cloud computing
Endsem exam

Name: Anjuru Lokesh
Roll:- 18BCS006

1)

```
def function (input ):

    if (input = name1 )
        print ( 10*(10-1)/2 );

    if (input = name3 )
        print ("welcome");
        return input;

    else
        print ("error");
```

2)

-> An Amazon API gateway is a collection of resources and methods.

-> we can create one resource and define one method on it

-> The method is backed by a lambda function that is when we call the API function through an HTTPS endpoint, API gateway invokes the lambda function

-> The post method on the DynamoDB Manager resource supports the following operations.

-> create, update and delete an item

-> read an item

-> scan an item

-> echo, ping other operations used for testing

The request payload we sent in the post request identifies the DynamoDB operation and provides incoming data.

-> pass through the entire request:-

-> A lambda function can receive the entire HTTP request and set the HTTP response using the AWS-proxy integration type.

-> Catch-all method:-

Map all methods of an API to a single lambd function with a single mapping using ANY cat all method.

-> Catch-all resource:-

map all sub-paths of a resource to a lamb function without any additional configuration the new path parameters ({proxy+}).

Anjuru Lokesh
18BCS006.

3)

⇒ Amazon cloud watch service allows users to create logs which will display metrics as per user monitoring needs.

6) It also creates simple notification service (SNS) and take actions based on the thresholds. Notifications for the same can be triggered which can send emails to the user mailbox.

14) → An If we need to host a static website then we need to follow DNS restrictions in S3 bucket.

-> As DNS helps to connect bucket and website. we need to be careful and follow the restrictions.

->If we are hosting a static website we need to configure DNS as we need to link the data files present in S3 bucket to our domain.

-> If we don't follow we cannot perfectly give access and integrate S3 to our domain which leads to an

-> And also it must not accessed by anyone so access will be only for DNS linked domain.

-> when we are hosting a static website we need to follow DNS restrictions as it is endpoint for bucket or else it results in getting errors while integrating S3 bucket to our website.

5) Various ways to access Aws cloud :-

→ a) Aws console :-

→ This is the most convenient way to manage Aws resources. You can log in using the username and password.

→ Copy the user login URL from the root account.

→ From the security credentials tab, copy the console sign-in-link.

→ logout from your root account and log back in with that user.

→ Since the user has only read-only access to the IAM you can't add a new user

b) Aws Command line Interface :-

→ The AWS CLI is a centralised tool for managing your amazon web services accounts.

→ You can control multiple Aws services from the command line and automate them using scripts with just one tool to download and configure.

→ We will configure the Aws CLI for the user we created

→ You'll need access to the keys you downloaded while creating.

→ You can use any service you have access to once you have configured it.

c) AWS SDK:-

→ AWS provides tools for creating and managing applications.

→ AWS SDK allows you to programically manage service on AWS.

→ AWS provide SDK for several programming languages.

6) DDOS protection techniques:-

→a) Reduce Attack surface Area:-

→ one of the first techniques to mitigate DDOS attack is to minimize the surface area that can be attacked.

→ we want to ensure that we do not expose our application

→. In some case, you can use firewalls, or ACLs to control what traffic reaches your applications.

b) plan for scale:-

→ Two key considerations for mitigating large scale volumetric.

→ i) Transit capacity

→ ii) server capacity.

-> 1) Know what is normal and abnormal topics!

-> More advanced protection techniques can go one step further and only accept traffic that is legitimate.

->To do this, you need to understand the characteristics of good traffic that the target usually receives

Anjuru Loresh.
18BCS006.

7) Instance stop:-

→ The EC2 stopped state indicates that an instance is shut down and cannot be used.

→ It's essentially a temporary shutdown for when you're not using an instance but will need it again later.

→ There will be no deletion of the attached bootable EBS volume.

→ Generally we stop and restart the instance to resolve unexpected status check fails or incorrectly running applications.

Instance terminate:-

→ Termination means a complete removal.

→ Terminated instances cannot be recovered.

→ We will terminate instance only when we are done with all the work in the instance.

→ You are not billed for terminated EC2 instances

→ The data and RAM is erased when terminated.

Arjuru Lokesh
18BCS006

8)

→ Steps required to recover the EC2 instance key:-

→ Obtain the original instance's configuration information

→ Turnoff the original EC2 instance to which you want to access

→ Create a new instance and a new key pair

→ Access the new recovery instance through ssh

→ Remove the original instances primary EBS volume

→ Connect the previously disconnected volume to the new instance

→ Copy the recovery instances authorized keys to the target volume.

→ Unmount the target volume from the recovery instance and reconnect to the original instance using the previously mentioned configs.

→ Restart the original instance with the new key pair.

→ Remove the temporary instance from the system.

→ Launch a new recovery instance by following features

→ Add a new a log for the new instance called 'recoverinstance'.

→ Select a security group and click Review and launch

Anjuru Lokesh
18BCS006.

→ Select 'Generate new key-pair' on the popup, enter a name for it and download

→ Launch the instance.

→ Connect to the newly created instance using termind and newly generated key-pair.

→ return to ec2 management and stop the original instance

→ Detach the volume of the target instance we will like to gain access to and attaches it to the newly created recovery instance.

→ Create a temporary directory and mount the volume.

→ Copy the authorized key file from our new instance to the mounted instance.

→ Now unmount the blocked device.

→ Next, we need to detach the volume from the instance using the ec2 console and reattach it back to the original instance.

→ Attach the volume back to its original instance.

→ On the popup, select the original instance name and set device root path back to the same on rotecorlin

→ Try to connect instance using terminal and it should be accessible.