Free Questions for ANS-C01 by go4braindumps

Shared by Bishop on 21-03-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Network Engineer is provisioning a subnet for a load balancer that will sit in front of a fleet of application servers in a private subnet. There is limited IP space left in the VPC CIDR. The application has few users now but is expected to grow quickly to millions of users.

What design will use the LEAST amount of IP space, while allowing for this growth?

Options:

A- Use two /29 subnets for an Application Load Balancer in different Availability Zones.

B- Use one /29 subnet for the Network Load Balancer. Add another VPC CIDR to the VPC to allow for future growth.

C- Use two /28 subnets for a Network Load Balancer in different Availability Zones.

D- Use one /28 subnet for an Application Load Balancer. Add another VPC CIDR to the VPC to allow for future growth.

Answer:

C

Question 2

Question Type: **MultipleChoice**

An AWS CloudFormation template is being used to create a VPC peering connection between two existing operational VPCs, each belonging to a different AWS account. All necessary components in the 'Remote' (receiving) account are already in place.

The template below creates the VPC peering connection in the Originating account. It contains these components:

AWSTemplateFormation Version: 2010-09-09

Parameters:

Originating VCId:

Type: String

RemoteVPCId:

Type: String

RemoteVPCAccountId:

Type: String

Resources:

newVPCPeeringConnection:

Type: 'AWS::EC2::VPCPeeringConnection'

Properties:

VpcdId: !Ref OriginatingVPCId

PeerVpcId: !Ref RemoteVPCId

PeerOwnerId: !Ref RemoteVPCAccountId

Which additional AWS CloudFormation components are necessary in the Originating account to create an operational cross-account VPC peering connection with AWS CloudFormation? (Select two.)

Options:

A- Resources:NewEC2SecurityGroup:Type: AWS::EC2::SecurityGroup

B- Resources:NetworkInterfaceToRemoteVPC:Type: "AWS::EC2NetworkInterface"

C- Resources:newEC2Route:Type: AWS::EC2::Route

D- Resources:VPCGatewayToRemoteVPC:Type: "AWS::EC2::VPCGatewayAttachment"

E- Resources:newVPCPeeringConnection:Type: 'AWS::EC2VPCPeeringConnection'PeerRoleArn: !Ref PeerRoleArn

Answer:

C, E

Explanation:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_EC2.html

Question 3

Question Type: MultipleChoice

A company is deploying a non-web application on an AWS load balancer. All targets are servers located on-premises that can be accessed by using AWS Direct Connect. The company wants to ensure that the source IP addresses of clients connecting to the application are passed all the way to the end server.

How can this requirement be achieved?

Options:

A- Use a Network Load Balancer to automatically preserve the source IP address.

B- Use a Network Load Balancer and enable the X-Forwarded-For attribute.

C- Use a Network Load Balancer and enable the ProxyProtocol v2 attribute.

D- Use an Application Load Balancer to automatically preserve the source IP address in the X-Forwarded-For header.

Answer:

C

Explanation:

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#proxy-protocol

Question 4

Question Type: MultipleChoice

A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven't yet upgraded.

What design will allow the company to serve both newer and earlier clients in the MOST efficient way?

Options:

A- Use an Amazon Route 53 multivalue answer routing policy to route older client traffic to the on-premises application version and the

rest of the traffic to the new AWS based version.

B- Use a Classic Load Balancer for the new application. Route all traffic to the new application by using an Elastic Load Balancing (ELB) load balancer DNS. Define a user-agent-based rule on the backend servers to redirect earlier clients to the on-premises application.

C- Use an Application Load Balancer for the new application. Register both the new and earlier applications as separate target groups and use path-based routing to route traffic based on the application version.

D- Use an Application Load Balancer for the new application. Register both the new and earlier application backends as separate target groups. Use header-based routing to route traffic based on the application version.

Answer:

D

Question 5

Question Type: MultipleChoice

An organization is using a VPC endpoint for Amazon S3. When the security group rules for a set of instances were initially configured, access was restricted to allow traffic only to the IP addresses of the Amazon S3 API endpoints in the region from the published JSON file. The application was working properly, but now is logging a growing number of timeouts when connecting with Amazon S3. No internet gateway is configured for the VPC.

Which solution will fix the connectivity failures with the LEAST amount of effort?

Options:

A- Create a Lambda function to update the security group based on AmazonIPSpaceChanged notifications.

B- Update the VPC routing to direct Amazon S3 prefix-list traffic to the VPC endpoint using the route table APIs.

C- Update the application server's outbound security group to use the prefix-list for Amazon S3 in the same region.

D- Create an additional VPC endpoint for Amazon S3 in the same route table to scale the concurrent connections to Amazon.

Answer:

C

Explanation:

https://aws.amazon.com/blogs/aws/subscribe-to-aws-public-ip-address-changes-via-amazon-sns/

Question 6

Question Type: **MultipleChoice**

All IP addresses within a 10.0.0.0/16 VPC are fully utilized with application servers across two Availability Zones. The application servers need to send frequent UDP probes to a single central authentication server on the Internet to confirm that is running up-to-date

packages. The network is designed for application servers to use a single NAT gateway for internal access. Testing reveals that a few of the servers are unable to communicate with the authentication server.

Options:

A- The NAT gateway does not support UDP traffic.

B- The authentication server is not accepting traffic.

C- The NAT gateway cannot allocate more ports.

D- The NAT gateway is launched in a private subnet.

Answer:

C

Explanation:

Ref: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

'A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. This limit also applies if you create approximately 900 connections per second to a single destination (about 55,000 connections per minute). If the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, you can create an additional 55,000 connections. For more than 55,000 connections, there is an increased chance of connection errors due to port allocation errors. These errors can be monitored by viewing the ErrorPortAllocation CloudWatch metric for your NAT gateway. For more information, see Monitoring NAT Gateways Using Amazon

CloudWatch.'

