VPC Quiz

Which of the below statements is true for any VPC security group, by default, when it is created?

1. All inbound traffic rule will be explicitly denied

2. All inbound traffic is allowed by default

3. All outbound traffic is allowed by default

4. Traffic to the internet gateway is allowed by default

Which of the below statements is true for any VPC security group, by default, when it is created?

1. All inbound traffic rule will be explicitly denied

2. All inbound traffic is allowed by default

3. All outbound traffic is allowed by default

4. Traffic to the internet gateway is allowed by default

Which of the below statements is true for a default security group in a default VPC, by default, when it is created? (Choose two)

1. It will have an inbound rule that allows all traffic sourced from the security group itself
2. It will have all inbound traffic allowed by default
3. It will have all outbound traffic allowed by default
4. It will by default allow traffic to the internet gateway

Which of the below statements is true for a default security group in a default VPC, by default, when it is created? (Choose two)

1.It will have an inbound rule that allows all traffic sourced from the security group itself

2.It will have all inbound traffic allowed by default

3.It will have all outbound traffic allowed by default

4.It will by default allow traffic to the internet gateway

A user has created a VPC with public and private subnets using the VPC Wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24. Which of the below mentioned entries are required in the main route table to allow the instances in VPC to communicate with each other?

1. Destination : 20.0.0.0/24 and Target : VPC

2. Destination : 20.0.0.0/16 and Target : ALL

3. Destination : 20.0.0.0/0 and Target : ALL

4. Destination : 20.0.0.0/16 and Target : Local

A user has created a VPC with public and private subnets using the VPC Wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24. Which of the below mentioned entries are required in the main route table to allow the instances in VPC to communicate with each other?

1. Destination : 20.0.0.0/24 and Target : VPC
2. Destination : 20.0.0.0/16 and Target : ALL
3. Destination : 20.0.0.0/0 and Target : ALL
4. **Destination : 20.0.0.0/16 and Target : Local**

A user has created a VPC with CIDR 10.0.0.0/24. The user has created a public subnet with CIDR 10.0.0.0/25. The user is trying to create the private subnet with CIDR 10.0.0.128/25. Which of the below mentioned statements is true in this scenario?

- It will not allow the user to create the private subnet due to a CIDR overlap
- It will allow the user to create a private subnet with CIDR as 10.0.0.128/25
- This statement is wrong as AWS does not allow CIDR 10.0.0.0/25
- It will not allow the user to create a private subnet due to a wrong CIDR range

A user has created a VPC with CIDR 10.0.0.0/24. The user has created a public subnet with CIDR 10.0.0.0/25. The user is trying to create the private subnet with CIDR 10.0.0.128/25. Which of the below mentioned statements is true in this scenario?

- It will not allow the user to create the private subnet due to a CIDR overlap
- **It will allow the user to create a private subnet with CIDR as 10.0.0.128/25**
- This statement is wrong as AWS does not allow CIDR 10.0.0.0/25
- It will not allow the user to create a private subnet due to a wrong CIDR range

You have created a VPC with CIDR 10.0.0.0/24. The VPC has two subnets: public (10.0.0.0/25) and private (10.0.0.128/25). How to increase the CIDR range your VPC CIDR block.

A) Change the subnet sizes to /28 subnets, then you will have more room to grow your VPC CIDR

B) You can always change a VPC's original CIDR block as needed

C) You can add additional VPC CIDR blocks, but can’t change the existing one

D) Delete all the subnets first, only then you can modify the size of the VPC

You have created a VPC with CIDR 10.0.0.0/24. The VPC has two subnets: public (10.0.0.0/25) and private (10.0.0.128/25). How to increase the CIDR range your VPC CIDR block.

A) Change the subnet sizes to /28 subnets, then you will have more room to grow your VPC CIDR

B) You can always change a VPC's original CIDR block as needed

C) You can add additional VPC CIDR blocks, but can’t change the existing one

D) Delete all the subnets first, only then you can modify the size of the VPC

A company wants to implement their website in a virtual private cloud (VPC). The web tier will use an Auto Scaling group across multiple Availability Zones (AZs). The database will use Multi-AZ RDS MySQL and should not be publicly accessible.

