

# *Department Of Computer Science*

## *Gujarat University*



## *Certificate*

*Roll No: 15*

*Seat No: \_\_\_\_\_*

*This is to certify that Mr. / Ms. LUVHAR PRINCE KUMAR GHISULAL student of MCA Semester – III, has duly completed his/her term work for the semester ending in December 2021, in the subject of CLOUD COMPUTING – towards partial fulfillment of his / her Degree of Masters in Computer Science & Application.*

*13-DEC-2021  
Date of Submission*

*DR.HARDIK JOSHI  
Internal Faculty*

*DR.JYOTI PAREEK  
Head of Department*

Rollno: 15

Name: Luhar Prince

## CC Assignment

Page 7  
Date

→ Write down the steps for the following

D1 Create Ec2 Instance.

Step 1 Sign Into the AWS management Console and Ec2 console

2 Choose the ~~Amazon~~ Linux 2 AMI

2 Choose Ec2 Dashboard then choose launch instances

3 Choose the Amazon Linux 2 AMI

4 Choose the t2 micro Instances type and then choose next 'Configure instance detail'

5 Choose next → Add storage

6 Choose Next → Add tags

7 Choose add Tag, enter key name & value and choose next 'Configure security group'

8 Choose "select an existing Security group" then choose any security group → then choose Review & launch.

- ⑨ In this page, Verify your setting and then Choose launch.
  - ⑩ In this Page, choose Create a new Key Value pair and set key-pair name to tutorial key-pair.
  - ⑪ Choose Download Key Pair & Save the Key Pair file to your local machine, You will use this file to Connect to your Ec2 instances.
  - ⑫ To launch Ec2 instances, choose launch instances.
  - ⑬ Choose view instances to find your Instances.
- ~~⑭~~ Connect to windows Instances.
- Step 1 Open the Amazon Ec2 console.
2. Select Instances, Select your instances and then choose ~~with~~ connect.

- (3) In the Connect to instance Page, choose RDP Client and then choose get Password.
- (4) Choose browser and navigate to the private key files you created when you launched the Instance. Select the file and choose open to copy the entire contents of file to this page.
5. Choose Decrypt Password. This Console displays the default administrator password for the instance Password, replacing the get Password link shown previously. Save the Password in a safe place, you need this Password to connect to the Instance.
6. choose download remote desktop file, your browser prompts you to either open or save the RDP ~~shortcut~~ shortcut file. select the option to save the file. why finished downloading cancel to return to instance Page.

7. Navigate to your downloads directory and open RDP shortcut file.
8. You might get a warning that the Publisher of the remote connection is unknown. Choose Connect to continue to connect your instance.
9. The Administrator account is chosen by default. Copy and Paste the Password that you saved previously.
10. Due to the nature 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 your remote computer, or simply choose Yes (Windows) or Continue (macOS), if you trust the certificate.
11. In the Amazon EC2 console, select the instance, choose action monitor, and troubleshoot to get System Log.

- 12 In the system log output look for RDP Certificate Thumbprint. If this value matches the thumbprint of the certificate, you have verified the identity of the remote computer.
  - 13 Windows choose Yes in the Remote Desktop Connection window to Connect to your instance.
- Q3 Connect the linux instance.
- 1 In a terminal window, use SSH Command to connect the instance. You specify the Path and file name of the private key, the Username for your instance and public DNS name or IP address for your instance.  
For more information about how to find the private key, the Username for your instance and the DNS name or IP address for your instance. To connect to your instance use one of the following Commands:-

SSH -i /Path/my-key-Pair.pem my-instance-username  
my-instance-public-dns-name.

② Verify that fingerprint in the security alert matches the fingerprint that you previously obtained in (Optional) get the instance fingerprint. If these fingerprints don't match someone might be attempting a man-in-the-middle-attack. If they match continue to the next step.

③ Step Enter yes.

④ Create S3 bucket

1. Sign into Amazon AWS.

2. Under Storage & Content Delivery choose S3 to open the Amazon S3 console.

3. From the Amazon S3 ~~control~~ Console dashboard choose Create bucket

4 In Create bucket type the bucket name. The bucket name you choose must be globally unique across all existing bucket names in Amazon S3.

