Openfiler Lab 1: Storage & Authentication Configuration

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:

- Partition locally attached storage
- Create a RAID array
- Create logical volumes using LVM
- Configure local LDAP authentication
- Create local LDAP users and groups

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 Openfiler Storage

A crucial step in setting up an Openfiler system is configuring the locally attached storage hardware. In this part of the lab, you will create a RAID-5 array out of four physical hard disks, which you will then use to create a volume group with two logical volumes. These logical volumes will be used in future labs with NAS and SAN protocols to provide storage for client systems.

Task 1: Software RAID

Step 1: Create RAID Partitions - Screenshot(s) 7.5%

Open a web browser on the Windows host and connect to the Openfiler web interface at `https://192.168.240.100:446/`, then login with the username "**`openfiler`**" and the password "**`password`**".

Click `Volumes` in the top menu bar. From this menu you can configure the physical storage attached to the Openfiler host. You will first create RAID partitions on the connected hard disks.

Under the `Volumes section` menu, click `Block Devices`. You will be presented with the screen in Figure 1. **DO NOT MODIFY `/dev/sda`, as the Openfiler operating system is installed on that disk.**

Block Device Management

Edit Disk	Type	Description	Size	Label type	Partitions
/dev/sda	SCSI	VMware, VMware Virtual S	2.19 GB	msdos	1 (view)
/dev/sdb	SCSI	VMware, VMware Virtual S	4.00 GB	gpt	0 (view)
/dev/sdc	SCSI	VMware, VMware Virtual S	4.00 GB	gpt	0 (view)
/dev/sdd	SCSI	VMware, VMware Virtual S	4.00 GB	gpt	0 (view)
/dev/sde	SCSI	VMware, VMware Virtual S	4.00 GB	gpt	0 (view)

Figure 1. Block Device Management

Click on `/dev/sdb` under `Edit Disk`. On the following screen, scroll down to the `Create a partition in /dev/sdb` section. Change the `Partition Type` option to **`RAID array member`**, and click `Create`. You will be presented with the screen in Figure 2.

Device	Type	Number	Start cyl	End cyl	Blocks	Size	Type	Delete
/dev/sdb1	Linux RAID Array Member (0xfd)	1	1	522	4191924	4.00 GB	Primary	Delete

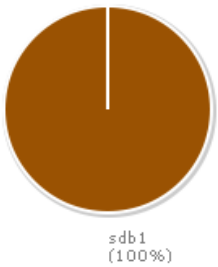


Figure 2. Partition List for `/dev/sdb`

Under the `Volumes section` menu, click `Block Devices`, and then repeat the previous step for each of the other three drives without partitions. When finished, you should see that all the drives are listed with one partition.

Step 2: Create RAID-5 Array - Screenshot(s) 7.5%

Under the `Volumes section` menu, click `Software RAID`. From here you can create and manage RAID arrays in software.

Scroll down to the `Create a new RAID array` section. Change the `Select RAID array type` box to **`RAID-5 (parity)`**, then check the boxes under the `X` column next to all four drives. Select the `Spare` radio button for `/dev/sde1`. When you are finished, your screen will look like Figure 3.

Select RAID array type				Select chunk size
RAID-5 (parity)				64 kB
Select RAID devices to add				
X	Device	Size	Member	Spare
☑	/dev/sdb1	4.00 GB	◉	○
☑	/dev/sdc1	4.00 GB	◉	○
☑	/dev/sdd1	4.00 GB	◉	○
☑	/dev/sde1	4.00 GB	○	◉
Add array				

Figure 3. RAID Array Creation

Click `Add array` to create the RAID array. The `Software RAID` screen will display progress synchronizing the new RAID array. When synchronization is complete, you will be presented with the screen in Figure 4. You may have to refresh your web browser.

Software RAID Management

Array	Level	Array Size	Device Size	State	Synchronization	Manage	Add	Used In	Delete
/dev/md0	RAID-5	8.00 GB	4.00 GB	Clean	Synchronized	View members	*All RAID partitions are used*	*Unknown / unused*	Delete

Figure 4. Software RAID Management

Question 1: How does RAID-5 differ from RAID-6? What are the main advantages and disadvantages of each? - **20%**

Task 2: Storage Volumes

Step 1: Create Volume Group - Screenshot(s) 7.5%
Under the `Volumes section` menu, click `Volume Groups`. From here you can create and manage volume groups.
Scroll down to the `Create a new volume group` section. Enter **`vg0`** as the `Volume group name`, and check the box next to `/dev/md0` under `Select physical volumes to add`. Click `Add volume group`. You will be presented with the screen in Figure 5.

