Updated: Oct 11, 2023

Milestone 6.1 Storage and Roles

Part 1: Storage with NFS

> 💣NFS is not natively secure and it is easily abused. There are options for authentication. For right now our NFS access is limited to the Joyce network
>
> One thing we do for the NFS shares used in the data center is have a dedicated private LAN where those NFS shares are exposed to the associated storage only interfaces on our hypervisors. This connection is high speed and the NFS shares are SSD backed.

The NFS Shares are set up on the two web servers we have used to download ISOs for the class.

Task 1: NFS File Share on Host

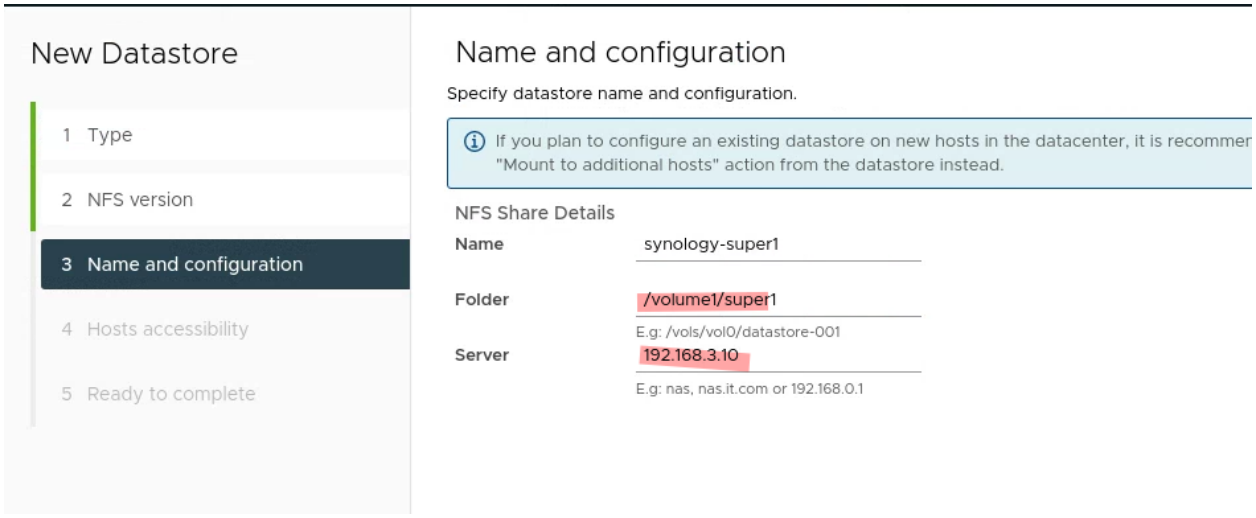
Goal: Using vcenter, add a new NFS Datastore that is mounted on your superX host. It will be used as a file share (e.g. could be used for ISOs or ova's…)

