Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 1
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is planning to create a service that requires encryption in transit. The traffic must not be decrypted between the client and the backend of the service. The company will implement the service by using the gRPC protocol over TCP port 443. The service will scale up to thousands of simultaneous connections. The backend of the service will be hosted on an Amazon Elastic Kubernetes Service (Amazon EKS) duster with the Kubernetes Cluster Autoscaler and the Horizontal Pod Autoscaler configured. The company needs to use mutual TLS for two-way authentication between the client and the backend.
Which solution will meet these requirements?

A. Install the AWS Load Balancer Controller for Kubernetes. Using that controller, configure a Network Load Balancer with a TCP listener on port 443 to forward traffic to the IP addresses of the backend service Pods.

B. Install the AWS Load Balancer Controller for Kubernetes. Using that controller, configure an Application Load Balancer with an HTTPS listener on port 443 to forward traffic to the IP addresses of the backend service Pods.

C. Create a target group. Add the EKS managed node group's Auto Scaling group as a target Create an Application Load Balancer with an HTTPS listener on port 443 to forward traffic to the target group.

D. Create a target group. Add the EKS managed node group's Auto Scaling group as a target. Create a Network Load Balancer with a TLS listener on port 443 to forward traffic to the target group.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 2

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is deploying a new application in the AWS Cloud. The company wants a highly available web server that will sit behind an Elastic Load Balancer. The load balancer will route requests to multiple target groups based on the URL in the request. All traffic must use HTTPS. TLS processing must be offloaded to the load balancer. The web server must know the user's IP address so that the company can keep accurate logs for security purposes.
Which solution will meet these requirements?

A. Deploy an Application Load Balancer with an HTTPS listener. Use path-based routing rules to forward the traffic to the correct target group. Include the X-Forwarded-For request header with traffic to the targets.

B. Deploy an Application Load Balancer with an HTTPS listener for each domain. Use host-based routing rules to forward the traffic to the correct target group for each domain. Include the X-Forwarded-For request header with traffic to the targets.

C. Deploy a Network Load Balancer with a TLS listener. Use path-based routing rules to forward the traffic to the correct target group. Configure client IP address preservation for traffic to the targets.

D. Deploy a Network Load Balancer with a TLS listener for each domain. Use host-based routing rules to forward the traffic to the correct target group for each domain. Configure client IP address preservation for traffic to the targets.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 3
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has developed an application on AWS that will track inventory levels of vending machines and initiate the restocking process automatically. The company plans to integrate this application with vending machines and deploy the vending machines in several markets around the world. The application resides in a VPC in the us-east-1 Region. The application consists of an Amazon Elastic Container Service (Amazon ECS) cluster behind an Application Load Balancer (ALB). The communication from the vending machines to the application happens over HTTPS.
The company is planning to use an AWS Global Accelerator accelerator and configure static IP addresses of the accelerator in the vending machines for application endpoint access. The application must be accessible only through the accelerator and not through a direct connection over the internet to the ALB endpoint.
Which solution will meet these requirements?

A. Configure the ALB in a private subnet of the VPC. Attach an internet gateway without adding routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the internet on the ALB listener port.

B. Configure the ALB in a private subnet of the VPC. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the internet on the ALB listener port.

C. Configure the ALB in a public subnet of the VPAttach an internet gateway. Add routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port.

D. Configure the ALB in a private subnet of the VPC. Attach an internet gateway. Add routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 4
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A global delivery company is modernizing its fleet management system. The company has several business units. Each business unit designs and maintains applications that are hosted in its own AWS account in separate application VPCs in the same AWS Region. Each business unit's applications are designed to get data from a central shared services VPC.
The company wants the network connectivity architecture to provide granular security controls. The architecture also must be able to scale as more business units consume data from the central shared services VPC in the future.
Which solution will meet these requirements in the MOST secure manner?

A. Create a central transit gateway. Create a VPC attachment to each application VPC. Provide full mesh connectivity between all the VPCs by using the transit gateway.

B. Create VPC peering connections between the central shared services VPC and each application VPC in each business unit's AWS account.

C. Create VPC endpoint services powered by AWS PrivateLink in the central shared services VPCreate VPC endpoints in each application VPC.

D. Create a central transit VPC with a VPN appliance from AWS Marketplace. Create a VPN attachment from each VPC to the transit VPC. Provide full mesh connectivity among all the VPCs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 5
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company uses a 4 Gbps AWS Direct Connect dedicated connection with a link aggregation group (LAG) bundle to connect to five VPCs that are deployed in the us-east-1 Region. Each VPC serves a different business unit and uses its own private VIF for connectivity to the on-premises environment. Users are reporting slowness when they access resources that are hosted on AWS.
A network engineer finds that there are sudden increases in throughput and that the Direct Connect connection becomes saturated at the same time for about an hour each business day. The company wants to know which business unit is causing the sudden increase in throughput. The network engineer must find out this information and implement a solution to resolve the problem.
Which solution will meet these requirements?

A. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Create a new 10 Gbps dedicated connection. Shift traffic from the existing dedicated connection to the new dedicated connection.

B. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Upgrade the bandwidth of the existing dedicated connection to 10 Gbps.

C. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Upgrade the existing dedicated connection to a 5 Gbps hosted connection.

D. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Create a new 10 Gbps dedicated connection. Shift traffic from the existing dedicated connection to the new dedicated connection.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 6
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A software-as-a-service (SaaS) provider hosts its solution on Amazon EC2 instances within a VPC in the AWS Cloud. All of the provider's customers also have their environments in the AWS Cloud.
A recent design meeting revealed that the customers have IP address overlap with the provider's AWS deployment. The customers have stated that they will not share their internal IP addresses and that they do not want to connect to the provider's SaaS service over the internet.
Which combination of steps is part of a solution that meets these requirements? (Choose two.)

A. Deploy the SaaS service endpoint behind a Network Load Balancer.

B. Configure an endpoint service, and grant the customers permission to create a connection to the endpoint service.

C. Deploy the SaaS service endpoint behind an Application Load Balancer.

D. Configure a VPC peering connection to the customer VPCs. Route traffic through NAT gateways.

E. Deploy an AWS Transit Gateway, and connect the SaaS VPC to it. Share the transit gateway with the customers. Configure routing on the transit gateway.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 7
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer is designing the architecture for a healthcare company's workload that is moving to the AWS Cloud. All data to and from the on-premises environment must be encrypted in transit. All traffic also must be inspected in the cloud before the traffic is allowed to leave the cloud and travel to the on-premises environment or to the internet.
The company will expose components of the workload to the internet so that patients can reserve appointments. The architecture must secure these components and protect them against DDoS attacks. The architecture also must provide protection against financial liability for services that scale out during a DDoS event.
Which combination of steps should the network engineer take to meet all these requirements for the workload? (Choose three.)

A. Use Traffic Mirroring to copy all traffic to a fleet of traffic capture appliances.

B. Set up AWS WAF on all network components.

C. Configure an AWS Lambda function to create Deny rules in security groups to block malicious IP addresses.

D. Use AWS Direct Connect with MACsec support for connectivity to the cloud.

E. Use Gateway Load Balancers to insert third-party firewalls for inline traffic inspection.

F. Configure AWS Shield Advanced and ensure that it is configured on all public assets.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 8
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A retail company is running its service on AWS. The company's architecture includes Application Load Balancers (ALBs) in public subnets. The ALB target groups are configured to send traffic to backend Amazon EC2 instances in private subnets. These backend EC2 instances can call externally hosted services over the internet by using a NAT gateway.
The company has noticed in its billing that NAT gateway usage has increased significantly. A network engineer needs to find out the source of this increased usage.
Which options can the network engineer use to investigate the traffic through the NAT gateway? (Choose two.)

A. Enable VPC flow logs on the NAT gateway's elastic network interface. Publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query and analyze the logs.

B. Enable NAT gateway access logs. Publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query and analyze the logs.

C. Configure Traffic Mirroring on the NAT gateway's elastic network interface. Send the traffic to an additional EC2 instance. Use tools such as tcpdump and Wireshark to query and analyze the mirrored traffic.

D. Enable VPC flow logs on the NAT gateway's elastic network interface. Publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure. Use Athena to query and analyze the logs.

E. Enable NAT gateway access logs. Publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure. Use Athena to query and analyze the logs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 9
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A banking company is successfully operating its public mobile banking stack on AWS. The mobile banking stack is deployed in a VPC that includes private subnets and public subnets. The company is using IPv4 networking and has not deployed or supported IPv6 in the environment. The company has decided to adopt a third-party service provider's API and must integrate the API with the existing environment. The service provider's API requires the use of IPv6.
A network engineer must turn on IPv6 connectivity for the existing workload that is deployed in a private subnet. The company does not want to permit IPv6 traffic from the public internet and mandates that the company's servers must initiate all IPv6 connectivity. The network engineer turns on IPv6 in the VPC and in the private subnets.
Which solution will meet these requirements?

A. Create an internet gateway and a NAT gateway in the VPC. Add a route to the existing subnet route tables to point IPv6 traffic to the NAT gateway.

B. Create an internet gateway and a NAT instance in the VPC. Add a route to the existing subnet route tables to point IPv6 traffic to the NAT instance.

C. Create an egress-only Internet gateway in the VPAdd a route to the existing subnet route tables to point IPv6 traffic to the egress-only internet gateway.

D. Create an egress-only internet gateway in the VPC. Configure a security group that denies all inbound traffic. Associate the security group with the egress-only internet gateway.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 10
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed an AWS Network Firewall firewall into a VPC. A network engineer needs to implement a solution to deliver Network Firewall flow logs to the company's Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster in the shortest possible time.
Which solution will meet these requirements?

A. Create an Amazon S3 bucket. Create an AWS Lambda function to load logs into the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Enable Amazon Simple Notification Service (Amazon SNS) notifications on the S3 bucket to invoke the Lambda function. Configure flow logs for the firewall. Set the S3 bucket as the destination.

B. Create an Amazon Kinesis Data Firehose delivery stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination. Configure flow logs for the firewall Set the Kinesis Data Firehose delivery stream as the destination for the Network Firewall flow logs.

C. Configure flow logs for the firewall. Set the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination for the Network Firewall flow logs.

D. Create an Amazon Kinesis data stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination. Configure flow logs for the firewall. Set the Kinesis data stream as the destination for the Network Firewall flow logs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 11
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is using custom DNS servers that run BIND for name resolution in its VPCs. The VPCs are deployed across multiple AWS accounts that are part of the same organization in AWS Organizations. All the VPCs are connected to a transit gateway. The BIND servers are running in a central VPC and are configured to forward all queries for an on-premises DNS domain to DNS servers that are hosted in an on-premises data center. To ensure that all the VPCs use the custom DNS servers, a network engineer has configured a VPC DHCP options set in all the VPCs that specifies the custom DNS servers to be used as domain name servers. Multiple development teams in the company want to use Amazon Elastic File System (Amazon EFS). A development team has created a new EFS file system but cannot mount the file system to one of its Amazon EC2 instances. The network engineer discovers that the EC2 instance cannot resolve the IP address for the EFS mount point fs-33444567d.efs.us-east-1.amazonaws.com. The network engineer needs to implement a solution so that development teams throughout the organization can mount EFS file systems.
Which combination of steps will meet these requirements? (Choose two.)

A. Configure the BIND DNS servers in the central VPC to forward queries for efs.us-east-1.amazonaws.com to the Amazon provided DNS server (169.254.169.253).

B. Create an Amazon Route 53 Resolver outbound endpoint in the central VPC. Update all the VPC DHCP options sets to use AmazonProvidedDNS for name resolution.

C. Create an Amazon Route 53 Resolver inbound endpoint in the central VPUpdate all the VPC DHCP options sets to use the Route 53 Resolver inbound endpoint in the central VPC for name resolution.

D. Create an Amazon Route 53 Resolver rule to forward queries for the on-premises domain to the on-premises DNS servers. Share the rule with the organization by using AWS Resource Access Manager (AWS RAM). Associate the rule with all the VPCs.

E. Create an Amazon Route 53 private hosted zone for the efs.us-east-1.amazonaws.com domain. Associate the private hosted zone with the VPC where the EC2 instance is deployed. Create an A record for fs-33444567d.efs.us-east-1.amazonaws.com in the private hosted zone. Configure the A record to return the mount target of the EFS mount point.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 12
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

An ecommerce company is hosting a web application on Amazon EC2 instances to handle continuously changing customer demand. The EC2 instances are part of an Auto Scaling group. The company wants to implement a solution to distribute traffic from customers to the EC2 instances. The company must encrypt all traffic at all stages between the customers and the application servers. No decryption at intermediate points is allowed.
Which solution will meet these requirements?

A. Create an Application Load Balancer (ALB). Add an HTTPS listener to the ALB. Configure the Auto Scaling group to register instances with the ALB's target group.

B. Create an Amazon CloudFront distribution. Configure the distribution with a custom SSL/TLS certificate. Set the Auto Scaling group as the distribution's origin.

C. Create a Network Load Balancer (NLB). Add a TCP listener to the NLB. Configure the Auto Scaling group to register instances with the NLB's target group.

D. Create a Gateway Load Balancer (GLB). Configure the Auto Scaling group to register instances with the GLB's target group.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 13
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has two on-premises data center locations. There is a company-managed router at each 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 for 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.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 14
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has expanded its network to the AWS Cloud by using a hybrid architecture with multiple AWS accounts. The company has set up a shared AWS account for the connection to its on-premises data centers and the company offices. The workloads consist of private web-based services for internal use. These services run in different AWS accounts. Office-based employees consume these services by using a DNS name in an on-premises DNS zone that is named example.internal.
The process to register a new service that runs on AWS requires a manual and complicated change request to the internal DNS. The process involves many teams. The company wants to update the DNS registration process by giving the service creators access that will allow them to register their DNS records. A network engineer must design a solution that will achieve this goal. The solution must maximize cost-effectiveness and must require the least possible number of configuration changes.
Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Create a record for each service in its local private hosted zone (serviceA.account1.aws.example.internal). Provide this DNS record to the employees who need access.

B. Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint's IP addresses that were created.

C. Create an Amazon Route 53 Resolver rule to forward any queries made to onprem.example.internal to the on-premises DNS servers.

D. Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for this domain.

E. Launch two Amazon EC2 instances in the shared AWS account. Install BIND on each instance. Create a DNS conditional forwarder on each BIND server to forward queries for each subdomain under aws.example.internal to the appropriate private hosted zone in each AWS account. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the IP addresses of the BIND servers.

F. Create a private hosted zone in the shared AWS account for each account that runs the service. Configure the private hosted zone to contain aws.example.internal in the domain (account1.aws.example.internal). Associate the private hosted zone with the VPC that runs the service and the shared account VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 15
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has multiple AWS accounts. Each account contains one or more VPCs. A new security guideline requires the inspection of all traffic between VPCs.
The company has deployed a transit gateway that provides connectivity between all VPCs. The company also has deployed a shared services VPC with Amazon EC2 instances that include IDS services for stateful inspection. The EC2 instances are deployed across three Availability Zones. The company has set up VPC associations and routing on the transit gateway. The company has migrated a few test VPCs to the new solution for traffic inspection.
Soon after the configuration of routing, the company receives reports of intermittent connections for traffic that crosses Availability Zones.
What should a network engineer do to resolve this issue?

A. Modify the transit gateway VPC attachment on the shared services VPC by enabling cross-Availability Zone load balancing.

B. Modify the transit gateway VPC attachment on the shared services VPC by enabling appliance mode support.

C. Modify the transit gateway by selecting VPN equal-cost multi-path (ECMP) routing support.

D. Modify the transit gateway by selecting multicast support.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 16
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is using a NAT gateway to allow internet connectivity for private subnets in a VPC in the us-west-2 Region. After a security audit, the company needs to remove the NAT gateway.
In the private subnets, the company has resources that use the unified Amazon CloudWatch agent. A network engineer must create a solution to ensure that the unified CloudWatch agent continues to work after the removal of the NAT gateway.
Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Validate that private DNS is enabled on the VPC by setting the enableDnsHostnames VPC attribute and the enableDnsSupport VPC attribute to true.

B. Create a new security group with an entry to allow outbound traffic that uses the TCP protocol on port 443 to destination 0.0.0.0/0

C. Create a new security group with entries to allow inbound traffic that uses the TCP protocol on port 443 from the IP prefixes of the private subnets.

D. Create the following interface VPC endpoints in the VPC: com.amazonaws.us-west-2.logs and com.amazonaws.us-west-2.monitoring. Associate the new security group with the endpoint network interfaces.

E. Create the following interface VPC endpoint in the VPC: com.amazonaws.us-west-2.cloudwatch. Associate the new security group with the endpoint network interfaces.

F. Associate the VPC endpoint or endpoints with route tables that the private subnets use.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 17
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

An international company provides early warning about tsunamis. The company plans to use IoT devices to monitor sea waves around the world. The data that is collected by the IoT devices must reach the company's infrastructure on AWS as quickly as possible. The company is using three operation centers around the world. Each operation center is connected to AWS through Its own AWS Direct Connect connection. Each operation center is connected to the internet through at least two upstream internet service providers.
The company has its own provider-independent (PI) address space. The IoT devices use TCP protocols for reliable transmission of the data they collect. The IoT devices have both landline and mobile internet connectivity. The infrastructure and the solution will be deployed in multiple AWS Regions. The company will use Amazon Route 53 for DNS services.
A network engineer needs to design connectivity between the IoT devices and the services that run in the AWS Cloud.
Which solution will meet these requirements with the HIGHEST availability?

A. Set up an Amazon CloudFront distribution with origin failover. Create an origin group for each Region where the solution is deployed.

B. Set up Route 53 latency-based routing. Add latency alias records. For the latency alias records, set the value of Evaluate Target Health to Yes.

C. Set up an accelerator in AWS Global Accelerator. Configure Regional endpoint groups and health checks.

D. Set up Bring Your Own IP (BYOIP) addresses. Use the same PI addresses for each Region where the solution is deployed.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 18

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is planning a migration of its critical workloads from an on-premises data center to Amazon EC2 instances. The plan includes a new 10 Gbps AWS Direct Connect dedicated connection from the on-premises data center to a VPC that is attached to a transit gateway. The migration must occur over encrypted paths between the on-premises data center and the AWS Cloud.

