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 an application running on Amazon EC2 instances in a VPC The application must publish custom metrics to Amazon CloudWatch in the same AWS Region The metrics include proprietary information All connectivity must be over private IP addresses.
Which solution will meet these requirements'?

A. Connect to CloudWatch through a NAT gateway
B. Connect to CloudWatch through a gateway endpoint
C. Connect to CloudWatch through an internet gateway
D. Connect to CloudWatch through an interface endpoint

Answer: D

NEW QUESTION 4
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 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 lo 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
C. VPCs do not have the routes to the on-premises environment that point to the transit gateway attachment
D. The on-premises route tables do not contain the exact CIDR blocks of the newly created VPCs
E. The route tables (or the newly created VPCs have only summary routes for (he on-premises environment (fiat point to the transit gateway attachment.
F. 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: AD

NEW QUESTION 6
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 7
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 8
You have to set up an AWS Direct Connect connection to connect your on-premises to an AWS VPC. Due to budget requirements, you can only provision a single Direct Connect port. You have two border gateway routers at your on-premises data center that can peer with the Direct Connect routers for redundancy.
Which two design methodologies, in combination, will achieve this connectivity? (Select two.)

A. Terminate the Direct Connect circuit on a L2 border switch, which in turn has trunk connections to thetwo routers.
B. Create two Direct Connect private VIFs for the same VPC, each with a different peer IP.
C. Terminate the Direct Connect circuit on any of the one routers, which in turn will have an IBGP session with the other router.
D. Create one Direct Connect private VIF for the VPC with two customer peer IPs.
E. Provision two VGWs for the VPC and create one Direct Connect private VIF per VGW.

Answer: AD

Explanation:
https://docs.aws.amazon.com/directconnect/latest/UserGuide/add-peer-to-vif.html (Adding a BGP Peer)

NEW QUESTION 9
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 10
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 10
A manufacturing company has a hybrid environment that includes an AWS Direct Connect gateway that is associated with an AWS Transit Gateway The company wants to extend a third-party application that is hosted in its on-premises data center into one of its VPCs
The application vendor has stated that It must use an overlay IP address to meet the company's requirement for high availability. The DHCP administrator has assigned a non-overlapping RFC1918 private address for use as the overlay IP address The security team requires connectivity to remain private
Which solution meets these requirements with the LEAST management overhead"

A. Create a layer 2 VPN across a public VIF by using a software-based VPN on a pair of Amazon EC2 instances Use BGP to advertise the routes over the VPN
B. Create a transit VIF with automatically propagated routes in the transit gateway route table Create a new subnet in the VPC for the overlay IP address, and propagate the route to the VPC route tabl
C. Update the route tables on premises as needed.
D. Create an external Network Load Balancer by using Amazon Route 53 to create records that point to the target application's overlay IP addres
E. Create static entries in the VPC route table
F. Create a transit VIF Then create static routes in the transit gateway route table to point to the VPC that contains the overlay IP address Create static routes in the VPC route table that point to the transit gateway Update the route tables on premises as needed

Answer: D

NEW QUESTION 11
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 13
A company runs a large-scale application on a feel of Amazon EC2 instances that ate distributed across several VPCs A Network Load Balancer (NLB) in a separate VPC routes traffic to the EC2 instances The NLB's VPC is peered to all the application VPCs
The application must process millions of requests each minute during times of peak utilization Users are reporting that the connections to the application are failing during peak times Monitoring shows an increase in port allocation errors on the NLB.
Which action will solve this issue with the LEAST change to the architecture?

A. Increase the number of EC2 instances in the target group
B. Create an Application Load Balancer for the target group
C. Add a new target group to the same NLB listener
D. Change the target group type to 'instance"

Answer: C

NEW QUESTION 14
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 16
An insurance company is planning the migration of workloads from its on-premises data center to the AWS Cloud The company requires end-to-end domain name resolution Bidirectional DNS resolution between AWS
and the existing on-premises environments must be established The workloads will be migrated into multiple VPCs. The workloads also have dependencies on each other, and not all the workloads will be migrated at the same time
Which solution meets these requirements? Which solution meets these requirements?

