# 

# 

# **Assessment**

# **VPC**

Trainee Name : Aditya Upadhyay

Newers ID : 3978

Mentor Name : Tarun Saxena

College : UPES

**Q1. When to use Elastic IP over Public IP**

Public ip changes each time we stop an instance so we can’t use it as endpoint or use it in configuration files. We also need elastic ip for NAT.

**Q2. Valid IP Ranges for LAN, Implication of using Public IP ranges for Private Network.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RFC1918 name** | **IP address range** | **Number of addresses** | **Largest** [**CIDR**](https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing) **block (subnet mask)** | **Host ID size** | **Mask bits** | [***Classful***](https://en.wikipedia.org/wiki/Classful_network) **description** |
| 24-bit block | 10.0.0.0 – 10.255.255.255 | 16777216 | 10.0.0.0/8 (255.0.0.0) | 24 bits | 8 bits | single class A network |
| 20-bit block | 172.16.0.0 – 172.31.255.255 | 1048576 | 172.16.0.0/12 (255.240.0.0) | 20 bits | 12 bits | 16 contiguous class B networks |
| 16-bit block | 192.168.0.0 – 192.168.255.255 | 65536 | 192.168.0.0/16 (255.255.0.0) | 16 bits | 16 bits | 256 contiguous class C networks |

A public IP is assigned to a range or block of addresses. The Internet Assigned Numbers Authority (IANA) controls ownership of these IP ranges and assigns each block to organizations such as Internet Service Providers (ISPs) who in turn allocate individual IP addresses to customers.

ISPs shouldn't let **private**-**IP ranges** out onto the **public** Internet. This convention is why people usually **use** them when indicated. If the two computers are only connected to each other, then you have no need - or ability - to **use public IP** addresses. A **public IP** is assigned to a **range** or block of **addresses**.

**Q3. List down the things to keep in mind while VPC peering.**

* VPC Peering is allowed for the connection of two VPC’s such that the instances in the VPC can communicate with each other. The VPC’s can be part of multiple accounts, ut must be in the same region.
* When you enable VPC peering between two VPCs, those VPCs must exist within the same region
* VPC peering is that the instances within a VPC communicate with instances in a peered VPC using either the IPv4 or the IPv6 protocol.
* VPCs that have been peered together cannot contain duplicate IP addresses or overlapping IP address scopes.
* AWS only allows you to create a single peering relationship between two VPCs. Of course this limitation is common sense, because there is no real advantage to creating multiple peer links between the same set of VPCs.
* No support for transitive peering.

**Q4. CIDR of a VPC is** [**10.0.0.0/16**](http://10.0.0.0/16)**, if the subnet mask is /20 calculate the number of subnets that could be created from the VPC. Also find the number of IP in subnet.**

CIDR of VPC is 10.0.0.0/16, Total number of IP’s in VPC = ​ 2^16

If one subnet is of /20 cidr then total Subnet= 2^16/2^12 = ​ 16 Subnet

Total number of IP in one sunet = ​ 2^12-5 = 4091

**Q5. Differentiate between NACL and Security Groups.**

|  |  |
| --- | --- |
| **Security Group** | **Network ACL** |
| **Supports Allow rules only {** by default all rules are denied **}**  You **cannot deny** a certain IP address from establishing a connection | **Supports Allow and Deny rules** |
| **Stateful:** This means any changes applied to an incoming rule will be automatically applied to the outgoing rule.  Example: If you allow an incoming port 80, the outgoing port 80 will be automatically opened. | **Stateless**: This means any changes applied to an incoming rule will not be applied to the outgoing rule.  Example: If you allow an incoming port 80, you would also need to apply the rule for outgoing traffic. |
| **Security groups are tied to an instance**. | **Network ACL are tied to the subnet.** |
| **All rules in a security group are applied.** | **Rules are applied** **in their order (the rule with the lower number gets processed first)** |
| **First Layer of Defence** | **Second Layer of the defence** |
| **Is the Firewall of EC2 Instances** | **Is the Firewall of the Subnet** |
| Security groups are used for many cases, for example restricting inbound traffic of an EC2 instance to be from Load balancer only. | The same thing applies for Network ACL  Used in running a production server |

**Q6. Implement a 2-tier vpc with following requirements:**

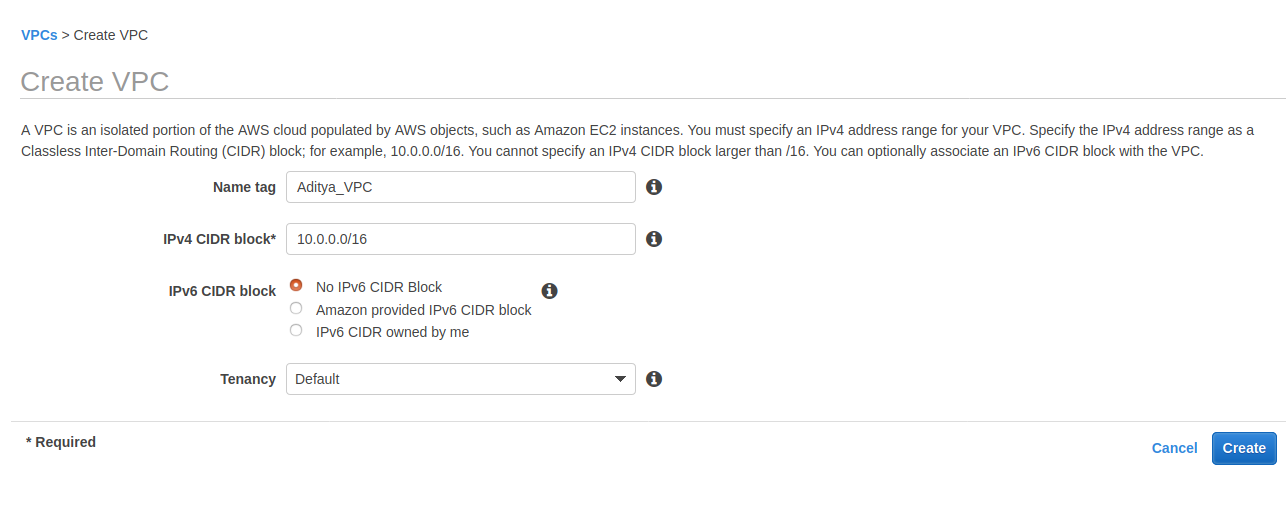
**1. Create a private subnet, attach NAT, and host an application server(Tomcat)**

