NAStorage

Administrator Guide

Security Policy Of NAStorage Under UNIX/LINUX Environment

Version 1.00

10/01/2002

Prepared by:

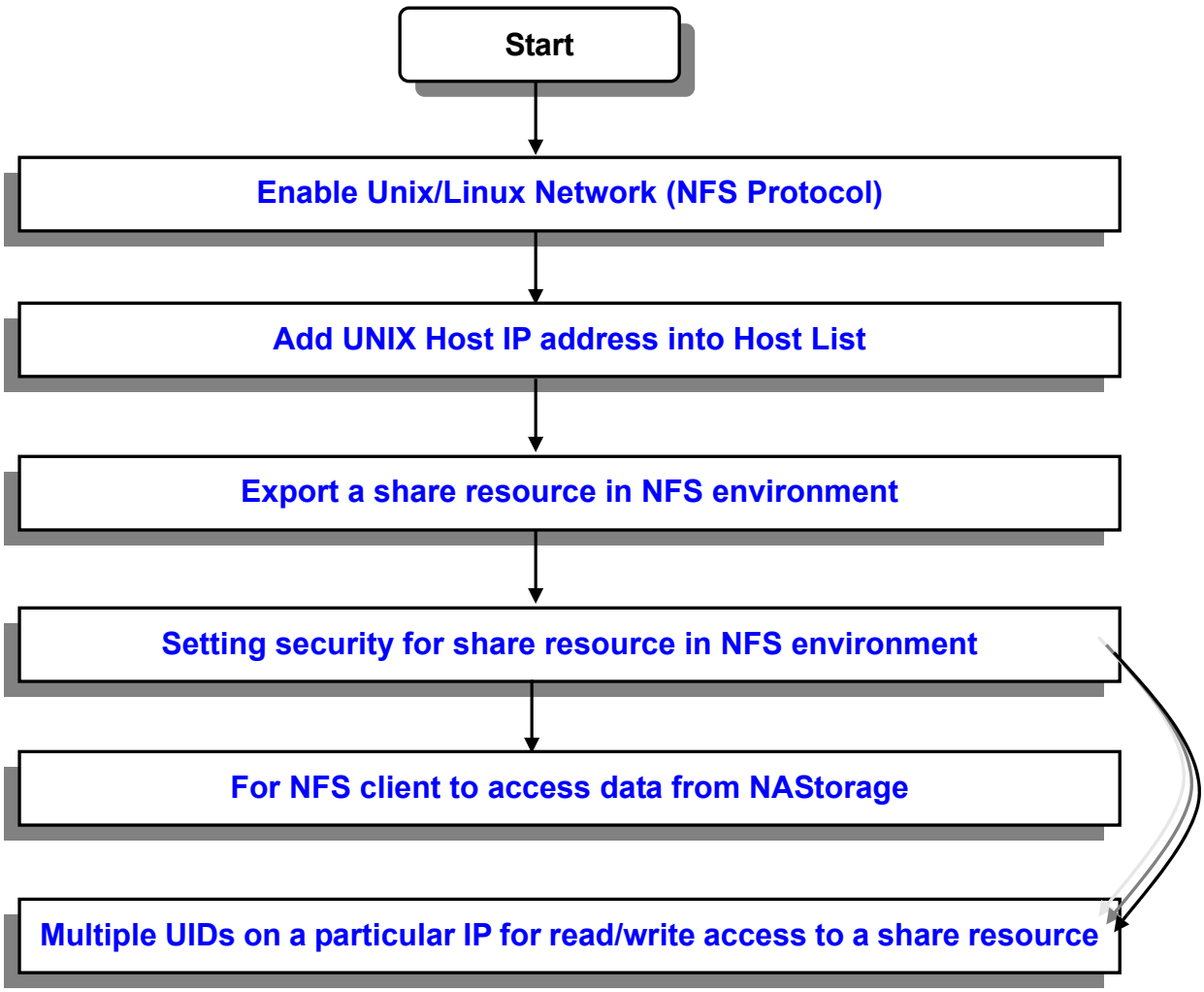
Leon Hsu

TS Engineer

Ingrasys Technology Inc.

E-mail: support@ingrasys.com

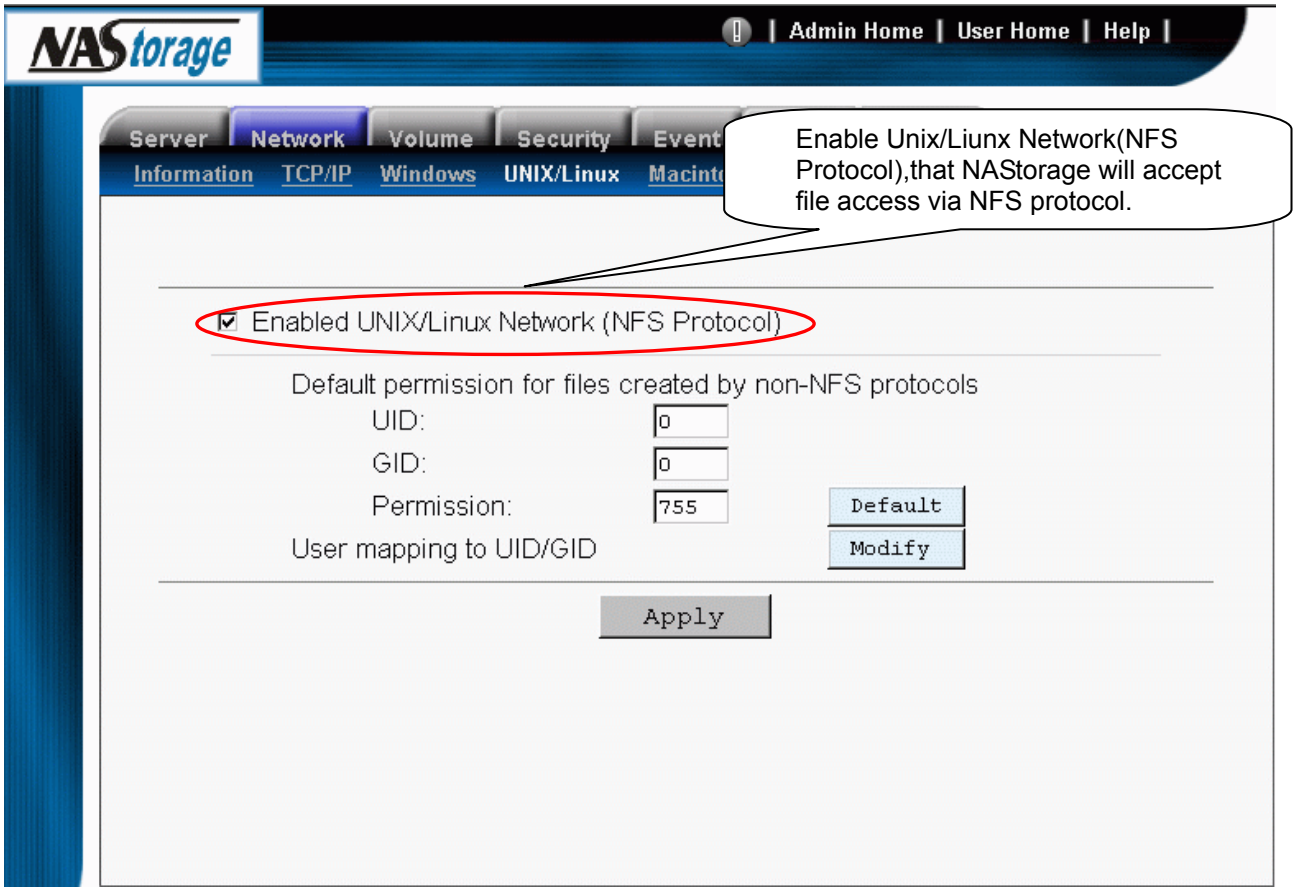
UNIX/LINUX environment Of NAStorage Under Security Policy