A. Configure a private hosted zone for each application VPC, and create the requisite records Create a set of Amazon Route 53 Resolver inbound and outbound endpoint In an egress VPC Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver Associate the application VPC private hosted zones with the egress VPC and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manage
B. Configure the on premises DNS servers to forward the cloud domains to the Route 53 inbound endpoint.
C. Configure a public hosted zone for each application VPC and create the requisite records Create a set of Amazon Route 53 Resolver Inbound and outbound endpoints in an egress VP
D. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver Associate the application VPC private hosted zones with the egress VPC and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manager Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints.
E. Configure a private hosted zone for each application VPC, and create the requisite records Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolve
F. Associate the application VPC private hosted zones with the egress VPC and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manage
G. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 outbound endpoint.
H. Configure a private hosted zone for each application VPC, and create the requisite records Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver Associate the Route 53 outbound rules with the application VPCs and share the private hosted zones with the application accounts by using AWS Resource Access Manager Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoint.

Answer: B

NEW QUESTION 19
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 20
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 24
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 29
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 30
A Network Engineer is troubleshooting a network connectivity issue for an instance within a public subnet that cannot connect to the internet. The first step the Engineer takes is to SSH to the instance via a local bastion within the VPC and runs an ifconfig command to inspect the IP addresses configured on the instance.
The output is as follows:

```
[ec2-user@ip-172-31-8-24 ~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 0A:A9:4A:21:41:BE
          inet addr:172.31.8.24  Bcast:172.31.15.255  Mask:255.255.240.0
          inet6 addr: fe80::8a9:4aff:fe21:41be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:557703 errors:0 dropped:0 overruns:0 frame:0
          TX packets:542300 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59639585 (56.8 MiB)  TX bytes:101633146 (96.9 MiB)
```

The Engineer notices that the command output does not contain a public IP address. In the AWS Management Console, the public subnet has a route to the internet gateway. The instance also has a public IP address associated with it.
What should the Engineer do next to troubleshoot this situation?

A. Configure the public IP on the interface.
B. Disable source/destination checking for the instance.
C. Associate an Elastic IP address to the interface.
D. Evaluate the security groups and the network access control list.

Answer: D

NEW QUESTION 35
A company has two redundant AWS Direct Connect connections to a VPC. The VPC is configured using BGP metrics so that one Direct Connect connection is used as the primary traffic path. The company wants the primary Direct Connect connection to fail to the secondary in less than one second.
What should be done to meet this requirement?

A. Configure BGP on the company's router with a keep-alive to 300 ms and the BGP hold timer to 900 ms.
B. Enable Bidirectional Forwarding Detection (BFD) on the company's router with a detection minimum interval of 300 ms and a BFD liveness detection multiplier of 3.
C. Enable Dead Peer Detection (DPD) on the company's router with a detection minimum interval of 300 ms and a DPD liveliness detection multiplier of 3.
D. Enable Bidirectional Forwarding Detection (BFD) echo mode on the company's router and disable sending the Internet Control Message Protocol (ICMP) IP packet requests.

Answer: B

NEW QUESTION 38
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 40
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 42
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. Configure AS-Prepending on your BGP session
B. Summarize your prefix announcement to less than 100
C. Announce a default route to the VPC over the BGP session
D. Enable route propagation on the VPC route table

Answer: B

NEW QUESTION 44
Your company maintains an Amazon Route 53 private hosted zone. DNS resolution is restricted to a single, pre-existing VPC. For a new application deployment, you create an additional VPC in the same AWS account. Both this new VPC and your on-premises DNS infrastructure must resolve records in the existing private hosted zone.
Which two activities are required to enable DNS resolution both within the new VPC and from the on-premises infrastructure? (Select two.)

A. Update the DHCP options set for the new VPC with the Route 53 nameserver IP addresses.
B. Update the Route 53 private hosted zone's VPC associations to include the new VPC.
C. Launch Amazon EC2-based DNS proxies in the new VP
D. Specify the proxies as forwarders in the on-premises DNS.
E. Update the on-premises DNS to include forwarders to the Route 53 nameserver IP addresses.
F. Launch Amazon EC2-based DNS proxies in the new VP
G. Specify the proxies in the DHCP options set.

Answer: BD

NEW QUESTION 46
Your company runs an HTTPS application using an Elastic Load Balancing (ELB) load balancer/PHP on nginx server/RDS in multiple Availability Zones. You need to apply Geographic Restriction and identify the client's IP address in your application to generate dynamic content.
How should you utilize AWS services in a scalable fashion to perform this task?

