Amazon

Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

NEW QUESTION 1
An organization is replacing a tape backup system with a storage gateway. there is currently no connectivity to AWS. Initial testing is needed.
What connection option should the organization use to get up and running at minimal cost?

A. Use an internet connection.
B. Set up an AWS VPN connection.
C. Provision an AWS Direct Connection private virtual interface.
D. Provision a Direct Connect public virtual interface.

Answer: A

NEW QUESTION 2
A company has a hybrid environment across its on-premises network and the AWS Cloud The company wants to use Amazon Elastic File System (Amazon EFS) to store and share data between on-premises services that are required to resolve DNS queries through on-premises DNS servers The company wants to use a custom domain name to connect to Amazon EFS The company also wants to avoid using the Amazon EFS target IP address.
What should a network engineer do to meet these requirements?

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

Answer: A

NEW QUESTION 3
An organization is migrating its on-premises applications to AWS by using a lift-and-shift approach, taking advantage of managed AWS services wherever possible. The company must be able to edit the application code during the migration phase. One application is a traditional three-tier application, consisting of a web presentation tier, an application tier, and a database tier. The external calling client applications need their sessions to remain sticky to both the web and application nodes that they initially connect to.
Which load balancing solution would allow the web and application tiers to scale horizontally independent from one another other?

A. Use an Application Load Balancer at the web tier and a Classic Load Balancer at the application tie
B. Set session stickiness on both, but update the application code to create an application-controlled cookie on the Classic Load Balancer.
C. Use an Application Load Balancer at both the web and application tiers, setting session stickiness at the target group level for both tiers.
D. Deploy a web node and an application node as separate containers on the same host, using task linking to create a relationship between the pai
E. Add an Application Load Balancer with session stickiness in front of all web node containers.
F. Use a Network Load Balancer at the web tier, and an Application Load Balancer at the application tier.Enable session stickiness on the Application Load Balancer, but take advantage of the native WebSockets protocols available to the Network Load Balancer.

Answer: A

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

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

Answer: BC

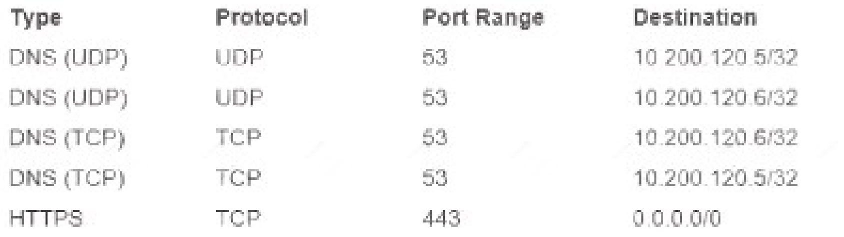
Explanation:
https://aws.amazon.com/blogs/security/how-to-set-up-an-outbound-vpc-proxy-with-domain-whitelisting-and-co

NEW QUESTION 5
A company's Network Engineering team is solely responsible for deploying VPC infrastructure using AWS CloudFormation. The company wants to give its Developers the ability to launch applications using CloudFormation templates so that subnets can be created using available CIDR ranges.
What should be done to meet these requirements?

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

Answer: D

NEW QUESTION 6
A company wants to enforce a compliance requirement that its Amazon EC2 instances use only on-premises DNS servers tor name resolution Outbound DNS requests lo all other name servers must be denied. A network engineer configures the following set of outbound rules for a security group.



