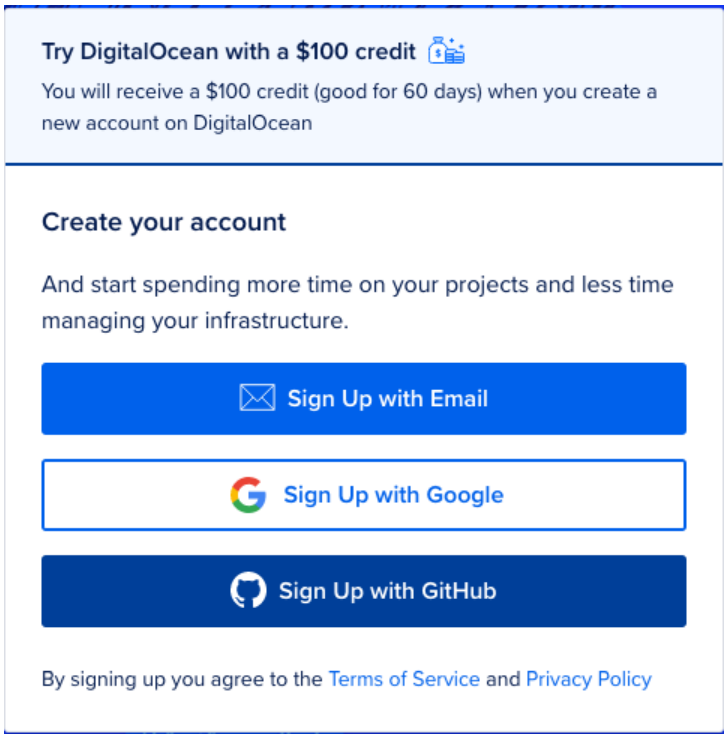
Introduction

This has the steps needed to create your own lab vm. We've tried to keep this as straightforward as possible.

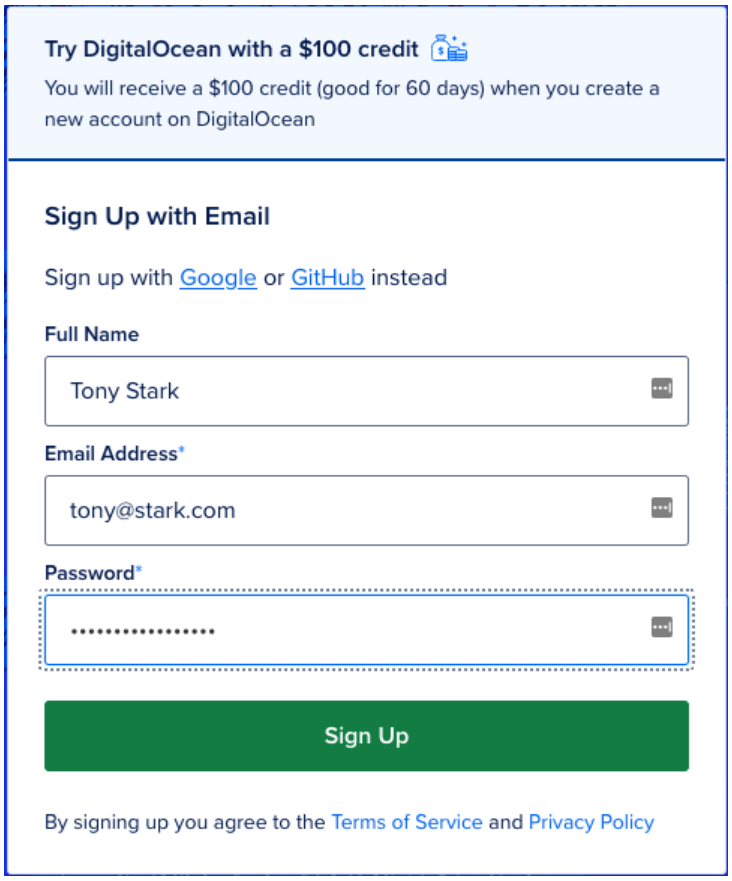
We'll be using DigitalOcean as our cloud provider in this walkthrough. When you sign up for the first time, they **may** offer a $100 credit for the first 60 days, meaning that you can set up and use the class vm for no cost for the first 60 days.

Create an account on DigitalOcean

If you already have an account at Digital Ocean, please Sign in and move on to the next step, Create a Droplet . Otherwise, start at https://www.digitalocean.com/ . Click the "Sign Up" button in the upper right. You can decide how to log in: Email, Google, or Github:



I'll sign up with email:



You'll get a link to click in your email to show you own it, and you'll be asked to add a credit card or paypal connection to pay for the services once your $100 credit or 60 days runs out.

