Course and Labs

Design Network in AWS

Mohanraj Shanmugam

Course and Labs

Topic 1: AWS VPC, Subnet, Routing Table, DHCP

Mohanraj Shanmugam

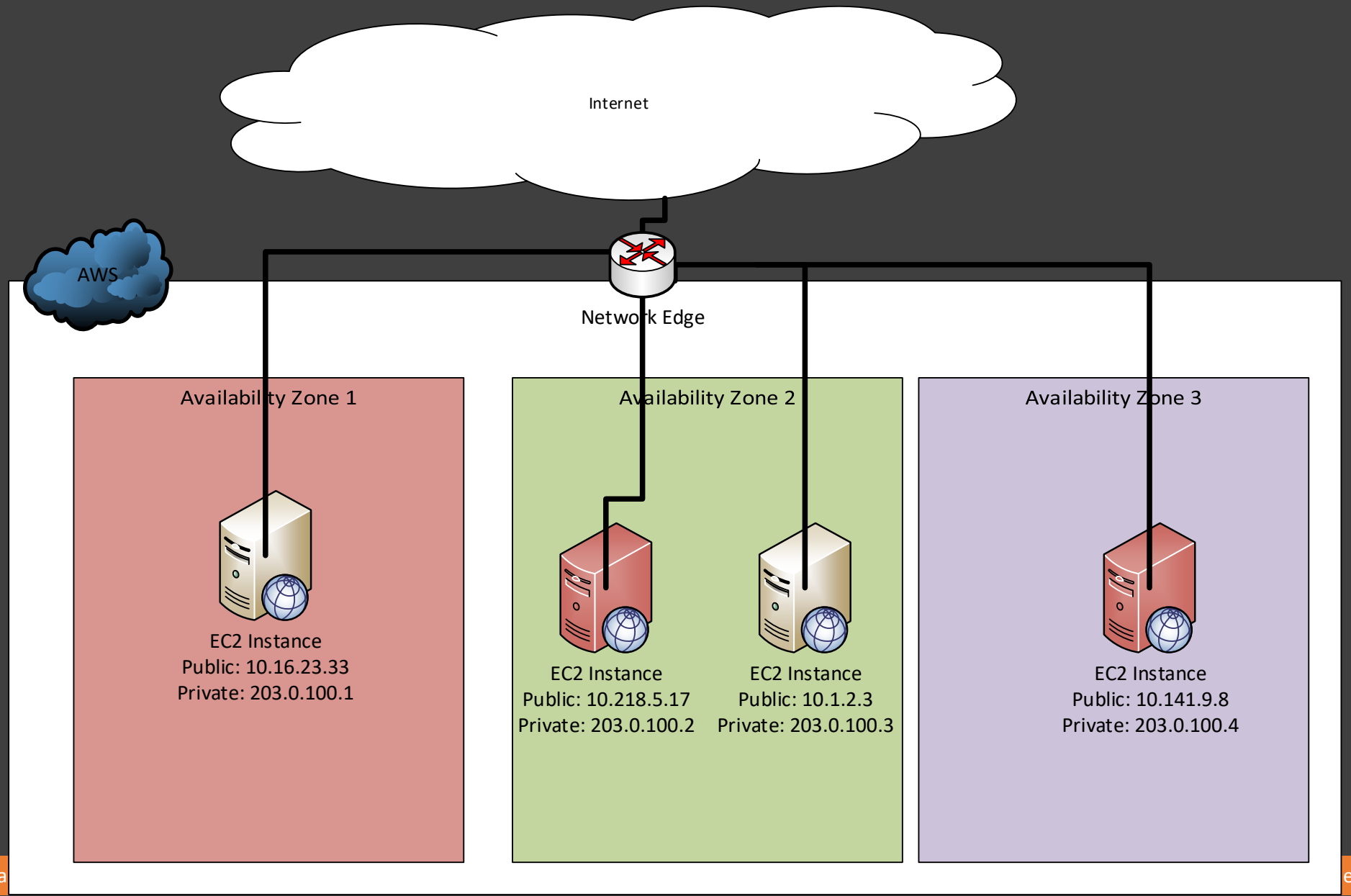
Cloud Networking

- Cloud networking is a new networking paradigm for building and managing secure private networks over the public Internet by utilizing global cloud computing infrastructure.
- In cloud networking, We Create Virtual Networks using Network Virtualization.
- Use SDN to make it more programmable networks
- Use Overlays to connect within or multiple cloud networks
- Use Network Function Virtualization to consume Network Functions as a Service and scale them as and when required.

AWS EC2 Classic Network

- EC2 Classic network is introduced initial period of AWS. It is available for Account only created before 12/4/2013
- Your instance receives a public IP and Private IP automatically assigned by Default
- AWS select a single private IP address for your instance; multiple IP addresses are not supported
- An EIP is disassociated from your instance when you stop it.
- DNS hostnames are enabled by default.
- A security group can reference security groups that belong to other AWS accounts.
- You can create up to 500 security groups in each region.
- You can assign an unlimited number of security groups to an instance when you launch it. You can't change the security groups of your running instance.
- Your instance can access the Internet directly through the AWS network edge.

