Amazon

Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

NEW QUESTION 1
A company has two AWS accounts: one for Production and one for Connectivity. A network engineer needs to connect the Production account VPC to a transit gateway in the Connectivity account. The feature to auto accept shared attachments is not enabled on the transit gateway.
Which sot of stops should the network engineer follow in each AWS account to meet those requirements?

A. * 1. In the Production account Create a resource share In AWS Resource Access Manager for the transit gateway Provide the Connectivity account ID Enable thefeature to allow external accounts* 2. In the Connectivity account Accept the resource* 3. In the Connectivity account Create an attachment to the VPC subnets* 4. In the Production account: Accept the attachmen
B. Associate a route table with the attachment.
C. * 1. In the Production account Create a resource share In AWS Resource Access Manager for the VPC subnets Provide the Connectivity account ID Enable the feature to allow external accounts.* 2. In the Connectivity account Accept the resource* 3. In the Production account Create an attachment on the transit gateway to the VPC subnets* 4. In the Connectivity account Accept the attachment Associate a route table will the attachment.
D. * 1. In the Connectivity account Create a resource share in AWS Resource Access Manager for the VPC subnet
E. Provide the Production account ID Enable the feature lo allow external accounts.* 2. In the Production account Accept the resource* 3. In the Connectivity account Create an attachment on the transit gateway to the VPC subnets A In the Production account Accept the attachment Associate a route table with the attachment.
F. * 1. In the Connectivity account Create a resource share in AWS Resource Access Manager for the transit gateway Provide the Production account ID Enable the feature to allow external accounts* 2. In the Production account Accept the resource.* 3 In the Production account Create an attachment to the VPC subnets* 4. In the Connectivity account Accept the attachmen
G. Associate a route tab e win toe attachment

Answer: A

NEW QUESTION 2
Your organization leverages an IP Address Management (IPAM) product to manage IP address distribution. The IPAM exposes an API. Development teams use CloudFormation to provision approved reference architectures. At deployment time, IP addresses must be allocated to the VPC. When the VPC is deleted, the IPAM must reclaim the VPC's IP allocation.
Which method allows for efficient, automated integration of the IPAM with CloudFormation?

A. AWS CloudFormation parameters using the "Ref::" intrinsic function
B. AWS CloudFormation custom resource using an AWS Lambda invocation.
C. CloudFormation::OpsWorks::Stack with custom Chef configuration.
D. AWS CloudFormation parameters using the "Fn::FindInMap" intrinsic function.

Answer: B

Explanation:
Cloudformation chapter under exam essentials it says "custom resources in an AWS cloudformation template allows you to configure non-aws resources not supported by AWS. You can use custom resources to make calls to an IPAM"

NEW QUESTION 3
A company has a hybrid environment across its on-premises network and the AWS Cloud The company wants to use Amazon Elastic File System (Amazon EFS) to store and share data between on-premises services that are required to resolve DNS queries through on-premises DNS servers The company wants to use a custom domain name to connect to Amazon EFS The company also wants to avoid using the Amazon EFS target IP address.
What should a network engineer do to meet these requirements?

A. Create an Amazon Route 53 Resolver outbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 public hosted zone, and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 public hosted zone
B. Create an Amazon Route 53 Resolver inbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone, and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 Resolver
C. Create an Amazon Route 53 Resolver outbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone,and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 Resolver
D. Create an Amazon Route 53 Resolver inbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone, and add a new PTR record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 private hosted zone

Answer: A

NEW QUESTION 4
You are deploying an EC2 instance in a private subnet that requires access to the Internet. One of the requirements for this solution is to restrict access to only particular URLs on a whitelist. In addition to the whitelisted URL, the instances should be able to access any Amazon S3 bucket in the same region via any URL.
Which of the following solutions should you deploy? (Select two.)

A. Include s3.amazonaws.com in the whitelist.
B. Create a VPC endpoint for S3.
C. Run Squid proxy on a NAT instance.
D. Deploy a NAT gateway into your VPC.
E. Utilize a security group to restrict access.

Answer: BC

Explanation:
https://aws.amazon.com/blogs/security/how-to-set-up-an-outbound-vpc-proxy-with-domain-whitelisting-and-co

NEW QUESTION 5
A logistics company has deployed a hybrid environment that has multiple VPCs in both the us-east-1 Region and the af-south-1 Region The on-premises data center is connected to us-east-1 through an AWS Direct Connect connection The Direct Connect connection is connected to a Direct Connect gateway that is associated with a transit gateway The transit gateway is attached to all the VPCs in us-east-1
An application that is deployed in af-south-1 requires access to a database in the data center The application also requires access to file storage in a VPC in us-east-1
Which solution will meet these requirements with the LOWEST latency?

A. Create a transit gateway in af-south-1, and attach the VPCs Create a transit gateway peering connection between the transit gateways
B. Create a Direct Connect connection in af-south-1, and attach the VPCs with a Direct Connect gateway and a transit gateway Create an AWS Site-to-Site VPN connection over the internet between the Direct Connect connections.
C. Create a transit gateway in af-south-1 and attach the VPCs Associate the transit gateway in af-south-1 with the Direct Connect gateway tn us-east-1
D. Create inter-Region VPC peering connections between the VPCs in each Region Use the transit gateway attachments in us-east-1 to access the database in the data center

Answer: A

NEW QUESTION 6
A company's Network Engineering team is solely responsible for deploying VPC infrastructure using AWS CloudFormation. The company wants to give its Developers the ability to launch applications using CloudFormation templates so that subnets can be created using available CIDR ranges.
What should be done to meet these requirements?

A. Create a CloudFormation templates with Amazon EC2 resources that rely on cfn-init and cfn-signals to inform the stack of available CIDR ranges.
B. Create a CloudFormation template with a custom resource that analyzes traffic activity in VPC Flow Logs and reports on available CIDR ranges.
C. Create a CloudFormation template that references the Fn::Cidr intrinsic function within a subnet resource to select an available CIDR range.
D. Create a CloudFormation template with a custom resource that uses AWS Lambda and Amazon DynamoDB to manage available CIDR ranges.

Answer: D

NEW QUESTION 7
Your company runs an application for the US market in the us-east-1 AWS region. This application uses proprietary TCP and UDP protocols on Amazon Elastic Compute Cloud (EC2) instances. End users run a
real-time, front-end application on their local PCs. This front-end application knows the DNS hostname of the service.
You must prepare the system for global expansion. The end users must access the application with lowest latency.
How should you use AWS services to meet these requirements?