Which solution will meet these requirements while providing the HIGHEST throughput?

A. Configure a public VIF on the Direct Connect connection. Configure an AWS Site-to-Site VPN connection to the transit gateway as a VPN attachment.

B. Configure a transit VIF on the Direct Connect connection. Configure an IPsec VPN connection to an EC2 instance that is running third-party VPN software.

C. Configure MACsec for the Direct Connect connection. Configure a transit VIF to a Direct Connect gateway that is associated with the transit gateway.

D. Configure a public VIF on the Direct Connect connection. Configure two AWS Site-to-Site VPN connections to the transit gateway. Enable equal-cost multi-path (ECMP) routing.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 19

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer must develop an AWS CloudFormation template that can create a virtual private gateway, a customer gateway, a VPN connection, and static routes in a route table. During testing of the template, the network engineer notes that the CloudFormation template has encountered an error and is rolling back. What should the network engineer do to resolve the error?

A. Change the order of resource creation in the CloudFormation template.

B. Add the DependsOn attribute to the resource declaration for the virtual private gateway. Specify the route table entry resource.

C. Add a wait condition in the template to wait for the creation of the virtual private gateway.

D. Add the DependsOn attribute to the resource declaration for the route table entry. Specify the virtual private gateway resource.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 20
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company operates its IT services through a multi-site hybrid infrastructure. The company deploys resources on AWS in the us-east-1 Region and in the eu-west-2 Region. The company also deploys resources in its own data centers that are located in the United States (US) and in the United Kingdom (UK). In both AWS Regions, the company uses a transit gateway to connect 15 VPCs to each other. The company has created a transit gateway peering connection between the two transit gateways. The VPC CIDR blocks do not overlap with each other or with IP addresses used within the data centers. The VPC CIDR prefixes can also be aggregated either on a Regional level or for the company's entire AWS environment.
The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through Interior BGP (iBGP) sessions. The data centers maintain connectivity to AWS through one AWS Direct Connect connection in the US and one Direct Connect connection in the UK. Each Direct Connect connection is terminated on a Direct Connect gateway and is associated with a local transit gateway through a transit VIF.
Traffic follows the shortest geographical path from source to destination. For example, packets from the UK data center that are targeted to resources in eu-west-2 travel across the local Direct Connect connection. In cases of cross-Region data transfers, such as from the UK data center to VPCs in us-east-1, the private WAN connection must be used to minimize costs on AWS. A network engineer has configured each transit gateway association on the Direct Connect gateway to advertise VPC-specific CIDR IP prefixes only from the local Region. The routes toward the other Region must be learned through BGP from the routers in the other data center in the original, non-aggregated form.
The company recently experienced a problem with cross-Region data transfers because of issues with its private WAN connection. The network engineer needs to modify the routing setup to prevent similar interruptions in the future. The solution cannot modify the original traffic routing goal when the network is operating normally.
Which modifications will meet these requirements? (Choose two.)

A. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add the company's entire AWS environment aggregate route to the list of subnets advertised through the local Direct Connect connection.

B. Add the CIDR prefixes from the other Region VPCs and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection. Configure data center routers to make routing decisions based on the BGP communities received.

C. Add the aggregate IP prefix for the other Region and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection.

D. Add the aggregate IP prefix for the company's entire AWS environment and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection.

E. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add both Regional aggregate IP prefixes to the list of subnets advertised through the Direct Connect connection on both sides of the network. Configure data center routers to make routing decisions based on the BGP communities received.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 21

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's network engineer needs to design a new solution to help troubleshoot and detect network anomalies. The network engineer has configured Traffic Mirroring. However, the mirrored traffic is overwhelming the Amazon EC2 instance that is the traffic mirror target. The EC2 instance hosts tools that the company's security team uses to analyze the traffic. The network engineer needs to design a highly available solution that can scale to meet the demand of the mirrored traffic. Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) as the traffic mirror target. Behind the NLB. deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring as necessary.

B. Deploy an Application Load Balancer (ALB) as the traffic mirror target. Behind the ALB, deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring only during non-business hours.

C. Deploy a Gateway Load Balancer (GLB) as the traffic mirror target. Behind the GLB. deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring as necessary.

D. Deploy an Application Load Balancer (ALB) with an HTTPS listener as the traffic mirror target. Behind the ALB. deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring only during active events or business hours.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 22
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company uses a hybrid architecture and has an AWS Direct Connect connection between its on-premises data center and AWS. The company has production applications that run in the on-premises data center. The company also has production applications that run in a VPC. The applications that run in the on-premises data center need to communicate with the applications that run in the VPC. The company is using corp.example.com as the domain name for the on-premises resources and is using an Amazon Route 53 private hosted zone for aws.example.com to host the VPC resources.
The company is using an open-source recursive DNS resolver in a VPC subnet and is using a DNS resolver in the on-premises data center. The company's on-premises DNS resolver has a forwarder that directs requests for the aws.example.com domain name to the DNS resolver in the VPC. The DNS resolver in the VPC has a forwarder that directs requests for the corp.example.com domain name to the DNS resolver in the on-premises data center. The company has deckled to replace the open-source recursive DNS resolver with Amazon Route 53 Resolver endpoints.
Which combination of steps should a network engineer take to make this replacement? (Choose three.)

A. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the outbound endpoint.

B. Configure the on-premises DNS resolver to forward aws.example.com domain queries to the IP addresses of the inbound endpoint.

C. Create a Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint.

D. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the inbound endpoint.

E. Create a Route 53 Resolver rule to forward corp.example.com domain queries to the IP address of the on-premises DNS resolver.

F. Configure the on-premises DNS resolver to forward aws.example.com queries to the IP addresses of the outbound endpoint.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 23
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A government contractor is designing a multi-account environment with multiple VPCs for a customer. A network security policy requires all traffic between any two VPCs to be transparently inspected by a third-party appliance.
The customer wants a solution that features AWS Transit Gateway. The setup must be highly available across multiple Availability Zones, and the solution needs to support automated failover. Furthermore, asymmetric routing is not supported by the inspection appliances.
Which combination of steps is part of a solution that meets these requirements? (Choose two.)

A. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. Connect the inspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the target group. Create a Network Load Balancer (NLB), and set it up to forward to the newly created target group. Configure a default route in the inspection VPCs transit gateway subnet toward the NLB.

B. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. Connect the inspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the target group. Create a Gateway Load Balancer, and set it up to forward to the newly created target group. Configure a default route in the inspection VPC's transit gateway subnet toward the Gateway Load Balancer endpoint.

C. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs. Associate the other route table with the inspection VPC's attachment. Propagate all VPC attachments into the inspection route table. Define a static default route in the application route table. Enable appliance mode on the attachment that connects the inspection VPC.

D. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs. Associate the other route table with the inspection VPCs attachment. Propagate all VPC attachments into the application route table. Define a static default route in the inspection route table. Enable appliance mode on the attachment that connects the inspection VPC.

E. Configure one route table on the transit gateway. Associate the route table with all the VPCs. Propagate all VPC attachments into the route table. Define a static default route in the route table.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 24
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed Amazon EC2 instances in private subnets in a VPC. The EC2 instances must initiate any requests that leave the VPC, including requests to the company's on-premises data center over an AWS Direct Connect connection. No resources outside the VPC can be allowed to open communications directly to the EC2 instances.
The on-premises data center's customer gateway is configured with a stateful firewall device that filters for incoming and outgoing requests to and from multiple VPCs. In addition, the company wants to use a single IP match rule to allow all the communications from the EC2 instances to its data center from a single IP address.
Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Create a VPN connection over the Direct Connect connection by using the on-premises firewall. Use the firewall to block all traffic from on premises to AWS. Allow a stateful connection from the EC2 instances to initiate the requests.

B. Configure the on-premises firewall to filter all requests from the on-premises network to the EC2 instances. Allow a stateful connection if the EC2 instances in the VPC initiate the traffic.

C. Deploy a NAT gateway into a private subnet in the VPC where the EC2 instances are deployed. Specify the NAT gateway type as private. Configure the on-premises firewall to allow connections from the IP address that is assigned to the NAT gateway.

D. Deploy a NAT instance into a private subnet in the VPC where the EC2 instances are deployed. Configure the on-premises firewall to allow connections from the IP address that is assigned to the NAT instance.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 25
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A global company operates all its non-production environments out of three AWS Regions: eu-west-1, us-east-1, and us-west-1. The company hosts all its production workloads in two on-premises data centers. The company has 60 AWS accounts and each account has two VPCs in each Region. Each VPC has a virtual private gateway where two VPN connections terminate for resilient connectivity to the data centers. The company has 360 VPN tunnels to each data center, resulting in high management overhead. The total VPN throughput for each Region is 500 Mbps.
The company wants to migrate the production environments to AWS. The company needs a solution that will simplify the network architecture and allow for future growth. The production environments will generate an additional 2 Gbps of traffic per Region back to the data centers. This traffic will increase over time.
Which solution will meet these requirements?

A. Set up an AWS Direct Connect connection from each data center to AWS in each Region. Create and attach private VIFs to a single Direct Connect gateway. Attach the Direct Connect gateway to all the VPCs. Remove the existing VPN connections that are attached directly to the virtual private gateways.

B. Create a single transit gateway with VPN connections from each data center. Share the transit gateway with each account by using AWS Resource Access Manager (AWS RAM). Attach the transit gateway to each VPC. Remove the existing VPN connections that are attached directly to the virtual private gateways.

C. Create a transit gateway in each Region with multiple newly commissioned VPN connections from each data center. Share the transit gateways with each account by using AWS Resource Access Manager (AWS RAM). In each Region, attach the transit gateway to each VPRemove the existing VPN connections that are attached directly to the virtual private gateways.

D. Peer all the VPCs in each Region to a new VPC in each Region that will function as a centralized transit VPC. Create new VPN connections from each data center to the transit VPCs. Terminate the original VPN connections that are attached to all the original VPCs. Retain the new VPN connection to the new transit VPC in each Region.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 26
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is building its website on AWS in a single VPC. The VPC has public subnets and private subnets in two Availability Zones. The website has static content such as images. The company is using Amazon S3 to store the content.
The company has deployed a fleet of Amazon EC2 instances as web servers in a private subnet. The EC2 instances are in an Auto Scaling group behind an Application Load Balancer. The EC2 instances will serve traffic, and they must pull content from an S3 bucket to render the webpages. The company is using AWS Direct Connect with a public VIF for on-premises connectivity to the S3 bucket.
A network engineer notices that traffic between the EC2 instances and Amazon S3 is routing through a NAT gateway. As traffic increases, the company's costs are increasing. The network engineer needs to change the connectivity to reduce the NAT gateway costs that result from the traffic between the EC2 instances and Amazon S3.
Which solution will meet these requirements?

A. Create a Direct Connect private VIF. Migrate the traffic from the public VIF to the private VIF.

B. Create an AWS Site-to-Site VPN tunnel over the existing public VIF.

C. Implement interface VPC endpoints for Amazon S3. Update the VPC route table.

D. Implement gateway VPC endpoints for Amazon S3. Update the VPC route table.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 27
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company wants to improve visibility into its AWS environment. The AWS environment consists of multiple VPCs that are connected to a transit gateway. The transit gateway connects to an on-premises data center through an AWS Direct Connect gateway and a pair of redundant Direct Connect connections that use transit VIFs. The company must receive notification each time a new route is advertised to AWS from on premises over Direct Connect.
What should a network engineer do to meet these requirements?

A. Enable Amazon CloudWatch metrics on Direct Connect to track the received routes. Configure a CloudWatch alarm to send notifications when routes change.

B. Onboard Transit Gateway Network Manager to Amazon CloudWatch Logs Insights. Use Amazon EventBridge (Amazon CloudWatch Events) to send notifications when routes change.

C. Configure an AWS Lambda function to periodically check the routes on the Direct Connect gateway and to send notifications when routes change.

D. Enable Amazon CloudWatch Logs on the transit VIFs to track the received routes. Create a metric filter Set an alarm on the filter to send notifications when routes change.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 28
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A software company offers a software-as-a-service (SaaS) accounting application that is hosted in the AWS Cloud The application requires connectivity to the company's on-premises network. The company has two redundant 10 GB AWS Direct Connect connections between AWS and its on-premises network to accommodate the growing demand for the application.
The company already has encryption between its on-premises network and the colocation. The company needs to encrypt traffic between AWS and the edge routers in the colocation within the next few months. The company must maintain its current bandwidth.
What should a network engineer do to meet these requirements with the LEAST operational overhead?

A. Deploy a new public VIF with encryption on the existing Direct Connect connections. Reroute traffic through the new public VIF.

B. Create a virtual private gateway Deploy new AWS Site-to-Site VPN connections from on premises to the virtual private gateway Reroute traffic from the Direct Connect private VIF to the new VPNs.

C. Deploy a new pair of 10 GB Direct Connect connections with MACsec. Configure MACsec on the edge routers. Reroute traffic to the new Direct Connect connections. Decommission the original Direct Connect connections

D. Deploy a new pair of 10 GB Direct Connect connections with MACsec. Deploy a new public VIF on the new Direct Connect connections. Deploy two AWS Site-to-Site VPN connections on top of the new public VIF. Reroute traffic from the existing private VIF to the new Site-to-Site connections. Decommission the original Direct Connect connections.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 29

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company hosts an application on Amazon EC2 instances behind an Application Load Balancer (ALB). The company recently experienced a network security breach. A network engineer must collect and analyze logs that include the client IP address, target IP address, target port, and user agent of each user that accesses the application.

What is the MOST operationally efficient solution that meets these requirements?

A. Configure the ALB to store logs in an Amazon S3 bucket. Download the files from Amazon S3, and use a spreadsheet application to analyze the logs.

B. Configure the ALB to push logs to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Analytics to analyze the logs.

C. Configure Amazon Kinesis Data Streams to stream data from the ALB to Amazon OpenSearch Service (Amazon Elasticsearch Service). Use search operations in Amazon OpenSearch Service (Amazon Elasticsearch Service) to analyze the data.

D. Configure the ALB to store logs in an Amazon S3 bucket. Use Amazon Athena to analyze the logs in Amazon S3.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 30
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A media company is implementing a news website for a global audience. The website uses Amazon CloudFront as its content delivery network. The backend runs on Amazon EC2 Windows instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The company's customers access the website by using service example com as the CloudFront custom domain name. The CloudFront origin points to an ALB that uses service-alb.example.com as the domain name.
The company's security policy requires the traffic to be encrypted in transit at all times between the users and the backend.
Which combination of changes must the company make to meet this security requirement? (Choose three.)

A. Create a self-signed certificate for service.example.com. Import the certificate into AWS Certificate Manager (ACM). Configure CloudFront to use this imported SSL/TLS certificate. Change the default behavior to redirect HTTP to HTTPS.

B. Create a certificate for service.example.com by using AWS Certificate Manager (ACM). Configure CloudFront to use this custom SSL/TLS certificate. Change the default behavior to redirect HTTP to HTTPS.

C. Create a certificate with any domain name by using AWS Certificate Manager (ACM) for the EC2 instances. Configure the backend to use this certificate for its HTTPS listener. Specify the instance target type during the creation of a new target group that uses the HTTPS protocol for its targets. Attach the existing Auto Scaling group to this new target group.

D. Create a public certificate from a third-party certificate provider with any domain name for the EC2 instances. Configure the backend to use this certificate for its HTTPS listener. Specify the instance target type during the creation of a new target group that uses the HTTPS protocol for its targets. Attach the existing Auto Scaling group to this new target group.

E. Create a certificate for service-alb.example.com by using AWS Certificate Manager (ACM). On the ALB add a new HTTPS listener that uses the new target group and the service-alb.example.com ACM certificate. Modify the CloudFront origin to use the HTTPS protocol only. Delete the HTTP listener on the ALB.

F. Create a self-signed certificate for service-alb.example.com. Import the certificate into AWS Certificate Manager (ACM). On the ALB add a new HTTPS listener that uses the new target group and the imported service-alb.example.com ACM certificate. Modify the CloudFront origin to use the HTTPS protocol only. Delete the HTTP listener on the ALB.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 31

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is hosting an application on Amazon EC2 instances behind a Network Load Balancer (NLB). A solutions architect added EC2 instances in a second Availability Zone to improve the availability of the application. The solutions architect added the instances to the NLB target group.

The company's operations team notices that traffic is being routed only to the instances in the first Availability Zone.

What is the MOST operationally efficient solution to resolve this issue?

A. Enable the new Availability Zone on the NLB

B. Create a new NLB for the instances in the second Availability Zone

C. Enable proxy protocol on the NLB

D. Create a new target group with the instances in both Availability Zones

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 32
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer needs to set up an Amazon EC2 Auto Scaling group to run a Linux-based network appliance in a highly available architecture. The network engineer is configuring the new launch template for the Auto Scaling group.
In addition to the primary network interface the network appliance requires a second network interface that will be used exclusively by the application to exchange traffic with hosts over the internet. The company has set up a Bring Your Own IP (BYOIP) pool that includes an Elastic IP address that should be used as the public IP address for the second network interface.
How can the network engineer implement the required architecture?

A. Configure the two network interfaces in the launch template. Define the primary network interface to be created in one of the private subnets. For the second network interface, select one of the public subnets. Choose the BYOIP pool ID as the source of public IP addresses.

B. Configure the primary network interface in a private subnet in the launch template. Use the user data option to run a cloud-init script after boot to attach the second network interface from a subnet with auto-assign public IP addressing enabled.

C. Create an AWS Lambda function to run as a lifecycle hook of the Auto Scaling group when an instance is launching. In the Lambda function, assign a network interface to an AWS Global Accelerator endpoint.