AWS EC2 Classic



Amazon VPC

- Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.
- This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
- Amazon VPC let you to create Virtual networks with in the cloud with Network Virtualization, SDN and Network Function Virtualization

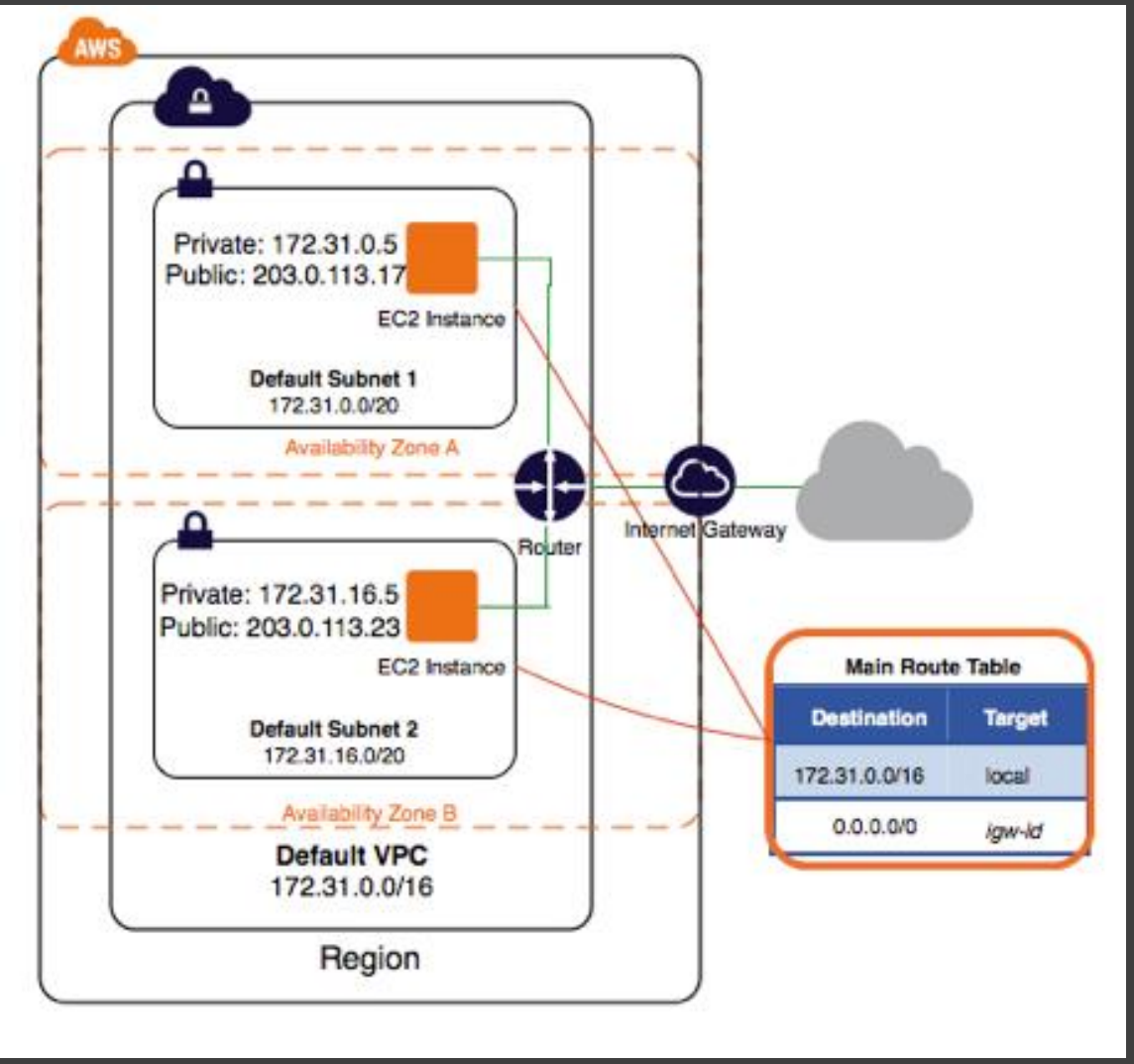
Amazon VPC

- A *virtual private cloud* (VPC) is a virtual network dedicated to your AWS account.
- It is logically isolated from other virtual networks in the AWS cloud.
- You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.
- You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings.

Amazon VPC - Subnet

- A *subnet* is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select.
- Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.
- To protect the AWS resources in each subnet, you can use multiple layers of security, including security groups and network access control lists (ACL).

AWS Default Virtual Private Cloud



- If your account created after 12/4/2013 it comes with Default VPC
- A *default VPC* that has a *default subnet* in each Availability Zone.
- If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC.
- Create an Internet gateway and connect it to your default VPC.
- Create a main route table for your default VPC with a rule that sends all traffic destined for the Internet to the Internet gateway.
- Create a default security group and associate it with your default VPC.
- Create a default network access control list (ACL) and associate it with your default VPC.
- Associate the default DHCP options set for your AWS account with your default VPC

You can use Advances VPC features as and when required.

