**AWS CONCEPTS**

Diagram

Description automatically generated

VPC is bound to a region, subnet is bound to availability zone

By default vpc has a default route table where it has routes to all it’s subnets. Subnet to subnet communication within a vpc is allowed by default (until there is a rule in sg to stop the communication between resources)

**CALCULATING cidrs :**

url : <https://matt-rickard.com/how-to-calculate-a-cidr/>

<https://erikberg.com/notes/networks.html>

/32 = 1

/30 = 32-30 = 2\*2 = 4

/29 = 32-29 = 2\*2\*2 = 8

/28 = 32 -28 = 2\*2\*2\*2 = 16

Table

Description automatically generated

30 = 8+8+8+6 =

29 = 8+8+8+5

28 = 8+8+8+4

26 = 8+8+8+2

**AWS**

**Resources:**

**S3, EC2, ECR, EKS, IAM, VPC**

**What is VPC?**

Virtual private cloud – This is the private network space within the AWS cloud where we can launch our resources. This will isolate our resources from other virtual networks.

It gives u a similar env as our private data centre.

VPC is region specific.

­­­­­­­

**What is Subnet?**

Subnet is part of ur vpc, where u can have a set of ips blocked for ur subnet from vpc ip range. This is also like grouping the resources (n/w inside n/w) but u can place in subnets based on requirements like if u want it to be accessible via internet place it in public subnet otherwise private.

Subnet is AZ specific

**What are the components of VPC?**

**VPC –** isolated network space

**INTERNET GATEWAY –** allows vpc to connect with internet

**SUBNET –** part of vpc

**NAT GATEWAY –** allows internet connection in private subnets

**VIRTUAL PRIVATE GATEWAY –** aws side vpn

**CUSTOMER GATEWAY –** users side vpn

**ROUTER -** Routers interconnect subnets and the direct traffic

**How to build a custom VPC?**

**What is the difference between security groups and network ACL’s ?**

Security groups in a VPC mention which traffic is allowed to or from an Amazon EC2 instance. Network ACLs operate at the subnet level and evaluate the traffic that is entering and exiting a subnet. Network ACLs can be used to set both Allow as well as Deny rules. Network ACLs do not filter traffic between the instances in the same subnet.

**Why security groups are stateful ?**

any rule that allows traffic into an EC2 instance, will automatically allow responses to pass back out to the sender without an explicit rule in the Outbound rule set

**What are route tables?**

A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic from your subnet or gateway is directed.

Each subnet must be attached with route table and this will control on where the traffic flows from your subnet. We can explicitly attach a route table or it will be associated with default main route table.

Subnet can have only 1 route table at a time and whenever a vpc is created it will have a main route table created and attached by default.

**What is VPC PEERING ?**

VPC peering is to allow resources in 2 vpc’s to communicate with each other as if they are same network. We can create vpc peering between vpc’s in 2 accounts or vpc’s in 2 regions.

First requester should initiate the peering request

Then vpc peering connection will be in pending acceptance state. The accepter vpc should now accept/reject the peering. Once after accepting it will go into provisioning state.

If u see the state is active then the peering connection is established

Now we have to attach the peer vpc cidr range to route tables in-order to allow the communication

Also modify the sgs if it is blocking any of the routes of peer VPC.

**What is AWS VPN?**

VPN creates secure link between your vpc and on premises network. You can connect with private ip of vpcs if u have vpc connection.

**What is NAT gateway ?**

It is a highly available AWS service that allows an instance in private subnet to communicate with internet.

It acts like a router b/w internet and the private subnet.

A public IP is assigned to the NAT gateway instance instead of attaching public ip to each EC2 instance in private subnet.

When ever the instance in private subnet wants to communicate with internet it goes through the NAT public ip.

[**https://www.youtube.com/watch?v=FTUV0t6JaDA**](https://www.youtube.com/watch?v=FTUV0t6JaDA)

**What is internet gateway ?**

This is the component that allows communication between VPC and internet.

Performs n/w address translation for public instances.

Horizontally scaled, redundant and highly available

It is a s/w component ( not a physical device)

1 VPC - 1 IG

Different than NAT gateway

**What is Transit Gateway?**

A *transit gateway* is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks.

**Steps:**

Create a transit gateway first

Attach your VPC’s through the transit gateway attachments

Add routes between the transit gateway and vpc

Share the transit gateway resource using RAM with other accounts if we want to attach vpcs from multiple accounts.

**What is Loadbalancer ?**

Load balancer will distribute traffic among servers in backend. This gives a better performance as load is distributed also gives high availability.

Types of load balancers in AWS –

**CLB –** classic load balancer is old generation(v1) lb which is deprecated now.

**Application load balancer** – works on layer 7 – https/http.

Load is balanced based on route. Client ip is not known to the application servers.

