How to setup an OnionDAO Tor Exit node

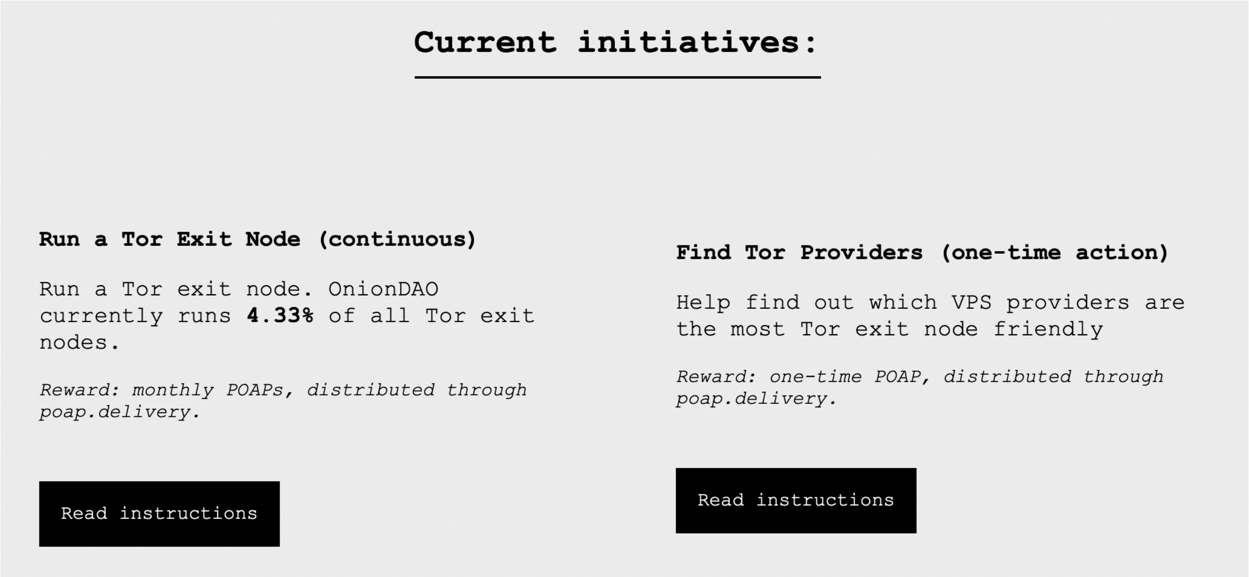
Hi everyone.

Today I'm going to demonstrate how easy it is to run a Tor exit node using the OnionDAO setup script.

In order to run the Tor exit node we will need to first purchase a Virtual Private Server, or VPS for short. The server needs at least 256MB of disk space and 1.5Gb of RAM. The OnionDAO maintains a curated list of Tor friendly data centers that you can use to find a suitable provider for your VPS. The link to that list can be found on the OnionDAO website, our Github, *and* in the description for this video.

Today's focus is on setting up an Ubuntu 20.04 LTSVPS that is capable of executing the OnionDAO Tor setup script, but if you would like to know more about the OnionDAO visit us at https://oniondao.web.app or join our Discord and say hi!

From the OnionDAO homepage we can scroll down to the current initiatives section which provides links to the GitHub for each initiative.



Current initiatives:

Run a Tor Exit Node (continuous)

Run a Tor exit node. OnionDAO currently runs **4.33%** of all Tor exit nodes.

Reward: monthly POAPs, distributed through poap.delivery.

Find Tor Providers (one-time action)

