06_AVNIBACHudasma
MCA-III

CLOUD COMPUTING
ASSIGNMENT - 2

Q. Create EC_2 Instance

Step 1
Sign in to the AWS Management console and open the Amazon EC_2 console

Step 2
Choose EC_2 Dashboard, and then choose Launch instance.

Step 3
Choose the Amazon Linux 2 AJI.

Step 4
Choose the t2micro instance type, as shown following, and then choose Next Configure Instance Details.

Step 5
On the Configure Instance Details page, show follo -wing, set these values and keep the other values as their defaults.

Network - Choose the VPC with both public and private subnets that you chose for the DB instance, such as the vpc-identifier tutorial-vpc.

Subnet - Choose an existing public subnet, such as us west -2a

Auto-assign Public IP - Choose Enable.

Step 6
Choose Next - Add Storage.

Step 7
On the Add Storage page, Keep the default values and choose
Next - Add Tags

Step 8
On the Add Tags page, shown following, choose Add Tag, the enter Name for Key and enter tutorial -web server for value.

Step 9
Choose Next - Configure Security Group.

Step 10
On the Configure Security Group page, shown following, choose select an existing security group. Then choose an existing security group, such as the tutorial- security group.
make sure that security group that you choose includes inbound rules for Secure Shell SSH and HTTP access.

Step 11
Choose Review and Launch

Step 12
On the Review Instance Launch Page, shown following verify your settings and then choose Launch.

Step 13.
On the Select an existing Key pair or create a new Key pair page, shown following, choose create a new Key pair and set Key pair name to tutorial - Key - pair.

Step 15
To launch your EC2 instance, choose Launch instance. On the Launch Status page, shown following, note the identifier for your new EC2 instance, for example - i-0288d65fd4470b6a9.

Step 15
Choose View Instances to find your instance.

Step 16
Wait until Instance Status for your instance reads as Running before continuing.

Q2. Connect to windows instance

Step 1
Open the Amazon EC2 console

Step 2
In the navigation pane, Select Instances. Select the instance and then choose Connect.

Step 3
In the Connect to instance page, choose RDP client and the choose Get password.

Step 4:
Choose Browse and navigate to the private key file you created when you launched the instances. Select the file and choose Open to copy the entire contents of the file to this page.

Step 5
Choose Decrypt Password. The console displays

the default administrator password for the instance in Password, replacing the Get password link shown previously. Save the pass-word in a safe place. You need this passw-ord to connect to the instance.

Step 6
Choose Download remote desktop file. Your brow-ser prompts you to either open or save the RDP shortcut file.

Select the option to save the file. When you have finished downloading the file, choose Cancel to return to the Instances page.

Step 7
Navigate to your downloads directly and open the RDP shortcut file.

Step 8
You might get a warning that the publisher of the remote connection is unknown. Choose Connect to continue to connect to your instance.

Step 9.
The administrator account is choosen by default. Copy and paste the password that you saved previously.

Step 10.
Due to the native of self-signed certificates, you might get a warning that the security certificate could not be authenticated. Use the following steps to verify the identity of the

remote computer, or simply choose Yes Windows or continue mac os x if you trust the certificate.

If you are using Remote Desktop Connection on a Windows computer, choose view certificate. If you are using Microsoft Remote Desktop on a Mac, choose show certificate.

Choose the Details tab, and scroll down to Thum-bprint Windows or SHA1 Fingerprints mac os x This is the unique identifier for the remote computers.

Security certificate

In the Amazon EC2 console, select the instance, choose Actions, ~~For~~ Monitor and Troubleshoot, Get system log.

In the system log output, look for RDPCERTIFICATE thumbprint. If this value matches the thumbprint or fingerprint of the certificate, you have verifi-ed the identity of the remote computer.

If you are using Remote Desktop Connection on a Windows computer, return to the certificate dialog box and choose OK. If you are using Microsoft Remote Desktop on a Mac, return to the verify certificate and choose continue.

Windows choose Yes in the Remote Desktop Connection window to connect to your instance.

Q3. Connect to Linux instance

Step 1

In a terminal window, use the ssh command to connect to the instance. You specify the path and file name on private key (pem), the user name for your instance, and the public DNS name or IPv6 address for your instance

for more information about how to find the private key the user name for your instance, and the DNS name or IPv6 address for an instance. To connect to your instance, use one of the following commands to connect using your instance's public DNS name, enter the following command.

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

Step 2

Verify that the fingerprint in the security alert matches the fingerprint that you previously obtained in optional Get the instance fingerprint. If these fingerprints dont match, someone might be a attempting a an-in-the-middle attack. If they match, continue the next step.

Step 3

Enter yes.

Q4. Create s3 bucket

Step 1

Sign in to amazon aws

Step 2

Under Storage and content Delivery, choose S3 to open the Amazon S3 console.

Step 3
From the Amazon S3 console dashboard, choose Create 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 bucket names in Amazon S3 that is, across all AWS customers.

