|  |  |
| --- | --- |
| 版 本 | 2023 |

《网络管理综合实习》指导书

|  |  |
| --- | --- |
| 学年学期： | 2022 - 2023 学年第 二 学期 |
| 专 业： | 网络工程 |
| 年 级： | 2020级 |

#### 信息工程学院计算机教研室

#### 2023 年 6 月

## 目 录

**[实验一：操作系统安装与升级 01](#_TOC_250008)**

**[实验二：基本操作与维护 09](#_TOC_250007)**

**[实验三：网站服务器 19](#_TOC_250006)**

**[实验四：代理服务器 31](#_TOC_250005)**

**[实验五：文件服务器实现 39](#_TOC_250004)**

**[实验六：系统防火墙管理 49](#_TOC_250003)**

**[实验七：系统基本管理 55](#_TOC_250002)**

**[实验八：系统高级管理 63](#_TOC_250001)**

**[实验九：系统运维管理 71](#_TOC_250000)**

**[实验十：Windows2016 DNS HTTP管理 81](#_TOC_250000)**

# 实验一：操作系统安装与升级

##### 一、实验目的

1、理解虚拟化软件的工作原理；

2、掌握VirtualBox 中 Linux 操作系统的安装；

3、掌握 OpenSSH 的安装与配置；

4、掌握操作系统升级的方法与流程。

##### 二、实验学时

2 学时

##### 三、实验类型

验证性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装VirtualBox 虚拟化软件，安装Putty 管理终端软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

无。

##### 五、实验任务

1、完成 VirtualBox 的安装与基本配置；

2、基于VirtualBox 创建虚拟主机，并完成CentOS 的安装；

3、完成 CentOS 操作系统下OpenSSH 的安装与配置，实现对操作系统的远程管理；

4、完成 CentOS 操作系统的在线升级。

##### 六、实验内容及步骤

###### 1、环境搭建

1. 安装VirtualBox 虚拟化软件，安装完成后，VirtualBox 的主界面如图 1-1 所示。

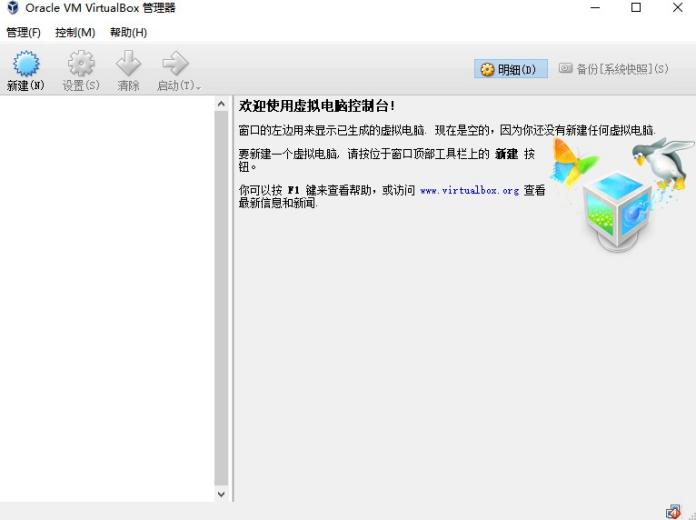
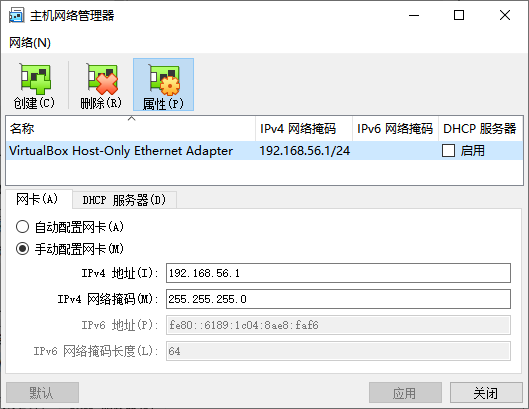


图 1-1 VirtualBox 主界面

1. 点击VirtualBox 的主菜单“管理”、“主机网络管理器”，按下图设置：



1. 根据表 1-1 的配置参数进行CentOS 虚拟主机创建。

**表 1-1 CentOS 虚拟主机配置**

|  |  |  |  |
| --- | --- | --- | --- |
| **配置项** | **配置值** | **配置项** | **配置值** |
| 名称 | CentOS 7 | 类型 | Linux |
| 版本 | CentOS 7.x | 内存大小 | 1024MB |
| 虚拟硬盘 | 现在创建虚拟硬盘 | 文件位置 | CentOS\_7 |
| 文件大小 | 20.00GB | 文件类型 | VDI |
| 存储在物理硬盘上分配类型 | 动态分配 |  |  |
| 网卡1连接方式 | 网络地址转换(NAT) | 网卡2连接方式 | 仅主机网络 |

###### 2、CentOS 安装

1. 安装规划

本次实验通过VirtualBox 虚拟化软件进行CentOS 安装，其具体配置如表 1-2 所示。

**表 1-2 CentOS 操作系统配置**

|  |  |  |  |
| --- | --- | --- | --- |
| **配置项** | **配置值** | **配置项** | **配置值** |
| 操作系统名称 | CentOS 7 | 虚拟主机兼容性 | VirtualBox |
| 主机名 | 学生名字全拼 | 分区格式 | 默认（swap，ext4） |
| CPU | 单路双核 | 内存 | 1G |
| 用户名 | 学号 | 密码 | 学号 |
| 硬盘 | 大 小 20G，类型为 SCSI，介质为虚拟磁盘 | | |
| 网卡1配置 | （默认值） | 网卡2配置 | IP 地址 192.168.56.x/24（x为学号后两位，学号1则改为201） |

1. 安装准备

获取 CentOS 7 的 ISO 镜像文件。镜像文件可通过下载获得，本实验所使用的镜像为 CentOS-7-x86\_64-DVD-2009.iso 。

64位建议下载页面（清华大学源）：

<http://ftp.sjtu.edu.cn/centos/7.9.2009/isos/x86_64/>

只有命令行的：CentOS-7-x86\_64-Minimal-2009.iso

含图形桌面的：CentOS-7-x86\_64-DVD-2009.iso

32位的在这个页面下载：

<https://mirrors.tuna.tsinghua.edu.cn/centos-altarch/7.9.2009/isos/i386/>

只有命令行的：7(2009) i386 Minimal (ISO)

含图形桌面的：7(2009) i386 Everything (ISO)

1. 安装操作系统

①启动虚拟主机并导入镜像文件，进入CentOS 7 操作系统的安装界面，如图1-2 所示。选择“Install CentOS Linux 7”选项后，点击键盘中【Enter】键开始进行安装。

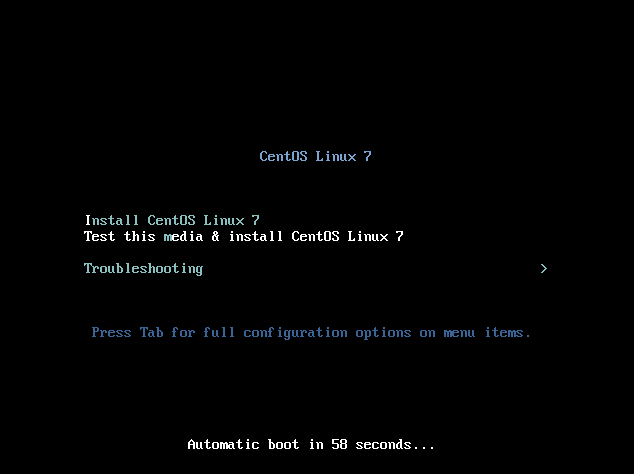


图 1-2 安装菜单

②选择安装语言为“中文Chinese-简体中文（中国）”后，进入“安装信息摘要（Insta llation Summary）”操作界面，如图 1-3 所示，根据表 1-2 配置选项完成系统分区、主机名等信息配置。



图 1-3 安装信息摘要

③“安装信息摘要”配置完成后，点击【开始安装(B)】按钮进入用户设置界面，如图 1

-4 所示，在此处对系统 root 密码以及创建新用户进行配置。



图 1-4 用户设置

④系统配置与相关软件安装完成后，需进行重启系统。重启完成后如图 1-5 所示，输入用户名及密码进行登录，因为是初次安装直接登录 root 用户即可。



图 1-5 登陆界面

1. 网络配置
2. 输入以下命令，查看当前的网卡接口的名称。其中，该命令共输出三个网卡信息， 第一个为循环地址的网卡接口，第二个为网络地址转换的网卡接口，第三个为仅主机网络的网卡接口，其查询结果如图 1-6 所示。

# ip addr



图 1-6 系统地址信息

查看各连接的名称，也就是id。如果安装时选择中文，默认连接名“网络连接1”在终端将显示为乱码：

# nmcli con

如果是乱码，可用下面命令修改连接的名称，下面的xxx-yyyy-zzzzzzzz应改为你的enp0s8那行记录的UUID值：

# nmcli con mod uuid xxx-yyyy-zzzzzzzz con-name enp0s8

②进行配置网络，根据表 1-2 中虚拟主机的网络配置参数，修改虚拟主机的网卡配置

文件进行网络配置，并将网卡配置信息填写至表 1-3 中。

命令行方式（建议）：

# nmcli con mod enp0s8 ipv4.address 192.168.56.x/24

# nmcli con down enp0s8

# nmcli con up enp0s8

修改配置文件方式：

# vi /etc/sysconfig/network-scripts/ifcfg-enp0s8

需要修改的信息内容及其详解如下（除第一、二项属性外，其余为自己添加）：

##dhcp 改为 static

BOOTPROTO="static" ##开机启用本配置ONBOOT="yes"

##配置静态 IP IPADDR=

##配置子网掩码NETMASK=

重启网络，以使文件的更改生效：

# systemctl restart network

**表 1-3 网络配置信息**

###### 4、SSH 配置

①进行 OpenSSH 的安装，其安装命令如下。

# yum install openssh -y

SSH 安装完成后，其配置文件所在目录为“/etc/ssh/sshd\_config”。以下为 SSH 服务常用配置含义，可通过修改配置文件进行 SSH 服务配置，以下是其需配置的内容及其含义。

##设置 SSH 的端口号是 22(默认端口号为 22)

Port=22

##启用 SSH 版本 2 协议

Protocol 2

##设置服务监听的地址#ListenAddress 192.168.1.1 ##拒绝访问的用户(用空格隔开)

DenyUsers user1 user2 foo ##允许访问的用户(用空格隔开) #AllowUsers root osmond vivek ##禁止 root 用户登陆将yes改为no

PermitRootLogin yes

##用户登陆需要密码认证PermitEmptyPasswords no ##启用口令认证方式PasswordAuthentication yes

②开启 SSH 服务，并设置开机自启动，其命令如下

# systemctl start sshd

# systemctl enable sshd

③SSH 使用的是 22 端口，这里需要查看防火墙是否开启此端口，其查看命令如下，系统恢复的结果为“yes”或“no”。

# firewall-cmd --query-port=22/tcp

④若没有开启，则开启命令如下，开启成功系统会回复“success”。

# firewall-cmd --zone=public --add-port=22/tcp --permanent

###### 5、使用 PuTTY 进行远程管理

①在本地机器上下载PuTTY 软件，通过其官网进行下载安装（https://[www.chiark.green](http://www.chiark.green/) end.org.uk/~sgtatham/putty/latest.html），该软件的主界面如图 1-7 示。

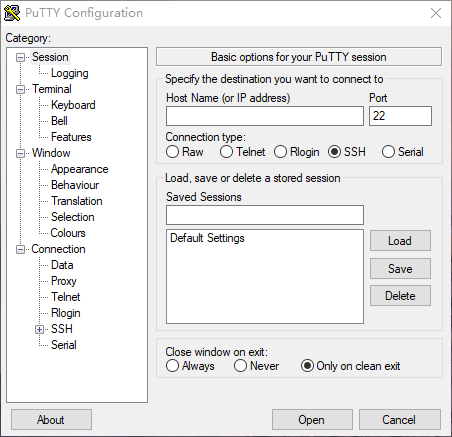


图 1-7 PuTTY 主界面

输入虚拟主机地址，点击【Open】进行远程访问，输入用户及密码登录虚拟化主机进行管理，与直接通过VirtualBox 控制台的命令行管理操作效果一样。

###### 6、CentOS 系统的维护

说明：本部分实验使用 PuTTY 通过 SSH 远程连接进行 CentOS 系统维护。

①查看系统版本及内核信息，其命令如下。

# uname –r #或者$sudo lsb\_release -a

阅读系统版本及内核信息，并将信息及其含义填写至表 1-4。

**表 1-4 系统版本及内核信息**

②系统升级。输入以下命令进行系统升级。

# yum -y update

④重启系统进行验证。

输入以下命令进行系统重启，系统重启完成后，再次查看系统版本及内核信息，并将查询结果填写至表 1-5 中。

# reboot

**表 1-5 系统版本及内核信息**

###### 7、更改升级源，获得更快升级

更新升级的 yum 源库，选择下载速度相对较快的 163 网易资源上的 yum 源进行系统更新，其配置过程如下。

①备份默认源。将系统默认使用的“/etc/yum.repos.d/CentOS-Base.repo”进行备份，其操作命令如下。

# mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-B ase.repo.backup

②下载源文件。将新的 yum 源文件下载到 yum 源配置目录中，其操作命令如下。

# cd /etc/yum.repos.d

# wget <http://mirrors.163.com/.help/CentOS6-Base-163.repo>

③将虚拟化云主机上的软件包信息临时缓存至本地，以提高升级系统时搜索软件包的速度，其操作命令如下所示。

# yum makecache

##### 七、实验扩展

###### 1、虚拟化软件的区别

1. 除了VirtualBox，在 Windows、Linux、MAC 系统下的虚拟化软件还有哪些？
2. 个人用的桌面虚拟化软件和服务器所采用的企业级虚拟化软件有哪些差异？
3. 常见的企业级虚拟化软件有哪些？

###### 2、如何选择合适的 Linux 发行版

1. 操作系统的版本是不是越新越好？若不是，请举例说明，并阐述理由。
2. 如何为笔记本、PC 机、服务器、云主机选择Linux 操作系统？
3. 选择合适 Linux 发行版的标准和依据是什么？

# 实验二：基本操作与维护

##### 一、实验目的

1、掌握 Linux 系统下基本的操作命令；

2、理解 Linux 下文件和目录的区别；

3、掌握对文件和目录的管理：建立、复制、剪切、删除、重命名、查找、统计等；

4、掌握常用文本内容处理工具的使用方法：vi、sed、awk。

##### 二、实验学时

2 学时

##### 三、实验类型

验证性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装VirtualBox 虚拟化软件，安装Putty 管理终端软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

