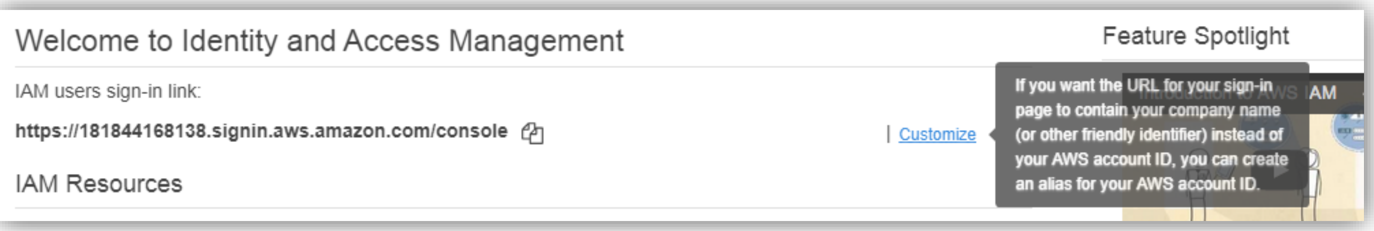
IAM(Identity access management)

Every time we cant able to remember the IAM link number. So we are customizing the url like the DNS



Welcome to Identity and Access Management

IAM users sign-in link:

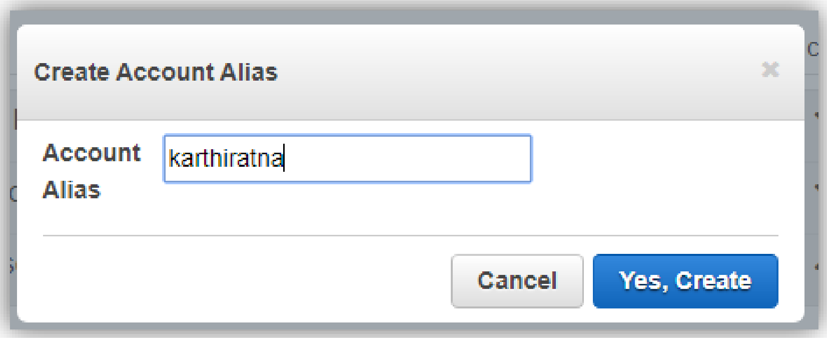
https://181844168138.signin.aws.amazon.com/console

| Customize

IAM Resources

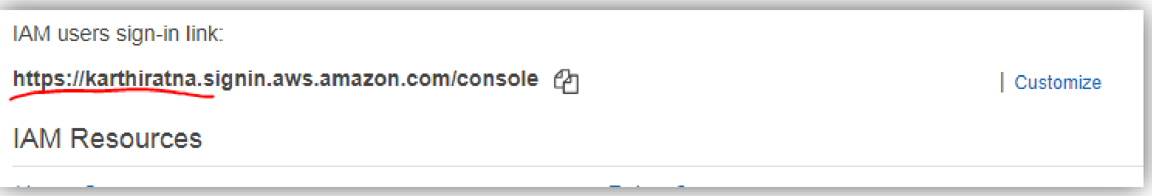
Feature Spotlight

If you want the URL for your sign-in page to contain your company name (or other friendly identifier) instead of your AWS account ID, you can create an alias for your AWS account ID.



Create Account Alias

Account Alias: karthiratna



IAM users sign-in link:

https://karthiratna.signin.aws.amazon.com/console

| Customize

IAM Resources

IAM Users

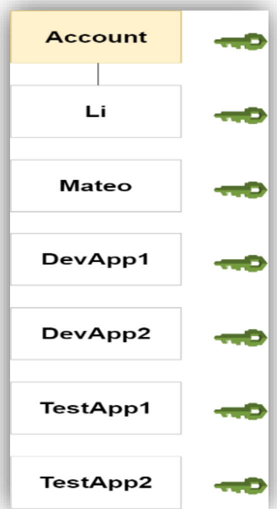
There are 2 types of identities in IAM

- User, developer, architect (person who can type username and password) [CITRIX Chubb login] (**authenticate**)

But however there will be an application(GRA) that needs to talk to you [**authorization**].

Likewise when u logged into the an IAM user account.Trying to create an new instance but failed because you are not authorized to create the EC2 instance. So any user that you create is denied from any permission by default

1. Create the user, password/ keys
2. Then assign permissions to the user

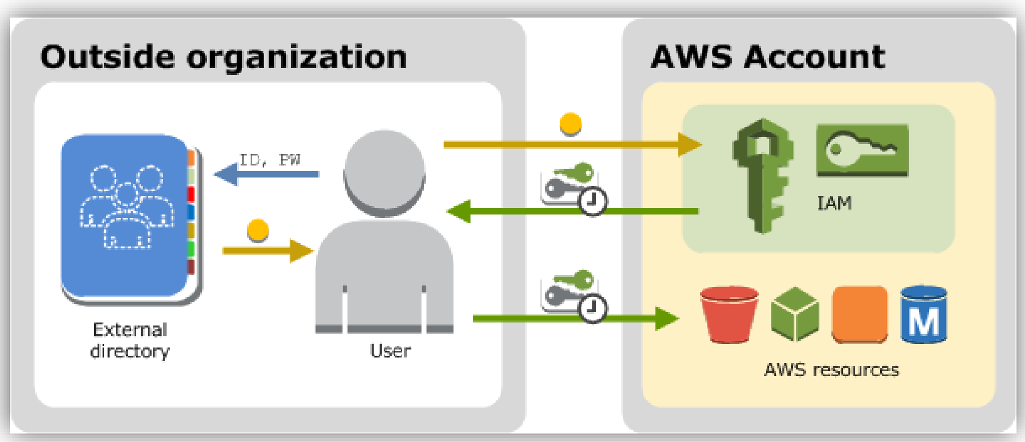


If EC2 Instance/application in my account would like to reach S3 to store an file/ object/download a file.That instance/application needs permission also

You can also create an individual access key for each user so that the user can make programmatic requests to work with resources in your account. In the figure, the users Li, Mateo, DevApp1, DevApp2, TestApp1, and TestApp2 have been added to a single AWS account. Each user has its own credentials.

Notice that some of the users are actually applications (for example, DevApp1). An IAM user doesn't have to represent an actual person; you can create an IAM user in order to generate an access key for an application that runs in your corporate network and needs AWS access.

We recommend that you create an IAM user for yourself and then assign yourself administrative permissions for your account. You can then sign in as that user to add more users as needed.



If the users in your organization already have a way to be authenticated, such as by signing in to your corporate network, you don't have to create separate IAM users for them. Instead, you can *federate* those user identities into AWS.

The following diagram shows how a user can use IAM to get temporary AWS security credentials to access resources in your AWS account.

IAM Roles [Secure Token service]

Virtual user—for application to access to that environment we need to create temporary credentials . That is called as IAM role. Through this credentials we can access other services. Like stored services can go to the database -> read from it Or like dynamo db to read/ write to it.

Conclusion

*****If the application require permanent credentials for the users (IAM Users) –Long Lived Credentials

*****If the application require temporary credentials (write, read, store something) for the users (IAM ROLE) – Short Lived Credentials –It will expire after some time

Live example: Linux academy la work pannum pothu. Practical session irunthuchi. They gave us the IAM Credential that is temporary. It lasted for only 1 hour. After that antha credential expire agiruchi.

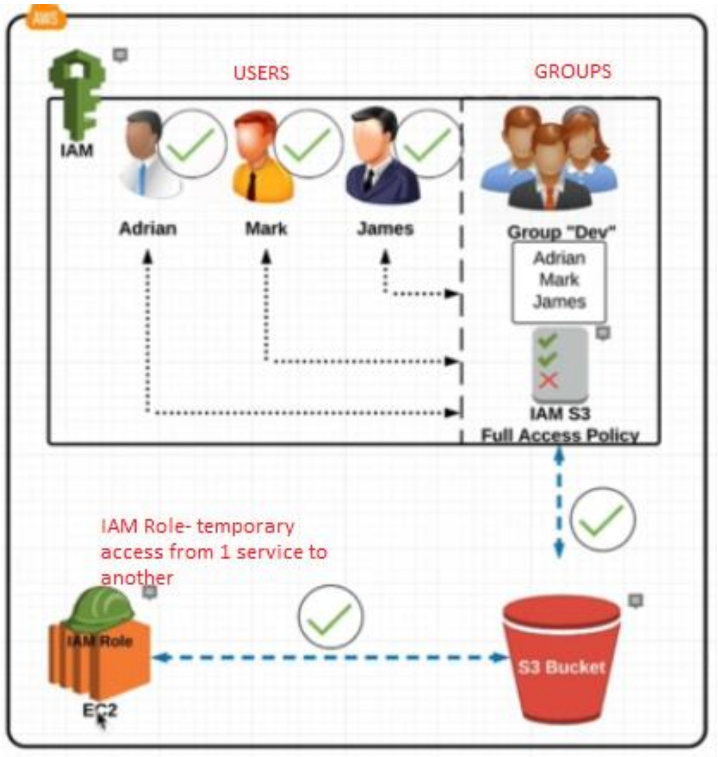
If I am an user can I use roles?

Yes, u can. I am the user. I need to access the email service. I need a phone/ any device to access the service. Here phone/ other devices acts as the IAM Role.

Usually, The IAM users have limited amount of users/ employees. What if we have 20000 or 40000 employees. Here role plays a major role. For other employees we will be assigning the roles… That is temporary credentials.

IAM Group

Instead of giving permission/ policy to each and every users. We can create a group in which we can assign the permission or policy.



IAM Users

1. **MFA – multi-factor authentication (MFA) - Eg:** arn:aws:iam::181844168138:mfa/root-account-mfa-device

   Arn – Amazon Resource Name

2. **Create Users**
   a. **Add user**
   b. **Enter the username**
   c. **There are 2 access type – Choose any one of them**
      - <u>AWS Management Console access</u> (console that is accessed through the username and password) and we can use MFA for further authentication for the user.
      - <u>Programmatic access:</u> What if I have the SDK and I would like to communicate with AWS and start using AWS Linux command line Interface. And I want to communicate with the Application Programming Interface and to do thing without logging into the console.

        You can do anything with commands and you can do anything with Rest API.You can do a lot of common things either way in any one of these access methods. So programming access can do anything other than console.

        Use the access Key/ secret key so that API/CLI/Developing tools/SDK etc can able to access AWS- **There is no username / password**

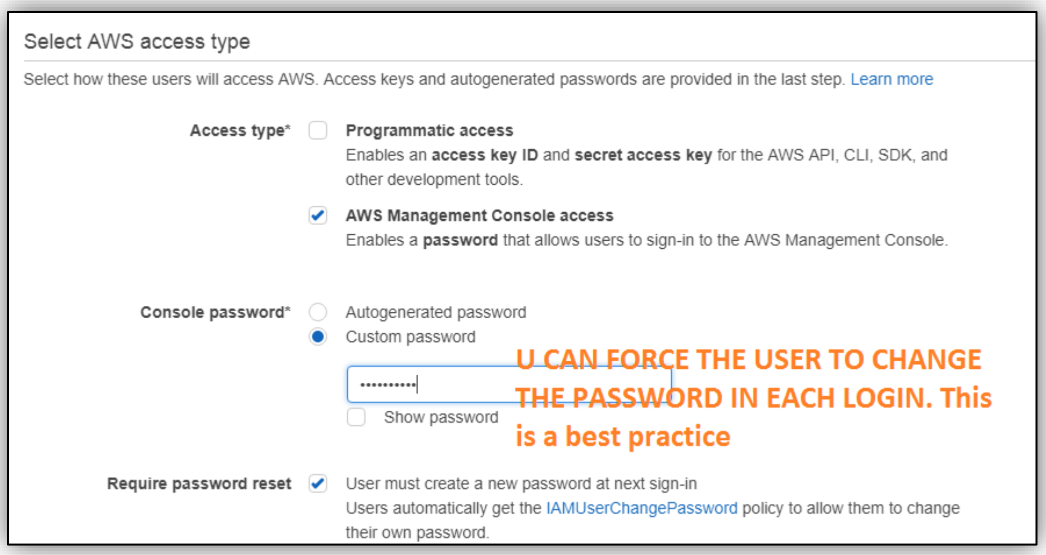
   d. **Each IAM User have authorised autogenerated password/ Custom password.**

3. **Create Groups**
4. **Create Roles**

If the user is a developer then they won't come inside the console – choose programmatic access – configure only the access keys

If the user need the console access – configure only the console

Give least privilege access is the IAM's best practices. Don't choose both the access to the user to do his / her job.choosing 1 is more than enough. But in the future they need the extra access na.. Create a group for the users and assign the access type to that particular group.



Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* □ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
● Custom password

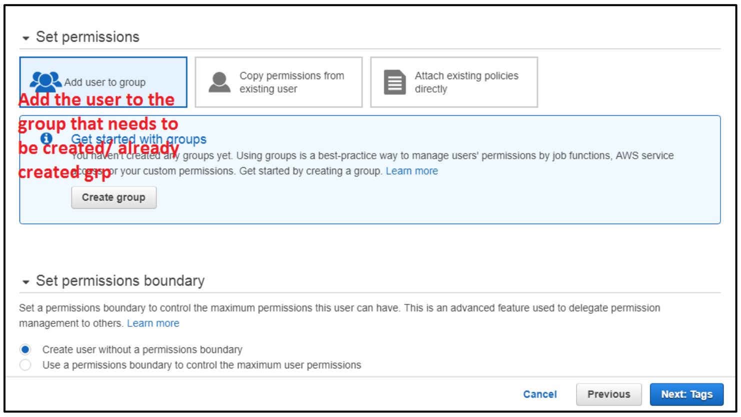
••••••••••

□ Show password

U CAN FORCE THE USER TO CHANGE THE PASSWORD IN EACH LOGIN. This is a best practice

Require password reset ☑ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

PERMISSION



Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

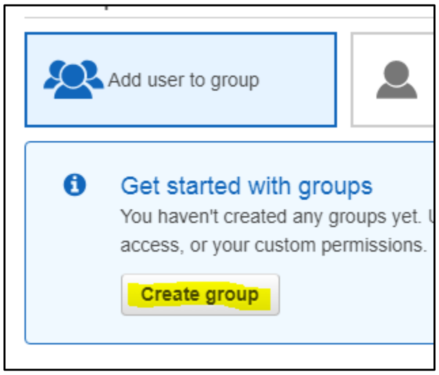
Add the user to the group that needs to be created/ already created grp

Get started with groups
You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more

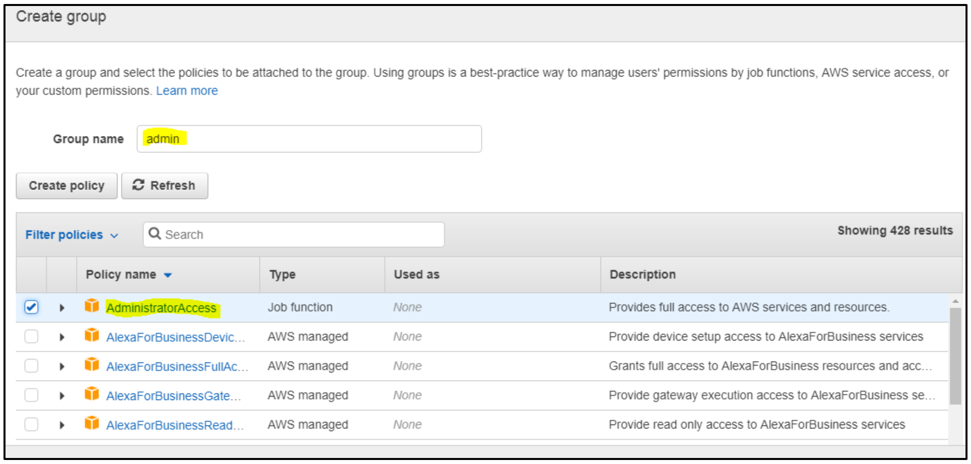
Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. Learn more

● Create user without a permissions boundary
○ Use a permissions boundary to control the maximum user permissions



Get started with groups
You haven't created any groups yet. U
access, or your custom permissions.



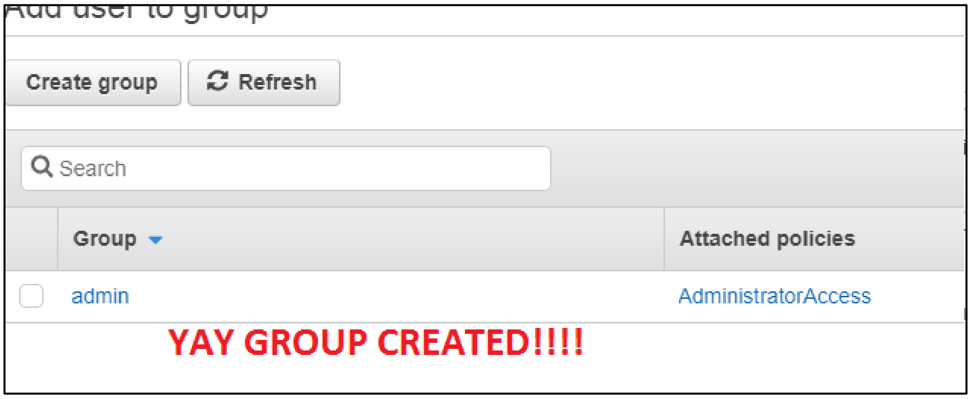
Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name: admin

		Policy name	Type	Used as	Description
☑	▸	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
□	▸	AlexaForBusinessDevic...	AWS managed	None	Provide device setup access to AlexaForBusiness services
□	▸	AlexaForBusinessFullAc...	AWS managed	None	Grants full access to AlexaForBusiness resources and acc...
□	▸	AlexaForBusinessGate...	AWS managed	None	Provide gateway execution access to AlexaForBusiness se...
□	▸	AlexaForBusinessRead...	AWS managed	None	Provide read only access to AlexaForBusiness services

Any user in the above group will get attached to the policy



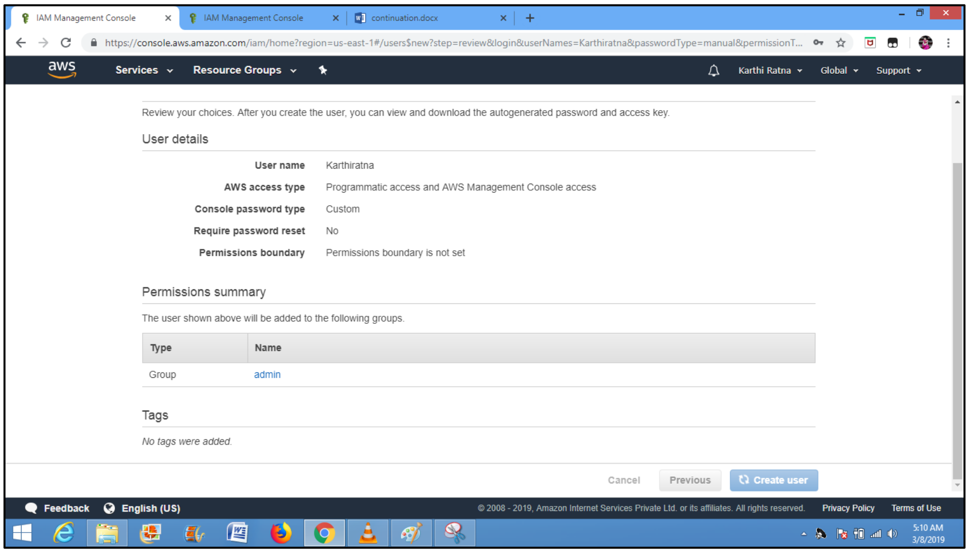
Add user to group

	Group	Attached policies
□	admin	AdministratorAccess

YAY GROUP CREATED!!!!

Tags - not explained

Review page



IAM Management Console
IAM Management Console
continuation.docx
https://console.aws.amazon.com/iam/home?region=us-east-1#/users$new?step=review&login&userNames=Karthiratna&passwordType=manual&permissionT...
aws
Services
Resource Groups
Karthi Ratna
Global
Support

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	Karthiratna
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

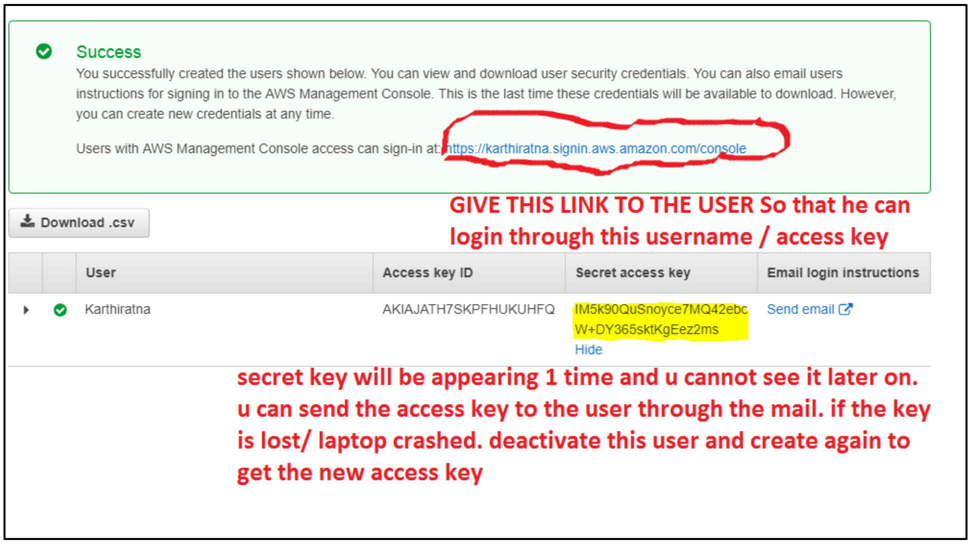
The user shown above will be added to the following groups.

Type	Name
Group	admin

Tags

No tags were added.

Cancel
Previous
Create user
Feedback
English (US)
© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
5:10 AM
3/8/2019



Success

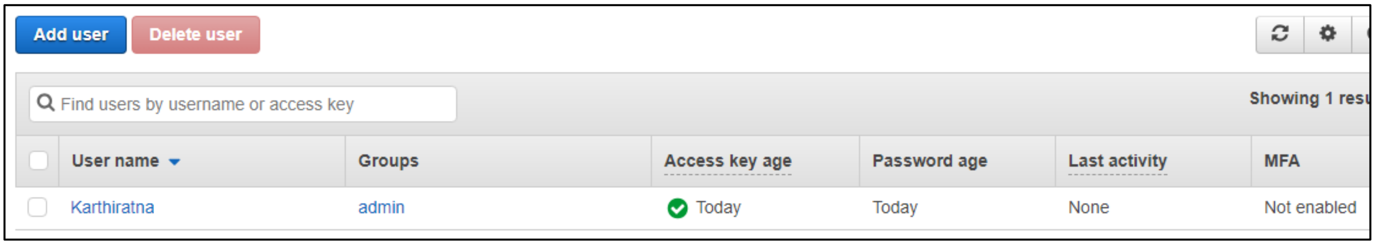
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://karthiratna.signin.aws.amazon.com/console

GIVE THIS LINK TO THE USER So that he can login through this username / access key

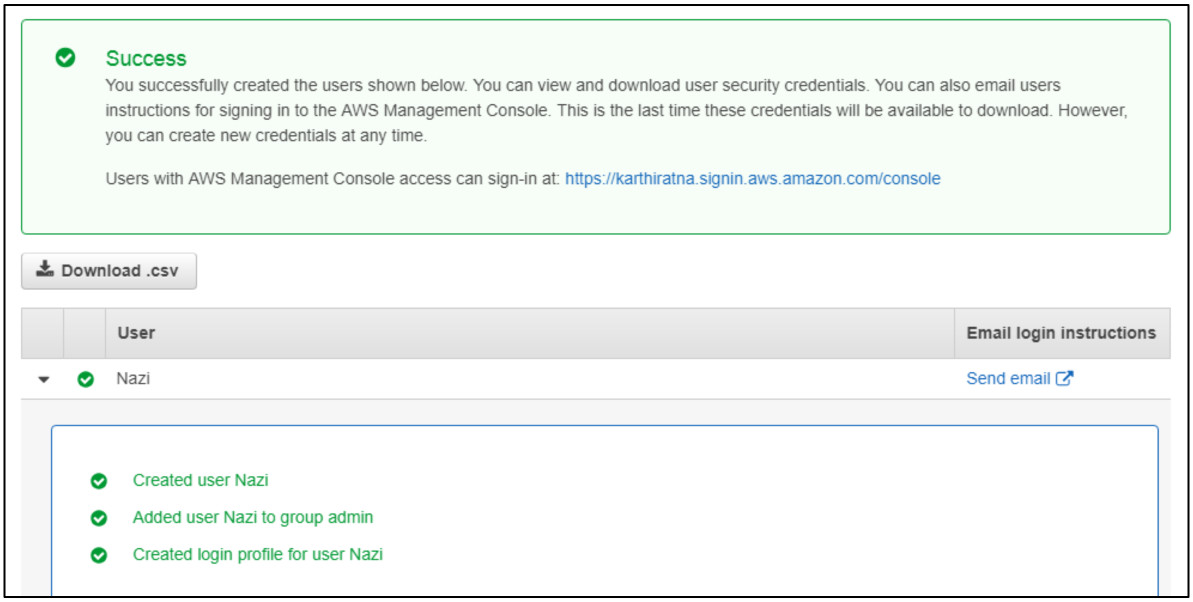
		User	Access key ID	Secret access key	Email login instructions
▸	✓	Karthiratna	AKIAJATH7SKPFHUKUHFQ	IM5k90QuSnoyce7MQ42ebcW+DY365sktKgEez2ms Hide	Send email

secret key will be appearing 1 time and u cannot see it later on. u can send the access key to the user through the mail. if the key is lost/ laptop crashed. deactivate this user and create again to get the new access key



□	User name ▾	Groups	Access key age	Password age	Last activity	MFA
□	Karthiratna	admin	✓ Today	Today	None	Not enabled

I have created another user **Nazi** where I give only the admin access. So there will not be any access key / secret key for her.