A. Modify the nginx log configuration to record value in X-Forwarded-For and use CloudFront to apply the Geographic Restriction.
B. Enable ELB access logs to store the client IP address and parse these to dynamically modify a blacklist.
C. Use X-Forwarded-For with security groups to apply the Geographic Restriction.
D. Modify the application code to use value of X-Forwarded-For and CloudFront to apply the Geographic Restriction.

Answer: D

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/elb-capture-client-ip-addresses/

NEW QUESTION 48
A company's developers wrote an AWS Lambda function to modify existing private route tables in response to a security appliance's auto scaling events. The Lambda function will be invoked on lifecycle hooks for an Auto Scaling group and Is configured to run in a VPC The developers are unsure if the following 1AM policy provides sufficient permissions to be used as an execution role for this Lambda function.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "ec2:CreateRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

The developers ask a network engineer to review the permissions.
Which set of permissions should the network engineer add lo the policy?

A. lambd
B. ListFunctions, lambda:GetPolicy, and ec2 Delete RouteTable
C. ec2:AssociateAddress, ec2 ModifylnstanceAttribut
D. and ec2 AssociateRouteTable
E. ec2:CreateNetworklntertace ec2 DeleteNetworklnterface, and ec2 ReplaceRoute
F. ec2:Describei.ifecydoHooks, ec2 DescribeScalingActivities, and ec2 DescribePolicies

Answer: C

NEW QUESTION 53
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 57
You need to set up an Amazon Elastic Compute Cloud (EC2) instance for an application that requires the lowest latency and the highest packet-per-second network performance. The application will talk to other servers in a peered VPC.
Which two of the following components should be part of the design? (Select two.)

A. Select an instance with support for single root I/O virtualization.
B. Select an instance that has support for multiple ENIs.
C. Ensure that the instance supports jumbo frames and set 9001 MTU.
D. Select an instance with Amazon Elastic Block Store (EBS)-optimization.
E. Ensure that proper OS drivers are installed.

Answer: AE

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

NEW QUESTION 61
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 66
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 68
A company has applications running in a single AWS Region and its on premises data center in a hybrid mode The company has a 1Gbps AWS Direct Connect connection from the data center to AWS that is 65% utilized. The company has an AWS Enterprise Support plan
The company is planning to deploy a new critical application on AWS that will connect with existing applications running in the data center. The application SLA requires a minimum ot 99.9% network uptime between the data center and AWS.
What is the MOST cost-effective way to meet this SLA requirement?

A. Create a second virtual interface (VIF) on the existing Direct Connect connection, and terminate this VIF in the existing VPC Use BGP for load balancing between the VIFs in active/active mode.
B. Purchase an additional 1Gbps Direct Connect connection from AWS In a different cross-connect location terminated in the associated Region Provision a new virtual interface (VIF) to the existing VP
C. and use BGP for load balancing
D. Set up two new hosted Direct Connect connections of 500 Mbps each through an AWS Direct Connect partne
E. Provision two virtual interfaces (VIFs) to the existing VPC on both Direct Connect connections, and use BGP for load balancing Terminate the existing 1Gbps Direct Connect connection
F. Purchase an additional 1Gbps Direct Connect connection from AWS in the existing cross-connect location Ask AWS to terminate this new connection in a different router Provision two virtual interfaces (VIFs) to the same VPC on both Direct Connect connections, and use BGP for load balancing

Answer: A

NEW QUESTION 70
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. Use an Amazon Route 53 multivalue answer routing policy to route older client traffic to the on-premises application version and the rest of the traffic to the new AWS based version.
B. Use a Classic Load Balancer for the new applicatio
C. Route all traffic to the new application by using an Elastic Load Balancing (ELB) load balancer DN
D. Define a user-agent-based rule on the backend servers to redirect earlier clients to the on-premises application.
E. Use an Application Load Balancer for the new applicatio
F. Register both the new and earlier applications as separate target groups and use path-based routing to route traffic based on the application version.
G. Use an Application Load Balancer for the new applicatio
H. Register both the new and earlier application backends as separate target group
I. Use header-based routing to route traffic based on the application version.

Answer: D

NEW QUESTION 75
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 77
A Network Engineer needs to be automatically notified when a certain TCP port is accessed on a fleet of Amazon EC2 instances running in an Amazon VPC.
Which of the following is the MOST reliable solution?

