Tutorial - Tor: Hosting an IPFS Gateway Through a Tor Proxy | Minds

6-8 minutes

There are many websites on what is known as *The Darkweb* which are only accessible through the Tor Network. In this Tutorial I will show you how to set up such a website combined with IPFS so that all of the files on the IPFS network can be available from your Onion domain. The entire script is available here.

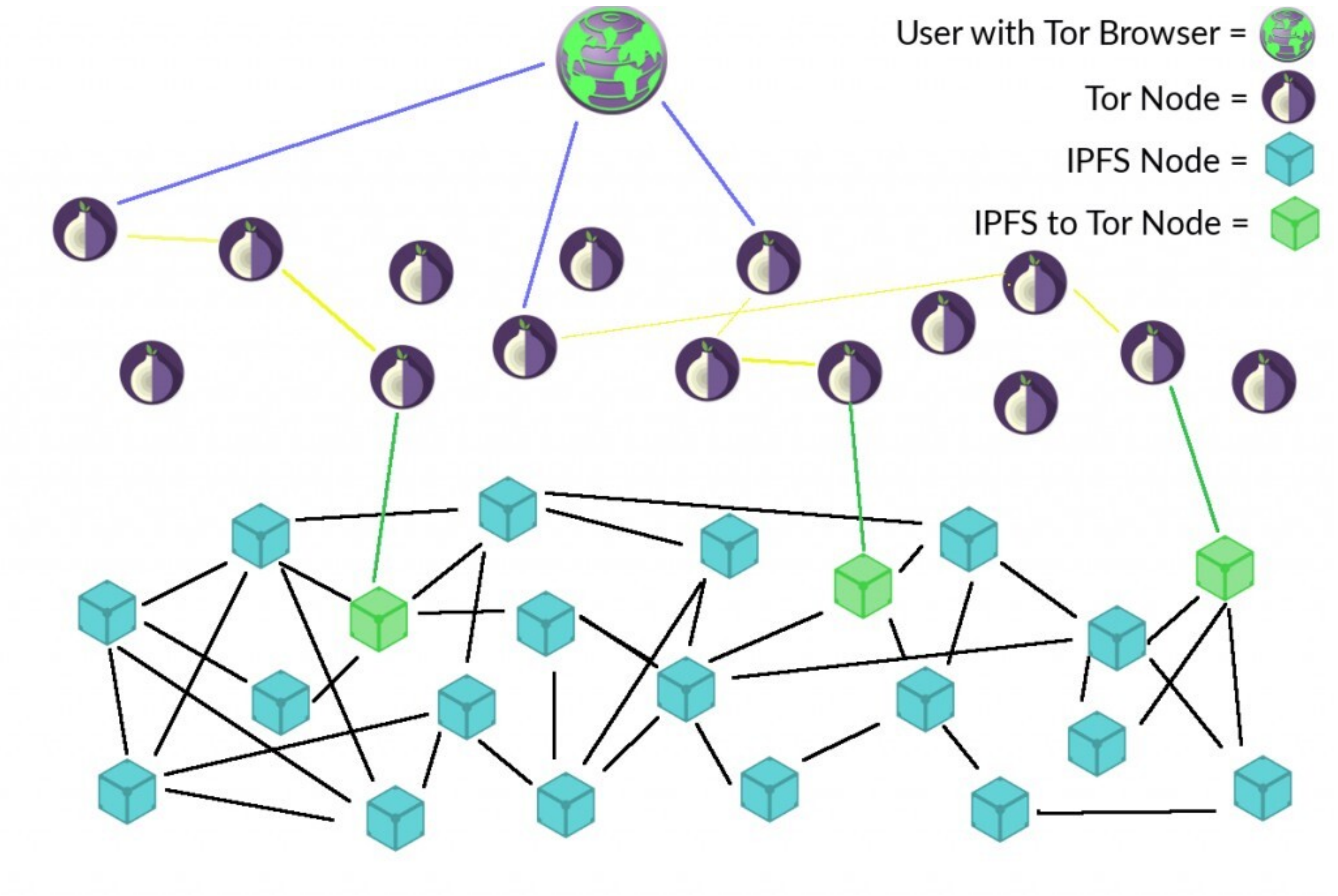
Tor will put up a layer between your web server and the outside world, but Tor itself is not a web server, this means that you will need both Tor and a web server installed. In this tutorial I will use IPFS as a web server. In another tutorial I will use Nginx as a web server. Because we are using IPFS in this tutorial, we wont need to upload any files to be able to use your Onion website, because Tor acts as a gateway to the entire IPFS permanent web.