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

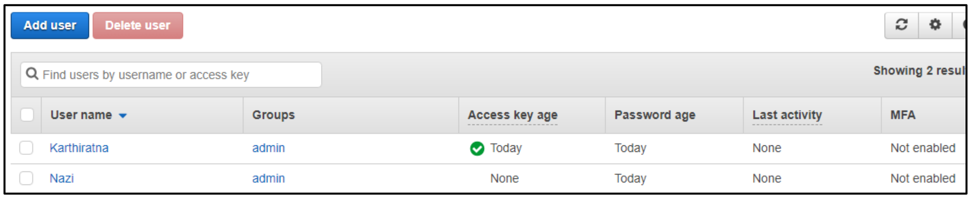
Users with AWS Management Console access can sign-in at: https://karthiratna.signin.aws.amazon.com/console

		User	Email login instructions
▾	✓	Nazi	Send email

✓ Created user Nazi

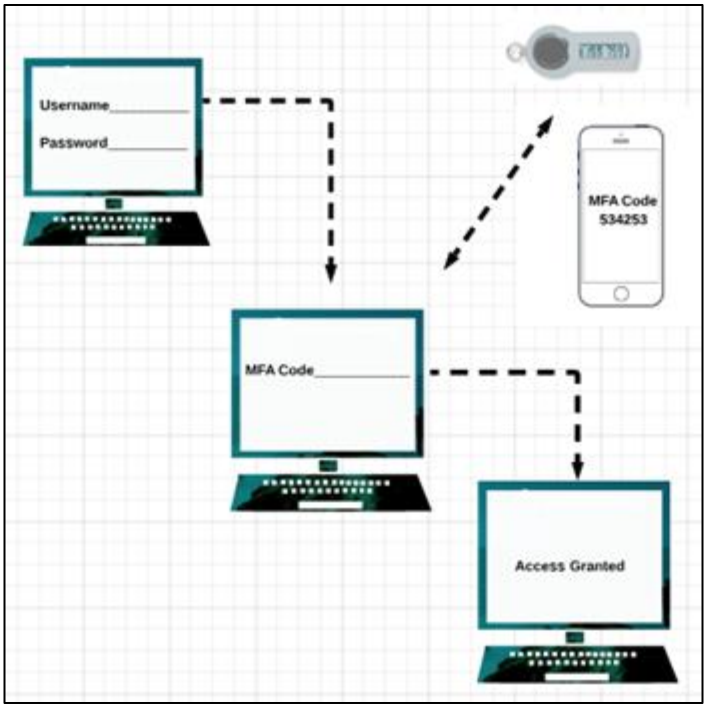
✓ Added user Nazi to group admin

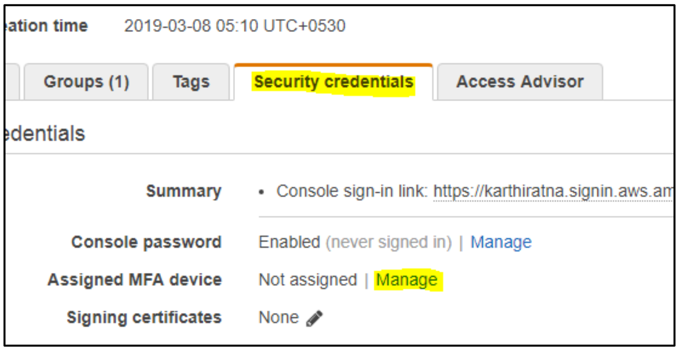
✓ Created login profile for user Nazi



□	User name ▾	Groups	Access key age	Password age	Last activity	MFA
□	Karthiratna	admin	✓ Today	Today	None	Not enabled
□	Nazi	admin	None	Today	None	Not enabled

Click on the particular user to add the MFA. We are giving this MFA for security purpose. Because we have given them the entire administrative access.

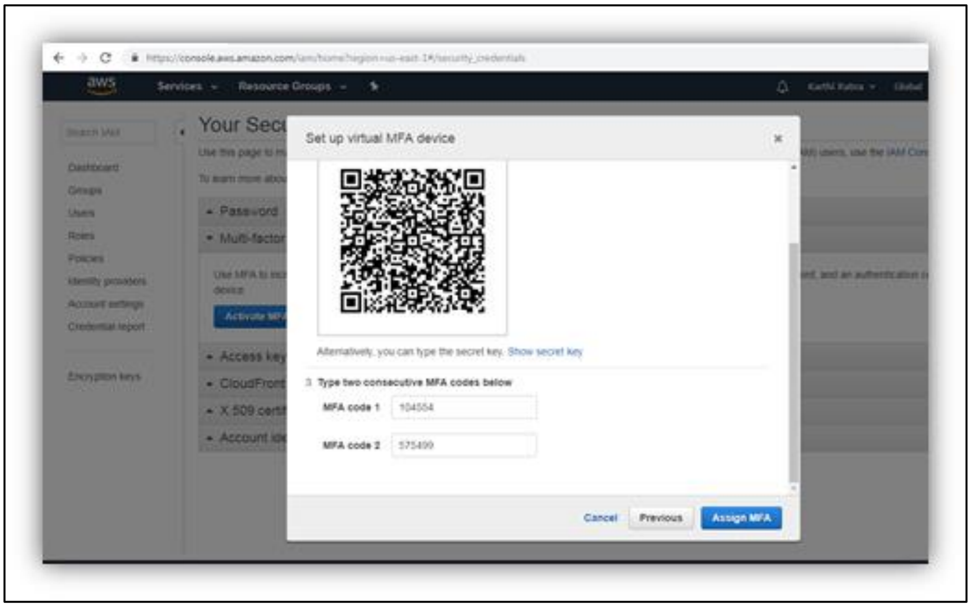




ation time 2019-03-08 05:10 UTC+0530

edentials

Summary	• Console sign-in link: https://karthiratna.signin.aws.am
Console password	Enabled (never signed in) | Manage
Assigned MFA device	Not assigned | Manage
Signing certificates	None



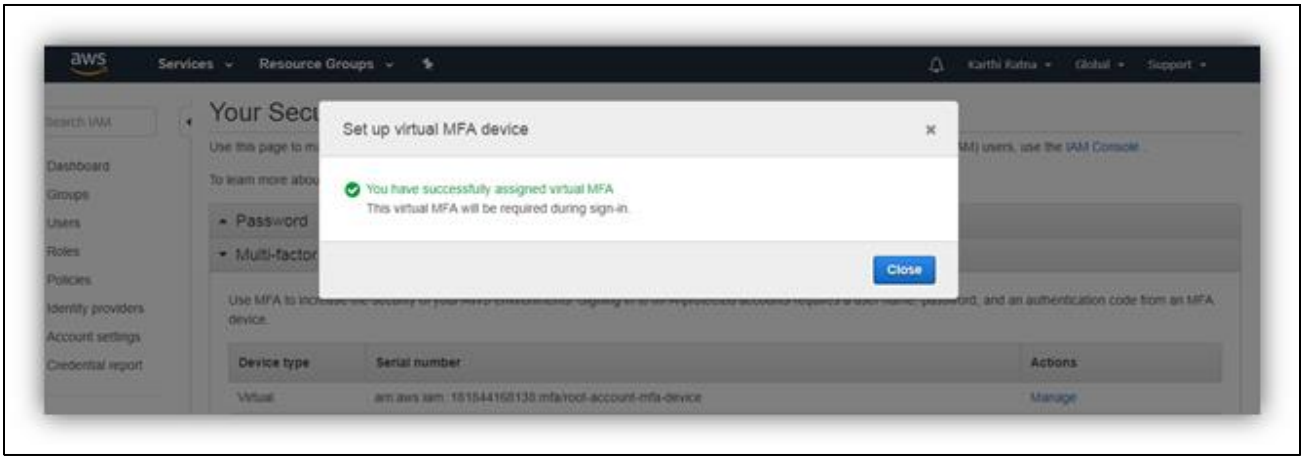
Set up virtual MFA device

Alternatively, you can type the secret key. Show secret key

3 Type two consecutive MFA codes below

MFA code 1 104554

MFA code 2 575499

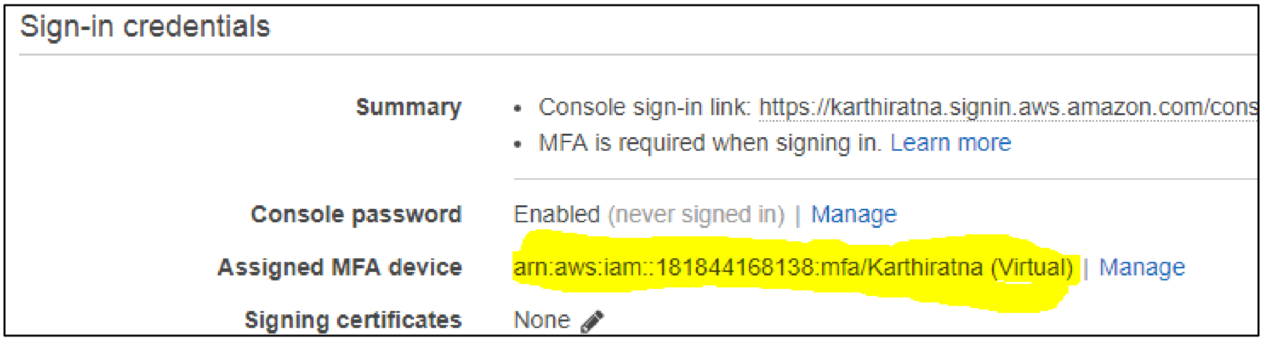


Set up virtual MFA device

You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.

Use MFA to increase the security of your AWS environment. Signing in to an MFA-protected account requires a user name, password, and an authentication code from an MFA device.

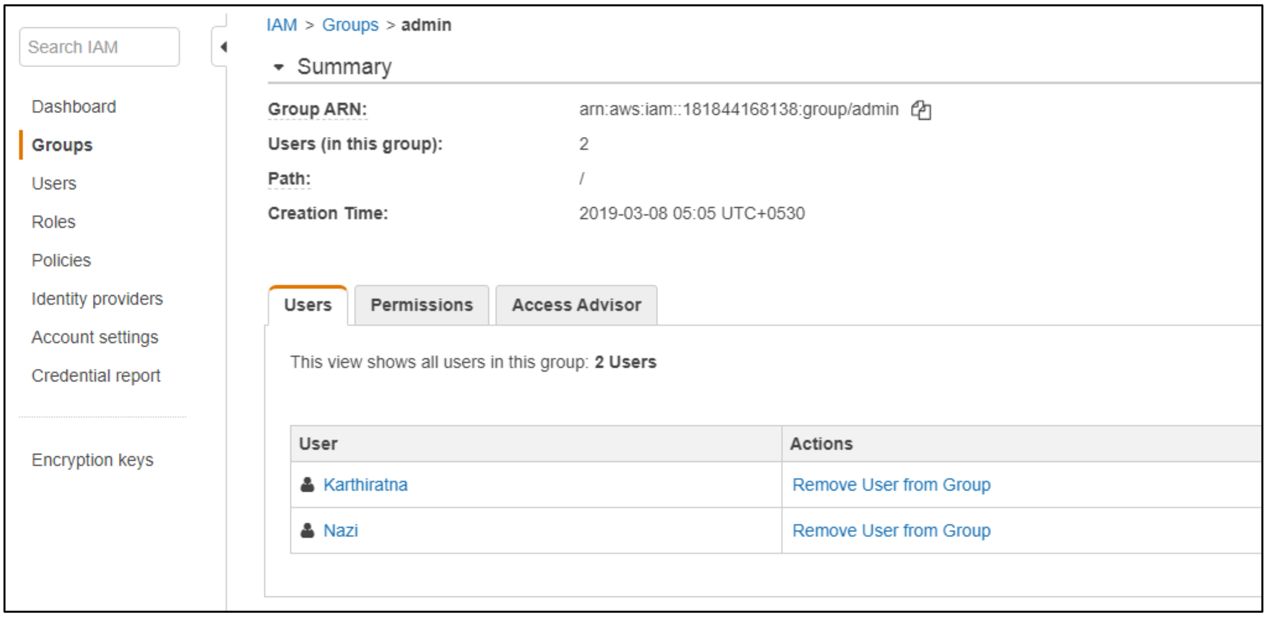
Device type	Serial number	Actions
Virtual	arn:aws:iam::181844168138:mfa/root-account-mfa-device	Manage



Sign-in credentials

Summary	• Console sign-in link: https://karthiratna.signin.aws.amazon.com/cons • MFA is required when signing in. Learn more
Console password	Enabled (never signed in) | Manage
Assigned MFA device	arn:aws:iam::181844168138:mfa/Karthiratna (Virtual) | Manage
Signing certificates	None

Go to **Group**



IAM > Groups > admin

Summary

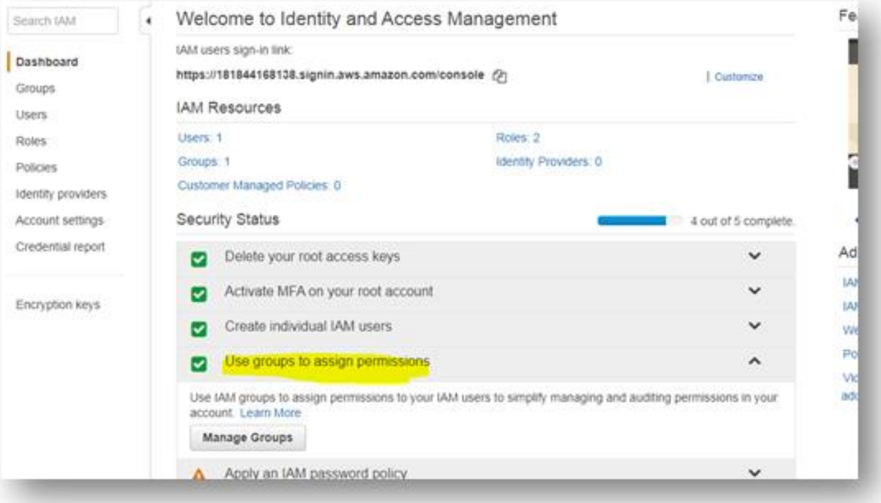
Group ARN:	arn:aws:iam::181844168138:group/admin
Users (in this group):	2
Path:	/
Creation Time:	2019-03-08 05:05 UTC+0530

This view shows all users in this group: **2 Users**

User	Actions
Karthiratna	Remove User from Group
Nazi	Remove User from Group

You can also add the group name – from the start

Use groups to assign permissions-> – It is easy to manage the group and assign permissions to the group. Instead of assigning permissions to the users individually



Welcome to Identity and Access Management

IAM users sign-in link:

https://181844168138.signin.aws.amazon.com/console

IAM Resources

Users: 1 Roles: 2
Groups: 1 Identity Providers: 0
Customer Managed Policies: 0

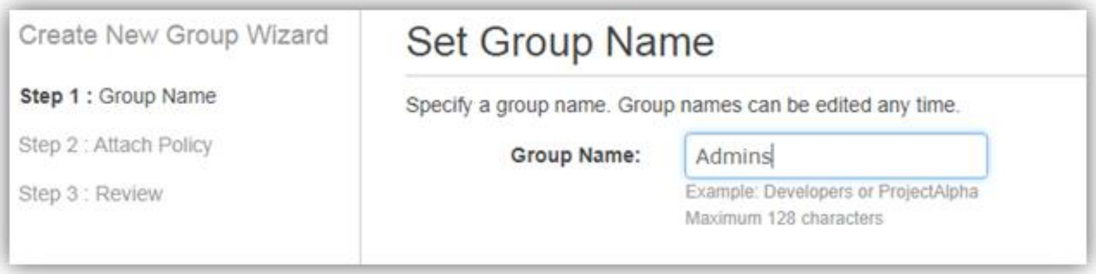
Security Status 4 out of 5 complete.

- ☑ Delete your root access keys
- ☑ Activate MFA on your root account
- ☑ Create individual IAM users
- ☑ Use groups to assign permissions

Use IAM groups to assign permissions to your IAM users to simplify managing and auditing permissions in your account. Learn More

- ⚠ Apply an IAM password policy

create new group ->



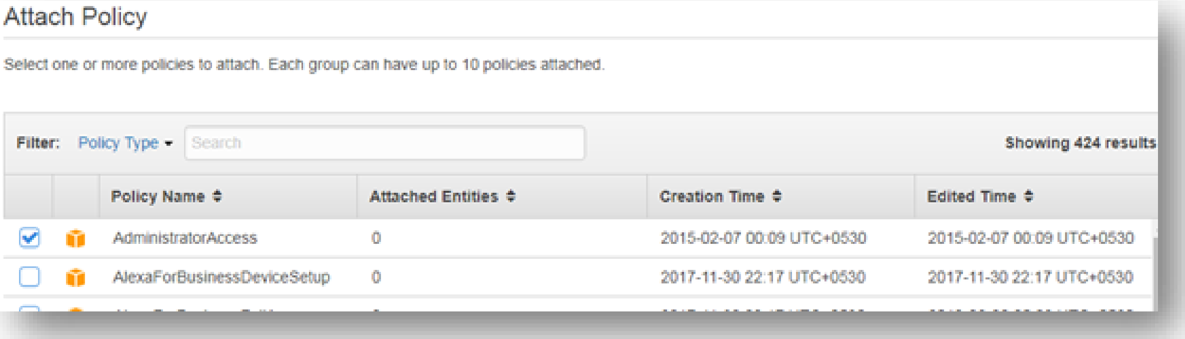
Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: Admins

Example: Developers or ProjectAlpha
Maximum 128 characters

Select policy type



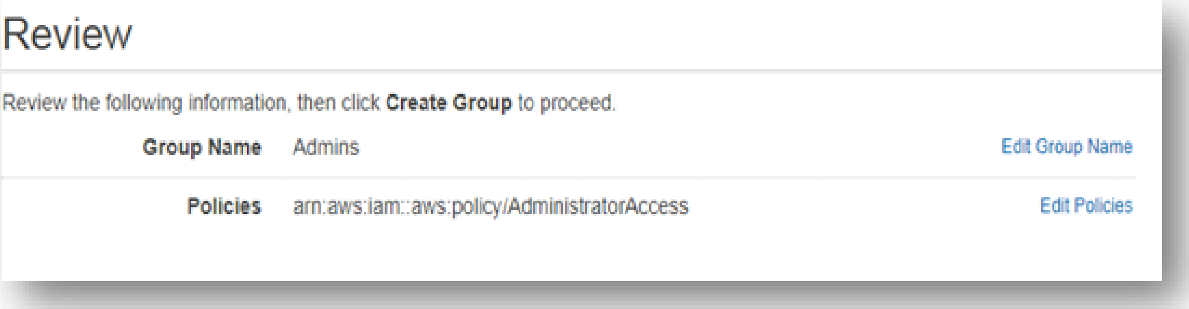
Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ Search Showing 424 results

		Policy Name ⬍	Attached Entities ⬍	Creation Time ⬍	Edited Time ⬍
☑		AdministratorAccess	0	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+0530
□		AlexaForBusinessDeviceSetup	0	2017-11-30 22:17 UTC+0530	2017-11-30 22:17 UTC+0530

Review



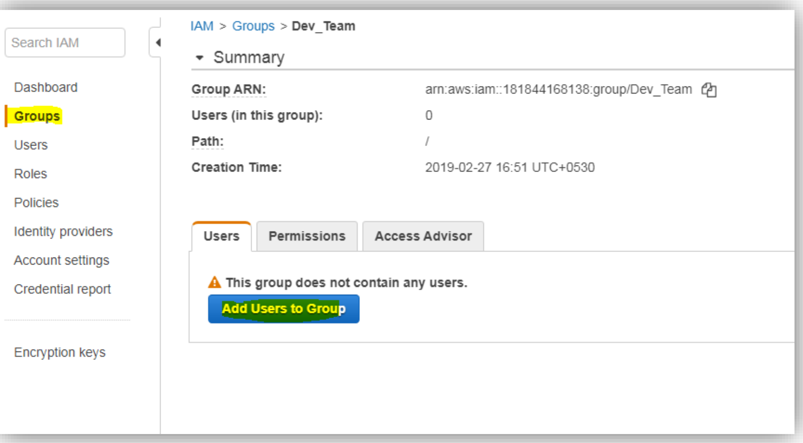
Review

Review the following information, then click **Create Group** to proceed.

Group Name Admins Edit Group Name

Policies arn:aws:iam::aws:policy/AdministratorAccess Edit Policies

ADD USERS TO THE GROUP

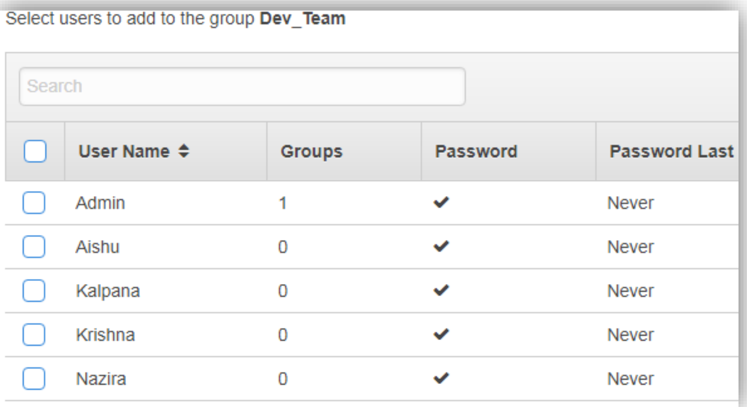


IAM > Groups > Dev_Team

Summary

Group ARN:	arn:aws:iam::181844168138:group/Dev_Team
Users (in this group):	0
Path:	/
Creation Time:	2019-02-27 16:51 UTC+0530

This group does not contain any users.



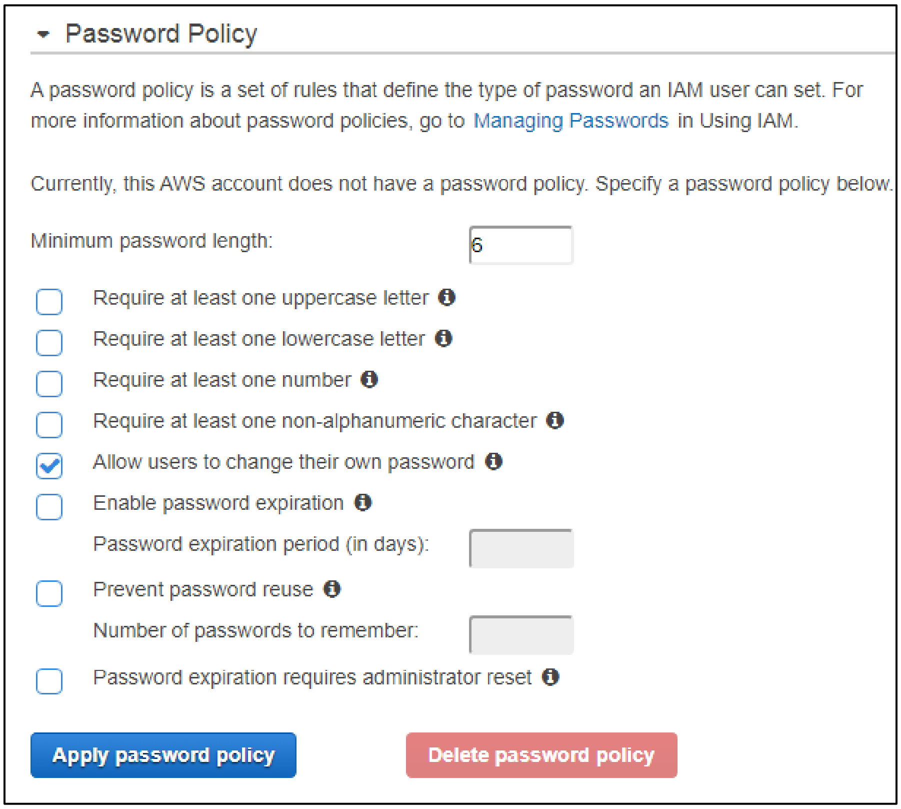
Select users to add to the group **Dev_Team**

□	User Name	Groups	Password	Password Last
□	Admin	1	✓	Never
□	Aishu	0	✓	Never
□	Kalpana	0	✓	Never
□	Krishna	0	✓	Never
□	Nazira	0	✓	Never

Can u remove the group that has more users?