A. Create an inbound rule in the VPC's network ACL that matches the TCP por
B. Create an Amazon CloudWatch alarm on the NetworkPackets metric for the ACL that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
C. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to notify the Administrator with Amazon SNS each time the TCP port is accessed.
D. Create VPC Flow Logs that write to Amazon CloudWatch Logs, with a metric filter matching connections on the required por
E. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
F. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to publish to a custom Amazon CloudWatch metric each time the TCP port is accesse
G. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

Answer: A

NEW QUESTION 80
A corporate network routing table contains 624 individual RFC 1918 and public IP prefixes. You have two AWS Direct Connect connectors. You congure a private

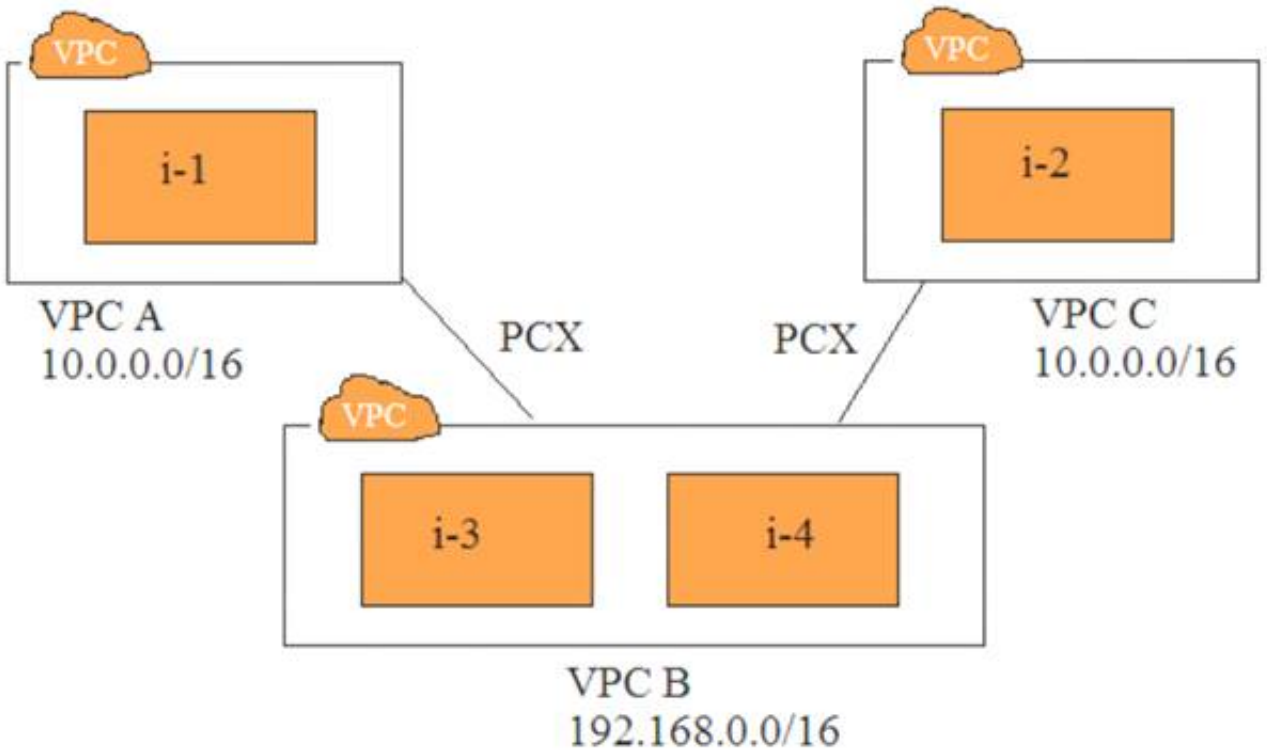
virtual interface on both connections to a virtual private gateway. The virtual private gateway is not currently attached to a VPC. Neither BGP session will maintain the Established state on the customer router. The AWS Management Console reports the private virtual interfaces as Down.
What could you do to address the problem so that the AWS Management Console reports the private virtual interface as Available?

A. Attach the virtual private gateway to a VPC and enable route propagation.
B. Filter the public IP prexes on the corporate network from the private virtual interface.
C. Change the BGP advertisements from the corporate network to only be a default route.
D. Attach the second virtual interface to an alternative virtual private gateway.

Answer: C

Explanation:
https://aws.amazon.com/es/premiumsupport/knowledge-center/virtual-interface-bgp-down/

NEW QUESTION 81
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 86
You use a VPN to extend your corporate network into a VPC. Instances in the VPC are able to resolve resource records in an Amazon Route 53 private hosted zone. Your on-premises DNS server is configured with a forwarder to the VPC DNS server IP address. On-premises users are unable to resolve names in the private hosted zone, although instances in a peered VPC can.
What should you do to provide on-premises users with access to the private hosted zone?

