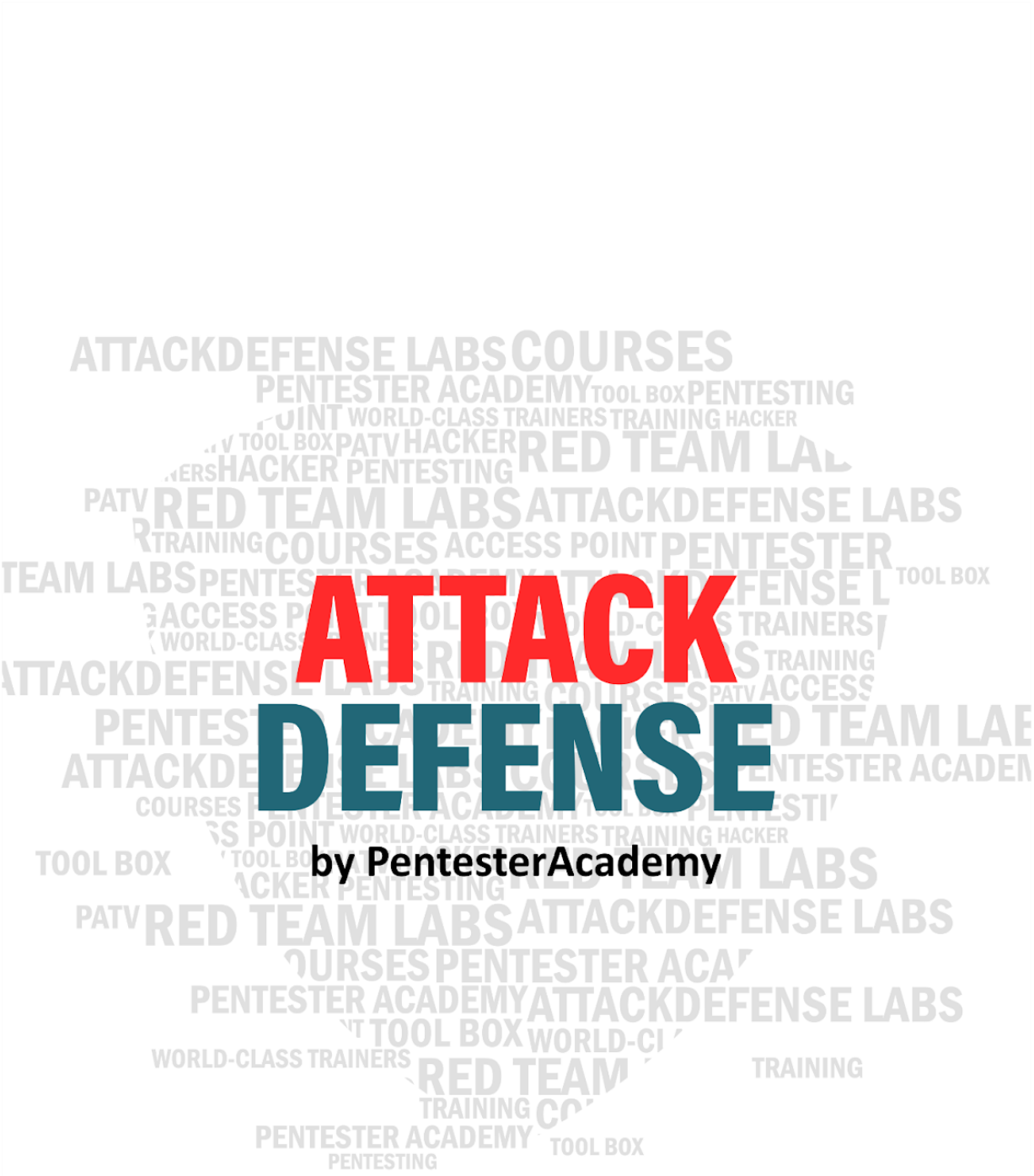

ATTACK
DEFENSE
by PentesterAcademy

Name	Tool: Portainer
URL	https://attackdefense.com/challengedetails?cid=1414
Type	DevSecOps : Docker Tools

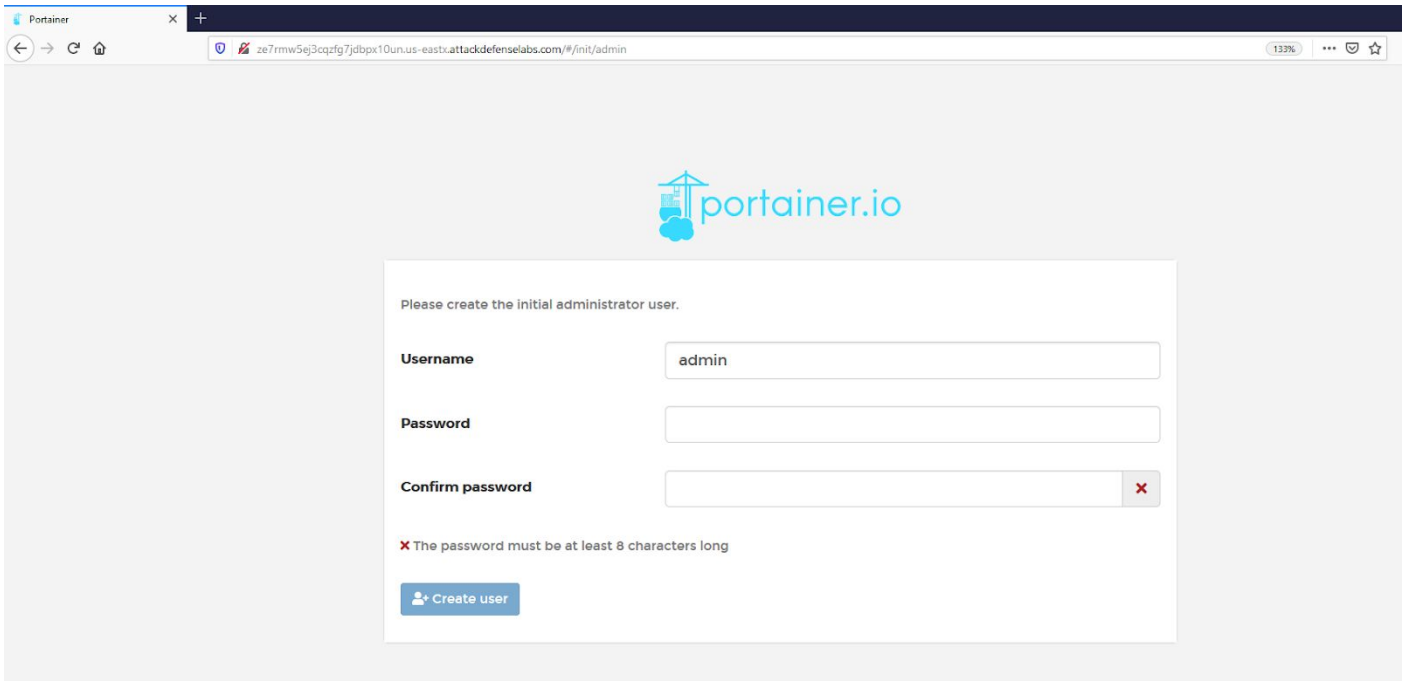
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Explore the Docker host system using Portainer and try out different operations!

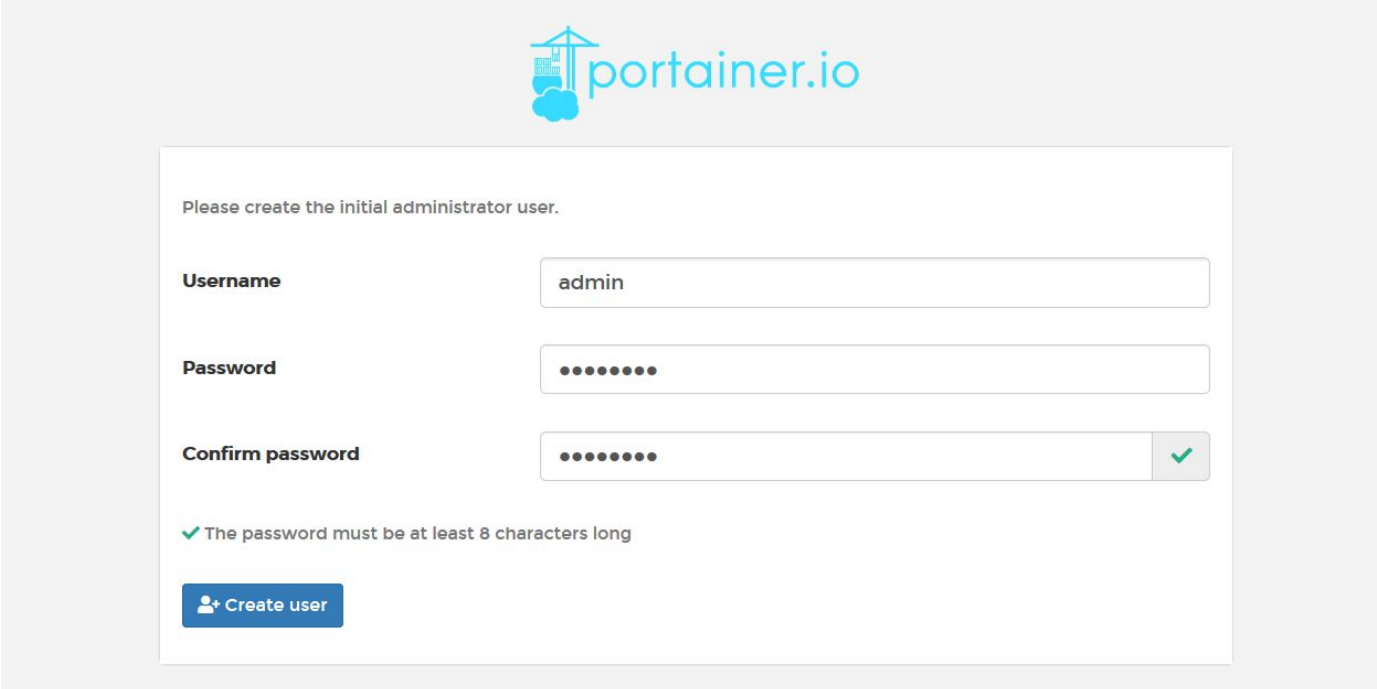
Solution:

Configuring portainer:

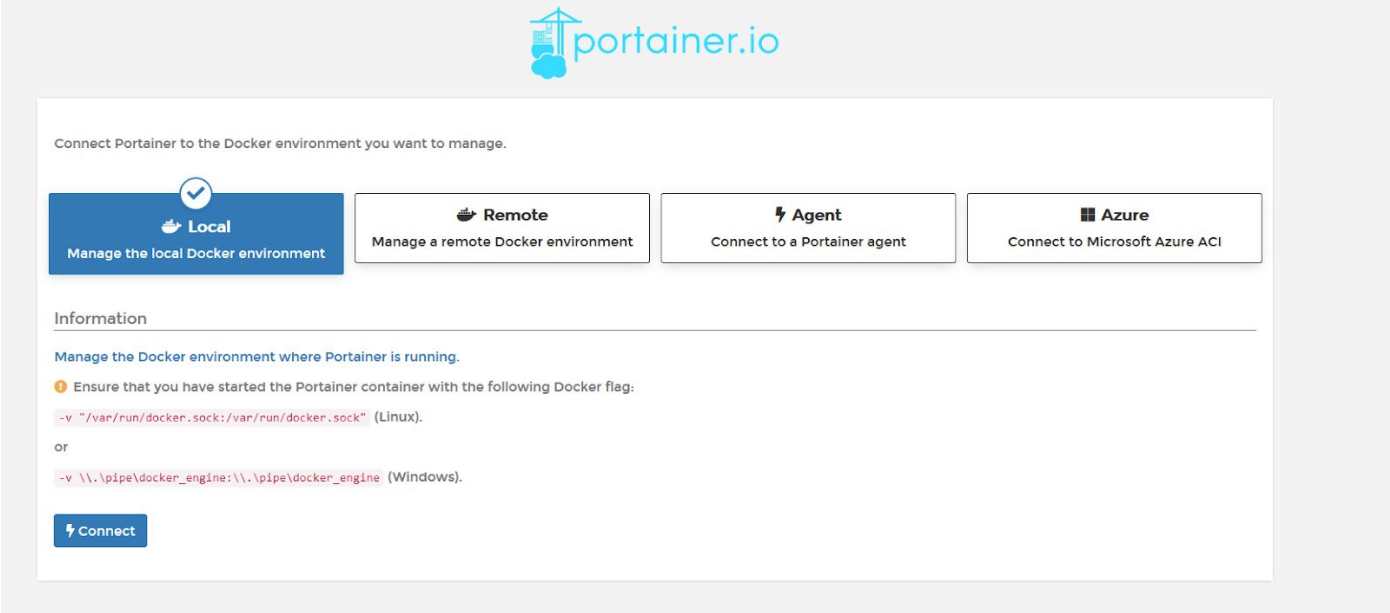
Landing page:



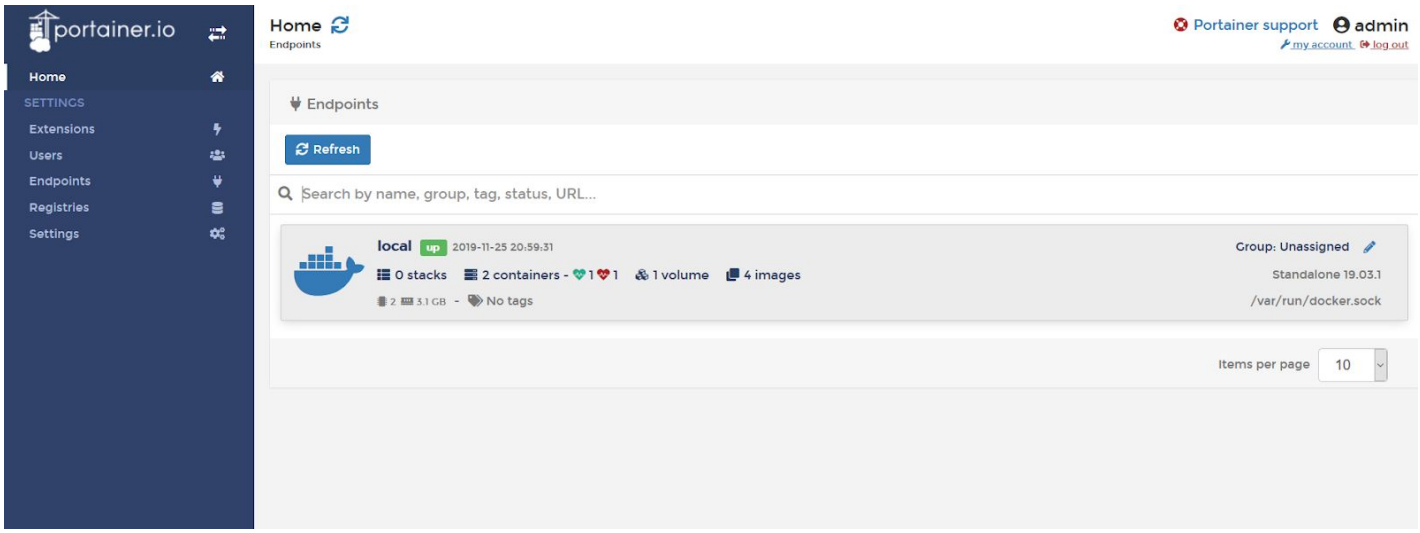
Step 1: Enter “password” in the password field as well as in the confirm password field.



