



45HomeLab
A Division of 45Drives

HL15 - STORAGE SERVER USER MANUAL



REVISION DETAILS

Version	Description
1.0	Initial published version
1.1	<ul style="list-style-type: none">- Changes made to update the unboxing images and racking.- Added network configuration from the desktop UI- Changed the login details that were incorrect- Re-ordered the software section

Contents

GETTING STARTED	6
ABOUT US	6
WHY 45HOMELAB HL15	6
HARDWARE	7
COMPONENTS AND SPECIFICATIONS	7
INITIAL SETUP	9
UNBOXING THE HL15	9
RACKING THE HL15	13
INSERTING THE STORAGE DRIVES	21
CABLE SETUP	22
Power requirements	23
45HOMELAB HL 15 INITIAL CABLING SETUP DIAGRAM	24
INITIAL CONFIGURATION /SETUP	25
NETWORK SETUP	25
USING THE DESKTOP UI	25
SETTING UP IPMI	29
SETTING THE NETWORKING USING NMTUI	31
Setting Static IP	33
Setting a Bond	36
HOUSTON LOGIN AND CONFIG	41
CREATING ZPOOL	42
CREATING ZFS FILESYSTEM/DATASET	44
CREATING YOUR SHARES	45
Samba/SMB shares	45
Setting up Local User Access SMB Shares	49
Set SMB permissions using local users and group	53
Connecting to SMB Share on Windows and MacOS	55
Connecting to SMB Share on Windows	55
Connecting to SMB Share on MacOS	57
Managing NFS in Houston UI	59
Mounting NFS Share to Linux Client	62
Add Mount on Reboot	63

Verify Share Mounted	63
Verify Mount on Reboot.....	64
SETUP ISCSI STORAGE.....	64
Configuring iSCSI Target.....	65
Create an iSCSI Target.....	66
Create iSCSI LUNs.....	67
Configure ACL (Initiator IQN)	67
Configure Authentication	67
Exit and Save the Configuration.....	67
Open Firewall for iSCSI and enable the iSCSI service	68
Verification /Connecting to the LUN.....	69
AUTOMATED ZFS REPLICATION/SNAPSHOTS IN HOUSTON UI	72
SOFTWARE	75
PORTAINER	75
INSTALLING NGINX PROXY MANAGER(NPM) ON PORTAINER.....	78
NEXTCLOUD AND NPM ON PORTAINER.....	81
CONFIGURING PLEX PORTAINER.....	86
IMMICH - self-hosted backup solution for photos and videos	96
Uploading Pictures	101
Explore Tab.....	101
Map Tab	101
Sharing Tab.....	101
Library	102
Mobile App.....	102
Administration.....	102
Server Status	104
CLI Commands.....	104
HOME ASSISTANT	105
Method 1 - Portainer deployment.....	105
Method 2 - Deploying in Rocky Terminal.....	106
WIREGUARD - fast, modern, and secure VPN tunnel.....	107
FRIGATE - open-source NVR built around real-time AI	109
docker-compose.....	109

Explanation of docker-compose.yml	110
Config.yml	111
Why is this file needed?	113
TROUBLESHOOTING	113
SERVER WONT POWER ON	113
HOUSTON UI IS NOT ACCESSIBLE	115
DRIVES ARE MISSING IN MY ZPOOL	115
ZPOOL IS IN A DEGRADED STATE.....	116
SAMBA SHARES ARE NOT ACCESSIBLE TO MOUNT	116
GETTING ACCESS DENIED WHEN ACCESSING THE FILES IN THE SHARE.....	116
HOW DO I UPDATE MY SERVER.....	116
45DRIVES DISK MODULE IS NOT WORKING s.....	117
SYSTEM WOULD NOT BOOT INTO THE OS.....	117

GETTING STARTED

Welcome to 45HomeLab community. We are so glad you chose us.

ABOUT US

Serving our customers well is at the core of everything we do at 45HomeLab. In an industry where technical support is strictly timed, automated and impersonal we are real people solving real storage problems. Our storage solutions are non-proprietary, giving you the freedom to run any software you choose.



OUR GOAL

Provide you with the best storage solution for your data needs - not the most expensive one. Today we provide the most affordable storage solutions in the industry.



OUR MISSION

To provide affordable open-source storage solutions while staying true to our community roots by giving back to the open-source community that we rely on.



OPEN DESIGN

Unlike mainstream data storage providers 45HomeLab maintains an open design and ongoing relationships with the open-source community.

WHY 45HOMELAB HL15

At 45HomeLab we know home labbers have a strong vision of the infrastructure they want, and how to build and configure it. A key pillar of a great home lab, is a sufficient storage that is customized and configured how you need it.

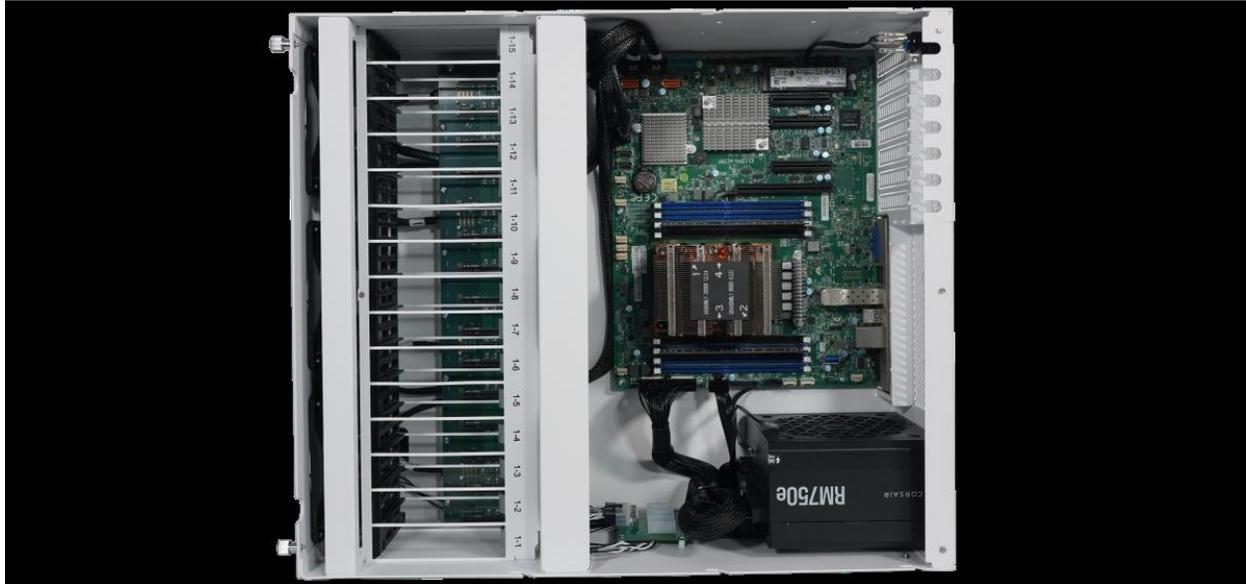
The problem is home storage offerings today are under powered and have locked down software, while enterprise solutions are just too big and expensive. We understand how frustrating this is, which is why we've created the 45HomeLab product line. It is big, strong, fast, while also being open and flexible so you can easily modify, upgrade, and repair it, all at a price that makes sense for a power home lab user.

Our new HL15 is a 15-bay server that was designed to provide the power and storage needed for a great home lab.

HARDWARE

COMPONENTS AND SPECIFICATIONS

Chassis Dimensions (LxWxH): 20" x 17" x 7"



Below are the components that will be in your HL15 if you have not requested for any modification in the order the below components will be present by default. Your CPU, motherboard, RAM, Boot drives etc. could change based on your customization.

ID	Component	Model - specs
1	Backplane	15HDD Backplane
2	Boot Storage	KINGSTON NV2 1TB Gen 4x4 NVMe M.2
3	Cables	miniSAS HD 0.6m
4	Cables	MiniSAS SFF-8087 to miniSAS HD SFF-8643 50cm
5	Chassis	HL15 Chassis
6	CPU	Xeon Bronze 3204
7	Fans	Cooler Guys 120mm Med Speed Fan
8	Heatsink	B8 2U Passive Cooler
9	Motherboard	X11SPH-nCTF – SFP+
10	Motherboard	X11SPH-nCTPE – RJ45
11	Networking	Copper transceiver (Optional with SFP+ Motherboard)
12	Networking	Fiber transceiver (Optional with SFP+ Motherboard)
13	NVME Riser Card	AOC-SLG3-2M2 – 2 Position M.2 NVMe Add on Card (Optional)
14	NVME Riser Card	AOC-SHG3-4M2P– 4 Position M.2 NVMe Add on Card (Optional)
15	Power Supply	Corsair RM750e (750W, 80 Plus Gold)
16	Rails	Sliding rails -26.5in -36.4in length (Optional)
17	RAM	16GB DDR4 ECC RDIMM (2x 8GB)
18	RAM	32GB DDR4 ECC RDIMM (2x 16GB)

INITIAL SETUP

UNBOXING THE HL15

- ⊕ Once you receive your new unit from shipping, inspect the box and make sure there isn't any shipping damage.



- ⊕ Put on protective gloves if needed and use a box cutter to open it.



- ⊕ Once the box is open you can take the unit out of the box.



- ⊕ Inside we can find another smaller box containing the accessories purchased with the server along with some paper documents.



- ⊕ Lay the new unit on a flat surface like a table and make one more inspection to make sure everything is in order. Lift the unit out of the box by the left and right side. Having a second person may help.



- ⊕ Remove foam padding and we are complete!



- ⊕ After the unboxing is complete you can move on to either racking the unit or placing the unit in its final destination with the provided rubber feet.
- ⊕ The Rubber feet can be screwed into the base of the system for desktop placement.

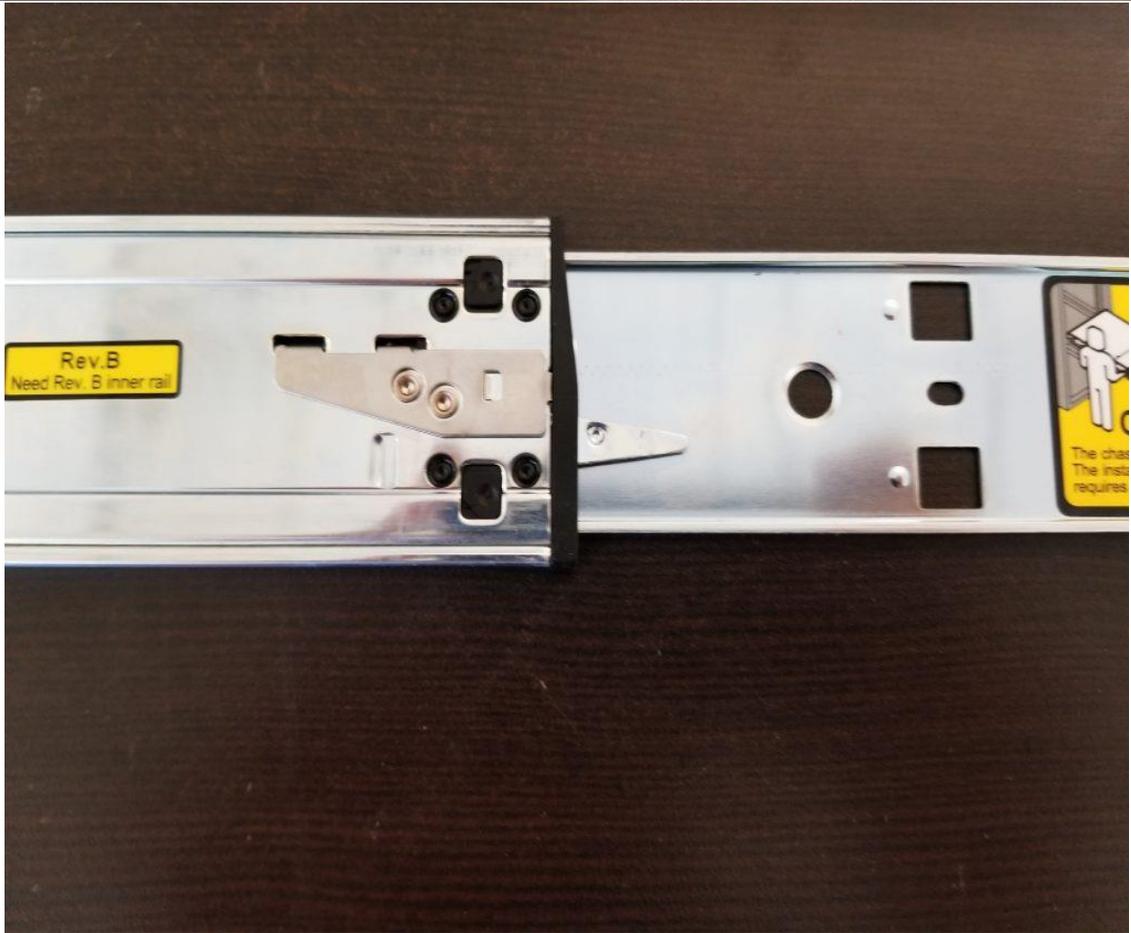


RACKING THE HL15

Note: Do not install the storage hard-drives before racking your new unit.

- ⊕ If you purchased rails with your new 45HomeLab unit or have supplied your own, you will be able to attach them to the sides of the unit.
- ⊕ Unbox the rails and disconnect the part that attaches to the unit. There should be a latch on the rail that allows the easy disconnection.







- ⊕ Locate the screws inside the included rail mount kit and screw the rails onto each side of the unit.



- ⊕ The rails only go one way so make sure you put them in correctly. The rails should have indicators on them to show which side and which side is up.



- ⊕ Screw the screws back in their respective places, holding the rail as you do this. (It may be easier if one person holds the rail and a second person screws them in.)



- Once the rails are attached to the side of the unit, you can install the other piece of the rail into the rack. Once again there are indicators showing which way needs to be up and which side is which.



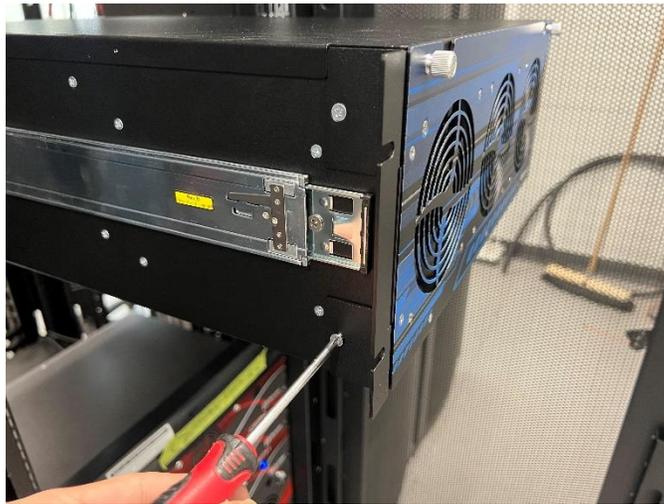
- ⊕ After both parts are installed, it is now time to connect them you have to align the sides perfectly.
- ⊕ Extend the rails on the rack to full length.



- ⊕ Pick up the unit with another person and align the sides of the rails on the rack with the sides of the 45HomeLab unit. Make sure that the rails are on securely or the unit may fall.
- ⊕ Slide the unit onto the rails until you hear a click. You will then need to flip the latch to fully move the unit into the rack.



- ⊕ Now let's attach the rack ears with the provided hardware.



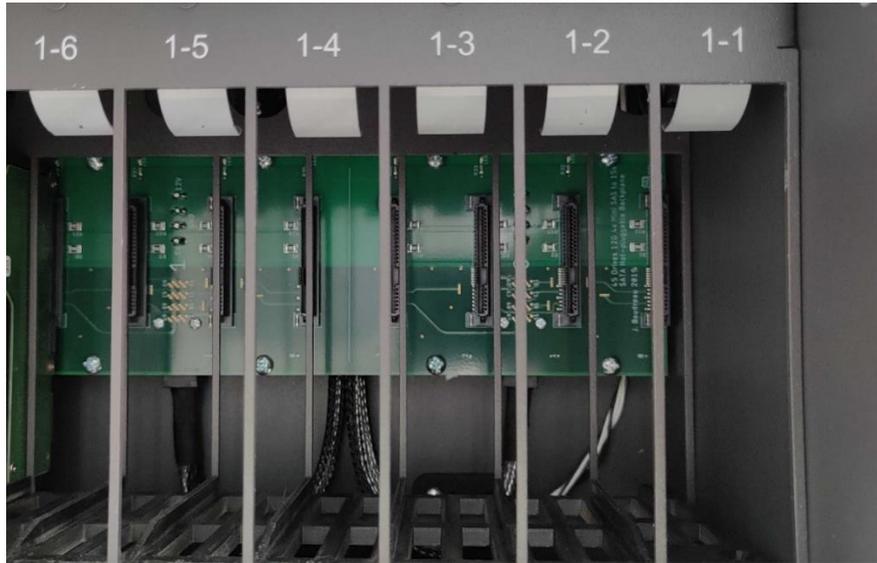
- ⊕ Your server is now racked!



- ⊕ After the unit is racked the next step is to Insert the Storage Drives

INSERTING THE STORAGE DRIVES

- ⊕ Once your unit is racked or in its final destination you can now start installing the storage drives.
- ⊕ It is best practice to install the drives from starting from index 1-1 and sequentially incrementing in order.



- ⊕ The drive should fit snugly into a slot. Make sure the back of the drive is facing the right when placing in the slot



- ⊕ After all the drives are inserted into the slots, you can close up the unit and move on to hooking up the needed cables to your unit.

CABLE SETUP

At this point, you should have the unit unboxed, racked, and storage drives installed. The next step is to connect the cables needed to connect and configure the unit.

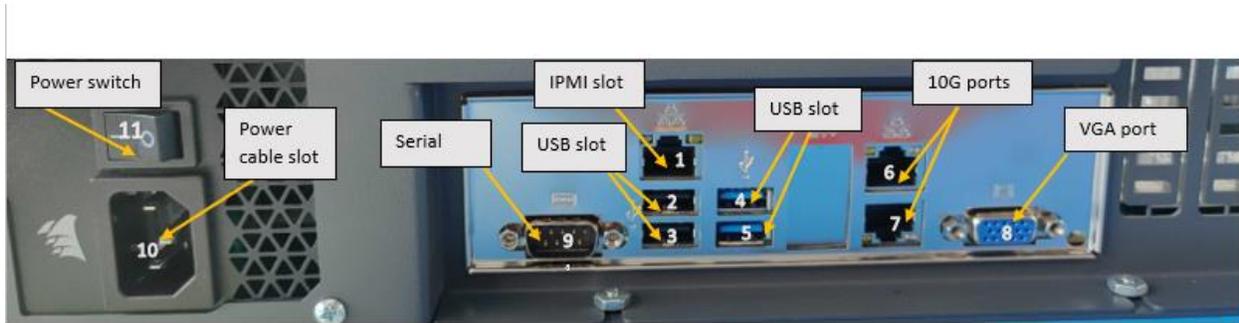


Fig: Back panel slots

No	Component
1	IPMI slot
2	USB slot
3	USB slot
4	USB slot
5	USB slot
6	10G port
7	10G port
8	VGA port
9	Serial
10	Power cable slot
11	Power switch

Table: Back panel slot details

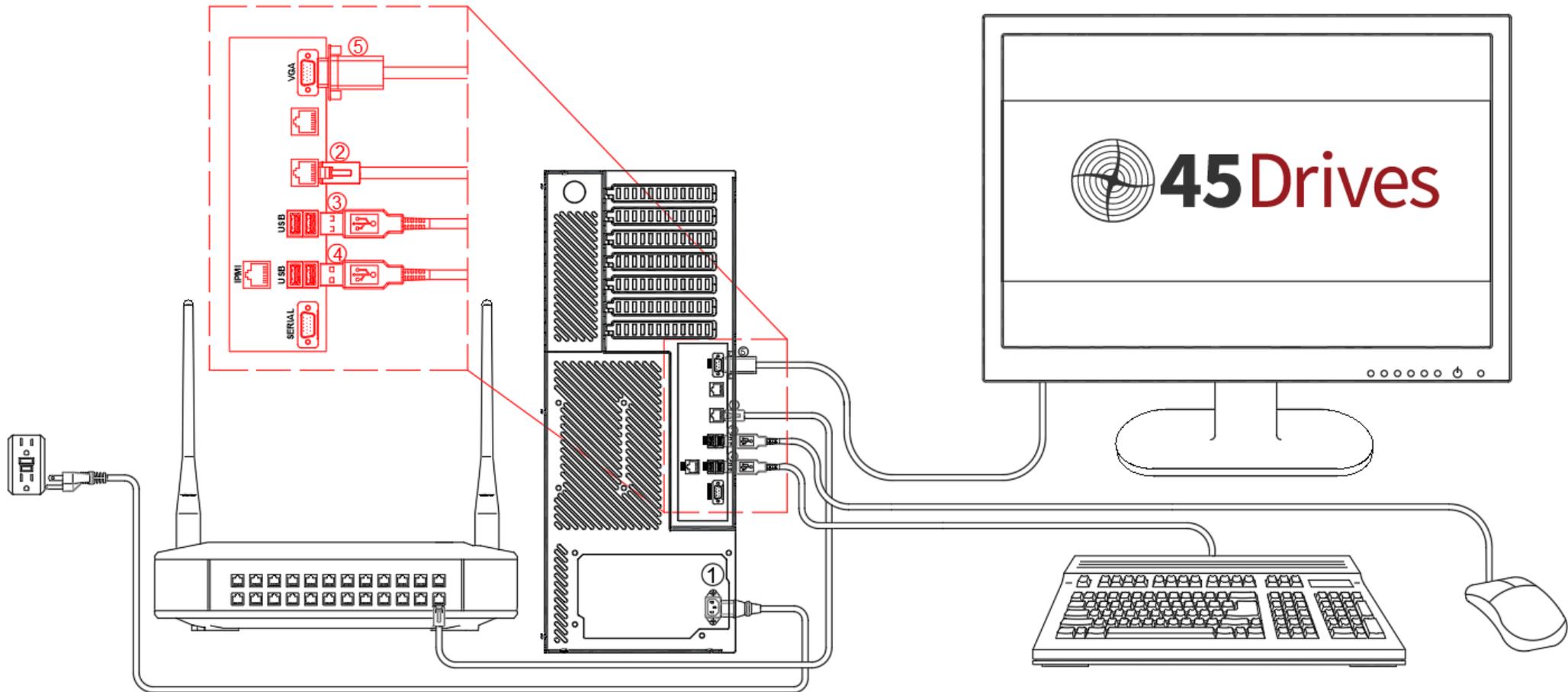
- ⊕ For the initial connection to your unit, you will need to connect an ethernet cable to the IPMI port (1) on the back of the unit. You can connect a 1GB LAN cable from your router or switch as per your network setup.
- ⊕ You can plug in another Ethernet/ LAN cable to provide internet to the server and where we will be accessing the data from to either slots labeled 6 or 7. If you want to bond or aggregate them then you can connect LAN cables to both 6 and 7.

- ⊕ A VGA monitor will also be connected initially so you can see the BMC IP address in the bottom right-hand corner of the screen when the unit first turns on. You can connect the monitor to the VGA port (8).
- ⊕ If you want to configure the unit locally, a USB keyboard will also be beneficial. You can use any of the USB slots labelled from 2 to 5 in fig above.
- ⊕ The last step would be to plug in the power cable to the power supply. Slot labelled 10.
- ⊕ After that you can turn on the power switch and the press the round blue power button to turn on.

Power requirements

- ⊕ The PSU we provide with the appropriate options is a Corsair RM750e
- ⊕ If you are sourcing your own power supply, you can use this as a minimum guideline. It is especially important to ensure you have at least 20A of 5v power.
- ⊕ In addition, if you plan on using a graphics card, or anything that will increase power draw, you may require a more powerful supply.
- ⊕ Corsair Modular ATX Power Supplies are guaranteed to fit

45HOMELAB HL 15 INITIAL CABLING SETUP DIAGRAM



INITIAL CONFIGURATION /SETUP

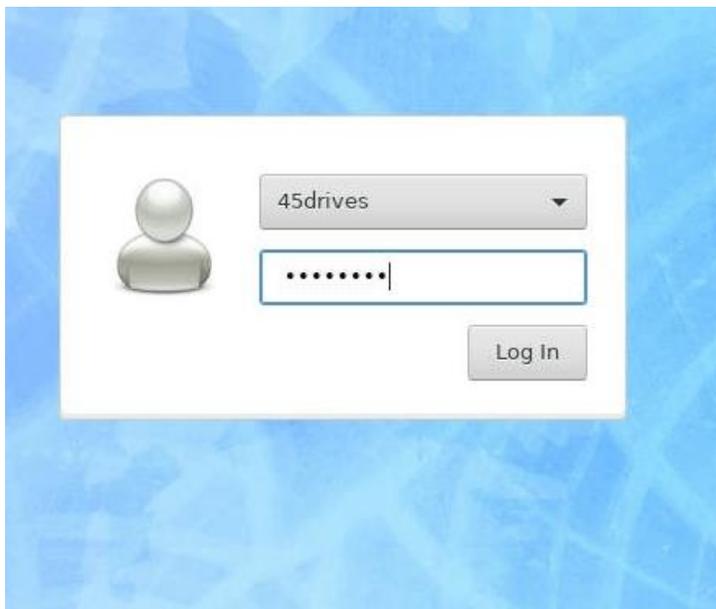
Now you have your HL15 all powered up and ready to be configured. Before we proceed you need to have the below steps completed.

1. The power cables have been connected.
2. The IPMI slot has been plugged in with a LAN cable
3. At least One of the 10G slots have a LAN cable plugged in
4. A monitor is to connected to take a note of the IPMI/BMC IPs

NETWORK SETUP

USING THE DESKTOP UI

- ⊕ Login to the desktop UI using the 45drives user and 45Dr!ves as the password.



