还原三台虚拟机classroom server desktop

[root@server0 ~]# rht-vmctl reset classroom

[root@server0 ~]# rht-vmctl reset server

[root@server0 ~]# rht-vmctl reset desktop

确认虚拟机server Yum是否可用

[root@server0 ~]# yum clean all

[root@server0 ~]# yum repolist

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

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

案例4：编写一个判断脚本

在server0 上创建/root/foo.sh 脚本

1）当运行/root/foo.sh redhat，输出为fedora

2）当运行/root/foo.sh fedora，输出为redhat

3）当没有任何参数或者参数不是redhat或者fedora时，

其错误输出产生以下信息：/root/foo.sh redhat|fedora

[root@server0 ~]# vim /root/foo.sh

#!/bin/bash

if [ $# -eq 0 ];then #判断是否输入参数

echo '/root/foo.sh redhat|fedora' >&2 #修改为错误输出

exit 3 #脚本退出返回值为3

elif [ $1 == redhat ];then

echo fedora

elif [ $1 == fedora ];then

echo redhat

else

echo '/root/foo.sh redhat|fedora' >&2 #修改为错误输出

exit 4 #脚本退出返回值为4

fi

[root@server0 ~]# /root/foo.sh redhat

[root@server0 ~]# /root/foo.sh fedora

[root@server0 ~]# /root/foo.sh abc

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

案例5:编写一个批量添加用户脚本

在 server0 上创建 /root/batchusers 脚本

1)此脚本要求提供用户名列表文件作为参数

[root@server0 ~]# vim /root/userlist

duanwu

zhongqiu

zhsan

lisi

[root@server0 ~]# vim /root/batchusers

#!/bin/bash

for i in `cat $1`

do

useradd $i

echo $i成功

done

[root@server0 ~]# /root/batchusers /root/userlist

)如果没有提供参数,此脚本应该给出

提示 Usage: /root/batchusers,退出并返回相应值

3)如果提供一个不存在的文件,此脚本应该给出提

示 Input file not found,退出并返回相应值

4)新用户的登录Shell为 /bin/false,无需设置密码

[root@server0 ~]# vim /root/batchusers

#!/bin/bash

if [ $# -eq 0 ];then

echo 'Usage: /root/batchusers' >&2

exit 1

elif [ -f $1 ];then

for i in `cat $1`

do

useradd -s /bin/false $i #指定登陆的Shell解释器

echo $i成功

done

else

echo 'Input file not found' >&2

exit 2

fi

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

系统安全保护

SELinux安全机制

SELinux运行模式的切换

• SELinux的运行模式

– enforcing(强制)、permissive(宽松)

– disabled(彻底禁用)

修改为 disabled(彻底禁用)状态，必须需要通过重起系统

• 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

1. 临时修改SELinux状态为permissive(宽松)

[root@server0 ~]# getenforce #查看当前SELinux状态

Enforcing

[root@server0 ~]# setenforce 0 #设置当前SELinux状态为宽松

[root@server0 ~]# getenforce

Permissive

2.修改固定配置:/etc/selinux/config 文件 #每次开机状态文件

SELINUX=permissive

虚拟机desktop0

1.临时修改SELinux状态为permissive(宽松)

[root@desktop0 ~]# getenforce

Enforcing

[root@desktop0 ~]# setenforce 0

[root@desktop0 ~]# getenforce

Permissive

2.修改固定配置: vim/etc/selinux/config 文件

SELINUX=permissive(宽松)

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

配置用户环境,永久别名的定义

• 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'

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

alias nsd='echo hello world'

关闭终端，从新开启一个终端进行远程管理gos

root用户可以执行hello与nsd

student用户可以执行hi与nsd

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

防火墙策略管理

搭建Web服务

服务端:虚拟机Server0

1.安装可以提供Web服务软件

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

2.重起httpd服务

[root@server0 /]# systemctl restart httpd #重起服务

[root@server0 /]# systemctl enable httpd #设置开机自启动

ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-user.target.wants/httpd.service'

