Openfiler Lab 2: Configuring NAS Shares

References

[1] Openfiler Overview: `http://www.openfiler.com/products`
[2] Openfiler Architecture: `http://www.openfiler.com/products/openfiler-architecture`
[3] Openfiler Feature Summary: `http://www.openfiler.com/products/feature-summary/feature-summary`

Background

Openfiler is a flexible, open source enterprise storage solution with support for a variety of common, industry standard access protocols. Because it is based on the Linux operating system, Openfiler can be run on most modern hardware without issue. Openfiler supports client access to storage at both the file and block levels. At the file level, Openfiler can export storage using such network-attached storage (NAS) protocols as NFS and CIFS, among others. Openfiler supports iSCSI and Fibre Channel storage area network (SAN) protocols for block level data access [1]. For a more detailed discussion of the Openfiler architecture, refer to the Openfiler website [2].
In order to simplify deployment, Openfiler provides a powerful web-based GUI to configure and control its various services. The GUI includes support for managing storage, shares, user accounts, quotas, and network protocols such as NFS and CIFS. Ideally, users should be able to configure Openfiler to meet their needs without ever running a single Linux command or editing a configuration file by hand [3].

Objectives

Upon completing this lab, students should understand how to use Openfiler to accomplish the following tasks:

- Configure access control for NAS services
- Configure NFS shares and start the NFS service
- Configure Linux clients for access to NFS shares
- Configure CIFS shares and start the CIFS service
- Configure Windows clients for access to CIFS shares

Note: Openfiler Lab 1: Storage & Authentication Configuration is a prerequisite for this lab and should be completed before continuing further.

Procedures

Follow the steps below to perform the lab. Take a screenshot or screenshots where noted in red to demonstrate successful completion. Also, there are questions throughout the lab that you are required to answer. Please take time to think about your response as these questions are weighted heavily in the grading rubric.

Note: IP addresses used in the lab are from network **192.168.255.0/24**. Addresses used in instruction need to be modified appropriately.

Part 1: Configuring NFS for Linux Client Access

NFS is a common NAS protocol used primarily with Linux-based operating systems. In this part of the lab you will configure Openfiler as an NFS server. You will also configure an access control list (ACL) to control access to the NFS share. NFS access will be tested with a Linux client.

Task 1: Openfiler NFS

Step 1: Create NFS Network ACL - Screenshot(s) 6.66%

Open a web browser on the Windows host and connect to the Openfiler web interface at `https://192.168.255.100:446/`, then login with the username **`openfiler`** and the password **`password`**.

Click `System` in the top menu bar. From this menu you can manage various components of the Openfiler server. You will first create an ACL to control client access to NFS.

Scroll down to the `Network Access Configuration` section. Enter **`NFS`** as the `Name` of the ACL, enter **`192.168.240.0`** as the `Network/Host`, select **`255.255.255.0`** as the `Netmask`, and select **`Share`** as the `Type`. Click `Update`. You will be presented with the screen in Figure 1.

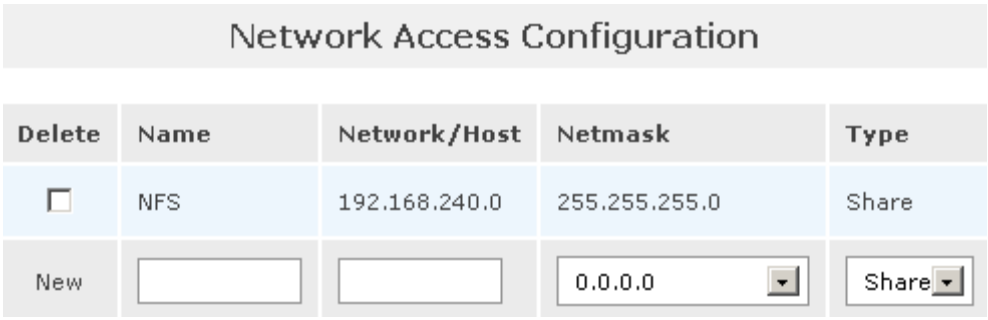

Figure 1. NFS Network ACL

Step 2: Create NFS Share - Screenshot(s) 6.66%

Click `Shares` in the top menu bar. From this menu you can create and configure NAS and SAN shares. Under the `Network Shares` section, click the `Used for file access LVM`. In the box that appears, enter **`NFS`** as the `Folder Name` and click `Create Sub-folder`. Click the newly created subfolder `NFS` and click `Make Share` in the box that appears. You will be taken to a page that provides configuration options for the `NFS` share.