Type	Protocol	Port Range	Destination
DNS (UDP)	UDP	53	10.200.120.5/32
DNS (UDP)	UDP	53	10.200.120.6/32
DNS (TCP)	TCP	53	10.200.120.6/32
DNS (TCP)	TCP	53	10.200.120.5/32
HTTPS	TCP	443	0.0.0.0/0

The network engineer discovers that the EC2 instances are still able to resolve DNS requests by using Amazon DNS servers inside the VPC Why is the solution tailing to meet the compliance requirement9

A. The security group cannot filter outbound traffic to the Amazon DNS servers
B. The security group must have inbound rules to prevent DNS requests from coming back to EC2 instances.
C. The EC2 instances are using the HTTPS port to send DNS queries to Amazon DNS servers
D. The security group cannot filter outbound traffic to destinations within the same VPC

Answer: A

NEW QUESTION 7
You manage a web service that is used by client applications deployed in 300 offices worldwide. The web service architecture is an Elastic Load balancer (ELB) distributing traffic across four application servers deployed in an autoscaling group across two availability zones.
The ELB is configured to use round robin, and sticky sessions are disabled. You have configured the NACLs and Security Groups to allow port 22 from your bastion host, and port 80 from 0.0.0.0/0. The client configuration is managed by each regional IT team.
Upon inspection you find that a large amount of requests from incorrectly configured sites are causing a single application server to degrade. The remainder of the requests are equally distributed across all servers with no negative effects.
What should you do to remedy the situation and prevent future occurrences?

A. Mark the affected instance as degraded in the ELB and raise it with the client application team.
B. Update the NACL to only allow port 80 to the application servers from the ELB servers.
C. Update the Security Groups to only allow port 80 to the application servers from the ELB.
D. Terminate the affected instance and allow Auto Scaling to create a new instance.

Answer: C

NEW QUESTION 8
A company hosts several applications in the AWS Cloud across multiple VPCs that are connected to a transit gateway Redundant AWS Direct Connect connections and a Direct Connect gateway provide private network connectivity lo the company's on-premises environment
During a maintenance window, the networking team adds eight VPCs The application management team notices that there is no reachability between the newly created VPCs and the on-premises environment Connectivity between all VPCs through the transit gateway is working as expected.
Which of the following are possible causes of the connectivity issues? (Choose TWO)

A. The prefixes that are advertised from the Direct Connect gateway to the on-premises router are shorter than the CIDR blocks of the newly created VPCs
B. The route tables for the newly created
C. VPCs do not have the routes to the on-premises environment that point to the transit gateway attachment
D. The on-premises route tables do not contain the exact CIDR blocks of the newly created VPCs
E. The route tables (or the newly created VPCs have only summary routes for (he on-premises environment (fiat point to the transit gateway attachment.
F. The prefixes that are advertised from the Direct Connect gateway to the on-premises router do not contain the CIDR blocks of the newly created VPCs

Answer: AD

NEW QUESTION 9
A company is deploying a non-web application on an AWS load balancer. All targets are servers located
on-premises that can be accessed by using AWS Direct Connect. The company wants to ensure that the source IP addresses of clients connecting to the application are passed all the way to the end server.
How can this requirement be achieved?

A. Use a Network Load Balancer to automatically preserve the source IP address.
B. Use a Network Load Balancer and enable the X-Forwarded-For attribute.
C. Use a Network Load Balancer and enable the ProxyProtocol v2 attribute.
D. Use an Application Load Balancer to automatically preserve the source IP address in the X-Forwarded-For header.

Answer: C

Explanation:
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#proxy-proto

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

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

D. Create a CloudWatch alarm for the StatusCheckFailed metric and choose Recover this instance, selecting a threshold value of 1.

Answer: C

NEW QUESTION 10
You are preparing to launch Amazon WorkSpaces and need to configure the appropriate networking resources. What must be configured to meet this requirement?

A. At least two subnets in different Availability Zones.
B. A dedicated VPC with Active Directory Services.
C. An IPsec VPN to on-premises Active Directory
D. Network address translation for outbound traffic.

Answer: AD

Explanation:
References: https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html

NEW QUESTION 15
You have to set up an AWS Direct Connect connection to connect your on-premises to an AWS VPC. Due to budget requirements, you can only provision a single Direct Connect port. You have two border gateway routers at your on-premises data center that can peer with the Direct Connect routers for redundancy.
Which two design methodologies, in combination, will achieve this connectivity? (Select two.)

