:iscsi-initiator-utils

[root@desktop0 ~]# yum repolist

[root@desktop0 ~]# rpm -q iscsi-initiator-utils

iscsi-initiator-utils-6.2.0.873-21.el7.x86\_64

[root@desktop0 ~]# yum -y install iscsi(tab)

2.设置客户端生成的名字

[root@desktop0 ~]# vim /etc/iscsi/initiatorname.iscsi

InitiatorName=iqn.2019-07.com.example:desktop

3.客户端刷新声称名字的服务

[root@desktop0 ~]# systemctl restart iscsid

Warning: Unit file of iscsid.service changed on

disk, 'systemctl daemon-reload' recommended.

[root@desktop0 ~]# systemctl daemon-reload

[root@desktop0 ~]# systemctl restart iscsid

4.发现共享存储

Linux查看命令帮助的方法 : man iscsiadm

全文查找/example 按n项下跳转匹配,看到EXAMPLES

[root@desktop0 ~]# iscsiadm --mode discoverydb --type sendtargets --portal 172.25.0.11 --discover

方法二:发现iSCSI磁盘

– iscsiadm -m discovery -t st -p 服务器地址[:端口]

5.加载共享存储

[root@desktop0 ~]# systemctl restart iscsi

[root@desktop0 ~]# systemctl enable iscsi

[root@desktop0 ~]# lsblk

7.数据库服务基础

什么是数据库: 存放数据的仓库

数据库中有众多库,在每一个库中有众多的表格

• 常见的关系型 数据库管理系统

– 微软的 SQL Server

– IBM的 DB2

– 甲骨文的 Oracle、MySQL

– 社区开源版 MariaDB

database:数据库

虚拟机server:部署mariadb数据库服务器

• RHEL7 中的 MariaDB相关包

mariadb-server :提供服务端有关的系统程序

[root@server0 ~]#yum -y install mariadb-server

[root@server0 ~]# systemctl restart mariadb

[root@server0 ~]# systemctl enable mariadb

[root@server0 ~]#

数据库的基本操作:

[root@server0 ~]# mysql #进入数据库

MariaDB [(none)]> show databases; #查看所有的库

MariaDB [(none)]> create database nsd; #创建nsd库

MariaDB [(none)]> show databases;

MariaDB [(none)]> drop database nsd; #删除nsd库

MariaDB [(none)]> show databases;

MariaDB [(none)]> create database nsd1906;

MariaDB [(none)]> show databases;

MariaDB [(none)]> use mysql; #切换到mysql库

MariaDB [nsd1906]> use mysql;

MariaDB [mysql]> show tables; #查看当前库中有哪些表格

MariaDB [mysql]> exit #退出整个数据库

在Linux命令行,为数据库管理员设置密码

数据库管理员为root,对数据库有最高权限用户,存放在mysql库user表

Linux系统管理员为root,对系统有最高权限用户,存放/etc/passwd

• 为数据库账号修改密码

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

]# mysqladmin -u root password '123' #首次设置密码

]# mysql -u root -p #交互式进入

Enter password:

]# mysql -u root -p123 #非交互式进入

已知旧密码修改新密码

]# mysqladmin -u root -p123 password '456'

##################################################

MariaDB主配置文件:

[root@server0 ~]# ls /etc/my.cnf

##################################################

表格 : 增(insert) 删(delete) 改(update) 查(select)

• 导入/恢复到数据库

– mysql [-u用户名] [-p[密码]] 数据库名 < 备份文件.sql #导入数据库

[root@server0 ~]# wget http://classroom.example.com/pub/materials/users.sql

[root@server0 ~]# ls

]# mysql -u root -p123 nsd1906 < /root/users.sql

]# mysql -u root -p123 #进入到数据库

MariaDB [(none)]> use nsd1906; #切换到nsd1906库

MariaDB [nsd1906]> show tables; #显示所有表格

查(select)

格式: select 表字段 from 库名.表名 where 条件 ;

]# mysql -u root -p123 #进入到数据库

> use nsd1906; #切换到nsd1906库

> show tables; #显示所有表格

> select \* from base; #查看表所有字段及所有记录内容

> select \* from location; #查看表所有字段及所有记录内容

###################################################

查询表结构: desc 表名;

MariaDB [(none)]> use nsd1906;

MariaDB [nsd1906]> desc base;

MariaDB [nsd1906]> use mysql;

MariaDB [mysql]> desc user;

MariaDB [mysql]> select user,host,password from user;

数据库授权

用户授权设置

• MariaDB [(none)]> 交互指令

– GRANT 权限列表 ON 数据库名.表名 TO 用户名@

客户机地址 IDENTIFIED BY '密码';

– 除了 root 用户,此nsd1906数据库只能被用户 lisi 查询,

此用户的密码为123

> grant select on nsd1906.\* to lisi@localhost identified by '123';

当lisi从localhost本地登录,输入密码123,将会获得nsd1906库中所有表格的查询权限;

> select user,host,password from user;

案例4:使用数据库查询

2. 在系统 server0 上使用数据库 nsd1906,并使用相

应的 SQL 查询以回答下列问题:

1)密码是 solicitous 的人的名字?

[root@server0 ~]# mysql -u root -p123

> use nsd1906;

> select \* from base;

> select \* from base where password='solicitous';

> select name from base where password='solicitous';

2)有多少人的姓名是 Barbara 同时居住在 Sunnyvale?

> select \* from base,location

where base.name='Barbara' and

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

> select count(\*) from base,location

where base.name='Barbara' and

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

> insert base values('6','Barbara','xixi'); #插入记录

> select \* from base;

> insert location values('6','Sunnyvale'); #插入记录

> select \* from location;

1. 禁止空密码root用户访问 mariadb 数据库

> use mysql;

> select user,host,password from user;

> select user,host,password from user where password='';

> delete from user where password=''; #删除记录

> select user,host,password from user;

> flush privileges; #刷新user表记录

验证登录失败:

[root@server0 ~]# mysql -u root -h server0.example.com

8.NFS共享

环境准备:防火墙设置

虚拟机server

]# firewall-cmd --set-default-zone=trusted

虚拟机desktop

]# firewall-cmd --set-default-zone=trusted

NFS共享概述

• Network File System,网络文件系统

– 用途:为客户机提供共享使用的文件夹

– 协议:NFS(TCP/UDP 2049)、RPC(TCP/UDP 111)

• 所需软件包:nfs-utils

• 系统服务:nfs-server

虚拟机server:构建NFS服务

1.安装nfs-utils软件包

[root@server0 ~]# rpm -q nfs-utils

nfs-utils-1.3.0-0.el7.x86\_64

2.配置共享

[root@server0 ~]# mkdir /nsd

[root@server0 ~]# echo 123 > /nsd/1.txt

[root@server0 ~]# ls /nsd/

[root@server0 ~]# vim /etc/exports

– 文件夹路径 客户机地址(权限) 客户机地址(权限) .. ..

/nsd \*(ro)

3.重启服务(重启程序)

[root@server0 ~]# systemctl restart nfs-server

虚拟机desktop:访问共享文件夹

1.挂载共享目录

]# mkdir /mnt/a /mnt/b

]# showmount -e 172.25.0.11 #查看服务端共享内容

]# mount 172.25.0.11:/nsd /mnt/a/

]# df -h

]# ls /mnt/a

]# df -ah #显示当前全部的挂载

2.开机自动挂载/etc/fstab

\_netdev:声明网络设备

指明挂载本设备需要有网络参数再进行挂载

[root@desktop0 ~]# vim /etc/fstab

172.25.0.11:/nsd /mnt/a nfs defaults,\_netdev 0 0

[root@desktop0 ~]# umount /mnt/a

[root@desktop0 ~]# umount /mnt/b

[root@desktop0 ~]# df -ah

[root@desktop0 ~]# mount -a

[root@desktop0 ~]# df -ah

9.HTTP服务基础

Web服务:提供网页内容

• 基于 B/S (Browser/Server)架构的网页服务

– 服务端提供网页

– 浏览器下载并显示网页

• 软件包:httpd(Apache组织) #专门实现Web服务的软件

虚拟机server:

1.安装httpd软件

[root@server0 ~]# yum -y install httpd

2.重启服务

[root@server0 ~]# systemctl restart httpd

3.访问测试

[root@server0 ~]# firefox 172.25.0.11

4.书写页面文件

]# echo '<h1>NSD1906 Web' > /var/www/html/index.html

]# cat /var/www/html/index.html

]# firefox 172.25.0.11

主配置文件配置字段:

– 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)

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

虚拟机classroom:

DNS服务器的解析:将域名解析为IP地址

server0.example.com----->172.25.0.11

www0.example.com----->172.25.0.11

webapp0.example.com----->172.25.0.11

[root@desktop0 ~]# nslookup webapp0.example.com

[root@desktop0 ~]# nslookup server0.example.com

[root@desktop0 ~]# nslookup www0.example.com

– DocumentRoot:网页文件的根目录(/var/www/html)

虚拟机server

]# mkdir /var/www/myweb

]# echo '<h1>wo shi myweb' > /var/www/myweb/index.html

]# cat /var/www/myweb/index.html

]# vim /etc/httpd/conf/httpd.conf

DocumentRoot "/var/www/myweb"

