NSD Study

2018-04

达内IT培训集团

案例练习,准备:

rht-vmctl reset classroom

rht-vmctl reset server

rht-vmctl reset desktop

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

案例1:为虚拟机 server0 配置以下静态地址参数，实现永久设置

– 主机名:server0.example.com

– IP地址:172.25.0.11

– 子网掩码:255.255.255.0

– 默认网关:172.25.0.254

– DNS服务器:172.25.254.254

案例2:为虚拟机 desktop0 配置以下静态地址参数，实现永久设置

– 主机名:desktop0.example.com

– IP地址:172.25.0.10

– 子网掩码:255.255.255.0

– 默认网关:172.25.0.254

– DNS服务器:172.25.254.254

案例3:指定yum软件源

为 server0 指定可用的 yum 软件源

– YUM软件库的地址为 http://classroom.example.com/content/rhel7.0/x86\_64/dvd

– 将此配置为虚拟机 server0 的默认软件仓库

– 确认可用的仓库列表

– 利用yum仓库安装httpd与vsftpd

案例4:指定yum软件源

为 desktop0 指定可用的 yum 软件源

– YUM软件库的地址为 http://classroom.example.com/content/rhel7.0/x86\_64/dvd

– 将此配置为虚拟机 server0 的默认软件仓库

– 确认可用的仓库列表

– 利用yum仓库安装httpd与vsftpd

案例5：虚拟机 server0上操作，复制、粘贴、移动

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

[root@server0 ~]# mkdir /nsddir

[root@server0 ~]# touch /nsddir/readme.txt

1）将“I love Linux”写入到文件readme.txt

[root@server0 ~]# echo ‘I love Linux’ > /nsddir/readme.txt

2）将readme.txt重命名为mylove.txt

[root@server0 ~]# mv /nsddir/readme.txt /nsddir/mylove.txt

3）将/etc/passwd、/boot、/etc/group同时拷贝到/nsddir目录下

[root@server0 ~]# cp -r /etc/passwd /boot /etc/group /nsddir

4）将ifconfig命令的前两行内容，追加写入mylove.txt

[root@server0 ~]# ifconfig | head -2 >> /nsddir/mylove.txt

5）将主机名永久配置文件，拷贝到/nsddir目录下

[root@server0 ~]# cp /etc/hostname /nsddir

6）将DNS永久配置文件，拷贝到/nsddir目录下

[root@server0 ~]# cp /etc/resolv.conf /nsddir

7）新建目录结构/nsd/test

[root@server0 ~]# mkdir -p /nsd/test

8）在目录/nsd/test创建文件nsd.txt并写入内容 NSD Student

[root@server0 ~]# echo ‘NSD Student’ > /nsd/test/nsd.txt

9）将/nsd/test/nsd.txt文件复制到/root目录下，同时 改名为 tedu.txt

[root@server0 ~]# cp /nsd/test/nsd.txt /root/tedu.txt

10）利用vim 修改文件/etc/hostname将其原有内容全部删除，写入新的内容为server0.example.com

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

命令模式dG

插入模式 server0.example.com

:wq 保存退出

11）将/etc/passwd 、/etc/resolv.conf、/etc/hostname 同时拷贝到/nsd/test/目录下

[root@server0 ~]# cp /etc/passwd /etc/resolv.conf /etc/hostname /nsd/test

12）将文件 /nsd/test/hostname 重改名为 hn.txt

[root@server0 ~]# mv /nsd/test/hostname /nsd/test/hn.txt

13）创建目录结构/nsd/test/kernel

[root@server0 ~]# mkdir /nsd/test/kernel

案例6:虚拟机 server0上操作，查找并处理文件

– 创建目录 /root/findfiles/

[root@server0 ~]# mkdir /root/findfiles

– 利用find查找所有用户 student 拥有的文件,把它们拷贝到 /root/findfiles/ 文件夹中

[root@server0 ~]# find / -user student -type f -exec cp {} /root/findfiles \;

– 利用find查找/boot目录下大于10M并且必须是文件，拷贝到/opt

[root@server0 ~]# find /boot -size +10M -type f -exec cp {} /opt \;

– 利用find查找/boot/ 目录下以 vm 开头且必须是文件，拷贝到/opt

[root@server0 ~]# find /boot -name “vm\*” -type f -exec cp {} /opt \;