Step 2: Select “Local” environment.

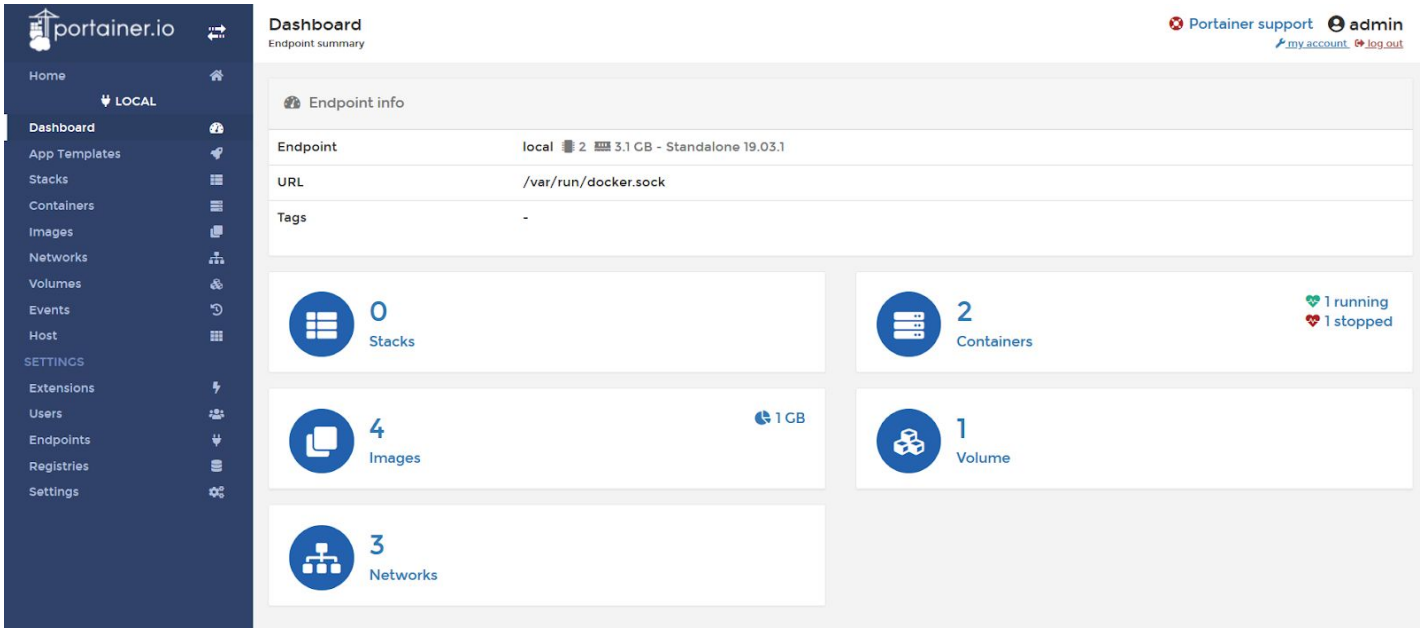


Dashboard:

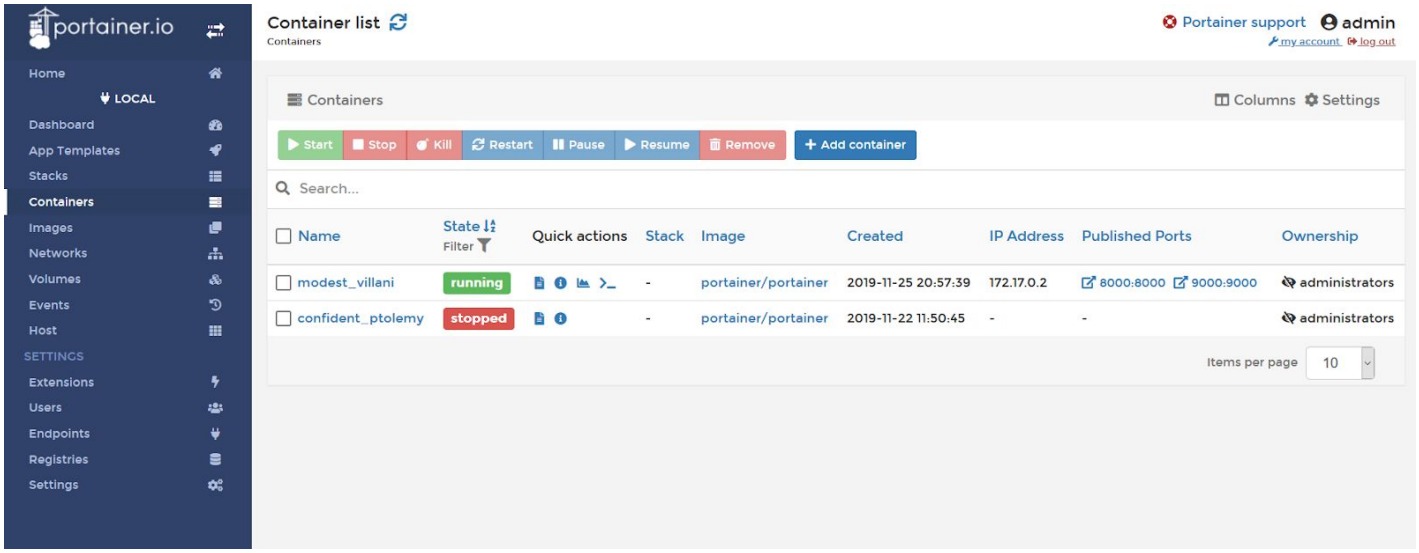


Listing running containers:

Step 1: Select the local endpoint.



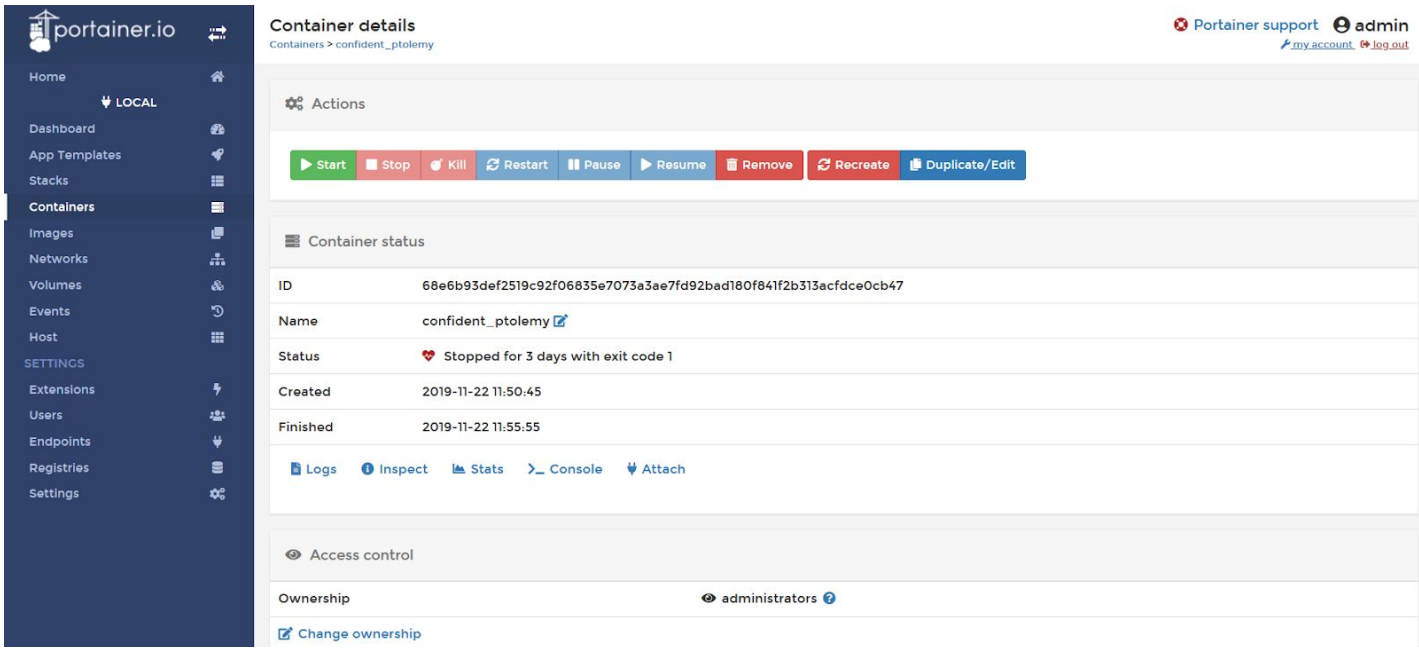
Step 2: Click on the containers section.



All the stopped and running container are listed. The image name, IP address and the published ports of the container are also listed on the webpage.

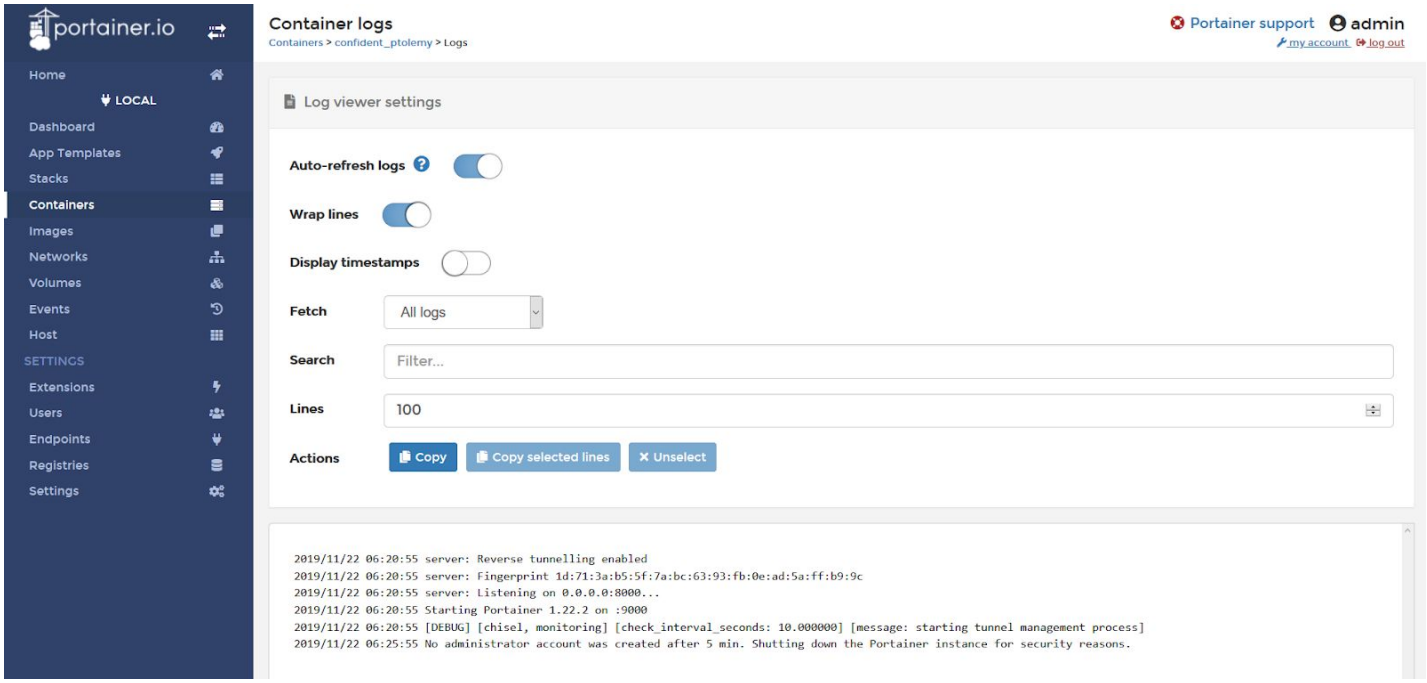
Viewing details of stopped containers.

Step 1: Click on the name of the stopped container.



The details of the stopped containers are provided on the web page.

Step 2: View the logs. Click on the Logs button.