A. Register the IP addresses of the service hosts as "A" records with latency-based routing policy in Amazon Route 53, and set a Route 53 health check for these hosts.
B. Set the Elastic Load Balancing (ELB) load balancer in front of the hosts of the service, and register the ELB name of the main service host as an ALIAS record with a latency-based routing policy in Route 53.
C. Set Amazon CloudFront in front of the host of the service, and register the CloudFront name of the main service as an ALIAS record in Route 53.
D. Set the Amazon API gateway in front of the service, and register the API gateway name of the main service as an ALIAS record in Route 53.

Answer: B

NEW QUESTION 8
An organization has created a web application inside a VPC and wants to make it available to 200 client VPCs. The client VPCs are in the same region but are owned by other business units within the organization.
What is the best way to meet this requirement, without making the application publicly available?

A. Configure the application as an AWS PrivateLink-powered service, and have the client VPCs connect to the endpoint service by using an interface VPC endpoint.
B. Enable VPC peering between the web application VPC and all client VPCs.
C. Deploy the web application behind an internet-facing Application Load Balancer and control which clients have access by using security groups.
D. Deploy the web application behind an internal Application Load Balancer and control which clients have access by using security groups.

Answer: A

NEW QUESTION 9
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. 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-proto

NEW QUESTION 10
A network engineer has configured a private hosted zone using Amazon Route 53. The engineer needs to configure health checks for record sets within the zone that are associated with instances.
How can the engineer meet the requirements?

A. Configure a Route 53 health check to a private IP associated with the instances inside the VPC to be checked.
B. Configure a Route 53 health check pointing to an Amazon SNS topic that notifies an Amazon CloudWatch alarm when the Amazon EC2 StatusCheckFailed metric fails.
C. Create a CloudWatch metric that checks the status of the EC2 StatusCheckFailed metric, add an alarm to the metric, and then create a health check that is based on the state of the alarm.
D. Create a CloudWatch alarm for the StatusCheckFailed metric and choose Recover this instance, selecting a threshold value of 1.

Answer: C

NEW QUESTION 10
A company wants to migrate its workloads to the AWS Cloud. The company has two web applications and wants to run them in separate, isolated VPCs. The company needs to use Elastic Load Balancing to distribute requests between application instances.
For security reasons, internet gateways must not be attached to the application VPCs. Inbound HTTP requests to the application must be routed through a centralized VPC. and the application VPCs must not be exposed to any other inbound traffic The application VPCs cannot be allowed to initiate any outbound connections
What should a network engineer do to meet these requirements?

A. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
B. Create a public Network Load Balancer (NLB) in the centralized VP
C. Create target groups for the private DNS names of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.
D. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
E. Create a public Network Load Balancer (NLB) in the centralized VP
F. Create target groups for the private IP addresses of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.
G. Run the applications behind private Network Load Balancers (NLBs) in separate VPC
H. Create VPC peering connections between the application VPCs and the centralized VP
I. Create a public Application Load Balancer (ALB) in the centralized VP
J. Create target groups for the private DNS names of the NLB
K. Configure host-based routing to route application traffic between individual applications though the ALB.
L. Run the applications behind private Network Load Balancers (NLBs) inseparate VPC
M. Configure each NLB as an AWS PrivateLink endpoint service with associated VPC endpoints in the centralized VPC Create target groups that include the private IP addresses of each endpoin
N. Create a public Application Load Balancer (ALB) in the centralized VP
O. Configurehost-based routing to route application traffic to the corresponding target group through the ALB.

Answer: D

NEW QUESTION 14
A company's application runs in a VPC and stores sensitive data in Amazon S3 The application's Amazon EC2 instances are located in a private subnet with a NAT gateway deployed in a public subnet to provide access to Amazon S3 The S3 bucket is located in the same AWS Region as the EC2 instances The company wants to ensure that this bucket can be accessed only from the VPC where the application resides
Which changes should a network engineer make to the architecture to meet these requirements?

A. Delete the existing S3 bucket and create a new S3 bucket inside the VPC in the private subnet Configure the S3 security group to allow only the application instances to access the bucket
B. Deploy an S3 VPC endpoint in the VPC where the application resides Configure an S3 bucket policy with a condition to allow access only from the VPC endpoint
C. Configure an S3 bucket policy, and use an IP address condition to restrict access to the bucket Allow access only from the VPC CIDR range, and deny all other IP address ranges
D. Create a new 1AM role for the EC2 instances that provides access to the S3 bucket and assign the role to the application instances Configure an S3 bucket policy to allow access only from the role

Answer: B

NEW QUESTION 18
An organization will be extending its existing on-premises infrastructure into the cloud. The design consists of a transit VPC that contains stateful firewalls that will be deployed in a highly available configuration across two Availability Zones for automatic failover.
What MUST be configured for this design to work? (Select two.)

A. A different Autonomous System Number (ASN) for each firewall.
B. Border Gateway Protocol (BGP) routing
C. Autonomous system (AS) path prepending
D. Static routing
E. Equal-cost multi-path routing (ECMP)

Answer: BC

Explanation:
https://docs.aws.amazon.com/solutions/latest/cisco-based-transit-vpc/appendix-a.html

NEW QUESTION 22
You are designing an AWS Direct Connect solution into your VPC. You need to consider requirements for the customer router to terminate the Direct Connect link at the Direct Connect location.
Which three factors that must be supported should you consider when choosing the customer router? (Select three.)

A. 802.1q trunking
B. 802.1ax or 802.3ad link aggregation
C. OSPF

D. BGP
E. single-mode optical fiber connectivity
F. 1-Gbps copper connectivity

Answer: ADE

Explanation:
https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html#overview_requirements

NEW QUESTION 24
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: AC

NEW QUESTION 26
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. Use the existing VPC and configure Amazon EMR in a private subnet with an Amazon S3 endpoint.
B. use the existing VPS and a NAT gateway, and configure Amazon EMR in a private subnet with an Amazon S3 endpoint.
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. 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: A

Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html

NEW QUESTION 27
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/

NEW QUESTION 31
An organization's Security team has a requirement that all data leaving its on-premises data center be encrypted at the network layer and use dedicated connectivity. There is also a requirement to centrally log all traffic flow in Amazon VPC environments. An AWS Direct Connect connection has been ordered to build out this design.
What steps should be taken to ensure that connectivity to AWS meets these security requirements? (Choose two.)