AWS Default Virtual Private Cloud

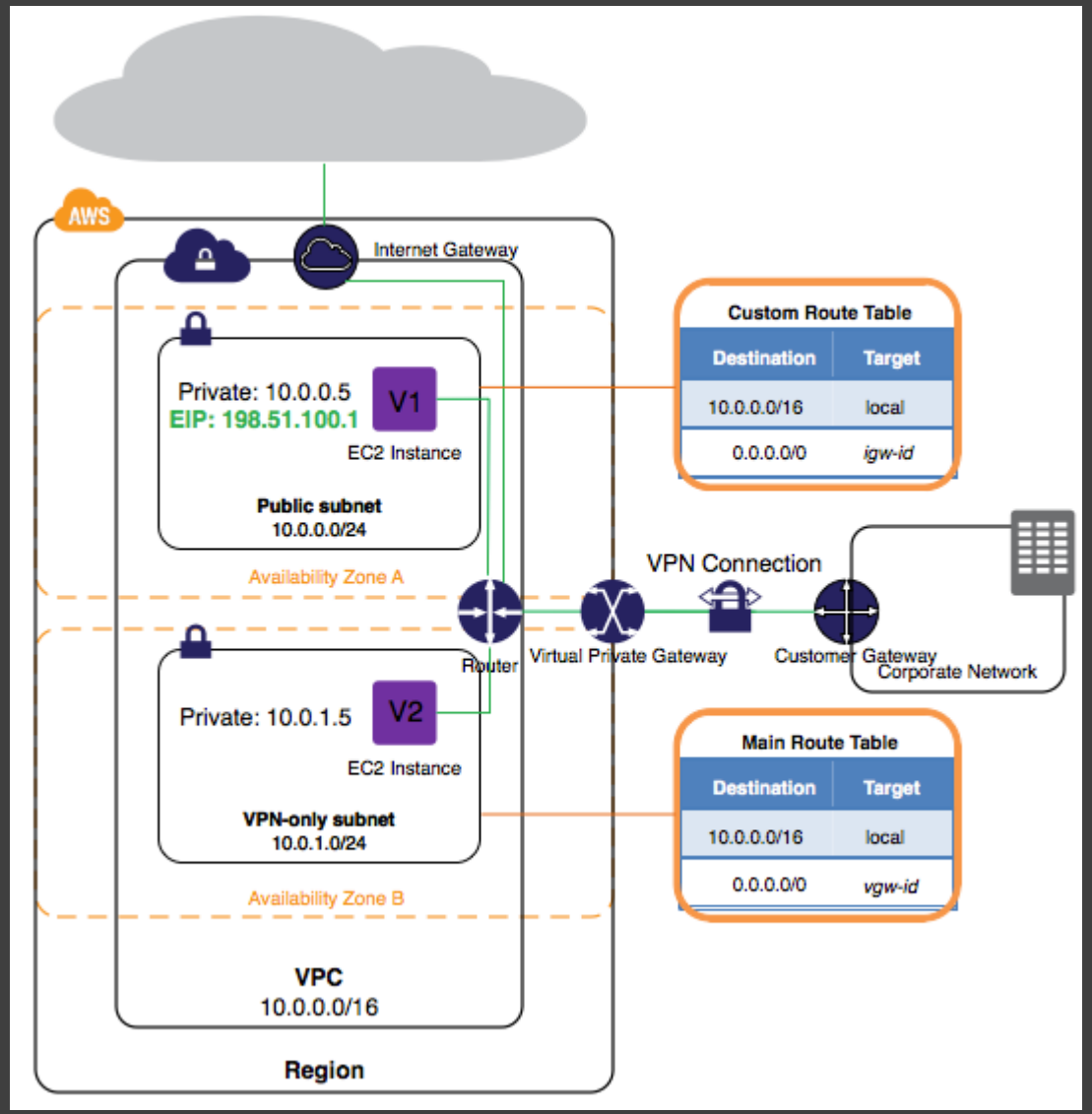
- Instances that you launch into a default subnet receive both a public IP address and a private IP address.
- Instances in a default subnet also receive both public and private DNS hostnames.
- Instances that you launch into a non default subnet in a default VPC don't receive a public IP address or a DNS hostname.
- You can change your subnet's default public IP addressing behavior.
- you can add subnets, modify the main route table, add additional route tables, associate additional security groups, update the rules of the default security group, and add VPN connections.
- You can use a default subnet as you would use any other subnet; you can add custom route tables and set network ACLs. You can also specify a default subnet when you launch an EC2 instance.

Non Default VPC

Course and Labs

- You can create non default VPC any time
- VPC gives you advanced networking features such as :
  - Elastic Network Interface (ENIs)
  - Multiple Ips
  - Routing Tables
  - Egress Security Groups
  - Network ACLS
  - Private Connectivity
  - Enhanced Networking
  - Connectivity to your corporate or Datacenter

Route Tables



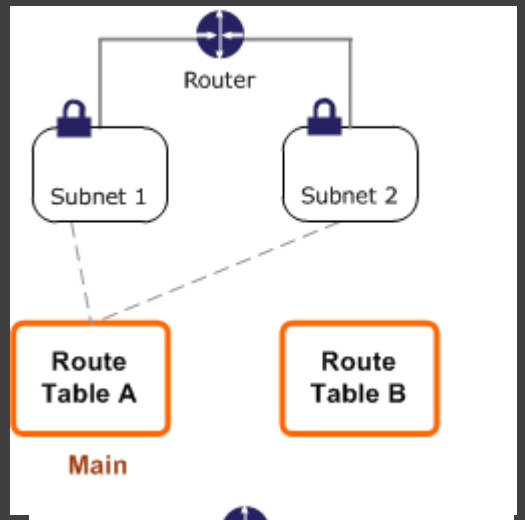
- A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed.
- Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet.
- A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

