AWS HACKATHON DOCUMENTATION

September 29, 2023

BRAINOVISION

TEAM MEMBERS:

g.anu deepika

b.uma devi

k.sriram

m.tarun

r.kishore

m.jogendra

# AWS PROJECT REPORT – DOCUMENTATION

**What Is AWS?**

AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon that includes a mixture of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and packaged-software-as-a-service (SaaS) offerings. AWS services can offer an organization tools such as compute power, database storage and content delivery services.

Amazon.com Web Services launched its first web services in 2002 from the internal infrastructure that Amazon.com built to handle its online retail operations. In 2006, it began offering its defining IaaS services

**AWS TOOLS**

AWS provides a wide range of tools and services However, there are a few tools that are widely used and considered fundamental in many AWS deployments. Here are some of the most commonly used tools of AWS:

* Amazon EC2 (Elastic Compute Cloud)

It provides a virtual server in the cloud, allowing you to run applications and services on a variety of operating systems.it also used to create various instances.

* Amazon RDS (Relational Database Service)

It Provides managed database services for various relational database engines, including Amazon Aurora, MySQL, PostgreSQL, Oracle, and SQL Server.

* Amazon VPC (Virtual Private Cloud)

It Offers a logically isolated virtual network within the AWS cloud. It allows you to launch AWS resources in a defined virtual network, providing control over IP addressing, subnets, and network gateways.

* *Amazon SQS (Simple Queue Service)*

It A fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.

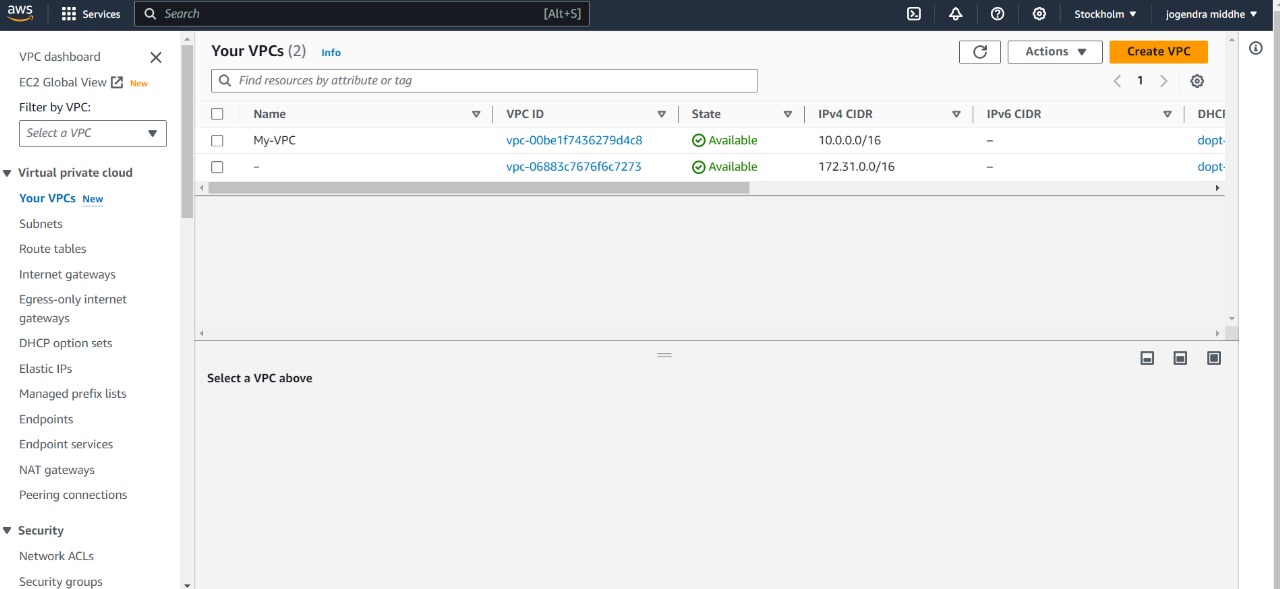
* AWS CloudTrail

It Captures and logs API activity and events within your AWS infrastructure, providing audit trails for compliance, security analysis, and troubleshooting.