1. Introduction - Describing the Network Topology

I have tried to give an outline of the topology of the Network which is todays subject. Please do not be scared! I have drawn many nodes, but this is to demonstrate that what we are creating is only one among a much larger network.

Today, we will only create one "Green" IPFS node and it's attached Tor Node. These will exist on the same computer (though this is not a necessity). The domain you are serving will only be accessible through the Tor Network. The World at the top of the image represents an internet surfer using the Tor Network and connecting to your Onion domain. The blue line coming out from this World icon represents the connection that the user makes with the Tor Network. From the Tor Node at the end of this blue line, there are two more connections made with yellow lines. The nodes touching the yellow lines represent the anonymizing layer of the Tor Network. This "anonymizing layer" means that when a user requests a web page through the Tor network, it travels through 3 nodes in the Tor network before it reaches its destination. The destination, in most cases, will be an ordinary web server like Nginx, which will respond to your request by delivering you the resource you requested(for example an HTML page). In our case, our IPFS web server is a portal to a whole new network: The Permanent Web. The Green IPFS node in the picture below represents this gateway.

Today we will set up the Tor Onion router, and a connecting IPFS Node, that is, the object at each end of one of the green lines below.



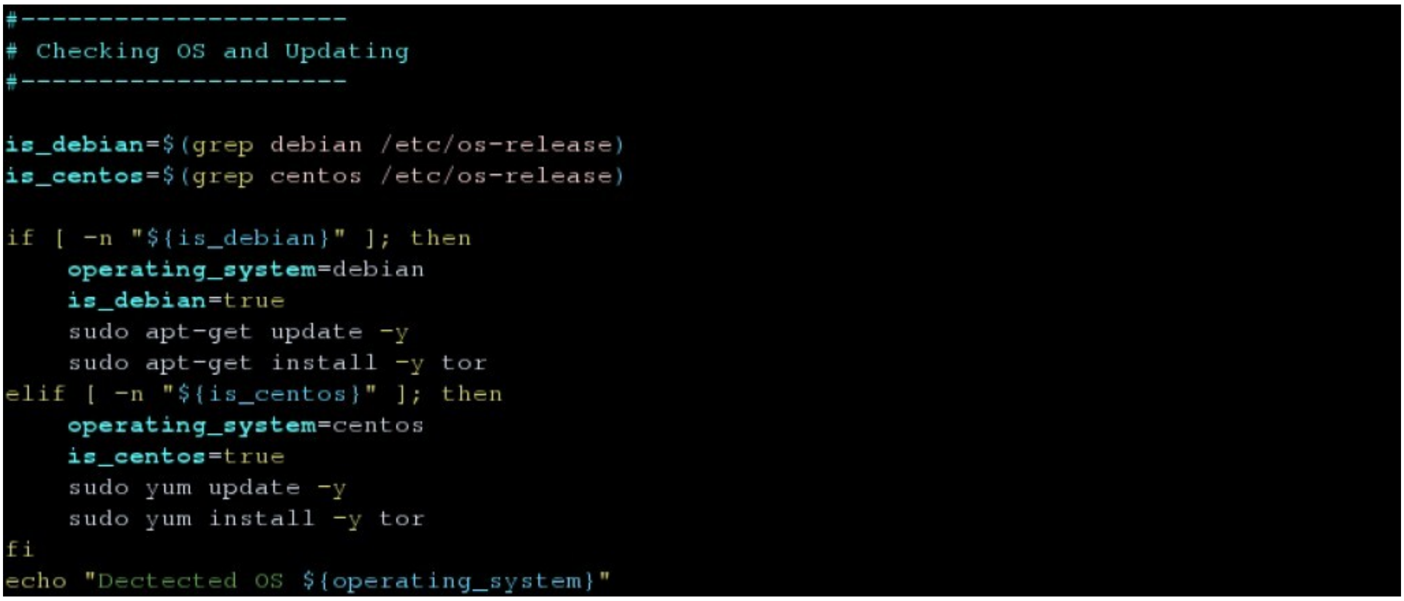
2. Installation

2a. Installing IPFS

I have covered this before, so I will only link to this here. The blog in that link will describe the process of installing IPFS. In short, you can see the whole script of that blog post here.

