**AWS**

**Normal Introduction :**

My name is Shubham Meshram, I am having 2.3 year of experience and currently working in linsyssoft technologies, Pune as an AWS Cloud Engineer. My role is to deploy the multitier applications on AWS as per client requirement and maintaining them**.** Sometimes I got a chance to create an infrastructure.

**Long Introduction :**

My name is Shubham Meshram, basically I am from Bramhapuri town which is located in Chandrapur district. I did my B.E in 2016 from MGM’s JNEC Aurangabad in stream of Information technology with aggregate of 61.2 %. I am having 2.3 year of experience and Currently working in linsyssoft technologies, Pune as an AWS Cloud Engineer. My role is to deploy the multitier applications on AWS as per client requirement and maintaining them. Sometimes I got a chance to create an infrastructure.

**Devops Introduction :**

My name is Shubham Meshram, I am having 2.3 year of experience and currently working in linsyssoft technologies, Pune as an AWS Cloud Engineer. My role is to deploy the multitier applications on AWS as per client requirement and maintaining them**.** Sometimes I got a chance to create an infrastructure. I am having relevant exp in aws for almost 2.3 years in which around 6 months of experience in devops. In which the tools like GIT, DOCKER.

**AWS General:**

1. What is your role? So did you create an architecture or you just implemented the already created architecture ?

Ans : My role is to deploy the infrastructure on AWS as per client requirement and their maintaining them. Actually sometimes I got a chance to create an architecture for multi – tier web applications and their deployment too.

2. Can you explain the architecture for social networking site ?

**AWS Therotical :**

1. What is difference between Network Load Balancer & Application Load Balancer?

Ans :a) **NLB** work on Network layer and transport layer i.e. 4th layer of OSI model and **ALB** work on Application Layer i.e. 7th layer of OSI model.

c) **NLB** helps just to forward the request but **ALB** examines the content of request like HTTP to Determine where to route the traffic.

c) Ex: Consider we deployed 2 different applications sharing same IP address so **NLB** will not differentiate between App1 and App2 whereas **ALB** can differentiate 2 applications by examining the application layer data available to it.

d) If extreme performance and Static IP is needed for application then use **NLB** whereas If you need Flexible application management then use **ALB.**

e) **NLB** supports TCP, UDP and TLS port whereas **ALB** supports HTTP and HTTPS port.

2. What is difference between Application Load Balancer & Classic Load Balancer?

Ans : a) Dynamic port mapping, multiple ports, multiple listeners is used in **ALB** whereas One port One Listeners is achieved by **CLB**.

b) If you need Flexible application management then use **ALB** whereas If you have an existing application that was built within EC2- Classic Network the use **CLB**.

c) **ALB** charged for each hour or partial hour based on running Load Balancer Capacity Units

(LCU) used per hour whereas **CLB** charged for each hour or partial hour based on Each GB data transferred.

3. What is difference between Network Load Balancer & Classic Load Balancer?

Ans : a) If extreme performance and Static IP is needed for application then use **NLB** whereas

If you have an existing application that was built within EC2- Classic Network the use **CLB**.

b) **NLB** charged for each hour or partial hour based on running Load Balancer Capacity Units

(LCU) used per hour whereas **CLB** charged for each hour or partial hour based on Each GB data transferred.

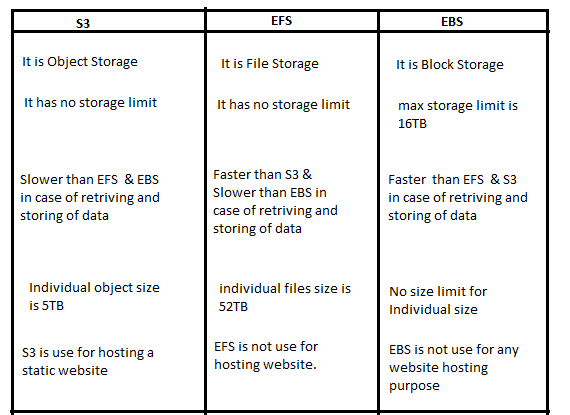
4. Why do you use EFS instead of S3 in your project?

Ans : Because it is faster that S3 in case of Storing and retrieving the data in the form of files.

5. What is egress only internet gateway?

Ans : It is a VPC Component that allows Outbound Communication over IPV6 from instance of Our VPC to the Internet and prevents from Initiating an IPV6 Connections with our Instance. It is similar to NAT Gateway but NAT Gateway is used for IPV4 address and Egress Only Internet Gateway is used for IPV6 address.