Volume Group Management

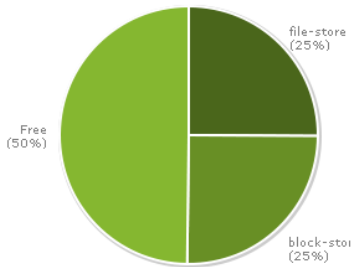
Volume Group Name	Size	Allocated	Free	Members	Add physical storage	Delete VG
vg0	7.97 GB	0 bytes	7.97 GB	View member PVs	*All PVs are used*	Delete

Figure 5. Volume Group Management

Step 2: Create Logical Volumes - Screenshot(s) 7.5%
Under the `Volumes section` menu, click `Add Volume`. From here you can create and manage logical volumes.
Scroll down to the `Create a volume in "vg0"` section. Enter **`file-store`** as the `Volume Name`, enter **`Used for file access`** as the `Volume Description`, enter **`2048`** in the `Required Space`

(MB) field, and select **XFS** as the Filesystem / Volume Type. Click Create. You will be taken to the Manage Volumes page.
Under the Volumes section menu, click Add Volume. Create another volume, entering **block-store** as the Volume Name, then entering **Used for block access** as the Volume Description, then entering **2048** in the Required Space (MB) field, and finally selecting **iSCSI** as the Filesystem / Volume Type. Click Create. You will be presented with the screen in Figure 6.

Volumes in volume group "vg0" (8160 MB)



Volume name	Volume description	Volume size	File system type	File system size	FS used space	FS free space	Delete	Properties	Snapshots
file-store	Used for file access	2048 MB	XFS	2.0G	4.3M	2.0G	Delete	Edit	Create
block-store	Used for block access	2048 MB	iSCSI	Not applicable	Not applicable	Not applicable	Delete	Edit	Create
0 MB allocated to snapshots									
4064 MB of free space left									

Figure 6. Volumes in "vg0"

Part 2: Configuring Openfiler Authentication

Restricting access to storage is important in a networked environment. In this part of the lab, you will enable and configure Openfiler's local LDAP server to allow for user-based authentication. You will also create several users and groups. This framework will be used in a future lab to authenticate users for a CIFS share.

Task 1: LDAP Authentication

Step 1: Enable Local LDAP Server - Screenshot(s) 7.5%

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

Step 2: Configure LDAP Server - Screenshot(s) 7.5%

Click Accounts in the top menu bar. From this menu you can administer LDAP and Active Directory for user authentication, and create and manage users and groups. You will first configure the local LDAP server.
Under the User Information Configuration section, check the box next to Use LDAP. Enter the following settings to configure the local LDAP server:

Local LDAP server: Use Local LDAP Server
LDAP Security: Use TLS
Server: **127.0.0.1**
Base DN: **dc=exampl,dc=com**
Root bind DN: **cn=openfiler,dc=example,dc=com**
Root bind password: **ISMlab**
SMB LDAP Configuration: Login SMB server to root DN
User password policy: Allow user to change password

Click `Submit` near the bottom of the page. When the page reloads, wait about one minute, then click `Administration` under the `Accounts section` menu. You will be presented with the screen in Figure 7, indicating that the local LDAP server was started and configured properly.