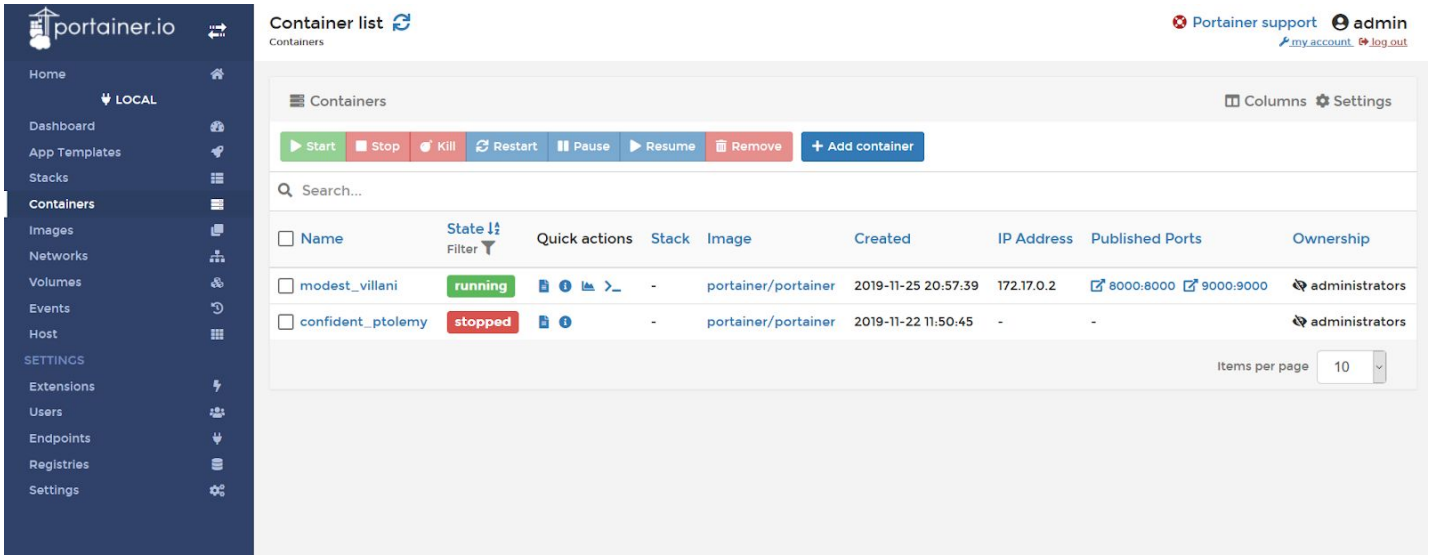


Logs:

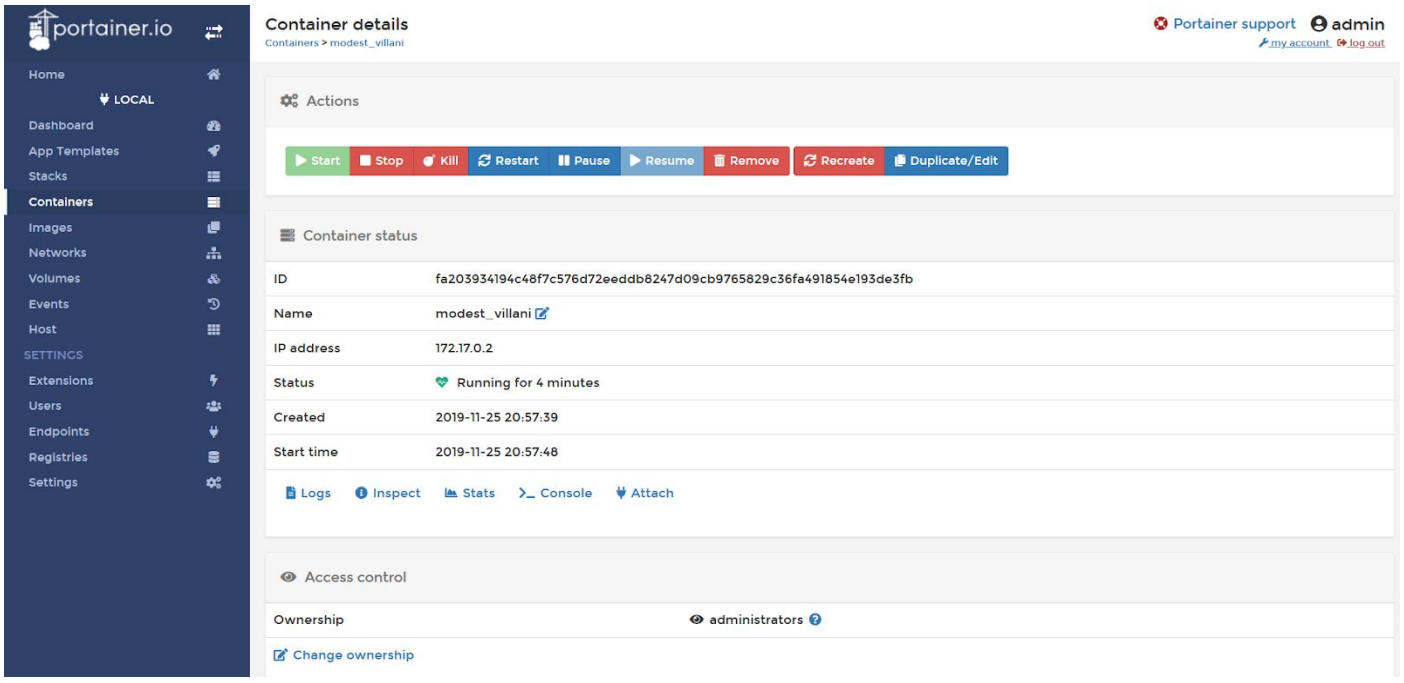
```
2019/11/22 06:20:55 server: Reverse tunnelling enabled
2019/11/22 06:20:55 server: Fingerprint 1d:71:3a:b5:5f:7a:bc:63:93:fb:0e:ad:5a:ff:b9:9c
2019/11/22 06:20:55 server: Listening on 0.0.0.0:8000...
2019/11/22 06:20:55 Starting Portainer 1.22.2 on :9000
2019/11/22 06:20:55 [DEBUG] [chisel, monitoring] [check_interval_seconds: 10.000000] [message: starting tunnel management process]
2019/11/22 06:25:55 No administrator account was created after 5 min. Shutting down the Portainer instance for security reasons.
```

Checking statistics of the running container:

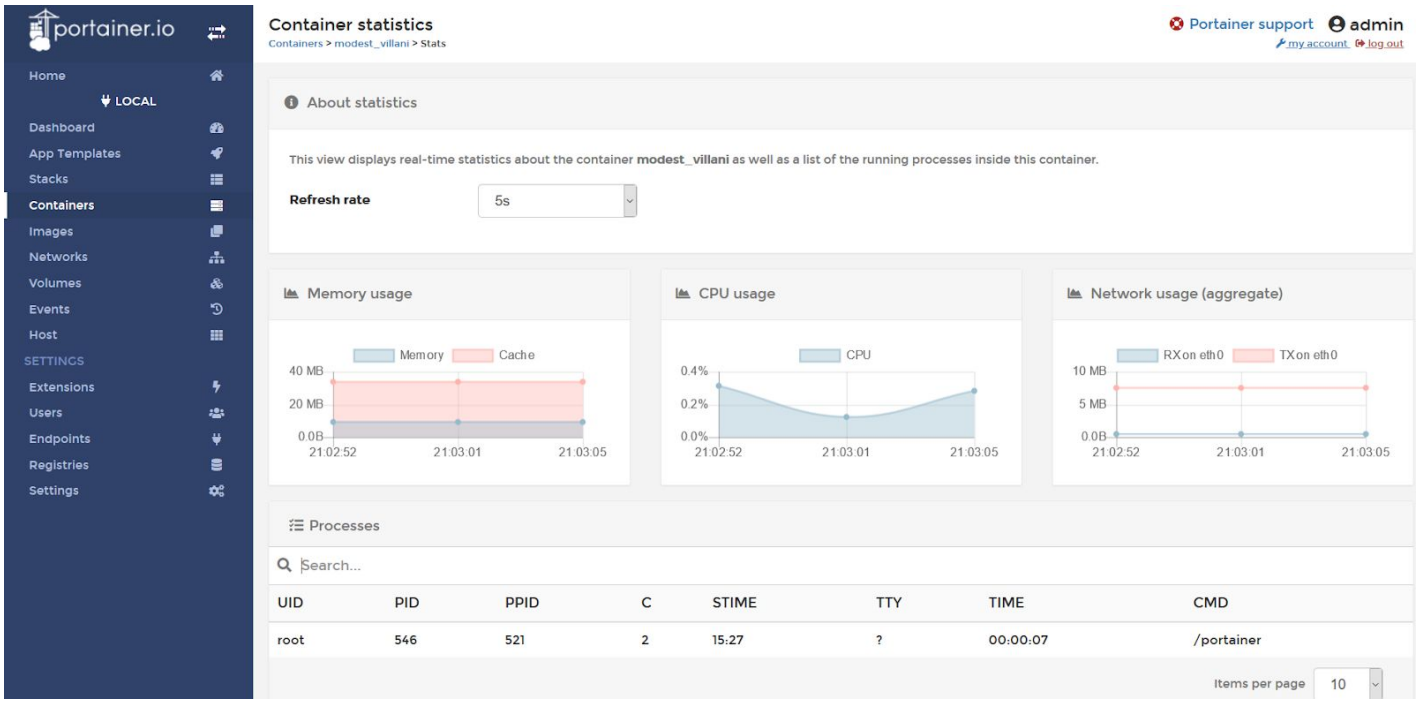
Step 1: View the list of containers. Click on the containers tab on the left panel.



Step 2: Click on the name of the running container.



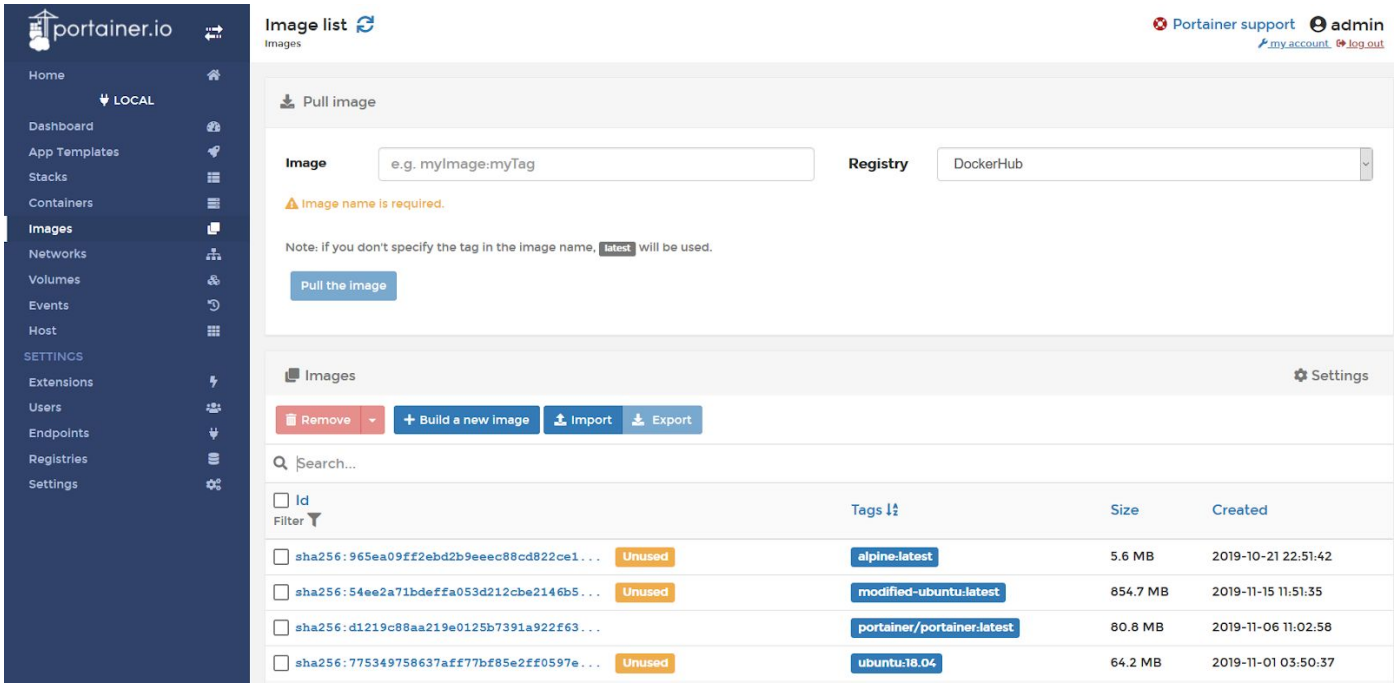
Step 3: Click on the stats button.



The CPU, Memory and network usage is displayed on the web page. The processes running on the container are also listed.

Identifying the images available on the machine.

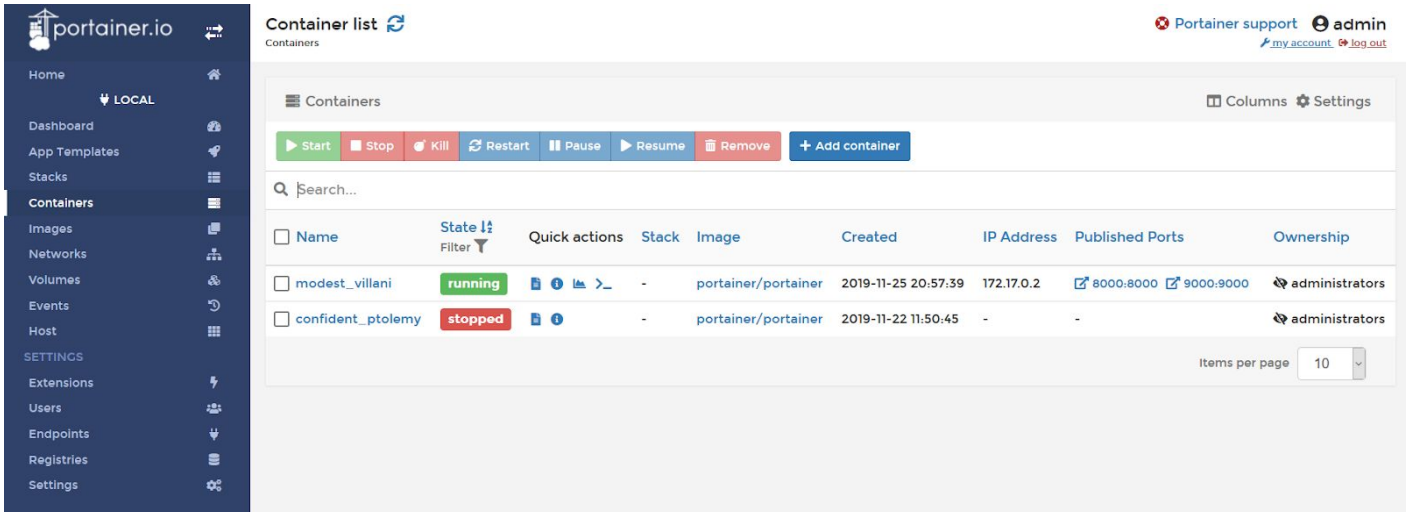
Step 1: Click on the Images tab on the left panel.



