AMAZON AWS SOLUTIONS ARCHITECT

AMAZON VPC AND NETWORKING OVERVIEW

AMAZON VIRTUAL PRIVATE CLOUD

- Networking layer for Amazon Elastic Compute Cloud (Amazon EC2)
- Allows you to create your own virtual Network within AWS
- Allows you to select your own IP Address Range(s), Subnet(s), Route Table(s), Gateway(s) and security settings
- VPCs are logically even if the IP Addresses are shared
- An IPv4 CIDR (Classless Inter-Domain Routing) Block is selected
  - The address range can not be changed after the VPC is created
  - The smallest subnet is /28 (16 Addresses)
  - The largest subnet is /16 (65,536 Addresses)
- Addresses should not be overlap with any other network with which they will be connected
- A Default VPC will be created in each region, with a default subnet created in each Availability zone
  - Default CIDR Block is 172.31.0.0/16

NETWORKING ADDRESS TYPES

Address Type	Description
Public DNS Name	• On launch, a public DNS name is generated for the instance • Persists only while that instance is running and can not be transferred to another instance under any circumstances • Mainly used to SSH into the box from a remote host. Otherwise, Route53 would be setup with a domain name
Public IP	• On launch, a publicly routable IP address is generated for the instance • Persists only while that instance is running and can not be transferred to another instance under any circumstances • IP address is from AWS's CIDR block
Elastic IP	• Address unique on the internet that is reserved independently from AWS and associated with an EC2 instance • Persistent until released by the customer, and is not tied to the lifetime or state of a particular instance

SECURITY GROUPS

- You can specify allow rules, but **not deny rules**.
- You can specify separate rules for inbound and outbound traffic.
- When you create a security group, it has **no inbound rules**. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
- By default, a security group includes an **outbound rule that allows all outbound traffic**. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.
- Security groups are stateful — **if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules**. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.
- Instances associated with a security group can't talk to each other unless you add rules allowing it (exception: the default security group has these rules by default).
- Security groups are **associated with network interfaces**. After you launch an instance, you can change the security groups associated with the instance, which changes the security groups associated with the primary network interface (eth0). You can also change the security groups associated with any other network interface.

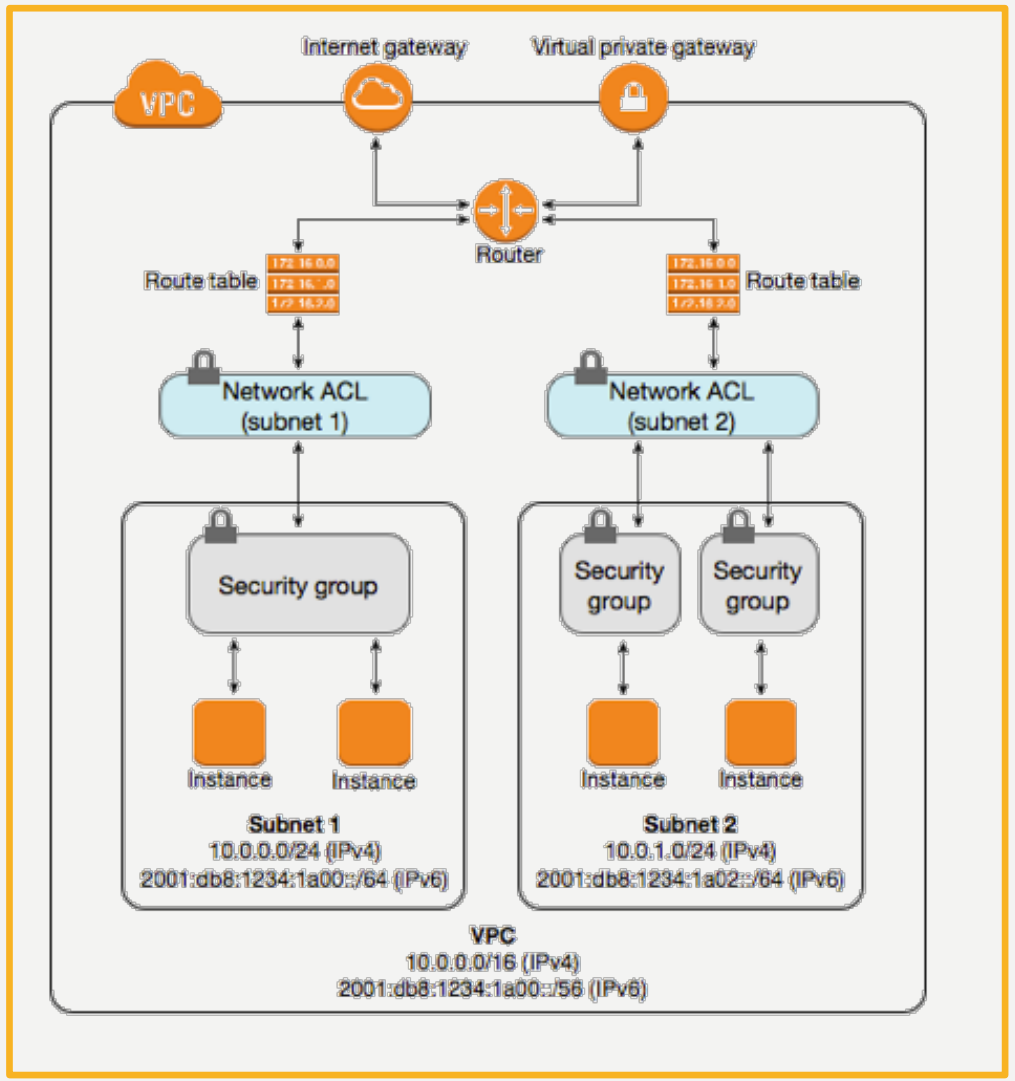
ACCESS SECURITY LISTS (ACL'S)

- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC 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.
- You can associate a network ACL with multiple subnets; however, **a subnet can be associated with only one network ACL at a time**. When you associate a network ACL with a subnet, the previous association is removed.
- A network ACL contains 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.
- Network ACLs **are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic** (and vice versa).

SECURITY GROUPS & ACL'S

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)

SECURITY GROUPS & ACL'S



1. Traffic from an Internet gateway is routed to the appropriate subnet using the routes in the routing table.
2. The rules of the network ACL associated with the subnet control which traffic is allowed to the subnet.
3. The rules of the security group associated with an instance control which traffic is allowed to the instance.

VPC COMPONENTS

- Subnets
- Route Tables
- Dynamic Host Configuration Protocol (DHCP) option sets
- Security Groups
- Network Access Control Lists (ACLs)
- Optional Components
  - Internet Gateways
  - Elastic IP Addresses
  - Elastic Network Interfaces
  - Endpoints
  - Peering
  - NAT Translations and NAT Gateways
  - Virtual Private Gateways, Customer Gateways, and Virtual Private Networks

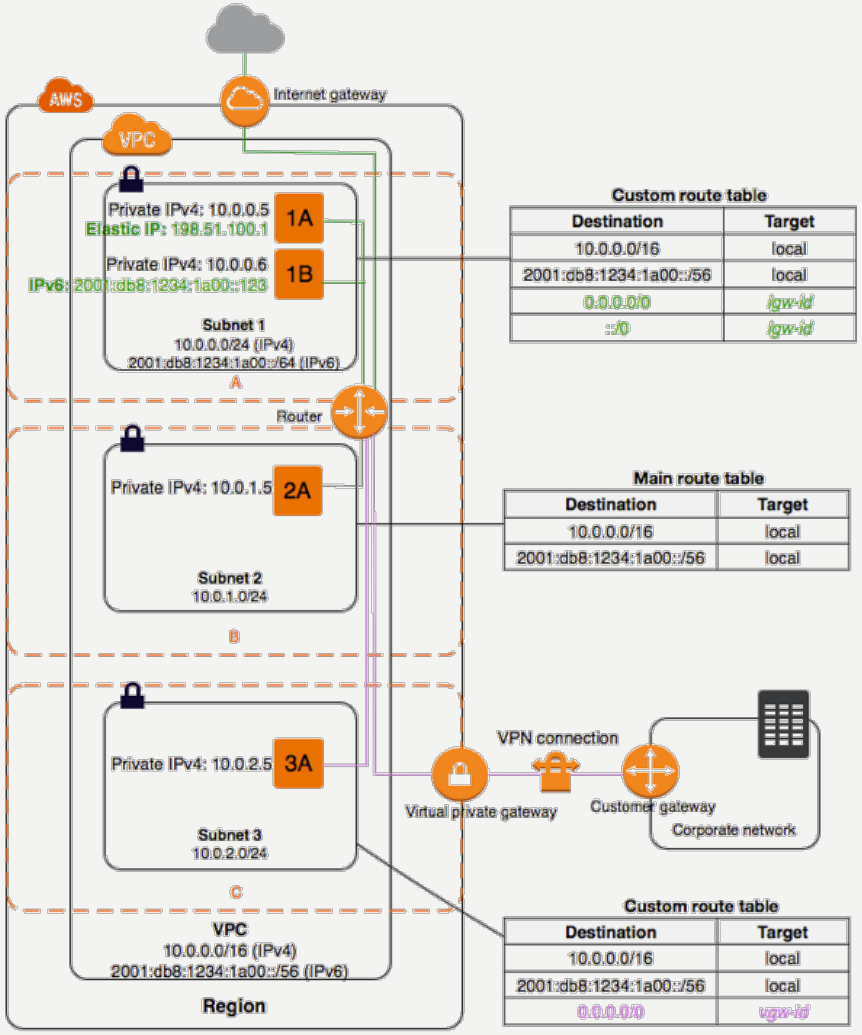
CIDR BLOCK RULES

- The allowed block size is between a /28 netmask and /16 netmask.
- The CIDR block must not overlap with any existing CIDR block that's associated with the VPC
- There are restrictions on the ranges of IPv4 addresses you can use. For more information, see IPv4 CIDR Block Association Restrictions.
- You cannot increase or decrease the size of an existing CIDR block.
- You have a limit on the number of CIDR blocks you can associate with a VPC and the number of routes you can add to a route table. You cannot associate a CIDR block if this results in you exceeding your limits. For more information, see Amazon VPC Limits.
- The CIDR block must not be the same or larger than the CIDR range of a route in any of the VPC route tables. For example, if you have a route with a destination of 10.0.0.0/24 to a virtual private gateway, you cannot associate a CIDR block of the same range or larger. However, you can associate a CIDR block of 10.0.0.0/25or smaller.

SUBNETS

- Subnet is a segment of an VPC's IP address range where you can launch EC2 instances or other resources
- CIDR blocks define subnets
- AWS Reserves the **first four** IP Addresses, and the **last** IP Address of each subnet
  - For example, a 10.0.0.0/28 subnet, will only have 11 IP Addresses available for use
