

# Terraform initial lab session

## Outline

This lab session will walk you through the steps to create a basic working Terraform managed cloud infrastructure as code. There will then be a series of tasks that will help you learn things that will be useful for your coursework.

If you are doing this lab session from home, then you will need to install Terraform from this link

<https://learn.hashicorp.com/terraform/getting-started/install.html>

## Start here

### Initial system setup

1. Download/clone this repository into a new directory  
`https://github.com/domroutley/openstack-terraform-example`
2. Generate a token to access OpenStack and export it to your environment (for detailed instructions on how to do this open the `TOKENGENERATIONHELP.md` file from the repository you have just downloaded)
3. Run `terraform init` in the repository directory

### Running the module for the first time

1. Assuming everything went ok with the setup, create an `ssh` key and copy the Public key into the `vars.tf` file as the default value of the variable `access_key`
2. You should now be all set. Run `terraform plan` to see the changes to be made to the cloud. `terraform plan` will also validate that your module is formed correctly and has no syntax errors.
3. If you are satisfied with what you see, run `terraform apply` and type and approve the changes.
4. You should be able to see the IP address of the instance as the output printed at the end of Terraforms run.
  - To bring this up again you can run `terraform output`
5. You can now SSH into the server with the following command  
`ssh -i LOCATION/OF/SSH/KEY ubuntu@INSTANCE_IP`

- It may take a couple of minutes for the server to be able to accept SSH requests so be patient
- If you are not on the university network, you will need to connect via the VPN before you can SSH into the instance.
  - Using OpenVPN to connect to Cardiff Uni VPN Windows  
<https://docs.cs.cf.ac.uk/notes/openvpn-windows>
  - Using OpenVPN to connect to Cardiff Uni VPN MacOS  
<https://docs.cs.cf.ac.uk/notes/openvpn-macos/>
  - For Linux, get the ovpn file from one of the above links, then add a new connection in your network manager from the ovpn template file.

## Further tasks

These further tasks will help prepare you for your coursework.

Don't forget to **terraform plan** after each task to test your syntax and structure, and then **terraform apply** to apply those changes to the cloud.

1. Add some more outputs to the module that output the DNS IP addresses
2. Add a new security group rule in the **networking.secgrouptf** that allows HTTP access from all IP addresses, attach this rule to the already created security group and change the security group name to be more appropriate
3. Create a new server for FTP
  - Create the new compute resource resource
  - Create a new security group and security group rule that allow incoming connections via FTP (port 21)
  - Add the server to the already created subnet
  - Attach the SSH and HTTP security group to the new server
  - Attach the already created key pair to the new server
  - Create a new floating IP resource and attach it to the new server
  - Add outputs for the new IP, and outputs detailing what servers have what security groups attached

After you are done, run **terraform destroy** to remove your infrastructure stack from the cloud.