案例7:虚拟机 server0上操作,查找并提取文件内容

1.在文件 /usr/share/dict/words 中查找到所有包含字符串 seismic 的行,将输出信息,写入到/opt/nsd.txt

[root@server0 ~]# grep seismic /usr/share/dict/words > /opt/nsd.txt

2.将/etc/login.defs文件有效内容 写入到/root/login.txt

[root@server0 ~]# grep -v ^# /etc/login.defs | grep -v ^$ > /root/login.txt

3.提取/etc/passwd以bash结尾的行，将其信息写入/opt/system.txt

[root@server0 ~]# grep bash$ /etc/passwd > /opt/system.txt

案例8:虚拟机 server0上操作,tar制作/释放归档压缩包（zcf、ztf、zxf、jcf、jtf、jxf、cf、tf）

1）备份/boot、/home这两个文件夹，保存为boothome.tar.gz文件

[root@server0 ~]# tar -zcf boothome.tar.gz /boot /home

2）查看boothome.tar.gz文件内包含哪些内容

[root@server0 ~]# tar -tf boothome.tar.gz

3）将boothome.tar.gz释放到文件夹/root/boothome/下

( [root@server0 ~]# mkdir /root/boothome )

[root@server0 ~]# tar -xf boothome.tar.gz -C /root/boothome

4）创建一个名为 /root/backup.tar.bz2 的归档文件，其中包含 /usr/local 目录中的内容

[root@server0 ~]# tar -jcf /root/backup.tar.bz2 /usr/local

案例9:虚拟机 server0上操作

新建用户 tom，其用户ID为1234，密码是abcdef

[root@server0 ~]# useradd -u 1234 tom

[root@server0 ~]# echo abcdef | passwd --stdin tom

创建下列用户、组以及组的成员关系：

– 一个名为 stugrp 的组

[root@server0 ~]# groupadd stugrp

– 一个名为 natasha 的用户，其属于 stugrp 组， 这个组是该用户的从属组

[root@server0 ~]# useradd -g stugrp natasha

– 一个名为 harry 的用户，其属于 stugrp 组，这个 组是该用户的附加组

[root@server0 ~]# useradd -G stugrp harry

– 一个名为 sarah 的用户，其在系统中没有可交互的 Shell（/sbin/nologin），并且不是 adminuser 组的成员

[root@server0 ~]# useradd -s /sbin/nologin sarah

问题 – natasha 、harry、sarah 的密码都要设置为 pass123

[root@server0 ~]# echo pass123 | passwd --stdin natasha

[root@server0 ~]# echo pass123 | passwd --stdin harry

[root@server0 ~]# echo pass123 | passwd --stdin sarah

案例10:虚拟机 server0上操作

为用户 natasha 配置一个定时任务

– 每天在本地时间 14:23 执行

– 需要完成的任务操作为 /bin/echo hiya

[root@server0 ~]# crontab -e -u natasha

23 14 \* \* \* /bin/echo hiya

案例11:虚拟机 server0上操作

将文件 /etc/fstab 拷贝为 /var/tmp/fstab，并调整文件 /var/tmp/fstab权限

[root@server0 ~]# cp /etc/fstab /var/tmp/fstab

满足以下要求：

– 此文件的拥有者是 root

– 此文件属于 root 组

– 此文件对任何人都不可执行

– 用户 natasha 能够对此文件执行读和写操作

[root@server0 ~]# chown root:root /var/tmp/fstab

[root@server0 ~]# chmod o-x /var/tmp/fstab

[root@server0 ~]# setfacl -m u:natasha:rw /var/tmp/fstab

– 用户 harry 对此文件既不能读，也不能写

[root@server0 ~]# setfacl -m u:harry:- /var/tmp/fstab

– 所有其他用户（当前的和将来的）能够对此文件进行 读操作

[root@server0 ~]# chmod o+r /var/tmp/fstab

案例12:虚拟机 server0上操作

创建一个共用目录 /home/admins，要求如下：

[root@server0 ~]# mkdir /home/admins

– 此目录的组所有权是 adminuser

[root@server0 ~]# chown :adminuser /home/admins

– adminuser 组的成员对此目录有读写和执行的权限，除此以外的其他所有用户没有任何权限

[root@server0 ~]# chmod g=rx,o= /home/admins