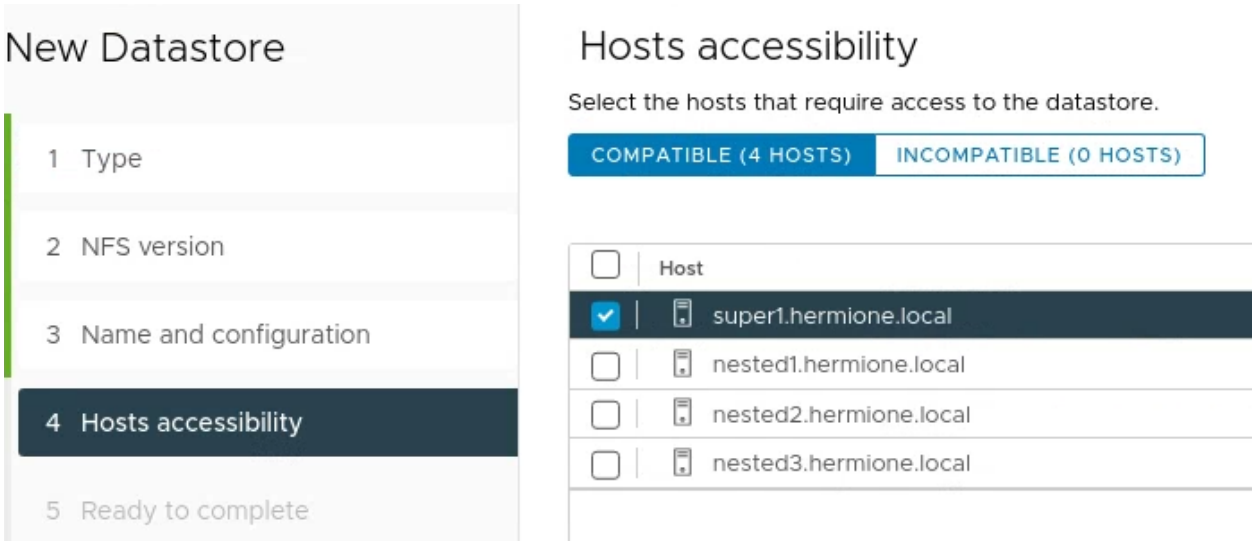
Steps

1. Figure out how to add a new Datastore in vcenter that mounts to a NFS Share. Attach the NFSShare to your physical SuperX box and not your nested esxi systems.
2. The NFS server details for the File Share Data Store
    a. NFS server: 192.168.7.240
    b. NFS Type: 4.1
    c. NFS Folder: /var/nfs/share
    d. No Kerberos
3. Name the datastore something like "SuperX-NFS-Shared"