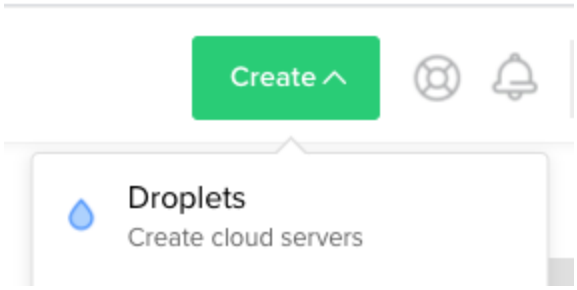
Create a Droplet

The control panel for Digital Ocean is at https://cloud.digitalocean.com .

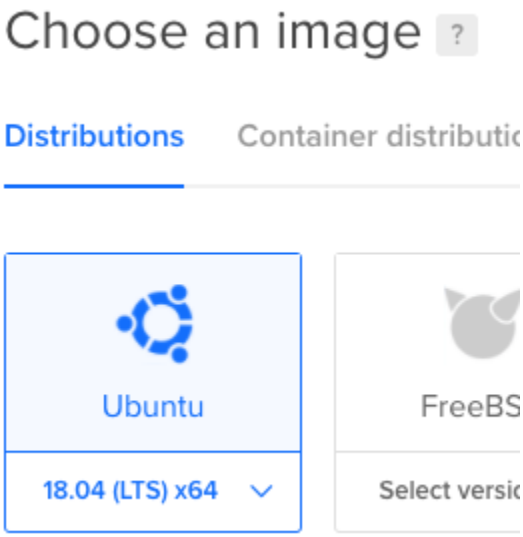
A "Droplet" is Digital Ocean's name for a virtual cloud server with a full operating system.

The instructions below will only cover the requirements for this lab virtual machine. You're welcome to change any other settings you feel are important to you or leave them at their defaults.

Press the green "Create" button at the top right, and from the drop-down menu, select "Droplets":

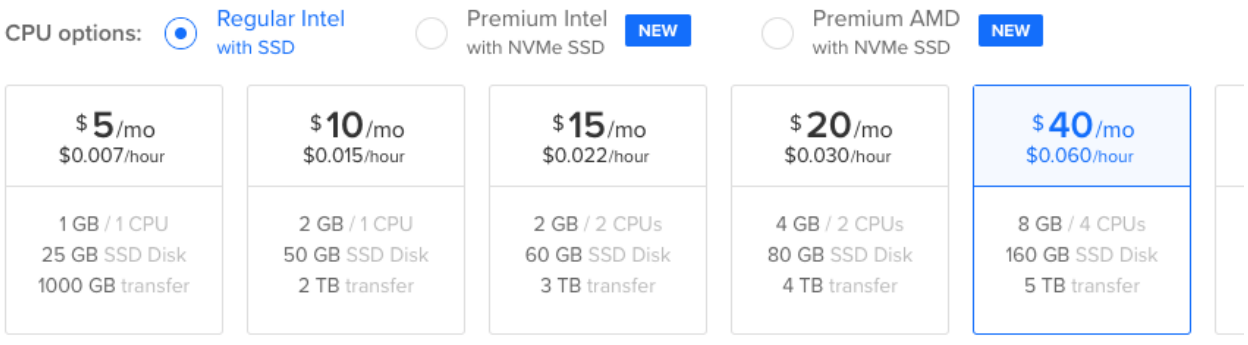


Under "Choose an image", "Distributions" should be highlighted. Below that, select Ubuntu **and change the version back to "18.04 (LTS) x64"** as 20.04 is not fully supported:



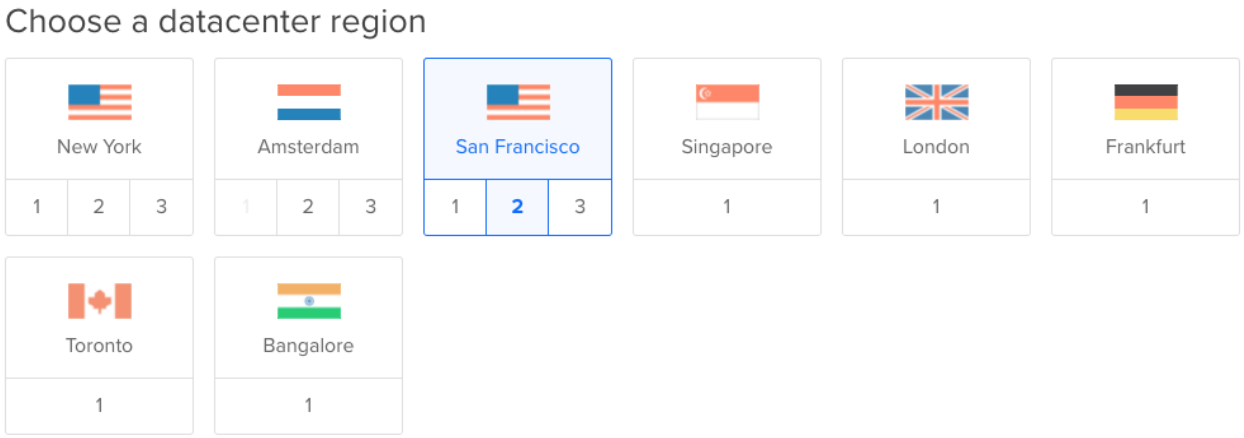
If you prefer an rpm-based distribution, pick Centos 7. Other distributions are not tested.

Under "Choose a plan", select "Basic". Change the CPU to "Regular Intel with SSD". The system we recommend is the highlighted box that shows "$40/mo, $0.060/hour, 8GB / 4 CPUs, 160GB SSD disk, 5TB transfer". 8GB of memory is needed to do all of the labs (if you have a 4GB system you can do all labs except "C2 over DNS with tshark").

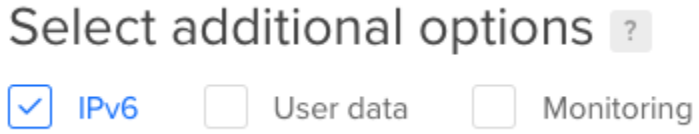


You won't need to add block storage (this is *additional* storage beyond the 160GB that comes with the base system).

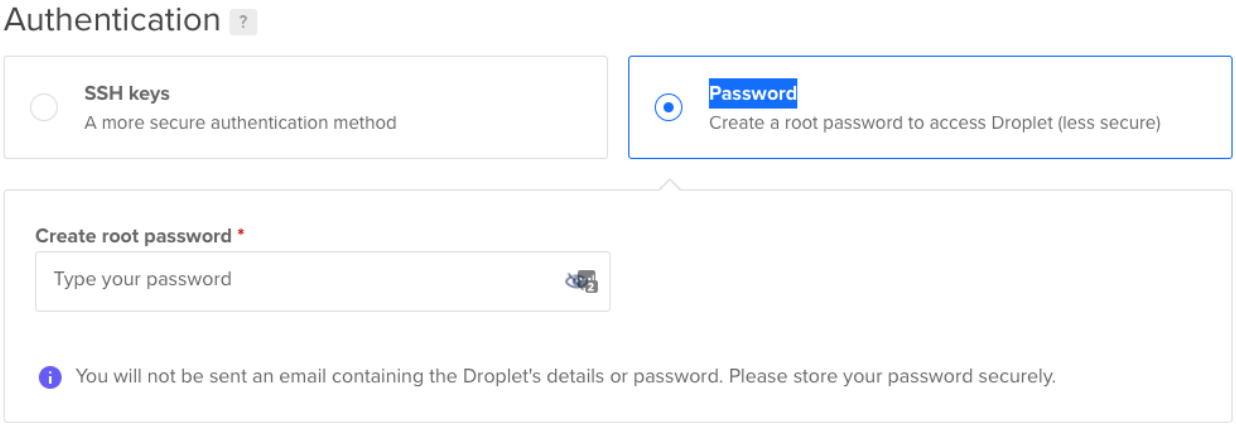
For your "Datacenter region", pick something geographically close - it'll make the system more responsive. Press on one of the available numbers below your preferred location - it doesn't matter which:



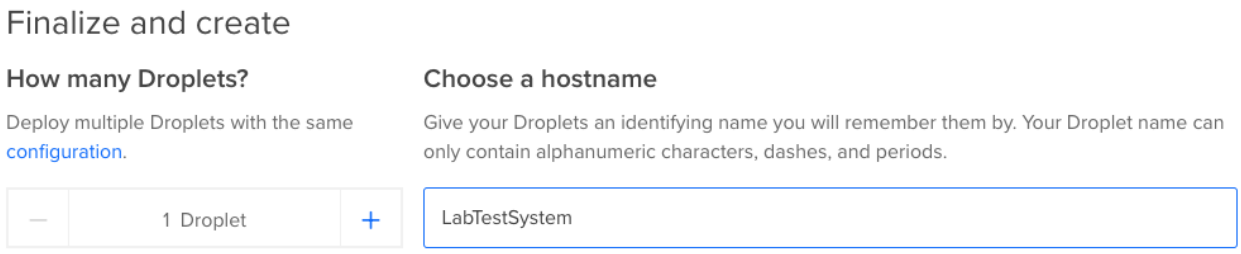
If you want to be able to reach the system via IPv6, check that off (IPv4 is always enabled):



