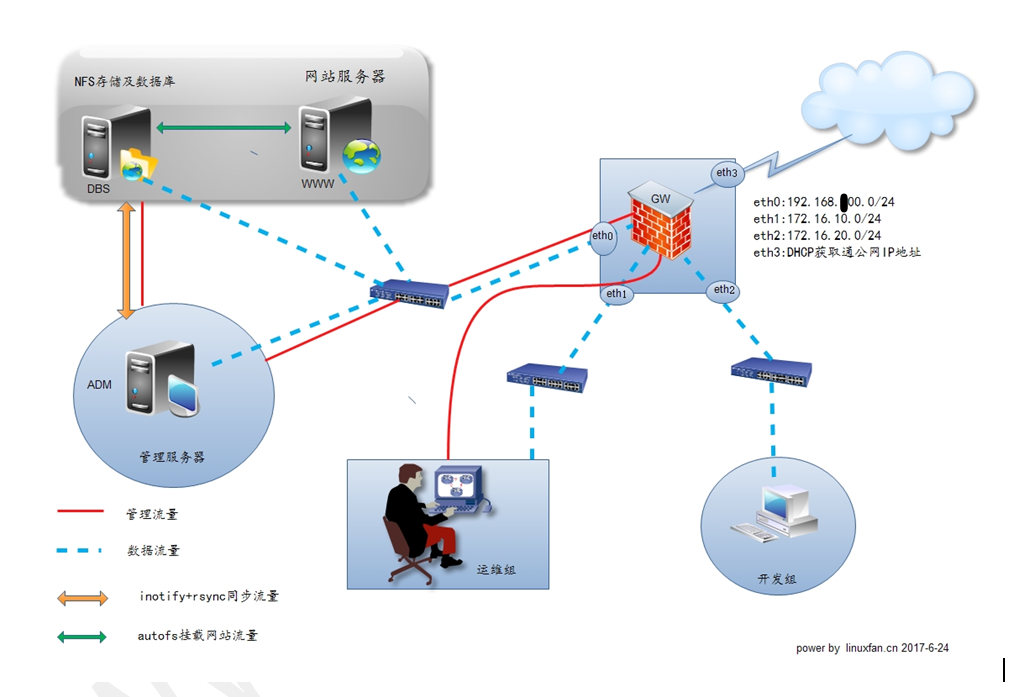
|  |
| --- |
| www.linuxfan.cn科技有限公司 |
| 项目：www.linuxfan.cn公司内部网络架构 |
| 版本：1-1 |