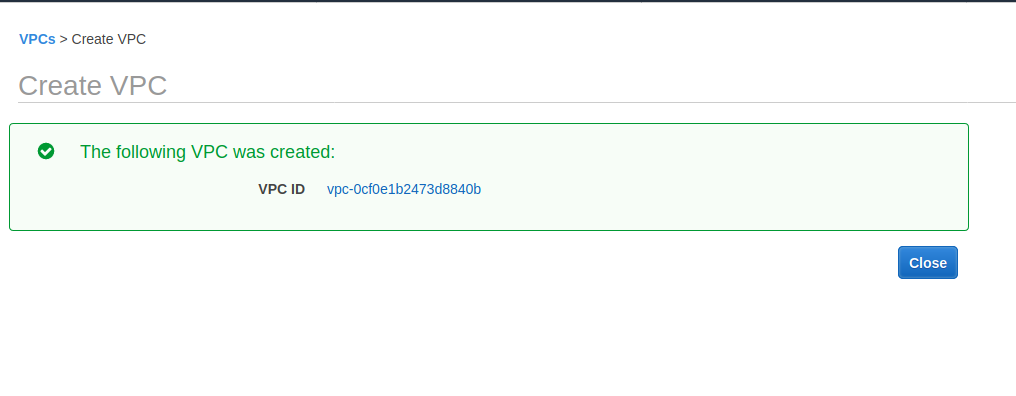
**2. Create a public subnet, and host a web server(Nginx), also proxypass to Tomcat from Nginx**

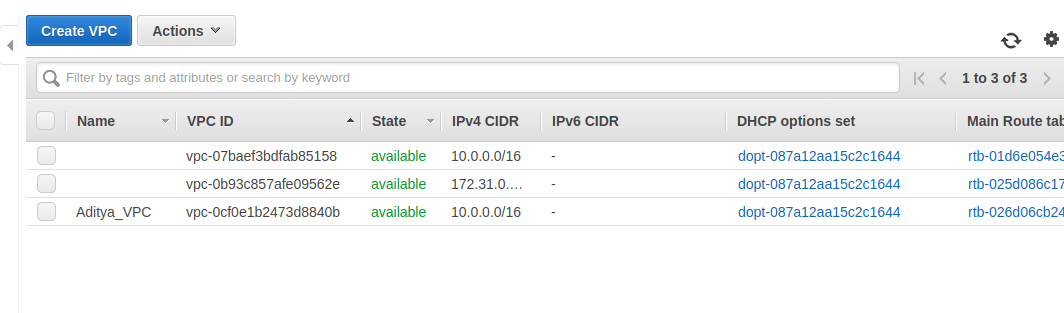
**After Implementing this on AWS, create an architecture diagram for this use case.**

