

Subject :- Cloud Computing.

→ Assignment - 1

①

EC2 :- Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable, compute capacity in the cloud.

- It is designed to make web-scale cloud computing easier for developers.
- Amazon EC2 simple web service interface allows you to obtain and configure capacity with minimal friction.

②

Elastic Beanstalk :-

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those application.

- Elastic Beanstalk reduces management complexity without restricting choice or control.
- You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning,

load balancing, Scaling and application health monitoring.

③ IAM :-

AWS Identity and Access Management (IAM) is a web service for security controlling access to AWS resources.

It enables you to create and control services for user authentication or limit access to a certain set of people who use your AWS resource.

④ ELB :-

Elastic Load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones.

It monitors the health of its registered target and routes traffic only to the healthy target.

⑤ S3:-

- Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

⑥ EBS:-

Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with EC2 instances.

You can create a file system on top of these volumes or use them in any way you would use a block device (such as a hard drive).

You can dynamically change the configuration of a volume attached to an instance.

⑦ FSx for Lustre:-

FSx for Lustre makes it easy and cost-effective to launch and run the popular, high performance Lustre file system.

you'll use. Lustre for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.

⑧ Glacier:-

Also Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 storage class for data archiving and long-term backup. With S3 Glacier, customers can store their data cost effectively for months, years, even decades.

⑨ SageMaker:-

Amazon SageMaker is a fully managed machine learning service with SageMaker data scientists and developers can quickly and easily build and train machine learning models, and then directly deploy them into a production-ready hosted environment.

⑩

Rekognition:-

Amazon Rekognition makes it easy to add image and video analysis to your applications.

You just provide an image or video to the Amazon Rekognition API and the service can identify objects, people, text, scenes, and activity. It can detect any inappropriate content as well.

⑪

SNS:- Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers.

(Also known as producers and consumers).

⑫

SES:- Simple Email Service

Amazon SES classic refers to the original Amazon SES Console, APIs and documentation which are available for a limited time until they are deprecated.

(13)

Lambda:-

Lambda is a compute service that lets you code without provisioning or managing servers.

Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the computing compute resources.

(14)

RDS:-

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud.

It provides cost-efficient and resizable capacity while automatically time-consuming administrative tasks such as hardware provisioning, database setup, patching and backups.

(15)

Cloud9 IDE

AWS Cloud9 is an integrated development environment, or IDE.

The AWS Cloud9 IDE offers a rich code-editing experience with support for several programming languages and runtime debuggers, and built-in terminal.

It contains a collection of tools that you need use to code, build, run, test, and debug software and helps you release software to the cloud.

(16)

Amazon Cognito

Amazon Cognito is a simple user identity and data synchronized service that helps you securely manage and synchronize app data for your users across their mobile & devices.

(17)

Amazon VPC

Amazon Virtual Private Cloud enables you to launch AWS resources into a virtual network.

that you have defined.

- In this virtual network closely resembles a traditional network that you'd operate in your data centre, with the benefits of using the scalable infrastructure of AWS.

18

Route 53 :-

Amazon Route 53 is a highly available and scalable cloud of Domain Name System (DNS) services that can automatically route traffic to multiple locations.

It is designed to give developers and business an extremely reliable and cost effective way to route and direct traffic to their applications by translating names like ~~hostnames~~ and hosts to IP addresses.

It's a cloud-based service automatically routes traffic to multiple locations based on the load and availability of each location.

Assignment - II

①

Create EC2 Instance.

→

Step 1:- Sign into AWS management console and open the Amazon EC2 console.

Step 2:- choose EC2 dashboard and then choose Launch instance.

Step 3:- choose me amazon linux 2 AMI as instance type.

Step 4:- choose the t2.micro type and then choose next:configure instance details.

Step 5:- on the configure instance details page, shown following set these values, and here the other as value as their default.

Network:- choose the VPC with both public private subnets that you choose for the PB instance. Such as the VPC identified tutorial VPC.

Step 6:- choose next>Add storage.

Step 7:- on the add storage page, keep the default value and

Step 8:- Go to Services

Next type Lambda and choose

Step 8:- On the Add stage page, choose Add Key then enter names. For key add other tutorial web services for values.

Step 9:- choose Next - Configuration security group

Step 10:- on the Configuration security group page, choose existing security group; then choose an existing security group such as the tutorial security group.

Step 11:- choose Review & launch

Step 12:- on the Review instance launch page verify your settings and then choose launch.

Step 13:- on the Select an existing key pair or create a new key pair page, choose a new key pair and a set key pair name to finalizing key pair.

Step 14: choose download Key Pair and then save the Key Pair file on your local machine you use this Key pair to connect to your EC2 instance.

Step 15: To launch your EC2 instance choose Launch instance on the Launch Stages page. note the identity for your new EC2 instance.

Step 16: choose new instance to find instances.

Step 17: wait until instance status for your instance need by running object (before continue)

Q2 Connect to windows instance.

Step 1: Open the Amazon EC2 console

Step 2: In the navigation, Select instances, select the instance and then choose Connect.

Step 3: on the Connect to instance page, choose the RDP Client

and then choose Get password.

Step 4:- choose Browser and navigate to the private key file you created when you launched the instance.

Select the file and choose open to copy the entire contents of the following to this window.

Step 5:- choose Decrypt password

The console displays the default administration password for the instance with password, replacing the get password code.

Step 6:- choose download remote desktop file.

Step 7:- you may get a warning that the publication of the remote connection is unknown.

choose the connect to continue to connect to your instance.

Step 8:- the administrators account is chosen by default.

Step 9:- due to the nature, self-signed certificates. you may set a warning that the security certificate could not be authenticated.

Q-3

Connect to Linux instance:

1)

In a terminal window, use the ssh command to connect the instance. You specify the path and file name of the private key.

the user's name for your instance, and Public DNS Name or IPv6 address-

ssh -i /path/my-key-pair.pem my-instance
-user-name@my-instance
-public-dns-name

(2)

(optional) verify that the fingerprint in the Security alert matches the fingerprint that you previously obtained in step the instance fingerprint

Step 3:- Enter yes

Step 4:- choose send a test email.

Step 5:- In the "Send test email" dialog box, for format choose Raw

Step 6:- For the to address type mailto:
simone.smithe@amazon.com
for Amazon SES. Mailto: Simone

Step 7:- choose send test email

Step 8:- Repeat this procedure a few times so you generate multiple email sending event. For a few of the emails changes the value of the campaign message. say to clothing do simulate. Sending a different email campaign -

O-4

Create S3 bucket.

Step-1: Start into Amazon AWS.

Step 2:- Under storage & content
directory choose S3 to open
the Amazon S3 console.

Step 3: From the Amazon S3
console dashboard choose
new bucket.

Step 4: In Create a Bucket type
a Bucket name. In Bucket
name, the Bucket name you
choose must be globally unique
across all existing buckets
mean in Amazon S3.

Step 5: In Region choose Oregon

Step 6: choose credit

O-5

Send an Email using SES

Step 1: Sign in to the AWS management
console and open the Amazon
SES console.

Step 2:- In me navigator pane click the Amazon SES console under Identity management (choose Email Address)

Step 4:- In the list of identities select Create New SES email address you have successfully verified Amazon SES.