|  |
| --- |
| 作者：www.linuxfan.cn  2018-8-19 |

项目：www.linuxfan.cn公司内部网络架构

一、项目拓扑：



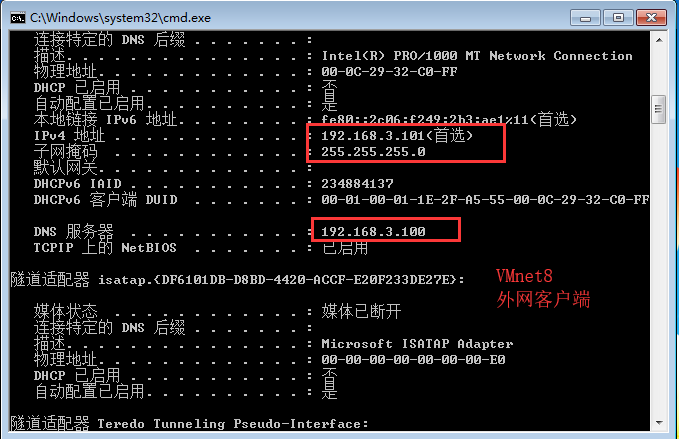
二、项目重点：

三、项目环境：

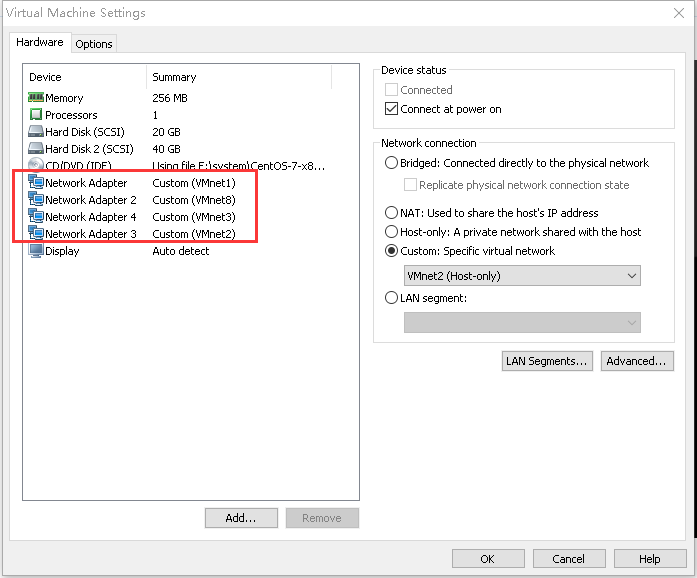
|  |  |  |  |
| --- | --- | --- | --- |
| 系统类型 | IP地址 | 主机名 | 所需软件 |
| Centos 6.5 64Bit | vm1：192.168.100.100/24  vm8：192.168.3.100/24  gw：192.168.3.88/24  vm2：172.16.10.100/16  vm3：172.15.10.100/16 | gw.linuxfan.cn | iptables、dhcp中继、 |
| Centos 7.4 1708 64bit | vm1：192.168.100.101/24  gw：192.168.100.100/24  DNS：192.168.100.101 | admin.linuxfan.cn | cobbler、vsftpd、dhcp、DNS、rsync、inotify、 |
| Centos 7.4 1708 64bit | vm1：192.168.100.102/24  gw：192.168.100.100/24  DNS：192.168.100.101 | st.linuxfan.cn | nfs-utils、rpcbind |
| Centos 7.4 1708 64bit | vm1：192.168.100.103/24  gw：192.168.100.100/24  DNS：192.168.100.101 | nginx.linuxfan.cn | nfs-utils、  nginx-1.12.2.tar.gz |
| Centos 7.4 1708 64bit | vm1：192.168.100.104/24  gw：192.168.100.100/24  DNS：192.168.100.101 | tm1.linuxfan.cn | nfs-utils、  jdk-8u171-linux-x64.tar.gz  apache-tomcat-9.0.10.tar.  gz、 |
| Centos 7.4 1708 64bit | vm1：192.168.100.105/24  gw：192.168.100.100/24  DNS：192.168.100.101 | tm2.linuxfan.cn | nfs-utils、  jdk-8u171-linux-x64.tar.gz  apache-tomcat-9.0.10.tar.  gz、 |
| Win7-1 | vm2：172.16.10.101/16  （自动获取）  gw：172.16.10.100/16  DNS：192.168.100.101 | Win7-1 | 内网运维人员 |
| Win7-2 | vm3：172.15.10.101/16  （自动获取）  gw：172.15.10.100/16  DNS：192.168.100.101 | Win7-2 | 内网开发人员 |
| Win7-3 | vm8：192.168.3.101/24  gw：无  DNS：192.168.3.100 | Win7-3 | 外网客户端 |

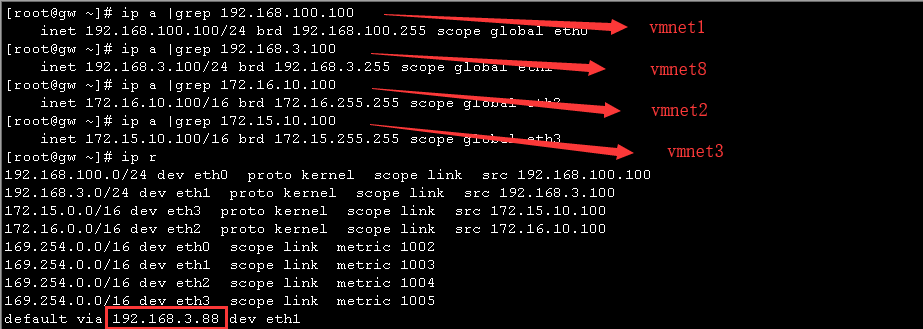
四、项目实施步骤：

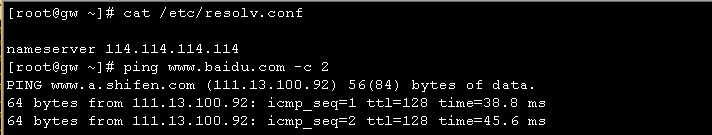
* **开启外网测试的win7客户端；**
* **配置网关服务器的网络参数及内网上网参数；**
* **配置内网管理服务器的网络参数及搭建dhcp、vsftpd、DNS、cobbler服务（略）；**
* **在网关服务器配置DHCP中继；**
* **开启内网运维组主机，测试自动获取的网络参数；**
* **开启内网开发组主机，测试自动获取的网络参数；**
* **搭建服务器组内的NFS服务；**
* **配置管理主机的ftp目录与NFS的共享目录进行实时同步；**
* **搭建服务器组内的Nginx服务并配置NFS挂载；**
* **搭建服务器组内的Tomcat服务并配置NFS挂载（两台Tomcat节点配置相同，在此列出一台）；**
* **搭建服务器组内的Mariadb数据库服务；**
* **内网开发组成员上传网站项目；**
* **上传测试sql数据库文件到mariadb服务器节点；**
* **内网运维人员测试访问网站项目；**
* **外网客户端访问测试项目；**
* **开启外网测试的win7客户端；**