无。

##### 五、实验任务

1、完成 Linux 基本操作命令的应用：ls、whereis、who、time、uname、man；

2、完成文件和目录操作命令的应用：mkdir、touch、rm、cp 、mv；

3、完成文本内容操作命令的应用：cat、more、head、vi、sed、awk。

##### 六、实验内容及步骤

###### 1、ls

进入“/etc/”目录，查看该目录下所有文件的详细信息，其操作命令如下，部分结果如图 2-1 所示。

# cd /etc/ # ls -al

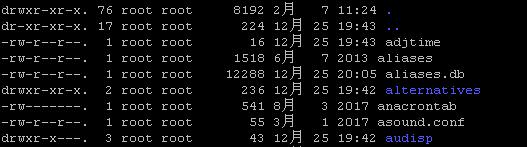


图 2-1 etc 目录下部分内容

###### 2、whereis

查找 openssh 文件的路径，其操作命令如下，查询结果如图 2-2 所示。

# whereis openssh



图 2-2 whereis 查询结果

###### 3、who

①查看当前用户登录的用户信息，其操作命令如下，查询结果如图 2-3 所示。

# who



图 2-3 who 命令查询结果

②使用“-H”选项，使其输出信息上方显示标题信息列，配置命令及其输出结果填写到表 2-1 中。

**表 2-1 显示标题信息列**

###### 4、time

①查看命令执行时间，其操作命令如下，在命令执行完成后，输出该命令执行的详细耗时，如图 2-4 所示。

$ time ls -al

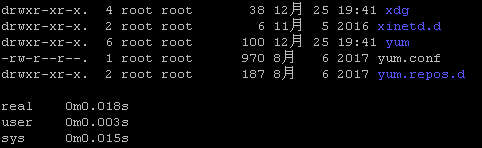


图 2-4 “ls -al”命令的耗时信息

②查看“whereis openssh”命令执行时间，将其操作命令及输出结果填写到表 2-2 中。

**表 2-2 查看“whereis openssh”命令耗时**

###### 6、uname

①查看操作系统名称，其操作命令如下，将其输出结果及含义填写到表 2-3 中。

# uname -s

**表 2-3 查看操作系统名称**

②分别使用该命令的“-m、-n、-r、-v、-p、-a”选项，对比不同选项命令输出结果， 将输出结果填写到表 2-4 中。

**表 2-4 不同选项执行结果对比**

###### 7、man

①查看“vi”命令描述的详细信息，其操作命令如下，查看结果如图 2-5 所示。

# man vi

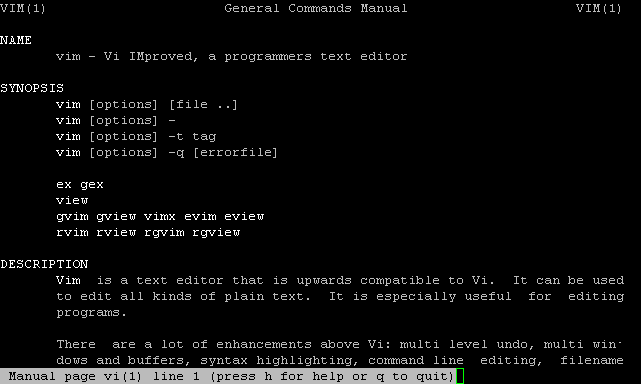


图 2-5 vi 命令的使用信息

②查看“sed”、“awk”命令描述的详细信息，将其操作命令及主要描述信息填写到表

2-5 中。

**表 2-5 查看不同命令描述信息**

###### 8、mkdir

①创建单目录“temptest”，其操作命令如下。

# mkdir temptest

②创建目录时显示返回信息，其操作命令如下。

# mkdir –v temptest2

③创建“test1”目录，并在该目录下逐级创建目录“test2”、“test3”、“test4” “te st5”，其操作命令如下所示。

# mkdir test1/test2/test3/test4/test5

该操作命令将出现如图 2-6 错误提示，这由于没有逐级的目录存在导致，可使用“-v”

和“-p”选项自动填充目录和显示返回结果，其操作命令如下，并将返回结果填写至表 2-6



图 2-6 mkdir 创建文件错误提示

中。

# mkdir –p test1/test2/test3/test4/test5

**表 2-6 逐级创建目录**

###### 9、touch

①创建文件“example”，其操作命令如下。

# touch example

②更改文件创建时间，其操作命令如下，并查看更改后的信息，将输出结果填写到表 2

-8 中。

# touch -d "2012-10-14 15:16" example # stat example

**表 2-8 修改文件创建时间**

###### 10、rm

①删除创建的 temptest 目录，其操作命令如下，将返回结果填写到表 2-9 中。

# rm temptest

**表 2-9 删除目录**

②分别使用“-r、-f、-rf”选项删除目录 temptest2，将输出结果填写到表 2-10 中。

**表 2-10 使用选项删除目录**

###### 11、cp

①创建 test1 目录，将/usr/bin/kernel-install 文件，复制至 test1 目录并修改其文件名为

“example1”，其操作命令如下所示。

# mkdir /root/test1 # cd /usr/bin/

# cp kernel-install /root/test1/example1

②创建 test2 目录，并在 test1 目录下创建 example2，使用“-r”选项将 test1 目录两个文件复制至 test2 目录下，将其操作命令填写到表 2-11 中。

**表 2-11 使用“r”选项进行文件复制**

###### 12、cat

①查看/etc/passwd 文件的内容，其操作命令如下，输出结果如图 2-7 所示。

# cat /etc/passwd

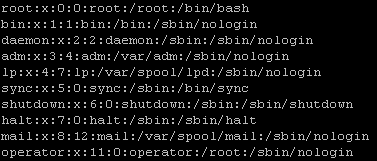


图 2-7 /etc/passwd 文件内容

②分别使用“-n”、“-b”选项查看/etc/passwd 文件，比对两个选项查看结果，将结果区别内容填写到表 2-12 中。

**表 2-12 “-n”和“-b”命令选项的结果区别**

###### 13、more

①查看/usr/bin/kernel-install 文件的内容，并使用【Enter】键和【Space】键进行翻阅， 将两个快捷键的差异处填写到表 2-13 中。

**表 2-13 快捷键的使用方法总结**

②分别使用“-c”和“-数字”选项进行查看/usr/bin/kernel-install 文件内容，比对输出结果展示，将两种选项使用的不同之处填写到表 2-14 中。

**表 2-14 “-c”和“-数字”命令选项不同之处**

###### 14、less

查看/usr/bin/kernel-install 文件，并使用“j、k、G、g、h”等快捷键进行查看，比对不同快捷键使用方法，将其不同之处填写到表 2-15 中。

**表 2-15 less 命令快捷键使用方法对比**

###### 15、head

①直接查看/usr/bin/kernel-install 文件，可看到其默认的显示前10 行，其操作命令如下。

# head /usr/bin/kernel-install

②使用“-n+数字”和“-c+数字”选项查看/usr/bin/kernel-install 文件，比对不同选项输出结果，将其选项的不同之处填写到表 2-16 中。

**表 2-16 head 命令选项对比说明**

###### 16、vi

①创建一个 example2 文件，并使用“vi”命令进行编辑，内容编写成三行分别为：学号、姓名（拼音表示）、学院（拼音表示），编写完毕后输入“:wq”退出，其操作命令如

下，并使用“cat”命令进行查看，将操作命令及其输出结果填写到表 2-17 中。

**表 2-17 example2 文件内容查看**

②使用内置“yy”（复制）和“p”（粘贴）快捷键将 example2 文件中光标所在行进行复制后保存退出，查看该文件内容将其结果填写到表 2-18 中。

**表 2-18 vi 命令的“yy”和“p”选项实验结果**

③使用内置“x”快捷键命令删除一个字符、“dd” 快捷键命令删除光标所在行、“n dd”快捷键命令删除光标所在行后 n-1 行。在进行删除命令操作后，使用“p”快捷键命令， 将其展示结果填写到表 2-19 中。

**表 2-19 vi 命令的“p”选项结果**

###### 17、awk

①使用如下命令进行查看/etc/passwd 文件的内容，将输出结果填写到表 2-20 中。

# awk '{print}' /etc/passwd

**表 2-20 awk 命令输出结果**

②查看文件指定信息，如查看/etc/passwd 文件中用户名称，其操作命令如下，将其输出结果填写到表 2-21 中。

# cat /etc/passwd |awk -F ' : ' '{print $1}'

**表 2-21 查看指定信息**

③查看指定多个信息，如查看/etc/passwd 文件中用户名称和用户可执行的 Shell 命令信息，其操作命令如下所示，将其输出结果填写到表 2-22 中。

# awk -F: '/root/' /etc/passwd

**表 2-22 指定输出多个信息**

###### 18、sed

①创建/root/example3 文件，并填写如 example2 中内容，实现在文件中第二行添加“\* Hello World \*”内容，其操作命令如下，查看文件内容并将其输出结果填写到表 2-23 中。

# sed ' 2a \* Hello World \* ' /opt/example3

**表 2-23 插入内容**

②实现将“Hello World”内容替换为“I like Linux”，其操作命令如下，查看文件内容并将其输出结果填写到表 2-24 中。

**表 2-24 内容替换**

# sed ' s / Hello World/ I like Linux/ g ' /opt/example3

③实现将文档的第 2 至 4 行删除并输出，其操作命令如下，将其输出结果填写至表 2-2

5 中。

# sed '2,4d' /opt/example3

**表 2-25 多行删除**

##### 七、实验扩展

###### 1、文件与目录

1. Linux 下的文件都是文本文件吗？
2. Linux 下是否可以通过 vi 等工具对音乐、视频等文件进行编辑？为什么？
3. Windows 下可以为文件目录创建快捷方式，Linux 下是否也可以为文件目录创建快捷方式？

###### 2、常用操作命令

1. Linux 的基本操作命令是系统内置的吗？
2. 是否可以为操作系统增加自己编写的命令？具体应该怎么做？

# 实验三：网站服务器

##### 一、实验目的

1、理解网站服务器的工作原理；

2、掌握Apache 服务器的安装、配置与管理；

3、掌握静态网站、PHP 动态网站的发布方法；

4、掌握单一网站、虚拟目录、多站点的发布与管理；

5、掌握通过 WordPress 创建个人网站的部署流程和具体方法。

##### 二、实验学时

2 学时

##### 三、实验类型

综合性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装VirtualBox 虚拟化软件，安装Putty 管理终端软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

预先下载WordPress 安装程序。

##### 五、实验任务

1、完成在 CentOS 操作系统上安装配置Apache 服务器；

2、完成 PHP 环境的安装与配置；

3、完成单站点、虚拟目录、多站点的发布； 4、完成 WordPress 的部署实施。

##### 六、实验内容及步骤

###### 1、Apache 安装

1. 安装软件

在 CentOS 操作系统中 Apache（Web 服务器）是通过 httpd 软件提供服务，其安装命令

如下，安装过程如图 3-1 所示。

# yum install httpd ##服务启动

# systemctl start httpd

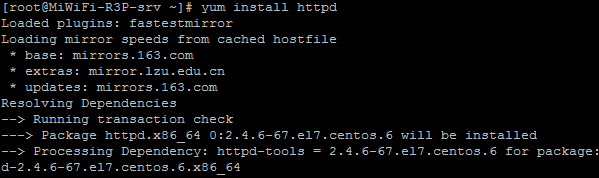


图 3-1 安装 httpd 服务

1. 关闭防火墙

为了网站能够在外部访问，简单的操作是关闭防火墙，当然这种做法不是安全的，在实验过程中可以这样来做，在真实环境中应该是通过配置防火墙规则来开放 80 端口来实现网站的外部访问。关闭防火墙命令如下。

# systemctl stop firewalld

1. 测试访问

用户在本地浏览器中输入[http://IP](http://IP/) 地址（IP 地址为虚拟主机配置地址，如 [http://172.16.](http://172.16/) 124.187）查看是否能够访问 Apache 测试界面，如图 3-2 所示，以验证 Apache 服务是否安装成功。



图 3-2 测试 httpd 服务

###### 2、发布第一个网站

1. 上传文件

网站页面内容在 Apache 服务中默认存放位置为/var/www/html，可通过 FileZilla 或 Win SCP 等桌面化工具，将HTML 代码文件放入该目录下，如图 3-3 所示。

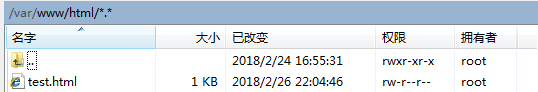


图 3-3 上传 HTML 文件

1. 服务重启

上传完 HTML 文件后重启httpd 服务，服务重启命令如下。

# systemctl restart httpd

1. 测试访问

在本地浏览器中输入 [http://IP](http://IP/) 地址/test.html，访问结果如图 3-4 所示。

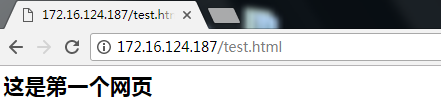


图 3-4 测试

###### 3、发布 PHP 网站

1. 环境准备

①安装 PHP 软件

发布PHP 程序前，需确保虚拟主机中已经安装PHP 相关软件。

本次实验采用在线安装方式进行 PHP 软件安装，安装命令如下，安装过程如图 3-5 所示。

# yum install php

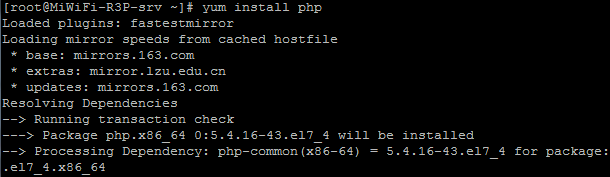


图 3-5 安装 PHP 服务

②测试PHP 环境

PHP 软件安装后可通过“phpinfo()”方法来检测是否安装成功。

在/var/www/html 目录下新建 test.php 文件，文件内容如图 3-6 所示。在本地浏览器中输入 [http://IP](http://IP/) 地址/test.php，查看文件是否能够访问，如图 3-7 所示。