5 In region choose Your region.

6 choose Create.

Q5 Send an Email using SES.

Step 1 Sign into the AWS management Console and open the Amazon SES Console.

2. In the Navigation Pane of the Amazon SES Console, under Identity management, choose email address.

3 In the list of identities select the checkbox of an email address that you have successfully verified with Amazon SES.

4 Choose send a test mail.

## Assignment \*

Page 14  
Date \_\_\_\_\_

- Give the detailed discussion for the followings:-

1. Open Source IaaS Software  
(Any one slw with architecture)

- Infrastructure as a Service is a service model where an organization outsource the equipment used to support storage, hardware, server and networking component.

- OpenStack is an open source cloud computing project to provide an Infrastructure as a Service. This integration is obtained through public API's that each service offers.
- OpenStack controls large pool of Compute, Storage and Networking resources throughout a data center. All managed through a web interface. It delivers a massively scalable cloud operating system.

- The technology consists of a series of connected projects that controls pool of processing, storage and networking resources throughout a data center all managed through a dashboard that gives admin control while empowering its user to provision resources through a web interface.

## Q2 Open Source PaaS Software

- Platform as a Service is a category of cloud computing services which offers a way to support the complete lifecycle of delivery web applications & service via the cloud.
- OKD (previously known as openshift origin) is a ~~PaaS~~ PaaS computing platform as a service product from Red Hat. It is an application platform where application developers and team can build test deploy and run their application. OKD takes care of infrastructure, middleware & management so that developers can focus on their app.

## Rating Layer

### Developer

Isom Crit/?

Svn

Code GLCo

Existing  
Automation  
toolsets

### operations

Master

API/Authenti  
cation

Data Store

Scheduler

management

Replication

Redhat

Enterprise

Linux

## Rating Layer

Node

Node

Node

Node

Node

Node

Persist  
Storage



## Service Layers

Physical Virtual Private Public

## Cloud Architecture

- OKD enables you to Create, deploy and manage application ~~as~~ within the Cloud. It provides disk ~~a~~ space, CPU resources memory ~~and~~ network connectivity and on Apache or JBoss server. Depending on the type of application being developed, a template file system layout is provided. OKD also generates a limited Dos So your application is accessible online.
- It provides support for wide variety of languages runtimes and data layers including Java EGG, Ruby, PHP, Python, Perl, mysql, MongoDB.

### Q3 Open Source SaaS Software.

- SaaS is a distribution model where in the third party is trusted with the responsibility of hosting application and make them available for customers with the help of Internet.



- Cloudify is an open source cloud orchestration framework. It helps in the automation of the entire lifecycle of an application. Enables users to deploy the application in 2 ways.
  - 1) By opting for CLI only
  - 2) By opting the Cloudify manager
- Application Configuration are defined through blueprints that are developed on YAML DSL Configuration files. These blueprints have completed information regarding the application lifecycle starting from installation to its monitoring.
- Cloudify is dependent on these blueprint files for the execution of the plans in the cloud. These blueprint files describe the configuration of each component allowing with their binary location. Installation.

## \* features

- Local blueprint
- IT governance & security
- Blueprint modeling
- TOSCA orchestration
- Built in node types
- 