Help find out which VPS providers are the most Tor exit node friendly

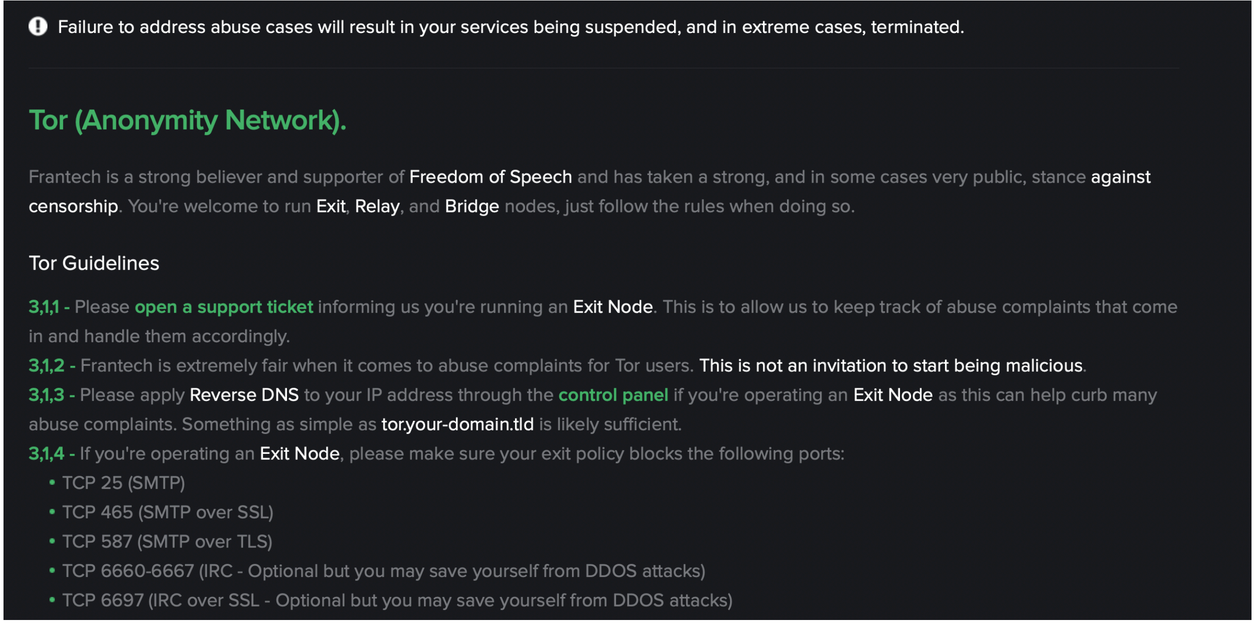
Reward: one-time POAP, distributed through poap.delivery.

Monthly POAPs are distributed to the wallet address of node operators running a Tor exit node each month. There is a limit of one POAP per wallet, regardless of how many exit nodes you are running.

I personally use BuyVM.net for my Tor Exit Node, but I encourage you all to check our curated list or submit your own recommendations. The list is accessible from the homepage by clicking on “Read Instructions” under the “Find Tor Providers” initiative, or by accessing it directly at https://docs.google.com/spreadsheets/d/1ztkonpfs0u3NP1HA-V6rhE6eK77W6y0Q8gG_yv9tI3s/edit#gid=1189411818

It’s vital for the health of the Tor network that we have a diverse set of data centers and operators across the world, so if you have a recommendation of your own please submit then and get your POAP!

Alright, once you’ve picked out your data center provider it’s important to check out their terms of service for guidelines on using Tor. Scroll down to the relevant Tor section of the BuyVM TOS found at https://buyvm.net/acceptable-use-policy/ and you’ll see a detailed list of requirements for running a Tor Exit Node.



Failure to address abuse cases will result in your services being suspended, and in extreme cases, terminated.

Tor (Anonymity Network).

Frantech is a strong believer and supporter of **Freedom of Speech** and has taken a strong, and in some cases very public, stance **against censorship**. You're welcome to run **Exit**, **Relay**, and **Bridge** nodes, just follow the rules when doing so.

Tor Guidelines

3,1,1 - Please **open a support ticket** informing us you're running an **Exit Node**. This is to allow us to keep track of abuse complaints that come in and handle them accordingly.