Yes you can remove the group. But when u are doing with the Command line interface , Software development kit (SDK) . You need to delete the users first and then group.

IAM Password policy



Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to Managing Passwords in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length: 6

□ Require at least one uppercase letter

□ Require at least one lowercase letter

□ Require at least one number

□ Require at least one non-alphanumeric character

☑ Allow users to change their own password

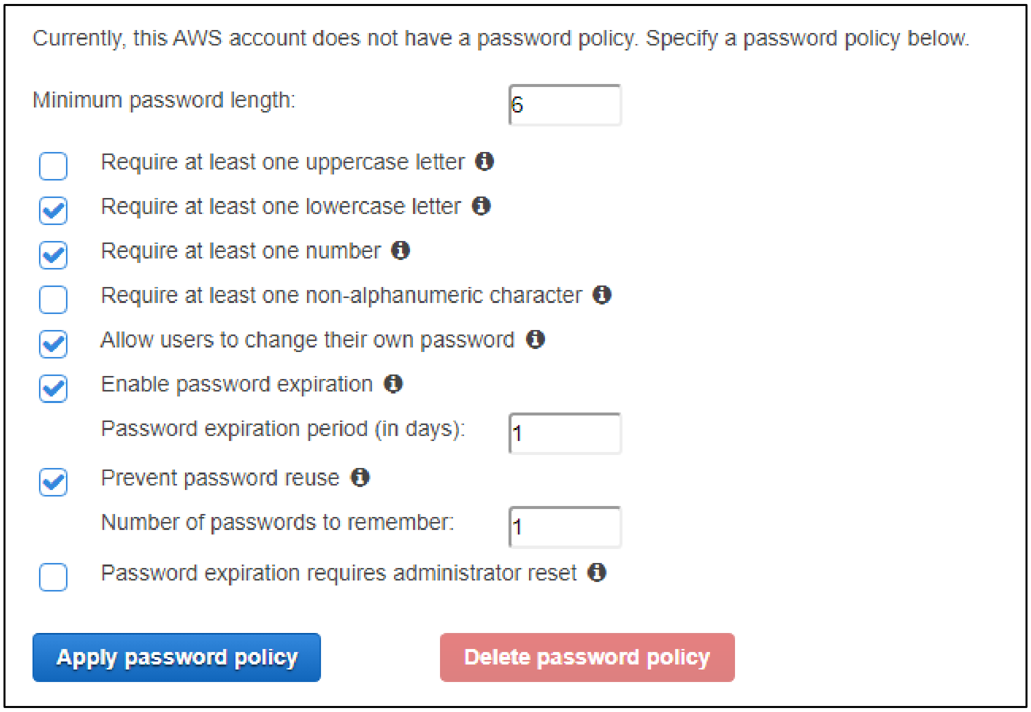
□ Enable password expiration

Password expiration period (in days):

□ Prevent password reuse

Number of passwords to remember:

□ Password expiration requires administrator reset



Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length: 6

□ Require at least one uppercase letter

☑ Require at least one lowercase letter

☑ Require at least one number

□ Require at least one non-alphanumeric character

☑ Allow users to change their own password

☑ Enable password expiration

Password expiration period (in days): 1

☑ Prevent password reuse

Number of passwords to remember: 1

□ Password expiration requires administrator reset

Usually the password expiration : 90 days

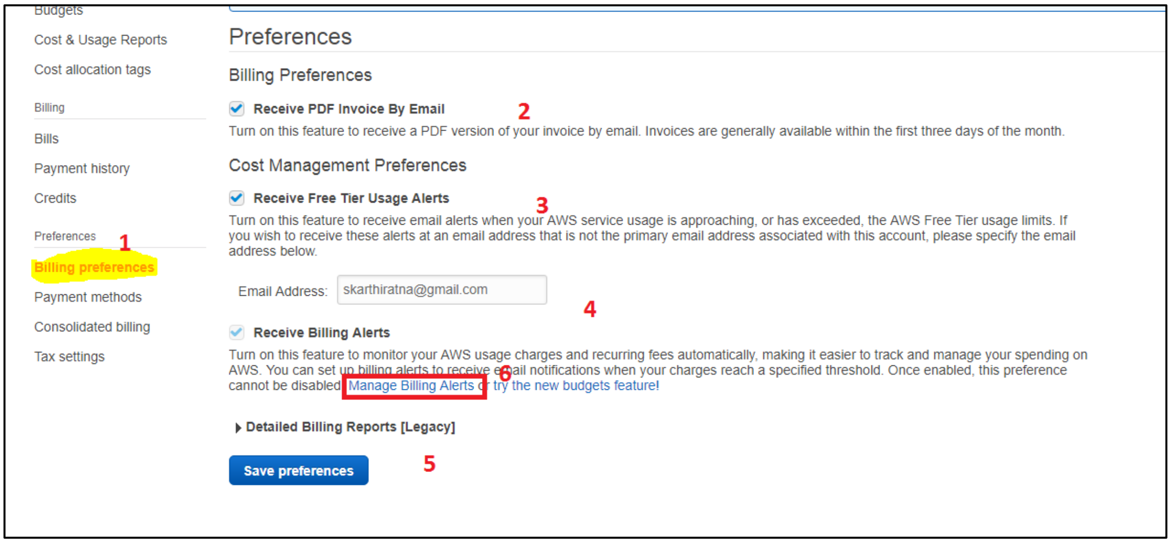
The password reuse to remember is 7 days.

The password policy once set will be applied to the entire console as the common policy.

BILLING ALARM

We are using the free tier for 12 months. What if we use the resource that is not free ? We will be charged without our notice... 🙁 so now we are going to set the billing alarm in order to escape from the unwanted charging 🙂

1. Go to the Account Name and click on the billing dashboard.



Preferences

Billing Preferences

☑ Receive PDF Invoice By Email

Turn on this feature to receive a PDF version of your invoice by email. Invoices are generally available within the first three days of the month.

Cost Management Preferences

☑ Receive Free Tier Usage Alerts

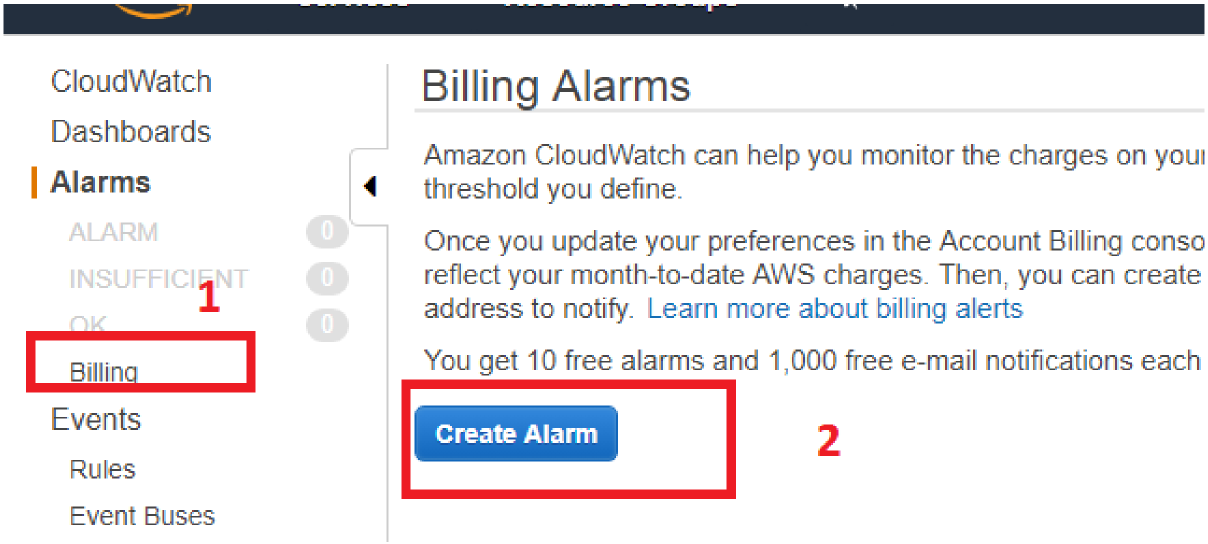
Turn on this feature to receive email alerts when your AWS service usage is approaching, or has exceeded, the AWS Free Tier usage limits. If you wish to receive these alerts at an email address that is not the primary email address associated with this account, please specify the email address below.

Email Address: skarthiratna@gmail.com

☑ Receive Billing Alerts

Turn on this feature to monitor your AWS usage charges and recurring fees automatically, making it easier to track and manage your spending on AWS. You can set up billing alerts to receive email notifications when your charges reach a specified threshold. Once enabled, this preference cannot be disabled. Manage Billing Alerts or try the new budgets feature!

2. Manage billing alerts -> cloud watch" - [To define the threshold amount for the alarm]

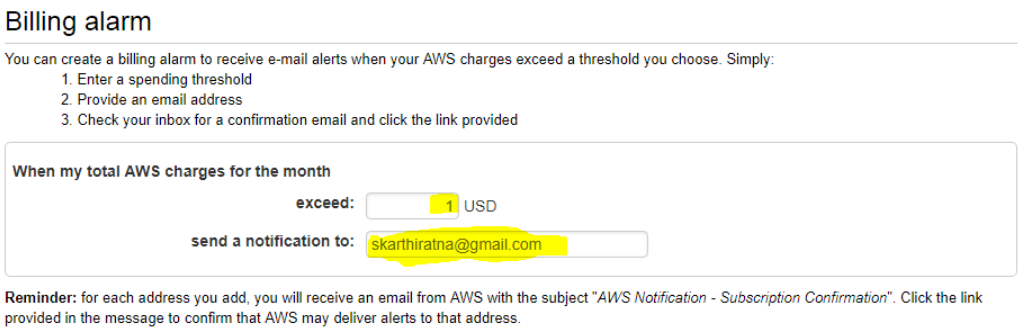


Billing Alarms

Amazon CloudWatch can help you monitor the charges on your threshold you define.

Once you update your preferences in the Account Billing conso reflect your month-to-date AWS charges. Then, you can create address to notify. Learn more about billing alerts

You get 10 free alarms and 1,000 free e-mail notifications each



Billing alarm

You can create a billing alarm to receive e-mail alerts when your AWS charges exceed a threshold you choose. Simply:

1. Enter a spending threshold
2. Provide an email address
3. Check your inbox for a confirmation email and click the link provided

When my total AWS charges for the month

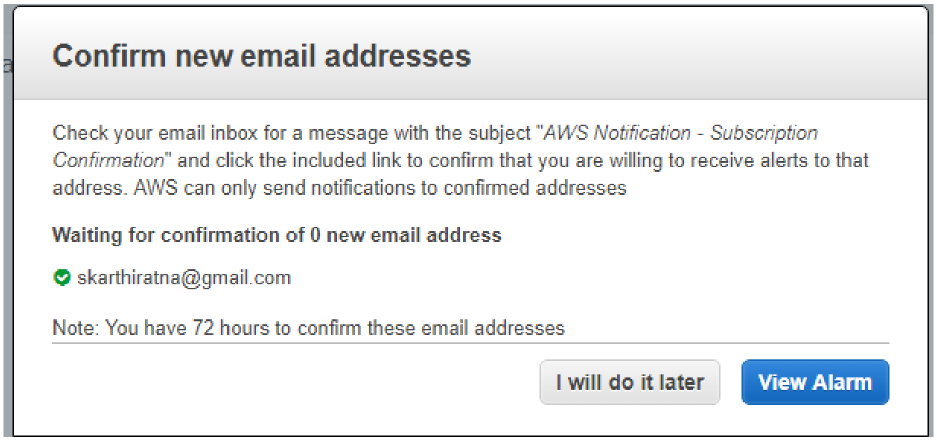
exceed: 1 USD

send a notification to: skarthiratna@gmail.com

Reminder: for each address you add, you will receive an email from AWS with the subject "*AWS Notification - Subscription Confirmation*". Click the link provided in the message to confirm that AWS may deliver alerts to that address.

-> Click "create"

3. We will receive the subscription mail-> click on the confirmation link in our mail -> Now all set … yeahhhhhh!!!!!!! 😛



Confirm new email addresses

Check your email inbox for a message with the subject "*AWS Notification - Subscription Confirmation*" and click the included link to confirm that you are willing to receive alerts to that address. AWS can only send notifications to confirmed addresses

Waiting for confirmation of 0 new email address

✓ skarthiratna@gmail.com

Note: You have 72 hours to confirm these email addresses

VPC- Virtual Private Cloud

[DOLFINED]

VPC is a virtual secure isolated environment for the customers in the AWS.

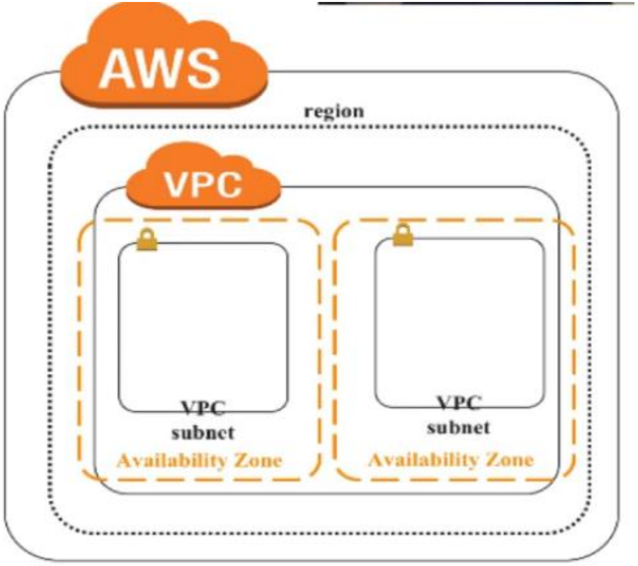
Traditionally we were building the datacenter in-house for each and every company. It will take too much of time, money, space.
So in cloud, instead of spending money for implementing the datacenter, we are outsourcing (obtain (goods or a service) by contract from an outside supplier.) the cloud.

Now cloud is more than a virtual environment dedicated for you Mr. Customer. Dedicated means a private cloud is virtually allocated to you/ 1 client/ 1 department/ enterprise.
So

- **There is no physical router, firewall dedicated to you ..but there is virtual router/ firewall is dedicated to you .**
- **You cannot talk to other private cloud by default.**

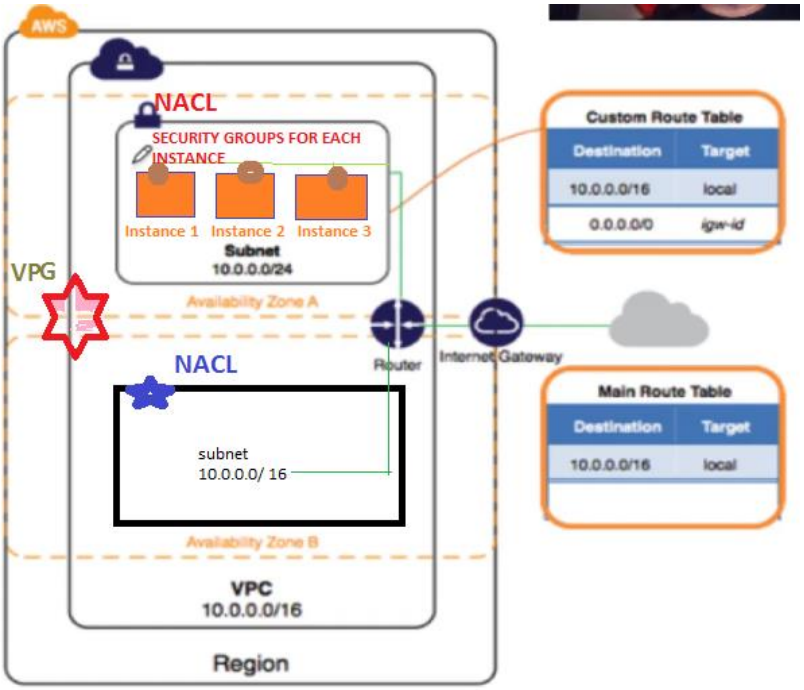
- VPC is similar to having the **own datacenter** inside the AWS (Think of the virtual data center u have under your account in the cloud. So no one can come into your VPC without your permission.)
- Logically isolated from other VPC (Ccloud Security)
- AWS has **multiple Regions**
- Regions have **multiple availability zones**.
- VPC is **region specific** (For hosting region is very important)
- Single VPC spends between the **multiple availability zone**
- You can have **1 or more IP address subnets** in one availability zone
  Can a subnet extend between the two availability zone? **It cannot**
  Can a VPC extends between the two regions? **It cannot**

  Whatever you are going to build under the VPC is in our control. I.e.) AWS Client has the full control over resources & virtual compute instances (virtual servers) hosted inside that VPC.
  you can create terminate stop restart reboot your own EC2 instances the same as we go through the storage and other services as well within the PC.



Components of VPC

Through the Virtual private Gateway -> expose the VPC to the headquaters of the company. So that the employees can use the server that is hosted in the VPC



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Main Route Table

Destination	Target
10.0.0.0/16	local

1. CIDR and IP address subnets

   Eg .. IP Range (10.0.0.0 , 172.16.0.0/16, 192.168.0.0/16) is used for VPC 1
   What is the same IP Range is used for another VPC? **It doesn't matter because the VPC is isolated**

2. Implied Router

   The communication between the subnets within / between the availability zone is made possible through the **Router**
   Scenerio flow:
   - Subnet 1 (web server) inside the availability zone 1 can contact with the Subnet 2 (database server) inside the availability zone 2 with the help of **then logical router. These routers will be there by default**
   - **Router** will also help the subnets to communicate with the outside world

3. Route Tables
   - *Ok, now I have question …how the* ***router*** *knows that subnet 1 is sending data to the subnet 2 and not to Subnet 3?*

     This can be made possible through the route table in which the Subnet 1 has the destination address of the Subnet 2 .

4. Internet Gateway –
   AWS can able to contact the outside world through the IGW (0.0.0.0/0)

5. Security Groups
   It will protect our server instances/ EC2 Instances defined within your VPC.
   It works at the Virtual NIC/ Elastic Network Interface. Think of the NIC Card in the computer/ laptop
   Thus the security group works at the EC2 Instance level (EG: each computer has 1 NIC)

6. Network Access Control Lists (N. ACLs)

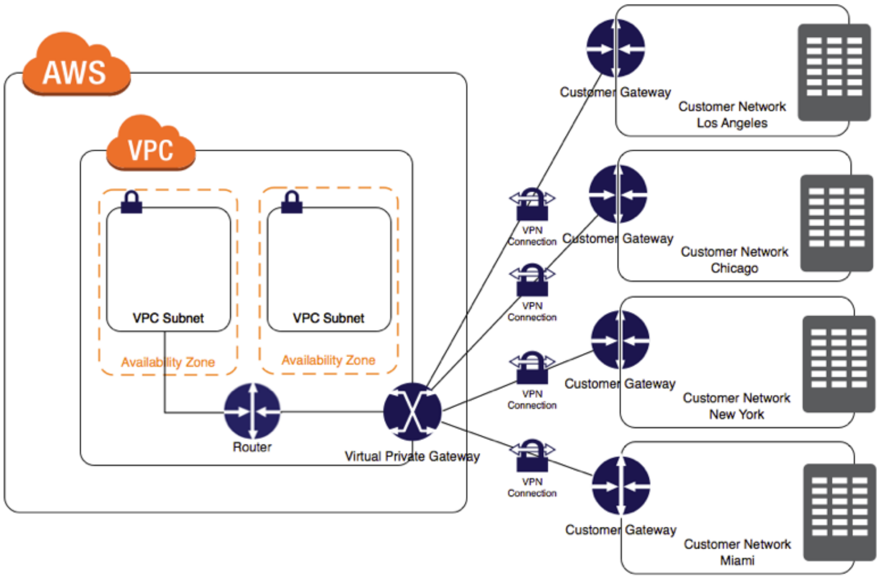
NACL is applied to the full subnet that acts as a firewall for controlling traffic in and out of one or more subnets..

7. Virtual Private Gateway

Connect the VPC to the headquarters of the company. If I would like to connect my VPC to my headquarters . So the employes can connect to my servers that are hosted in the VPC. It is like the IGW (Internet Gateway) which will take our data to the outside world
VPG will take our data to the Private network world(ie) any private company.

Eg) onecognizant.cognizant.com server is hosted in the VPC inside the aws.

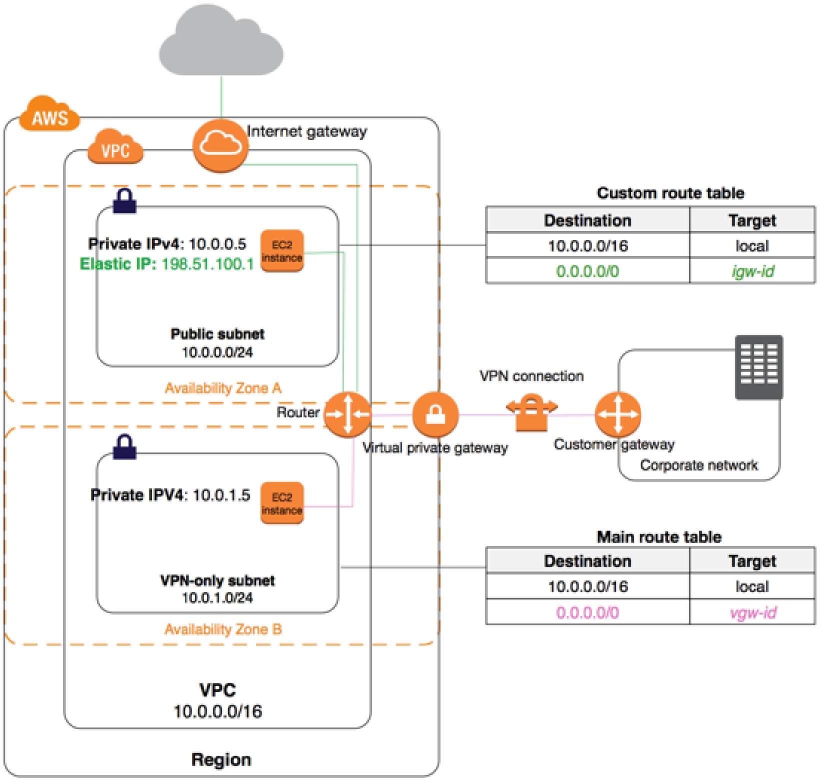
Employees can able to access the server in the cognizant network. So with the help of VPG the data can be accessed by the employees in the cognizant from the AWS VPC. This occurs in the VPN (Virtual private network)



IPV6 Addressing

- *IPV6 Addresses are always public. There is no private.*
- *AWS host any server through the IPV6 address range . so that the ip address will not be duplicated as it is public*

Let's see everything in detail………………



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*vgw-id*

IMPLIED ROUTER (common router / public router)

We don’t need to configure in the implied router because already aws people have configured in our default Implied router.

- Implied Router is the **CENTRAL VPC Routing** function, that communicates between the subnets or from subnets to the outside world (IGW) or from subnets to VPG(Virtual private Gateway)

- Sometimes there will be more subnets in one availability zone. All the subnets will be connected to the router.Subnets cannot be connected directly to another subnets eventhough they are in the same availability zone.

  Now how does this routing happens in the route table??

- **Each subnet** will have the custom route table (created by us not AWS)

- **MAIN Route table** is created default automatically by the AWS for the VPC
- **Each route table has multiple entries** in the table and the multiple entries determines the multiple internal destinations / external/any destinations (outside world) [0.0.0.0 / 0]
  - **For external/any destinations** If the data packet from the subnet 1 points to the [0.0.0.0/ 0] in the routing table na then the router target will be ***igw-id.*** So the router send the data packet to the Internet Gateway ID (IGW) which will communicate with the external world

  - **For internal destinations** if the data packet from the subnet 1 (range 10.0…something) points to the range of (10.0… something) in the route table .. then it comes under the **CIDR block** of our own VPC and the target will be local. Thus the routing takes place internally within the VPC. It wont send the data packet to the gateways/ virtual gateways

- You can have **200 Route tables** in the single VPC
- You can have **50 Route entries** in the single route table

- Each subnet **must be associated with only one route table** at any given time. If the subnet is not associated with any route table then that particular subnet will be automatically / by default routed to the **MAIN/default route table**

  Can I attach the subnet to multiple Route tables at the same time? No

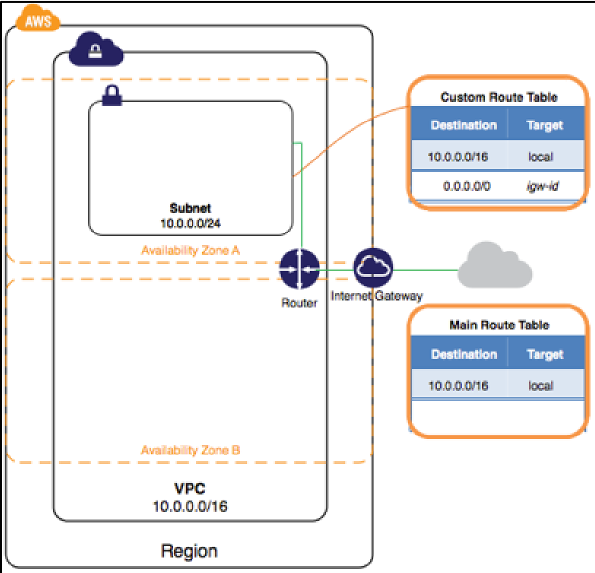
  Can I use the route table to associate multiple subnet at the same time ? yes

  "Oru route table la multiple subnet irukalam but oru saubnet multiple route table la irukka koodathu.."