**Note: For hosting Nginx in public subnet, use Elastic IP.**

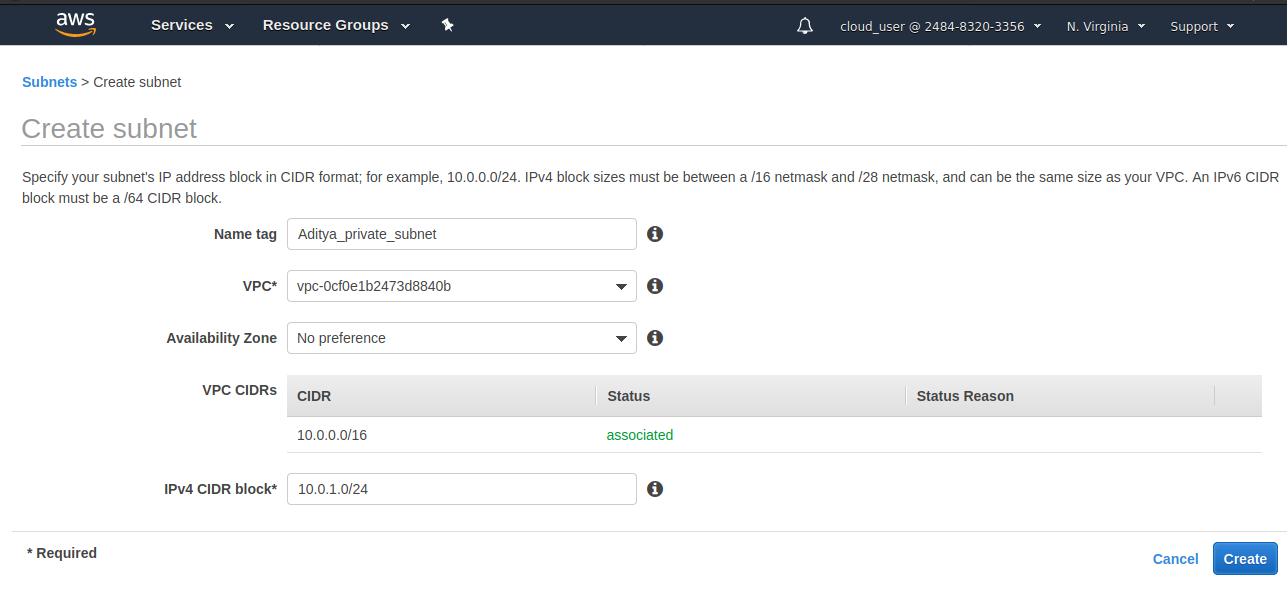
Create VPC

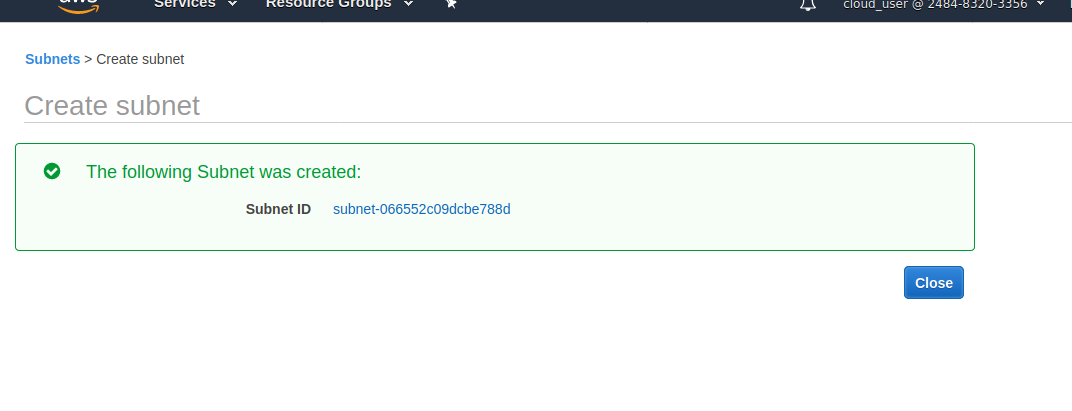




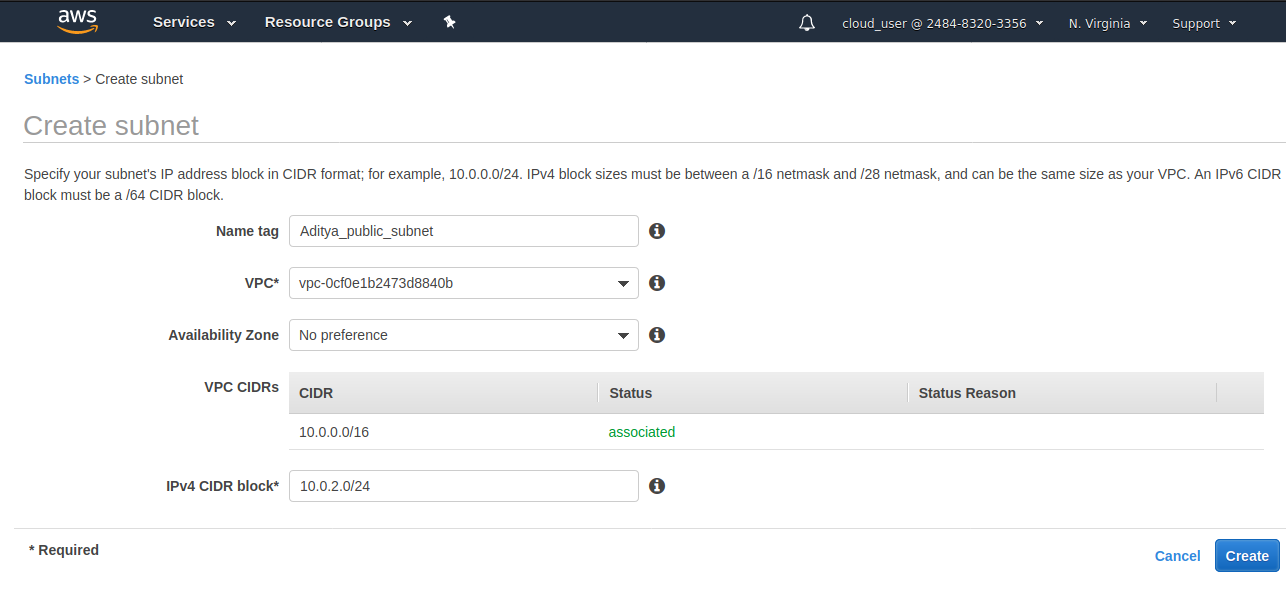


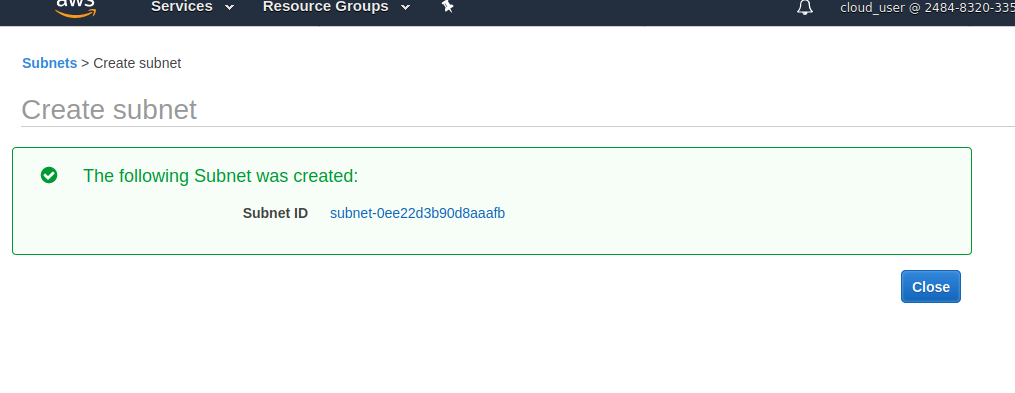
Create private subnet