A. Create a proxy resolver within the VP
B. Point the on-premises forwarder to the proxy resolver.
C. Modify the network access control list on the VPC to allow DNS queries from on-premises systems.
D. Configure the on-premises server as a secondary DNS for the private zon
E. Update the NS records.
F. Update the on-premises forwarders with the four name servers assigned to the private hosted zone.

Answer: A

Explanation:
References:
https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-b

NEW QUESTION 88
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 92
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 94
A Network Engineer is designing a new system on AWS that will take advantage of Amazon CloudFront for both content caching and for protecting the underlying origin. There is concern that an external agency might be able to access the IP addresses for the application’s origin and then attack the origin despite it being served by CloudFront. Which of the following solutions provides the strongest level of protection to the origin?

A. Use an IP whitelist rule in AWS WAF within CloudFront to ensure that only known-client IPs are able to access the application.
B. Configure CloudFront to use a custom header and configure an AWS WAF rule on the origin’s Application Load Balancer to accept only traffic that contains that header.
C. Configure an AWS Lambda@Edge function to validate that the traffic to the Application Load Balancer originates from CloudFront.
D. Attach an origin access identity to the CloudFront origin that allows traffic to the origin that originates from only CloudFront.

Answer: B

NEW QUESTION 98
A legacy, on-premises web application cannot be load balances effectively. There are both planned and unplanned events that cause usage spikes to millions of concurrent users. The existing infrastructure cannot handle the usage spikes. The CIO has mandated that the application be moved to the cloud to avoid further disruptions, with the additional requirement that source IP addresses be unaltered to support network traffic-monitoring needs. Which of the following designs will meet these requirements?

A. Use an Auto Scaling group of Amazon EC2 instances behind a Classic Load Balancer.
B. Use an Auto Scaling group of EC2 instances in a target group behind an Application Load Balancer.
C. Use an Auto Scaling group of EC2 instances in a target group behind a Classic Load Balancer.
D. Use an Auto Scaling group of EC2 instances in a target group behind a Network Load Balancer.

Answer: D

Explanation:
NLBs are highly scalable AND also preserve the source IP address. https://aws.amazon.com/elasticloadbalancing/features/

NEW QUESTION 99
A space exploration company owns a series of telescopes that capture a large number of images and data of the night sky. The images and data are processed on an application hosted on AWS Fargate in a target group assigned to an Application Load Balancer (ALB). The application is made available through the address https:/'space example com
Scientists require another custom-built application hosted on several Amazon EC2 instances within an Auto Scaling group. This application will be made available from the address https://space.example.com/meteor. The company needs a solution that can automatically scale from a small number of requests overnight to a large number of requests for a future meteor shower.
What is the MOST operationally efficient solution that meets these requirements?

A. Update the existing target group with the new EC2 instance
B. Update the application's ALB by adding a listener rule that redirects /meteor to the newly added EC2 instances.
C. Create a new target grou
D. Configure the Auto Scaling group of the EC2 instances to use the target group Update the ALB by adding a listener rule that redirects /meteor to the new target group.

E. Create a Network Load Balancer (NLB). Configure the NLB to listen on two port
F. Configure a target group for one port to deliver all IP traffic to the Auto Scaling group to process the custom image
G. Configure a target group for the second port to deliver all IP traffic to Fargate Use path-based routing in the ALB to route traffic for the URL prefix /meteor to the first target grou
H. Route all other paths to the second target group.
I. Place the ALB behind an Amazon CloudFront distributio
J. Create a Lambda@Edge function that parses the request URI and adds the path-pattern header with the IP addresses of the EC2 instances to any request for /meteo
K. Add a listener rule to the ALB that looks for the HTTP header and uses the IP addresses of the EC2 instances to forward the traffic.

Answer: A

NEW QUESTION 101
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*? (Select 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: CE

NEW QUESTION 103
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 106
A company's network engineer needs to evaluate and monitor DNS traffic The company uses Amazon Route 53 as the DNS service for its public hosted zone All DNS queries must be captured for future analysis.
What should the network engineer do to meet these requirements?