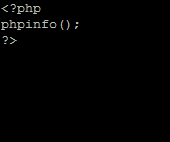


图 3-6 安装 PHP 服务

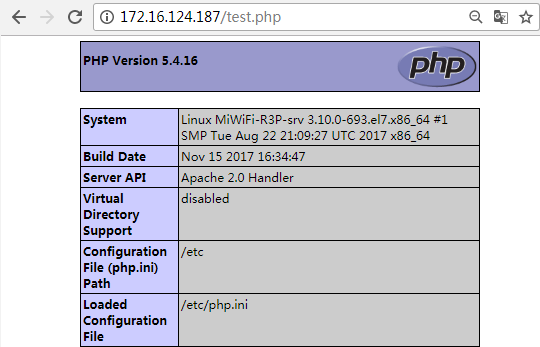


图 3-7 测试 PHP 服务

1. 部署PHP 网站

编写“计算出半径为 10 个单位的圆的面积”的 PHP 程序页面，并能够访问该页面，将

其实现的操作过程填写到表 3-1 中。

**表 3-1 部署 PHP 网站**

###### 4、发布虚拟目录

1. 修改虚拟目录配置文件

①创建目录

在/etc/httpd/目录下创建 vhost-conf.d 目录，其操作命令如下，如图 3-8 所示。

# cd /etc/httpd/

# mkdir vhost-conf.d

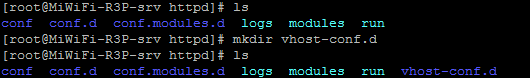


图 3-8 创建虚拟主机目录

②编辑配置文件

在 vhost-conf.d 目录下新增虚拟目录配置文件 VirtualHost.conf，其操作命令如下。

# cd /etc/httpd/vhost-conf.d # touch VirtualHost.conf

在配置文件中增加如下内容后保存退出。

<VirtualHost \*:80>

ServerAdmin root@localhost

#通过虚拟目录/cs 代替实际/var/www/html 目录

Alias /cs /var/www/html

<Directory "/var/www/html"> Options FollowSymLinks AllowOverride All

Require all granted

</Directory>

</VirtualHost>

1. 引用虚拟文件

虚拟文件配置完成保存后，需要在 httpd 的主配置文件引用才可以实现其相应的功能。引用的方法是在配置文件/etc/httpd/conf/httpd.conf 末尾添加如下命令。

IncludeOptional vhost-conf.d/\*.conf

1. 服务重启

完成配置文件编辑后，需重启 httpd 服务，其操作命令如下。

# systemctl restart httpd

1. 虚拟目录验证

在本地浏览器中输入 [http://IP](http://IP/) 地址/cs/test.html，测试虚拟目录是否生效，将访问结果及其配置虚拟目录目的意义填写到表 3-2 中。

**表 3-2 访问结果及目的意义**

###### 5、发布多个网站

1. 使用同一 IP 和不同端口发布多个网站

①创建网站页面

根据发布第一个网站操作过程，完成第二个网站目录及文件创建。并将配置信息填写到表 3-3 中。

●在/var/www/目录下创建html1 目录；

* 在/var/www/html1 目录下创建 test.html，并将展示出“这是第二个网页”字样。

**表 3-3 创建网站页面**

②配置监听端口

编辑 httpd 服务的全局配置文件/etc/httpd/conf/httpd.conf，增加 httpd 服务的监听端口 82

（80 为默认配置的监听端口），编辑完成后保存退出，配置内容如图 3-9 所示。



图 3-9 增加监听端口

③修改配置文件

编辑虚拟目录创建的配置文件VirtualHost.conf，将原本内容替换成如下内容，编辑完成后保存退出。

<VirtualHost \*:80>

ServerAdmin root@localhost

##第一个网站使用 80 端口，配置根目录为/var/www/html DocumentRoot /var/www/html

<Directory "/var/www/html">

Options FollowSymLinks

AllowOverride All

Require all granted

</Directory>

</VirtualHost>

<VirtualHost \*:82>

ServerAdmin root@localhost

##第一个网站使用 82 端口，配置根目录为/var/www/html1

DocumentRoot /var/www/html1

<Directory "/var/www/html1">

Options FollowSymLinks

AllowOverride All

Require all granted

</Directory>

</VirtualHost>

④服务重启

完成配置文件编辑后，需重启httpd 服务,如果重启httpd 过程中报错的话重启下服务器， 然后再启动httpd 服务，重启命令如下。

# systemctl restart httpd

⑤测试访问

在本地浏览器中分别输入两个网站的地址：[http://IP](http://IP/) 地址/test.html、[http://IP](http://IP/) 地址:82/tes t.html，验证端口是否生效，访问结果如图 3-10、3-11 所示。

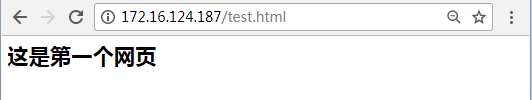


图 3-10 通过 80 端口发布



图 3-11 通过 82 端口发布

1. 使用域名发布多个网站

①修改配置文件

编辑虚拟目录创建的配置文件VirtualHost.conf，将原本内容替换成如下内容，编辑完成后保存退出。

<VirtualHost \*:80> ServerAdmin root@localhost

##第一个网站使用 80 端口，其网站使用域名为 [www.yi.com](http://www.yi.com/)

ServerName [www.yi.com](http://www.yi.com/) DocumentRoot /var/www/html

<Directory "/var/www/html"> Options FollowSymLinks AllowOverride All

Require all granted

</Directory>

</VirtualHost>

<VirtualHost \*:80>

ServerAdmin root@localhost

##第二个网站使用 80 端口，其网站使用域名为 [www.two.com](http://www.two.com/)

ServerName [www.two.com](http://www.two.com/) DocumentRoot /var/www/html1

<Directory "/var/www/html1"> Options FollowSymLinks AllowOverride All

Require all granted

</Directory>

</VirtualHost>

②服务重启

完成配置文件编辑后，需重启 httpd 服务，其操作命令如下。

# systemctl restart httpd

③hosts 配置

编辑本地 hosts 文件，其文件路径为 C:\Windows\System32\drivers\etc\hosts，hosts 文件增加内容如图 3-12 所示。

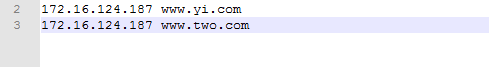


图 3-12 修改本地 hosts 文件

④测试访问

在本地浏览器中分别输入两个网站的地址：<http://www.yi.com/test.html>、http://www.two. com/test.html，验证域名发布网站是否生效，访问结果如图 3-13、3-14 所示。



图 3-13 通过 [www.yi.com](http://www.yi.com/) 域名访问



图 3-14 通过[www.two.com](http://www.two.com/) 域名访问

###### 6、使用 WordPress 创建个人网站

1. 环境准备

运行WordPress 程序，虚拟主机上需先安装运行 httpd、php、mariadb 相关软件。

①基础软件安装

根据实验步骤 1、3 完成 httpd、php 软件安装和服务启动，本部分主要介绍 mariadb 软件的安装，其安装命令如下，安装过程如图 3-15 所示。

# yum install mariadb mariadb-server php-mysql

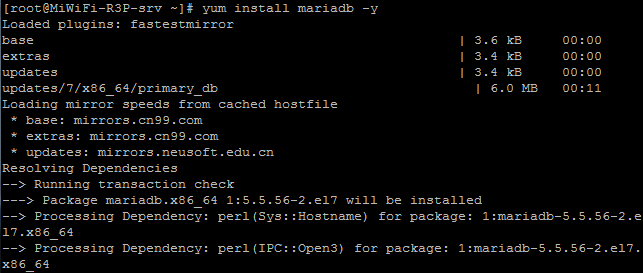


图 3-15 安装 mariadb 服务

②配置 mariadb

启动 mariadb 数据库服务，其操作命令如下。

# systemctl start mariadb.service

由于安装完 mariadb 后没有设置密码，输入以下命令，点击【Enter】可直接进入登录数据库，从而进行数据库权限配置，如图 3-16 所示。

# mysql -uroot -p

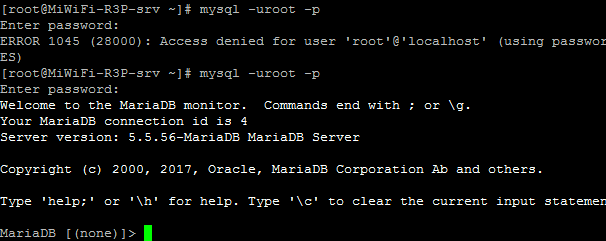


图 3-16 登录数据库

根据数据库操作命令，完成以下数据操作，其操作命令如下，配置过程如图 3-17 所示。

* 在 mariadb 中创建一个名为“wpdb”的数据库；
* 在数据库中为“wpdb”数据库创建用户（wpadmin）、密码（pass）及访问权限（本地

localhost 访问）。

> create database wpdb character set utf8; ##为 wpdb 数据库创建用户名和密码

> grant all privileges on wpdb.\* to 'wpadmin'@'localhost' identified by 'pass';

##刷新数据库权限使配置生效

> flush privileges;

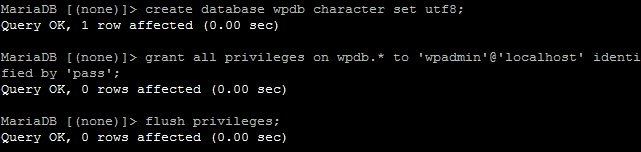


图 3-17 配置数据库

③获取 WordPress 软件

获取WordPress 安装包软件可通过本课程网站（[http://linux.xg.hactcm.edu.cn](http://linux.xg.hactcm.edu.cn/)）下载获得， 也可通过 WordPress 官方网站（https://cn.wordpress.org/txt-download）下载获得，如图 3-18 所示。本实验所使用的 WordPress 软件为 wordpress-4.9.4-zh\_CN.tar.gz。

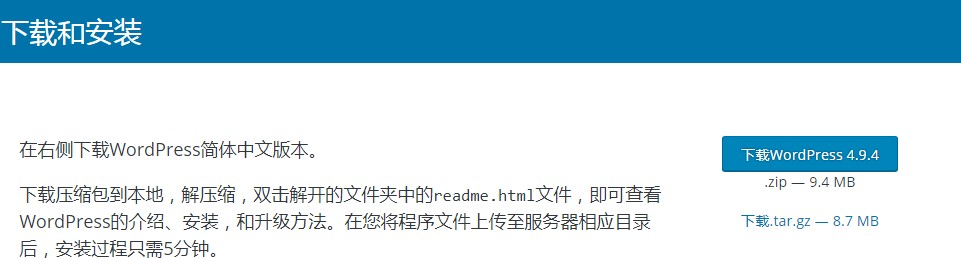


图 3-18 下载 WordPress 安装包

1. WordPress 软件安装

将下载的WordPress 软件包使用工具上传至/var/www/html 目录中，其软件过程如下。

①压缩包解压

进入/var/www/html 目录中，解压 WordPress 安装包压缩文件，其操作命令如下，过程如图 3-19 所示。

# cd /var/www/html

# tar –zxvf wordpress-4.9.4-zh\_CN.tar.gz

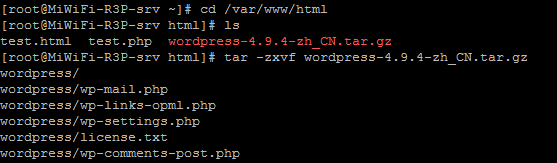


图 3-19 解压安装包

②编辑配置文件

安装包解压缩完成后，将其 wordpress/wp-config-sample.php 配置文件进行复制重命名为

wp-config.php，其操作命令如下。

# cp wordpress/wp-config-sample.php wordpress/wp-config.php

编辑WordPress 配置文件 wp-config.php 为以下内容，编辑完成后保存退出。

##编辑配置文件

# vi wordpress/wp-config.php

##WordPress 数据库的名称define('DB\_NAME', 'wpdb'); ##MySQL 数据库用户名define('DB\_USER', 'wpadmin'); ##MySQL 数据库密码define('DB\_PASSWORD', 'pass'); ##MySQL 主机define('DB\_HOST', 'localhost'); ##创建数据表时默认的文字编码define('DB\_CHARSET', 'utf8');

##数据库整理类型。如不确定请勿更改define('DB\_COLLATE', '');

1. 服务重启

完成配置文件编辑后，需重启 httpd 服务，其操作命令如下。

# systemctl restart httpd

1. Web 化安装

在本地浏览器中输入 [http://IP](http://IP/) 地址/wordpress，WordPress 软件自动跳转到安装界面，用户可以根据提示完成 WordPress 安装，如图 3-20 所示。



图 3-20 Web 化安装WordPress

1. 访问测试

安装完成后，用户在本地浏览器中输入 [http://IP](http://IP/) 地址/wordpress，即可访问创建的博客网站，如图 3-21 所示。



图 3-21 使用WordPress 发布测试网站

1. 目录修改

修改 httpd 服务的配置文件，使 WordPress 博客网站可以直接通过 [http://IP](http://IP/) 地址进行访问，将配置信息及过程填写到表 3-4 中

**表 3-4 修改网站配置根目录**

##### 七、实验分析

###### 1、Web 服务器安全

1. 目前网络安全越来越得到重视，网站安全也不能忽视，如何通过对 Apache 进行配置保证网站的安全？
2. Apache 的运行会产生访问日志和错误日志，请分别对其中的一条错误日志和访问日志进行解读。

###### 2、多站点发布

1. 使用一个 IP 地址发布多个网站，有哪些方法？
2. 进行多站点发布时，一个网站遭受攻击，其它网站会出现哪些问题？

# 实验四：代理服务器

##### 一、实验目的

1、理解正向代理服务器和反向代理服务器的工作原理；

2、掌握搭建反向代理服务器的方法；

3、掌握使用方向代理实现负载均衡。

##### 二、实验学时

1. 学时

##### 三、实验类型

创新性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装VirtualBox 虚拟化软件，安装Putty 管理终端软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

无。

##### 五、实验任务

1、完成 Nginx 反向代理服务器部署安装；

2、完成反向代理服务器实现内部 Web 服务器的负载均衡；

3、完成对内部Web 服务器的性能测试。

##### 六、实验内容及步骤

###### 1、应用场景设计

1. 场景描述

本实验使用 3 台 CentOS 虚拟主机，其中 2 台为Web 服务器，进行 http 业务发布，1 台为 Nginx 服务器，进行代理服务实现，并通过 VirtualBox 软件中网卡模式的选择，实现内外网的分类，其场景应用结构如图 4-1 所示。

1. 台CentOS 虚拟主机的 IP 地址地址配置如表 4-1 所示。

**表 4-1 虚拟主机 IP 地址配置**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **虚拟主机名称** | **网络配置** | **网关** | **网卡模式** | **描述** |
| 1 | Web 服务器 1 | 10.0.2.14/24 | 10.0.2.1 | 桥接 | 业务网卡 |
| 2 | Web 服务器 2 | 10.0.2.15/24 | 10.0.2.1 | 桥接 | 业务网卡 |
| 3 | Nginx 服务器 | 172.16.124.102/24 | 172.16.124.1 | 桥接 | 代理服务 |
| 4 | 10.0.2.102/24 | 10.0.2.1 | 内部业务通信 |