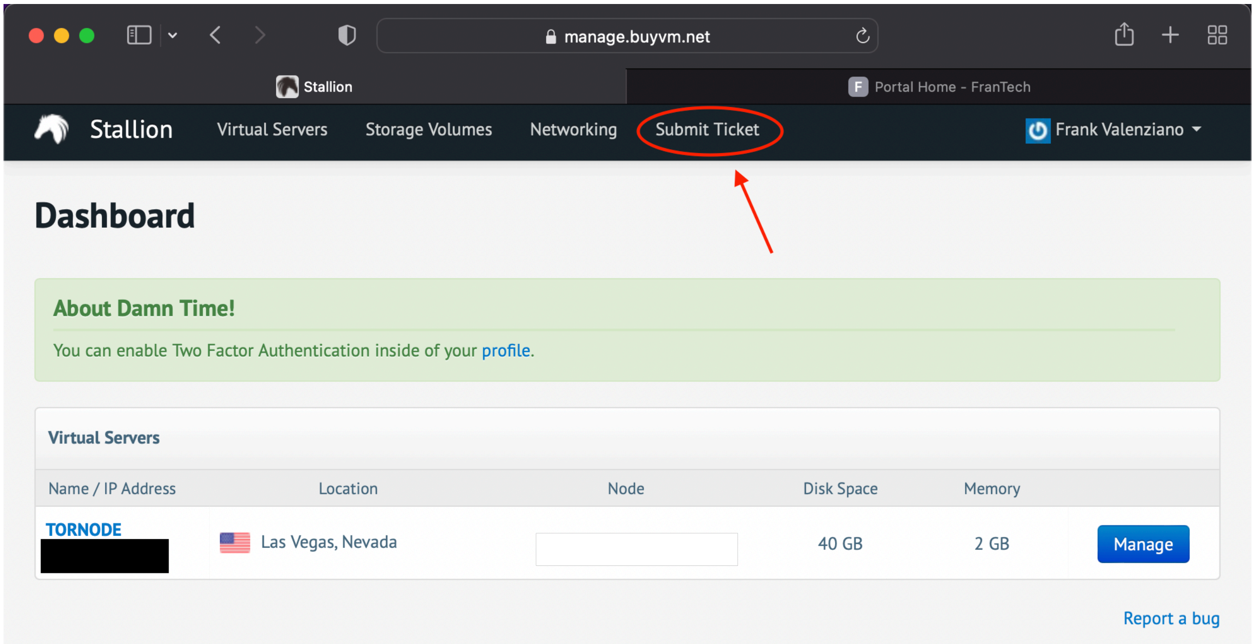
3,1,2 - Frantech is extremely fair when it comes to abuse complaints for Tor users. **This is not an invitation to start being malicious**.

3,1,3 - Please apply **Reverse DNS** to your IP address through the **control panel** if you're operating an **Exit Node** as this can help curb many abuse complaints. Something as simple as **tor.your-domain.tld** is likely sufficient.

3,1,4 - If you're operating an **Exit Node**, please make sure your exit policy blocks the following ports:

- TCP 25 (SMTP)
- TCP 465 (SMTP over SSL)
- TCP 587 (SMTP over TLS)
- TCP 6660-6667 (IRC - Optional but you may save yourself from DDOS attacks)
- TCP 6697 (IRC over SSL - Optional but you may save yourself from DDOS attacks)

The first requirement is that we open a support ticket notifying BuyVM that we will be running a Tor Exit Node. The link is at the top of your account page once logged into the dashboard. A simple message will suffice, I just wrote “Hi, I will be running a Tor Exit Node” and then setup the node once BuyVM support acknowledged my ticket.



Dashboard

About Damn Time!

You can enable Two Factor Authentication inside of your profile.

Virtual Servers

Name / IP Address	Location	Node	Disk Space	Memory	
TORNODE [redacted]	Las Vegas, Nevada		40 GB	2 GB	Manage

Frantech isn't lying when they say they are extremely fair with handling abuse complaints. I've run my exit node with them for over a month and have not had any issues.

Please, don't abuse the network.

To comply with section 3.1.3 I simply set my Reverse DNS to tor.fav53.tld.

As for section 3.1.4, the OnionDAO script enables the Tor "ReducedExitPolicy" which blocks each of these ports. Tor and the OnionDAO Tornode source-code is available on Github. (https://github.com/torproject) (https://github.com/Onion-DAO/tornode) (https://gitlab.torproject.org/legacy/trac/-/wikis/doc/ReducedExitPolicy)