Some example screenshots that are different from our settings

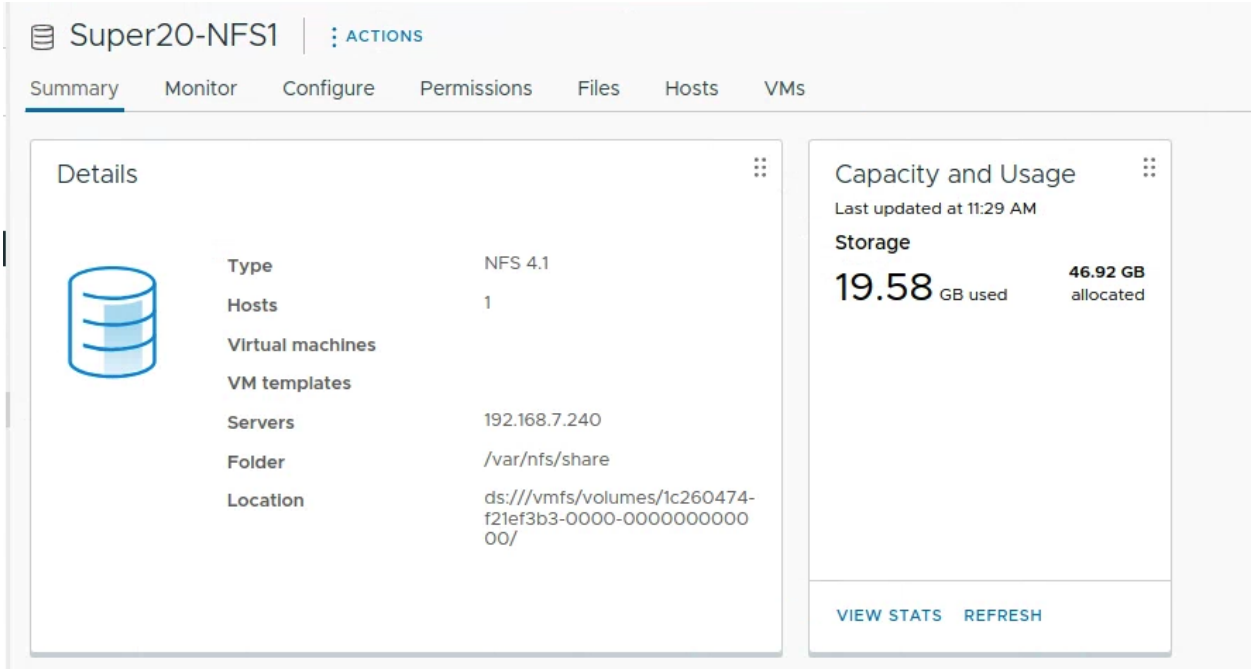
Updated: Oct 11, 2023





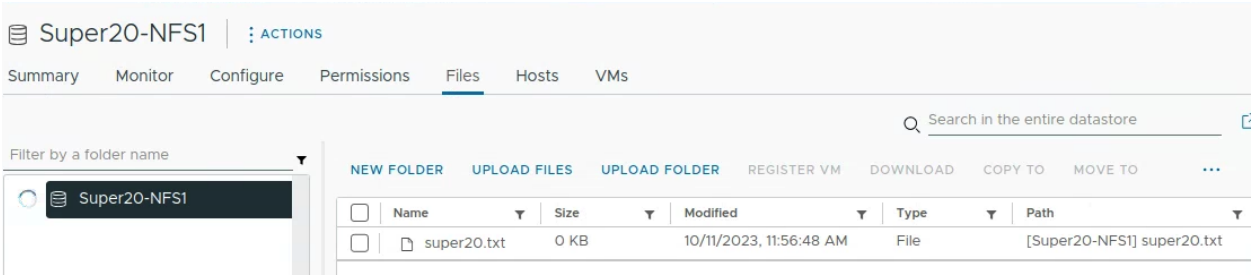
Updated: Oct 11, 2023

`Deliverable 1. Provide a screenshot similar to the one below that shows the NFS properties of your NFS share.`



4. From vcenter - figure out how to upload a small text file called “superX.txt to your new NFS datastore

`Deliverable 2. Provide a screenshot similar to the one below that shows the uploaded file in your NFS share.`



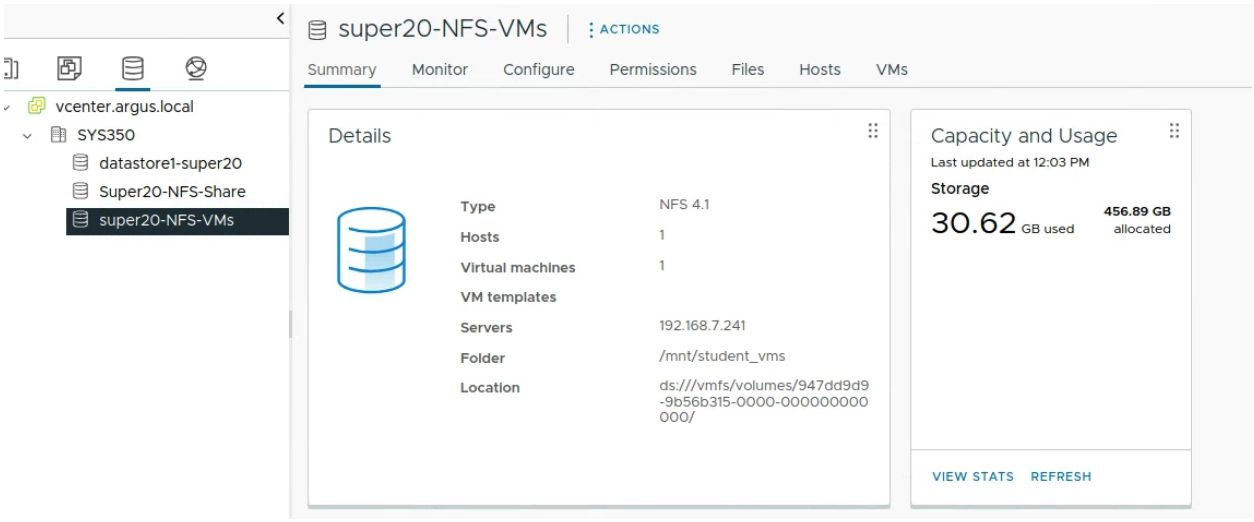
Task 2: Another NFS Datastore for VMs

In this next task, you will add a second NFS Datastore to your SuperX Host and use your Rocky Template to launch a **Thin Provisioned** VM (**NOTE: Must be thin provisioned to have enough capacity on the NFS share!)**