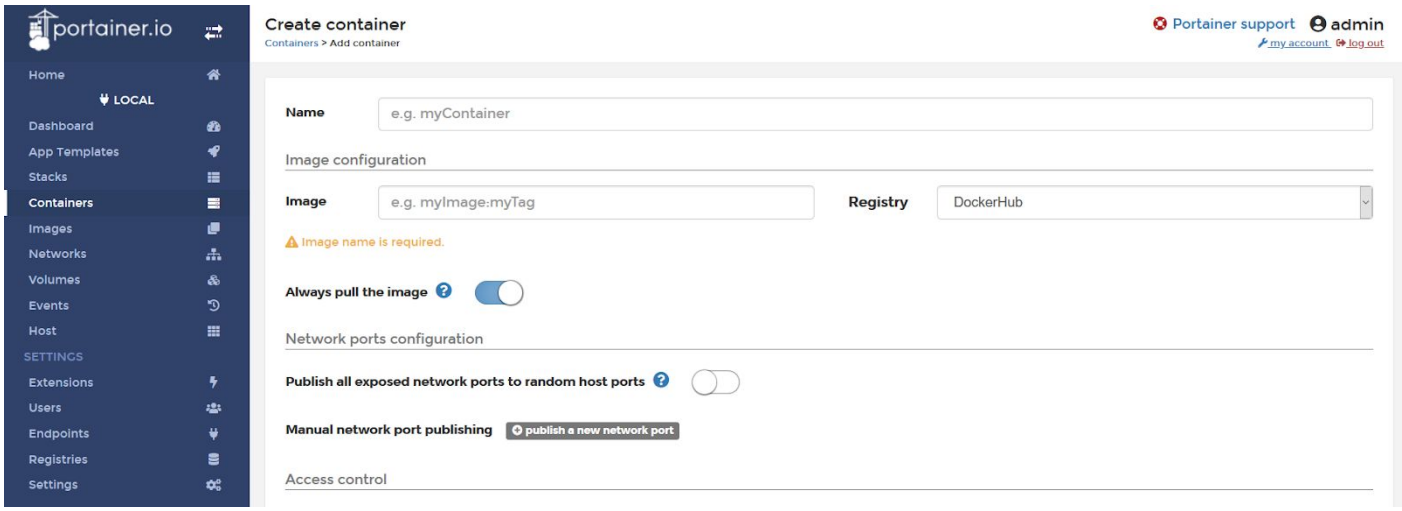
List of images are displayed on the web page.

Starting a container:

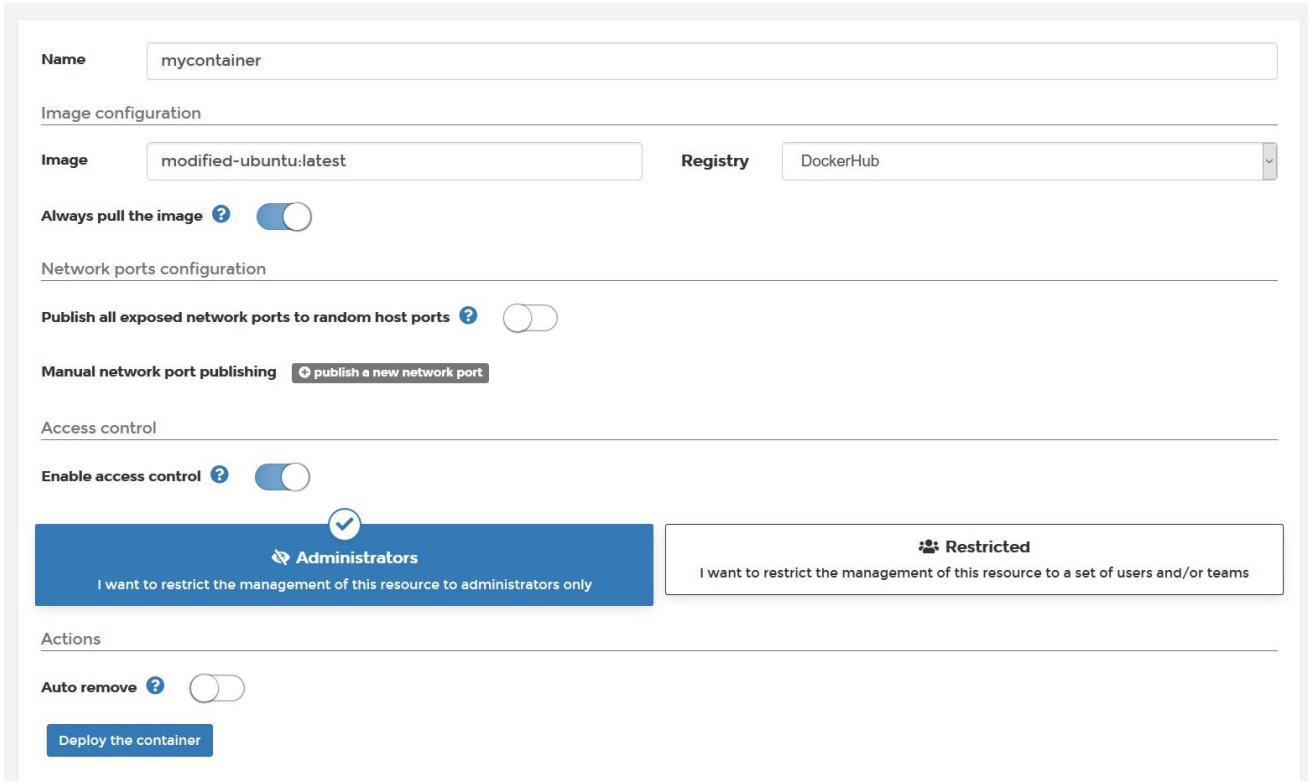
Step 1: Navigate to Containers webpage. Click on the containers tab on the left panel



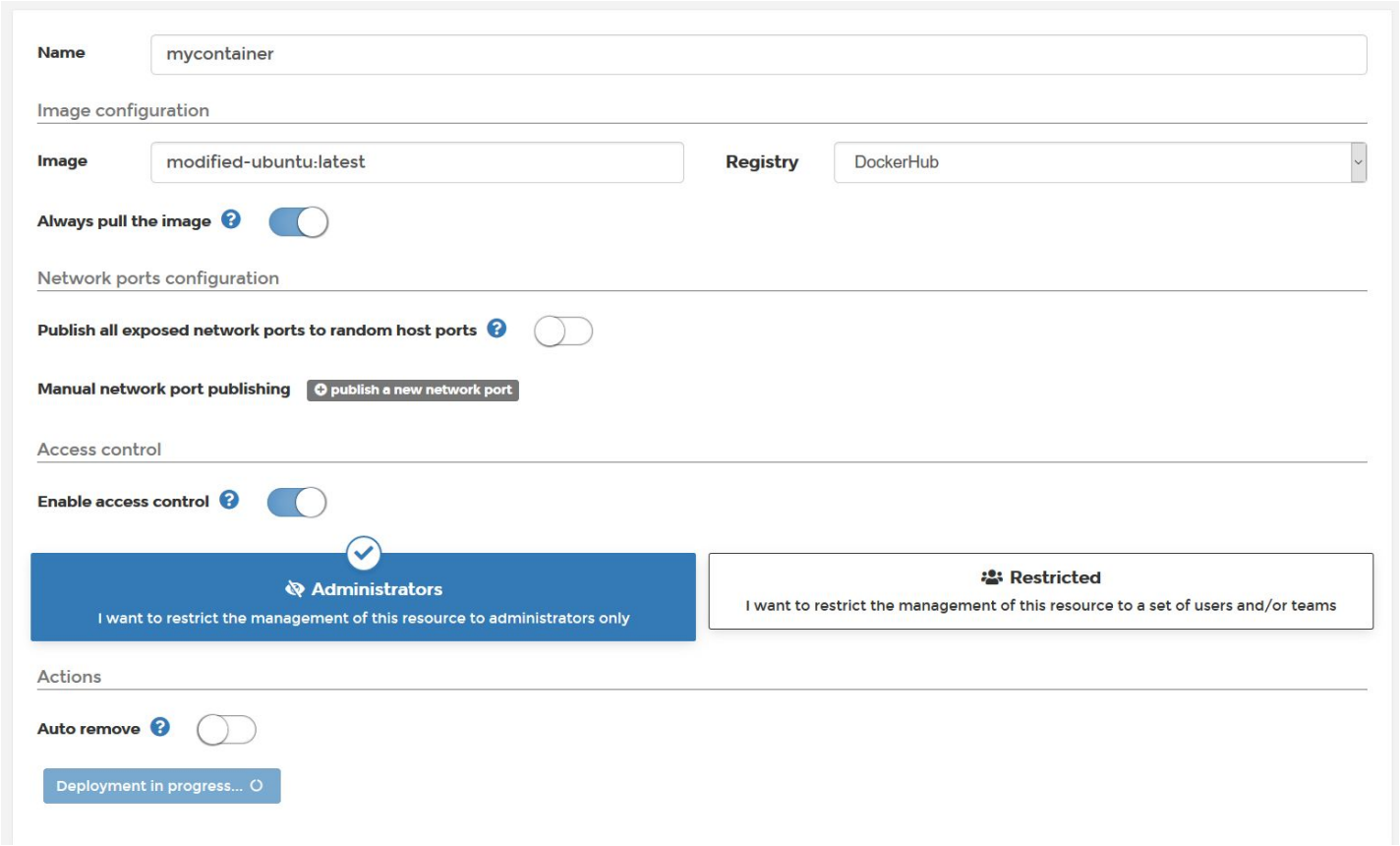
Step 2: Click on the “Add container” button.

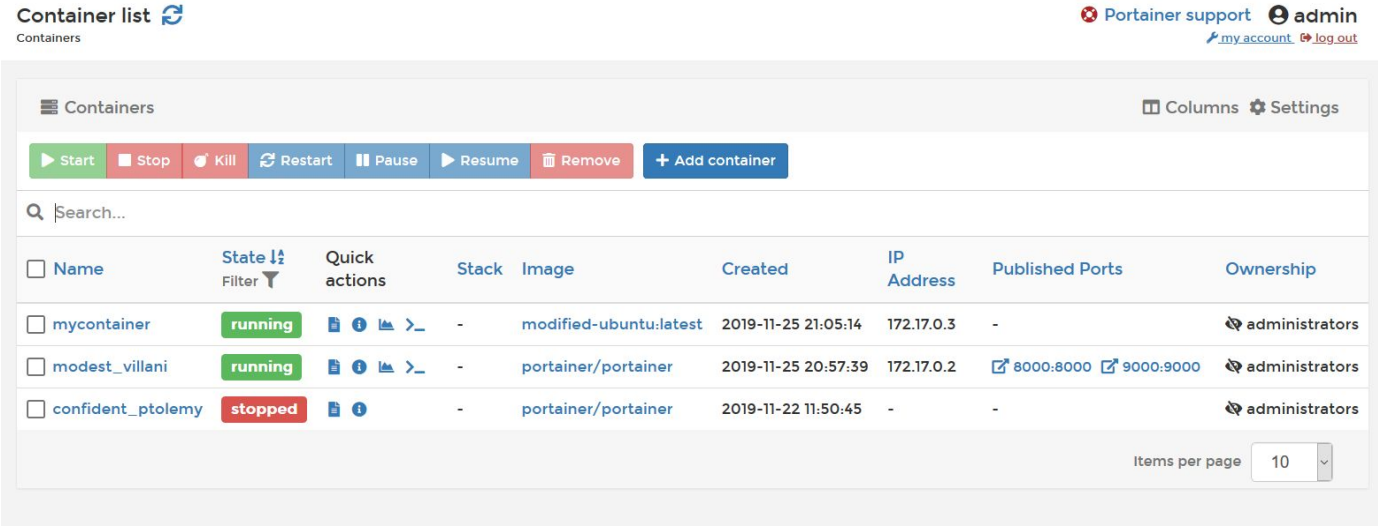


Step 3: Enter “mycontainer” in the name field and select “modified-ubuntu:latest” in the image field.



Step 4: Click on the “Deploy the container” button.

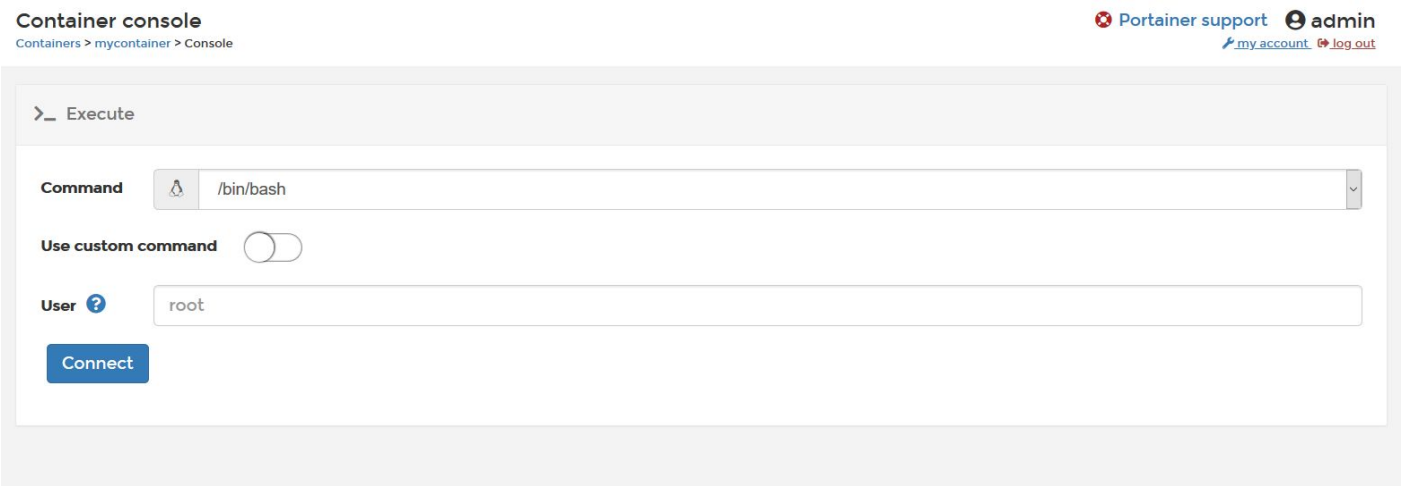




The container was started successfully.