- One of more subnets can exist in each Availability Zone
- Subnets reside within one Availability Zone and cannot span zones
- Subnets can be either:
  - **Public**: **All** traffic is directed to the VPC's Internet Gateway
  - **Private**: **No** traffic directed towards the Internet Gateway
  - **VPN Only**: Traffic is directed only towards the VPC's **Virtual Private Gateway**
- Default VPCs contain one public subnet in every AZ within the region, with a subnet of /20
- The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset of the CIDR block for the VPC (for multiple subnets).

SUBNETS



- Subnet 1 is an example of a **Public** Subnet
  - All non-internal traffic is routed to an Internet Gateway
- Subnet 2 is an example of a **Private** Subnet
  - There is no traffic that is routable to the internet through an Internet Gateway
- Subnet 3 is an example of a **Virtual-Private** Subnet
  - There is no traffic routable to the Internet, and all non-internal traffic is routed back to the Virtual Private Gateway (typically a VPN)

RESERVED SUBNET ADDRESSES

- 10.0.0.**0**: Network address.
- 10.0.0.**1**: Reserved by AWS for the VPC router.
- 10.0.0.**2**: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. For more information, see Amazon DNS Server.
- 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.

SUBNET ROUTING

- A route table (RT) is a logical construct within a VPC that applies rules to direct network traffic
- RT's allow resources within different subnets within a VPC to communicate with each other
- RT's can be modified by users, by adding or modifying custom rules
- Route tables are used to specify which subnets are public, or private
- Each route table contains the default route, called the **local route**
  - This route can not be modified or removed
  - Enables communication within the VPC
- Additional routes can be added to direct traffic to exit outside of the VP

INTERNET GATEWAYS

- An Internet Gateway is a logical connection between an Amazon VPC and the Internet.
- IG's therefore impose no availability risks or bandwidth constraints on your network traffic.
- It is not a physical device.
- 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 IPv4 addresses.
- Only one can be associated with each VPC.
- It does not limit the bandwidth of Internet connectivity. (The only limitation on bandwidth is the size of the Amazon EC2 instance, and it applies to all traffic -- internal to the VPC and out to the Internet.
- If a VPC **does not have** an Internet Gateway, then the resources in the VPC **cannot be accessed from the Internet** (unless the traffic flows via a corporate network and VPN/Direct Connect).