A. Provision a public virtual interface on AWS Direct Connect and set up a VPN to each VPC.
B. Provision a private virtual interface for each VPC connection.
C. Enable VPC Flow Logs for each VPC.
D. Use AWS KMS to encrypt traffic between on-premises and AWS.
E. Provision a VPN connection to each VPC over the internet.

Answer: AC

NEW QUESTION 33
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. Enable enhanced networking
B. Select G2 instance types
C. Enable jumbo frames

D. Use multiple elastic network interfaces

Answer: A

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

NEW QUESTION 34
A company has an application running on Amazon EC2 instances in a private subnet that connects to a third-party service provider's public HTTP endpoint through a NAT gateway. As request rates increase, new connections are starting to fail. At the same time, the ErrorPortAllocation Amazon CloudWatch metric count for the NAT gateway is increasing.
Which of the following actions should improve the connectivity issues? (Choose two.)

A. Allocate additional elastic IP addresses to the NAT gateway.
B. Request that the third-party service provider implement HTTP keepalive.
C. Implement TCP keepalive on the client instances.
D. Create additional NAT gateways and update the private subnet route table to introduce the new NAT gateways.
E. Create additional NAT gateways in the public subnet and split client instances into multiple privatesubnets, each with a route to a different NAT gateway.

Answer: CE

NEW QUESTION 39
A gaming company is running an online multiplayer game in multiple AWS Regions The company needs traffic from its end users to be routed to the Region that is closest to the end users geographically When maintenance occurs in a Region, traffic must be routed to the next closest Region with no changes to the IP addresses being used as connections by the end users
Which solution will meet these requirements?

A. Create an Amazon CloudFront distribution in front of all the Regions
B. Use an Amazon Route 53 geoproximity routing policy to navigate traffic to the closest Region
C. Use an Amazon Route 53 geolocation routing policy to navigate traffic to the closest Region
D. Configure AWS Global Accelerator in front of all the Regions

Answer: A

NEW QUESTION 43
A company has an application running in an Amazon VPC that must be able to communicate with on-premises resources in a data center. Network traffic between AWS and the data center will initially be minimal, but will increase to more than 10 Gbps over the next few months. The company's goal is to launch the application as quickly as possible. The Network Engineer has been asked to design a hybrid IT connectivity solution. What should be done to meet these requirements?

A. Submit a 1 Gbps AWS Direct Connect connection request, then increase the number of Direct Connect connections, as needed.
B. Allocate elastic IPs to Amazon EC2 instances for temporary access to on-premises resources, then provision AWS VPN connections between an Amazon VPC and the data center.
C. Provision an AWS VPN connection between an Amazon VPC and the data center, then submit an AWS Direct Connect connection reques
D. Later, cut over from the VPN connection to one or more Direct Connect connections, as needed.
E. Provision a 100 Mbps AWS Direct Connect connection between an Amazon VPC and the data center, then submit a Direct Connect connection reques
F. Later, cut over from the hosted connection to one or more Direct Connect connections, as needed.

Answer: C

NEW QUESTION 46
A company is delivering web content from an Amazon EC2 instance in a public subnet with address 2001 db8 1 100 1 Users report they are unable to access the web content The VPC Flow Logs tor the subnet contain the following entries.

```
2 012345678912 eni-0596e500123456789 2001:db8:2:200::2 2001:db8:1:100::1 0 0 58 234 24336 1551299195 1551299434 ACCEPT OK
2 012345678912 eni-0596e500123456789 2001:db8:1:100::1 2001:db8:2:200::2 0 0 58 234 24336 1551299195 1551299434 REJECT OK
```

Which action will restore network reachability to the EC2 instance1?

A. Update the security group associated with eni-0596e500l23456789 to permit inbound traffic
B. Update the security group associated with eni-059€«500i234 56~89 to permit outbound traffic
C. Update the network ACL associated with the subnet to permit inbound traffic
D. Update the network ACL associated with the subnet to permit outbound traffic

Answer: C

NEW QUESTION 50
A company with several VPCs in the us-east-1 Region wants to reduce the cost of its workloads A network engineer has identified that all traffic bound to Amazon services is flowing through a NAT gateway. Additionally, all the VPCs are peered to a hub VPC for access to common services.

A. Disable the private DNS name for the SQS endpoin
B. Create an Amazon Route 53 private hosted zone for the domain us-east-1.sqs.amazonaws.co
C. Create a CNAME record to the DNS name of the SQS endpoint Share the private hosted zone with ail other VPCs
D. Disable the private DNS name for the SOS endpoin
E. Create an Amazon Route 53 private hosted zone for the domain sqs.us-east-1 .amazonaws.co
F. Create an alias record to the DNS name of the SOS endpoin
G. Share the private hosted zone with all other VPCs
H. Enable the private DNS name for the SOS endpoint Create an Amazon Route 53 private hosted zone for the domain SQS.us-east-t.amazonaws.co

I. Create a CNAME record to the DNS name of the SQS endpoin
J. Share the private hosted zone with all other VPCs.
K. Enable the private DNS name for the SQS endpoin
L. Create an Amazon Route 53 private hosted zone for the domain us-east-1 .sqs.amazonaws.co
M. Create an alias record to the DNS name of the SQS endpoin
N. Share the private hosted zone with all other VPCs.

Answer: A

NEW QUESTION 53
You run a well-architected, multi-AZ application in the eu-central-1 (Frankfurt) AWS region. The application is hosted in a VPC and is only accessed from the corporate network. To support large volumes of data transfer and administration of the application, you use a single 10-Gbps AWS Direct Connect connection with multiple private virtual interfaces. As part of a review, you decide to improve the resilience of your connection to AWS and make sure that any additional connectivity does not share the same Direct Connect routers at AWS. You need to provide the best levels of resilience to meet the application's needs.
Which two options should you consider? (Select two.)

A. Install a second 10-Gbps Direct Connect connection to the same Direct Connection location.
B. Deploy an IPsec VPN over a public virtual interface on a new 10-Gbps Direct Connect connection.
C. Install a second 10-Gbps Direct Connect connection to a Direct Connect location in eu-west-1.
D. Deploy an IPsec VPN over the Internet to the eu-west-1 region for diversity.
E. Install a second 10-Gbps Direct Connect connection to a second Direct Connect location for eu-central-1.

Answer: AE

Explanation:
https://aws.amazon.com/directconnect/resiliency-recommendation/

NEW QUESTION 56
A company is deploying a critical application on two Amazon EC2 instances in a VPC Failed client connections to the EC2 instances must be logged according to company policy.
What is the MOST cost-effective solution to meet these requirements'?