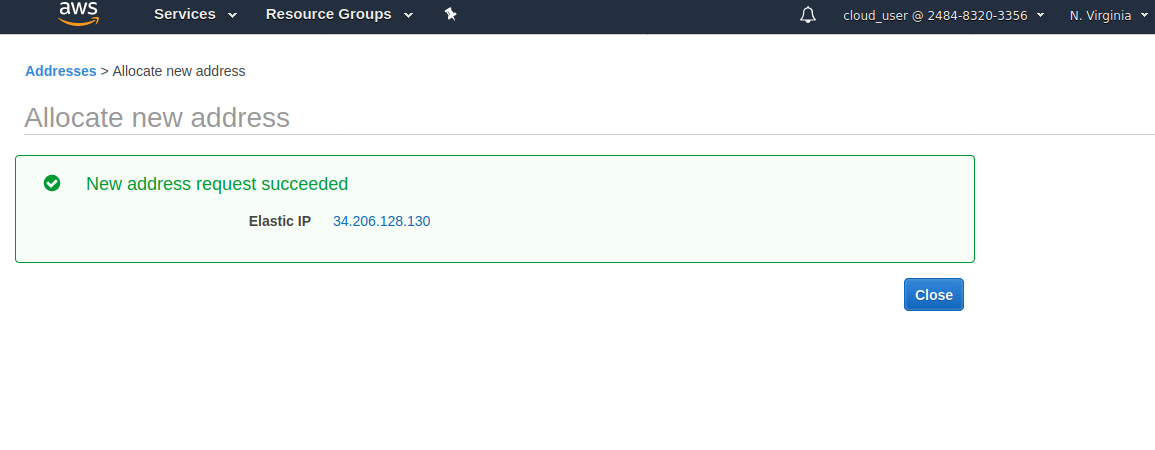


Create public subnet

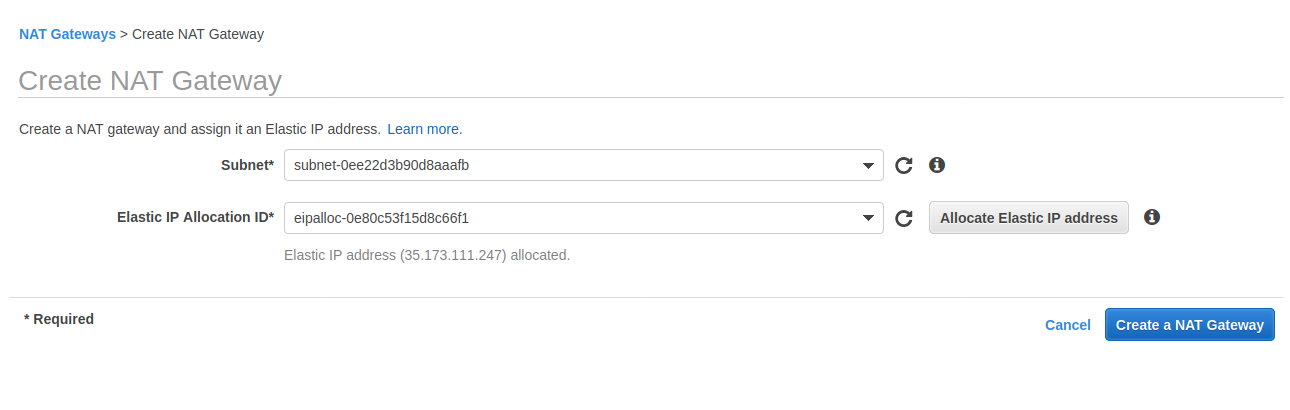


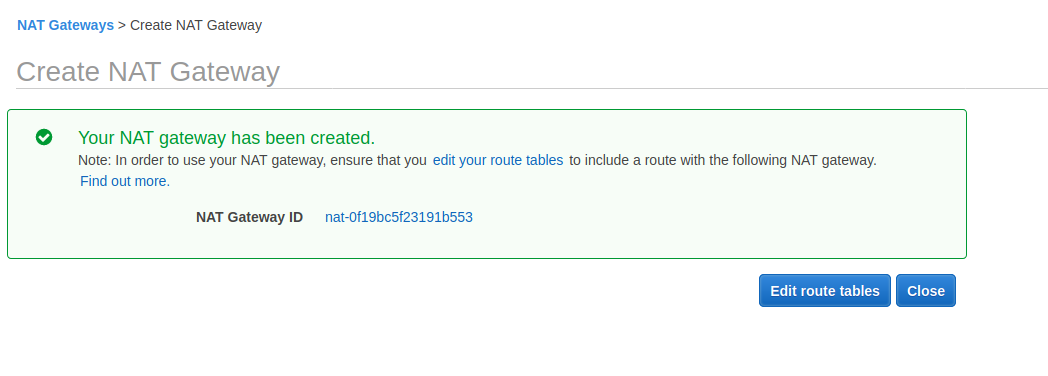


Allocate EIP for NAT

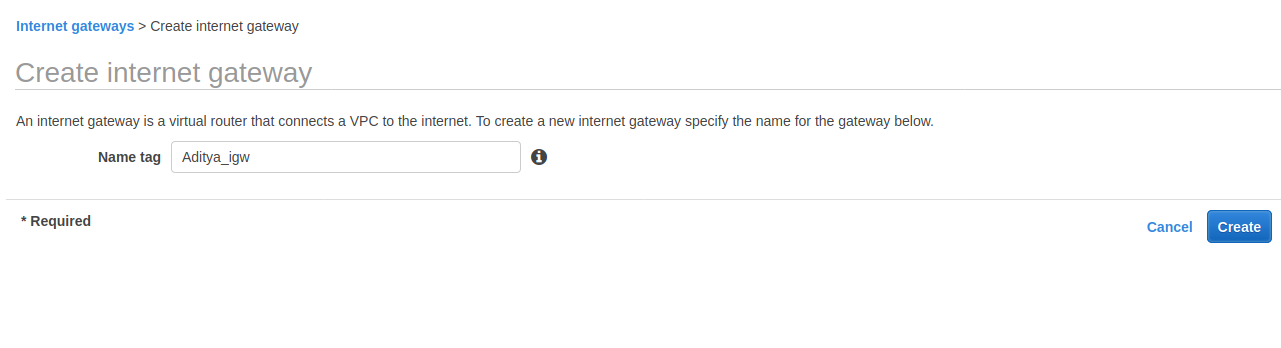


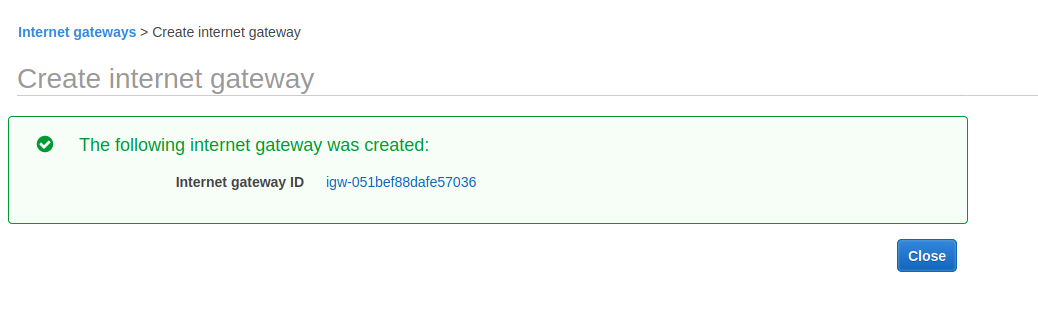
Create NAT



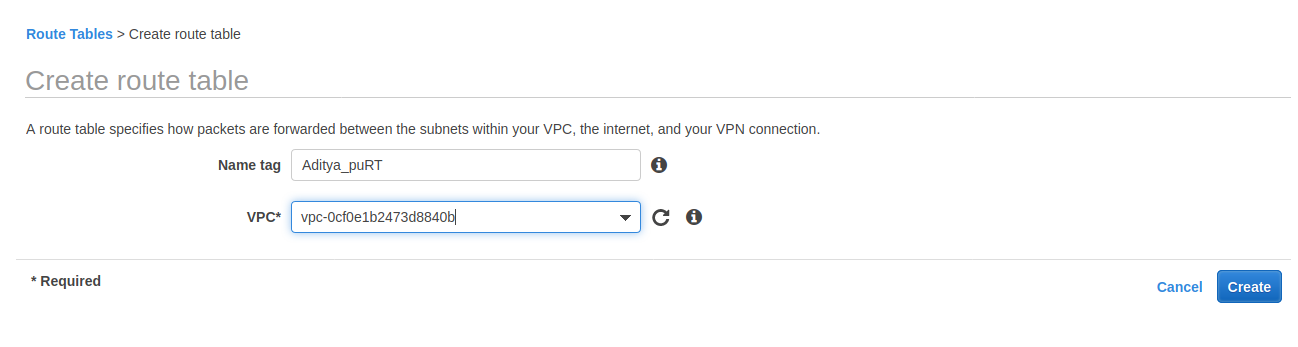