2b. Installing Tor

This is just a script to check your OS, then update and install Tor accordingly. See it here.



```
#----------------------
# Checking OS and Updating
#----------------------

is_debian=$(grep debian /etc/os-release)
is_centos=$(grep centos /etc/os-release)

if [ -n "${is_debian}" ]; then
    operating_system=debian
    is_debian=true
    sudo apt-get update -y
    sudo apt-get install -y tor
elif [ -n "${is_centos}" ]; then
    operating_system=centos
    is_centos=true
    sudo yum update -y
    sudo yum install -y tor
fi
echo "Dectected OS ${operating_system}"
```

3. Configuration

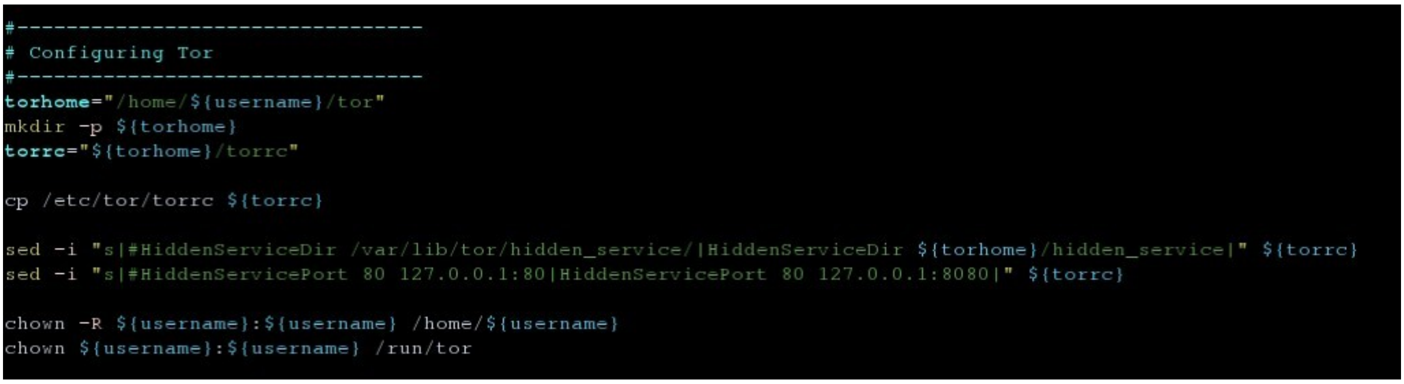
3a. Configuring IPFS

IPFS by default listens on the local IP 127.0.0.1 and the port 8080, this configuration is fine, because we only want IPFS to be accessible locally. Tor essentially is functioning as a reverse proxy to our IPFS Server. We will configure Tor to connect to this local IPFS gateway. The previous blog on installing IPFS shows the IPFS setup.

3b. Configuring Tor

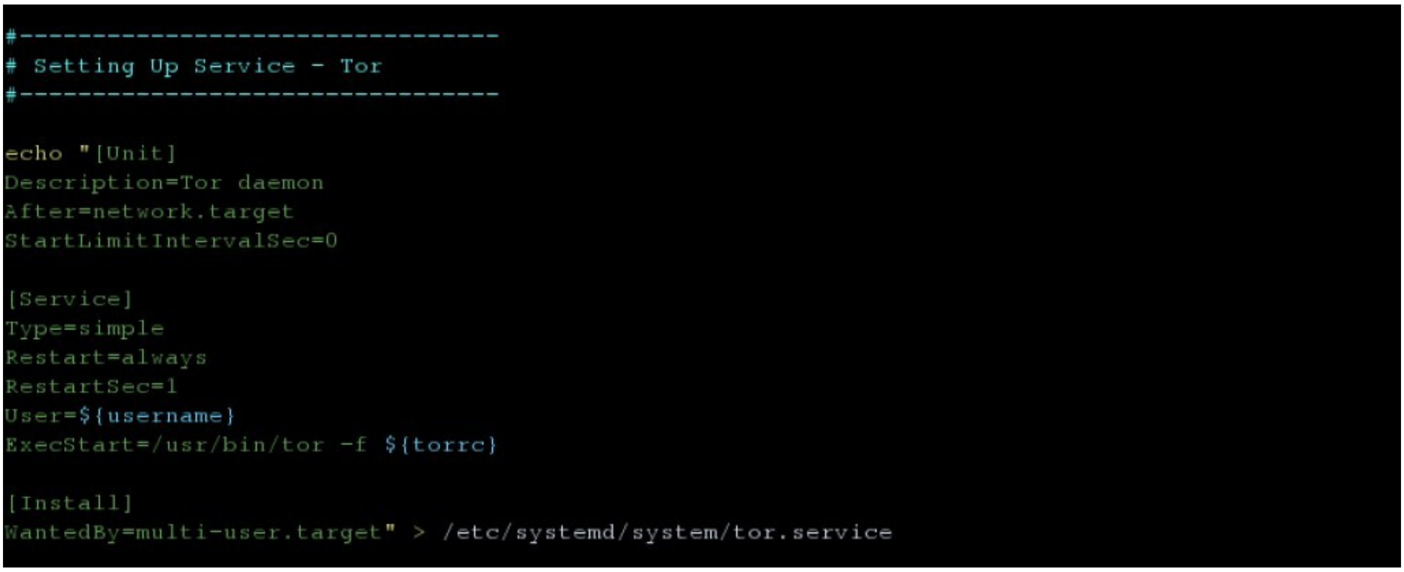
We don't want to run Tor as the root user, instead the variable ${username} represents which user we are using. The first three commands in this section create the necessary directories and names. The *cp* line copies the torrc file(the tor configuration file), from its standard place to a place in the users home directory. The first *sed -i* line changes the configuration file to store important information in the home directory. The second *sed -i* line changes the port to 8080, the port where the IPFS server listens by default.