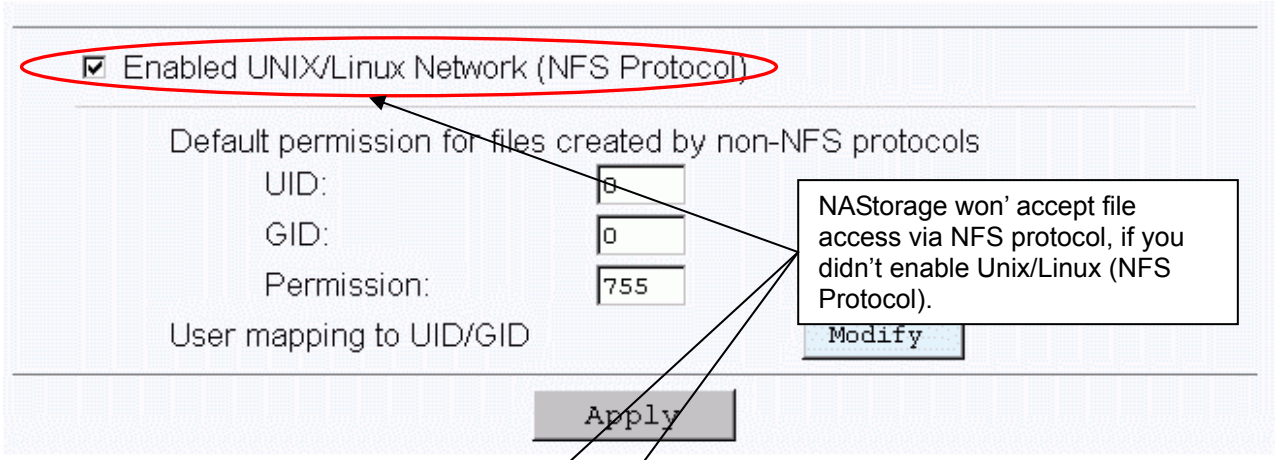
1. Enable Unix/Linux Network (NFS Protocol)

For file accessing, users can access NAStorage via NFS(UNIX/Linux) protocol. You just need to enable Unix/Linux Network(NFS Protocol) for NAStorage.

Configuration flow: **"Network–UNIX/Linux "**→ "Select" check box –Enable Unix/Linux Network (NFS Protocols)→ then "**Apply".**

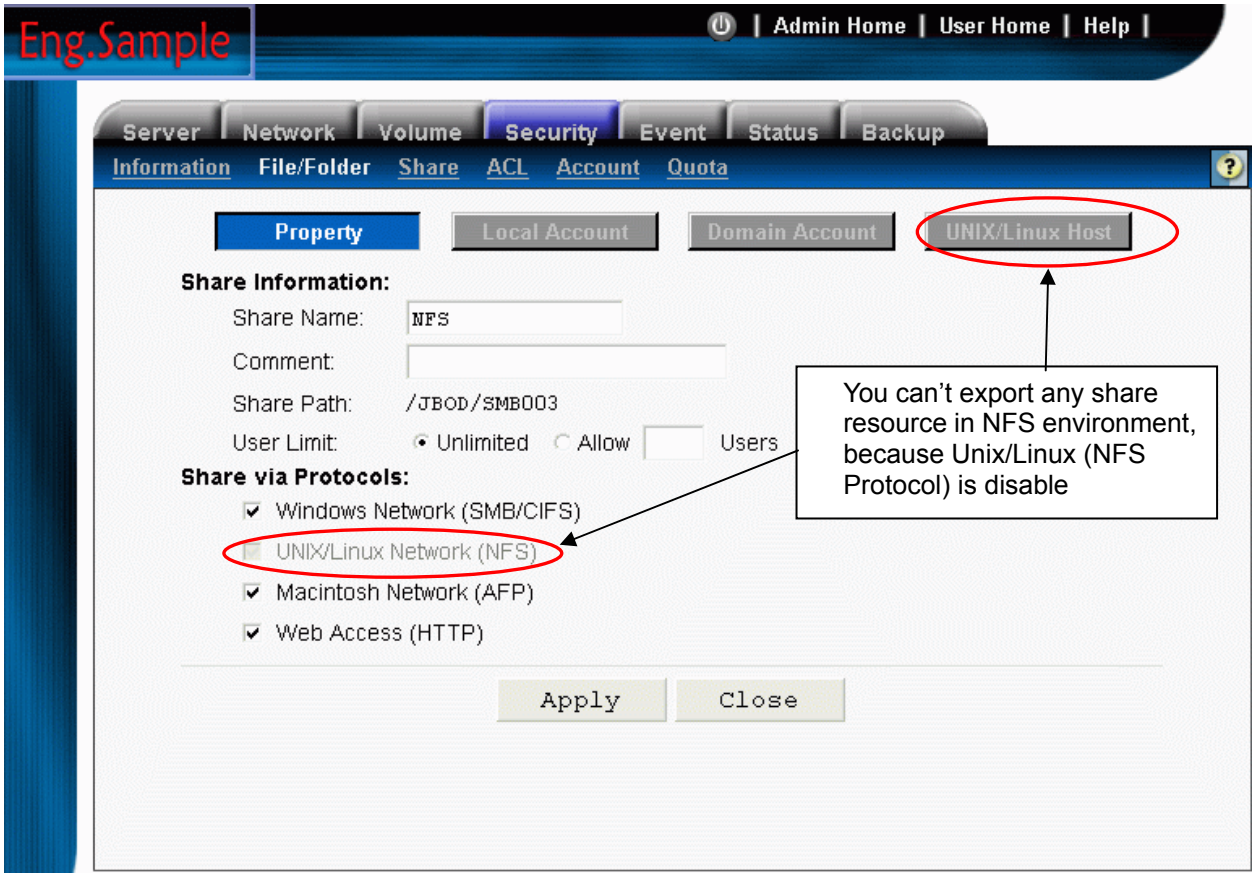


If you didn't enable Unix/Linux (NFS Protocol), NAStorage won' accept file access via NFS protocol. That mean you can't use "showmount" command to list share resource for NAStorage or use "rpcinfo" command to check NAStorage nfs service status, you will receive a **"Port mapper failure**" message.




```
[root@Leon-redhat root]# rpcinfo -u 203.67.163.92 nfs
rpcinfo: RPC: Port mapper failure - RPC: Unable to receive
program 100003 is not available
[root@Leon-redhat root]# showmount -e 203.67.163.92
mount clntudp_create: RPC: Port mapper failure - RPC: Unable to receive
[root@Leon-redhat root]#
```

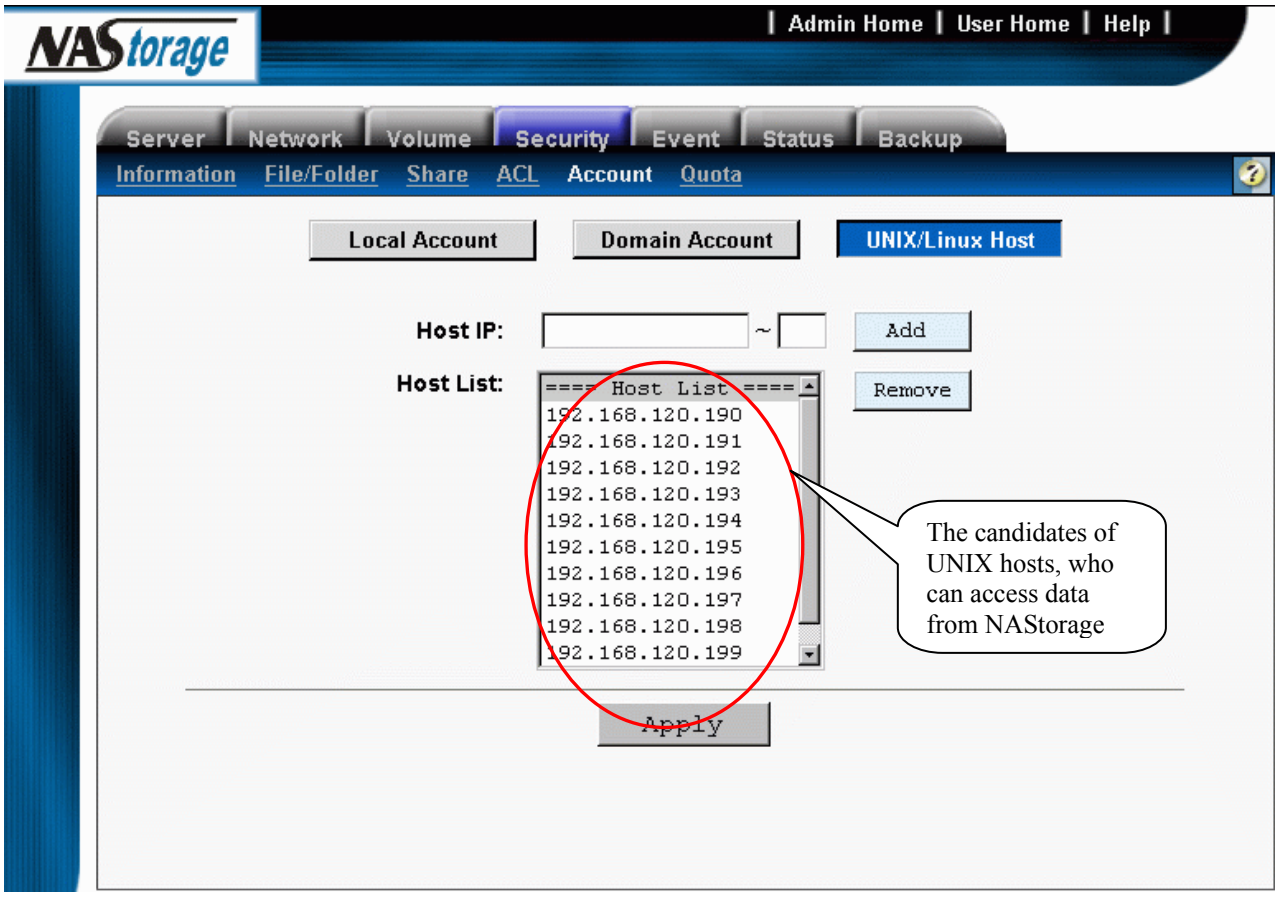
If you disable Unix/Linux (NFS Protocol) for NAStorage, you won't export any share resource in NFS environment,