Scroll down to the `Share Access Control Mode` section. Select the radio button for `Public guest access`, and click `Update`. Scroll down to the `Host access configuration` section, and select the `RW` radio button in the `NFS` column. Click `Edit` under `NFS Options`, and select **`root_squash`** as the `UID/GID Mapping`. Click `Update`. You will be presented with the screen in Figure 2.

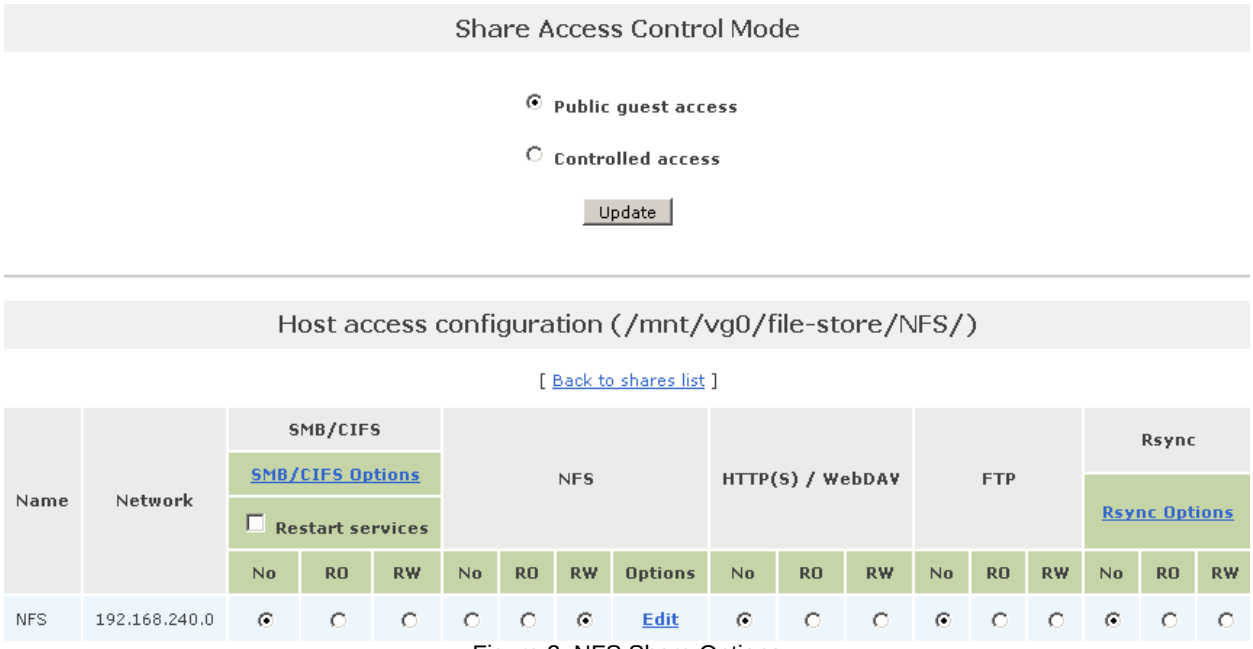

Figure 2. NFS Share Options

Question 1: What is the significance of the NFS **`root_squash`** option? What are the advantages of setting the option? - **20%**

Note: The Public guest access option removes the requirement for users to authenticate with a username and password. Access to the share is still controlled by an ACL. The ACL with the same name as the share is applied.

Step 3: Start NFS Service - Screenshot(s) 6.66%

Click Services in the top menu bar. From this menu you can enable and disable the various services that Openfiler uses. You will use this menu to enable the NFS server.