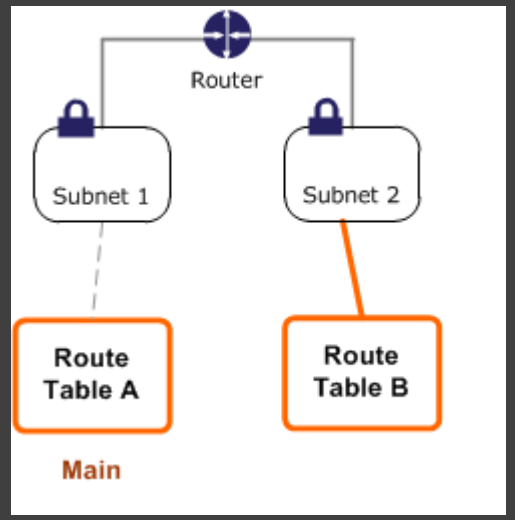
Route Table Basics

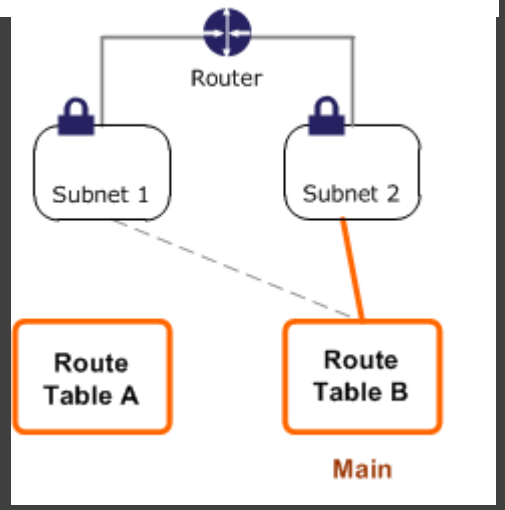
Course and Labs

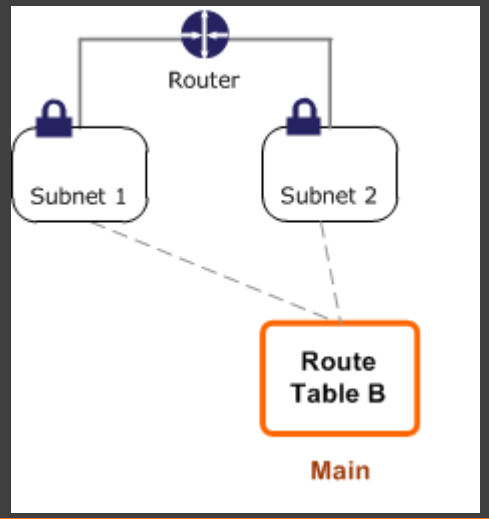
- Your VPC has an implicit router.
- Your VPC automatically comes with a main route table that you can modify.
- You can create additional custom route tables for your VPC.
- Each subnet must be associated with a route table, which controls the routing for the subnet. If you don't explicitly associate a subnet with a particular route table, the subnet is implicitly associated with the main route table.
- You can replace the main route table with a custom table that you've created (so that this table is the default table each new subnet is associated with).
- Each route in a table specifies a destination CIDR and a target (for example, traffic destined for 172.16.0.0/12 is targeted for the virtual private gateway). We use the most specific route that matches the traffic to determine how to route the traffic.
- Every route table contains a local route that enables communication within a VPC. You cannot modify or delete this route.
- When you add an Internet gateway, a virtual private gateway, a NAT device, a peering connection, or a VPC endpoint in your VPC, you must update the route table for any subnet that uses these gateways or connections.
- There is a limit on the number of route tables you can create per VPC, and the number of routes you can add per route table.
    - Route tables per VPC: 100
    - Routes per route table : 50
    - BGP advertised routes per route table :100

Route Table Association









- The VPC console shows the number of subnets explicitly associated with each route table and provides information about subnets that are implicitly associated with the main route table.
- 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.

Route Priority

Destination	Target
10.0.0.0/16	Local
172.31.0.0/16	pcx-1a2b1a2b
0.0.0.0/0	igw-11aa22bb

- We use the most specific route in your route table that matches the traffic to determine how to route the traffic (longest prefix match).
- . For example, the following route table has a route for Internet traffic (`0.0.0.0/0`) that points to an Internet gateway, and a route for`172.31.0.0/16` traffic that points to a peering connection (`pcx-1a2b3c4d`). Any traffic from the subnet that's destined for the `172.31.0.0/16` IP address range uses the peering connection, because this route is more specific than the route for Internet gateway.
- Any traffic destined for within the VPC (10.0.0.0/16)is covered by local route

Route Priority

Course and Labs

- If you've attached a virtual private gateway to your VPC and enabled route propagation on your route table, routes representing your VPN connection automatically appear as propagated routes in your route table's list of routes.
- If these routes overlap with existing static routes and longest prefix match cannot be applied, then we prioritize the routes as follows in your VPC, from most preferred to least preferred:
  - Local routes for the VPC
  - Static routes whose targets are an Internet gateway, a virtual private gateway, a network interface, an instance ID, a VPC peering connection, or a VPC endpoint
  - Any propagated routes from a VPN connection or AWS Direct Connect connection

Route Priority

- If you have overlapping routes within a VPN connection and longest prefix match cannot be applied, then we prioritize the routes as follows in the VPN connection, from most preferred to least preferred:
  - BGP propagated routes from an AWS Direct Connect connection
  - Manually added static routes for a VPN connection
  - BGP propagated routes from a VPN connection

