review

review questions

Virtual Private Cloud (VPC)
V1.01

Course title

BackSpace Academy
AWS Certified Associate

BackSpace

This "learning by quizzes" exercise will be based upon the course videos and the following reference material:

Section: VPCs and Subnets

Reference: Amazon Virtual Private Cloud User Guide

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

Question

If your VPC is too small to meet your needs, you can change the CIDR block size using the AWS console, CLI or API tools.

Answers

- True
- False

B
You must terminate all the instances in the VPC, delete the VPC, and then create a new, larger VPC. You can although associate a secondary IPv4 CIDR block in order to increase the VPC size. See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Sizing

Question

If your VPC is too small to meet your needs, you can associate a secondary IPv4 CIDR block in order to increase the VPC size.

Answers

A. True
B. False

A
You can associate a secondary IPv4 CIDR block in order to increase the VPC size. See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Sizing

Question

Your VPC CIDR range should be one large enough for expected future growth, but not one that overlaps with current or expected future subnets anywhere in your corporate or home network, or that overlaps with current or future VPCs.

Answers

A. True
B. False

A
You can optionally set up a connection between your VPC and your corporate or home network. If you have an IPv4 address prefix in your VPC that overlaps with one of your networks' prefixes, any traffic to the network's prefix is dropped. We therefore recommend that you create a VPC with a CIDR range large enough for expected future growth, but not one that overlaps with current or expected future subnets anywhere in your corporate or home network, or that overlaps with current or future VPCs.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VGW

Question

If a subnet doesn't have a route to the Internet gateway, but has its traffic routed to a virtual private gateway, the subnet is known as a_____.

Answers

VPN-only subnet
private subnet
public subnet
None of the above

A
See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#vpc-subnet-basics

Question

You cannot use the first four IP addresses and the last four IP address in each subnet CIDR block.

Answers

A. True
B. False

B
AWS reserves both the first four IP addresses and the last IP address in each subnet CIDR block. They're not available for you to use.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Sizing

This "learning by quizzes" exercise will be based upon the course videos and the following reference material:

Section: Default VPC and Default Subnets

Reference: Amazon Virtual Private Cloud User Guide

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/default-vpc.html

Question

A newly created default VPC includes:

Answers

A. A default subnet in each Availability Zone.
B. An Internet gateway connected to your default VPC.
C. A main route table for your default VPC with a rule that sends all traffic destined for the Internet to the Internet gateway.
D. A default security group, network access control list (ACL) and, default DHCP options set for your AWS account associated with your default VPC.
E. All of the above

E
When we create a default VPC, we do the following to set it up for you:

A. Create a VPC with a size /16 IPv4 CIDR block (172.31.0.0/16). This provides up to 65,536 private IPv4 addresses.
B. Create a size /20 default subnet in each Availability Zone. This provides up to 4,096 addresses per subnet, a few of which are reserved for our use.
C. Create an internet gateway and connect it to your default VPC.
D. Create a main route table for your default VPC with a rule that sends all IPv4 traffic destined for the internet to the internet gateway.
E. Create a default security group and associate it with your default VPC.
F. Create a default network access control list (ACL) and associate it with your default VPC.
G. Associate the default DHCP options set for your AWS account with your default VPC.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/default-vpc.html

Question

The CIDR block for a default VPC is always 172.31.0.0/24.

Answers

A. True
B. False

B
The CIDR block for a default VPC is always 172.31.0.0/16.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/default-vpc.html

This "learning by quizzes" exercise will be based upon the course videos and the following reference material:

Section: Security

Reference: Amazon Virtual Private Cloud User Guide

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html

Question

You can secure your VPC instances using only security groups; however, you can add _____ as a second layer of defense.

Answers

A. Route Tables
B. Network ACLs
C. VPN
D. Virtual Private Gateway

B
You can secure your VPC instances using only security groups; however, you can add network ACLs as a second layer of defense.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html

Question

Security Groups operate at the _____ level.

Answers

A. Subnet
B. Instance
C. VPC
D. None of the above

B
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

Question

Network ACL operate at the _____ level.