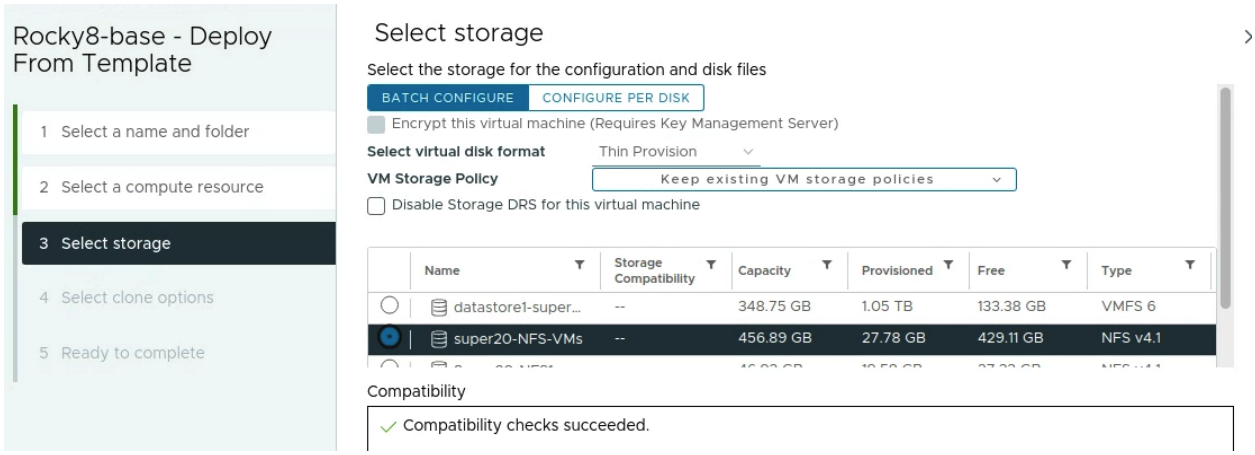
Steps:

Updated: Oct 11, 2023

1. Using vcenter - add a **second datastore**. The following screenshot should have enough information for the settings. Call is “superX-NFS-VMs” as we can use this for VM storage

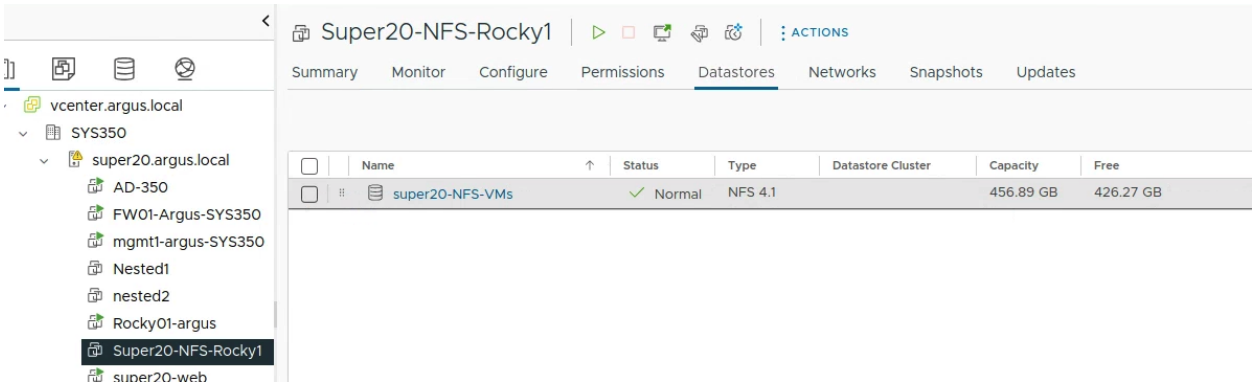


2. **Deliverable 3** Take a screenshot similar to the one above showing the second NFS Datastore
3. Use your Rocky8 Template to launch a new VM called “SuperX-Rocky-NFS”
    a. Make sure to pick the superX-NFS-VM Datastore
    b. And, make sure it is **thin-provisioned!**
    c. Should be something like list when your are launching the VM