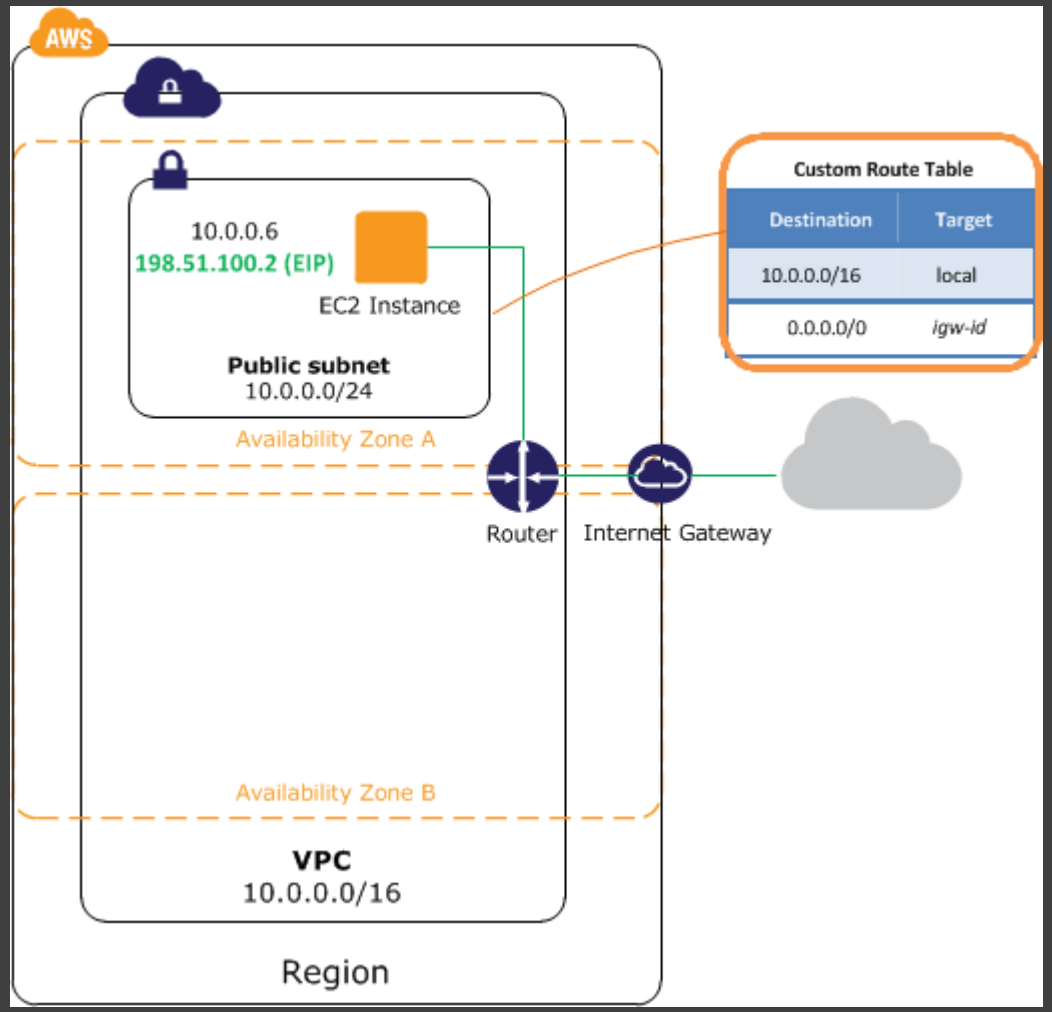
Destination	Target
10.0.0.0/16	Local
172.31.0.0/24	vgw-1a2b3c4d (propagated)
172.31.0.0/24	igw-11aa22bb

Routing Options

Course and Labs

- The Following routing Option are enabled in VPC
  - Internet Gateway
  - NAT Device
  - Virtual Private Gateway
  - VPC Peering Connections
  - VPC endpoint

Internet Gateways



- An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet.
- It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- An Internet gateway serves two purposes:
  - to provide a target in your VPC route tables for Internet-routable traffic,
  - To perform network address translation (NAT) for instances that have been assigned public IP addresses.

Internet Gateway Lifecycle

Course and Labs

- Create Internet Gateway
- Attaching a Internet gateway to a VPC
- Update Route table for Internet gateway
- Allow Security Group for Instance access to internet
- Assaign Public IP or Elastic IP to Instance
- Delete Route table for Internet Gateway
- Detach Internet Gateway to VPC
- Delete Internet Gateway