D. During creation of the Auto Scaling group, select subnets for the primary network interface. Use the user data option to run a cloud-init script to allocate a second network interface and to associate an Elastic IP address from the BYOIP pool.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 33
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company delivers applications over the internet. An Amazon Route 53 public hosted zone is the authoritative DNS service for the company and its internet applications, all of which are offered from the same domain name.
A network engineer is working on a new version of one of the applications. All the application's components are hosted in the AWS Cloud. The application has a three-tier design. The front end is delivered through Amazon EC2 instances that are deployed in public subnets with Elastic IP addresses assigned. The backend components are deployed in private subnets from RFC1918.
Components of the application need to be able to access other components of the application within the application's VPC by using the same host names as the host names that are used over the public internet. The network engineer also needs to accommodate future DNS changes, such as the introduction of new host names or the retirement of DNS entries.
Which combination of steps will meet these requirements? (Choose three.)

A. Add a geoproximity routing policy in Route 53.

B. Create a Route 53 private hosted zone for the same domain name Associate the application's VPC with the new private hosted zone.

C. Enable DNS hostnames for the application's VPC.

D. Create entries in the private hosted zone for each name in the public hosted zone by using the corresponding private IP addresses.

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs when AWS CloudTrail logs a Route 53 API call to the public hosted zone. Create an AWS Lambda function as the target of the rule. Configure the function to use the event information to update the private hosted zone.

F. Add the private IP addresses in the existing Route 53 public hosted zone.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 34

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is deploying an application. The application is implemented in a series of containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The company will use the Fargate launch type for its tasks. The containers will run workloads that require connectivity initiated over an SSL connection. Traffic must be able to flow to the application from other AWS accounts over private connectivity. The application must scale in a manageable way as more consumers use the application.
Which solution will meet these requirements?

A. Choose a Gateway Load Balancer (GLB) as the type of load balancer for the ECS service. Create a lifecycle hook to add new tasks to the target group from Amazon ECS as required to handle scaling. Specify the GLB in the service definition. Create a VPC peer for external AWS accounts. Update the route tables so that the AWS accounts can reach the GLB.

B. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allow the application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPC endpoint service for the ALB Share the VPC endpoint service with other AWS accounts.

C. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allow the application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPC peer for the external AWS accounts. Update the route tables so that the AWS accounts can reach the ALB.

D. Choose a Network Load Balancer (NLB) as the type of load balancer for the ECS service. Specify the NLB in the service definition. Create a VPC endpoint service for the NLB. Share the VPC endpoint service with other AWS accounts.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 35
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's development team has created a new product recommendation web service. The web service is hosted in a VPC with a CIDR block of 192.168.224.0/19. The company has deployed the web service on Amazon EC2 instances and has configured an Auto Scaling group as the target of a Network Load Balancer (NLB).
The company wants to perform testing to determine whether users who receive product recommendations spend more money than users who do not receive product recommendations. The company has a big sales event in 5 days and needs to integrate its existing production environment with the recommendation engine by then. The existing production environment is hosted in a VPC with a CIDR block of 192.168.128 0/17.
A network engineer must integrate the systems by designing a solution that results in the least possible disruption to the existing environments.
Which solution will meet these requirements?

A. Create a VPC peering connection between the web service VPC and the existing production VPC. Add a routing rule to the appropriate route table to allow data to flow to 192.168.224.0/19 from the existing production environment and to flow to 192.168.128.0/17 from the web service environment. Configure the relevant security groups and ACLs to allow the systems to communicate.

B. Ask the development team of the web service to redeploy the web service into the production VPC and integrate the systems there.

C. Create a VPC endpoint service. Associate the VPC endpoint service with the NLB for the web service. Create an interface VPC endpoint for the web service in the existing production VPC.

D. Create a transit gateway in the existing production environment. Create attachments to the production VPC and the web service VPC. Configure appropriate routing rules in the transit gateway and VPC route tables for 192.168.224.0/19 and 192.168.128.0/17. Configure the relevant security groups and ACLs to allow the systems to communicate.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 36
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer needs to update a company's hybrid network to support IPv6 for the upcoming release of a new application. The application is hosted in a VPC in the AWS Cloud. The company's current AWS infrastructure includes VPCs that are connected by a transit gateway. The transit gateway is connected to the on-premises network by AWS Direct Connect and AWS Site-to-Site VPN. The company's on-premises devices have been updated to support the new IPv6 requirements. The company has enabled IPv6 for the existing VPC by assigning a new IPv6 CIDR block to the VPC and by assigning IPv6 to the subnets for dual-stack support. The company has launched new Amazon EC2 instances for the new application in the updated subnets.
When updating the hybrid network to support IPv6 the network engineer must avoid making any changes to the current infrastructure. The network engineer also must block direct access to the instances' new IPv6 addresses from the internet. However, the network engineer must allow outbound internet access from the instances.
What is the MOST operationally efficient solution that meets these requirements?

A. Update the Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Create a new VPN connection that supports IPv6 connectivity. Add an egress-only internet gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices

B. Update the Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Update the existing VPN connection to support IPv6 connectivity. Add an egress-only internet gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.

C. Create a Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Create a new VPN connection that supports IPv6 connectivity. Add an egress-only internet gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.

D. Create a Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Create a new VPN connection that supports IPv6 connectivity. Add a NAT gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 37

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer must provide additional safeguards to protect encrypted data at Application Load Balancers (ALBs) through the use of a unique random session key. What should the network engineer do to meet this requirement?

A. Change the ALB security policy to a policy that supports TLS 1.2 protocol only

B. Use AWS Key Management Service (AWS KMS) to encrypt session keys

C. Associate an AWS WAF web ACL with the ALBs. and create a security rule to enforce forward secrecy (FS)

D. Change the ALB security policy to a policy that supports forward secrecy (FS)

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 38
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed a software-defined WAN (SD-WAN) solution to interconnect all of its offices. The company is migrating workloads to AWS and needs to extend its SD-WAN solution to support connectivity to these workloads.
A network engineer plans to deploy AWS Transit Gateway Connect and two SD-WAN virtual appliances to provide this connectivity. According to company policies, only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time.
How should the network engineer configure routing to meet these requirements?

A. Add a static default route in the transit gateway route table to point to the secondary SD-WAN virtual appliance. Add routes that are more specific to point to the primary SD-WAN virtual appliance.

B. Configure the BGP community tag 7224:7300 on the primary SD-WAN virtual appliance for BGP routes toward the transit gateway.

C. Configure the AS_PATH prepend attribute on the secondary SD-WAN virtual appliance for BGP routes toward the transit gateway.

D. Disable equal-cost multi-path (ECMP) routing on the transit gateway for Transit Gateway Connect.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 39
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is planning to deploy many software-defined WAN (SD-WAN) sites. The company is using AWS Transit Gateway and has deployed a transit gateway in the required AWS Region. A network engineer needs to deploy the SD-WAN hub virtual appliance into a VPC that is connected to the transit gateway. The solution must support at least 5 Gbps of throughput from the SD-WAN hub virtual appliance to other VPCs that are attached to the transit gateway.
Which solution will meet these requirements?

A. Create a new VPC for the SD-WAN hub virtual appliance. Create two IPsec VPN connections between the SD-WAN hub virtual appliance and the transit gateway. Configure BGP over the IPsec VPN connections

B. Assign a new CIDR block to the transit gateway. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to the transit gateway with a VPC attachment. Add a transit gateway Connect attachment. Create a Connect peer and specify the GRE and BGP parameters. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway.

C. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to the transit gateway with a VPC attachment. Create two IPsec VPN connections between the SD-WAN hub virtual appliance and the transit gateway. Configure BGP over the IPsec VPN connections.

D. Assign a new CIDR block to the transit gateway. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to the transit gateway with a VPC attachment. Add a transit gateway Connect attachment. Create a Connect peer and specify the VXLAN and BGP parameters. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 40
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is deploying a new application on AWS. The application uses dynamic multicasting. The company has five VPCs that are all attached to a transit gateway Amazon EC2 instances in each VPC need to be able to register dynamically to receive a multicast transmission.
How should a network engineer configure the AWS resources to meet these requirements?

A. Create a static source multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address.

B. Create a static source multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.

C. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address.

D. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 41

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is creating new features for its ecommerce website. These features will use several microservices that are accessed through different paths. The microservices will run on Amazon Elastic Container Service (Amazon ECS). The company requires the use of HTTPS for all of its public websites. The application requires the customer's source IP addresses.

A network engineer must implement a load balancing strategy that meets these requirements.

Which combination of actions should the network engineer take to accomplish this goal? (Choose two.)

A. Use a Network Load Balancer

B. Retrieve client IP addresses by using the X-Forwarded-For header

C. Use AWS App Mesh load balancing

D. Retrieve client IP addresses by using the X-IP-Source header

E. Use an Application Load Balancer.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 42
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is migrating its containerized application to AWS. For the architecture the company will have an ingress VPC with a Network Load Balancer (NLB) to distribute the traffic to front-end pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The front end of the application will determine which user is requesting access and will send traffic to 1 of 10 services VPCs. Each services VPC will include an NLB that distributes traffic to the services pods in an EKS cluster. The company is concerned about overall cost. User traffic will be responsible for more than 10 TB of data transfer from the ingress VPC to services VPCs every month. A network engineer needs to recommend how to design the communication between the VPCs.
Which solution will meet these requirements at the LOWEST cost?

A. Create a transit gateway. Peer each VPC to the transit gateway. Use zonal DNS names for the NLB in the services VPCs to minimize cross-AZ traffic from the ingress VPC to the services VPCs.

B. Create an AWS PrivateLink endpoint in every Availability Zone in the ingress VPC. Each PrivateLink endpoint will point to the zonal DNS entry of the NLB in the services VPCs.

C. Create a VPC peering connection between the ingress VPC and each of the 10 services VPCs. Use zonal DNS names for the NLB in the services VPCs to minimize cross-AZ traffic from the ingress VPC to the services VPCs.

D. Create a transit gateway. Peer each VPC to the transit gateway. Turn off cross-AZ load balancing on the transit gateway. Use Regional DNS names for the NLB in the services VPCs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 43
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has stateful security appliances that are deployed to multiple Availability Zones in a centralized shared services VPC. The AWS environment includes a transit gateway that is attached to application VPCs and the shared services VPC. The application VPCs have workloads that are deployed in private subnets across multiple Availability Zones. The stateful appliances in the shared services VPC inspect all east west (VPC-to-VPC) traffic.
Users report that inter-VPC traffic to different Availability Zones is dropping. A network engineer verified this claim by issuing Internet Control Message Protocol (ICMP) pings between workloads in different Availability Zones across the application VPCs. The network engineer has ruled out security groups, stateful device configurations and network ACLs as the cause of the dropped traffic.
What is causing the traffic to drop?

A. The stateful appliances and the transit gateway attachments are deployed in a separate subnet in the shared services VPC.

B. Appliance mode is not enabled on the transit gateway attachment to the shared services VPC.

C. The stateful appliances and the transit gateway attachments are deployed in the same subnet in the shared services VPC.

D. Appliance mode is not enabled on the transit gateway attachment to the application VPCs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 44

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has hundreds of Amazon EC2 instances that are running in two production VPCs across all Availability Zones in the us-east-1 Region. The production VPCs are named

VPC A and VPC B.

A new security regulation requires all traffic between production VPCs to be inspected before the traffic is routed to its final destination. The company deploys a new shared VPC that contains a stateful firewall appliance and a transit gateway with a VPC attachment across all VPCs to route traffic between VPC A and VPC B through the firewall appliance for inspection. During testing, the company notices that the transit gateway is dropping the traffic whenever the traffic is between two Availability Zones.

What should a network engineer do to fix this issue with the LEAST management overhead?

A. In the shared VPC, replace the VPC attachment with a VPN attachment. Create a VPN tunnel between the transit gateway and the firewall appliance. Configure BGP.

B. Enable transit gateway appliance mode on the VPC attachment in VPC A and VPC B.

C. Enable transit gateway appliance mode on the VPC attachment in the shared VPC.

D. In the shared VPC, configure one VPC peering connection to VPC A and another VPC peering connection to VPC B.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 45
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed a critical application on a fleet of Amazon EC2 instances behind an Application Load Balancer. The application must always be reachable on port 443 from the public internet. The application recently had an outage that resulted from an incorrect change to the EC2 security group.
A network engineer needs to automate a way to verify the network connectivity between the public internet and the EC2 instances whenever a change is made to the security group. The solution also must notify the network engineer when the change affects the connection.
Which solution will meet these requirements?

A. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture REJECT traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for rejected traffic. Create an alarm to notify the network engineer.

B. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture all traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for all traffic. Create an alarm to notify the network engineer

C. Create a VPC Reachability Analyzer path on port 443. Specify the security group as the source. Specify the EC2 instances as the destination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connection. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fail Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security group occurs.

D. Create a VPC Reachability Analyzer path on port 443. Specify the internet gateway of the VPC as the source. Specify the EC2 instances as the destination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connection. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fail. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security group occurs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 46
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A security team is performing an audit of a company's AWS deployment. The security team is concerned that two applications might be accessing resources that should be blocked by network ACLs and security groups. The applications are deployed across two Amazon Elastic Kubernetes Service (Amazon EKS) clusters that use the Amazon VPC Container Network Interface (CNI) plugin for Kubernetes. The clusters are in separate subnets within the same VPC and have a Cluster Autoscaler configured.
The security team needs to determine which POD IP addresses are communicating with which services throughout the VPC. The security team wants to limit the number of flow logs and wants to examine the traffic from only the two applications.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create VPC flow logs in the default format. Create a filter to gather flow logs only from the EKS nodes. Include the srcaddr field and the dstaddr field in the flow logs.

B. Create VPC flow logs in a custom format. Set the EKS nodes as the resource Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.

C. Create VPC flow logs in a custom format. Set the application subnets as resources. Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.

D. Create VPC flow logs in a custom format. Create a filter to gather flow logs only from the EKS nodes. Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 47
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A data analytics company has a 100-node high performance computing (HPC) cluster. The HPC cluster is for parallel data processing and is hosted in a VPC in the AWS Cloud. As part of the data processing workflow, the HPC cluster needs to perform several DNS queries to resolve and connect to Amazon RDS databases, Amazon S3 buckets, and on-premises data stores that are accessible through AWS Direct Connect. The HPC cluster can increase in size by five to seven times during the company's peak event at the end of the year.
The company is using two Amazon EC2 instances as primary DNS servers for the VPC. The EC2 instances are configured to forward queries to the default VPC resolver for Amazon Route 53 hosted domains and to the on-premises DNS servers for other on-premises hosted domain names. The company notices job failures and finds that DNS queries from the HPC cluster nodes failed when the nodes tried to resolve RDS and S3 bucket endpoints.
Which architectural change should a network engineer implement to provide the DNS service in the MOST scalable way?

A. Scale out the DNS service by adding two additional EC2 instances in the VPC. Reconfigure half of the HPC cluster nodes to use these new DNS servers. Plan to scale out by adding additional EC2 instance-based DNS servers in the future as the HPC cluster size grows.

B. Scale up the existing EC2 instances that the company is using as DNS servers. Change the instance size to the largest possible instance size to accommodate the current DNS load and the anticipated load in the future.

C. Create Route 53 Resolver outbound endpoints. Create Route 53 Resolver rules to forward queries to on-premises DNS servers for on premises hosted domain names. Reconfigure the HPC cluster nodes to use the default VPC resolver instead of the EC2 instance-based DNS servers. Terminate the EC2 instances.

D. Create Route 53 Resolver inbound endpoints. Create rules on the on-premises DNS servers to forward queries to the default VPC resolver. Reconfigure the HPC cluster nodes to forward all DNS queries to the on-premises DNS servers. Terminate the EC2 instances.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 48
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's network engineer is designing an active-passive connection to AWS from two on-premises data centers. The company has set up AWS Direct Connect connections between the on-premises data centers and AWS. From each location, the company is using a transit VIF that connects to a Direct Connect gateway that is associated with a transit gateway.
The network engineer must ensure that traffic from AWS to the data centers is routed first to the primary data center. The traffic should be routed to the failover data center only in the case of an outage.
Which solution will meet these requirements?

A. Set the BGP community tag for all prefixes from the primary data center to 7224:7100. Set the BGP community tag for all prefixes from the failover data center to 7224:7300

B. Set the BGP community tag for all prefixes from the primary data center to 7224:7300. Set the BGP community tag for all prefixes from the failover data center to 7224:7100

C. Set the BGP community tag for all prefixes from the primary data center to 7224:9300. Set the BGP community tag for all prefixes from the failover data center to 7224:9100

D. Set the BGP community tag for all prefixes from the primary data center to 7224:9100. Set the BGP community tag for all prefixes from the failover data center to 7224:9300

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 49
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A real estate company is building an internal application so that real estate agents can upload photos and videos of various properties. The application will store these photos and videos in an Amazon S3 bucket as objects and will use Amazon DynamoDB to store corresponding metadata. The S3 bucket will be configured to publish all PUT events for new object uploads to an Amazon Simple Queue Service (Amazon SQS) queue.
A compute cluster of Amazon EC2 instances will poll the SQS queue to find out about newly uploaded objects. The cluster will retrieve new objects, perform proprietary image and video recognition and classification update metadata in DynamoDB and replace the objects with new watermarked objects. The company does not want public IP addresses on the EC2 instances.
Which networking design solution will meet these requirements MOST cost-effectively as application usage increases?

A. Place the EC2 instances in a public subnet. Disable the Auto-assign Public IP option while launching the EC2 instances. Create an internet gateway. Attach the internet gateway to the VPC. In the public subnet's route table, add a default route that points to the internet gateway.

B. Place the EC2 instances in a private subnet. Create a NAT gateway in a public subnet in the same Availability Zone. Create an internet gateway. Attach the internet gateway to the VPC. In the public subnet's route table, add a default route that points to the internet gateway

C. Place the EC2 instances in a private subnet. Create an interface VPC endpoint for Amazon SQS. Create gateway VPC endpoints for Amazon S3 and DynamoDB.