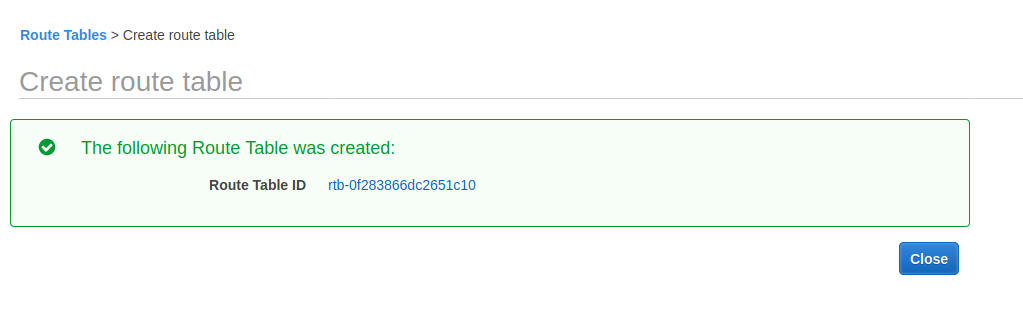
Create internet gateway



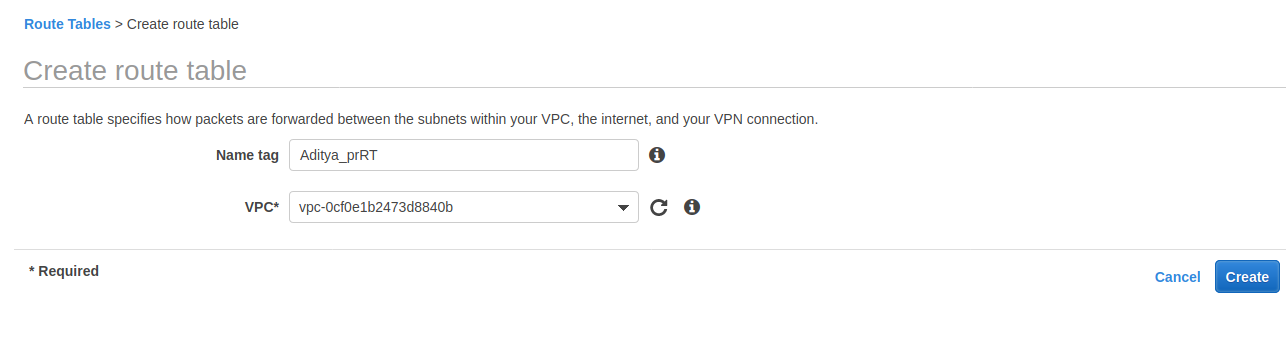


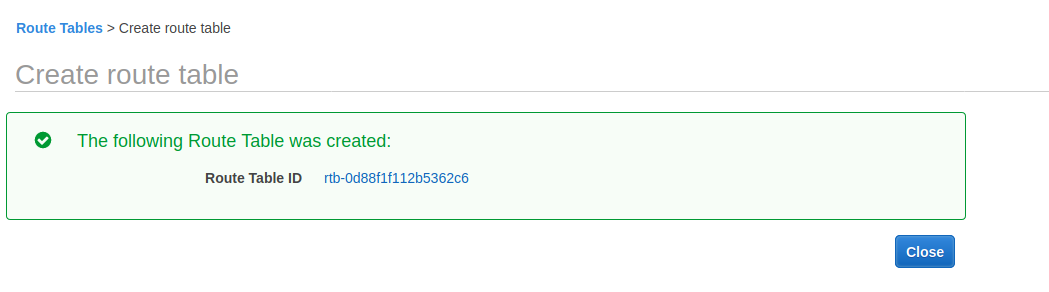
Create Route table for public subnet



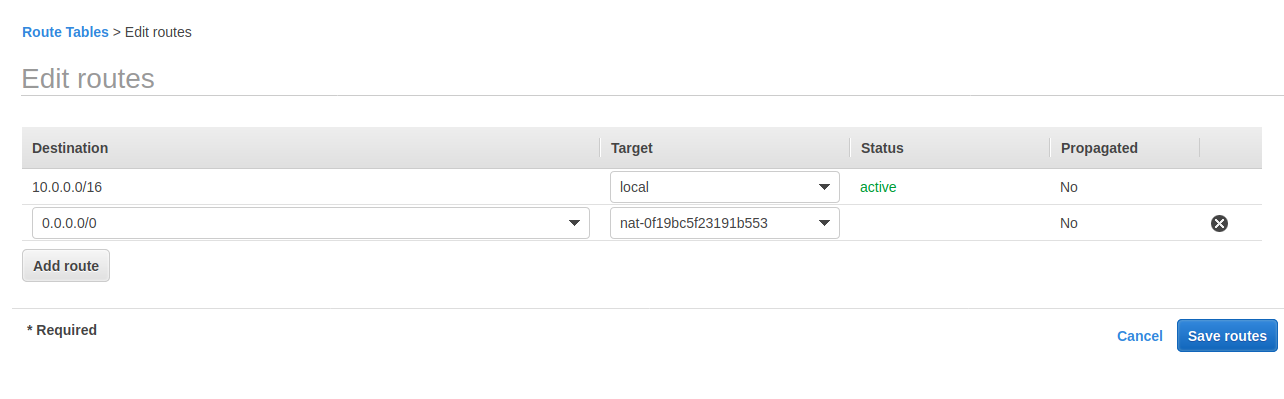


Create route table for private subnet