* **配置网关服务器的网络参数及内网上网参数；**







[root@gw ~]# vi /etc/sysctl.conf

net.ipv4.ip\_forward = 1

:wq

[root@gw ~]# sysctl -p

net.ipv4.ip\_forward = 1

[root@gw ~]# /etc/init.d/httpd stop

[root@gw ~]# /etc/init.d/dhcpd stop

[root@gw ~]# /etc/init.d/named stop

[root@gw ~]# /etc/init.d/iptables stop

[root@gw ~]# iptables -t nat -A POSTROUTING -o eth1 -s 192.168.100.0/24 -j MASQUERADE

[root@gw ~]# iptables -t nat -A POSTROUTING -o eth1 -s 172.16.0.0/16 -j MASQUERADE

[root@gw ~]# iptables -t nat -A POSTROUTING -o eth1 -s 172.15.0.0/16 -j MASQUERADE

[root@gw ~]# iptables -t nat -A PREROUTING -i eth1 -d 192.168.3.100 -p tcp --dport 80 -j DNAT --to-destination 192.168.100.103

[root@gw ~]# iptables -t nat -A PREROUTING -i eth1 -d 192.168.3.100 -p tcp --dport 53 -j DNAT --to-destination 192.168.100.101

[root@gw ~]# iptables -t nat -A PREROUTING -i eth1 -d 192.168.3.100 -p udp --dport 53 -j DNAT --to-destination 192.168.100.101

* **配置内网管理服务器的网络参数及搭建dhcp、vsftpd、DNS、cobbler服务（略）；**

[root@admin ~]# ip a|grep 192.168.100.101

inet 192.168.100.101/24 brd 192.168.100.255 scope global eth0

[root@admin ~]# yum -y install dhcp

[root@admin ~]# vi /etc/dhcp/dhcpd.conf

option domain-name "linuxfan.cn";

option domain-name-servers 192.168.100.101;

default-lease-time 600;

max-lease-time 7200;

log-facility local7;

subnet 192.168.100.0 netmask 255.255.255.0 {

range 192.168.100.200 192.168.100.250;

option routers 192.168.100.100;

}

subnet 172.16.0.0 netmask 255.255.0.0 {

range 172.16.10.101 172.16.10.150;

option routers 172.16.10.100;

}

subnet 172.15.0.0 netmask 255.255.0.0 {

range 172.15.10.101 172.15.10.150;

option routers 172.15.10.100;

}

:wq

[root@admin ~]# systemctl start dhcpd

[root@admin ~]# systemctl enable dhcpd

Created symlink from /etc/systemd/system/multi-user.target.wants/dhcpd.service to /usr/lib/systemd/system/dhcpd.service.

[root@admin ~]# netstat -utpln |grep dhcp

udp 0 0 0.0.0.0:67 0.0.0.0:\* 1222/dhcpd

udp 0 0 0.0.0.0:11934 0.0.0.0:\* 1222/dhcpd

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

[root@admin ~]# vi /etc/vsftpd/vsftpd.conf

anonymous\_enable=YES

local\_enable=NO

write\_enable=YES

local\_umask=022

anon\_upload\_enable=YES

anon\_mkdir\_write\_enable=YES

anon\_other\_write\_enable=YES

dirmessage\_enable=YES

xferlog\_enable=YES

connect\_from\_port\_20=YES

xferlog\_file=/var/log/xferlog

xferlog\_std\_format=YES

listen=YES

listen\_ipv6=NO

pam\_service\_name=vsftpd

userlist\_enable=YES

tcp\_wrappers=YES

:wq

[root@admin ~]# systemctl start vsftpd

[root@admin ~]# systemctl enable vsftpd

Created symlink from /etc/systemd/system/multi-user.target.wants/vsftpd.service to /usr/lib/systemd/system/vsftpd.service.