D. Place the EC2 instances in a private subnet. Create a gateway VPC endpoint for Amazon SQS. Create interface VPC endpoints for Amazon S3 and DynamoDB.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 50
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has an AWS Direct Connect connection between its on-premises data center in the United States (US) and workloads in the us-east-1 Region. The connection uses a transit VIF to connect the data center to a transit gateway in us-east-1.
The company is opening a new office in Europe with a new on-premises data center in England. A Direct Connect connection will connect the new data center with some workloads that are running in a single VPC in the eu-west-2 Region. The company needs to connect the US data center and us-east-1 with the Europe data center and eu-west-2. A network engineer must establish full connectivity between the data centers and Regions with the lowest possible latency.
How should the network engineer design the network architecture to meet these requirements?

A. Connect the VPC in eu-west-2 with the Europe data center by using a Direct Connect gateway and a private VIF. Associate the transit gateway in us-east-1 with the same Direct Connect gateway. Enable SiteLink for the transit VIF and the private VIF.

B. Connect the VPC in eu-west-2 to a new transit gateway. Connect the Europe data center to the new transit gateway by using a Direct Connect gateway and a new transit VIF. Associate the transit gateway in us-east-1 with the same Direct Connect gateway. Enable SiteLink for both transit VIFs. Peer the two transit gateways.

C. Connect the VPC in eu-west-2 to a new transit gateway. Connect the Europe data center to the new transit gateway by using a Direct Connect gateway and a new transit VIF. Create a new Direct Connect gateway. Associate the transit gateway in us-east-1 with the new Direct Connect gateway. Enable SiteLink for both transit VIFs. Peer the two transit gateways.

D. Connect the VPC in eu-west-2 with the Europe data center by using a Direct Connect gateway and a private VIF. Create a new Direct Connect gateway. Associate the transit gateway in us-east-1 with the new Direct Connect gateway. Enable SiteLink for the transit VIF and the private VIF.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 51
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer has deployed an Amazon EC2 instance in a private subnet in a VPC. The VPC has no public subnet. The EC2 instance hosts application code that sends messages to an Amazon Simple Queue Service (Amazon SQS) queue. The subnet has the default network ACL with no modification applied. The EC2 instance has the default security group with no modification applied.
The SQS queue is not receiving messages.
Which of the following are possible causes of this problem? (Choose two.)

A. The EC2 instance is not attached to an IAM role that allows write operations to Amazon SQS.

B. The security group is blocking traffic to the IP address range used by Amazon SQS

C. There is no interface VPC endpoint configured for Amazon SQS

D. The network ACL is blocking return traffic from Amazon SQS

E. There is no route configured in the subnet route table for the IP address range used by Amazon SQS

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 52
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer needs to standardize a company's approach to centralizing and managing interface VPC endpoints for private communication with AWS services. The company uses AWS Transit Gateway for inter-VPC connectivity between AWS accounts through a hub-and-spoke model. The company's network services team must manage all Amazon Route 53 zones and interface endpoints within a shared services AWS account. The company wants to use this centralized model to provide AWS resources with access to AWS Key Management Service (AWS KMS) without sending traffic over the public internet.
What should the network engineer do to meet these requirements?

A. In the shared services account, create an interface endpoint for AWS KMS. Modify the interface endpoint by disabling the private DNS name. Create a private hosted zone in the shared services account with an alias record that points to the interface endpoint. Associate the private hosted zone with the spoke VPCs in each AWS account.

B. In the shared services account, create an interface endpoint for AWS KMS. Modify the interface endpoint by disabling the private DNS name. Create a private hosted zone in each spoke AWS account with an alias record that points to the interface endpoint. Associate each private hosted zone with the shared services AWS account.

C. In each spoke AWS account, create an interface endpoint for AWS KMS. Modify each interface endpoint by disabling the private DNS name. Create a private hosted zone in each spoke AWS account with an alias record that points to each interface endpoint. Associate each private hosted zone with the shared services AWS account.

D. In each spoke AWS account, create an interface endpoint for AWS KMS. Modify each interface endpoint by disabling the private DNS name. Create a private hosted zone in the shared services account with an alias record that points to each interface endpoint. Associate the private hosted zone with the spoke VPCs in each AWS account.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 53
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A development team is building a new web application in the AWS Cloud. The main company domain, example.com, is currently hosted in an Amazon Route 53 public hosted zone in one of the company's production AWS accounts.
The developers want to test the web application in the company's staging AWS account by using publicly resolvable subdomains under the example.com domain with the ability to create and delete DNS records as needed. Developers have full access to Route 53 hosted zones within the staging account, but they are prohibited from accessing resources in any of the production AWS accounts.
Which combination of steps should a network engineer take to allow the developers to create records under the example com domain? (Choose two.)

A. Create a public hosted zone for example com in the staging account

B. Create a staging example.com NS record in the example.com domain. Populate the value with the name servers from the staging.example.com domain. Set the routing policy type to simple routing.

C. Create a private hosted zone for staging example com in the staging account.

D. Create an example com NS record in the staging example.com domain. Populate the value with the name servers from the example.com domain. Set the routing policy type to simple routing.

E. Create a public hosted zone for staging.example.com in the staging account.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 54
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company plans to deploy a two-tier web application to a new VPC in a single AWS Region. The company has configured the VPC with an internet gateway and four subnets. Two of the subnets are public and have default routes that point to the internet gateway. Two of the subnets are private and share a route table that does not have a default route.
The application will run on a set of Amazon EC2 instances that will be deployed behind an external Application Load Balancer. The EC2 instances must not be directly accessible from the internet. The application will use an Amazon S3 bucket in the same Region to store data. The application will invoke S3 GET API operations and S3 PUT API operations from the EC2 instances. A network engineer must design a VPC architecture that minimizes data transfer cost.
Which solution will meet these requirements?

A. Deploy the EC2 instances in the public subnets. Create an S3 interface endpoint in the VPC. Modify the application configuration to use the S3 endpoint-specific DNS hostname.

B. Deploy the EC2 instances in the private subnets. Create a NAT gateway in the VPC. Create default routes in the private subnets to the NAT gateway. Connect to Amazon S3 by using the NAT gateway.

C. Deploy the EC2 instances in the private subnets. Create an S3 gateway endpoint in the VPSpecify die route table of the private subnets during endpoint creation to create routes to Amazon S3.

D. Deploy the EC2 instances in the private subnets. Create an S3 interface endpoint in the VPC. Modify the application configuration to use the S3 endpoint-specific DNS hostname.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 55
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

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 set of steps should the network engineer follow in each AWS account to meet these 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 the feature 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 attachment. Associate a route table with the attachment.

B. 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 with the attachment.

C. 1. In the Connectivity account: Create a resource share in AWS Resource Access Manager for the VPC subnets. Provide the Production account ID. Enable the feature to 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.
4. In the Production account: Accept the attachment. Associate a route table with the attachment.

D. 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 attachment. Associate a route table with the attachment.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 56
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is running multiple workloads on Amazon EC2 instances in public subnets. In a recent incident, an attacker exploited an application vulnerability on one of the EC2 instances to gain access to the instance. The company fixed the application and launched a replacement EC2 instance that contains the updated application.
The attacker used the compromised application to spread malware over the internet. The company became aware of the compromise through a notification from AWS. The company needs the ability to identify when an application that is deployed on an EC2 instance is spreading malware.
Which solution will meet this requirement with the LEAST operational effort?

A. Use Amazon GuardDuty to analyze traffic patterns by inspecting DNS requests and VPC flow logs.

B. Use Amazon GuardDuty to deploy AWS managed decoy systems that are equipped with the most recent malware signatures.

C. Set up a Gateway Load Balancer. Run an intrusion detection system (IDS) appliance from AWS Marketplace on Amazon EC2 for traffic inspection.

D. Configure Amazon Inspector to perform deep packet inspection of outgoing traffic.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 57
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company deploys a new web application on Amazon EC2 instances. The application runs in private subnets in three Availability Zones behind an Application Load Balancer (ALB). Security auditors require encryption of all connections. The company uses Amazon Route 53 for DNS and uses AWS Certificate Manager (ACM) to automate SSL/TLS certificate provisioning. SSL/TLS connections are terminated on the ALB.
The company tests the application with a single EC2 instance and does not observe any problems. However, after production deployment, users report that they can log in but that they cannot use the application. Every new web request restarts the login process.
What should a network engineer do to resolve this issue?

A. Modify the ALB listener configuration. Edit the rule that forwards traffic to the target group. Change the rule to enable group-level stickiness. Set the duration to the maximum application session length.

B. Replace the ALB with a Network Load Balancer. Create a TLS listener. Create a new target group with the protocol type set to TLS Register the EC2 instances. Modify the target group configuration by enabling the stickiness attribute.

C. Modify the ALB target group configuration by enabling the stickiness attribute. Use an application-based cookie. Set the duration to the maximum application session length.

D. Remove the ALB. Create an Amazon Route 53 rule with a failover routing policy for the application name. Configure ACM to issue certificates for each EC2 instance.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 58

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

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 for 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 through the NAT gateway.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 59
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company uses AWS Direct Connect to connect its corporate network to multiple VPCs in the same AWS account and the same AWS Region. Each VPC uses its own private VIF and its own virtual LAN on the Direct Connect connection. The company has grown and will soon surpass the limit of VPCs and private VIFs for each connection.
What is the MOST scalable way to add VPCs with on-premises connectivity?

A. Provision a new Direct Connect connection to handle the additional VPCs. Use the new connection to connect additional VPCs.

B. Create virtual private gateways for each VPC that is over the service quota. Use AWS Site-to-Site VPN to connect the virtual private gateways to the corporate network.

C. Create a Direct Connect gateway, and add virtual private gateway associations to the VPCs. Configure a private VIF to connect to the corporate network.

D. Create a transit gateway, and attach the VPCs. Create a Direct Connect gateway, and associate it with the transit gateway. Create a transit VIF to the Direct Connect gateway.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 60
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer is designing a hybrid architecture that uses a 1 Gbps AWS Direct Connect connection between the company's data center and two AWS Regions: us-east-1 and eu-west-1. The VPCs in us-east-1 are connected by a transit gateway and need to access several on-premises databases. According to company policy, only one VPC in eu-west-1 can be connected to one on-premises server. The on-premises network segments the traffic between the databases and the server.
How should the network engineer set up the Direct Connect connection to meet these requirements?

A. Create one hosted connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use one Direct. Connect gateway for both VIFs to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

B. Create one hosted connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use two Direct Connect gateways, one for each VIF, to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

C. Create one dedicated connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use one Direct Connect gateway for both VIFs to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

D. Create one dedicated connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use two Direct Connect gateways, one for each VIF, to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 61
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed an application in a VPC that uses a NAT gateway for outbound traffic to the internet. A network engineer notices a large quantity of suspicious network traffic that is traveling from the VPC over the internet to IP addresses that are included on a deny list. The network engineer must implement a solution to determine which AWS resources are generating the suspicious traffic. The solution must minimize cost and administrative overhead.
Which solution will meet these requirements?

A. Launch an Amazon EC2 instance in the VPC. Use Traffic Mirroring by specifying the NAT gateway as the source and the EC2 instance as the destination. Analyze the captured traffic by using open-source tools to identify the AWS resources that are generating the suspicious traffic.

B. Use VPC flow logs. Launch a security information and event management (SIEM) solution in the VPC. Configure the SIEM solution to ingest the VPC flow logs. Run queries on the SIEM solution to identify the AWS resources that are generating the suspicious traffic.

C. Use VPC flow logs. Publish the flow logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the flow logs to identify the AWS resources that are generating the suspicious traffic.

D. Configure the VPC to stream the network traffic directly to an Amazon Kinesis data stream. Send the data from the Kinesis data stream to an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Athena to query the data to identify the AWS resources that are generating the suspicious traffic.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 62
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has its production VPC (VPC-A) in the eu-west-1 Region in Account 1. VPC-A is attached to a transit gateway (TGW-A) that is connected to an on-premises data center in Dublin, Ireland, by an AWS Direct Connect transit VIF that is configured for an AWS Direct Connect gateway. The company also has a staging VPC (VPC-B) that is attached to another transit gateway (TGW-B) in the eu-west-2 Region in Account 2.
A network engineer must implement connectivity between VPC-B and the on-premises data center in Dublin.
Which solutions will meet these requirements? (Choose two.)

A. Configure inter-Region VPC peering between VPC-A and VPC-B. Add the required VPC peering routes. Add the VPC-B CIDR block in the allowed prefixes on the Direct Connect gateway association.

B. Associate TGW-B with the Direct Connect gateway. Advertise the VPC-B CIDR block under the allowed prefixes.

C. Configure another transit VIF on the Direct Connect connection and associate TGW-B. Advertise the VPC-B CIDR block under the allowed prefixes.

D. Configure inter-Region transit gateway peering between TGW-A and TGW-B. Add the peering routes in the transit gateway route tables. Add both the VPC-A and the VPC-B CIDR block under the allowed prefix list in the Direct Connect gateway association.

E. Configure an AWS Site-to-Site VPN connection over the transit VIF to TGW-B as a VPN attachment.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 63
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's network engineer is designing a hybrid DNS solution for an AWS Cloud workload. Individual teams want to manage their own DNS hostnames for their applications in their development environment. The solution must integrate the application-specific hostnames with the centrally managed DNS hostnames from the on-premises network and must provide bidirectional name resolution. The solution also must minimize management overhead.
Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Use an Amazon Route 53 Resolver inbound endpoint.

B. Modify the DHCP options set by setting a custom DNS server value.

C. Use an Amazon Route 53 Resolver outbound endpoint.

D. Create DNS proxy servers.

E. Create Amazon Route 53 private hosted zones.

F. Set up a zone transfer between Amazon Route 53 and the on-premises DNS.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 64
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company hosts a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin in an Amazon CloudFront distribution. The company wants to implement a custom authentication system that will provide a token for its authenticated customers.
The web application must ensure that the GET/POST requests come from authenticated customers before it delivers the content. A network engineer must design a solution that gives the web application the ability to identify authorized customers.
What is the MOST operationally efficient solution that meets these requirements?

A. Use the ALB to inspect the authorized token inside the GET/POST request payload. Use an AWS Lambda function to insert a customized header to inform the web application of an authenticated customer request.

B. Integrate AWS WAF with the ALB to inspect the authorized token inside the GET/POST request payload. Configure the ALB listener to insert a customized header to inform the web application of an authenticated customer request.

C. Use an AWS Lambda@Edge function to inspect the authorized token inside the GET/POST request payload. Use the Lambda@Edge function also to insert a customized header to inform the web application of an authenticated customer request.

D. Set up an EC2 instance that has a third-party packet inspection tool to inspect the authorized token inside the GET/POST request payload. Configure the tool to insert a customized header to inform the web application of an authenticated customer request.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 65
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has created three VPCs: a production VPC, a nonproduction VPC, and a shared services VPC. The production VPC and the nonproduction VPC must each have communication with the shared services VPC. There must be no communication between the production VPC and the nonproduction VPC. A transit gateway is deployed to facilitate communication between VPCs.
Which route table configurations on the transit gateway will meet these requirements?

A. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for only the shared services VPC. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

B. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for each VPC. Create an additional route table with only the shared services VPC attachment associated with propagated routes from each VPC.

C. Configure a route table with all the VPC attachments associated with propagated routes for only the shared services VPCreate an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

D. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes disabled. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 66
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is using an AWS Site-to-Site VPN connection from the company's on-premises data center to a virtual private gateway in the AWS Cloud Because of congestion, the company is experiencing availability and performance issues as traffic travels across the internet before the traffic reaches AWS. A network engineer must reduce these issues for the connection as quickly as possible with minimum administration effort.
Which solution will meet these requirements?

A. Edit the existing Site-to-Site VPN connection by enabling acceleration. Stop and start the VPN service on the customer gateway for the new setting to take effect.

B. Configure a transit gateway in the same AWS Region as the existing virtual private gateway. Create a new accelerated Site-to-Site VPN connection. Connect the new connection to the transit gateway by using a VPN attachment. Update the customer gateway device to use the new Site to Site VPN connection. Delete the existing Site-to-Site VPN connection

C. Create a new accelerated Site-to-Site VPN connection. Connect the new Site-to-Site VPN connection to the existing virtual private gateway. Update the customer gateway device to use the new Site-to-Site VPN connection. Delete the existing Site-to-Site VPN connection.

D. Create a new AWS Direct Connect connection with a private VIF between the on-premises data center and the AWS Cloud. Update the customer gateway device to use the new Direct Connect connection. Delete the existing Site-to-Site VPN connection.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 67
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

An Australian ecommerce company hosts all of its services in the AWS Cloud and wants to expand its customer base to the United States (US). The company is targeting the western US for the expansion.
The company's existing AWS architecture consists of four AWS accounts with multiple VPCs deployed in the ap-southeast-2 Region. All VPCs are attached to a transit gateway in ap-southeast-2. There are dedicated VPCs for each application service. The company also has VPCs for centralized security features such as proxies, firewalls, and logging.
The company plans to duplicate the infrastructure from ap-southeast-2 to the us-west-1 Region. A network engineer must establish connectivity between the various applications in the two Regions. The solution must maximize bandwidth, minimize latency and minimize operational overhead.
Which solution will meet these requirements?

A. Create VPN attachments between the two transit gateways. Configure the VPN attachments to use BGP routing between the two transit gateways.

B. Peer the transit gateways in each Region. Configure routing between the two transit gateways for each Region's IP addresses.

C. Create a VPN server in a VPC in each Region. Update the routing to point to the VPN servers for the IP addresses in alternate Regions.

D. Attach the VPCs in us-west-1 to the transit gateway in ap-southeast-2.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 68
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

An IoT company sells hardware sensor modules that periodically send out temperature, humidity, pressure, and location data through the MQTT messaging protocol. The hardware sensor modules send this data to the company's on-premises MQTT brokers that run on Linux servers behind a load balancer. The hardware sensor modules have been hardcoded with public IP addresses to reach the brokers.
The company is growing and is acquiring customers across the world. The existing solution can no longer scale and is introducing additional latency because of the company's global presence. As a result, the company decides to migrate its entire infrastructure from on premises to the AWS Cloud. The company needs to migrate without reconfiguring the hardware sensor modules that are already deployed across the world. The solution also must minimize latency.
The company migrates the MQTT brokers to run on Amazon EC2 instances.
What should the company do next to meet these requirements?

A. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listeners. Use Bring Your Own IP (BYOIP) from the on-premises network with the NLB.

B. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listeners. Create an AWS Global Accelerator accelerator in front of the NLUse Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator.

C. Place the EC2 instances behind an Application Load Balancer (ALB). Configure TCP listeners. Create an AWS Global Accelerator accelerator in front of the ALB. Use Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator

D. Place the EC2 instances behind an Amazon CloudFront distribution. Use Bring Your Own IP (BYOIP) from the on-premises network with CloudFront.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 69

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed a web application on AWS. The web application uses an Application Load Balancer (ALB) across multiple Availability Zones. The targets of the ALB are AWS Lambda functions. The web application also uses Amazon CloudWatch metrics for monitoring.

Users report that parts of the web application are not loading properly. A network engineer needs to troubleshoot the problem. The network engineer enables access logging for the ALB.

What should the network engineer do next to determine which errors the ALB is receiving?

A. Send the logs to Amazon CloudWatch Logs. Review the ALB logs in CloudWatch Insights to determine which error messages the ALB is receiving.

B. Configure the Amazon S3 bucket destination. Use Amazon Athena to determine which error messages the ALB is receiving.

C. Configure the Amazon S3 bucket destination. After Amazon CloudWatch Logs pulls the ALB logs from the S3 bucket automatically, review the logs in CloudWatch Logs to determine which error messages the ALB is receiving.

D. Send the logs to Amazon CloudWatch Logs. Use the Amazon Athena CloudWatch Connector to determine which error messages the ALB is receiving.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 70
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is planning to use Amazon S3 to archive financial data. The data is currently stored in an on-premises data center. The company uses AWS Direct Connect with a Direct Connect gateway and a transit gateway to connect to the on-premises data center. The data cannot be transported over the public internet and must be encrypted in transit.
Which solution will meet these requirements?

A. Create a Direct Connect public VIF. Set up an IPsec VPN connection over the public VIF to access Amazon S3. Use HTTPS for communication.

B. Create an IPsec VPN connection over the transit VIF. Create a VPC and attach the VPC to the transit gateway. In the VPC, provision an interface VPC endpoint for Amazon S3. Use HTTPS for communication.

C. Create a VPC and attach the VPC to the transit gateway. In the VPC, provision an interface VPC endpoint for Amazon S3. Use HTTPS for communication.

D. Create a Direct Connect public VIF. Set up an IPsec VPN connection over the public VIF to the transit gateway. Create an attachment for Amazon S3. Use HTTPS for communication.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 71
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is using Amazon Route 53 Resolver DNS Firewall in a VPC to block all domains except domains that are on an approved list. The company is concerned that if DNS Firewall is unresponsive, resources in the VPC might be affected if the network cannot resolve any DNS queries. To maintain application service level agreements, the company needs DNS queries to continue to resolve even if Route 53 Resolver does not receive a response from DNS Firewall.
Which change should a network engineer implement to meet these requirements?

A. Update the DNS Firewall VPC configuration to disable fail open for the VPC.

B. Update the DNS Firewall VPC configuration to enable fail open for the VPC.

C. Create a new DHCP options set with parameter dns_firewall_fail_open=false. Associate the new DHCP options set with the VPC.

D. Create a new DHCP options set with parameter dns_firewall_fail_open=true. Associate the new DHCP options set with the VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 72
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is migrating an existing application to a new AWS account. The company will deploy the application in a single AWS Region by using one VPC and multiple Availability Zones. The application will run on Amazon EC2 instances. Each Availability Zone will have several EC2 instances. The EC2 instances will be deployed in private subnets.

The company's clients will connect to the application by using a web browser with the HTTPS protocol. Inbound connections must be distributed across the Availability Zones and EC2 instances. All connections from the same client session must be connected to the same EC2 instance. The company must provide end-to-end encryption for all connections between the clients and the application by using the application SSL certificate.

Which solution will meet these requirements?

A. Create a Network Load Balancer. Create a target group. Set the protocol to TCP and the port to 443 for the target group. Turn on session affinity (sticky sessions). Register the EC2 instances as targets. Create a listener. Set the protocol to TCP and the port to 443 for the listener. Deploy SSL certificates to the EC2 instances.

B. Create an Application Load Balancer. Create a target group. Set the protocol to HTTP and the port to 80 for the target group. Turn on session affinity (sticky sessions) with an application-based cookie policy. Register the EC2 instances as targets. Create an HTTPS listener. Set the default action to forward to the target group. Use AWS Certificate Manager (ACM) to create a certificate for the listener.

C. Create a Network Load Balancer. Create a target group. Set the protocol to TLS and the port to 443 for the target group. Turn on session affinity (sticky sessions). Register the EC2 instances as targets. Create a listener. Set the protocol to TLS and the port to 443 for the listener. Use AWS Certificate Manager (ACM) to create a certificate for the application.

D. Create an Application Load Balancer. Create a target group. Set the protocol to HTTPS and the port to 443 for the target group. Turn on session affinity (sticky sessions) with an application-based cookie policy. Register the EC2 instances as targets. Create an HTTP listener. Set the port to 443 for the listener. Set the default action to forward to the target group.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 73

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is developing an application in which IoT devices will report measurements to the AWS Cloud. The application will have millions of end users. The company observes that the IoT devices cannot support DNS resolution. The company needs to implement an Amazon EC2 Auto Scaling solution so that the IoT devices can connect to an application endpoint without using DNS.

Which solution will meet these requirements MOST cost-effectively?

A. Use an Application Load Balancer (ALB)-type target group for a Network Load Balancer (NLB). Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the ALB. Set up the IoT devices to connect to the IP addresses of the NLB.

B. Use an AWS Global Accelerator accelerator with an Application Load Balancer (ALB) endpoint. Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the ALSet up the IoT devices to connect to the IP addresses of the accelerator.

C. Use a Network Load Balancer (NLB). Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the NLB. Set up the IoT devices to connect to the IP addresses of the NLB.

D. Use an AWS Global Accelerator accelerator with a Network Load Balancer (NLB) endpoint. Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the NLB. Set up the IoT devices to connect to the IP addresses of the accelerator.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 74

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed a new web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Amazon EC2 Auto Scaling group. Enterprise customers from around the world will use the application. Employees of these enterprise customers will connect to the application over HTTPS from office locations.

The company must configure firewalls to allow outbound traffic to only approved IP addresses. The employees of the enterprise customers must be able to access the application with the least amount of latency.

Which change should a network engineer make in the infrastructure to meet these requirements?

A. Create a new Network Load Balancer (NLB). Add the ALB as a target of the NLB.

B. Create a new Amazon CloudFront distribution. Set the ALB as the distribution's origin.

C. Create a new accelerator in AWS Global Accelerator. Add the ALB as an accelerator endpoint.

D. Create a new Amazon Route 53 hosted zone. Create a new record to route traffic to the ALB.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 75
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has hundreds of VPCs on AWS. All the VPCs access the public endpoints of Amazon S3 and AWS Systems Manager through NAT gateways. All the traffic from the VPCs to Amazon S3 and Systems Manager travels through the NAT gateways. The company's network engineer must centralize access to these services and must eliminate the need to use public endpoints.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a central egress VPC that has private NAT gateways. Connect all the VPCs to the central egress VPC by using AWS Transit Gateway. Use the private NAT gateways to connect to Amazon S3 and Systems Manager by using private IP addresses.

B. Create a central shared services VPC. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access. Ensure that private DNS is turned off. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway. Create an Amazon Route 53 forwarding rule for each interface VPC endpoint. Associate the forwarding rules with all the VPCs. Forward DNS queries to the interface VPC endpoints in the shared services VPC.

C. Create a central shared services VPIn the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access. Ensure that private DNS is turned off. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway. Create an Amazon Route 53 private hosted zone with a full service endpoint name for Amazon S3 and Systems Manager. Associate the private hosted zones with all the VPCs. Create an alias record in each private hosted zone with the full AWS service endpoint pointing to the interface VPC endpoint in the shared services VPC.

D. Create a central shared services VPC. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway. Ensure that private DNS is turned on for the interface VPC endpoints and that the transit gateway is created with DNS support turned on.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 76
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company manages resources across VPCs in multiple AWS Regions. The company needs to connect to the resources by using its internal domain name. A network engineer needs to apply the aws.example.com DNS suffix to all resources.

What must the network engineer do to meet this requirement?

A. Create an Amazon Route 53 private hosted zone for aws.example.com in each Region that has resources. Associate the private hosted zone with that Region's VPC. In the appropriate private hosted zone, create DNS records for the resources in each Region.

B. Create one Amazon Route 53 private hosted zone for aws.example.com. Configure the private hosted zone to allow zone transfers with every VPC.

C. Create one Amazon Route 53 private hosted zone for example.com. Create a single resource record for aws.example.com in the private hosted zone. Apply a multivalue answer routing policy to the record. Add all VPC resources as separate values in the routing policy.

D. Create one Amazon Route 53 private hosted zone for aws.example.com. Associate the private hosted zone with every VPC that has resources. In the private hosted zone, create DNS records for all resources.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 77
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

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. Bi-directional 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?

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 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 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.

B. 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 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 Manager. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints.

C. 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 VPDefine 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 VPand 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 outbound endpoints.

D. 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 endpoints.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 78

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A global company runs business applications in the us-east-1 Region inside a VPC. One of the company's regional offices in London uses a virtual private gateway for an AWS Site-to-Site VPN connection tom the VPC. The company has configured a transit gateway and has set up peering between the VPC and other VPCs that various departments in the company use.

Employees at the London office are experiencing latency issues when they connect to the business applications.

What should a network engineer do to reduce this latency?

A. Create a new Site-to-Site VPN connection. Set the transit gateway as the target gateway. Enable acceleration on the new Site-to-Site VPN connection. Update the VPN device in the London office with the new connection details.

B. Modify the existing Site-to-Site VPN connection by setting the transit gateway as the target gateway. Enable acceleration on the existing Site-to-Site VPN connection.

C. Create a new transit gateway in the eu-west-2 (London) Region. Peer the new transit gateway with the existing transit gateway. Modify the existing Site-to-Site VPN connection by setting the new transit gateway as the target gateway.

D. Create a new AWS Global Accelerator standard accelerator that has an endpoint of the Site-to-Site VPN connection. Update the VPN device in the London office with the new connection details.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 79
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has a hybrid cloud environment. The company's data center is connected to the AWS Cloud by an AWS Direct Connect connection. The AWS environment includes VPCs that are connected together in a hub-and-spoke model by a transit gateway. The AWS environment has a transit VIF with a Direct Connect gateway for on-premises connectivity.

The company has a hybrid DNS model. The company has configured Amazon Route 53 Resolver endpoints in the hub VPC to allow bidirectional DNS traffic flow. The company is running a backend application in one of the VPCs.

The company uses a message-oriented architecture and employs Amazon Simple Queue Service (Amazon SQS) to receive messages from other applications over a private network. A network engineer wants to use an interface VPC endpoint for Amazon SQS for this architecture. Client services must be able to access the endpoint service from on premises and from multiple VPCs within the company's AWS infrastructure.

Which combination of steps should the network engineer take to ensure that the client applications can resolve DNS for the interface endpoint? (Choose three.)

A. Create the interface endpoint for Amazon SQS with the option for private DNS names turned on.

B. Create the interface endpoint for Amazon SQS with the option for private DNS names turned off.

C. Manually create a private hosted zone for sqs.us-east-1.amazonaws.com. Add necessary records that point to the interface endpoint. Associate the private hosted zones with other VPCs.

D. Use the automatically created private hosted zone for sqs.us-east-1.amazonaws.com with previously created necessary records that point to the interface endpoint. Associate the private hosted zones with other VPCs.

E. Access the SQS endpoint by using the public DNS name sqs.us-east-1 amazonaws.com in VPCs and on premises.

F. Access the SQS endpoint by using the private DNS name of the interface endpoint .sqs.us-east-1.vpce.amazonaws.com in VPCs and on premises.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 80

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's network engineer builds and tests network designs for VPCs in a development account. The company needs to monitor the changes that are made to network resources and must ensure strict compliance with network security policies. The company also needs access to the historical configurations of network resources.

Which solution will meet these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with a custom pattern to monitor the account for changes. Configure the rule to invoke an AWS Lambda function to identify noncompliant resources. Update an Amazon DynamoDB table with the changes that are identified.

B. Create custom metrics from Amazon CloudWatch logs. Use the metrics to invoke an AWS Lambda function to identify noncompliant resources. Update an Amazon DynamoDB table with the changes that are identified.

C. Record the current state of network resources by using AWS Config. Create rules that reflect the desired configuration settings. Set remediation for noncompliant resources.

D. Record the current state of network resources by using AWS Systems Manager Inventory. Use Systems Manager State Manager to enforce the desired configuration settings and to carry out remediation for noncompliant resources.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 81

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is migrating an application from on premises to AWS. The company will host the application on Amazon EC2 instances that are deployed in a single VPC. During the migration period, DNS queries from the EC2 instances must be able to resolve names of on-premises servers. The migration is expected to take 3 months After the 3-month migration period, the resolution of on-premises servers will no longer be needed.

What should a network engineer do to meet these requirements with the LEAST amount of configuration?

A. Set up an AWS Site-to-Site VPN connection between on premises and AWS. Deploy an Amazon Route 53 Resolver outbound endpoint in the Region that is hosting the VPC.

B. Set up an AWS Direct Connect connection with a private VIF. Deploy an Amazon Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint in the Region that is hosting the VPC.

C. Set up an AWS Client VPN connection between on premises and AWS. Deploy an Amazon Route 53 Resolver inbound endpoint in the VPC.

D. Set up an AWS Direct Connect connection with a public VIF. Deploy an Amazon Route 53 Resolver inbound endpoint in the Region that is hosting the VPC. Use the IP address that is assigned to the endpoint for connectivity to the on-premises DNS servers.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 82

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is hosting an application on Amazon EC2 instances behind an Application Load Balancer. The instances are in an Amazon EC2 Auto Scaling group. Because of a recent change to a security group, external users cannot access the application.

A network engineer needs to prevent this downtime from happening again. The network engineer must implement a solution that remediates noncompliant changes to security groups.

Which solution will meet these requirements?

A. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

B. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

C. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

D. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 83

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is deploying third-party firewall appliances for traffic inspection and NAT capabilities in its VPC. The VPC is configured with private subnets and public subnets. The company needs to deploy the firewall appliances behind a load balancer.

Which architecture will meet these requirements MOST cost-effectively?

A. Deploy a Gateway Load Balancer with the firewall appliances as targets. Configure the firewall appliances with a single network interface in a private subnet. Use a NAT gateway to send the traffic to the internet after inspection.

B. Deploy a Gateway Load Balancer with the firewall appliances as targets. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection.

C. Deploy a Network Load Balancer with the firewall appliances as targets. Configure the firewall appliances with a single network interface in a private subnet. Use a NAT gateway to send the traffic to the internet after inspection.

D. Deploy a Network Load Balancer with the firewall appliances as targets. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 84

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's AWS architecture consists of several VPCs. The VPCs include a shared services VPC and several application VPCs. The company has established network connectivity from all VPCs to the on-premises DNS servers.

Applications that are deployed in the application VPCs must be able to resolve DNS for internally hosted domains on premises. The applications also must be able to resolve local VPC domain names and domains that are hosted in Amazon Route 53 private hosted zones.

What should a network engineer do to meet these requirements?

A. Create a new Route 53 Resolver inbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC. Update each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.

B. Create a new Route 53 Resolver outbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC.

C. Create a new Route 53 Resolver outbound endpoint in the shared services VPCreate forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPUpdate each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.

D. Create a new Route 53 Resolver inbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 85

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has been using an outdated application layer protocol for communication among applications. The company decides not to use this protocol anymore and must migrate all applications to support a new protocol. The old protocol and the new protocol are TCP-based, but the protocols use different port numbers.

After several months of work, the company has migrated dozens of applications that run on Amazon EC2 instances and in containers. The company believes that all the applications have been migrated, but the company wants to verify this belief. A network engineer needs to verify that no application is still using the old protocol.

Which solution will meet these requirements without causing any downtime?

A. Use Amazon Inspector and its Network Reachability rules package. Wait until the analysis has finished running to find out which EC2 instances are still listening to the old port.

B. Enable Amazon GuardDuty. Use the graphical visualizations to filter for traffic that uses the port of the old protocol. Exclude all internet traffic to filter out occasions when the same port is used as an ephemeral port.

C. Configure VPC flow logs to be delivered into an Amazon S3 bucket. Use Amazon Athena to query the data and to filter for the port number that is used by the old protocol.

D. Inspect all security groups that are assigned to the EC2 instances that host the applications. Remove the port of the old protocol if that port is in the list of allowed ports. Verify that the applications are operating properly after the port is removed from the security groups.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 86
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has deployed its AWS environment in a single AWS Region. The environment consists of a few hundred application VPCs, a shared services VPC, and a VPN connection to the company's on-premises environment. A network engineer needs to implement a transit gateway with the following requirements:

- Application VPCs must be isolated from each other.
- Bidirectional communication must be allowed between the application VPCs and the on-premises network.
- Bidirectional communication must be allowed between the application VPCs and the shared services VPC.

The network engineer creates the transit gateway with options disabled for default route table association and default route table propagation. The network engineer also creates the VPN attachment for the on-premises network and creates the VPC attachments for the application VPCs and the shared services VPC.

The network engineer must meet all the requirements for the transit gateway by designing a solution that needs the least number of transit gateway route tables.

Which combination of actions should the network engineer perform to accomplish this goal? (Choose two.)

A. Configure a separate transit gateway route table for on premises. Associate the VPN attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

B. Configure a separate transit gateway route table for each application VPC. Associate each application VPC attachment with its respective transit gateway route table. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.

C. Configure a separate transit gateway route table for all application VPCs. Associate all application VPCs with this transit gateway route table. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.