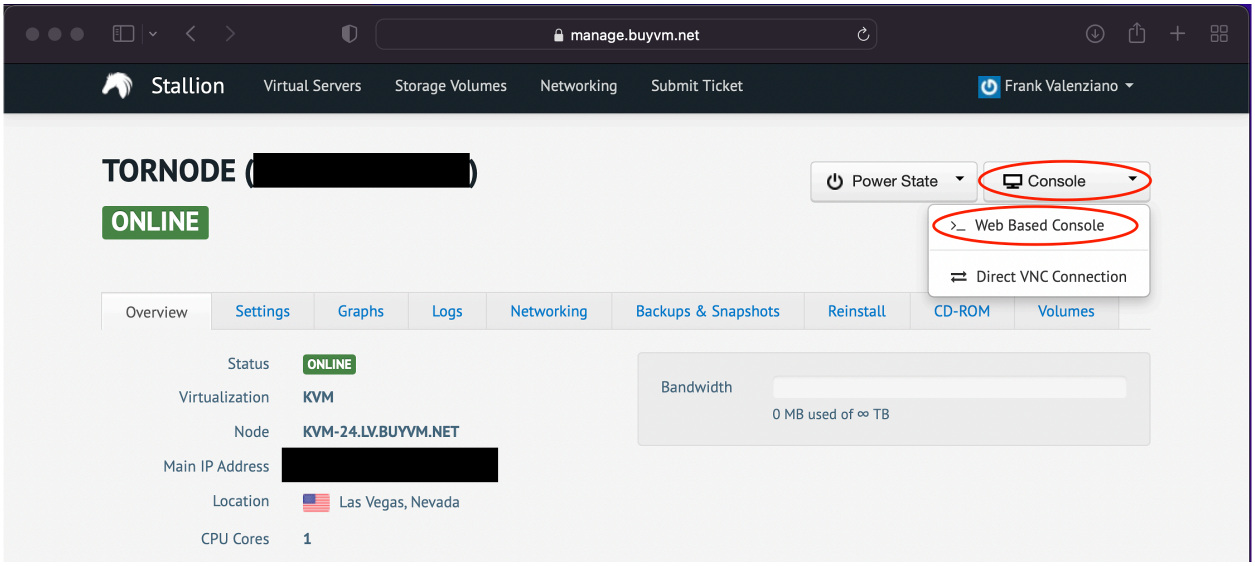
— —

Alright, on to the technical configuration. Going forward it is assumed that you have signed up for a data center, reviewed their TOS, and launched an Ubuntu 20.04 LTS instance and have enabled SSH.

If your provider doesn't have Ubuntu 20.04 LTSas one of the pre-selected options then you can install Ubuntu 20.04 LTS manually. Digital Ocean has a great guide on how to achieve this if you need to install Ubuntu 20.04 LTS manually (https://www.digitalocean.com/community/tutorials/initial-server-setup-with-Ubuntu 20.04 LTS-20-04) so we won't cover that again here.

Setting up the Tor exit node is pretty straightforward, if you run into any issues you can check out the Tor project Relay Operator (https://forum.torproject.net/c/support/relay-operator/17) forums as well as our Discord for assistance.

If you're using BuyVM head to manage.buyvm.net and connect to your server using the web console, or by enabling SSH and connecting from a shell of your choice. Go to Console > Web Console from the menu at the top right of the dashboard. Once selected a new window will appear, if it doesn't then you probably have popups blocked.



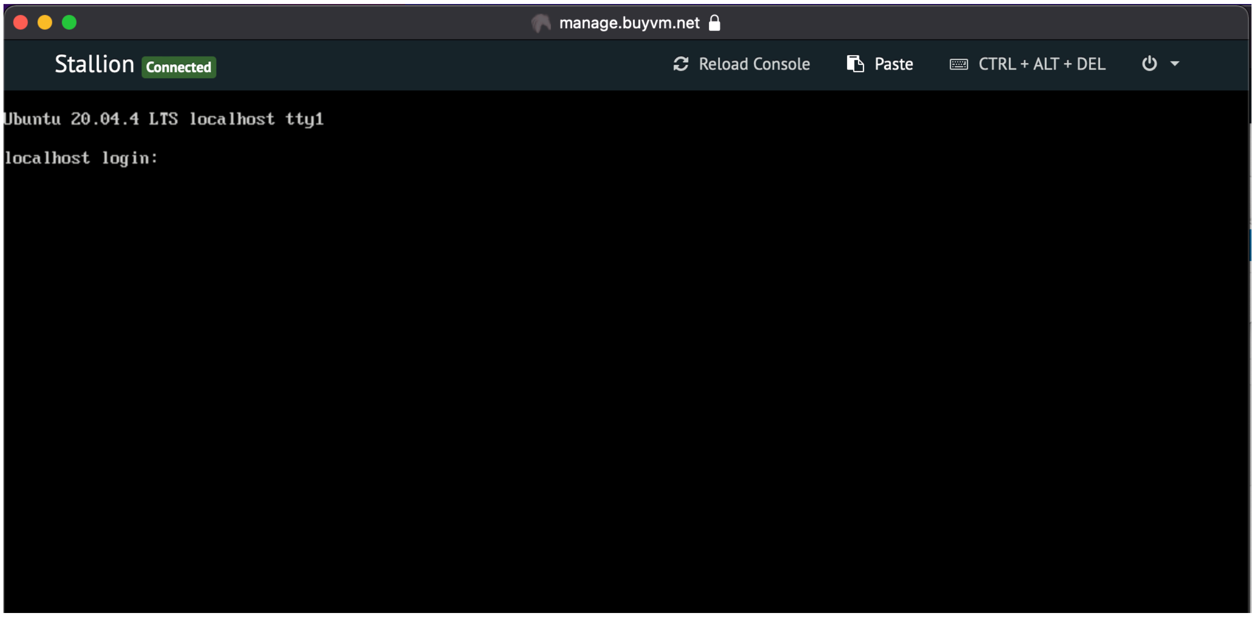
TORNODE ([redacted])

