AWS Certified Advanced Networking - Specialty

1. 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.

A. Reveal

Answer(s): C

---

2. An organization with a growing e-commerce presence uses the AWS CloudHSM to offload the SSL/TLS processing of its web server fleet. The company leverages Amazon EC2 Auto Scaling for web servers to handle the growth. What architectural approach is optimal to scale the encryption operation?

A. A. Use multiple CloudHSM instances, and load balance them using a Network Load Balancer.

B. B. Use multiple CloudHSM instances to the cluster;requests to it will automatically load balance.

C. C. Enable Auto Scaling on the CloudHSM instance, with similar configuration to the web tier Auto Scaling group.

D. D. Use multiple CloudHSM instances, and load balance them using an Application Load Balancer.

Answer(s): B

---

3. 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?

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

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

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

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

Answer(s): D

---

4. 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?

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

B. 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. 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. 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(s): D

---

5. 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?

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

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

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

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

Answer(s): C

---

6. 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.

A. A. The NAT gateway does not support UDP traffic.

B. B. The authentication server is not accepting traffic.

C. C. The NAT gateway cannot allocate more ports.

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

Answer(s): C

---

7. 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?

A. A. Use an internet connection.

B. B. Set up an AWS VPN connection.

C. C. Provision an AWS Direct Connection private virtual interface

D. D. Provision a Direct Connect public virtual interface.

Answer(s): A

---

8. DNS name resolution must be provided for services in the following four zones:

A. <code>company.private.</code>

B. <code>emea.company.private.</code>

C. <code>apac.company.private.</code>

D. <code>amer.company.private.</code>

Answer(s): D

---

9. A Systems Administrator is designing a hybrid DNS solution with spilt-view. The apex-domain “example.com” should be served through name servers across multiple top-level domains (TLDs). The name server for subdomain “dev.example.com” should reside on-premises. The administrator has decided to use Amazon Route 53 to achieve this scenario. What procedurals steps must be taken to implement the solution?

A. A. Use a Route 53 public hosted zone for example.com and a private hosted zone for dev.example.com

B. B. Use a Route 53 public and private hosted zone for example.com and perform subdomain delegation for dev.example.com

C. C. Use a Route 53 public hosted zone for example.com and perform subdomain delegation for dev.example.com

D. D. Use a Route 53 private hosted zone for example.com and perform subdomain delegation for dev.example.com

Answer(s): C

---

10. An organization has three AWS accounts with each containing VPCs in Virginia, Canada and the Sydney regions. The organization wants to determine whether all available Elastic IP addresses (EIPs) in these accounts are attached to Amazon EC2 instances or in use elastic network interfaces (ENIs) in all of the specified regions for compliance and cost-optimization purposes. Which of the following meets the requirements with the LEAST management overhead?

A. A. use an Amazon CloudWatch Events rule to schedule an AWS Lambda function in each account in all three regions to find the unattached and unused EIPs.

B. B. Use a CloudWatch event bus to schedule Lambda functions in each account in all three regions to find the unattached and unused EIPs.

C. C. Add an AWS managed, EIP-attached AWS Config rule in each region in all three accounts to find unattached and unused EIPs.

D. D. Use AWS CloudFormation StackSets to deploy an AWS Config EIP-attached rule in all accounts and regions to find the unattached and unused EIPs.

Answer(s): C

---

11. An organization wants to process sensitive information using the Amazon EMR service. The information is stored in on-premises databases. The output of processing will be encrypted using AWS KMS before it is uploaded to a customer-owned Amazon S3 bucket. The current configuration includes a VPS with public and private subnets, with VPN connectivity to the on premises network. The security organization does not allow Amazon EC2 instances to run in the public subnet. What is the MOST simple and secure architecture that will achieve the organization’s goal?

A. A. Use the existing VPC and configure Amazon EMR in a private subnet with an Amazon S3 endpoint

B. B. use the existing VPS and a NAT gateway, and configure Amazon EMR in a private subnet with an Amazon S3 endpoint.

C. C. Create a new VPS without an IGW and configure the VPN and Amazon EMR in a private subnet with an Amazon S3 endpoint.

D. D. Create a new VPS without an IGW and configure the VPN and Amazon EMR in a private subnet with an Amazon S3 endpoint and a NAT gateway.

Answer(s): B

---

12. Your company has a 1-Gbps AWS Direct Connect connection to AWS. Your company needs to send traffic from on-premises to a VPC owned by a partner company. The connectivity must have minimal latency at the lowest price. Which of the following connectivity options should you choose?

A. A. Create a new Direct Connect connection, and set up a new circuit to connect to the partner VPC using a private virtual interface.

