* **What is cloud?**

A cloud is a distributed collection of servers that hosts software and infrastructure, and it is accessed over the internet.

A cloud computing refers to delivery of various services over the internet.

Basically the cloud represents network pf servers, databases, software and infrastructure hosted and managed by cloud providers such as (AWS ,GCP ,Azure)

* **Public vs Private cloud:**

In a public cloud, resources such as (servers, storage and networking) are shared multiple users, often refers to as ‘tenants’. Public cloud services are managed by third party providers such as (AWS,GCP, Azure) .

A private cloud is dedicated to a single organisation It can be hosted on premises ( within companies data centre) or by third party provider but isolated from other users.

**Public Cloud Private Cloud**

Multi- tenancy Single-tenancy

Cost effective Higher cost

Shared infrastructure one organisation

Medium security as provider High security as user

Manages it Controls and manages.

Pay- as-you go & affordable. Higher charges

Limited customization High customisation

Managed by provider Managed by organisation or

Third party.

* **AWS IAM (Identity And access Management)**

IAM is solving problem of authentication and authorization.

* **Authentication :-**

- It is a process of verifying who a user is.

- typically means confirming the identity of user

- it verifies user credentials like username & password.

* **Authorization**

- Authorisation happens after authentication and determine what actions the authenticated user can perform in application.

- as admin have access to create, edit or delete user while regular user can only view content.

* **IAM USER :-**

Allows the creation of individual IAM user within an AWS account. Each user has unique security credentials and can be given specific permissions. creates users and given permissions to access in applications.

* **IAM Policies :-**

This IAM policies defines permissions and can be attached to users , groups or roles. Policies use Json format to specify actions ( eg. S3:Listbucket), resources and conditions for access.

* **IAM Groups :-**

We can organise users into groups and manage permission for groups rather individual user. this makes easy to apply permissions to multiple users. A group is a collection of users and a single person can be a member of several groups.

* **IAM Roles :-**

IAM roles allows you to assign permissions to a AWS services applications or user in a temporary and secure manner useful for scenarios like cross account access or service-to-service communications by using roles, we can provide AWS Service access to other AWS services.

* **For USER:- (IAM)**

Fill user details > username> access to console> Autogenerated password> user must create new password for next sign in> next.

Set permissions> next with default

Download .CSV file which have info of username, password and console sign in URK

Account id is in URL (12digits id)

You can change the permissions any time as root users.

* **For Groups :- (IAM)**

User groups>create group>fill details add user> attach permission policies.

* **EC2 :- (Elastic cloud compute)**

EC2 instance provides computing capacity in the cloud.

EC2 Is nothing but the virtual server you are asking for.

It helps to create virtual servers called ‘instance’.

EC2 instances are flexible and can be quickly scalled up or down based on needs.

Fully maintained by AWS And pay-as-you-go model.

^

Popularity reasons.

* **EC2 instance Types :**

1. General purpose instances :

Balance performance at variety of applications, including web servers, code repositories and general purpose apps.

Eg. T series (T3, T3a ,T4g) M series (M5, M5a, M6g)

1. Compute optimized Instance :-

Designed for compute- intensives applications requiring high-performance processors.

Eg. C series (C5, C5a , C6g) : ideal for CPU Bound task.

1. Memory Optimized Instance :

Optimized for memory- intensive application such as high-performances databases , in memory caching and big data processing.

Eg. R series ( R5, R5a ,R6g)n memory intensive work.

X series : optimized for large scale

Z1d series : high memory with high CPU, Frequency.

1. Storage optimized Instance :

Designed for I/O intensive application that require high sequential read and write access to large scale set.

Eg. I series (I3, I3en)

D Series (D2)

H series (H1)

1. Accelerated Computing Instance :

Equipped with hardware accelerator =s , such as GPU’s FPGA’s Foe high performance computing tasks . AI/ML and graphics-intensive applications.

Eg. P series (9P3,P4)

G series (G4, G5)

F series (F1)

* **Regions and availability zones:**

Region is a geographical area where AWS has data centre for avoid latency in request Scenarios. we choose region as near as possible.

for one region there are multiple data centres called as availability zone.

suppose you have a client from Europe so far fast data processing can avoid latency you will choose the region as Europe and respective ability zone.

