Latest Version: 20.0

Question: 1

Your organization's corporate website must be available on www.acme.com and acme.com.
How should you configure Amazon Route 53 to meet this requirement?

A. Configure acme.com with an ALIAS record targeting the ELB. www.acme.com with an ALIAS record targeting the ELB.
B. Configure acme.com with an A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
C. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
D. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.

Answer: A

Explanation:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

Question: 2

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: A

Explanation:
https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networksand-aws-using-aws-directory-service-and-microsoft-active-directory/

Question: 3

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? (Select two.)

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

Answer: BD

Explanation:
Reference: https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-calledby-using-aws-cloudtrail-amazon-sns-and-aws-lambda/

Question: 4

You are designing the network infrastructure for an application server in Amazon VPC. Users will access all the application instances from the Internet and from an on-premises network. The on-premises network is connected to your VPC over an AWS Direct Connect link.
How should you design routing to meet these requirements?

A. Configure a single routing table with two default routes: one to the Internet via an IGW, the other to the on-premises network via the VGW. Use this routing table across all subnets in your VPC.
B. Configure two routing tables: one that has a default route via the IGW, and another that has a default route via the VGW. Associate both routing tables with each VPC subnet.
C. Configure a single routing table with a default route via the IGW. Propagate a default route via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnet.
D. Configure a single routing table with a default route via the IGW. Propagate specific routes for the onpremises networks via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets.

Answer: D

Explanation:
0/0 to IGW and advertise specific routes or (10/8) from onprem to VGW and propogate to VPC

Question: 5

Your company decides to use Amazon S3 to augment its on-premises data store. Instead of using the company's highly controlled, on-premises Internet gateway, a Direct Connect connection is ordered to provide high bandwidth, low latency access to S3. Since the company does not own a publically routable

IPv4 address block, a request was made to AWS for an AWS-owned address for a Public Virtual Interface (VIF).
The security team is calling this new connection a “backdoor”, and you have been asked to clarify the risk to the company.
Which concern from the security team is valid and should be addressed?

A. AWS advertises its aggregate routes to the Internet allowing anyone on the Internet to reach the router.
B. Direct Connect customers with a Public VIF in the same region could directly reach the router.
C. EC2 instances in the same region with access to the Internet could directly reach the router.
D. The S3 service could reach the router through a pre-configured VPC Endpoint.

Answer: C

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/control-routes-direct-connect/