第五课 用户管理和软件安装

FTP

DHCP

DNS

HTTP

安装VMware Tools，可以方便的直接在windows主机和内部虚机之间进行文字以及文件的复制粘贴

mount /dev/cdrom /media/cdrom 挂载光驱

umount /media/cdrom 卸载光驱

点击VMware workstation的虚拟机选项，然后选择安装VMware tools

mount /dev/cdrom /media/cdrom 挂载光驱

ls /media/cdrom 里面应该能看到以VMware开头的文件，现在版本的VMware基本上都不提供rpm软件包只提供源码包

tar xf /media/cdrom/VMwareTool\* -C /usr/src 解压源码包文件至/usr/src目录下

cd /usr/src/vmware-tools-distrib 切换至解压目录下

./vmware-install.pl 一切默认值即可

reboot 重启加载vmware-tools

可以直接和真机进行文本包括文件的复制粘贴了，而且可以自动适应全屏

FTP

* vsftpd软件包
  + 官方站点:http://vsftpd.beasts.org/
  + 主程序：/usr/sbin/vsftpd
  + 服务名：vsftpd
  + 用户列表文件
    - /etc/vsftpd/ftpusers
    - /etc/vsftpd/user\_list
  + 主配置文件
    - /etc/vsftpd/vsftpd.conf

光驱每次重启不会自动挂载，如果希望自动挂载，下节课将分区会讲到

mount /dev/cdrom /media/cdrom 手动mount光驱

yum install vsftpd -y 使用yum安装vsftpd软件，vsftpd就是ftp服务器

rpm -q vsftpd 或

yum info vsftpd 查看软件包是否已安装

centos中ftp服务器默认支持用户认证方式：

匿名：任何人都可以连接，不需要用户和密码，安全性最差，默认就是支持匿名登录

本地：用户通过useradd创建用户，通过passwd设置密码，建议这些用户shell是非交互式

虚拟：用户是假的，系统中不存在，可以将用户放在系统的文本文件中，或者写入到系统的数据库中，这类安全性最高

启动vsftpd服务，默认支持本地和匿名登录

service vsftpd start 手动开启ftp服务

chkconfig vsftpd on 保证每次开机有效

service iptables stop 停止防火墙，如果不停止防火墙需要修改iptables配置

chkconfig iptables off 保证防火墙都是关闭

在7的系统中，启动和关闭服务的命令

systemctl start vsftpd.services 手动启动

systemctl enable vsftpd 开机启动

systemctl stop vsftpd 手动关闭

systemctl disable vsftpd 开启关闭

yum install ftp -y 安装ftp客户端命令，客户端做，服务器安装不安装无所谓

客户端测试

ftp 服务器ip地址 匿名用户可以使用ftp用户，密码随便输入

ftp>ls 查看文件，FTP匿名用户默认会将/var/ftp目录作为匿名用户目录

如果希望用户密码登录，首先需要服务器创建用户和密码

useradd -s /sbin/nologin ftpuser1 建议所有的ftp用户默认都写成不允许本地登录（使用参数-s /sbin/nologin）

passwd ftpuser1 设置用户密码

setenforce 0 临时关闭SELinux，默认是开启，开启状态下本地用户无法查看

vim /etc/sysconfig/selinux 修改SELinux配置文件，可以永久有效

SELINUX=permissive 修改这一项

SELinux会为每个文件打标签，每个服务会有默认允许的标签类型，客户访问本地的ftp服务器，首先防火墙要过滤客户来源进行访问控制，当可以访问本地的ftp以后，SELinux会为ftp打开哪些标签的文件允许通过ftp协议让客户访问，调节SELinux方法可以修改文件的标签（修改上下文），第二种让服务支持更多的标签（修改布尔值）

[root@www ~]# setsebool -P ftp\_home\_dir on 开放布尔值

[root@www ~]# getsebool -a | grep ftp 查看布尔值

客户端测试

ftp 服务器ip地址 输入服务器提供的用户和密码，默认连接的用户的宿主目录

默认vsftpd允许匿名和本地用户登录，禁用匿名用户

vim /etc/vsftpd/vsftpd.conf

anonymous\_enable=NO 默认是yes改为no

service vsftpd restart 重启服务

客户端再次访问服务器做认证，发现ftp用户不可用，ftpuser1用户仍然可以连接

DHCP服务器，分配IP地址给主机，要求DHCP服务器自身必须是静态IP，一个网络内一般只有一台DHCP，如果有多台则客户端可能获取的地址会不同，实验环境下，虚拟机网卡必须设置成vmnet，千万不要桥接（可能会导致网络中断），可以设置vmnet2等，不建议设置vmnet1或vmnet8（这俩网络默认VMware开放DHCP，如果希望设置这俩网络建议关闭VMware的DHCP功能）