- You can change/swap the subnet association to another route table but that particular subnet should not be in 2 route table

- You can edit the main route table but you cannot delete the main route table from the console/ Command line interface

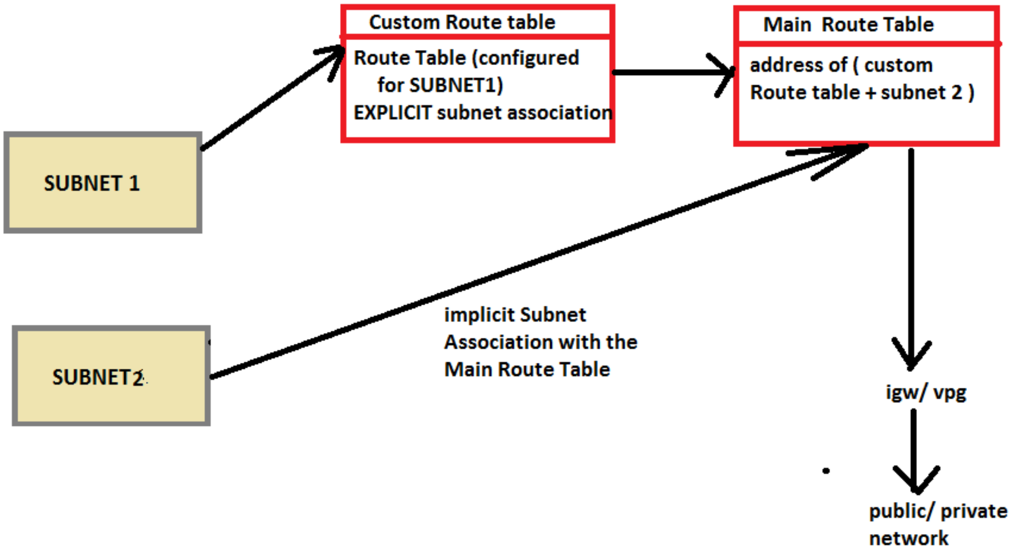
- Every route table in the VPC comes with the default rule that allows all VPC subnets to communicate with one another. ***you cannot modify or delete this rule.***



****10.0.0.0/16 is the default entry in the main route table and all other route Table when a VPC is created**

****because inside the vpc there are many availability zones and many subnets. They all are in local target. ie) if the data packet is pointing to the 10.0.0.0/16 . then the router will not send the data packet to the IGW/ VPG and the data packet revolves inside the VPC**

Route Table Association

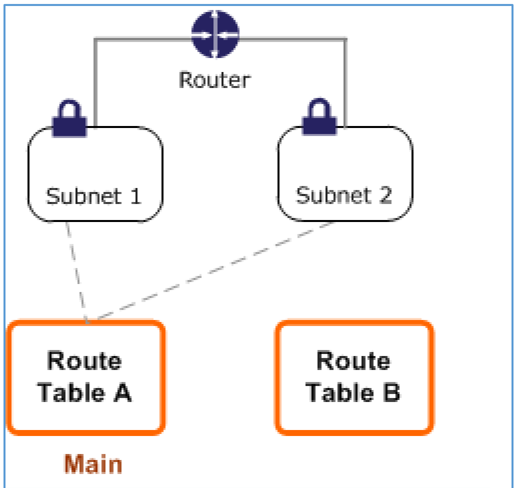

Custom Route table
Route Table (configured for SUBNET1)
EXPLICIT subnet association
Main Route Table
address of (custom Route table + subnet 2)
SUBNET 1
SUBNET2
implicit Subnet Association with the Main Route Table
igw/ vpg
public/ private network

Subnets can be implicitly or explicitly associated with the main route table. Subnets typically won't have an explicit association to the main route table, although it might happen temporarily if you're replacing the main route table.

You might want to make changes to the main route table, but to avoid any disruption to your traffic, you can first test the route changes using a custom route table. After you're satisfied with the testing, you then replace the main route table with the new custom table.

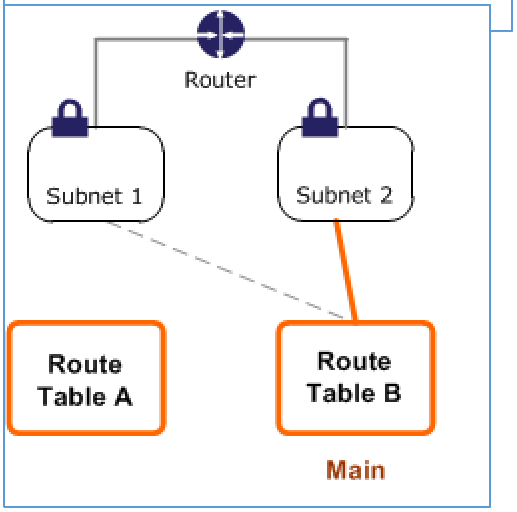
the "Main" route table will be used by subnets unless another route table is specifically configured for those subnets. You can think of the "Main" route table as the default route table, which will be used until another route table is specifically assigned.

As far as defining the terms implicit and explicit, in this context implicit means that it's using that route table because it's the "Main" route table and nothing else has been defined. Explicit would mean that a route table has been configured for use on that subnet.

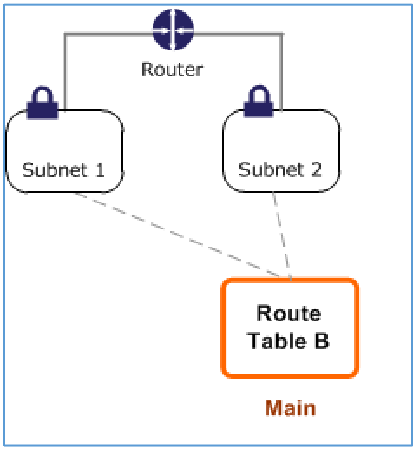


The following diagram shows a VPC with two subnets that are implicitly associated with the main route table (Route Table A), and a custom route table (Route Table B) that isn't associated with any subnets.

You can create an explicit association between Subnet 2 and Route Table B.



After you've tested Route Table B, you can make it the main route table. Note that Subnet 2 still has an explicit association with Route Table B, and Subnet 1 has an implicit association with Route Table B because it is the new main route table. Route Table A is no longer in use.



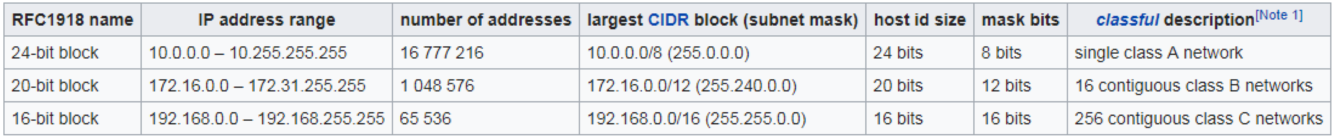
If you disassociate Subnet 2 from Route Table B, there's still an implicit association between Subnet 2 and Route Table B. If you no longer need Route Table A, you can delete it.

VPC IP addressing .

In VPC , AWS have given full control to us to create and use the IP Address range . But the IP address range should be from RFC 1918 or Public routable IP Address block that you have registered / assigned to u

RFC 1918:

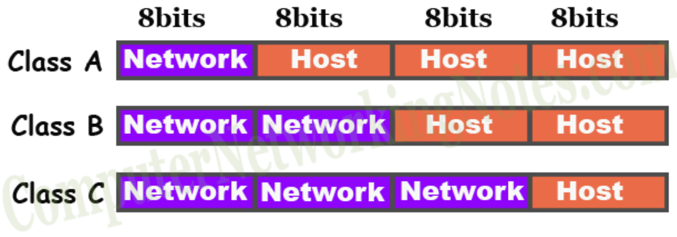
- It is the private address space.
- The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP Address space for the private Internets

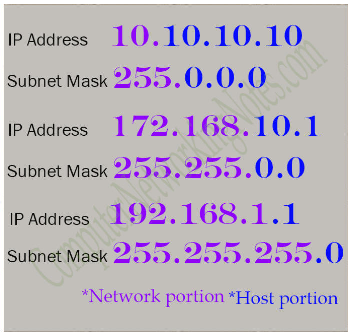


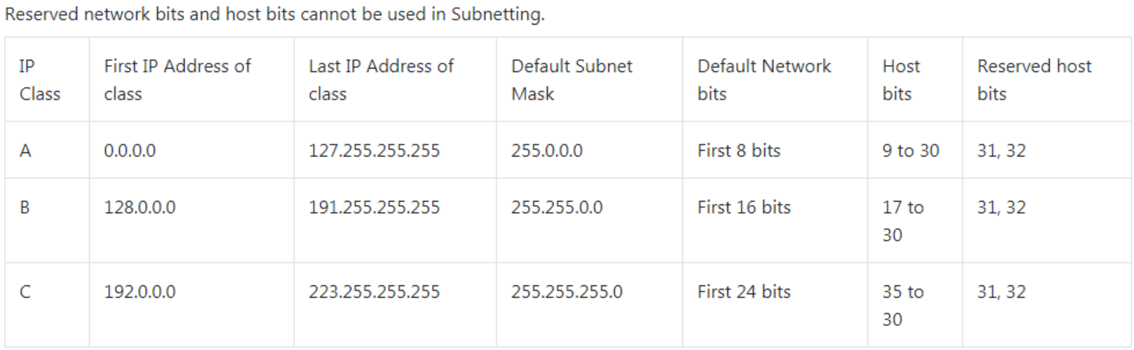
RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits	*classful* description[Note 1]
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65 536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

In class A, B and C: -

First 8, 16 and 24 bits are reserved for network portion respectively.
Last 2 bits (31 & 32) are reserved for host portion.





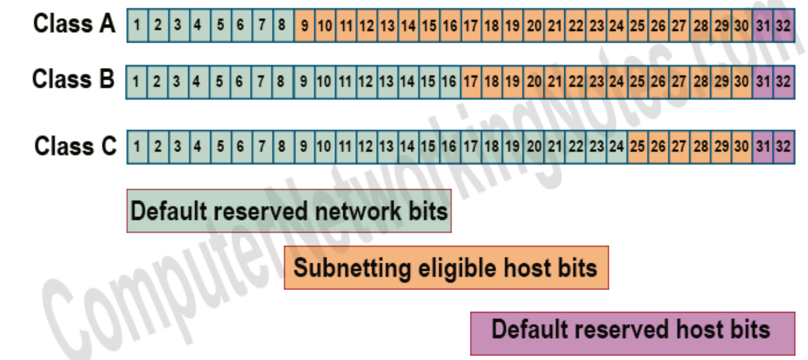


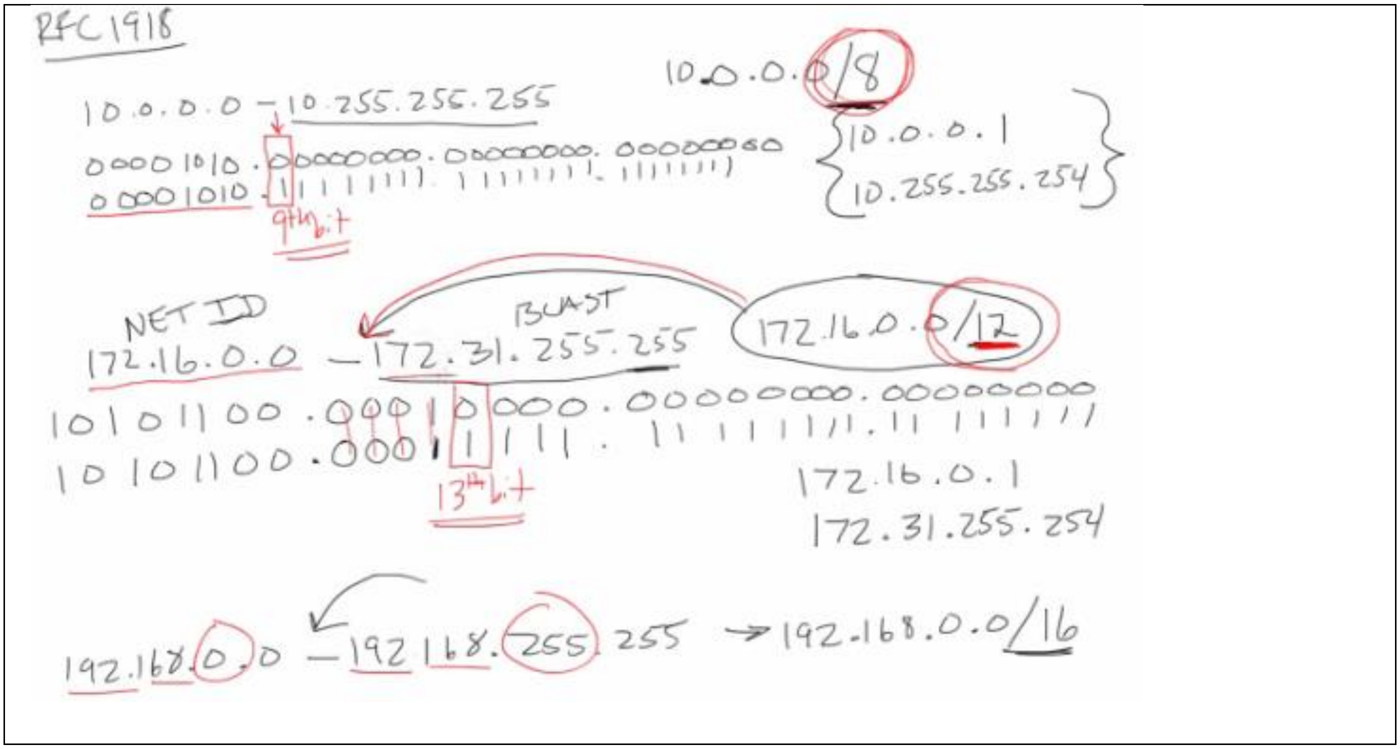
Reserved network bits and host bits cannot be used in Subnetting.

IP Class	First IP Address of class	Last IP Address of class	Default Subnet Mask	Default Network bits	Host bits	Reserved host bits
A	0.0.0.0	127.255.255.255	255.0.0.0	First 8 bits	9 to 30	31, 32
B	128.0.0.0	191.255.255.255	255.255.0.0	First 16 bits	17 to 30	31, 32
C	192.0.0.0	223.255.255.255	255.255.255.0	First 24 bits	35 to 30	31, 32

Subnetting eligible host bits

After excluding reserved network bits and host bits, remaining bits are considered as Subnetting eligible host bits.

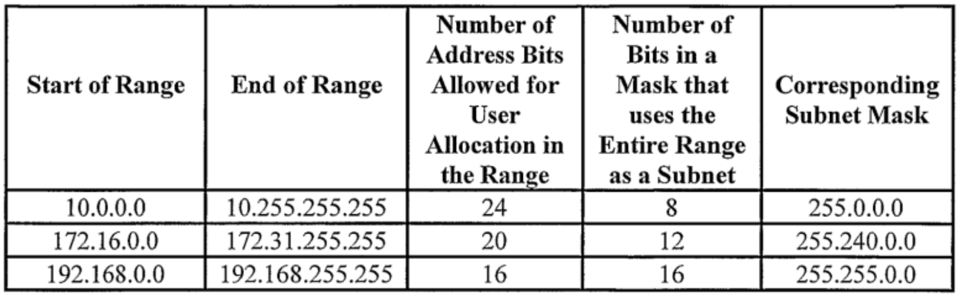




1. Once the VPC is created then, you cannot change its CIDR (***Classless Inter-Domain Routing** is a method for allocating IP addresses and IP routing*.) block range

The CIDR block address range is assigned like

- 10.0.0.0/8 [8 subnets and each subnet have 24 host ids and 2^24 ip addresses] - Consists of total 16,777,216 IPv4 Addresses. Class A range of private IPv4 addresses are used for large network which need a bigger pool IPv4 addresses.
- 176.16.0.0/16 [16 subnets and each subnet have 16 host ids and 2^16 ip addresses] - Consists of total 1,048,576 IPv4 Addresses. Class B range of private IPv4 addresses are used for medium-sized network.
- 192.168.0.0/24 [24 subnets and each subnet have 8 host ids and 2^8 ip addresses] - Consists of total 65,536 IPv4 Addresses. Class C range of private IPv4 addresses are used for small networks.



Start of Range	End of Range	Number of Address Bits Allowed for User Allocation in the Range	Number of Bits in a Mask that uses the Entire Range as a Subnet	Corresponding Subnet Mask
10.0.0.0	10.255.255.255	24	8	255.0.0.0
172.16.0.0	172.31.255.255	20	12	255.240.0.0
192.168.0.0	192.168.255.255	16	16	255.255.0.0

Once the "CREATE VPC" button is clicked – then the CIDR address block will be assigned that cannot be changed further. If u start a company with few IP address in the VPC and gradually if u want to increase the ip address then u can't do anything, 🙁 you need to create a new VPC with the large IP address and migrate the old VPC to the new VPC

Note: CIDR block can be create with either /28 and /16

- /28 - IPV4 address length or identification of network or subnets and 4 - number of host / EC2 instances and 2^4=16 Ip addresses are assigned [Minimum size]

- /16 - IPV4 address length or identification of network or subnets and 16 - number of host / EC2 instances and 2^16 Ip addresses are assigned [Maximum size]

2. If u need a different CIDR Size, Create a new VPC.

3. Different subnets in the VPC cannot overlap (basic TCP/IP rule)

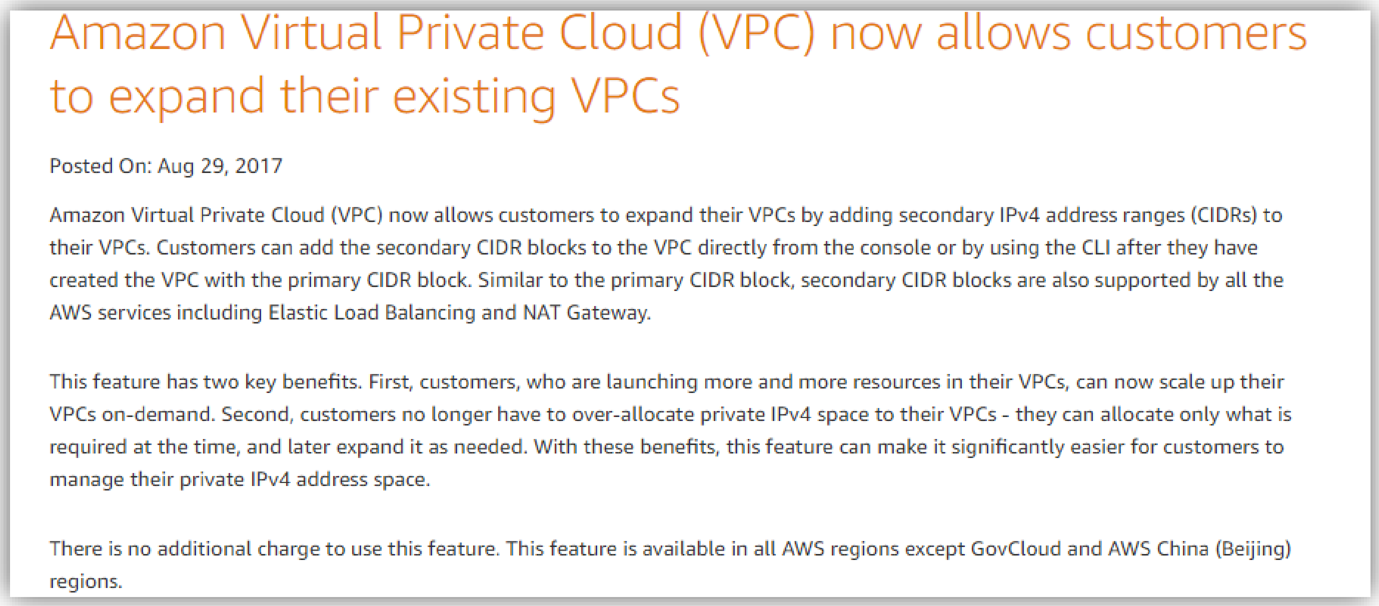
In the particular VPC, the subnets cannot overlap
Eg) if one subnet is 10.0.0.0/24
00001010.00000000.00000000 (Network).00000000(host)
00001010.00000000.00000000 (Network).11111111(host)
[10.0.0.0 - 10.0.0.255] - Range of IP Address
10.0.0.0- Network ID
10.0.0.255- Host ID
2^8 -> 256 ->0-255 ip address
10.0.0.1 to 10.0.0.254 -> usable IP address

If another subnet is 10.0.0.0/28
00001010.00000000.00000000.11110000(host)
00001010.00000000.00000000.11111111(host)
[10.0.0.236 - 10.0.0.255] - Range of IP Address
10.0.0.236 - Network ID
10.0.0.255 - Host ID
2^4 ->16 -> 0-15 ip address
10.0.0.237 to 10.0.0.254 -> usable IP address

Result ->
0-255 -> IP address for 10.0.0.0/24
0-15-> IP address for 10.0.0.0/28
" ip addresses overlaps that is not possible”

4. You can however, expand your VPC CIDR block by adding new / extra ip address ranges/ CIDR block

If your VPC is in production and u want more IP address for expanding but u don’t want to delete / migrate the VPC. Then u can add the CIDR block with some limitations.



Amazon Virtual Private Cloud (VPC) now allows customers to expand their existing VPCs

Posted On: Aug 29, 2017

Amazon Virtual Private Cloud (VPC) now allows customers to expand their VPCs by adding secondary IPv4 address ranges (CIDRs) to their VPCs. Customers can add the secondary CIDR blocks to the VPC directly from the console or by using the CLI after they have created the VPC with the primary CIDR block. Similar to the primary CIDR block, secondary CIDR blocks are also supported by all the AWS services including Elastic Load Balancing and NAT Gateway.

This feature has two key benefits. First, customers, who are launching more and more resources in their VPCs, can now scale up their VPCs on-demand. Second, customers no longer have to over-allocate private IPv4 space to their VPCs - they can allocate only what is required at the time, and later expand it as needed. With these benefits, this feature can make it significantly easier for customers to manage their private IPv4 address space.

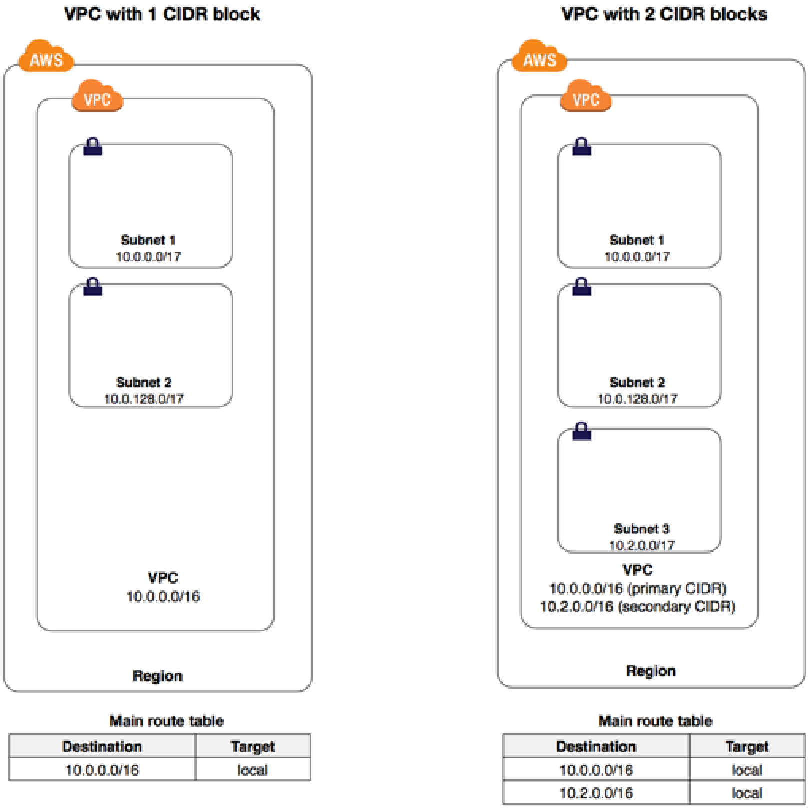
There is no additional charge to use this feature. This feature is available in all AWS regions except GovCloud and AWS China (Beijing) regions.

