# Create directories for 'rao' logs

sudo mkdir -p /opt/powerpipedata/rao/logs

sudo chmod 777 /opt/powerpipedata/rao/logs

#You need to create Docker networks for each group of containers to communicate with each other. Ensure that you create networks with unique names for each logical group:

sudo docker network create rao-network

sudo docker run -d --name rao-pp-sp-container-3 \

--network rao-network \

-p 9021:9021 \

-p 9121:9121 \

-e AWS\_ACCESS\_KEY\_ID=AK34566666543SUI \

-e AWS\_SECRET\_ACCESS\_KEY=7234567yvw \

-e AWS\_REGION=us-east-1 \

-v /opt/powerpipedata/rao/logs:/home/powerpipe/mod \

pp-sp-img

Verify Running Containers

Use the following command to check that your containers are running:

docker ps

Execute Commands Inside Containers

To execute commands inside the containers, use docker exec:

Rao Container:

sudo docker exec -it rao-pp-sp-container-3 /bin/bash

Setup and Run Services

Inside each container, execute the following commands to set up and start the services:

powerpipe --version

steampipe --version

mkdir -p /home/powerpipe/mod

cd /home/powerpipe/mod

powerpipe mod init

powerpipe mod install github.com/turbot/steampipe-mod-aws-compliance

Verify Log Persistence

Verify the Logs: After running the container, any logs created inside /home/powerpipe/mod should now appear in /opt/powerpipedata/rao/logs on the host.

Rao Service:

nohup steampipe service start --port 9021 > steampipe.log 2>&1 &

nohup powerpipe server --port 9121 > powerpipe.log 2>&1 &

To test this:

powerpipe@container$ echo "Log data" >> /home/powerpipe/mod/powerpipe.log

Then check the host directory:

cat /opt/powerpipedat