B. B. Create a new Direct Connect connection, and leverage the existing circuit to connect to the partner VPC.

C. C. Create a new private virtual interface, and leverage the existing connection to connect to the partner VPC.

D. D. Enable VPC peering and use your VPC as a transitive point to reach the partner VPC.

Answer(s): C

---

13. You deploy your Internet-facing application is the us-west-2(Oregon) region. To manage this application and upload content from your corporate network, you have a 1–Gbps AWS Direct Connect connection with a private virtual interface via one of the associated Direct Connect locations. In normal operation, you use approximately 300 Mbps of the available bandwidth, which is more than your Internet connection from the corporate network. You need to deploy another identical instance of the application is us-east-1(N Virginia) as soon as possible. You need to use the benefits of Direct Connect. Your design must be the most effective solution regarding cost, performance, and time to deploy. Which design should you choose?

A. A. Use the inter-region capabilities of Direct Connect to establish a private virtual interface from us-west-2 Direct Connect location to the new VPC in us-east-1.

B. B. Deploy an IPsec VPN over your corporate Internet connection to us-east-1 to provide access to the new VPC.

C. C. Use the inter-region capabilities of Direct Connect to deploy an IPsec VPN over a public virtual interface to the new VPC in us-east-1.

D. D. Use VPC peering to connect the existing VPC in us-west-2 to the new VPC in us-east-1, and then route traffic over Direct Connect and transit the peering connection.

Answer(s): C

---

14. The Payment Card Industry Data Security Standard (PCI DSS) merchants that handle credit card data must use strong cryptography. These merchants must also use security protocols to protect sensitive data during transmission over public networks. You are migrating your PCI DSS application from on-premises SSL appliance and Apache to a VPC behind Amazon CloudFront. How should you configure CloudFront to meet this requirement?

A. A. Configure the CloudFront Cache Behavior to require HTTPS and the CloudFront Origin's Protocol Policy to 'Match Viewer'.

B. B. Configure the CloudFront Cache Behavior to allow TCP connections and to forward all requests to the origin without TLS termination at the edge.

C. C. Configure the CloudFront Cache Behavior to require HTTPS and to forward requests to the origin via AWS Direct Connect.

D. D. Configure the CloudFront Cache Behavior to redirect HTTP requests to HTTPS and to forward request to the origin via the Amazon private network.

Answer(s): A

---

15. You are building an application that provides real-time audio and video services to customers on the Internet. The application requires high throughput. To ensure proper audio and video transmission, minimal latency is required. Which of the following will improve transmission quality?

A. A. Enable enhanced networking

B. B. Select G2 instance types

C. C. Enable jumbo frames

D. D. Use multiple elastic network interfaces

Answer(s): A

---

16. You have a global corporate network with 153 individual IP prefixes in your internal routing table. You establish a private virtual interface over AWS Direct Connect to a VPC that has an Internet gateway (IGW). All instances in the VPC must be able to route to the Internet via an IGW and route to the global corporate network via the VGW. How should you configure your on-premises BGP peer to meet these requirements?

A. A. Configure AS-Prepending on your BGP session

B. B. Summarize your prefix announcement to less than 100

C. C. Announce a default route to the VPC over the BGP session

D. D. Enable route propagation on the VPC route table

Answer(s): B

---

17. 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? (Select three.)

A. A. AWS Config

B. B. AWS Simple Notification Service

C. C. AWS CloudWatch metrics

D. D. AWS Lambda

E. E. AWS CloudFormation

F. F. AWS Identify and Access Management

Answer(s): A B D

---

18. Your company operates a single AWS account. A common services VPC is deployed to provide shared services, such as network scanning and compliance tools. Each AWS workload uses its own VPC, and each VPC must peer with the common services VPC. You must choose the most efficient and cost effective approach. Which approach should be used to automate the required VPC peering?

A. A. AWS CloudTrail integration with Amazon CloudWatch Logs to trigger a Lambda function.

B. B. An OpsWorks Chef recipe to execute a command-line peering request.

C. C. Cfn-init with AWS CloudFormation to execute a command-line peering request.

D. D. An AWS CloudFormation template that includes a peering request.

Answer(s): D

---

19. You have multiple Amazon Elastic Compute Cloud (EC2) instances running a web server in a VPC configured with security groups and NACL. You need to ensure layer 7 protocol level logging of all network traffic (ACCEPT/REJECT) on the instances. What should be enabled to complete this task?

A. A. CloudWatch Logs at the VPC level

B. B. Packet sniffing at the instance level

C. C. VPC flow logs at the subnet level

D. D. Packet sniffing at the VPC level

Answer(s): C

---

20. You are preparing to launch Amazon WorkSpaces and need to configure the appropriate networking resources. What must be configured to meet this requirement?

A. A. At least two subnets in different Availability Zones.

B. B. A dedicated VPC with Active Directory Services.

C. C. An IPsec VPN to on-premises Active Directory

D. D. Network address translation for outbound traffic.

Answer(s): A D