]# systemctl restart httpd

虚拟机desktop:测试

[root@desktop0 ~]# firefox 172.25.0.11

#####################################################

网络路径与实际服务器路径 网页文件的根目录

客户端:firefox http://172.25.0.11:80---->服务端172.25.0.11

----->httpd 80----->DocumentRoot /var/www/myweb--->index.html

客户端: firefox 172.25.0.11

服务端: /var/www/myweb

客户端: firefox 172.25.0.11/abc

服务端: /var/www/myweb/abc/index.html

DocmentRoot /var/www/myweb

客户端: firefox 172.25.0.11/var/www/myweb/abc

服务端: /var/www/myweb/var/www/myweb/abc

虚拟机server:

]# mkdir /var/www/myweb/abc

]# echo '<h1>wo shi abc' > /var/www/myweb/abc/index.html

]# firefox 172.25.0.11/abc

vsftpd----->/var/ftp

httpd------>/var/www/html

10.虚拟Web主机

• 虚拟Web主机

– 由同一台服务器提供多个不同的Web站点

• 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

• 配置文件路径

– /etc/httpd/conf/httpd.conf #主配置文件

– /etc/httpd/conf.d/\*.conf #调用配置文件

• 为每个虚拟站点添加配置

<VirtualHost IP地址:端口>

ServerName 此站点的DNS名称

DocumentRoot 此站点的网页根目录

</VirtualHost>

虚拟机server: vim命令模式下 u 可以撤销

虚拟Web主机优先级,由上到下依次匹配,匹配即停止

一旦使用虚拟Web主机功能,所有的网站都必须利用虚拟Web主机实现

[root@server0 ~]# vim /etc/httpd/conf.d/nsd01.conf

<VirtualHost \*:80>

ServerName www0.example.com

DocumentRoot /var/www/baidu

</VirtualHost>

<VirtualHost \*:80>

ServerName server0.example.com

DocumentRoot /var/www/qq

</VirtualHost>

<VirtualHost \*:80>

ServerName webapp0.example.com

DocumentRoot /var/www/myweb

</VirtualHost>

[root@server0 ~]# systemctl restart httpd

###########################################################

Web访问控制,针对存放网页文件的目录

子目录默认继承父目录的Web访问控制

<Directory />

Require all denied #拒绝所有人访问

</Directory>

<Directory "/var/www">

Require all granted #允许所有人访问

</Directory>

案例:自定义Web的网页文件根目录

1.实现server0.example.com访问网页文件根目录修改为/webroot

]# vim /etc/httpd/conf.d/nsd01.conf

<VirtualHost \*:80>

ServerName server0.example.com

DocumentRoot /webroot

</VirtualHost>

]# mkdir /webroot

]# echo '<h1>wo shi webroot' > /webroot/index.html

2.修改访问控制

[root@server0 ~]# vim /etc/httpd/conf/httpd.conf

[root@server0 ~]# vim /etc/httpd/conf.d/nsd02.conf

<Directory "/webroot"> #针对/webroot路径

Require all granted #允许所有人访问

</Directory>

[root@server0 ~]# systemctl restart httpd

3.SELinux策略

[root@server0 ~]# setenforce 0

[root@server0 ~]# getenforce

Permissive

[root@server0 ~]# vim /etc/selinux/config

SELINUX=permissive

[root@server0 ~]# firefox server0.example.com

环境准备:防火墙设置

虚拟机server

]# firewall-cmd --set-default-zone=trusted

虚拟机desktop

]# firewall-cmd --set-default-zone=trusted

文件夹权限

• 针对 DocumentRoot 网页目录的权限控制

– httpd 运行身份(用户/组):apache

客户机地址限制

• 使用 <Directory> 配置区段

– 每个文件夹自动继承其父目录的ACL访问权限

– 除非针对子目录有明确设置

<Directory 目录的绝对路径>

.. ..

Require all denied|granted

Require ip IP或网段地址 .. ..

</Directory>

案例1:配置网页内容访问

在 Web 网站 http://server0.example.com 的

DocumentRoot 目录下创建一个名为 private 的子目录,要求如下:

1.创建目录

]# cat /etc/httpd/conf.d/nsd01.conf #查看DocumentRoot

]# mkdir /var/www/abc01/private

2.从 http://classroom.example.com/pub/materials/private.html下载一个文件副本到这个目录,重命名为 index.html

不要对文件 index.html 的内容作任何修改

]# cd /var/www/abc01/private

]# wget http://classroom.example.com/pub/materials/private.html

]# mv private.html index.html

]# firefox server0.example.com/private

3.从虚拟机server0 上,任何人都可以浏览 private 的内容

但是从其他系统不能访问这个目录的内容

[root@server0 /]# vim /etc/httpd/conf/httpd.conf

[root@server0 /]# vim /etc/httpd/conf.d/nsd02.conf

<Directory "/var/www/abc01/private">

Require ip 172.25.0.11 #仅允许172.25.0.11访问

</Directory>

[root@server0 /]# systemctl restart httpd

虚拟机desktop:

[root@desktop0 ~]# firefox server0.example.com/private

Forbidden

You don't have permission to access /private on this server.

####################################################

案例2:使用自定Web根目录

调整 Web 站点 http://server0.example.com 的网页目录,要求如下:

1)新建目录 /webroot,作为此站点新的网页目录

]# mkdir /webroot

]# echo '<h1> wo shi webroot' > /webroot/index.html

[root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf

<VirtUalHost \*:80>

ServerName server0.example.com

DocumentRoot /webroot

</VirtUalHost>

2)修改访问控制

[root@server0 /]# vim /etc/httpd/conf.d/nsd02.conf

<Directory "/webroot">

Require all granted #允许所有人可以访问

</Directory>

[root@server0 /]# systemctl restart httpd

3)修改SELinux策略:安全上下文值(打标签) 布尔值策略 非默认端口开放

]# semanage --help

]# semanage fcontext -l | less #查看所有上下文值

]# ls -Zd /var/www/ #专查看目录上下文值

]# ls -Zd /webroot/

• 方式1:参照标准目录,重设新目录的属性

– chcon [-R] --reference=模板目录 新目录

]# chcon -R --reference=/var/www /webroot/

]# ls -Zd /webroot/

测试:

[root@desktop0 ~]# firefox server0.example.com

11.部署动态网站

静态网站的运行

• 服务端的原始网页 = 浏览器访问到的网页

– 由Web服务软件处理所有请求

– 文本(txt/html)、图片(jpg/png)等静态资源

动态网站的运行

• 服务端的原始网页 ≠ 浏览器访问到的网页

– 由Web服务软件接受请求,动态程序转后端模块处理

– PHP网页、Python网页、JSP网页......

为站点 webapp0.example.com 配置提供动态Web内容,要求如下:

1.部署Python页面文件

]# cat /etc/httpd/conf.d/nsd01.conf #查看DocumentRoot

]# cd /var/www/abc03

]# wget http://classroom.example.com/pub/materials/webinfo.wsgi

]# ls

2.页面跳转(页面别名 地址重写)方便用户的访问

当用户访问 webapp0.example.com将webinfo.wsgi页面进行呈现

格式: Alias 网络路径 实际路径

Alias / /var/www/abc03/webinfo.wsgi

当用户访问的时网页文件根目录时,跳转到/var/www/abc03/webinfo.wsgi

[root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf

<VirtUalHost \*:80>

ServerName webapp0.example.com

DocumentRoot /var/www/abc03

Alias / /var/www/abc03/webinfo.wsgi

当用户访问的是网页文件根目录时,跳转到/var/www/abc03/webinfo.wsgi

</VirtUalHost>

[root@server0 /]# systemctl restart httpd

[root@desktop0 ~]# firefox webapp0.example.com

3.翻译Python页面代码

[root@server0 /]# yum -y install mod\_wsgi

[root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf

<VirtUalHost \*:80>

ServerName webapp0.example.com

DocumentRoot /var/www/abc03

WsgiScriptAlias / /var/www/abc03/webinfo.wsgi

</VirtUalHost>

[root@server0 /]# systemctl restart httpd

页面内容显示:

UNIX时间戳:从1970-1-1 0:0:0到达现在时间,所经历的秒数

[root@desktop0 ~]# firefox webapp0.example.com

4.此虚拟Web主机侦听在端口8909

[root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf

Listen 8909 #设置httpd程序监听8909端口

<VirtUalHost \*:8909> #设置虚拟Web主机监听8909端口

ServerName webapp0.example.com

DocumentRoot /var/www/abc03

WsgiScriptAlias / /var/www/abc03/webinfo.wsgi

</VirtUalHost>

]# semanage port -l | grep http #查看关于http开放的端口

]# semanage port -a -t http\_port\_t -p tcp 8909

此命令会占用较多内存, -a 添加 -t 类型 -p 协议

]# systemctl restart httpd

测试验证: firefox webapp0.example.com:8909

总结:访问时端口优先级最高

12.安全Web服务

PKI公钥基础设施

• 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、......)