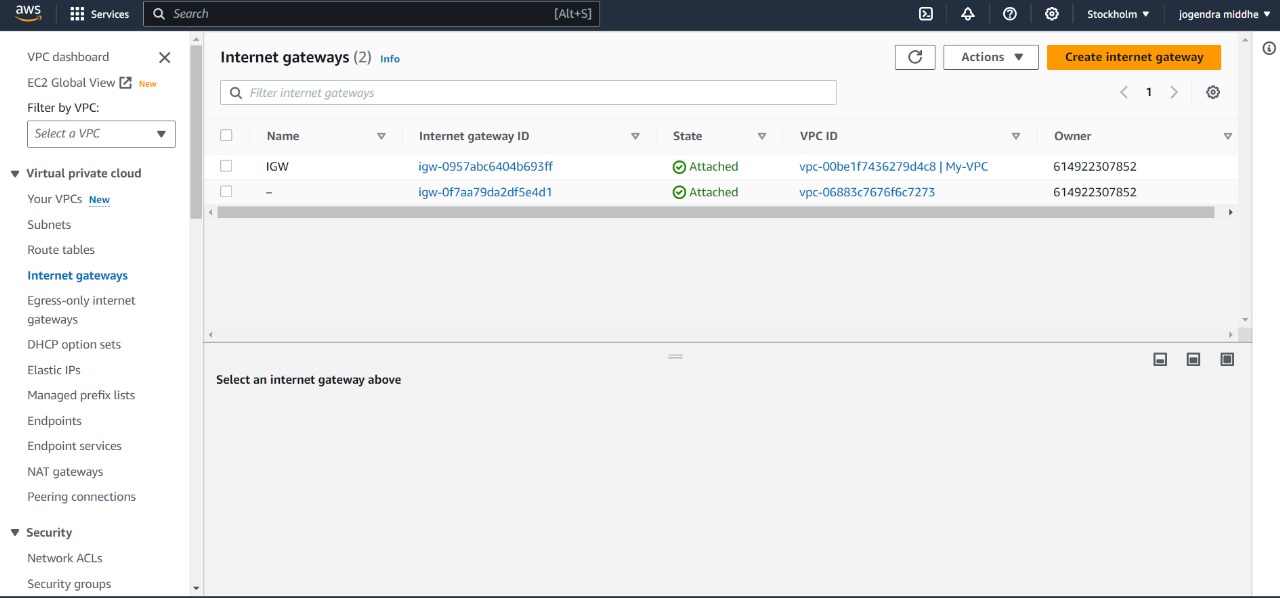
**STEP-1:**

**Creating a Virtual Private Cloud(VPC):**

* Go to VPC dashboard click on the “create VPC” to start the VPC creation.
* Configure the VPC settings:
  + - Give a name for your VPC.
    - Specify the IPv4 CIDR block for your VPC's IP address range (10.0.0.0/16).
    - you can also assign an IPv6 CIDR block to your VPC.
* Configure the VPC's subnets:
* Specify the IPv4 CIDR block for your first subnet (e.g., 10.0.0.0/24).
* Choose the availability zone where you want to create the subnet.
* Repeat this step to create additional subnets if needed.
* Configure the VPC's route table:
* Create a new route table or select an existing one.
* Associate the subnets created in the previous step with the route table
* Configure the VPC's internet gateway:
* Create a new internet gateway or select an existing one.
* Attach the internet gateway to your VPC.
* Configure the VPC's security groups:
* Create new security groups or select existing ones.
* Define the inbound and outbound rules for each security group to control network traffic.
* Review all the configuration details and settings for your VPC. If everything looks correct, click on the "Create VPC" button to create your VPC.