NAT INSTANCES AND GATEWAYS

- NAT device to enable instances in a private subnet to connect to the Internet (for example, for software updates) or other AWS services, but prevent the Internet from initiating connections with the instances.
- When traffic goes to the Internet, the source IPv4 address is replaced with the NAT device's address and similarly, when the response traffic goes to those instances, the NAT device translates the address back to those instances' private IPv4 addresses.
- NAT Instances
  - Created from AWS Instances
  - Bandwidth depends on the Instance Type
  - Managed by the user
- NAT Gateways
  - Highly available appliances
  - Supports bursts of data up to 10Gbps
  - Managed by AWS
  - Uniform offering; you don't need to decide on the type or size.

NAT INSTANCES VS NAT GATEWAYS

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.

NAT INSTANCES VS NAT GATEWAYS

Attribute	NAT gateway	NAT instance
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.
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.

NAT INSTANCES VS NAT GATEWAYS

Attribute	NAT gateway	NAT 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.

NAT INSTANCES VS NAT GATEWAYS

Attribute	NAT gateway	NAT instance
Port forwarding	Not supported.	Manually customize the configuration to support port forwarding.
Bastion servers	Not supported.	Use as a bastion server.
Traffic metrics	View CloudWatch metrics for the NAT gateway.	View CloudWatch metrics for the instance.
Timeout behavior	When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet).	When a connection times out, a NAT instance sends a FIN packet to resources behind the NAT instance to close the connection.
IP fragmentation	Supports forwarding of IP fragmented packets for the UDP protocol. Does not support fragmentation for the TCP and ICMP protocols. Fragmented packets for these protocols will get dropped.	Supports reassembly of IP fragmented packets for the UDP, TCP, and ICMP protocols.

VPC LIMITS

Resource	Default limit	Comments
VPCs per region	5	The limit for internet gateways per region is directly correlated to this one. Increasing this limit increases the limit on internet gateways per region by the same amount. The number of VPCs in the region multiplied by the number of security groups per VPC cannot exceed 5000.
Subnets per VPC	200	-
IPv4 CIDR blocks per VPC	5	This limit is made up of your primary CIDR block plus 4 secondary CIDR blocks.
IPv6 CIDR blocks per VPC	1	This limit cannot be increased.
Elastic IP addresses per region	5	This is the limit for the number of Elastic IP addresses for use in EC2-VPC

ROUTING TABLES

- 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 cannot delete the main route table, but 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 the external corporate network 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.

ROUTING TABLES

- Every route table contains a local route for communication within the VPC over IPv4.
  - If your VPC has more than one IPv4 CIDR block, your route tables contain a local route for each IPv4 CIDR block.
  - If you've associated an IPv6 CIDR block with your VPC, your route tables contain a local route for the IPv6 CIDR block. You cannot modify or delete these routes.
- When you add an Internet gateway, an egress-only 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.
- Your VPC can have route tables other than the default table.
  - One way to protect your VPC is to leave the main route table in its original default state (with only the local route), and explicitly associate each new subnet you create with one of the custom route tables you've created.
  - This ensures that you explicitly control how each subnet routes outbound traffic.

ROUTE PRIORITY

- We use the most specific route in your route table that matches the traffic to determine how to route the traffic (longest prefix match).
- Routes to IPv4 and IPv6 addresses or CIDR blocks are independent of each other; we use the most specific route that matches either IPv4 traffic or IPv6 traffic to determine how to route the traffic.
- The following route table has a route for:
  - IPv4 Internet traffic (0.0.0.0/0) that points to an Internet gateway,
  - A route for172.31.0.0/16 IPv4 traffic that points to a peering connection (pcx-1a2b3c4d).
  - Any traffic from the subnet that's destined for the172.31.0.0/16 IP address range uses the peering connection, because this route is more specific than the route for Internet gateway.
  - Any traffic destined for a target within the VPC (10.0.0.0/16) is covered by the Local route, and therefore routed within the VPC. All other traffic from the subnet uses the Internet gateway.