Client request reaches alb then connection is terminated and a new connection is initiated by alb to application server.

After the load balancer receives a request, it evaluates the listener rules in priority order to determine which rule to apply, and then selects a target from the target group for the rule action.

Graphical user interface, application

Description automatically generated

Diagram

Description automatically generated

How it works?

Create target groups first

Create alb by registering the target

Now we can go to listeners and edit/add the rules.

­­­­­­­­­­­­­­­

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

url: <https://www.youtube.com/watch?v=JhH7epqrvF0>

**Network load balancer –** TCP traffic - 4th layer of osi model(network layer)

Diagram

Description automatically generated

Health checks are crucial for a lb. they enable the lb to know if they can route traffic to that instance and whether it is healthy or not.

It is done on port : 4567 route : /health

How NLB works:

Loadbalancer : this is the single point of contact for users

Listener : This listens to the client request and based on protocol u configure it will redirect traffic to the target group.

Target groups : we register ec2 instances as targets where our actual application is running.

Steps to create nlb:

First create target group

To create lb choose lb type as nlb

Leave listener at default settings with tcp 80

**What is s3?**

Amazon S3 is an object storage service that stores data as objects within buckets. An *object* is a file and any metadata that describes the file. A *bucket* is a container for objects. S3 is globally accessible.

A bucket is a container for objects stored in Amazon S3.

Objects are the fundamental entities stored in Amazon S3.

An *object key* (or *key name*) is the unique identifier for an object within a bucket. Every object in a bucket has exactly one key. The combination of a bucket, object key, and optionally, version ID (if S3 Versioning is enabled for the bucket) uniquely identify each object.

aws s3api put-object --bucket cyclones-terraform-state-2 --key env:/fit4/forgerock\_access\_manager\_backup --body /Users/m1055938/Downloads/forgerock\_access\_manager.json

A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy that you can use to grant access permissions to your bucket and the objects in it.

You can use ACLs to grant read and write permissions to authorized users for individual buckets and objects.

**Storage class:**

Amazon s3 standard for frequent data access

Amazon s3 standard for infrequent data access

Amazon Glacier

One zone-IA storage class

Amazon s3 standard reduced redundancy storage

**FEATURES:**

**Life cycle rules:**

We can create life cycle rules to move buckets from one storage class to another based on conditions.

**Bucket Policy:**

Allow or deny access to the s3 resources

**Versioning:**

Goto properties and we have bucket versioning section there click on enable

**AWS MONITORING**

**Difference between AUDIT and MONITORING:**

Audit means to verify who is doing wat

Monitor means to check if system is working as expected

**What is AMAZON CLOUD WATCH ?**

Cloud monitoring is required in order to detect early failures of systems, improve the performance by using metrics etc.

Amazon cloud watch is 1 such amazon service which monitors various aws resources and customer applications running on cloud.

2 levels of monitoring :

Basic monitoring : monitored less frequently (every 5mins) with limited range of metrics

Detailed monitoring : monitored frequently (every 1min) with wide range of metrics

**NAMESPACE :**

Namespace is a container for cloudwatch metrics. AWS/service

Eg: AWS/EC2 namespace

**METRICS :**

This is the fundamental concept. “Variable to monitor” is metric.

CPU usage of ec2 is a metric.

Metrics are uniquely identified by name , namespace and 0 or more dimensions.

**DATAPOINTS:**

Values of that variable over time is datapoint.

We can send our own custom metrics to cloudwatch and add datapoints in any order and at any rate of our choice.

NOTE: Metrics exist only in the region it is created they are completely separate between regions.

**STATISTICS :**

Datapoints as an ordered set of time-series data.

**TIMESTAMP:**

We can create time stamp for metrics. It can be upto 2 weeks past and 2hrs future.

Date+hrs+mins+seconds

**CLOUDWATCH ALARMS:**

It can be created to watch single cloudwatch metric or for a result of a math based on cloudwatch metrics.

States of alarm :

OK – metric is within defined threshold.

ALARM – metric is outside defined threshold

INSUFFICIENT\_DATA – alarm has just started, or there is no enough data of the metric to determine alarm

**Features**:

Collect

Monitor

Act

Analyze

Compliance & Security

**How it works?**

Diagram

Description automatically generated

**What is aws sns ?**

It is simple notification service and a managed service that provides message delivery from publishers to subscribers.

Publishers are also known as producers that produce and send the message to the SNS which is a logical access point.

Subscribers such as web servers, email addresses, Amazon SQS queues, AWS Lambda functions receive the message or notification from the SNS over one of the supported protocols (Amazon SQS, email, Lambda, HTTP, SMS).

Topic is used to filter out the messages that have to be sent to different subscribers.