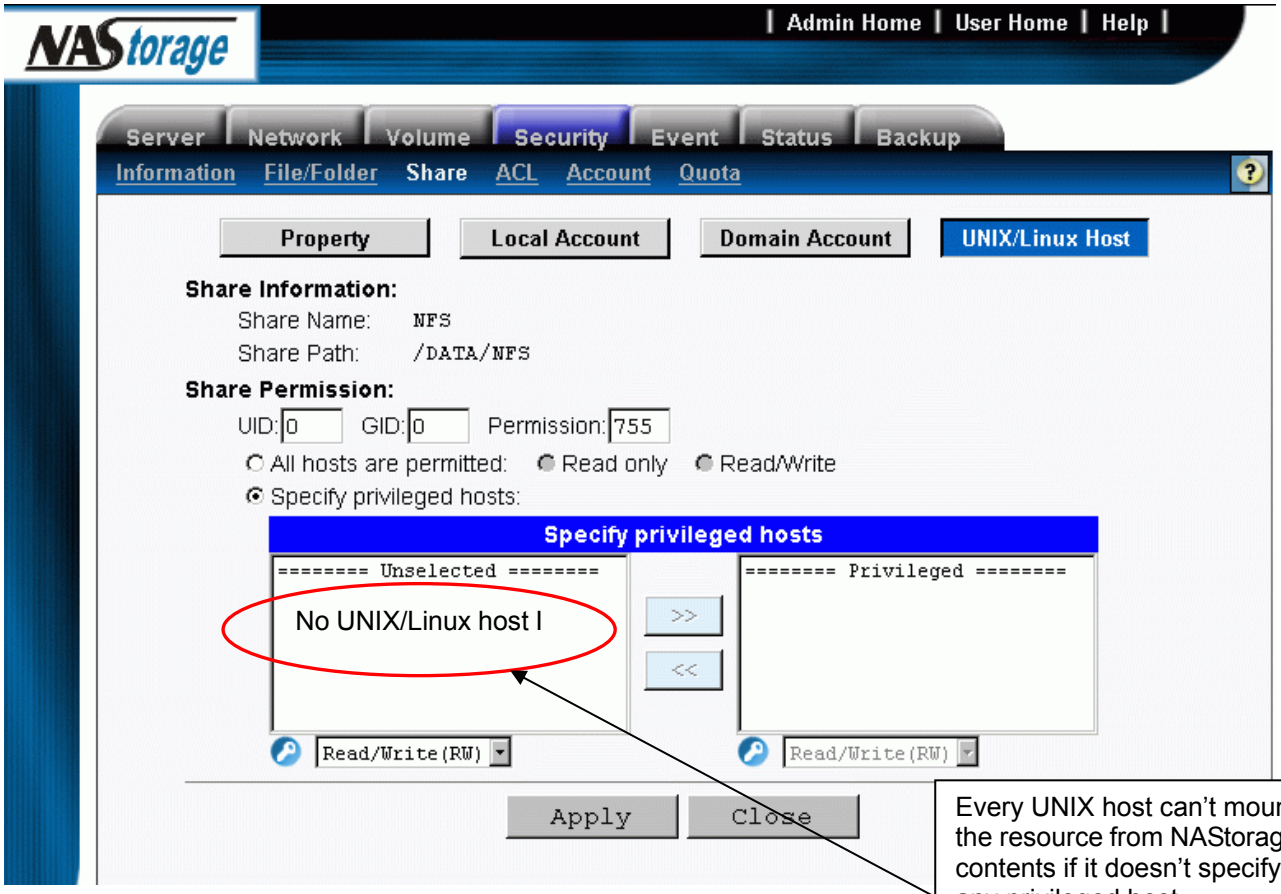
2. Add UNIX Host IP address into Host List

NAStorage support Local authentication policy for NFS protocol, that means if someone want to mount a share resource from NAStorage, the IP address of the UNIX/Linux host must be add to Local User DataBase first.

Configuration flow: "**Security Manager–Account** "→ "**UNIX Host**" → **Add Host.**



- If you don't add any host IP address in UNIX Host table, the default setting was "Specify privileged hosts", that means no any UNIX host can't mount the resource from NAStorage contents, UNIX host only can see the available share resource by using "showmount" command but doesn't have permission to mount .



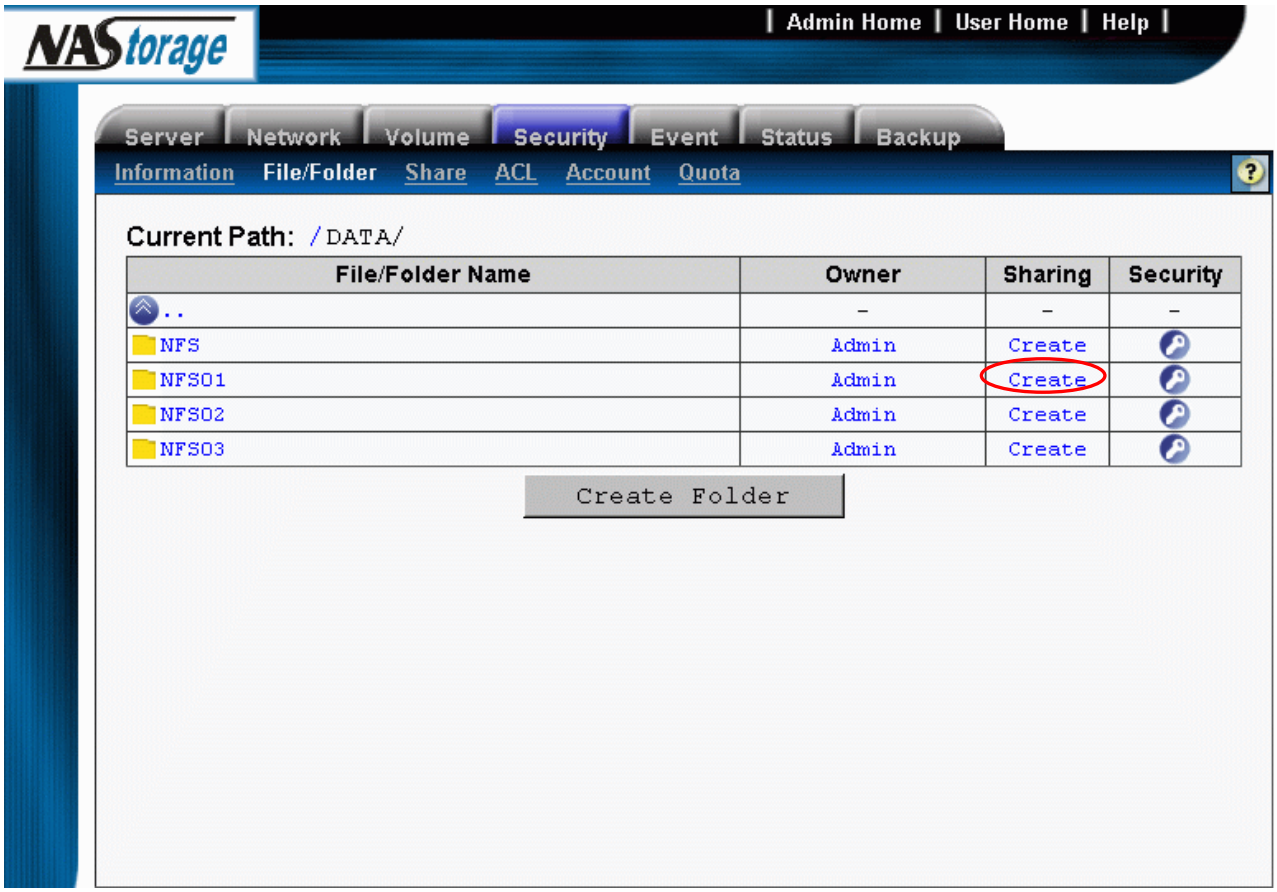
Every UNIX host can't mount the resource from NAStorage contents if it doesn't specify any privileged host