Search EC2> Instances> launch instance> fill info. Launch instance.

Use SSH Command to join with EC2 or putty or mobaxterm.

* **VPC : (Virtual private cloud)**

A VPC is a private network environment within a public cloud. It allows you to define and control a virtualized network in a secure, isolated segment of the cloud provider infrastructure VPC’s are commonly used to set up secure environments for applications databases and other services in cloud, allowing organisation to enjoy the benefit of cloud resources while maintaining strict network controls.

1. **Subnet:-**

(Subnetwork) is a segment within BPC that divides the network into smaller network and each subnet has its own IP address range and can be configured as public or private subnet.

1. **Public subnet:-**

(It is a subnet having public IP address and are accessible from the Internet.)

1. **Routing tables:-**

A routing table is a set of rules used to determine where network traffic is directed within UPC each subnet is associate with a crowding table.

1. **Internet Gateways:-**

It is a component that allows communication between resource in vpc and the internet. (specifically, in public subnet to internet connection).

1. **NAT Gateway** :- (Network Address Translation Gateway)

NAT allows instances in a private subnet to initiate connection to the outer Internet, while preventing internal internet connections from reaching outside.

NAT Gatewayis a door that makes subnet in a vpc can access content of outside but any outside are not able to access that subnet.

1. **NACL (Network Address Control List) :-**

NACL is a stateless firewall that controls traffic at the subnet level. Each subnet have only one in NACL associated with it, NACL has a set of rules that allows or denied traffic based on ip address protocol or part.

1. **Load Balances :-**

Load balances distribute incomming traffic across multiple instances increasing reliability and performance.

AWS elastic load balance.

1. **Security Groups:-**

Security groups acts as a stateful firewall for resources in VPC. They control inbound and outbound traffic at the instant level based on rules you define.

* **AWS Security groups and NACL**

1. Security groups operate at the instant label each instant within VPC associates with multiple security groups.
2. security groups are stateful as if you allow inbound traffic on a specific part then outbound traffic automatically allowed further connection.
3. security groups don’t have rules number and evaluate all rules at once if no rule match the traffic is denied.
4. by default sg deny inbound traffic by default but allow all outbound traffic.
5. ideal for instance specific access control.
6. NACL operates at the submit level they control traffic entering and exiting a subnet.
7. NACL are stateless if you allow inbound traffic on part then you must explicitly allow outbound traffic on that part as well each request and responses evaluated independently.
8. NACL use numbered rules which evaluated in order once a rule matches the process stops.
9. by default NACL deny all inbound and outbound traffic requires rules to permit specific type of traffic.
10. NACL are useful for broad control at subnet level.

Practically, NACL and SG can be used together for layered security where NACL provides broad network key level control SG provides more specific instance level control.

* Practice:

VPC> create VPC> VPC& more > fill info. Check network ACL’s and security groups.



Subnet (logical nw within VPC)



NACL (subnet level firewall)



Instance A



(Specific IP)



SG Instance EW



* **Route 53 :**

DNS : (Domain name system)

DNS is fundamental protocol on the Internet that translates human readable domain names into machine readable IP address.

Eg. for examplemazon.com>192.0.2.1

Route 53 scalable domain name system DNS web service provided by AWS that is used to domain registration DNS routing and health checking.

Primary features and components of route 53:

* 1. Domain registration

route 53 allows you to register new domain and manage Them in AWS.

* 1. DNS Reading:

used to direct user traffic based on different policies ensuring that request reaches the correct server or resource.

* 1. Health Cheques:

route 53 automatically routes traffic away unhealthy endpoints

* 1. Integration with AW services:

route 53 integrated with elastic local balances elb cloudfront, EC2,S3 and VPC. hence easy to way to manage all network settings in one place.

**Key use of route 53:**

1. Directing web traffic to application hosted in AWS.
2. Implementing disaster recovery by routing traffic away from failed resources.
3. Optimising performance through intensity based and geolocation routing.
4. Providing global DNS service with built in security and DDOS protection analysis.