– root用户能够访问系统中的所有文件和目录

– 在此目录中创建的文件，其组的所有权会自动设置为 属于 adminuser 组

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

案例13：虚拟机 server0上操作,绑定到LDAP验证服务

– 使用系统 classroom.example.com 提供的LDAP服务

– 验证服务的基本DN是：dc=example,dc=com

– 账户信息和验证信息都是由 LDAP 提供的

– 连接要使用证书加密，证书可以在下面的链接下载：

http://classroom.example.com/pub/example-ca.crt

– 确认本地可以识别ldapuser10用户

1.安装一个客户端sssd软件,与LDAP 服务端沟通

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

2.安装authconfig-gtk 图形的工具 配置sssd软件

[root@server0 ~]# yum -y install authconfig-gtk

3.运行authconfig-gtk 图形的工具

[root@server0 ~]# authconfig-gtk

4.重起客户端服务sssd服务，设置开机自启动

[root@server0 ~]# systemctl restart sssd

5.验证

[root@server0 ~]# id ldapuser0

案例14：虚拟机 server0上操作,访问NFS共享

– 查看classroom.example.com的NFS共享

– 将classroom.example.com的NFS共享目录，挂载到本地/home/guests

1.查看共享classroom.example.com

[root@server0 ~]# showmount -e classroom.example.com

2.访问共享内容,将服务端的共享文件夹数据，挂载到本地/home/guests以本地的/home/guests作为访问点

[root@server0 ~]# mkdir /home/guests

[root@server0 ~]# mount classroom.example.com:/home/guests /home/guests

案例15:虚拟机 server0上操作,（GPT分区模式）规划分区

关闭虚拟机，图形添加一块60G的硬盘并规划分区：

划分4个10G的主分区；

1个12G的主分区

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

mktable gpt

mkpart

案例16:在server上操作,分区使用

1、案例15中新添加60G硬盘的第一个主分区

– 格式化成xfs分区，实现该分区开机自动挂载/mnt/xpart

[root@server0 ~]# mkfs.xfs /dev/vdc1

[root@server0 ~]# echo /dev/vdc1 /mnt/xpart xfs defaults 0 0 >> /etc/fstab

2、案例15中新添加60G硬盘的第二个主分区

– 完成开机自动挂载，挂载点/mnt/mypart,文件系统为ext4

[root@server0 ~]# mkfs.ext4 /dev/vdc2

[root@server0 ~]# echo /dev/vdc2 /mnt/mypart ext4 defaults 0 0 >> /etc/fstab

案例17:虚拟机 server0操作，构建 LVM 存储

– 新建一个名为 systemvg 的卷组

[root@server0 ~]# vgcreate systemvg /dev/vdc3

– 在此卷组中创建一个名为 vo 的逻辑卷，大小为8G

[root@server0 ~]# lvcreate -n vo -L 8G systemvg

– 将逻辑卷 vo 格式化为 xfs 文件系统

[root@server0 ~]# mkfs.xfs /dev/systemvg/vo

– 将逻辑卷 vo 挂载到 /vo 目录，并在此目录下建立一个测试文件 votest.txt，内容为“I AM KING”

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

[root@server0 ~]# echo I AM KING > /vo/votest.txt

– 实现逻辑卷vo开机自动挂载到/vo

[root@server0 ~]# echo /dev/systemvg/vo /vo xfs defaults 0 0 >> /etc/fstab

案例18:虚拟机 server0操作，构建 LVM 存储(修改PE大小)

– 在 datastore 卷组中的所有逻辑卷，其PE的大小为1M

– 新的逻辑卷命名为 database，其大小为50个PE的大小，属于 datastore 卷组

– 使用 EXT3 文件系统对逻辑卷 database 格式化，此逻辑卷应该在开机时自动挂载到 /mnt/database 目录

[root@server0 ~]# vgcreate -s 1M datastore /dev/vdc4

[root@server0 ~]# lvcreate -n database -l 50 datastore

[root@server0 ~]# mkfs.ext3 database

[root@server0 ~]# echo /dev/datastore/database /mnt/database ext3 defaults 0 0 >> /etc/fstab