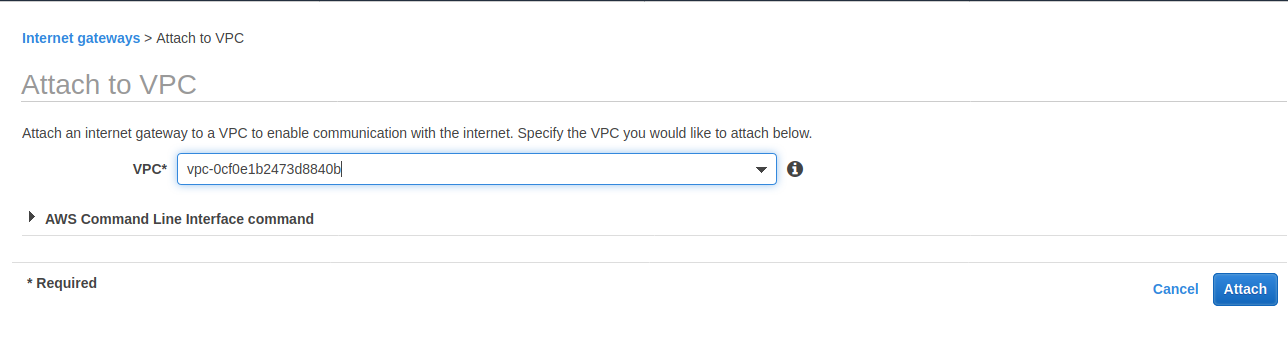




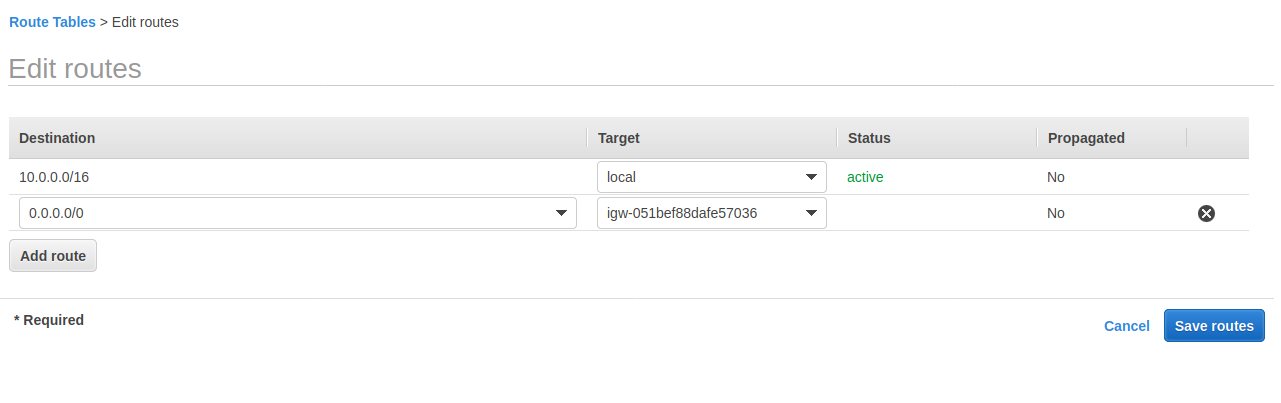
Edit routes for private subnet



Attach igw to VPC



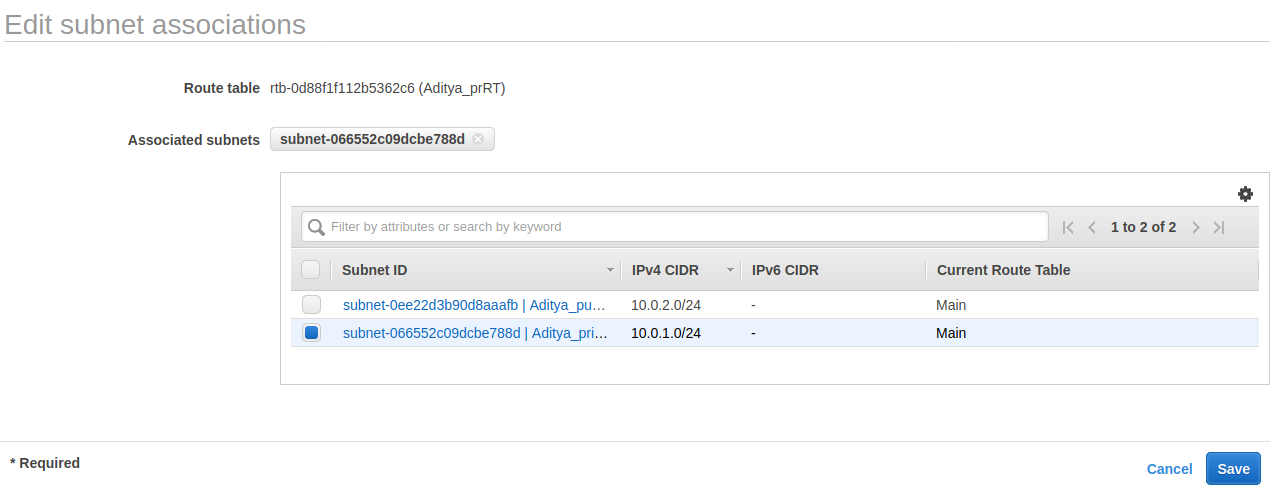
Edit routes for public subnet

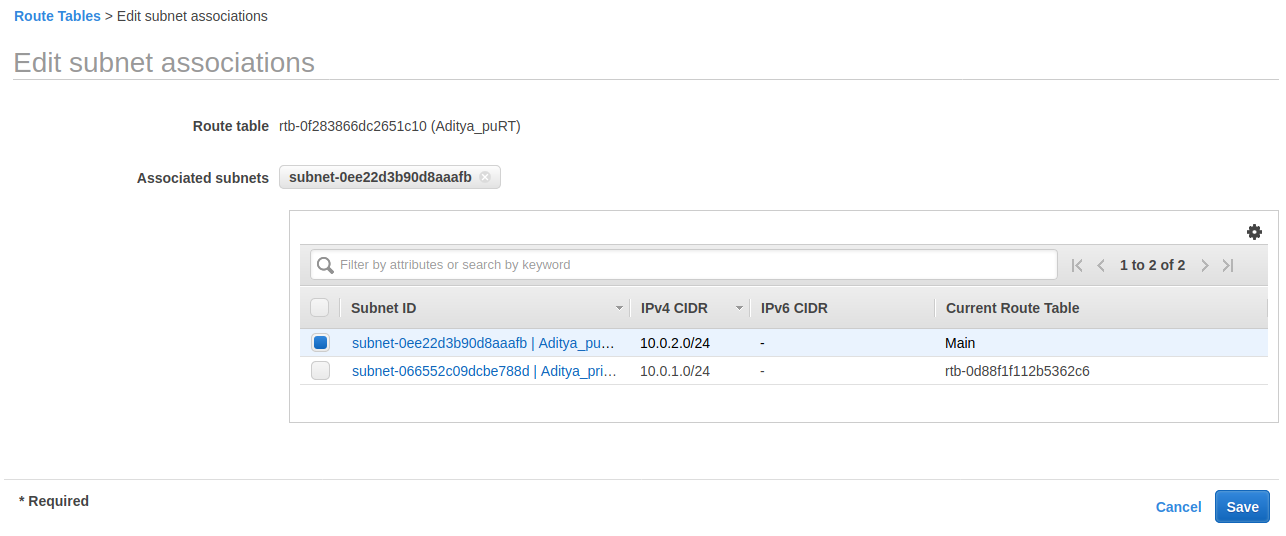