- ⊕ Once logged in we can check if our interfaces are up
- ⊕ Open a terminal and type the command `ip a` to check if your interface is up. You should be able to see that a broadcast carrier is available like below.

```

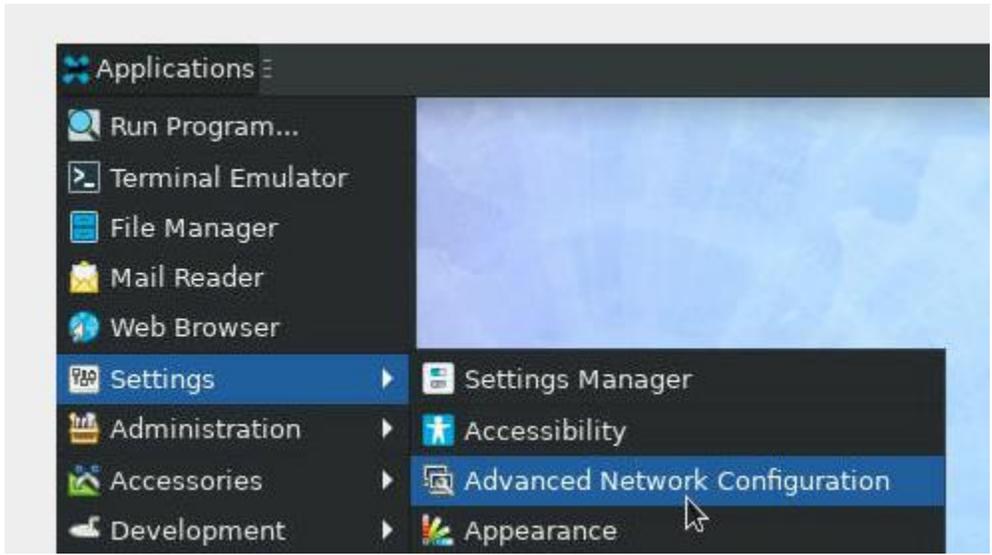
root@iaustine:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 3c:8c:ef:79:9c:20 brd ff:ff:ff:ff:ff:ff
   inet 192.168.250.100/16 brd 192.168.255.255 scope global noprefixroute eno1
       valid_lft forever preferred_lft forever
   inet6 fe80::52b6:addy:a436:4fic/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
   link/ether 3c:8c:ef:79:9c:21 brd ff:ff:ff:ff:ff:ff
4: ens7f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
   link/ether a0:36:9f:b1:ba:90 brd ff:ff:ff:ff:ff:ff
5: ens7f1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
   link/ether a0:36:9f:b1:ba:92 brd ff:ff:ff:ff:ff:ff
6: bond0: <NO-CARRIER,BROADCAST,MULTICAST,MASTER,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
   link/ether 10:10:10:10:10:10 brd ff:ff:ff:ff:ff:ff
   inet 192.168.168.192/16 brd 192.168.255.255 scope global noprefixroute bond0
       valid_lft forever preferred_lft forever
7: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
   link/ether 52:54:00:40:97:fe brd ff:ff:ff:ff:ff:ff
   inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
8: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
   link/ether 52:54:00:40:97:fe brd ff:ff:ff:ff:ff:ff
root@iaustine:~#

```

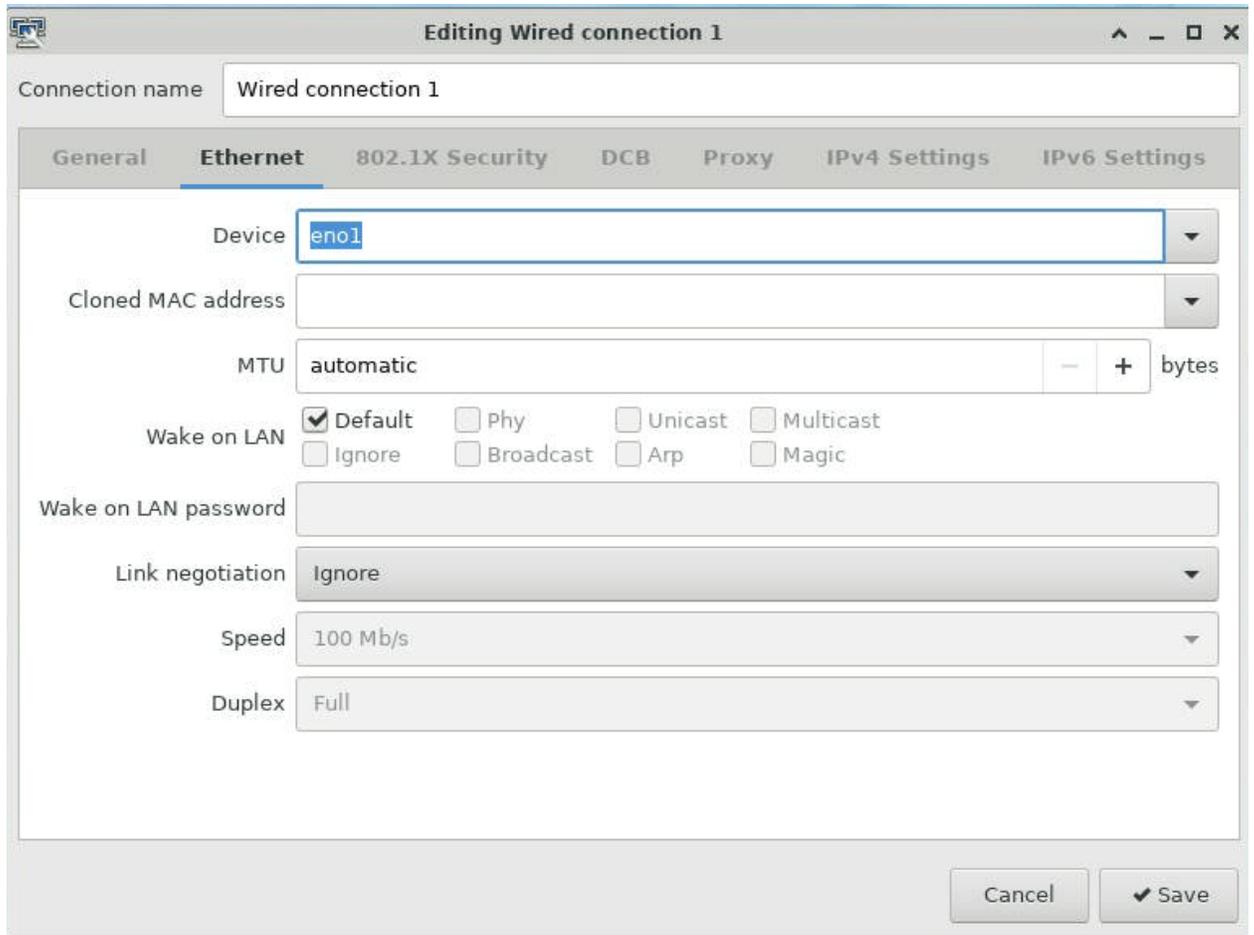
carrier/connection detected

No carrier/connection detected

- ⊕ Go to the applications in the top left corner. Go to settings -> Advanced network Configurations



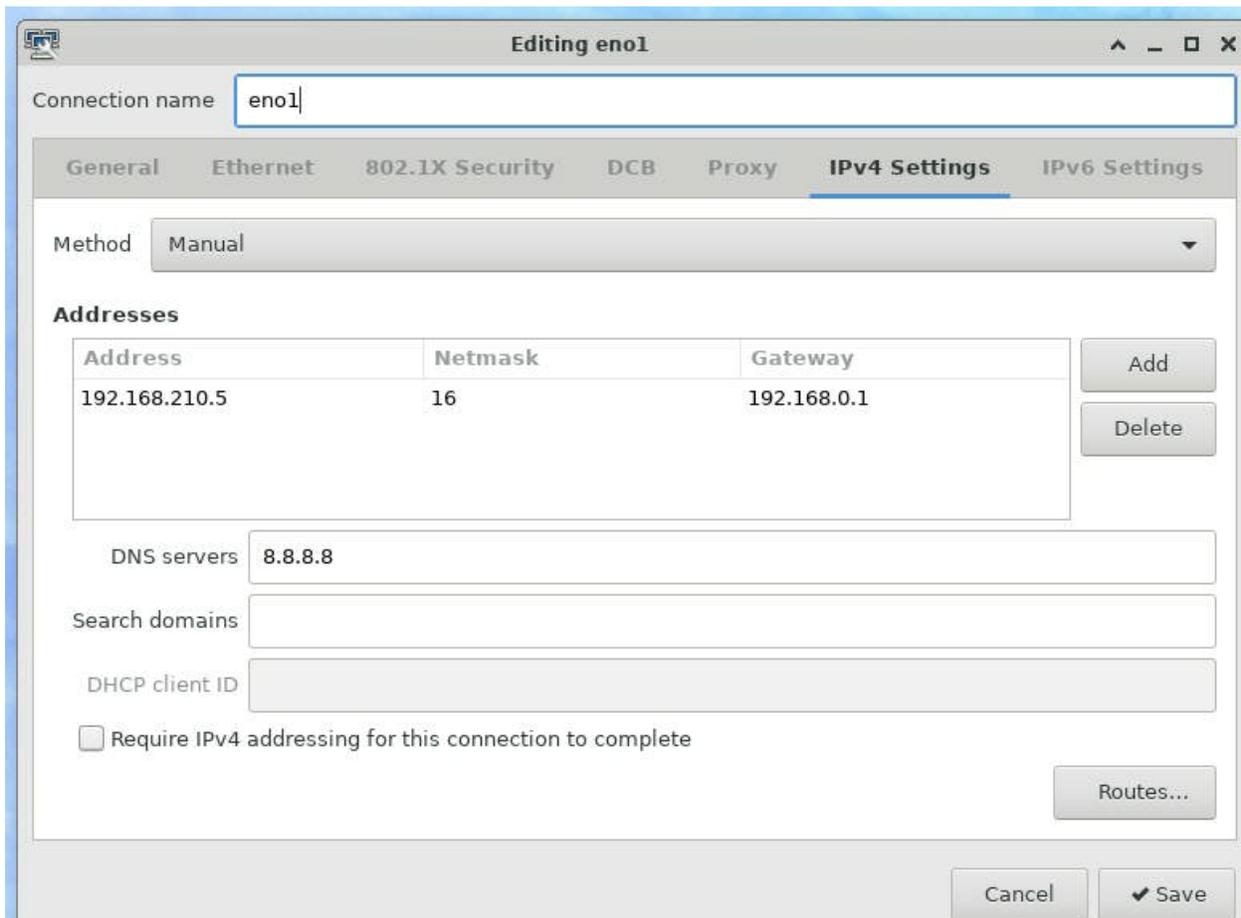
- ⊕ You should be able to see your network connections/ interfaces there
- ⊕ It will either show the interface name or might say like wired connection1, 2 etc
- ⊕ You can double click on it to check the actual interface name
- ⊕ If the interface is not showing you can click on the plus sign and add a new ethernet connection.



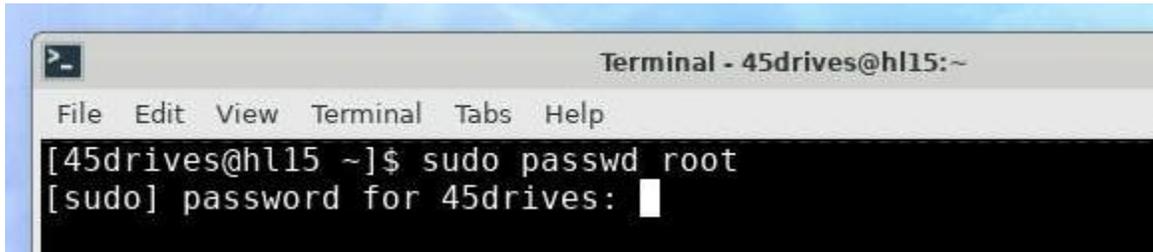
- ⊕ Edit the interface and go to the IPV4 settings section to set the IP. Change the method to manual for setting the static IP and click on add to enter the IP details.



Once the details have been entered click save



After this you can start setting password for your root user using below command in the terminal and set the password.



```
Terminal - 45drives@hl15:~  
File Edit View Terminal Tabs Help  
[45drives@hl15 ~]$ sudo passwd root  
[sudo] password for 45drives: █
```

SETTING UP IPMI

This is just an optional setup, IPMI is not required for the setup. IPMI would help you with remote monitoring. You can skip this step if you prefer.

IPMI or Intelligent Platform Management Interface is an open, industry-standard interface that was designed for the management of server systems over network. It enables you to monitor and control your server platform, as well as to retrieve information about your server platform is a standard. It supports FRU inventory reporting, system monitoring, logging of system events, system recovery (system reset or power off) or alerting.

- ⊕ Turn on the server by pressing the power button at the back panel.
- ⊕ Once the server starts booting up the IPMI address will be shown during bootup in the bottom right-hand corner.



Fig – Finding IPMI/BMC IP

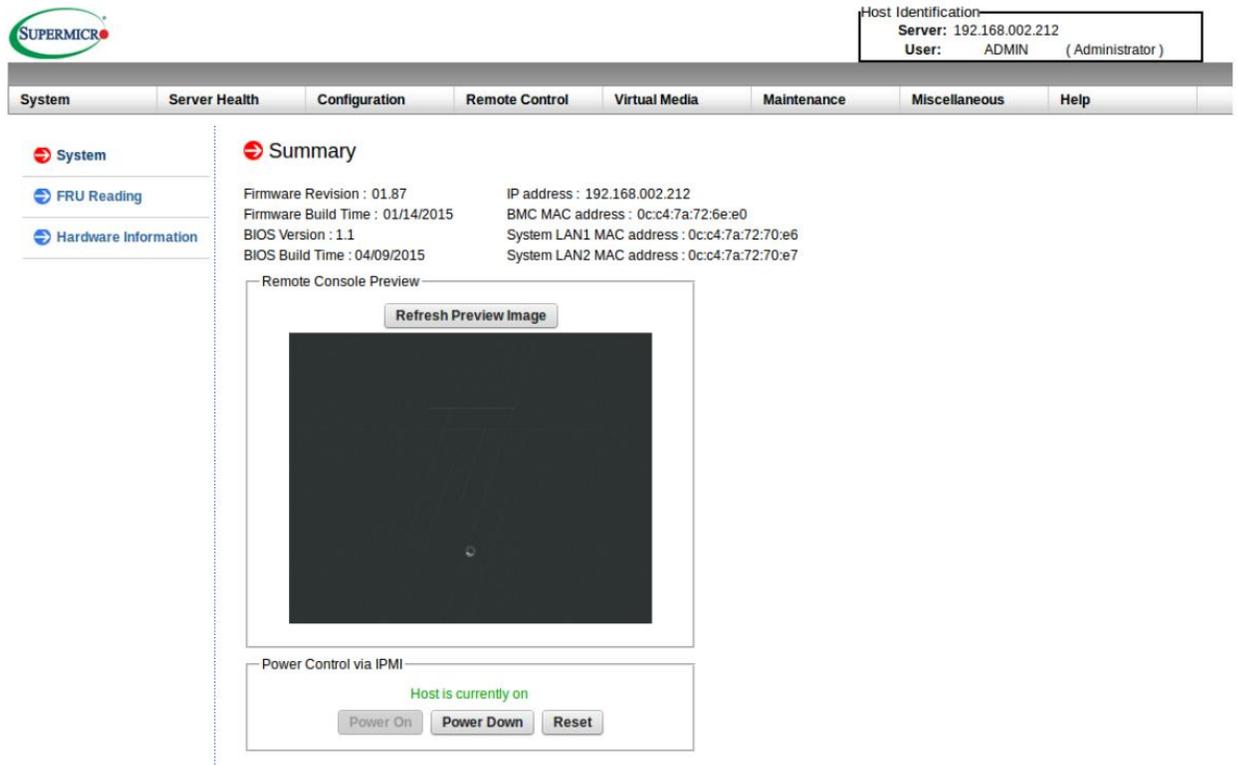
- ⊕ Once you have noted the IPMI IP you can open the same in the browser in your laptop or your desktop as per your preference.

- ⊕ You need to open the browser and type <https://BMCIP> to access the IPMI interface
- ⊕ The login user name will be ADMIN and the default password would be on a white sticker on the side of the unit.



Fig-IPMI log screen

- ⊕ Pictured below is the IPMI set up screen



- ⊕ Go to remote control -> remote console



- You can click on launch console to launch the remote console in a new window. If you want to change the default interface you can click on that here to change it to JAVA or HTML5



- Once you click on launch console a new window opens.
- Here you can login to the desktop using your login user account.

SETTING THE NETWORKING USING NMTUI

This is just an addition option to set up network other than using the UI. You can ignore this if you have already set the IP using the UI and move to the Houston login and config section.

- You can run “ip -c a” to show your interfaces with colored IP addresses. This helps to distinguish what you’re looking at.

```
root@iaustine:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 3c:8c:81:79:9c:20 brd ff:ff:ff:ff:ff:ff
    inet 192.168.250.100/16 brd 192.168.255.255 scope global noprefixroute eno1
        valid_lft forever preferred_lft forever
    inet6 fe80::52b6:addy:a436:4fic/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 3c:8c:81:79:9c:21 brd ff:ff:ff:ff:ff:ff
4: ens7f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether a0:36:9f:b1:ba:90 brd ff:ff:ff:ff:ff:ff
5: ens7f1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether a0:36:9f:b1:ba:92 brd ff:ff:ff:ff:ff:ff
6: bond0: <NO-CARRIER,BROADCAST,MULTICAST,MASTER,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 10:10:10:10:10:10 brd ff:ff:ff:ff:ff:ff
    inet 192.168.168.192/16 brd 192.168.255.255 scope global noprefixroute bond0
        valid_lft forever preferred_lft forever
7: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:40:97:fe brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
8: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:40:97:fe brd ff:ff:ff:ff:ff:ff
root@iaustine:~#
```

carrier/connection detected

No carrier/connection detected

Fig – showing connection detected on the network interfaces

- ⊕ So, you can see in the above diagram that the interface eno1 has carrier detected which means there is a LAN cable connected to NIC slot.
- ⊕ Similarly, eno2 has no carrier which means its not connected. If it is connected and still not detected it will need further troubleshooting.
- ⊕ Once you have your interface connected with the carrier detected next step is to set a static ip for your server.
- ⊕ We will be using this IP going forward to access the server.

Setting Static IP

- ⊕ Run the command “nmtui” to access NMTUI, network manager.

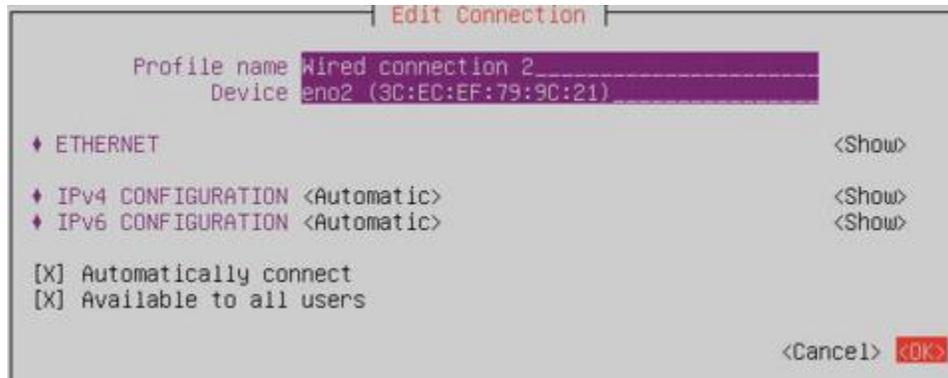


Fig: NMTUI

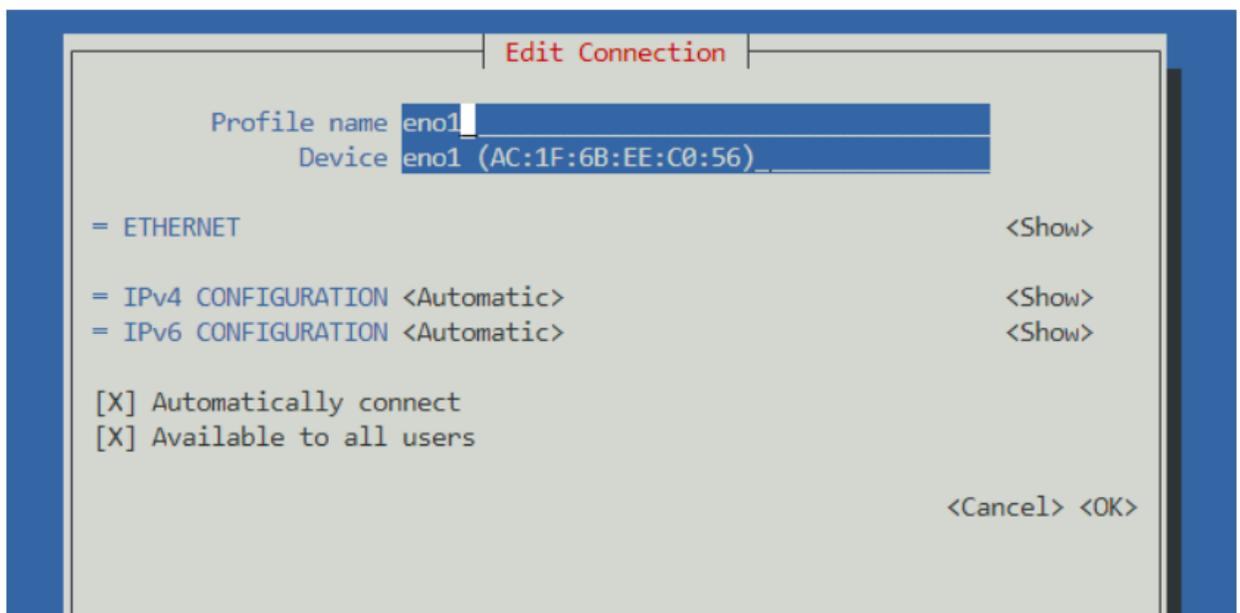
- ⊕ First, we will set a static IP. Click Edit a connection.
- ⊕ Select the interface that we want to set the static IP. This example it is eno1. Select that interface and click on edit.



- ⊕ In case the interface names show up as wired connection 1,2 etc you can select that and confirm what the actual interface name is by checking device name like below screenshot.



- ⊕ Navigate to IPv4 configuration and change automatic to manual and then click show.



- ⊕ Here we can enter our static IP information. Be sure to remember to add your subnet after your IP address. (Most common would be /24, which correlates to a subnet mask of 255.255.255.0) If you will be joining a domain, you can set your server's DNS. Click OK. (Even if you aren't joining a domain, if you want to be able to resolve internet addresses via names you will need to give a DNS whether its a public one or an internal one. Because were setting a static IP, if you don't include a DNS at all you won't be able to download packages or anything because it needs DNS.)

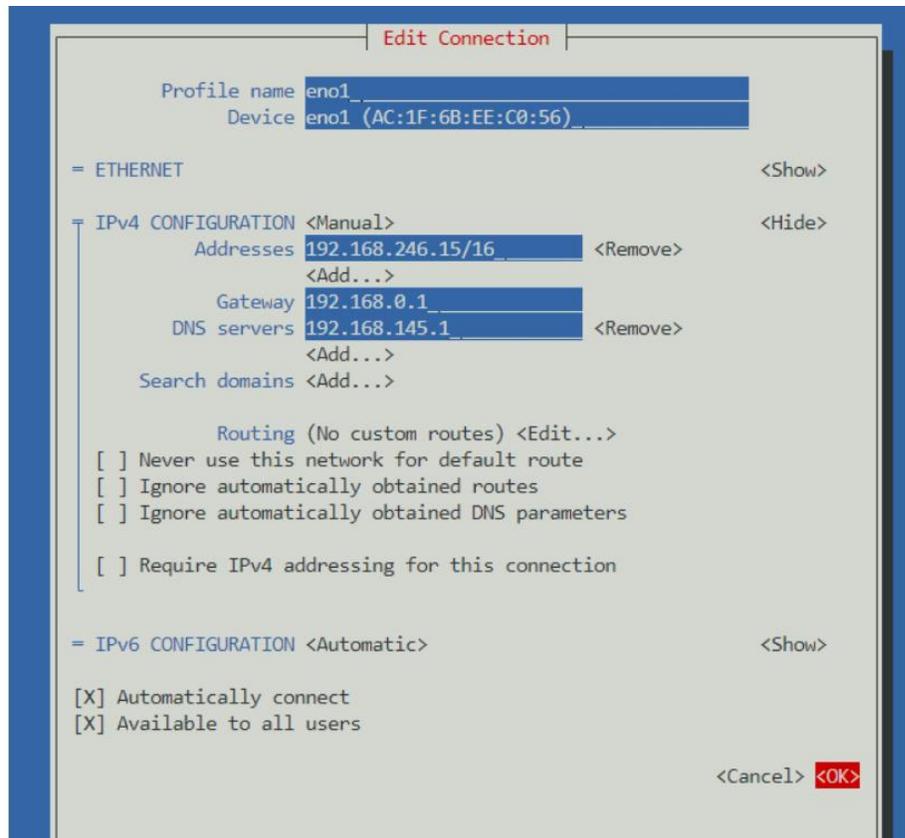
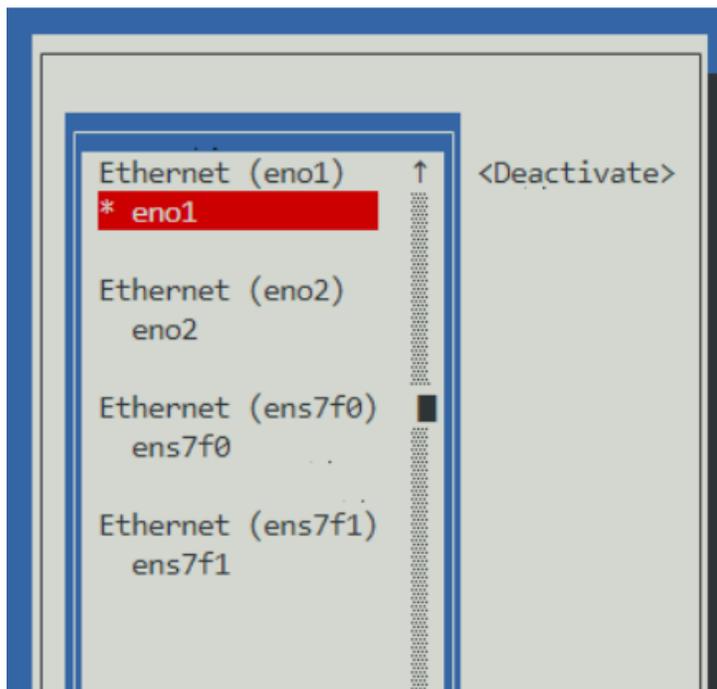


Fig – Setting static IP

- ⊕ Next, click Back and then click on Activate a connection.
- ⊕ You will need to activate that interface .



- ⊕ Deactivate and reactivate the interface. This resets the connection and ensures proper communication. (If you are SSH'd over the interface that you are working on, deactivating will kick you out of your SSH session, so either doing this when you are physically at the server, or over IPMI will allow for you to be able to disable and enable the interface.)

Setting a Bond

- ⊕ Click Edit a connection, and click Add.