[root@admin ~]# netstat -utpln |grep vsftpd

tcp 0 0 0.0.0.0:21 0.0.0.0:\* LISTEN 1287/vsftpd

[root@admin ~]# mkdir /var/ftp/tomcat

[root@admin ~]# mkdir /var/ftp/nginx

[root@admin ~]# chmod 777 /var/ftp/\*

[root@admin ~]# yum -y install bind bind-utils

[root@admin ~]# vi /etc/named.conf

options {

listen-on port 53 { 192.168.100.101; };

directory "/var/named";

dump-file "/var/named/data/cache\_dump.db";

statistics-file "/var/named/data/named\_stats.txt";

memstatistics-file "/var/named/data/named\_mem\_stats.txt";

allow-query { any; };

recursion yes;

pid-file "/run/named/named.pid";

};

logging {

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

view "internal" {

match-clients {

localhost;

192.168.100.0/24;

172.16.0.0/16;

172.15.0.0/16;

};

zone "linuxfan.cn." IN {

type master;

file "linuxfan.cn.nei";

};

zone "." IN {

type hint;

file "named.ca";

};

};

view "external" {

match-clients { any; };

allow-query { any; };

recursion no;

zone "linuxfan.cn." IN {

type master;

file "linuxfan.cn.wai";

};

};

:wq

[root@admin ~]# vi /var/named/linuxfan.cn.nei

$TTL 86400

@ IN SOA linuxfan.cn. root.linuxfan.cn. (

20151211

1D

1H

1W

3H )

IN NS admin.linuxfan.cn.

admin IN A 192.168.100.101

IN A 192.168.100.101

www IN A 192.168.100.103

ftp IN CNAME admin

:wq

[root@admin ~]# cp /var/named/linuxfan.cn.nei /var/named/linuxfan.cn.wai

[root@admin ~]# vi /var/named/linuxfan.cn.wai

$TTL 86400

@ IN SOA linuxfan.cn. root.linuxfan.cn. (

20151211

1D

1H

1W

3H )

IN NS admin.linuxfan.cn.

admin IN A 192.168.3.100

IN A 192.168.3.100

www IN A 192.168.3.100

:wq

[root@admin ~]# chown named:named /etc/named.conf /var/named/linuxfan.cn.\*

[root@admin ~]# systemctl start named

[root@admin ~]# systemctl enable named

Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /usr/lib/systemd/system/named.service.

[root@admin ~]# netstat -utpln |grep named

tcp 0 0 192.168.100.101:53 0.0.0.0:\* LISTEN 1466/named

tcp 0 0 127.0.0.1:953 0.0.0.0:\* LISTEN 1466/named

udp 0 0 192.168.100.101:53 0.0.0.0:\* 1466/named

udp 0 0 0.0.0.0:58976 0.0.0.0:\* 1466/named

* **在网关服务器配置DHCP中继；**

[root@gw ~]# yum -y install dhcp

[root@gw ~]# vi /etc/sysconfig/dhcrelay

# Command line options here

DHCRELAYARGS=""

# DHCPv4 only

INTERFACES="eth0 eth2 eth3" ##指定需要中继的网卡

# DHCPv4 only

DHCPSERVERS="192.168.100.101" ##指定dhcp服务器的ip地址

:wq

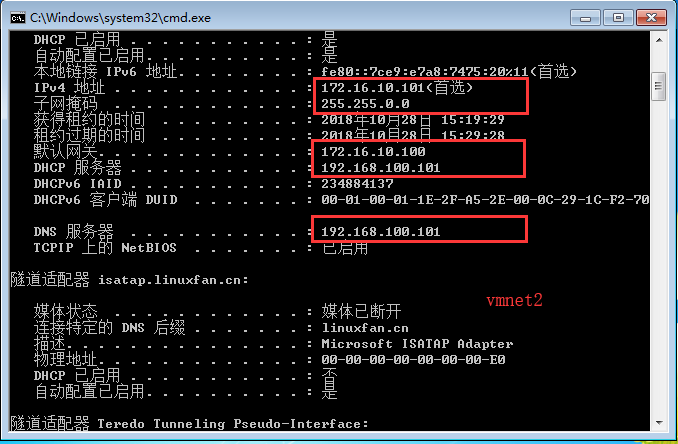
[root@gw ~]# /etc/init.d/dhcrelay start

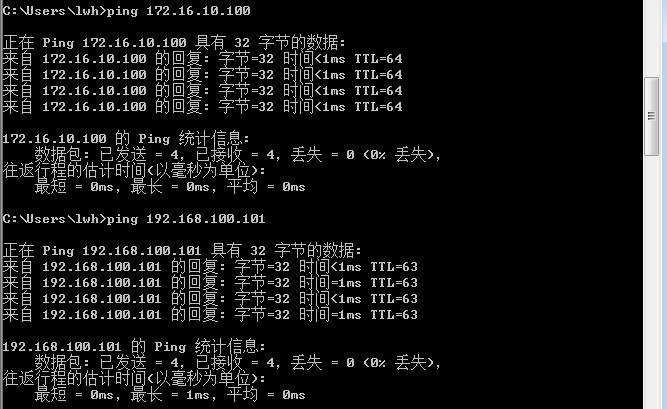
正在启动 dhcrelay： [确定]