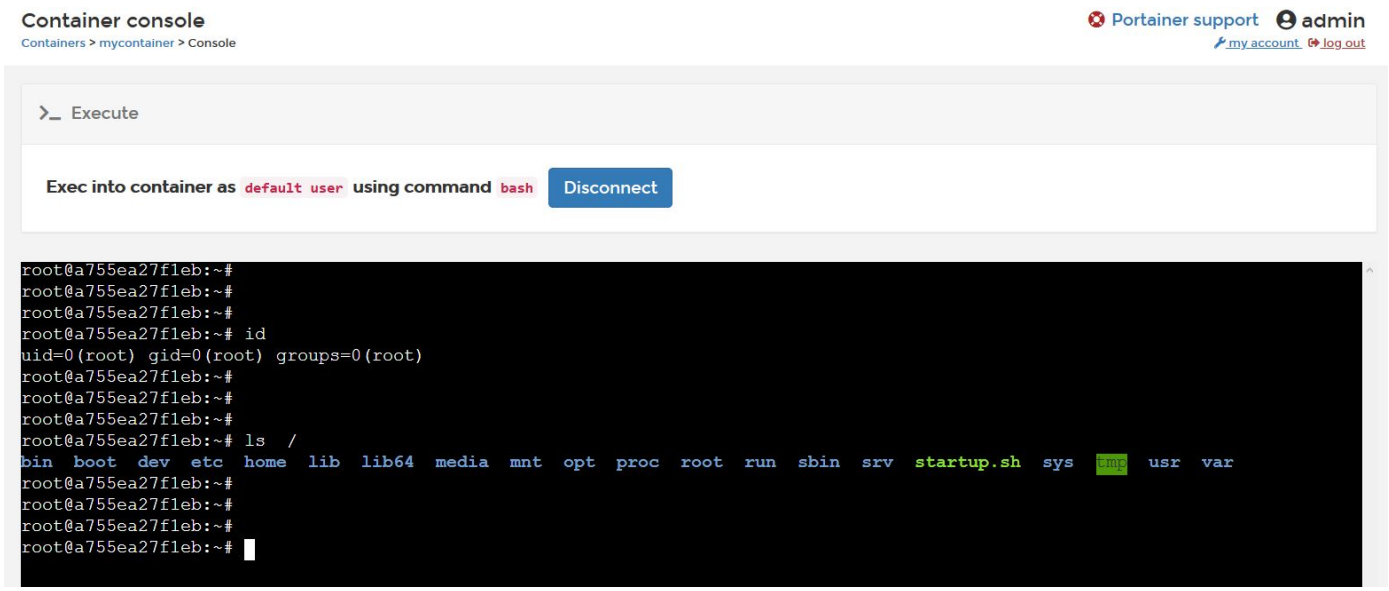
Executing commands on the running container.

Step 1: Click on the “Exec Console” button of the mycontainer container from the quick action columns.



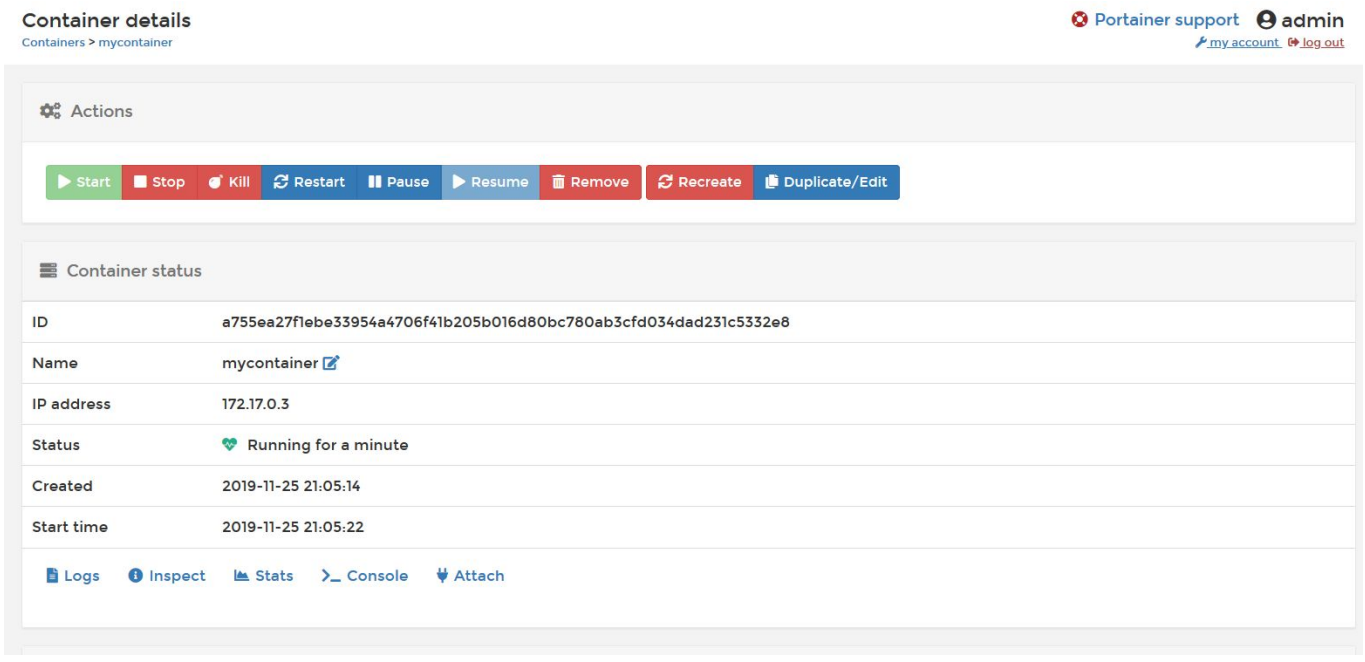
Step 2: Click on the Connect button.

Commands:
id
ls /

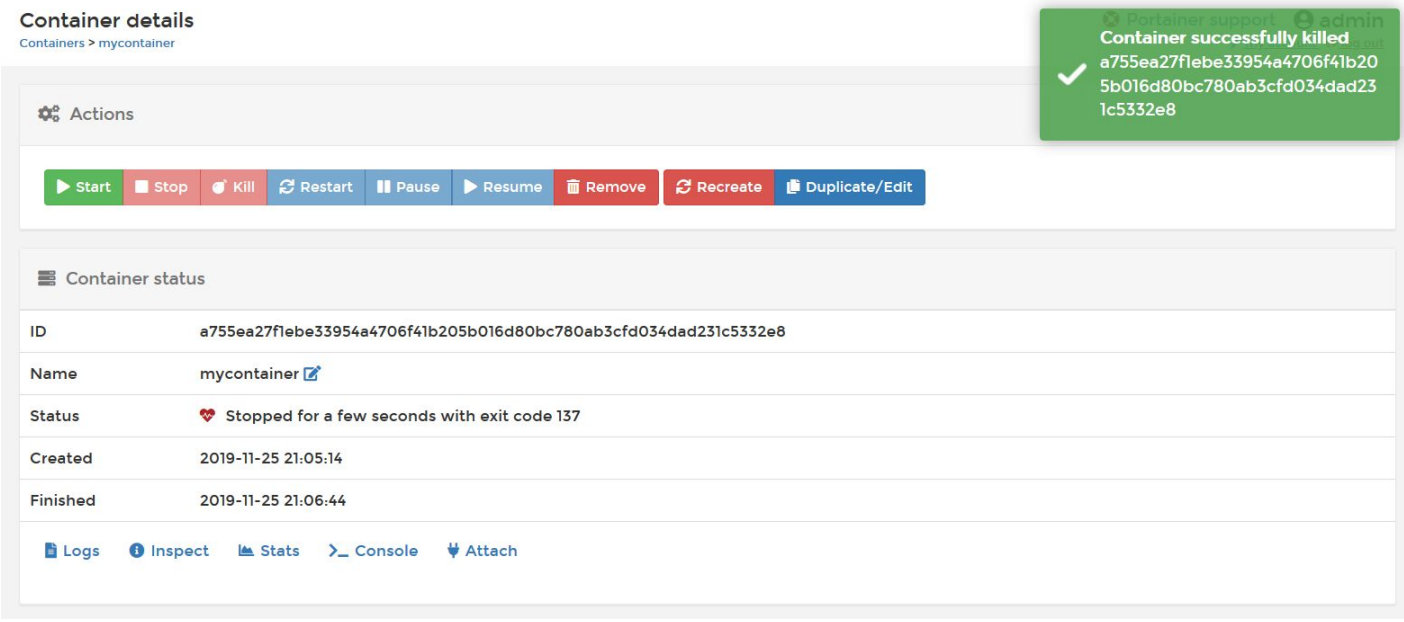


Killing a container:

Step 1: Access the container details page. Click on the mycontainer container hyperlink below "Container console" heading.



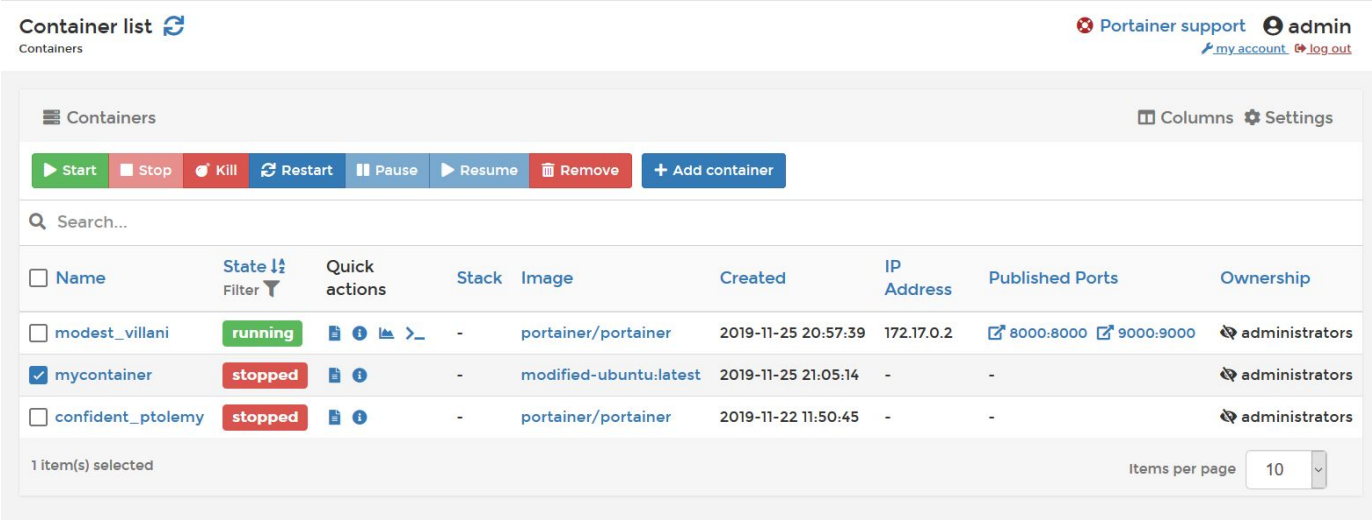
Step 2: Click on the kill button.



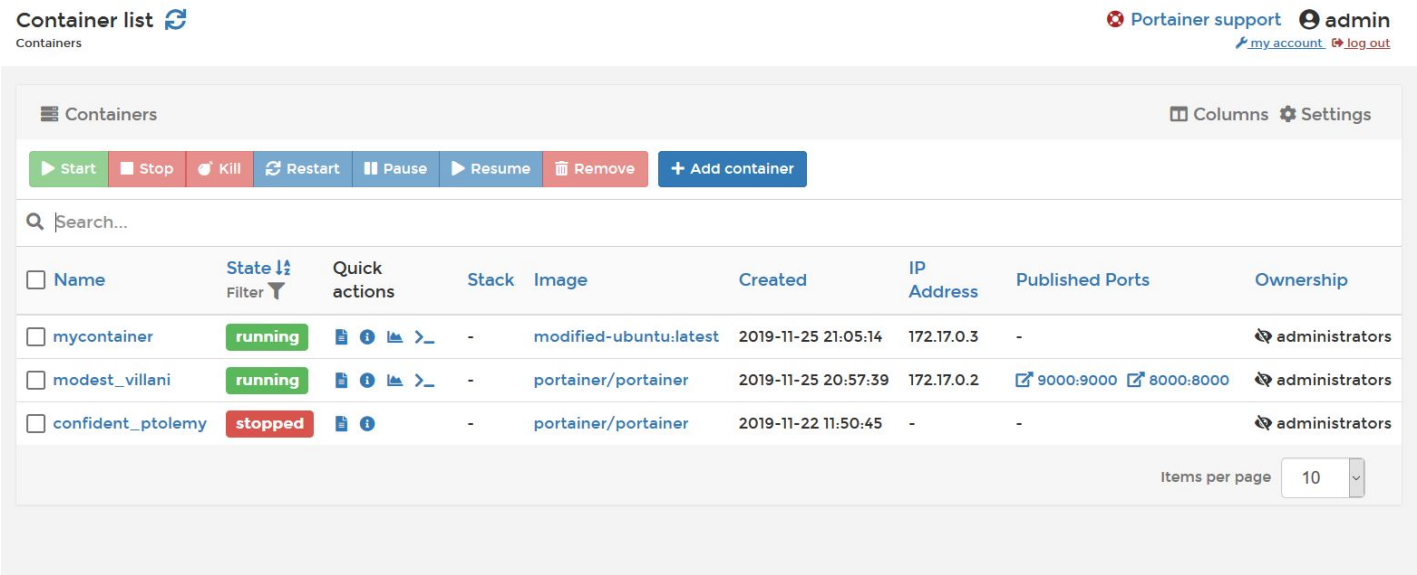
The container was killed successfully.

Starting a stopped a container:

Step 1: Tick the checkbox for mycontainer container.



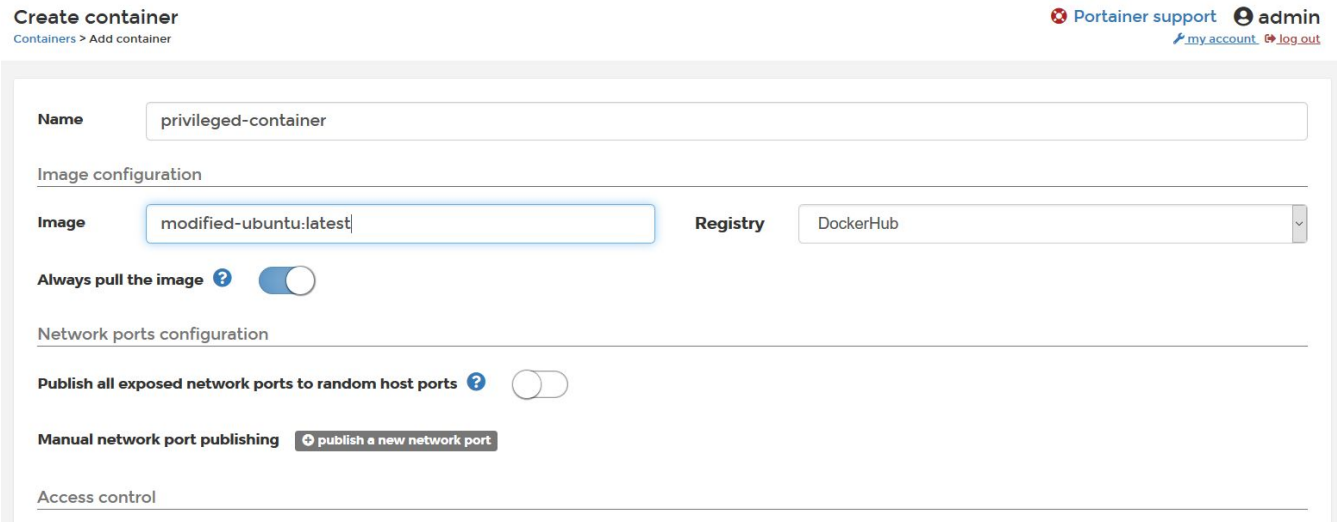
Step 2: Click on the start button.