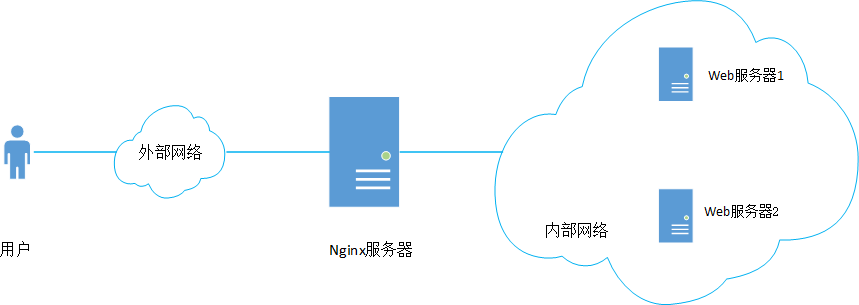


图 4-1 场景设计结构

1. 网络配置

Nginx 服务器需要配置 2 个 IP 地址，一个用于代理服务，供外网访问；一个用于内部业务通信，本次实验的虚拟主机网卡名为“ifcfg-enp0s3”。

其“代理服务”网络配置如下所示，如图 4-2 所示。

#vi /etc/sysconfig/network-scripts/ifcfg-enp0s3 TYPE=Ethernet

BOOTPROTO=static IPADDR=172.16.124.102 PREFIX=24 GATWAY=172.16.124.1 DEFROUTE=yes IPV4\_FAILURE\_FATAL=no

NAME=enp0s3 DEVICE=enp0s3 ONBOOT=yes PROXY\_METHOD=none BROWSER\_ONLY=no

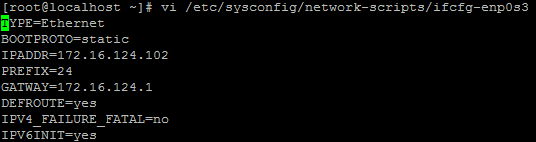


图 4-2 配置 Nginx 服务器IP-1

将网卡配置文件 ifcfg-enp0s3 进行复制并重命名为 ifcfg-enp0s3:1，编辑 ifcfg-enp0s3:1 文件进行“内部业务通信”网络配置，其操作命令如下。

# cd /etc/sysconfig/network-scripts/ # cp ifcfg-enp0s3 ifcfg-enp0s3:1

# vi ifcfg-enp0s3:1 TYPE=Ethernet BOOTPROTO=static IPADDR=10.0.2.102 PREFIX=24 GATWAY=10.0.2.1 DEFROUTE=yes IPV4\_FAILURE\_FATAL=no

NAME=enp0s3 DEVICE=enp0s3 ONBOOT=yes PROXY\_METHOD=none BROWSER\_ONLY=no

##启动网卡

# ifup ifcfg-enp0s3:1 ##重启网络

# systemctl restart network

Nginx 服务器配置完成后，通过如下命令查看 IP 地址配置，网络配置结果如图 4-3 所示。

# ip addr

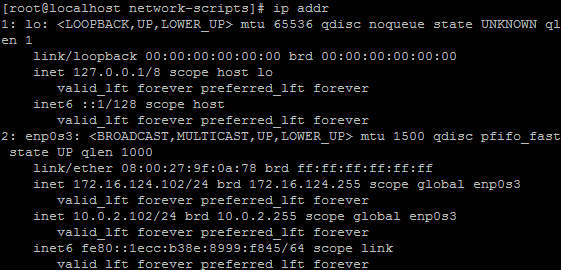


图 4-3 Nginx 服务器网络配置

参照表 4-1，完成 3 台虚拟化主机的部署，完成 2 台Web 服务器的网络配置，并将配置命令填写到表 4-2 中。

**表 4-2 Web 服务器网络配置**

###### 2、部署 Apache 服务器

在 2 台 CentOS 的 Web 服务器上安装Apache 服务，可参照《实验三：网站服务器》实验指导书中 Apache 安装过程，进行软件安装、服务启动操作。

###### 3、部署 Nginx 服务器

1. 配置安装源

本次实验获取 Nginx 软件包，是通过引用官方的 RPM 源进行获取，其操作命令如下， 配置过程如图 4-4 所示。

##导入 Nginx 官方 GPG 密码，如果没有该密码，下载 RPM 包是会出现错误

# rpm --import <http://nginx.org/keys/nginx_signing.key> ##加入 Nginx 的 RPM 包软件

# rpm -ivh <http://nginx.org/packages/centos/7/noarch/RPMS/nginx-r> elease-centos-7-0.el7.ngx.noarch.rpm

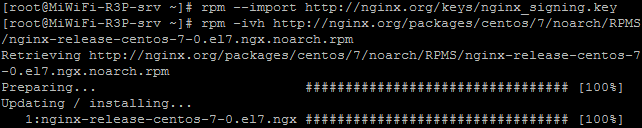


图 4-4 配置 Nginx 安装源

1. 安装Nginx

加入 Nginx 的安装源后，输入以下命令进行 Nginx 的安装，其安装过程如图 4-5 所示。

# yum install nginx

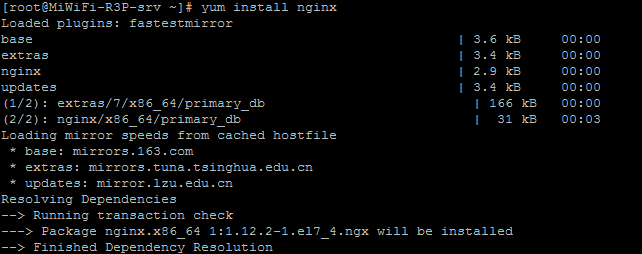


图 4-5 安装 Nginx

1. Nginx 服务配置

①防火墙配置

开启防火墙的TCP/80 端口，从而可远程访问 Nginx 的 Web 服务，其命令如下所示。

##添加 TCP/80 端口永久访问

# firewall-cmd --zone=public --add-port=80/tcp --permanent ##重新加载 firewalld 防火墙规则

# firewall-cmd --reload

②服务启动

完成安装后，需重启 Nginx 服务，其操作命令如下，

##启动 Nginx 服务

# systemctl start nginx

##设置 Nginx 服务开机自启动

# systemctl enable nginx

1. Nginx 测试

用户在本地浏览器中输入 [http://IP](http://IP/) 地址（IP 地址为 Nginx 虚拟化主机外部服务地址），查看是否能够访问 Nginx 欢迎界面，如图 4-6 所示，以验证 Nginx 服务是否安装



图 4-6 测试 Nginx 服务

成功。

###### 4、负载均衡的实现

本次实验所使用的负载均衡算法是轮询算法，在轮询算法中 Weight 越大，通过 Nginx

代理分配访问的几率就越大。

本次实验设置 Web 服务器 1 的 Weight 值为 1，Web 服务器 2 值为 2，简单地说，例如通过Nginx 服务器进行三次业务访问，一次请求转发给Web 服务器 1，两次请求转发给 We b 服务器 2，具体配置如下所示。

1. 修改配置文件

编辑Nginx 服务的默认配置文件 default.conf，该文件存放的目录为/etc/nginx/conf.d，将配置文件中内容修改成如下所示，编辑完成后保存退出。

# vi /etc/nginx/conf.d/default.conf server {

##设置监听端口为 80

listen 80; server\_name localhost;

……

location / {

root /usr/share/nginx/html; index index.html index.htm; proxy\_pass http://fzjh;

}

……

编辑Nginx 服务的配置文件 nginx.conf，该文件存放的目录为/etc/nginx，在该配置文件中进行负载均衡的配置，将配置文件中部分内容修改成如下所示，编辑完成后保存退出。

# vi /etc/nginx/nginx.conf

……

http {

include /etc/nginx/mime.types; default\_type application/octet-stream;

log\_format main '$remote\_addr - $remote\_user [$time\_local]

"$request" '

'$status $body\_bytes\_sent "$http\_referer" ' '"$http\_user\_agent" "$http\_x\_forwarded\_for"'; access\_log /var/log/nginx/access.log main; sendfile on;

#tcp\_nopush on; keepalive\_timeout 65; #gzip on;

##设置负载均衡，并设置轮询的依据upstream fzjh {

server 10.0.2.14:80 weight=1;

server 10.0.2.15:80 weight=2;

}

……

本次实验通过设置 Weight 的轮询算法实现业务的负载均衡，请查找 Nginx 的其他负载均衡调度算法，并将算法实现填写到表 4-3 中。

**表 4-3 负载均衡算法**

1. 服务重启

完成配置文件编辑后，需重启 Nginx 服务，其操作命令如下。

# systemctl restart nginx

1. 访问测试

在本地浏览器中输入 Nginx 服务地址，检测能否访问到内部 Web 服务器发布的内容， 以验证代理服务是否配置成功，访问结果如图 4-7 所示，该页面为内部 Web 服务器 1 的网站访问界面。

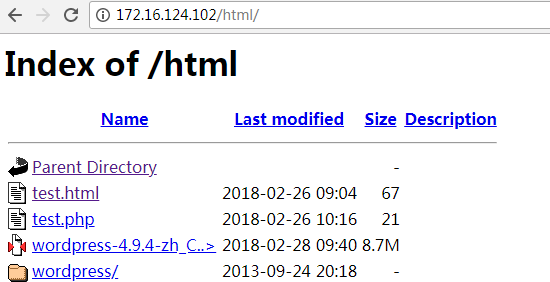


图 4-7 测试负载均衡发布网页

###### 5、性能测试

1. 安装测试工具

在 Nginx 接收到请求之后，需把请求分发到后端 Web 服务集群中，需记录 Nginx 的分发日志来分析每台Web 服务器处理的请求数目。

ab 是 apache 自带的压力测试工具，可以对 Apache、Nginx、Tomcat、IIS 等 Web 服务器进行模拟用户访问，进而进行压力测试，安装 ab 命令如下所示。

# yum install httpd-tools

1. 修改配置文件

通过修改Nginx 配置文件 nginx.conf，将 Nginx 的访问日志进行记录，为后续测试结果查看提供参考，将其配置文件部分内容修改为如下所示。

default\_type application/octet-stream; log\_format main

' $remote\_user [$time\_local] $http\_x\_Forwarded\_for $remote

\_addr $request '

'$http\_x\_forwarded\_for ' '$upstream\_addr '

'ups\_resp\_time: $upstream\_response\_time ' 'request\_time: $request\_time';

#设置 Nginx 的访问日志

access\_log /var/log/nginx/access.log main; sendfile on;

#tcp\_nopush on; keepalive\_timeout 65; #gzip on;

#设置负载均衡配置upstream fzjh {

server 10.0.2.14:80 weight=1;

server 10.0.2.15:80 weight=2;

}

include /etc/nginx/conf.d/\*.conf;

}

/etc/nginx/mime.types;

http {

include

1. 服务重启

完成配置文件编辑后，需重启 Nginx 服务，其操作命令如下。

# systemctl restart nginx

1. 设置测试命令

通过 ad 压力测试工具进行 Nginx 代理业务访问，其测试命令如下所示。

##–n 表示请求数，-c 表示并发数

# ab –n 100 –c 10 <http://172.16.124.102/html/test>

1. 查看测试结果

执行 ab 压力测试后，查看 Nginx 的日志文件，其日志默认存放在/var/log/nginx/目录下， 其查看命令如下，部分日志结果如图 4-8 所示，将 Nginx 日志结果进行分析填写到表 4-4 中。

# cat /var/log/nginx/access.log

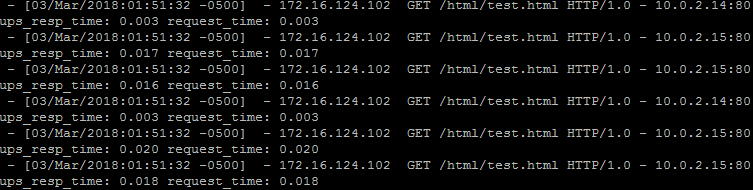


图 4-8 Nginx 日志查看

**表 4-4 Nginx 日志分析结果**

##### 七、实验扩展

###### 1、Nginx 服务器功能

1. Nginx 除做反向代理服务器外，可以做正向代理服务器吗？如果能，怎样实现？
2. Nginx 和Tomcat、Apache 的区别是什么？请简要描述。

###### 2、性能测试

（1）性能测试工具有哪几种？请简要描述。

# 实验五：文件服务器实现

##### 一、实验目的

1、理解文件服务器的工作原理；

2、掌握文件服务器的部署与实施；

3、掌握 FTP 文件服务器的实现方法。

##### 二、实验学时

2 学时

##### 三、实验类型

综合性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装 VirtualBox 虚拟化软件，安装 Putty 管理终端软件，安装 File Zilla Client 软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

无。

##### 五、实验任务

1、完成 vsftpd 的部署，实现 FTP 服务器；

2、基于 vsftpd 构建开放共享的 FTP 文件服务。

##### 六、实验内容及步骤

###### 1、实验常见

①在VirtalBox 虚拟化软件上安装 CentOS 7 操作系统；

②虚拟化主机配置固定的 IP 地址；

③在虚拟化主机上安装并开启 SSH 远程管理服务，并设置防火墙规则，运行 TCP/22 端口进行访问系统；

④本次安装PuTTY 软件能够进行 SSH 远程管理虚拟化主机；

⑤本地安装 FileZilla 客户端软件，用户连接 FTP 服务器。

###### 2、安装 vsftpd

vsftpd 服务软件是目前最为流行的 Linux 操作系统中的 FTP 服务软件，且被广泛的集成在 Linux 发行版中。

1. 检测 vsftpd

目前 vsftpd 服务软件被广泛集成在 Linux 发行版中，检测系统中是否已经安装 vsftpd 服务，其操作命令如下所示。

##检测 vsftpd 状态，验证服务是否安装

# systemctl status vsftpd

1. 安装 vsftpd

通过 yum 的方式进行安装vsftpd，其操作命令如下所示。

# yum install vsftpd

1. 服务配置

安装完成后，进行 FTP 服务配置，其主要操作命令如下所示。

#开启 FTP 服务

#查看 FTP 服务状态

#重启 FTP 服务

#停止 FTP 服务

#设置 FTP 服务开机自启

#取消 FTP 服务开机自启

# systemctl start vsftpd

# systemctl status vsftpd # systemctl restart vsftpd # systemctl stop vsftpd

# systemctl enable vsftpd

# systemctl disable vsftpd

1. 验证 FTP 服务

①安装工具

安装 ftp 工具进行验证 vsftpd 服务安装的正确性，安装命令如下所示。

# yum install ftp

②vsftpd 服务验证

使用 ftp 命令工具登录 FTP 服务，vsftpd 默认配置仅允许匿名用户访问，进而验证 vsft pd 服务是否安装成功。匿名用户名为 anonymous，密码为空。

##登录 FTP 服务器# ftp localhost Trying ::1...