Answers

A. Subnet
B. Instance
C. VPC
D. None of the above

A
A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. 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.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

Question

Network ACL

Answers

A. Is stateless: Return traffic must be explicitly allowed by rules
B. Is stateful: Return traffic is automatically allowed, regardless of any rules
C. None of the above

A
Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#ACLs

Question

Security Groups support allow rules and deny rules

Answers

A. True
B. False

B
You can specify allow rules, but not deny rules.

See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html#VPCSecurityGroups

Question

Security Group automatically applies to all instances in the subnets it's associated with.

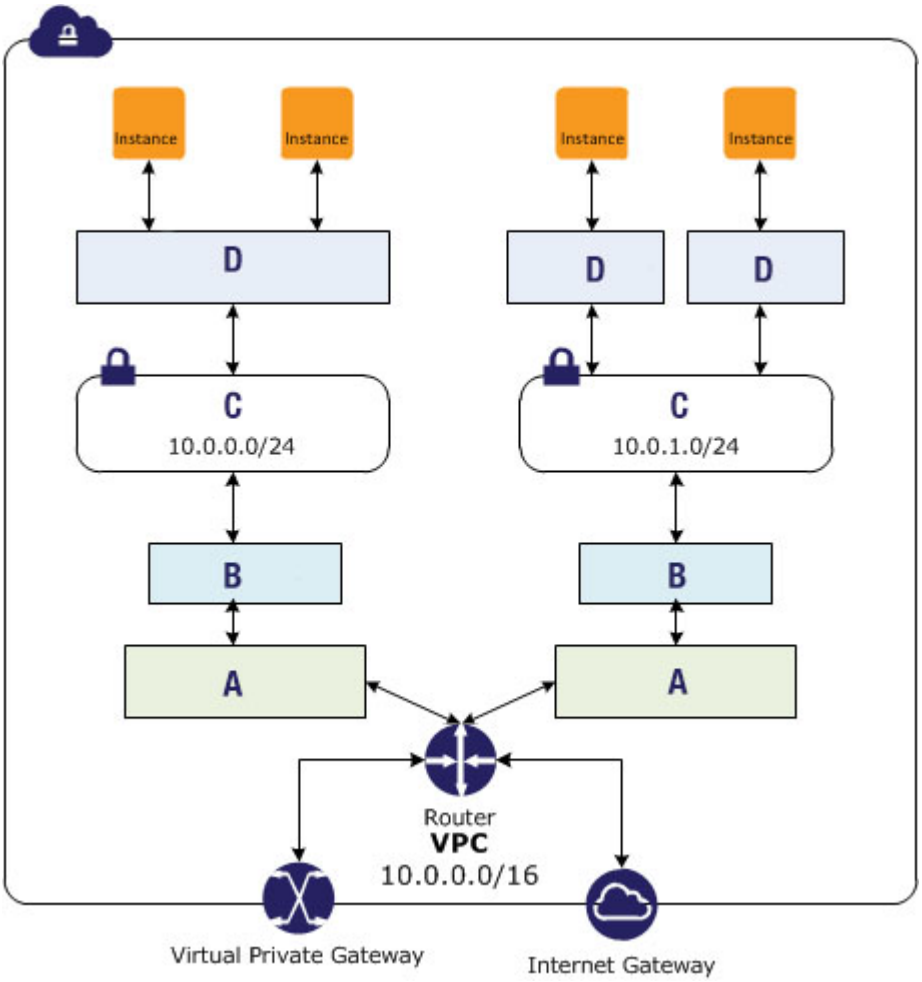
Answers

A. True
B. False

B
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.