A. Move the EC2 instances to a dedicated VPC Enable VPC Flow Logs with a filter on the deny action Publish the flow logs to Amazon CloudWatch Logs
B. Move the EC2 instances to a dedicated VPC subnet Enable VPC Flow Logs for the subnet with a filter on the reject action Publish the flow logs to an Amazon Kinesis Data Firehose stream with a data delivery to an Amazon S3 bucket
C. Enable VPC Flow Logs, filtered for rejected traffic for the elastic network interfaces associated with the instances Publish the flow logs to an Amazon Kinesis Data Firehose stream with a data delivery to an Amazon S3 bucket
D. Enable VPC Flow Logs, filtered for rejected traffic for the elastic network interfaces associated with the instances Publish the flow logs to Amazon CloudWatch Logs

Answer: D

NEW QUESTION 59
An application runs on a fleet of Amazon EC2 instances in a VPC. All instances can reach one another using private IP addresses. The application owner has a new requirement that the domain name received via DHCP should be different for a particular set of instances that are currently in one particular subnet.
What changes should be made to meet this requirement while continuing to support the existing application requirements?

A. Modify the existing DHCP option set and specify the different domain name for the specified subnet.
B. Create a new DHCP option set with the different domain name, associate it with the specified subnet, and re-launch the Amazon EC2 instances.
C. Create a new subnet, configure the DHCP option set with the different domain name, and re-launch the required instances there.
D. Create a new peered VPC, configure the DHCP option set with the different domain name, and re-launch the required instances there.

Answer: D

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_DHCP_Options.html

NEW QUESTION 60
A company uses multiple AWS accounts within AWS Organizations and has services deployed in a single AWS Region. The instances in a private subnet occasionally download patches from the internet through a NAT gateway The company recently migrated from VPC peering to AWS Transit Gateway The cumulative traffic through deployed NAT gateways Is less than 1Gbps The NAT gateway hourly charge contributes to most of the NAT gateway costs across all linked accounts.
What should the company do to reduce NAT gateway hourly costs?

A. Deploy and use NAT gateways in the same Availability Zone as the heavy-traffic resources.
B. Move to a centralized NAT gateway architecture with NAT gateways deployed in an egress VPC Use VPC peering to send traffic through the centralized NAT gateways.
C. Use VPC endpoints to send traffic to AWS services in the same Region.
D. Move to a centralized NAT gateway architecture with NAT gateways deployed in an egress VPC Use AWS Transit Gateway to send traffic through the centralized NAT gateways.

Answer: B

NEW QUESTION 61
A company has a hybrid IT architecture with two AWS Direct Connect connections to provide high availability. The services hosted on-premises are accessible using public IPs, and are also on the 172.16.0.0/16 range. The AWS resources are on the 192.168.0.0/18 range. The company wants to use Amazon Elastic Load Balancing for SSL offloading, health checks, and sticky sessions.
What should be done to meet these requirements?

A. Create a Network Load Balancer pointing to the on-premises server's private IP address.
B. Create an Amazon CloudFront distribution for the on-premises service and use the public IPs of the on-premises servers as the origin.
C. Create a Network Load Balancer pointing to the on-premises server's public IP address.
D. Create an Application Load Balancer pointing to the on-premises server's private IP address.

Answer: D

NEW QUESTION 65
An IT company wants to securely perform an on-off migration of its on-premises VMs to the AWS Cloud by using AWS Server Migration Service {AWS SMS) For the first phase of the migration, the company must migrate 50 development VMs m batches during non-peak times over the next 7 days The VMs are between 2 GB and 5 GB in size The company has 1 Gbps of available bandwidth over the internet
Which network connectivity option meets these requirements MOST cost-effectively?

A. Contact an AWS partner to order a hosted VIF
B. Use the existing internet connection
C. Order an AWS Direct Connect connection Provision a public VIF
D. Create a VPN connection to AWS.

Answer: D

NEW QUESTION 70
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 issued

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: A

NEW QUESTION 74
An architecture is being designed to support an Amazon WorkSpaces deployment of 1,000 desktops. Which architecture will support this deployment while allowing for future expansion?

A. A VPC with a /16 CIDR and one /21 subnet
B. A VPC with a /20 CIDR and two /21 subnets
C. A VPC with a /16 CIDR and one /22 subnet
D. A VPC with a /20 CIDR and two /23 subnets

Answer: B

NEW QUESTION 79
A company has Iwo on-premises data center locations. There is a company-managed router at earn data center. Each data center has a dedicated AWS Direct Connect connection to a Direct Connect gateway through a private virtual interface The router for the first location is advertising 110 routes to the Direct Connect gateway by using BGP and the router tor the second location is advertising 60 routes to the Direct Connect gateway by using BGP The Direct Connect gateway is attached to a company VPC through a virtual private gateway
A network engineer receives reports that resources In the VPC are not reachable from various locations in either data center. The network engineer checks the VPC route table and sees that the routes from the first data center. location are not being populated into the route table The network engineer must resolve this issue in the most operationally efficient manner
What should the network engineer do to meet these requirements'

A. Remove the Direct Connect gateway, and create a new private virtual interface from each company router to the virtual private gateway of the VPC
B. Change the router configurations to summarize the advertised routes
C. Open a support ticket to increase the quota on advertised routes to the VPC route table
D. Create an AWS Transit Gateway Attach the transit gateway to the VPC and connect the Direct Connect gateway to the transit gateway.

Answer: D

NEW QUESTION 81
An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used.
Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: “There are not enough free addresses in subnet ‘subnet-12345677’ to satisfy the requested number of instances.”
What action will resolve the availability problem?

A. Create a new subnet using a VPC secondary IPv6 CIDR, and associate an IPv6 CID
B. Include the new subnet in the Auto Scaling group.
C. Create a new subnet using a VPC secondary IPv4 CIDR, and associate an IPv6 CID
D. Include the new subnet in the Auto Scaling group.
E. Resize the IPv6 CIDR on each of the existing subnet
F. Modify the Auto Scaling group maximum number of instances.
G. Add a secondary IPv4 CIDR to the Amazon VP
H. Assign secondary IPv4 address space to each of the existing subnets.

Answer: B

NEW QUESTION 82
A multinational organization has applications deployed in three different AWS regions. These applications must securely communicate with each other by VPN.
According to the organization's security team, the VPN must meet the following requirements:
AES 128-bit encryption
SHA-1 hashing
User access via SSL VPN
PFS using DH Group 2
Ability to maintain/rotate keys and passwords
Certificate-based authentication
Which solution should you recommend so that the organization meets the requirements?