Modify auto assign ip setting for public subnet

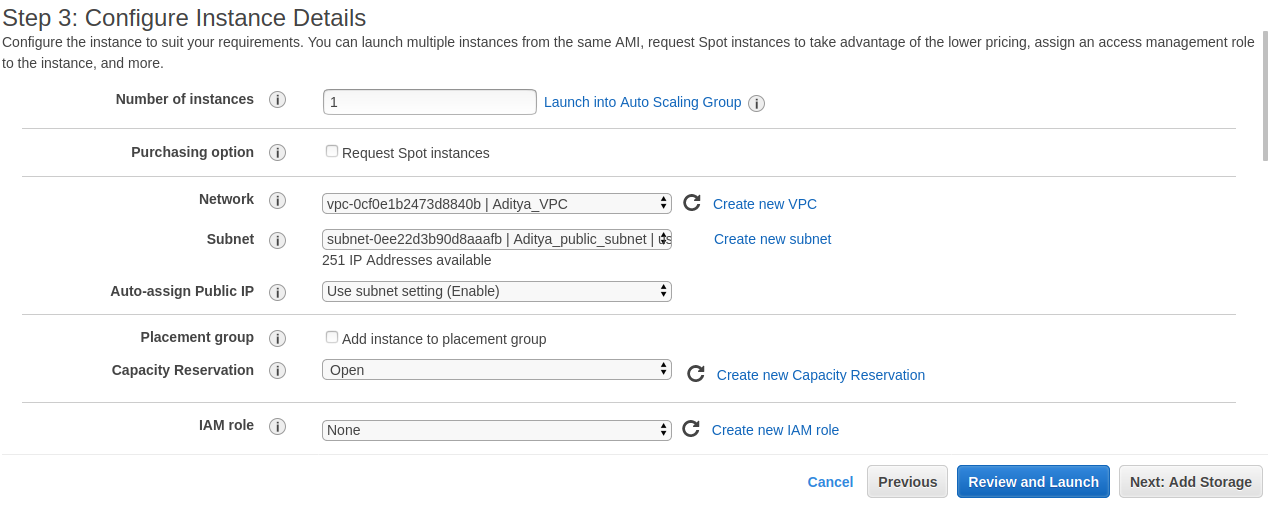


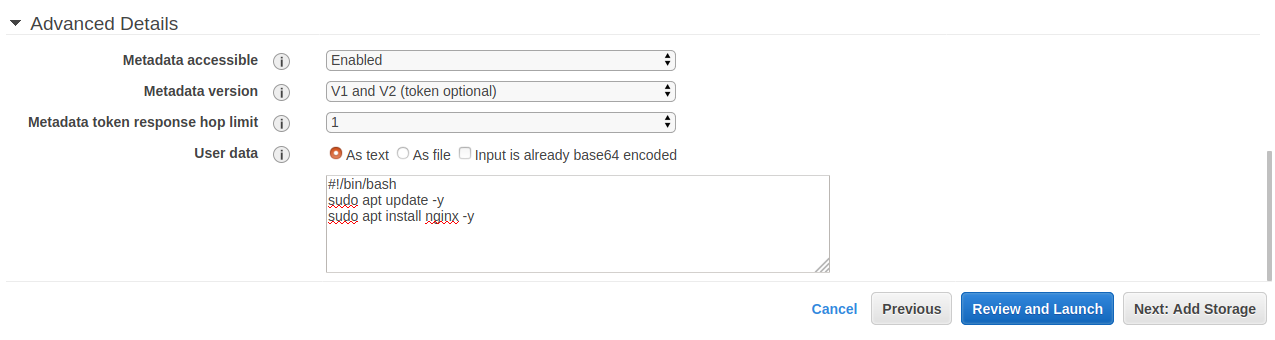
Edit subnet association for route tables

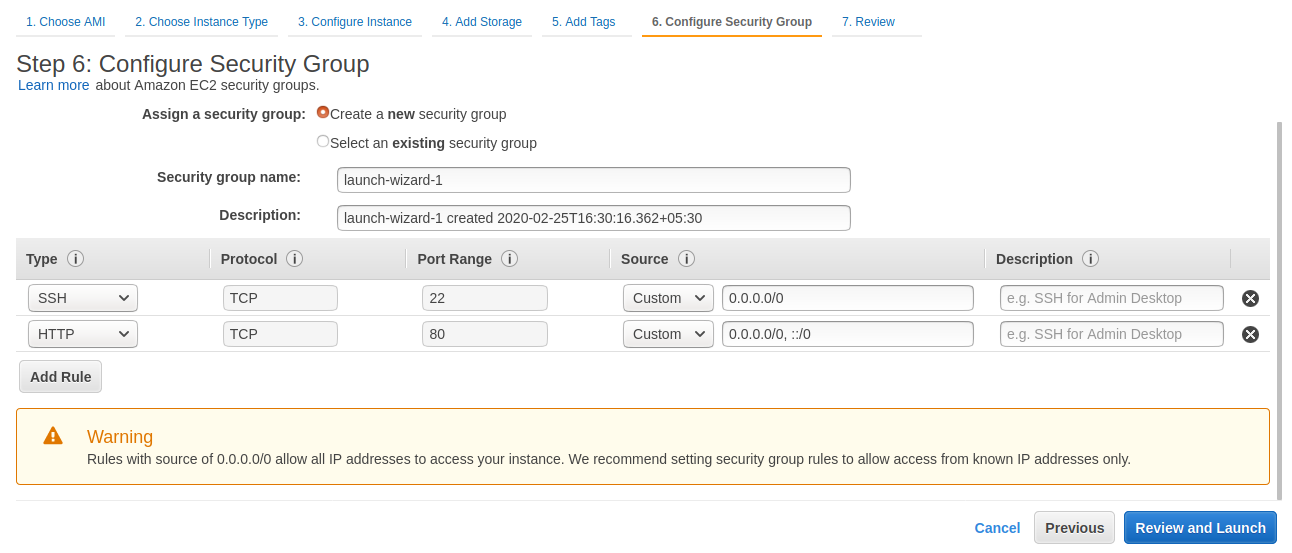




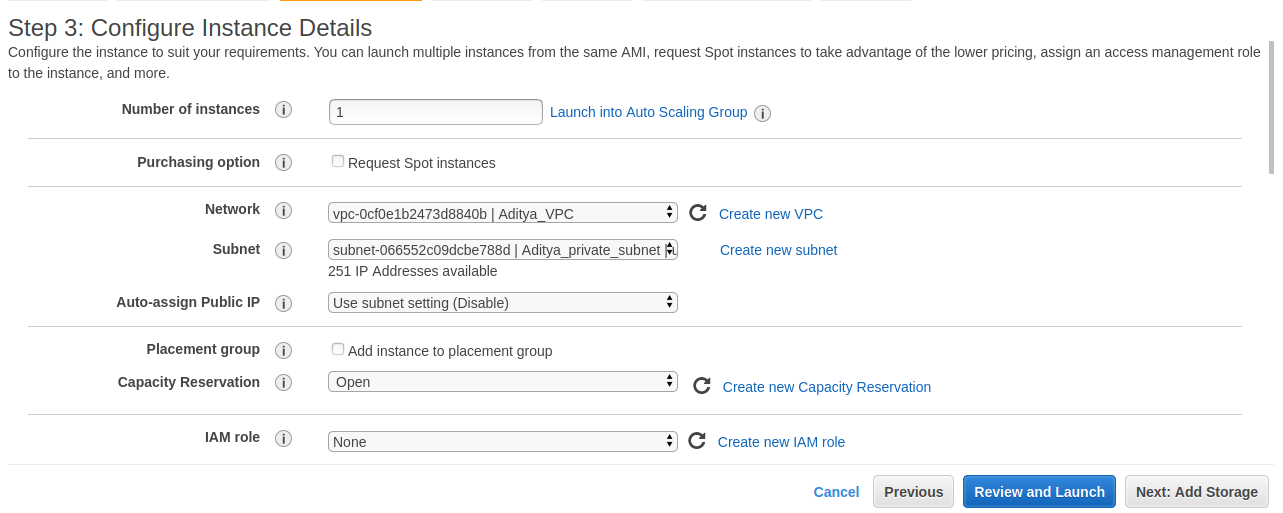
Create instance with nginx in public subnet