What is the minimum required number of VPC subnets to achieve this?

1. 1

2. 2

3. 3

4. 4

A company wants to implement their website in a virtual private cloud (VPC). The web tier will use an Auto Scaling group across multiple Availability Zones (AZs). The database will use Multi-AZ RDS MySQL and should not be publicly accessible.

What is the minimum required number of VPC subnets to achieve this?

1. 1

2. 2

3. 3

4. 4

You have created an EC2 instance in a subnet within a VPC. You want to delete the subnet and change it with a bigger CIDR block. What will happen in this scenario?

1. You can delete the subnet and make the EC2 instance as a part of the default subnet
2. You can not delete the subnet until the instances are terminated
3. You can delete the subnet as well as terminate the instances at the same time
4. You can not delete subnets, you have to delete the VPC instead

You have created an EC2 instance in a subnet within a VPC. You want to delete the subnet and change it with a bigger CIDR block. What will happen in this scenario?

1. You can delete the subnet and make the EC2 instance as a part of the default subnet
2. You can not delete the subnet until the instances are terminated
3. You can delete the subnet as well as terminate the instances at the same time
4. You can not delete subnets, you have to delete the VPC instead

One of your company's AWS developers needs to build a test environment. He has created a VPC with CIDR 10.0.0.0/24. Within that VPC, he created a public subnet of CIDR 10.0.0.0/25 and a private subnet of CIDR 10.0.0.128/25. He, then, launched one instance in the private subnet and one instance in the public subnet.

Which of the below can not be an IP address assigned to either Instance ?

1. 10.0.0.1

2. 10.0.0.132

3. 10.0.0.111

4. 10.0.0.65

One of your company's AWS developers needs to build a test environment. He has created a VPC with CIDR 10.0.0.0/24. Within that VPC, he created a public subnet of CIDR 10.0.0.0/25 and a private subnet of CIDR 10.0.0.128/25. He, then, launched one instance in the private subnet and one instance in the public subnet.

Which of the below can not be an IP address assigned to either Instance ?

1. 10.0.0.1

2. 10.0.0.132

3. 10.0.0.111

4. 10.0.0.65

A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance. The internet gateway has also been created. What can be the reason for the error?

1. The internet gateway is not configured with the route table
2. The private IP is not present
3. The outbound traffic on the security group is disabled
4. The internet gateway is not configured with the security group

A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance. The internet gateway has also been created. What can be the reason for the error?

1. The internet gateway is not configured with the route table

2. The private IP is not present

3. The outbound traffic on the security group is disabled

4. The internet gateway is not configured with the security group

A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet. How can the instances in the private subnet connect to the internet?

1. Use the internet gateway with a private IP

2. Allow outbound traffic in the security group for port 80 to allow internet updates

3. The private subnet can never connect to the internet

4. Use NAT with an elastic IP

A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet. How can the instances in the private subnet connect to the internet?

1. Use the internet gateway with a private IP

2. Allow outbound traffic in the security group for port 80 to allow internet updates

3. The private subnet can never connect to the internet

4. Use NAT with an elastic IP

A user has created a VPC with CIDR 10.0.0.0/16. The user has created one subnet with CIDR 10.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 10.0.0.1/24. How can the user create the second subnet?

- There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet's CIDR
- The user can modify the first subnet CIDR from the console
- It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created
- The user can modify the first subnet CIDR with AWS CLI

A user has created a VPC with CIDR 10.0.0.0/16. The user has created one subnet with CIDR 10.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 10.0.0.1/24. How can the user create the second subnet?

- There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet's CIDR
- The user can modify the first subnet CIDR from the console
- **It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created**
- The user can modify the first subnet CIDR with AWS CLI

You have problems connecting via RDP into a Microsoft Windows EC2 instance you launched in your VPC, in a public subnet. You have verified that, the instance has a public IP address, and that the VPC has an Internet Gateway attached, which is properly referenced as a target in the public subnet's route table. While checking the instance's assigned security group and the subnet NACL you noticed that; they both allow all inbound traffic, and deny all outbound traffic.