A. AWS hardware VPN between the virtual private gateway and customer gateway
B. A third-party VPN solution deployed from AWS Marketplace
C. A private MPLS solution from an international carrier
D. AWS hardware VPN between the virtual private gateways in each region

Answer: B

Explanation:
https://blog.cloudthat.com/configuring-vpn-between-the-vpcs-across-regionsaccounts/

NEW QUESTION 83
A company is building a hybrid PCI-DSS compliant application that runs in the us-west-2 Region and
on-premises. The application sends access logs from all locations to a single Amazon S3 bucket in us-west-2 To protect this sensitive data, the bucket policy is configured to deny access from public IP addresses
How should an engineer configure the network to meet these requirements?

A. Configure an AWS Direct Connect private virtual interface to the company's AWS VPC in us-west-2 Create a VPC endpoint and configure the on-premises systems to leverage an HTTPS proxy in the VPC to access Amazon S3
B. Configure a VPN connection to the company's AWS VPC in us-west-2 and use BGP to advertise routes for Amazon S3
C. Configure a Direct Connect connection public virtual interface to us-west-2 Leverage an on-premises HTTPS proxy to send traffic to Amazon S3 over a Direct Connect connection
D. Configure a VPN connection to the company's AWS VPC in us-west-2 Create a NAT gateway and configure the on-premises systems to leverage an HTTPS proxy in the VPC to access Amazon S3

Answer: C

NEW QUESTION 84
A financial company is designing a secure AWS network architecture to support a hybrid cloud strategy. Systems deployed in the AWS Cloud are mission critical and have strict availability requirements. The
company anticipates the need for hundreds of VPCs. Instances will be transient and rely heavily on DNS resolution The applications must be designed to have Availability Zone isolation and tolerate the loss of an Availability Zone
What is the MOST reliable way to implement DNS in this scenario?

A. Create a new DHCP options set with DNS settings with on-premises DNS servers that traverse an AWS Direct Connect connection.
B. Create private hosted zones and share them with each VP
C. Use Amazon Route 53 Resolver for hybrid DNS.
D. Modify the default DHCP options set with a fleet of proxy DNS servers that are deployed in each VPC.
E. Create a fleet of DNS proxy servers in a central VP
F. Share the proxy fleet with each VPC using AWS PrivateLink.

Answer: C

NEW QUESTION 89
You ping an Amazon Elastic Compute Cloud (EC2) instance from an on-premises server. VPC Flow Logs record the following:
2 123456789010 eni-1235b8ca 10.123.234.78 172.11.22.33 0 0 1 8 672 1432917027
1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.11.22.33 10.123.234.78 0 0 1 4 336 1432917027
1432917082 ACCEPT OK
2 123456789010 eni-1235b8ca 172.11.22.33 10.123.234.78 0 0 1 4 336 1432917094
1432917142 REJECT OK
Why are ICMP responses not received by the on-premises system?

A. The inbound network access control list is blocking the traffic
B. The outbound network access control list is blocking the traffic
C. The inbound security group is blocking the traffic.
D. The outbound security group is blocking the traffic.

Answer: B

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html

NEW QUESTION 94
DNS name resolution must be provided for services in the following four zones: company.private.
emea.company.private. apac.company.private. amer.company.private.

The contents of these zones is not considered sensitive, however, the zones only need to be used by services hosted in these VPCs, one per geographic region. Each VPC should resolve the names in all zones.
How can you use Amazon route 53 to meet these requirements?

A. Create a Route 53 Private Hosted Zone for each of the four zones and associate them with the three VPCs.
B. Create a single Route 53 Private Hosted Zone for the zone company.private and associate it with thethree VPCs.
C. Create a Route Public Hosted Zone for each of the four zones and configure the VPS DNS Resolver to forward
D. Create a single Route 53 Public Hosted Zone for the zone company.private and configure the VPS DNS Resolver to forward

Answer: A

NEW QUESTION 99
A company is running services in a VPC with a CIDR block of 10.5.0.0/22 End users report that they no longer can provision new resources because some ot the subnets in theVPC have run out of IP addresses
How should a network engineer resolve this issue?

A. Add 10 5.2.0/23 as a second CIDR block to the VPC Create a new subnet with a new CIDR block, and provision new resources in the new subnet
B. Add 10 5.4.0/21 as a second CIDR block to the VPC Assign a second network from this CIDR block to the existing subnets that have run out of IP addresses
C. Add 10.5.4.0/22 as a second CIDR block to the VP
D. Assign a second network from this CIDR block to the existing subnets that have run out of IP addresses
E. Add 10.5.4.0/22 as a second CIDR block to the VP
F. Create a new subnet with a new CIDR block, and provision new resources in the new subnet

Answer: D

NEW QUESTION 103
An organization runs a consumer-facing website on AWS. The Amazon EC2-based web fleet is load balanced using the AWS Application Load Balancer, Amazon Route 53 is used to provide the public DNS services.
The following URLs need to server content to end users: test.example.com
web.example.com example.com
Based on this information, what combination of services must be used to meet the requirement? (Select two.)

A. Path condition in ALB listener to route example.com to appropriate target groups.
B. Host condition in ALB listener to route *.example.com to appropriate target groups.
C. Host condition a ALB listener to route example.com to appropriate target groups.
D. Path condition in ALB listener to route *.example.com to appropriate target groups.
E. Host condition in ALB listener to route $$$$.example.com to appropriate target groups.

Answer: BC

Explanation:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#rule-condition
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html

NEW QUESTION 105
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. 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."

NEW QUESTION 106
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: AC

NEW QUESTION 110

A company needs to allow its remote users to access company resources in the AWS Cloud. The company has two VPCs that are connected through VPC peering. The remote users must be able to access resources in both VPCs by using secure connections from their laptop computers The company does not want to implement an access management solution that requires additional costs or effort.
Which solution meets these requirements?

A. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target networ
B. Add a rule to authorize client access to the target VP
C. and add a rule to authorize client access to the peered VP
D. Update resource security groups in both VPCs to allow traffic from the security group for the subnet associatio
E. Instruct the users to sign in to the AWS Management Console and navigate to Client VPN to connect to the Client VPN endpoint.
F. Deploy an AWS Client VPN endpoint in both VPCs, associate subnets, and define a target networ
G. Add a rule to authorize client access to each target VP
H. Update resource security groups in both VPCs to allow traffic from the security groups of each VPC for the subnet association
I. Securely send the users the configuration options, and instruct the users to install Client VPN endpoints at the same time to gain access to the resources.
J. Deploy a Network Load Balancer in front of the company resource
K. Set up security groups that contain the IP addresses of each of the user laptop
L. Instruct the users to connect to the application securely over TCP.
M. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target networ
N. Add a rule to authorize client access to the target VP
O. and add a rule to authorize client access to the peered VP
P. Update resource security groups in both VPCs to allow traffic from the security group for the subnet associatio
Q. Securely send the users the configuration options, and instruct the users to install Client VPN on their laptop
R. Instruct the users to connect to the Client VPN endpoint to gain access to the resources.

Answer: B

NEW QUESTION 115
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. Use a Route 53 public hosted zone for example.com and a private hosted zone for dev.example.com
B. Use a Route 53 public and private hosted zone for example.com and perform subdomain delegation for dev.example.com
C. Use a Route 53 public hosted zone for example.com and perform subdomain delegation for dev.example.com
D. Use a Route 53 private hosted zone for example.com and perform subdomain delegation for dev.example.com

Answer: A

Explanation:
aws.amazon.com/premiumsupport/knowledge-center/internal-version-website/

NEW QUESTION 120
A Network Engineer has enabled VPC Flow Logs to troubleshoot an ICMP reachability issue for an echo reply from an Amazon EC2 instance. The flow logs reveal an ACCEPT record for the request from the client to the EC2 instance, and a REJECT record for the response from the EC2 instance to the client.
What is the MOST likely reason for there to be a REJECT record?

A. The security group is denying inbound ICMP.
B. The network ACL is denying inbound ICMP.
C. The security group is denying outbound ICMP.
D. The network ACL is denying outbound ICMP.

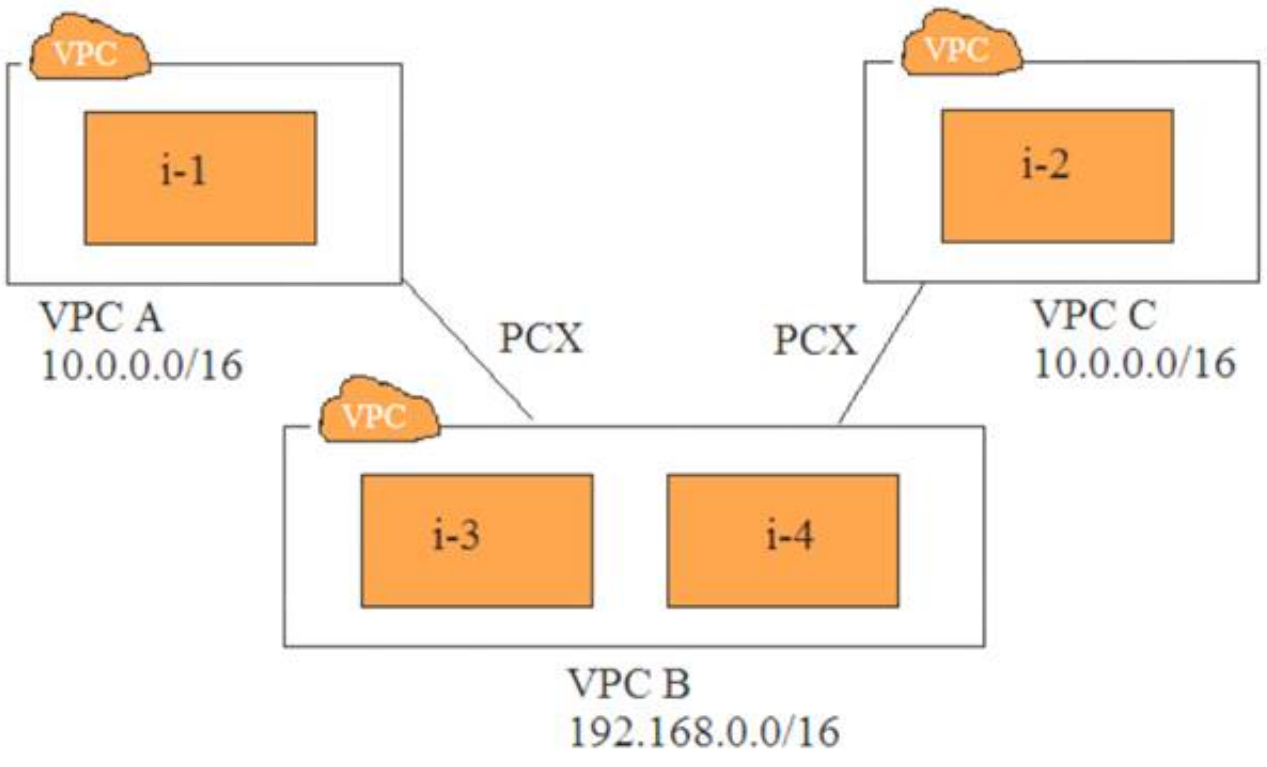
Answer: D

NEW QUESTION 122
A company wants to use thin clients running virtual desktops to replace 500 desktop computers used by its call center employees The company is evaluating Amazon Workspaces as a solution
A network engineer who is testing with a thin client is unable to conned to Amazon Workspaces After entering credentials the network engineer receives the following error:
"An error occurred while launching your Workspace Please try again" What should the network engineer do to resolve this issue?

A. Update the inbound rules on the network ACL on the subnets used for Amazon Workspaces to allow UDP on port 4172 and TCP on port 4172
B. Update the company's corporate firewall to allow outbound access to UDP on port 4172 and TCP on port 4172 Open inbound ephemeral ports explicitly to allow return communication
C. Update the inbound rules on the security group assigned to Amazon Workspaces to allow UDP on port 4172 and TCP on port 4172
D. Update the company's corporate firewall to allow inbound access to UDP on port 4172 and TCP on port 4172 Open outbound ephemeral ports explicitly to allow return communication

Answer: C

NEW QUESTION 126
Refer to the image.



You have three VPCs: A, B, and C. VPCs A and C are both peered with VPC B. The IP address ranges are as follows:
VPC A: 10.0.0.0/16
VPC B: 192.168.0.0/16
VPC C: 10.0.0.0/16
Instance i-1 in VPC A has the IP address 10.0.0.10. Instance i-2 in VPC C has the IP address 10.0.0.10. Instances i-3 and i-4 in VPC B have the IP addresses 192.168.1.10 and 192.168.1.20, respectively, i-3 and i-4 are in the subnet 192.168.1.0/24.
i-3 must be able to communicate with i-1
i-4 must be able to communicate with i-2
i-3 and i-4 are able to communicate with i-1, but not with i-2.
Which two steps will fix this problem? (Select two.)