A. Use AWS WAF to log information to Amazon CloudWatch Logs about the queries that Route 53 receives
B. Use VPC Flow Logs to log information to Amazon CloudWatch Logs Insights about the queries that Route 53 receives
C. Use Route 53 query logging to log information to Amazon CloudWatch Logs about the queries that Route 53 receives
D. Use AWS CloudTrail to log information to Amazon CloudWatch Logs Insights about the queries that Route 53 receives

Answer: A

NEW QUESTION 109
Your organization has a newly installed 1-Gbps AWS Direct Connect connection. You order the cross-connect from the Direct Connect location provider to the port on your router in the same facility. To enable the use of your first virtual interface, your router must be configured appropriately.
What are the minimum requirements for your router?

A. 1-Gbps Multi Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
B. 1-Gbps Single Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
C. IPsec Parameters, Pre-Shared key, Peer IP Address, BGP Session with MD5
D. BGP Session with MD5, 802.1Q VLAN, Route-Map, Prefix List, IPsec encrypted GRE Tunnel

Answer: B

NEW QUESTION 112
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 113
Your organization needs to resolve DNS entries stored in an Amazon Route 53 private zone “awscloud:internal” from the corporate network. An AWS Direct Connect connection with a private virtual interface is configured to provide access to a VPC with the CIDR block 192.168.0.0/16. A DNS Resolver (BIND) is configured on an Amazon Elastic Compute Cloud (EC2) instance with the IP address 192.168.10.5 within the VPC. The DNS Resolver has standard root server hints configured and conditional forwarding for “awscloud.internal” to the IP address 192.168.0.2.
From your PC on the corporate network, you query the DNS server at 192.168.10.5 for www.amazon.com. The query is successful and returns the appropriate response. When you query for “server.awscloud.internal”, the query times out. You receive no response.
How should you enable successful queries for “server.awscloud.internal”?

A. Attach an internet gateway to the VPC and create a default route.
B. Configure the VPC settings for enableDnsHostnames and enableDnsSupport as True
C. Relocate the BIND DNS Resolver to the corporate network.
D. Update the security group for the EC2 instance at 192.168.10.5 to allow UDP Port 53 outbound.

Answer: B

NEW QUESTION 116
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 120
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 125
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-networks-and-aws-u

NEW QUESTION 129
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 133
You are configuring a virtual interface for access to your VPC on a newly provisioned 1-Gbps AWS Direct Connect connection. Which two configuration values do you need to provide? (Select two.)

A. Public AS number
B. VLAN ID
C. IP prefixes to advertise
D. Direct Connect location
E. Virtual private gateway

Answer: BE

Explanation:
References: https://aws.amazon.com/directconnect/faqs/

NEW QUESTION 135
You are moving a two-tier application into an Amazon VPC. An Elastic Load Balancing (ELB) load balancer is configured in front of the application tier. The application tier is driven through RESTful interfaces. The data tier uses relational database service (RDS) MySQL. Company policy requires end-to-end encryption of all data in transit. in front
What ELB configuration complies with the corporate encryption policy?

A. Configure the ELB load balancer protocol as HTT
B. Configure the application instances for SSL terminatio
C. Configure Amazon RDS for SSL, and use REQUIRE SSL grants.
D. Configure the ELB protocols in TCP mod
E. Configure the application instances for SSL termination.Configure Amazon RDS for SSL, and use REQUIRE SSL grants.
F. Configure the ELB load balancer protocol as HTTP
G. Offload application instance encryption to the load balance
H. Install your SSL certificate on Amazon RDS, and configure SSL.
I. Configure the ELB protocols in SSL mod
J. Offload application instance encryption to the load balancer.Install your SSL/TLS certificate on Amazon RDS, and configure SSL.

Answer: B

Explanation:
Refer: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html

NEW QUESTION 136
A Network Engineer is provisioning a subnet for a load balancer that will sit in front of a fleet of application servers in a private subnet. There is limited IP space left in the VPC CIDR. The application has few users now but is expected to grow quickly to millions of users.
What design will use the LEAST amount of IP space, while allowing for this growth?

A. Use two /29 subnets for an Application Load Balancer in different Availability Zones.
B. Use one /29 subnet for the Network Load Balance
C. Add another VPC CIDR to the VPC to allow for future growth.
D. Use two /28 subnets for a Network Load Balancer in different Availability Zones.
E. Use one /28 subnet for an Application Load Balance
F. Add another VPC CIDR to the VPC to allow for future growth.

Answer: C

NEW QUESTION 141
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 146
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 150
.....

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