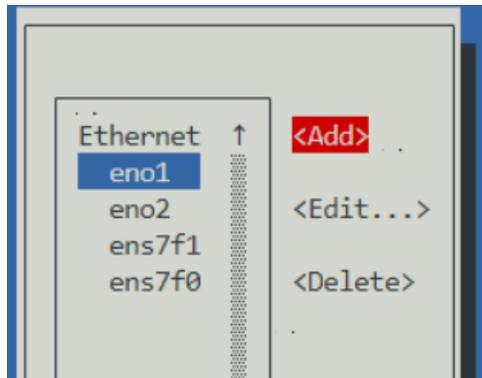
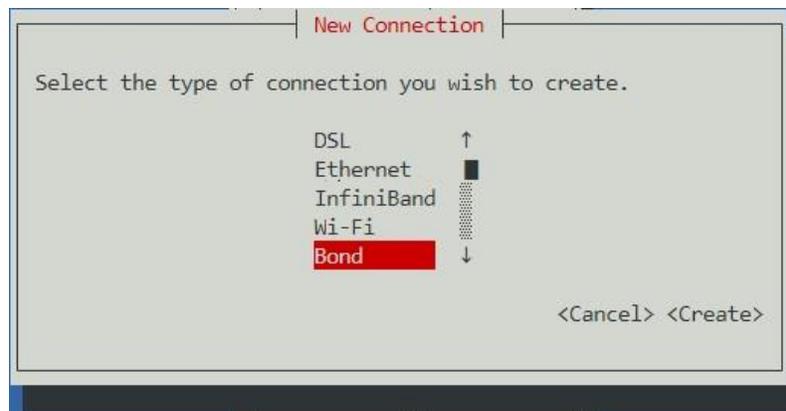
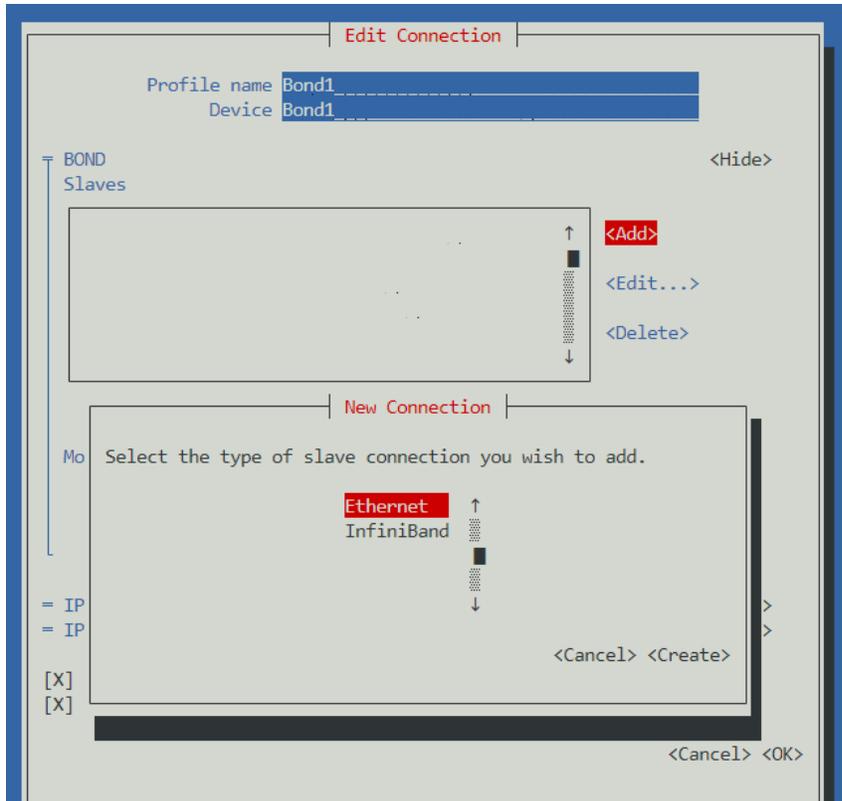


Fig – Add Bond

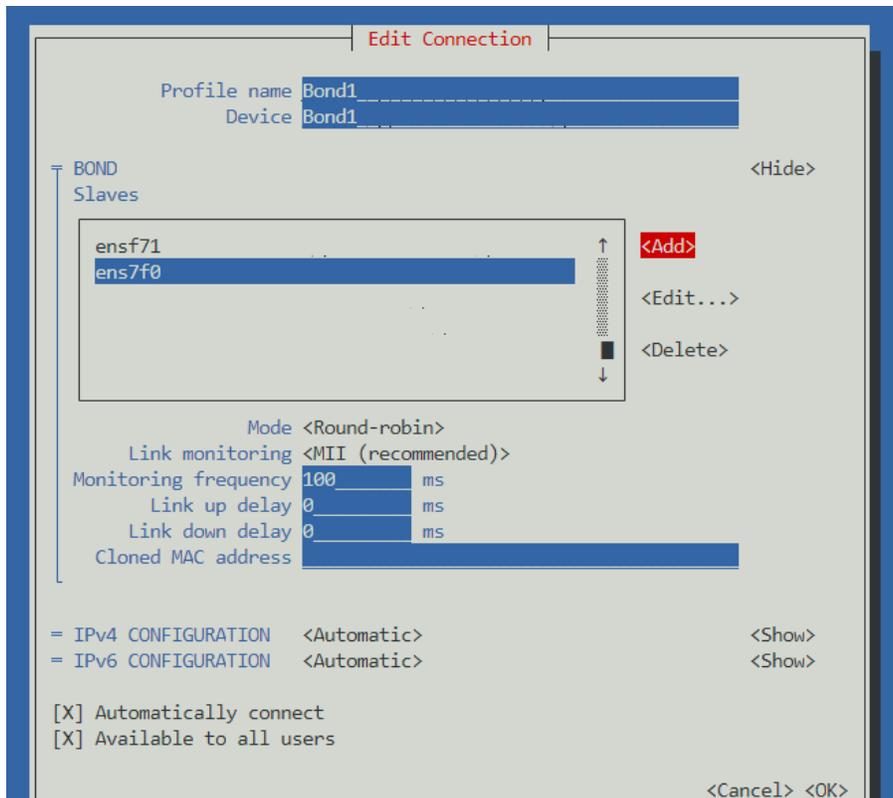
- ⊕ For the type of connection, select Bond.



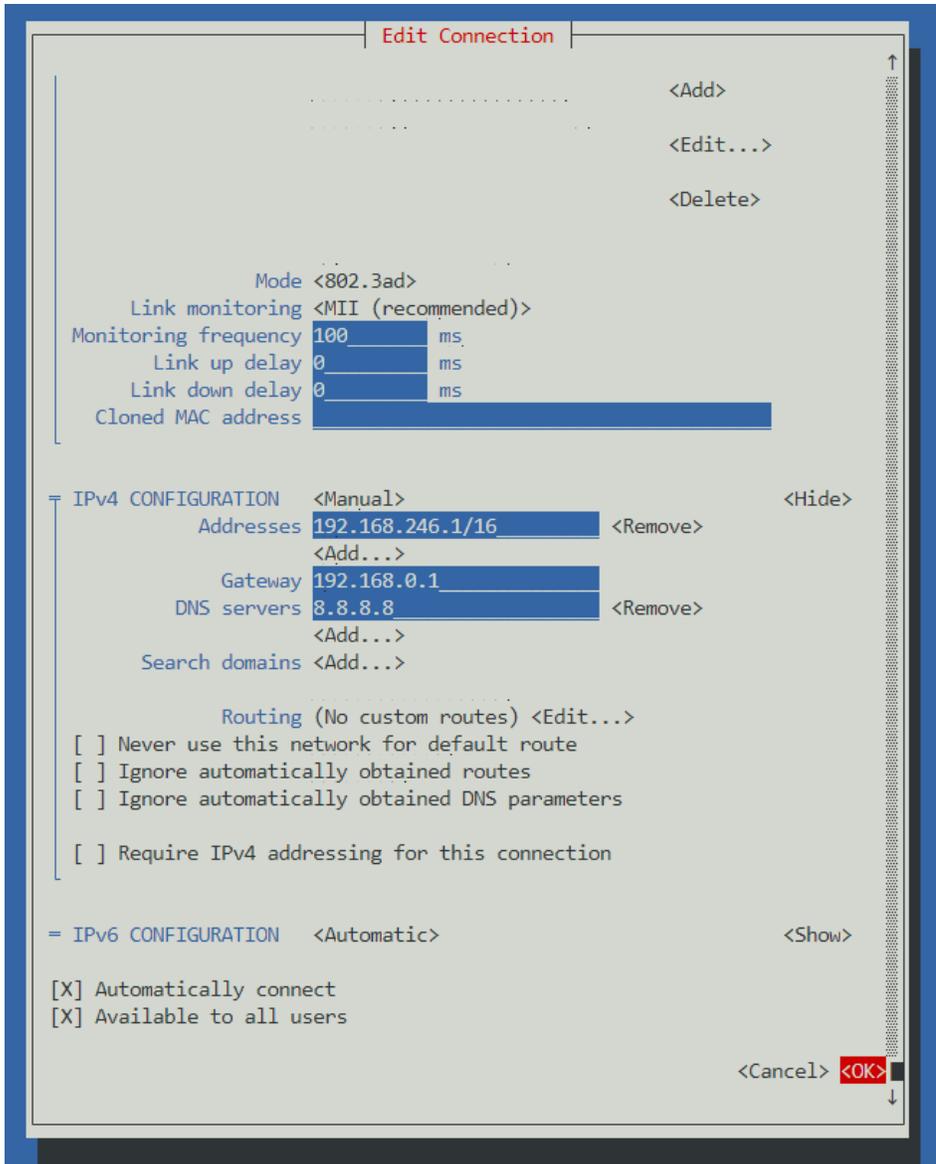
- ⊕ Enter your Profile name and Device name. For this example, we have used Bond1. Under Slaves, click Add and select Ethernet.



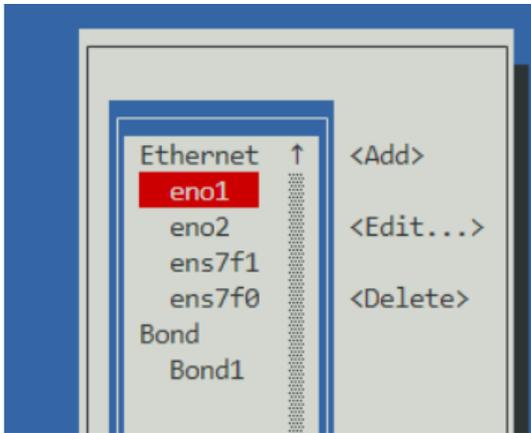
- ⊕ For this example, we will be using the NIC ports. Enter your interface name under Profile name and Device, and click OK.
- ⊕ Do the same for ens7f1. Your Slaves table should look like this.



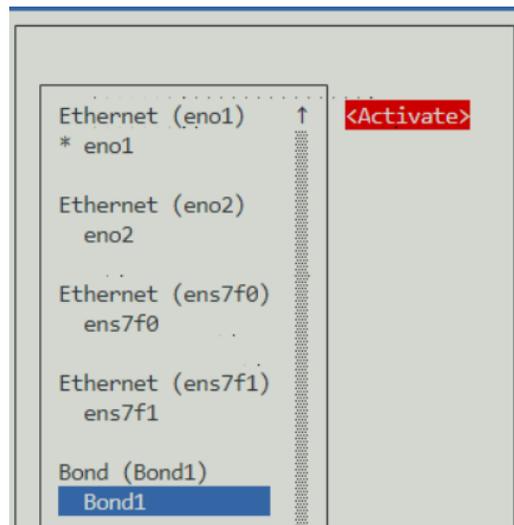
⊕ Add your IP address info for your bond, and click OK.



📍 Here we can see our bond has been created.



- ⊕ Click Back, and go to Activate a connection. Highlight Bond1 and Deactivate it.
- ⊕ Now activate it. Make sure the two slave ports are deactivated.



- ⊕ Now, run another "ip a" command. Your bond is now listed.

```
[root@krocky45d ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether ac:1f:6b:ee:c0:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.246.15/16 brd 192.168.255.255 scope global noprefixroute eno1
        valid_lft forever preferred_lft forever
    inet6 fe80::ae1f:6bff:feee:c056/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether ac:1f:6b:ee:c0:57 brd ff:ff:ff:ff:ff:ff
4: ens7f0: <NO-CARRIER,BROADCAST,MULTICAST,SLAVE,UP> mtu 1500 qdisc mq master Bond1 state DOWN group default qlen 1000
    link/ether a0:36:9f:2f:ff:40 brd ff:ff:ff:ff:ff:ff
5: ens7f1: <NO-CARRIER,BROADCAST,MULTICAST,SLAVE,UP> mtu 1500 qdisc mq master Bond1 state DOWN group default qlen 1000
    link/ether a0:36:9f:2f:ff:40 brd ff:ff:ff:ff:ff:ff permaddr a0:36:9f:2f:ff:42
9: Bond1: <NO-CARRIER,BROADCAST,MULTICAST,MASTER,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether a0:36:9f:2f:ff:40 brd ff:ff:ff:ff:ff:ff
    inet 192.168.246.1/16 brd 192.168.255.255 scope global noprefixroute Bond1
        valid_lft forever preferred_lft forever
[root@krocky45d ~]#
```

HOUSTON LOGIN AND CONFIG

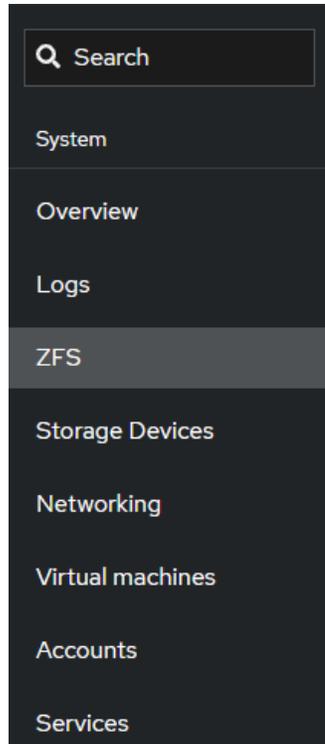
You should already have the Houston modules installed in your server. You can access Houston UI at <https://SERVER-IP:9090> .

You can use the root account you created and the password or the 45drives user as well to login. Root account would have the elevated privileges.



CREATING ZPOOL

- ⊕ Once we're logged into Houston, you should see a list of modules. You will see the ZFS tab. Click on this to continue.



- ⊕ On the top right of the ZFS page you will notice Storage Pools. Click on this to begin creating your first storage pool. When we create a pool with ZFS, we select the drives we want to be part of the pool. In our case all 15 drives



- ⊕ Provide a name for your new storage pool, in this test environment we have named the pool tank in this example.
- ⊕ Select which raid you would like to use under "Virtual Device ". We usually recommend RAIDZ2 which is equivalent to RAID 6 and has two drive redundancy.
- ⊕ Then select your hard drives and click on "Create" to finish. Ensure you uncheck Disks WWN, and then select "Device Alias" so the pool is created with the Disk Aliasing to easily identify drives (i.e 1-1, 1-2, etc.)



We do not recommend setting “refreservation” below 10%. With this disabled we can write to the ZFS Pool/Dataset and fill it entirely, at which point the pool may be unusable and data could be lost.

Create Storage Pool

Name ?

Virtual Device

Disks WWN

Disks Identifier

Disks ?

- 1-1
12 TB ST12000NM0007-2A (5000c500b17dc72b)
Physical Sector Size: 4 KiB
- 2-5
10 TB WDC_WD101KRYZ-01 (5000cca273d9632b)
Physical Sector Size: 4 KiB
- /dev/sdn
10 TB WDC_WD101KRYZ-01 (5000cca273d971ef) ⚠
Physical Sector Size: 4 KiB

One or more disks is missing a Device Alias identifier.

One or more disks used to be a member of a Storage Pool. ⚠

Sector Size

Record Size

Deduplication

Refreservation 10 %

Options

- LZ4 compression
- Automatically expand storage pool when larger devices are added
- Automatically replace devices
- Automatic TRIM
- SELinux contexts for Samba
- Forcefully create storage pool

CREATING ZFS FILESYSTEM/DATASET

- With your new storage pool created, we can now create some datasets to share out. You will see **Create Filesystem**. Click on this to continue.

Storage Pools

Create Storage Pool Import Storage Pool Refresh

Name	Health	Size	Allocated	Free	Fragmentation	Usage
tank	ONLINE	81.86 TiB	4.14 MiB	81.86 TiB	0 %	

File Systems Snapshots Status

7/12/2021, 9:36:17 AM 3 Create Filesystem Refresh

Name	Available	Used	Snapshots	Refreservation	Record Size	Compression	Deduplication	Share	Mounted	Replication
tank	60.41 TiB	2.29 MiB	0 B	0 B	128 KiB	LZ4	Off	Off	Yes	No

- In the new window that appears, give your new filesystem a name. We can leave all of the options at the default settings. In this example, we have used `nfs`.

The screenshot shows the 'Create Filesystem' dialog box. The 'Parent File System' is 'tank'. The 'Name' is 'nfs'. The 'Encryption' checkbox is unchecked. 'Access Time' is 'Inherited (On)'. 'Case Sensitivity' is 'Inherited (Sensitive)'. 'Compression' is 'Inherited (LZ4)'. 'Deduplication' is 'Inherited (Off)'. 'DNode Size' is 'Inherited (Legacy)'. 'Extended Attributes' is 'Inherited (System Attribute)'. 'NFS Share' is checked. 'Quota' is 0 KiB. 'Record Size' is 'Inherited (128 KiB)'. 'Options' include 'SELinux contexts for Samba' (unchecked), 'Enable Samba share' (unchecked), and 'Read only' (unchecked). 'Cancel' and 'Create' buttons are at the bottom.

- If you wish you can change those other parameters as per your preference and even set quota as well.
- Once you click on create you will have your dataset created.

File Systems Snapshots Status

7/12/2021, 10:18:39 AM 4 Create Filesystem Refresh

Name	Available	Used	Snapshots	Refreservation	Record Size	Compression	Deduplication	Share	Mounted	Replication
tank	60.41 TiB	2.59 MiB	0 B	0 B	128 KiB	LZ4	Off	Off	Yes	No
tank/nfs	60.41 TiB	279.38 KiB	0 B	0 B	128 KiB	LZ4	Off	Off	Yes	No

- ⊕ Now you will be able to see your ZFS pool, datasets, and drives within the File Systems Tab, and Status Tab within the ZFS module.
- ⊕ If you are to run `zpool status` command within the Terminal you should see the output of the ZFS Pool, it's VDEVs, and Disks.
- ⊕ You can create as many datasets you want based on how many shares you are planning to create.



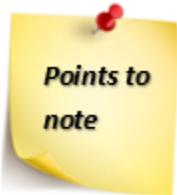
If you are unable to create the pool, ensure the drives you are using are free of any partitions.

Ensure the disks you are using to create the pool are of the same size

CREATING YOUR SHARES

Once you have your pool and dataset created next step is to create network shares. You can either create SAMBA/NFS shares.

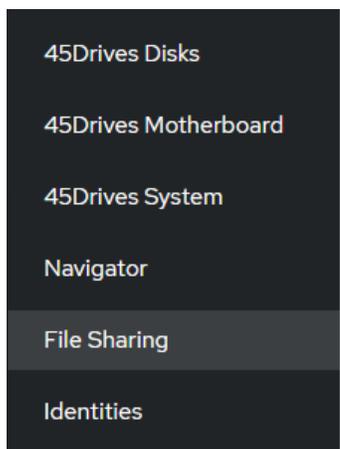
Samba/SMB shares



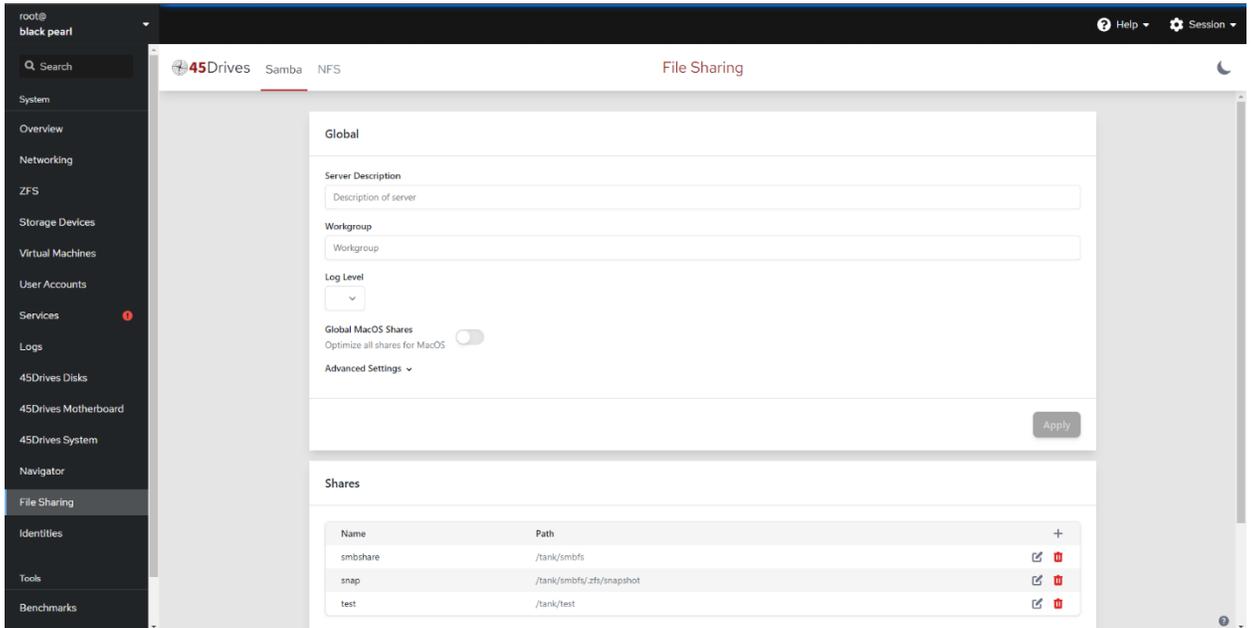
Points to note

- Make sure SMB Services Running and Enabled
- SMB Ports Open on Firewall (133/tcp, 445/tcp and 137/udp, 138/udp)

- ⊕ In Houston UI, navigate to the File Sharing tab. And click on the Samba tab, if not selected.

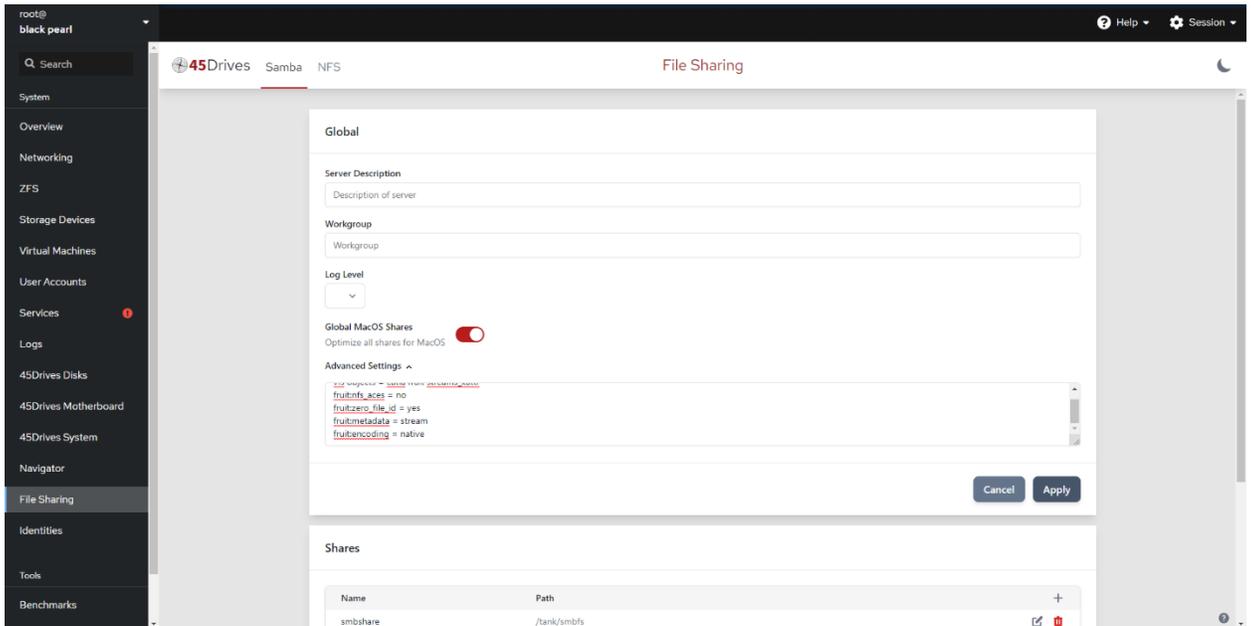


Once here, we can begin configuring our SMB Shares



First, we can add any options to the Global SMB configuration.

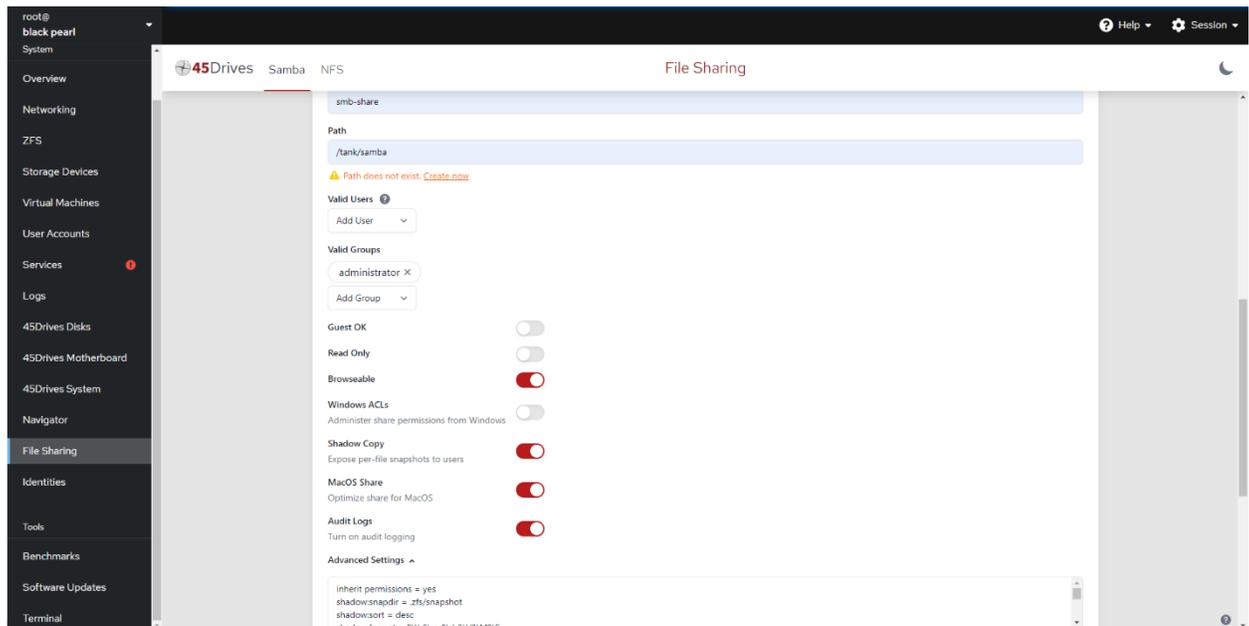
Here we can change the Server Description, the Workgroup, Log Level, and add any additional parameters to the SMB configuration in the Advanced Settings box by clicking the down arrow. For example, here we've added a few parameters to help with MacOS performance on an SMB share.



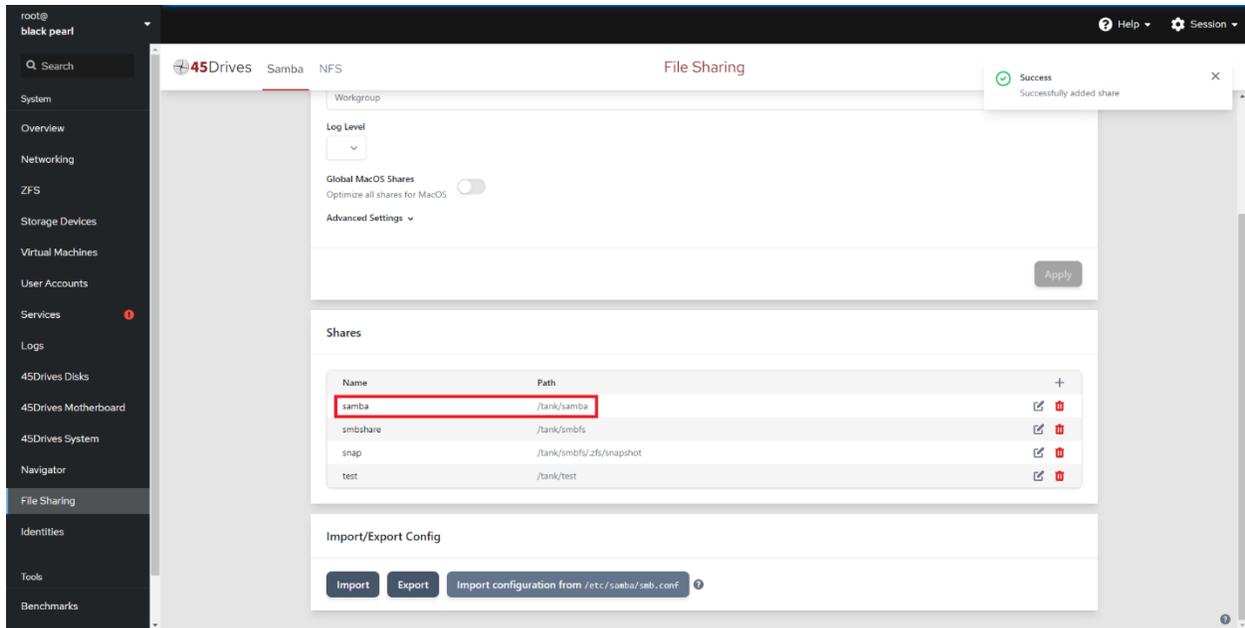
- ⊕ Next, we can create an SMB share, we can scroll down to Shares and select the Plus button to begin.
- ⊕ Here we can set the SMB Share Name, a Description, the Path to be shared out. It will be usually /pool_name/dataset_name (you can now create the path here instead of ZFS)
- ⊕ if we are domain joined, we can select to use Windows ACLs.
- ⊕ We can specify any Valid Users and Valid Groups, allow Guest Access, make the SMB share Read Only, make itBrowsable, and enable Windows ACLs, as well as some other options.

