There are totally 6 types of engineering

1.Server Engineering

2.Database Engineering

3.Application Engineering

4.Middleware Engineering

5.Storage Engineering

6.Security Engineering

Cloud computing:

In simple terms its just accessing a remote server and working on that.

To know the regions where aws infrastructure is available :

<https://aws.amazonproducts>

How to create EC2 Instance:

We can create different types of machine

Windows

Linus

Ubuntu etc

To launch a windows machine:

->Click on the EC2 service

->Click on the free tier eligible windows machine

->T2.micro is the 1 GB Ram and free tier eligible.

->Add network Configurations(yet to take)

->After add the protocol(https or http)

->After launching the machine we have to generate the key pair

->\*create a new key pair

->give the name of the new key pair and download the key pair

->We will get one .pem file .

Now to login to the machine

->Ckick on the ec2 machine and it will show the IP address

->click on connect

* We will get the uname and decrypt the pwd
* Now we can get the pwd and login into windows machine.
* Same steps should be followed for linux machine.

Application engineering :

It the combo of Developer-code-server(web/appli) -user

Code is the dormant data

Application is the active form of dormant data

What is middleware:

Middleware consist of following components

1.Webserver apache,IIS,IHS

2.application server - JBOSS,WAS,WEBLOGIC

3.Data Power -is used for security and transaction spped

4.Message queueing is for passing messages bw two applications-WMQ,MSMQ,Tabbit snake etc

5.Message brooker – WMQ(acts as a translator)

Webserver is used for hosting application. Any application will be hosted over a server.

WAR: Web Archive: file is used for applications that contain only presentation logic ie only look and feel applications . For example : [www.greenstechnology.com](http://www.greenstechnology.com) website which will show only the presentation.

EAR : Enterprise archive: This contains both business logic and presentation logic for eg: Banking applications.

Creating a Linux Machine:

The same procedures are followed as in windows machine creation. But the last step when we create a pem file it should be converted to ppk file(putty private key) and it should be pasted in the auth. The user name will be ec2-user.

So once the machine is created in order to view the services running the machine just type the host name(IP address) and search.

Now we have to enter the machine using putty, and we have to switch as root user and later we can add as many user we want.

As a root user we have to user this ppk file to login whereas for the additional users we create we can give the pwds.

UBUNTU Machine:

Same procedure is followed for ubuntu machine whereas user name is “ubuntu”

How to install java in ubuntu machine :

1.Java binary download-Repository pulling

2.Environment update

3.Java install(jdk1.8 is recommended)

4.Check version

How to install Jenkins

1.Jenkin key download

2.mentioning the jenkin binary url into the file Jenkins.list

3.update the environment

4.install the Jenkins

Verification of Jenkins:

Default port number of Jenkins 8080.

\*Once the jenkin is install login into jenkin using IP:8080 in browser.

\*We will directed to a page here it will ask for initial password.

\*In the same page will have the path for initial pwd so take the path and run it in ubuntu machine.

\*We will get the initial pwd. So after that we will be setting the new pwd and once this pwd is set we wont be able to see the initial pwd. Process ID ensures that Jenkins is installed in the machine.

Jenkins:

In order to create a new job create a new item

Give the name of the project and we can do some shell scrits or we can configure what the job needs to be done.

Similarly we can create multiple jobs.

We can also schedule the jobs to run in some particular time.

We can also queue the job.

For eg: we are creating 3 jobs

1.Dev 2.Pstage 3.Prod

We can schedule like once dev should run first and then pstage and then prod.

Inorder to schedule open the job , Go to configure, go to post build actions and type the name of the successor job.

Inorder to schedule the job, go to the job and configure post build actions.

Role nased strategy is helpful for managing multiple users with different levels of permission.

To get that feauture we need to install specific plugin called as Role based strategy which we can download from manage Jenkins.

Enable role based strategy in configure security roles.

Restart Jenkins

Now go to manage Jenkins-> Configure global security->Authorization->select role based strategy

Now again manage Jenkins and there you will find a new option regarding role based security .

There you can configure

Jenkins CLI:

In order to work in Jenkins CLI we need to download the corresponsing jar.

Once the jar is downloaded we need to paste the jar in the server.

We need to go to manage Jenkins and there we have CLI option. There we can find the commands that we can use on putty.

In This the role based strategy has some vital role to play. So please browse on that part for more information.

During the training they changed the role based security as anonymous user can do anything and then they interacted with putty to restart the machine.

