Create IAM Dashboard Roles and Policies.

First Click on Create policy.

Select CloudWatch Logs Services for the applications.

Select AllCloudWatch Logs actions (logs:*) as Manual actions.

Select S3 Service.

Select All S3 actions (s3: *) as manual actions for S3 service.

Again, Add More Permissions and add DynamoDB.

Add DynamoDB actions (dynamodb: *)

Give your policy name to the policy details that you want to create and click on create policy.

Select the roles in IAM resources.

Click on create role.

Select AWS service as entity type and select use case as lambda.

Add Custom type as permissions and click next.

Provide the Role name at role details and Create role.

Open S3 Services and create bucket.

Provide the Bucket name and create bucket.

Enable the bucket key.

Click on Create Bucket.

Bucket has been created successfully.

Select DynamoDB and create table.

Provide the table name and partition key and create table.

Table has been created successfully.

Create Lambda Services.

Create a function.

Provide functional name while creating the function.

Select runtime as python 3.7

Change default execution role to Use and existing role.

Select the created role e.g.: pgk-role.

Click on create function.

Add your triggers to your function.

Select your bucket in trigger concept and accept the acknowledgment and click add.

Open Triggers code.

Delete all the default code and paste copied code.

Open DynamoDB services and open tables.

Copy the name, place the name inside the code.

Click on Dynamodb service in table info.

Explore table items and add new attribute as String.

Create item by providing string attribute information.

Edit the item that has been created.

Copy the Json view code and paste it in the note pad.

Modify the code copied and save the txt file into json file.

Open bucket in S3 service.

Upload the Json file to the bucket.

Add the created JSON file.

Click on upload.

Autoscaling:

Create EC2 on server.

Click on Target Groups.

Click on create target group.

Give your preferred Target group name.

Click on next.

Click on create target group.

The target groups is created.

Create the load balancer.

Compare and select the load balancer and then click create.

Provide load balancer name.

Select all the mapping options.

Create security group name.

Type description in security group info.

Add rule in inbound rules info.

Search and Select the HTTP in VPC info.

After adding rule then select in source “Anywhere-IPv4”.

Select “https” in the type in inbound rules .

Select the source.

Create SSH protocol.

Add https protocol.

Click on create security group.

Select security groups.

Select GGN security group.

Select a target group.

Create the load balancer.

View the load balancer.

Select the load balancer in the interface.

In the actions click on start to make it active.

Copy the DNS name in the details.

Paste it in the browser.

It will display that the service is unavailable.

Create the launch template.

Provide a meaningful name.

Select amazon Linux software.

Select the instance type and create a new key pair.

Give a name and create a new key pair.

Create a new security group.

Select the existing security group.

Click on advanced details.

Select the free tier and launch a template.

The template has been created.

Select the launch template.

Go to auto scaling groups and click on it.

Click on create auto scaling group.

Choose the launch template and name it.

Select the launch template and click on next.

Select available zones and subnets.

Select all the zones.

Click on next.

Configure it to attach an existing load balancer.

Select a target group.

Turn on elastic load balancing health checks.

Configure the group size.

Click on next.

Click on next.

Create auto scaling group.

Select the auto scaling group.

Go to details.

Double click on load balancer.

Go to details and copy the DNS name.

RDS:

Create an EC2 instance.

Launch an Instance

Under name and tags, for Name, Enter database.

Under Application and OS select WINDOWS OS that are free OS.

Create the Create Key Pair as database for connectivity.

Change Anywhere to My IP it help to work with in our IP address.

Create RDS Services of Dashboard feature .

Create Database

Select Microsoft SQL Server oprations.

Enter Password for your database and confirm master password by re-entering the password

Set up EC2 Connection to an EC2 Compute resource.

Select EC2 instance.

Then finally the database is created.

Go to Dashboard and open EC2 Instance.

Click on Instances(running) that you have created before.

Select the database that is created.

Connect the database .

Open RDP client and Download remote desktop file .

Uploud private key content and Decrypt password .

Copy the Public DNS