When the CIDR BLOCK is included in the VPC, then all the route table in the VPC will get updated as below

Adding IPv4 CIDR Blocks to a VPC

You can associate secondary IPv4 CIDR blocks with your VPC. When you associate a CIDR block with your VPC, a route is automatically added to your VPC route tables to enable routing within the VPC (the destination is the CIDR block and the target is local).

In the following example, the VPC on the left has a single CIDR block (10.0.0.0/16) and two subnets. The VPC on the right represents the architecture of the same VPC after you've added a second CIDR block (10.2.0.0/16) and created a new subnet from the range of the second CIDR.

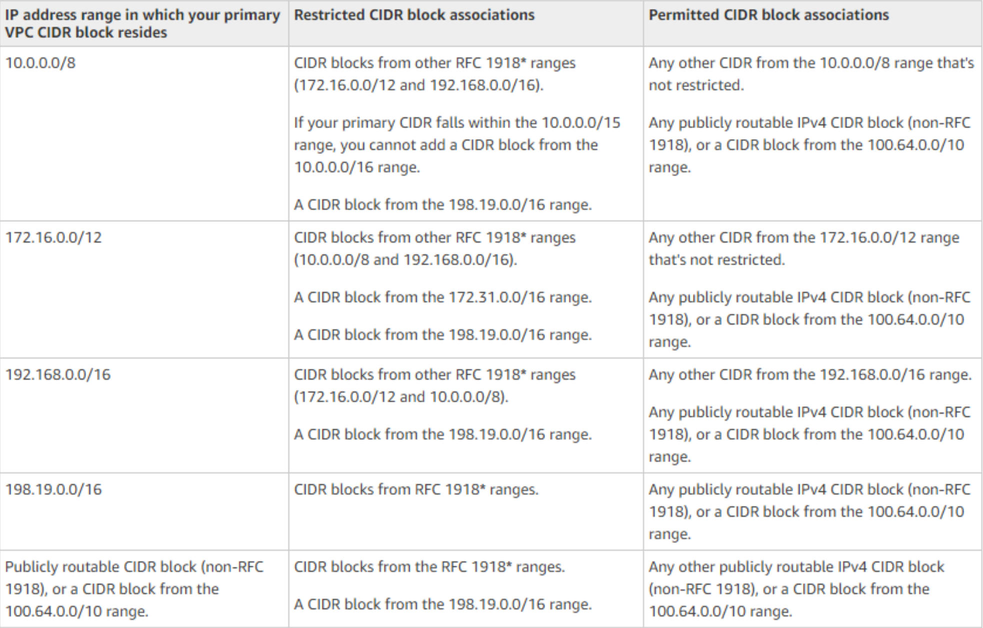


Main route table

Destination	Target
10.0.0.0/16	local

Main route table

Destination	Target
10.0.0.0/16	local
10.2.0.0/16	local



IP address range in which your primary VPC CIDR block resides	Restricted CIDR block associations	Permitted CIDR block associations
10.0.0.0/8	CIDR blocks from other RFC 1918* ranges (172.16.0.0/12 and 192.168.0.0/16). If your primary CIDR falls within the 10.0.0.0/15 range, you cannot add a CIDR block from the 10.0.0.0/16 range. A CIDR block from the 198.19.0.0/16 range.	Any other CIDR from the 10.0.0.0/8 range that's not restricted. Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
172.16.0.0/12	CIDR blocks from other RFC 1918* ranges (10.0.0.0/8 and 192.168.0.0/16). A CIDR block from the 172.31.0.0/16 range. A CIDR block from the 198.19.0.0/16 range.	Any other CIDR from the 172.16.0.0/12 range that's not restricted. Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
192.168.0.0/16	CIDR blocks from other RFC 1918* ranges (172.16.0.0/12 and 10.0.0.0/8). A CIDR block from the 198.19.0.0/16 range.	Any other CIDR from the 192.168.0.0/16 range. Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
198.19.0.0/16	CIDR blocks from RFC 1918* ranges.	Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
Publicly routable CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.	CIDR blocks from the RFC 1918* ranges. A CIDR block from the 198.19.0.0/16 range.	Any other publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.

AWS Reserved IP for each subnets

If subnet **10.0.0.0/24** - has

00001010.00000000.00000000.00000000 - 0

00001010.00000000.00000000.11111111 - 255

0 to 255 -> 256 ip address.

My question is can we use all the 256 IP address? The answer is **NO**

AWS has some reserved IP address for each subnet u create .

- First 4 IP addresses and last one are reserved by the AWS
- If subnet **10.0.0.0/24** - has

  00001010.00000000.00000000.00000000 - 0

  00001010.00000000.00000000.11111111 - 255

  0 to 255 -> 256 ip address.

  In that 4-254 ->251 usable IP address

10.0.0.0 - Network address (base router)

10.0.0.1- Reserved by AWS for the VPC router. (Implied Router)

10.0.0.2- Reserved by AWS for mapping to the Amazon-provided DNS with the subnet . (Note that the IP address of the DNS server is the base of the VPC network range plus two.)

10.0.0.3- Reserved by AWS for future use.

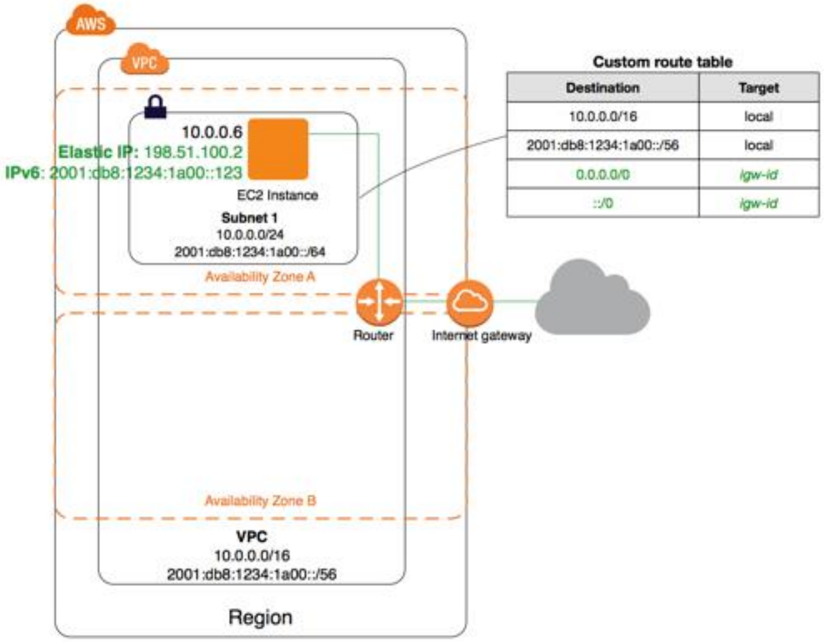
10.0.0.255- Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

INTERNET GATEWAY

If the VPC is created, then by default we will be having the IGW (Internet Gateway) to communicate with the VPC. IGW has the VPC Subnets and the EC2 instance configured on them to communicate with the internet

- It is horizontally scalable or scale dynamically (more physical component (eg.load balancer) can be added for balancing the node)and It is used whenever a high availability of (server) services are required. Horizontal-scaling is often based on partitioning of the data in which each node contains only part of the data. Load balancer will take care of the bandwidth constraints
- Redundant – There will be components that is not used but when the working component fails then this back up component will come into action
- It supports IPV4 and IPV6
- Performs **NAT(Network Address Translator)** for the instances ie) Our instance will be in the private ipv4 address .. this NAT will translate the private address to the Public address (elastic IP) and vice versa.

Instances will have the Metadata and in the metadata the Elastic IP is configured . They cannot be exposed on the instance . This elastic IP will be in the IGW and in metadata of the Instance.

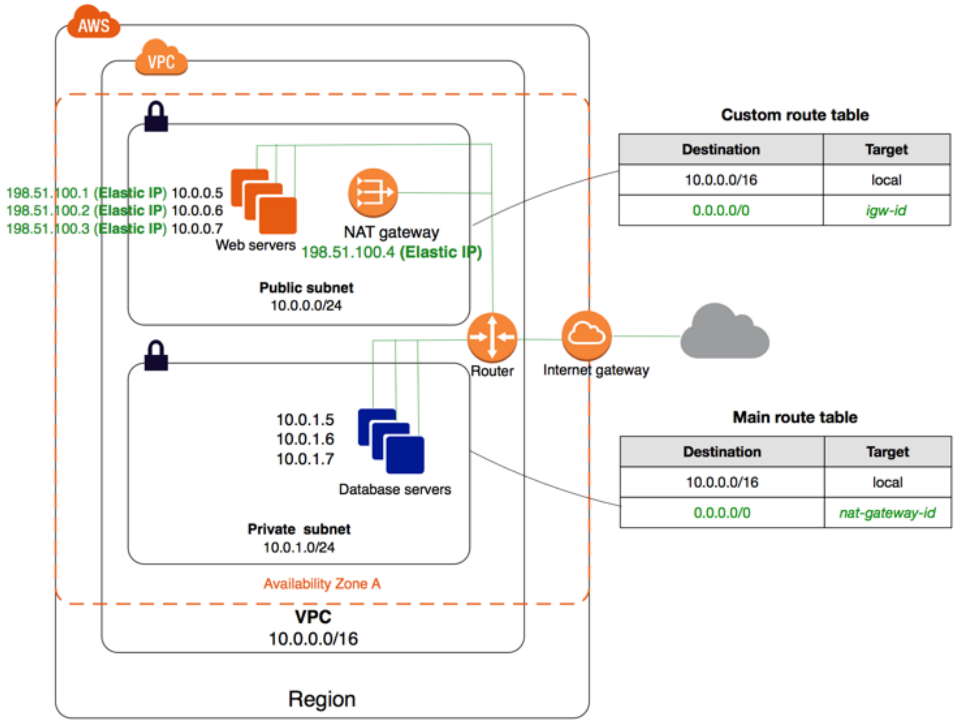


Custom route table

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	igw-id
::/0	igw-id

- A virtual private cloud (VPC) with a size /16 IPv4 CIDR block (example: 10.0.0.0/16). This provides 65,536 private IPv4 addresses.
- A subnet with a size /24 IPv4 CIDR block (example: 10.0.0.0/24). This provides 256 private IPv4 addresses.
- An Internet gateway. This connects the VPC to the Internet and to other AWS services.
- An instance with a private IPv4 address in the subnet range (example: 10.0.0.6), which enables the instance to communicate with other instances in the VPC, and an Elastic IPv4 address (example: 198.51.100.2), which is a public IPv4 address that enables the instance to be reached from the Internet.
- A custom route table associated with the subnet. The route table entries enable instances in the subnet to use IPv4 to communicate with other instances in the VPC, and to communicate directly over the Internet. A subnet that's associated with a route table that has a route to an Internet gateway is known as a *public subnet*.

PUBLIC SUBNET AND PRIVATE SUBNET



Custom route table

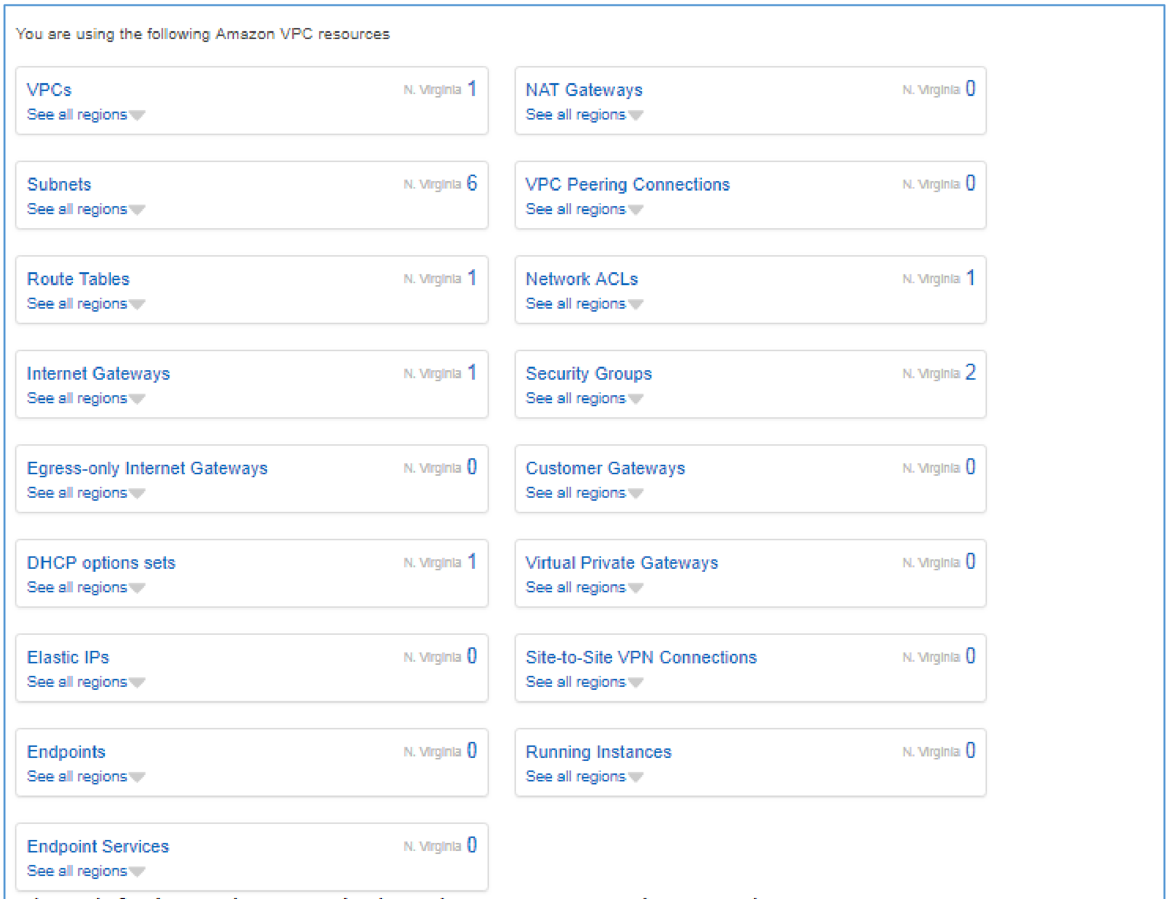
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

1. **Public subnet** may be the web servers that is available for the users of the web application -> Each instance in the public subnet will have the mapped Elastic IP -> The elastic IP is used to contact the internet through the internet gateway id
2. **Private Subnet** may be the database servers that is not available directly to the internet / may be back-end servers that don't need to accept incoming traffic from the Internet and therefore do not have public IP addresses; however, they can send requests to the Internet using the NAT gateway But for some software updates we need internet . In that case the private subnet will be having the NAT GATEWAY ID. The NAT gateway ID is located in the public subnet which has its own Elastic IP. Thus, the private subnets communicate to the internet through the NAT – Gateway - id

PRACTICAL SESSION- VPC



You are using the following Amazon VPC resources

VPCs N. Virginia 1
See all regions

NAT Gateways N. Virginia 0
See all regions

Subnets N. Virginia 6
See all regions

VPC Peering Connections N. Virginia 0
See all regions

Route Tables N. Virginia 1
See all regions

Network ACLs N. Virginia 1
See all regions

Internet Gateways N. Virginia 1
See all regions

Security Groups N. Virginia 2
See all regions

Egress-only Internet Gateways N. Virginia 0
See all regions

Customer Gateways N. Virginia 0
See all regions

DHCP options sets N. Virginia 1
See all regions

Virtual Private Gateways N. Virginia 0
See all regions

Elastic IPs N. Virginia 0
See all regions

Site-to-Site VPN Connections N. Virginia 0
See all regions

Endpoints N. Virginia 0
See all regions

Running Instances N. Virginia 0
See all regions

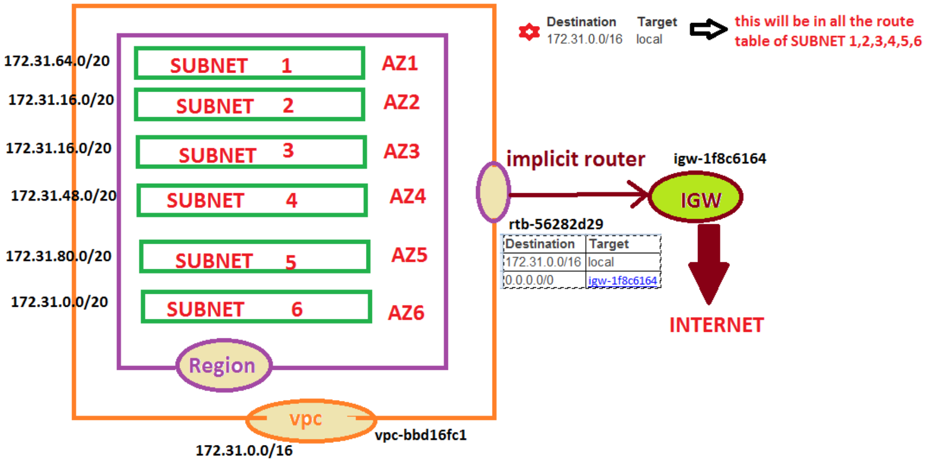
Endpoint Services N. Virginia 0
See all regions

* A default VPC is created when the AWS account is created

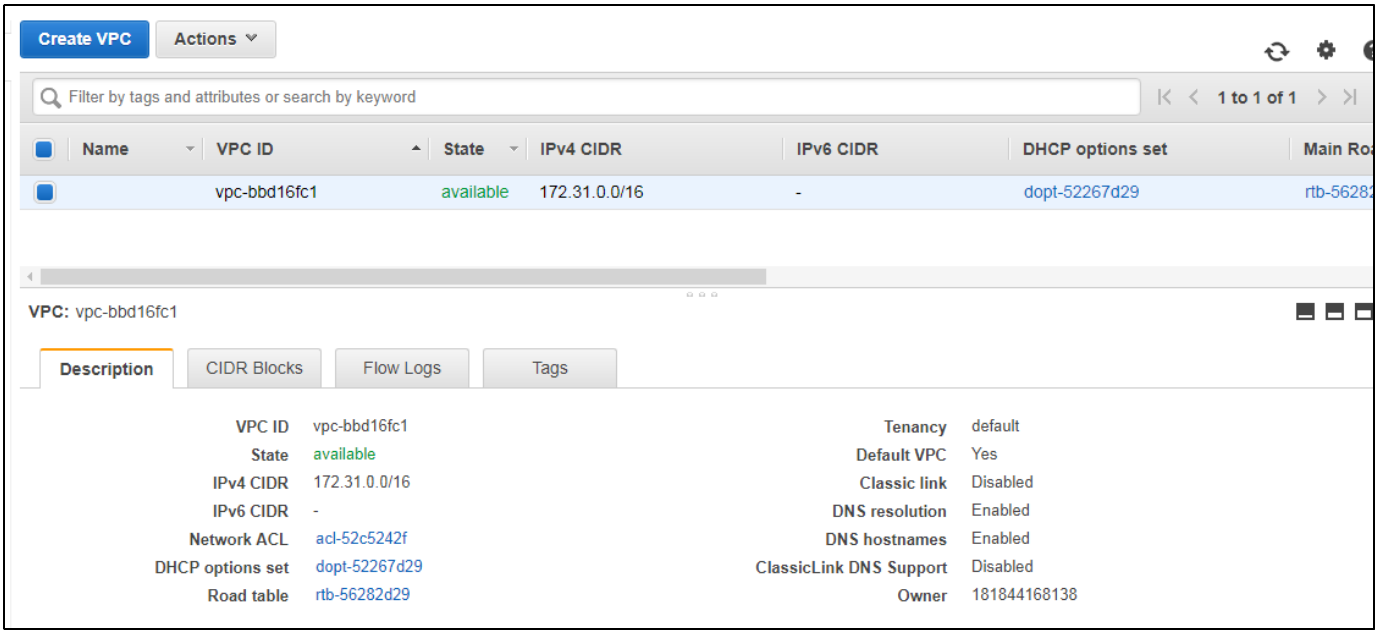
* The numbers mentioned in the above diagram varies with respect to the regions choosen

* Here Each VPC has some availability zone

*** Each availability zone has 1 subnet . Here we have 6 subnets , ie) North.Virginia has 6 availability zone**



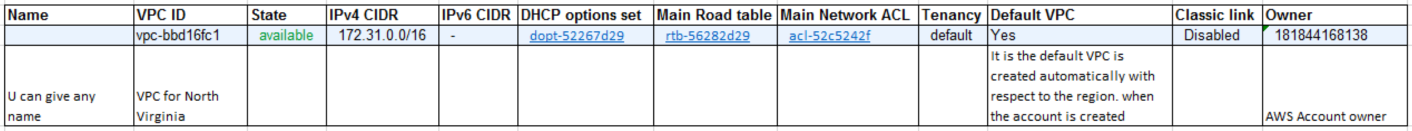
DEFAULT VPC



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Ro
	vpc-bbd16fc1	available	172.31.0.0/16	-	dopt-52267d29	rtb-5628

VPC: vpc-bbd16fc1

VPC ID	vpc-bbd16fc1	Tenancy	default
State	available	Default VPC	Yes
IPv4 CIDR	172.31.0.0/16	Classic link	Disabled
IPv6 CIDR	-	DNS resolution	Enabled
Network ACL	acl-52c5242f	DNS hostnames	Enabled
DHCP options set	dopt-52267d29	ClassicLink DNS Support	Disabled
Road table	rtb-56282d29	Owner	181844168138



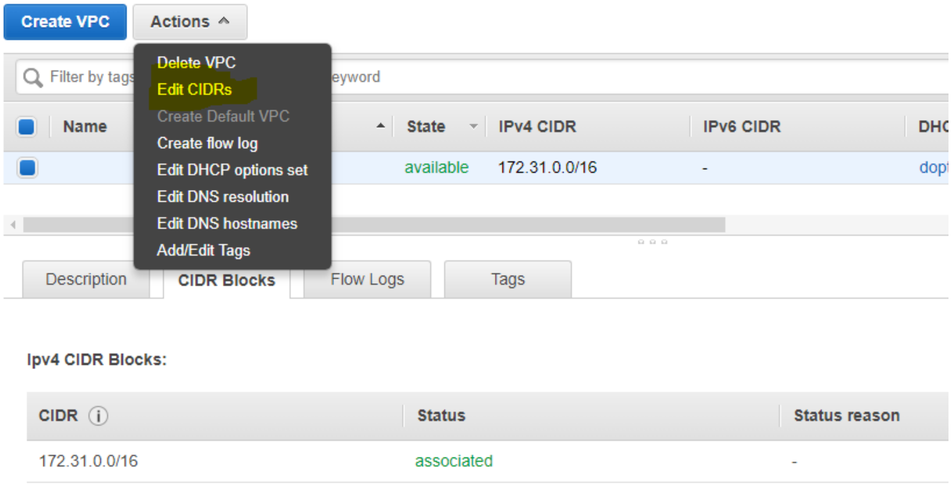
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Road table	Main Network ACL	Tenancy	Default VPC	Classic link	Owner
	vpc-bbd16fc1	available	172.31.0.0/16	-	dopt-52267d29	rtb-56282d29	acl-52c5242f	default	Yes	Disabled	181844168138
U can give any name	VPC for North Virginia								It is the default VPC is created automatically with respect to the region. when the account is created		AWS Account owner

IPV4 CIDR:

This CIDR consist of larger IP address
172.31.0.0 - 172.31.255.255
172.31.0.0- Network address
172.31.0.1 - Implicit Router
172.31.0.2 - DNS Server
172.31.0.3- Reserved by AWS for future use
172.31.255.255- Network broadcast Address
172.31.0.4 - 172.31.255.254 - Usable IP address

****/16 - Large set of IP address - 2^(32-16) = 2^16 IP address**
****/28 - small set of IP address - 2_(32-28) = 2^4 IP address**

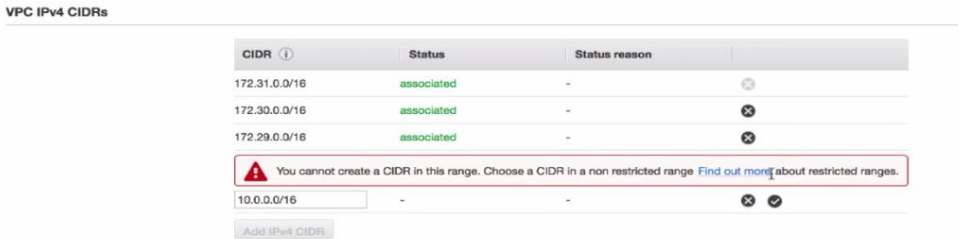
- Before August 2017, Once the CIDR Block is created in VPC it cannot be expanded. But if u need to expand na, just delete/ migrate the VPC and create a new one.
- After August 2018, u can add extra the CIDR block with some limitations but u cannot resize it.