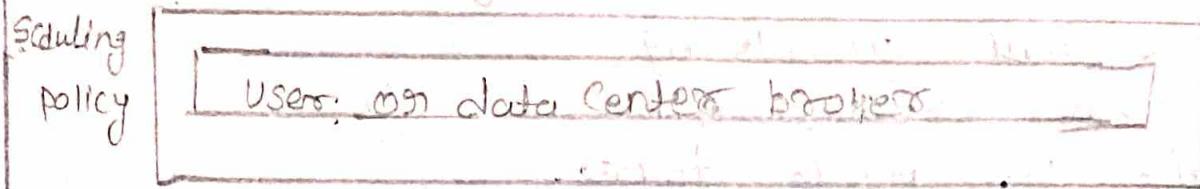
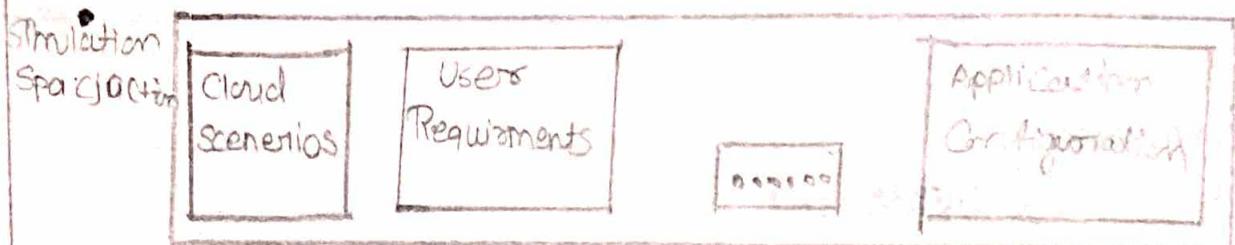
## ~~Cloud~~ Open source cloud simulation software

### - CloudSim

Cloudsim is a new highly generalized and extensible Java based simulation Toolkit and is actually regarded as software framework. It supports several core functionality like creating & processing of events, the creation of Cloudsim entities. ~~and~~ communication among components of the management of the simulation clock. CloudSim has been developed by the Cloud Laboratory of the Computer Science & Software Engineering department of the University of Melbourne. This toolkit enables seamless modeling, simulation & experimentation in

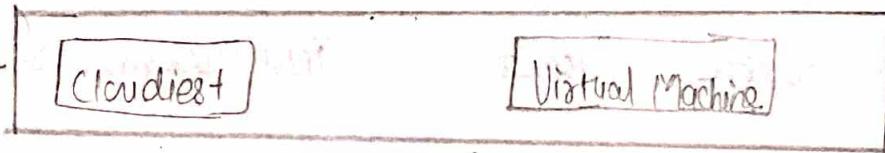
# CLOUDSIM Architecture

## USER CODE

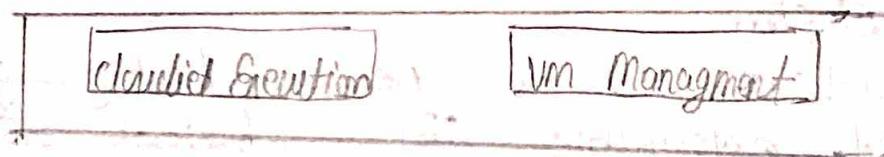


## CLOUDSIM

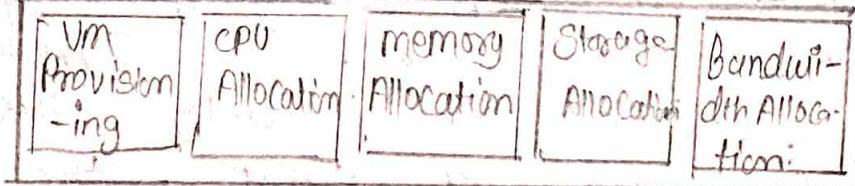
### User Interface Structures



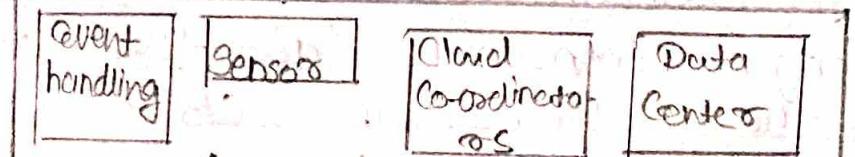
### VM Services



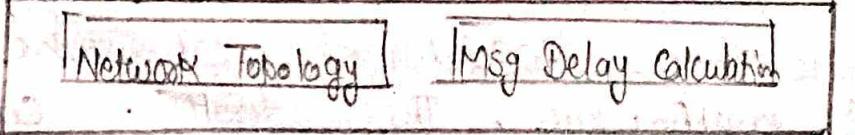
### Cloud Services



### Cloud Resources



### Network



Cloud Simulation Engine

Cloud Computing and application services.  
It can be treated as running a model of an environment by taking the hardware as base where technology specific details are abstracted.