6. What is difference between S3, EFS , and EBS ?

Ans :

7. What is types of volumes for EC2 instances ?

Ans: **a) Instance store volumes :** It is temporary block level storage for instance. It is directly attached to our host computer. It stores temporary storage of information like buffers, caches, scratch data etc.

**b) Elastic Block Stores :** They are persistent volumes that you can attach to the instances. With EBS volumes, your data will be preserved even when you stop your instances, unlike your instance store volumes where the data is deleted when you stop the instances.

8. What are types of volumes in EBS ?

Ans : GPTMC

**a) General purpose :** recommended for most workloads volume size 1GB to 16TB

**b) Provisioned IOPS :** recommended for database workloads volume size 4GB to 16TB

**c) Throughput optimized :** recommended for big data, data warehouse volume size 500GB to 16TB

**e) Magnetic :** recommended for infrequent data access volume size 1GB to 1TB

**f) Cold HDD :** recommended when lowest storage cost is important volume size 500GB to 16TB

9. What are different storage class in S3?

Ans : Standard frequently accessed -> default

Standard infrequently accessed

One-zone infrequently accessed.

Glacier

RRS – reduced redundancy storage

10. what is security groups ?

Ans : Security groups are act as firewall to an EC2 instance which specifies Inbound and Outbound access policies for an EC2 Instance.

11. What is mean by Bucket Policy?

Ans : Bucket Policy means providing a permissions to an S3 bucket for

which IAM User can Access It.

11. What are Target Groups and Listeners in ELB?

Ans : **Target Groups** are logical group of servers or endpoints which the load balancer can route the traffic to it. Usually load balancer will check for a specific URL on each target node within the group to make sure it is healthy before routing traffic to it.

& **Listeners** is are the real servers and additional ports which are associated with load balancers

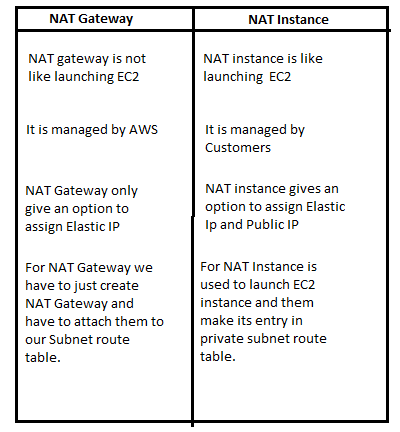
12. **What is the maximum number of S3 buckets you can create?**  
**Ans :** 100

13. **How many total VPCs per account/region and subnets per VPC can you have?**  
**Ans:** 5, 200

### 14. **Can you change the private IP address of an EC2 instance while it is in running or in a stopped state?**

Ans : No, it cannot be changed. When an EC2 instance is launched, a private IP address is assigned to that instance at the boot time. This private IP address is attached to the instance for its entire lifetime and can never be changed.

15. Difference Between NAT Gateway and NAT Instance

Ans : 

16. What is NAT Gateway?

Ans : You can use a NAT device to enable instances in a private subnet to connect to the internet (for example, for software updates) or other AWS services, but prevent the internet from initiating connections with the instances.

NAT device forwards traffic from the instances in the private subnet to the internet or other AWS services, and then sends the response back to the instances. When traffic goes to the internet, the source IPv4 address is replaced with the NAT device’s address and similarly, when the response traffic goes to those instances, the NAT device translates the address back to those instances’ private IPv4 addresses.

17.What is NAT, Egress only Internet Gateway, IGW, Ingress only internet gateway in Short ?

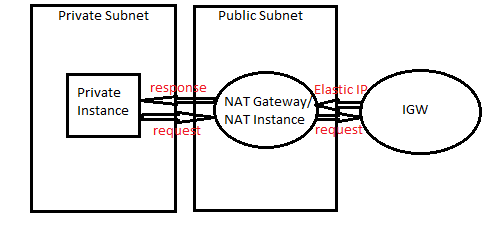
Ans : NAT : Outbound-IPV4 0.0.0.0/0

Egress : Outbound-IPV6 ::/0

IGW : Inbound-Outbound-IPV4 & IPV6 0.0.0.0/0 ::/0

Ingress : Inbound-IPV6 ::/0

18. How NAT Gateway /NAT instance Works ?

Ans :

19.What is Elastic IP ?