– Certificate Authority,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

数据证书授权中心:虚拟机classroom

虚拟机server:

为站点 www0.example.com 配置安全加密的Web内容

1.部署网站证书(营业执照)

]# cd /etc/pki/tls/certs/

]# wget http://classroom.example.com/pub/tls/certs/server0.crt

2.部署网站的根证书(工商局的信息)

]# cd /etc/pki/tls/certs/

]# wget http://classroom.example.com/pub/example-ca.crt

3.部署解密数据的私钥

]# cd /etc/pki/tls/private/

]# wget http://classroom.example.com/pub/tls/private/server0.key

4.安装可以进行加密支持的软件mod\_ssl

[root@server0 /]# yum -y install mod\_ssl

[root@server0 /]# vim /etc/httpd/conf.d/ssl.conf

补充:vim末行模式 输入set nu 可以开启行号

59 DocumentRoot "/var/www/abc02"

60 ServerName www0.example.com:443

指定网站证书

100 SSLCertificateFile /etc/pki/tls/certs/server0.crt

指定解密的私钥

107 SSLCertificateKeyFile /etc/pki/tls/private/server0.key

指定网站的根证书

122 SSLCACertificateFile /etc/pki/tls/certs/example-ca.crt

[root@server0 /]# systemctl restart httpd

[root@server0 /]# firefox https://www0.example.com

我已了解可能的风险--->添加例外---->确认安全例外

###################################################

13.补充:Samba共享服务(Windows与Linux跨平台的共享)

smb(用户验证通信协议) cifs(Samba独有文件系统)

程序名(服务名):smb

虚拟机server:

1.安装软件包

[root@server0 /]# yum -y install samba

2.创建Samba共享帐号

1.建立在本地用户的基础上

2.采用独立的密码,与用户登录系统的密码不同

[root@server0 /]# useradd harry

[root@server0 /]# pdbedit -a harry #添加为samba帐号

new password:

retype new password:

[root@server0 /]# pdbedit -L #查看所有的samba帐号

[root@server0 /]# pdbedit -x harry #删除samba帐号harry

[root@server0 /]# pdbedit -a harry

3.创建共享目录及配置共享

[root@server0 /]# mkdir /public

[root@server0 /]# echo haha > /public/1.txt

[root@server0 /]# vim /etc/samba/smb.conf

命令模式: G(大写) 到全文的末行

[nsd] #设置共享名

path = /public #设置实际共享的路径

[root@server0 /]# systemctl restart smb

4.修改SELinux策略: 布尔值策略(服务功能的开关)

[root@server0 /]# getsebool -a | grep samba

[root@server0 /]# setsebool samba\_export\_all\_ro on

[root@server0 /]# getsebool -a | grep samba

客户端:虚拟机desktop0

1.安装软件包,支持cifs文件系统

[root@desktop0 ~]# yum -y install cifs-utils

2.进行挂载访问

]# mkdir /mnt/smb

格式:mount -o user=用户名,pass=密码 //服务器IP地址/共享名 挂载点目录

]# mount -o user=harry,pass=123 //172.25.0.11/nsd /mnt/smb/

]# df -h

]# ls /mnt/smb/

3.开机自动挂载/etc/fstab

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

[root@desktop0 ~]# umount /mnt/smb/

[root@desktop0 ~]# df -h

[root@desktop0 ~]# mount -a

[root@desktop0 ~]# df -h

14.设置网络参数

一 设置永久的主机名,配置文件为/etc/hostname

[root@server0 ~]# echo 'nsd.tedu.cn' > /etc/hostname

[root@server0 ~]# cat /etc/hostname

nsd.tedu.cn

[root@server0 ~]# hostname

二 永久设置设置IP地址 子网掩码 网关地址

1.查看识别的网卡名

[root@nsd ~]# nmcli connection show

名称

System eth0

2.设置永久的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

]# nmcli connection 修改 '网卡名'

ipv4.方法 手工设置

ipv4.地址 'IP地址/子网掩码 网关地址'

每次开机自动启用配置

3.激活配置

[root@nsd ~]# nmcli connection up 'System eth0'

[root@nsd ~]# ifconfig | head -2

[root@nsd ~]# route #查看网关地址

Gateway

172.25.0.254

三 DNS服务器的地址

永久配置文件:/etc/resolv.conf

]# echo 'nameserver 172.25.254.254' > /etc/resolv.conf

]# cat /etc/resolv.conf

nameserver 172.25.254.254

]# nslookup server0.example.com

15.聚合连接(链路聚合 网卡绑定)

作用:实现网卡的高可用

eth1 eth2

虚拟网卡:team0 192.168.1.1

1.生成虚拟的网卡team0 参考:man teamd.conf

全文搜索/example 按 n跳转匹配

]# nmcli connection add type team

con-name team0 ifname team0 autoconnect yes

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

]# nmcli connection 添加 类型 组队

配置文件名 team0 网卡名 team0 开机自动启用

配置运行方式为 活跃备份方式

]# ifconfig team0

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

]# nmcli connection 添加 类型 team-成员

配置文件名 team0-2 网卡名为 eth2 主设备 team0

3.team0配置IP地址

]# nmcli connection modify team0

ipv4.method manual ipv4.addresses 192.168.1.1/24

connection.autoconnect yes

]# nmcli connection up team0

]# teamdctl team0 state #专用于查看team0信息

]# ifconfig eth2 down

]# teamdctl team0 state

如果有敲错,删除所有重新开始

]# nmcli connection delete team0 #删除配置文件

]# nmcli connection delete team0-1 #删除配置文件

]# nmcli connection delete team0-2 #删除配置文件

16.基础邮件服务

前提:修改IP地址,符合DNS解析结果

[root@nsd ~]# nmcli connection modify 'System eth0'

ipv4.method manual

ipv4.addresses '172.25.0.11/24 172.25.0.254'

connection.autoconnect yes

[root@nsd ~]# nmcli connection up 'System eth0'

查看DNS服务器地址:

[root@nsd ~]# cat /etc/resolv.conf

nameserver 172.25.254.254

[root@nsd ~]# nslookup server0.example.com #测试解析

###########################################################

电子邮件通信

• 电子邮件服务器的基本功能

– 为用户提供电子邮箱存储空间(用户名@邮件域名)

– 处理用户发出的邮件 —— 传递给收件服务器

– 处理用户收到的邮件 —— 投递到邮箱

DNS服务器:虚拟机classroom

yg@qq.com

yg@server0.example.com

###########################################################

虚拟机server:构建邮件服务器

1.安装postfix软件,实现邮件服务

[root@nsd ~]# rpm -q postfix

postfix-2.10.1-6.el7.x86\_64

2.修改配置文件

[root@nsd ~]# vim /etc/postfix/main.cf

vim末行模式: set nu 开启行号

99 myorigin = server0.example.com #默认补全的域名后缀

116 inet\_interfaces = all #在本机所有网卡启用邮件功能

164 mydestination = server0.example.com #判断为本域邮件的依据

3.重启邮件服务

[root@nsd ~]# systemctl restart postfix

使用mail命令发信/收信

• mail 发信操作

– mail -s '邮件标题' -r 发件人 收件人

[root@nsd ~]# useradd yg

[root@nsd ~]# useradd xln

[root@nsd ~]# mail -s 'test01' -r yg xln

hahaxixihehelele

.

EOT

[root@nsd ~]# mail -u xln #查看xln的邮件

>N 1 yg@server0.example.c Sat Jul 13 14:2118/569

& 1 #输入邮件编号1查看邮件内容

[root@nsd ~]# echo '123' | mail -s 'abc' -r yg xln

[root@nsd ~]# mail -u xln

17.parted分区工具,进行GPT分区模式

MBR分区模式: fdisk分区工具

最多有4个主分区,划分3个主分区,1个扩展分区,n个逻辑分区

最大的空间支持:2.2TB

GPT分区模式:parted分区工具

最多有128个主分区

最大的空间支持:18EB

[root@nsd ~]# lsblk

[root@nsd ~]# parted /dev/vdb

(parted) mktable gpt #指定分区模式gpt

(parted) print #输出分区表信息

(parted) mkpart #划分新的分区

分区名称？ []? nsd #随意起名字

文件系统类型？ [ext2]? xfs #随意写不起决定性作用

起始点？ 0

结束点？ 2G

忽略/Ignore/放弃/Cancel? Ignore #输入 i 忽略

(parted) unit GB #使用GB作为单位显示

(parted) print

# 第三部分 系统&服务管理进阶

1.构建新的教学环境

1.构建两台虚拟机,操作系统为CentOS7.5

[student@room9pc01 ~]$ clone-vm7

Enter VM number: 8

[student@room9pc01 ~]$ clone-vm7

Enter VM number: 9

#修改两台虚拟机名为A与B

2.利用root进入两台虚拟机,密码为:123456

3.配置永久主机名

虚拟机A:svr7.tedu.cn 虚拟机B:pc207.tedu.cn

4.配置IP地址

虚拟机A:为eth0配置 192.168.4.7/24 虚拟机B:为eth0配置 192.168.4.207/24

5.利用真机进行远程管理两台虚拟机

[student@room9pc01 ~]$ ping 192.168.4.7

[student@room9pc01 ~]$ ping 192.168.4.207

6.为真机上设置永久别名

[student@room9pc01 ~]$ vim /home/student/.bashrc

alias goa='ssh -X root@192.168.4.7'

alias gob='ssh -X root@192.168.4.207'

新开一个终端验证

7.构建Yum仓库

服务端:真机构建FTP服务器,共享光盘所有内容

1)真机检测软件包vsftpd的安装

[student@room9pc01 ~]$ rpm -q vsftpd

vsftpd-3.0.2-22.el7.x86\_64

[student@room9pc01 ~]$ systemctl status vsftpd

2)共享光盘所有内容

默认共享的路径:/var/ftp

]$ mkdir /var/ftp/centos-1804/

]$ mount /iso/CentOS7-1804.iso /var/ftp/centos-1804/

]$ ls /var/ftp/centos-1804/

]$ vim /etc/fstab

/var/lib/libvirt/images/iso/CentOS7-1804.iso /var/ftp/centos-1804 iso9660 defaults 0 0