Connected to localhost (::1). 220 (vsFTPd 3.0.2)

##输入匿名用户名

Name (localhost:root): anonymous ##提示输入密码信息

331 Please specify the password ##点击【Enter】输入空密码信息Password:

230 Login successful

Remote system type is UNIX.

Using binary mode to transfer files. ##登录成功，进入 FTP 服务器

ftp>

###### 3、发布 FTP 服务

1. 防火墙配置

FTP 服务默认使用的是TCP/21 端口，更新其防火墙策略使其 FTP 服务可以在外部登录访问，其操作命令如下。

##开启 FTP 服务外部访问

# firewall-cmd --zone=public --add-service=ftp --permanent ##重新加载防火墙策略规则

# firewall-cmd --reload

1. FileZilla 客户端软件

获取 FileZilla 客户端软件可通过本课程网站（[http://linux.xg.hactcm.edu.cn](http://linux.xg.hactcm.edu.cn/)）下载获得， 也可通过 FileZilla 官方网站（https://filezilla-project.org/）下载获得。本实验所使用的 FileZil la 软件为 FileZilla\_Server-0\_9\_60\_2.exe。

点击下载的 EXE 执行安装文件，可根据安装过程提示进行默认选择安装。

1. 验证测试

软件安装后，打开客户端软件测试 FTP 服务是否能够进行远程登录。

在【主机】中输入 FTP 服务地址（CentOS 虚拟主机 IP 地址），在【用户名】中输入“a nonymous”，在【密码】中输入空，点击【快速连接】按钮，进行 FTP 远程登录访问，记录登录过程显示信息与登录结果信息，并填写到表 5-1 中。

**表 5-1 FTP 服务远程登录**

###### 4、开放共享的 FTP 服务

FTP 服务默认的匿名用户权限受到很大的限制，下面进行匿名用户的配置，来构建一个开放共享的FTP 服务。

①创建匿名用户上传文件的目录，其操作命令如下。

# mkdir /www

# mkdir /www/ftp

# mkdir /www/ftp/pub ##设置匿名用户的上传目录

# mkdir /www/ftp/pub/upload

②修改上传目录的权限。

##修改上传目录的权限为 777，所有系统用户都有读、写、执行权限# chmod 777 /www/ftp/pub/upload

③编辑 FTP 服务的配置文件/etc/vsftpd/vsftpd.conf，在编辑配置前可将配置文件先进行备份，可用于用户恢复原始的配置选项，其操作命令如下。

# cp /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.bak

将配置文件部分内容修改成如下所示配置，编辑完成后保存退出，其操作命令如下。

# vi /etc/vsftpd/vsftpd.conf anonymous\_enable=YES anon\_mkdir\_write\_enable=YES anon\_root=/www/ftp/pub local\_enable=YES write\_enable=YES local\_umask=022 anon\_upload\_enable=YES dirmessage\_enable=YES xferlog\_enable=YES connect\_from\_port\_20=YES xferlog\_std\_format=YES listen=YES pam\_service\_name=vsftpd userlist\_enable=YES tcp\_wrappers=YES

④服务重启，配置文件编辑完成后，需重启 FTP 服务，其操作命令如下。

# systemctl restart vsftpd

⑤关闭 Linux 操作系统中SELinux，其配置命令如下。

# setenforce 0

⑥验证匿名服务。在本地 FileZilla 客户端软件中，使用匿名用户登录 FTP 服务，检测匿名用户服务是否配置成功，并将登录结果填写到表 5-2 中。

**表 5-2 查看共享 FTP 服务**

###### 5、创建用户与私人目录

1. 修改配置文件

修改 FTP 服务的配置文件vsftpd.conf，完成以下要求配置，具体配置文件修改内容如下所示。

①关闭 FTP 匿名访问权限；

②配置操作系统本地用户具有 FTP 访问权限和写权限。

# vi /etc/vsftpd/vsftpd.conf ##关闭匿名用户访问权限anonymous\_enable=NO ##开启本地用户访问权限local\_enable=YES

##开启本地用户写权限write\_enable=YES local\_umask=022 xferlog\_enable=YES

xferlog\_std\_format=YES

##用户只能操作自己的主目录chroot\_local\_user=YES

##允许用户写入文件allow\_writeable\_chroot=YES

1. 用户创建

在 FTP 虚拟化主机中创建用户，完成以下要求，具体配置命令如下所示。

①在 FTP 虚拟化主机操作系统中创建普通用户 student、student2，并设置该用户不能登录操作系统；

②配置本地用户具有 FTP 访问权限，且禁止虚拟化主机中系统用户通过 FTP 进行访问。

##创建本地用户 student，并指定用户不能登录操作系统# useradd student -s /sbin/nologin

##创建用户之后，需要对用户的主目录进行修改# mkdir /var/ftp/student\_root

# chown -R student /var/ftp/student\_root # chmod -R 755 /var/ftp/student\_root

##设置 student 的密码

# passwd student

根据 student 用户配置，完成 student2 用户的配置，并将配置命令填写到表 5-3 中。

**表 5-3 student2 用户配置**

1. FTP 服务测试

①通过命令行测试

在虚拟化云主机中通过 ftp 命令进行 FTP 服务测试，其操作命令如下。

##本地登录 FTP 服务器

# ftp localhost ##输入用户名

Name (localhost:student):student ##提示信息

331 Please specifty the password Password：

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files. ##创建文件进行测试

ftp>mkdir /var/ftp/student\_root/test ##创建成功

257 "/var/ftp/student\_root/test " created ##退出登录

quit

##远程登录 FTP 服务器

ftp 172.16.2.100

##输入用户名

Name (localhost:student):student ##提示输入信息

331 Please specifty the password Password：

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files. ##删除目录进行测试

ftp>rm /var/ftp/student\_root/test ##删除目录成功

250 Remove directory operation successful

②通过客户端软件测试

在本地打开 Filezilla 客户端软件进行 FTP 服务测试，其操作过程如下所示。

* 登录测试。打开 Filezilla 客户端软件，在相应的栏目中输入主机地址、用户名、密码， 输入完成后点击【快速连接】进行登录测试，并将测试结果填写到表 5-3 中。

**表 5-3 student 用户登录测试**

* 上传文件测试。在本地文件中选择需要上传的文件，右击选择【上传】按钮，测试上传是否成功，若上传成功，可在 FTP 服务器中进行查看文件，并将测试结果填写到表 5-4 中。

**表 5-4 student 用户上传文件**

* 匿名用户测试。测试匿名用户是否能够登录 FTP 服务，在相应的栏目中输入主机地址、用户名、密码，输入完成后点击【快速连接】进行登录测试，并将测试结果填写到表 5

-5 中。

**表 5-5 匿名用户登录**

###### 6、基于 FTP 的文件共享服务系统

1. 场景

河南 XX 信息技术有限公司是一个 100 人以下的企业，该公司有 5 个部门，部门员工 F TP 服务权限信息如表 5-6 所示。

**表 5-6 河南 XX 信息技术有限公司员工 FTP 账户信息表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **部门** | **人员** | **职位** | **用户名** | **密码** |
| **市场拓展部** | 赵一 | 部门经理 | zhaoyi | zhaoyi@001 |
| 赵二 | 员工 | zhaodong | zhaodong@002 |
| 赵三 | 员工 | zhaosan | zhaosan@003 |
| 赵四 | 员工 | zhaosi | zhaosi@004 |
| 赵五 | 员工 | zhaowu | zhaowu@005 |
| 赵六 | 员工 | zhaoliu | zhaoliu@006 |
| 赵七 | 员工 | zhaoqi | zhaoqi@007 |
| 赵八 | 员工 | zhaoba | zhaoba@008 |
| 赵九 | 员工 | zhaojiu | zhaojiu@009 |
| 赵十 | 员工 | zhaoshi | zhaoshi@010 |
| **技术开发部** | 钱一 | 部门经理 | qianyi | qianyi@011 |
| 钱二 | 员工 | qiandong | qiandong@012 |
| 钱三 | 员工 | qiansan | qiansan@013 |
| 钱四 | 员工 | qiansi | qiansi@014 |
| 钱五 | 员工 | qianwu | qianwu@015 |
| 钱六 | 员工 | qianliu | qianliu@016 |
| 钱七 | 员工 | qianqi | qianqi@017 |
| 钱八 | 员工 | qianba | qianba@018 |
| 钱九 | 员工 | qianjiu | qianjiu@019 |
| 钱十 | 员工 | qianshi | qianshi@020 |
| 钱十一 | 员工 | qianshiyi | qianshiyi@021 |
| 钱十二 | 员工 | qianshidong | qianshidong@022 |
| 钱十三 | 员工 | qianshisan | qianshisan@023 |
| **人力资源部** | 孙一 | 部门经理 | sunyi | sunyi@024 |
| 孙二 | 员工 | sundong | sundong@025 |
| 孙三 | 员工 | sunsan | sunsan@026 |
| 孙四 | 员工 | sunsi | sunsi@027 |
| 孙五 | 员工 | sunwu | sunwu@028 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 孙六 | 员工 | sunliu | sunliu@029 |
| 孙七 | 员工 | sunqi | sunqi@030 |
| 孙八 | 员工 | sunba | sunba@031 |
| 孙九 | 员工 | sunjiu | sunjiu@032 |
| 孙十 | 员工 | sunshi | sunshi@033 |
| 孙十一 | 员工 | sunshiyi | sunshiyi@034 |
| 孙十二 | 员工 | sunshidong | sunshidong@035 |
| 孙十三 | 员工 | sunshisan | sunshisan@036 |
| 孙十四 | 员工 | sunshisi | sunshisi@037 |
| 孙十五 | 员工 | sunshiwu | sunshiwu@038 |
| 孙十六 | 员工 | sunshiliu | sunshiliu@039 |
| **后勤部** | 李一 | 部门经理 | liyi | liyi@040 |
| 李二 | 员工 | lidong | lidong@041 |
| 李三 | 员工 | lisan | lisan@042 |
| 李四 | 员工 | lisi | lisi@043 |
| 李五 | 员工 | liwu | liwu@044 |
| 李六 | 员工 | liliu | liliu@045 |
| 李七 | 员工 | liqi | liqi@046 |
| 李八 | 员工 | liba | liba@047 |
| 李九 | 员工 | lijiu | lijiu@048 |
| 李十 | 员工 | lishi | lishi@049 |
| 李十一 | 员工 | lishiyi | lishiyi@050 |
| 李十二 | 员工 | lishidong | lishidong@051 |
| 李十三 | 员工 | lishisan | lishisan@052 |
| 李十四 | 员工 | lishisi | lishisi@053 |
| 李十五 | 员工 | lishiwu | lishiwu@054 |
| **财务部** | 周一 | 部门经理 | zhouyi | zhouyi@055 |
| 周二 | 员工 | zhoudong | zhoudong@056 |
| 周三 | 员工 | zhousan | zhousan@057 |
| 周四 | 员工 | zhousi | zhousi@058 |
| 周五 | 员工 | zhouwu | zhouwu@059 |
| 周六 | 员工 | zhouliu | zhouliu@060 |
| 周七 | 员工 | zhouqi | zhouqi@061 |
| 周八 | 员工 | zhouba | zhouba@062 |
| 周九 | 员工 | zhoujiu | zhoujiu@063 |
| 周十 | 员工 | zhoushi | zhoushi@064 |
| 周十一 | 员工 | zhoushiyi | zhoushiyi@065 |
| 周十二 | 员工 | zhoushidong | zhoushidong@066 |
| 周十三 | 员工 | zhoushisan | zhoushisan@067 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 周十四 | 员工 | zhoushisi | zhoushisi@068 |
| 周十五 | 员工 | zhoushiwu | zhoushiwu@069 |
| 周十六 | 员工 | zhoushiliu | zhoushiliu@070 |

1. 资源服务要求

该公司 FTP 服务的资源要求具体如下所示。

①每个人有自己的私人文件存储空间；

②每个部门有部门内部的文件存储空间（由部门经理管理）；

③全公司有临时文件交换空间；

④全公司有资源共享空间（指定人员管理，所有人员可读）。

1. 配置实现

请根据场景以及资源服务要求，完成该公司 FTP 文件共享服务系统的部署。请将配置命令填写到表 5-7 中，并标注命令的含义与作用。

**表 5-7 FTP 文件服务器搭建**

##### 七、实验扩展

###### 1、文件服务器

1. 常见的文件服务器有哪些？分别使用了什么网络协议？
2. 不同的文件服务器分别有什么特点与优势？

###### 2、FTP 文件服务器

1. 在 Linux 上除了 vsftpd 还能使用哪些软件来搭建 FTP 服务器？
2. 在 Linux 上 FTP 常用的客户端软件有哪些？
3. 对于 FTP 上的文件如何进行备份才合理？

# 实验六：系统防火墙管理

##### 一、实验目的

1、理解 iptables 的工作原理；

2、掌握 iptables 防火墙的安装与配置；

3、掌握 iptables 防火墙的基本操作方法，能够熟练使用防火墙。

##### 二、实验学时

2 学时

##### 三、实验类型

综合性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装 VirtualBox 虚拟化软件，安装 Putty 管理终端软件，安装 Nm ap 工具软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

无。

##### 五、实验任务

1、完成 iptables 防火墙的安装与配置；

2、完成 iptables 防火墙规则的管理，满足实验的场景要求。

##### 六、实验内容及步骤

###### 1、iptables 的安装与管理

1. 防火墙检测

①关闭 firewall 防火墙

关闭CentOS 的 firewall 防火墙，并取消开机自动启动，其操作命令如下。

# systemctl stop firewalld

# systemctl disable firewalld

②检查 iptables 是否安装

一般情况下，iptables 已经包含在 Linux 系统中，可以通过命令来检测系统是否已经安装 iptables，具体命令如下，检测结果如图 6-1 所示则表示系统已经安装 iptables 防火墙。