See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html#VPCSecurityGroups

Question



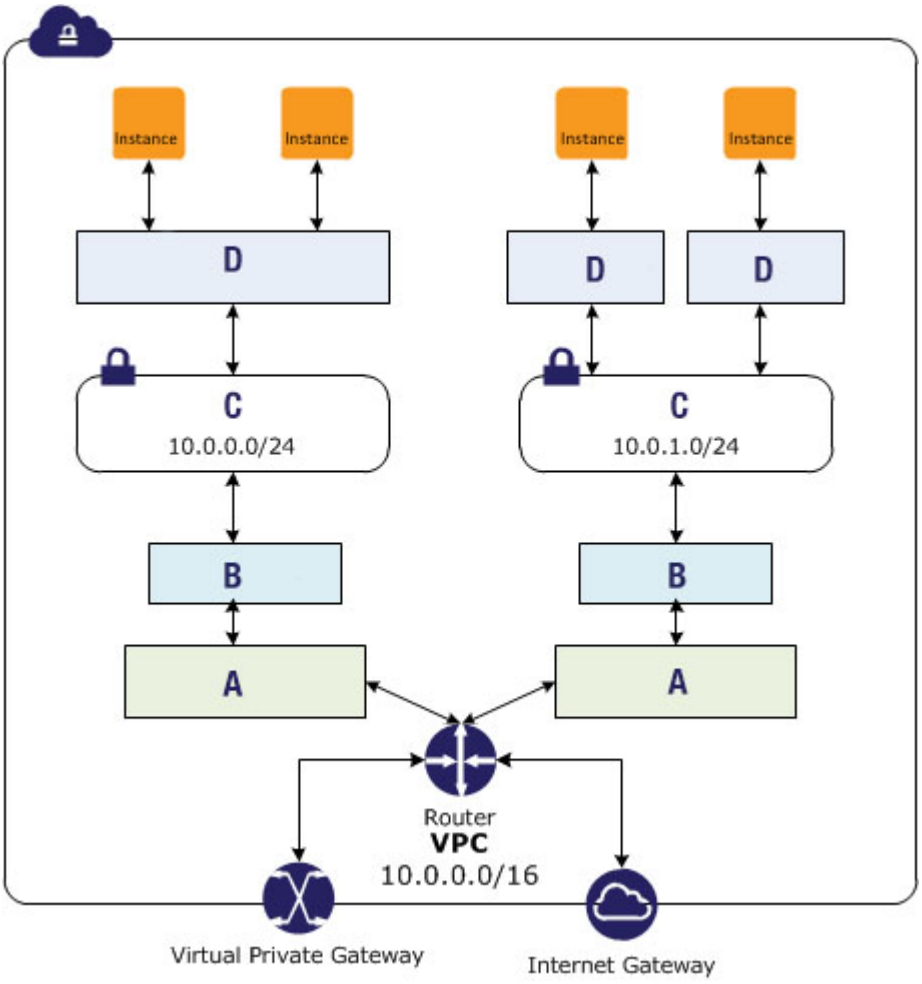
The Subnet is located at:

