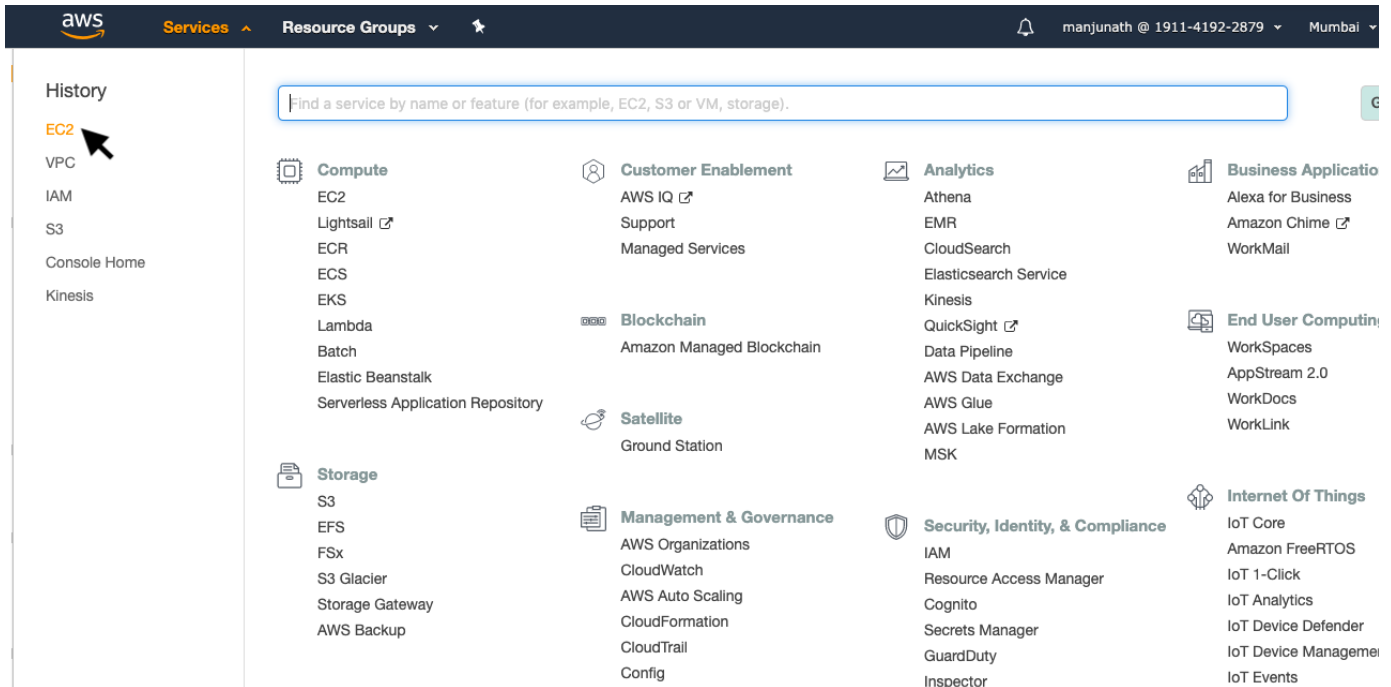


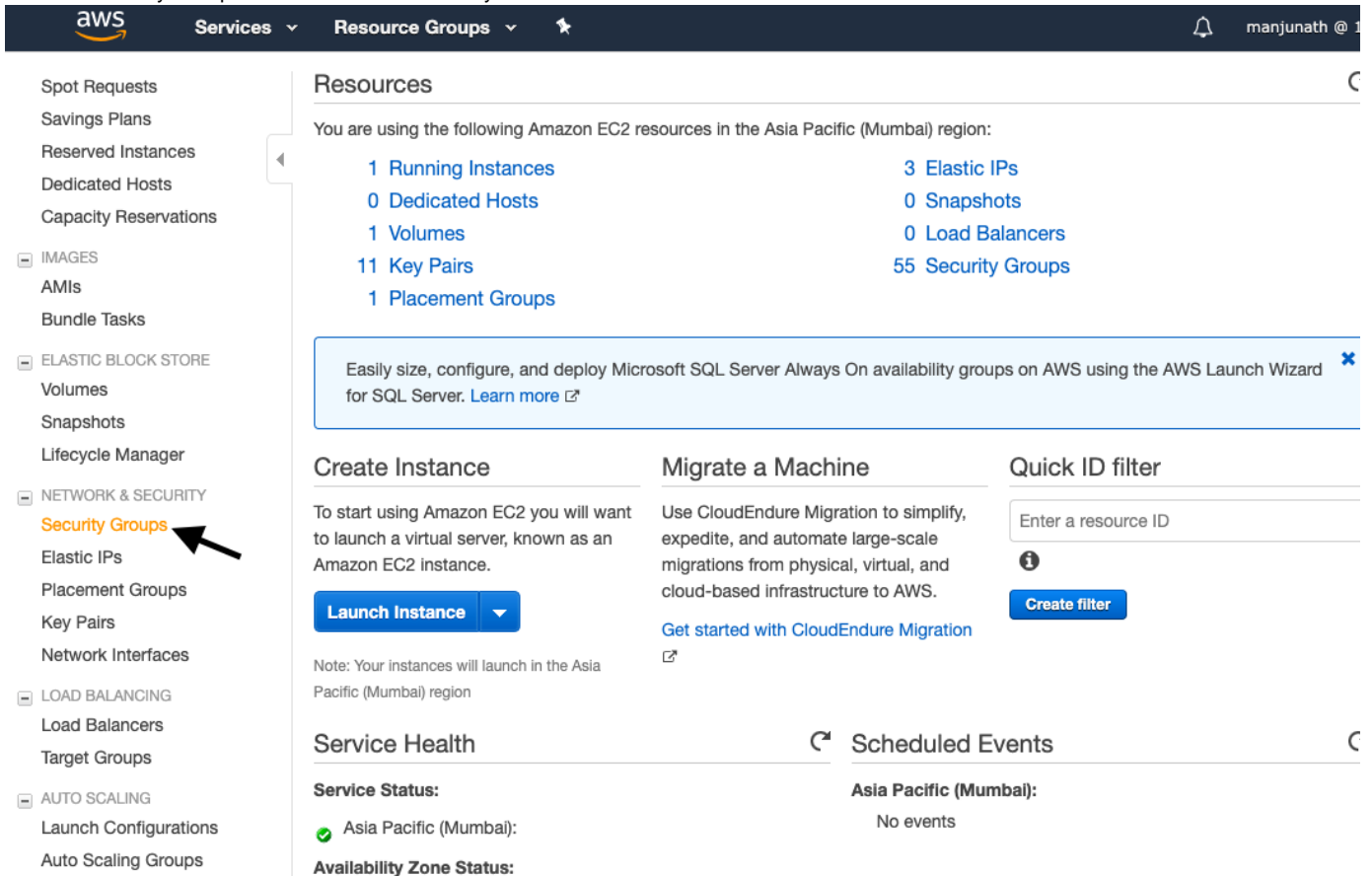
# Enabling Inbound Traffic in AWS VPC

1. login to AWS console for a specified Data Center

2. select under Services >> EC2



3. select 'Security Groups' under 'Network & Security'



4. There could be a list of security groups, select for the required security group which is attached to your instance

- here we are selecting a security group called by 'argoid-private'
- select for 'Inbound' and 'Edit' button

