

DUMPSBOSS.

AWS Certified Advanced Networking - Specialty (ANS-C00)

Amazon AWS AWS-Certified-Advanced-Networking-Specialty-
ANS-C00

Version Demo

Total Demo Questions: 20

Total Premium Questions: 470

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems.

Which two AWS Services cloud you leverage to build an automated notification system? (Choose two.)

- A. Internet gateway
- B. VPC Flow Logs
- C. AWS CloudTrail
- D. Lambda
- E. AWS Inspector

ANSWER: C D

Explanation:

References: <https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-by-using-aws-cloudtrail-amazon-sns-and-aws-lambda/>

QUESTION NO: 2

A team implements a highly available solution using Amazon AppStream 2.0. The AppStream 2.0 fleet needs to communicate with resources both in an existing VPC and on-premises. The VPC is connected to the on-premises environment using an AWS Direct Connect private virtual interface.

What implementation enables on-premises users to connect to AppStream and existing VPC resources?

- A. Deploy two subnets into the existing VPC. Add a public virtual interface to the Direct Connect connection for users to access the AppStream endpoint
- B. Deploy two subnets into the existing VPC. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.
- C. Deploy a new VPC with two subnets. Create a VPC peering connection between the two VPCs for users to access the AppStream endpoint.
- D. Deploy one subnet into the existing VPC. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.

ANSWER: B

QUESTION NO: 3

Over which of the following Ethernet standards does AWS Direct Connect link your internal network to an AWS Direct Connect location?

- A. Copper backplane cable
- B. Twisted pair cable
- C. Single mode fiber-optic cable
- D. Shielded balanced copper cable

ANSWER: C

Explanation:

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet single mode fiber-optic cable.

Reference: <http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

QUESTION NO: 4

The Security department has mandated that all outbound traffic from a VPC toward an on-premises datacenter must go through a security appliance that runs on an Amazon EC2 instance.

Which of the following maximizes network performance on AWS? (Choose two.)

- A. Support for the enhanced networking drivers
- B. Support for sending traffic over the Direct Connect connection
- C. The instance sizes and families supported by the security appliance
- D. Support for placement groups within the VPC
- E. Security appliance support for multiple elastic network interfaces

ANSWER: A C

QUESTION NO: 5

A company hosts several applications in the AWS Cloud across multiple VPCs that are connected to a transit gateway. Redundant AWS Direct Connect connections and a Direct Connect gateway provide private network connectivity to the company's on-premises environment.

During a maintenance window, the networking team adds eight VPCs. The application management team notices that there is no reachability between the newly created VPCs and the on-premises environment. Connectivity between all VPCs through the transit gateway is working as expected.

Which of the following are possible causes of the connectivity issues? (Choose two.)

- A. The prefixes that are advertised from the Direct Connect gateway to the on-premises router are shorter than the CIDR blocks of the newly created VPCs
- B. The route tables for the newly created VPCs do not have the routes to the on-premises environment that point to the transit gateway attachment
- C. The on-premises route tables do not contain the exact CIDR blocks of the newly created VPCs
- D. The route tables for the newly created VPCs have only summary routes for the on-premises environment that point to the transit gateway attachment
- E. The prefixes that are advertised from the Direct Connect gateway to the on-premises router do not contain the CIDR blocks of the newly created VPCs

ANSWER: A D

Explanation:

Reference: <https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html>
<https://docs.aws.amazon.com/directconnect/latest/UserGuide/prefix-example.html>

QUESTION NO: 6

A company is deploying a new web application that uses a three-tier model with a public-facing Network Load Balancer and web servers in an Amazon VPC. The application servers are hosted in the company's data center. There is an AWS Direct Connect connection between the VPC and the company's data center. Load testing results indicate that up to 100 servers, equally distributed across multiple Availability Zones, are required to handle peak loads.

The network engineer needs to design a VPC that has a /24 CIDR assigned to it.

How should the engineer allocate subnets across three Availability Zones for each tier?