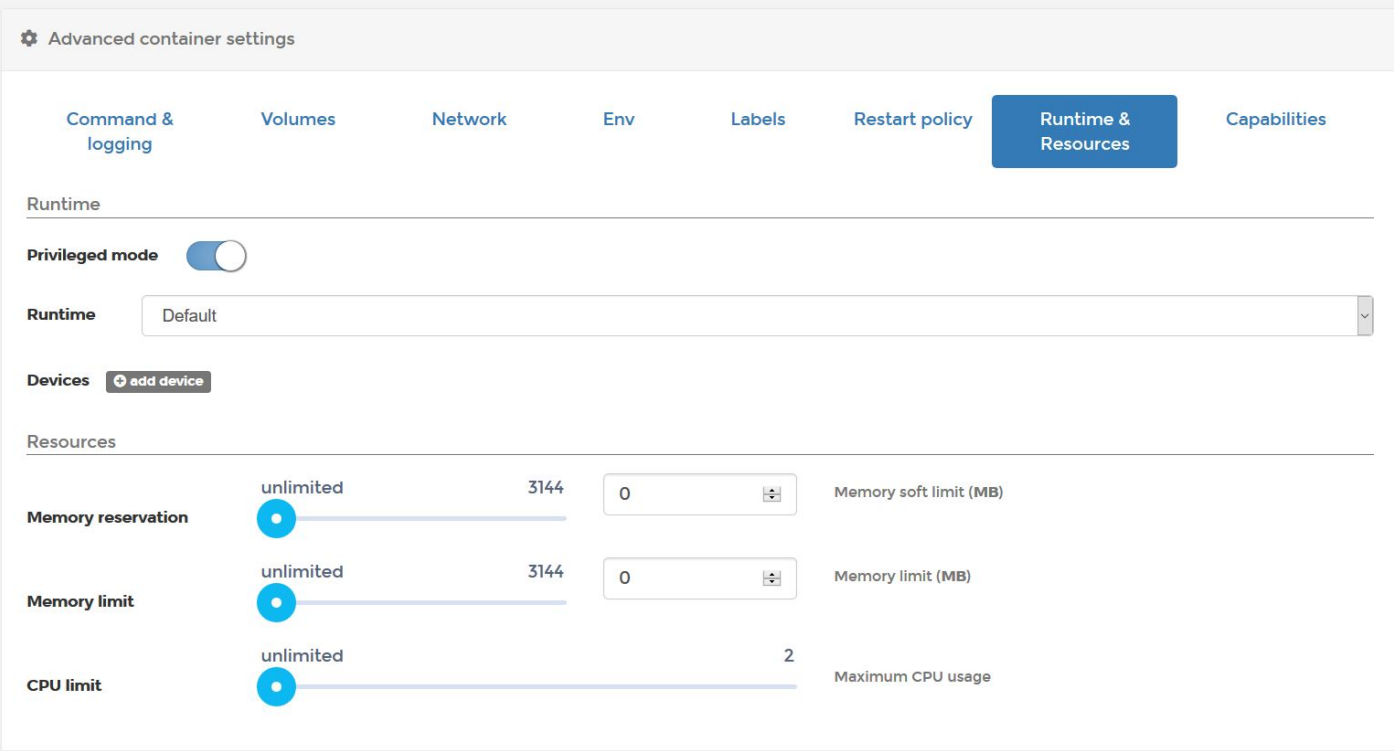
The stopped container was started successfully.

Starting a privileged Container with mounted volume:

Step 1: Click on “Add container” button. Enter “privileged-container” in the name field and select modified-ubuntu:latest in the image field.

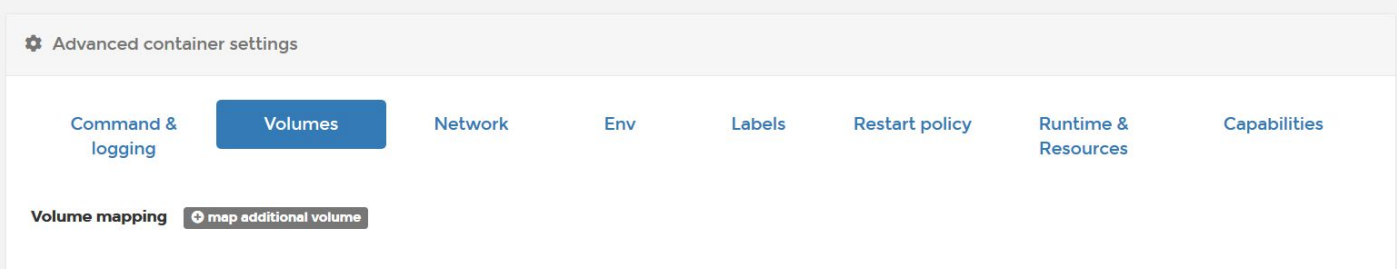


Step 2: Scroll down and enable the privileged mode option in the “Runtime & Resources” section.



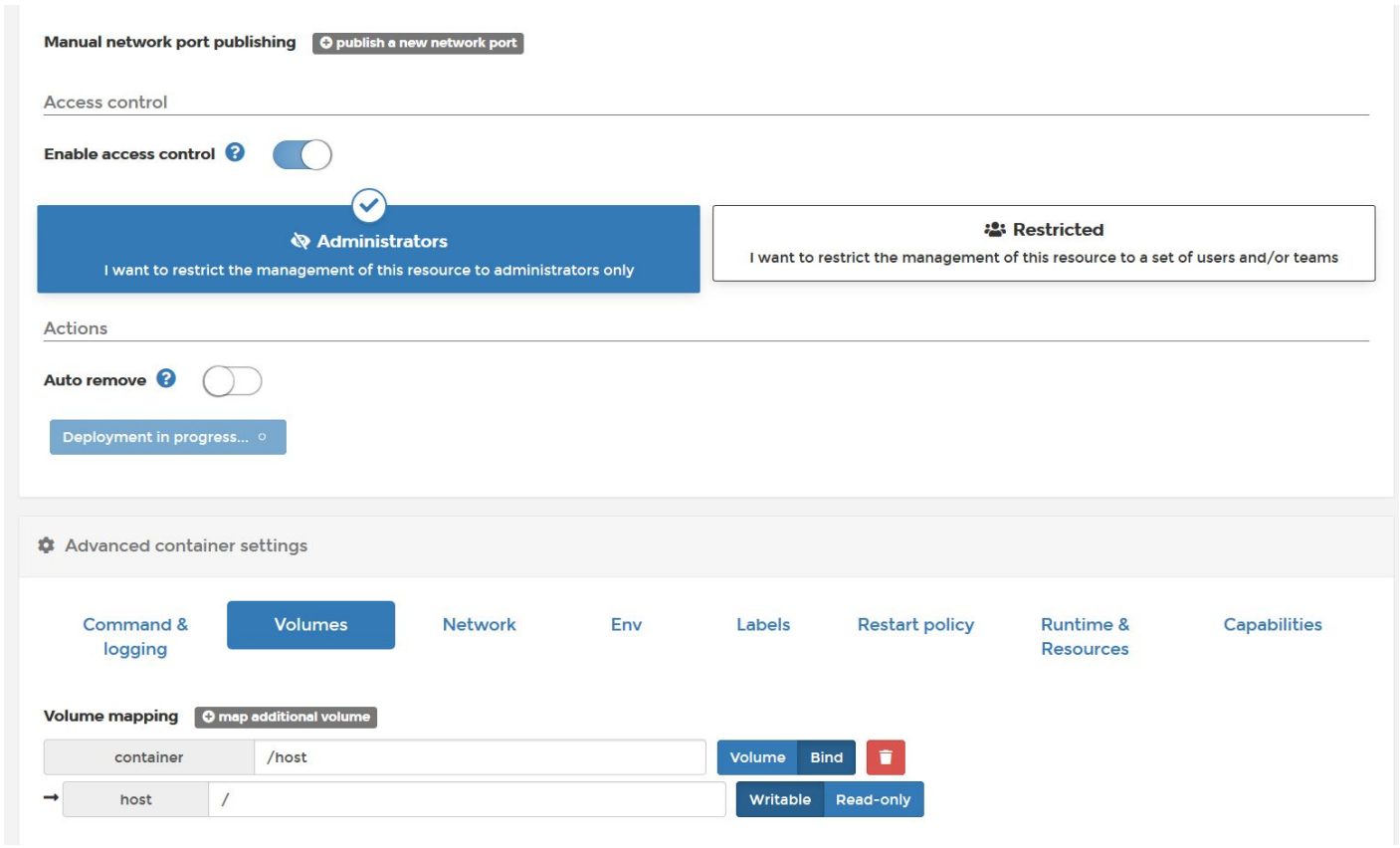
Memory and CPU restrictions can be placed through the settings in resources section.

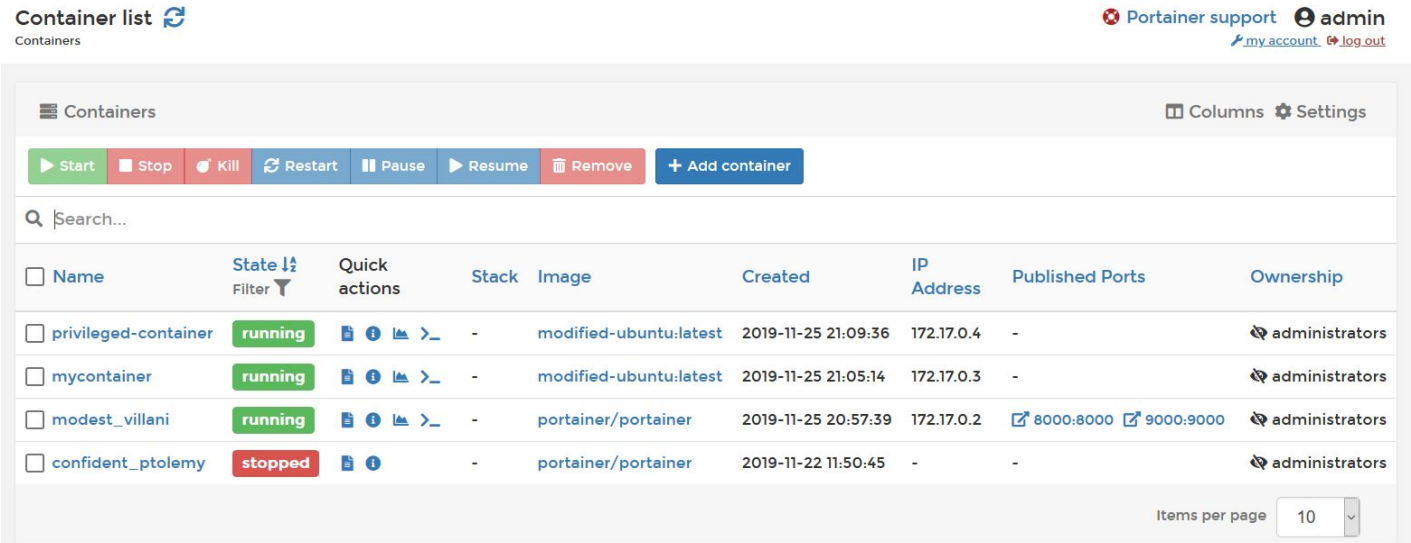
Step 3: Click on the Volumes tab.



Step 4: Click on the “map additional volume” button and select the bind option. Enter “/host” in the container field and enter “/” in the host field.

Step 5: Click on the “Deploy the container button”.





The container was started successfully.

Step 6: Access the Container console of the container.

Commands:
capsh --print
ls /host

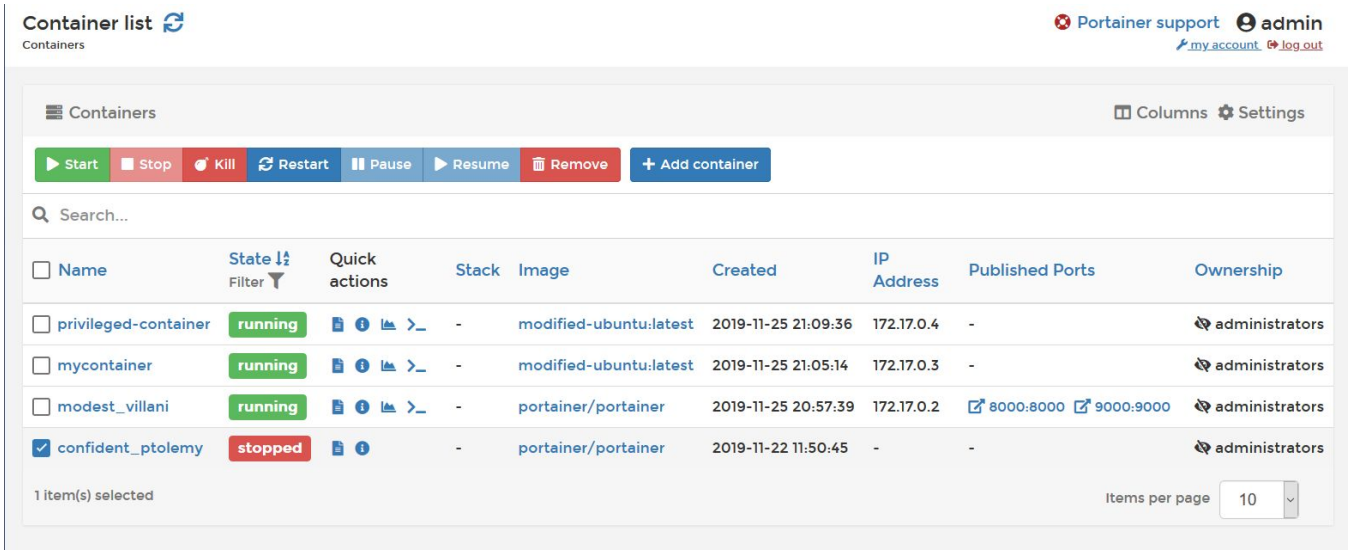
```
root@389acc394af7:~#
root@389acc394af7:~#
root@389acc394af7:~# capsh --print
Current: = cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,ca
p_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_module,
cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_ti
me,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_override,cap_mac_admin,cap_sy
slog,cap_wake_alarm,cap_block_suspend,cap_audit_read+eip
Bounding set =cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap
,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_modu
le,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys
_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_override,cap_mac_admin,cap
_syslog,cap_wake_alarm,cap_block_suspend,cap_audit_read
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=0(root)
gid=0(root)
groups=
root@389acc394af7:~#
root@389acc394af7:~#
root@389acc394af7:~# ls /host
bin  boot  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@389acc394af7:~#
```

The container is running in privileged mode and has all capability. The host filesystem is mounted on /host directory.