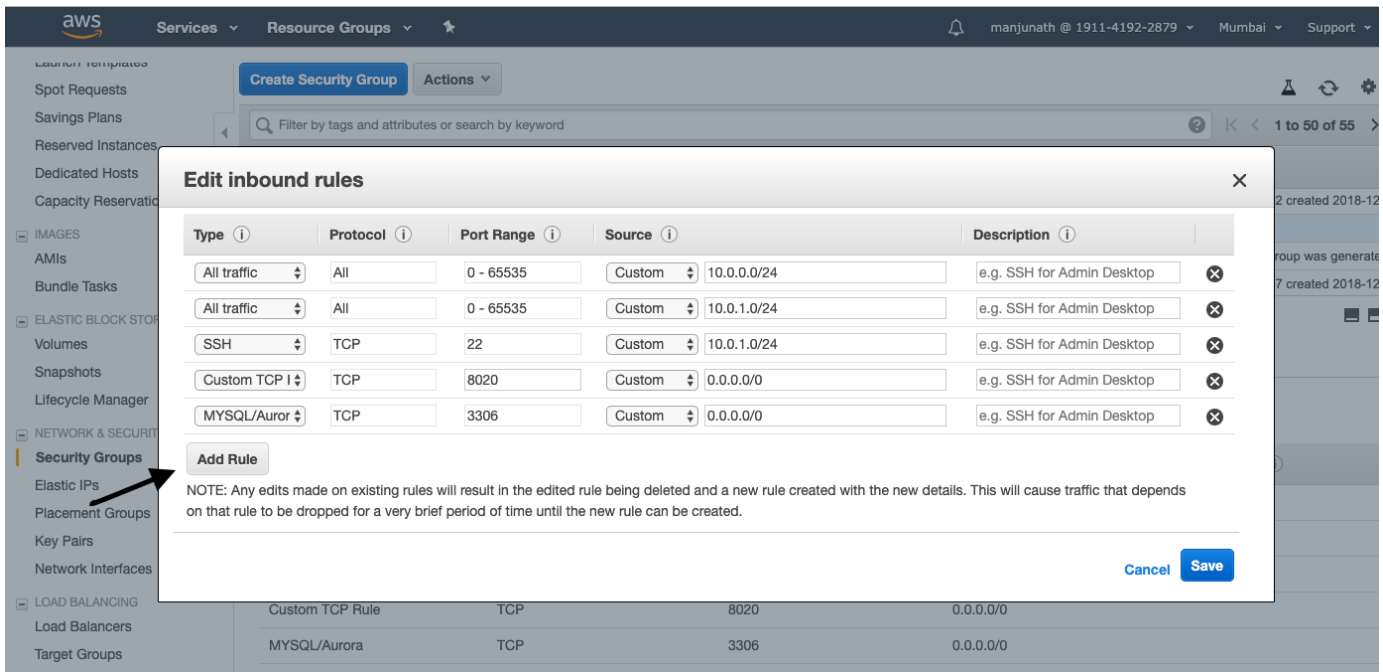
Type	Protocol	Port Range	Source	Description
All traffic	All	All	10.0.0.0/24	
All traffic	All	All	10.0.1.0/24	
SSH	TCP	22	10.0.1.0/24	
Custom TCP Rule	TCP	8020	0.0.0.0/0	
MYSQL/Aurora	TCP	3306	0.0.0.0/0	

Another simple way of editing the required 'Security Group' is by, Select the 'Instances' >> select required instance >> select required 'Security Groups:some-security-rules'

Instance: **i-04edd3489a9492792 (sentienz-wordpress)** Elastic IP: 13.127.220.35

Property	Value
Instance ID	i-04edd3489a9492792
Instance state	running
Instance type	t2.small
Elastic IPs	13.127.220.35*
Availability zone	ap-south-1a
Security groups	launch-wizard-18, view inbound rules, view outbound rules
Scheduled events	No scheduled events
AMI ID	CentOS Linux 7 x86_64 HVM EBS ENA 1805_01-b7ee8a69-ee97-4a49-9e68-afae216db2e-ami-77ec9308.4 (ami-1780a878)
Platform	-
IAM role	-
Public DNS (IPv4)	-
IPv4 Public IP	13.127.220.35
IPv6 IPs	-
Private DNS	ip-10-0-0-230.ap-south-1.compute.internal
Private IPs	10.0.0.230
Secondary private IPs	-
VPC ID	vpc-000d7c3801645ad3b (argoid-vpc)
Subnet ID	subnet-0be49cd11fe5b5bfd (argoid-public-subnet)
Network interfaces	eth0
Source/dest. check	True

5. Edit existing rule, or else 'Add Rule'



6. To pass all the traffic across the nodes in the cluster, select

- Choose 'All traffic', Protocol 'ALL', Port Range '0-65535'
- in 'Source', the CIDR has to be chosen in the way of 172.31.0.0/24. (CIDR blocks depends on the public subnet CIDR)
- Select 'Save'