The two *chown* lines make the files we have created accessible for the user which will run the tor daemon, the script runs the whole setup as root, because it's easier to do it this way, and then change the permissions after the script runs, as does the script below.



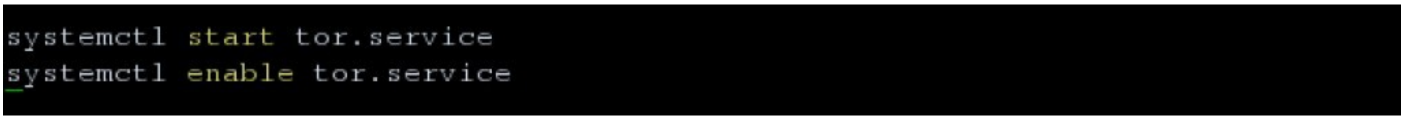
```
#---------------------------------
# Configuring Tor
#---------------------------------
torhome="/home/${username}/tor"
mkdir -p ${torhome}
torrc="${torhome}/torrc"

cp /etc/tor/torrc ${torrc}

sed -i "s|#HiddenServiceDir /var/lib/tor/hidden_service/|HiddenServiceDir ${torhome}/hidden_service|" ${torrc}
sed -i "s|#HiddenServicePort 80 127.0.0.1:80|HiddenServicePort 80 127.0.0.1:8080|" ${torrc}

chown -R ${username}:${username} /home/${username}
chown ${username}:${username} /run/tor
```

This sets up the daemon, which is a service that can be set to automatically run when the computer boots.



```
#---------------------------------
# Setting Up Service - Tor
#---------------------------------

echo "[Unit]
Description=Tor daemon
After=network.target
StartLimitIntervalSec=0

[Service]
Type=simple
Restart=always
RestartSec=1
User=${username}
ExecStart=/usr/bin/tor -f ${torrc}

[Install]
WantedBy=multi-user.target" > /etc/systemd/system/tor.service
```