Ans : EIP is Static IPV4 address which is used to assign to an instance. If Your Instance having EIP and your instance is Stopped, Restart then the elastic IP will remain same. We can assign max 5 EIP per region.

An Elastic IP address is a public IPv4 address, which is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the internet. For example, this allows you to connect to your instance from your local computer.

20.What is VPC Endpoints?

Ans : VPC endpoints enable you to privately connect your VPC to services hosted on AWS without requiring an Internet gateway, a NAT device, VPN, or firewall proxies.

Endpoints are horizontally scalable and highly available virtual devices that allow communication between instances in your VPC and AWS services.

Amazon VPC offers two different types of endpoints:

gateway type endpoints and interface type endpoints.

Gateway type endpoints are available only for AWS services including S3 and DynamoDB. These endpoints will add an entry to your route table you selected and route the traffic to the supported services through Amazon’s private network.

Interface type endpoints provide private connectivity to services powered by PrivateLink, being AWS services, your own services or SaaS solutions, and supports connectivity over Direct Connect. More AWS and SaaS solutions will be supported by these endpoints in the future. Please refer to VPC Pricing for the price of interface type endpoints.

21.How do instances without public IP addresses access the Internet?

 Ans : Instances without public IP addresses can access the Internet in one of two ways:

Instances without public IP addresses can route their traffic through a NAT gateway or a NAT instance to access the Internet. These instances use the public IP address of the NAT gateway or NAT instance to traverse the Internet. The NAT gateway or NAT instance allows outbound communication but doesn’t allow machines on the Internet to initiate a connection to the privately addressed instances.

For VPCs with a hardware VPN connection or Direct Connect connection, instances can route their Internet traffic down the virtual private gateway to your existing datacenter. From there, it can access the Internet via your existing egress points and network security/monitoring devices.

 22. Does traffic go over the internet when two instances communicate using public IP addresses?

 Ans : Traffic between two EC2 instances in the same AWS Region stays within the AWS network, even when it goes over public IP addresses.

Traffic between EC2 instances in different AWS Regions stays within the AWS network, if there is an Inter-Region VPC Peering connection between the VPCs where the two instances reside.

Traffic between EC2 instances in different AWS Regions where there is no Inter-Region VPC Peering connection between the VPCs where these instances reside, is not guaranteed to stay within the AWS network.

 23.How does an AWS Site-to-Site VPN connection work with Amazon VPC?

 Ans : An AWS Site-to-Site VPN connection connects your VPC to your datacenter. Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and datacenter routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit. An internet gateway is not required to establish an AWS Site-to-Site VPN connection.

24. What is VPC ?

Ans : VPC is Virtual Private Cloud in which we can create our own customizable network.

We are able to create our own subnets, IP ranges, IGW, NAT, Route Tables etc.

We can launch our AWS resources in VPC.

25. Can we change public subnet to private subnet ?

Ans: Yes, By removing Internet Gateway from the public Subnet.

26. Can we decrease the EBS volume size of running instance?

Ans: No, We can’t decrease the EBS volume size of running instance.

27. What is Policies and their types?

Ans: <https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html>

We manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources.

There are 6 types of policies are there :

1. Identity-Based Policies.

2. Resource-Based Policies.

3. Permission Boundaries.

4. Service Control Policies.

5. Access Control Policies.

6. Session Policies.

Identity Based Policies : Identity-based policies are JSON permissions policy documents that you can attach to an identity (user, group of users, or role). These policies control what actions an entity (user or role) can perform, on which resources, and under what conditions.

Resource Based Policies : Resource-based policies are JSON policy documents that you attach to a resource such as an Amazon S3 bucket. These policies grant the specified principal permission to perform specific actions on that resource and defines under what conditions this applies. Resource-based policies are inline policies. There are no managed resource-based policies.

Permission Boundries : A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity. When you set a permissions boundary for an entity, the entity can perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role as the principal are not limited by the permissions boundary.

28. Which service supports both resource and identity based policies?

Ans : An **IAM role** is both an identity and a resource that supports resource-based policies.

29.What is ARN?

Ans : Amazon Resource Names (ARNs) uniquely identify AWS resources. We require an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls.

Format :

arn:aws:s3:::elasticbeanstalk-us-east-1-477291727479

arn:partition:service:region:account-id:resource-id

arn:partition:service:region:account-id:resource-type/resource-id

arn:partition:service:region:account-id:resource-type:resource-id

*partition :*

The partition in which the resource is located. A *partition* is group of AWS Regions. Each AWS account is scoped to one partition.