Answers

A
B
C
D

C

Question



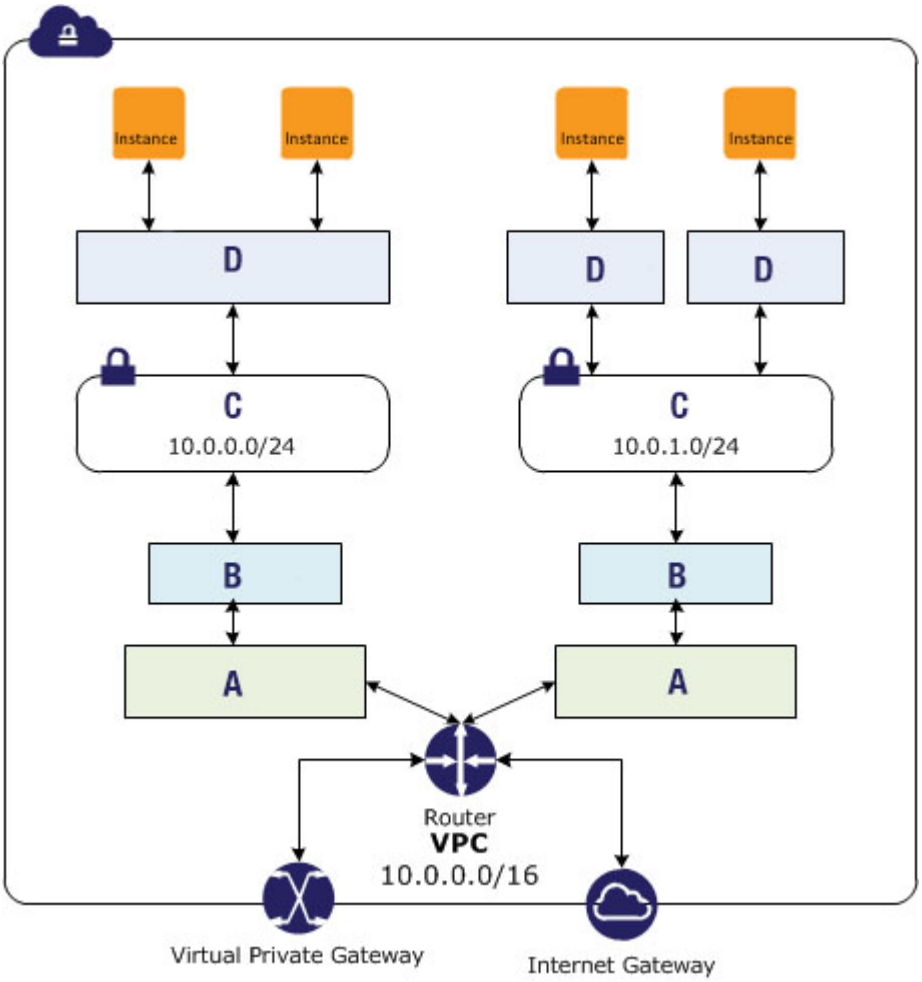
The Network ACL is located at:

Answers

A. A
B. B
C. C
D. D

B
Network ACL operate in front of the subnet

Question



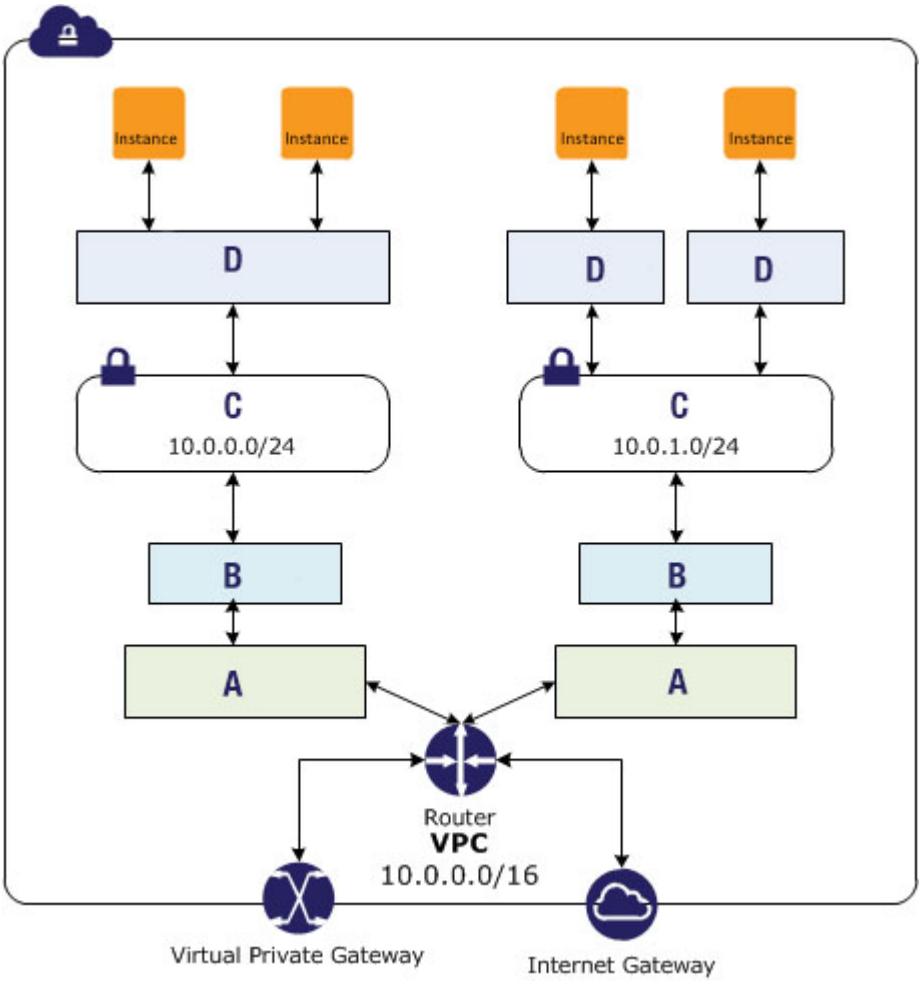
The Security Group is located at:

Answers

A. A
B. B
C. C
D. D

D
Security Groups operate in front of an instance

Question



The Routing Table is located at:

Answers

A. A
B. B
C. C
D. D

A
The Routing Table is located after the router.

Question

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Answers

A. True
B. False

A
See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

Question

By default, no outbound traffic is allowed until you add outbound rules to the security group.

Answers

A. True
B. False

B
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.

See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html#VPCSecurityGroups

Question

Responses to inbound traffic allowed by security group rules are allowed to flow outbound regardless of outbound rules, and vice versa.

Answers

A. True
B. False

A
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.

See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html#VPCSecurityGroups

Question

When you specify a security group as the source for a rule, this allows instances associated with the source security group to access instances in the security group.

Answers

A. True
B. False

A
When you specify a security group as the source for a rule, this allows instances associated with the source security group to access instances in the security group. This does not add rules from the source security group to this security group. Incoming traffic is allowed based on the private IP addresses of the instances that are associated with the source security group (and not the public IP or Elastic IP addresses).

See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html#SecurityGroupRules

Question

With EC-2 Classic you can reference security groups from other AWS accounts.

Answers

A. True
B. False

A
See table at:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html#VPC_Security_Group_Differences

Question

Your VPC automatically comes with a modifiable default network ACL; by default, it allows all inbound and outbound traffic.

Answers

A. True
B. False

A
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 add or remove rules from the default network ACL, or create additional network ACLs for your VPC. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets it's associated with.
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 also 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.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#ACLs

Question

If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.

Answers

A. True
B. False

A
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.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#ACLs

Question

A network ACL with an asterix for its rule number:

- Is automatically created
- Denies any packet that doesn’t match any of the rules
- Can be modified
- Can’t be removed

Answers

A. True
B. False

B
You can't modify or remove this rule.
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 also 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.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#default-network-acl

Question

If you use a load balancer in the same VPC as your backend instances, and your subnet has a network ACL with an inbound DENY rule for all traffic with a source of 0.0.0.0/0, then your load balancer cannot carry out health checks on instances in your subnet.

Answers

A. True
B. False

A
With Elastic Load Balancing, if the subnet for your back-end instances has a network ACL in which you've added a DENY rule for all traffic with a source of 0.0.0.0/0 or the subnet's CIDR, then your load balancer can't carry out health checks on the instances.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#custom-network-acl

This "learning by quizzes" exercise will be based upon the course videos and the following reference material:

Section: VPC Networking Components

Reference: Amazon Virtual Private Cloud User Guide

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Networking.html

Question

Every subnet that you create is automatically associated with the main route table for the VPC.

Answers

A. True
B. False

A
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.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

Question

AWS provides the following feature/s that you can use to increase security in your VPC:

- NAT instances
- security groups
- network ACLs

Answers

A. True
B. False

B
security groups, network ACLs

This "learning by quizzes" exercise will be based upon the course videos and the following reference material:

Section: VPC Networking Components

Reference: Amazon Virtual Private Cloud User Guide

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Networking.html

Question

_____ are the IP addresses that are within the CIDR range of the VPC.

Answers

A. route tables
B. public IP addresses
C. private IP addresses
D. None of the above

C

We refer to private IP addresses as the IP addresses that are within the IPv4 CIDR range of the VPC.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#vpc-private-ipv4-addresses

Question

Unlike a primary private IP address, you can reassign a secondary private IP address from one network interface to another.