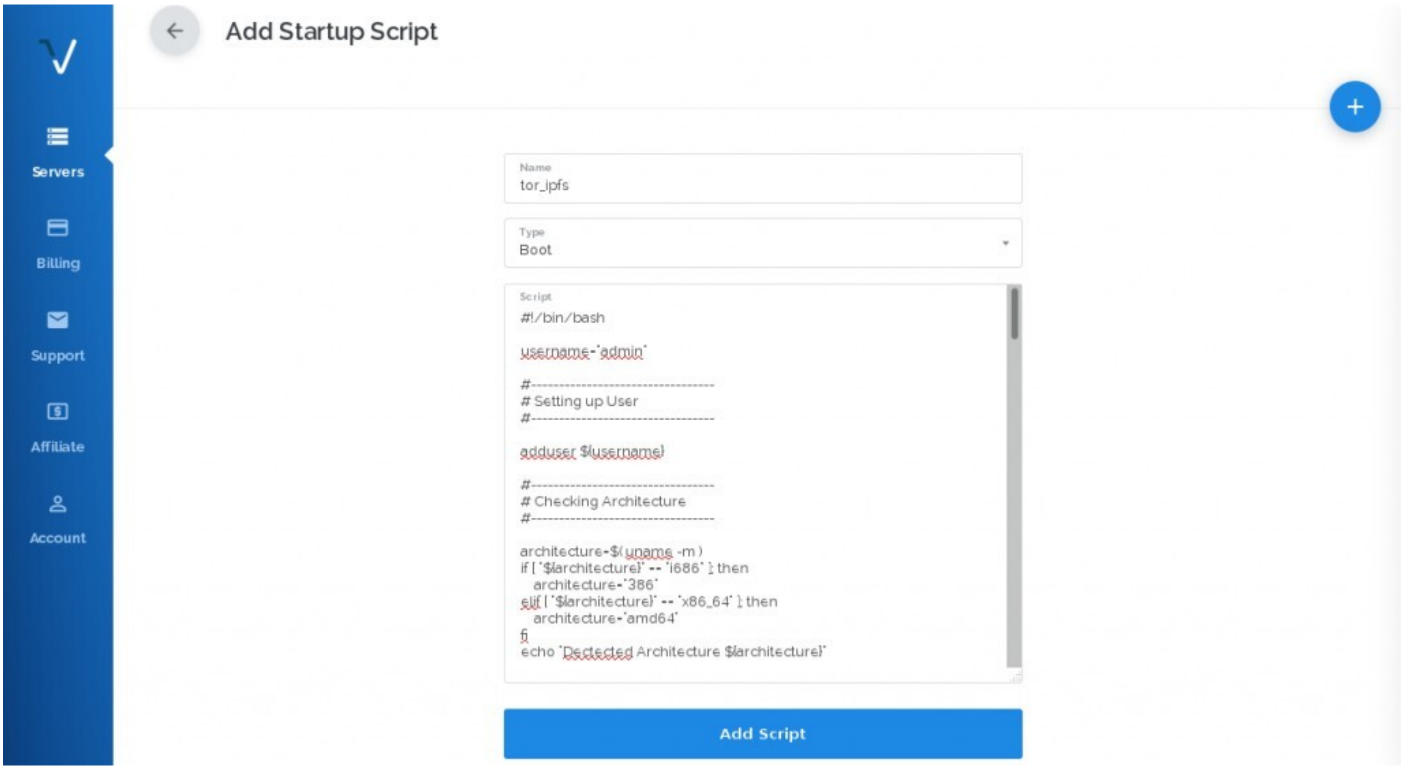
This section starts the daemon above and enables it to start automatically when the computer boots.



```
systemctl start tor.service
systemctl enable tor.service
```

4. Testing

You can test this on a Virtual Private Server(VPS). To use a VPS, see my Tutorial - Tech Sovereign: Setting up a Private Server. Or click here to go straight to Vultr and setup a server yourself. You can do a point and click install of the script I have described in this article by copying the entire script which I link to in the introduction of this article. You can copy and paste this script into the startup script area on your Vultr account, or install on your own PC, but I can't guarantee the script is safe, and it's usually better to separate servers from private data, so I recommend Vultr. If you install this on your home PC, I WILL NOT TAKE RESPONSIBILITY FOR LOSS OF DATA.