A. Create subnets 192.168.1.0/28 and 192.168.1.16/28. Move i-3 and i-4 to these subnets, respectively.
B. Create subnets 192.168.1.0/27 and 192.168.1.16/27. Move i-3 and i-4 to these subnets, respectively.
C. Change the IP address of i-2 to 10.0.0.100. Assign it an elastic IP address.
D. Create a new route table for VPC B, with unique route entries for destination VPC A and destination VPC C.
E. Create two route tables: one with a route for destination VPC A, and another for destination VPC C.

Answer: AE

Explanation:
https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-partial-access.html#one-to-two-vpcs-sim

NEW QUESTION 130
A company has a hybrid architecture with dual AWS Direct Connect connections and applications running in the AWS Cloud and on premises The company uses its on-premises DNS servers to provide name resolution tor its internal domain company com The company uses an Amazon Route 53 private hosted zone, aws company com for resolution of AWS resource records
A new application that runs on Amazon EC2 in the company's VPC needs to resolve records in the company.com domain and on other AWS resources
What should the company do to meet these requirements?

A. Create a new DHCP options set Configure the DHCP options set name servers to be the on-premises DNS servers, and configure the domain name to be company com Assign the DHCP options set to the VPC with the EC2 instances
B. Create Route 53 Resolver outbound endpoints in each subnet in the VPC Configure a Route 53 forwarding rule with a rule type of Forward for company com that points to the on-premises DNS servers Configure a Route 53 forwarding rule with a rule type of System for aws company com
C. Create Route 53 Resolver outbound endpoints in each subnet in the VPC Configure conditional forwarding rules on the on-premises DNS servers to forward queries for the domain aws company com to the Route 53 Resolver endpoints Modify the DHCP options set to configure instances to resolve hostnames using the on-premises DNS servers
D. Create a private hosted zone for company com within the AWS account Create Route 53 Resolver inbound endpoints in each subnet in the VPC Configure the on-premises DNS servers to send outbound zone transfers for company com to the Route 53 Resolver endpoints

Answer: C

NEW QUESTION 133
Under increased cybersecurity concerns, a company is deploying a near real-time intrusion detection system (IDS) solution. A system must be put in place as soon as possible. The architecture consists of many AWS accounts, and all results must be delivered to a central location.
Which solution will meet this requirement, while minimizing downtime and costs?

A. Deploy a third-party vendor solution to perform deep packet inspection in a transit VPC.
B. Enable VPC Flow Logs on each VP
C. Set up a stream of the flow logs to a central Amazon Elasticsearch cluster.
D. Enable Amazon Macie on each AWS account and configure central reporting.
E. Enable Amazon GuardDuty on each account as members of a central account.

Answer: D

Explanation:
References:
https://aws.amazon.com/blogs/security/how-to-manage-amazon-guardduty-security-findings-across-multiple-acc

NEW QUESTION 138
A network engineer is managing two AWS Direct Connect connections. Each connection has a public virtual interface configured with a private ASN. The engineer wants to configure active/passive routing between the Direct Connect connections to access Amazon public endpoints. What BGP configuration is required for the on-premises equipment? (Select two.)

A. Use Local Pref to control outbound traffic.
B. Use AS Prepending to control inbound traffic.
C. Use eBGP multi-hop between loopback interfaces.
D. Use BGP Communities to control outbound traffic.
E. Advertise more specific prefixes over one Direct Connect connection.

Answer: AE

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/active-passive-direct-connect/

NEW QUESTION 140
Your application is hosted behind an Elastic Load Balancer (ELB) within an autoscaling group. The autoscaling group is configured with a minimum of 2, a maximum of 14, and a desired value of 2. The autoscaling cooldown and the termination policies are set to the default value.
CloudWatch reports that the site typically requires just two servers, but spikes at the start and end of the business day can require eight to ten servers. You receive intermittent reports of timeouts and partially loaded web pages.
Which configuration change should you make to address this issue?

A. Configure connection draining on the ELB.
B. Configure the autoscaling cooldown to 600 seconds.
C. Configure the termination policy to oldest instance.
D. Configure a Terminating: Wait lifecycle hook on a scale in event.

Answer: A

Explanation:
References: https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html

NEW QUESTION 141
Your hybrid networking environment consists of two application VPCs, a shared services VPC, and your corporate network. The corporate network is connected to the shared services VPC via an IPsec VPN with dynamic (BGP) routing enabled.
The applications require access to a common authentication service in the shared services VPC. You need to enable native network access from the corporate network to both application VPCs.
Which step should you take to meet the requirements?

A. Use VPC peering to peer the application VPCs with the shared services VPC, and enable associated routing in the shared services VPC via the corporate VPN.
B. Configure an IPsec VPN between the virtual private gateway in each application VPC to the virtual private gateway in the shared services VPC.
C. Configure additional IPsec VPNs for each application VPC back to the corporate network, and enable VPC peering to the shared services VPC.
D. Enable CloudHub functionality to route traffic between the three VPCs and the corporate network using dynamic BGP routing.

Answer: C

NEW QUESTION 144
A company has 225 mobile and desktop devices and 300 partner VPNs that need access to an AWS VPC. VPN users should not be able to reach one another.
Which approach will meet the technical and security requirements while minimizing costs?

A. Use the AWS IPsec VPN for the mobile, desktop, and partner VPN connection
B. Use network access control lists (Network ACLs) and security groups to maintain routing separation.
C. Use the AWS IPsec VPN for the partner VPN connection
D. Use an Amazon EC2 instance VPN for the mobile and desktop device
E. Use Network ACLs and security groups to maintain routing separation.
F. Create an AWS Direct Connect connection between on-premises and AWS Use a public virtual interface to connect to the AWS IPsec VPN for the mobile, desktop, and partner VPN connections.
G. Use an Amazon EC2 instance VPN for the desktop, mobile, and partner VPN connection
H. Use features of the VPN instance to limit routing and connectivity.

Answer: D

NEW QUESTION 147
An organization is deploying an application in a VPC that requires SSL mutual authentication with a client-side certificate, as that is the primary method of identifying clients. The Network Engineer has been tasked with defining the mechanism used within AWS to provide the SSL mutual authentication.
Which of the following options meets the organization's requirements?

