**环境介绍：**

1. 服务器： 192.168.0.100

2. 客户机： 192.168.0.101

**安装软件包：**

服务器和客户机都要安装nfs 和 rpcbind 软件包：

yum -y install nfs-utils  rpcbind

**服务器端配置：**

1. 在服务器上创建NFS共享目录：mkdir /usr/local/test

2. 设置共享目录的读写权限: chmod 666 /usr/local/test

3. 编辑export文件：  vi /etc/exports

/usr/local/test/ 192.168.0.101(rw,no\_root\_squash,no\_all\_squash,sync)

注意地址和参数表之间没有空格。如果下面设置的mountd端口大于1024，需要在参数表里加入参数：insecure  
4. 配置生效：

exportfs  -r

**注：配置文件说明：**

/usr/local/test/ 为共享的目录，使用绝对路径。  
192.168.0.101(rw,no\_root\_squash,no\_all\_squash,sync) 为客户端的地址及权限，地址可以是一个网段（如：192.168.0.0/24），一个IP地址或者是一个域名，域名支持通配符，如：\*.hpce.cn，地址与权限中间没有空格。

**权限说明：**rw：read-write，可读写；  
ro：read-only，只读；  
sync：文件同时写入硬盘和内存；  
async：文件暂存于内存，而不是直接写入内存；  
no\_root\_squash：NFS客户端连接服务端时如果使用的是root的话，那么对服务端分享的目录来说，也拥有root权限。显然开启这项是不安全的。  
root\_squash：NFS客户端连接服务端时如果使用的是root的话，那么对服务端分享的目录来说，拥有匿名用户权限，通常他将使用nobody或nfsnobody身份；  
all\_squash：不论NFS客户端连接服务端时使用什么用户，对服务端分享的目录来说都是拥有匿名用户权限；  
anonuid：匿名用户的UID值，通常是nobody或nfsnobody，可以在此处自行设定；  
anongid：匿名用户的GID值。  
  
5. 启动服务rpcbind、nfs服务:

service rpcbind  start

service nfs  start

**服务器端防火墙设置（NFS 开启防墙配置）：**

**修改/etc/services文件：**

配置**rpc，nfsd，rquotad，mountd**使用的端口。配置之前先检查一下是否已经配置过了，已经配过的就不用配置了。没有配置的，要分配一个在此文件中未被使用的端口号。我的机器默认配置了：**rpc、nfsd、rquotad**

**mountd:** 没有配置。手工加上：

mountd          48620/tcp               #rpc.mountd

mountd          48620/udp               #rpc.mountd

如果**mountd**占用端口大于 1024，在文件 /etc/exports里需要加入参数**insecure**。如：192.168.0.100(insecure,rw,async,root\_squash,no\_all\_squash)

**重启NFS服务：**

service nfs restart

**在防火墙配置文件里开放上面配置的端口：**

打开文件：vim /etc/sysconfig/iptables

加入红色部分的内容：

-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT

#rpc

-A INPUT -m state --state NEW -m tcp -p tcp --dport 121 -j ACCEPT

-A INPUT -m state --state NEW -m udp -p udp --dport 121 -j ACCEPT

#nfsd

-A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT

-A INPUT -m state --state NEW -m udp -p udp --dport 2049 -j ACCEPT

#rquotad

-A INPUT -m state --state NEW -m tcp -p tcp --dport 875 -j ACCEPT

-A INPUT -m state --state NEW -m udp -p udp --dport 875 -j ACCEPT

#mountd

-A INPUT -m state --state NEW -m tcp -p tcp --dport 48620 -j ACCEPT

-A INPUT -m state --state NEW -m udp -p udp --dport 48620 -j ACCEPT

-A INPUT -j REJECT --reject-with icmp-host-prohibited

或者：

/sbin/iptables -I INPUT -p tcp --dport 121 -j ACCEPT 

/sbin/iptables -I INPUT -p tcp --dport 2049 -j ACCEPT 

/sbin/iptables -I INPUT -p tcp --dport 875 -j ACCEPT 

/sbin/iptables -I INPUT -p tcp --dport 48620 -j ACCEPT 

**客户端挂载：**

**创建挂载目录：** mkdir /usr/local/test

查看服务器抛出的共享目录信息：

showmount -e 192.168.0.100

Export list for 192.168.0.100:

/usr/local/test 192.168.0.101

如果显示：rpc mount export: RPC: Unable to receive; errno = No route to host，则需要在服务端关闭防火墙。

为了提高NFS的稳定性，使用TCP协议挂载，NFS默认用UDP协议：

mount -t nfs 192.168.0.100:/usr/local/test  /usr/local/test  -o proto=tcp -o nolock

挂载成功后即可访问共享的NFS文件系统了。

**卸载已挂在的NFS**

umount /usr/local/test

**查看挂载目录的信息：**

fuser -m -v /usr/local/test

来源： <<http://blog.chinaunix.net/uid-23500957-id-4217525.html>>