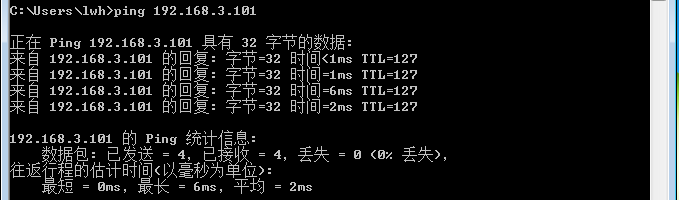
[root@gw ~]# netstat -utpln |grep 67

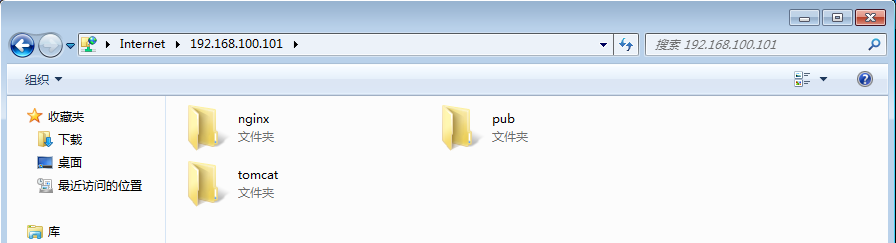
udp 0 0 0.0.0.0:67 0.0.0.0:\* 2291/dhcrelay

* **开启内网运维组主机，测试自动获取的网络参数；**

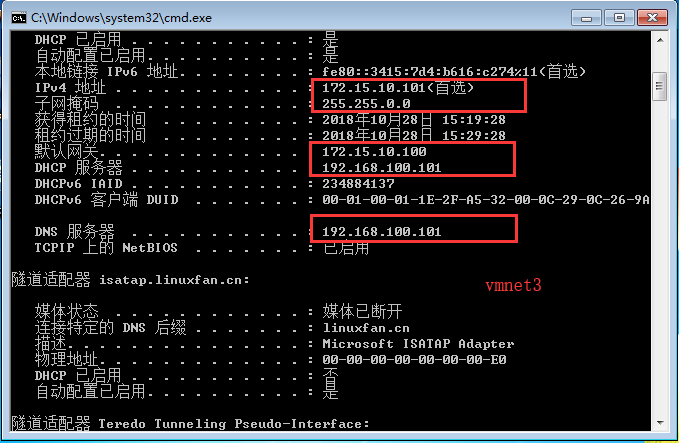


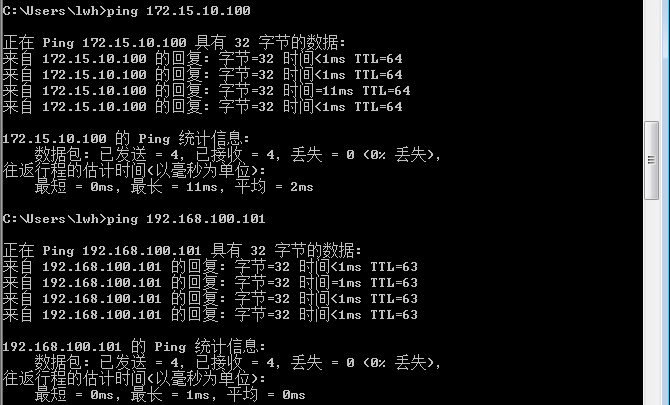


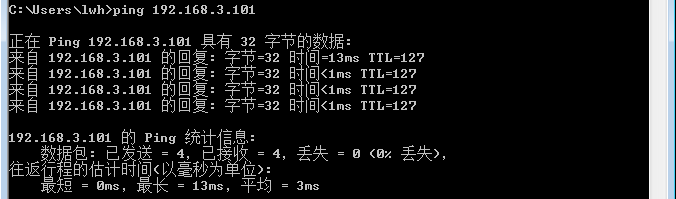


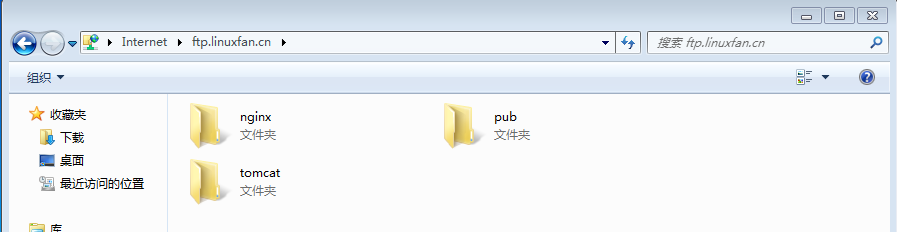


* **开启内网开发组主机，测试自动获取的网络参数；**









* **搭建服务器组内的NFS服务；**

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

[root@st ~]# mkdir /opt/nginx

[root@st ~]# mkdir /opt/tomcat

[root@st ~]# chmod 777 /opt/nginx

[root@st ~]# chmod 777 /opt/tomcat/

[root@st ~]# vi /etc/exports

/opt/nginx 192.168.100.0/24(rw,sync,no\_root\_squash)