- A. Network Load Balancer: /29 per subnet Web: /26 per subnet
- B. Network Load Balancer: /28 per subnet Web: /25 per subnet
- C. Network Load Balancer: /28 per subnet Web: /27 per subnet
- D. Network Load Balancer: /28 per subnet Web: /26 per subnet

ANSWER: D

QUESTION NO: 7

Your security team implements a host-based firewall on all of your Amazon Elastic Compute Cloud (EC2) instances to block all outgoing traffic. Exceptions must be requested for each specific requirement. Until you request a new rule, you cannot access the instance metadata service. Which firewall rule should you request to be added to your instances to allow instance metadata access?

- A. Inbound; Protocol tcp; Source [Instance's EIP]; Destination 169.254.169.254
- B. Inbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
- C. Outbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
- D. Outbound; Protocol tcp; Destination 169.254.169.254; Destination port 443

ANSWER: C

QUESTION NO: 8

You have two enhanced networking capable instances in a placement group. One with an Intel network interface and one with an ENA.

What network speed will be achieved between the two?

- A. 10Gbps
- B. 20Gbps
- C. 5Gbps
- D. You cannot have different network interfaces in a placement group.

ANSWER: A

Explanation:

10Gbps. The Intel interface has a max speed of 10 and the ENA is 20. The speed will be the lesser of the two.

QUESTION NO: 9

Which two choices can serve as a directory service for WorkSpaces? (Choose two.)

- A. Simple AD
- B. Enhanced AD
- C. Direct Connection
- D. AWS Microsoft AD

ANSWER: A D

Explanation:

There is no such thing as "Enhanced AD" and DX is not a directory service.

QUESTION NO: 10

Your organization requires strict adherence to a change control process for its Amazon Elastic Compute Cloud (EC2) and VPC environments. The organization uses AWS CloudFormation as the AWS service to control and implement changes. Which combination of three services provides an alert for changes made outside of AWS CloudFormation? (Choose three.)

- A. AWS Config
- B. AWS Simple Notification Service
- C. AWS CloudWatch metrics
- D. AWS Lambda
- E. AWS CloudFormation
- F. AWS Identity and Access Management

ANSWER: B C D

QUESTION NO: 11

In AWS, which tool records API calls for a specific AWS account and also delivers the log files for that account?

- A. CloudTrail
- B. Redshift
- C. Beanstalk
- D. Cognito

ANSWER: A

Explanation:

The AWS CloudTrail is a web service that is used to record AWS API call for a specific AWS account. It also delivers log files, which provide the following details:

- Identity of the API caller
- Time of the API call
- Source IP address of API caller
- Request parameters
- Response elements

Reference: <https://aws.amazon.com/cloudtrail/>

QUESTION NO: 12

You have just peered two VPCs, and you need to improve performance for instances you plan on deploying. What are two steps you would take to do this? (Choose two.)

- A. Create two subnets in the same AZ and create a placement group.
- B. Set the MTU of your instances to 1500.
- C. Create two subnets in different AZs and create a placement group.
- D. Ensure you choose instances that use enhanced networking.

ANSWER: A D

Explanation:

A placement group can only be deployed in the same AZ and is only useful with enhanced networking instances.

QUESTION NO: 13

Due to security requirements, all traffic must be encrypted between your VPC and your on-premises data center. You also want to maintain reliability.

What two options will allow you to achieve this? (Choose two.)

- A. A Direct Connect connection with a Private VIF
- B. A VPN connection
- C. A Direct Connect connection with a Hosted VIF
- D. A Direct Connect connection with a Public VIF

ANSWER: B D

Explanation:

To run VPN over DX, you need to have a public VIF to access the VPN endpoints.

QUESTION NO: 14

You have two VPCs that you need to connect to an on-premises datacenter using VPNs. When you create the tunnels, you find that both tunnels use the same addresses. What two things can you do to overcome this? (Choose two.)

- A. Delete the VPN, create a "dummy VPN", recreate the VPN, then delete the "dummy" VPN.
- B. Delete your AWS account and create a new one since the VPN tunnel addresses are created from a hash of your account number and a proprietary algorithm.
- C. Create a VHF within you router for each network.