ONLINE

Status ONLINE
Virtualization KVM
Node KVM-24.LV.BUYVM.NET
Main IP Address [redacted]
Location Las Vegas, Nevada
CPU Cores 1

Bandwidth
0 MB used of ∞ TB

Login as the root user using the credentials you chose when setting up the VPS.



```
Ubuntu 20.04.4 LTS localhost tty1

localhost login:
```

Login as root and create a new user, set their password and enable sudo access by issuing the following commands:

```
mkdir /home/tor && useradd -d /home/tor -G sudo tor && chown -R tor /home/tor && passwd tor
```

Typically the following installation steps would be performed from a standard user account, but there's a bug with installation from elevated sessions so we will configure Tor from the root account and user our local account to monitor it with Nyx.

As root and run the following commands to bring our system up-to-date and the required packages installed:

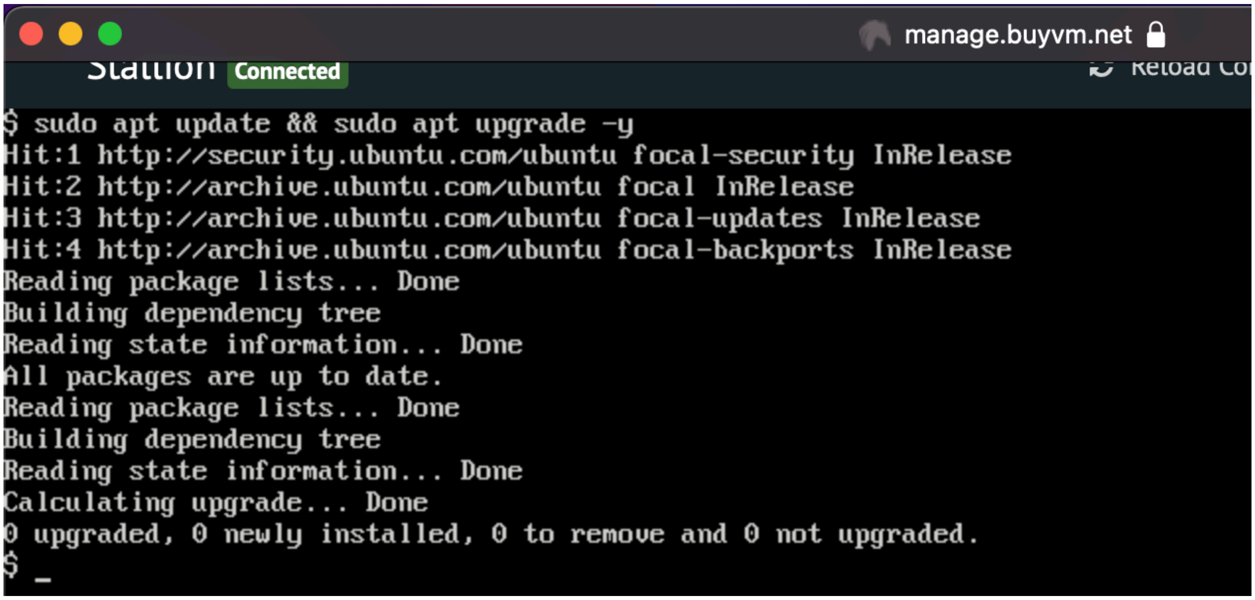
```
apt update && apt upgrade -y && apt install build-essential libevent-dev libssl-dev zlib1g zlib1g-dev git gnupg2 -y
```

Logout by typing logout and then sign back in as the tor user. Let's test our new sudo access and update our system at the same time by issuing the following command:

```
sudo apt update && sudo apt upgrade -y
```

If all goes well your system should install any missing updates. This can take a few minutes, reboot once the updates are finished installing if prompted to do so by typing:

```
sudo reboot
```



```
$ sudo apt update && sudo apt upgrade -y
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
$ _
```