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

Answer: AD

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

NEW QUESTION 16
An organization will be extending its existing on-premises infrastructure into the cloud. The design consists of a transit VPC that contains stateful firewalls that will be deployed in a highly available configuration across two Availability Zones for automatic failover.
What MUST be configured for this design to work? (Select two.)

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

Answer: BC

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

NEW QUESTION 19
Your organization runs a popular e-commerce application deployed on AWS that uses autoscaling in conjunction with an Elastic Load balancing (ELB) service with an HTTPS listener. Your security team reports that an exploitable vulnerability has been discovered in the encryption protocol and cipher that your site uses.
Which step should you take to fix this problem?

A. Generate new SSL certificates for all web servers and replace current certificates.
B. Change the security policy on the ELB to disable vulnerable protocols and ciphers.
C. Generate new SSL certificates and use ELB to front-end the encrypted traffic for all web servers.
D. Leverage your current configuration management system to update SSL policy on all web servers.

Answer: B

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

A. 802.1q trunking
B. 802.1ax or 802.3ad link aggregation
C. OSPF
D. BGP
E. single-mode optical fiber connectivity
F. 1-Gbps copper connectivity

Answer: ADE

Explanation:

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

NEW QUESTION 24
A company is migrating a legacy storefront web application to the AWS Cloud. The application is complex and will take several months to refactor A solutions architect recommended an interim solution of using Amazon CloudFront with a custom origin pointing to the SSL endpoint URL for the legacy web application until the replacement is ready and deployed
The interim solution has worked for several weeks However, all browser connections recently began showing an HTTP 502 Bad Gateway error with the header "X-Cache Error from cloudfront" Monitoring services show that the HTTPS port 443 on the legacy web application is open and responding to requests
What is the likely cause of the error and what is the solution?

A. The origin access identity is not correct Edit the CloudFront distribution and update the identity in the origins settings
B. The SSL certificate on the CloudFront distribution has expired Use AWS Certificate Manager (ACM) in the us-east-1 Region to replace the SSL certificate in the CloudFront distribution with a new certificate
C. The SSL certificate on the legacy web application server has expired Use AWS Certificate Manager (ACM) in the us-east-1 Region to create a new SSL certificate Export the public and private keys and install the certificate on the legacy web application
D. The SSL certificate on the legacy web application server has expired Replace the SSL certificate on the web server with one signed by a globally recognized certificate authority (CA) Install the full certificate chain onto the legacy web application server

Answer: A

NEW QUESTION 27
A company has established an AWS Direct Connect connection between its customer gateway at its on-premises data center and a virtual private gateway m the AWS Cloud The BGP routing protocol
configuration includes the Autonomous System Number {ASN) of 7224 on the AWS end of the connection
and the BGP ASN of 65004 on the company end of the connection
The company's IT administrators report that servers that run at the on-premises data center are not able to
communicate with the company's web application that runs on a fleet of Amazon EC2 Instances A network engineer performs initial troubleshooting The network engineer finds that the private VIF is operational and that there is a fully established BGP peering session However, the company still cannot route traffic over the private VIF
Which of the following is a possible cause of this connectivity issue?

A. Firewall or ACL rules are blocking TCP pod 179 or are blocking high-numbered ephemeral TCP pons
B. The provider is advertising 50 prefixes for private VIFs
C. VPC route tables am lacking prefixes that point to the virtual private gateway to which the private VIF is connected
D. Peer IP addresses for both sides of the BGP peering session are not configured correctly.

Answer: A

NEW QUESTION 29
A financial services company receives real-time stock quotes in its ingestion VPC. The company plans to perform customer-specific data analysis on the stock quotes in various VPCs. The stock quotes must be distributed simultaneously from Amazon EC2 instances in the ingestion VPC to EC2 instances in the data analysis VPCs
Which set of configuration steps should the company lake to meet these requirements?