/opt/tomcat 192.168.100.0/24(rw,sync,no\_root\_squash)

:wq

[root@st ~]# systemctl start rpcbind

[root@st ~]# systemctl start nfs

Job for nfs-server.service failed because the control process exited with error code. See "systemctl status nfs-server.service" and "journalctl -xe" for details.

[root@st ~]# kill -HUP `cat /run/gssproxy.pid`

[root@st ~]# systemctl start nfs

**[root@st ~]# showmount -e 192.168.100.102**

**Export list for 192.168.100.102:**

**/opt/tomcat 192.168.100.0/24**

**/opt/nginx 192.168.100.0/24**

* **配置管理主机的ftp目录与NFS的共享目录进行实时同步；**

[root@admin ~]# ssh-keygen -t rsa

[root@admin ~]# ssh-copy-id root@192.168.100.102

[root@admin ~]# ssh root@192.168.100.102

Last login: Sun Oct 28 23:34:15 2018 from 192.168.100.1

[root@st ~]# exit

登出

Connection to 192.168.100.102 closed.

[root@admin ~]# ls inotify-tools-3.14.tar.gz

inotify-tools-3.14.tar.gz

[root@admin ~]# tar zxf inotify-tools-3.14.tar.gz -C /usr/src/

[root@admin ~]# cd /usr/src/inotify-tools-3.14/

[root@admin inotify-tools-3.14]# ./configure &&make &&make install

[root@admin inotify-tools-3.14]# cd

[root@admin ~]# vi /etc/sysctl.conf

fs.inotify.max\_queued\_events = 16384

fs.inotify.max\_user\_instances = 1024

fs.inotify.max\_user\_watches = 1048576

:wq

[root@admin ~]# sysctl -p

fs.inotify.max\_queued\_events = 16384

fs.inotify.max\_user\_instances = 1024

fs.inotify.max\_user\_watches = 1048576

[root@admin ~]# vi /root/rsync\_ino.sh

#!/bin/bash

RSYNC1="rsync -avzH /var/ftp/nginx/ root@192.168.100.102:/opt/nginx/ --delete"

RSYNC2="rsync -avzH /var/ftp/tomcat/ root@192.168.100.102:/opt/tomcat/ --delete"

INT\_CMD="inotifywait -mrq -e modify,create,move,delete,attrib /var/ftp/"

$INT\_CMD |while read DIRECOTRY EVENT FILE;do

chown root:root /var/ftp/nginx/\* -R

chown root:root /var/ftp/tomcat/\* -R

$RSYNC1

$RSYNC2

done

:wq

[root@admin ~]# chmod +x /root/rsync\_ino.sh

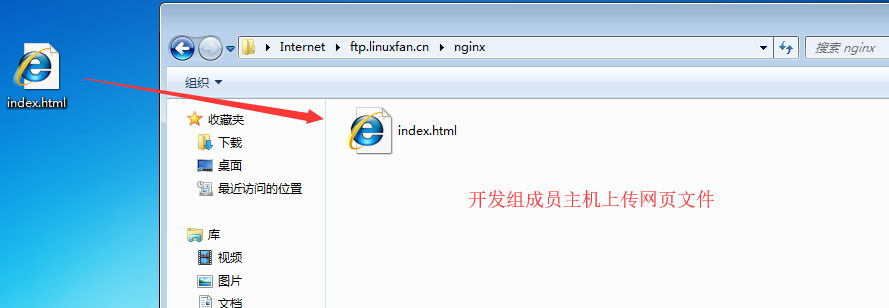
[root@admin ~]# /root/rsync\_ino.sh &

[1] 4026

[root@admin ~]# jobs -l

[1]+ 4026 运行中 /root/rsync\_ino.sh &

* **测试ftp服务器目录与NFS共享目录的实时同步情况；**





* **搭建服务器组内的Nginx服务并配置NFS挂载；**

[root@nginx ~]# yum -y install pcre-devel zlib-devel

[root@nginx ~]# useradd -M -s /sbin/nologin nginx

[root@nginx ~]# tar zxf nginx-1.12.2.tar.gz -C /usr/src/

[root@nginx ~]# cd /usr/src/nginx-1.12.2/

[root@nginx nginx-1.12.2]# ./configure --prefix=/usr/local/nginx --user=nginx --group=nginx &&make && make install