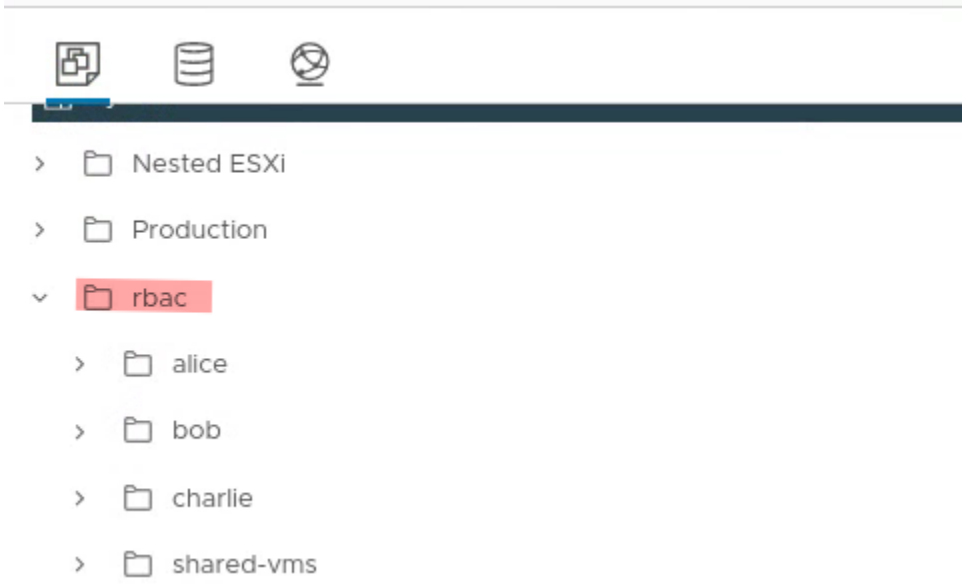
Deliverable 3.5: Take a screenshot of your new VM like the one below

Updated: Oct 11, 2023



Part 2: Roles

Create an rbac folder with folders for three users (alice, bob and charlie in the example) and a shared-vms folder as shown below.



Create 3 AD-Users (alice, bob and charlie). Make sure passwords don't need to be changed at first login.

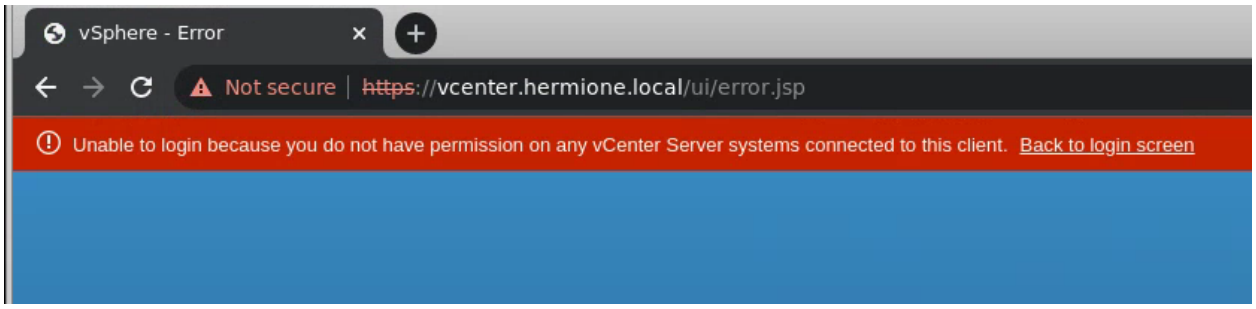
Create 2 AD Groups

- sys350-power-user (members are: alice)

