ID :837279786

15 -10-2019

**Security Groups :**

Go to inbound of the particular security group – give security group as ICMP – any where - then ping should work from the IP ( typed public IP)

If I am unable to ssh then check outbound

Ec2 is piniging google then outbound ( it is safe to have ec2 from out bound ) but it is not safe to have inbound to ec2 from any where

* Every ec2 must have one security group,( max is 5
* Multiple ec2 instances can have same security groups ( ex: we have web site running on 100 servers they can have same security rules)
* Every ec2 can have max 5 security groups for ENI ( elastic network interface )

Security group source :

Option 1 : My ip – it will automatically picks u r current laptop

Option 2:Any where : any one can connect from any lap

Option 3:Custom :

I) in custom we can have Cider blocks ( cider block represents N/w)

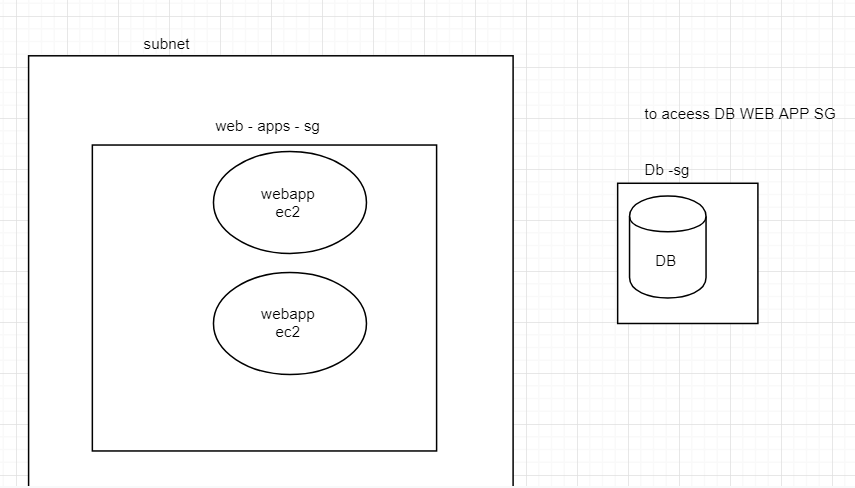
II)under cider blocks Ip adresees

iii)Source can be security group ( ec2 instances having this security group can be ssh)

If we put security group source , it means all ec2 instances have that security group is allowed

SSH – should not be any where It should be Custom

HTTP may be from anywhere it depends

,

In the above fig DB is in private subnet , my ec2 is in public subnet if my ec2 instances wants toa cess DB then how to configure security grps .

If I give ip address of each ec2 instances when I increase my ec2 instances we need to give those many Ip adresses (as inbound to acess DB)

In such cases I give security groups of the web apps in **db source.**

--------------------------------------------------------------------------------------------------------------------------------------

**NACL :**

It is a virtuall firewall which secures subnets

It has inbound/outbound rules

Nacl’s are **stateless**. (i.e inbound traffic

One subnet must have one NACL

Multiple subnet can have same NACl \*D

Nacl has explicit allow/deny ( i.e if we want to block all traffic from specific source we can do it.

**Understanding NAcl rules :**

**Every** rule must have unique rule number

Rules are executed in ascending order

When a matcing rule is found the action against that rule is applied ( i.e if it say allows it allow else if it says deny it deny )

When matching rule is found that rule is applied it wont go to next rule.

Note : Give sufficient spaces between rule numbers. ( ex : have rule numbers like 100 , 200 , 250)

**Default NACL :** This is implicitly created when VPC is created and by default all subnets are associated to Default Nacl

By default, default nacl allows all inbound & outbound ( when u create vpc default nacl cretates \*D ( subnets uses Nacl obviously ec2 instances uses (for my clarify \*D)

Along with default we can maintain custom Nacl’s.

Default rules of custom nacl is deny all inbound & outbound.

17-10-18

Czlb: (cross zone load balancing)

If web server is storing stay of a client then stickiness is required ( ex ; amazon cart products are stores in web server)

By default it is enabled , if enabled every Ec2 gets same amount of load

If disabled every zone gets same amount of load

( if zone 1 is having 10 ec2 , and zone 2 is having 5 ec2 if enabled every ec2 gets same traffic , if disabled 50 % of traffic gets to zone1 and 50% of traffic gets to Zone2)

ALB : ( Application load balancer)

* Used for Microservices applications
* It has path based o/p.
* The traffic based on a path and port