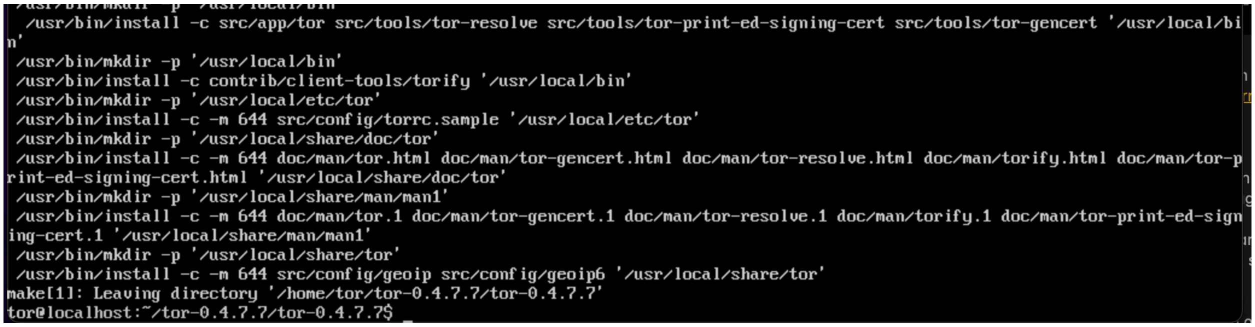
Once that's finished, download the latest version of Tor from https://forum.torproject.net/t/stable-release-0-4-7-7/3108 by issuing the command:

    wget https://archive.torproject.org/tor-package-archive/tor-0.4.7.7.tar.gz && tar xvf tor-0.4.7.7.tar.gz && cd tor-0.4.7.7 && ./configure && make && sudo make install

I recommend checking the torproject archive before downloading to make sure you're still using the latest version.

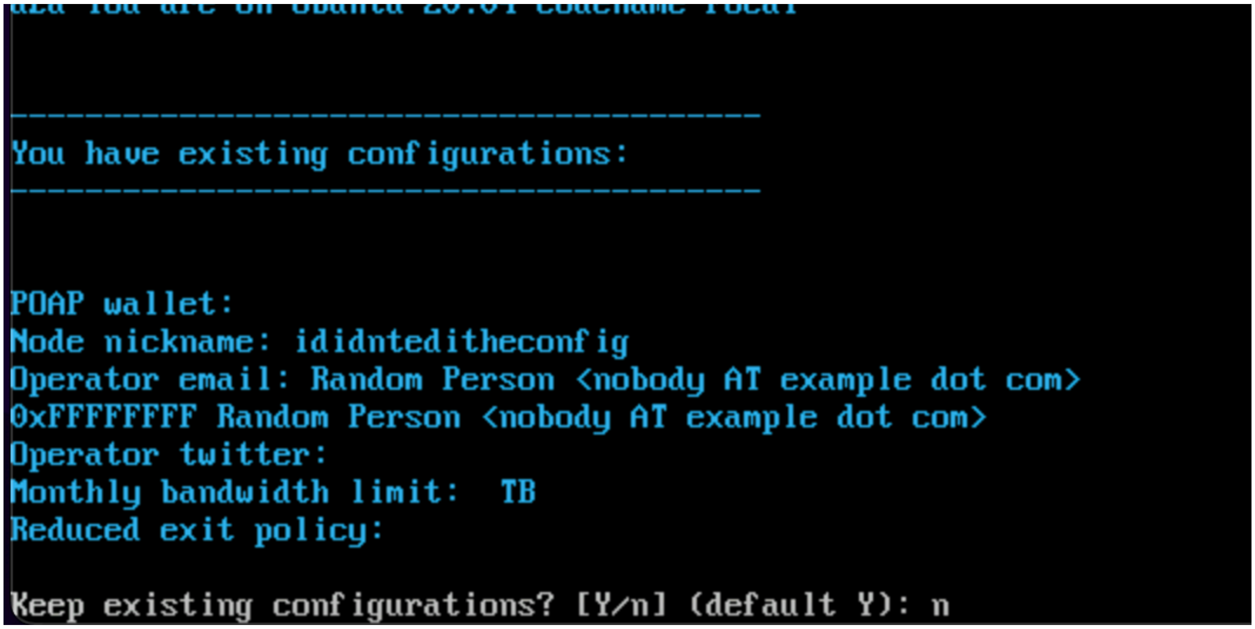
If your build runs into any errors they usually tell you which missing packages to install, otherwise come find us on Discord or check the torproject forums for help.