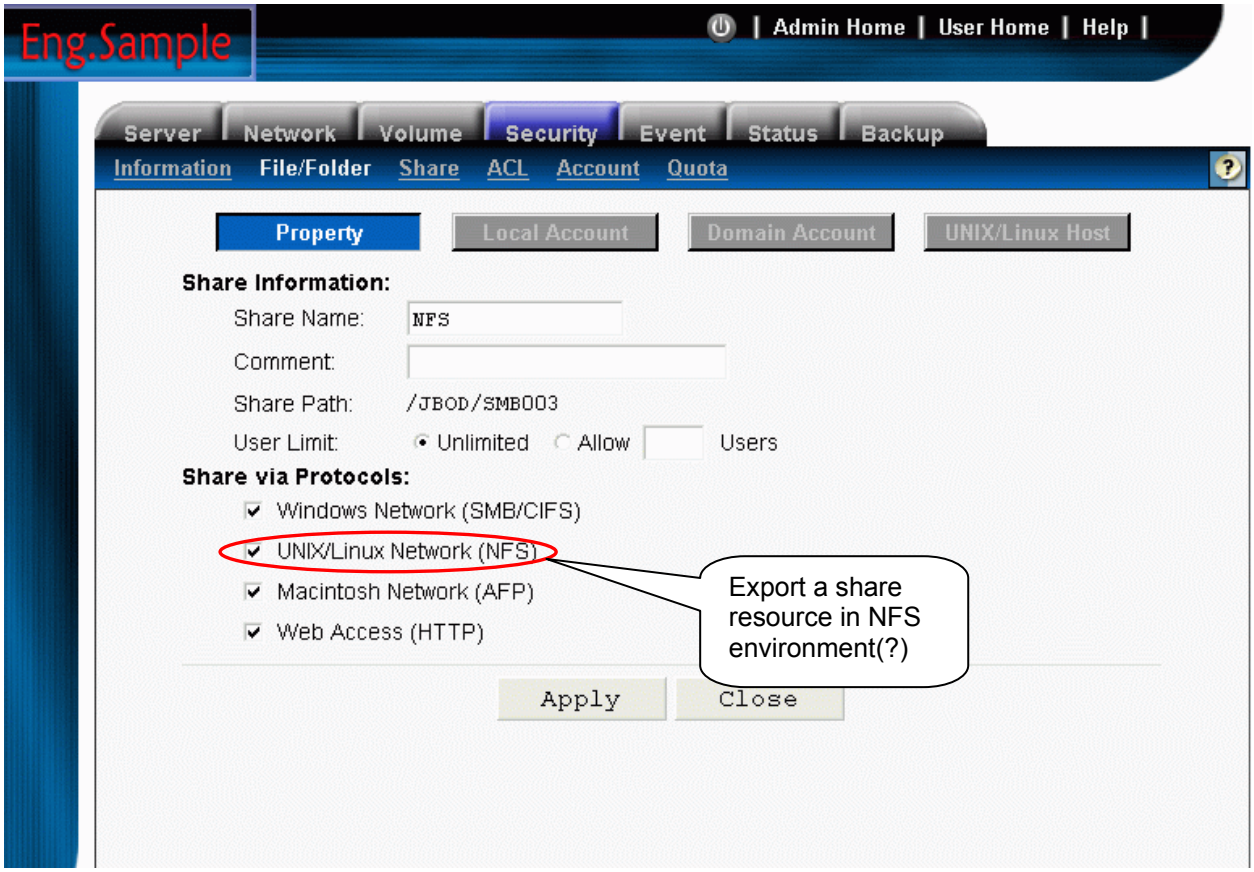
```
[root@Leon-redhat root]# showmount -e 203.67.163.92
Export list for 203.67.163.92:
/NFS (everyone)
/SMB (everyone)
[root@Leon-redhat root]# mount 203.67.163.92:/NFS /root/nastorage/
mount: 203.67.163.92:/NFS failed, reason given by server: Permission denied
[root@Leon-redhat root]#
```

3. Export a share resource in NFS environment

NAStorage supports NFS v3 network file protocol. If someone want to export a share resource from NAStorage in NFS environment, just need to enable “UNIX/Linux Network (NFS)” for share resource.

Configuration flow: **“Security Manager–File/Folder “**→click **“create"** → enable **“UNIX/Linux Network (NFS)”** then **Apply**.





Use "**showmount"** command for list the available share resource under NAStorage

```
[root@Leon-redhat root]# showmount -e 203.67.163.92
Export list for 203.67.163.92:
/NFS (everyone)
```

Available share resource list under NAStorage

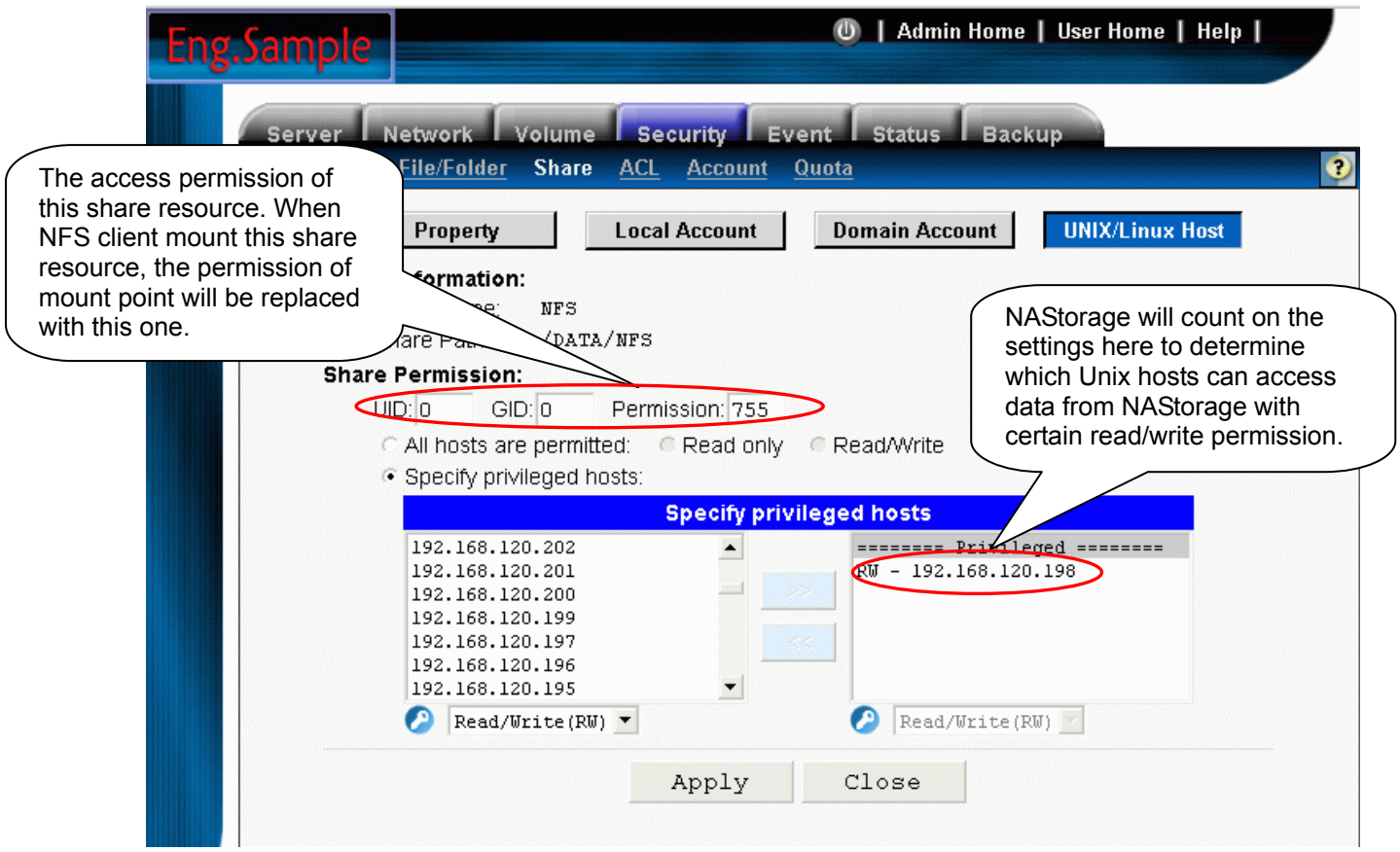
4. Setting security for share resource in NFS environment