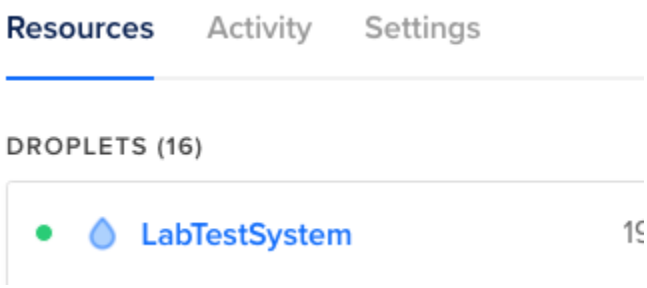
For authentication, password login is the simplest, though feel free to set up ssh keys if you prefer. Remember that ssh is open to the world and allows password authentication, so pick a strong password.



Finally, leave the number of droplets at 1 and put in a hostname that's meaningful for you:



Once all is good, press "Create Droplet". You'll be returned to the list of droplets you have. Click on the name of the system you just built:



and you'll be in the details screen for this system. Jot down the ipv4 address for the droplet. At the top of the details screen there'll be a progress bar for the build.

Once the build is complete, ssh to the system with:

`ssh root@`*`system.ip.address`*

Once you accept the system's SSH host key[1] and enter the root password you provided while creating the droplet, you'll get a command prompt:

```
$ ssh root@system.ip.here
The authenticity of host 'labtestsystem (system.ip)' can't be established.
ECDSA key fingerprint is SHA256:......
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'labtestsystem' (ECDSA) to the list of known hosts.
root@labtestsystem's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-121-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Mar 26 20:14:02 UTC 2021

  System load:  0.01               Processes:           107
  Usage of /:   0.7% of 154.90GB   Users logged in:     0
  Memory usage: 1%                 IP address for eth0: system.ip
  Swap usage:   0%                 IP address for eth1: 10.reserved.ip
```

[1] If you want to check the ssh fingerprint before blindly accepting it in the first ssh login, click on "Console" in the Digitalocean control panel for this system, log in, and run:

`ssh-keygen -l -f /etc/ssh/ssh_host_ecdsa_key.pub`

The fingerprint you get back should match what SSH reports on first connect.

```
0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@LabTestSystem:~#
```

Install the tools and data files needed for the lab

Download install-tools.sh:

```
wget https://threat-huntiing.s3.amazonaws.com/install-tools.v0.3.2.sh
```

Note, the "ii" in "huntiing" is not a typo.

Run install-tools.v0.2.3.sh as root:

```
bash ./install-tools.v0.3.2.sh
```

This script will pull down needed utilities, install rita and supporting tools, and pull down the sample data needed for the labs. It'll take a few minutes.

In this script you'll be asked if users other than root should be allowed to run wireshark to capture packets. Unless you know you'll be using this long term, will be creating non-root user accounts, and want them to sniff packets, leave the answer at the default of "No".

You'll also be asked to configure Zeek ("`Would you like to continue running the zeek configuration script and generate a new node.cfg file? (y/n)?`"). Respond with "`y`" (no quotes). For eth0 you'll be asked "`Would you like to include it as a sniff interface (y/n)?`" ; say "`y`" here too (again, no quotes). For eth1, answer "`n`". Finally, answer "`y`" to "`Would you like to replace the existing node.cfg with the above file?`"

When you're done, you can see the 3 lab directories by running the command:

```
ls -Al ~/lab*
```