setup 设置静态IP地址，随意配置，vmnet都是独立

service network restart 重启网络服务

ifconfig 验证网络设置

yum install -y dhcp 安装DHCP服务器

vim /etc/dhcpd/dhcpd.conf dhcp服务器的主配置文件，这个文件没有任何有效配置信息，全为注释的内容

subnet 192.168.10.0 netmask 255.255.255.0 { 声明自己的网络信息，就是网络号

range 192.168.10.100 192.168.10.200; 分配地址的范围

option routers 192.168.10.1; 分配的网关地址

option domain-name "test.com"; 分配默认域名信息

option domain-name-servers 192.168.10.1,8.8.8.8; 分配的DNS服务器地址

}

service dhcpd start

chkconfig dhcpd on

如果启动dhcpd服务失败，可以通过日志文件帮助troubleshooting

cat /var/log/messages 一般都有^附近，上面会提示多少行大概什么错误

DNS服务器，域名解析，将域名解析为IP（正向解析），或者将IP解析为域名（反向解析）

yum install bind bind-chroot -y

bind软件是DNS服务器的主服务，必须安装，提供域名解析

bind-chroot软件是可选，可装可不装，建议安装，为了提高DNS服务器的安全性，当安装了chroot软件包后，启动服务器将会使用named用户之前使用root，如果安装chroot后，配置文件将会发生变化，域名主配置文件之前是/etc/named.conf，安装后将是/var/named/chroot/etc/named.conf，区域文件之前是/var/named目录下，安装后将会读取/var/named/chroot/var/named目录，在5的系统时候需要自己来修改指定文件，6不需要，6系统中，当启动带有chroot的dns服务器的时候将会自动把配置文件和区域文件挂载至/var/named/chroot下相应的目录下，在6系统中，安装chroot后配置文件可以和安装前一样用，mout命令可以查看到挂载信息

vim /etc/named.conf 修改DNS主配置文件

配置内容修改：

1）listen-on port 53 { 127.0.0.1; }; 默认只侦听本地地址，其他主机无法访问DNS服务，可以写自己的某个IP，多个IP可以使用,分隔，如果所有IP可以使用any，建议使用any

2）allow-query { localhost; }; 允许查询，建议改为any

3）include "/etc/named.rfc1912.zones"; include代表包含，后面的文件是配置文件的补充，自定义配置写在主配置文件是可以的，写在include后面的文件也一样生效，它会加载完自己的配置后，再加载include后面的文件。Include有助于配置文件模块化。

写入正向查找区域配置，可以写在主配置文件中，也可以写入include文件中

zone "test.com" IN { 解析的区域名为test.com

type master; 定义为主区域，需要自己写区域文件

file "test.com.zone"; 区域文件的名字

};

zone "10.168.192.in-addr.arpa" IN { 写入反向解析记录，当查询192.168.10.0/24网段查找下面记录

type master; 定义为主区域

file "192.168.10.zone"; 定义区域文件

};

写入反向查找区域

**制作区域文件，复制建议使用-a选项可以保留源文件的拥有者和拥有组，否则会启动不了**

[root@www ~]# cp -a /var/named/named.empty /var/named/test.com.zone

[root@www ~]# cp -a /var/named/named.empty /var/named/192.168.10.zone

vim /var/named/test.com.zone

$TTL 3H

@ IN SOA www.test.com. rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS www.test.com.

IN MX 5 mail.test.com. 定义MX记录（邮件交换）

www IN A 192.168.10.1 定义www.test.com的A（Address）记录

mail IN A 192.168.10.10 定义mail.test.com

web IN CNAME www 定义别名

vim /etc/named/192.168.10.zone

$TTL 3H

@ IN SOA www.test.com. rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS www.test.com.

1 IN PTR www.test.com. 定义反向记录查询192.168.10.1解析为www.test.com

10 IN PTR mail.test.com. 反向192.168.10.10解析为mail.test.com

service named restart

chkconfig named on

[root@www ~]# nslookup

> server

Default server: 192.168.10.1

Address: 192.168.10.1#53

> www.test.com

Server: 192.168.10.1

Address: 192.168.10.1#53

Name: www.test.com

Address: 192.168.10.1

> 192.168.10.1

Server: 192.168.10.1

Address: 192.168.10.1#53

1.10.168.192.in-addr.arpa name = www.test.com.

> mail.test.com

Server: 192.168.10.1

Address: 192.168.10.1#53

Name: mail.test.com

Address: 192.168.10.10

> web.test.com

Server: 192.168.10.1

Address: 192.168.10.1#53

web.test.com canonical name = www.test.com.

Name: www.test.com

Address: 192.168.10.1

> abc.test.com

> set type=mx

> test.com

Server: 192.168.10.1

Address: 192.168.10.1#53

test.com mail exchanger = 5 mail.test.com.