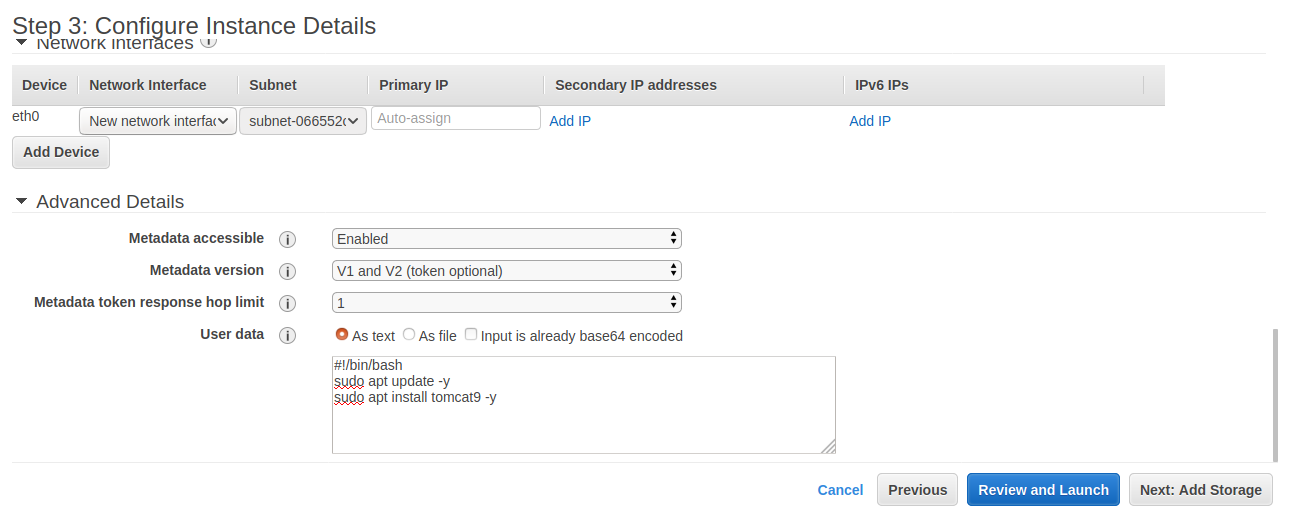


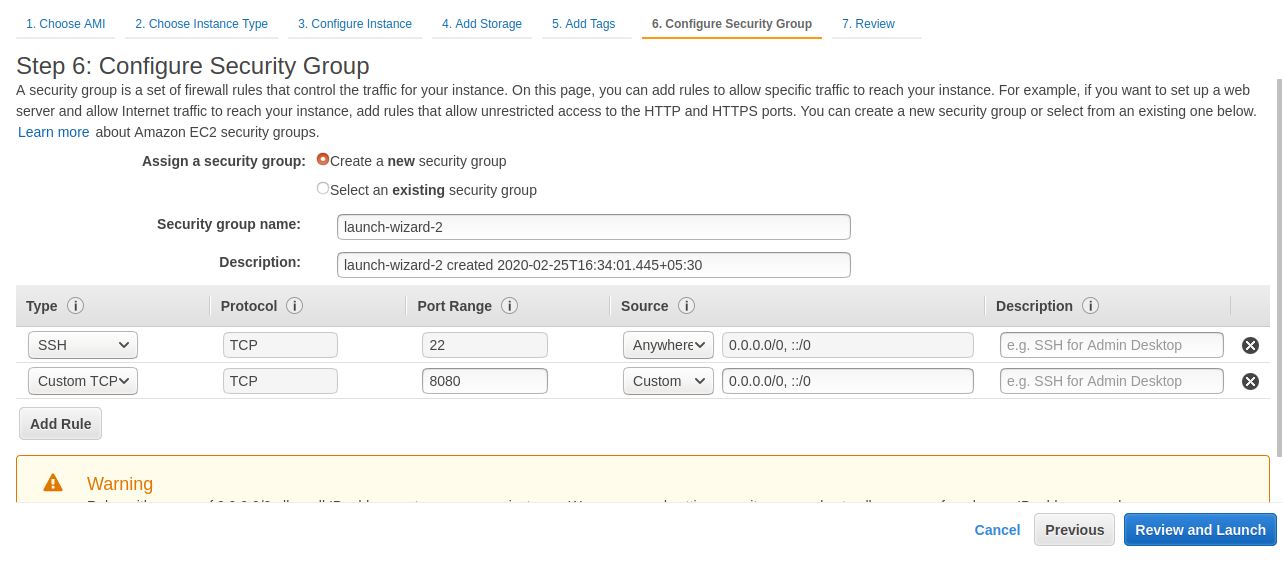




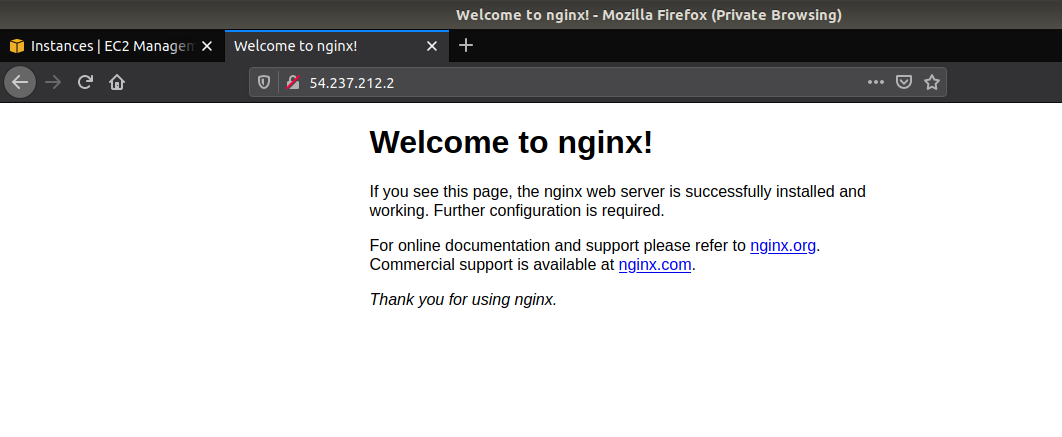
Create instance with tomcat9 in private subnet







Nginx on instance running



SSH to nginx server



Proxy pass to application server