]$ firefox ftp://192.168.4.254/centos-1804

客户端:两台虚拟机

[root@svr7 ~]# vim /etc/yum.repos.d/local.repo

[local\_repo]

name=CentOS-$releasever - Base

baseurl="ftp://192.168.4.254/centos-1804"

enabled=1

gpgcheck=0

[root@svr7 ~]# yum -y install httpd

虚拟机C

1.配置主机名为:svr10.tedu.cn

2.配置eth0的IP地址:192.168.4.10/24

3.配置Yum仓库,指向服务端为真机的FTP服务

虚拟机D

1.配置主机名为:pc20.tedu.cn

2.配置eth0的IP地址:192.168.4.20/24

3.配置Yum仓库,指向服务端为真机的FTP服务

2.目录结构

[1]认识Linux的目录层次: – man hier

• 常见一级目录的用途

/boot 存放系统引导必需的文件,包括内核、启动配置

/bin、/sbin 存放各种命令程序

/dev 存放硬盘、键盘、鼠标、光驱等各种设备文件

/etc 存放Linux系统及各种程序的配置文件

/root、/home/用户名 分别是管理员root、普通用户的默认家目录

/var 存放日志文件、邮箱目录等经常变化的文件

/proc 存放内存中的映射数据,不占用磁盘

/tmp 存放系统运行过程中使用的一些临时文件

[root@svr7 ~]# ls -ld /tmp

drwxrwxrwt. 8 root root 172 7月 15 10:34 /tmp

[2]权限的数值表示

• 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

[root@svr7 ~]# chmod 750 /nsd01

[root@svr7 ~]# chmod 700 /nsd01

[root@svr7 ~]# chmod 755 /nsd01

[3]历史命令

• 管理/调用曾经执行过的命令

– history:查看历史命令列表

– history -c:清空历史命令

– !n:执行命令历史中的第n条命令

– !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

[root@svr7 ~]# vim /etc/profile

HISTSIZE=1000 //默认记录1000条

[root@svr7 ~]# history #显示历史命令列表

[root@svr7 ~]# history -c #清空所有的历史命令

[root@svr7 ~]# cat -n /etc/redhat-release

[root@svr7 ~]# history

[root@svr7 ~]# !cat #执行临时命令中最近以cat开头的命令

[4]实用小命令工具

• du,统计文件的占用空间

– du [选项]... [目录或文件]...

– -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(K、M等)

[root@svr7 ~]# du -sh /root

[root@svr7 ~]# du -sh /root/ /etc/ /boot/

[root@svr7 ~]# du -sh /

• date,查看/调整系统日期时间

– date +%F、date +%R

– date +"%Y-%m-%d %H:%M:%S"

– date -s "yyyy-mm-dd HH:MM:SS"

[root@svr7 ~]# date +%F #显示 年-月-日 2019-07-15

[root@svr7 ~]# date +%Y #显示 年 2019

[root@svr7 ~]# date +%m #显示 月 07

[root@svr7 ~]# date +%d #显示 日期 15

[root@svr7 ~]# date +%H #显示 时 11

[root@svr7 ~]# date +%M #显示 分 42

[root@svr7 ~]# date +%S #显示 秒

3.制作快捷方式 制作连接(链接)文件

制作软连接

格式: ln -s /路径/源文件 /路径/快捷方式名 #必须时绝对路径

]# cat /etc/sysconfig/network-scripts/ifcfg-eth0

]# ln -s /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/net0

]# ls /etc/net0

]# cat /etc/net0

软连接特点:

若原始文件或目录被删除,连接文件将失效

软连接可存放在不同分区/文件系统

硬连接特点:

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

[root@svr7 ~]# ln -s /opt/A /opt/B #制作软连接

[root@svr7 ~]# ls /opt/

[root@svr7 ~]# cat /opt/B

[root@svr7 ~]# ln /opt/A /opt/C #制作硬连接

[root@svr7 ~]# ls /opt/

[root@svr7 ~]# rm -rf /opt/A

[root@svr7 ~]# ls /opt/

[root@svr7 ~]# cat /opt/B #软连接不可用

[root@svr7 ~]# cat /opt/C #硬连接可以使用

获取命令帮助

[root@svr7 ~]# man 5 passwd #5代表配置文件类型帮助信息

4.zip归档工具,跨平台的压缩格式

• 归档+压缩操作

– zip [-r] 备份文件.zip 被归档的文档...

[root@svr7 ~]# yum -y install zip

[root@svr7 ~]# zip -r /opt/file.zip /root/ /etc/passwd

[root@svr7 ~]# ls /opt

• 释放归档+解压操作

– unzip 备份文件.zip [-d 目标文件夹]

[root@svr7 ~]# yum -y install unzip

[root@svr7 ~]# unzip /opt/nsd.zip -d /mnt/

[root@svr7 ~]# ls /mnt/

###########################################################

5.自定义Yum源

1.具备从互联网下载一些软件包

[student@room9pc01 ~]$ ls /linux-soft/01/

2.将tools.tar.gz传递到虚拟机A

[student@room9pc01 ~]$ scp /linux-soft/01/tools.tar.gz root@192.168.4.7:/root/

3.在虚拟机A查看

]# ls /root

]# tar -xf /root/tools.tar.gz -C /

]# ls /

]# ls /tools/

]# ls /tools/other/

4.在虚拟机A生成仓库数据文件

[root@svr7 ~]# yum -y install createrepo

[root@svr7 ~]# createrepo /tools/other/

[root@svr7 ~]# ls /tools/other/

[root@svr7 ~]# ls /tools/other/repodata

5.书写客户端配置文件

[root@svr7 ~]# vim /etc/yum.repos.d/local.repo

[local\_repo]

name=CentOS-$releasever - Base

baseurl="ftp://192.168.4.254/centos-1804"

enabled=1

gpgcheck=0

[myrpm]

name=other rpm

baseurl=file:///tools/other #指定为本机为Yum服务端

enabled=1

gpgcheck=0

[root@svr7 ~]# yum repolist

[root@svr7 ~]# yum -y install cmatrix

[root@svr7 ~]# cmatrix

[root@svr7 ~]# cmatrix -C red

[root@svr7 ~]# yum -y install sl

[root@svr7 ~]# sl

[root@svr7 ~]# yum -y install oneko

[root@svr7 ~]# oneko

[root@svr7 ~]# oneko & #将程序放入后台

6.vim编辑技巧

命令模式操作

[root@svr7 ~]# cp /etc/passwd /opt/a.txt

[root@svr7 ~]# vim /opt/a.txt

光标跳转

Home 键 或 ^、数字 0 跳转到行首

End 键 或“$”键 跳转到行尾

PgUp 键、PgDn 键 向上翻页、向下翻页

1G 或 gg 跳转到文件的首行

G 跳转到文件的末尾行

复制/粘贴/删除

复制 yy、3yy 复制光标处的一行、3行

粘贴 p、P 粘贴到光标处之后、之前

x 或 Delete键 删除光标处的单个字符

dd、#dd 删除光标处的一行、#行

d^ 从光标处之前删除至行首

d$或D(大写) 从光标处删除到行尾

C(大写) 从光标处删除到行尾,进入插入模式

查找/撤销/保存

/word 向后查找字符串“word”

n、N 跳至后/前一个结果

u 撤销最近的一次操作

U(大写) 撤销对当前行的所有修改

Ctrl + r 取消前一次撤销操作

ZZ(大写) 保存修改并退出

末行模式操作

:r /etc/filesystems 读入其他文件内容

[root@svr7 ~]# echo 123456 > /opt/2.txt

[root@svr7 ~]# echo hahaxixi > /opt/3.txt

[root@svr7 ~]# vim /opt/3.txt

:r /opt/2.txt #读入/opt/2.txt到当前文件

:r /etc/passwd #读入/etc/passwd到当前文件

字符串替换

:s/root/admin 替换当前行第一个“root”

:s/root/admin/g 替换当前行所有的“root”

:1,10 s/root/admin/g 替换第1-10行所有的“root”

:% s/root/admin/g 替换文件内所有的“root

[root@svr7 ~]# cat /etc/passwd > /opt/a.txt

[root@svr7 ~]# vim /opt/a.txt

开关参数的控制

:set nu或nonu 显示/不显示行号

:set ai或noai 启用/关闭自动缩进

7.源码编译安装

RPM包: rpm -ivh yum -y install

源码包----gcc make---->可以执行的程序-------->运行安装

• 主要优点

– 获得软件的最新版,及时修复bug

– 软件功能可按需选择/定制,有更多软件可供选择

– 源码包适用各种平台

步骤一:安装gcc与make开发工具

[root@svr7 ~]# yum -y install gcc

[root@svr7 ~]# yum -y install make

步骤二:进行tar解包

]# tar -xf /tools/inotify-tools-3.13.tar.gz -C /

]# cd /inotify-tools-3.13/

步骤三:运行configure脚本

作用1:检测是否安装gcc

作用2:可以选择软件的功能,也可以指定软件安装的路径

--prefix=指定安装的位置

]# cd /inotify-tools-3.13/

]# ./configure --prefix=/opt/myrpm

步骤四:make编译生成可以执行的程序

]# cd /inotify-tools-3.13/

]# make

步骤五:make install将可以执行的程序运行安装

]# cd /inotify-tools-3.13/

]# make install

8.手动图形安装虚拟机名为nsd01

利用光盘镜像安装

内存2048M

虚拟机名为:nsd01

网络类型选择为:private1

软件包:带GUI的服务器

分区:自动分区

设置root的密码为1,建立lisi用户设置密码1

虚拟化概述

• virtualization 资源管理

– x个物理资源 --> y个逻辑资源

– 实现程度:完全、部分、硬件辅助(CPU)

CPU支持虚拟化所有的指令集(vmx)