**IQ)**

We want to Load balancer which does routing based on a path and port

we have to use ALB/NLB

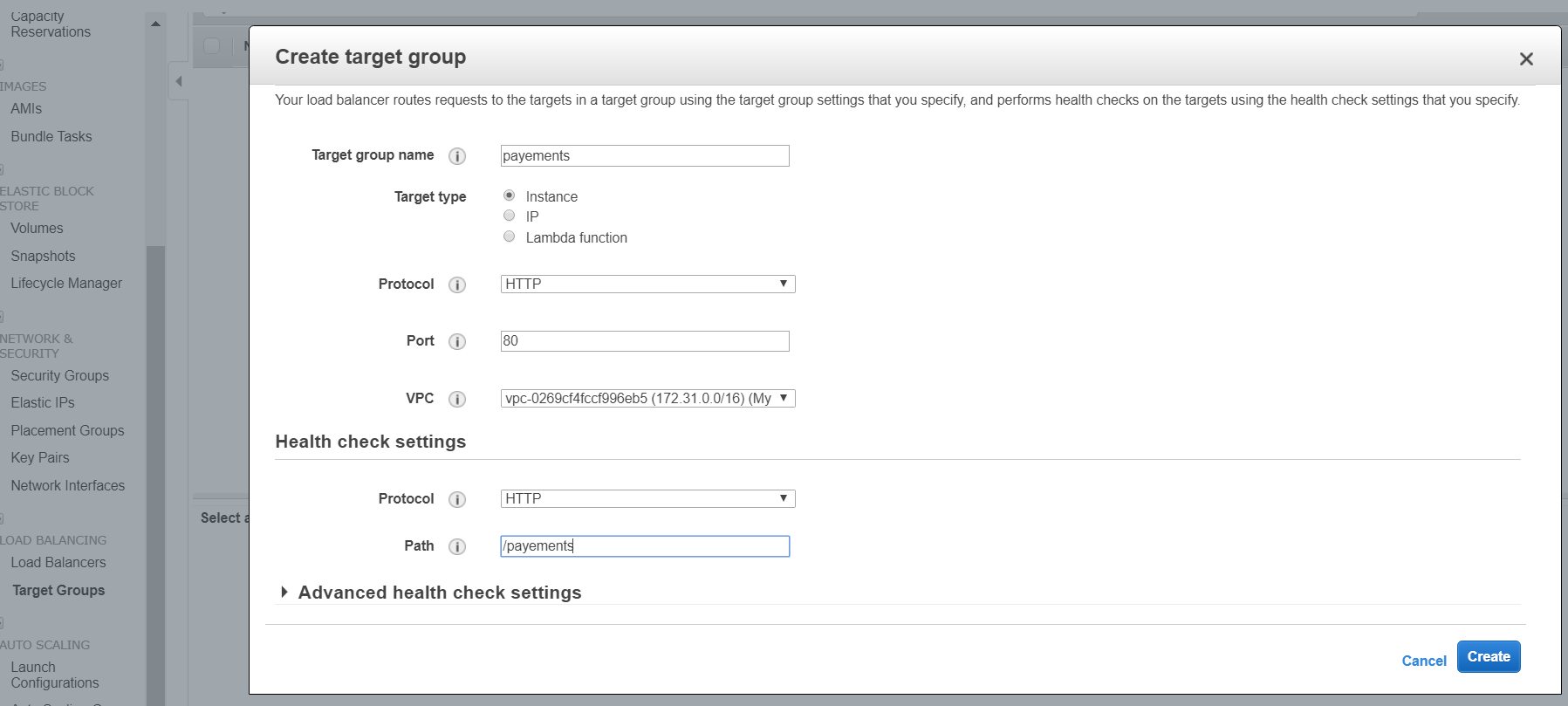
I TAKE GROUP EC2 INSTANCE WHICH RUNS ORDERS APPLICATION

I TAKE GROUP EC2 INSTANCE WHICH RUNS PAYEMENTS APPLICATION

I WILL CREATE RULE :\_ WHEN ROUTE A TRAFFIC TO ORDERS AND WHEN TO ROUTE A TRAFFIC TO PAYEMENTS , IF PATH CONTAINS ORDER THEN GO TO ORDERS ,PATH CNTAINS PAYEMENTS THEN ROUTE TO PAYEMNTS

ALB runs on port 80

Create target group :



Then create – targets – edit – select the particular one

Configure ALB

Create ALB :

GO TO LISTENERS UNDER alb - PUT RULES : NAME :/PAYEMENTS

Nlb :Choose network load balancer when you need ultra high performance

There are capable of handling millions of requests per second

Auto scalling:

* Auto scaling is used to manage Amazon ec2 capacity automatically . maintain the right number of instances for your application , -operate a healthy group of instances and scale it according to your needs.
* Autoscalling is free , if auto scaling launches additional resources for that we need to pay
* It is cost effective , it always maintains the exact capacity we need to serve the traffic.
* It manages health checks if any ec2 found unhealthy it terminates and launches new Ec2.
* ELB can be integrated with auto scalling such that Ec2 instances are dynamically added or removed.

