**Assignment summary**

Steps:

1. Installing terraform on windows desktop
2. Creating an aws account.
3. Create tf-user and tf-group
4. Create access key.
5. Use access key ID and secret key in terraform provider configuration.
6. Using terraform module - Create vpc (nginx-vpc) and 2 subnets in each Availability zone, one public and one private and more.
7. Dockerized nginx app with edited index.html text was inserted into the index.html file.
8. Pushed the container image to my public dockerhub repository 'sagitur100/nginx'
9. Install docker and run the nginx image as container as a bootstrap script of the EC2 instance (inside user\_data).
10. The EC2 instance is on private subnet.
11. The module created NAT Gateway and that’s what enable access from outside into the private subnet.
12. Create ALB for forwarding traffic in port 80.
13. Save public DNS name of ALB as terraform output, responding "yo this is nginx".

* The container image saved in sagitur100/nginx dockerhub public repository
* Least privileges policy using iamlive open-source tool.
* Least open ports policy.
* Document everything inside the code and in outside documentation (this).
* Generate tf\_private\_key on local. That’s using to connect to EC2 instances and its part of a public-private key pair.
* 28 resources created.

|  |  |
| --- | --- |
| **Resource type** | **Resource name** |
| aws\_instance | nginx-docker-host |
| aws\_key\_pair | tf\_key\_pair |
| aws\_lb | nginx-docker-host-lb |
| aws\_lb\_listener | lb\_listener |
| aws\_lb\_target\_group | lb\_target\_group |
| aws\_lb\_target\_group\_attachment | tgr\_attachment |
| aws\_security\_group | nginx\_sg |
| local\_file | tf\_private\_key |
| tls\_private\_key | rsa |
| aws\_default\_network\_acl | this |
| aws\_default\_route\_table | default |
| aws\_default\_security\_group | this |
| aws\_eip | nat |
| aws\_internet\_gateway | this |
| aws\_nat\_gateway | this |
| aws\_route | private\_nat\_gateway |
| aws\_route | public\_internet\_gateway |
| aws\_route\_table | private |
| aws\_route\_table | public |
| aws\_route\_table\_association | private |
| aws\_route\_table\_association | private |
| aws\_route\_table\_association | public |
| aws\_route\_table\_association | public |
| aws\_subnet | private |
| aws\_vpc | this |

|  |  |  |
| --- | --- | --- |
| **variable** | **Default values** | **Type** |
| Region | Us-west-2 | string |
| azs | us-west-2a, us-west-2b | List(string) |
| public\_subnet\_cidrs | 10.0.1.0/24, 10.0.2.0/24 | list(string) |
| private\_subnet\_cidrs | 10.0.3.0/24, 10.0.4.0/24 | list(string) |
| Access\_key\_id | <MY\_ACCESS\_KEY> | String |
| Secret\_key | <MY\_SECRET\_KEY> | string |
| Security\_group\_name | Nginx\_sg | String |

|  |  |
| --- | --- |
| Output | value |
| lb\_public\_dns\_name | Dynamic |