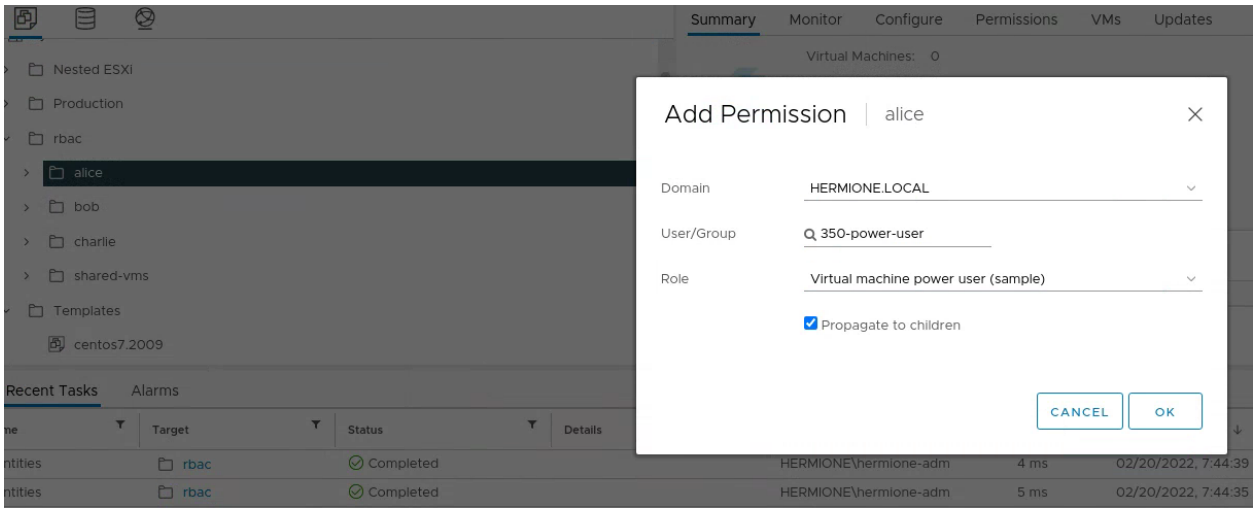
Updated: Oct 11, 2023

- sys350-restricted-user (members are: bob and charlie)

Try connecting to vCenter as bob, you should be rejected (note, if you want to keep your administrative session going, open up an incognito session to test user access controls)



Adjust the permissions on the alice folder so they look like this:

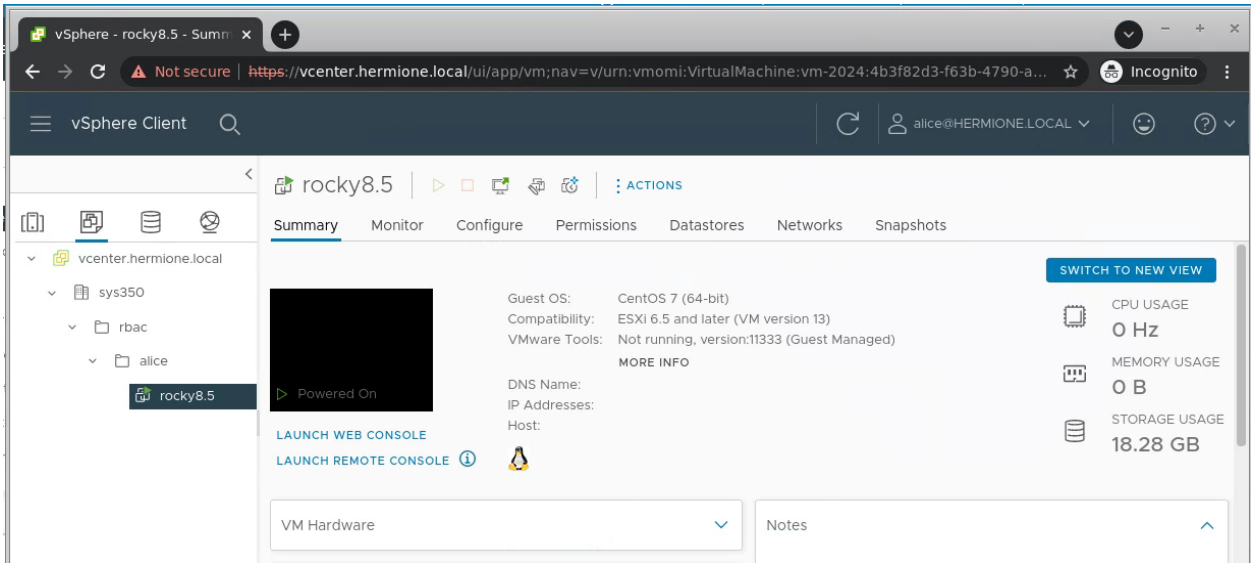


If the AD groups don't show up in the drop down you can either wait a bit or logoff and login again.