NAStorage will trust the UNIX host (mounting volumes from NAStorage) to check UID, GID of logon user with the permission of mounted NAStorage share resource and the files/folders. The permission (Owner – User & Group, and access right – rwx rwx rwx) configured in NAStorage web admin page will be set as the default permission of mount point while NFS client mounts it.

Share Permission: Specify privileged hosts

NAStorage will count on the settings here to determine which UNIX hosts can access data from NAStorage with certain read/write permission.

Configuration flow: **"Security Manager–Share "**→ click **"Permission"** → **"UNIX Host"** → "**Add"** UNIX host IP address from left to right window and select the permission then **Apply**



For example,(UNIX/Linux host 192.168.120.198) you assign Read/Write permission for “192.168.120.198” host in NAStorage. Therefore this host can mount the share resource from NAStorage and can also create file/folder in the mount point.

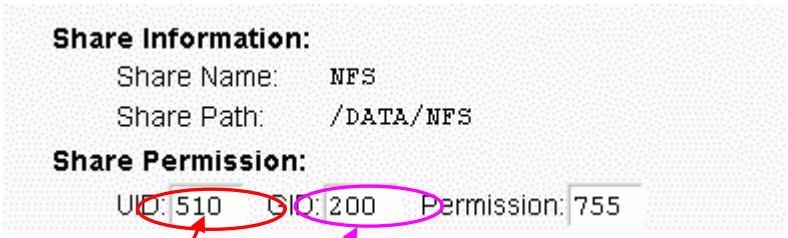
```
[root@Leon-redhat root]# showmount -e 203.67.163.92
Export list for 203.67.163.92:
/NFS (everyone)
/SMB (everyone)
[root@Leon-redhat root]# mount 203.67.163.92:/NFS /root/nastorage/
[root@Leon-redhat root]# ls -l
total 28
-rw-r--r--    1 root     root         1121 Jun 25 17:26 anaconda-ks.cfg
drwxr-xr-x    2 root     root         4096 Jul 11 15:23 autosave
drwx------    3 root     root         4096 Jul 11 18:21 Desktop
drwxr-xr-x    2 root     root           48 Jul 12 10:21 nastorage
drwx------    2 root     root         4096 Jul  3 14:04 nsmail
drwx--x--x    2 root     root         4096 Jul  4 10:06 Picture
drwxrwxr-x    3 root     root         4096 Jun 26 11:31 profile
[root@Leon-redhat root]# cd nastorage/
[root@Leon-redhat nastorage]# mkdir test
[root@Leon-redhat nastorage]# ls -l
total 4
drwxrwxrwx    2 root     root           48 Jul 12 11:35 test
[root@Leon-redhat nastorage]#
```

This host has Read/Write permission for the share resource point from NAStorage and also can create file/folder in the mount point.

You can check this mount point permission already changed to UID:root GID:root Permission:755. If the UNIX host has R/W permission for this share, root user also can issue **"chown / chmod"** command to change the owner/permission for this mount point.

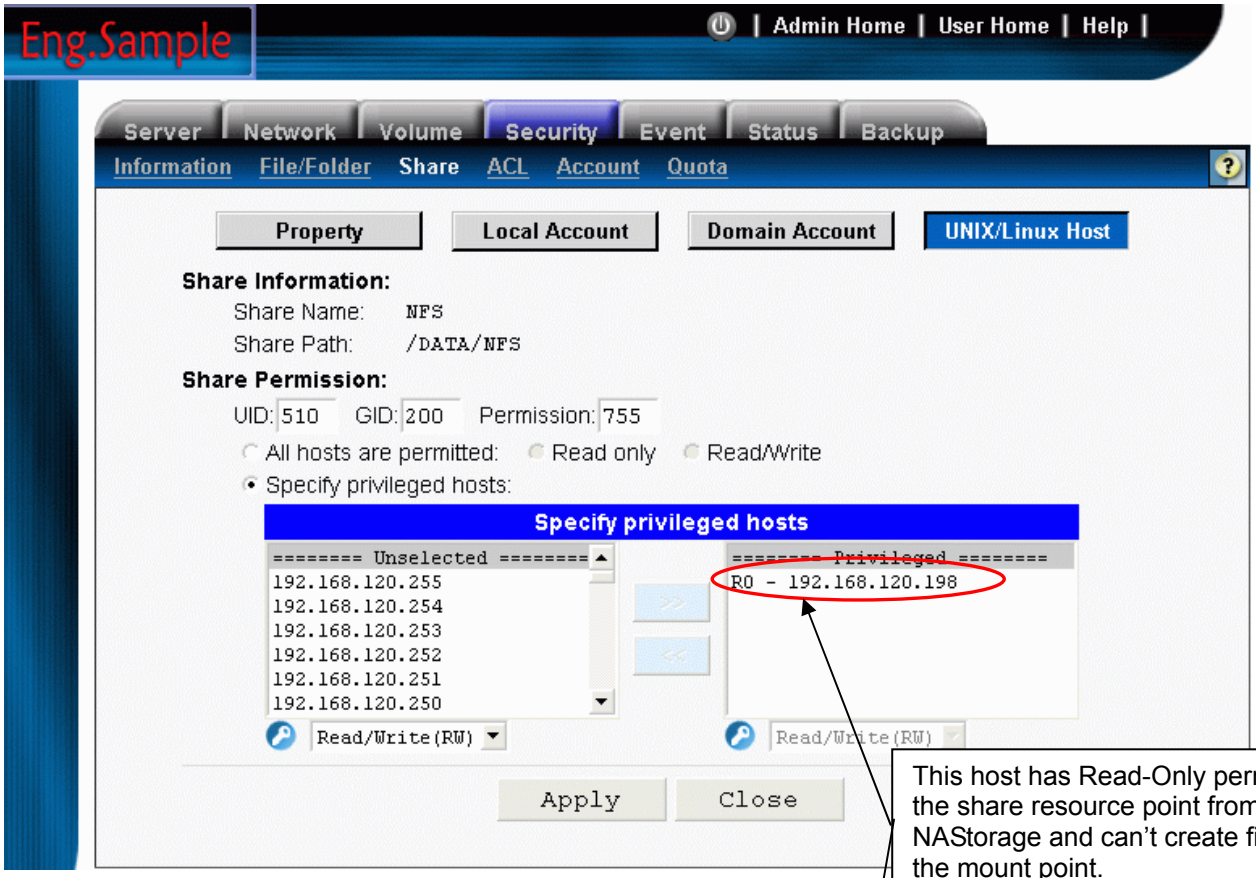
```
[root@Leon-redhat root]# ls -l
total 32
-rw-r--r--    1 root     root         1121 Jun 25 17:26 anaconda-ks.cfg
drwxr-xr-x    2 root     root         4096 Jul 11 15:23 autosave
-rwxr-xr-x    1 root     root         2223 Sep  4 13:47 compare
drwx------    3 root     root         4096 Jul 11 18:21 Desktop
drwxr-xr-x    2 root     root           48 Sep  9 11:01 nastorage
drwx------    2 root     root         4096 Jul  3 14:04 nsmail
drwx--x--x    2 root     root         4096 Jul  4 10:06 Picture
drwxrwxr-x    3 root     root         4096 Jun 26 11:31 profile
[root@Leon-redhat root]# chown nfs001:nasuser nastorage/
[root@Leon-redhat root]# ls -l
total 32
-rw-r--r--    1 root     root         1121 Jun 25 17:26 anaconda-ks.cfg
drwxr-xr-x    2 root     root         4096 Jul 11 15:23 autosave
-rwxr-xr-x    1 root     root         2223 Sep  4 13:47 compare
drwx------    3 root     root         4096 Jul 11 18:21 Desktop
drwxr-xr-x    2 nfs001   nasuser        48 Sep  9 11:01 nastorage
drwx------    2 root     root         4096 Jul  3 14:04 nsmail
drwx--x--x    2 root     root         4096 Jul  4 10:06 Picture
drwxrwxr-x    3 root     root         4096 Jun 26 11:31 profile
```