# iptables --version



图 6-1 检测 iptables 是否安装

③检查是否安装 iptables-services

查看 iptables 服务是否安装，其命令如下所示。

# systemctl status iptables

若出现如图 6-2 所示的结果则说明 iptables 服务未安装，若出现如图 6-3 所示的结果则说明 iptables 服务已安装。

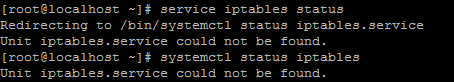


图 6-2 iptables service 未安装

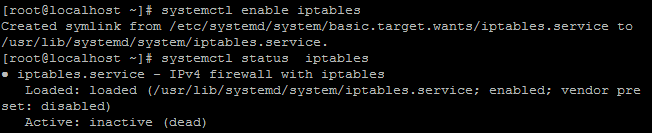


图 6-3 iptables service 已安装

1. 安装 iptables 软件

安装 iptables 以及 iptables services 服务软件，其操作命令如下所示。

# yum install -y iptables

# yum install –y iptables-services

1. iptables 服务配置

进行 iptables 服务管理，其操作命令如下所示。

##开启 iptables 服务

# systemctl start iptables ##设置开机自动启动

# systemctl enable iptables ##关闭 iptables 服务

# systemctl stop iptables ##重启 iptables 服务

# systemctl restart iptables ##取消开机自动启动

# systemctl disable iptables

###### 2、iptables 的基本配置

1. 规则的查看

使用一下命令进行防火墙规则查看，并将防火墙规则信息填写到表 6-1 中。

# iptables -n -L

**表 6-1 防火墙规则**

1. 规则的添加

①端口配置

* 开启需要的端口，如配置 TCP 协议的 22 端口允许进出系统，其配置命令如下。

# iptables -A INPUT -p tcp --dport 22 -j ACCEPT # iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

* 关闭不安全的端口，如配置不允许通过 TCP 协议的 445 端口进出系统，其配置命令如下所示。

# iptables -A INPUT -p tcp --dport 445 -j DROP # iptables -A OUTPUT -p tcp --sport 445 -j DROP

* 配置服务端口，如配置允许通过HTTP 访问系统的 80 端口，其配置命令如下。

# iptables -A INPUT -p tcp --dport http -j DROP

②IP 地址配置

* 拒绝某单一IP 地址，如拒绝某一单独IP 地址访问系统，且系统拒绝访问该IP 地址， 其配置命令如下。

# iptables -A INPUT -s xxx.xxx.xxx.xxx -j DROP

# iptables -A OUTPUT -d xxx.xxx.xxx.xxx -j DROP

* 拒绝某 IP 地址段，如拒绝某 IP 地址段中任一地址访问系统，且系统拒绝访问该 IP

地址段中任一 IP 地址，其配置命令如下。

# iptables -A INPUT -s xxx.xxx.xxx.xxx/xx -j DROP

# iptables -A OUTPUT -d xxx.xxx.xxx.xxx/xx -j DROP

③IP 地址与端口结合

* 拒绝某 IP 地址访问某端口，如拒绝某一单独 IP 地址访问系统的 22 端口（TCP 协议），其配置命令如下。

# iptables -A INPUT -s xxx.xxx.xxx.xxx -p tcp --dport 22 -j DROP

* 允许某段 IP 地址访问系统的服务端口，如允许某段 IP 地址访问系统的 HTTP 服务端口，其配置命令如下。

# iptables -A INPUT -s xxx.xxx.xxx.xxx/xx -p tcp --dport http -j ACC EPT

④网络协议配置

配置拒绝 ICMP 协议通过，如配置拒绝网络中通过 PING 方式发现系统 IP 地址，其配

置命令如下。

# iptables -A INPUT -p icmp -j DROP

⑤网卡接口配置

iptables 防火墙可单独为某个网卡接口设定不同的策略规则，如不允许任何主机通过防火墙本机的 eth0 网卡访问系统的 80 端口，其配置命令如下。

# iptables -A INPUT -i eth0 -p tcp --dport 80 -j DROP

⑥MAC 地址配置

* 拒绝某 MAC 地址主机的所有通信请求访问，其配置命令如下。

# iptables -A INPUT -m mac --mac-source XX:XX:XX:XX:XX:XX -j DR OP

* 拒绝网络中某一固定 IP 地址且固定 MAC 地址的主机访问系统任意端口，其配置命令如下。

# iptables -A INPUT -s xxx.xxx.xxx.xxx/x -m mac --mac-source XX:X X:XX:XX:XX:XX -j DROP

* 允许网络中某一固定 IP 地址且固定MAC 地址的主机访问系统的 22 号端口，其配置命令如下。

# iptables -A INPUT -p tcp --dport 22 -s xxx.xxx.xxx.xxx/x -m mac -

-mac-source XX:XX:XX:XX:XX:XX -j ACCEPT

1. 规则的测试

①软件获取

获取端口扫描工具 Zenmap 软件可通过本课程网站（[http://linux.xg.hactcm.edu.cn](http://linux.xg.hactcm.edu.cn/)）下载获得，也可通过 Zenmap 官方网站（[https://nmap.org/zenmap](https://nmap.org/zenmap/)）下载获得，如图 6-4 所示。本实验所使用的 Zenmap 软件为 nmap-7.60-setup.exe。



图 6-4 Zenmap 官网

②软件安装

点击下载的 EXE 执行安装文件，可根据安装过程提示进行默认选择安装。

③软件使用

打开工具，展示如图 6-2 所示工具界面。在“配置”下拉框中选择“Regular scan”（使用规则扫描），在“命令”输入框输入“nmap –p 1-1024 -T4 –A -v 172.16.124.127”命令规则，点击【扫描】按钮，工具将自动扫描 IP 地址为“172.16.124.127”的主机，其 1-1024 端

口的状态情况。

④信息查看

在“Nmap 输出”选项卡中可查看扫描的过程，如图 6-2 所示，查看主机端口的状态信息，并将信息填写到表 6-2 中。通过该工具可测试防火墙规则配置是否正确且生效。

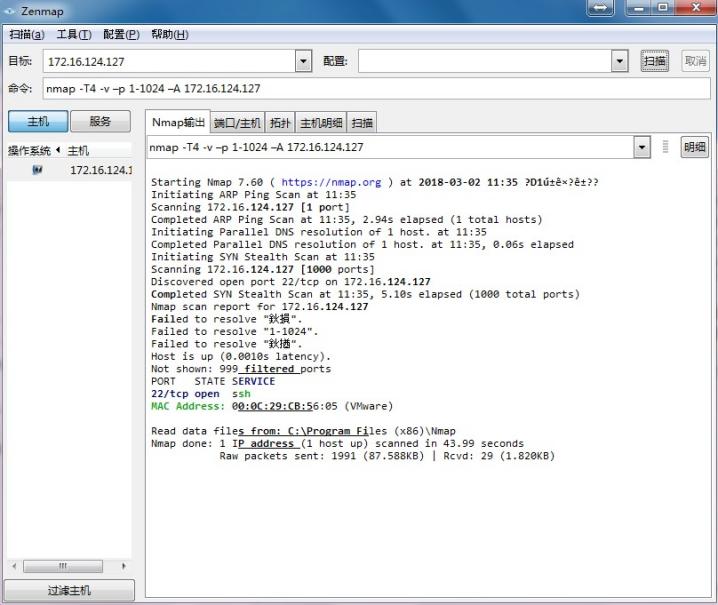


图 6-5 扫描结果

**表 6-2 端口检测结果**

###### 3、iptables 的应用

请根据下面的要求，写出防火墙的配置，将配置命令写入到实验报告册中。

①允许来自于 IP A 地址的报文，通过 UDP 方式，访问系统的 4486 端口。

②丢弃来至 IP B 地址的使用 TCP 方式，访问系统 20 和 21 端口的报文。

③允许 IP 地址属于 xxx.xxx.xxx.xxx/x 段的主机、由指定 eth0 网口，通过 SSH 远程连接本机。

④允许 IP 地址为 C 的主机通过 422 端口进行 SSH 远程连接本机。

⑤将来自 IP D 地址的主机使用 TCP 协议，访问 21 端口的数据包信息记录到 messages

日志中。

⑥当超过 100 个用户同时访问系统的 80 端口时，限制每分钟最大连接数为 25 个，防止系统遭受 DOS 攻击。

##### 七、实验扩展

###### 1、防火墙

1. 防火墙一共有几种？分别是什么，主要作用是什么？
2. iptables 防火墙是工作在计算机网络的哪一层上的？

###### 2、iptables 防火墙规则

1. iptables 防火墙规则除了可以通过配置端口、IP 地址，还能通过配置哪些选项来制定防火墙策略？请举例说明。
2. 如何将防火墙规则进行备份？

# 实验七：系统基本管理

##### 一、实验目的

1、掌握 Linux 系统中常用磁盘管理的命令以及操作方法；

2、掌握 Linux 系统中内存管理的命令及操作方法；

3、掌握 Linux 系统中用户和用户组管理的命令及操作方法。

##### 二、实验学时

2 学时

##### 三、实验类型

验证性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核 CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装VirtualBox 虚拟化软件，安装Putty 管理终端软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

无。

##### 五、实验任务

1、完成 Linux 磁盘管理命令的应用：fdisk、df；

2、完成 Linux 内存管理命令的应用：vmstat；

3、完成Linux 用户和用户组管理命令的应用：useradd、usermod、userdel、groupadd、

groupmod、groupdel。

##### 六、实验内容及步骤

###### 1、存储管理

1. 使用 fdisk 进行磁盘管理

①查看系统中磁盘详细信息，其配置命令如下所示，并将输出结果以及各参数表达的含义写入表 7-1。

# fdisk -l

**表 7-1 查看磁盘信息**

②创建分区

使用 VirtualBox 虚拟化软件为虚拟机添加 20GB 的虚拟磁盘/dev/sdb，使用该磁盘创建一个大小为 10GB 的主分区/dev/sdb1，其操作命令如下所示。

/dev/sdb1 2048 19533823 9765888 83 Linux ##保存分区配置操作

Command (m for help): w

The partition table has been altered!

Calling ioctl() to re-read partition table. Syncing disks.

End Blocks Id System

Start

Device Boot

# fdisk /dev/sdb ##创建新的扩展分区

Command (m for help): n

##输入 p 为创建主分区，输入 e 为创建扩展分区

Partition type:

p primary (0 primary, 0 extended, 4 free) e extended

Select (default p): p

##选择分区号，默认分区号为 1

Partition number (1-4, default 1): 1

First sector (2048-41943039, default 2048):2018 Using default value 2048

##设置分区大小

Last sector, +sectors or +size{K,M,G} (2048-41943039, default 41943 039): +10GB

##查看已经创建的分区信息Command (m for help): p

Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors Units = sectors of 1 \* 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes I/O size (minimum/optimal): 512 bytes / 512 bytes Disk label type: dos

Disk identifier: 0x689a8b25

参考主分区配置命令，完成第二个 10GB 的扩展分区的创建，并将配置过程写入表 7-

2。

**表 7-2 创建磁盘分区**

1. 使用df 进行磁盘管理

①查看所有磁盘信息，其配置命令如下所示，并将输出结果填写至表 7-2。

# df

**表 7-2 磁盘使用情况**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **Filesystem** | **1K-blocks** | **Used** | **Available** | **Use%** | **Mounted on** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |
| … | … | … | … | … | … | … |

②查看指定文件系统的磁盘使用情况，同时使用“Th”选项进行直观展示磁盘使用情况，其配置命令如下所示，并将输出结果填写至表 7-3。

# df –Th /home

**表 7-3 指定文件系统磁盘信息**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Filesystem** | **Type** | **Size** | **Used** | **Avail** | **Use%** | **Mounted on** |
|  |  |  |  |  |  |  |

1. 使用 vmstat 进行内存监控

本实验中使用的 CentOS 7 操作系统默认已安装 vmstat 命令工具，可直接进行使用。

①查看当前系统运行信息，其操作命令如下所示，并将输出结果填写至表 7-4。

# vmstat

**表 7-4 系统运行信息**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **procs** | | **memory** | | | | **swap** | | |
| **r** | **b** | **swpd** | **free** | **buff** | **cache** | **si** | | **so** |
|  |  |  |  |  |  |  | |  |
| **io** | | **system** | | **cpu** | | | | |
| **bi** | **bo** | **in** | **cs** | **us** | **sy** | **id** | **wa** | **st** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |

②设置以 2 秒为时间间隔的多次执行任务，连续收集 10 次性能数据，其操作命令如下所示。

# vmstat 2 10

1. 磁盘的挂载与移除

①磁盘挂载

创建/root/disk1 目录，并将已创建的/dev/sdb1 分区挂载到该目录下，通过 df 命令进行磁盘挂载检测，其配置命令如下所示，并将检查结果填写入表 7-5。

##创建挂载目录文件# mkdir /root/disk1

##将磁盘分区进行格式化# mkfs.ext4 /dev/sdb1

# mount /dev/sdb1 /root/disk1 # df –Th /root/disk1

②开机自动挂载

重启操作系统，查看硬盘分区是否仍能挂载到/root/disk1 目录下，如果不能，查找资料配置开机自动挂载磁盘分区，并将配置过程写入表 7-5。

**表 7-5 磁盘分区开机自动挂载**

③磁盘移除

使用 umount 命令移除硬盘分区，其操作命令如下所示，移除后查看磁盘信息，将输出结果写入表 7-。

# umount /dev/sdb1 # df

**表 7- 移除后磁盘信息**

###### 2、存储安全

1. 磁盘检查

使用 fsck 命令进行磁盘检查，其操作命令及其输出结果如下所示。

# fsck /dev/sdb1

fsck from util-linux 2.23.2 e2fsck 1.42.9 \(28-Dec-2013\)

/dev/sdb1: clean, 11/610800 files, 80342/2441472 blocks

阅读磁盘检查信息，将其中各参数的含义写入表 7-6。

**表 7-6 磁盘信息含义**

1. 使用RAID 1 提供存储安全性

提示：本实验的操作均在VirtualBox 虚拟化软件上进行。

①环境准备

虚拟机：通过VirtualBox 虚拟化软件创建一个 CentOS 7 操作系统的主机；

虚拟磁盘：给虚拟机配置 3 块 20GB 磁盘，第一块磁盘上为系统盘，另外 2 块磁盘配置 RAID 1。

软件：mdadm 工具，可直接使用yum 进行安装，其安装命令如下所示。

# yum install –y mdadm

②磁盘分区

基于 fdisk 磁盘管理命令，将磁盘/dev/sdb 中的主分区/dev/sdb1 修改其类型为“fd”（L inux RAID 自动识别类型），其操作流程如下所示。

# fdisk /dev/sdb Command (m for help): t Selected partition 1

Hex code (type L to list all codes):fd Command (m for help): w

参照/dev/sdb 磁盘配置命令，完成/dev/sdc 磁盘的分区创建以及分区类型修改配置，并将配置流程写入表 7-7。

**表 7-7 磁盘分区**

③创建 RAID 1 阵列

使用 mdadm 命令进行 RAID 1 磁盘阵列配置，输入以下命令创建RAID 1 阵列。

# mdadm -C /dev/md0 -ayes -l1 -n2 /dev/sd[b,c]1 mdadm: Note: this array has metadata at the start and

may not be suitable as a boot device. If you plan to store '/boot' on this device please ensure that

your boot-loader understands md/v1.x metadata, or use

--metadata=0.90

#确定创建磁盘阵列组，输入 y 继续进行操作

Continue creating array?y

mdadm: Defaulting to version 1.2 metadata

mdadm: array /dev/md0 started.