If auto scaling wants to launch instance :

Launch configuration : it’s a template which contains following details

* -ami
* -instance type
* volume type and size
* Sg (security group
* Iam role
* Private key or key pair

Auto scalling wil use launch config for launching ec2 instances in auto scalling group.

Create Ami that should contain our appinstalled and configured

RDS:

Rds has automated backup’s with default retention 7 days and max is 35

When backups are performed there is brief suspension of i/o operations which leads to performance problems , ( if you want to fix this problems, if we have multiple Az enabled , backups are taken on a standby which doesnot impact performance of primary db.

It supports point- in time recovery ( if I want to restore my db in, specific day, specific hour,specific minute and specific second

We also can make manualbackups if required

Rds- dashboard

Step 1: make sure vpc and subnets are configured

Create a subnet group where we want to launch RDS (

(Rds must go in to private subnet ,

Create subnet group ( this subnet group contains private subnet))

Apps can connect to db using iam role or iam user.

Take backup in non business hours sothat customers wont impact.

Read replica : it is another db which is in sync

Multi az deployement

Supports read replicas.

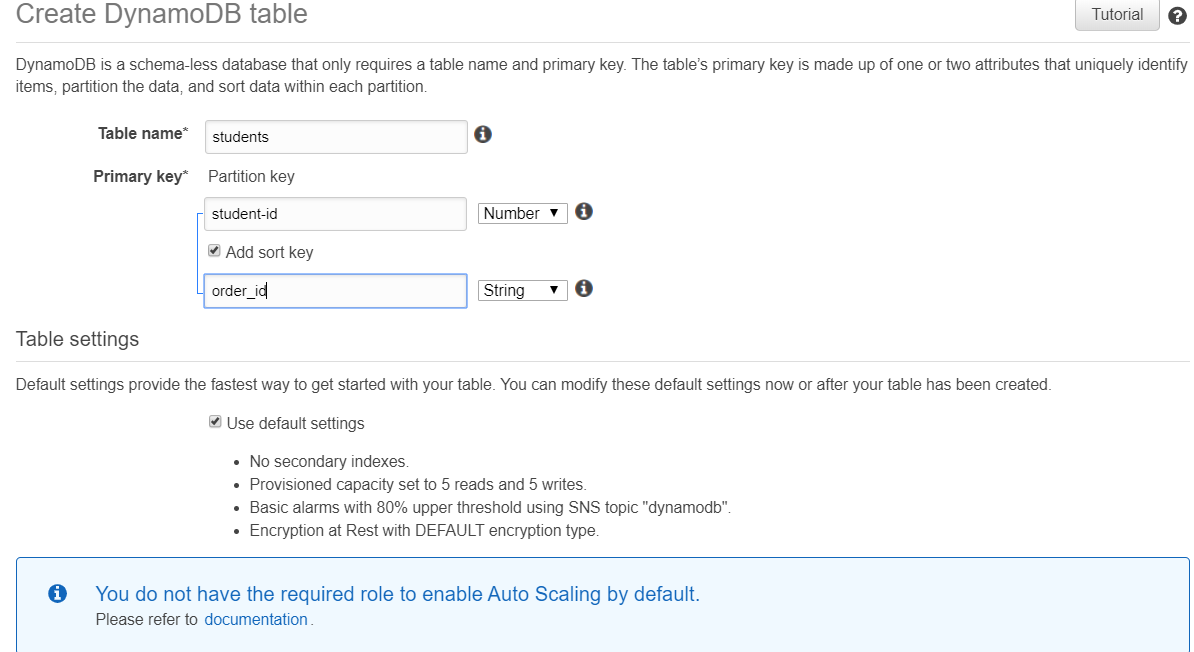
RDS notifications :

Event subscription :