### Q5 Opensource ~~software~~ Distributed System Software.

- The Apache Hadoop project develops open source software for reliable, Scalable, distributed Computing
- The Apache Hadoop Software library is a framework that allows for distributed processing of larger data sets across clusters of ~~com~~ computers using single server to thousands of machines each offering local Computation & Storage. Rather than only rely on hardware to deliver high availability, the library itself is designed to detect and handle failures at the application layer, so delivering a highly available service on the top ~~of~~ of a Cluster of computers each of which may prone to failures

Hadoop Common :- The Common Utilities that support the other hadoop ~~need~~ modules

Hadoop distributed file system :- HDFS is a distributed file system that provide high throughput access to application data.

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

Hadoop mapreduce :- A YARN based System for Parallel processing of large data sets.

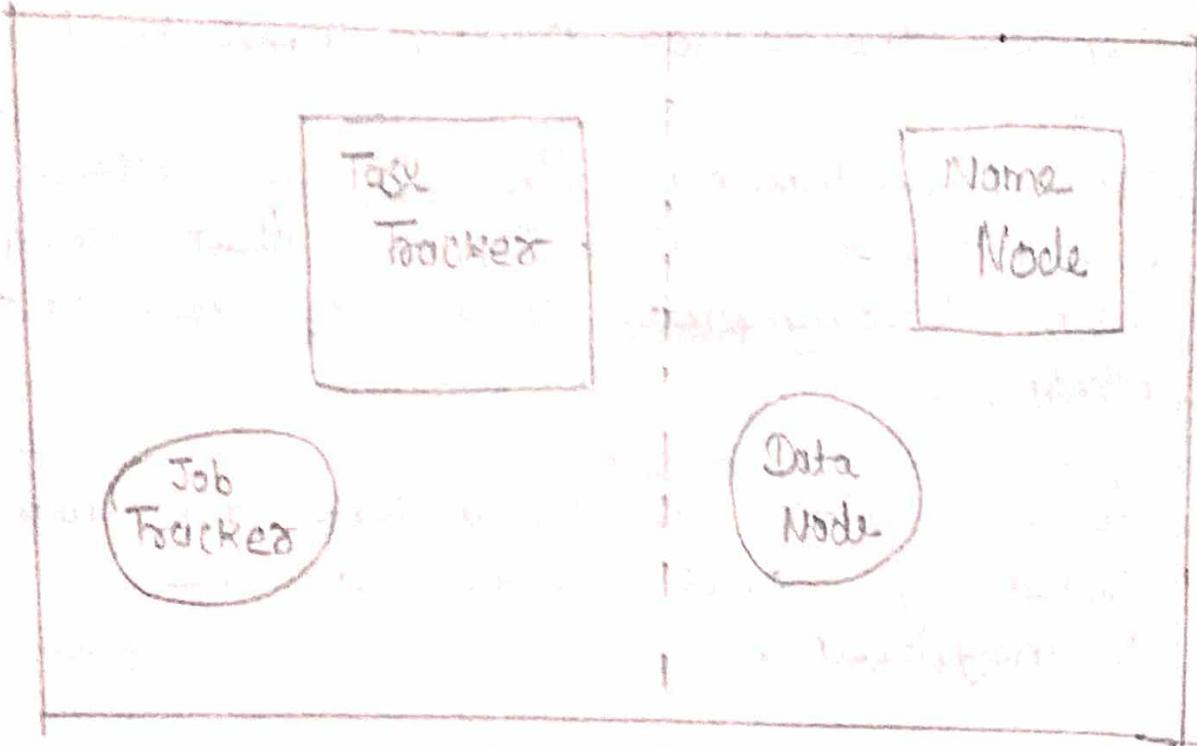
Hadoop ozone :- An object store for hadoop

MapReduce Layer

## MapReduce Layer

## HDFS Layer

Master



Slave