D. Configure a separate transit gateway route table for the shared services VPC. Associate the shared services VPC attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

E. Configure a separate transit gateway route table for on premises and the shared services VPC. Associate the VPN attachment and the shared services VPC attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 87
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has an AWS Site-to-Site VPN connection between its existing VPC and on-premises network. The default DHCP options set is associated with the VPC. The company has an application that is running on an Amazon Linux 2 Amazon EC2 instance in the VPC. The application must retrieve an Amazon RDS database secret that is stored in AWS Secrets Manager through a private VPC endpoint. An on-premises application provides internal RESTful API service that can be reached by URL (https://api.example.internal). Two on-premises Windows DNS servers provide internal DNS resolution.

The application on the EC2 instance needs to call the internal API service that is deployed in the on-premises environment. When the application on the EC2 instance attempts to call the internal API service by referring to the hostname that is assigned to the service, the call fails. When a network engineer tests the API service call from the same EC2 instance by using the API service's IP address, the call is successful.

What should the network engineer do to resolve this issue and prevent the same problem from affecting other resources in the VPC?

A. Create a new DHCP options set that specifies the on-premises Windows DNS servers. Associate the new DHCP options set with the existing VPC. Reboot the Amazon Linux 2 EC2 instance.

B. Create an Amazon Route 53 Resolver rule. Associate the rule with the VPC. Configure the rule to forward DNS queries to the on-premises Windows DNS servers if the domain name matches example.internal.

C. Modify the local host file in the Amazon Linux 2 EC2 instance in the VPMap the service domain name (api.example.internal) to the IP address of the internal API service.

D. Modify the local /etc/resolv.conf file in the Amazon Linux 2 EC2 instance in the VPC. Change the IP addresses of the name servers in the file to the IP addresses of the company's on-premises Windows DNS servers.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 88
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has several production applications across different accounts in the AWS Cloud. The company operates from the us-east-1 Region only. Only certain partner companies can access the applications. The applications are running on Amazon EC2 instances that are in an Auto Scaling group behind an Application Load Balancer (ALB). The EC2 instances are in private subnets and allow traffic only from the ALB. The ALB is in a public subnet and allows inbound traffic only from partner network IP address ranges over port 80.

When the company adds a new partner, the company must allow the IP address range of the partner network in the security group that is associated with the ALB in each account. A network engineer must implement a solution to centrally manage the partner network IP address ranges.

Which solution will meet these requirements in the MOST operationally efficient manner?

A. Create an Amazon DynamoDB table to maintain all IP address ranges and security groups that need to be updated. Update the DynamoDB table with the new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IP address ranges and security groups from the DynamoDB table to update the security groups. Deploy this solution in all accounts.

B. Create a new prefix list. Add all allowed IP address ranges to the prefix list. Use Amazon EventBridge (Amazon CloudWatch Events) rules to invoke an AWS Lambda function to update security groups whenever a new IP address range is added to the prefix list. Deploy this solution in all accounts.

C. Create a new prefix list. Add all allowed IP address ranges to the prefix list. Share the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM). Update security groups to use the prefix list instead of the partner IP address range. Update the prefix list with the new IP address range when the company adds a new partner.

D. Create an Amazon S3 bucket to maintain all IP address ranges and security groups that need to be updated. Update the S3 bucket with the new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IP address ranges and security groups from the S3 bucket to update the security groups. Deploy this solution in all accounts.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 89
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company uses a 1 Gbps AWS Direct Connect connection to connect its AWS environment to its on-premises data center. The connection provides employees with access to an application VPC that is hosted on AWS. Many remote employees use a company-provided VPN to connect to the data center. These employees are reporting slowness when they access the application during business hours. On-premises users have started to report similar slowness while they are in the office.

The company plans to build an additional application on AWS. On-site and remote employees will use the additional application. After the deployment of this additional application, the company will need 20% more bandwidth than the company currently uses. With the increased usage, the company wants to add resiliency to the AWS connectivity. A network engineer must review the current implementation and must make improvements within a limited budget.

What should the network engineer do to meet these requirements MOST cost-effectively?

A. Set up a new 1 Gbps Direct Connect dedicated connection to accommodate the additional traffic load from remote employees and the additional application. Create a link aggregation group (LAG).

B. Deploy an AWS Site-to-Site VPN connection to the application VPC. Configure the on-premises routing for the remote employees to connect to the Site-to-Site VPN connection.

C. Deploy Amazon Workspaces into the application VPInstruct the remote employees to connect to Workspaces.

D. Replace the existing 1 Gbps Direct Connect connection with two new 2 Gbps Direct Connect hosted connections. Create an AWS Client VPN endpoint in the application VPC. Instruct the remote employees to connect to the Client VPN endpoint.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 90

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has a global network and is using transit gateways to connect AWS Regions together. The company finds that two Amazon EC2 instances in different Regions are unable to communicate with each other. A network engineer needs to troubleshoot this connectivity issue.

What should the network engineer do to meet this requirement?

A. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables and in the VPC route tables. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

B. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables are correct. Use AWS Firewall Manager to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

C. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables are correct. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

D. Use VPC Reachability Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables are correct. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 91

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company needs to transfer data between its VPC and its on-premises data center. The data must travel through a connection that has dedicated bandwidth. The data also must be encrypted in transit. The company has been working with an AWS Partner Network (APN) Partner to establish the connection.

Which combination of steps will meet these requirements? (Choose three.)

A. Request a hosted connection from the APN Partner.

B. Request a hosted public VIF from the APN Partner.

C. Create an AWS Site-to-Site VPN connection.

D. Create an AWS Client VPN connection.

E. Create a private VIF.

F. Create a public VIF.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 92

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's security guidelines state that all outbound traffic from a VPC to the company's on-premises data center must pass through a security appliance. The security appliance runs on an Amazon EC2 instance. A network engineer needs to improve the network performance between the on-premises data center and the security appliance.

Which actions should the network engineer take to meet these requirements? (Choose two.)

A. Use an EC2 instance that supports enhanced networking.

B. Send outbound traffic through a transit gateway.

C. Increase the EC2 instance size.

D. Place the EC2 instance in a placement group within the VPC.

E. Attach multiple elastic network interfaces to the EC2 instance.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 93

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's application team is unable to launch new resources into its VPC. A network engineer discovers that the VPC has run out of usable IP addresses. The VPC CIDR block is 172.16.0.0/16.

Which additional CIDR block can the network engineer attach to the VPC?

A. 172.17.0.0/29

B. 10.0.0.0/16

C. 172.17.0.0/16

D. 192.168.0.0/16

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 94
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A financial trading company is using Amazon EC2 instances to run its trading platform. Part of the company's trading platform includes a third-party pricing service that the EC2 instances communicate with over UDP on port 50000.

Recently, the company has had problems with the pricing service. Some of the responses from the pricing service appear to be incorrectly formatted and are not being processed successfully. The third-party vendor requests access to the data that the pricing service is returning. The third-party vendor wants to capture request and response data for debugging by logging in to an EC2 instance that accesses the pricing service. The company prohibits direct access to production systems and requires all log analysis to be performed in a dedicated monitoring account.

Which set of steps should a network engineer take to capture the data and meet these requirements?

A. 1. Configure VPC flow logs to capture the data that flows in the VPC.
2. Send the data to an Amazon S3 bucket.
3. In the monitoring account, extract the data that flows to the EC2 instance's IP address and filter the traffic for the UDP data.
4. Provide the data to the third-party vendor.

B. 1. Configure a traffic mirror filter to capture the UDP data.
2. Configure Traffic Mirroring to capture the traffic for the EC2 instance's elastic network interface.
3. Configure a packet inspection package on a new EC2 instance in the production environment. Use the elastic network interface of the new EC2 instance as the target for the traffic mirror.
4. Extract the data by using the packet inspection package.
5. Provide the data to the third-party vendor.

C. 1. Configure a traffic mirror filter to capture the UDP data.
2. Configure Traffic Mirroring to capture the traffic for the EC2 instance's elastic network interface.
3. Configure a packet inspection package on a new EC2 instance in the monitoring account. Use the elastic network interface of the new EC2 instance as the target for the traffic mirror.
4. Extract the data by using the packet inspection package.
5. Provide the data to the third-party vendor.

D. 1. Create a new Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to the EC2 instance.
2. Log in to the EC2 instance in the production environment. Run the tcpdump command to capture the UDP data on the EBS volume.
3. Export the data from the EBS volume to Amazon S3.
4. Provide the data to the third-party vendor.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 95

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's network engineer is configuring an AWS Site-to-Site VPN connection between a transit gateway and the company's on-premises network. The Site-to-Site VPN connection is configured to use BGP over two tunnels in active/active mode with equal-cost multi-path (ECMP) routing activated on the transit gateway.

When the network engineer attempts to send traffic from the on-premises network to an Amazon EC2 instance, traffic is sent over the first tunnel. However, return traffic is received over the second tunnel and is dropped at the customer gateway. The network engineer must resolve this issue without reducing the overall VPN bandwidth.

Which solution will meet these requirements?

A. Configure the customer gateway to use AS PATH prepending and local preference to prefer one tunnel over the other.

B. Configure the Site-to-Site VPN options to set the first tunnel as the primary tunnel to eliminate asymmetric routing.

C. Configure the virtual tunnel interfaces on the customer gateway to allow asymmetric routing.

D. Configure the Site-to-Site VPN to use static routing in active/active mode to ensure that traffic flows over a preferred path.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 96

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company runs an application on Amazon EC2 instances. A network engineer implements a NAT gateway in the application's VPC to replace self-managed NAT instances. After the network engineer shifts traffic from the self-managed NAT instances to the NAT gateway, users begin to report issues.

During troubleshooting, the network engineer discovers that the connection to the application is closing after approximately 6 minutes of inactivity.

What should the network engineer do to resolve this issue?

A. Check for increases in the IdleTimeoutCount Amazon CloudWatch metric for the NAT gateway. Configure TCP keepalive on the application EC2 instances.

B. Check for increases in the ErrorPortAllocation Amazon CloudWatch metric for the NAT gateway. Configure an HTTP timeout value on the application EC2 instances.

C. Check for increases in the PacketsDropCount Amazon CloudWatch metric for the NAT gateway. Configure an HTTPS timeout value on the application EC2 instances.

D. Check for decreases in the ActiveConnectionCount Amazon CloudWatch metric for the NAT gateway. Configure UDP keepalive on the application EC2 instances.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 97

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A software-as-a-service (SaaS) company is migrating its private SaaS application to AWS. The company has hundreds of customers that connect to multiple data centers by using VPN tunnels. As the number of customers has grown, the company has experienced more difficulty in its effort to manage routing and segmentation of customers with complex NAT rules.

After the migration to AWS is complete, the company's AWS customers must be able to access the SaaS application directly from their VPCs. Meanwhile, the company's on-premises customers still must be able to connect through IPsec encrypted tunnels.

Which solution will meet these requirements?

A. Connect the AWS customer VPCs to a shared transit gateway. Use AWS Site-to-Site VPN connections to the transit gateway for the on-premises customers

B. Use AWS PrivateLink to connect the AWS customers. Use a third-party routing appliance in the SaaS application VPC to terminate onpremises Site-to-Site VPN connections.

C. Peer each AWS customer's VPCs to the VPC that hosts the SaaS application. Create AWS Site-to-Site VPN connections on the SaaS VPC virtual private gateway.

D. Use Site-to-Site VPN tunnels to connect each AWS customer's VPCs to the VPC that hosts the SaaS application. Use AWS Site-to-Site VPN to connect the on-premises customers.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 98
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's existing AWS environment contains public application servers that run on Amazon EC2 instances. The application servers run in a VPC subnet. Each server is associated with an Elastic IP address.

The company has a new requirement for firewall inspection of all traffic from the internet before the traffic reaches any EC2 instances. A security engineer has deployed and configured a Gateway Load Balancer (GLB) in a standalone VPC with a fleet of third-party firewalls.

How should a network engineer update the environment to ensure that the traffic travels across the fleet of firewalls?

A. Deploy a transit gateway. Attach a GLB endpoint to the transit gateway. Attach the application VPC to the transit gateway. Update the application subnet route table's default route destination to be the GLB endpoint. Ensure that the EC2 instances' security group allows traffic from the GLB endpoint.

B. Update the application subnet route table to have a default route to the GLOn the standalone VPC that contains the firewall fleet, add a route in the route table for the application VPC's CIDR block with the GLB endpoint as the destination. Update the EC2 instances' security group to allow traffic from the GLB.

C. Provision a GLB endpoint in the application VPC in a new subnet. Create a gateway route table with a route that specifies the application subnet CIDR block as the destination and the GLB endpoint as the target. Associate the gateway route table with the internet gateway in the application VPUpdate the application subnet route table's default route destination to be the GLB endpoint.

D. Instruct the security engineer to move the GLB into the application VPC. Create a gateway route table. Associate the gateway route table with the application subnet. Add a default route to the gateway route table with the GLB as its destination. Update the route table on the GLB to direct traffic from the internet gateway to the application servers. Ensure that the EC2 instances' security group allows traffic from the GLB.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 99

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has an AWS Site-to-Site VPN connection between its office and its VPC. Users report occasional failure of the connection to the application that is hosted inside the VPC. A network engineer discovers in the customer gateway logs that the Internet Key Exchange (IKE) session ends when the connection to the application fails.

What should the network engineer do to bring up the IKE session if the IKE session goes down?

A. Set the dead peer detection (DPD) timeout action to Clear. Initiate traffic from the VPC to on premises.

B. Set the dead peer detection (DPD) timeout action to Restart. Initiate traffic from on premises to the VPC.

C. Set the dead peer detection (DPD) timeout action to None. Initiate traffic from the VPC to on premises.

D. Set the dead peer detection (DPD) timeout action to Cancel. Initiate traffic from on premises to the VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 100
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer is designing a hybrid networking environment that will connect a company's corporate network to the company's AWS environment. The AWS environment consists of 30 VPCs in 3 AWS Regions.

The network engineer needs to implement a solution to centrally filter traffic by using a firewall that the company's security team has approved. The solution must give all the VPCs the ability to connect to each other. Connectivity between AWS and the corporate network must meet a minimum bandwidth requirement of 2 Gbps.

Which solution will meet these requirements?

A. Deploy an IPsec VPN connection between the corporate network and a new transit gateway. Connect all VPCs to the transit gateway. Associate the approved firewall with the transit gateway.

B. Deploy a single 10 Gbps AWS Direct Connect connection between the corporate network and virtual private gateway of each VPC. Connect the virtual private gateways to a Direct Connect gateway. Build an IPsec tunnel to a new transit VPC. Deploy the approved firewall to the transit VPC.

C. Deploy two 1 Gbps AWS Direct Connect connections in different Direct Connect locations to connect to the corporate network. Build a transit VIF on each connection to a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway for each Region. Configure the VIFs to use equal-cost multipath (ECMP) routing. Connect all the VPCs in the three Regions to the transit gateway. Configure the transit gateway route table to route traffic to an inspection VPDeploy the approved firewall to the inspection VPC.

D. Deploy four 1 Gbps AWS Direct Connect connections in different Direct Connect locations to connect to the corporate network. Build a transit VIF on each connection to a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway for each Region. Connect the transit gateways by using a transit gateway peering attachment. Configure the VIFs to use equal-cost multipath (ECMP) routing. Configure transit gateway route tables to route traffic to an inspection VPC. Deploy the approved firewall to the inspection VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 101
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company uses an AWS Direct Connect private VIF with a link aggregation group (LAG) that consists of two 10 Gbps connections. The company's security team has implemented a new requirement for external network connections to provide layer 2 encryption. The company's network team plans to use MACsec support for Direct Connect to meet the new requirement.

Which combination of steps should the network team take to implement this functionality? (Choose three.)

A. Create a new Direct Connect LAG with new circuits and ports that support MACsec.

B. Associate the MACsec Connectivity Association Key (CAK) and the Connection Key Name (CKN) with the new LAG.

C. Associate the Internet Key Exchange (IKE) with the existing LAG.

D. Configure the MACsec encryption mode on the existing LAG.

E. Configure the MACsec encryption mode on the new LAG.

F. Configure the MACsec encryption mode on each Direct Connect connection that makes up the existing LAG.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 102
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company recently implemented a security policy that prohibits developers from launching VPC network infrastructure. The policy states that any time a NAT gateway is launched in a VPC, the company's network security team must immediately receive an alert to terminate the NAT gateway. The network security team needs to implement a solution that can be deployed across AWS accounts with the least possible administrative overhead. The solution also must provide the network security team with a simple way to view compliance history.

Which solution will meet these requirements?

A. Develop a script that programmatically checks for NAT gateways in an AWS account, sends an email alert, and terminates the NAT gateway if a NAT gateway is detected. Deploy the script on an Amazon EC2 instance in each account. Use a cron job to run the script every 5 minutes. Log the results of the checks to an Amazon RDS for MySQL database.

B. Create an AWS Lambda function that programmatically checks for NAT gateways in an AWS account, sends an email alert, and terminates the NAT gateway if a NAT gateway is detected. Deploy the Lambda function to each account by using AWS Serverless Application Model (AWS SAM) templates. Store the results of the checks on an Amazon OpenSearch Service cluster in each account.

C. Enable Amazon GuardDuty. Create an Amazon EventBridge rule for the Behavior:EC2/NATGatewayCreation GuardDuty finding type. Configure the rule to invoke an AWS Step Functions state machine to send an email alert and terminate a NAT gateway if a NAT gateway is detected. Store the runtime log as a text file in an Amazon S3 bucket.

D. Create a custom AWS Config rule that checks for NAT gateways in an AWS account. Configure the AWS Config rule to perform an AWS Systems Manager Automation remediation action to send an email alert and terminate the NAT gateway if a NAT gateway is detected. Deploy the AWS Config rule and the Systems Manager runbooks to each account by using AWS CloudFormation StackSets

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 103

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is running an online game on AWS. The game is played globally and is gaining popularity. Users are reporting problems with the game's responsiveness. Replay rates are dropping, and the company is losing subscribers. Game servers are located in the us-west-2 Region and use an Elastic Load Balancer to distribute client traffic.