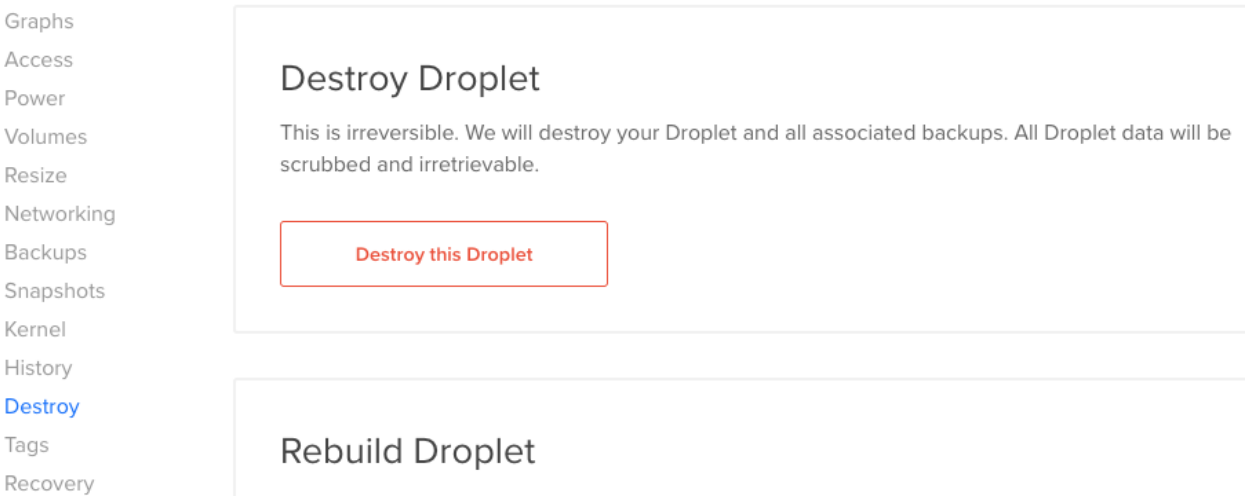
```
/root/lab1:
total 88512
-rw-rw-r-- 1 1000 1000  1769129 Feb 17 17:25 conn.log
-rw-rw-r-- 1 1000 1000    48722 Feb 17 17:25 dhcp.log
-rw-rw-r-- 1 1000 1000  1529159 Feb 17 17:25 dns.log
-rw-rw-r-- 1 1000 1000   169343 Feb 17 17:25 files.log
-rw-rw-r-- 1 1000 1000  1444115 Feb 17 17:25 http.log
```

```
-rw-rw-r-- 1 1000 1000      819 Feb 17 17:25 ntp.log
-rw-rw-r-- 1 1000 1000      254 Feb 17 17:25 packet_filter.log
-rw-rw-r-- 1 1000 1000   109204 Feb 17 17:25 ssl.log
-rwxrwxr-x 1 1000 1000 85294077 Jun 10  2020 trace1.pcap
-rw-rw-r-- 1 1000 1000    15630 Feb 17 17:25 weird.log
-rw-rw-r-- 1 1000 1000   235138 Feb 17 17:25 x509.log

/root/lab2:
total 456
-rw-rw-r-- 1 1000 1000   1281 Jan 22 16:01 conn.log
-rw-rw-r-- 1 1000 1000 453834 Jan 22 16:01 dns.log
-rw-rw-r-- 1 1000 1000    253 Jan 22 16:01 packet_filter.log
-rw-rw-r-- 1 1000 1000    470 Jan 22 16:01 weird.log

/root/lab3:
total 319724
-rw-rw-r-- 1 1000 1000   1294975 Feb 18 09:09 conn.log
-rw-rw-r-- 1 1000 1000     48738 Feb 18 09:09 dhcp.log
-rw-rw-r-- 1 1000 1000   1463736 Feb 18 09:09 dns.log
-rw-rw-r-- 1 1000 1000    176430 Feb 18 09:09 files.log
-rw-rw-r-- 1 1000 1000     26802 Feb 18 09:09 http.log
-rw-rw-r-- 1 1000 1000       254 Feb 18 09:09 packet_filter.log
-rw-rw-r-- 1 1000 1000    125354 Feb 18 09:09 ssl.log
-rw-r--r-- 1 1000 1000 323949399 Feb 17 17:17 trace3.pcap
-rw-rw-r-- 1 1000 1000     15621 Feb 18 09:09 weird.log
-rw-rw-r-- 1 1000 1000    266437 Feb 18 09:09 x509.log
```

If you get back a listing that includes "lab1", "lab2", and "lab3" similar to the above, you have everything installed. Your last step is to log out and log back in over ssh for the path changes to take effect.

Closing notes

You're welcome to continue using this Droplet after the class is done; we hope you'll take some more time to try out the tools and do the labs! **Remember: Digital Ocean continues to bill you for the Droplet until you delete it!** Logging out of it, halting it, or pressing the "On" button in the cloud control panel **will not stop the billing**. The only way to stop paying for the instance is to go to the details page for that droplet, choose "Destroy" from the left hand menu:



, press "Destroy this Droplet" and confirm the choice. Only then will billing stop.