Adding options to the SMB share

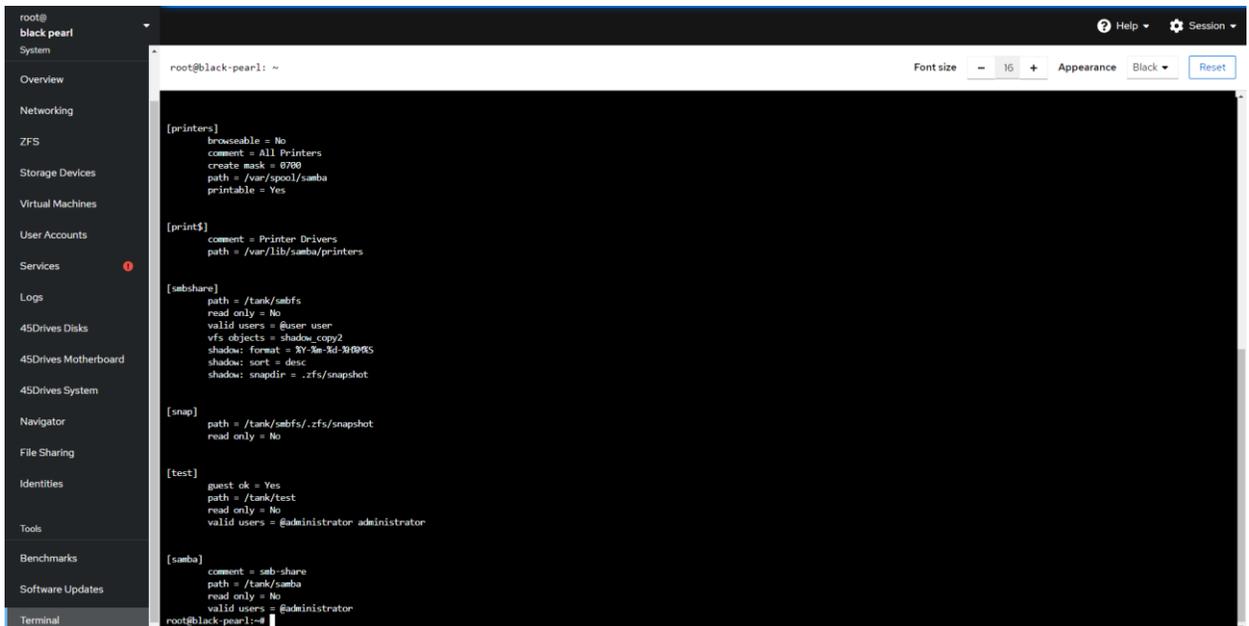
- ⊕ We can also add any additional options in the Advanced Settings box via the drop-down arrow.
- ⊕ In the Advanced Settings box, we entered “inherit permissions = yes” ourselves. This is to make sure that the permissions are inherited from the parent folder.
- ⊕ There are a few preselected options we can enter into the Advanced Settings box by selecting one of the buttons below: Shadow Copy, MacOS Share, Audit Logs.
- ⊕ Here we can see we’ve created a share called “samba” with a description of “smb-share”. It is pathed to our ZFS dataset at “/tank/samba”. We have added the “administrator” to Valid Groups, and left the shareBrowsable.



- ⊕ Here we can see our SMB share is created.



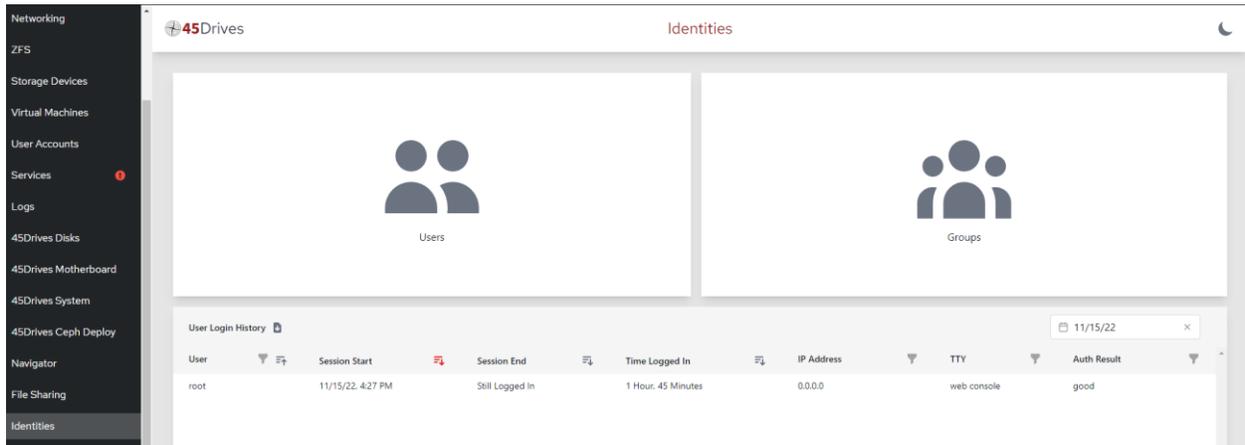
- If you were to run “testparm -s” on the command line you will see your samba share has been added and configured properly in its own section.



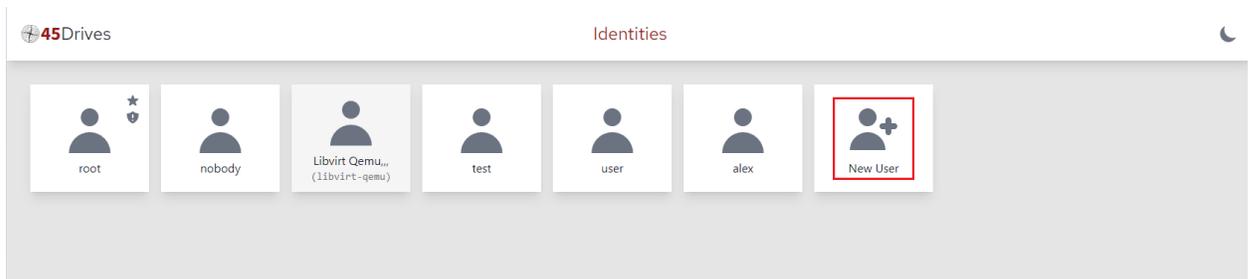
Setting up Local User Access SMB Shares

This is to create local users and groups and add them to provide access to your samba share.

Go to the identities tab in Houston



Click the 'Users' section, this will open a page with a list of users. Select "New User".



Fill in the Username, Full Name/Description. Then click "Apply". It is also possible to assign this new user to a group at the bottom of the prompt. If applicable it can be done here, or a user can be assigned at a later time.

New User

Details

Username

Full Name/Description

Home Directory

Login Shell

Groups +

- ⊕ A prompt will come up to set the users password. This is a local Linux password, it can be used to SSH into the machine, or to authenticate to Houston.

Set login password for smbuser

The password should satisfy the following requirements:

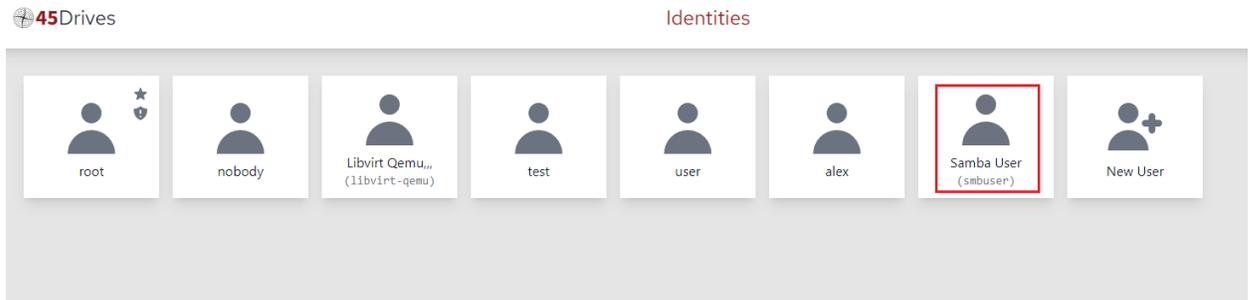
- one lowercase letter ✓
- one uppercase letter ✓
- one number ✓
- one special character ✓
- 8 characters long ✓

- ⊕ The user generation will complete successfully. The user should now be able to authenticate to Houston or SSH with that password.

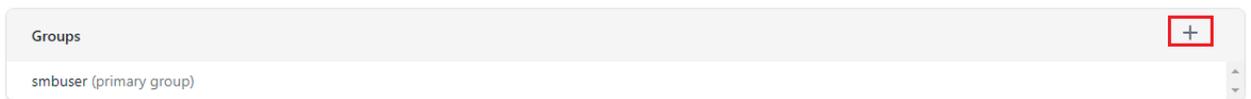
- ⊕ The below sections will detail assigning a user to a specific group, and setting an SMB password if applicable.

Assigning a Linux Group to a User

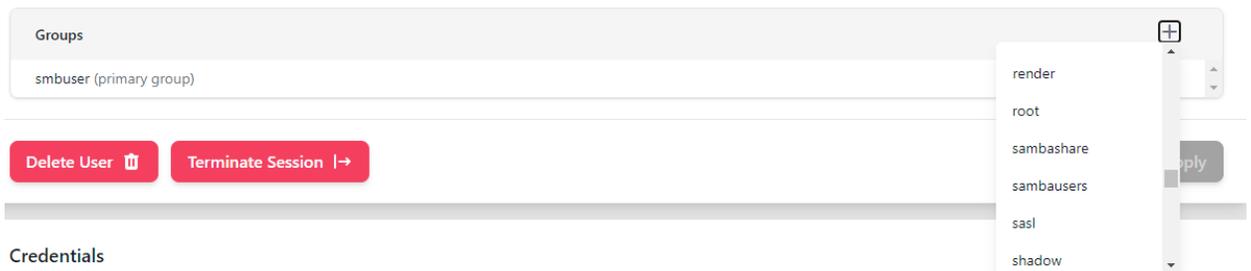
- ⊕ In the “Users” section the new user should be seen. Click on the user to assign a group.



- ⊕ Click on the “+” under the Groups section.



- ⊕ A dropdown will pop up and you can now select a group to assign to the user.



- ⊕ The newly added group should be displayed under the Groups section. Click “Apply” to save changes.

Details

Full Name/Description
Samba User

Home Directory
/home/smbuser

Login Shell
Bash /bin/bash

Groups

- sambausers
- smbuser (primary group)

Delete User
Terminate Session
Cancel
Apply

Configuring a Samba Password for a User

- Select the user you wish to assign a Samba password. The Samba password will need to be set to allow users to authenticate to Samba shares. It can be the same as the Linux password, but does not have to be. Click on “Set Samba Password”. Enter a password and click “Apply”.

Identities

Samba User (login=smbuser,uid=1003,gid=1004)

Credentials

User Login

Change Account Password
Lock Account Password
Edit Password Expiry

Password never expires.

Samba

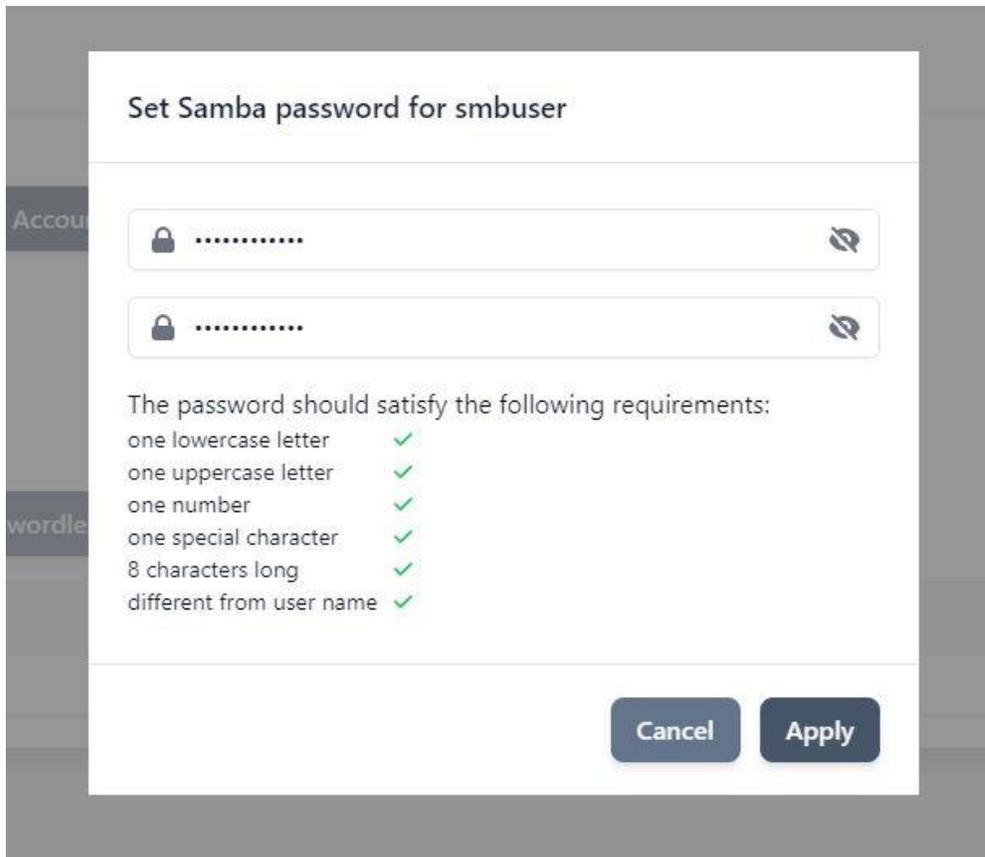
Set Samba Password

SSH

Generate SSH Key Pair
Test Passwordless SSH

Authorized SSH Access Keys

No keys. Click '+' to add one.



Set SMB permissions using local users and group

- Click on the edit button of the share you want to add the user to grant the permissions.

Shares		
Name	Path	+
audit	/zfs_pool/audit	 

- Click on edit permissions

samba /tank-mirror/samba

Share Name

samba

Share Description

Describe your share

Path

/tank-mirror/samba

Edit Permissions

Valid Users ?

Add User ▾

Valid Groups

Add Group ▾

- ⊕ Select the owner and the group for the share and set the permissions as well as per your preference.

Share Directory Permissions

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Other	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Mode	rwxrwxr-x (775)		

Owner

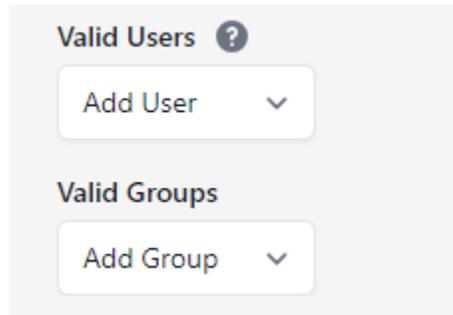
admin ▾

Group

smbgroup ▾

Cancel Apply

- ⊕ You can also select valid users and groups if you want to provide access to multiple of them.

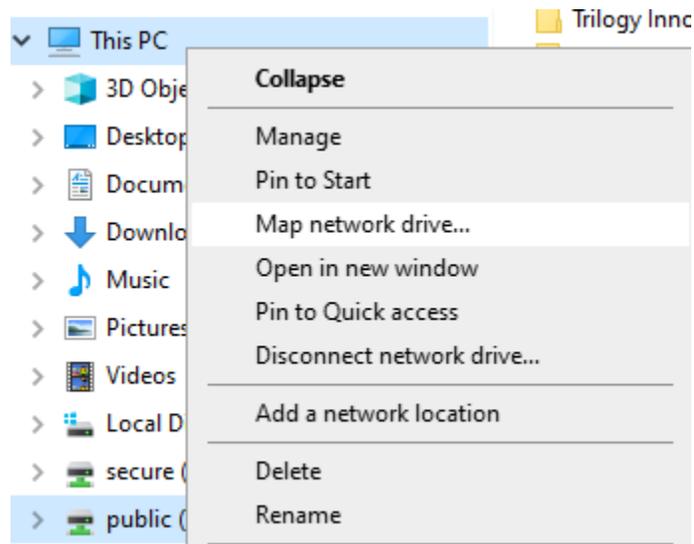


- ⊕ Now you can verify by connecting the share.

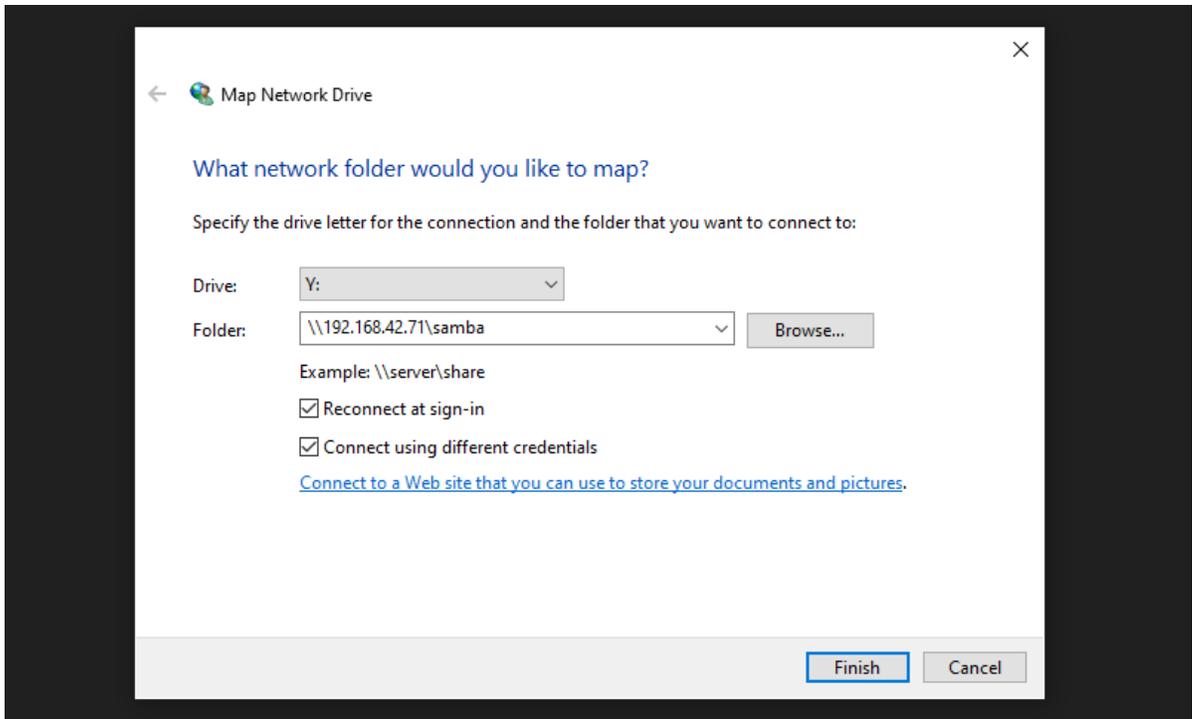
Connecting to SMB Share on Windows and MacOS

Connecting to SMB Share on Windows

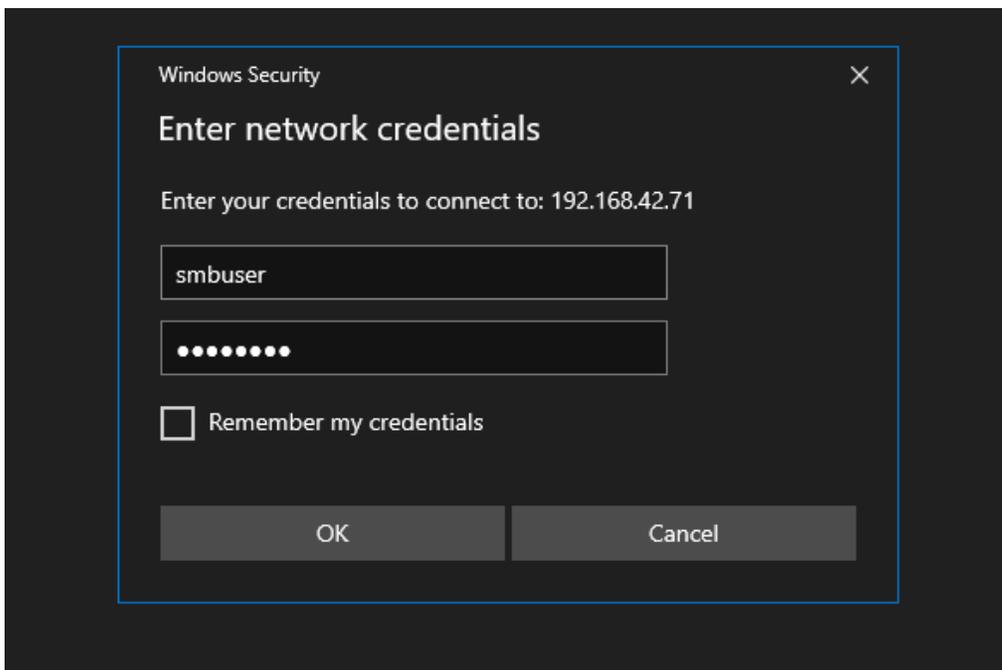
- ⊕ On a Windows client, go to This PC in File Explorer.
- ⊕ Right click and select Map network drive.



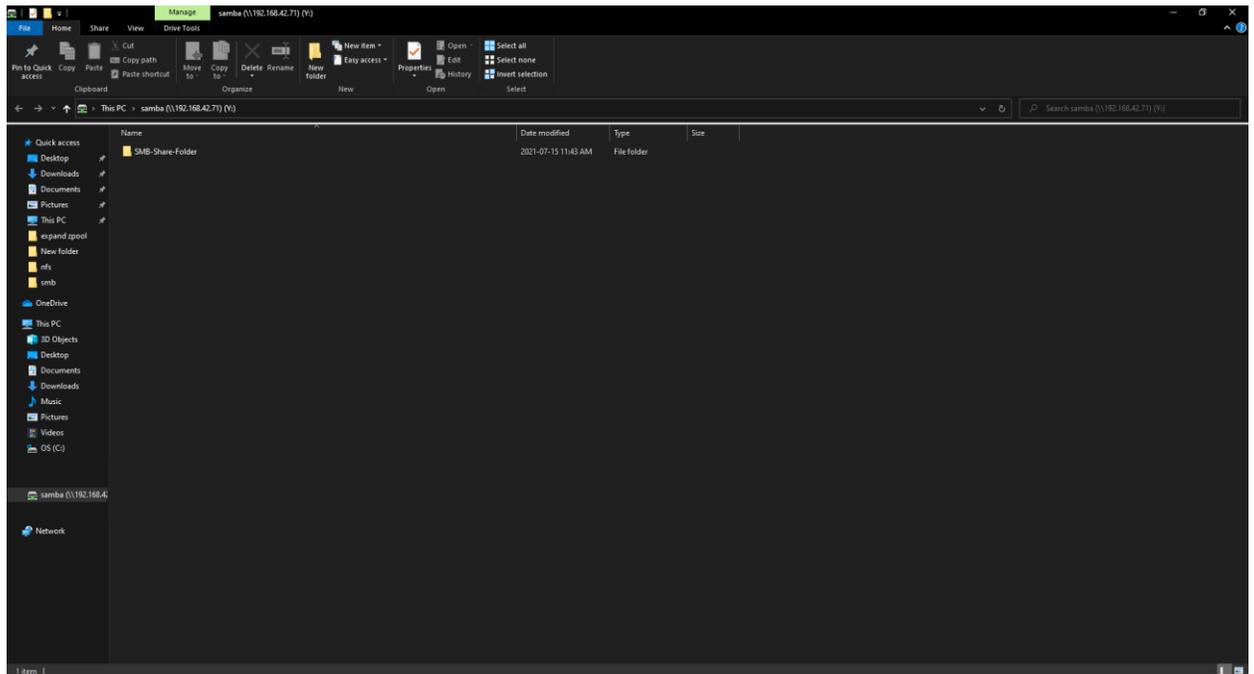
- ⊕ In this menu, enter the server IP address in the following format `\\SERVER-IP\SHARE-NAME` and select **Connect using different credentials**.



⊕ Enter the login to connect to the SMB share.

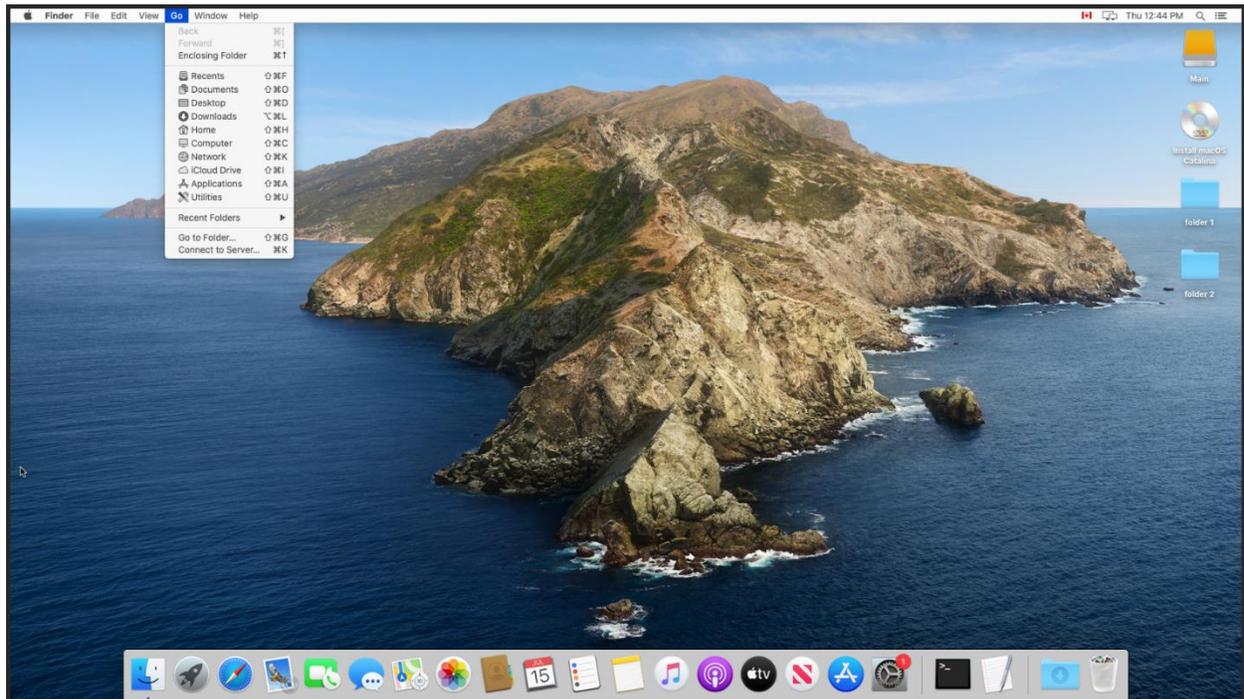


Here we can see our SMB share is connected, and we can create a folder.