24-10-19

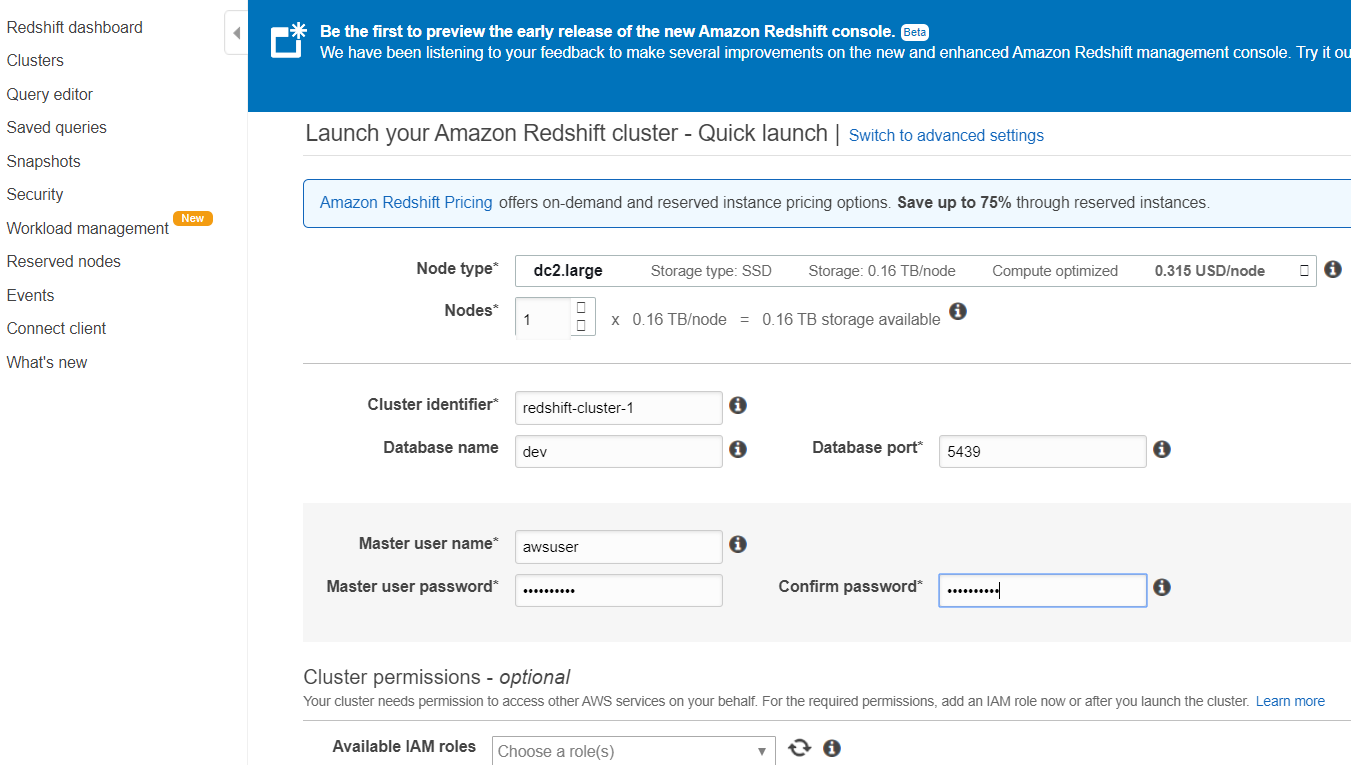
DYNAMO DB :

* Highly scalable, highly durable , no sql db from amazon
* Can handle unlimited amount of data and throughput
* Good option for large data sets
* Data is stored as json documents
* If we properly design our schema, we can fit all our data into 1 table
* Create table
* Follows dynamic schema
* We have app we are using rds , we want to add new column , if we want new column in the miidle it will throw exception, as dynamo db follows dynamic schema we can add column



* Items are known as records
* Attribtes are known as columns
* Increase read and write capacity units it scales

RED SHIFT

* Highly available ,highly scalable data warehousing solution from AWS
* It is widley used in reporting and analytics
* It is relational
* Red shift is called as columunar data base
* Specially designed for reporting 
* Always uses agreegate f/n ‘s like mean ,average,max.

1 r 2 questions in certific

**Elastic cache:**

* Highly available ,highly scalable durable
* Stores data in RAM , data acess is fast
* Cache readaing disk is not there so with ram it is fast
* Used to improve app performance

Q) we have entreprise app and wants to store API tokens for better performance.

1. Rds
2. DYnamobd
3. S3
4. Elastic cache

Ans) dynamo and elastic cache

Elastic cache supports 2 engines

- redis

- Memcached

25/10/19

**On demand instances:**

By default any ec2 **ins**tsance falls under on demand

We wont give any long term commitments we have flexibility when to launch and when to terminate

Cost is high compared to other options

Billing stops when you stop the server

**Reserved instances :**

We are going to give amazon long term commitments either 1 or 3 yrs.

Amazon gives good discounts

We have diff payement options

* All upfront
* Partial upfront
* No upfront

Depending on payement options discounts vary

Billing wont stop when reserved ec2 stops.