④查看磁盘阵列

查看 RAID 1 磁盘阵列的状态及其详细信息，将 RAID 参数信息以及各参数表示含义写入表 7-8。

##检查 RAID 状态信息

# cat cat /proc/mdstat

##查看 RAID 的详细参数信息

# mdadm -D /dev/md0

**表 7-8 RAID 1 参数信息**

⑤修改配置文件

●扫描系统中的全部阵列，其操作命令如下，将扫描结果进行复制，后续配置 RAID

需要用到。（扫描结果的UUID 根据硬盘不同而不同）

# mdadm --detail –scan

ARRAY /dev/md0 metadata=1.2 name=CentOS:0 UUID=6d8a4125:5d 60d903:57357ea5:cd3a2bdd

●添加 RAID 1 到RAID 配置文件/etc/mdadm.conf 中，其配置命令如下所示。

# vi /etc/ mdadm.conf

##在文件的末尾添加如下内容

DEVICE /dev/sdb1 /dev/sdc1

ARRAY /dev/md0 metadata=1.2 name=CentOS:0 UUID=6d8a4125:5d 60d903:57357ea5:cd3a2bdd

⑥阵列挂载

结合磁盘管理基本命令，完成以下要求配置，并将配置信息写入表 7-9。

●格式化磁盘阵列，将磁盘阵列格式化为 ext4 类型；

●创建/home/test 目录，并将 RAID 1 磁盘阵列挂载到该目录下；

●设置自动挂载，将 RAID 1 磁盘阵列设置开机自动挂载到/home/test 目录下。

**表 7-9 阵列挂载**

###### 3、用户管理

1. 用户管理

①添加新用户 user1，并配置用户主目录为：/home/user1，其配置命令如下所示。

# useradd -d /home/user1 -m user1

②设置用户 user1 密码为 test1pwd，其配置过程如下所示。

# passwd user1

Changing password for user user1. New password: test1pwd

Retype new password: test1pwd

passwd: all authentication tokens updated successfully.

③删除用户 user1，其配置命令如下所示。

# userdel user1

④结合用户管理基本命令，完成以下要求配置，并将配置命令填写到表 7-10 中。

●新建用户 user2，并设置其主目录为/home/dir2；

●自定义设置用户 user2 密码；

●修改用户主目录为/home/test。

**表 7-10 用户管理基本命令**

⑤结合用户管理基本命令，完成以下要求配置，并将配置过程写入表 7-11。

●完成使用 user2 用户登录系统；

* 在主目录下创建目录/dir1 和文件 file；
* 查看目录与文件属主信息。

**表 7-11 用户登录**

1. 用户组管理

①添加用户组 grouptest，其配置命令如下所示。

# groupadd grouptest

②结合用户组基本管理命令，完成添加新用户 user1 到 student 组中，设置该用户主目录为/home/user1 操作，并将配置流程写入表 7-12。

**表 7-12 用户添加**

③结合用户组基本管理命令，完成用户组 GID 修改操作，并将配置流程写入表 7-13。

**表 7-13 用户组配置**

④结合用户组基本管理命令，完成用户组grouptest 和student 用户组删除，并将配置流程写入表 7-14。

**表 7-14 用户组配置**

##### 七、实验扩展

###### 1、存储管理

1. 常用的提高存储安全性的方法有哪些？主要应用在哪些场景？
2. 常用的内存监控命令有哪些？请列举相应的性能指标。

###### 2、用户与用户组管理

1. 除了使用用户和用户组管理的命令可以进行用户管理外，有哪些进行用户管理的图形工具？
2. 是否可以通过直接编辑/etc/passwd、/etc/shadow、/etc/group、/etc/gshadow 文件的方式进行用户和用户组管理？

# 实验八：系统高级管理

##### 一、实验目的

1、掌握 Linux 系统中文件和目录权限管理的命令及操作方法；

2、掌握 Linux 系统中用户和用户组权限管理的命令及操作方法；

3、掌握 Linux 系统中进程管理的命令及操作方法。

##### 二、实验学时

2 学时

##### 三、实验类型

创新性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装VirtualBox 虚拟化软件，安装Putty 管理终端软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

无。

##### 五、实验任务

1、完成 Linux 权限管理命令的应用：chmod、chown、chgrp；

2、完成 Linux 进程管理命令的应用：ps、kill、killall；

3、完成 Linux 任务计划命令的应用：at、crontab。

##### 六、实验内容及步骤

###### 1、权限管理

提示：本实验的操作均以超级用户 root 权限进行。

1. 文件和目录的权限管理

①切换至 root 用户，并查看 umask 参数，其操作命令如下，将输出结果写入表 8-1。

# sudo su # umask

②在/home 目录下创建新目录 dir1，查看并记录 dir1 的详细信息，其操作命令如下，并将输出结果写入表 8-1.

# mkdir dir1 # ls -l

③改变 umask 参数为 066，并在/home 目录下创建新目录 dir2，查看并记录 dir2 的详细信息，比较 dir1 和dir2 目录权限不同，将不同信息填写到表 8-1 中。

# umask 066 # mkdir dir2 # ls -l

**表 8-1 dir1 和dir2 目录比较**

④结合权限管理基本命令，完成以下要求配置，并将操作流程写入表 8-2。

●创建文件 file1，查看 file1 权限信息；

●改变文件 file1 的权限为 755，查看文件 file1 权限信息。

**表 8-2 文件权限管理**

1. 属主和属组管理

①新建用户组 demogroup。

# groupadd demogroup

②新建用户 demo1、demo2、demo3，同属于用户组 demogroup。分别修改用户口令为demo1pwd、demo2pwd、demo3pwd，其操作命令如下所示。

# useradd -g demogroup demo1 # useradd -g demogroup demo2 # useradd -g demogroup demo3 # passwd demo1

# passwd demo2 # passwd demo3

③创建目录/var/ftpshare，查看目录权限，制定目录权限为 777，其操作命令如下所示。

# mkdir /var/ftpshare # ls -l

# chmod 777 /var/ftpshare

④使用用户 demo1、demo2、demo3 登录系统，并访问目录/var/ftpshare，进行权限测试，并将测试结果填写至表 8-3。

**表 8-3 测试访问权限**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **用户名称** | **能否登录系统** | **能否访问到**  **/var/ftpshare** | **能否执行 ls 命令** | **能够执行 touch**  **命令** | **能否执行 mkdir**  **命令** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| demo1 |  |  |  |  |  |
| demo2 |  |  |  |  |  |
| demo3 |  |  |  |  |  |

⑤修改 ftpshare 目录的属主为 demo1，属组为 demogroup，其操作命令如下所示。

# chown demo1 /var/ftpshare

# chgrp demogroup /var/ftpshare

⑥使用用户 demo1、demo2、demo3 登录系统，并访问目录/var/ftpshare，进行权限测试，并将测试结果填写至表 8-4。

**表 8-4 测试访问权限**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **用户名称** | **能否登录系统** | **能否访问到**  **/var/ftpshare** | **能否执行 ls 命令** | **能够执行 touch**  **命令** | **能否执行 mkdir**  **命令** |
| demo1 |  |  |  |  |  |
| demo2 |  |  |  |  |  |
| demo3 |  |  |  |  |  |

1. 系统权限管理

结合权限管理的命令，完成以下要求配置，并将操作流程写入表 8-5。

①在当前系统中创建目录/var/www/fileshare；

②在当前系统中创建用户manageuser、student1、student2、student3、student4；

③用户 manageuser 能够对/var/www/fileshare 进行读写操作；

④用户 student1、student2、student3、student4 能够进行读操作，不能够执行写操作；

⑤用户 manageuser 在创建文件和目录时，用户 student1、student2、student3、student4

能够自动获得新创建目录和文件的读权限。

**表 8-5 系统权限管理**

###### 2、进程管理

1. 进程信息查看

①查看当前系统信息或查看指定用户的信息，其操作命令如下。

# w

# w root

②使用 ps aux 命令可查看系统所有程序进程或者也可查看指定程序的进程信息，其操作命令如下。

##实现分页查看进程信息# ps aux | more

##查看 SSH 进程相关信息

# ps aux | grep sshd

根据进程信息，选择其中一条进程信息进行分析，并将分析结果填写至表 8-6。

**表 8-6 ps aux 命令结果解读**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **USER** | **PID** | **%CPU** | **%MEM** | **VSZ** | **RSS** | **TTY** | **STAT** | **START** | **TIME** |
|  |  |  |  |  |  |  |  |  |  |
| **COMMAND** |  | | | | | | | | |
| **信息描述** |  | | | | | | | | |

②使用 ps lax 命令可查看系统中进程的父进程 ID 和进程优先级信息，其操作命令如下。

##实现分页查看进程相关信息# ps lax | more

##查看 SSH 进程相关信息

# ps lax | grep sshd

根据进程信息，选择其中一条进程信息进行分析，并将分析结果填写至表 8-7。

**表 8-7 ps lax 命令结果解读**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **F** | **UID** | **PID** | **PPID** | **PRI** | **NI** | **VSZ** | **RSS** | **WCHAN** | **STAT** | **TTY** | **TIME** |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **COMMA**  **ND** |  | | | | | | | | | | |
| **信息描述** |  | | | | | | | | | | |

②使用 lsof 命令查看占用文件的进程信息，其操作命令如下。

##查看所有文件的进程信息# lsof

##查看占用指定文件目录的进程和用户# lsof /proc/

根据进程信息，选择其中一条进程信息进行分析，并将分析结果填写至表 8-8。

**表 8-8 lsof 命令结果解读**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **COMMADN** | **PID** | **TID** | **USER** | **FD** | **TYPE** | **DEVICE** | **SIZE/OFF** | **WCHAN** | **NODE** |
|  |  |  |  |  |  |  |  |  |  |
| **NAME** |  | | | | | | | | |

|  |  |
| --- | --- |
|  |  |
| **信息描述** |  |

1. 进程管理

①kill 命令

kill 命令是通过进程 ID 终止进程，其操作命令如下所示。

##安装 ntp 服务

# yum install –y ntp ##ntp 服务启动

# systemctl start ntpd

##查看 ntp 服务进程 ID 为 2424（根据查询结果获得进程 ID） # ps aux | grep ntpd

##根据进程号终止进程（根据查询结果进行终止进程 ID） # kill 2424

##查看进程是否存在

# ps aux | grep ntpd

②killall 命令

killall 命令是通过匹配进程名称终止进程，但 CentOS 7 的部分版本中，没有默认安装

killall 命令，可通过以下命令进行安装并终止相关进程，其操作命令如下所示。

#ntp 服务启动

# systemctl start ntpd ##查看 ntp 服务是否启动# ps aux | grep ntpd ##安装 killall 命令工具

# yum install –y psmisc ##终止 ntp 名称进程

# killall ntpd

##查看 ntp 服务是否终止

# ps aux | grep ntpd

1. 进程优先级

①nice 命令

nice 命令可以在启动程序时设置其谦让度，高谦让度意味着低优先级，谦让度的值应该在-20~+19 之间浮动。nice 命令修改的谦让度值是相对的，通过 nice 命令设置的谦让度值，其操作命令如下所示。

##设置优先级命令格式

# nice –n [谦让值] [指令或选项] ##设置命令优先级为-19

# nice –19 systemctl restart ntpd

②renice 命令

renice 命令可调整正在运行的进程的优先级信息，其操作命令如下所示。

##设置进程的优先级

# renice [谦让度绝对值] PID ##查看服务进程 ID 为 4798

# ps aux | grep ntpd ##将进程 ntp 优先级号+1 # renice +1 4798

###### 3、任务计划

1. 定时任务计划

①安装 at 命令工具

CentOS 7 系统部分版本中，没有默认安装 at 命令，可通过以下命令进行安装。

##安装 at 命令工具# yum install –y at ## 启动 at 服务

# systemctl start atd

②使用 at 命令，定时输出内容到文件中，其操作命令如下所示。

##现在开始 1 分钟后执行任务计划

# at now +1minutes

##输出 hello 到文本文件中

at> echo 'hello' > /root/temp.txt ##输入 crtl+D 完成编辑

at> <EOT>

通过 1 分钟可查看文件是否存在，文件内容是否为“hello”验证任务计划是否执行。

③使用 at 命令，定时启动服务，其操作命令如下所示。

##关闭 ntp 服务

# systemctl stop ntpd ##设置 1 分钟后的任务计划# at now +1minuts

##设置重启 ntp 服务的任务at> systemctl start ntpd ##输入 crtl+D 完成编辑at> <EOT>

##1 分钟后验证服务是否启动

# ps aux | grep ntpd

④删除未执行的定时任务计划，其操作命令如下所示。

##查看未执行的定时任务计划# atq

##未执行的任务计划列表

3 Fri Mar 2 10:12:00 2018 a root ##根据未执行任务计划 ID，删除任务计划

# atrm 3

⑤使用 at 命令，制定“下课后自动关闭系统”定时任务计划，并将配置流程填写至表

* 1. 。

**表 8-9 设置定时关机任务**

1. 周期性任务计划

①启动 crond 服务，其操作命令如下所示。

# systemctl start crond

②使用 crontab 命令，定时输出内容到指定文件中，其操作命令如下所示。

# crontab –e

##设置每分钟执行任务计划，输入 hello 到/root/temp2.txt 文件中

\*/1 \* \* \* \* echo 'hello' >> /root/temp2.txt

等待 3 分钟后，查看文件是否存在，且查看文件内容中是否包含 3 个“hello”，从而验证周期性任务计划是否执行成功。

③使用 crontab 命令，制定“每 10 分钟备份/root/temp2.txt 文件到/home 目录下”的周期任务计划，并将配置流程填写至表 8-10。

**表 8-10 设置周期任务**

1. 任务计划执行日志

查看任务计划执行日志，其配置命令如下所示。

# cat /var/log/cron

阅读日志信息，选择其中一条日志信息进行分析，并将分析结果写入表 8-11。

**表 8-11 任务计划执行日志解读**

##### 七、实验扩展

###### 1、umask、chmod、chown、chgrp

1. umask 命令的作用是什么？在进行文件权限管理时，可以提供哪些方便？
2. umask、chmod、chown、chgrp 的基本功能和常用参数有哪些？上述四个命令的应用场景和使用目的分别是什么？

###### 2、权限管理

1. 能否将不同的用户设置相同 UID？为什么？
2. 在 Linux 中，root 用户的 UID 为 0，通过直接修改/etc/passwd 文件将某一普通用户的UID 变更为 0 后，系统会发生什么？