D. Create a VRF within your router for each network.

ANSWER: A D

QUESTION NO: 15

You are building an application in AWS that requires Amazon Elastic MapReduce (Amazon EMR). The application needs to resolve hostnames in your internal, on-premises Active Directory domain. You update your DHCP Options Set in the VPC to point to a pair of Active Directory integrated DNS servers running in your VPC.

Which action is required to support a successful Amazon EMR cluster launch?

- A. Add a conditional forwarder to the Amazon-provided DNS server.
- B. Enable seamless domain join for the Amazon EMR cluster.
- C. Launch an AD connector for the internal domain.
- D. Configure an Amazon Route 53 private zone for the EMR cluster.

ANSWER: B

Explanation:

References: <https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

QUESTION NO: 16

A company has a VPC in the us-west-1 Region and another VPC in the ap-southeast-2 Region. Network engineers set up an AWS Direct Connect connection from their data center to the us-east-1 Region. They create a private virtual interface (VIF) that references a Direct Connect gateway, which is then connected to virtual private gateways in both VPCs. When the setup is complete, the engineers cannot access resources in us-west-1 from ap-southeast-2.

What should the network engineers do to resolve this issue?

- A. Add the subnet range for the VPCs in us-west-1 and ap-southeast-2 to the route tables for both VPCs. Add the Direct Connect gateway as a target.
- B. Configure the Direct Connect gateway to route traffic between the VPCs in ap-southeast-2 and us-west-2.
- C. Establish a VPC peering connection between the VPCs in ap-southeast-2 and us-west-2. Add the subnet ranges to the routing tables.
- D. Create static routes in each VPC that point to the destination VPC with the virtual private gateway as the route target.

ANSWER: B

QUESTION NO: 17

You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a

self-referencing rule using the cluster security group's group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions. How should you enable secure cluster communication while deploying additional cluster members in another AWS region?

- A.** Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other's security group-id in each region.
- B.** Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
- C.** Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
- D.** Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other's security group-id in each region.

ANSWER: D

QUESTION NO: 18

A company deployed its production Amazon VPC using CIDR block 33.16.0.0/16. The company has nearly depleted its addresses and now needs to extend the VPC network.

Which CIDR blocks meet the company's requirement to extend the VPC network with a secondary CIDR? (Choose two.)

- A.** 33.17.0.0/16
- B.** 172.16.0.0/18
- C.** 100.70.0.0/17
- D.** 192.168.1.0/24
- E.** 10.0.0.0/8

ANSWER: A C

QUESTION NO: 19

A company installed an AWS Site-to-Site VPN and configured it to use two tunnels. The company has learned that the VPN connectivity is unstable. During a ping test from the on-premises data center to AWS, a network engineer notices that the first few ICMP replies time out but that subsequent requests are successful. The AWS Management Console shows that the status for both tunnels last changed at the same time the ping responses were successfully received.

Which steps should the network engineer take to resolve the instability? (Choose two.)

- A. Enable dead peer detection (DPD) on the customer gateway device.
- B. Change the tunnel configuration to active/standby on the virtual private gateway.
- C. Use AS PATH prepending on one path to cause all traffic to prefer that tunnel.
- D. Send ICMP requests to an instance in the VPC every 5 seconds from the on-premises network.
- E. Use a higher multi-exit discriminator (MED) value on the preferred path to prefer that tunnel.

ANSWER: C E

QUESTION NO: 20

Your network utilizes jumbo frames on its servers and your router. You are trying to access your AWS resources, and you are having issues with packet loss. What is the best solution?

- A. Remove the "Do not Fragment" flag on the packets.
- B. Lower the MTU for your network.
- C. Call AWS support.
- D. You will have to upgrade to Direct Connect.

ANSWER: A

Explanation:

Remove the "Don't Fragment" Flag on your router. AWS will drop any data with an MTU of greater than 1500 if the "Do not Fragment" flag is set, so you need your router to indicate that data can be fragmented.