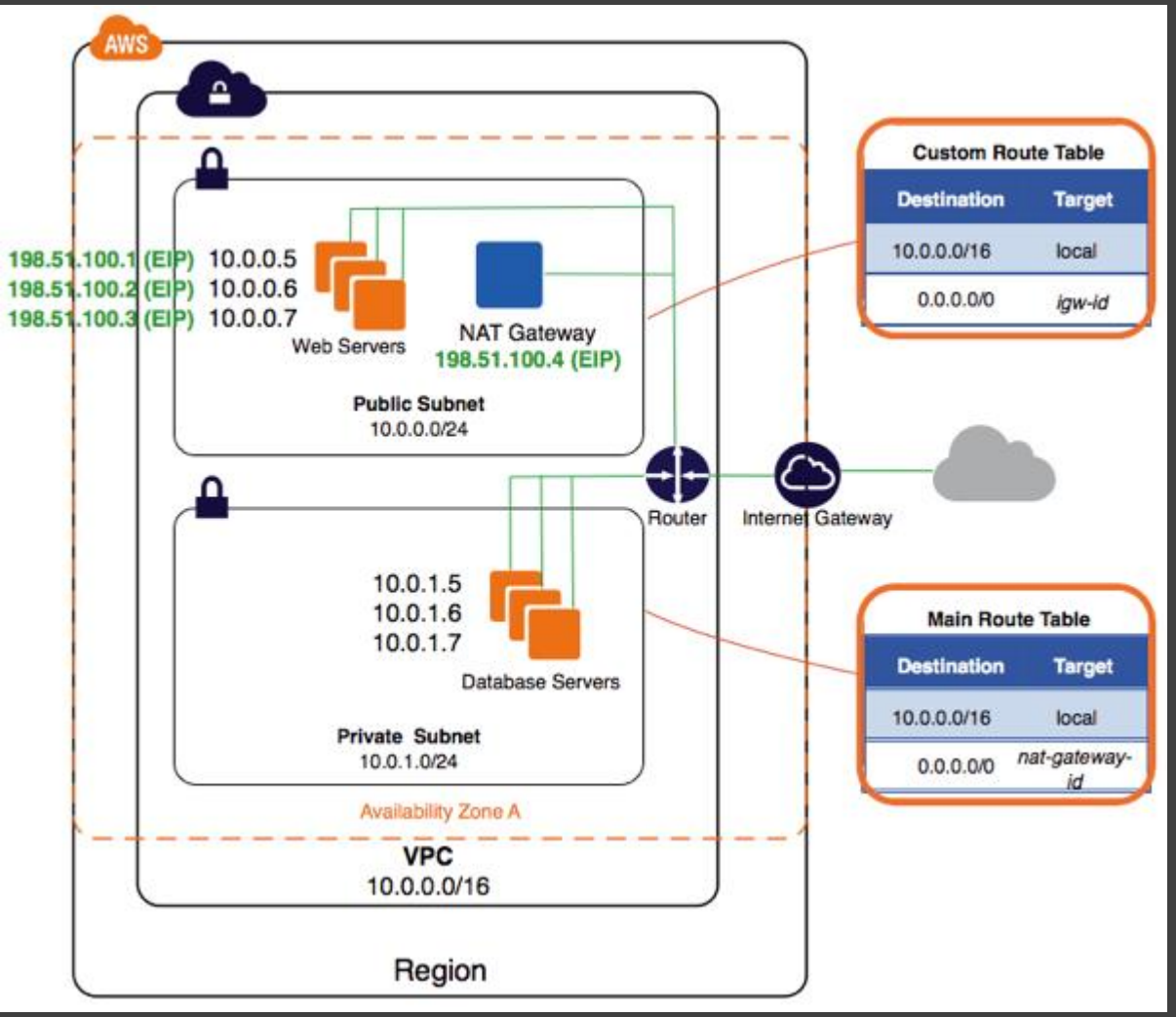
NAT Devices

- AWS offers two kinds of NAT devices
  - *NAT gateway*
  - *NAT instance*.

NAT Gateways

- You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances.
- You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply. Amazon EC2 charges for data transfer also apply.

NAT Gateway Basics



- To create a NAT gateway, you must specify the public subnet in which the NAT gateway will reside.
- You must also specify an Elastic IP address to associate with the NAT gateway when you create it.
- After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway.
- This enables instances in your private subnets to communicate with the Internet.
- Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone.
- You can create up to maximum of 5 NAT gateway per AZs
- Always create NAT Gateway in the same AZs of your instance to avoid AZ failure scenario

A NAT gateway characteristics:

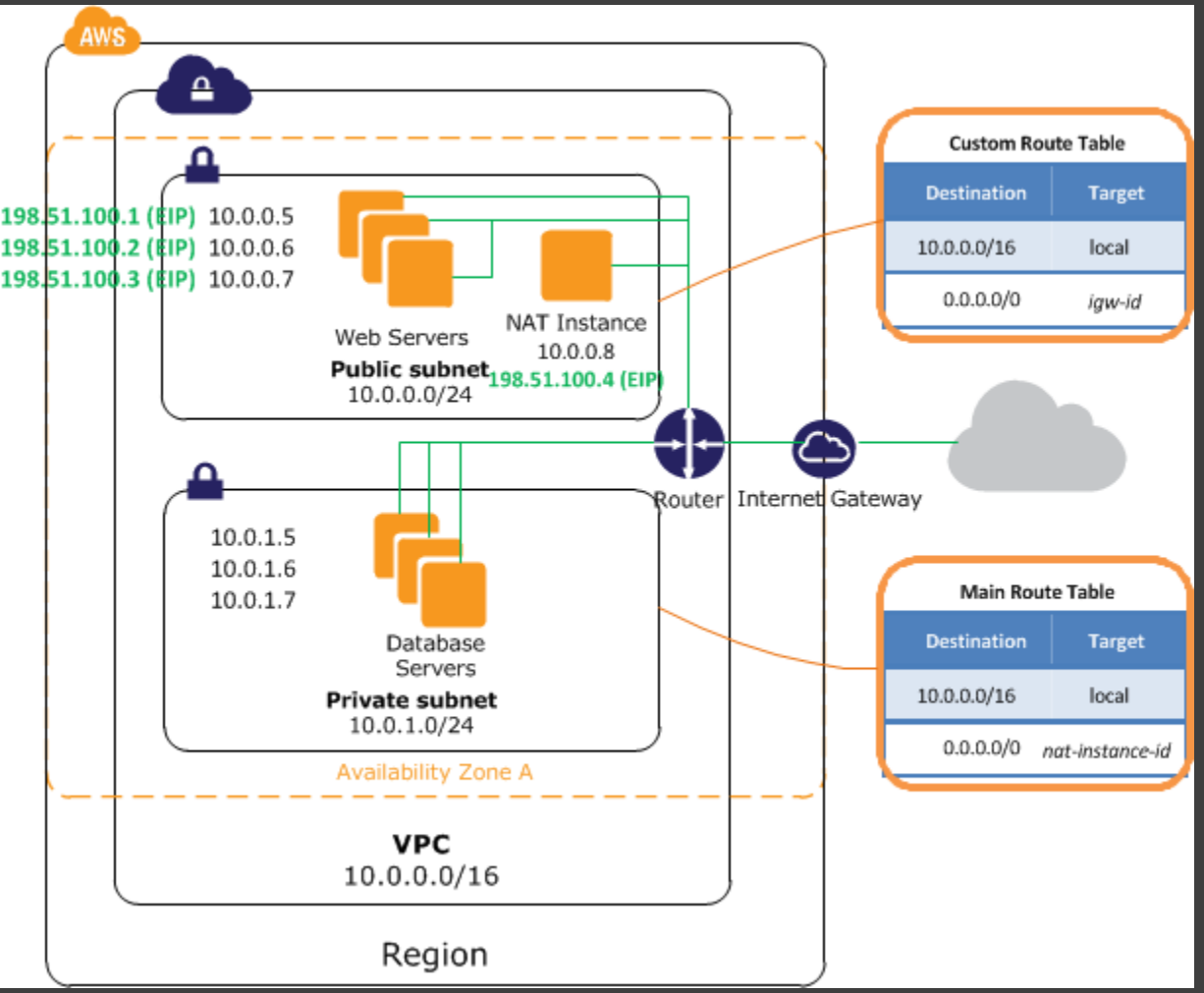
Course and Labs

- A NAT gateway supports bursts of up to 10 Gbps of bandwidth. If you require more than 10 Gbps bursts, you can distribute the workload by splitting your resources into multiple subnets, and creating a NAT gateway in each subnet.
- You can associate exactly one Elastic IP address with a NAT gateway. The association cannot be changed after you've created the NAT gateway. If you need to use a different Elastic IP address for your NAT gateway, you must create a new NAT gateway with the required address, update your route tables, and then delete the existing NAT gateway if it's no longer required.
- A NAT gateway supports the following protocols: TCP, UDP, and ICMP

A NAT gateway characteristics:

- You cannot associate a security group with a NAT gateway. You can use security groups for your instances in the private subnets to control the traffic to and from those instances.
- You can use a network ACL to control the traffic to and from the subnet in which the NAT gateway is located. The network ACL applies to the NAT gateway's traffic.
- When a NAT gateway is created, it receives an elastic network interface that's automatically assigned a private IP address from the IP address range of your subnet. You can view the NAT gateway's network interface in the Amazon EC2 console.

NAT Instances



- You can use a network address translation (NAT) instance in a public subnet in your VPC to enable instances in the private subnet to initiate outbound traffic to the Internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by someone on the Internet.
- Amazon provides Amazon Linux AMIs that are configured to run as NAT instances.
- These AMIs include the string `amzn-ami-vpc-nat` in their names, so you can search for them in the Amazon EC2 console. When you launch an instance from a NAT AMI, the following configuration occurs on the instance:
  - IPv4 forwarding is enabled and ICMP redirects are disabled in `/etc/sysctl.d/10-nat-settings.conf`
  - A script located at `/usr/sbin/configure-pat.sh` runs at startup and configures iptables IP masquerading

NAT Gateway Vs NAT Instances

Course and Labs

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Supports bursts of up to 10Gbps.	Depends on the bandwidth of the instance type.
Maintenance	Managed by AWS.You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.
Performance	Software is optimized for handling NAT traffic.	A generic Amazon Linux AMI that's configured to perform NAT.
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Type and size	Uniform offering; you don’t need to decide on the type or size.	Choose a suitable instance type and size, according to your predicted workload.