Question 7

Question Type: MultipleChoice

An organization is replacing a tape backup system with a storage gateway. there is currently no connectivity to AWS. Initial testing is needed.

What connection option should the organization use to get up and running at minimal cost?

Options:

A- Use an internet connection.

B- Set up an AWS VPN connection.

C- Provision an AWS Direct Connection private virtual interface.

D- Provision a Direct Connect public virtual interface.

Answer:

A

Question 8

Question Type: MultipleChoice

All IP addresses within a 10.0.0.0/16 VPC are fully utilized with application servers across two Availability Zones. The application servers need to send frequent UDP probes to a single central authentication server on the Internet to confirm that is running up-to-date packages. The network is designed for application servers to use a single NAT gateway for internal access. Testing reveals that a few of the servers are unable to communicate with the authentication server.

Options:

A- The NAT gateway does not support UDP traffic.

B- The authentication server is not accepting traffic.

C- The NAT gateway cannot allocate more ports.

D- The NAT gateway is launched in a private subnet.

Answer:

C

Explanation:

Ref: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

'A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. This limit also applies if you create approximately 900 connections per second to a single destination (about 55,000 connections per minute). If the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, you can create an additional 55,000 connections. For more than 55,000 connections, there is an increased chance of connection errors due to port allocation errors. These errors can be monitored by viewing the ErrorPortAllocation CloudWatch metric for your NAT gateway. For more information, see Monitoring NAT Gateways Using Amazon CloudWatch.'

Question 9

Question Type: MultipleChoice

An organization is using a VPC endpoint for Amazon S3. When the security group rules for a set of instances were initially configured, access was restricted to allow traffic only to the IP addresses of the Amazon S3 API endpoints in the region from the published JSON file. The application was working properly, but now is logging a growing number of timeouts when connecting with Amazon S3. No internet gateway is configured for the VPC.

Which solution will fix the connectivity failures with the LEAST amount of effort?

Options:

A- Create a Lambda function to update the security group based on AmazonIPSpaceChanged notifications.

B- Update the VPC routing to direct Amazon S3 prefix-list traffic to the VPC endpoint using the route table APIs.

C- Update the application server's outbound security group to use the prefix-list for Amazon S3 in the same region.

D- Create an additional VPC endpoint for Amazon S3 in the same route table to scale the concurrent connections to Amazon.

Answer:

C

Explanation:

https://aws.amazon.com/blogs/aws/subscribe-to-aws-public-ip-address-changes-via-amazon-sns/

Question 10

Question Type: MultipleChoice

A company is deploying a non-web application on an AWS load balancer. All targets are servers located on-premises that can be accessed by using AWS Direct Connect. The company wants to ensure that the source IP addresses of clients connecting to the

application are passed all the way to the end server.

How can this requirement be achieved?

Options:

A- Use a Network Load Balancer to automatically preserve the source IP address.

B- Use a Network Load Balancer and enable the X-Forwarded-For attribute.

C- Use a Network Load Balancer and enable the ProxyProtocol v2 attribute.

D- Use an Application Load Balancer to automatically preserve the source IP address in the X-Forwarded-For header.

Answer:

C

Explanation:

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#proxy-protocol

Question 11

Question Type: MultipleChoice

A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven't yet upgraded.

What design will allow the company to serve both newer and earlier clients in the MOST efficient way?

Options:

A- Use an Amazon Route 53 multivalue answer routing policy to route older client traffic to the on-premises application version and the rest of the traffic to the new AWS based version.

B- Use a Classic Load Balancer for the new application. Route all traffic to the new application by using an Elastic Load Balancing (ELB) load balancer DNS. Define a user-agent-based rule on the backend servers to redirect earlier clients to the on-premises application.

C- Use an Application Load Balancer for the new application. Register both the new and earlier applications as separate target groups and use path-based routing to route traffic based on the application version.

D- Use an Application Load Balancer for the new application. Register both the new and earlier application backends as separate target groups. Use header-based routing to route traffic based on the application version.

Answer:

D

Question 12

Question Type: MultipleChoice

An AWS CloudFormation template is being used to create a VPC peering connection between two existing operational VPCs, each belonging to a different AWS account. All necessary components in the 'Remote' (receiving) account are already in place.

The template below creates the VPC peering connection in the Originating account. It contains these components:

AWSTemplateFormation Version: 2010-09-09

Parameters:

Originating VCId:

Type: String

RemoteVPCId:

Type: String

RemoteVPCAccountId:

Type: String

Resources:

newVPCPeeringConnection:

Type: 'AWS::EC2::VPCPeeringConnection'

Properties:

VpcdId: !Ref OriginatingVPCId

PeerVpcId: !Ref RemoteVPCId

PeerOwnerId: !Ref RemoteVPCAccountId

Which additional AWS CloudFormation components are necessary in the Originating account to create an operational cross-account VPC peering connection with AWS CloudFormation? (Select two.)

Options:

A- Resources:NewEC2SecurityGroup:Type: AWS::EC2::SecurityGroup

B- Resources:NetworkInterfaceToRemoteVPC:Type: "AWS::EC2NetworkInterface"

C- Resources:newEC2Route:Type: AWS::EC2::Route

D- Resources:VPCGatewayToRemoteVPC:Type: "AWS::EC2::VPCGatewayAttachment"

E- Resources:newVPCPeeringConnection:Type: 'AWS::EC2VPCPeeringConnection'PeerRoleArn: !Ref PeerRoleArn

Answer:

C, E

Explanation:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_EC2.html