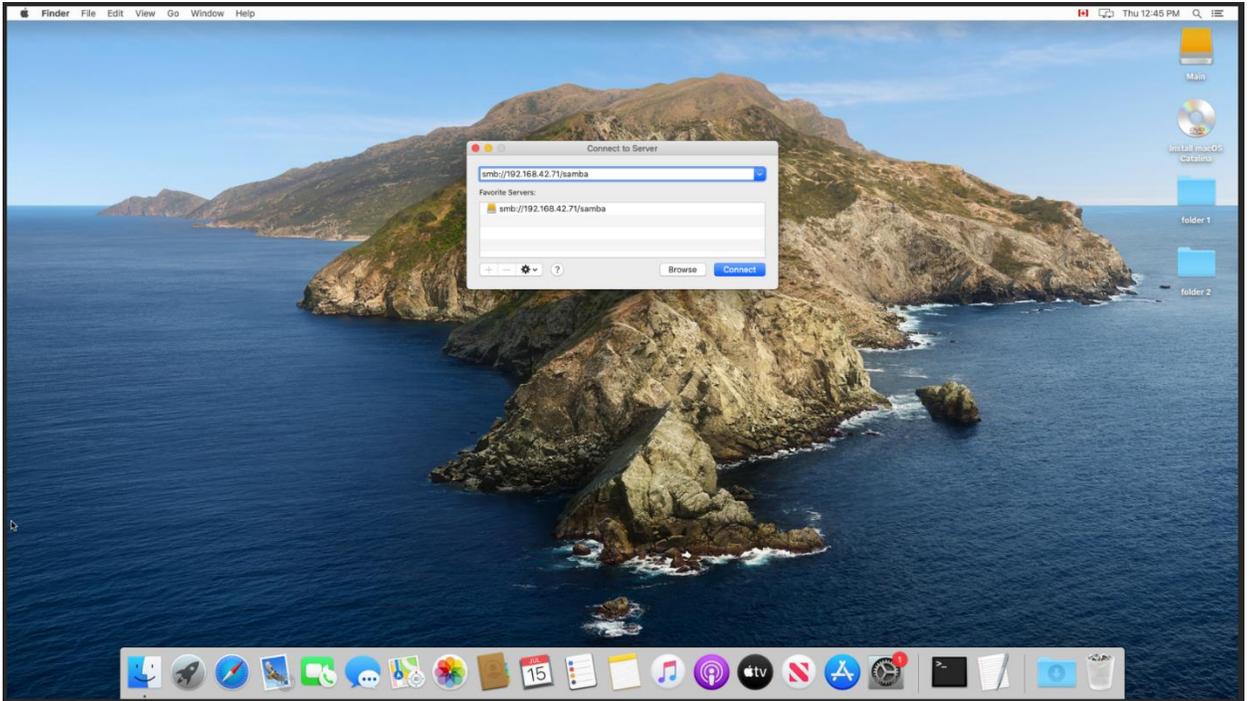


Connecting to SMB Share on MacOS

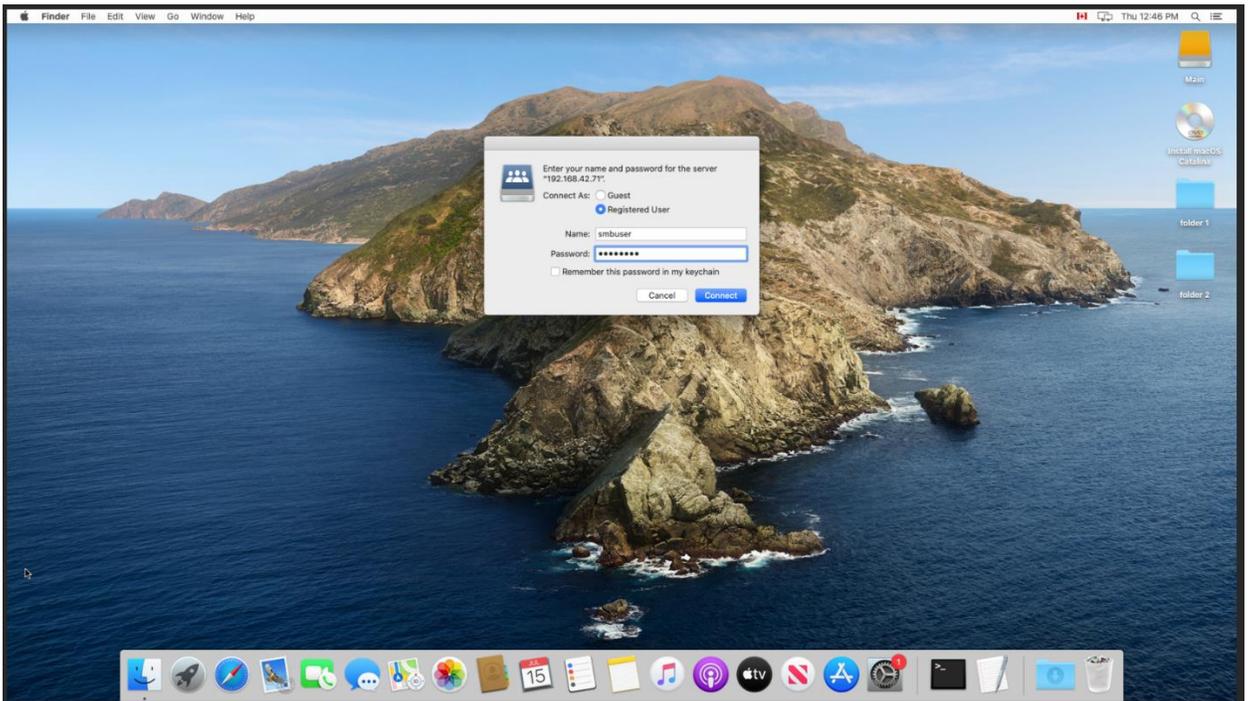
At the toolbar on the top of the screen, press Go and then “Connect to Server...”.



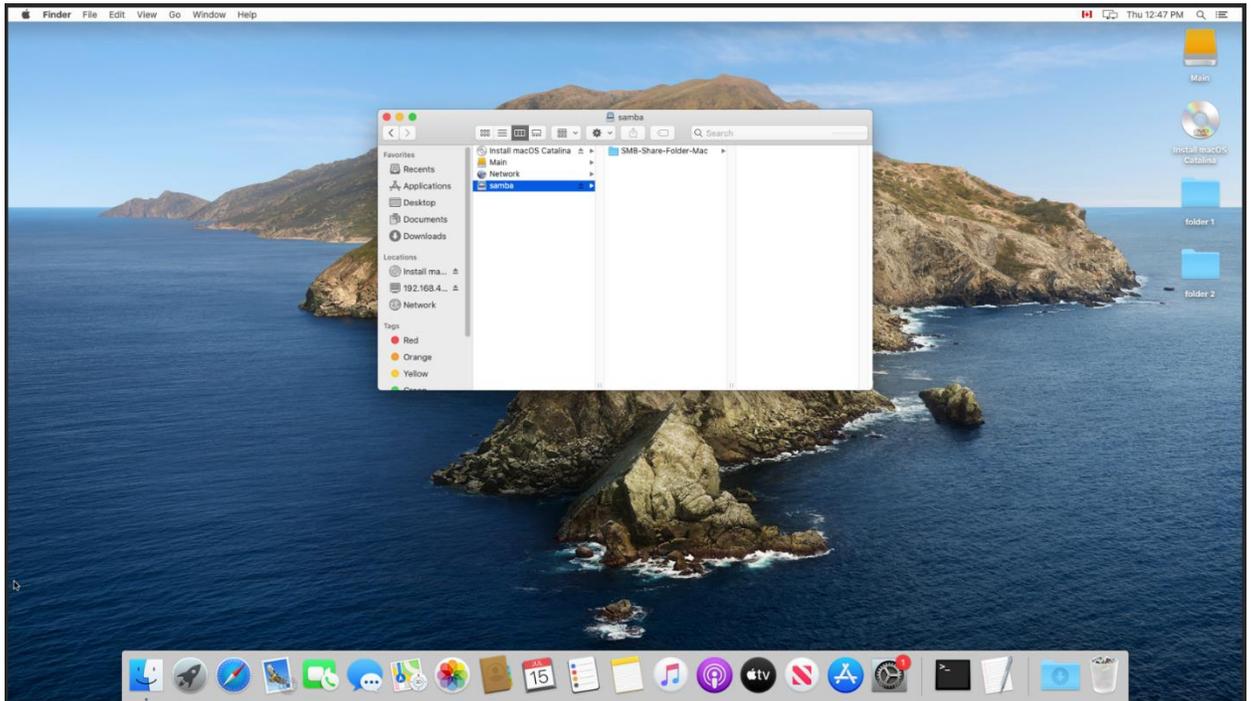
- ⊕ In the address bar, enter **smb://SERVER-IP/SHARE** and click **Connect**. We can also select the plus at the bottom to save this information if we need to reconnect.



- ⊕ Enter the login to connect to the SMB share.



- ⊕ Here we can see our SMB share is connected, and we can create a folder.

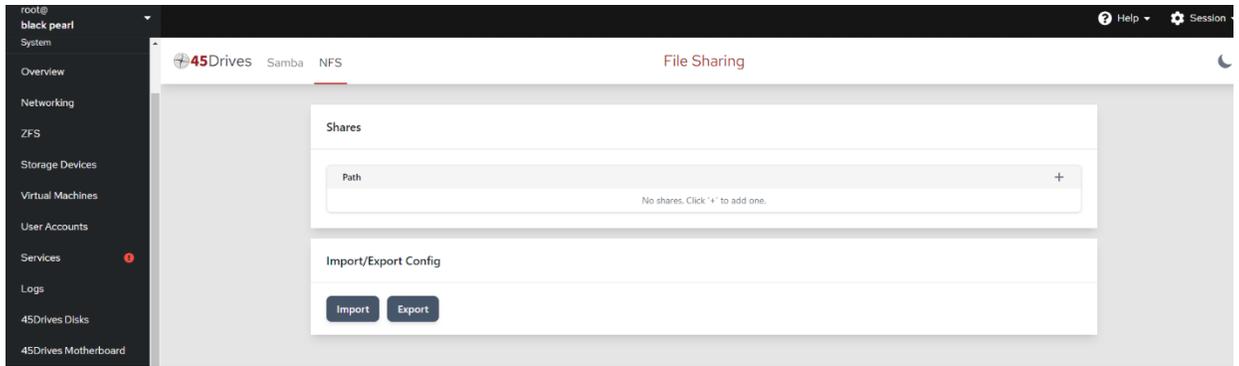


Managing NFS in Houston UI

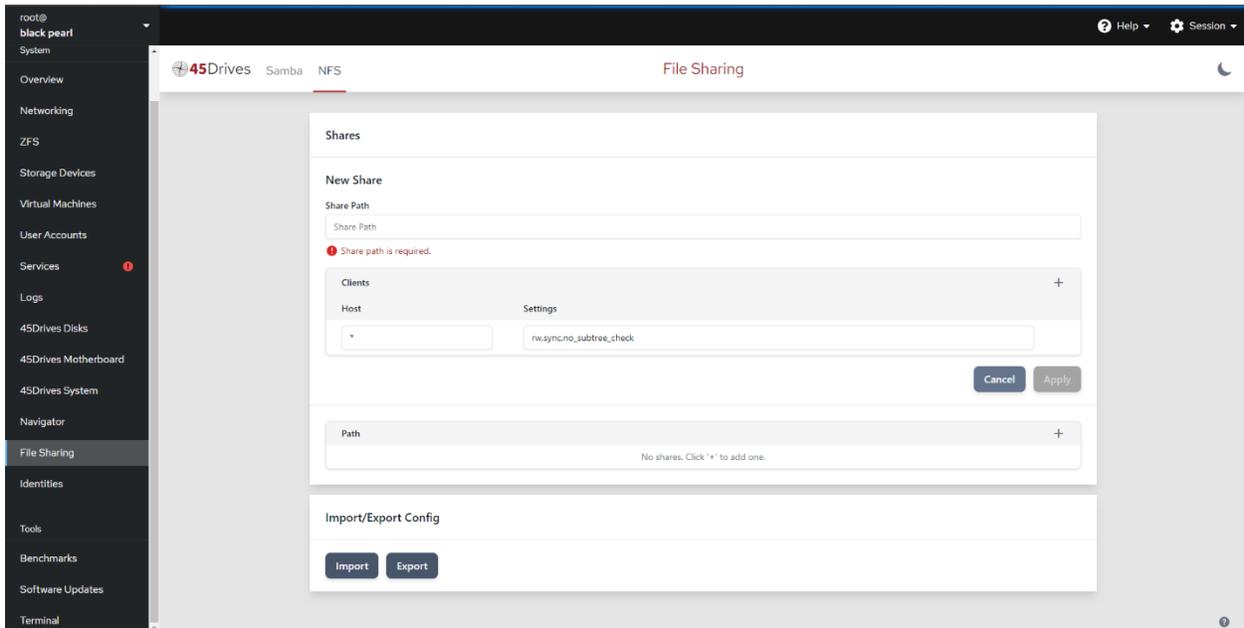


- NFS Packages Installed
- NFS Services Running and Enabled
- NFS Ports Open on Firewall (2049/tcp, and 2049/udp if NFSv3)

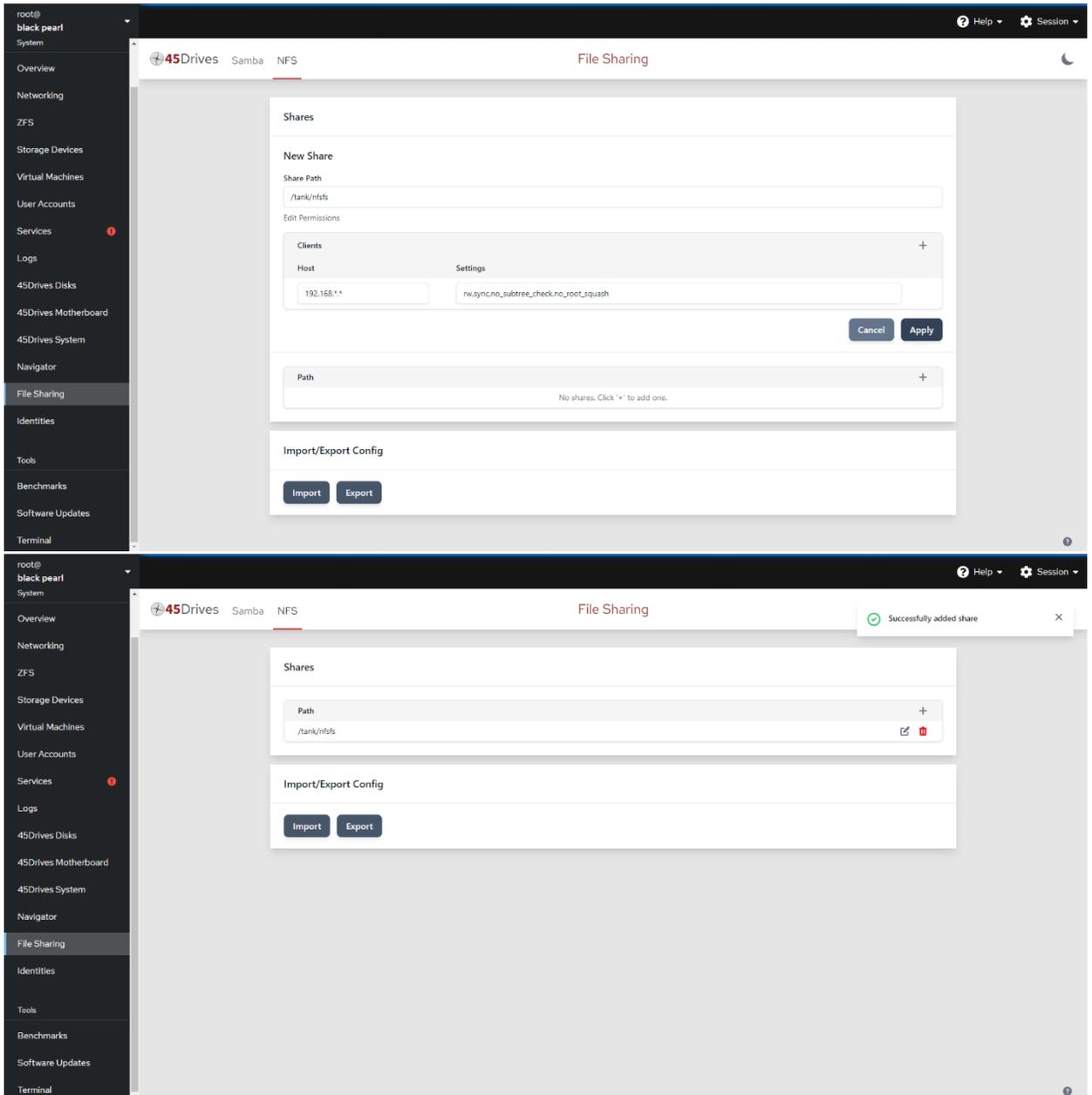
- ⊕ In Houston UI, navigate to the File Sharing tab.
- ⊕ Once in that page, we can select the NFS Tab to begin configuring our NFS shares.



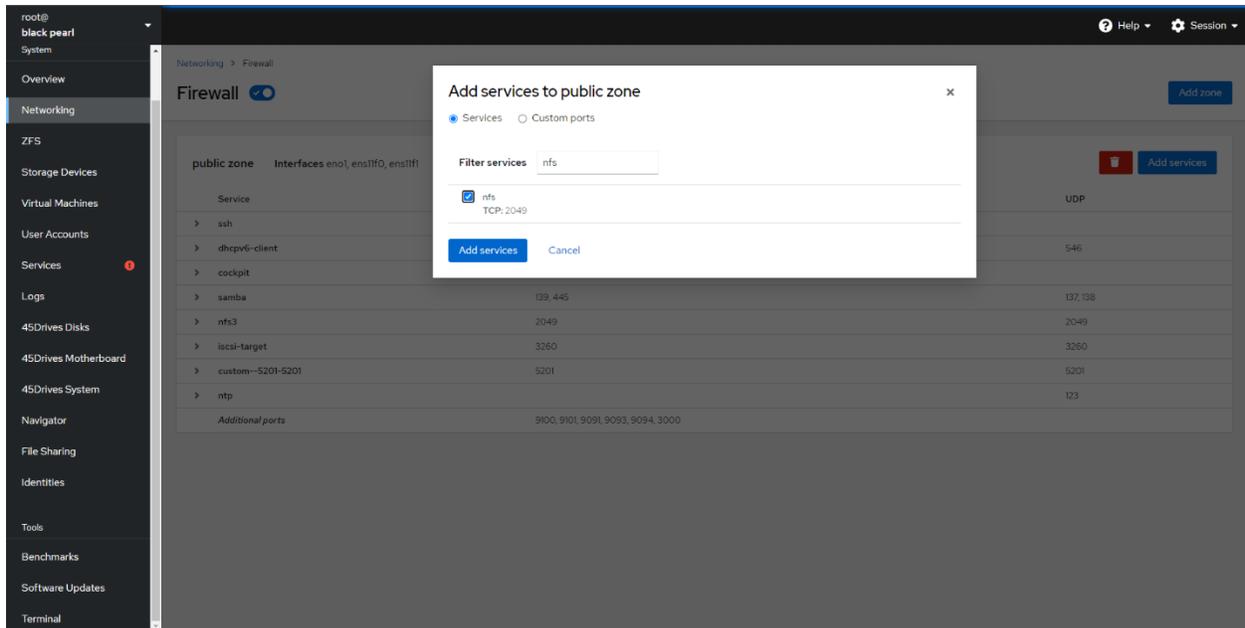
- ⊕ We first begin to create our NFS export by selecting the Plus Icon on the right.
- ⊕ We can define the path to be shared out. It would be usually /pool_name/dataset_name
- ⊕ select the range of IPs for client access, and add any additional NFS options to our share.
- ⊕ If we leave Client IP empty, it will default to everyone, and if we leave Options empty, it will default to 'rw,sync,no_subtree_check'



- ⊕ Here we create an NFS share, with a path to our NFS dataset at /tank/nfsfs. We have set the Client IP to be available to 192.168.*.*. For settings you can give "rw,sync,no_subtree_check,no_root_squash"



🌐 If you haven't opened the firewall ports then follow the below steps



Mounting NFS Share to Linux Client

Here we will discuss on the process of mounting an NFS share to a Linux client and to mount on reboot.

- ➊ Go to the terminal and run the command below to install the nfs package

install nfs-utils

- ➋ To mount an NFS share, first create a directory to mount it to.

mkdir /mnt/(mount_point)

eg :

```
mkdir /mnt/nfs_share
```

- ➌ Now use this command to mount it to the share. Edit the fields for your specific case, i.e. Server IP, Pool Name, and Share Name. See example below.

```
mount -t nfs {ServerIP}:/({pool_name})/({nfs_share_name}) /mnt/({mount_point})
```

```
mount -t nfs 192.168.35.39:/tank/nfs_sharetest /mnt/nfs_share
```

Add Mount on Reboot

- ⊕ To allow the share to mount on reboot, you will need to edit the fstab. You can use your preferred text editor, here we have used vim.

```
vim /etc/fstab
```

- ⊕ Add the mount point in the format see below.

```
{ServerIP}:/({pool_name})/({share_name}) /mnt/({mount_point}) nfs defaults,_netdev 0 0
```

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
/dev/disk/by-id/md-uuid-5bef0df4:f65beb63:7f835222:41ec8940 none swap sw 0 0
# / was on /dev/md125p1 during curtin installation
/dev/disk/by-id/md-uuid-2a10c4dd:c02a5098:0ee79f38:2078a857-part1 / ext4 defaults 0 0
# /boot was on /dev/md/swap during curtin installation
/dev/disk/by-id/md-uuid-5fbc9b25:25381cd8:2b507526:40ea9196 /boot ext4 defaults 0 0
/swap.img none swap sw 0 0
/dev/RBD-VOL GROUP/RBD-LVM /mnt/rhd xfs defaults,_netdev 0 0
192.168.35.39:/tank/nfs_sharetest /mnt/nfs_share nfs defaults 0 0
```

Verify Share Mounted

- ⊕ To ensure the share has mounted, you can run the command **df**.

```
root@ubuntu-45d:~# df
Filesystem                1K-blocks    Used   Available Use% Mounted on
udev                      65907972      0 65907972  0% /dev
tmpfs                     13190628    4004 13186624  1% /run
/dev/md126p1              117313456 16268152 95043028 15% /
tmpfs                     65953124      0 65953124  0% /dev/shm
tmpfs                      5120         0     5120    0% /run/lock
tmpfs                     65953124      0 65953124  0% /sys/fs/cgroup
/dev/md125                 4057792    221160 3610792  6% /boot
tank                      36654107136 256 36654106880 1% /tank
tank/samba-windows-acl    29137914624 256 29137914368 1% /tank/samba-wind
tank/nfs                   29137914624 256 29137914368 1% /tank/nfs
tank/samba                 29137914624 256 29137914368 1% /tank/samba
tank/smb-windows          29137914624 256 29137914368 1% /tank/smb-window
tmpfs                     13190624      0 13190624  0% /run/user/0
192.168.35.39:/tank/nfs_sharetest 2798961664 0 2798961664 0% /mnt/nfs_share
```

Verify Mount on Reboot

- ⊕ To ensure the share will mount on reboot after editing the `/etc/fstab`, unmount the share.

```
umount /mnt/nfs_share
```

- ⊕ Remount the share using the following command, this command will mount all shares in the `/etc/fstab` file.

```
mount -a
```

- ⊕ Run the command **df** again to ensure the share was mounted.

SETUP ISCSI STORAGE

- ⊕ Install necessary packages for iSCSI

```
dnf -y install targetcli
```

- ⊕ Create a ZFS dataset with your naming scheme of choice, in this case we'll use "images".
- ⊕ Multiple iSCSI LUNs can be stored in this singular dataset or new datasets can be created for each iSCSI LUN.

Create Filesystem

Parent File System: tank

Name: images

Encryption:

Access Time: Inherited (On)

Case Sensitivity: Inherited (Sensitive)

Compression: Inherited (LZ4)

Deduplication: Inherited (Off)

DNode Size: Inherited (Legacy)

Extended Attributes: Inherited (System Attribute)

NFS Share:

Quota: 0 KiB

Record Size: Inherited (128 KiB)

Options:

- SELinux contexts for Samba
- Enable Samba share
- Read only

Configuring iSCSI Target

- ⊕ Before using targetcli, we'll need to create a sparse image file. Creating large files in targetcli can be a very time-consuming process.

```
cd /tank/images  
dd if=/dev/zero of=lun0 bs=1 count=0 seek=1T
```

```
root@rocky-45d:/tank/images  
  
[root@rocky-45d ~]# cd /tank/images  
[root@rocky-45d images]# dd if=/dev/zero of=lun0 bs=1 count=0 seek=1T  
0+0 records in  
0+0 records out  
0 bytes copied, 8.9868e-05 s, 0.0 kB/s  
[root@rocky-45d images]# ls  
lun0  
[root@rocky-45d images]#
```

- ⊕ The above will create a 1 TB sparse image file named “lun0”
- ⊕ Now we’ll launch targetcli and create a fileio backstore with the sparse image we’ve created.