NAT Gateway Vs NAT Instances

Attribute	NAT gateway	NAT instance
Public IP addresses	Choose the Elastic IP address to associate with a NAT gateway at creation.	Use an Elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new Elastic IP address with the instance.
Private IP addresses	Automatically selected from the subnet's IP address range when you create the gateway.	Assign a specific private IP address from the subnet's IP address range when you launch the instance.
Security groups	Cannot be associated with a NAT gateway. You can associate security groups with your resources behind the NAT gateway to control inbound and outbound traffic.	Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic.
Network ACLs	Use a network ACL to control the traffic to and from the subnet in which your NAT gateway resides.	Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides.
Flow logs	Use flow logs to capture the traffic.	Use flow logs to capture the traffic.
Port forwarding	Not supported.	Manually customize the configuration to support port forwarding.
Bastion servers	Not supported.	Use as a bastion server.
Traffic metrics	Not supported	View CloudWatch metrics

DHCP Options Sets

- The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network.
- The Options field of a DHCP message contains the configuration parameters. Some of those parameters are the domain name, domain name server, and the netbios-node-type.
- DHCP options sets are associated with your AWS account so that you can use them across all of your virtual private clouds (VPC).
- When you create a VPC, we automatically create a set of DHCP options and associate them with the VPC. This set includes two options: `domain-name-servers=AmazonProvidedDNS`, and `domain-name=`*`domain-name-for-your-region`*. AmazonProvidedDNS is an Amazon DNS server, and this option enables DNS for instances that need to communicate over the VPC's Internet gateway. The string `AmazonProvidedDNS` maps to a DNS server running on a reserved IP address at the base of the VPC network range plus two. For example, the DNS server on a 10.0.0.0/16 network is located at 10.0.0.2.

DNS with Your VPC

- When you launch an instance in Default VPC we provide the instance with public and private DNS hostnames.
- Instances that you launch into a nondefault VPC might have public and private DNS hostnames, depending on the settings you specify for the VPC and for the instance.
- We support the following VPC attributes to control DNS support.

Attribute	Description
enableDnsHostnames	Indicates whether the instances launched in the VPC get DNS hostnames. If this attribute is true, instances in the VPC get DNS hostnames; otherwise, they do not.
enableDnsSupport	Indicates whether the DNS resolution is supported for the VPC. If this attribute is false, the Amazon provided DNS service in the VPC that resolves public DNS hostnames to IP addresses is not enabled. If this attribute is true, queries to the Amazon provided DNS server at the 169.254.169.253 IP address, or the reserved IP address at the base of the VPC network range plus two will succeed.

DHCP Options Sets

DHCP Option Name	Description
domain-name-servers	The IP addresses of up to four domain name servers, or AmazonProvidedDNS. The default DHCP option set specifies AmazonProvidedDNS. If specifying more than one domain name server, separate them with commas.
domain-name	If you're using AmazonProvidedDNS in us-east-1, specify ec2.internal. If you're using AmazonProvidedDNS in another region, specifyregion.compute.internal (for example, ap-northeast-1.compute.internal). Otherwise, specify a domain name (for example, MyCompany.com). Important Some Linux operating systems accept multiple domain names separated by spaces. However, other Linux operating systems and Windows treat the value as a single domain, which results in unexpected behavior. If your DHCP options set is associated with a VPC that has instances with multiple operating systems, specify only one domain name.
ntp-servers	The IP addresses of up to four Network Time Protocol (NTP) servers.
netbios-name-servers	The IP addresses of up to four NetBIOS name servers.
netbios-node-type	The NetBIOS node type (1, 2, 4, or 8). We recommend that you specify 2 (broadcast and multicast are not currently supported).

Network ACLs

- A *network access control list (ACL)* is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Security Group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group)

Network ACL Basics

- A network ACL is a numbered list of rules that we evaluate in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules with rule numbers that are multiples of 100, so that you can insert new rules where you need to later on.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Your VPC automatically comes with a modifiable default network ACL; by default, it allows all inbound and outbound traffic.
- You can create custom network ACL. Each custom network ACL starts out closed (permits no traffic) until you add rules.
- Each subnet must be associated with a network ACL; if you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

Network ACL Rules

- Rule number. Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that may contradict it.
- Protocol. You can specify any protocol that has a standard protocol number, If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.
- [Inbound rules only] The source of the traffic (CIDR range) and the destination (listening) port or port range.
- [Outbound rules only] The destination for the traffic (CIDR range) and the destination port or port range.
- Choice of ALLOW or DENY for the specified traffic.

Default Network ACL

Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	ALLOW
*	All traffic	All	All	0.0.0.0/0	DENY
Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
100	All traffic	all	all	0.0.0.0/0	ALLOW
*	All traffic	all	all	0.0.0.0/0	DENY

- The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated.
- Each network ACL includes a rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule.

VPC Flow Logs

- VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.
- Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.
- It helps to troubleshoot why specific traffic is not reaching an instance, which in turn can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.

Flow Logs Basics

- You can create a flow log for a VPC, a subnet, or a network interface. If you create a flow log for a subnet or VPC, each network interface in the VPC or subnet is monitored.
- Flow log data is published to a log group in CloudWatch Logs, and each network interface has a unique log stream. Log streams contain *flow log records*, which are log events consisting of fields that describe the traffic for that network interface.
- To create a flow log, Specify the Following
  - Resource
  - type of traffic to capture (accepted traffic, rejected traffic, or all traffic),
  - name of a log group in CloudWatch Logs to which the flow log will be published
  - ARN of an IAM role that has sufficient permission to publish the flow log to the CloudWatch Logs log group.
- You can create flow logs for network interfaces that are created by other AWS services; for example, Elastic Load Balancing, Amazon RDS, Amazon ElastiCache, Amazon Redshift, and Amazon WorkSpaces.
- If you no longer require a flow log, you can delete it. Deleting a flow log disables the flow log service for the resource, and no new flow log records or log streams are created. It does not delete any existing flow log records or log streams for a network interface. To delete an existing log stream, you can use the CloudWatch Logs console. After you've deleted a flow log, it can take several minutes to stop collecting data.