[student@room9pc01 ~]$ lscpu | grep vmx

• 虚拟化主要厂商及产品

VMware VMware Workstation、vSphere

Microsoft VirtualPC、Hyper-V

RedHat KVM、RHEV

Citrix Xen

Oracle Oracle VM VirtualBox

9.虚拟机nsd01进行配置

1.配置永久主机名:kvm.tedu.cn

[root@localhost ~]# echo kvm.tedu.cn > /etc/hostname

[root@localhost ~]# hostname kvm.tedu.cn

2.配置永久IP地址:192.168.4.30/24

[root@localhost ~]# nmcli connection modify eth0 ipv4.method manual ipv4.addresses 192.168.4.30/24 connection.autoconnect yes

[root@localhost ~]# nmcli connection up eth0

[root@localhost ~]# ifconfig

3.修改防火墙默认区域与SELinux

[root@kvm ~]# firewall-cmd --set-default-zone=trusted

[root@kvm ~]# setenforce 0

[root@kvm ~]# getenforce

[root@kvm ~]# vim /etc/selinux/config

SELINUX=permissive

4.构建Yum仓库

]# cd /etc/yum.repos.d/

]# mkdir repo

]# mv \*.repo repo

]# vim dvd.repo

[dvd]

name=centos7

baseurl=ftp://192.168.4.254/centos-1804

enabled=1

gpgcheck=0

]# yum repolist

]# yum -y install xeyes

10.安装虚拟化服务器平台

• 主要软件包

– qemu-kvm :为 kvm 提供底层仿真支持

– libvirt-daemon :libvirtd 守护进程,管理虚拟机

– libvirt-client :用户端软件,提供客户端管理命令

– libvirt-daemon-driver-qemu :libvirtd 连接 qemu 的驱动

– virt-manager :图形管理工具

]# yum -y install qemu-kvm

]# yum -y install libvirt-daemon

]# yum -y install libvirt-client

]# yum -y install libvirt-daemon-driver-qemu

]# yum -y install virt-manager

虚拟化服务: libvirtd

[root@kvm /]# systemctl status libvirtd #查看服务的状态

11.通过命令管理虚拟机

virsh命令工具介绍

• 提供管理各虚拟机的命令接口

– 支持交互模式,查看/创建/停止/关闭 .. ..

– 格式:virsh 控制指令 [虚拟机名称] [参数]

• 查看KVM节点(服务器)信息

]$ virsh nodeinfo

• 列出虚拟机

]$ virsh list [--all] #重点

• 列出虚拟网络

]$ virsh net-list [--all]

• 查看指定虚拟机的信息

]$ virsh dominfo 虚拟机名称 #重点

]$ virsh autostart nsd01 #设置虚拟机开机自启动

]$ virsh autostart --disable nsd01 #禁止虚拟机开机自启动

• 开关机操作

]$ virsh start或reboot或shutdown 虚拟机名称 #重点

• 强制关闭指定的虚拟机

]$ virsh destroy 虚拟机名称 #重点

###########################################################

12.一台KVM虚拟机的组成

– xml配置文件(虚拟机描述文件):定义虚拟机的名称、UUID、CPU、内

存、虚拟磁盘、网卡等各种参数设置

[student@room9pc01 ~]$ ls /etc/libvirt/qemu/

– 磁盘镜像文件:保存虚拟机的操作系统及文档数据,

镜像路径取决于xml配置文件中的定义

[student@room9pc01 ~]$ ls /var/lib/libvirt/images/

###########################################################

查看虚拟机xml文件内容

[student@room9pc01 /]$ virsh dumpxml nsd01

虚拟机名称

虚拟机的UUID唯一标识

虚拟机磁盘文件路径

<source file='/var/lib/libvirt/images/nsd01.qcow2'/>

虚拟机网卡信息

<interface type='network'>

<mac address='52:54:00:d4:fe:59'/>

[student@room9pc01 /]$ virsh dumpxml nsd01 | less

###########################################################

13.在命令行手动制作一台虚拟机

1.磁盘镜像文件

]$ cd /var/lib/libvirt/images/

]$ du -sh .node\_base.qcow2

]$ cp .node\_base.qcow2 nsd02.qcow2

]$ du -sh nsd02.qcow2

2.建立新的xml配置文件, uuidgen可以生成随机的UUID值

]$ cd /etc/libvirt/qemu/

]$ virsh dumpxml nsd01 > /etc/libvirt/qemu/nsd02.xml

]$ vim /etc/libvirt/qemu/nsd02.xml

1)虚拟机名称 <name>nsd02</name>

2)虚拟机的UUID唯一标识 删除整行内容 UUID

3)虚拟机磁盘文件路径 <source file='/var/lib/libvirt/images/nsd02.qcow2'/>

4)虚拟机网卡信息

<mac address='52:54:00:d4:fe:59'/> 删除整行内容

3.导入虚拟机配置信息

]$ virsh define /etc/libvirt/qemu/nsd02.xml

]$ virsh list --all

]$ virsh start nsd02

###########################################################

命令行删除虚拟机

]$ virsh list --all

]$ virsh destroy nsd02 #强制关闭虚拟机

域 nsd02 被删除

]$ virsh list --all

]$ virsh undefine nsd02 #删除虚拟机xml配置文件

域 nsd02 已经被取消定义

]$ virsh list --all

]$ rm -rf /var/lib/libvirt/images/nsd02.qcow2 #手动删除

14.在命令行手动创建虚拟机

1.建立新的磁盘文件

]$ cp /var/lib/libvirt/images/.node\_base.qcow2 /tmp/nsd03.qcow2

]$ du -sh /tmp/nsd03.qcow2

2.建立xml配置文件

]$ virsh dumpxml nsd01 > /home/student/nsd03.xml

]$ ls /home/student/nsd03.xml

]$ vim /home/student/nsd03.xml

1)虚拟机名称 <name>nsd03</name>

2)虚拟机的UUID唯一标识 删除整行内容 UUID

3)虚拟机磁盘文件路径 <source file='/tmp/nsd03.qcow2'/>

4)虚拟机网卡信息

<mac address='52:54:00:d4:fe:59'/> 删除整行内容

3.导入虚拟机配置信息

]$ ls /etc/libvirt/qemu

]$ virsh define /home/student/nsd03.xml #导入虚拟机信息

]$ ls /etc/libvirt/qemu

]$ virsh start nsd03

]$ virsh list

15.三合一:导出 修改 导入

• 对虚拟机的配置进行调整

– 编辑:virsh edit 虚拟机名

1.建立磁盘文件

]$ cp /var/lib/libvirt/images/.node\_base.qcow2 /var/lib/libvirt/images/nsd04.qcow2

]$ du -sh /var/lib/libvirt/images/nsd04.qcow2

2.建立xml配置文件

[student@room9pc01 /]$ virsh edit nsd01

1)虚拟机名称 <name>nsd04</name>

2)虚拟机的UUID唯一标识 删除整行内容 UUID

3)虚拟机磁盘文件路径 <source file='/var/libvirt/images/nsd04.qcow2'/>

4)虚拟机网卡信息

<mac address='52:54:00:d4:fe:59'/> 删除整行内容

[student@room9pc01 /]$ virsh list --all

#################################################

常用镜像盘类型

• 虚拟机的磁盘镜像文件格式

特点\类型 RAW QCOW2

KVM默认 否 是

I/O效率 高 较高

占用空间 大 小

压缩 不支持 支持

后端盘复用 不支持 支持

快照 不支持 支持

查看磁盘镜像文件信息

]$ qemu-img info /var/lib/libvirt/images/nsd04.qcow2

virtual size: 2.0G (2147483648 bytes) #虚拟大小

disk size: 633M #实际占用空间

#################################################

COW技术原理

• Copy On Write,写时复制

– 直接映射原始盘的数据内容

– 当原始盘的旧数据有修改时,在修改之前自动将旧数据存入前端盘

– 对前端盘的修改不回写到原始盘

– 原始盘的数据不能做修改

快速创建qcow前端盘

• qemu-img 通过 -b 选项复用指定原始盘

– qemu-img create -f qcow2 -b 原始盘 前端盘 大小

1.命令手动创建虚拟机磁盘文件

]$ cd /var/lib/libvirt/images/

]$ qemu-img create -f qcow2 -b .node\_base.qcow2 nsd05.qcow2 5G #通过原始盘产生前端盘

]$ qemu-img info nsd05.qcow2 #查看虚拟磁盘文件信息

virtual size: 5.0G (5368709120 bytes) #虚拟大小

disk size: 196K #实际占用空间大小

backing file: .node\_base.qcow2 #原始盘

2.建立xml文件

]$ virsh dumpxml nsd01 > /tmp/nsd05.xml #导出虚拟机信息

]$ vim /tmp/nsd05.xml #修改 虚拟机名 UUID 磁盘路径 网卡MAC

]$ virsh define /tmp/nsd05.xml

###########################################################

离线访问虚拟机

• 使用 guestmount 工具

– 支持离线挂载 raw、qcow2 格式虚拟机磁盘

– 可以在虚拟机关机的情况下,直接修改磁盘中的文档

– 方便对虚拟机定制、修复、脚本维护

]$ virsh destroy nsd01

]$ guestmount -a /var/lib/libvirt/images/nsd01.qcow2 -i /mnt/

16.DNS服务器的功能

– 正向解析:根据注册的域名查找其对应的IP地址

– 反向解析:根据IP地址查找对应的注册域名,不常用

域名结构: 树型结构

所有的域名都必须以点结尾

www.qq.com. www.baidu.com.

根域名: .