If successful the output will look something similar to the below screenshot:

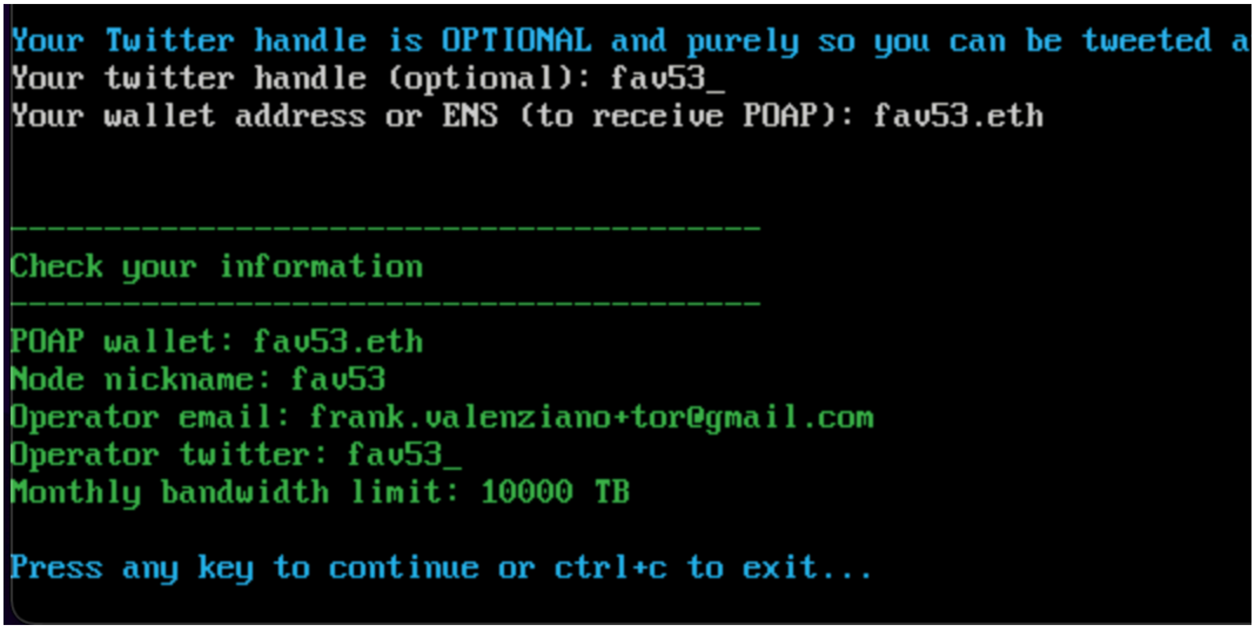


```
 /usr/bin/install -c src/app/tor src/tools/tor-resolve src/tools/tor-print-ed-signing-cert src/tools/tor-gencert '/usr/local/bi
n'
 /usr/bin/mkdir -p '/usr/local/bin'
 /usr/bin/install -c contrib/client-tools/torify '/usr/local/bin'
 /usr/bin/mkdir -p '/usr/local/etc/tor'
 /usr/bin/install -c -m 644 src/config/torrc.sample '/usr/local/etc/tor'
 /usr/bin/mkdir -p '/usr/local/share/doc/tor'
 /usr/bin/install -c -m 644 doc/man/tor.html doc/man/tor-gencert.html doc/man/tor-resolve.html doc/man/torify.html doc/man/tor-p
rint-ed-signing-cert.html '/usr/local/share/doc/tor'
 /usr/bin/mkdir -p '/usr/local/share/man/man1'
 /usr/bin/install -c -m 644 doc/man/tor.1 doc/man/tor-gencert.1 doc/man/tor-resolve.1 doc/man/torify.1 doc/man/tor-print-ed-sign
ing-cert.1 '/usr/local/share/man/man1'
 /usr/bin/mkdir -p '/usr/local/share/tor'
 /usr/bin/install -c -m 644 src/config/geoip src/config/geoip6 '/usr/local/share/tor'
make[1]: Leaving directory '/home/tor/tor-0.4.7.7/tor-0.4.7.7'
tor@localhost:~/tor-0.4.7.7/tor-0.4.7.7$ _
```

Once we've manually installed the latest Tor package we can run our OnionDAO script again to ensure we have all the necessary tools, such as Nyx, and are registered for the monthly POAPS. Note that by manually installing Tor we have overwritten the OnionDAO configurations, so if you’ve been running previous setups you may need to fill out the requested details again. If so, just select “n” when prompted to accept the existing configuration.



```
You are on Ubuntu 20.04 codename focal



----------------------------------------
You have existing configurations:
----------------------------------------


POAP wallet:
Node nickname: ididnteditheconfig
Operator email: Random Person <nobody AT example dot com>
0xFFFFFFFF Random Person <nobody AT example dot com>
Operator twitter:
Monthly bandwidth limit:  TB
Reduced exit policy:

Keep existing configurations? [Y/n] (default Y): n
```