Name	State	IPv4 CIDR	IPv6 CIDR	DHC
	available	172.31.0.0/16	-	dopt

Ipv4 CIDR Blocks:

CIDR	Status	Status reason
172.31.0.0/16	associated	-


VPC IPv4 CIDRs

CIDR	Status	Status reason
172.31.0.0/16	associated	-
172.30.0.0/16	associated	-
172.29.0.0/16	associated	-

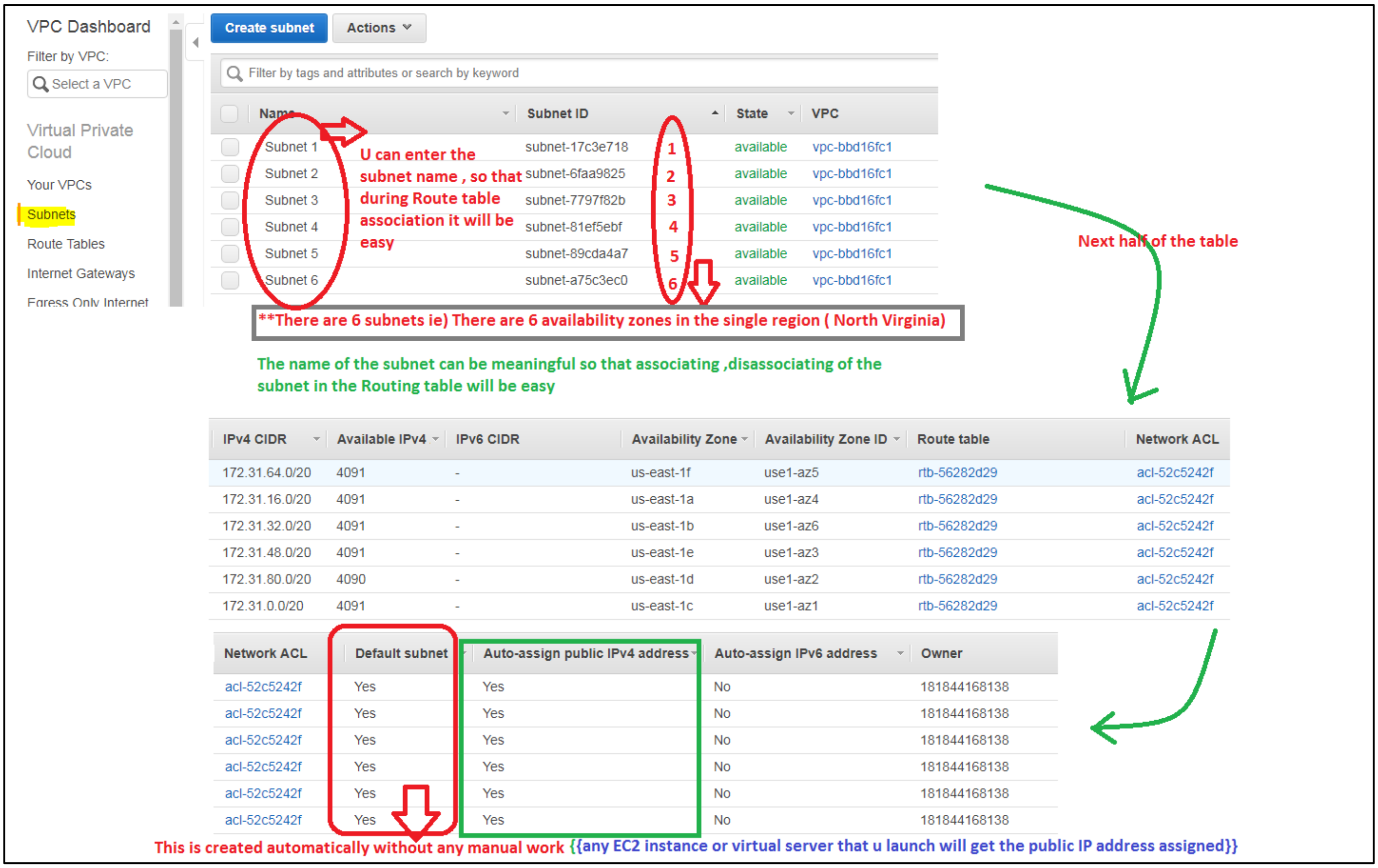
You cannot create a CIDR in this range. Choose a CIDR in a non restricted range Find out more about restricted ranges.

10.0.0.0/16 -

DEFAULT SUBNET

A subnet can be thought of as dividing a large network into smaller networks. This is done because maintenance of smaller networks is easier and it also provides security to the network from other networks

Can we stretch the subnet between the availability zone? The answer is **NO**. because the subnet should be within the availability zone and it cannot be shared/ stretched between the availability zone. U can have more subnets in an availability zone



U can enter the subnet name , so that during Route table association it will be easy

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table	Network ACL	Default subnet	Auto-assign public IPv4 address	Auto-assign IPv6 address	Owner
Subnet 1	subnet-17c3e718	available	vpc-bbd16fc1	172.31.64.0/20	4091	-	us-east-1f	use1-az5	rtb-56282d29	acl-52c5242f	Yes	Yes	No	181844168138
Subnet 2	subnet-6faa9825	available	vpc-bbd16fc1	172.31.16.0/20	4091	-	us-east-1a	use1-az4	rtb-56282d29	acl-52c5242f	Yes	Yes	No	181844168138
Subnet 3	subnet-7797f82b	available	vpc-bbd16fc1	172.31.32.0/20	4091	-	us-east-1b	use1-az6	rtb-56282d29	acl-52c5242f	Yes	Yes	No	181844168138
Subnet 4	subnet-81ef5ebf	available	vpc-bbd16fc1	172.31.48.0/20	4091	-	us-east-1e	use1-az3	rtb-56282d29	acl-52c5242f	Yes	Yes	No	181844168138
Subnet 5	subnet-89cda4a7	available	vpc-bbd16fc1	172.31.80.0/20	4090	-	us-east-1d	use1-az2	rtb-56282d29	acl-52c5242f	Yes	Yes	No	181844168138
Subnet 6	subnet-a75c3ec0	available	vpc-bbd16fc1	172.31.0.0/20	4091	-	us-east-1c	use1-az1	rtb-56282d29	acl-52c5242f	Yes	Yes	No	181844168138

**There are 6 subnets ie) There are 6 availability zones in the single region (North Virginia)

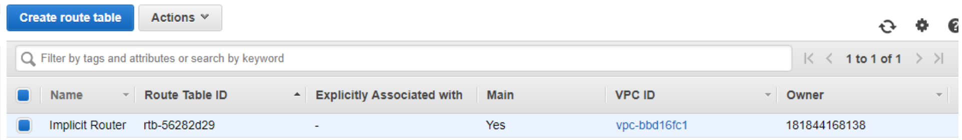
The name of the subnet can be meaningful so that associating ,disassociating of the subnet in the Routing table will be easy

This is created automatically without any manual work {{any EC2 instance or virtual server that u launch will get the public IP address assigned}}

Auto Assign IPv4 address: You will get the public IP address. So that u can access the server/ instance anywhere and anytime. But should have right credentials to authenticate and be authourize to work on.

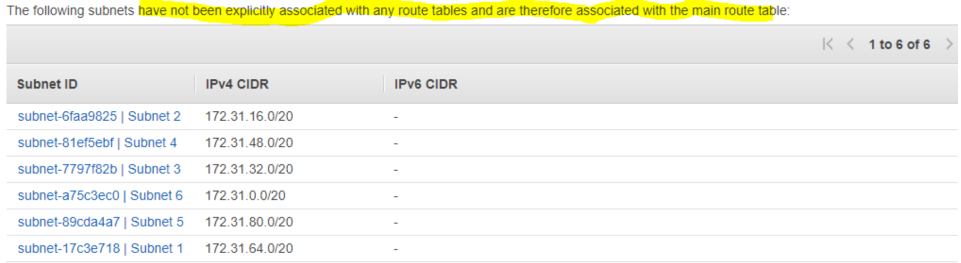
Default Route Table

The router is a device that could be a logical, device, software that can route ur traffic. The traffic comes from the VPC would like to go out / to another availability zone. **The traffic within, to , from the VPC is taken care by the router.**



Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
Implicit Router	rtb-56282d29	-	Yes	vpc-bbd16fc1	181844168138

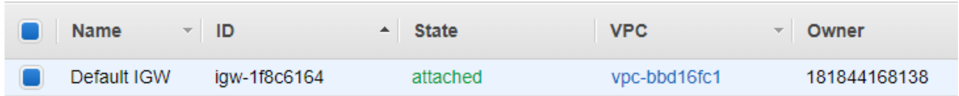
All the subnets are directly pointed to the Implicit Router because by default they are considered as the public network


The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

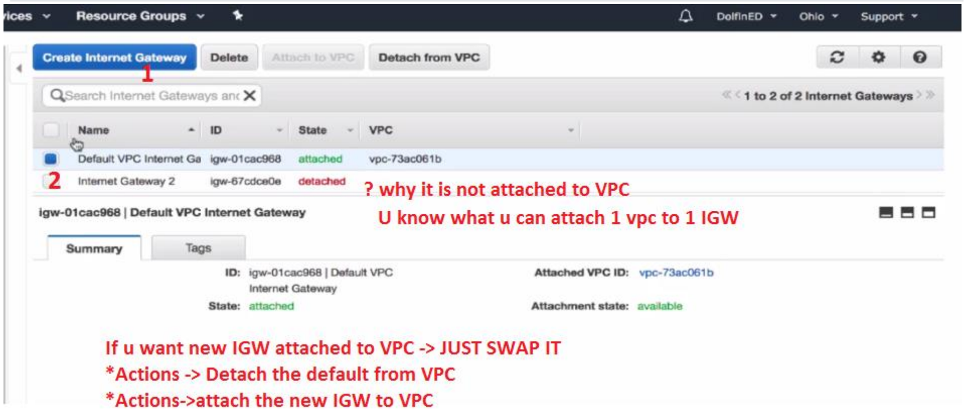
Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-6faa9825 | Subnet 2	172.31.16.0/20	-
subnet-81ef5ebf | Subnet 4	172.31.48.0/20	-
subnet-7797f82b | Subnet 3	172.31.32.0/20	-
subnet-a75c3ec0 | Subnet 6	172.31.0.0/20	-
subnet-89cda4a7 | Subnet 5	172.31.80.0/20	-
subnet-17c3e718 | Subnet 1	172.31.64.0/20	-

Can I attach 1 route table to Multiple subnets	yes
can I have 1 subnets associated with the multiple route table?	No
can I have 1 subnets associated with the 1 route table change or being associate with another route table?	yes
Can I attach more than 1 IGW in a VPC	No

Default IGW



Name	ID	State	VPC	Owner
Default IGW	igw-1f8c6164	attached	vpc-bbd16fc1	181844168138



Name	ID	State	VPC
Default VPC Internet Ga	igw-01cac968	attached	vpc-73ac061b
Internet Gateway 2	igw-67cdce0e	detached	

? why it is not attached to VPC
U know what u can attach 1 vpc to 1 IGW

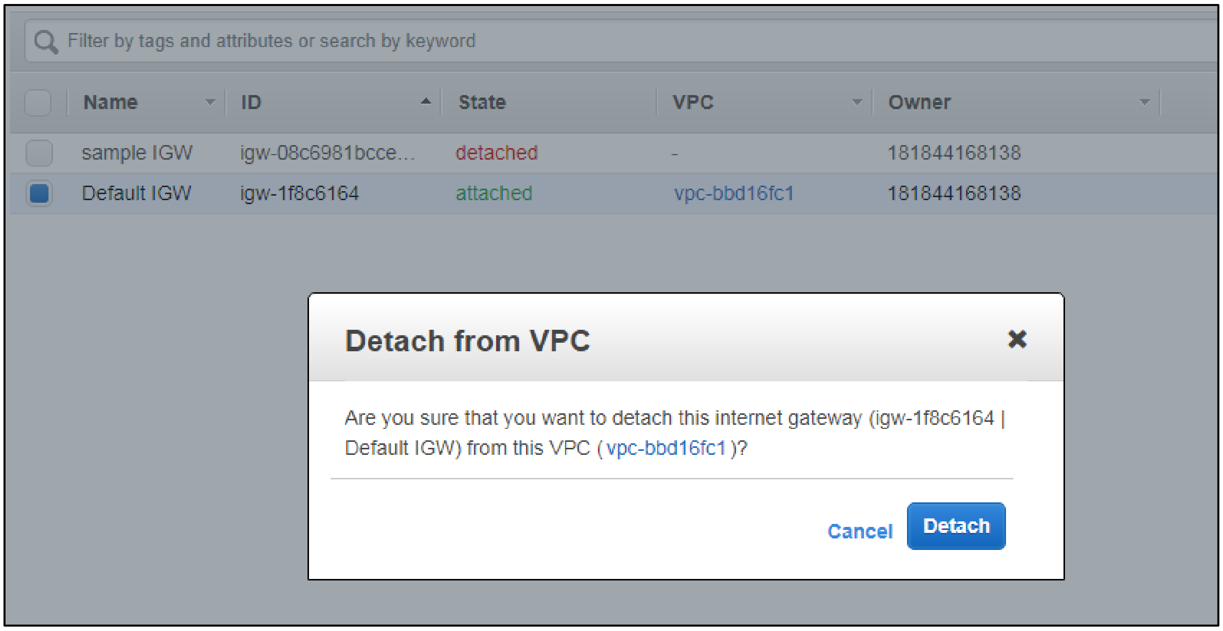
igw-01cac968 | Default VPC Internet Gateway

ID: igw-01cac968 | Default VPC Internet Gateway
State: attached
Attached VPC ID: vpc-73ac061b
Attachment state: available

If u want new IGW attached to VPC -> JUST SWAP IT
*Actions -> Detach the default from VPC
*Actions->attach the new IGW to VPC

STEPS:

1. CREATE THE Internet gateway -> name the tag (SAMPLE IGW)-> create
2. State will be detached because 1VPC = 1 IGW
3. If u want to attach the VPC in the sample IGW, First detach the VPC in Default IGW -> To detach it – go to Actions-> “**Detach from VPC”**

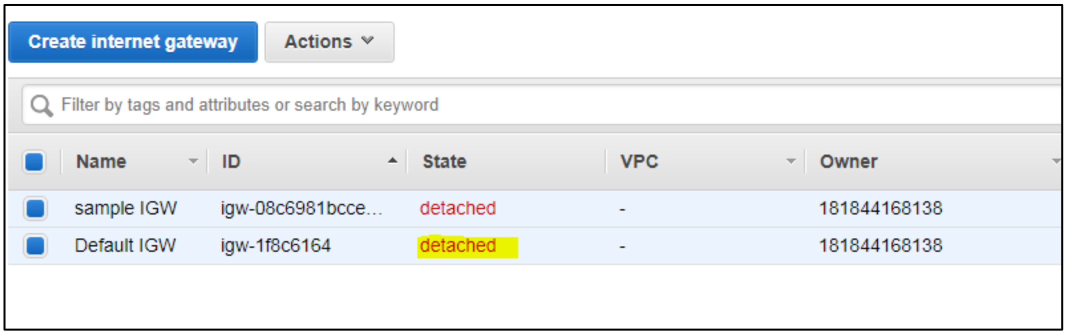


Name	ID	State	VPC	Owner
sample IGW	igw-08c6981bcce...	detached	-	181844168138
Default IGW	igw-1f8c6164	attached	vpc-bbd16fc1	181844168138

Detach from VPC

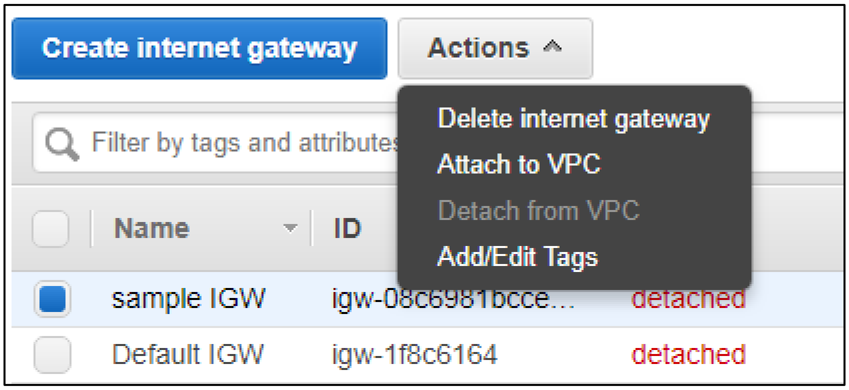
Are you sure that you want to detach this internet gateway (igw-1f8c6164 | Default IGW) from this VPC (vpc-bbd16fc1)?

4. CLICK -> “detach”

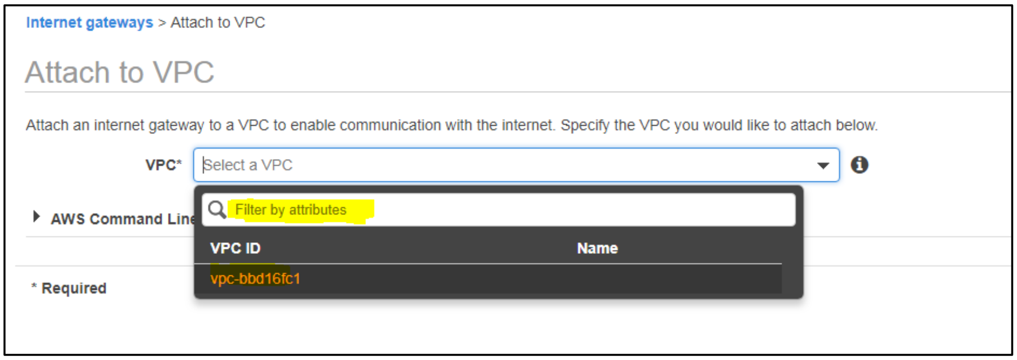


Name	ID	State	VPC	Owner
sample IGW	igw-08c6981bcce...	detached	-	181844168138
Default IGW	igw-1f8c6164	detached	-	181844168138

Select Sample IGW -> Actions -> **Attach to VPC**



Name	ID	
sample IGW	igw-08c6981bcce...	detached
Default IGW	igw-1f8c6164	detached


Internet gateways > Attach to VPC

Attach to VPC

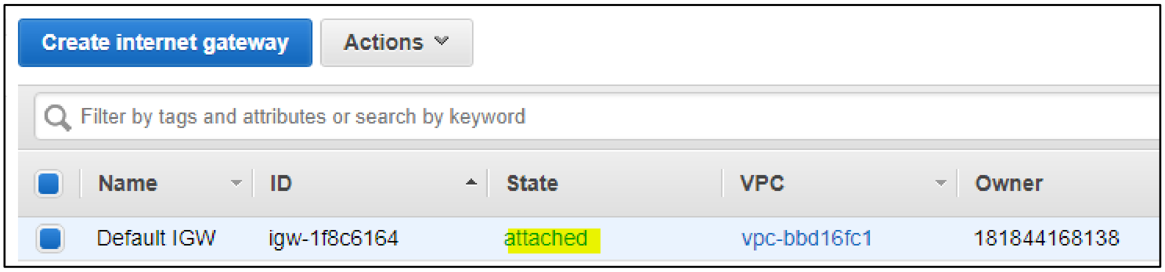
Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC* Select a VPC

VPC ID	Name
vpc-bbd16fc1	

* Required

CLICK on “**ATTACH**”



■	Name	ID	State	VPC	Owner
■	Default IGW	igw-1f8c6164	attached	vpc-bbd16fc1	181844168138

NOTE: It is not a rule to have the internet gateway for all the VPC connection.VPC can able to run without the need of IGW. Ie) it acts as the private network. The network will not be able to contact

VPC Types and VPC Security

VPC Types

- Default VPC
- Custom VPC

Default VPC:

- It is created by default in each AWS region when the AWS account is created
- Has default CIDR, Security Group, N ACL, and route table settings
- Has internet Gateway by default

Custom (Non Default) VPC:

If you don't want to use the default VPC and you need to create your own Custom VPC for production Testing/ developing reason

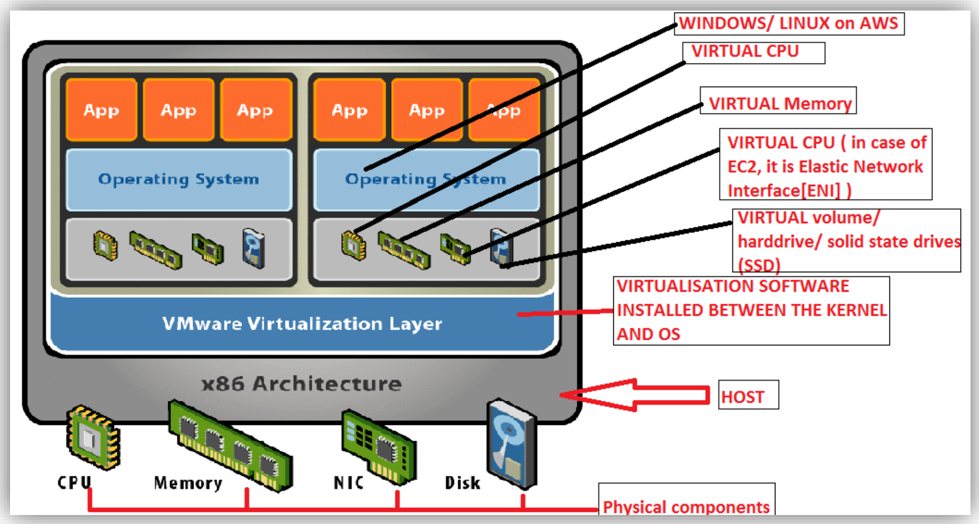
- The *AWS Account Owner* creates this **CUSTOM** VPC
- The account owner who creates the custom VPC can *decide the CIDR*
- Has *default Security Group, N ACL, and route table* settings
- They *does not have Internet gateways by default* , one needs to be created if needed.

If you need web access for the resources that u use in the VPC like EC2 , then u need to create the internet gateway and attach it to the VPC

VPC Security

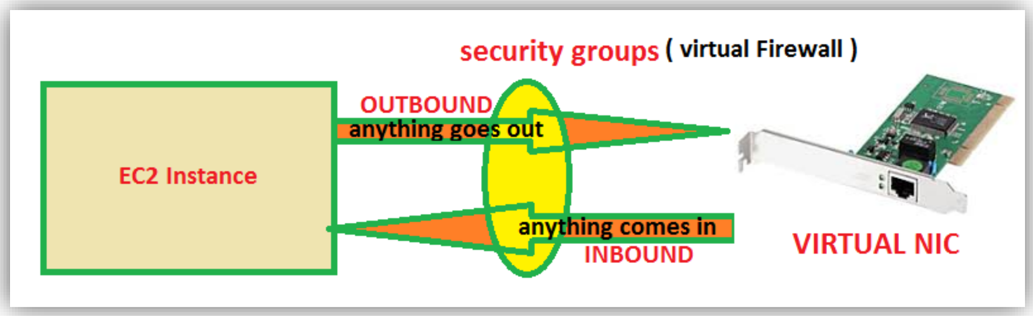
It is very important and crucial component in AWS.

First we need to know about the virtualisation.


App
App
App
App
App
App
Operating System
Operating System
VMware Virtualization Layer
x86 Architecture
CPU
Memory
NIC
Disk
WINDOWS/ LINUX on AWS
VIRTUAL CPU
VIRTUAL Memory
VIRTUAL CPU (in case of EC2, it is Elastic Network Interface[ENI])
VIRTUAL volume/ harddrive/ solid state drives (SSD)
VIRTUALISATION SOFTWARE INSTALLED BETWEEN THE KERNEL AND OS
HOST
Physical components

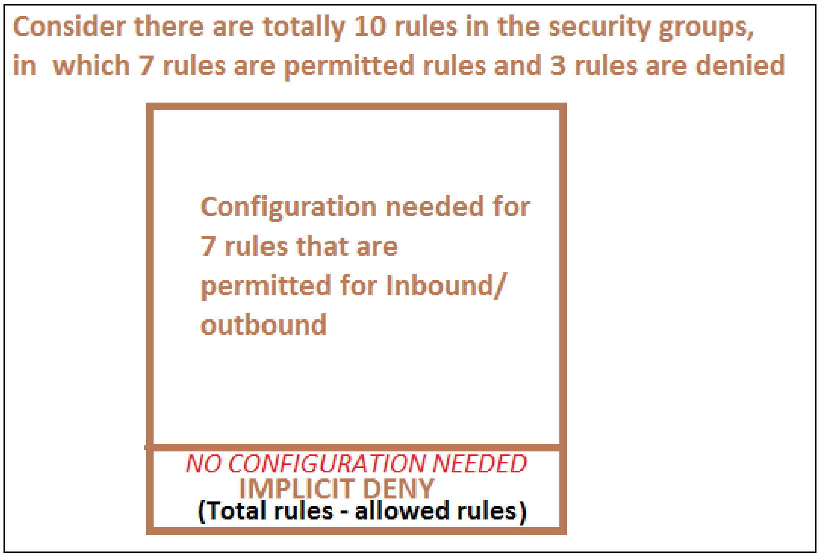
The software that it is installed between the kernel and OS. The layer can be able to virtualize the physical component into logical compute instances. Virtualization software like XEN, VM WARE will have some specifications that how many EC2 instances/ any instances can be installed.