[root@nginx nginx-1.12.2]# cd

[root@nginx ~]# ln -s /usr/local/nginx/sbin/nginx /usr/local/sbin/

[root@nginx ~]# vi /usr/lib/systemd/system/nginx.service

[Unit]

Description=nginxapi

After=network.target

[Service]

Type=forking

PIDFile=/usr/local/nginx/logs/nginx.pid

ExecStart=/usr/local/nginx/sbin/nginx

ExecReload=kill -s HUP $(cat /usr/local/nginx/logs/nginx.pid)

ExecStop=kill -s QUIT $(cat /usr/local/nginx/logs/nginx.pid)

PrivateTmp=Flase

[Install]

WantedBy=multi-user.target

:wq

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

[root@nginx ~]# vi /etc/fstab

192.168.100.102:/opt/nginx /usr/local/nginx/html nfs defaults,\_netdev 0 0

:wq

[root@nginx ~]# mount -a

[root@nginx ~]# ls /usr/local/nginx/html/

index.html

[root@nginx ~]# cat /usr/local/nginx/html/index.html

www.linuxfan.cn

[root@nginx ~]# vi /usr/local/nginx/conf/nginx.conf

34 upstream tomcatserver {

35 ip\_hash;

36 server 192.168.100.104:8080 weight=1;

37 server 192.168.100.105:8080 weight=1;

38 }

52 location ~ \.(jsp|js|css|png|do|jpg|jpeg)$ {

53 proxy\_pass http://tomcatserver;

54 }

:wq

[root@nginx ~]# systemctl start nginx

[root@nginx ~]# systemctl enable nginx

Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.

[root@nginx ~]# netstat -utpln |grep 80

tcp 0 0 0.0.0.0:80 0.0.0.0:\* LISTEN 3774/nginx: master

* **搭建服务器组内的Tomcat服务并配置NFS挂载（两台Tomcat节点配置相同，在此列出一台）；**

[root@tm1 ~]# ls

apache-tomcat-9.0.10.tar.gz jdk-8u171-linux-x64.tar.gz

[root@tm1~]# rpm -qa |grep java

[root@tm1 ~]# tar zxvf jdk-8u171-linux-x64.tar.gz

[root@tm1 ~]# mv jdk1.8.0\_171/ /usr/local/java

[root@tm1 ~]# cat <<END >>/etc/profile

export JAVA\_HOME=/usr/local/java

export PATH=$PATH:/usr/local/java/bin

END

[root@tm1~]# source /etc/profile

[root@tm1 ~]# java -version

java version "1.8.0\_171"

Java(TM) SE Runtime Environment (build 1.8.0\_171-b11)

Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)