###### 3、进程管理

1. 进程有哪些状态？这些状态所表示的含义是什么？
2. 进程和线程有什么关系？如何查看线程的信息？

# 实验九：系统运维管理

##### 一、实验目的

1、掌握 Linux 系统下常用的监控命令；

2、掌握 Shell 编程的基本语法；

3、掌握使用 Shell 编程实现系统运维的方法。

##### 二、实验学时

2 学时

##### 三、实验类型

创新性

##### 四、实验需求

###### 1、硬件

每人配备计算机 1 台，不低于双核CPU、8G 内存、500GB 硬盘。

###### 2、软件

Windows 操作系统，安装VirtualBox 虚拟化软件，安装Putty 管理终端软件。

###### 3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过NAT 方式访问互联网。

###### 4、工具

提供第三方 FTP 服务，虚拟主机能够访问该 FTP 服务。

##### 五、实验任务

1、完成 Linux 基本运维命令的应用：top、iotop、iftop、sar；

2、编写 Linux Shell 脚本，完成系统日志中用户登录过程分析；

3、编写 Linux Shell 脚本，完成系统指定目录的本地与远程定时数据备份。

4、编写 Linux Shell 脚本，完成批量化网站的创建与发布。

##### 六、实验内容及步骤

###### 1、使用监控命令进行系统监控

1. top

使用 top 命令查看系统运行状态，并分析系统进程变化。

# top

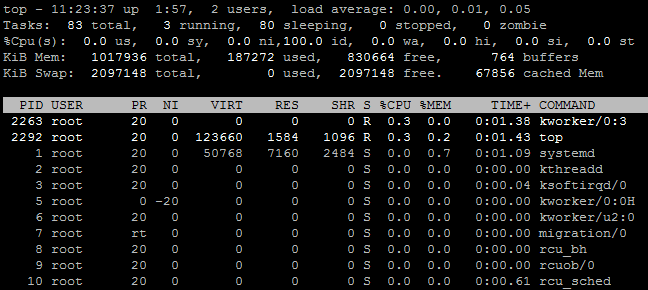


图 9-1 系统运行状态

请分析 top 命令下各字段的含义，并将结果写入表 9-1。

**表 9-1 top 命令含义**

1. iotop

①使用 yum 安装 iotop

# yum install iotop

②使用 iotop 查看磁盘 I/O 使用状况

# iotop

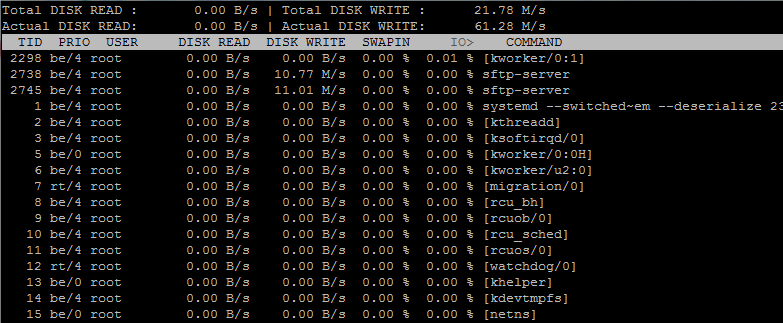


图 9-2 磁盘 I/O 使用状况

③使用 iotop -o 查看磁盘正在产生 I/O 的进程或线程

# iotop -o

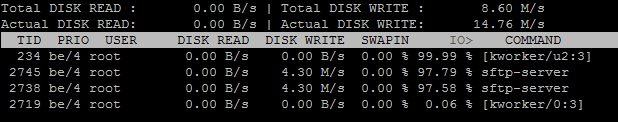


图 9-3 正在产生磁盘 I/O 的进程

请分析 iotop 命令下各字段的含义，并将结果写入表 9-2。

**表 9-2 iotop 命令含义**

1. iftop

①使用 yum 安装所需依赖包

# yum install flex byacc libpcap ncurses ncurses-devel libpcap-devel

②访问 iftop 官网，下载 iftop 安装包

[http://www.ex-parrot.com/~pdw/iftop/download/iftop-0.17.tar.gz](http://www.ex-parrot.com/%7Epdw/iftop/download/iftop-0.17.tar.gz)

③使用 FileZilla 上传 iftop 安装包至/home 目录

④使用 yum 安装 gcc-c++

#yum install gcc-c++

⑤解压 iftop-0.17.tar.gz，安装 iftop

#tar -xvzf /home/iftop-0.17.tar.gz #cd iftop-0.17

#./configure

#make && make install

⑥使用 iftop 查看接口流量

# iftop -i enp0s3

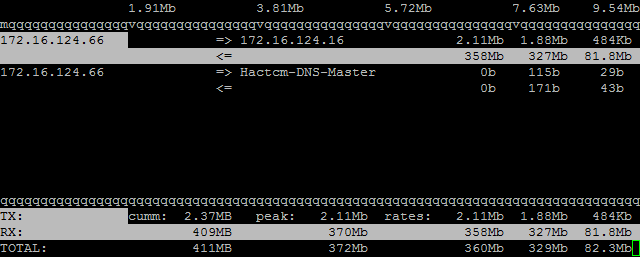


图 9-4 enp0s3 接口流量

1. sar

①使用 yum 安装 sar

#yum install sysstat

②使用 sar 查看 CPU 使用信息，每隔 1 秒，共输出 6 次

#sar -u 1 6

③使用 sar 查看 CPU 所有核心运行数据，每隔 1 秒，共输出 6 次

#sar -P ALL 1 6

④使用 sar 每隔 1 秒记录 CPU 的使用情况，直到 11 点 02 分，数据将保存到/opt/cpu.lo g 文件中

#sar 1 -u -e 11:02:00 > /opt/cpu.log

记录当前 CPU 的使用情况，将结果写入表 9-3，并分析各字段含义。

**表 9-3 cpu 使用情况**

⑤使用 sar 每隔 1 秒记录内存的使用情况，直到 11 点 02 分，数据将保存到/opt/memor y.log 文件中

#sar 1 -r -e 11:02:00 > /opt/memory.log

记录当前内存的使用情况，将结果写入表 9-4，并分析各字段含义。

**表 9-4 内存使用情况**

⑥使用 sar 每隔 1 秒记录网络的使用情况，直到 11 点 02 分，数据将保存到/opt/memor y.log 文件中。

#sar 1 -n DEV -e 11:02:00 > /opt/network.log

记录当前网络使用情况，并将结果写入表 9-5，并分析各字段含义。

**表 9-5 网络使用情况**

###### 2、使用 Shell 编写脚本进行系统维护

1. 编写Shell 脚本，查看系统用户登录日志

Centos 中记录登录信息的日志文件如下表所示。

**表 1-1 登录信息日志一览表**

|  |  |
| --- | --- |
| **登录日志类型** | **日志存储位置** |
| 当前正在登录系统的用户信息 | /var/run/utmp |
| 当前正在登录和历史登录系统的用户信息 | /var/log/wtmp |
| 最后一次登录的用户信息 | /var/log/btmp |

wtmp 和 utmp 文件是二进制文件，可使用 who、w、users、last 和 ac 来查看两个文件包含的信息。

编写 Shell 脚本，将用户登录历史信息导入到文本中。

#!/bin/bash logPath="/var/log/wtmp" savePath="/home"

\who ${logPath} >> ${savePath}/"userLogin.txt

1. 编写Shell 脚本，实现指定目录的定时备份

①日志获取

将/var/log/下的系统日志备份到临时目录，将该目录进行日志压缩和上传。

#!/bin/bash

##定义日志存放路径path="/var/log" zipPath="/home" ##创建临时文件夹

time=`date +%Y%m%d` mkdir ${zipPath}/${time}-"log"

\cp -r ${path}/\* ${zipPath}/${time}-"log"/

②日志压缩

将临时目录中日志进行压缩，压缩后删除临时目录文件，文件压缩使用“zip”命令。

①使用 yum 安装 zip。

#yum install zip

②临时目录压缩

zip -r ${time}-"log.zip" ${zipPath}/${time}-"log"/ ##删除原有的目录文件

rm -rf ${zipPath}/${time}-"log"/

③使用 yum 安装 ftp

#yum install ftp

④上传压缩文件

##将当天的日志文件进行上传ftp -n <<- EOF

open FTP 服务器 IP 地址user User Password bin

if ![ -f /${time} ] ;then mkdir /${time}

fi

cd ${time}

put ${time}-"log.zip" bye

EOF

⑤本地保存

##将文件移到本地文件夹下进行保存mv ${time}-"log.zip" ${path}/log

##判断本地 LOG 日志文件总个数，大于 15 时自动删除之前的文件

cd ${path}/log/

FileNum=$(ls -l | grep ^- | wc -l)

ReservedNum=15

while(( ${FileNum} > ${ReservedNum} )) do

##取最旧的文件，\*.\*可以改为指定文件类型OldFile=$(ls -rt \*.\* | head -1)

rm -f ${path}/log/${OldFile} let "FileNum--"

done

⑥日志清空

##清除本地存放日志的初始日志rm -rf ${path}/data/query/\*

##创建目录，目录名称可自定义设置mkdir –p ${path}/data/query

##创建日志文件，日志文件名称可自定义设置touch ${path}/data/query/名称.log

##将新创建的日志文件赋予权限chown -R named ${path}/data/

chgrp -R named ${path}/data/#取最旧的文件，\*.\*可以改为指定文件类型OldFile=$(ls -rt \*.\* | head -1)

rm -f ${path}/log/${OldFile} let "FileNum--"

done

⑦定时任务

通过 Linux 下定时任务定期执行 shell 脚本，以实现日志每天定时（每天晚上 23.59）保存备份，将定时任务写入/etc/crontab 文件下，其操作命令如下所示。

径/file.sh

/bin/bash 脚本存放路

root

\*

\*

# vi /etc/crontab

59 23 \*

将完整的 Shell 脚本写入表 9-6 中。

**表 9-6 定时任务 shell 脚本**

1. 编写Shell 脚本，实现网站创建

①Apache 安装

使用 yum 命令安装Apache 服务，并设置服务自动开机启动，其安装命令如下。

#yum install httpd #systemctl start httpd #systemctl enable httpd

②配置虚拟目录并引用

本次实验需发布 10000 个网站，每个网站需创建一个配置文件，将所有网站配置文件放入虚拟目录中，其操作命令如下。

# mkdir /etc/httpd/conf.d/vhost

创建虚拟目录完成后，需要在 Apache 的主配置文件中进行引用才能实现对每个网站的配置文件加载，其操作方法是在配置文件/etc/httpd/conf/httpd.conf 末尾添加如下命令。

IncludeOptional conf.d/vhost/\*.conf

③安全配置

关闭系统 SELinux 安全访问控制，本次实验通过 Alias 网站虚拟目录方法实现 10000 个网站的创建，默认使用 80 端口，所以修改防火墙配置运行 TCP/80 通过防火墙，其操作命令如下。

# vi /etc/selinux/config

##将 SELINUX=enforcing 改为 SELINUX=disabled SELINUX=disabled

##配置 SELinux 文件后，需重启操作系统

# reboot

##重启完成后修改防火墙规则

# firewall-cmd --zone=public --add-port=80/tcp --permanent # firewall-cmd --reload

③编写 Shell 脚本

* + - 编写 Shell 脚本，使用循环方法，创建 10000 个网站目录，并将每个网站下创建 1 个

index.html 首页，并将展示出“这是 shell 生成的第 XX 个网页”内容，其操作命令如下。

htmlPath="/var/www/html"

\rm -rf ${htmlPath}/\* for i in `seq 1 10000` do

websiteName="website"$i

\cd ${htmlPath}

\mkdir ${websiteName}

\chmod -R 777 ${websiteName}

echo "" > ${htmlPath}/${websiteName}/index.html

echo "<html><head><title>shell 生成 HTML 文件</title></head><bo dy>" >> ${htmlPath}/${websiteName}/index.html

echo "<h1>这是 shell 生成的第$i 个网页</h1>" >> ${htmlPath}/${web siteName}/index.html

echo "</body></html>" >> ${htmlPath}/${websiteName}/index.html done

* + - 编写 Shell 脚本，使用循环方法，为 10000 个网站创建虚拟配置文件，每个网站创建虚拟目录，并将配置文件放入在/etc/httpd/conf.d/vhost 虚拟目录中，其操作命令如下。

httpdConfdPath="/etc/httpd/conf.d/vhost"

\rm -rf ${httpdConfdPath}/\* for j in `seq 1 10000`

do

websiteConfName="websiteConf${portNum}".conf

echo "Alias /website$j ${htmlPath}/website$j" >> ${httpdConfdPat h}/${websiteConfName}

echo "<Directory \"${htmlPath}/website$j\">" >> ${httpdConfdPat h}/${websiteConfName}

echo "AllowOverride All" >> ${httpdConfdPath}/${websiteConfNam

e}

echo "Require all granted" >> ${httpdConfdPath}/${websiteConfN ame}

echo "</Directory>" >> ${httpdConfdPath}/${websiteConfName} done

④服务重启

网站和配置文件生成后，需重启 httpd 服务，其操作命令如下。

# systemctl restart httpd

⑤测试访问

在本地浏览器中可输入网站地址：[http://IP](http://IP/) 地址/website9999（访问为第 9999 个网站， 虚拟目录名称为 website+第N 个网站），验证网站是否创建成功，并将结果填写至表 9-7 中。

**表 9-7 网站访问测试**

##### 七、实验扩展

###### 1、系统监控

1. 除了上述列举的监控命令，还有哪些监控命令？其主要功能是什么？
2. 常用的系统监控软件有哪些？并简要说出其主要特点。
3. 除了编写 Shell 脚本进行系统运维外，还有哪些系统自动化运维工具？并简要说出其主要特点。

###### 2、Shell

1. Shell 是否有数据类型？能否可将字符型数据转换为整型数据？
2. Shell 中常见的数据结构有哪些？
3. Shell 脚本是否可以编译、封装、加密？
4. Shell 脚本程序如何进行知识产权保护？

###### 3、自动化运维

1. 假如有 1000 台 Linux 服务器，如何进行高效率的系统升级？

# 实验十：Windows2016 DNS HTTP管理

# 1、使用Windows2016 搭建DNS;

# 2、域名解析type=A，新建主机记录nnlgw+学号.net.cn 如nnlgw20030001.net.cn

# 3、主站域名：www.nnlgw20030001.net.cn

# 4、在HTTP服务器实现WordPress搭建，主站域名绑定到该台HTTP服务器。

# 5、开启系统防火墙，只允许53、80、3306、3389端口放行。

# 6、完成相关配置后使用御剑端口开放截图。