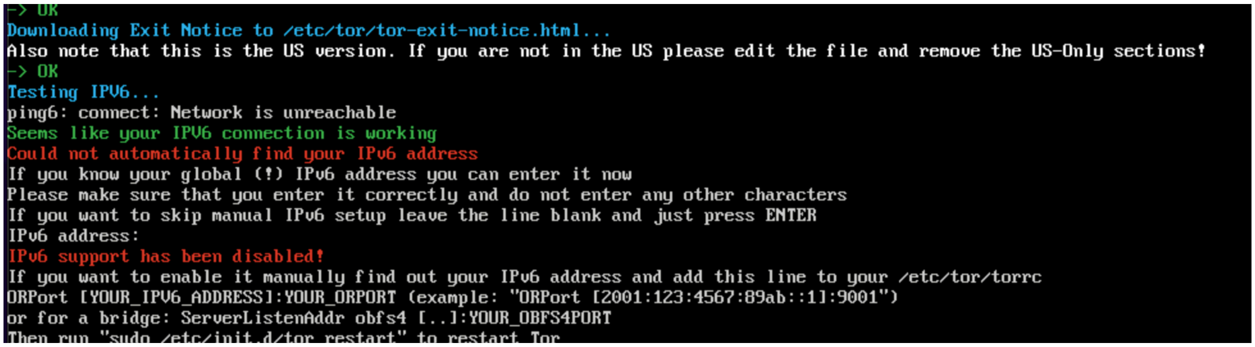


```
Your Twitter handle is OPTIONAL and purely so you can be tweeted a
Your twitter handle (optional): fav53_
Your wallet address or ENS (to receive POAP): fav53.eth



----------------------------------------
Check your information
----------------------------------------
POAP wallet: fav53.eth
Node nickname: fav53
Operator email: frank.valenziano+tor@gmail.com
Operator twitter: fav53_
Monthly bandwidth limit: 10000 TB

Press any key to continue or ctrl+c to exit...
```

Press enter to accept the settings once you’ve reviewed them. These addresses are publicly visible to the entire world, so don’t use any details that you want to keep private.

Note: Tor will use all your bandwidth if you allow it, so if you have a data cap it may be exceeded within days of running your node. If you need help configuring advanced throttling check out the official documentation from https://support.torproject.org/relay-operators/limit-total-bandwidth/ and feel free to ask in the Tor relay operator forums or the OnionDAO Discord if you have any questions.

Setting up IPv6 is specific to your data center so that won't be covered here. If you don't have IPv6 just leave the entry blank and press enter when prompted, this will trigger the script to disable IPv6 automatically.



```
-> OK
Downloading Exit Notice to /etc/tor/tor-exit-notice.html...
Also note that this is the US version. If you are not in the US please edit the file and remove the US-Only sections!
-> OK
Testing IPV6...
ping6: connect: Network is unreachable
Seems like your IPV6 connection is working
Could not automatically find your IPv6 address
If you know your global (!) IPv6 address you can enter it now
Please make sure that you enter it correctly and do not enter any other characters
If you want to skip manual IPv6 setup leave the line blank and just press ENTER
IPv6 address:
IPv6 support has been disabled!
If you want to enable it manually find out your IPv6 address and add this line to your /etc/tor/torrc
ORPort [YOUR_IPV6_ADDRESS]:YOUR_ORPORT (example: "ORPort [2001:123:4567:89ab::1]:9001")
or for a bridge: ServerListenAddr obfs4 [..]:YOUR_OBFS4PORT
Then run "sudo /etc/init.d/tor restart" to restart Tor
```

Once the setup script completes we can check on our node using Nyx. But first we need to be in the right group. Run:

```
usermod -G Debian-tor tor
```

From here you'll want to log off your root account and log in as our standard user, tor and try running Nyx. If you get an authcookie related error while trying to run Nyx as a standard user you'll need to update your Torrc by adding the following to the bottom of the /etc/tor/torrc file:

```
CacheDirectoryGroupReadable 1
```

Note the spaces there should be one space before the start of the Cache option to match the rest of the Torch file. Reboot the server and log back in as tor and run Nyx again.

This will require running 'oniondao update' from the root account again before Nyx will work.

Nyx will show you the recent logs as well as your current utilization statistics. Note that there's a bonding period before your Exit node starts accepting any real traffic. (https://blog.torproject.org/lifecycle-of-a-new-relay)

You can search for your node by its nickname using https://metrics.torproject.org/rs.html and get insight into the stats for your node.