****

**INTERNET GATEWAYS (IGW)**

****

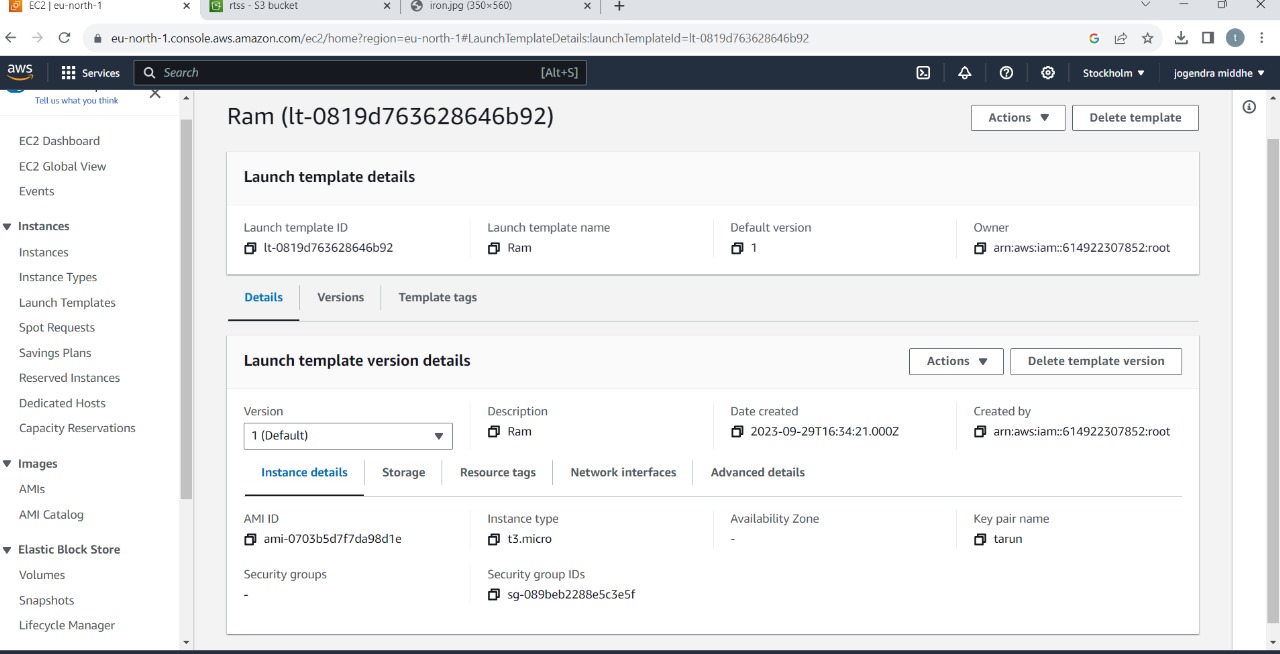
**ROUTE TABLES (RT):**

* Go to the "Route Tables" section: Within the selected VPC, click on the "Route Tables" option in the left navigation menu. This will display the list of existing route tables in the selected VPC**.**
* Create a new route table: Click on the "Create Route Table" button to create a new route table within the selected VPC.
* Configure the route table settings:
* Provide a name for the route table to identify it.
* Select the VPC in which you want to create the route table.
* Choose the desired subnet associations for the route table. Subnets can be associated with multiple route tables, and each subnet must be associated with at least one route table.
* Configure the routes:
* Click on the "Edit routes" button to add or edit routes in the route table.
* Add the desired routes by specifying the destination IP range and the target (e.g., an internet gateway, a virtual private gateway, or a NAT gateway)
* Save the route table: Click on the "Save" button to save the configured route table.
* Associate subnets with the route table:
* In the "Associations" tab of the route table, click on the "Edit subnet associations" button.
* Select the subnets you want to associate with the route table and click on the "Save" button.
* Review the route table: Verify the route table settings, associations, and routes in the AWS Management Console.
* Create a new route table: Click on the "Create Route Table" button to create a new route table within the selected VPC.

**STEP 2:**

Create an Auto Scaling Group:

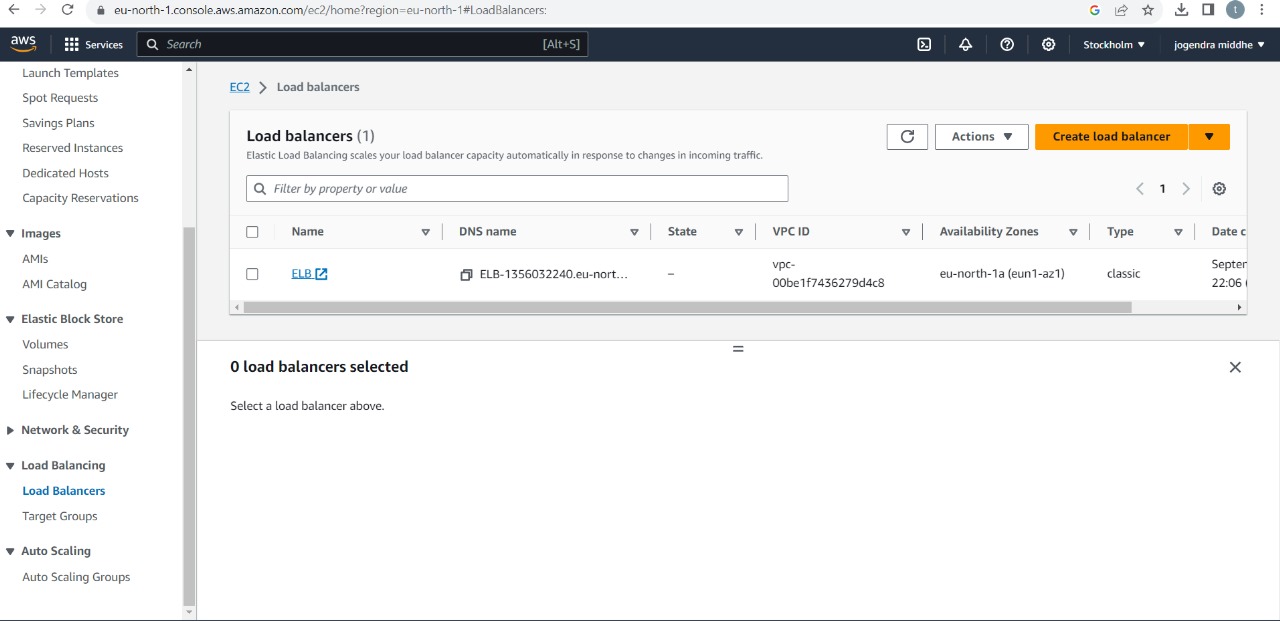
* In the EC2 Auto Scaling console, click on "Auto Scaling Groups" in the sidebar.
* Click on "Create an Auto Scaling group" .