一级域名: .cn .us .kr .tw .hk .jp .......

二级域名: .com.cn .tedu.cn .net.cn .org.cn ......

三级域名: nb.com.cn dc.com.cn tc.com.cn ........

完全合格的域名(FQDN)=主机头部+注册的域名

Full Qualified Domain Name,完全合格主机名

###########################################################

– 系统服务:named

– 默认端口:TCP/UDP 53

– 运行时的虚拟根环境:/var/named/chroot/

• 主配置文件:/etc/named.conf #本机负责解析的域名

• 地址库文件存放路径:/var/named/ #域名的解析结果

17.构建基本DNS服务

虚拟机A:

1.安装软件包

[root@svr7 ~]# yum -y install bind-chroot bind

bind-9.9.4-29.el7.x86\_64 //域名服务包

bind-chroot-9.9.4-29.el7.x86\_64 //提供虚拟根支持,牢笼

2.修改主配置文件

[root@svr7 ~]# cp /etc/named.conf /etc/named.bak

[root@svr7 ~]# vim /etc/named.conf

options {

directory "/var/named"; #指定地址库文件位置

};

zone "tedu.cn" IN { #设置本机负责的域名

type master; #设置本机为权威主DNS服务器

file "tedu.cn.zone"; #设置地址库文件名称

};

3.建立地址库文件tedu.cn.zone

]# cd /var/named/

]# cp -p named.localhost tedu.cn.zone #-p保持权限不变

]# ls -l tedu.cn.zone

]# vim tedu.cn.zone

所有的域名在地址库文件必须以点结尾

当没有以点结尾时,自动补全地址库负责的域名

tedu.cn. NS svr7 #声明区域DNS服务器

svr7 A 192.168.4.7 #声明DNS服务器IP地址

www A 1.1.1.1 #常规DNS正向解析

ftp A 2.2.2.2

[root@svr7 /]# systemctl restart named

虚拟机B:客户端验证

]# echo nameserver 192.168.4.7 > /etc/resolv.conf

]# cat /etc/resolv.conf

]# nslookup www.tedu.cn

]# nslookup ftp.tedu.cn

18.多域名的DNS服务器,负责解析qq.com域名

虚拟机A:

1.修改主配置文件

[root@svr7 /]# vim /etc/named.conf

options {

directory "/var/named";

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

[root@svr7 /]# cd /var/named/

[root@svr7 named]# cp -p tedu.cn.zone qq.com.zone

[root@svr7 named]# vim qq.com.zone

qq.com. NS svr7

svr7 A 192.168.4.7

www A 3.3.3.3

[root@svr7 named]# systemctl restart named

19.特殊解析记录

1.基于DNS解析记录负载均衡

[root@svr7 /]# vim /var/named/tedu.cn.zone

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

www A 192.168.4.20

www A 192.168.4.30

ftp A 2.2.2.2

[root@svr7 /]# systemctl restart named

2.泛域名解析

虚拟机A

[root@svr7 /]# vim /var/named/tedu.cn.zone

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

ftp A 2.2.2.2

\* A 1.2.3.4

[root@svr7 /]# systemctl restart named

虚拟机B:测试 nslookup haha.tedu.cn

3.解析记录的别名

虚拟机A:

[root@svr7 /]# vim /var/named/tedu.cn.zone

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

ftp A 2.2.2.2

\* A 1.2.3.4

mail CNAME ftp

[root@svr7 /]# systemctl restart named

虚拟机B测试:

[root@pc207 ~]# nslookup mail.tedu.cn

4.有规律的泛域名解析

pc1.tedu.cn -----> 192.168.10.1

pc2.tedu.cn -----> 192.168.10.2

pc3.tedu.cn -----> 192.168.10.3

.......

pc50.tedu.cn -----> 192.168.10.50

内置函数:$GENERATE 制造连续范围的数字

虚拟机A

[root@svr7 ~]# vim /var/named/tedu.cn.zone

$GENERATE 1-50 pc$ A 192.168.10.$

[root@svr7 ~]# !sys

[root@svr7 ~]# systemctl restart named

虚拟机B测试:

[root@pc207 ~]# nslookup pc1.tedu.cn

[root@pc207 ~]# nslookup pc2.tedu.cn

[root@pc207 ~]# nslookup pc3.tedu.cn

###########################################################

DNS资源解析记录有哪些?

正向解析记录(A记录)

DNS声明记录(NS记录)

解析记录的别名(CNAME记录)

20.DNS子域授权

父域:qq.com 由虚拟机A进行解析

子域:bj.qq.com 由虚拟机B进行解析

虚拟机B,构建DNS服务器,负责解析bj.qq.com

[root@pc207 ~]# yum -y install bind bind-chroot

[root@pc207 ~]# cp /etc/named.conf /etc/named.bak

[root@pc207 ~]# vim /etc/named.conf

options {

directory "/var/named";

};

zone "bj.qq.com" IN {

type master;

file "bj.qq.com.zone";

};

[root@pc207 ~]# cd /var/named/

[root@pc207 named]# cp -p named.localhost bj.qq.com.zone

[root@pc207 named]# vim bj.qq.com.zone

bj.qq.com. NS pc207

pc207 A 192.168.4.207

www A 50.60.70.80

[root@pc207 /]# systemctl restart named

[root@pc207 /]# nslookup www.bj.qq.com 192.168.4.207

[root@pc207 /]# nslookup www.qq.com 192.168.4.7

###########################################################

子域授权: 让父域的DNS服务器知晓子域DNS服务器

让父域的DNS服务器可以解析子域的域名

虚拟机A:

[root@svr7 ~]# vim /var/named/qq.com.zone

qq.com. NS svr7

bj.qq.com. NS pc207

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A 3.3.3.3

[root@svr7 ~]# systemctl restart named

[root@pc207 /]# nslookup www.bj.qq.com 192.168.4.7

Server: 192.168.4.7

Address: 192.168.4.7#53

Non-authoritative answer: #非权威解答

Name: www.bj.qq.com

Address: 50.60.70.80

###########################################################

递归解析:

由客户端发出请求,首选DNS服务器接受请求,将解析结果带回过程

[root@svr7 ~]# vim /etc/named.conf

options {

directory "/var/named";

recursion no; #禁止递归解析:

};

迭代解析:首选DNS服务器与其他DNS服务器交互过程

专业测试DNS工具

[root@pc207 /]# dig www.bj.qq.com 192.168.4.7

###########################################################

主机名映射文件:/etc/hosts

没有DNS服务器前提下,解析域名,只能为本机做域名解析

[root@svr7 ~]# vim /etc/hosts

192.168.4.110 www.nb.com

[root@svr7 ~]# ping www.nb.com

域名解析过程中最高优先级为/etc/hosts 匹配即停止

然后在读取/etc/resolv.conf

21.缓存DNS,缓存解析结果,加快解析过程

三个角色:客户端 缓存DNS服务 真DNS服务器

虚拟机A:真DNS服务器

虚拟机B:缓存DNS服务

虚拟机C:客户端

1.建立虚拟机C

配置IP地址192.168.4.10/24,主机名为svr10.tedu.cn

虚拟机B:缓存DNS服务

[root@pc207 /]# vim /etc/named.conf

options {

directory "/var/named";

forwarders { 192.168.4.7; }; #转发给虚拟机A的IP地址

};

[root@pc207 /]# systemctl restart named

虚拟机C上验证:

[root@svr10 ~]# nslookup www.tedu.cn 192.168.4.207

虚拟机A:构建DNS服务器,实现www.sina.com的解析结果为10.20.30.40

1.修改主配置文件

[root@svr7 named]# vim /etc/named.conf

options {

directory "/var/named";

recursion no;

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

zone "sina.com" IN {

type master;

file "sina.com.zone";

};

2.建立地址库文件

[root@svr7 named]# cd /var/named/

[root@svr7 named]# cp -p qq.com.zone sina.com.zone

[root@svr7 named]# vim /var/named/sina.com.zone

sina.com. NS svr7

svr7 A 192.168.4.7

www A 10.20.30.40

[root@svr7 named]# systemclt restart named

22.Split分离解析(视图解析)

什么是分离解析

• 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

– 不同客户端解析同一个域名,解析结果不同

– 作用:为客户端就近提供服务器

BIND的view视图

• 根据源地址集合将客户机分类

由上到下匹配及停止,所有的客户端都要找到自己的分类

所有的zone都必须在view中

view "nsd" {

match-clients { 192.168.1.1; }; #匹配客户机来源地址

zone "12306.cn" IN {

...... 地址库文件12306.zone;

}; };

view "abc" {

match-clients { 192.168.2.1; };

zone "12306.cn" IN {

...... 地址库文件12306.abc;

}; };

view "other" {

match-clients { any; };

zone "12306.cn" IN {

...... 地址库文件12306.other;

}; };

###################################################

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

– A记录分离解析 —— 以 www.tedu.cn 为例

客户机来自 解析结果

192.168.4.207-----> 192.168.4.100

其他地址 -----> 1.2.3.4

[root@svr7 /]# vim /etc/named.conf

options {

directory "/var/named";

};

view "nsd" { #分类名称

match-clients { 192.168.4.207; }; #匹配客户机来源地址

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";---->解析结果写192.168.4.100

};

};

view "other" {

match-clients { any; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.other";---->解析结果写1.2.3.4

};

};

建立地址库文件tedu.cn.zone与tedu.cn.other写入不同的解析结果

###########################################################多个域名的分离解析,每一个view中zone个数保持一致