Name: tor_ipfs

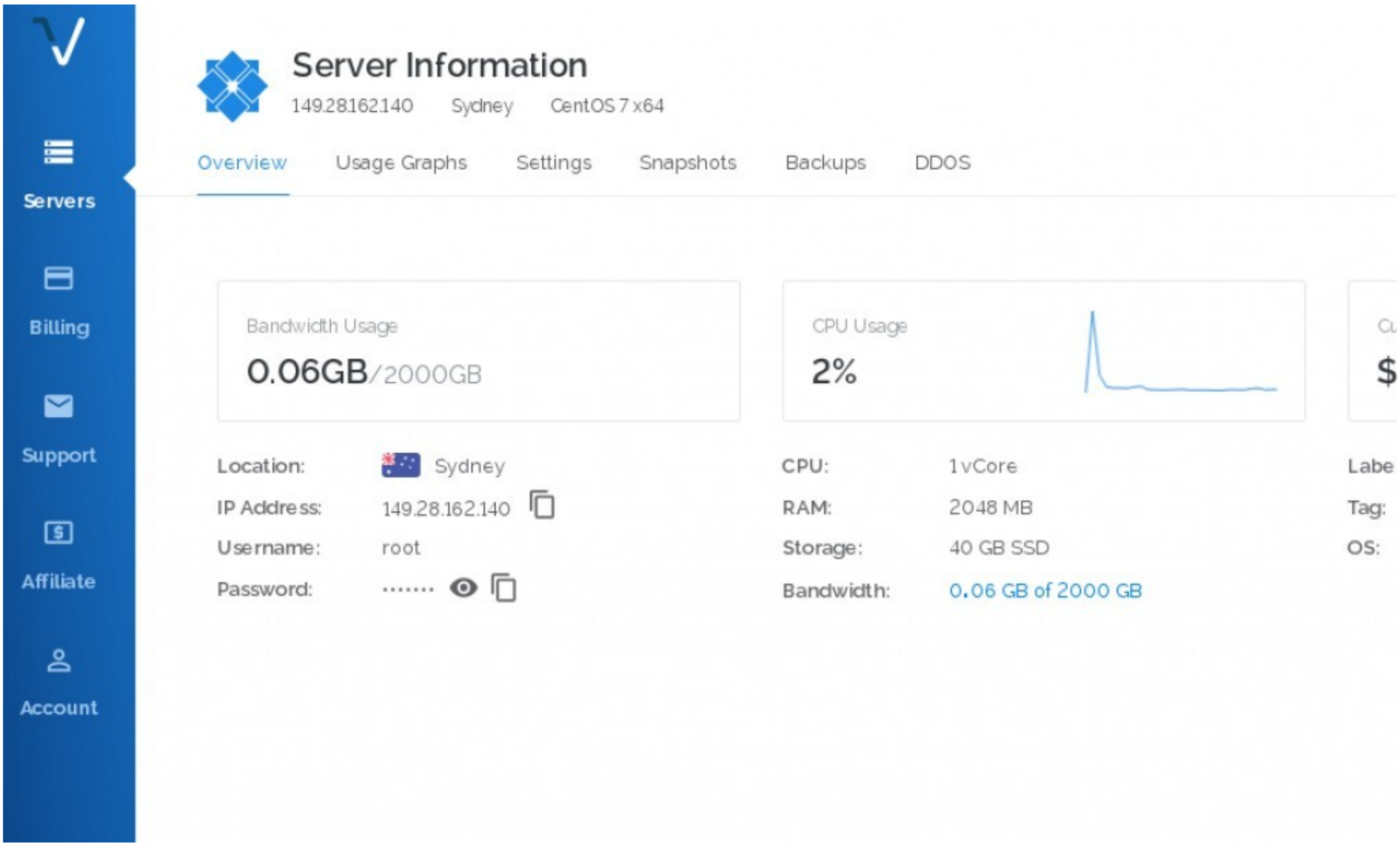
Type: Boot

Script:

```
#!/bin/bash

username="admin"

#--------------------------------
# Setting up User
#--------------------------------

adduser ${username}

#--------------------------------
# Checking Architecture
#--------------------------------

architecture=$( uname -m )
if [ "${architecture}" == "i686" ]; then
   architecture="386"
elif [ "${architecture}" == "x86_64" ]; then
   architecture="amd64"
fi
echo "Dectected Architecture ${architecture}"
```

Once you have added the startup script, deploy your server with that startup script and wait a few minutes before logging in to the server. Unlike in other tutorials, you will need to log in to the server to get the Onion address, as you do not connect to your server through the IP Address displayed on the Vultr account, but through the Onion domain name.

After a few minutes, log into the server using IP address and the password on the Vultr dashboard:



Server Information
149.28.162.140 Sydney CentOS 7 x64

Bandwidth Usage
0.06GB/2000GB

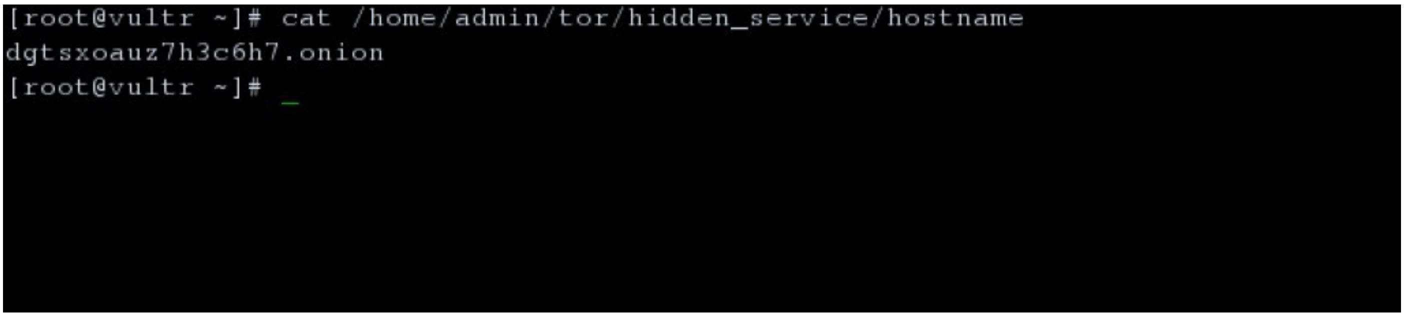
CPU Usage
2%

Location: Sydney
IP Address: 149.28.162.140
Username: root
Password: •••••••

CPU: 1 vCore
RAM: 2048 MB
Storage: 40 GB SSD
Bandwidth: 0.06 GB of 2000 GB

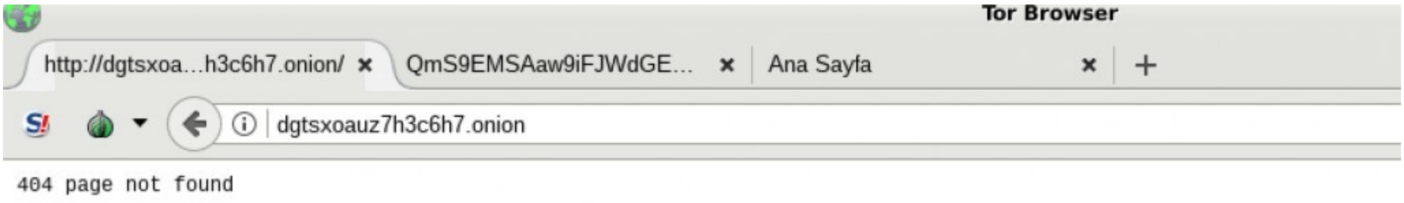
Labe
Tag:
OS:

Once logged in, type the following command to get your Onion address:



```
[root@vultr ~]# cat /home/admin/tor/hidden_service/hostname
dgtsxoauz7h3c6h7.onion
[root@vultr ~]# _
```

You can then test this address in a Tor Browser. If you get this response, you have successfully installed the Tor - IPFS server. It says 404 because the server isn't configured to serve files at the base directory. We have installed an IPFS gateway, which means you will be serving anything on the IPFS network.