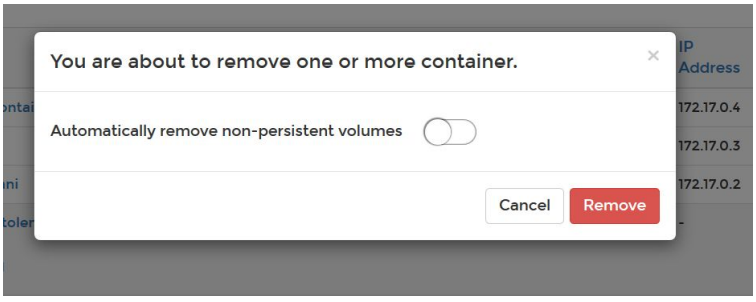
A container with additional capabilities or a mounted device can be started in a similar manner.

Removing a stopped container:

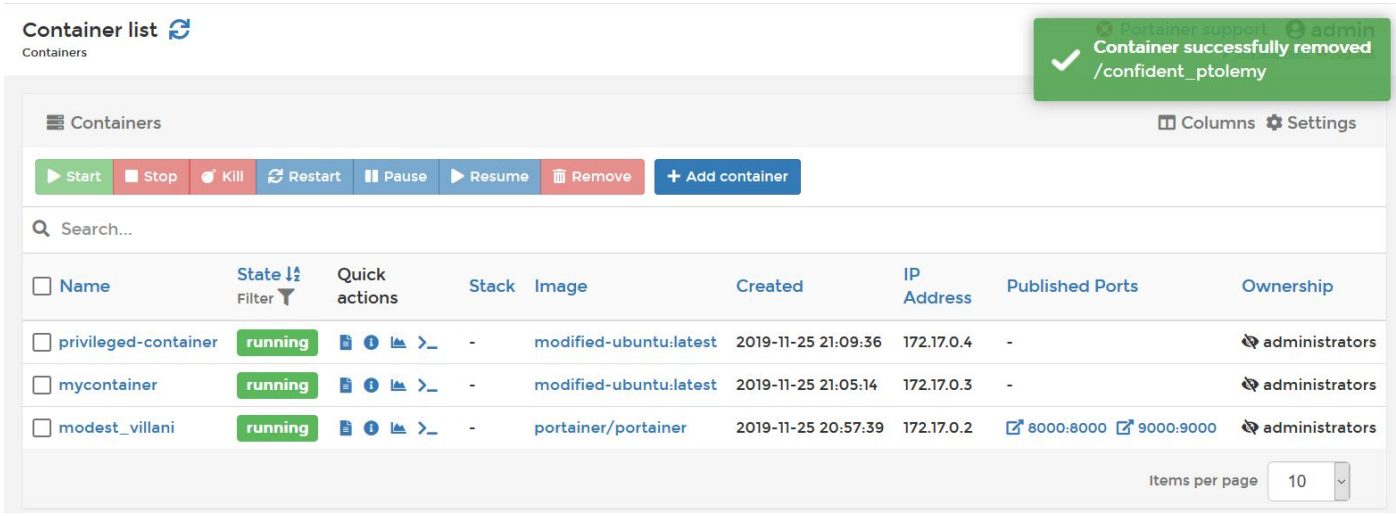
Step 1: Select the checkbox of the stopped container.



Step 2: Click on the Remove button and a dialog box will appear.



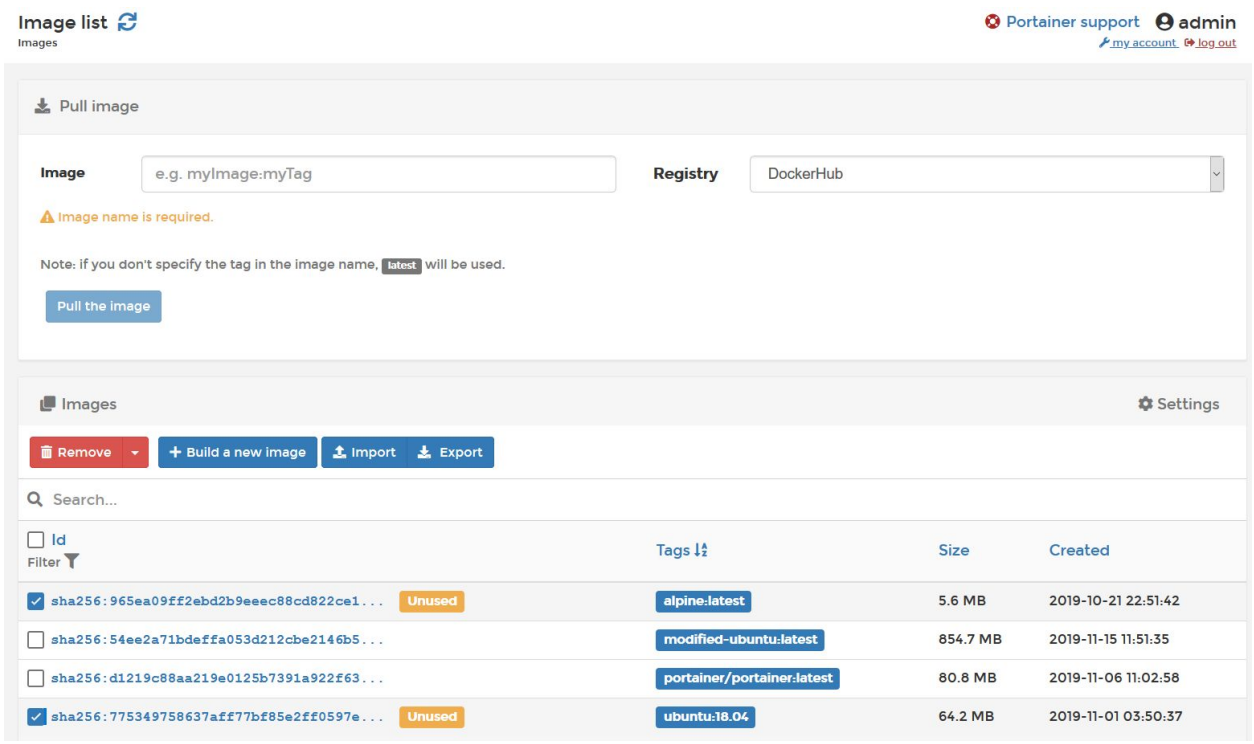
Step 3: Click on the Remove button to remove the container.



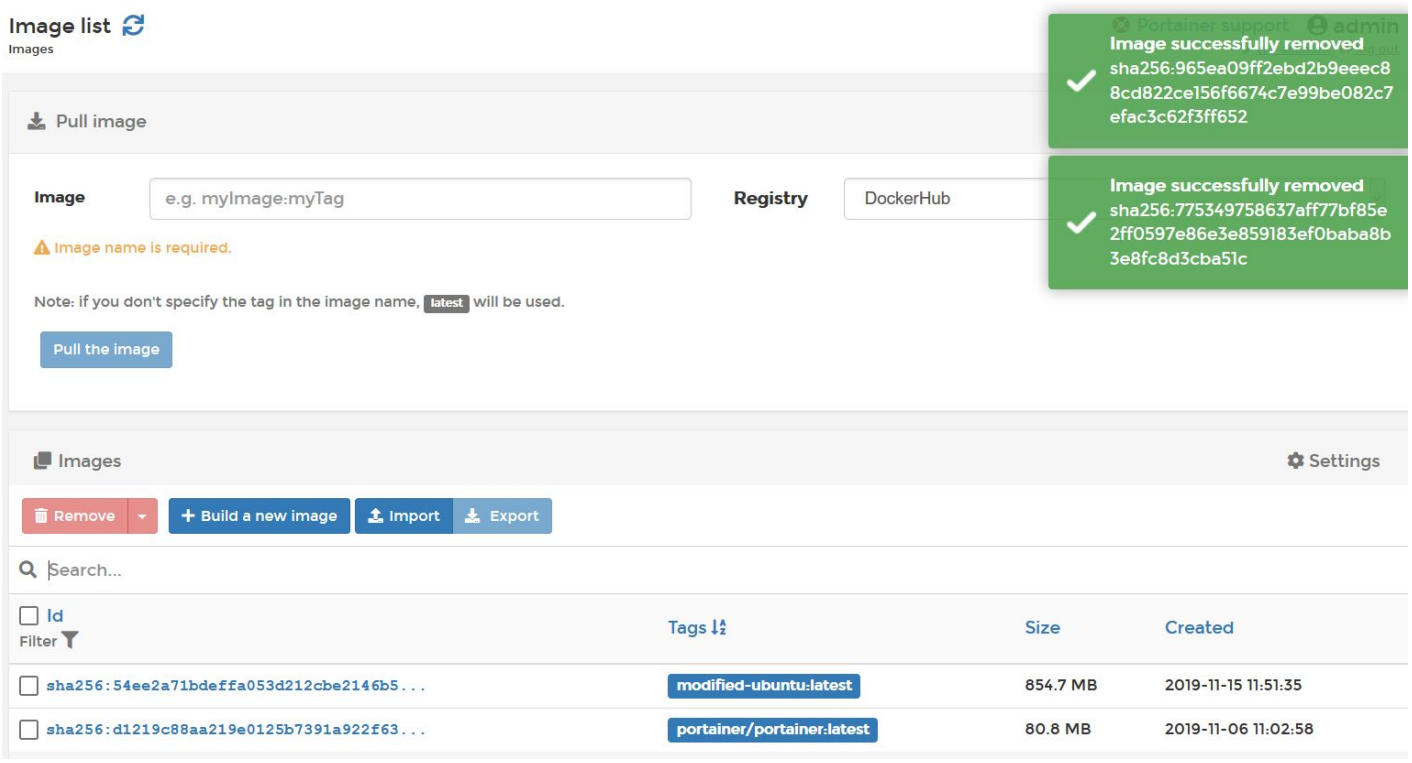
The container was removed successfully.

Delete unused images:

Step 1: Click on the images tab on the left panel. Tick the checkboxes of the unused images.



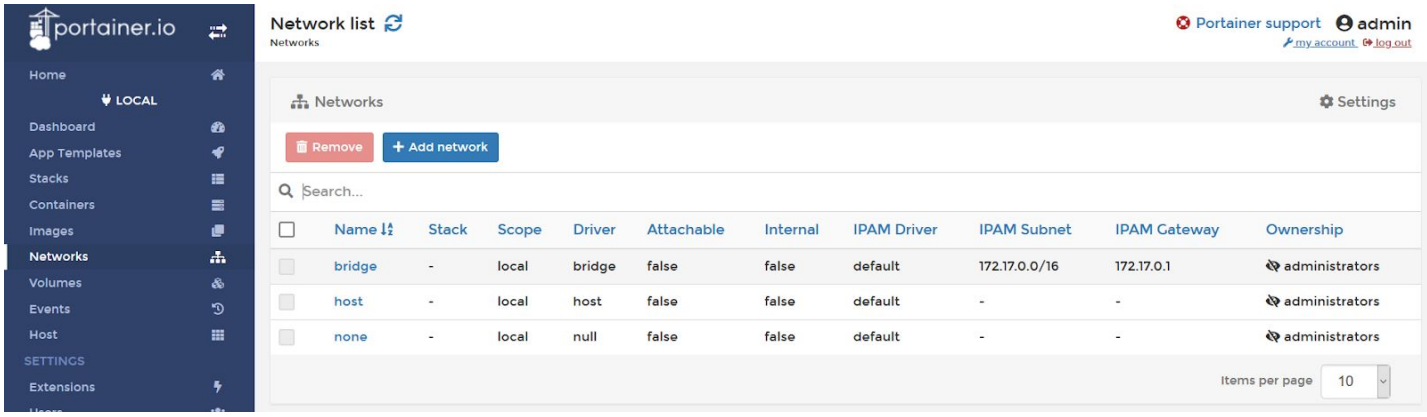
Step 2: Click on the remove button.