案例19:在在 server0、desktop0 上操作

– 将防火墙默认区域设置为trusted

[root@server0 ~]# firewall-cmd --set-default-zone=trusted

案例21:在server上操作，搭建mariadb数据库系统（安装软件，启动服务即可）

1. 在 server0 上安装 MariaDB 数据库系统

1)安装 mariadb-server软件包

2)启动 mariadb 服务

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

[root@server0 ~]# mysql

案例22：配置聚合连接

在两个虚拟机之间配置一个链路，要求如下：

– 此链路使用接口 eth1 和 eth2

– 此链路在其中一个接口失效时仍然能工作

– 此链路在 server0 上使用下面的地址 172.16.3.20/255.255.255.0

– 此链路在 desktop0 上使用下面的地址 172.16.3.25/255.255.255.0

– 此链路在系统重启之后依然保持正常状态

**1.制作虚拟网卡 team0, 参考 man teamd.conf 全文查找/example 按n跳转匹配项**

[root@server0 ~]#

2. 为 team0添加成员

[root@server0 ~]#

3.配置team0的ip地址与激活

[root@server0 ~]#

案例23:配置Samba文件夹共享，防火墙默认区域设置为trusted，修改SElinux状态为Enforcing

在 server0 上发布共享文件夹

1）此服务器必须是 STAFF 工作组的一个成员

2）发布目录 /devops，共享名为 devops

5）用户 harry 对共享 devops可读可写，密码是 123

6）用户 kenji 对共享 devops可读，密码是 123

1.安装软件包:samba

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

2.建立Samba共享帐号

[root@server0 ~]# useradd -s /sbin/nologin harry

[root@server0 ~]# pdbedit -a harry

123

3.修改Samb服务配置

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

workgroup = STAFF

[devops]

path = /devops

write list = harry

4.重起smb服务，设置开机自起

[root@server0 ~]# systemctl restart smb

5. SELinux设置布尔值（功能的开关）

– 需要加 -P 选项才能实现永久设置

[root@server0 ~]# setsebool samba\_export\_all\_rw on

6.修改本地权限

[root@server0 ~]# chmod o+w /devops

在 desktop0 上访问共享文件夹

1）访问 server0 上发布共享文件夹,实现开机自动挂载到/mnt/smb

2）实现对/mnt/smb目录可以读和写

1 创建挂载点

[root@server0 ~]# mkdir /mnt/nsd

2 所需软件包:cifs-utils

[root@server0 ~]# yum -y install cifs-utils

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

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

案例25：普通NFS共享的实现

– 在 server0 上配置NFS服务

1）只读的方式共享目录 /public，只能被172.25.0.0/24网段中的客户机系统访问

– 在 desktop0 上访问NFS共享目录

1）将 server0 的 /public 挂到本地 /mnt/nfsmount

2）这些文件系统在系统启动时自动挂

虚拟机Server0

[root@server0 ~]# yum -y install nfs-utils

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

/public \*(ro)

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

问题

虚拟机Desktop0

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

172.25.0.11:/public /mnt/nfsmount nfs defaults,\_netdev 0 0

案例26:在在 server0、desktop0 上操作

– 将防火墙默认区域设置为trusted

[root@server0 ~]# firewall-cmd --set-default-zone=trusted

案例27:为虚拟机 server 配置Web服务，实现网站的部署

- 实现客户端访问172.25.0.11网页内容为 环太平洋之雷霆再起

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

#echo 环太平洋之雷霆再起 > /var/www/html/index.html

#systemctl restart httpd

案例20:在server上操作,验证端口转发策略

– 从desktop0上访问server0的5423端口，与访问server0的80端口效果一样

虚拟机Server0

[root@server0 ~]# firewall-cmd --zone=trusted --add-forward-port=port=5423:proto=tcp:toport=80

案例28:在server上操作，配置一个数据库

– 为mariadb数据库root设置登陆密码为 haxi

– 新建一个数据库名为 nsd

– 除了 root 用户,此数据库只能被用户 lisi 查询,此用户的密码为 123(用户的授权)

– 数据库 nsd 中应该包含来自数据库复制的内容,

复制文件的 URL为:http://classroom/pub/materials/users.sql

[root@server0 ~]# mysqladmin -u root password ‘haxi’

>create database nsd;

>grant select on nsd.\* to lisi@localhost identified by ‘123’;

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

[root@server0 ~]# mysql -u root -phaxi nsd < users.sql

案例29:在server上操作，使用数据库查询

1)密码是 solicitous 的人的名字?

2)有多少人的姓名是 Barbara 同时居住在 Sunnyvale?