A. Use a Classic Load Balancer and upload the client certificate private keys to i
B. Perform SSL mutual authentication of the client-side certificate there.
C. Use a Network Load Balancer with a TCP listener on port 443, and pass the request through for the SSL mutual authentication to be handled by a backend instance.
D. Use an Application Load Balancer and upload the client certificate private keys to it by using the native server name indication (SNI) features with smart certificate selection to handle multiple calling applications.
E. Front the application with Amazon API Gateway, and use its client-side SSL mutual authentication feature that uses the backend instances to verify the source of the request.

Answer: B

NEW QUESTION 149
A network architect is designing an internet website. It has web, application, and database tiers that will run in AWS. The website uses Amazon DynamoDB.
Which architecture will minimize public exposure of the back-end instances?

A. A VPC with public subnets for the NLB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.
B. A VPC with public subnets for the ALB, private subnets for the web tier, and private subnets for the application tie
C. The application tier connects DynamoDB through a VPC endpoint.
D. A VPC with public subnets for the ALB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.
E. A VPC with public subnets for the NLB, private subnets for the web tier, and public subnets for theapplication tie
F. The application tier connects DynamoDB through a VPC endpoint.

Answer: B

NEW QUESTION 151
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 VP
B. Add a public virtual interface to the Direct Connect connection for users to access the AppStream endpoint
C. Deploy two subnets into the existing VP
D. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.
E. Deploy a new VPC with two subnet
F. Create a VPC peering connection between the two VPCs for users to access the AppStream endpoint.
G. Deploy one subnet into the existing VP
H. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.

Answer: B

NEW QUESTION 154
A network engineer is deploying an application on an Amazon EC2 instance. The instance is reachable within the VPC through its private IP address and from the internet using an elastic IP address. Clients are connecting to the instance over the Internet and within the VPC, and the application needs to be identified by a single custom Fully Qualified Domain Name that is publicly resolvable –'app.example.com'.
Instances within the VPC should always connect to the private IP to minimize data transfer costs.
How should the engineer configure DNS to support these requirements?

A. Use Amazon Route 53 to create a geo-based routing entry for the hostname 'app' in the DNS zone 'example.com'.
B. Create two A record entries for 'app' in the DNS zone 'example.com' – one for the public IP and one for the private IP.
C. Use Route 53 to create an ALIAS record to the public DNS name for the instance.
D. Create a CNAME for 'app' in the DNS zone 'example.com' to the public DNS name for the Amazon EC2 instance.

Answer: D

NEW QUESTION 156
You have been asked to monitor traffic flows on your Amazon EC2 instance. You will be performing deep packet inspection, looking for atypical patterns.
Which tool will enable you to look at this data?

A. Wireshark
B. VPC Flow Logs
C. AWS CLI
D. CloudWatch Logs

Answer: A

NEW QUESTION 161
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. Use multiple CloudHSM instances, and load balance them using a Network Load Balancer.
B. Use multiple CloudHSM instances to the cluster;request to it will automatically load balance.
C. Enable Auto Scaling on the CloudHSM instance, with similar configuration to the web tier Auto Scaling group.
D. Use multiple CloudHSM instances, and load balance them using an Application Load Balancer.

Answer: B

Explanation:
https://docs.aws.amazon.com/cloudhsm/latest/userguide/clusters.html#cluster-high-availability-load-balancing

NEW QUESTION 165
A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2 instances now use a NAT gateway tor internet access After the migration, some long-running database queries from private EC2 instances to a publicly accessible third-party database no longer receive responses The database query logs reveal that the queries successfully completed after 7 minutes but that the client EC2 instances never received the response.
Which configuration change should a network engineer implement to resolve this issue"

A. Configure the NAT gateway timeout to allow connections for up to 600 seconds
B. Enable enhanced networking on the client EC2 instances

C. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds
D. Close idle TCP connections though the NAT gateway

Answer: C

NEW QUESTION 166
An organization delivers high-resolution, dynamic web content. Internet users access the content from a variety of platforms, including mobile, tablet and desktop. Each platform receives a customized experience to account for the differences in viewing modes. A dedicated, automatic-scaling fleet of Amazon EC2 instances is used for each platform to server content based on path-based headers.
Which combination of services will MINIMIZE cost and MAXIMIZE performance? (Select two.)

A. Amazon CloudFront with Lambda@Edge
B. Network Load Balancer
C. Amazon S3 static websites
D. Amazon Route 53 with traffic flow policies
E. Application Load Balancer

Answer: AE

Explanation:
References: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html

NEW QUESTION 170
A Lambda function needs to access the private address of an Amazon ElastiCache cluster in a VPC. The Lambda function also needs to write messages to Amazon SQS. The Lambda function has been configured to run in a subnet in the VPC.
Which of the following actions meet the requirements? (Select two.)

A. The Lambda function needs an IAM role to access Amazon SQS
B. The Lambda function must route through a NAT gateway or NAT instance in another subnet to access the public SQS API.
C. The Lambda function must be assigned a public IP address to access the public Amazon SQS API.
D. The ElastiCache server outbound security group rules must be configured to permit the Lambda function's security group.
E. The Lambda function must consume auto-assigned public IP addresses but not elastic IP addresses.

Answer: AB

Explanation:
https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

NEW QUESTION 173
You operate a production VPC with both a public and a private subnet. Your organization maintains a restricted Amazon S3 bucket to support this production workload. Only Amazon EC2 instances in the private subnet should access the bucket. You implement VPC endpoints(VPC-E) for Amazon S3 and remove the NAT that previously provided a network path to Amazon S3. The default VPC-E policy is applied. Neither EC2 instances in the public or private subnets are able to access the S3 bucket.
What should you do to enable Amazon S3 access from EC2 instances in the private subnet?

A. Add the CIDR address range of the private subnet to the S3 bucket policy.
B. Add the VPC-E identified to the S3 bucket policy.
C. Add the VPC identifier for the production VPC to the S3 bucket policy.
D. Add the VPC-E identifier for the production VPC to endpoint policy.

Answer: B

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html#vpc-endpoints-policies-s3

NEW QUESTION 178
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

NEW QUESTION 183
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AWS-Certified-Advanced-Networking-Specialty Practice Exam Features:

* AWS-Certified-Advanced-Networking-Specialty Questions and Answers Updated Frequently

* AWS-Certified-Advanced-Networking-Specialty Practice Questions Verified by Expert Senior Certified Staff

* AWS-Certified-Advanced-Networking-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AWS-Certified-Advanced-Networking-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year