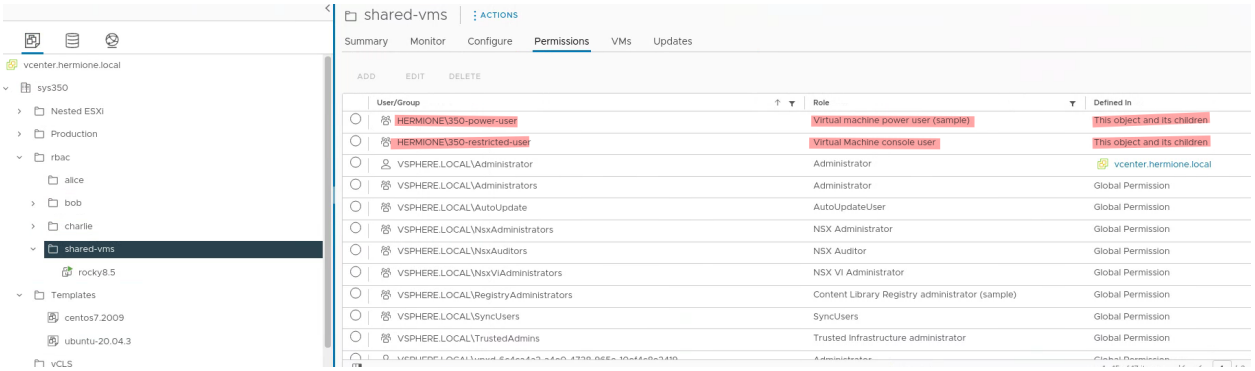
Move one of your VMs into the alice folder.

Updated: Oct 11, 2023

Deliverable 4 Login as alice and demonstrate you are limited to the VM placed in the alice folder. Provide a screenshot similar to the one below.

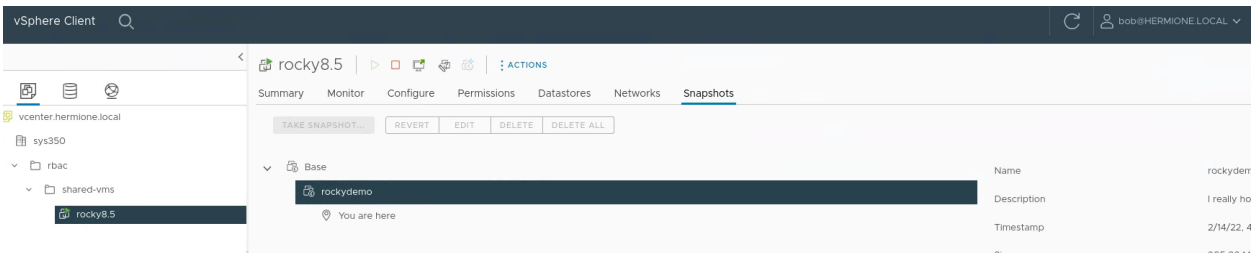


Move another VM into the shared-vms folder and assign the following permissions to that folder



Alice should enjoy power level privileges over VMs in the shared-vms folder. Bob and Charlie should be limited to a handful of console operations. For instance Bob should not be able to Grab a snapshot.

Deliverable 5. Provide a screenshot demonstrating that Bob's Take snapshot option is grayed out.



Updated: Oct 11, 2023

Deliverable 6. Ok, we've decided that the Virtual Machine console user role has far too much power. Figure out how to clone the role, name it something like "Virtual Machine console no power user". Edit this cloned role such that those assigned that role will not be able to perform power operations. Change the permissions for share-vms so that the restricted user group gets your new limited role. Provide a screenshot of Charlie's VM with the PowerOn, Off actions disabled.

Deliverable 7. Provide a link to your tech journal that details how you created a new NFS datastore and how Permissions are applied to folders (and objects) in vSphere.

Deliverable 8. Cover any issue you had in the completion of the lab. Consider the security implications for NFS (version 3 in particular).