[root@tm1 ~]# tar zxvf apache-tomcat-9.0.10.tar.gz

[root@tm1 ~]# mv apache-tomcat-9.0.10 /usr/local/tomcat

[root@tm1 ~]# yum -y install nfs-utils

[root@tm1 ~]# vi /etc/fstab

192.168.100.102:/opt/tomcat /usr/local/tomcat/webapps/ nfs defaults,\_netdev 0 0

:wq

[root@tm1 ~]# mount -a

[root@tm1 ~]# ls /usr/local/tomcat/webapps/

[root@tm1 ~]# /usr/local/tomcat/bin/startup.sh

[root@tm1 ~]# netstat -utpln |grep 8080

tcp 0 0 0.0.0.0:8080 0.0.0.0:\* LISTEN 1345/java

* **搭建服务器组内的Mariadb数据库服务；**

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

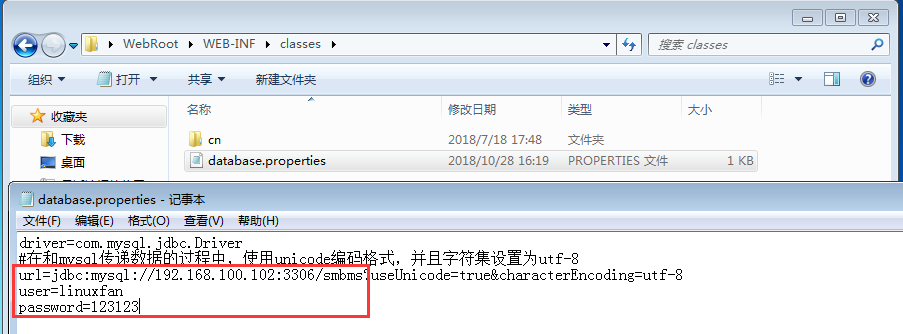
[root@st ~]# systemctl start mariadb

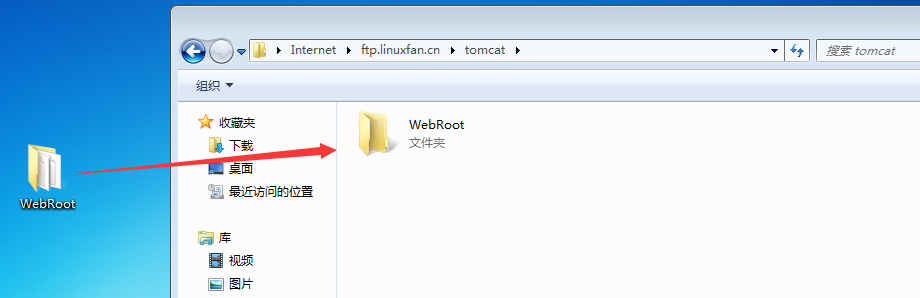
[root@st ~]# systemctl enable mariadb

Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service.

[root@st ~]# mysqladmin -uroot password 123123

* **内网开发组成员上传网站项目；**





* **上传测试sql数据库文件到mariadb服务器节点：**

[root@st ~]# ls smbms\_db.sql

smbms\_db.sql

[root@st ~]# mysql -uroot -p123123 <smbms\_db.sql

[root@st ~]# mysql -uroot -p123123

MariaDB [(none)]> grant all on smbms.\* to 'linuxfan'@'192.168.100.%' identified by '123123';

Query OK, 0 rows affected (0.00 sec)

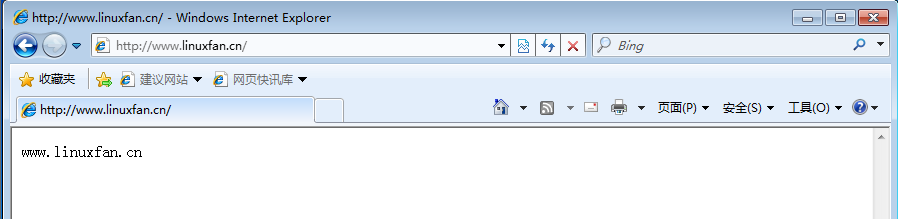
MariaDB [(none)]> flush privileges;

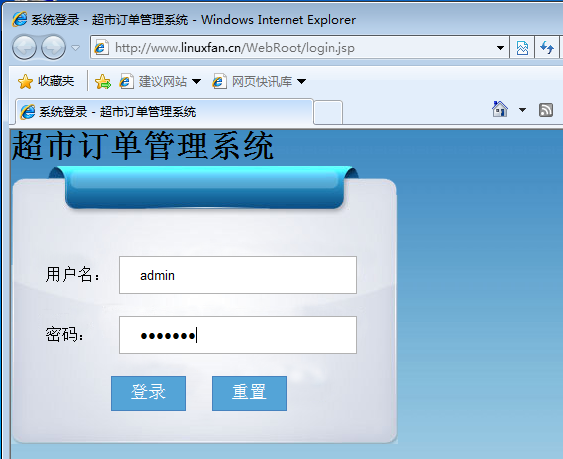
Query OK, 0 rows affected (0.00 sec)

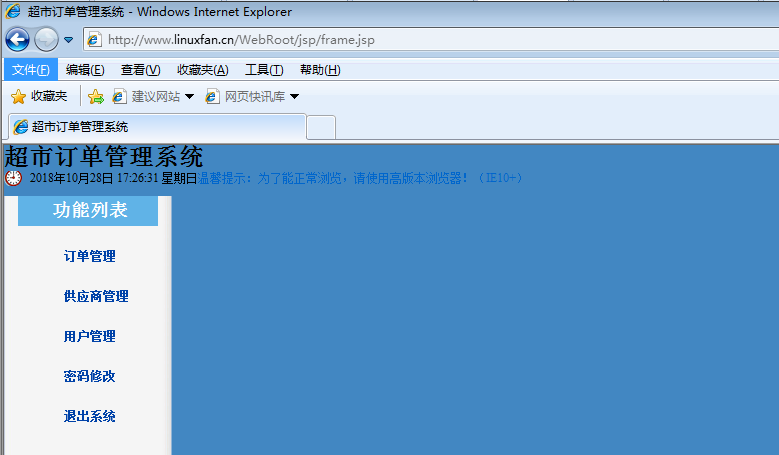
MariaDB [(none)]> exit

Bye

* **内网运维人员测试访问网站项目；**







* **外网客户端访问测试项目；**