- In AWS, NIC is called as **ELASTIC NETWORK INTERFACE**



- Security groups are nothing but the virtual Firewall. **What is firewall?** It is the line of defense that controls the traffic between the data packets that comes in and out of the EC2/ any other instances
- You can have 5 security group per single EC2 instance interface. EC2 instance interface / ENI (where the EC2 instance connect to the network) is associated with security group.
- **SECURITY GROUP rules – restricted for inbound (data coming inside instance)
  SECURITY GROUP rules – allow/ restricted for outbound (data going out)
- ** SECURITY GROUP rules – allowed for inbound (data coming inside instance)
  Should allow for outbound (data going out) irrespective of rules
  "Stateful"- returns the traffic for the allowed inbound traffic , even if there is no rules in the security group
- Security group can define allow/permit rules and it cannot define deny rules

	Inbound	Outbound
Security Group rule	restricted	**allow**/restricted
Security Group rule	**allow**	**allow** (irrespective of rules)



Consider there are totally 10 rules in the security groups, in which 7 rules are permitted rules and 3 rules are denied

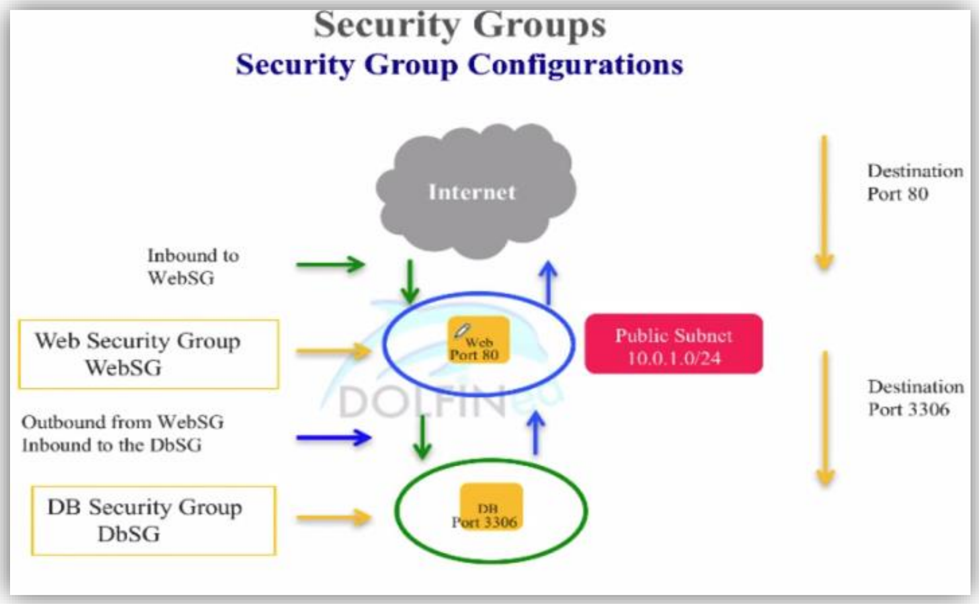
Configuration needed for 7 rules that are permitted for Inbound/ outbound

NO CONFIGURATION NEEDED

IMPLICIT DENY

(Total rules - allowed rules)

- Security group is bidirectional



Security Groups

Security Group Configurations

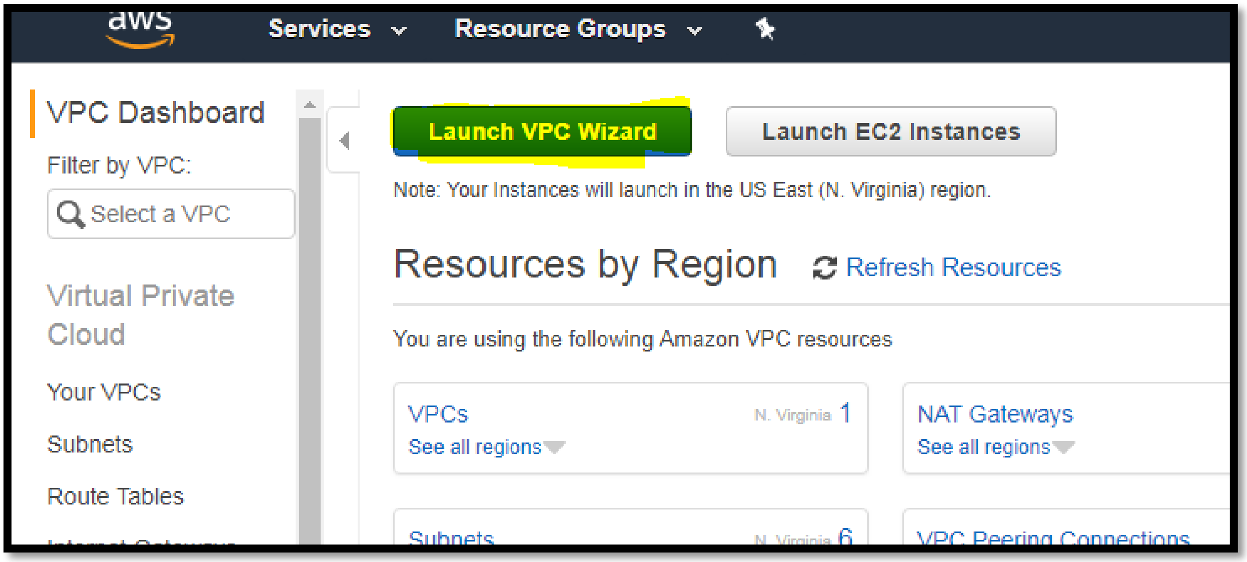
Default VPC already we have seen , now we can see the custom VPC

Sometimes you want to create more than one VPC.

- One for the testing
- One for development
- One for Preproduction

Steps:

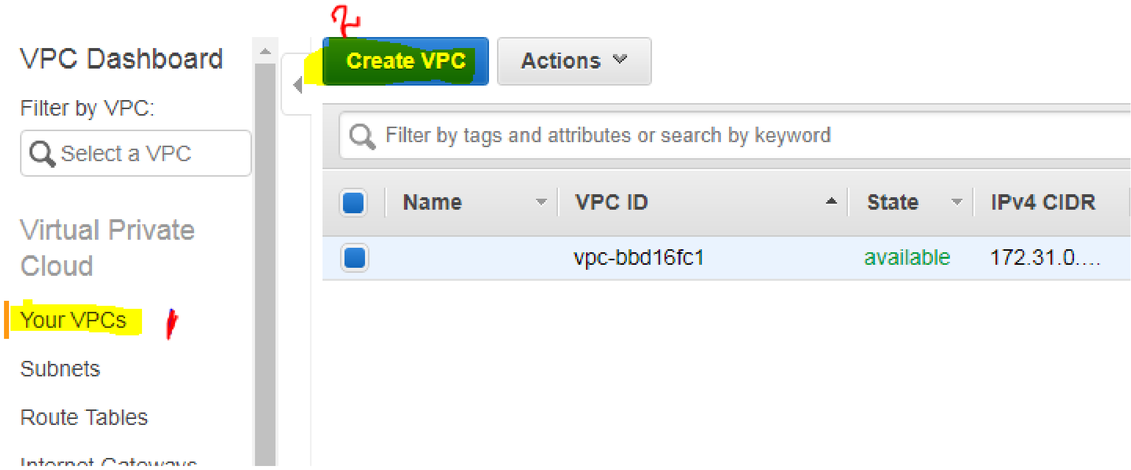
1. **VPC Dashboard –> Click on “Launch VPC Wizard” -> Through this also we can create the VPC**



Note: Your Instances will launch in the US East (N. Virginia) region.

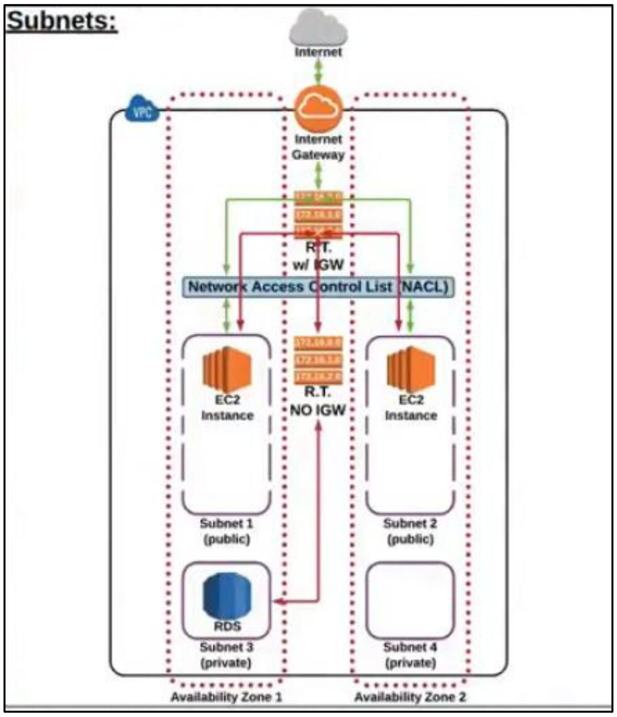
You are using the following Amazon VPC resources

2. **Click “Your VPC” -> “CREATE VPC”**

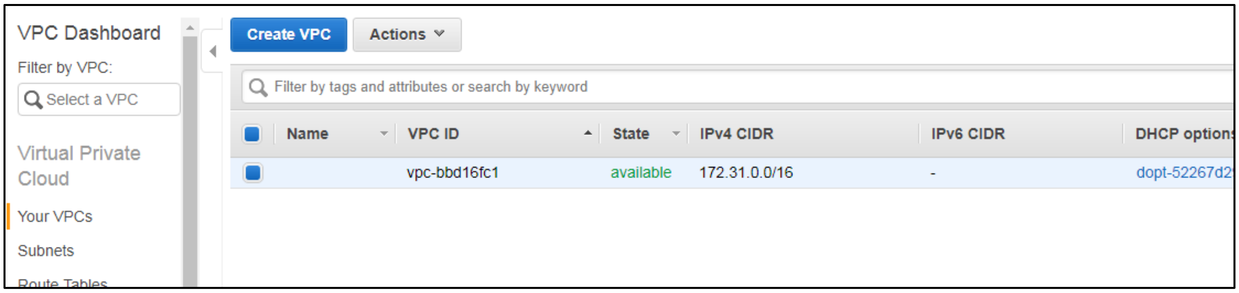


Name	VPC ID	State	IPv4 CIDR
	vpc-bbd16fc1	available	172.31.0.…

3.

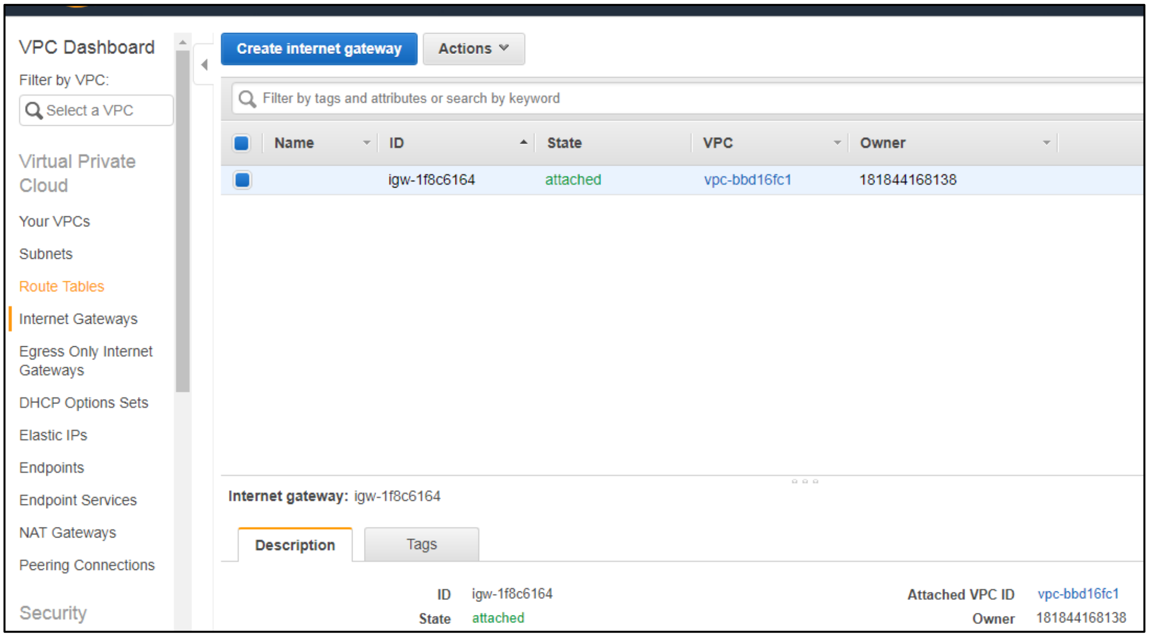


IGW- Internet Gateway – every vpc have only one internet gateway.



	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option
■		vpc-bbd16fc1	available	172.31.0.0/16	-	dopt-52267d2

Default VPC with respect to nearer region.

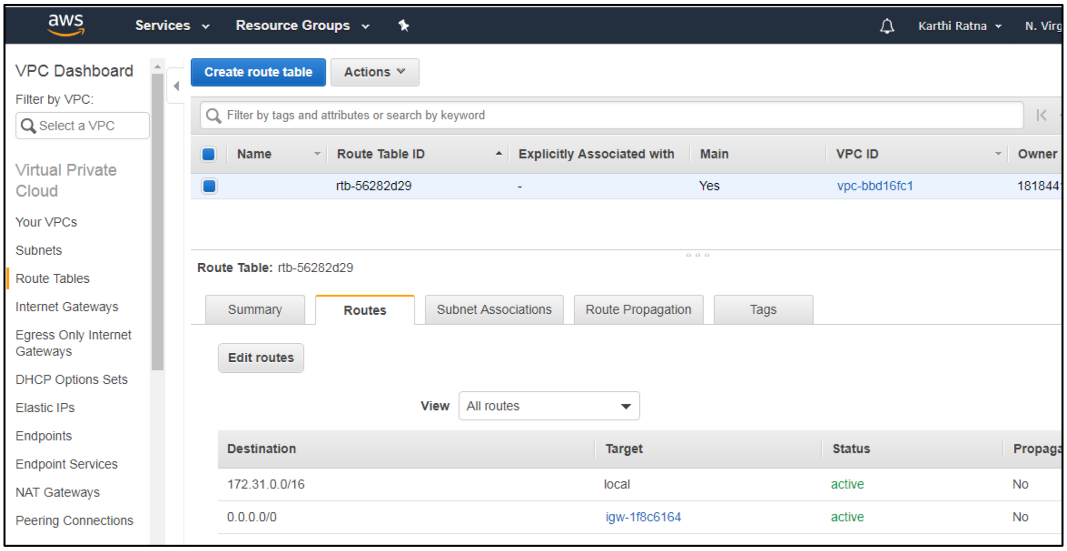


	Name	ID	State	VPC	Owner
■		igw-1f8c6164	attached	vpc-bbd16fc1	181844168138

Internet gateway: igw-1f8c6164

ID	igw-1f8c6164	Attached VPC ID	vpc-bbd16fc1
State	attached	Owner	181844168138

Default Internet Gateway that is connected to the Default VPC.



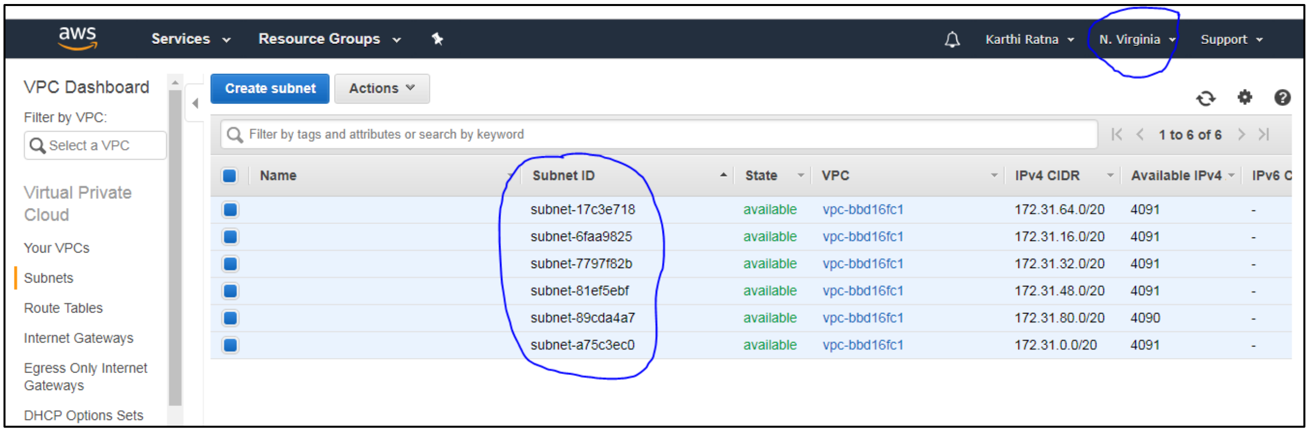
	Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
■		rtb-56282d29	-	Yes	vpc-bbd16fc1	181844

Route Table: rtb-56282d29

View: All routes

Destination	Target	Status	Propaga
172.31.0.0/16	local	active	No
0.0.0.0/0	igw-1f8c6164	active	No

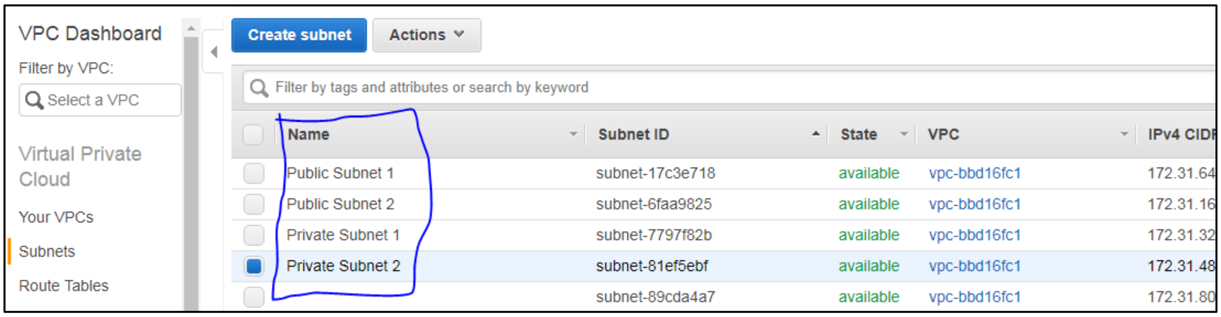
Default Route Table that is connected to the Default Internet Gateway (Route Table with the internet gateway).



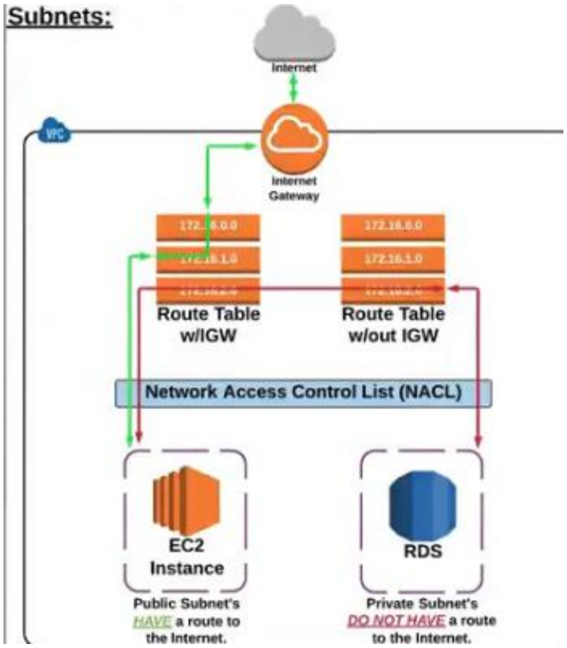
☑	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 C
☑		subnet-17c3e718	available	vpc-bbd16fc1	172.31.64.0/20	4091	-
☑		subnet-6faa9825	available	vpc-bbd16fc1	172.31.16.0/20	4091	-
☑		subnet-7797f82b	available	vpc-bbd16fc1	172.31.32.0/20	4091	-
☑		subnet-81ef5ebf	available	vpc-bbd16fc1	172.31.48.0/20	4091	-
☑		subnet-89cda4a7	available	vpc-bbd16fc1	172.31.80.0/20	4090	-
☑		subnet-a75c3ec0	available	vpc-bbd16fc1	172.31.0.0/20	4091	-

There will be default subnets with respect to the area (or region) (eg. N. Virginia has 6 subnets)
Each route table has subnets. Each subnets have AWS Resources (eg. EC2, RDS)
Route table can be shared between the availability zone but Subnet cannot be shared between the availability zone.

- Add subnets to the route table before that determine the public and private subnet.(Public and private network is determined with respect to the subnet.)
- Name the subnet whether (PUBLIC or PRIVATE) so that assigning the subnet to the routing table will be easy.

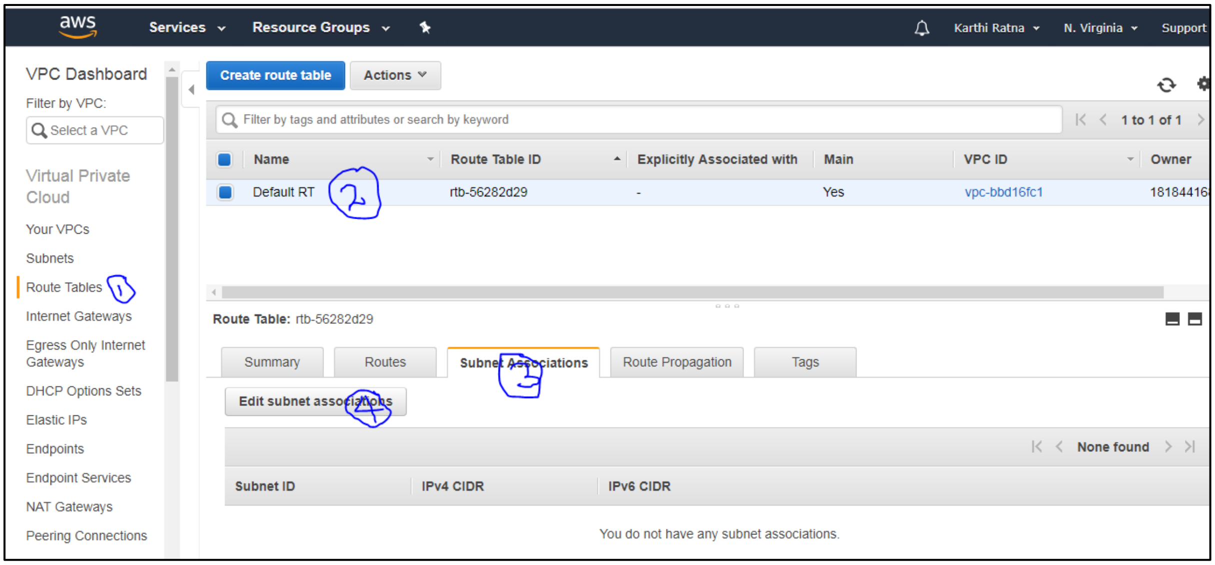


☐	Name	Subnet ID	State	VPC	IPv4 CIDF
☐	Public Subnet 1	subnet-17c3e718	available	vpc-bbd16fc1	172.31.64
☐	Public Subnet 2	subnet-6faa9825	available	vpc-bbd16fc1	172.31.16
☐	Private Subnet 1	subnet-7797f82b	available	vpc-bbd16fc1	172.31.32
☑	Private Subnet 2	subnet-81ef5ebf	available	vpc-bbd16fc1	172.31.48
☐		subnet-89cda4a7	available	vpc-bbd16fc1	172.31.80



Subnets:
Internet
VPC
Internet Gateway
172.16.0.0
172.16.1.0
172.16.0.0
172.16.1.0
Route Table w/IGW
Route Table w/out IGW
Network Access Control List (NACL)
EC2 Instance
RDS
Public Subnet's HAVE a route to the Internet.
Private Subnet's DO NOT HAVE a route to the Internet.