**---------------------------------30-19-19--------**

**Vpc peerng connections.**

They cant talk to each other using private IP.

VPc peering coneection is virtuall Gateway for connecting VPC’s

After creating peering conection servers can communicate over its private (servers in both vpc can communicate using private IP)

These two vpc’s can be in same A/c , diff A/c’s ,same region, or different regions.

Cider blocks should not overlap, for creating VPC peering connections.

**Steps for creating VPC Peering Connections.**

Make sure you have 2 vpc.

Create Vpc connection by choosing source and target

Vpc connection must be accepted

Add vpc peering conection with route table ss

Connect to HCL and ping IBM

We need igw or vpn from doin this

**IAM :**

* **Iam is a service where we mnage users,groups,roles , permissions**

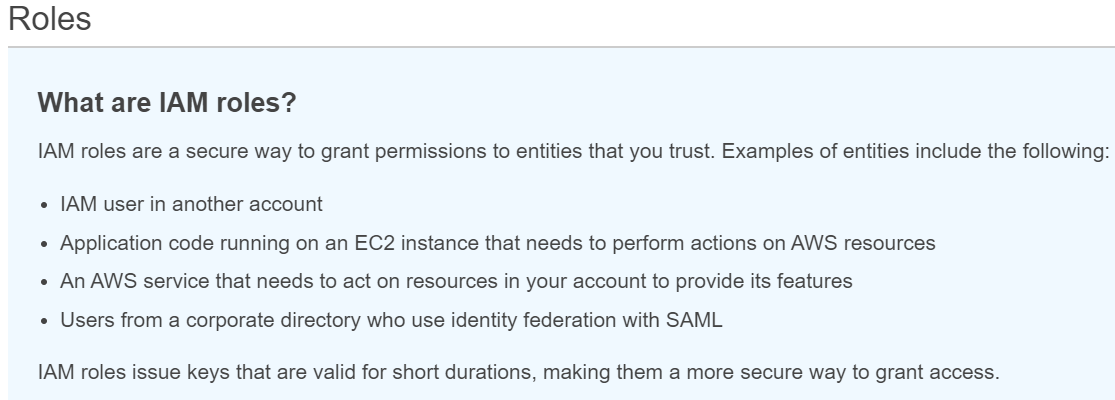
**Features of IAM :**

* **We can share AWS acess to other users**
* **We canshare aws acess with other development tools. (linux, java python terraform, CLI etc) it is also called as programmatic acess.**
* **It can integrate our AWS A/c with ldap OR AD or other 3rd party**

**7**

Iam roles or iam users

* Roles will be associate with policis
* When we use role and when we use user
* Cross a/c acess (i.e – users in one a/c want to access resources in another a/c)
* If you have app code running on ec2 instance, that needs to perform on aws instance



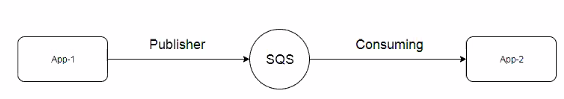
Create and assign IAMrole ec2 instance

Create -role

Choose service that will use role

4-11-19

It is used for integrating asynchronously



SQS is server less .(i.e : we don’t have any servers to manage)

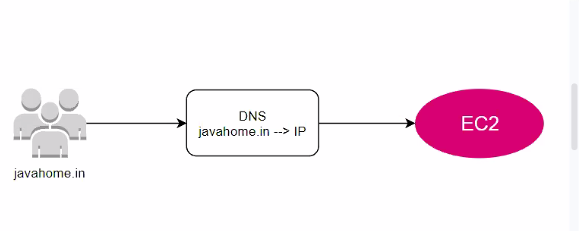
We don’t have to architect for High availability & scalability

We don’t have to pay for ideal time.

-------------------------------------------------------------

11-11-19

When users hit javahome.in it is



In place of Ec2 it can be ELB/ALB/NLB, S3 static end point( elastic bean stack end point)

There are others services which comes under devops elastic bean stack.

By default DNS runs on port 53 ,so its called Route53.

Using route53 we can register domains.

We can setup public (internet facing) or private dns (within vpc) ,route53 supports both

(Route53-dashboard

-register domains- choose domain name-add to cart-continue-checout-go to billing dashboard)

If u r domain is created elsewhere we can migrate that to route53.

(We have option to transfer domain)

Register domain in 3rd party websites like dot.tk- signin-

I can route .tk t0 route53

Rote53-hosted zones -create new -domaine name like in.tk - type=public.

We need to do domain name and ip address mapping

For every hosted zone

Hosted zone represent a specific domain & by default hosted zone contains 2 records

Ex1: Map your domain with Ec2 instance

Setup ec2 with website