– A记录分离解析 —— 以 www.tedu.cn 为例

– A记录分离解析 —— 以 www.sina.com 为例

客户机来自 解析结果

192.168.4.207-----> 192.168.4.100

其他地址 -----> 1.2.3.4

view "nsd" {

match-clients { 192.168.4.207; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone"; -------> 解析结果为192.168.4.100

};

zone "sina.com" IN {

type master;

file "sina.com.zone"; -------> 解析结果为192.168.4.100

};

};

view "other" {

match-clients { any; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.other"; -------> 解析结果为1.2.3.4

};

zone "sina.com" IN {

type master;

file "sina.com.other"; -------> 解析结果为1.2.3.4

};

};

###########################################################

扩展:

– A记录分离解析 —— 以 www.tedu.cn 为例

– A记录分离解析 —— 以 www.sina.com 为例

客户机来自 解析结果

192.168.4.207---www.tedu.cn--> 192.168.4.100

192.168.4.7---www.sina.com--> 192.168.4.200

其他地址 --www.tedu.cn---> 1.2.3.4

其他地址 --www.sina.com---> 1.2.3.4

view "nsd" {

match-clients { 192.168.4.207; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "sina.com" IN {

type master;

file "sina.com.other";

};

};

view "abc" {

match-clients { 192.168.4.7; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.other";

};

zone "sina.com" IN {

type master;

file "sina.com.zone";

};

};

view "other" {

match-clients { any; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.other";

};

zone "sina.com" IN {

type master;

file "sina.com.other";

};

};

###########################################################

acl地址列表,类似于变量作

acl "test" { 192.168.4.207; 192.168.1.1; 192.168.2.1; 192.168.3.1; 192.168.7.0/24; };

view "nsd" {

match-clients { test; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "sina.com" IN {

type master;

file "sina.com.other";

};

};

view "abc" {

match-clients { test; };

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "sina.com" IN {

type master;

file "sina.com.other";

};

};

23.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

– 同一个文档分散存放在不同磁盘

– 并行写入以提高效率

– 至少需要两块磁盘组成

• RAID 1,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

– 至少需要两块磁盘组成

• 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

– 至少需要三块磁盘组成

• 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

– 至少需要四块磁盘组成

• 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

– 至少需要四块磁盘组成

24.进程管理

程序: 静态的代码 占用磁盘空间

进程: 动态执行的代码 占用CPU 内存

父进程/子进程 树型结构 僵尸进程 孤儿进程

进程唯一标识: PID 进程的编号

systemd:上帝进程,所有进程的父进程

查看进程树

• pstree — Processes Tree

– 格式:pstree [选项] [PID或用户名]

• 常用命令选项

– -a:显示完整的命令行

– -p:列出对应PID编号

[root@svr7 /]# pstree

[root@svr7 /]# useradd lisi

[root@svr7 /]# pstree lisi

bash───vim

[root@svr7 /]# pstree -a lisi

bash

└─vim a.txt

[root@svr7 /]# pstree -ap lisi

• ps aux 操作,信息全面

– 列出正在运行的所有进程

用户 进程ID %CPU %内存 虚拟内存 固定内存 终端 状态 起始时间 CPU时间 程序指令

• ps -elf 操作,有进程的父进程的PID值

– 列出正在运行的所有进程

PPID:父进程的PID号

统计正在运行的进程有多少?

[root@svr7 /]# ps aux

[root@svr7 /]# ps aux | wc -l

[root@svr7 /]# ps -elf | wc -l

进程动态排名

• top 交互式工具

– 格式:top [-d 刷新秒数] [-U 用户名]

[root@svr7 /]# top -d 1

按P(大写)可以进行CPU的排序

按M(大写)可以进行内存的排序

load average: 0.00, 0.01, 0.05 #CPU负载量 1分 5分钟 15 分钟

检索进程

• pgrep — Process Grep

– 用途:pgrep [选项]... 查询条件

• 常用命令选项

– -l:输出进程名,而不仅仅是 PID

– -U:检索指定用户的进程

– -x:精确匹配完整的进程名

[root@svr7 /]# pgrep -l a #检索所有进程名带a的

[root@svr7 /]# pgrep -lU lisi #检索lisi的所有进程

[root@svr7 /]# pstree -ap lisi #检索lisi的所有进程

进程的前后台调度

• 后台启动,正在运行放入后台

– 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

• bg 命令

– 激活后台被挂起的任务

[root@svr7 /]# sleep 9000 & #正在运行放入后台

[root@svr7 /]# jobs #查看后台运行的进程

[root@svr7 /]# sleep 8000

^Z #输入Ctrl+z 暂停放入后台

[2]+ 已停止 sleep 8000

[root@svr7 /]# jobs

[root@svr7 /]# bg 2 #将后台编号为2的进程继续运行

[root@svr7 /]# jobs

[root@svr7 /]# fg 1 #将后台编号为1的进程恢复到前台

sleep 9000

^C #输入Ctrl+C 结束

[root@svr7 /]# jobs

[root@svr7 /]# fg 2 #将后台编号为2的进程恢复到前台

sleep 8000

^C #输入Ctrl+C 结束

[root@svr7 /]# jobs

###########################################################

杀死进程

• 干掉进程的不同方法

– Ctrl+c 组合键,中断当前命令程序

– kill [-9] PID... 、kill [-9] %后台任务编号

– killall [-9] 进程名...

– pkill 查找条件

[root@svr7 /]# sleep 1000 &

[root@svr7 /]# jobs -l

[root@svr7 /]# kill 4013 #按照PID进行杀死

[root@svr7 /]# sleep 1000 &

[root@svr7 /]# jobs -l

[root@svr7 /]# kill -9 4015 #按照PID强制杀死

[root@svr7 /]# jobs -l

[root@svr7 /]# sleep 1000 &

[root@svr7 /]# sleep 1000 &

[root@svr7 /]# sleep 1000 &

[root@svr7 /]# jobs

[root@svr7 /]# killall sleep #杀死所有sleep进程

杀死一个用户开启的所有进程(强制踢出一个用户)

[root@svr7 /]# killall -9 -u 用户名

25.日志管理

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

• 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 记录邮件收发相关的消息

/var/log/secure 记录与访问限制相关的安全消息

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

tailf:实时跟踪日志消息

[root@svr7 /]# echo 123 > /opt/1.txt

[root@svr7 /]# cat /opt/1.txt

123

[root@svr7 /]# tailf /opt/1.txt

123

26.用户登录分析

• users、who、w 命令

– 查看已登录的用户信息,详细度不同

pts:图形命令行终端

• last、lastb 命令

– 查看最近登录成功/失败的用户信息

[root@svr7 /]# last -2 #最近登录的2条成功信息

[root@svr7 /]# lastb -2 #最近登录的2条失败信息

[root@svr7 /]# users #查看已登录的用户信息

[root@svr7 /]# who #查看已登录的用户信息

[root@svr7 /]# w #查看已登录的用户信息

27.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8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"

28.systemctl控制

• Linux系统和服务管理器

– systemd是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

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

– 配置目录:/etc/systemd/system/

– 服务目录:/lib/systemd/system/

– 主要管理工具:systemctl

对于服务的管理

systemctl restart 服务名 #重起服务

systemctl start 服务名 #开启服务

systemctl stop 服务名 #停止服务

systemctl status 服务名 #查看服务当前的状态

systemctl enable 服务名 #设置服务开机自启动

systemctl disable 服务名 #设置服务不开机自启动

systemctl is-enabled 服务名 #查看是否为开机自启

RHEL6 运行级别 不同级别,开启的服务不同

0：关机

1：单用户模式（基本功能的实现，破解Linux密码）

2：多用户字符界面（不支持网络）

3：多用户字符界面（支持网络）服务器默认的运行级别

4：未定义

5：图形界面

6：重起

切换运行级别：init 5

RHEL7 运行模式

字符模式：multi-user.target

图形模式：graphical.target

[student@room9pc01 ~]$ rht-vmctl reset classroom

classroom [OK]

域 classroom 已开始

[student@room9pc01 ~]$ rht-vmctl reset server

server [OK]

域 server 已开始

[root@svr7 /]# ls -l /lib/systemd/system/

当前直接切换到字符模式

]# systemctl isolate multi-user.target = init 3

当前直接切换到图形模式

]# systemctl isolate graphical.target = init 5

查看每次开机默认进入模式

[root@svr7 /]# systemctl get-default

multi-user.target

设置永久策略，每次开机自动进入graphical.target

# systemctl set-default graphical.target

# reboot

29.DNS分离解析与Web结合

虚拟机C:构建Web服务

[root@svr10 ~]# yum -y install httpd

[root@svr10 ~]# cat /etc/httpd/conf.d/nsd01.conf

<VirtualHost \*:80>

ServerName www.qq.com

DocumentRoot /var/www/qq

</VirtualHost>

<VirtualHost \*:80>

ServerName www.163.com

DocumentRoot /var/www/163

</VirtualHost>

[root@svr10 ~]# mkdir /var/www/qq /var/www/163

[root@svr10 ~]# echo '<h1>Web1 QQ' > /var/www/qq/index.html

[root@svr10 ~]# echo '<h1>Web1 163' > /var/www/163/index.html

[root@svr10 ~]# systemctl restart httpd

###########################################################

虚拟机D构建Web服务

[root@pc20 ~]# yum -y install httpd

[root@pc20 ~]# cat /etc/httpd/conf.d/nsd01.conf

<VirtualHost \*:80>

ServerName www.qq.com

DocumentRoot /var/www/qq

</VirtualHost>

<VirtualHost \*:80>

ServerName www.163.com

DocumentRoot /var/www/163

</VirtualHost>

[root@pc20 ~]# mkdir /var/www/qq /var/www/163

[root@pc20 ~]# echo '<h1>Web2 QQ' > /var/www/qq/index.html

[root@pc20 ~]# echo '<h1>Web2 163' > /var/www/163/index.html

[root@pc20 ~]# systemctl restart httpd

###########################################################

虚拟机A实现DNS分离解析

[root@svr7 /]# yum -y install bind bind-chroot

[root@svr7 /]# cat /etc/named.conf

options {

directory "/var/named";