The company has decided to deploy game servers to 11 additional AWS Regions to reduce the round-trip times of network traffic to game clients. A network engineer must design a DNS solution that uses Amazon Route 53 to ensure that user traffic is delivered to game servers with an optimal response time.

What should the network engineer do to meet these requirements?

A. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a weighted routing policy. Calculate the weight by using the number of clients in each Region.

B. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a latency routing policy. Set the Region to the Region where the Elastic Load Balancer is deployed.

C. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a multivalue answer routing policy. Test latency from the game client, and connect to the server with the best response.

D. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a geolocation routing policy. Set the location to the Region where the Elastic Load Balancer is deployed.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 104
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer needs to build an encrypted connection between an on-premises data center and a VPC. The network engineer attaches the VPC to a virtual private gateway and sets up an AWS Site-to-Site VPN connection. The VPN tunnel is UP after configuration and is working. However, during rekey for phase 2 of the VPN negotiation, the customer gateway device is receiving different parameters than the parameters that the device is configured to support.

The network engineer checks the IPsec configuration of the VPN tunnel. The network engineer notices that the customer gateway device is configured with the most secure encryption algorithms that the AWS Site-to-Site VPN configuration file provides.

What should the network engineer do to troubleshoot and correct the issue?

A. Check the native virtual private gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the virtual private gateway requires.

B. Check the native customer gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the customer gateway requires.

C. Check Amazon CloudWatch logs of the virtual private gateway. Restrict the VPN tunnel options to the specific VPN parameters that the virtual private gateway requires.

D. Check Amazon CloudWatch logs of the customer gateway. Restrict the VPN tunnel options to the specific VPN parameters that the customer gateway requires.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 105
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is growing rapidly. Data transfers between the company's on-premises systems and Amazon EC2 instances that run in VPCs are limited by the throughput of a single AWS Site-to-Site VPN connection between the company's on-premises data center firewall and an AWS Transit Gateway.

A network engineer must resolve the throttling by designing a solution that is highly available and secure. The solution also must scale the VPN throughput from on premises to the VPC resources to support the increase in traffic.

Which solution will meet these requirements?

A. Configure multiple dynamic BGP-based Site-to-Site VPN connections to the transit gateway. Configure equal-cost multi-path routing (ECMP).

B. Configure multiple static routing-based Site-to-Site VPN connections to the transit gateway. Configure equal-cost multi-path routing (ECMP).

C. Configure a new Site-to-Site VPN connection to the transit gateway. Enable acceleration for the Site-to-Site VPN connection.

D. Configure a software appliance-based VPN connection over the internet from the on-premises firewall to an EC2 instance that has a large instance size and networking capabilities.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 106

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company uses Amazon Route 53 to host a public hosted zone for example.com. A network engineer recently reduced the TTL on several records to 60 seconds. The network engineer wants to assess whether the change has increased the number of queries to Route 53 beyond the expected levels that the company identified before the change. The network engineer must obtain the number of queries that have been made to the example.com public hosted zone.

Which solution will provide this information?

A. Create a new trail in AWS CloudTrail to include Route 53 data events. Send logs to Amazon CloudWatch Logs. Set up a CloudWatch metric filter to count the number of queries and create graphs.

B. Use Amazon CloudWatch to access the AWS/Route 53 namespace and to check the DNSQueries metric for the public hosted zone.

C. Use Amazon CloudWatch to access the AWS/Route 53 Resolver namespace and to check the InboundQueryVolume metric for a specific endpoint.

D. Configure logging to Amazon CloudWatch for the public hosted zone. Set up a CloudWatch metric filter to count the number of queries and create graphs.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 107

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is establishing connectivity between its on-premises site and an existing VPC on AWS to meet a new security requirement. According to the new requirement, all public DNS queries must use an on-premises DNS security solution. The company's security team has allowed an exception for the AWS service endpoints because the company is using VPC endpoints to access AWS services.

Which combination of steps should a network engineer take to configure the architecture to meet these requirements? (Choose three.)

A. Create a system rule for the domain name "." (dot) with a target IP address of the on-premises DNS security solution.

B. Create a new DHCP options set that provides the IP address of the on-premises DNS security solution. Update the VPC to use this new DHCP options set.

C. Create an Amazon Route 53 Resolver inbound endpoint. Associate this endpoint with the VPC.

D. Create an Amazon Route 53 Resolver outbound endpoint. Associate this endpoint with the VPC.

E. Create a system rule for the domain name amazonaws.com.

F. Create a forwarding rule for the domain name "." (dot) with a target IP address of the on-premises DNS security solution.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 108
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer is designing the DNS architecture for a new AWS environment. The environment must be able to resolve DNS names of endpoints on premises, and the on-premises systems must be able to resolve the names of AWS endpoints. The DNS architecture must give individual accounts the ability to manage subdomains.

The network engineer needs to create a single set of rules that will work across multiple accounts to control this behavior. In addition, the network engineer must use AWS native services whenever possible.

Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Create an Amazon Route 53 private hosted zone for the overall cloud domain. Plan to create subdomains that align to other AWS accounts that are associated with the central Route 53 private hosted zone.

B. Create AWS Directory Service for Microsoft Active Directory server endpoints in the central AWS account that hosts the private hosted zone for the overall cloud domain. Create a conditional forwarding rule in Microsoft Active Directory DNS to forward traffic to a DNS resolver endpoint on premises. Create another rule to forward traffic between subdomains to the VPC resolver.

C. Create Amazon Route 53 Resolver inbound and outbound endpoints in the central AWS account that hosts the private hosted zone for the overall cloud domain. Create a forwarding rule to forward traffic to a DNS resolver endpoint on premises. Create another rule to forward traffic between subdomains to the Resolver inbound endpoint.

D. Ensure that networking exists between the other accounts and the central account so that traffic can reach the AWS Directory Service for Microsoft Active Directory DNS endpoints.

E. Ensure that networking exists between the other accounts and the central account so that traffic can reach the Amazon Route 53 Resolver endpoints.

F. Share the Amazon Route 53 Resolver rules between accounts by using AWS Resource Access Manager (AWS RAM). Ensure that networking exists between the other accounts and the central account so that traffic can reach the Route 53 Resolver endpoints.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 109

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company wants to migrate its DNS registrar and DNS hosting to Amazon Route 53. The company website receives tens of thousands of visits each day, and the company's current DNS provider cannot keep up. The company wants to migrate as quickly as possible but cannot tolerate any downtime.

Which solution will meet these requirements?

A. Transfer the domain name to Route 53. Create a Route 53 private hosted zone, and copy all the existing DNS records. Update the name servers on the domain to use the name servers that are specified in the newly created private hosted zone.

B. Copy all DNS records from the existing DNS servers to a Route 53 private hosted zone. Update the name servers with the existing registrar to use the private hosted zone name servers. Transfer the domain name to Route 53. Ensure that all the changes have propagated.

C. Transfer the domain name to Route 53. Create a Route 53 public hosted zone, and copy all the existing DNS records. Set the TTL value on each record to 1 second. Update the name servers on the domain to use the name servers that are specified in the newly created public hosted zone.

D. Copy all DNS records from the existing DNS servers to a Route 53 public hosted zone. Update the name servers with the existing registrar to use the Route 53 name servers for the hosted zone. When the changes have propagated, perform a domain name transfer to Route 53.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 110

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has an AWS account with four VPCs in the us-east-1 Region. The VPCs consist of a development VPC and three production VPCs that host various workloads.

The company has extended its on-premises data center to AWS with AWS Direct Connect by using a Direct Connect gateway. The company now wants to establish connectivity to its production VPCs and development VPC from on premises. The production VPCs are allowed to route data to each other. However, the development VPC must be isolated from the production VPCs. No data can flow between the development VPC and the production VPCs.

In preparation to implement this solution, a network engineer creates a transit gateway with a single transit gateway route table. Default route table association and default route table propagation are turned off. The network engineer attaches the production VPCs, the development VPC, and the Direct Connect gateway to the transit gateway. For each VPC route table, the network engineer adds a route to 0.0.0.0/0 with the transit gateway as the next destination.

Which combination of steps should the network engineer take next to complete this solution? (Choose three.)

A. Associate the production VPC attachments with the existing transit gateway route table. Propagate the routes from these attachments.

B. Associate all the attachments with the existing transit gateway route table. Propagate the routes from these attachments.

C. Associate the Direct Connect gateway attachment with the existing transit gateway route table. Propagate the Direct Connect gateway attachment to this route table.

D. Change the security group inbound rules on the existing transit gateway network interfaces in the development VPC to allow connections to and from the on-premises CIDR range only.

E. Create a new transit gateway route table. Associate the new route table with the development VPC attachment. Propagate the Direct Connect gateway and development VPC attachment to the new route table.

F. Create a new transit gateway with default route table association and default route table propagation turned on. Attach the Direct Connect gateway and development VPC to the new transit gateway.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 111
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer needs to provide dual-stack connectivity between a company's office location and an AWS account. The company's on-premises router supports dual-stack connectivity, and the VPC has been configured with dual-stack support. The company has set up two AWS Direct Connect connections to the office location. This connectivity must be highly available and must be reliable for latency-sensitive traffic.

Which solutions will meet these requirements? (Choose two.)

A. Configure a single private VIF on each Direct Connect connection. Add both IPv4 and IPv6 peering to each private VIF. Configure the on- premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6 peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

B. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with the IPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6 peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

C. Configure a single private VIF and IPv4 peering on each Direct Connect connection. Configure the on-premises equipment with this peering to advertise the IPv6 routes in the same BGP neighbor configuration. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

D. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with the IPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise all IPv4 routes and IPv6 routes on all peering sessions. Keep the Bidirectional Forwarding Detection (BFD) configuration unchanged.

E. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with the IPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6 peering. Reduce the BGP hello timer to 5 seconds on both the on-premises equipment and the Direct Connect configuration.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 112

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company recently started using AWS Client VPN to give its remote users the ability to access resources in multiple peered VPCs and resources in the company's on-premises data center. The Client VPN endpoint route table has a single entry of 0.0.0.0/0. The Client VPN endpoint is using a new security group that has no inbound rules and a single outbound rule that allows all traffic to 0.0.0.0/0.

Multiple remote users report that web search results are showing incorrect geographic location information for the users.

Which combination of steps should a network engineer take to resolve this issue with the LEAST amount of service interruption? (Choose three.)

A. Switch users to AWS Site-to-Site VPNs.

B. Enable the split-tunnel option on the Client VPN endpoint.

C. Add routes for the peered VPCs and for the on-premises data center to the Client VPN route table.

D. Remove the 0.0.0.0/0 outbound rule from the security group that the Client VPN endpoint uses.

E. Delete and recreate the Client VPN endpoint in a different VPC.

F. Remove the 0.0.0.0/0 entry from the Client VPN endpoint route table.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 113
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has set up hybrid connectivity between its VPCs and its on-premises data center. The company has the on-premises.example.com subdomain configured at its DNS server in the on-premises data center. The company is using the aws.example.com subdomain for workloads that run on AWS across different VPCs and accounts. Resources in both environments can access each other by using IP addresses. The company wants workloads in the VPCs to be able to access resources on premises by using the on-premises.example.com DNS names.

Which solution will meet these requirements with MINIMUM management of resources?

A. Create an Amazon Route 53 Resolver outbound endpoint. Configure a Resolver rule that conditionally forwards DNS queries for on-premises.example.com to the on-premises DNS server. Associate the rule with the VPCs.

B. Create an Amazon Route 53 Resolver inbound endpoint and a Resolver outbound endpoint. Configure a Resolver rule that conditionally forwards DNS queries for on-premises.example.com to the on-premises DNS server. Associate the rule with the VPCs.

C. Launch an Amazon EC2 instance. Install and configure BIND software to conditionally forward DNS queries for on-premises.example.com to the on-premises DNS server. Configure the EC2 instance's IP address as a custom DNS server in each VPC.

D. Launch an Amazon EC2 instance in each VPC. Install and configure BIND software to conditionally forward DNS queries for on-premises.example.com to the on-premises DNS server. Configure the EC2 instance's IP address as a custom DNS server in each VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 114

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is in the early stage of AWS Cloud adoption. The company has an application that is running in an on-premises data center in Asia. The company needs to deploy new applications in the us-east-1 Region. The applications in the cloud need connectivity to the on-premises data center.

The company needs to set up a communication channel between AWS and the data center. The solution must improve latency, minimize the possibility of performance impact from transcontinental routing over the public internet, and encrypt data in transit.

Which solution will meet these requirements in the LEAST amount of time?

A. Create an AWS Site-to-Site VPN connection with acceleration turned on. Create a virtual private gateway. Attach the Site-to-Site VPN connection to the virtual private gateway. Attach the virtual private gateway to the VPC where the applications will be deployed.

B. Create an AWS Site-to-Site VPN connection with acceleration turned on. Create a transit gateway. Attach the Site-to-Site VPN connection to the transit gateway. Create a transit gateway attachment to the VPC where the applications will be deployed.

C. Create an AWS Direct Connect connection. Create a virtual private gateway. Create a public VIF and a private VIF that use the virtual private gateway. Create an AWS Site-to-Site VPN connection over the public VIF.

D. Create an AWS Site-to-Site VPN connection with acceleration turned off. Create a transit gateway. Attach the Site-to-Site VPN connection to the transit gateway. Create a transit gateway attachment to the VPC where the applications will be deployed.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 115

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is moving its record-keeping application to the AWS Cloud. All traffic between the company's on-premises data center and AWS must be encrypted at all times and at every transit device during the migration.

The application will reside across multiple Availability Zones in a single AWS Region. The application will use existing 10 Gbps AWS Direct Connect dedicated connections with a MACsec capable port. A network engineer must ensure that the Direct Connect connection is secured accordingly at every transit device.

The network engineer creates a Connection Key Name and Connectivity Association Key (CKN/CAK) pair for the MACsec secret key.

Which combination of additional steps should the network engineer take to meet the requirements? (Choose two.)

A. Configure the on-premises router with the MACsec secret key.

B. Update the connection's MACsec encryption mode to must_encrypt. Then associate the CKN/CAK pair with the connection.

C. Update the connection's MACsec encryption mode to should encrypt. Then associate the CKN/CAK pair with the connection.

D. Associate the CKN/CAK pair with the connection. Then update the connection's MACsec encryption mode to must_encrypt.

E. Associate the CKN/CAK pair with the connection. Then update the connection's MACsec encryption mode to should_encrypt.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 116

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer is designing hybrid connectivity with AWS Direct Connect and AWS Transit Gateway. A transit gateway is attached to a Direct Connect gateway and 19 VPCs across different AWS accounts. Two new VPCs are being attached to the transit gateway. The IP address administrator has assigned 10.0.32.0/21 to the first VPC and 10.0.40.0/21 to the second VPC. The prefix list has one CIDR block remaining before the prefix list reaches the quota for the maximum number of entries.

What should the network engineer do to advertise the routes from AWS to on premises to meet these requirements?

A. Add 10.0.32.0/21 and 10.0.40.0/21 to both AWS managed prefix lists.

B. Add 10.0.32.0/21 and 10.0.40.0/21 to the allowed prefix list.

C. Add 10.0.32.0/20 to both AWS managed prefix lists.

D. Add 10.0.32.0/20 to the allowed prefix list.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 117

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

Two companies are merging. The companies have a large AWS presence with multiple VPCs and are designing connectivity between their AWS networks. Both companies are using AWS Direct Connect with a Direct Connect gateway. Each company also has a transit gateway and multiple AWS Site-to-Site VPN connections from its transit gateway to on-premises resources. The new solution must optimize network visibility, throughput, logging, and monitoring.

Which solution will meet these requirements?

A. Configure a Site-to-Site VPN connection between each company's transit gateway to establish reachability between the respective networks. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use VPC Reachability Analyzer to monitor connectivity.

B. Configure a Site-to-Site VPN connection between each company's transit gateway to establish reachability between the respective networks. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use AWS Transit Gateway Network Manager to monitor the transit gateways and their respective connections.

C. Configure transit gateway peering between each company's transit gateway. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use VPC Reachability Analyzer to monitor connectivity.

D. Configure transit gateway peering between each company's transit gateway. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use AWS Transit Gateway Network Manager to monitor the transit gateways, their respective connections, and the transit gateway peering link.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 118

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has a single VPC in the us-east-1 Region. The company is planning to set up a new VPC in the us-east-2 Region. The existing VPC has an AWS Site-to-Site VPN connection to the company's on-premises environment and uses a virtual private gateway.

A network engineer needs to implement a solution to establish connectivity between the existing VPC and the new VPC. The solution also must implement support for IPv6 for the new VPC. The company has new on-premises resources that need to connect to VPC resources by using IPv6 addresses.

Which solution will meet these requirements?

A. Create a new virtual private gateway in us-east-1. Attach the new virtual private gateway to the new VPC. Create two new Site-to-Site VPN connections to the new virtual private gateway with IPv4 and IPv6 support. Configure routing between the VPCs by using VPC peering.

B. Create a transit gateway in us-east-1 and in us-east-2. Attach the existing VPC and the new VPC to each transit gateway. Create a new Site-to-Site VPN connection to each transit gateway with IPv4 and IPv6 support. Configure transit gateway peering. Configure routing between the VPCs and the on-premises environment.

C. Create a new virtual private gateway in us-east-2. Attach the new virtual private gateway to the new VPCreate two new Site-to-Site VPN connections to the new virtual private gateway with IPv4 and IPv6 support. Configure routing between the VPCs by using VPC peering.

D. Create a transit gateway in us-east-1. Attach the existing VPC and the new VPC to the transit gateway. Create two new Site-to-Site VPN connections to the transit gateway with IPv4 and IPv6 support. Configure transit gateway peering. Configure routing between the VPCs and the on-premises environment.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 119

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A network engineer is working on a private DNS design to integrate AWS workloads and on-premises resources. The AWS deployment consists of five VPCs in the eu-west-1 Region that connect to the on-premises network over AWS Direct Connect. The VPCs communicate with each other by using a transit gateway. Each VPC is associated with a private hosted zone that uses the aws.example.internal domain. The network engineer creates an Amazon Route 53 Resolver outbound endpoint in a shared services VPC and attaches the shared services VPC to the transit gateway.