If you change the permission for this mount point, the admin page share permission will also be change.




```
[root@Leon-redhat root]# tail /etc/group
ingrasys:x:501:
es:x:502:
ts:x:503:
qa:x:504:
guest:x:505:
test:x:506:
Leon-CDH:x:509:
nasuser:x:200:leonhsu
carolhsu:x:513:
bady:x:514:
[root@Leon-redhat root]# tail /etc/passwd
qa:x:504:200::/home/qa:/bin/bash
guest:x:505:200::/home/guest:/bin/bash
test:x:506:506::/home/test:/bin/bash
LEONCDH$:x:508:100:LEONCDH:/dev/null:/bin/false
winner$:x:509:100::/dev/null:/bin/false
nfs001:x:510:200::/home/nfs001:/bin/bash
nfs002:x:511:200::/home/nfs002:/bin/bash
nfs003:x:512:200::/home/nfs003:/bin/bash
carolhsu:x:513:200::/home/carolhsu:/bin/bash
bady:x:514:514::/home/bady:/bin/bash
[root@Leon-redhat root]#
```

If you change the permission Read/Write to Read-Only for “192.168.120.198” host, you can mount this share resource but you don’t have write permission in the mount point.

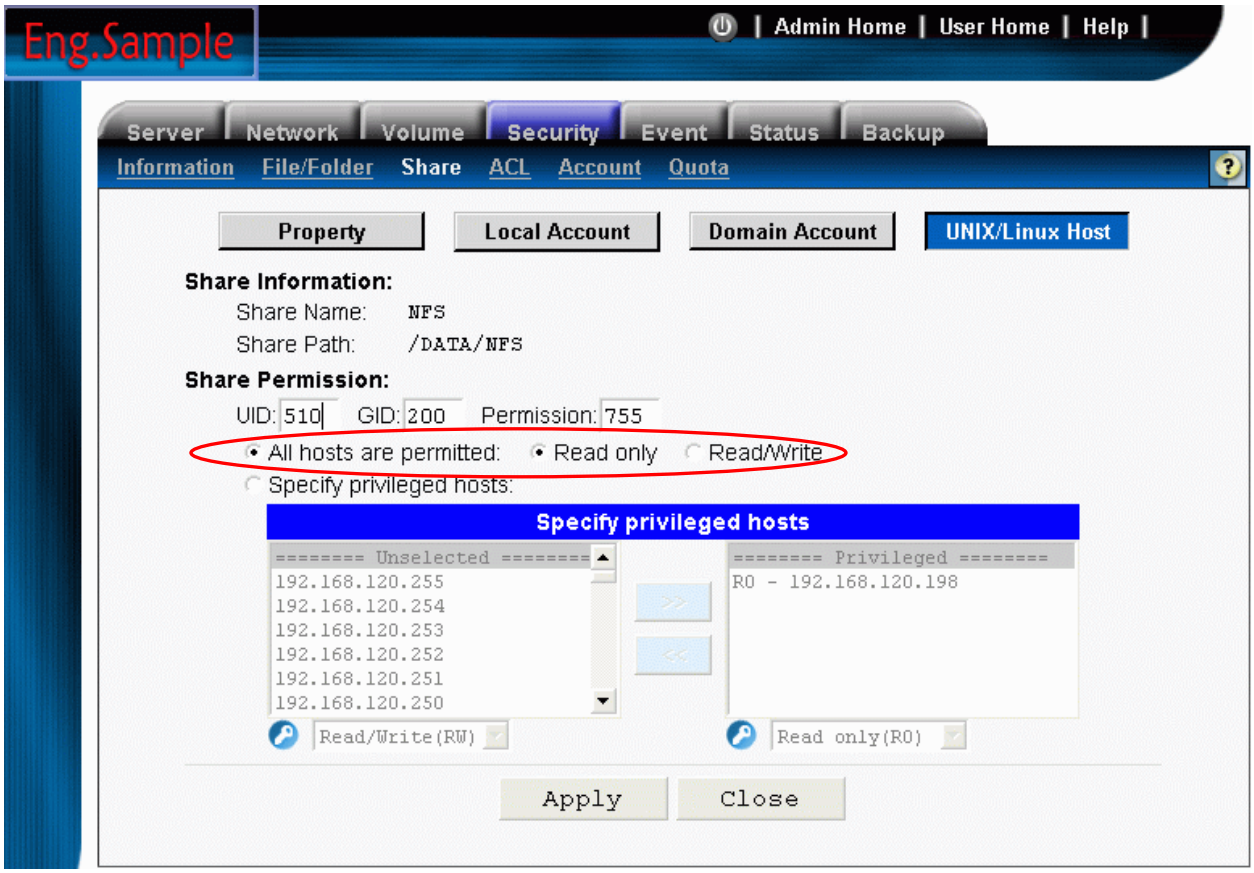


This host has Read-Only permission for the share resource point from NAStorage and can’t create file/folder in the mount point.

```
[root@Leon-redhat root]# showmount -e 203.67.163.92
Export list for 203.67.163.92:
/NFS (everyone)
/SMB (everyone)
[root@Leon-redhat root]# mount 203.67.163.92:/NFS /root/nastorage/
[root@Leon-redhat root]# ls -l
total 28
-rw-r--r--    1 root     root         1121 Jun 25 17:26 anaconda-ks.cfg
drwxr-xr-x    2 root     root         4096 Jul 11 15:23 autosave
drwx------    3 root     root         4096 Jul 11 18:21 Desktop
drwxr-xr-x    2 root     root           48 Jul 12 14:46 nastorage
drwx------    2 root     root         4096 Jul  3 14:04 nsmail
drwx--x--x    2 root     root         4096 Jul  4 10:06 Picture
drwxrwxr-x    3 root     root         4096 Jun 26 11:31 profile
[root@Leon-redhat root]# cd nastorage/
[root@Leon-redhat nastorage]# mkdir test
mkdir: cannot create directory `test': Permission denied
[root@Leon-redhat nastorage]# rm -rf tmp
rm: cannot remove directory `tmp': Permission denied
[root@Leon-redhat nastorage]#
```

Share Permission: All hosts are permitted

NAStorage will allow set permission (Read-Only/Read-Write) for all hosts, that means if someone wants to share a share resource for all host and assign all host Read-Only/Read-Write permission in NFS environment, just select **"All host are permitted"** and assign **"Read-Only/Read-Write"** permission.