The following are the supported partitions:

aws - Standard Regions

aws-cn - China Regions

aws-us-gov - AWS GovCloud (US) Regions

*service :*

The service namespace that identifies the AWS product. For example, s3 for Amazon S3 resources.

*Region :*

The Region. For example, us-east-2 for US East (Ohio).

*account-id :*

The ID of the AWS account that owns the resource, without the hyphens. For example, 123456789012.

*resource-id :*

The resource identifier. This part of the ARN can be the name or ID of the resource or a [resource path](https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html#arns-paths). For example, user/Bob for an IAM user or instance/i-1234567890abcdef0 for an EC2 instance. Some resource identifiers include a parent resource (sub-resource-type/parent-resource/sub-resource) or a qualifier such as a version (resource-type:resource-name:qualifier).

30.What is VPC Peering?

Ans : A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.

Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

31. What is Shared AMI?

Ans : A shared AMI is an AMI that a developer created and made available for other developers to use.

Use a shared AMI that has the components you need and then add custom content. You can also create your own AMIs and share them with others.

It can be of two types :

1. Public shared AMI.

2. Private Shared AMI.

32. What are different ports in AWS?

Ans : SSH : 22

RDP : 3389

HTTP : 80

HTTPS : 443

MYSQL/Aurora : 3306

NFS : 2049

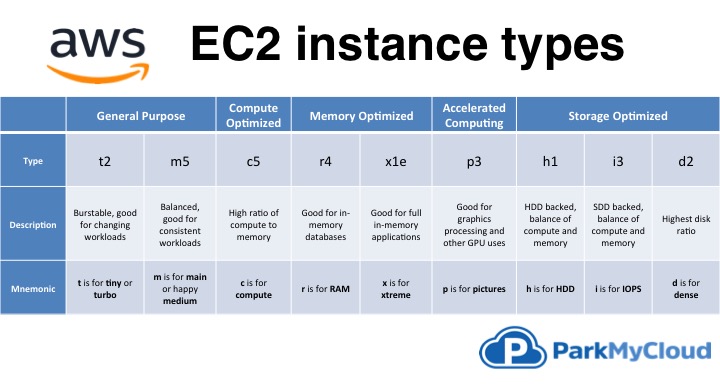
SMTP : 25

(DNS)TCP /UDP : 53

Oracle/RDS : 1521

FTP : 21

33. What are diffrerent EC2 Instance types?

Ans : 

34. Steps to download S3 bucket using CLI?

Ans : Step1 : download AWS CLI from below link :

Download the AWS CLI MSI installer for Windows (64-bit) from

<https://s3.amazonaws.com/aws-cli/AWSCLI64PY3.msi>

Step2 : After download install the CLI and after installing try this following command to check CLI works or not :

# aws --version

Step3 : Now Create IAM user with Admin permission or with S3 full access permission and save the Credentials.csv file.

Step4 : Now Write the following command to fillup the details :

# aws configure

Step4 : Now you will see following details to fillup as follows :

AWS Access Key ID : AKIAW6IGNZJ3Z4UDC4G6

AWS Secret Access Key : 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

Default region name : us-east-1

Default output format: text

Step5 : Now write the following command to sync with aws:

# aws s3 sync s3://portfoliomy1 C://shubhu

OR

# aws s3 cp s3:// portfoliomy1 C://shubhu

The above commands download all the buckets present in AWS to shubhu folder.

35. Steps to create EC2 instance using CLI?

Ans :

# aws ec2 run-instances --image-id ami-0323c3dd2da7fb37d --key-name myone --instance-type t2.micro --region us-east-1 --subnet-id subnet-2816ce26 --count 1

35. What is Launch template in EC2?

Ans : In Launch Template , we define all the required configurations like AMI , Security groups , Subnets , VPCs , Volumes, Keys etc to create an instances.

When we want to create an instances, we can use the Launch templates, this helps us to minimize the work. Earlier when we have to launch the instances , we have to select the AMIs , SG, Volumes , Keypair , etc .

35. Explain AWS EC2 Pricing models?

Ans : AWS offers primary 4 pricing models :

1. Spot Instances :

Spot instances are used when you want to decrease the price of your instances and you can’t afford the instances prices. .