The network engineer is implementing a solution for DNS resolution. Queries for hostnames that end with aws.example.internal must use the private hosted zone. Queries for hostnames that end with all other domains must be forwarded to a private on-premises DNS resolver.

Which solution will meet these requirements?

A. Add a forwarding rule for "*" that targets the on-premises server's DNS IP address. Add a system rule for aws.example.internal that targets Route 53 Resolver.

B. Add a forwarding rule for aws.example.internal that targets Route 53 Resolver. Add a system rule for "." that targets the Route 53 Resolver outbound endpoint.

C. Add a forwarding rule for "*" that targets the Route 53 Resolver outbound endpoint.

D. Add a forwarding rule for "." that targets the Route 53 Resolver outbound endpoint.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 120

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A global film production company uses the AWS Cloud to encode and store its video content before distribution. The company's three global offices are connected to the us-east-1 Region through AWS Site-to-Site VPN links that terminate on a transit gateway with BGP routing activated.

The company recently started to produce content at a higher resolution to support 8K streaming. The size of the content files has increased to three times the size of the content files from the previous format. Uploads of files to Amazon EC2 instances are taking 10 times longer than they did with the previous format.

Which actions should a network engineer recommend to reduce the upload times? (Choose two.)

A. Create a second VPN tunnel from each office location to the transit gateway. Activate equal-cost multi-path (ECMP) routing.

B. Modify the transit gateway to activate Jumbo MTU on the VPN tunnels to each office location.

C. Replace the existing VPN tunnels with new tunnels that have acceleration activated.

D. Upgrade each EC2 instance to a modern instance type. Activate Jumbo MTU in the operating system.

E. Replace the existing VPN tunnels with new tunnels that have IGMP activated.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 121
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

An application team for a startup company is deploying a new multi-tier application into the AWS Cloud. The application will be hosted on a fleet of Amazon EC2 instances that run in an Auto Scaling group behind a publicly accessible Network Load Balancer (NLB). The application requires the clients to work with UDP traffic and TCP traffic.

In the near term, the application will serve only users within the same geographic location. The application team plans to extend the application to a global audience and will move the deployment to multiple AWS Regions around the world to bring the application closer to the end users. The application team wants to use the new Regions to deploy new versions of the application and wants to be able to control the amount of traffic that each Region receives during these rollouts. In addition, the application team must minimize first-byte latency and jitter (randomized delay) for the end users.

How should the application team design the network architecture for the application to meet these requirements?

A. Create an Amazon CloudFront distribution to align to each Regional deployment. Set the NLB for each Region as the origin for each CloudFront distribution. Use an Amazon Route 53 weighted routing policy to control traffic to the newer Regional deployments.

B. Create an AWS Global Accelerator accelerator and listeners for the required ports. Configure endpoint groups for each Region. Configure a traffic dial for the endpoint groups to control traffic to the newer Regional deployments. Register the NLBs with the endpoint groups.

C. Use Amazon S3 Transfer Acceleration for the application in each Region. Adjust the amount of traffic that each Region receives from the Transfer Acceleration endpoints to the Regional NLBs.

D. Create an Amazon CloudFront distribution that includes an origin group. Set the NLB for each Region as the origins for the origin group. Use an Amazon Route 53 latency routing policy to control traffic to the new Regional deployments.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 122
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is deploying a new stateless web application on AWS. The web application will run on Amazon EC2 instances in private subnets behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The web application has a stateful management application for administration that will run on EC2 instances that are in a separate Auto Scaling group.

The company wants to access the management application by using the same URL as the web application, with a path prefix of/management. The protocol, hostname, and port number must be the same for the web application and the management application. Access to the management application must be restricted to the company's on-premises IP address space. An SSL/TLS certificate from AWS Certificate Manager (ACM) will protect the web application.

Which combination of steps should a network engineer take to meet these requirements? (Choose two.)

A. Insert a rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the source-ip condition type for the on-premises IP address space. Forward requests to the management application target group if there is a match. Edit the management application target group and enable stickiness.

B. Modify the default rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the source-ip condition type for the on-premises IP address space. Forward requests to the management application target group if there is not a match. Enable group-level stickiness in the rule attributes.

C. Insert a rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the X-Forwarded-For HTTP header for the on-premises IP address space. Forward requests to the management application target group if there is a match. Enable group-level stickiness in the rule attributes.

D. Modify the default rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the source-ip condition type for the on-premises IP address space. Forward requests to the web application target group if there is not a match.

E. Forward all requests to the web application target group. Edit the web application target group and disable stickiness.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 123

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company deploys a software solution on Amazon EC2 instances that are in a cluster placement group. The solution's UI is a single HTML page. The HTML file size is 1,024 bytes. The software processes files that exceed 1,024 MB in size. The software shares files over the network to clients upon request. The files are shared with the Don't Fragment flag set. Elastic network interfaces of the EC2 instances are set up with jumbo frames.

The UI is always accessible from all allowed source IP addresses, regardless of whether the source IP addresses are within a VPC, on the internet, or on premises. However, clients sometimes do not receive files that they request because the files fail to travel successfully from the software to the clients.

Which options provide a possible root cause of these failures? (Choose two.)

A. The source IP addresses are from on-premises hosts that are routed over AWS Direct Connect.

B. The source IP addresses are from on-premises hosts that are routed over AWS Site-to-Site VPN.

C. The source IP addresses are from hosts that connect over the public internet.

D. The security group of the EC2 instances does not allow ICMP traffic.

E. The operating system of the EC2 instances does not support jumbo frames.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 124
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has users who work from home. The company wants to move these users to Amazon WorkSpaces for additional security visibility.

The company has deployed WorkSpaces in its own AWS account in VPC A. A network engineer decides to provide the security visibility by using two firewall appliances behind a Gateway Load Balancer (GWLB). The network engineer provisions another VPC, VPC B, in a separate account and deploys the two firewall appliances in separate Availability Zones.

What should the network engineer do to configure the network connectivity for this solution?

A. Create a GWLB in VPC A with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the default route to the VPC endpoint.

B. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the default route to the GWLB endpoint.

C. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the WorkSpaces subnet to the VPC endpoint.

D. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the account that contains the firewall appliances to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the default route to the VPC endpoint.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 125
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company plans to run a computationally intensive data processing application on AWS. The data is highly sensitive. The VPC must have no direct internet access, and the company has applied strict network security to control access.

Data scientists will transfer data from the company's on-premises data center to the instances by using an AWS Site-to-Site VPN connection. The on-premises data center uses the network range 172.31.0.0/20 and will use the network range 172.31.16.0/20 in the application VPC.

The data scientists report that they can start new instances of the application but that they cannot transfer any data from the on-premises data center. A network engineer enables VPC flow logs and sends a ping to one of the instances to test reachability. The flow logs show the following:

```
2 123456789010 eni-1235b8ca123456789 172.31.8.29 172.31.18.139 0 0 1 4 336 1622433184 1622433194 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.18.139 172.31.8.29 0 0 1 3 252 1622433216 1622433232 REJECT OK
```

The network engineer must recommend a solution that will give the data scientists the ability to transfer data from the on-premises data center.

Which solution will meet these requirements?

A. Modify the security group for the application. Add an inbound rule to allow traffic from the on-premises data center network range to the application.

B. Modify the network ACLs for the VPC subnet. Add an inbound rule to allow traffic from the on-premises data center network range to the VPC subnet range.

C. Modify the network ACLs for the VPC subnet. Add an outbound rule to allow traffic from the VPC subnet range to the on-premises data center network range.

D. Modify the security group for the application. Add an outbound rule to allow traffic from the application to the on-premises data center network range.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 126
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company needs to temporarily scale out capacity for an on-premises application and wants to deploy new servers on Amazon EC2 instances. A network engineer must design the networking solution for the connectivity and for the application on AWS.

The EC2 instances need to share data with the existing servers in the on-premises data center. The servers must not be accessible from the internet. All traffic to the internet must route through the firewall in the on-premises data center. The servers must be able to access a third-party web application.

Which configuration will meet these requirements?

A. Create a VPC that has public subnets and private subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a NAT gateway in a public subnet. Create a route table, and associate the public subnets with the route table. Add a default route to the internet gateway. Create a route table, and associate the private subnets with the route table. Add a default route to the NAT gateway. Add routes for the data center subnets to the virtual private gateway. Deploy the application to the private subnets.

B. Create a VPC that has private subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a route table, and associate the private subnets with the route table. Add a default route to the virtual private gateway. Deploy the application to the private subnets.

C. Create a VPC that has public subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a route table, and associate the public subnets with the route table. Add a default route to the internet gateway. Add routes for the on-premises data center subnets to the virtual private gateway. Deploy the application to the public subnets.

D. Create a VPC that has public subnets and private subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a route table, and associate the public subnets with the route table. Add a default route to the internet gateway. Create a route table, and associate the private subnets with the route table. Add routes for the on-premises data center subnets to the virtual private gateway. Deploy the application to the private subnets.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 127
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is deploying a web application into two AWS Regions. The company has one VPC in each Region. Each VPC has three Amazon EC2 instances as web servers behind an Application Load Balancer (ALB). The company already has configured an Amazon Route 53 public hosted zone for example.com. Users will access the application by using the fully qualified domain name (FQDN) of app.example.com.

The company needs a DNS solution that allows global users to access the application. The solution must route the users' requests to the Region that provides the lowest response time. The solution must fail over to the Region that provides the next-lowest response time if the application is unavailable in the initially intended Region.

Which solution will meet these requirements?

A. For each ALB, create an A record that has a geolocation routing policy to route app.example.com to the IP addresses of the ALB. Configure a Route 53 HTTP health check that monitors each ALB by IP address. Associate the health check with the A records.

B. Create an A record that has a geolocation routing policy to route app.example.com to the IP addresses for both ALBs. Configure a Route 53 health check that monitors TCP port 80 for each ALB by IP address. Associate the health check with the A records.

C. Create an A record that has a latency-based routing policy to route app.example.com as an alias to one of the ALBs. Configure a Route 53 health check that monitors TCP port 80 for each ALB by IP address. Associate the health check with the A records.

D. For each ALB, create an A record that has a latency-based routing policy to route app.example.com as an alias to the ALB. Set the value for Evaluate Target Health to Yes for the records.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 128

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A consulting company manages AWS accounts for its customers. One of the company's customers needs to add intrusion prevention for its environment without having to re-architect the environment. The customer's environment includes five VPCs in two AWS Regions in the United States. VPC-to-VPC connectivity is achieved through VPC peering. The customer does not plan to increase the number of VPCs within the next 2 years. The solution must accommodate unencrypted traffic.

Which solution will meet these requirements?

A. Configure VPC security groups and network ACLs.

B. Use an AWS Network Firewall centralized deployment model in each VPC.

C. Use an AWS Network Firewall distributed deployment model in each VPC.

D. Deploy AWS Shield in each VPC.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 129

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company hosts its IT infrastructure in an on-premises data center. The company wants to migrate the infrastructure to the AWS Cloud in phases. A network engineer wants to set up a 10 Gbps AWS Direct Connect dedicated connection between the on-premises data center and VPCs. The company's network provider needs 3 months to provision the Direct Connect connection.

In the meantime, the network engineer implements a temporary solution by deploying an AWS Site-to-Site VPN connection that terminates to a virtual private gateway. The network engineer observes that the bandwidth of the Site-to-Site VPN connection is capped at 1.25 Gbps despite a powerful customer gateway device.

What should the network engineer do to improve the VPN connection bandwidth before the implementation of the Direct Connect connection?

A. Contact AWS Support to request a bandwidth quota increase for the existing Site-to-Site VPN connection.

B. Discuss the issue with the hardware vendor. Buy a bigger and more powerful customer gateway device that has faster encryption and decryption capabilities.

C. Create several additional Site-to-Site VPN connections that terminate on the same virtual gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously.

D. Create a transit gateway. Attach the VPCs to the transit gateway. Create several additional Site-to-Site VPN connections that terminate on the transit gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 130

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has business operations in the United States and in Europe. The company's public applications are running on AWS and use three transit gateways. The transit gateways are located in the us-west-2, us-east-1, and eu-central-1 Regions. All the transit gateways are connected to each other in a full mesh configuration.

The company accidentally removes the route to the eu-central-1 VPCs from the us-west-2 transit gateway route table. The company also accidentally removes the route to the us-west-2 VPCs from the eu-central-1 transit gateway route table.

How can a network engineer identify the misconfiguration with the LEAST operational overhead?

A. Use the Route Analyzer feature for AWS Transit Gateway Network Manager.

B. Use the AWSSupport-SetupIPMonitoringFromVPC AWS Systems Manager Automation runbook. Push network telemetry data to Amazon CloudWatch Logs for analysis.

C. Use VPC flow logs in eu-central-1 and us-west-2 to analyze the missing routes.

D. Use Amazon VPC Traffic Mirroring in eu-central-1 or us-west-2 to take packet captures and troubleshoot the connectivity issues.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 131

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A marketing company is using hybrid infrastructure through AWS Direct Connect links and a software-defined wide area network (SD-WAN) overlay to connect its branch offices. The company connects multiple VPCs to a third-party SD-WAN appliance transit VPC within the same account by using AWS Site-to-Site VPNs.

The company is planning to connect more VPCs to the SD-WAN appliance transit VPC. However, the company faces challenges of scalability, route table limitations, and higher costs with the existing architecture. A network engineer must design a solution to resolve these issues and remove dependencies.

Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Configure a transit gateway to attach the VPCs. Configure a Site-to-Site VPN connection between the transit gateway and the third-party SD-WAN appliance transit VPC. Use the SD-WAN overlay links to connect to the branch offices.

B. Configure a transit gateway to attach the VPCs. Configure a transit gateway Connect attachment for the third-party SD-WAN appliance transit VPC. Use transit gateway Connect native integration of SD-WAN virtual hubs with AWS Transit Gateway.

C. Configure a transit gateway to attach the VPCs. Configure VPC peering between the VPCs and the third-party SD-WAN appliance transit VPUse the SD-WAN overlay links to connect to the branch offices.

D. Configure VPC peering between the VPCs and the third-party SD-WAN appliance transit VPC. Use transit gateway Connect native integration of SD-WAN virtual hubs with AWS Transit Gateway.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01

Question #: 132

Topic #: 1

[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company is running a hybrid cloud environment. The company has multiple AWS accounts as part of an organization in AWS Organizations. The company needs a solution to manage a list of IPv4 on-premises hosts that will be allowed to access resources in AWS. The solution must provide version control for the list of IPv4 addresses and must make the list available to the AWS accounts in the organization.

Which solution will meet these requirements?

A. Create a customer-managed prefix list. Add entries for the initial list of on-premises IPv4 hosts. Create a resource share in AWS Resource Access Manager. Add the managed prefix list to the resource share. Share the resource with the organization.

B. Create a customer-managed prefix list. Add entries for the initial list of on-premises IPv4 hosts. Use AWS Firewall Manager to share the managed prefix list with the organization.

C. Create a security group. Add inbound rule entries for the initial list of on-premises IPv4 hosts. Create a resource share in AWS Resource Access Manager. Add the security group to the resource share. Share the resource with the organization.

D. Create an Amazon DynamoDB table. Add entries for the initial list of on-premises IPv4 hosts. Create an AWS Lambda function that assumes a role in each AWS account in the organization to authorize inbound rules on security groups based on entries from the DynamoDB table.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 133
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company's application is deployed on Amazon EC2 instances in a single VPC in an AWS Region. The EC2 instances are running in two Availability Zones. The company decides to use a fleet of traffic inspection instances from AWS Marketplace to inspect traffic between the VPC and the internet. The company is performing tests before the company deploys the architecture into production.

The fleet is located in a shared inspection VPC behind a Gateway Load Balancer (GWLB). To minimize the cost of the solution, the company deployed only one inspection instance in each Availability Zone that the application uses.

During tests, a network engineer notices that traffic inspection works as expected when the network is stable. However, during maintenance of the inspection instances, the internet sessions time out for some application instances. The application instances are not able to establish new sessions.

Which combination of steps will remediate these issues? (Choose two.)

A. Deploy one inspection instance in the Availability Zones that do not have inspection instances deployed.

B. Deploy one additional inspection instance in each Availability Zone where the inspection instances are deployed.

C. Enable the cross-zone load balancing attribute for the GWLB.

D. Deploy inspection instances in an Auto Scaling group. Define a scaling policy that is based on CPU load.

E. Attach the GWLB to all Availability Zones in the Region.

Show Suggested Answer

Exam question from Amazon's AWS Certified Advanced Networking - Specialty ANS-C01
Question #: 134
Topic #: 1
[All AWS Certified Advanced Networking - Specialty ANS-C01 Questions]

A company has developed a new web application on AWS. The application runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate behind an Application Load Balancer (ALB) in the us-east-1 Region. The application uses Amazon Route 53 to host the DNS records for the domain. The content that is served from the website is mostly static images and files that are not updated frequently. Most of the traffic to the website from end users will originate from the United States. Some traffic will originate from Canada and Europe.

A network engineer needs to design a solution that will reduce latency for end users at the lowest cost. The solution also must ensure that all traffic is encrypted in transit until the traffic reaches the ALB.

Which solution will meet these requirements?

A. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that is assigned to the accelerator for the ALB.

B. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point to the DNS record that is assigned to the ALConfigure the CloudFront distribution to use an SSL certificate. Set all behaviors to force HTTPS. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that is assigned to the ALB.

C. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point to the DNS record that is assigned to the ALB. Configure the CloudFront distribution to use an SSL certificate and redirect HTTP to HTTPS. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the CloudFront distribution.

D. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create a second application stack on Amazon ECS on Fargate in the eu-west-1 Region. Create another secure HTTPS listener. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to use a latency-based routing policy to route to the DNS name that is assigned to the accelerator for the ALBs.

Show Suggested Answer