What needs to be changed such that you can access your instance via RDP?

1.The Instance security group needs to allow outbound traffic.
2.The Subnet N. ACL needs to allow outbound traffic.
3.Nothing, the problem must be in the Internet gateway blocking traffic.
4.Both security group and N ACL need to allow outbound traffic.

You have problems connecting via RDP into a Microsoft Windows EC2 instance you launched in your VPC, in a public subnet. You have verified that, the instance has a public IP address, and that the VPC has an Internet Gateway attached, which is properly referenced as a target in the public subnet's route table. While checking the instance's assigned security group and the subnet NACL you noticed that; they both allow all inbound traffic, and deny all outbound traffic.

What needs to be changed such that you can access your instance via RDP?

1.The Instance security group needs to allow outbound traffic.
2.The Subnet N. ACL needs to allow outbound traffic.
3.Nothing, the problem must be in the Internet gateway blocking traffic.
4.Both security group and N ACL need to allow outbound traffic.

What security group configuration rule is required for your bastion host, in a VPC, in order to allow SSH inbound access to a Linux Bastion host from your IP address 192.168.32.5?

1.Allow Port: SSH (UDP 22), Source 192.168.32.4/30, Inbound

2.Allow Port: SSH (TCP 22), Source 192.168.32.5/31, Outbound

3.Allow Port: SSH (TCP 22), Source 192.168.32.5/0, Outbound

4.Allow Port: SSH (TCP 22), Source 192.168.32.5/32, Inbound

What security group configuration rule is required for your bastion host, in a VPC, in order to allow SSH inbound access to a Linux Bastion host from your IP address 192.168.32.5?

1.Allow Port: SSH (UDP 22), Source 192.168.32.4/30, Inbound

2.Allow Port: SSH (TCP 22), Source 192.168.32.5/31, Outbound

3.Allow Port: SSH (TCP 22), Source 192.168.32.5/0, Outbound

4.Allow Port: SSH (TCP 22), Source 192.168.32.5/32, Inbound

A user has setup a VPC with CIDR 10.0.0.0/16. The VPC has a private subnet (10.0.1.0/24) and a public subnet (10.0.0.0/24). The user's data centre has CIDR of 10.0.54.0/24 and 10.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?

- It will allow traffic communication on both the CIDRs of the data centre
- It will not allow traffic with data centre on CIDR 10.1.0.0/24 but allows traffic communication on 10.0.54.0/24
- It will not allow traffic communication on any of the data centre CIDRs
- It will allow traffic with data centre on CIDR 10.1.0.0/24 but does not allow on 10.0.54.0/24

A user has setup a VPC with CIDR 10.0.0.0/16. The VPC has a private subnet (10.0.1.0/24) and a public subnet (10.0.0.0/24). The user's data centre has CIDR of 10.0.54.0/24 and 10.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?

- It will allow traffic communication on both the CIDRs of the data centre
- It will not allow traffic with data centre on CIDR 10.1.0.0/24 but allows traffic communication on 10.0.54.0/24
- It will not allow traffic communication on any of the data centre CIDRs
- **It will allow traffic with data centre on CIDR 10.1.0.0/24 but does not allow on 10.0.54.0/24**

Which two components provide connectivity with external networks? When attached to an Amazon VPC which two components provide connectivity with external networks? **Choose 2 answers**

1. Elastic IPs (EIP)
2. NAT Gateway (NAT)
3. Internet Gateway (IGW)
4. Virtual Private Gateway (VGW)

Which two components provide connectivity with external networks? When attached to an Amazon VPC which two components provide connectivity with external networks? **Choose 2 answers**

1. Elastic IPs (EIP)

2. NAT Gateway (NAT)

3. Internet Gateway (IGW)

4. Virtual Private Gateway (VGW)