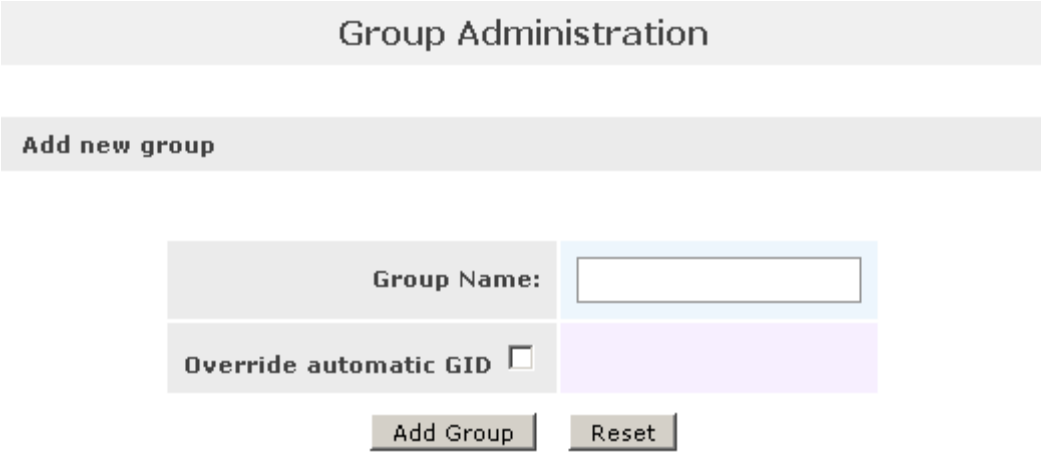


Figure 7. Successful LDAP Configuration

Question 2: What are some of the advantages of using LDAP or Active Directory authentication for Openfiler instead of local authentication? - **20%**

Note: If you receive the `ldap_bind: Invalid Credentials (49)` error as in Figure 8 when attempting to access the `Administration` page, then perform the following steps to solve the problem. Otherwise, continue on to Task 2: Users & Groups.

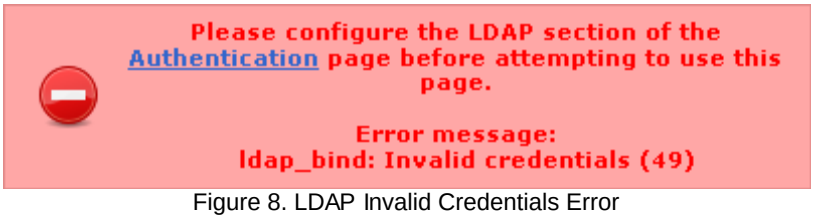


Figure 8. LDAP Invalid Credentials Error

Click `Services` in the top menu bar. Under the `Services section` menu, click `LDAP Setup`. Scroll down to the `Clear LDAP directory` option, and click `Clear LDAP`. On the next page, click `Yes` to confirm that you wish to clear the LDAP configuration. Repeat Step 2: Configure LDAP Server and the error will not appear.

Task 2: Users & Groups

Step 1: Create Groups - Screenshot(s) 7.5%

Ensure that you are on the `Administration` page after successfully configuring the local LDAP server. Under the `Group Administration` section, add a new group by entering **`admins`** for the `Group Name` and clicking `Add Group`. Add another group by entering **`users`** for the `Group Name` and clicking `Add Group`. You will be presented with the screen in Figure 9.

Figure 9. Group Control

Step 2: Create Users - Screenshot(s) 7.5%

Click the `User Administration` tab. Using the `Add new user` form, add the following users:

Username: **admin1**
Password: **ISMlab**
Retype password: **ISMlab**
Primary Group: **500: admins**
Override automatic UID:
Username: **admin2**
Password: **ISMlab**
Retype password: **ISMlab**
Primary Group: **500: admins**
Override automatic UID:
Username: **user1**
Password: **ISMlab**
Retype password: **ISMlab**
Primary Group: **501: users**
Override automatic UID:
Username: **user2**
Password: **ISMlab**
Retype password: **ISMlab**
Primary Group: **501: users**
Override automatic UID:

Click Add User after entering the information for each user. When finished, you will be presented with the screen in Figure 10.

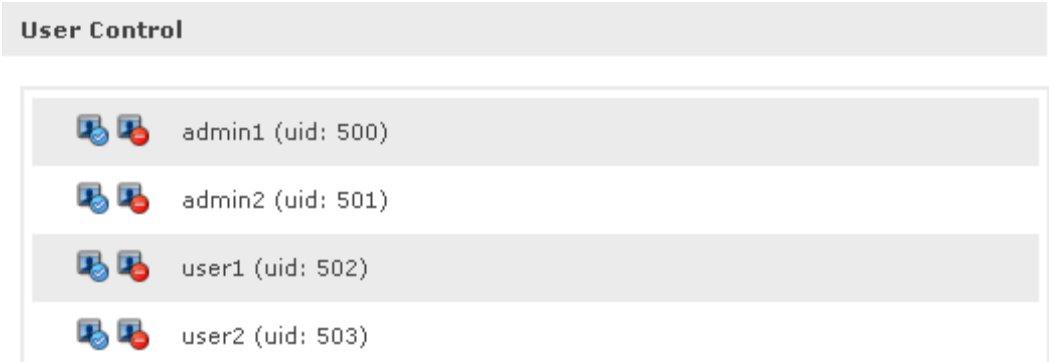


Figure 10. User Control