Answers

A. True
B. False

A
You can assign additional private IP addresses, known as secondary private IP addresses, to instances that are running in a VPC. Unlike a primary private IP address, you can reassign a secondary private IP address from one network interface to another. A private IP address remains associated with the network interface when the instance is stopped and restarted, and is released when the instance is terminated.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#vpc-private-ipv4-addresses

Question

You cannot manually associate or disassociate an Elastic IP address.

Answers

A. True
B. False

B
You cannot manually associate or disassociate a public IP address from your instance. Instead, in certain cases, we release the public IP address from your instance, or assign it a new one:

- We release the public IP address for your instance when it's stopped or terminated. Your stopped instance receives a new public IP address when it's restarted.
- We release the public IP address for your instance when you associate an Elastic IP address with your instance, or when you associate an Elastic IP address with the primary network interface (eth0) of your instance in a VPC. When you disassociate the Elastic IP address from your instance, it receives a new public IP address.
- If the public IP address of your instance in a VPC has been released, it will not receive a new one if there is more than one network interface attached to your instance.

See: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-public-addresses

Question

A public IP address is mapped to the primary private IP address through____.

Answers

A. NACL
B. NAT
C. Route table
D. None of the above

B
All subnets have an attribute that determines whether a network interface created in the subnet automatically receives a public IPv4 address (also referred to as a public IP address in this topic). Therefore, when you launch an instance into a subnet that has this attribute enabled, a public IP address is assigned to the primary network interface (eth0) that's created for the instance. A public IP address is mapped to the primary private IP address through network address translation (NAT).

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#vpc-public-ipv4-addresses

Question

You cannot associate an Elastic IP address with your instance after it's launched.

Answers

A. True
B. False

B
Whether or not you assign a public IPv4 address to your instance during launch, you can associate an Elastic IP address with your instance after it's launched.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#vpc-working-with-ip-addresses

Question

The advantage of associating the Elastic IP address with the network interface instead of directly with the instance is that you can move all the attributes of the network interface from one instance to another in a single step.

Answers

A. True
B. False

A
You can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. A network interface's attributes follow it as it is attached or detached from an instance and reattached to another instance. When you move a network interface from one instance to another, network traffic is redirected to the new instance.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ElasticNetworkInterfaces.html

Question

When you move an ENI from one instance to another, network traffic is redirected to the new instance.

Answers

A. True
B. False

A
When you move a network interface from one instance to another, network traffic is redirected to the new instance.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ElasticNetworkInterfaces.html

Question

A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Answers

A. True
B. False

A
To apply route table routes to a particular subnet, you must associate the route table with the subnet. A route table can be associated with multiple subnets; however, a subnet can only be associated with one route table at a time. Any subnet not explicitly associated with a table is implicitly associated with the main route table by default.

See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#WorkWithRouteTables

Question

When you add a new subnet, it automatically uses the routes specified in the main route table.

Answers

A. True
B. False

A
Any subnet not explicitly associated with a table is implicitly associated with the main route table by default.

See:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#WorkWithRouteTables

Question

_____ is a feature that enables you to link an EC2-Classic instance to a VPC.

Answers

A. VPC Peering
B. ClassicLink
C. VPC Classic
D. None of the above

B
ClassicLink allows you to link your EC2-Classic instance to a VPC in your account, within the same region. This allows you to associate the VPC security groups with the EC2-Classic instance, enabling communication between your EC2-Classic instance and instances in your VPC using private IPv4 addresses. ClassicLink removes the need to make use of public IPv4 addresses or Elastic IP addresses to enable communication between instances in these platforms.

See: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/vpc-classiclink.html

Question

To enable access to or from the Internet for instances in a VPC subnet, you must:

Answers

A. attach an Internet gateway to your VPC
B. ensure that your subnet's route table points to the Internet gateway
C. ensure that instances in your subnet have public IP addresses or Elastic IP addresses
D. ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.
E. All of the above

E
See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html#Overview

Question

_____ provides a standard for passing configuration information to hosts on a TCP/IP network.

Answers

A. Network Address Translation
B. Dynamic Host Configuration Protocol
C. Port Address Translation
D. None of the above

B
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).