[root@server0 ~]# select \* from base where password=’solicitous’;

案例30：发布iSCSI网络磁盘

1）配置 server0 提供 iSCSI 服务，要求如下：

2）磁盘名为iqn.2016-02.com.example:server0

3）服务端口为 3260

4）使用 iscsi\_store（后端存储的名称） 作其后端卷，其大小为 3GiiB

5）此磁盘服务只能被 desktop0.example.com 访问，在Server0上配置客户端ACL为iqn.2016-02.com.example:desktop0

6）配置 desktop0 使用 server0 提供 iSCSI 服务

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

# yum -y install targetcli

# targetcli

>/backstores/block create name=iscsi\_store dev=/dev/vdb1

>iscsi/ create iqn.2018-09.com.example:server0

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

>iscsi/iqn.2018-09.com.example:server0/tpg1/acls create iqn.2018-09.com.example:desktop0

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

#systemcl resetart target

客户端：

#yum -y install iscsi-initiator-utils

#vim /etc/iscsi/initiatorname.iscsi

...........................................desktop0

#systemctl restart iscsid

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

#systemctl restart iscsi

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

案例练习,准备:

rht-vmctl reset classroom

rht-vmctl reset server

rht-vmctl reset desktop

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

案例1:为虚拟机 server 配置

- 实现三个网站的部署

- 实现客户端访问server0.example.com网页内容为 test01

- 实现客户端访问www0.example.com网页内容为 test02

- 实现客户端访问webapp0.example.com网页内容为 test03

[root@server0 ~]# firewall-cmd --set-default-zone=trusted

# mkdir /var/www/test01 /var/www/test02 /var/www/test03

# echo test01 > /var/www/test01

............................................

# vim /etc/httpd/conf.d/xuniweb.conf

<VirtualHost \*:80>

ServerName server0.example.com

DocumentRoot /var/www/test01

</VirtualHost>

......................................................

# systemctl restart httpd

案例2:为虚拟机 server 配置Web访问控制

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）在server0.example.com的DocumentRoot目录下，private的子目录里书写网页文件index.html内容为 test04

2）此页面只能在本机浏览，但是从其他系统不能访问这个目录的内容

[root@server0 ~]# cat /etc/httpd/conf.d/xuniweb.conf

# mkdir /var/www/test01/private

# echo test04 > /var/www/test01/private/index.html

# vim /etc/httpd/conf.d/qx.conf

<Directory “/var/www/test01/private”>

Require ip 172.25.0.11

</Directory>

# systemctl restart httpd

案例3:为虚拟机 server 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

2）确保站点 http://server0.example.com 仍然可访问

[root@server0 ~]# mkdir /webroot

# echo asdlfslkfjl > /webroot/index.html

# vim /etc/httpd/conf.d/xuniweb.conf

<VirtualHost \*:80>

ServerName server0.example.com

DocumentRoot /webroot

</VirtualHost>

# vim /etc/httpd/conf.d/qx.conf

<Directory /webroot>

Require all granted

</Directory>

# systemctl restart httpd

# ls -Zd /var/www

# ls -Zd /webroot

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

案例4：为虚拟机 server 部署动态WSGI站点

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

1）此虚拟主机侦听在端口8909

2）测试网页从以下地址下载，不要作任何更改http://classroom/pub/materials/webinfo.wsgi

3）从浏览器访问 http://webapp0.example.com:8909 可接收到动态生成的 Web 页面

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

# cat /etc/httpd/conf.d/xuniweb.conf

# cd /var/www/test03

# wget http://classroom/pub/materials/webinfo.wsgi

# vim /etc/httpd/conf.d/xuniweb.conf

Listen 8909

<VirtualHost \*:8909>

ServerName webapp0.example.com

DocumentRoot /var/www/test03

WsgiScriptAlias / /var/www/test03/webinfo.wsgi

</VirtualHost>

# vim /etc/httpd/conf.d/qx.conf

<Directory /var/www/test03/webinfo.wsgi>

Require all granted

</Directory>

# systemctl restart httpd

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

案例5：配置安全Web服务

为站点 http://server0.example.com 配置TLS加密

1）一个已签名证书从以下地址获取 http://classroom/pub/tls/certs/server0.crt

2）此证书的密钥从以下地址获取 http://classroom/pub/tls/private/server0.key

3）此证书的签名授权信息从以下地址获取 http://classroom/pub/example-ca.crt

[root@server0 ~]# cd /etc/pki/tls/certs

# wget <http://classroom/pub/tls/certs/server0.crt>

# wget <http://classroom/pub/example-ca.crt>

# cd /etc/pli/tls/private

# wget <http://classroom/pub/tls/private/server0.key>

# yum -y install mod\_ssl

# vim /etc/httpd/conf.d/ssl.conf

DocumentRoot “/var/www/html”

ServerName www0.example.com:443

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

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

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

# echo dfjalskdfj > /var/www/html/index.html

# systemctl restart httpd

# firefox <https://www0.example.com>

我已了解可能的风险——>确认安全例外