- Assume Public network for EC2 Instance – Routing table with IGW
  And Private network for RDS(database) – Routing table without IGW
- Go to Routing Tables -> Name and Assign Default routing table that is already created to PUBLIC NETWORK -> Go to Subnet Associations -> add the public Subnets -> save

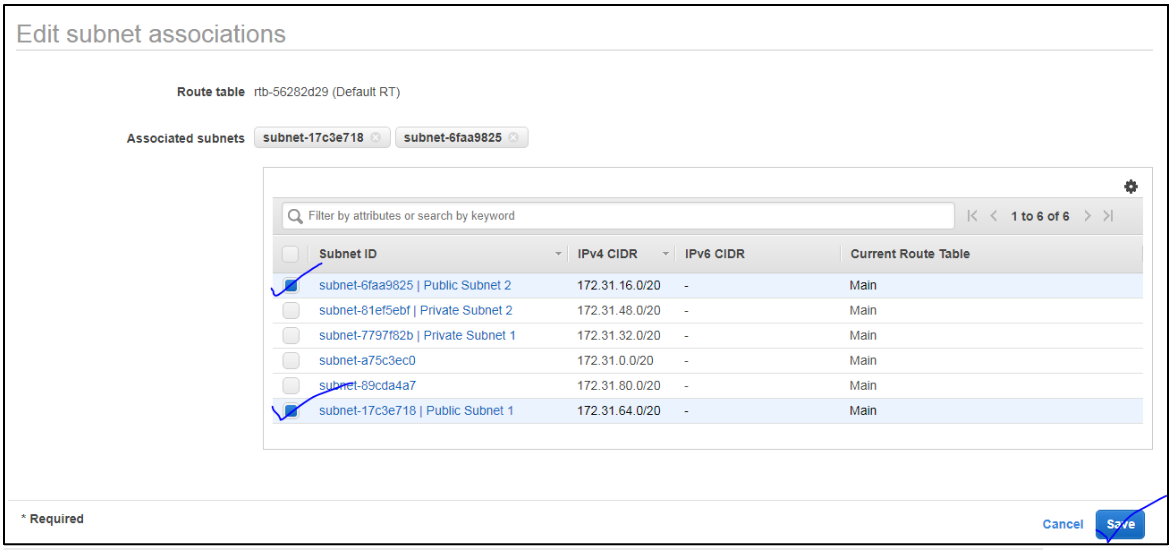


Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
Default RT	rtb-56282d29	-	Yes	vpc-bbd16fc1	18184416

Route Table: rtb-56282d29

Subnet ID	IPv4 CIDR	IPv6 CIDR

You do not have any subnet associations.



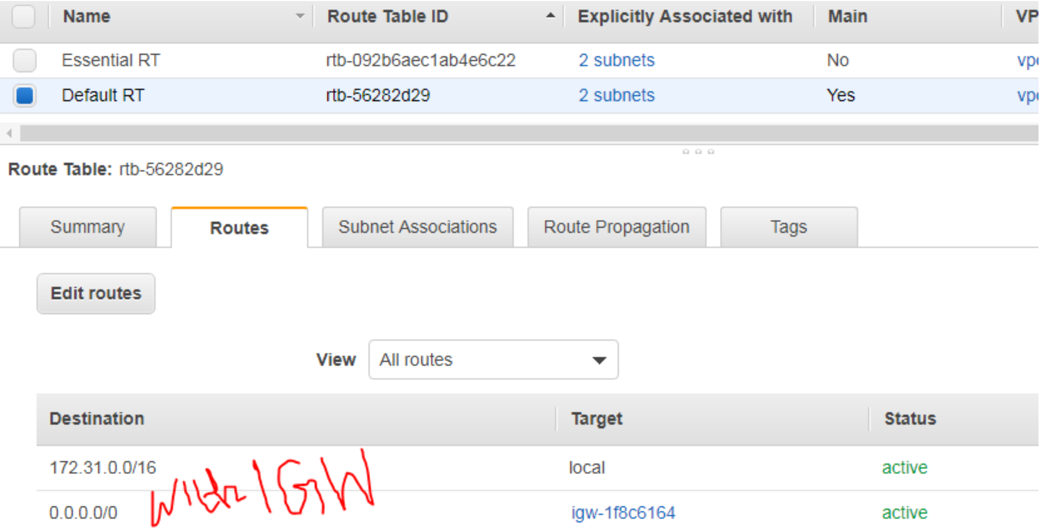
Edit subnet associations

Route table rtb-56282d29 (Default RT)

Associated subnets subnet-17c3e718 subnet-6faa9825

	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
☑	subnet-6faa9825 | Public Subnet 2	172.31.16.0/20	-	Main
□	subnet-81ef5ebf | Private Subnet 2	172.31.48.0/20	-	Main
□	subnet-7797f82b | Private Subnet 1	172.31.32.0/20	-	Main
□	subnet-a75c3ec0	172.31.0.0/20	-	Main
□	subnet-89cda4a7	172.31.80.0/20	-	Main
☑	subnet-17c3e718 | Public Subnet 1	172.31.64.0/20	-	Main

* Required



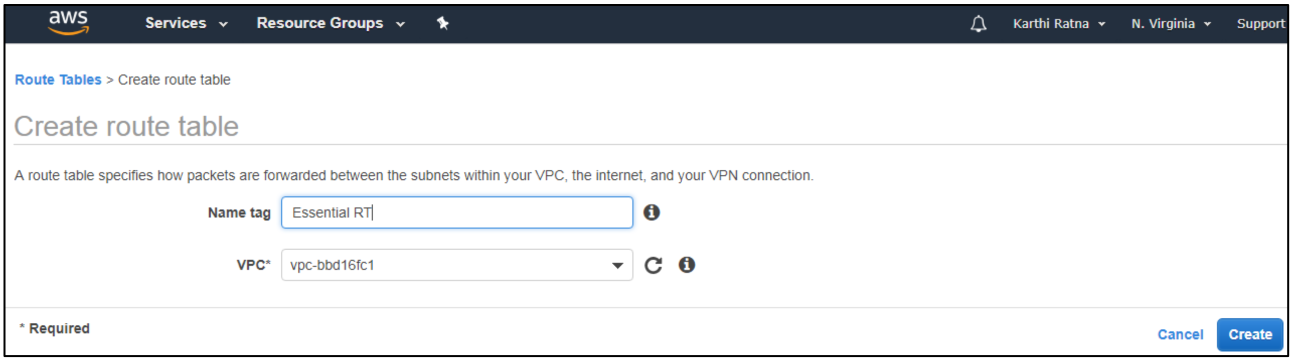
	Name	Route Table ID	Explicitly Associated with	Main	VP
□	Essential RT	rtb-092b6aec1ab4e6c22	2 subnets	No	vp
☑	Default RT	rtb-56282d29	2 subnets	Yes	vp

Route Table: rtb-56282d29

View All routes

Destination	Target	Status
172.31.0.0/16	local	active
0.0.0.0/0	igw-1f8c6164	active

- Go to **Routing Tables** -> Create routing table so that Private network will be determined -> Go to **CREATE ROUTE TABLE** -> Name tag, VPC -> **CREATE**



Route Tables > Create route table

Create route table

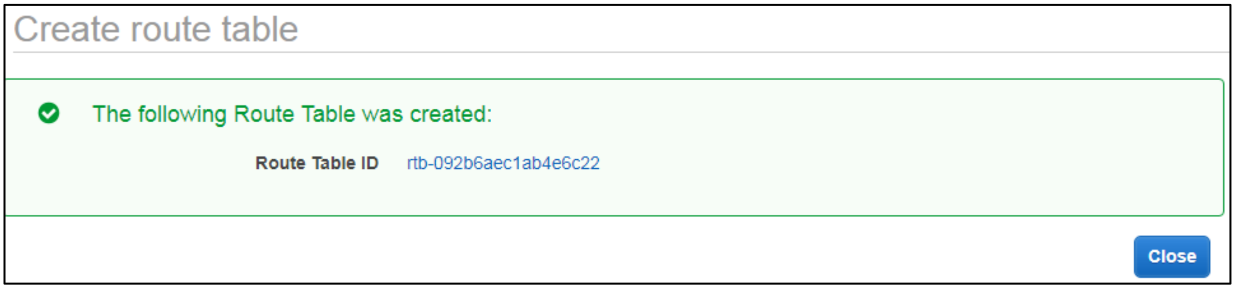
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag: Essential RT

VPC*: vpc-bbd16fc1

* Required

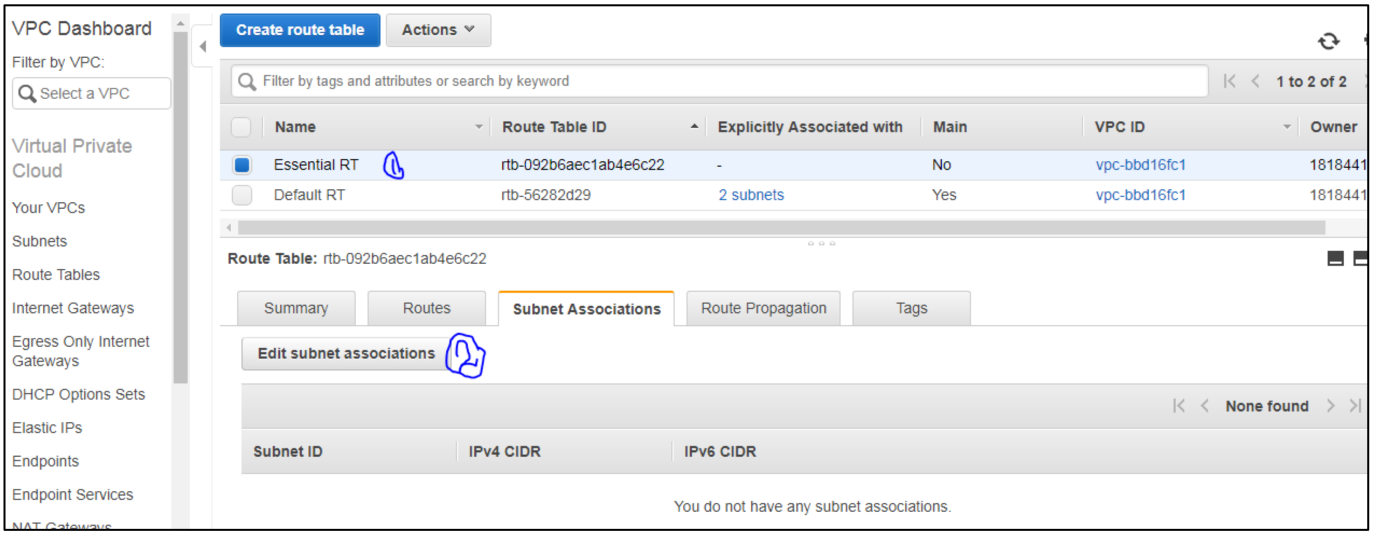
Now route table has been **created with no IGW.**


Create route table

The following Route Table was created:

Route Table ID rtb-092b6aec1ab4e6c22

Now It’s time to add our private network in this route table



Filter by tags and attributes or search by keyword — 1 to 2 of 2

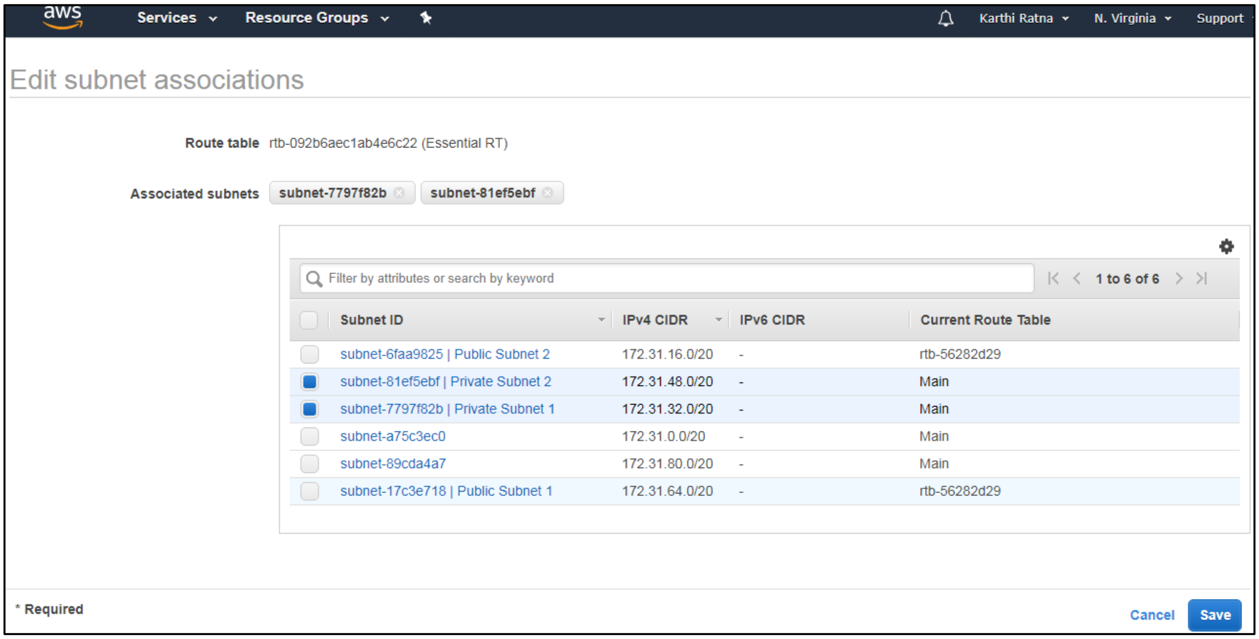
	Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
■	Essential RT	rtb-092b6aec1ab4e6c22	-	No	vpc-bbd16fc1	1818441
□	Default RT	rtb-56282d29	2 subnets	Yes	vpc-bbd16fc1	1818441

Route Table: rtb-092b6aec1ab4e6c22

None found

Subnet ID	IPv4 CIDR	IPv6 CIDR

You do not have any subnet associations.



Edit subnet associations

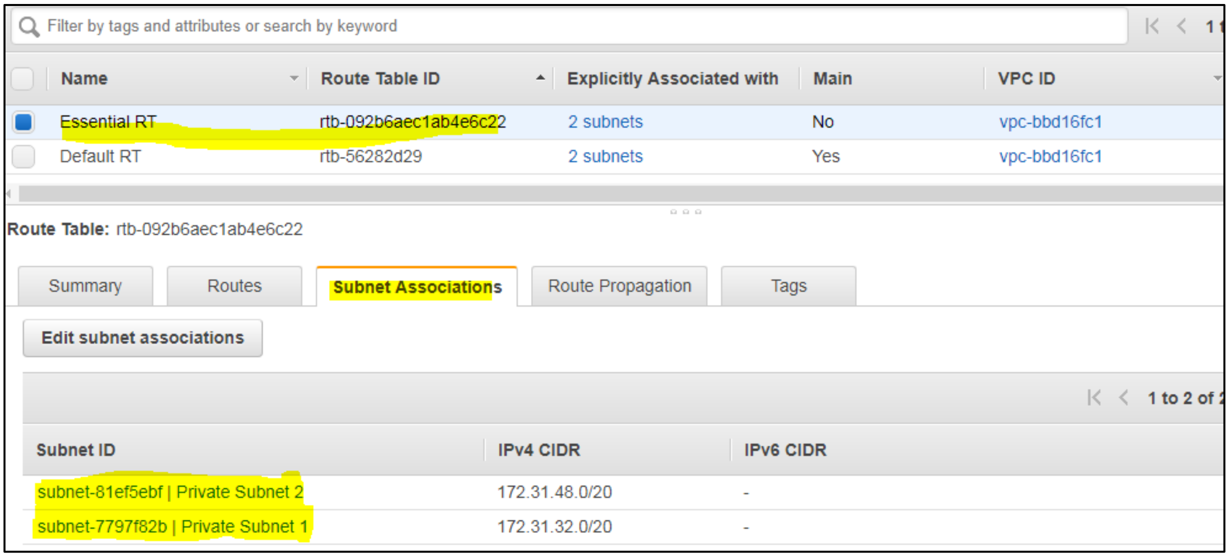
Route table rtb-092b6aec1ab4e6c22 (Essential RT)

Associated subnets subnet-7797f82b subnet-81ef5ebf

Filter by attributes or search by keyword — 1 to 6 of 6

	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
□	subnet-6faa9825 | Public Subnet 2	172.31.16.0/20	-	rtb-56282d29
■	subnet-81ef5ebf | Private Subnet 2	172.31.48.0/20	-	Main
■	subnet-7797f82b | Private Subnet 1	172.31.32.0/20	-	Main
□	subnet-a75c3ec0	172.31.0.0/20	-	Main
□	subnet-89cda4a7	172.31.80.0/20	-	Main
□	subnet-17c3e718 | Public Subnet 1	172.31.64.0/20	-	rtb-56282d29

* Required

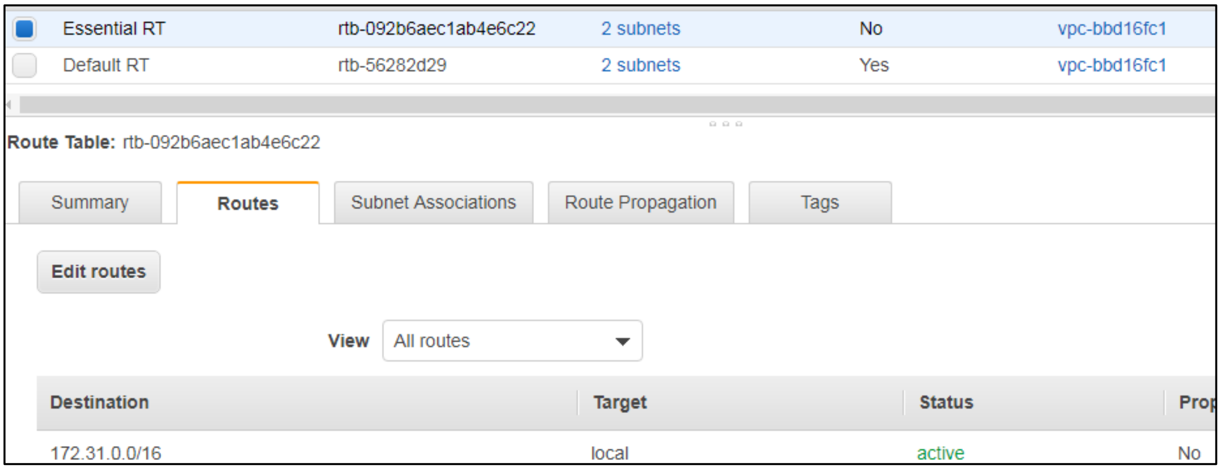


Filter by tags and attributes or search by keyword

	Name	Route Table ID	Explicitly Associated with	Main	VPC ID
■	Essential RT	rtb-092b6aec1ab4e6c22	2 subnets	No	vpc-bbd16fc1
□	Default RT	rtb-56282d29	2 subnets	Yes	vpc-bbd16fc1

Route Table: rtb-092b6aec1ab4e6c22

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-81ef5ebf | Private Subnet 2	172.31.48.0/20	-
subnet-7797f82b | Private Subnet 1	172.31.32.0/20	-

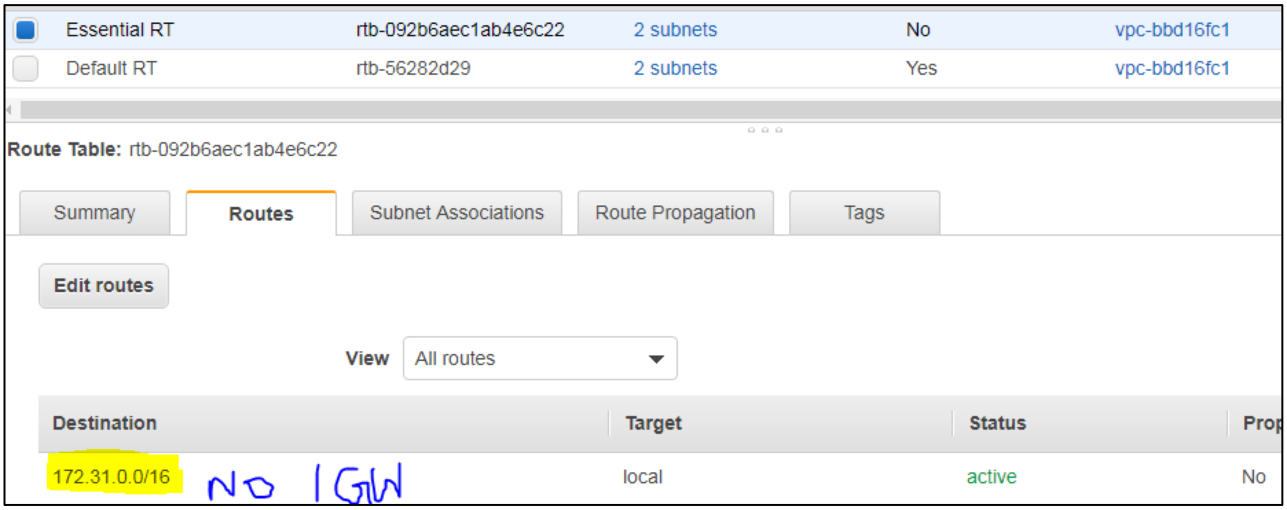


	Name	Route Table ID	Explicitly Associated with	Main	VPC ID
■	Essential RT	rtb-092b6aec1ab4e6c22	2 subnets	No	vpc-bbd16fc1
□	Default RT	rtb-56282d29	2 subnets	Yes	vpc-bbd16fc1

Route Table: rtb-092b6aec1ab4e6c22

View: All routes

Destination	Target	Status	Prop
172.31.0.0/16	local	active	No



	Name	Route Table ID	Explicitly Associated with	Main	VPC ID
■	Essential RT	rtb-092b6aec1ab4e6c22	2 subnets	No	vpc-bbd16fc1
□	Default RT	rtb-56282d29	2 subnets	Yes	vpc-bbd16fc1

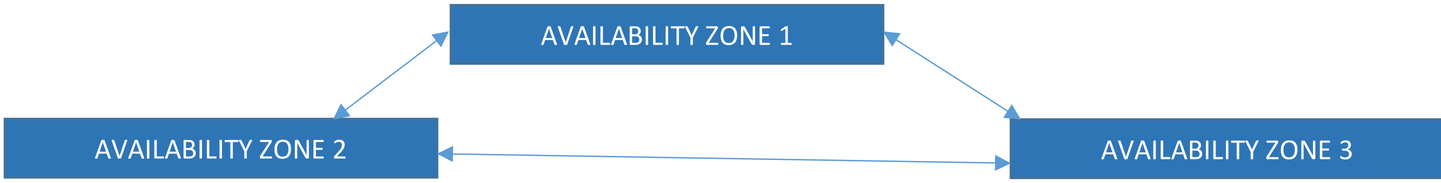
Route Table: rtb-092b6aec1ab4e6c22

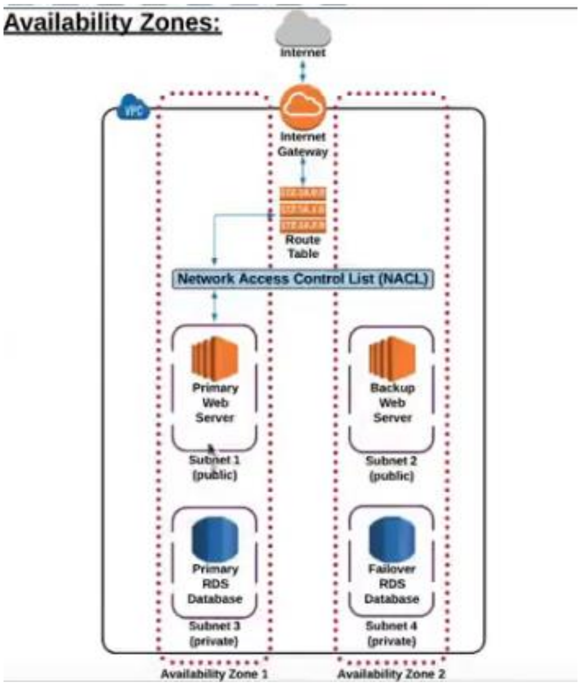
View: All routes

Destination	Target	Status	Prop
172.31.0.0/16 NO IGW	local	active	No

AVAILABILY ZONES(based on VPC SPECIFIC)

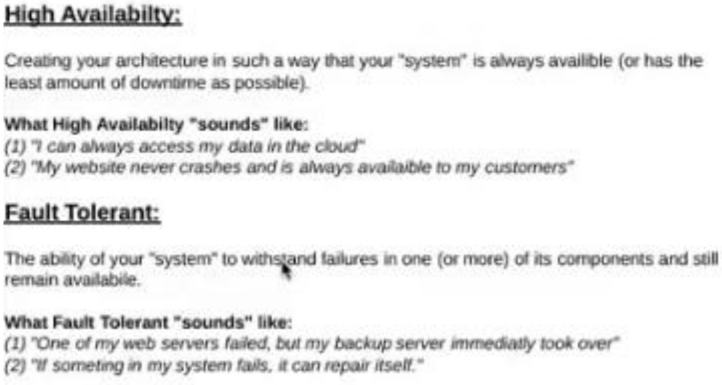
Each AWS Resources will be under the subnet. Each subnet should be under the availability zone.U can utilize multiple availability zones.and create redundancy in the architecture. This is what allows for the **high availability** and **Fault Tolerant** systems.





Availability Zones:

if one availability zone failed, the next availability zone will take care of the server.



High Availabilty:

Creating your architecture in such a way that your "system" is always availible (or has the least amount of downtime as possible).

What High Availabilty "sounds" like:
(1) "I can always access my data in the cloud"
(2) "My website never crashes and is always availaible to my customers"

Fault Tolerant:

The ability of your "system" to withstand failures in one (or more) of its components and still remain availabile.

What Fault Tolerant "sounds" like:
(1) "One of my web servers failed, but my backup server immediatly took over"
(2) "If someting in my system fails, it can repair itself."