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html

Question

By default, all instances in a nondefault VPC receive an _____ that AWS assigns (for example, ip-10-0-0-202).

Answers

A. unresolvable host name
B. resolvable host name
C. elastic IP address
D. none of the above

A
The Amazon EC2 instances you launch into a nondefault 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 nondefault 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. To do that, you must specify a special set of DHCP options to use with the VPC.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#DHCPOptionSets

Question

You can assign your own domain name to your instances, and use up to five of your own DNS servers.

Answers

A. True
B. False

B
You can assign your own domain name to your instances, and use up to four of your own DNS servers.
See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#DHCPOptionSets

Question

After you create a set of DHCP options, you can't modify them.

Answers

A. True
B. False

A
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 also set up your VPC to use no DHCP options at all.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#DHCPOptions

Question

You can set up your VPC to use no set of DHCP options.

Answers

A. True
B. False

A

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#DHCPOptions

This "learning by quizzes" exercise will be based upon the course videos and the following reference material:

Section: VPN Connections

Reference: Amazon Virtual Private Cloud User Guide

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

Question

A virtual private gateway is the VPN concentrator on the customer side of the VPN connection.

Answers

A. True
B. False

B
You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a virtual private gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your customer gateway on the remote side of the VPN connection.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

Question

AWS recommends that you use BGP-capable VPN devices.

Answers

A. True
B. False

A
We recommend that you use BGP-capable devices, when available, because the BGP protocol offers robust liveness detection checks that can assist failover to the second VPN tunnel if the first tunnel goes down. Devices that don't support BGP may also perform health checks to assist failover to the second tunnel when needed.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#VPNRoutingTypes

Question

A VPN connection has two tunnels to help ensure connectivity in case your customer gateway becomes unavailable.

Answers

A. True
B. False

B
A VPN connection has two tunnels to help ensure connectivity in case one of the VPN connections becomes unavailable. To protect against a loss of connectivity in case your customer gateway becomes unavailable, you can set up a second VPN connection to your VPC by using a. second customer gateway.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#VPNConnections

This "learning by quizzes" exercise will be based upon the course videos and the following reference material:

Section: VPC Peering

Reference: Amazon Virtual Private Cloud Peering User Guide

https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.html

Question

You cannot create a VPC peering connection between VPCs that have overlapping CIDR blocks.

Answers

A. True
B. False

A

You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks. This limitation also applies to VPCs that have non-overlapping IPv6 CIDR blocks.

See: https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/invalid-peering-configurations.html#overlapping-cidr

Question

To activate a VPC peering connection, the owner of the requester VPC (or local VPC) sends a request to the owner of the peer VPC to create the VPC peering connection.

Answers

A. True
B. False

B
To create a VPC peering connection, first create a request to peer with another VPC. You can request a VPC peering connection with another VPC in your account, or with a VPC in a different AWS account. For an inter-region VPC peering connection where the VPCs are in different regions, the request must be made from the region of the requester VPC.

To activate the request, the owner of the accepter VPC must accept the request. For an inter-region VPC peering connection, the request must be accepted in the region of the accepter VPC.

See: https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/create-vpc-peering-connection.html

Question

If no action is taken on a VPC Peering request, it will expire after 7 days.

Answers

A. True
B. False

A
Do not accept VPC peering connections from unknown AWS accounts. A malicious user may have sent you a VPC peering connection request to gain unauthorized network access to your VPC. This is known as peer phishing. You can safely reject unwanted VPC peering connection requests without any risk of the requester gaining access to any information about your AWS account or your VPC.
You can also ignore the request and let it expire; by default, requests expire after 7 days.

See: https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/create-vpc-peering-connection.html#accept-vpc-peering-connection

Question

You can create a VPC peering connection between VPCs from different accounts.

Answers

A. True
B. False

A
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.

See: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

Question

You can create a VPC peering connection between VPCs in different regions.

Answers

A. True
B. False

A
As of December 2017 you can create a VPC Peering connection in different regions.

See: https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/

For certification practice exams please go to:

backspace.academy