```
targetcli
cd backstores/fileio
create lun0 /tank/images/lun0
```

```
lun0
[root@rocky-45d images]# targetcli
Warning: Could not load preferences file /root/.targetcli/prefs.bin.
targetcli shell version 2.1.53
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/> cd backstores/fileio
/backstores/fileio> create lun0 /tank/images/lun0
Created fileio lun0 with size 1099511627776
/backstores/fileio> █
```

- ⊕ Verify the block device has been created in targetcli

```
/backstores/fileio> ls
o- fileio ..... [Storage Objects: 1]
  o- lun0 ..... [/tank/images/lun0 (1.0TiB) write-back activated]
    o- alua ..... [ALUA Groups: 1]
      o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
/backstores/fileio>
```

Create an iSCSI Target

- ⊕ Create the iSCSI target by selecting a name
- ⊕ Naming scheme: iqn.YYYY-MM.REVERSE.DOMAIN.NAME:unique
- ⊕ For this example, we’ll be using “iqn.2021-11.fourfive.lab:test.environment”

```
cd /iscsi
create iqn.2021-11.fourfive.lab:test.environment
```

```
/backstores/fileio> cd /iscsi
/iscsi> create iqn.2021-11.fourfive.lab:test.environment
Created target iqn.2021-11.fourfive.lab:test.environment.
Created TPG 1.
Global pref auto_add_default_portal=true
Created default portal listening on all IPs (0.0.0.0), port 3260.
```

Create iSCSI LUNs

```
cd iqn.2021-11.fourfive.lab:test.environment/tpg1/luns
create /backstores/fileio/lun0
```

```
/iscsi> cd iqn.2021-11.fourfive.lab:test.environment/tpg1/
/iscsi/iqn.20...ironment/tpg1> cd luns
/iscsi/iqn.20...ent/tpg1/luns> create /backstores/fileio/lun0
Created LUN 0.
```

Configure ACL (Initiator IQN)

- ⊕ When creating the ACL, it needs to be the name of the initiator IQN name of the client that will be connecting to the LUN.
- ⊕ In this example, the IQN name of the client will be "iqn.2019-05.com.archie:client"

```
/iscsi> cd iqn.2021-11.fourfive.lab:test.environment/tpg1/acls
/iscsi/iqn.20...ent/tpg1/acls> create iqn.2019-05.com.archie:client
Created Node ACL for iqn.2019-05.com.archie:client
Created mapped LUN 0.
```

Configure Authentication

- ⊕ We'll need to configure the userid and password when connecting to the LUN from the client. *This step is optional.*
- ⊕ Choose any name and password for userid and password

```
set auth userid=username
set auth password=password

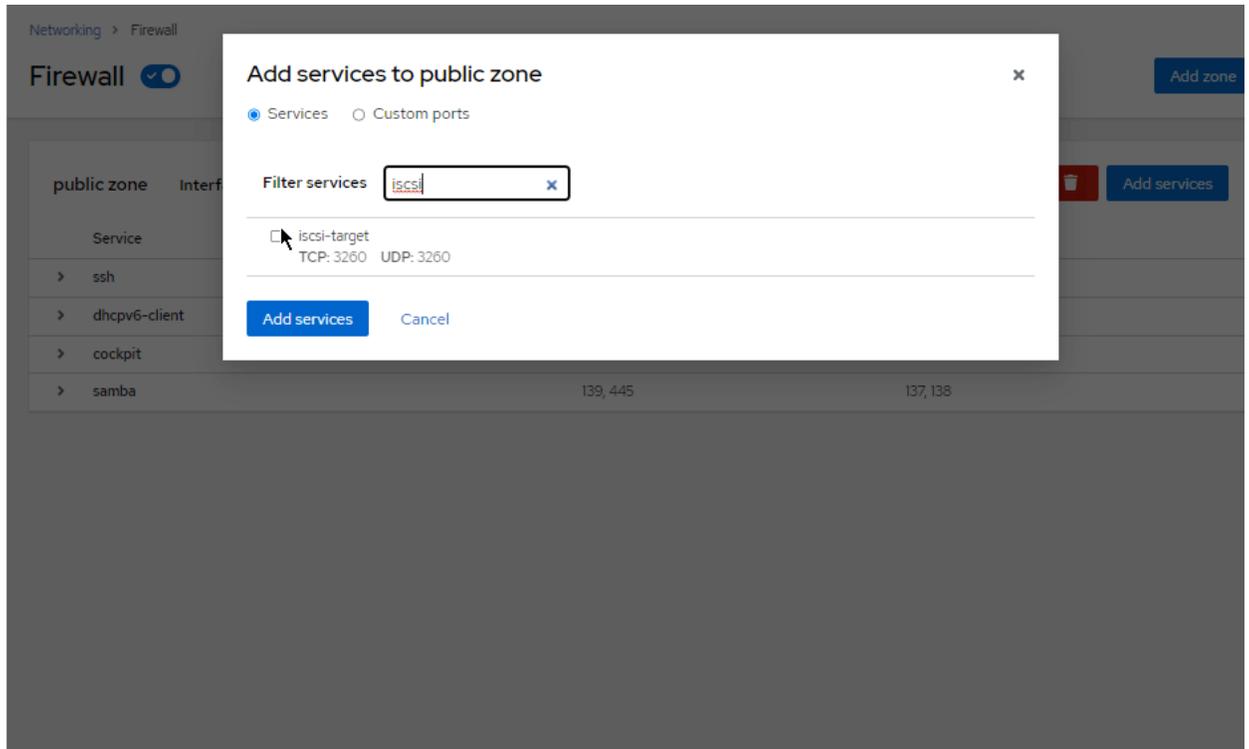
/iscsi/iqn.20...ent/tpg1/acls> cd iqn.2019-05.com.archie:client/
/iscsi/iqn.20...archie:client> set auth userid=username
Parameter userid is now 'username'.
/iscsi/iqn.20...archie:client> set auth password=password
Parameter password is now 'password'.
/iscsi/iqn.20...archie:client> █
```

Exit and Save the Configuration

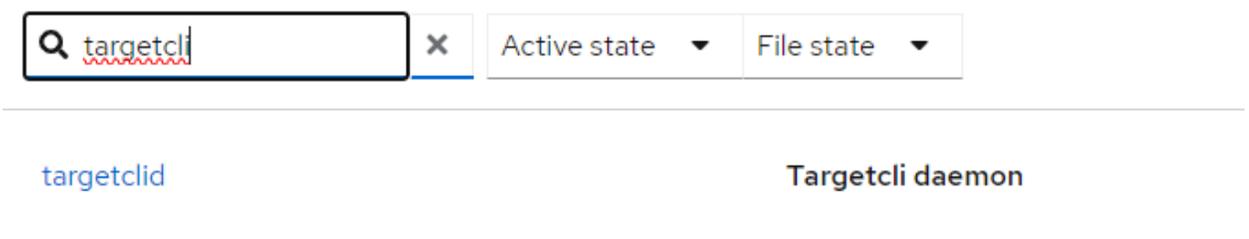
```
/iscsi/iqn.20...archie:client> exit
Global pref auto_save_on_exit=true
Configuration saved to /etc/target/saveconfig.json
```

Open Firewall for iSCSI and enable the iSCSI service

- 🔗 In the Houston UI, navigate to Networking > Firewall > Edit Zones and Rules
- 🔗 Add “iscsi-target” to the services



- 🔗 In the Houston service tab, search for “target” and enable the Targetcli daemon



Targetcli daemon  **Start and enable**

Status  Disabled

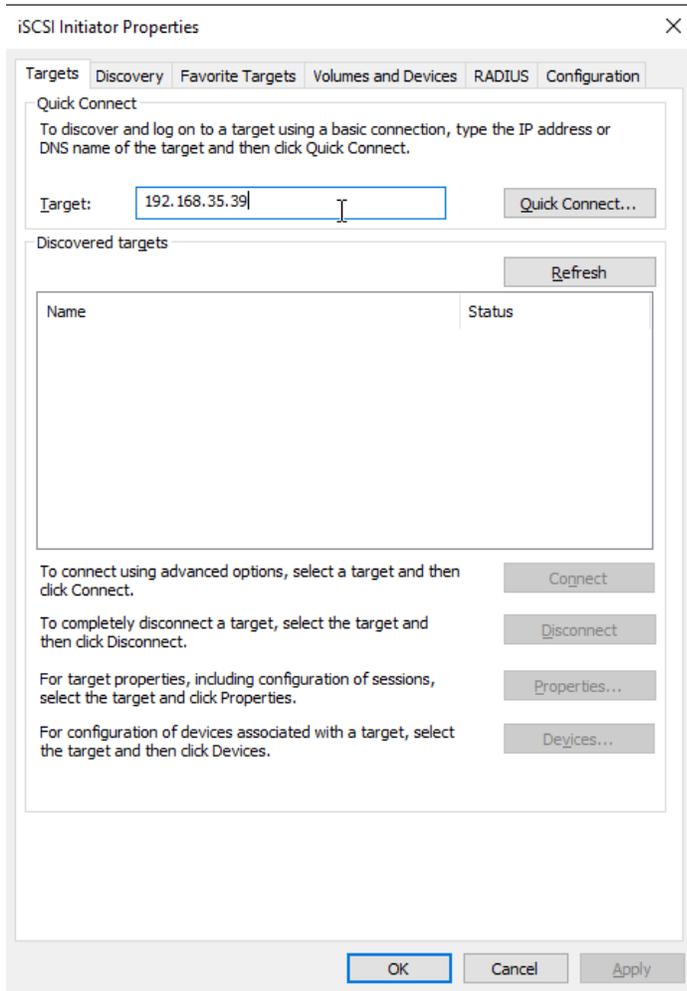
Path `/lib/systemd/system/targetcli.service`

Triggered by `targetcli.socket`

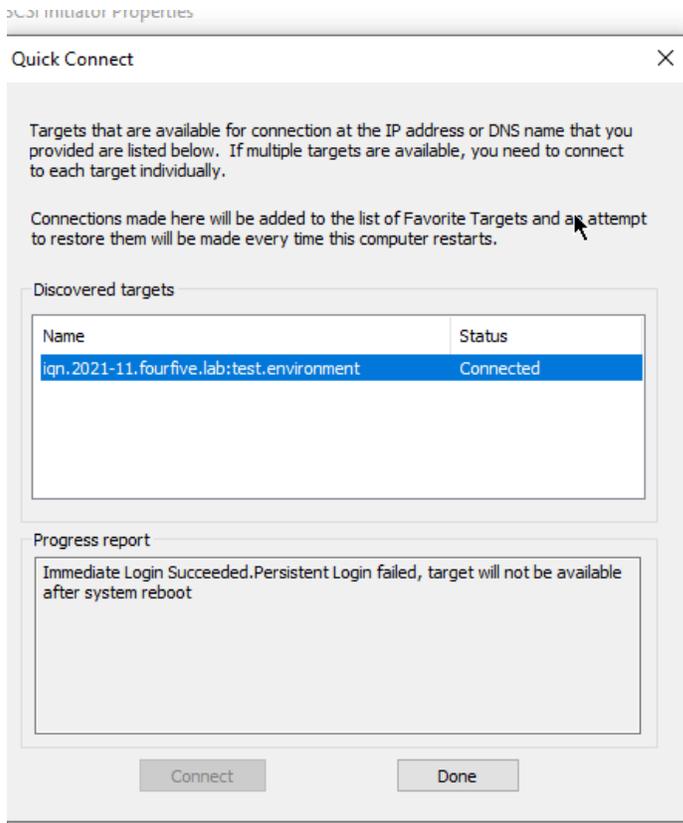
[Show more relationships](#)

Verification /Connecting to the LUN

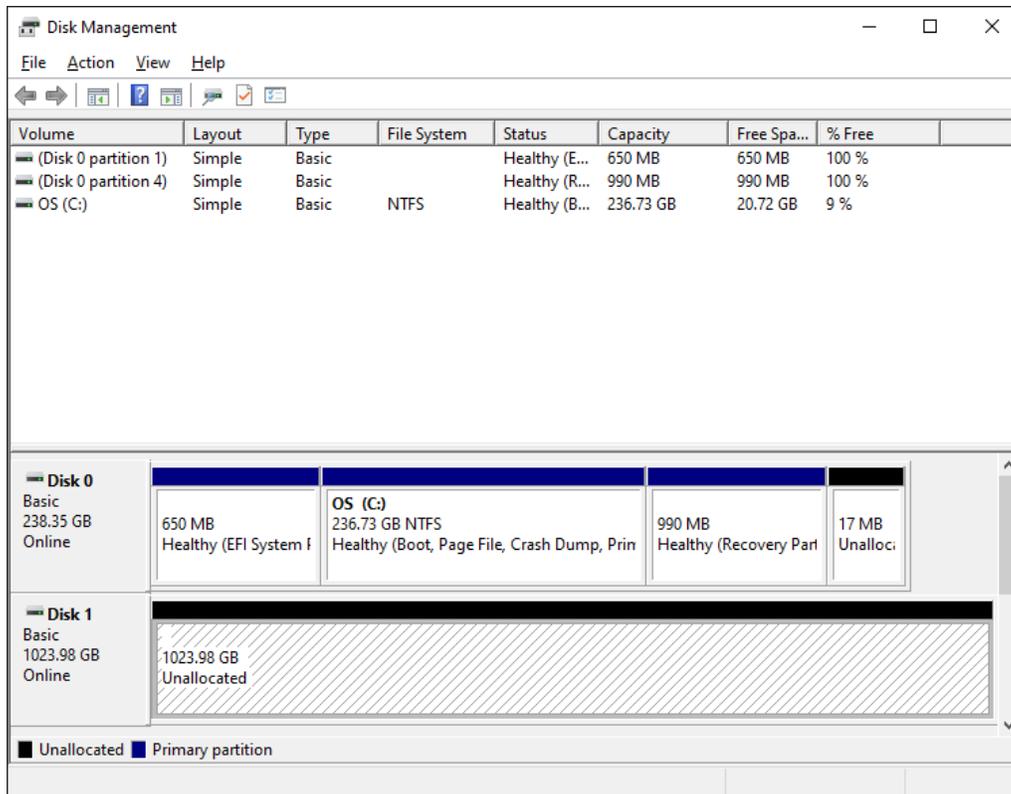
-  On a Windows client, open "iSCSI Initiator"
-  Enter the target IP address into the 'target' field



Click 'quick connect'



- ⊕ In Disk Management, there should now be a new disk that is unallocated and ready for formatting.



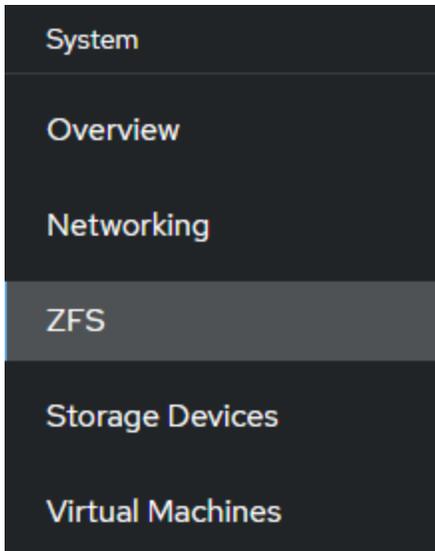
AUTOMATED ZFS REPLICATION/SNAPSHOTS IN HOUSTON UI

- ⊕ Make sure to install mbuffer and remove the old auto snapshot service on all Storinators you wish to use snapshots to use with znapzend.

```
dnf install mbuffer
```

```
systemctl restart znapzend
```

- ⊕ In the Houston UI, go to the ZFS tab.



- ⊕ Select the Dataset you wish to backup. Click the drop down on the left and select “Configure Replication Task”

tank	52.13 TiB	70.52 MiB	127.83 KiB	0 B	128 KiB	LZ4	Off	Off	Yes	No	
tank/backup	52.13 TiB	170.44 KiB	0 B	0 B	128 KiB	LZ4	Off	Off	Yes	No	!
tank/nfs	52.13 TiB	170.44 KiB	0 B	0 B	128 KiB	LZ4	Off	Off	Yes		
tank/samba	52.13 TiB	291.16 KiB	99.42 KiB	0 B	128 KiB	LZ4	Off	Off	Yes		
tank/samba-test	52.13 TiB	170.44 KiB	0 B	0 B	128 KiB	LZ4	Off	Off	Yes		
tank/samba-windows-acd	52.13 TiB	170.44 KiB	0 B	0 B	128 KiB	LZ4	Off	Off	Yes		

- Configure File System
- Edit Permissions
- Rename File System
- Unmount File System
- Destroy File System
- Configure Replication Task
- Enable Samba Share

- ⊕ The screenshot below details a task that takes a snapshot once daily, and retains the snapshots for 1 month. This can be customized to your use case.
- ⊕ Also, you can add multiple rules by clicking the +, for example setup below is for every hour for 7 days, every 4 hours for 30 days, and every 90 days for a year.

Configure Replication Task

Recursive

Destination

mBuffer Size

mBuffer Unit

Source Plans +

Retention Time

Retention Time Unit

Interval Time

Interval Time Unit

Retention Time

Retention Time Unit

Interval Time

Interval Time Unit

Retention Time

Retention Time Unit

Interval Time

Interval Time Unit

Cancel

Configure



Make sure to restart the 'znapzend' service after any change has been made to snapshot tasks

`znapzend`

ZnapZend - ZFS Backup System

- ⊕ To ensure the snapshots are being created you can go to the Snapshots section of the ZFS to see all snapshots that were created.

SOFTWARE

45HomeLab comes with Rocky as the default OS and Houston UI for the server management. Apart from that you can install other software stacks as well as per your preference. We have included some of them for your reference.

PORTAINER



With the help of Portainer, you can easily interact with containerized programs, monitor your Docker installation, and set up new stacks. To centralize your container administration around a single application, a single Portainer instance may link to numerous Docker hosts.

Make sure docker is installed before you proceed.

- ⊕ Create the docker volume
`docker volume create portainer_data`

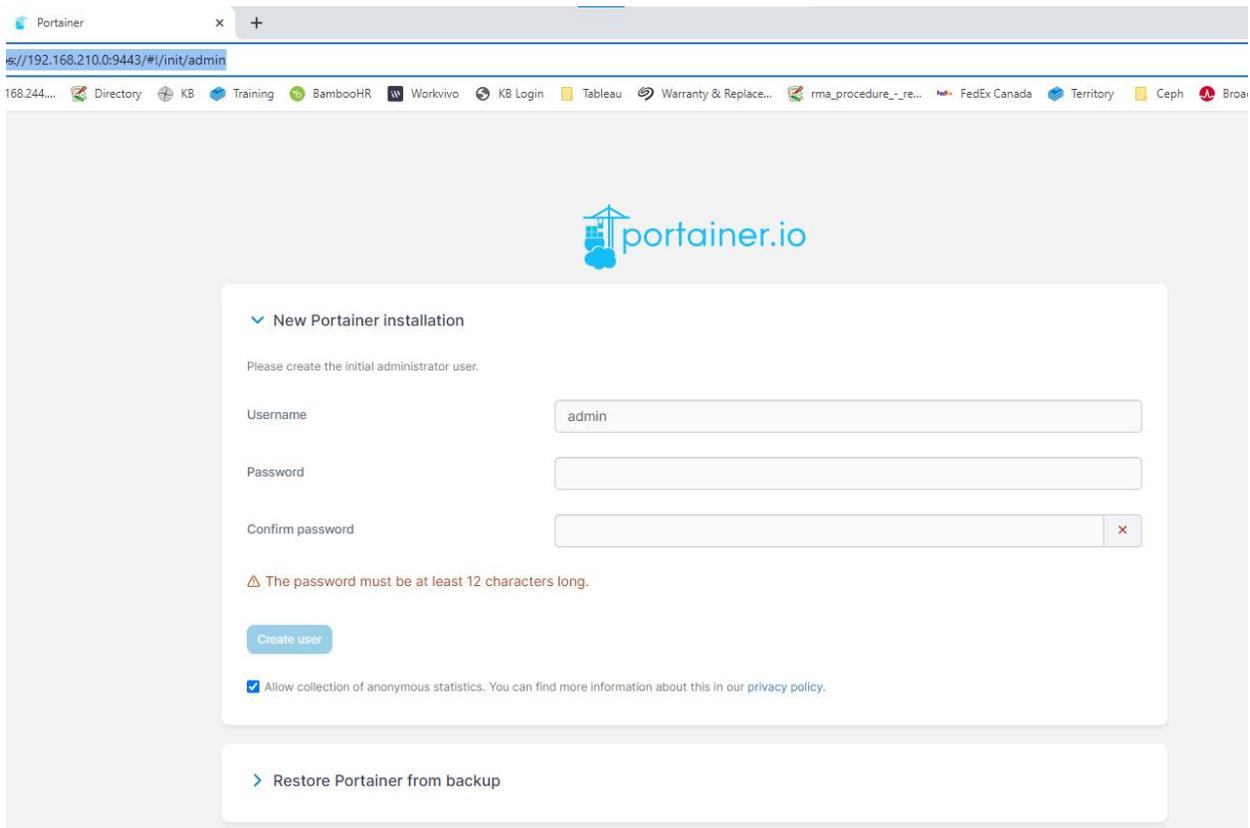
```
[root@storinator ~]# docker volume create portainer_data
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
portainer_data
[root@storinator ~]# █
```

- ⊕ `docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest`

```
[root@HL15 ~]# docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest
Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.
? Please select an image:
  registry.access.redhat.com/portainer/portainer-ce:latest
  registry.redhat.io/portainer/portainer-ce:latest
  > docker.io/portainer/portainer-ce:latest

[root@HL15 ~]# docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest
Unable to find image 'portainer/portainer-ce:latest' locally
latest: Pulling from portainer/portainer-ce
795a208431d7: Pull complete
4f272ca3dde3: Pull complete
5171176db7f2: Pull complete
52e9438966a5: Pull complete
43d4775415ac: Pull complete
c1cad9f5200f: Pull complete
27d6dca9cab4: Pull complete
231d7e50ef35: Pull complete
589f2af34593: Pull complete
5fc2ddaa6f07: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:f29cbc7b26ebd701b1fe92b4df42edea350e871372a6296a1fa16ba999481fb2
Status: Downloaded newer image for portainer/portainer-ce:latest
f786478bed70e71711e9c1540c15a94980ccaf401bd8ca9f1be857dde24f156
[root@HL15 ~]#
```

- ⊕ The portainer will be on port 9443 so access it using <https://serverip:9443>
- ⊕ Make sure the port is open in firewall.
- ⊕ Create the admin user



- ⊕ You can click on getting started.
- ⊕ You can check more on the documentation at <https://docs.portainer.io/>

The screenshot shows the Portainer web interface. On the left is a dark blue sidebar with the Portainer logo and a navigation menu including Home, Environment (None selected), Settings, Users, Environments, Registries, Authentication logs, Notifications, and Settings. The main content area is titled 'Environment Wizard' and 'Quick Setup'. It features a 'Welcome to Portainer' message stating that the local Docker environment is connected. Below the message are two large buttons: 'Get Started' (with a Docker ship icon) and 'Add Environments' (with a plug icon). The 'Get Started' button includes the text 'Proceed using the local environment which Portainer is running in', and the 'Add Environments' button includes 'Connect to other environments'.

- ⊕ You should have portainer local environment like below

The screenshot shows the 'Environments' page in Portainer. At the top, there's a header 'Environments' and a sub-header 'Click on an environment to manage'. Below this are several filter buttons: Platform, Connection Type, Status, Tags, and Groups. A table lists the environments. The first entry is 'local', which is marked as 'Up' with a green checkmark. It shows a timestamp of '2023-10-03 11:47:48', connection type 'Standalone 24.0.6', and socket path '/var/run/docker.sock'. Below the table, there are statistics for the 'local' environment: 0 stacks, 1 container, 1 volume, 1 image, 1 CPU, and 1.9 GB RAM.

Now you have your portainer ready to deploy other software stacks.

INSTALLING NGINX PROXY MANAGER(NPM) ON PORTAINER

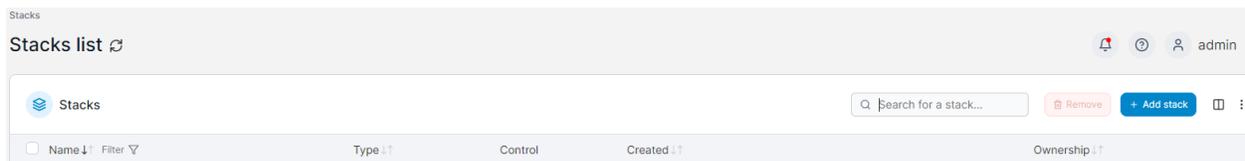


NGINX

PROXY MANAGER

Below would be the steps to install NPM to set up proxy for custom ports for various applications.

- ➊ Go to your portainer home and select your environment.
- ➋ Click on stacks and add a new stack.



- ➌ Give a name for your stack. For example, we can give npm.
- ➍ Paste the below contents on the web editor

```
version: '3'  
volumes:  
  npm-data:  
  npm-ssl:  
  npm-db:  
networks:  
  frontend:
```

backend:

services:

npm-app:

image: jc21/nginx-proxy-manager:2.9.19

restart: always

ports:

- "80:80"
- "81:81"
- "443:443"

environment:

- DB_MYSQL_HOST=npm-db
- DB_MYSQL_PORT=3306
- DB_MYSQL_USER=npm
- DB_MYSQL_PASSWORD=thisisjustatest
- DB_MYSQL_NAME=npm

volumes:

- npm-data:/data
- npm-ssl:/etc/letsencrypt

networks:

- frontend
- backend

npm-db:

image: jc21/mariadb-aria:latest

restart: always

environment:

- MYSQL_ROOT_PASSWORD=thisisjustatest
- MYSQL_DATABASE=npm
- MYSQL_USER=npm
- MYSQL_PASSWORD=thisisjustatest



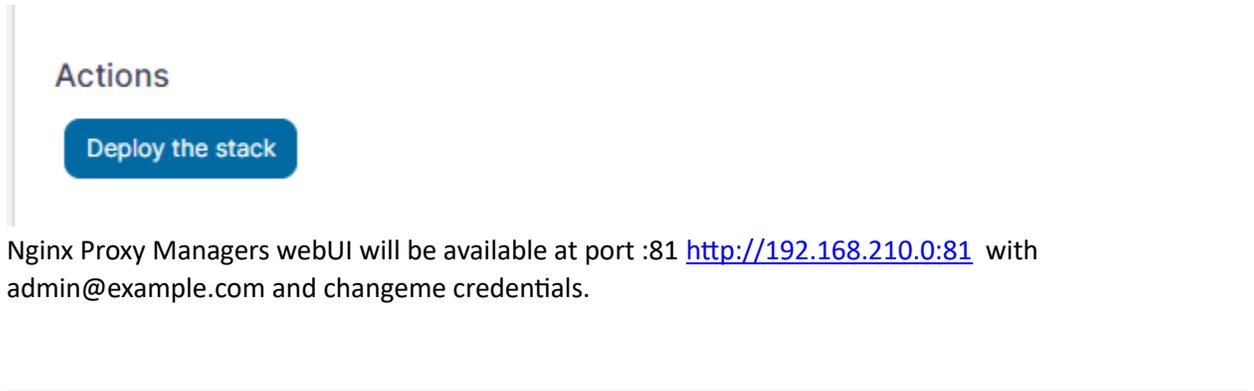
volumes:

- npm-db:/var/lib/mysql

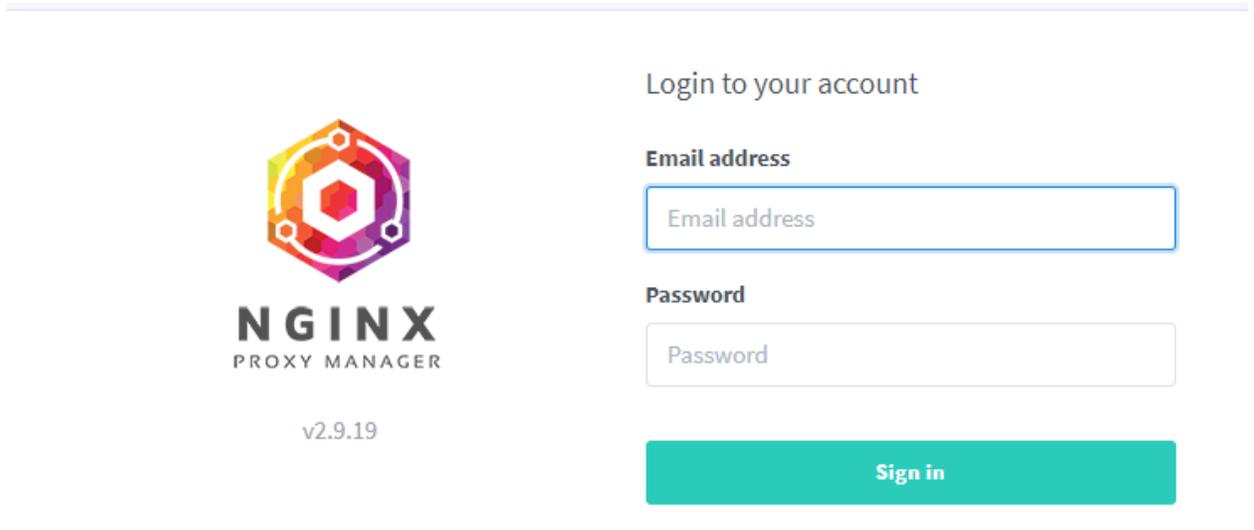
networks:s

- backend

- ⊕ After that click on deploy stack and wait for the deployment to be completed.



- ⊕ Nginx Proxy Managers webUI will be available at port :81 <http://192.168.210.0:81> with admin@example.com and changeme credentials.



- ⊕ Once in set the admin account email id and password
- ⊕ After that you can start creating your proxies.

NEXTCLOUD AND NPM ON PORTAINER



In portainer navigate to "Images" and select Build a New Image:

A screenshot of the Portainer web interface showing the "Images" section. The left sidebar contains navigation options like Home, local, Dashboard, App Templates, Stacks, Containers, Images (highlighted), Networks, Volumes, Events, Host, Settings, Users, Environments, Registries, Authentication logs, and Notifications. The main content area is titled "Image list" and includes a "Pull image" form with fields for Registry (set to Docker Hub) and Image*. Below the form is a table of existing images with columns for Id, Tags, Size, and Created. A notification at the bottom left indicates a new version (2.19.1) is available.

Id	Tags	Size	Created
sha256:189de649cd8acd751d8098d4433eee...	ghcr.io/mmlch-app/mmlch-server:release	1 GB	2023-09-21 11:54:45
sha256:222c92ef03b46a36f2d0cbf3db5823...	ghcr.io/mmlch-app/mmlch-web:release	237.6 MB	2023-09-21 11:19:37
sha256:8eefd35967bda5f3081cf0f830ca60...	ghcr.io/mmlch-app/mmlch-machine-learning:release	1.7 GB	2023-09-21 11:19:32
sha256:c12ce36b74c55dd3cdc0ebae1a38fa...	45cloud:latest	1.8 GB	2023-09-21 10:35:27
sha256:79e49d7ee6ecc058f871549090dad2...	nextcloud:latest	1.2 GB	2023-09-21 05:30:01
sha256:ca907ba6074f5396e8b47e4520c93a...	linuxserver/plex:latest	339.2 MB	2023-09-18 13:37:20
sha256:63b1b25d35d2ed445c1f0f5ef202f8...	plexinc/plex-docker:latest	325.3 MB	2023-09-18 12:04:38

- 🌐 Name the new image "45cloud" and paste the contents of <https://github.com/45Drives/scripts/blob/main/nextcloud/Dockerfile>

The screenshot shows the Portainer Builder interface. At the top, there are tabs for 'Builder' and 'Output'. Below this is the 'Naming' section, which includes a text input field containing '45cloud' and a 'Build method' section with three options: 'Web editor' (selected), 'Upload', and 'URL'. Below the 'Web editor' section, there is a text area containing a Dockerfile script:

```
1 FROM nextcloud
2 RUN apt-get update && apt-get install -y bash
3 RUN apt install smbclient libsmbclient-dev -y
4 RUN apt install cron -y
5 RUN apt install libmagiccore-6.q16-6-extra -y
6 RUN apt install ffmpeg -y
7 RUN apt install nano -y
8 RUN pecl install smbclient
9 RUN docker-php-ext-enable smbclient
```

- 🌐 Then click "Build the image", this will start the build process, wait until this completes.
- 🌐 Then navigate to the "Stacks" tab, and click "Add Stack"

The screenshot shows the Portainer Stacks list interface. On the left is a sidebar with navigation options: Home, local, Dashboard, App Templates, Stacks (highlighted), Containers, Images, Networks, Volumes, Events, and Host. The main area displays a 'Stacks list' table with the following data:

Name	Type	Control	Created	Ownership
nginx-proxy-manager	Compose	Total	2023-09-20 11:52:57 by admin	administrators

- 🌐 Name the stack nextcloud-nginx and paste the following into the text box:

- ⊕ If you already have NPM installed remove those NPM sections from the text below when pasting into the web editor.