Vpc:

It is mainly used for security purpose.

Two type of vps are there

->Public vpc

->private vpc

It enables you to launch aws resources into a defined virtual network and gives complete control over the network. It is logically isolated from other virtual n/w in AWS cloud.

VPC-> Intergnet gateway->public n/w ->customer gateway ->branch officers

Benefits of VPC:

Launch instance into a subnet and define a ip address range inside each subnet .

Configure route table b/w subnets, which will create layer of n/w’s.

Subnet: breaking of big address into smaller ones.

Values of subnets: /8 =>1 lakh ip address

/16 => 65536 ip iddress

/24=> 256 ip address

Whatever be the values of subnets 5 ip’s will not be used.

Subnets:

A portion of nw that shares common address component, which will divide longer ip address into small small chunks.

IP Addressing:

**Private :**

Its not reacheable over the internet.

It can be used for communication bw instances in vpc.

**Public:**

They are reacheaable over the internet

It is used for communication between your instances and the internet or with any other aws services that has public end point.

**Security group VPC:**

-It acts as a virtual firewall for your instances to control inbound and ooutbound traffic.Security group acts at the instance level and not at subnet level.

**Components of vpc:**

**VPC ->IP Addressing -> Route table**

* **Public and private subnet- > access control list**
* **Nat instance and gateway and vpc peering**

**Route table :**

**Route table contains set of rules called routes, that are used to determine Where n/w ttraffic is directed.**

**ACL: Its an optional layer of security that are used to determine where the traffic is in and out of one or more subnets. ACL has separate inbound and outbound rules and each rule can either allow or deny the traffic.**

**NAT Device:**

**N/w address translation. It forwards traffic from instances in private subnet to internet and sends response backs to instances**

**Internet gateway:**

**It allows communication between instanes in your vpc and internet, which imposes no availability risk.**

**Steps for creating public subnet :**

**Create a vpc and name it as Maruti vpc whose ip range is 10.50.0.0/16 and enable DNS hopst name on vpc.**

**Create a subnet and enable auto assign ip**

* **Webserver 10.50.1.0/24**
* **App server 10.50.2.0/24**

**Create IG and attach to vpc.**

**Use default route table and subnet to it, to send the traffic outside vpc.**

**Deploy vm 1 in ap south 1a and other in ap south 1 b and check their communication.**

**Pracs:**

**\*Go to vpc**

**\* once vpc is created right click on vpc nd yu can fine DNS hostname .**

**\*Enable DNS hostaname.**

**\*Click on the vpc and check the availability zones.**

**\*create two subnet. Now we are creating (10.50.1.0/24)and (10.50.2.0/24)**

**\*right click on the Subnet and enable Auto assign ip.**

**\*create an IGW . This IGW will be in detached state so we have to attach it to VPC.**

**\*for pubic we we can use default routetabel**

**\*click on subnet association and edit subnet association and add**

**\*Route table , do to edit route and add default ip for outbound.(0.0.0.0.)**

**Deletion :**

**Instance -Subnet- IG and -VPC**

**Nat Gateway :**

**In Nat gateway we have to cffreate new EIP and in subnet column give public subnet.**

**Don’t fprget to edit subetassociation.**

**To connect to another machine :**

**Ssh ec-2user@IP**

**But we will not have permission so we shud give the pem file .**

**Ssh -I pemfilename ec2-user @IP**

**Amazon S3:**

**Simple storage service.**

**It is a cloud storage which allows you to use the server or app without any need to attach to server. I e kind of invisible storage**

**Storage will be mirrored and copied to two dif data centres or in different zone to provide secured access(R-W-X) permission to the users.**

**General URL:** [**http://Bucket-s3.amazon.aws.com**](http://Bucket-s3.amazon.aws.com)

**If it’s a region specific:**

[**http://bucket.s3-awsregion.Amazon.aws.com**](http://bucket.s3-awsregion.Amazon.aws.com)

**s3 has wide variety of property, Mainly we will use versioning and static website hosting which enables you to have a history of files to save it in your database.**

**Bucket name must be minimum 3 character and not more that 64 character.**

**Name must be unique and bucket name should not be started with upper case letter.**

**Bucket name can contain lower case letter , numbers and hifen.**

**Maximum 100 buckets can be created per user.**

**You cannot transfer ownership of the bucket.**

**Yu can store unlimited number of objects in s3 bucket.**

**You cannot create bucket within another bucket.**

**S3 storage classes(Life cycle management):**

**\*S3 standard access**

**\*S3 standard infrequent access**

**\*Reduced redundancy storage**

**\*Amazon Glacier**

**Standard frequent access:**

**It stores frequently accessed data with high availability and durability.**

**It has the property of low latency and high throughput. (Eg Mobile apps)**

**Standard infrequent access:**

**It is designed for objects that are accessed less frequently with the rapid demand access for low cost per GB retrieval file.**