Step 5
In Region, choose Oregon

Step 6
Choose Create

Q5. Send An Email Using SES

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

Step 2:
In the Navigation pane of the Amazon SES console, under Identify Management, choose Email Addresses.

Step 3:
In the list of identities, select the check box of an address that you have successfully verified with Amazon SES.

Step 4:
Choose Send a Test Email.

Step 5:
In the Send Test Email dialog box, for Email format, choose Raw.

Step 6:
For the To address, type an address from the Amazon SES mailbox simulator.

Step 7:
Copy and paste the following message in its entirety into the message text box, replacing CONFIGURATION-SET-NAME with the name of the configuration set you created in Set up Configuration Set, and replacing FROM ADDRESS with the verified address you are sending this email from.

Step 8:
Choose Send Test Email.

Step 9:
Repeat this procedure a few times so that you generate multiple email sending events. For a few of the emails, change the value of the campaign message tag to clothing to simulate sending for a different email campaign.

06-Avniba-Chudasma
MCA-III

CLOUD COMPUTING

ASSIGNMENT - 3

Q1. Open source IASS software?

Cloudstack

Cloudstack is also an open-source Iaas platform that is specially designed for deploying and managing networks. This is now owned and developed by Apache software foundation.

Cloudstack has an easy to use interface which is web-based. Also, it has been observed by various users that the infrastructure management capability of this Iaas platform is highly scalable.

The Cloudstack Iaas platform consists of management servers that helps in managing resources like IP address, storage, etc.

Q2. Open source PASS Software?

Cloud Foundry

Cloud Foundry is an open source cloud computing platform as a service Paas software developed by Vmware. It offers a faster and easier way to build, test, deploy and scale applications.

It is primarily written in Ruby.

Cloud Foundry supports a wide range of services, and offers a choice of clouds such as vsphere or vCloud, Amazon Web Services, Openstack, Rackspace, Ubuntu, and more, and runs on either private or public infrastructure.

Cloud Foundry is an open source project and is available through a variety of private and cloud distributions and public cloud instances. micro cloud foundry is a free downloadable version of cloud Foundry that can run on a developers laptop, for developers interested in a single instance, personal Paas on your local machine. micro cloud Foundry is only available on cloud Foundry V1 not V2.

Features include

Includes a self-service application execution engine.
Automation engine for application deployment and lifecycle management
Scriptable command line interface CLI.

Integration with development tools to ease development and deployment processes.

Open architecture for quick development framework integration, application services interface and cloud provider interface.

Supports applications written in the JVM based languages - Java, Ruby, Node.js, Groovy, Scala

Supported frameworks include Spring and play for Java, Lift for Scala, Grails for Groovy, and Rails Sinatra for Ruby.

Application Services supported JySQL, MongoDB, vFabric Postgres, Redis and Rabbiting.

Q3. Open source SAAS software?

Openshift

It is one among the family of containerization software developed by Red Hat.

Openshift container platform is based upon the Kubernetes.

Openshift online is offered as a software-as-a-service.

Openshift includes container images allowing users to deploy frameworks and databases with one click.

Its user interface allows users to monitor the containers as well as their health.

Some of the products of Openshift are mentioned as under.

Openshift Origin - Supported by application lifecycle management functionally and Devops tools.

Openshift Online - Runs on AWS.

Openshift Dedicated - It is Red Hats private cluster offering, available on AWS, GCP, Microsoft Azure.

Features:

continuous integration and release management.
multiple environment support.
Choice of cloud infrastructure.
Pod autoscaling
Standardized developer workflow.

Q. Open Source cloud Simulation Software?

Greencloud

Greencloud is an energy-aware cloud computing data centres with a focus on cloud communications. It is sophisticated packet-level simulator.

It offers a detailed fine-grained modeling of the energy consumed by the data centre IT equi-pment, such as computing servers, network, switches, and communication links.

It is originally built at University of Luxemburg, Luxembourg.

Key-Features

Focus on cloud networking and energy awareness

Simulation of CPU, memory, storage and networ-king resources.

Independent energy models for each type of resource.

Q. Open source Distributed system Software:

Hadoop.

The Apache Hadoop project develops open-source software for reliable, scalable, distributed computing.

The Apache Hadoop software library is a framew-ork that allows for the distributed processing of large data sets across clusters of comput-ers using simple programming models.

It is designed to scale up from single servers to thousands of machines, each offering local computation and storage. Rather than rely on hardware to deliver high-availability, the library itself ~~at th~~ is designed to detect and handle failures at the application layer, so delivering a highly-available service on top of a cluster of computers, each of which may be prone to failures.

Hadoop Common - The common utilities that support the other Hadoop modules.

Hadoop Distributed File System a.k.a HDFS - A distributed file system that provides high-throughput access to application data.

Hadoop YARN - A framework for job scheduling & cluster resource management.

Hadoop MapReduce - A YARN-based system for parallel processing of large data sets.

Hadoop Ozone - An object store for Hadoop.