```
version: "3"

volumes:
  nextcloud-data:
  nextcloud-db:
  npm-data:
  npm-ssl:
  npm-db:

networks:
  frontend:
  backend:

services:
  nextcloud-app:
    image:
    45cloud:latest
    restart: always
    volumes:
      - nextcloud-
    data:/var/www/html
    environment:
      - MYSQL_PASSWORD=thisisjustatest
      - MYSQL_DATABASE=nextcloud
      - MYSQL_USER=nextcloud
      - MYSQL_HOST=nextcloud-db
      - PHP_UPLOAD_LIMIT=200G
    networks:
      - frontend
```

- backend

nextcloud-db:

image:

mariadb:10.5

restart: always

command: --transaction-isolation=READ-COMMITTED --binlog-

format=ROW volumes:

- nextcloud-

db:/var/lib/mysql

environment:

- MYSQL_ROOT_PASSWORD=thisisjustatest
- MYSQL_PASSWORD=thisisjustatest
- MYSQL_DATABASE=nextcloud
- MYSQL_USER=nextcloud
- OVERWRITEPROTOCOL=https

networks:

- backend

npm-app:

image: jc21/nginx-proxy-

manager:2.9.19 restart: always

ports:

- "80:80"
- "81:81"
- "443:443"
- "8900:8900"
- "32400:32400"
- "2283:2283"

environment:

- DB_MYSQL_HOST=npm-db
- DB_MYSQL_PORT=3306
- DB_MYSQL_USER=npm
- DB_MYSQL_PASSWORD=thisisjustatest
- DB_MYSQL_NAME=npm

volumes :

- npm-data:/data
- npm-

ssl:/etc/letsencrypt

networks:

- frontend
- backend

npm-db:

image: jc21/mariadb-aria:latest restart:

always

environment:

- ⊕ MYSQL_ROOT_PASSWORD=thisisjustatest
- ⊕ MYSQL_DATABASE=npm
- ⊕ MYSQL_USER=npm
- ⊕ MYSQL_PASSWORD=thisisjustat

est volumes:

- ⊕ npm-

db:/var/lib/mysql

networks:

- ⊕ backend

- ⊕ Click Deploy Stack and wait for it to finish
- ⊕ At this point all configuration steps are identical to:
<https://knowledgebase.45drives.com/kb/kb450427-nextcloud-with-nginx-proxy-manager-on-ubuntu-20-04/>
- ⊕ Nginx Proxy Managers webUI will be available at port :81 with admin@example.com and changeme credentials.
- ⊕ When creating your proxy host use the name of the container found in the containers tab of portainer.

CONFIGURING PLEX PORTAINER



➦ Go to portainer and create a new volume called plex_config

A screenshot of the Portainer web interface showing the 'Create volume' configuration page. The page title is 'Create volume'. The 'Name' field contains 'plex_config'. Under 'Driver configuration', the 'Driver' is set to 'local'. There are two toggle switches for 'Use NFS volume' and 'Use CIFS volume', both currently turned off. Under 'Access control', the 'Enable access control' toggle is turned on. Two access control options are shown: 'Administrators' (selected with a blue checkmark) and 'Restricted'. At the bottom, there is a 'Create the volume' button. The left sidebar shows the Portainer navigation menu with 'Volumes' highlighted.

➦ Then go to create a container name as you want example "plexmedia"

➦ For the image give **linuxserver/plex:latest**

Create container

Name

Image configuration

Registry

Image*

 Advanced mode

Always pull the image 

-  Under volumes click on map additional volume and create a volume with container path of /config to the volume you created in step 1

 Advanced container settings

Command & logging **Volumes** Network Env Labels R

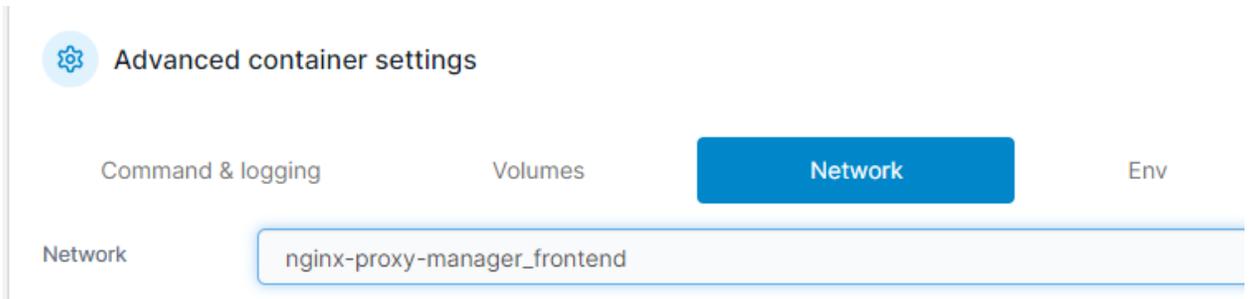
Volume mapping [+ map additional volume](#)

container	/config	Volume	Bind	
→ volume	plex_config - local	Writable	Read-only	

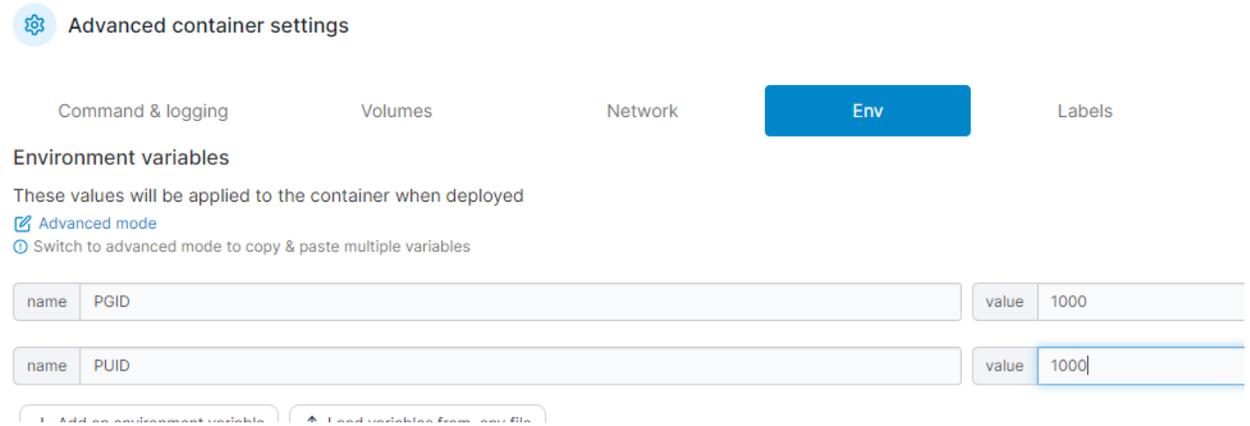
-  Click on map additional volume and create a second bind volume with container path to /media. This name can change to whatever and bind it to the host path that they want to store media such as a zpool, etc. (here we can use our path in the zpool where our storage is).

container	/media	Volume	Bind	
→ host	/tank/plexmedia	Writable	Read-only	

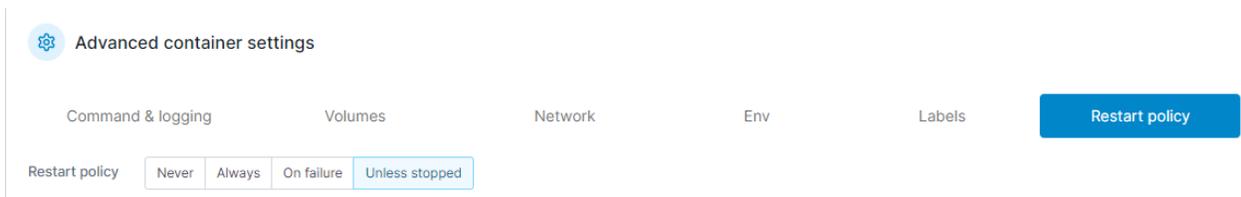
-  Under network select the nginx proxy frontend network



Under ENV click on add environment variable and throw in PGID 1000 and PUID 1000. Here 1000 is the ID of the user that we are given ownership of the content, so add the ID accordingly.



Select a restart policy of unless stopped



deploy the container

Actions

Auto remove ?

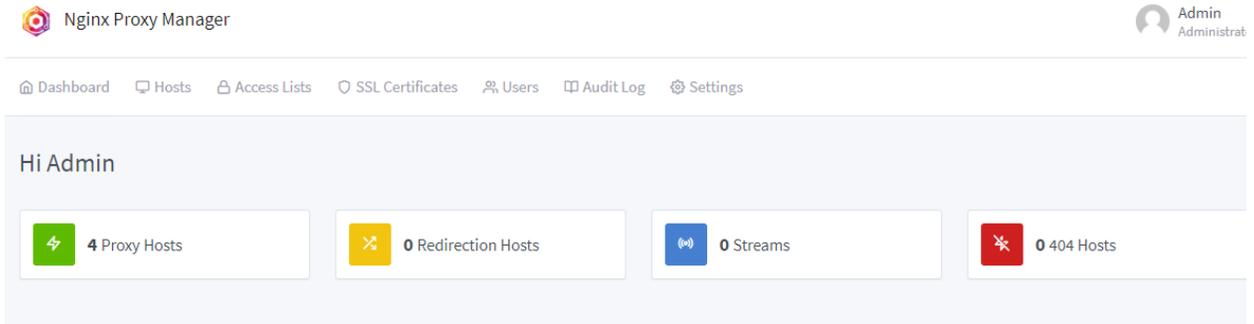


Deploy the container

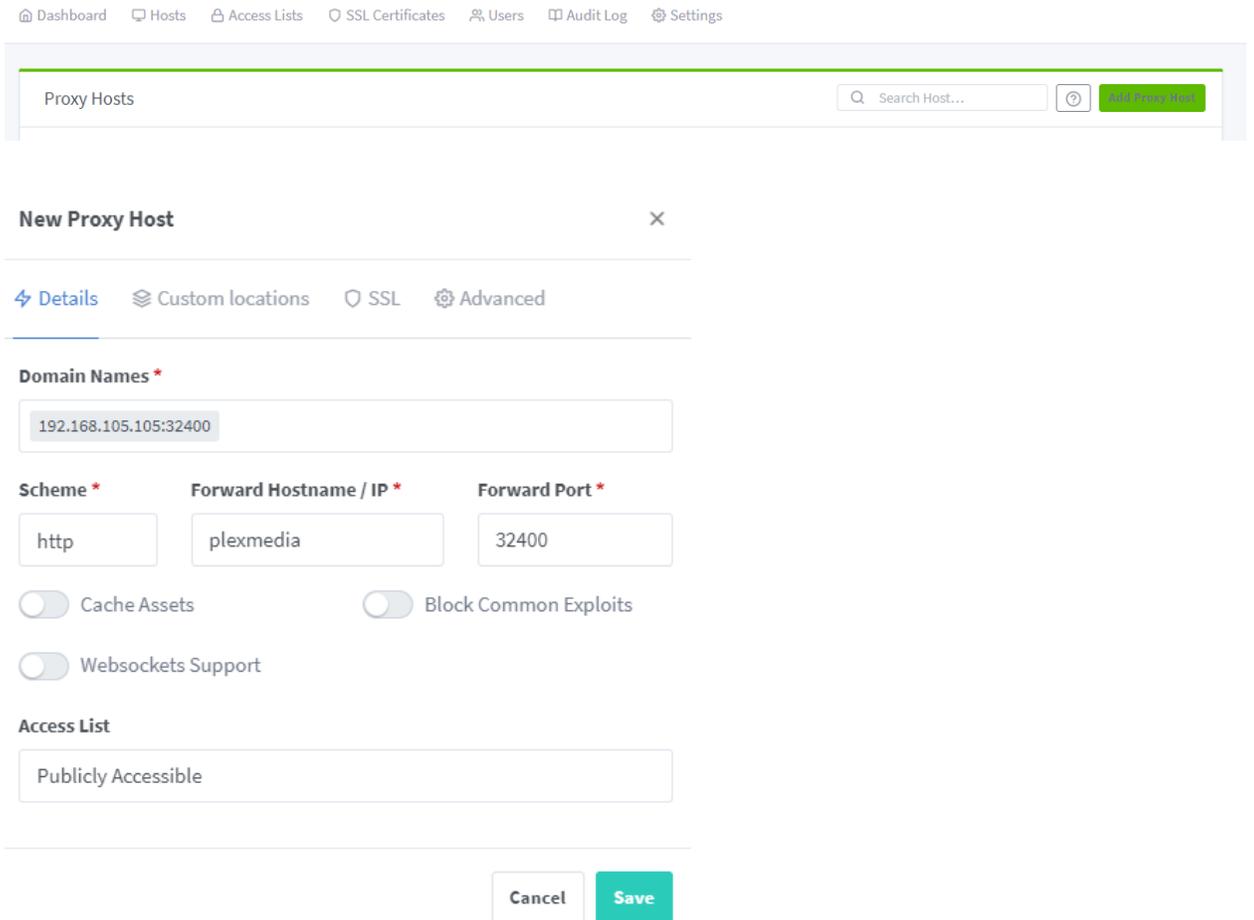
You should be able to see that the container is deployed and running.



- ⊕ Nginx Proxy Managers web UI will be available at port :81 with admin@example.com and 'change me' credentials.
- ⊕ When creating your proxy host use the name of the container found in the containers tab of portainer.
- ⊕ Create a proxy host with domain name IP:PORT or DNS name if they are port forwarding or have a hostname select scheme (http/https), forward hostname is the name of the container and forward port by default would be 32400. Then under advanced custom nginx config put in "listen 32400;"
- ⊕ Click on proxy hosts



- ⊕ Add proxy host



- ⊕ In the advanced give the below and save

Edit Proxy Host ✕

⚡ Details  Custom locations  SSL  **Advanced**

These proxy details are available as nginx variables:

- `$server` Forward Hostname / IP
- `$port` Forward Port
- `$forward_scheme` Scheme

Custom Nginx Configuration

```
listen 32400;
```

⚠ Please note, that any `add_header` or `set_header` directives added here will not be used by nginx. You will have to add a custom location `'/'` and add the header in the custom config there.

- ⊕ Now you can access your plex using <http://serverip:32400/web/index.html#!/>
- ⊕ Make sure the port is open in firewall.
- ⊕ Sign in or create a plex account

Plex Web

would like to sign in to your Plex account



This application is at **192.168.105.105** and is not hosted by Plex. Continue only if you recognize this server and wish to grant access.

 Continue with Google

 Continue with Facebook

 Continue with Apple

or

Email or Username

Password

[Forgot?](#)

Sign In

Need an account? Press the Google, Facebook, or Apple buttons above, or **sign up with email**

How Plex Works

Plex Media Server runs on the computer where you keep your media



Plex scans your media, automatically organizes it, and makes it beautiful

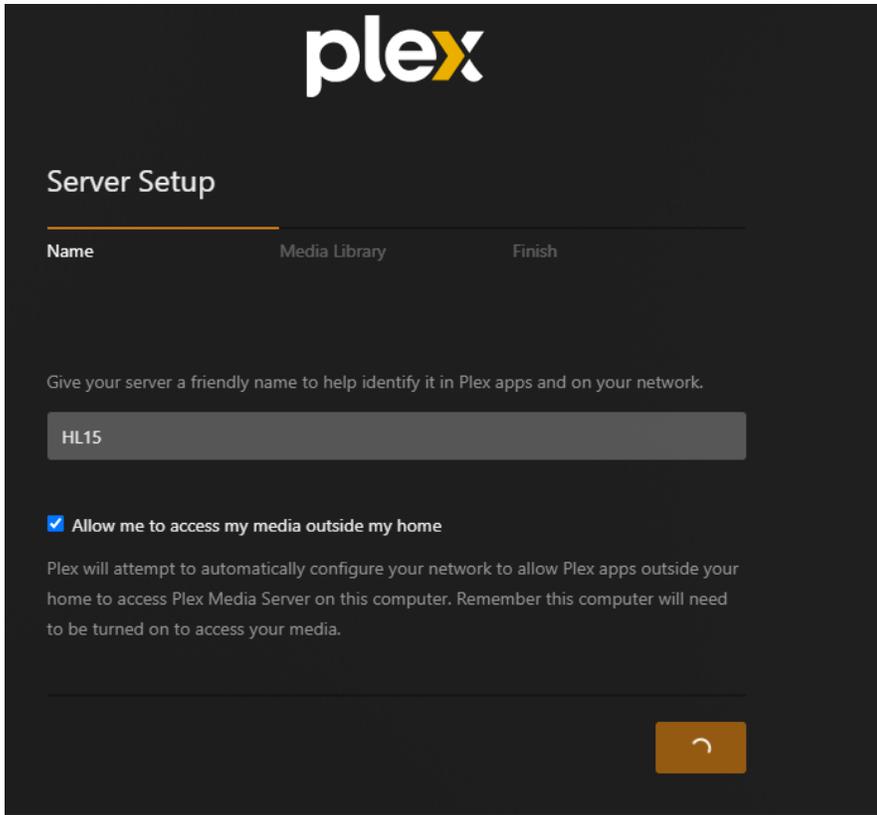


Play your media on any screen with your favorite Plex app

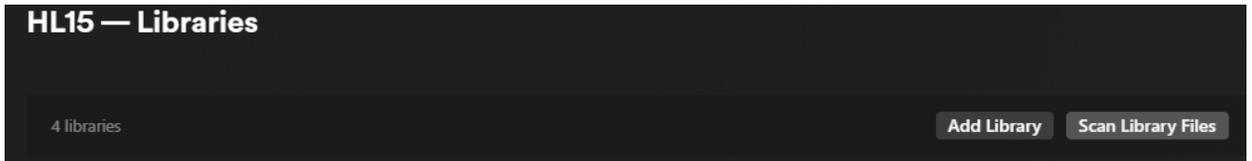


Got It!

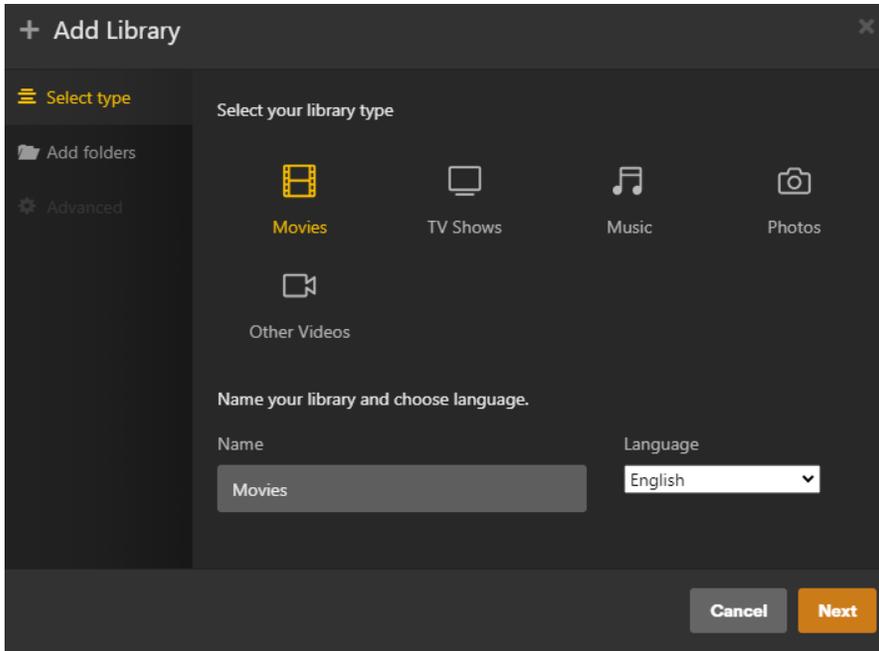
⊕ After that you can set up the library as per your wish



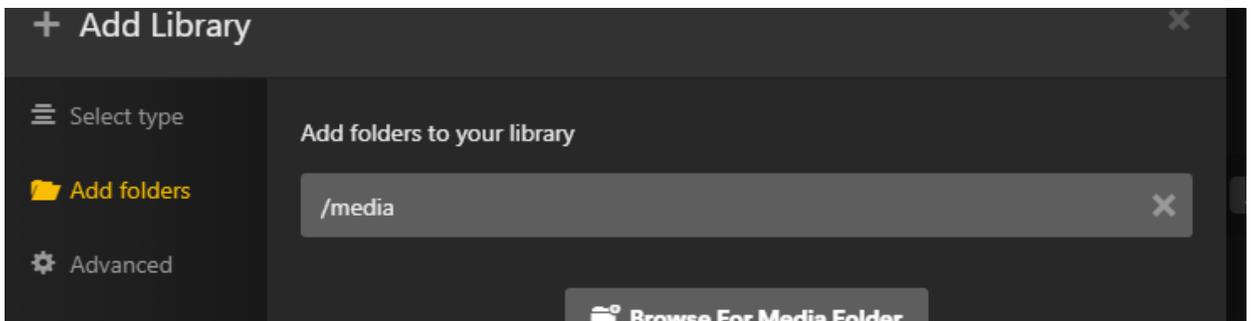
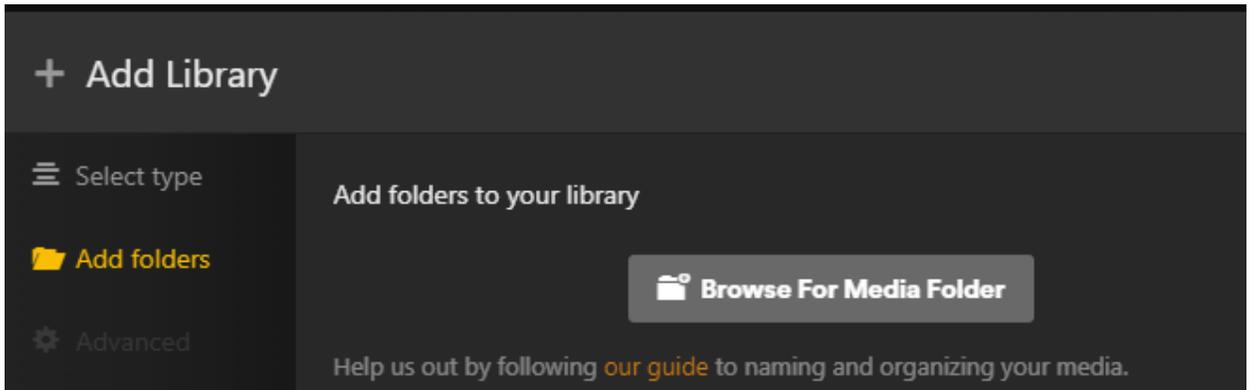
- Click on add libraries



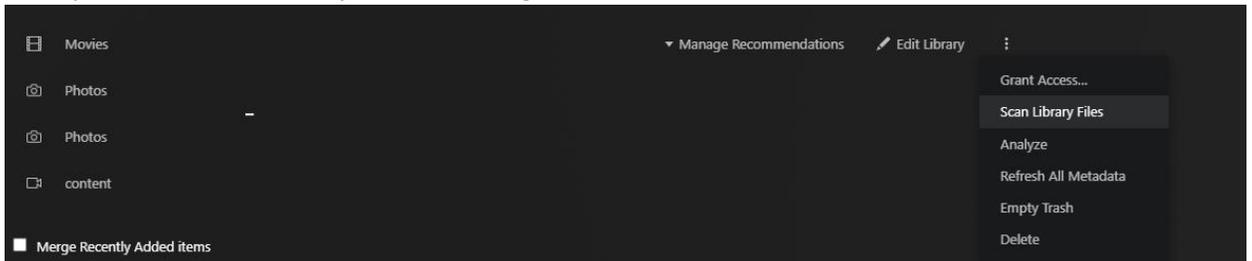
- You can select the library type and then select the media folder that we had linked to our storage in HL15



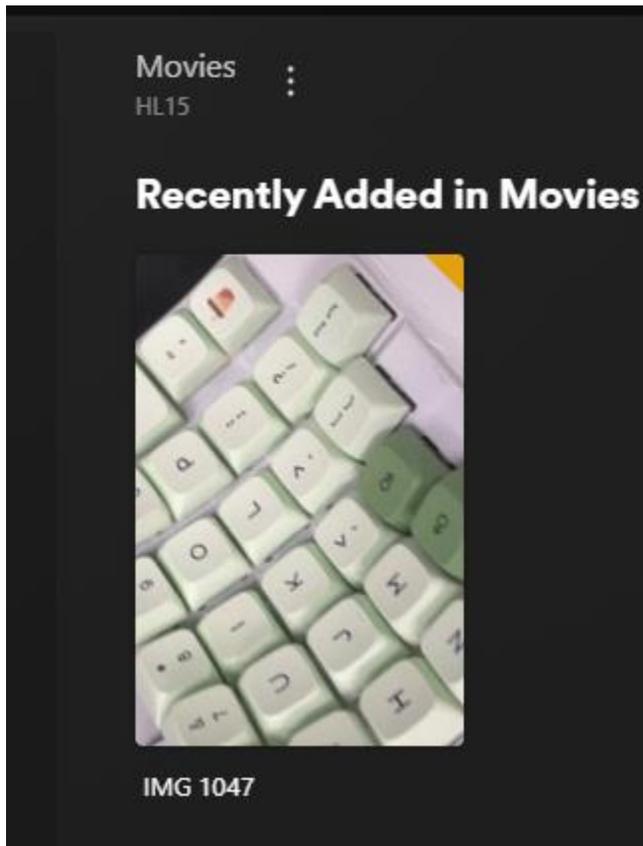
- ⊕ After that select the folder, we are selecting media as we had given that during our container creation.



- Then you can scan the library for the existing files



- You will be able to see the videos that are there in your server in the dataset or path you had given.



You can check <https://support.plex.tv/articles/200264746-quick-start-step-by-step-guides/> for more guides and info.

IMMICH- self-hosted backup solution for photos and videos



- ⊕ Go to "Stacks" in the left sidebar.
- ⊕ Click on "Add stack".
- ⊕ Give the stack a name (i.e. Immich), and select "Web Editor" as the build method.
- ⊕ Copy the content of the docker-compose.yml file (github repo - <https://github.com/immich-app/immich/releases/latest/download/docker-compose.yml>)