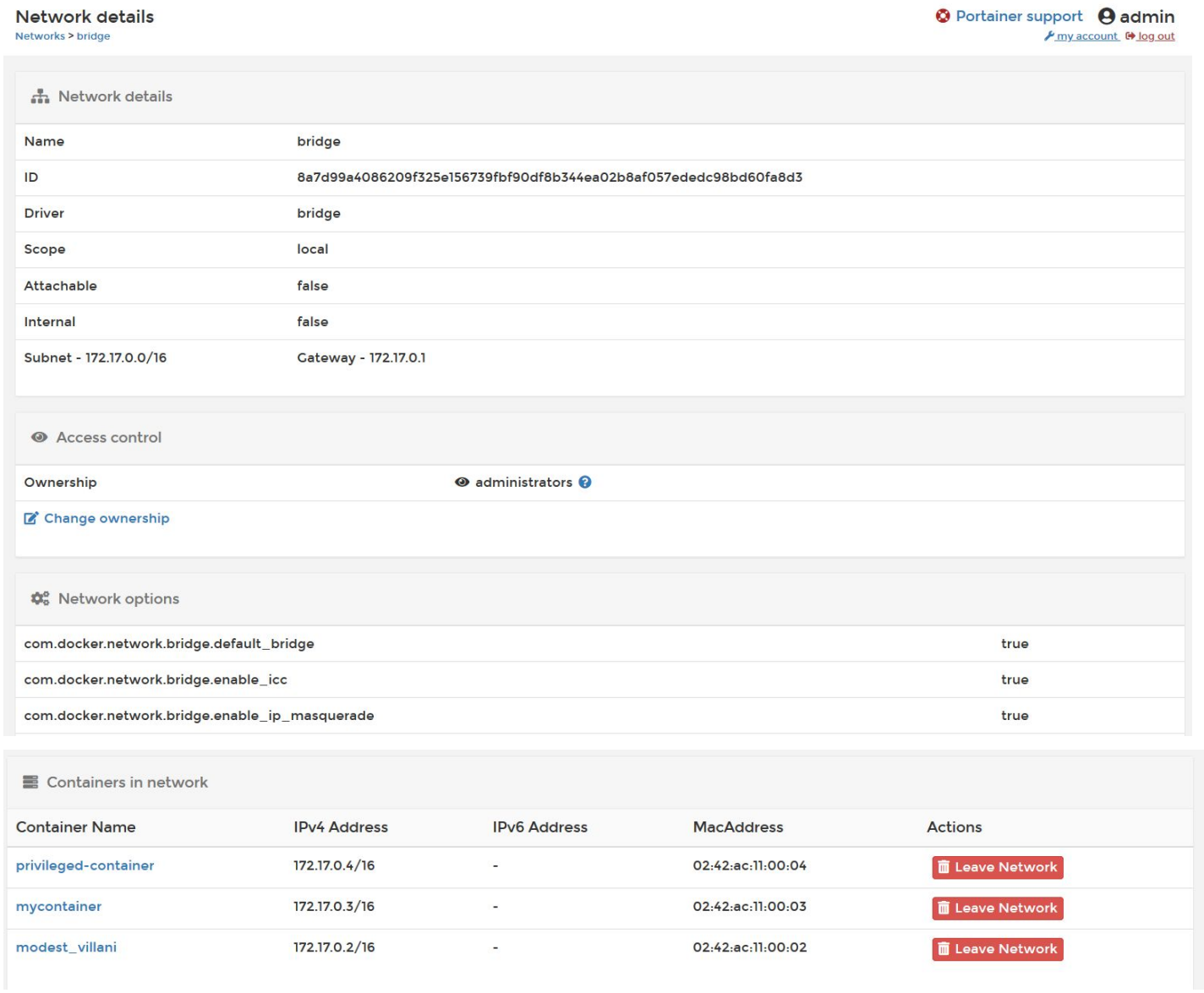
The images were deleted successfully.

Listing docker networks:

Step 1: Click on the Networks tab on the left panel



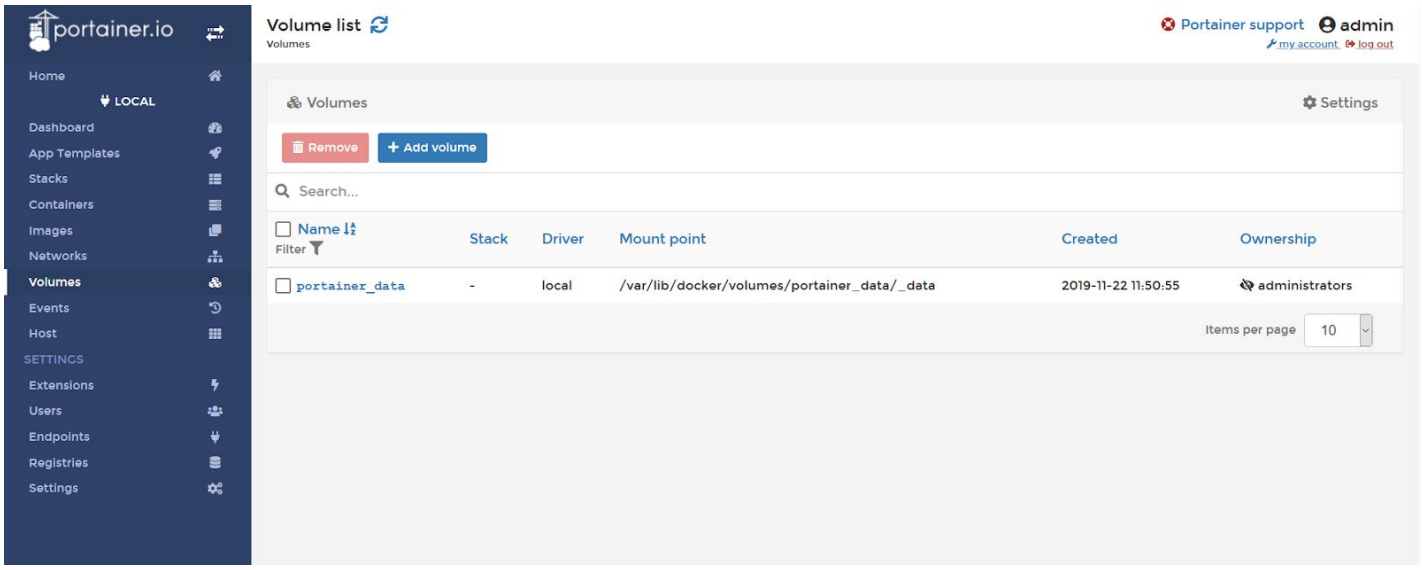
Step 2: Click on any of the network to view details of the network.



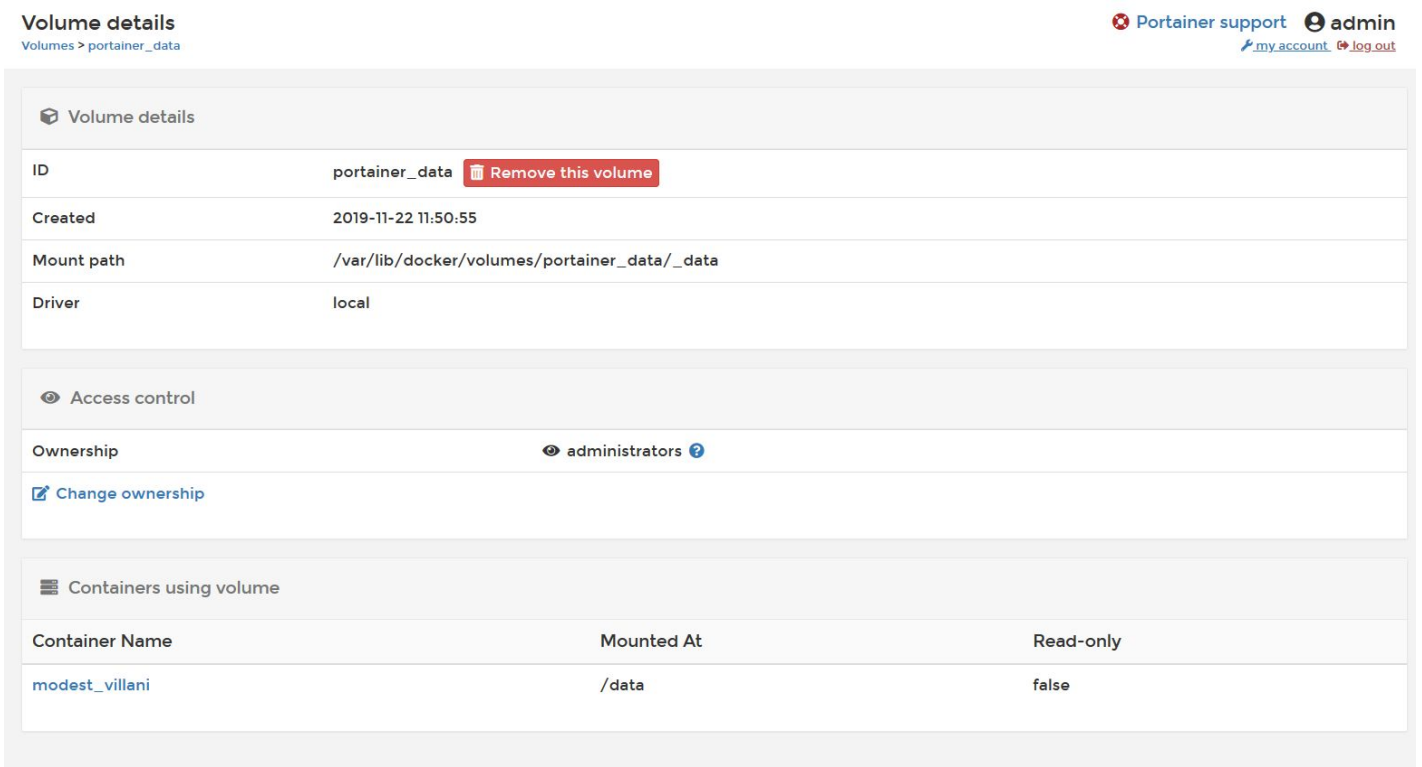
The bridge network is connected to all of the three running containers.

Listing docker volumes:

Step 1: Click on the volumes tab on the left panel.



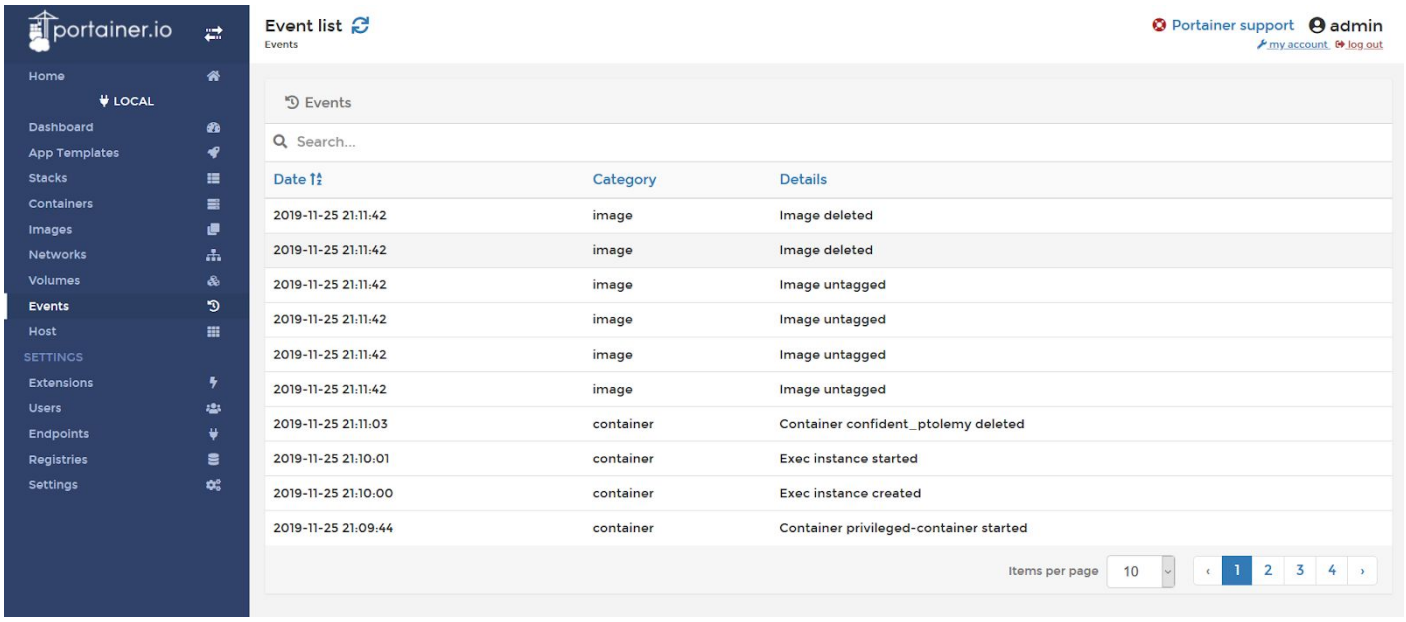
Step 2: Click on the name of the volume to view more details.



Viewing event logs:

Step 1: Click on the Events tab on the left panel.

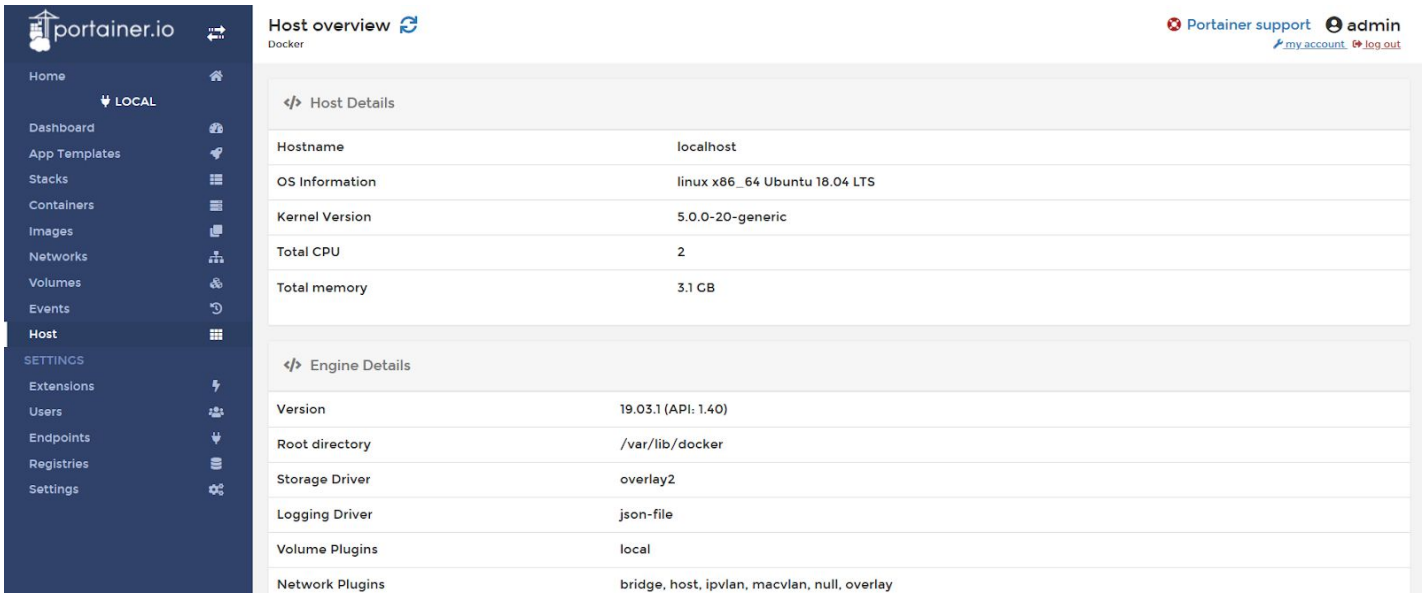
'



The information regarding all the events are listed on the webpage.

Viewing information regarding the host machine:

Step 1: Click on the Host tab on the left panel.



Information regarding the host machine as well as information regarding the docker engine is displayed in the Host overview section.

References:

1. Docker (https://www.docker.com/)
2. Portainer (https://www.portainer.io/)