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

ROUTING OPTIONS

Connection Type	Description
Internet Gateway	Create and attach an Internet gateway to your VPC, and then add a route with a destination of 0.0.0.0/0 for IPv4 traffic or ::/0 for IPv6 traffic, and a target of the Internet gateway ID (igw-xxxxxxxx).
NAT Device	Create a NAT gateway or launch a NAT instance in a public subnet, and then add a route for the private subnet that routes IPv4 Internet traffic (0.0.0.0/0) to the NAT device.
Virtual Private Gateway	Create and attach a virtual private gateway to your VPC, and then add a route with the destination of your network and a target of the virtual private gateway (vgw-xxxxxxxx).
VPC Peering Connection	Create a route to one or more of your VPC route tables that points to the VPC peering connection to access all or part of the CIDR block of the other VPC in the peering connection. Similarly, the owner of the other VPC must add a route to their VPC route table to route traffic back to your VPC.

GATEWAY LIMITS

Resource	Default limit	Comments
Customer gateways per region	50	To increase this limit, contact AWS Support.
Egress-only internet gateways per region	5	This limit is directly correlated with the limit on VPCs per region. To increase this limit, increase the limit on VPCs per region. Only one egress-only internet gateway can be attached to a VPC at a time.
Internet gateways per region	5	This limit is directly correlated with the limit on VPCs per region. To increase this limit, increase the limit on VPCs per region. Only one internet gateway can be attached to a VPC at a time.
NAT gateways per Availability Zone	5	A NAT gateway in the pending, active, or deleting state counts against your limit.
Virtual private gateways per region	5	Only one virtual private gateway can be attached to a VPC at a time.

DHCP OPTION SETS

- The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network
- The Amazon EC2 instances you launch into a non default VPC are private by default; they're not assigned a public IPv4 address unless you specifically assign one during launch, or you modify the subnet's public IPv4 address attribute.
- By default, all instances in a non default VPC receive an unresolvable host name that AWS assigns (for example, ip-10-0-0-202).
- You can assign your own domain name to your instances, and use up to four of your own DNS servers.
- After you create a set of DHCP options, you can't modify them. If you want your VPC to use a different set of DHCP options, you must create a new set and associate them with your VPC.
- You can have multiple sets of DHCP options, **but you can associate only one set of DHCP options with a VPC at a time.** If you delete a VPC, the DHCP options set associated with the VPC are also deleted.

DHCP OPTION SETS

DHCP Option	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. Although you can specify up to four domain name servers, note that some operating systems may impose lower limits.
domain-name	If you're using Amazon Provided DNS in us-east-1, specify ec2.internal. If you're using Amazon Provided DNS in another region, specify *region*.compute.internal (for example, ap-northeast-1.compute.internal). Otherwise, specify a domain name (for example, foobar.com). This value is used to complete unqualified DNS hostnames.
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 (point-to-point, or P-node). Broadcast and multicast are not currently supported.

AMAZON DNS SERVER

- When you create a VPC, we automatically create a set of DHCP options and associate them with the VPC
- 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 IPv4 network range, plus two.
  - For example, the DNS Server on a 10.0.0.0/16 network is located at 10.0.0.2.
  - For VPCs with multiple IPv4 CIDR blocks, the DNS server IP address is located in the primary CIDR block.
- When you launch an instance into a VPC, we provide the instance with a private DNS hostname, and a public DNS hostname if the instance receives a public IPv4 address.

AMAZON DNS SERVER

- If domain-name-servers in your DHCP options is set to AmazonProvidedDNS, the public DNS hostname takes the form **ec2-*public-ipv4-address*.compute-1.amazonaws.com** for the us-east-1 region, and **ec2-*public-ipv4-address.region*.compute.amazonaws.com** for other regions.
- The private hostname takes the form **ip-*private-ipv4-address*.ec2.internal** for the us-east-1 region, and i**p-*private-ipv4-address.region*.compute.internal** for other regions.
- The Amazon DNS server in your VPC is used to resolve the DNS domain names that you specify in a private hosted zone in Route 53.

ELASTIC IP ADDRESSES

- You can associate an Elastic IP address with any instance or network interface for any VPC in your account.
- With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.
- You first allocate an Elastic IP address for use in a VPC, and then associate it with an instance in your VPC (it can be assigned to only one instance at a time).
- An Elastic IP address is a property of network interfaces. You can associate an Elastic IP address with an instance by updating the network interface attached to the instance.
- If you associate an Elastic IP address with the eth0 network interface of your instance, its current public IPv4 address (if it had one) is released to the EC2-VPC public IP address pool.
- You can move an Elastic IP address from one instance to another. The instance can be in the same VPC or another VPC, but not in EC2-Classic.
- Your Elastic IP addresses remain associated with your AWS account until you explicitly release them.
- You're limited to five Elastic IP addresses; to help conserve them, you can use a NAT device
- An Elastic IP address is accessed through the Internet gateway of a VPC. If you have set up a VPN connection between your VPC and your network, the VPN traffic traverses a virtual private gateway, not an Internet gateway, and therefore cannot access the Elastic IP address.