Under the Manage Services section, click Enable next to NFSv3 server. The page will reload, and you will see that the NFS server has been enabled.

Task 2: Linux Client Access

Step 1: Test NFS Access - Screenshot(s) 6.66%

Login to the Linux host as a **root** (or use sudo command)

In order to test access to the Openfiler NFS share, run the following commands:

```
[root@localhost ~]# mkdir /mnt/NFS
[root@localhost ~]# mount 192.168.240.100://mnt/vg0/file-store/NFS /mnt/NFS
[root@localhost ~]# echo "Hello world" > /mnt/NFS/testfile
[root@localhost ~]# ls -l /mnt/NFS
total 8
-rw-rw-rw-+ 1 hsqldb hsqldb 12 May 3 2010 testfile
```

Note: If you wish to investigate further, you may use the getfacl command to view extended permissions on the NFS share. Experiment with creating files as different users and note how the permissions change.

Step 2: Make Mount Point Persistent - Screenshot(s) 6.66%

Using the text editor of your choice, add the following line to the /etc/fstab file on the Linux host in order to make the NFS share persistent across reboots:

```
192.168.240.100://mnt/vg0/file-store/NFS /mnt/NFS nfs defaults 0 0
```

Run the following commands to unmount the NFS share and remount it using the specifications from /etc/fstab:

```
[root@localhost ~]# umount /mnt/NFS
[root@localhost ~]# mount -a
[root@localhost ~]# mount
<Output Omitted>
192.168.240.100://mnt/vg0/file-store/NFS on /mnt/NFS type nfs
(rw,addr=192.168.240.100)
```

Part 2: Configuring CIFS for Windows Client Access

CIFS is a common NAS protocol used primarily with Windows operating systems. In this part of the lab you will configure Openfiler as a CIFS server and use LDAP for user authentication. You will also configure an ACL to control access to the CIFS share. CIFS access will be tested with a Windows client.

Task 1: Openfiler CIFS

Step 1: Create CIFS Network ACL - Screenshot(s) 6.66%

Click System in the top menu bar. From this menu you can manage various components of the Openfiler server. You will first create an ACL to control client access to CIFS.

Scroll down to the Network Access Configuration section. Enter **CIFS** as the Name of the ACL, enter **192.168.240.0** as the Network/Host, select **255.255.255.0** as the Netmask, and select **Share** as the Type. Click Update. You will be presented with the screen in Figure 3.

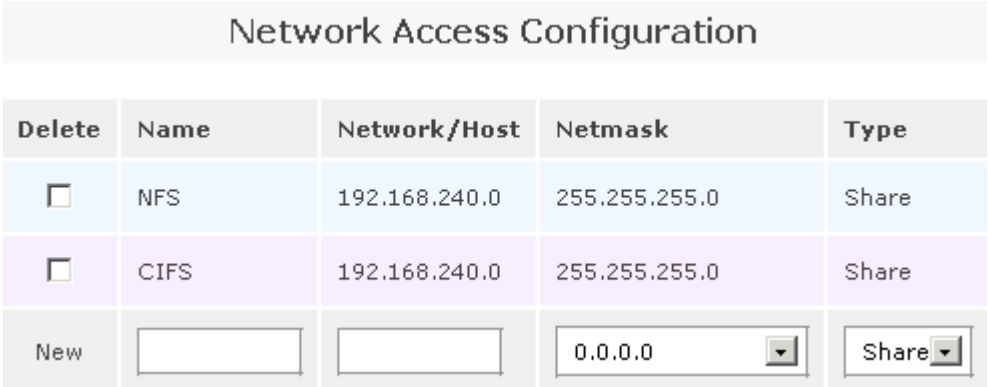

Figure 3. CIFS Network ACL

Step 2: Create CIFS Share - Screenshot(s) 6.66%

Click Shares in the top menu bar. From this menu you can create and configure NAS and SAN shares. Under the Network Shares section, click the Used for file access LVM. In the box that appears, enter **CIFS** as the Folder Name and click Create Sub-folder. Click the newly created subfolder CIFS and click Make Share in the box that appears. You will be taken to a page that provides configuration options for the CIFS share.