};

view "nsd" {

match-clients { 192.168.4.7; };

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

zone "163.com" IN {

type master;

file "163.com.zone";

};

};

view "other" {

match-clients { any; };

zone "qq.com" IN {

type master;

file "qq.com.other";

};

zone "163.com" IN {

type master;

file "163.com.other";

};

};

[root@svr7 /]# cat /var/named/qq.com.zone

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

[root@svr7 /]# cat /var/named/163.com.zone

163.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

[root@svr7 /]# cat /var/named/qq.com.other

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.20

[root@svr7 /]# cat /var/named/163.com.other

163.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.20

[root@svr7 /]# systemctl restart named

为四台虚拟机指定DNS服务器地址

[root@svr7 /]# echo nameserver 192.168.4.7 > /etc/resolv.conf

[root@pc207 ~]# echo nameserver 192.168.4.7 > /etc/resolv.conf

[root@svr10 ~]# echo nameserver 192.168.4.7 > /etc/resolv.conf

[root@pc20 ~]# echo nameserver 192.168.4.7 > /etc/resolv.conf

30.部署DHCP服务器

• Dynamic Host Configuration Protocol

– 动态主机配置协议,由 IETF(Internet 网络工程师任

务小组)组织制定,用来简化主机地址分配管理

• 主要分配以下入网参数

– IP地址/子网掩码/广播地址

– 默认网关地址、DNS服务器地址

• DHCP地址分配的四次会话,以广播进行,先到先得

– DISCOVERY --> OFFER --> REQUEST -->ACK

一个网络中,只能有一台DHCP服务器

• 服务端基本概念

– 租期:允许客户机租用IP地址的时间期限,单位为秒

– 作用域:分配给客户机的IP地址所在的网段

– 地址池:用来动态分配的IP地址的范围

虚拟机A:

1.安装软件包dhcp

[root@svr7 /]# yum -y install dhcp

2.修改配置文件

[root@svr7 /]# vim /etc/dhcp/dhcpd.conf

:r /usr/share/doc/dhcp\*/dhcpd.conf.example

subnet 192.168.4.0 netmask 255.255.255.0 { #分配网段

range 192.168.4.100 192.168.4.200; #分配IP地址范围

option domain-name-servers 192.168.4.7; #分配DNS地址

option routers 192.168.4.254; #网关地址

default-lease-time 600;

max-lease-time 7200;

}

3.重启服务

[root@svr7 /]# systemctl restart dhcpd

31.网络装机概述

网络装机的优势

• 规模化:同时装配多台主机

• 自动化:装系统、配置各种服务

• 远程实现:不需要光盘、U盘等物理安装介质

什么是PXE网络

• PXE,Pre-boot eXecution Environment

– 预启动执行环境,在操作系统之前运行

– 可用于远程安装

• 工作模式

– PXE client 集成在网卡的启动芯片中

– 当计算机引导时,从网卡芯片中把PXE client调入内存

执行,获取PXE server配置、显示菜单,根据用户选

择将远程引导程序下载到本机运行

PXE组件及过程分析

• 需要哪些服务组件?

– DHCP服务,分配IP地址、定位引导程序

– TFTP服务,提供引导程序下载

– HTTP服务(或FTP/NFS),提供yum安装源

• 客户机应具备的条件

– 网卡芯片必须支持PXE协议

– 主板支持从网卡启动

###########################################################

一 构建DHCP服务,指定tftp服务器地址以及网卡引导文件名称

[root@svr7 /]# vim /etc/dhcp/dhcpd.conf

subnet 192.168.4.0 netmask 255.255.255.0 {

range 192.168.4.100 192.168.4.200;

option domain-name-servers 192.168.4.7;

option routers 192.168.4.254;

default-lease-time 600;

max-lease-time 7200;

next-server 192.168.4.7; #指定下一个服务器tftp服务器地址

filename "pxelinux.0"; #指定网卡引导文件名称

}

[root@svr7 /]# systemctl restart dhcpd

pxelinux.0:网卡引导文件(网络装机说明书) 二进制文件

安装一个软件即可获得该文件

###########################################################

二 构建tftp服务,提供众多的引导文件

tftp:简单的文件传输协议 默认端口 69

默认共享路径:/var/lib/tftpboot/

1.安装软件tftp-server

[root@svr7 /]# yum -y install tftp-server

[root@svr7 /]# systemctl restart tftp

2.部署pxelinux.0文件

]# yum provides \*/pxelinux.0 #查询那个软件包产生该文件

]# yum -y install syslinux

]# rpm -ql syslinux | grep pxelinux.0 #查询软件安装清单

]# cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot/

]# ls /var/lib/tftpboot/

pxelinux.0-->读取菜单文件

/var/lib/tftpboot/pxelinux.cfg/default

3.部署菜单文件

]# poweroff #关闭机器,图形添加光驱设备,放入光盘文件

]# mount /dev/cdrom /mnt/

]# ls /mnt/

]# mkdir /var/lib/tftpboot/pxelinux.cfg

]# cp /mnt/isolinux/isolinux.cfg /var/lib/tftpboot/pxelinux.cfg/default

]# ls /var/lib/tftpboot/

]# ls /var/lib/tftpboot/pxelinux.cfg/

4.部署图形模块与背景图片

vesamenu.c32(图形模块)

splash.png(背景图片)

[root@svr7 ~]# cp /mnt/isolinux/vesamenu.c32 /mnt/isolinux/splash.png /var/lib/tftpboot/

[root@svr7 ~]# ls /var/lib/tftpboot/

pxelinux.0 pxelinux.cfg splash.png vesamenu.c32

5.部署启动内核与驱动程序

vmlinuz(启动内核)

initrd.img(驱动程序)

[root@svr7 ~]# cp /mnt/isolinux/vmlinuz /mnt/isolinux/initrd.img /var/lib/tftpboot/

[root@svr7 ~]# ls /var/lib/tftpboot/

initrd.img pxelinux.cfg vesamenu.c32

pxelinux.0 splash.png vmlinuz

6.修改菜单文件

]# vim /var/lib/tftpboot/pxelinux.cfg/default

末行模式 开启行号 :set nu

1 default vesamenu.c32 #默认加载图形的模块

2 timeout 600 #读秒时间 1/10秒

10 menu background splash.png #背景图片

11 menu title NSD1906 PXE Server #标题

61 label linux

62 menu label ^Install CentOS 7 #菜单的显示内容

63 menu default #读秒结束后默认选择

64 kernel vmlinuz #加载启动内核

65 append initrd=initrd.img #加载驱动程序

###########################################################

总结:

1.DHCP---> IP地址 next-server filename

2.tftp---> pxelinux.0

3.pxelinux.0---> 访问菜单文件

/var/lib/tftpboot/pxelinux.cfg/default

4.default--->图形的模块 背景图片 启动内核 驱动程序

测试验证:

[root@svr7 ~]# systemctl restart dhcpd

[root@svr7 ~]# systemctl restart tftp

创建一台新的虚拟机进行测试验证

1.安装方式: 网络引导安装(PXE)

2.内存需要: 2048M

3.网络类型: private1

构建Web服务器,共享众多的软件包

1.安装软件包

[root@svr7 ~]# yum -y install httpd

2.重启httpd服务

[root@svr7 ~]# systemctl restart httpd

3.挂载光驱设备

[root@svr7 ~]# mkdir /var/www/html/centos

[root@svr7 ~]# mount /dev/cdrom /var/www/html/centos

mount: /dev/sr0 写保护，将以只读方式挂载

[root@svr7 ~]# ls /var/www/html/centos

[root@svr7 ~]# systemctl restart httpd

[root@svr7 ~]# firefox 192.168.4.7/centos

###################################################

实现无人值守安装,生成应答文件

1.安装可以生成应答文件的软件包

[root@svr7 ~]# yum -y install system-config-kickstart

2.运行system-config-kickstart

]# LANG=en system-config-kickstart #英文进行运行

点击 "软件包选择(Package Selection)" 查看是否可以进行选择

需要Yum仓库的支持:指向光盘的内容仓库,标识必须为[development]

[root@svr7 ~]# vim /etc/yum.repos.d/local.repo

[development]

name=CentOS-$releasever - Base

baseurl=ftp://192.168.4.254/centos-1804

enabled=1

gpgcheck=0

[root@svr7 ~]# LANG=en system-config-kickstart

点击 "软件包选择(Package Selection)" 查看是否可以进行选择

[root@svr7 ~]# ls /root/ks.cfg

/root/ks.cfg

[root@svr7 ~]# vim /root/ks.cfg

3.利用Web服务器将ks.cfg进行共享

[root@svr7 ~]# cp /root/ks.cfg /var/www/html/

[root@svr7 ~]# ls /var/www/html/

4.修改菜单文件,指定应答文件位置

]# vim /var/lib/tftpboot/pxelinux.cfg/default

label linux

menu label ^Install CentOS 7

menu default

kernel vmlinuz

append initrd=initrd.img ks=http://192.168.4.7/ks.cfg