CREATING CUSTOM VPC, EC2 INSTANCE AND WORKING ON SG & NACL

1. Login into AWS account

2. Choose VPC service

3. Choose the region Mumbai

4. Delete the existing VPC and setup custom VPC and its components
- delete default vpc, see that the subnets, ip gateways and route tables are also deleted
- create new VPC - give a name
    - Ipv4 CIDR = 192.168.0.0/16
- go to subnets - create subnet
    - select new vpc and give the subnet a name
    - choose availability zone as Asia Pacific (Mumbai)
    - Ipv4 subnet CIDR block = 192.168.1.0/24
- go to internet gateways – create new internet gateway
    - give a new name and create it
    - go back to internet gateways
    - actions -> attach to VPC -> select created VPC -> attach internet gateway
- go to route table – click on route table ID
    - click on edit routes
    - add route –> 0.0.0.0/0 -> Below target select internet gateway -> select the created internet gateway -> save changes

5. Get 2 elastic public IP

6. Create two EC2 instances and attach the public IP address
    - search EC2 -> open in new tab
    - go to instances -> launch instance -> number of instance =2 -> give a name (VMs) -> select Ubuntu -> key pair login (proceed without key pair) -> Launch instance
    - go to EC2 -> instances (running) -> change the VMs names to Web Server and Web Client
    - go to elastic Ips -> click on web server IP -> Associate elastic IP address -> choose instance -> associate
    - similarly associate web client also

7. Name VM1 as Web server and VM2 as Web client (already done)

8. Connect to the instance via EC2 instance connect
    - go to instances -> select web server -> connect -> no changes -> connect
    - a browser console will open -> sudo apt update
      -> sudo apt install apache2
      -> service apache2 status
    - go to instances -> select web client -> connect -> no changes -> connect
    - a browser console will open -> sudo apt update
      -> sudo apt install links

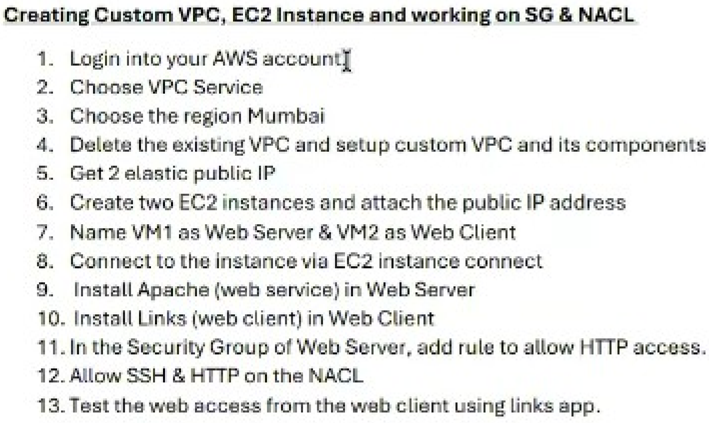
9. Install Apache (web service) in web server (explained in step 8)

10. Install Links (web client) in web client (explained in step 8)

11. In the security group of web server, add rule to allow HTTP access
- go to instances
- click on web server instance ID -> security -> security groups -> edit inbound rules
- inside edit inbound rules -> select type http
  -> select source anywhere Ipv4
  -> save rules

(STEP 12: REMOVED SINCE ITS NOT WORKING,
let this be there Rule no=100, type=all traffic)
12. Allow SSH & HTTP on the NACL
- go to VPC
- go to network ACLs -> click on network ACL ID -> edit inbound rules
- inside edit inbound rules -> remove existing one -> add new
  -> Rule no =100, type =SSH(22)
  -> Rule no =101, type =HTTP(80)
  -> save changes

13. Test the web access from the web client using links app
- go to web client browser console -> links <web server ip>
  (web server public ip is available below web server console)



Creating Custom VPC, EC2 Instance and working on SG & NACL

1. Login into your AWS account
2. Choose VPC Service
3. Choose the region Mumbai
4. Delete the existing VPC and setup custom VPC and its components
5. Get 2 elastic public IP
6. Create two EC2 instances and attach the public IP address
7. Name VM1 as Web Server & VM2 as Web Client
8. Connect to the instance via EC2 instance connect
9. Install Apache (web service) in Web Server
10. Install Links (web client) in Web Client
11. In the Security Group of Web Server, add rule to allow HTTP access.
12. Allow SSH & HTTP on the NACL
13. Test the web access from the web client using links app.

TESTING ROUTE 53 SERVICE

13. Create a hosted zone in AWS Route 53 service with your 11 digit registration number for ngaws.xyz (ex: 21011101072.ngaws.xyz)

```
        - go to Route 53 dashboard -> create hosted zone -> domain name=21011101072.ngaws.xyz
                                                            -> create hosted zone
```

14. Login to GoDaddy domain:
URL: https://www.godaddy.com
username: aws-ng
pwd: Welcome1!

- go to Domain -> manage DNS

15. Get the name server (any one) information from the route 53 dashboard and update the NS record in GoDaddy portal for your subdomain

```
        - go to Route 53
        - from Value/Route traffic to -> copy one name server
        - go to GoDaddy website -> manage DNS -> add new record
        - inside add new record -> Type=NS
                                -> Name=21011101072
                                -> Value=copied name server from AWS
                                -> Save
```

16. Back to AWS Route 53 service, create a record in your hosted zone with the following details
Subdomain: www
IP: IP addresss of the web server (get it from running instances)
Routing policy: Simple routing

- go to hosted zones -> create record -> fill the above details -> create records

17. Check the website reachability with the URL
URL: www.21011101072.ngaws.xyz

```
- go to web client console -> links www.21011101072.ngaws.xyz
                           -> nslookup www.21011101072.ngaws.xyz
```

IAM

1. Search and click on IAM -> go to users -> create user
-> inside create user -> give name
-> check provide console access
-> check I want to create an IAM user
-> check autogenerated password
-> check user must create new password
-> next
-> check add user to group
-> next
-> create user
- the you will get console sign in url, username and autogenerated pwd (note all these)

2. open new tab and login into IAM user with the above details -> all permissions are denied

3. Giving permissions from root user console
- go to users -> click on alice -> add permissions -> attach policies directly
-> search ec2
-> select AmazonEC2FullAccess
-> add permissions

4. Creating groups
- go to groups -> create group
-> give name
-> add IAM user
-> attach polices
-> create group

5. Create user with full access instead of providing root user credentials
-go to users or groups ->attach policies
-> AdministrativeAccess

6. Creating account alias (just giving a name instead of the account ID)
- go to IAM dashboard -> account alias (right side box)
-> create
-> give a name (should be globally unique, the signin URL will change)
-> create alias

7. An IAM user, though provided with Administrative access will not be able to see billing information. To give an IAM user access to billing information -> google and explore