**Reduced redundancy storage:**

**Noncritical data at lower cost, designed for object that are reproductive.**

**Amazon glacier:**

**Designed for archiving, rarely accessed data with longer retrieval time and low cost availability. It is also called secured wallet locker.**

**ARN: Amazon resource number.**

**This is for the bucket identification.**

**Creation of bucket**

**Public permission for the bucket and public permission for content.**

**Life cycle management**

**Elastic Block Storage:**

**\*It is a distributed block data store that is optimised for consistency and low latency.**

**Features of EBS:**

**\*It has persistent storage whose storage volume varies from 1gb to 1tb with high performance and reliability**

**Create volume ->It will come to available state->attach to instance->snapshot->delete.**

**AMI=> Amazon machine image.**

**It is used to clone the entire machine whereas snapshot will clone only a particular resource like volume.**

**Types of EBS:**

**\*General purpose SSD(Mostly frequently used used)**

**\*Provisioned IOPS(input Output Processing speed)**

**\*Magnetic SSD(100 IOPS Processing speed)**

**\*Cold HDD(Hard drive disk)**

**\*Throughput optimised HDD(The cheapest one)**

**General purpose:**

**It has 3000IOPS processing speed where the life time will vary with high availability and low latency.**

**Provisioned IPOS:**

**It has 4000 IOPS processing speed with additional 1000 IOPS with stable life time volume.**

**Magnetic SSD:**

**Low cost per GB , data availability with 100 IOPS speed.**

**In EBS:**

**Volume -> create volume->If we have snapshot we shud give the snapshot ID->Encryption is done with kms**

**Command : lsblk =>Long list the background running task.**

**Even after attaching the volume we should mount the volume to filesystem.**

**I node: recovery of your damaged file.**

**Mkfs.ext4 /dev/xvdf=> making the file system ready**

**Now we need a directory to mount the file system.**

**Mkdir /app**

**Mount -t ext4 /dev/xvdf /app**

**Elastic Load balancer:**

**It belongs to networking group. It is usually route incoming request to multiple Ec2 instances.**

**It can easily configured with FTP and SFTP. It support both public and ip addresses. Doing the health check of the server ois the moto of ELB.**

**4 component:**

**1.response time**

**2.Interval time**

**3.Healthy threshold**

**4.Unhealthy threshold.**

**Browser->origin server->customer**

**From browser to customer , the time window used is interval time.**

**Browser to customer, its response time and depending upon the response time we will decide healthy or unhealthy.**

**Thisworks on round robin algorithm. It will maintain a detailed report for yur health check.**

**Autoscaling:**

**It is used to maintain app availability by scaling up/down your Ec2 instances automatically based on high/less loads. It ensures you have desired no of ec2 instaces.**

**Two main steps:**

**1.Launch configuration**

**2.Autoscaling groups**

**SNS:**

**Simple notification service. Its called as push model by sending notifications to customer by email, sms , and many mediums.**

**Cloudwatch:**

**It is a monitoring tool. It is used to set alarm and monitor all your log files and send alert to customer. It is also called as pull model.**

**Cloud Trial:**

**It is used to keep a track of audit log files API call interfaces by maintaining track of , how much information is passed from origin to destination.**

**IAM-Identity Access Management.**

**It is a web service that helps you securely control access to AWS resources for your users.You can use IAM to control who can use your resources and what resources they can use.**

**Utility of IAM:**

**Admin-> will be granting permission to the users**

**Developer-> Graphics module will be assigned to a developer.**

**BA(Bussiness analyst)->Who handle analytics module of the company infrastructure.**

**Components of IAM:**

**\*Users**

**\*Group**

**\*Roles**

**\*policies**

**Two types of acess:**

* **Management console access ->Conventional method of logging in with uid and pwd.**
* **Programmatic access -> Pwd will be in encrypted type(Used mainly for Multi factor authentication)**

**You can create and manage AWS resources where they allow /deny their authentication.**

**IAM defines set of permissions AWS service requests.**

**IAM roles are not associated with specific users or group but instead trusted entities assume roles(Apps or user level authentication).**