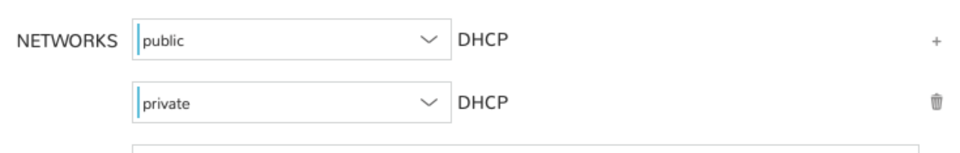
Shared storage via NFS

Block devices can only be mounted on one machine at a time. If you need to share some storage space across multiple VMs, you can export a directory via NFS from the machine with that volume mounted.

For EUMETSAT EWC side you should have a look at SFS EUMETSAT - Shared File System (SFS) usage in tenants.

Provisioning the VMs

Make sure both server and client have a private network enabled, in order to see each other.



NETWORKS public DHCP

private DHCP

You may want to also set up an extra volume other than the root one to use as the export. See Adding extra disk storage to your instances to see how to set it up.

Installing and configuring the NFS server

1. Install the NFS server and tools if not installed. On CentOS:

   ```
   sudo yum install nfs-utils
   ```

   On Ubuntu:

   ```
   sudo apt install nfs-kernel-server
   ```

2. Configure the directory or directories to export. For example, if you want to share a directory called /data within your private tenant network (here, we assume it's **192.168.1.0/24**)

   ```
   echo "/data 192.168.1.0/24(rw,sync,no_root_squash)" | sudo tee -a /etc/exports
   ```

   You may want to adapt it to suit your needs.
3. Start the services. On CentOS:

   ```
   sudo systemctl enable rpcbind
   sudo systemctl enable nfs-server
   sudo systemctl enable nfs-lock
   sudo systemctl enable nfs-idmap
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   sudo systemctl start nfs-lock
   sudo systemctl start nfs-idmap
   ```

   On Ubuntu:

   ```
   sudo service nfs-kernel-server restart
   ```

4. You may need to configure the firewall to recognise your private network IP range (here assumed to be **192.168.1.0/24**) as trusted, enabling access to the NFS server. On CentOS:

```
sudo firewall-cmd --permanent --zone=trusted --add-source=192.168.1.0/24
sudo firewall-cmd --reload
```

> Do not enable NFS on a public / internet-facing interface!

5. Take note of the private IP of the server, as you will need it when configuring the clients. On the EUMETSAT part of EWC, you can also use the name of the machine, but the IP will work too.

```
ip addr show
```

> **EUMETSAT: Creating new Security Group for NFS server**
>
> If your VM runs on the EUMETSAT cloud, you will need to use a special security group. NFS uses 111 (UDP and TCP) and 2049 (TCP and UDP) ports for communicating through the network, which are not open by default in EUMETSAT configuration. In order to allow connections coming from the network to those ports, you need to create a new security group and set rules. Our "Creating Security Groups in Morpheus" knowledge base article covers the details regarding the task and you can follow it to create your own rule to allow NFS connections. After creating the new security group for NFS, you need to change the NFS Server's current security group to your new rule.

Installing and configuring the NFS clients

You may now mount the share from the server

1. Create the directory where the mount is going to go. We are using **`/data`** in this example:

```
sudo mkdir /data
```

2. Add an entry to your /etc/fstab. In this basic example we assume our server is on **192.168.1.1**:

```
echo "192.168.1.1:/data /data nfs defaults 0 0" | sudo tee -a /etc/fstab > /dev/null
```

You may add extra options to your entry.

3. The shared filesystem will be automatically mounted on the next reboot. To mount it straight away, you may run:

```
sudo mount -av
```

Using the NFS share

When you use an NFS share across multiple machines, the machines need to agree on the identity of the users in order to properly support permissions, otherwise you will see a lot of "permission denied" difficulties.

This is normally accomplished by using a numeric id that every user and group has (type `id` on a console to see yours) - this numeric id must be the same between the server and all clients. This can be accomplished manually (i.e. creating/altering user ids to match on all machines) or automatically (e.g. using networked authentication such as LDAP, which normally comes pre-installed on EUMETSAT tenants).

If security within the tenant is not a concern, you can simply use the root account to open permissions fully (`chmod -R a+rwX DIRECTORY`) or change ownership (see chown command). You can also add "squash_all" to the export options in /etc/exports to force all operations to happen as if they were owned by the "nobody" user, effectively granting everyone complete access.

Related articles

- How to create S3 buckets in Morpheus
- Object storage: How to use s3cmd and s3fs
- Creating Security Groups in Morpheus
- Adding extra disk storage to your instances
- Backup your instance