Spot instances are identical to a normal EC2 instance, except for two things. First, spot instances use a different billing model than a regular EC2 instance does. The other difference is that spot instances are subject to interruption. Therefore, you should not use spot instances for running workloads that are mission-critical. Spot instances tend to be useful for dev/test workloads, or perhaps for adding extra computing power to large-scale data analytics projects.

 In actuality, spot instances do not use flat-rate billing. Instead, AWS calculates a cost for spot instances that is based on supply and demand. As the demand for compute resources increases, spot instance costs also increase. As demand wanes, the cost of a spot resource decreases.

The key to understanding spot instances is to look at the way that cloud service providers such as Amazon Web Services (AWS) operate. Cloud service providers invest in hardware resources and then release those resources (often on a per-hour basis) to subscribers. One of the problems with this business model, however, is that at any given time, there are likely to be compute resources that are not being utilized. These resources represent hardware capacity that AWS has paid for but are sitting idle, and not making AWS any money at the moment.

Rather than allowing these computing resources to go to waste, AWS offers them at a substantially discounted rate, with the understanding that if someone needs those resources for running a normal EC2 instance, that instance will take priority over spot instances that are using the hardware resources at a discounted rate. In fact, spot instances will be stopped if the resources are needed elsewhere.

Spot Instances are available at a discount of up to 90% off compared to On-Demand pricing.

Spot instances are recommended for:

* Applications that have flexible start and end times
* Applications that are only feasible at very low compute prices
* Users with urgent computing needs for large amounts of additional capacity

2. On-Demand : With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

EC2 on-demand is the most expensive option of the three.

On-Demand instances are recommended for:

* Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
* Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
* Applications being developed or tested on Amazon EC2 for the first time

3. Reserved Instances : This option consists of an upfront financial commitment for 1 or 3 years of EC2 usage which in turn provides users with guaranteed capacity for the instance type selected. Savings compared to on-demand are roughly in the 75% range. However, reserved instances create financial lock-in, so if you don’t use what you committed to, you could potentially end up with a negative ROI.

4. Saving Plans : This option is similar to reserved instances in the commitment terms of 1 or 3 years, but   does not require you to select a specific instance and rather can be applied to any EC2 instance (as well as other AWS services). For example, you can commit to spend a desired amount per hour, e.g. $35/hour, for either 1 or 3 years. Anything spent up to $35 will be charged in accordance with Savings Plans rates (between 66-72% savings). Any spend above the committed amount will be charged at On-Demand rates.

35. ?

Ans :

**AWS Scenario's:**

**3. How do you configure CloudWatch to recover an EC2 instance?**

Ans : Here’s how you can configure them:

a) Create an Alarm using Amazon CloudWatch

b) In the Alarm, go to Define Alarm -> Actions tab

c) Choose Recover this instance option

**8. How would you handle a situation where the relational database engine crashes often whenever the traffic to your RDS instances increases, given that the replica of RDS instance is not promoted as the master instance?**

Ans : A bigger RDS instance type needs to be opted for handling large amounts of traffic, creating manual or automated snapshots to recover data in case the RDS instance goes down.

**10. I created a key in North Virginia region to encrypt my data in Oregon region. I also added three users to the key and an external AWS account. Then, to encrypt an object in S3, when I tried to use the same key, it was not listed. Where did I go wrong?**

Ans :The data and the key should be in the same region. That is, the data that has to be encrypted should be in the same region as the one in which the key was created. In this case, the data is in Oregon region, whereas the key is created in North Virginia region.

14. How to install nodejs on Amazon linux EC2 Instance ?

Ans :

Step 1 : # sudo yum install –y gcc-c++ make

Step 2 : # curl –sL <https://rpm.nodesource.com/setup_14.x> | sudo -E bash –

Step 3 : # yum install –y nodejs

Step 4 : check nodejs version & npm version using # node -v & # npm –v

Step 6 : Now, to create Demo web server : create a nodejs script file like “ home.js ” and Write the code into it.

13. How to install MongoDB on Amazon linux EC2 Instance ?

Ans :

Step 1 : Create a file # vi etc/yum.repos.d/mongodb-org-3.0.repo

& Write following code into it :

[mongodb-org-3.0]

name=MongoDB Repository

baseurl=https://repo.mongodb.org/yum/amazon/2013.03/mongodb- org/3.0/x86\_64/

gpgcheck=0

enabled=1

Step 2 : # yum install –y mongodb-org

Step 3 : # service mongod start

Step 4 : # mongo

Step 5 : > use shubham (to create database)

Step 6 : > show dbs (to show database)