* Select the launch configuration you created in the previous step.
* Configure the desired minimum, maximum, and desired capacity of instances.
* Configure any additional settings such as scaling policies and tags.
* Save your Auto Scaling group.

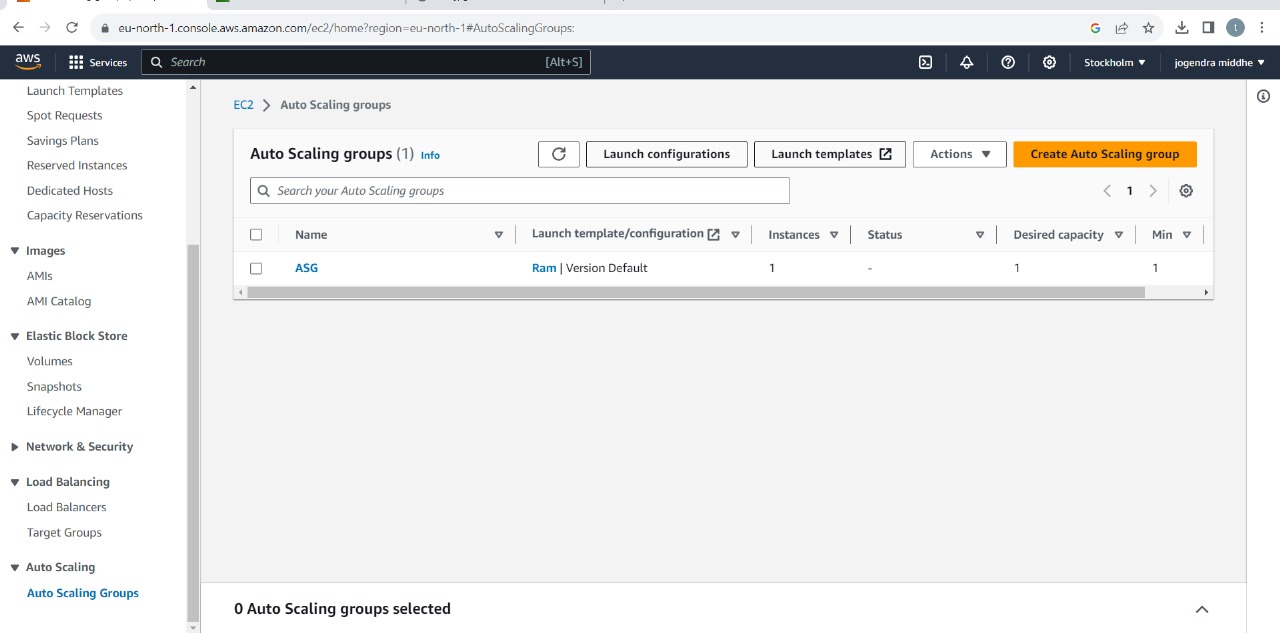
Create an Elastic Load Balancer:

* Go to the EC2 console.
* Click on "Load Balancers" in the sidebar.
* Click on "Create Load Balancer" and select the type of load balancer you want to create (e.g., Application Load Balancer, Network Load Balancer, or Classic Load Balancer).
* Configure the load balancer's settings, such as listeners, target groups, security groups, and availability zones.
* Save your load balancer.



Configure the Auto Scaling Group with the Load Balancer:

* In the EC2 Auto Scaling console, select your Auto Scaling group.
* Click on the "Edit" button in the "Details" tab.
* In the "Load balancing" section, select "Enable" for "Classic Load Balancer" or "Target groups" for "Application Load Balancer" or "Network Load Balancer."
* Select the load balancer and target groups you created in the previous step.
* Save your changes.



After following the above steps, we can connect to the webserver

USER DATA:

sudo su

yum update -y

yum install httpd -y

cd/var/www/html

echo “how”>index.html

service httpd start

chkconfig httpd on