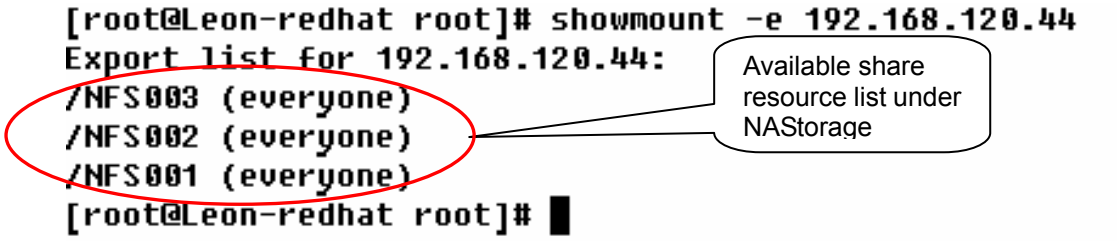


5. For NFS client to access data from NAStorage

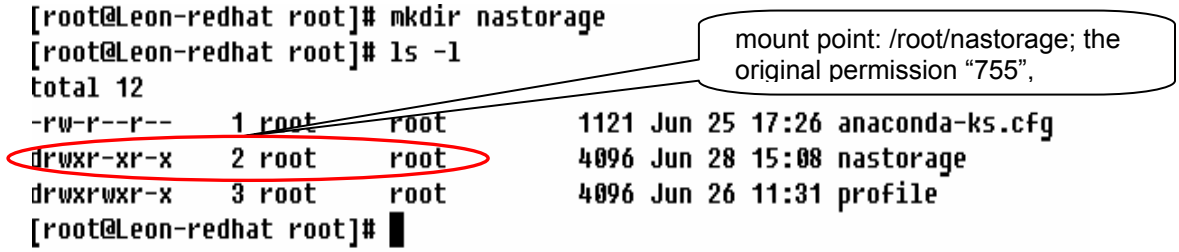
In UNIX-like network environment, we could use **"mount"** command mounting a share resource from NAStorage. (For example, the IP address of NAStorage is 192.168.120.44)

First of all, login UNIX/Linux host in Root permission, because only root user can use **"mount"** command.

Use "**showmount"** command to list the available share resource under NAStorage

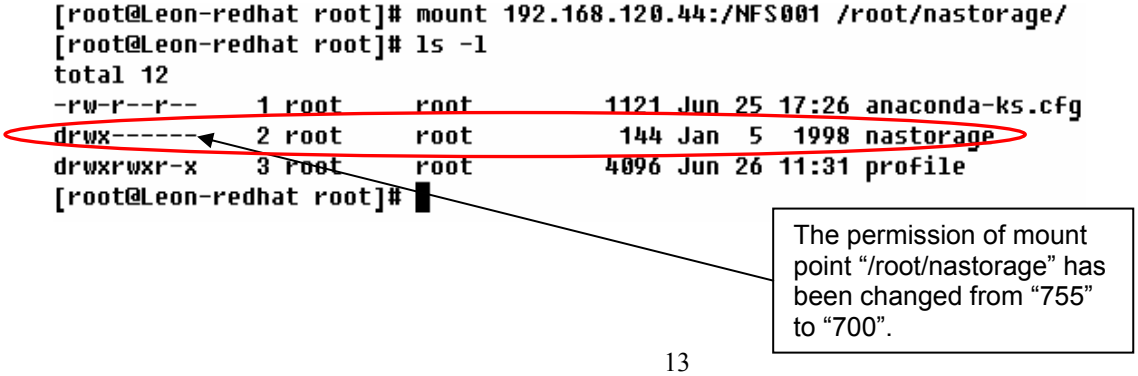


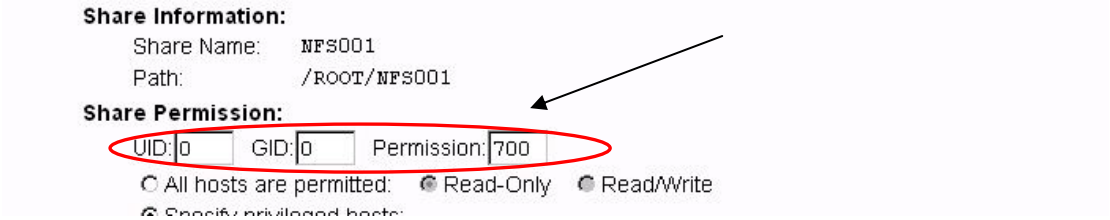
Make an empty directory /nastorage as a mounting point under /root directory.



Use mount command mounting **/NFS001** to mounting point **/root/nastorage.** Please make sure the case sensitive of the share resource, because **"NFS001"** was totally different with **"nfs001"** in NFS file system.

- The permission (Owner – User & Group, and access right – rwx rwx rwx) configured in NAStorage web admin page will be set as the default permission of mount point while NFS client mounts it.





Change to directory **/nastorage** and use **ls** command to see the contents. You will find the contents of /NFS001 already be mounted under /root/nastorage

```
[root@Leon-redhat root]# cd nastorage/
[root@Leon-redhat nastorage]# ls -l
total 524
-rwx------    1 leonhsu  leonhsu    512784 Jan  5  1998 dialer.exe
-rwxrwxrwx    1 root     root        11536 Jan  5  1998 htrn_jis.dll
-rwxrwxrwx    1 root     root         6416 Jan  5  1998 hypertrm.exe
[root@Leon-redhat nastorage]#
```

Use **mount** command to check the all mounting point of this local machine.

```
[root@Leon-redhat nastorage]# mount
/dev/hda2 on / type ext3 (rw)
none on /proc type proc (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
/dev/hda1 on /boot type ext3 (rw)
none on /dev/pts type devpts (rw,gid=5,mode=620)
none on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
192.168.120.44:/NFS001 on /root/nastorage type nfs (rw,addr=192.168.120.44)
[root@Leon-redhat nastorage]#
```

Use UNIX command: “chmod” & “chown” to change file/folder permission

```
[root@Leon-redhat nastorage]# chmod 700 dialer.exe
[root@Leon-redhat nastorage]# chown leonhsu:leonhsu dialer.exe
[root@Leon-redhat nastorage]# ls -l
total 524
-rwx------    1 leonhsu  leonhsu    512784 Jan  5  1998 dialer.exe
-rwxrwxrwx    1 root     root        11536 Jan  5  1998 htrn_jis.dll
-rwxrwxrwx    1 root     root         6416 Jan  5  1998 hypertrm.exe
[root@Leon-redhat nastorage]#
```

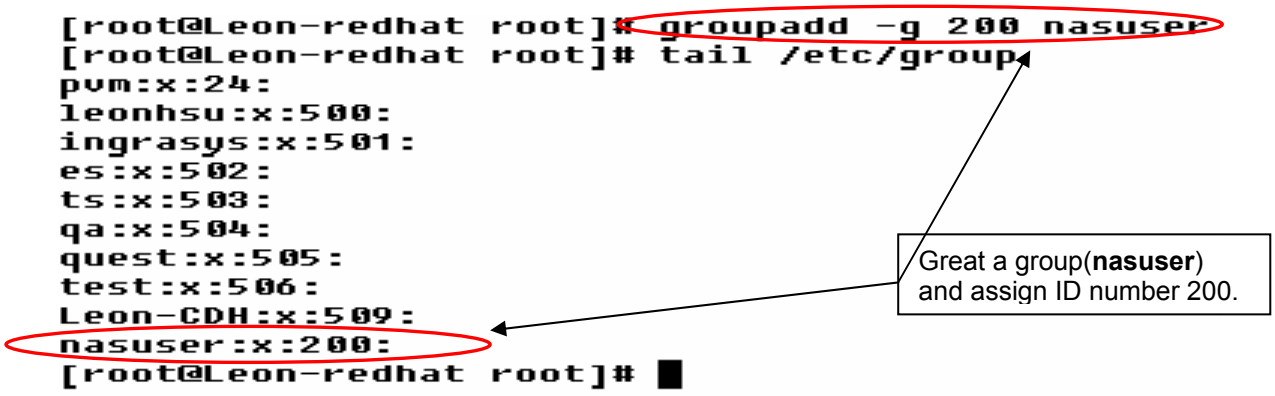
Un-mount volume from NAStorage.

```
[root@Leon-redhat root]# umount  nastorage/
[root@Leon-redhat root]# mount
/dev/hda2 on / type ext3 (rw)
none on /proc type proc (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
/dev/hda1 on /boot type ext3 (rw)
none on /dev/pts type devpts (rw,gid=5,mode=620)
none on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
[root@Leon-redhat root]#
```