VPC PEERING

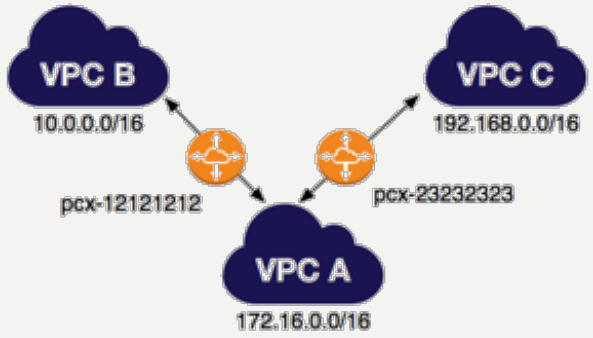
- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately
- Instances in either VPC can communicate with each other as if they are within the same network.
- You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware.

VPC PEERING STEPS

1. The owner of the requester VPC sends a request to the owner of the accepter VPC to create the VPC peering connection. The accepter VPC can be owned by you, or another AWS account, and **cannot have a CIDR block that overlaps with the requester** VPC's CIDR block.
2. The owner of the accepter VPC accepts the VPC peering connection request to activate the VPC peering connection.
3. To enable the flow of traffic between the VPCs using private IP addresses, the owner of each VPC in the VPC peering connection **must manually add a route to one or more of their VPC route tables** that points to the IP address range of the other VPC (the peer VPC).
4. If required**, update the security group rules that are associated with your instance** to ensure that traffic to and from the peer VPC is not restricted. If both VPCs are in the same region, you can reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group rules.
5. If both VPCs are in the same region, **you can modify your VPC connection to enable DNS hostname resolution.** By default, if instances on either side of a VPC peering connection address **each other using a public DNS hostname**, the hostname resolves to the instance's public IP address.

VPC PEERING

- A VPC peering connection is a one to one relationship between two VPCs.
- You can create multiple VPC peering connections for each VPC that you own, but transitive peering relationships are not supported.
- You do not have any peering relationship with VPCs that your VPC is not directly peered with.
- The following diagram is an example of one VPC peered to two different VPCs.
  - There are two VPC peering connections: VPC A is peered with both VPC B and VPC C.
  - VPC B and VPC C are not peered, and you cannot use VPC A as a transit point for peering between VPC B and VPC C.
  - If you want to enable routing of traffic between VPC B and VPC C, you must create a unique VPC peering connection between them.



VPC PEERING LIMITATIONS

- You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv4 or IPv6 CIDR blocks
- You have a limit on the number active and pending VPC peering connections that you can have per VPC
- VPC peering does not support **transitive peering relationships**. In a VPC peering connection, your VPC does not have access to any other VPCs with which the peer VPC may be peered. This includes VPC peering connections that are established entirely within your own AWS account
- You cannot have more than one VPC peering connection between the same two VPCs at the same time
- A placement group can span peered VPCs that are in the same region; however, you do not get full-bisection bandwidth between instances in peered VPCs.
- Inter-Region VPC Peering is **allowed** as of November 2017. The exam MIGHT not acknowledge this fact yet

MANAGED VPN CONNECTIONS

- By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network.
- You can enable access to your remote network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.
- VPN connection is a general term, in the Amazon VPC documentation, a VPN connection refers to the connection between your VPC and your own network.
- AWS supports Internet Protocol security (IPsec) VPN connections.

VIRTUAL PRIVATE GATEWAY

- You can connect an existing data center to Amazon VPC using either hardware or software VPN Connections
- A Virtual Private Gateway (VPG) is the VPN appliance on the AWS side of the VPN Connection
- A Customer Gateway (CGW) represents the physical device or application on the customer's side of the VPN
- After the two elements are created, the next step is to create a VPN Tunnel
- You must specify the type of routing for a VPN Connection
  - Dynamic routing will be used if the CGW supports Border Gateway Protocol
  - Static routing is used otherwise, and the routes must be manually entered
  - Routes will be propagated back to Amazon VPC to allow the routing of traffic
- VPC supports multiple CGWs each having a connection to a single VPG
- The VPN Tunnel must be initiated from the customer gateway to the virtual private gateway

QUESTIONS?