```
version: "3.8"
```

```
services:
```

```
  immich-server:
```

```
    container_name: immich_server
```

```
    image: ghcr.io/immich-app/immich-server:${IMMICH_VERSION:-release}
```

```
    command: ["start.sh", "immich"]
```

```
    volumes:
```

```
      - ${UPLOAD_LOCATION}:/usr/src/app/upload
```

```
      - /etc/timezone:/etc/timezone:ro
```

```
      - /etc/localtime:/etc/localtime:ro
```

```
    env_file:
```

```
- stack.env
depends_on:
  - redis
  - database
  - typesense
restart: always
```

immich-microservices:

```
container_name: immich_microservices
image: ghcr.io/immich-app/immich-server:${IMMICH_VERSION:-release}
# extends:
#   file: hwaccel.yml
#   service: hwaccel
command: ["start.sh", "microservices"]
volumes:
  - ${UPLOAD_LOCATION}:/usr/src/app/upload
  - /etc/timezone:/etc/timezone:ro
  - /etc/localtime:/etc/localtime:ro
env_file:
  - stack.env
depends_on:
  - redis
  - database
  - typesense
restart: always
```

immich-machine-learning:

```
container_name: immich_machine_learning
image: ghcr.io/immich-app/immich-machine-learning:${IMMICH_VERSION:-release}
volumes:
  - model-cache:/cache
env_file:
  - stack.env
```

```
restart: always

immich-web:
  container_name: immich_web
  image: ghcr.io/immich-app/immich-web:${IMMICH_VERSION:-release}
  env_file:
    - stack.env
  restart: always

typesense:
  container_name: immich_typesense

  image:
typesense/typesense:0.24.1@sha256:9bcff2b829f12074426ca044b56160ca9d777a0c488303469143dd9f8259
d4dd

  environment:
    - TYPESENSE_API_KEY=${TYPESENSE_API_KEY}
    - TYPESENSE_DATA_DIR=/data
    # remove this to get debug messages
    - GLOG_minloglevel=1
  volumes:
    - tsdata:/data
  restart: always

redis:
  container_name: immich_redis

  image: redis:6.2-
alpine@sha256:70a7a5b641117670beae0d80658430853896b5ef269ccf00d1827427e3263fa3

  restart: always

database:
  container_name: immich_postgres

  image: postgres:14-
alpine@sha256:28407a9961e76f2d285dc6991e8e48893503cc3836a4755bbc2d40bcc272a441

  env_file:
    - stack.env
```

```
environment:
  POSTGRES_PASSWORD: ${DB_PASSWORD}
  POSTGRES_USER: ${DB_USERNAME}
  POSTGRES_DB: ${DB_DATABASE_NAME}
```

```
volumes:
  - pgdata:/var/lib/postgresql/data
```

```
restart: always
```

```
immich-proxy:
```

```
  container_name: immich_proxy
```

```
  image: ghcr.io/immich-app/immich-proxy:${IMMICH_VERSION:-release}
```

```
  environment:
```

```
    # Make sure these values get passed through from the env file
```

```
    - IMMICH_SERVER_URL
```

```
    - IMMICH_WEB_URL
```

```
  ports:
```

```
    - 2283:8080
```

```
  depends_on:
```

```
    - immich-server
```

```
    - immich-web
```

```
  restart: always
```

```
volumes:
```

```
  pgdata:
```

```
  model-cache:
```

```
  tsdata:
```

 Click on "Advanced Mode" in the Environment Variables section.

Environment variables

These values will be used as substitutions in the stack file. To reference the .env file in your compose file, use 'stack.env'

 [Advanced mode](#)

 Switch to advanced mode to copy & paste multiple variables

- ⊕ Copy the content of the example.env from below and paste into the editor. (github repo - <https://github.com/immich-app/immich/releases/latest/download/example.env>)

```
# You can find documentation for all the supported env variables at
https://immich.app/docs/install/environment-variables

# The location where your uploaded files are stored
UPLOAD_LOCATION=./library

# The Immich version to use. You can pin this to a specific version like "v1.71.0"
IMMICH_VERSION=release

# Connection secrets for postgres and typesense. You should change these to random passwords
TYPESENSE_API_KEY=some-random-text
DB_PASSWORD=postgres

# The values below this line do not need to be changed
#####
DB_HOSTNAME=immich_postgres
DB_USERNAME=postgres
DB_DATABASE_NAME=immich
REDIS_HOSTNAME=immich_redis
```

- ⊕ Switch back to "Simple Mode".
- ⊕ Populate custom database information if necessary.
- ⊕ Populate UPLOAD_LOCATION with your preferred location for storing backup assets.
- ⊕ Click on "Deploy the stack".

Actions



- ⊕ Immich will be accessible via <http://serverip:2283/>
- ⊕ Make sure the port is open in firewall.

Post installation you can use the guide below to set up <https://documentation.immich.app/docs/install/post-install>

Immich user guide

Uploading Pictures

- ⊕ For First-Time Users
 - ⊕ On the main home page, you'll see a noticeable box labeled "CLICK TO UPLOAD YOUR FIRST PHOTO." Click on it to begin the upload process.
- ⊕ For Users with Existing Uploads:
 - ⊕ If you already have pictures uploaded, simply click the "Upload" option located in the top-right corner of the screen. This will allow you to select images, videos, or other media from your local computer. ****YOU MUST BE IN THE PHOTOS TAB FOR THE UPLOAD BUTTON TO APPEAR****

Explore Tab

- ⊕ Within the Explore tab, you have access to a range of tools that make searching and viewing your photos a breeze. Leveraging the capabilities of ChatGPT, facial recognition, and geolocation technology, finding your pictures has never been more convenient.
- ⊕ You can also narrow down your search by categories such as Favorites, Recently Added, Videos, Motion Pictures, and Panorama Photos, making it

Map Tab

- ⊕ In the Map tab, you can harness the geolocation data of your photos to visualize them on a world map. This feature allows you to see exactly where each of your photos was taken, providing a unique and interactive way to explore your memories.
- ⊕ Inside Map Settings, you have the capability to adjust the map's visual mode (dark or light), decide whether to display only your favorite photos on the map, and specify a date range for the displayed photos. These options enable you to tailor your map experience to your preferences.

Sharing Tab

- ⊕ Within the Sharing tab, you have the capability to create shared albums with other IMMICH members or share album links with individuals who don't have IMMICH accounts. This feature simplifies the process of sharing your albums with others, regardless if they use IMMICH or not.

Library

Favorites Tab

- ⊕ In the Favorites tab, you can conveniently locate all the photos you've marked as your favorites. This tab serves as a dedicated space where your cherished photos are readily accessible.

Albums Tab

- ⊕ In the Albums tab, you can seamlessly create and organize photos into distinct albums. This feature allows you to categorize your photos and easily access them based on the specific albums they belong to.

Archive Tab

- ⊕ In the Albums tab serves as a storage space for your photos, keeping them separate from the main photo view. This feature is useful for safely tucking away photos that you may not want readily accessible or visible in the main photos tab or to other users.

Mobile App

Settings

In the Albums tab serves as a storage space for your photos, keeping them separate from the main photo view. This feature is useful for safely tucking away photos that you may not want readily accessible or visible in the main photos tab

Administration

When logged into IMMICH as an administrative account in the WebUI, you will notice an "Administration" button located in the top-left corner. Clicking this button will navigate you to the administration window, where you can access and configure all the administrative settings for IMMICH.

Users

Within the "User" tab, you have the ability to both view existing users and manage them by adding or removing users as needed. To make changes to a user's settings, simply locate the user and click on the blue pencil icon situated to the right of their entry. This enables you to edit various aspects of their profile, such as their email address, name, storage label, external path, and even reset their password.

Furthermore, each user account has its dedicated personal settings accessible by clicking on your name or icon located in the top right corner. Within this section, you can perform various actions, including

managing your account details, handling API keys, authorizing devices, managing memories, overseeing password settings for your account, and configuring sharing preferences.

Jobs

When in the 'Jobs' tab, you can conveniently monitor all currently active tasks, such as generating thumbnails, extracting metadata, sidecar metadata, tagging objects, encoding clips, recognizing faces, transcoding videos, and handling storage template migration jobs, which can be initiated from the bottom of the page. Furthermore, you have the option to control the concurrency settings by navigating to the top right corner of the page, where you will find a blue box labeled 'Manage Concurrency'.

Settings

Inside the settings tab, we have a number of options to choose from. Starting with Job Settings - These settings are the same settings that are found in the jobs tab in the “manage concurrency” button.

- ⊕ Machine Learning – In this section, you can configure Machine Learning settings, including the option to enable or disable features such as Image Tagging, Smart Search, and Facial Recognition.
- ⊕ Map Settings – In this section, you have the flexibility to enable or disable the map features, and you can also modify the tile URL if needed.
- ⊕ OAuth Authentication – In this section, you have the ability to control the login settings using OAuth. You can manage various parameters such as the Issuer URL, Client ID, Client Secret, Scope, Storage Label Claim, Button Text, as well as options like Auto Register, Auto Launch, and Mobile Redirect URL override
- ⊕ Password Authentication – In this section, you can toggle the option to log in using a username and password, allowing you to either enable or disable this feature.
- ⊕ Storage Template – In this section, you can customize how your images and videos are saved, as well as configure the desired file structure.
- ⊕ Thumbnail Settings – Here, you have the option to modify the resolution of both small and large thumbnails, as well as fine-tune the quality percentage. Additionally, there's a setting available for those who prefer the Wide Gamut display.
- ⊕ Video Transcoding Settings – This tab is for the bit more advanced users. Here we manage the resolutions and encoding information of the video files. We can find things such as:
 - Constant Rate Factor (-crf)
 - Present (-present)
 - Audio Codec
 - Video Codec
 - Target Resolution
 - Max Bitrate
 - Threads
 - Transcode Policy
 - Tone-Mapping

- Two-Pass Encoding

This is also two subdirectories inside the Video Transcoding settings being

- Hardware Acceleration (Experimental)
- And Advanced in side advanced are settings most users will not need to change

Server Status

In the Server Status tab, you can access information like the total number of photos and videos stored, as well as the amount of storage used. Additionally, you can view detailed user usage data, which provides insights into the number of photo and video uploads for each individual user.

You can also check the server status, version, and storage usage from any page or tab by looking in the bottom left corner of the WebUI interface.

CLI Commands

You can find the CLI and bulk upload commands / guides here

<https://immich.app/docs/features/bulk-upload>

HOME ASSISTANT



An Open-source home automation that puts local control and privacy first. Powered by a worldwide community of tinkerers and DIY enthusiasts.

Method 1- Portainer deployment

Points to note

This is the bare minimum to get the container up and running, to access the Home Assistant web UI.

1. Go to your portainer UI → stacks → “Add Stack” → Web editor → Paste your docker-compose.yml

```
version: "3.9"
services:
  homeassistant:
    image: homeassistant/home-assistant:stable
    container_name: homeassistant
    network_mode: host
    environment:
      - TZ=America/Halifax
    volumes:
      - /opt/docker/stack/home_assistant/config:/config
restart: unless-stopped
```

The only things that need to change in this file are the time zone (TZ) and the volume path.

2. Click “Deploy the stack”.
3. Navigate to <http://IP:8123>
4. Make sure the port is open in firewall.
5. Follow guided [Home Assistant Web UI setup](#).

Method 2- Deploying in Rocky Terminal

Step 1: Create a Docker Compose file

- ⊕ Create a directory for your Home Assistant configuration, and inside this directory, create a docker-compose.yml file

```
mkdir -p /opt/docker/stack/home_assistant
cd /opt/docker/stack/home_assistant
vim docker-compose.yml
```

- ⊕ In the docker-compose.yml file, paste the following content:

```
version: "3.9"
services:
  homeassistant:
    image: homeassistant/home-assistant:stable
    container_name: homeassistant
    network_mode: host
    environment:
      - TZ=America/Halifax #Replace with your timezone
    volumes:
      - /opt/docker/stack/home_assistant/config:/config
    restart: unless-stopped
```

- ⊕ Save the file and exit the editor.

Step 2: Start the Service

Run Docker Compose from the same directory as your docker-compose.yml file:

```
docker-compose up -d
```

This command will pull the necessary image and start the container in the background.

Step 3: Accessing Home Assistant

Since you're using `network_mode: host`, you can access the Home Assistant UI by navigating to `http://<host-ip>:8123` or `http://localhost:8123` if you're on the host machine, replacing `<host-ip>` with the actual IP address of your host.

Additional Notes:

- ⊕ Ensure that no other services are using port 8123 on your host.
- ⊕ If you face any issues accessing Home Assistant, consider checking firewall rules or network policies that might be blocking the port.
- ⊕

WIREGUARD- fast, modern, and secure VPN tunnel



- ⊕ Go to "Stacks" in the left sidebar.
- ⊕ Click on "Add stack".
- ⊕ Give the stack a name (i.e. wireguard), and select "Web Editor" as the build method.
- ⊕ Copy the content of the `docker-compose.yml` file
- ⊕ You will need to set a secure password in the section in the `.yml` (`WGUI_PASSWORD`) file if you are planning to do port forwarding.

```
version: "3"
services:
  wireguard:
    image: linuxserver/wireguard:latest
    container_name: wireguard
    cap_add:
      - NET_ADMIN
    volumes:
```

```
- ./config:/config
```

```
ports:
```

```
- "5000:5000"
```

```
- "51820:51820/udp"
```

```
wireguard-ui:
```

```
image: ngoduykhanh/wireguard-ui:latest
```

```
container_name: wireguard-ui
```

```
depends_on:
```

```
- wireguard
```

```
cap_add:
```

```
- NET_ADMIN
```

```
network_mode: service:wireguard
```

```
environment:
```

```
- SENDGRID_API_KEY
```

```
- EMAIL_FROM_ADDRESS
```

```
- EMAIL_FROM_NAME
```

```
- SESSION_SECRET
```

```
- WGUI_USERNAME=admin
```

```
- WGUI_PASSWORD=kGMrU6S7(+`Ah93ENLK><8
```

```
- WG_CONF_TEMPLATE
```

```
- WGUI_MANAGE_START=true
```

```
- WGUI_MANAGE_RESTART=true
```

```
logging:
```

```
driver: json-file
```

```
options:
```

```
max-size: 50m
```

```
volumes:
```

```
- ./db:/app/db
```

```
- ./config:/etc/wireguard
```

⊕ Click on "Deploy the stack".

⊕ If you want to do port forwarding after that you could follow that steps as well.

FRIGATE- open-source NVR built around real-time AI



This is the bare minimum to get the container up and running and will need further configuration based on your specific environment, cameras, needs, storage etc.

Environment:

- ⊕ rocky 8
- ⊕ docker files in default location /var/lib/docker
- ⊕ Example containers location & structure

```
opt
├── docker
│   └── stack
│       ├── frigate
│       │   ├── config
│       │   │   └── config.yml
│       │   └── docker-compose.yml
```

docker-compose.yml

```
version: "3.9"
services:
  frigate:
    container_name: frigate
    image: ghcr.io/blakeblackshear/frigate:stable
    privileged: true # This may not be necessary for all setups
    restart: unless-stopped

    - /opt/docker/stack/frigate/config:/config # Mounting config directory
    - frigate_media:/media/frigate
    - type: tmpfs
      target: /tmp/cache
      tmpfs:
        size: 100000000

volumes:
  frigate_media: # Named volume for media storage
```

Note: Ensure to use the image in the docker-compose.yml searching will often provide results for the depreciateds images.

Explanation of docker-compose.yml

1. **version: "3.9"**

Defines the version of Docker Compose file syntax. 3.9 is a specific version of the Docker Compose file format.

2. **services:**

Defines the services (containers) to be created.

2.1 **frigate:**

Defines the name of the service (container) to be created.

2.2 **container_name: frigate**

Specifies the name of the container that will be created.

2.3 **image: ghcr.io/blakeblackshear/frigate:stable**

Specifies the Docker image to be used for this service, pointing to Frigate's stable release.

2.4 **privileged: true**

Allows the service to access the host's devices and possibly other privileged functionalities.

2.5 **restart: unless-stopped**

Ensures the container will restart automatically unless explicitly stopped by the user.

2.6 **shm_size: "64mb"**

Allocates shared memory for the container, useful when your application has specific memory requirements.

2.7 **ports:**

Maps the container's ports to the host's ports.

2.8 **environment:**

Sets environment variables within the container.

2.9 volumes:

Mounts host paths or named volumes to paths inside the container.

- `/etc/localtime:/etc/localtime:ro` binds the host's timezone settings to the container in read-only mode.
- `/opt/docker/stack/frigate/config:/config` binds the configuration directory from the host to the container.
- `frigate_media:/media/frigate` creates a named volume for storing media.
- `type: tmpfs` creates a temporary filesystem in memory, providing high-speed read/write access.

3. volumes:

Defines named volumes used by services.

3.1 frigate_media:

This is a named volume declaration, which creates persistent storage independent of the container lifecycle, used here for storing media.

Additional Notes:

- `FRIGATE_RTSP_PASSWORD: "password"` is setting an environment variable with the password for RTSP access. This will be found in your cameras configuration settings
- `"5000:5000"` makes the web UI of Frigate accessible on port 5000 of the host machine.
- `"8554:8554"` is for RTSP feeds, `"8555:8555/tcp"` and `"8555:8555/udp"` are for WebRTC over TCP and UDP, respectively.
- Each line in this file serves to configure the behavior, access, or setup of the Docker container or its interaction with the host system or other containers.

Config.yml

The `config.yml` file is used to specify configuration settings for Frigate. Frigate needs this file to know how to connect to your cameras, how to process the video streams, how to interact with other services, and many other settings.

Ensure you have this file created & populated with the correct path in your `docker-compose.yml` before running the container.

```
cameras:
front_door: # This is just an example name for your camera
  ffmpeg:
    inputs:
      - path: rtsp://your_camera_ip:554/your_stream_path
        roles:
          - detect
# Other camera settings go here
```

1. **mqtt:**

This denotes the configuration section related to MQTT, a lightweight messaging protocol typically used in IoT setups.

2. **enabled: False**

This line is configuring whether or not to enable MQTT. Here, it is set to False , meaning MQTT is disabled.

3. **cameras:**

This is the start of the section where you define the configurations for each of your cameras.

4. **name_of_your_camera:**

This is where you name your camera; it is just a placeholder, so you should replace it with a name that makes sense for your setup (e.g., front_door).

5-7. **ffmpeg: ... roles: - detect**

These lines are defining how Frigate should use FFmpeg to interact with the camera. FFmpeg is a multimedia framework used to handle video, audio, and other multimedia files and streams. Here, it is specified to use the camera for detection purposes.

8. **inputs:**

This denotes the start of a list of input streams from the camera that Frigate should use.

9. **path: rtsp://IP_OF_CAMERA:554/rtsp**

This line is specifying the RTSP (Real-Time Streaming Protocol) path to your camera stream. You should replace IP_OF_CAMERA with the actual IP of your camera, and the rest of the path may vary based on the camera model and manufacturer.

10. **roles:**

This specifies the roles that this input stream will be used for.

11. **detect**

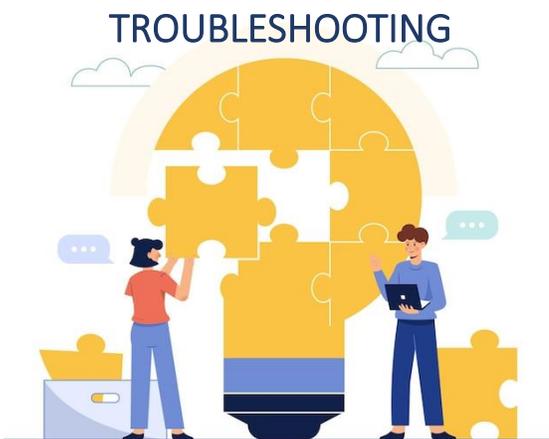
This specifies that the input stream should be used for detection purposes.

12. **detect:**

This is the start of the section where you define the detection settings for this camera.

Why is this file needed?

This file is crucial because it allows you to tailor Frigate to your specific needs and hardware. By providing this file, you are informing Frigate about your camera(s), their properties, locations, and how you want Frigate to process their streams, enabling Frigate to function correctly according to your use case. Without this configuration file, Frigate would not know how to interact with your camera(s) or how to process their streams.



SERVER WONT POWER ON

- ⊕ Try powering the server using the switch
- ⊕ Check if you are seeing lights on the motherboard and the PSU
- ⊕ Check if the fans are spinning
- ⊕ If you have IPMI access check if the PSU is detected and if yes what the status are.

Slot:1	
Power Supply Status	PS OK
AC Input Voltage	230 (V)
AC Input Current	0 (A)
DC 12V Output Voltage	12.1 (V)
DC 12V Output Current	5.039 (A)
Temperature 1	35 C/ 95 F
Temperature 2	0 C/ 32 F
Fan 1	12384 RPM
Fan 2	11584 RPM
DC 12V Output Power	66 (W)
AC Input Power	90 (W)
Serial Number	

Slot:2	
Power Supply Status	PS OK
AC Input Voltage	230 (V)
AC Input Current	0 (A)

⊕ Also check the health event logs.

⊕ Server Health

⊕ Sensor Readings

⊕ Health Event Log

⊕ Power Consumption

⊕ Power Source

⊕ Health Event Log

For more advanced health event log settings, please click [here](#)

This page shows the system event log (SEL). You can choose a category from the pull-down box to filter the events, and can also sort them by clicking on a column header.

Clear Health Event Log Save Mark as Acknowledged Clear Acknowledgements

Select an event log category: All Events Severity: Critical Keyword Search:

ACK	EID	Severity	Time Stamp	Sensor	Description
<input type="checkbox"/>	98	●	2023/09/25 19:41:14	Components Changed(OEM)	HDD removed on PCH HDD Slot0 on SATA controller 1 - Assertion
<input type="checkbox"/>	99	●	2023/09/25 19:41:14	Components Changed(OEM)	HDD removed on PCH HDD Slot1 on SATA controller 1 - Assertion
<input type="checkbox"/>	92	●	2023/07/26 12:15:58	Power supply(P51 Status)	Power Supply Failure detected - Assertion
<input type="checkbox"/>	88	●	2023/03/23 17:51:59	Power supply(P51 Status)	Power Supply Failure detected - Assertion

Event Log:Max= 512, Used= 24(event entries)

- ⊕ If the PSU status says it is failed its most likely a failed PSU
- ⊕ But if it just says the PSU is not detected and the fans are spinning and you can see the lights on the motherboard and PSU it could be one of the hardware components
- ⊕ If you are not getting any video output it is most likely a motherboard issue or a CPU issue.
- ⊕ Replace the faulty component and you should be able to power up the server.

HOUSTON UI IS NOT ACCESSIBLE

If your Houston UI is not loading.

- ⊕ First thing would be to check if the server IP is accessible.
- ⊕ Open a terminal or command prompt and try pinging the server IP.
- ⊕ If you get a response then your IP / network settings is fine.
- ⊕ Either ssh into the server or open your IPMI web interface.
- ⊕ Once you have connected to the server via terminal/IPMI check if the cockpit service is running
- ⊕ **systemctl status cockpit**

```
[root@homelabs ~]# systemctl status cockpit
● cockpit.service - Cockpit Web Service
   Loaded: loaded (/usr/lib/systemd/system/cockpit.service; static; vendor preset: disabled)
   Active: active (running) since Tue 2023-09-26 11:09:05 EDT; 2h 58min ago
     Docs: man:cockpit-ws(8)
  Process: 66010 ExecStartPre=/usr/libexec/cockpit-certificate-ensure (code=exited, status=0/SUCCESS)
 Main PID: 66013 (cockpit-tls)
    Tasks: 2 (limit: 408093)
   Memory: 5.4M
   CGroup: /system.slice/cockpit.service
           └─66013 /usr/libexec/cockpit-tls

Sep 26 11:09:05 homelabs systemd[1]: Starting Cockpit Web Service...
Sep 26 11:09:05 homelabs systemd[1]: Started Cockpit Web Service.
```

- ⊕ If the status is inactive then restart the service using `systemctl restart cockpit`
- ⊕ Your Houston interface should load fine after that.
- ⊕ If the you were not getting ping response during our troubleshooting steps, then you need to check your networking
- ⊕ You can use the NMTUI interface and check the interface that has the IP set and check if it up and active.
- ⊕ If all good check if your device is in the correct network.

DRIVES ARE MISSING IN MY ZPOOL

- ⊕ Try checking which are the drives in your pool that are missing
- ⊕ You can either use the zpool status or check in the UI using ZFS tab
- ⊕ Check the server logs using `dmesg -T` to see if it has any drives drop warning.
- ⊕ Try re-seating the drive and see if it is getting picked up.
- ⊕ If the drive is still not detected try swapping it with a drive in another slot and see if it is getting detected.
- ⊕ If the drives is still not detected it is most likely a failed drive.
- ⊕ But if the drive gets detected on a different slot. It could be a bad slot.

ZPOOL IS IN A DEGRADED STATE

- ⊕ Try checking which are the drives in your pool that are missing
- ⊕ You can either use the zpool status or check in the UI using ZFS tab
- ⊕ Check the server logs using `dmesg -T` to see if it has any drives drop warning.
- ⊕ Check if it is an actual failed drive by running SMART diagnostics on the drive
- ⊕ Check if you are noticing any uncorrectable or offline sectors if yes then it is most likely a failed drive and needs replacement.
- ⊕ If the drive is good you would need to troubleshoot if it is the underlying hardware such as backplane/cables etc.

SAMBA SHARES ARE NOT ACCESSIBLE TO MOUNT

- ⊕ Check if you have samba ports added to the firewall.

Firewall Add zone

public zone Interfaces eno1 Add services

Service	TCP	UDP
> ssh	22	
> dhcpv6-client		546
> cockpit	9090	
> https	443	
> samba	139, 445	137, 138

- ⊕ Check if the samba services is running
- ⊕ Check if you have set a separate samba password for the user
- ⊕ Make sure you are accessing the share using the right password.

GETTING ACCESS DENIED WHEN ACCESSING THE FILES IN THE SHARE

- ⊕ Make sure you are having the appropriate permission to access the files.
- ⊕ Check the permission granted and see if the user getting access denied has access.
- ⊕ It is most likely that he is not having access or is having access to just the top-level folder and not the child folders and files.
- ⊕ Modify the permission as per your preference and you should be able to access the files.

HOW DO I UPDATE MY SERVER

- ⊕ You can update the server by using the software updates tab in the Houston UI

45DRIVES DISK MODULE IS NOT WORKING s

- ⊕ If the 45drives disks module does not show up and does not detect the drives you can perform device mapping manually using **sudo dalias -t HL15**
- ⊕ Once the command finishes, reload the 45drives disks module and it should show the drives.

SYSTEM WOULD NOT BOOT INTO THE OS

- ⊕ If the system is stuck in boot loop try accessing the server using the IPMI web UI.
- ⊕ Try to go the boot menu by pressing F11 during the reboot.
- ⊕ Once you are in the boot menu try manually select the boot drive and boot into it.
- ⊕ If that works check if the boot order is set properly.
- ⊕ Press Delete key to go to BIOS and check the boot order.