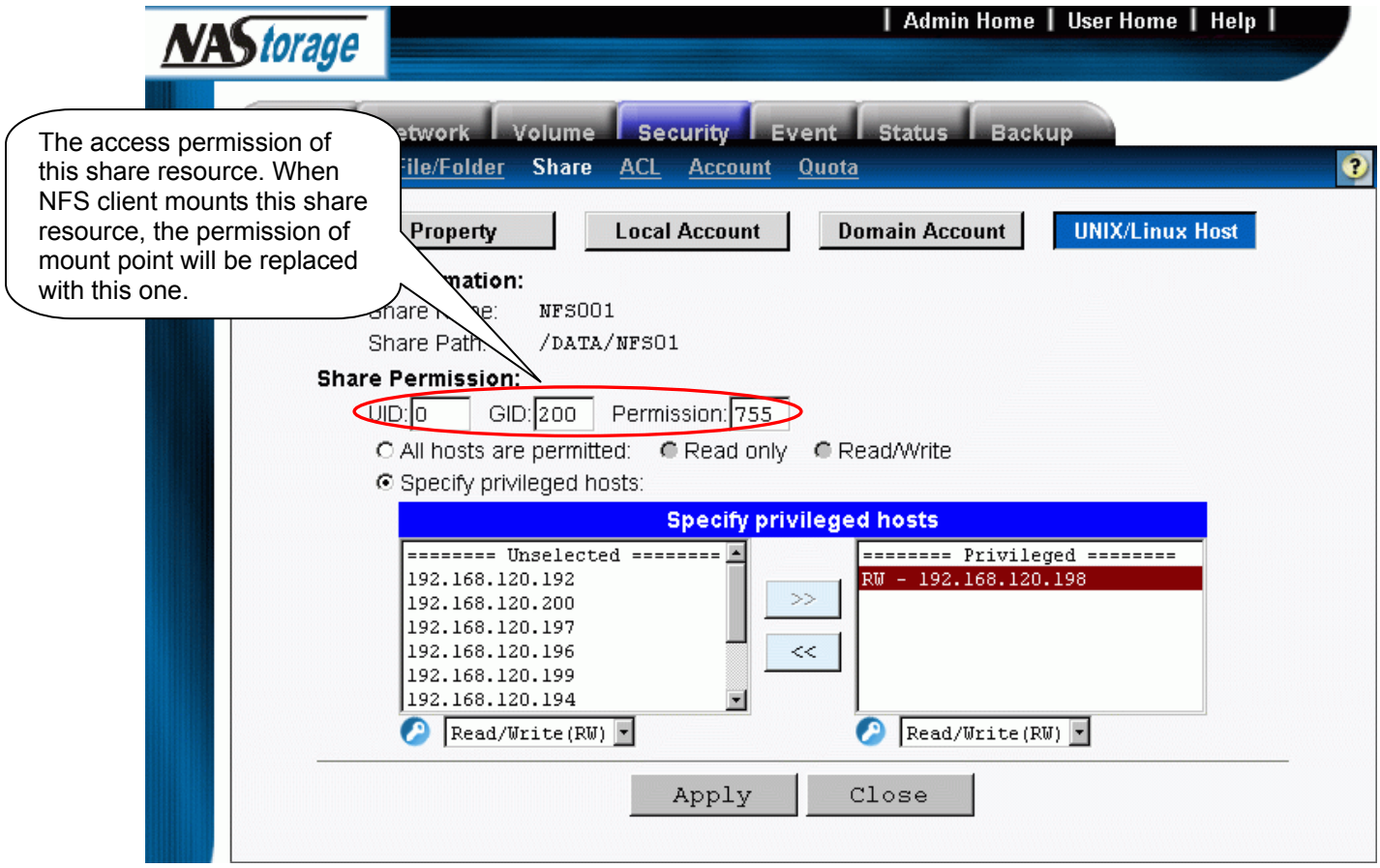
6. Multiple UIDs on a particular IP for read/write access to a share resource.

In our NAStorage (NFS environment) design, we just assign UID, GID and Access right to the mounting directory as its default permission. If you want give multiple UIDs has read/write access right, it should be handle by UNIX/Linux machine, not by NAStorage. But anyway, we still make an example for you if you went reach the purpose.

First of all, login UNIX/Linux host in Root permission, create a group **"nasuser".** You can check this new group'ID (GID) by checking file **/etc/group.**



Then flied it to NAStorage as below picture. If group **"nasuser"** ID is **200**, type GID **"200"** and change the default permission 755 to 775,that means this group has read/write permission (group attribute=7) to access share resource.



Use **mount** command mounting a share resource from NAStorage to mounting point /root/nastorage in Unix host. Basically, you will see the permission of the mounting point is 775, UID root , GID nasuser.

```
[root@Leon-redhat root]# mount 203.67.163.92:/NFS /root/nastorage/
[root@Leon-redhat root]# ls -l
total 20
-rw-r--r--    1 root     root         1121 Jun 25 17:26 anaconda-ks.c
drwxrwxr-x    2 root     nasuser        48 Jul  4 11:14 nastorage
drwx------    2 root     root         4096 Jul  3 14:04 nsmail
drwx--x--x    2 root     root
drwxrwxr-x    3 root     root         4096
[root@Leon-redhat root]#
```

The permission of mount point "/root/nastorage" has been changed from "755" to "775". UID root/0 , GID nasuser/200.

In UNIX host , You can assign the multiple UIDs (base on you want) to GID **"nasuser"** that mean these UIDs can read/write access to this volume. Because the second bit already change to 7 (755 to 775).

```
[root@Leon-redhat root]# useradd -g nasuser nfs001
[root@Leon-redhat root]# useradd -g nasuser nfs002
[root@Leon-redhat root]# useradd -g nasuser nfs003
[root@Leon-redhat root]# tail /etc/passwd
es:x:502:502::/home/es:/bin/bash
ts:x:503:503::/home/ts:/bin/bash
qa:x:504:504::/home/qa:/bin/bash
quest:x:505:505::/home/quest:/bi
test:x:506:506::/home/test:/bin/
LEONCDH$:x:508:100:LEONCDH:/dev/null:/bin/false
winner$:x:509:100::/dev/null:/bin/false
nfs001:x:510:200::/home/nfs001:/bin/bash
nfs002:x:511:200::/home/nfs002:/bin/bash
nfs003:x:512:200::/home/nfs003:/bin/bash
[root@Leon-redhat root]#
```

Create user (nfs001、nfs002、nfs003) and assign them into "nasuser" group.

Login UNIX/Linux host in these UIDs permission. for example **"nfs001"** user. You will find the contents of **/NFS** already be mounted under **/root/nastorage** with UID **"root"** GID **"nasuser"** **"775"** permission. That means you have Read/Write permission to access share resource, because you were belong to **"nasuser"** group.

```
[nfs001@Leon-redhat root]$ ls -l
total 28
-rw-r--r--    1 root     root         1121 Jun 25 17:26 anaconda-ks.cfg
drwxr-xr-x    2 root     root         4096 Jul 11 15:23 autosave
drwx------    3 root     root         4096 Jul 11 18:21 Desktop
drwxrwxr-x    3 root     nasuser        72 Jul 12 15:34 nastorage
drwx------    2 root     root         4096 Jul  3 14:04 nsmail
drwx--x--x    2 root     root         4096 Jul  4 10:06 Picture
drwxrwxr-x    3 root     root         4096 Jun 26 11:31 profile
[nfs001@Leon-redhat root]$ cd nastorage/
[nfs001@Leon-redhat nastorage]$ mkdir tmp
[nfs001@Leon-redhat nastorage]$ ls -l
total 8
drwxr-xr-x    2 nfs001   nasuser        48 Jul 12 15:34 test
drwxr-xr-x    2 nfs001   nasuser        48 Jul 12 15:51 tmp
[nfs001@Leon-redhat nastorage]$
```

User "nfs001" can Read/Write for this mount point and the create file belong to user "nfs001".