
Creating a
Secure
Cloud Server
with UpCloud

# Installing and securing cloud server using wireguard

The steps to this are the following

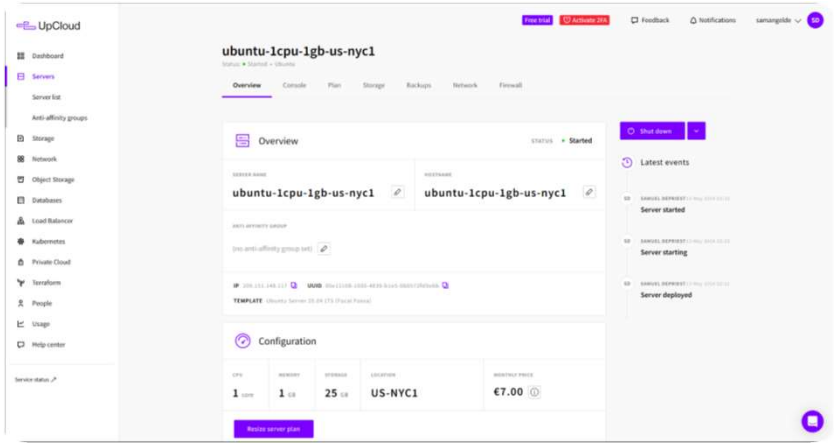
-Deploy- Using upcloud we are going to deploy the server

SSH- We are going to use SSH with PuttY to access the server with a OTP

Wireguard- We are going to install wireguard into the server which is a Ubuntu based Linux distro

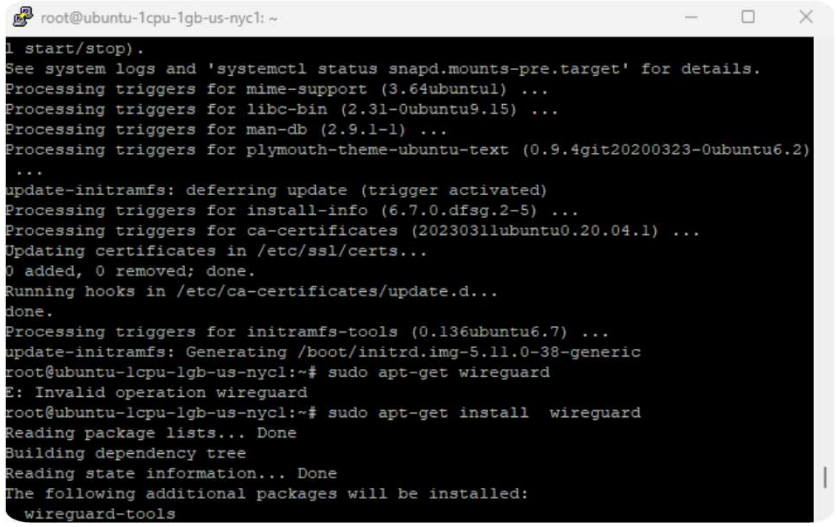
Firewall- We are going to setup the ufw and allow wireguard to access through it using port 51820/udp

# Deploying the server

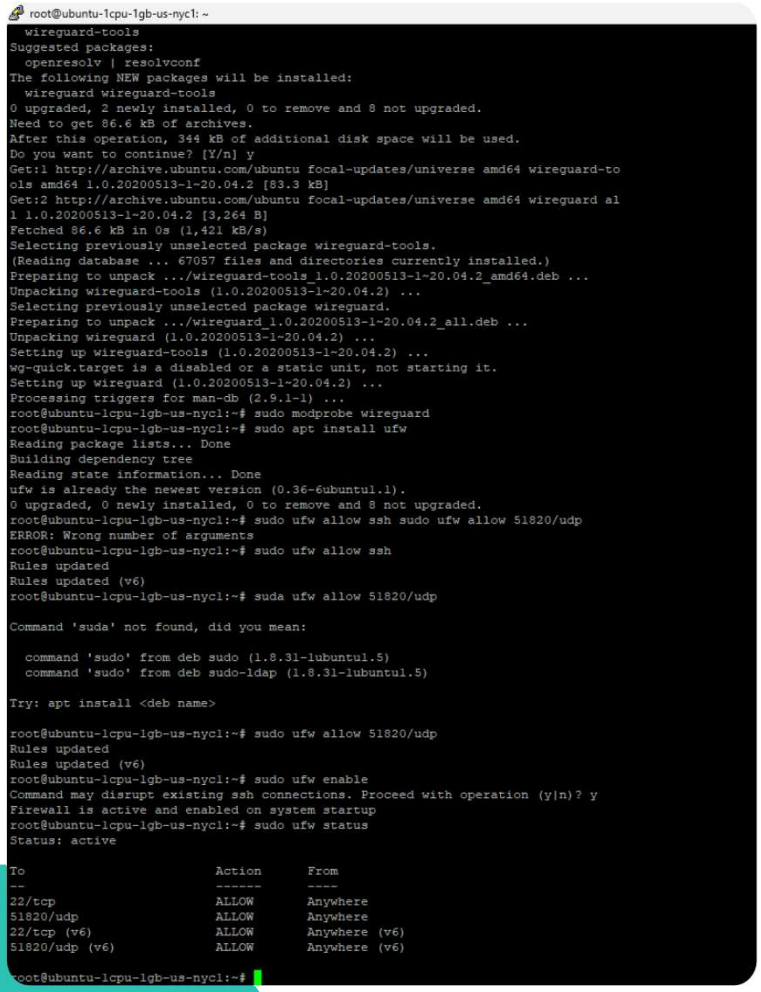



- I was able to use upcloud.com for a cloud service provider to manage and deploy my server. I went with a Ubuntu linux distro for this project. This was simple as choosing the plan, designating the password for SSH, then using putty to access it.

# Installing Wireguard




- After gaining SSH I then ran sudo apt update and after that sudo apt-get update && sudo apt-get upgrade –y. This provided all the tools needed plus updating ones already available.After doing this, I ran sudo apt-get install wireguard so we could encrypt the traffic on the server. This was a easy and smooth installation.




# Installing and setting up ufw

- After installing wireguard we then installed and implemented rules with ufw. Ufw is a unproblematic firewall that is easy to use. We installed it with sudo apt-get install ufw. Once this finished we then setup the allow connection at port 51820/udp which is where wireguard operates through with sudo ufw allow 51820/udp. We then enabled the rule for ssh connection with sudo ufw allow ssh. We then enabled the fire wall with sudo ufw enable, and verified it was running and up with sudo ufw status.