Under the Edit share section, enter **CIFS** in the Override SMB/Rsync share name box and click Change. Scroll down to the Group access configuration section. For the admins group, select the radio buttons for PG and for RW, and for the users group select the radio button for RO. Click Update. Scroll down to the Host access configuration section, and select the RW radio button in the SMB/CIFS column and CIFS row. Click Update. You will be presented with the screen in Figures 4, 5, and 6.

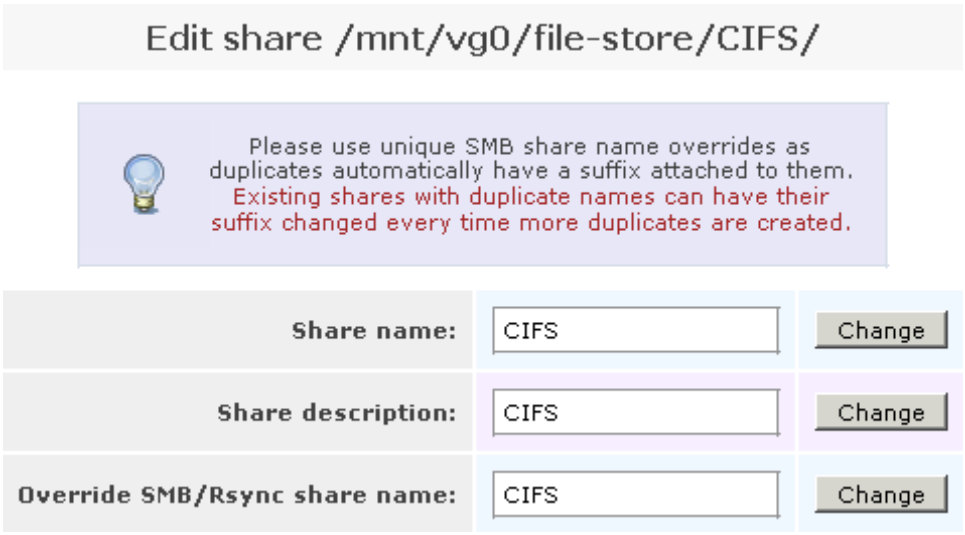

Figure 4. CIFS Share Name

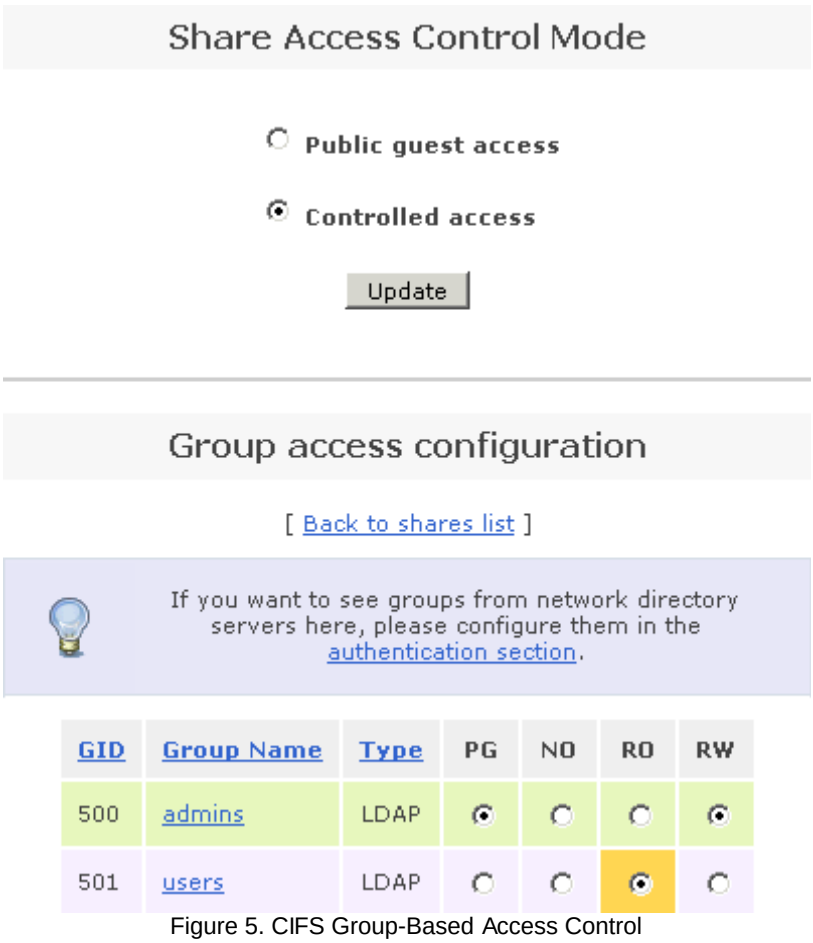

Figure 5. CIFS Group-Based Access Control

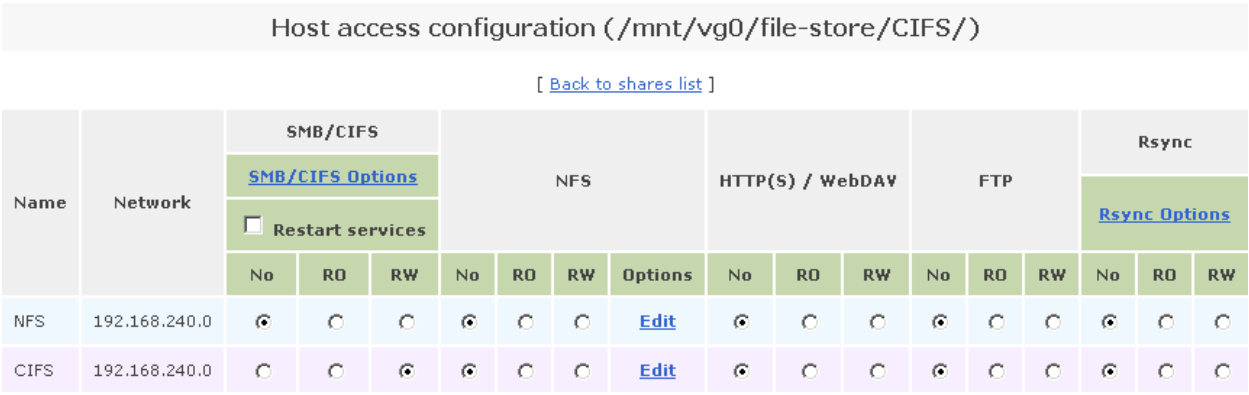

Figure 6. CIFS Network-Based Access Control

Question 2: Click `SMB/CIFS Options` under the `Host access configuration` section. What does the `Browseable` option control? - **20%**

Note: The `Controlled access` option enforces user and group-based authentication, in this case via LDAP. Access to the share is also controlled by an ACL. The ACL with the same name as the share is applied.

Step 3: Start CIFS Service - Screenshot(s) 6.66%

Click `Services` in the top menu bar. From this menu you can enable and disable the various services that Openfiler uses. You will use this menu to enable the CIFS server.

Under the `Manage Services` section, click `Enable` next to `SMB / CIFS server`. The page will reload, and you will see that the CIFS server has been enabled.

Task 2: Windows Client Access

Step 1: Test Access & Mount CIFS Share - Screenshot(s) 6.66%

Click the `Start Menu` on your Windows host and select `My Computer`. In the `My Computer` window, click the `Tools` menu, and click `Map Network Drive`. Enter **`\\192.168.240.100\CIFS`** as the `Folder`, click `Finish`, and login as username **`admin1`** with password **`ISMlab`** when prompted.

The **`CIFS`** share should now be mounted on the Windows host.

Note: If you wish to investigate further, you may experiment with mounting the CIFS share as different users. Refer to Openfiler Lab 1: Storage & Authentication Configuration for a list of available users. Notice that the **`admin1`** and **`admin2`** users have read/write access to the CIFS share, while the **`user1`** and **`user2`** users may only read.