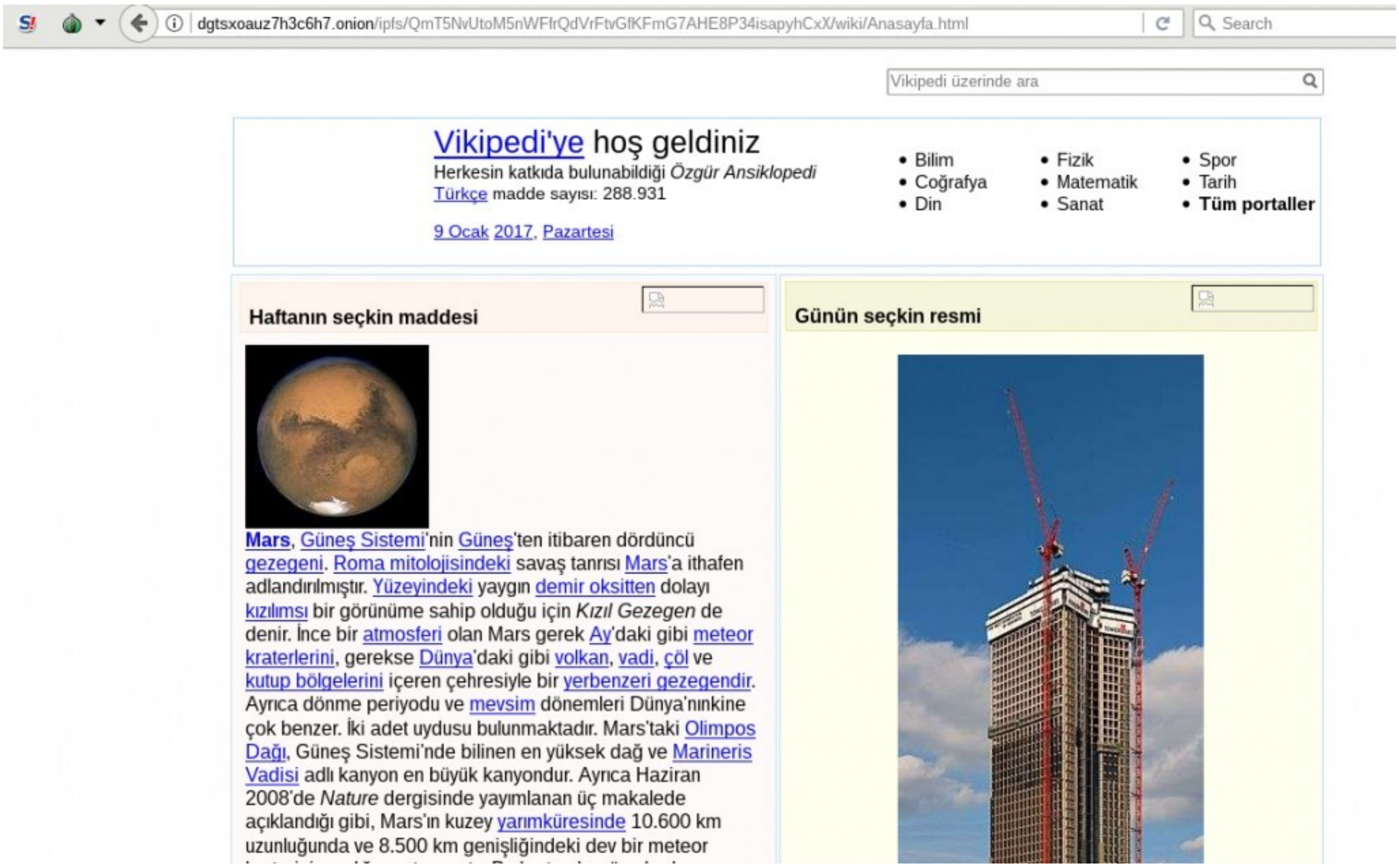


dgtsxoauz7h3c6h7.onion

```
404 page not found
```

Anything that is served on the IPFS network, should be available from your Onion domain *without any uploading*. That means that because IPFS is officially hosting the Turkish Wikipedia, this will be accessible through your domain with the correct hash. You can copy paste the following at the end of your onion domain and you should see the page in the image:

/ipfs/QmT5NvUtoM5nWFfrQdVrFtvGfKFmG7AHE8P34isapyhCxX/wiki/Anasayfa.html



dgtsxoauz7h3c6h7.onion/ipfs/QmT5NvUtoM5nWFfrQdVrFtvGfKFmG7AHE8P34isapyhCxX/wiki/Anasayfa.html

Vikipedi'ye hoş geldiniz

Herkesin katkıda bulunabildiği *Özgür Ansiklopedi*

Türkçe madde sayısı: 288.931

9 Ocak 2017, Pazartesi

- Bilim
- Coğrafya
- Din
- Fizik
- Matematik
- Sanat
- Spor
- Tarih
- **Tüm portaller**

Haftanın seçkin maddesi

Mars, Güneş Sistemi'nin Güneş'ten itibaren dördüncü gezegeni. Roma mitolojisindeki savaş tanrısı Mars'a ithafen adlandırılmıştır. Yüzeyindeki yaygın demir oksitten dolayı kızılımsı bir görünüme sahip olduğu için *Kızıl Gezegen* de denir. İnce bir atmosferi olan Mars gerek Ay'daki gibi meteor kraterlerini, gerekse Dünya'daki gibi volkan, vadi, çöl ve kutup bölgelerini içeren çehresiyle bir yerbenzeri gezegendir. Ayrıca dönme periyodu ve mevsim dönemleri Dünya'nınkine çok benzer. İki adet uydusu bulunmaktadır. Mars'taki Olimpos Dağı, Güneş Sistemi'nde bilinen en yüksek dağ ve Marineris Vadisi adlı kanyon en büyük kanyondur. Ayrıca Haziran 2008'de *Nature* dergisinde yayımlanan üç makalede açıklandığı gibi, Mars'ın kuzey yarımküresinde 10.600 km uzunluğunda ve 8.500 km genişliğindeki dev bir meteor

Günün seçkin resmi