3.测试：

[root@server0 /]# firefox 172.25.0.11

4.书写一个页面文件

默认存放网页文件的路径:/var/www/html

默认网页文件的命令: index.html

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

<marquee><font color=red><h1>NSD1804万岁 阳关明媚

滚动 字体颜色 最大字体

[root@server0 /]# firefox 172.25.0.11

搭建FTP服务

1.安装一个可以提供FTP功能的软件

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

2.重起vsftpd服务，设置为开机自起

[root@server0 /]# systemctl restart vsftpd

[root@server0 /]# systemctl enable vsftpd

ln -s '/usr/lib/systemd/system/vsftpd.service' '/etc/systemd/system/multi-user.target.wants/vsftpd.service'

3.测试：

默认FTP共享路径：/var/ftp

[root@server0 /]# firefox ftp://172.25.0.11

默认可以看到pub目录

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

RHEL7防火墙：

隔离作用：过滤所有的入站请求，允许出站

硬件防火墙

软件防火墙：firewalld

• 管理工具:firewall-cmd、firewall-config

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

• 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sshd、dhcp、ping服务

– trusted:允许任何访问

– block:阻塞任何来访请求，明确回绝

– drop:丢弃任何来访的数据包，直接丢弃不给回应，最节省资源

防火墙的判定：匹配及停止

1.防火墙会查看请求中的源IP地址，再查询本防火墙所有区域中，那一个区域有该源IP地址的规则，则进入该区域

2.进入默认区域（public）

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

默认区域的修改

虚拟机Server0

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

虚拟机desktop0

# ping -c 2 172.25.0.11 #可以ping通

虚拟机Server0

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

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

虚拟机desktop0

# ping -c 2 172.25.0.11 #不可以ping通，有回应

虚拟机Server0

# firewall-cmd --set-default-zone=drop #修改默认区域为drop

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

虚拟机desktop0

# ping -c 2 172.25.0.11 #不可以ping通，无回应

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

服务的添加

虚拟机Server0

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

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

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

虚拟机desktop0

# firefox 172.25.0.11 #无法访问

# firefox ftp://172.25.0.11 #无法访问

虚拟机Server0

# firewall-cmd --zone=public --add-service=http #添加可以访问的协议

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

虚拟机desktop0

# firefox 172.25.0.11 #访问成功

# firefox ftp://172.25.0.11 #无法访问

虚拟机Server0

# firewall-cmd --zone=public --add-service=ftp #添加可以访问的协议

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

虚拟机desktop0

# firefox 172.25.0.11 #访问成功

# firefox ftp://172.25.0.11 #访问成功

服务协议：

http:超文本传输协议 默认的端口：80

https：安全的超文本传输协议 默认的端口：443

ftp:文件传输协议 默认的端口：21

tftp：简单的文件传输协议 默认的端口：69

telnet：远程管理协议 默认的端口：23

DNS：域名解析协议 默认的端口：53

smtp：用户发邮件协议 默认的端口：25

pop3：用户收邮件协议 默认的端口：110

snmp：网络管理协议 默认的端口：161

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

防火墙策略的永久设置

– 永久(permanent)

虚拟机Server0

# 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

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

# firewall-cmd --reload #重新加载防火墙所有配置

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

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

源IP地址的添加

虚拟机Server0

# firewall-cmd --zone=block --add-source=172.25.0.10

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

虚拟机desktop0

# firefox 172.25.0.11 #不可以访问

# ping 172.25.0.11 #不可以访问

真机：

# firefox 172.25.0.11 #可以访问

# ping 172.25.0.11 #可以访问

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

防火墙设置方式：

严格：默认区域设置为drop区域,允许的放入trusted区域

宽松：默认区域设置为trusted区域，拒绝的单独放入drop区域

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

防火墙的端口转发：

端口：利用编号，标识一个服务或程序

客户端访问172.25.0.11:5423服务端将其请求转发给本地的80端口

虚拟机Server0

[root@server0 ~]# firewall-cmd --reload

虚拟机desktop0

[root@desktop0 ~]# firefox 172.25.0.11:5423

虚拟机Server0

# 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desktop0

[root@desktop0 ~]# firefox 172.25.0.11:5423

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

配置IPv6地址

IPv4地址：32个二进制 用 点 分隔4个部分 4个进制数表示

IPv6地址：128个二进制 用 冒号 分隔 8个部分 每部分化成4个16进制数

虚拟机server0:

[root@server0 ~]# nmcli connection modify 'System eth0' ipv6.method manual ipv6.addresses 2003:ac18::305/64 connection.autoconnect yes

# nmcli connection up 'System eth0'

# ping6 2003:ac18::305

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