A. Configure EC2 instances m f he ingestion VPC as IP unicast senders Configure a transit gateway to serve as a unicast router for instances that send traffic destined for the EC2 instances in the data analysis VPCs.
B. Configure VPC peering between the ingestion VPC and the data analysis VPCs Configure an Application Load Balancer to distribute Virtual Extensible LAN (VXLAN)-encapsulated traffic from the sender EC2 instances to the receiver EC2 instances.
C. Configure EC2 instances m the ingestion VPC as IP multicast senders Configure a transit gateway to serve as a multicast router for instances that send traffic destined for the EC2 instances m the data analysis VPCs
D. Configure Amazon Kinesis Data Forehose to capture streaming data from the ingestion VPC and load the data into Amazon S3 Configure the instances in the data analysis VPCs to download the data from Amazon S3 for processing

Answer: D

NEW QUESTION 33
An insurance company is planning the migration of workloads from its on-premises data center to the AWS Cloud The company requires end-to-end domain name resolution Bidirectional DNS resolution between AWS
and the existing on-premises environments must be established The workloads will be migrated into multiple VPCs. The workloads also have dependencies on each other, and not all the workloads will be migrated at the same time
Which solution meets these requirements? Which solution meets these requirements?

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

Route 53 outbound rules with the application VPCs and share the private hosted zones with the application accounts by using AWS Resource Access Manager Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoint.

Answer: B

NEW QUESTION 36
You are building an application that provides real-time audio and video services to customers on the Internet. The application requires high throughput. To ensure proper audio and video transmission, minimal latency is required.
Which of the following will improve transmission quality?

A. Enable enhanced networking
B. Select G2 instance types
C. Enable jumbo frames
D. Use multiple elastic network interfaces

Answer: A

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

NEW QUESTION 38
A company has an application running on Amazon EC2 instances in a private subnet that connects to a third-party service provider's public HTTP endpoint through a NAT gateway. As request rates increase, new connections are starting to fail. At the same time, the ErrorPortAllocation Amazon CloudWatch metric count for the NAT gateway is increasing.
Which of the following actions should improve the connectivity issues? (Choose two.)

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

Answer: CE

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

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

Answer: A

NEW QUESTION 44
A company has an application running in an Amazon VPC that must be able to communicate with on-premises resources in a data center. Network traffic between AWS and the data center will initially be minimal, but will increase to more than 10 Gbps over the next few months. The company's goal is to launch the application as quickly as possible. The Network Engineer has been asked to design a hybrid IT connectivity solution. What should be done to meet these requirements?

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

Answer: C

NEW QUESTION 48
Your organization’s corporate website must be available on www.acme.com and acme.com. How should you configure Amazon Route 53 to meet this requirement?

A. Configure acme.com with an ALIAS record targeting the EL
B. www.acme.com with an ALIAS record targeting the ELB.
C. Configure acme.com with an A record targeting the EL
D. www.acme.com with a CNAME record targeting the acme.com record.
E. Configure acme.com with a CNAME record targeting the EL
F. www.acme.com with a CNAME record targeting the acme.com record.
G. Configure acme.com using a second ALIAS record with the ELB targe
H. www.acme.com using a PTR record with the acme.com record target.

Answer: A

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

NEW QUESTION 52
The Payment Card Industry Data Security Standard (PCI DSS) merchants that handle credit card data must use strong cryptography. These merchants must also use security protocols to protect sensitive data during transmission over public networks.
You are migrating your PCI DSS application from on-premises SSL appliance and Apache to a VPC behind Amazon CloudFront.
How should you configure CloudFront to meet this requirement?

A. Configure the CloudFront Cache Behavior to require HTTPS and the CloudFront Origin’s Protocol Policy to ‘Match Viewer’.
B. Configure the CloudFront Cache Behavior to allow TCP connections and to forward all requests to the origin without TLS termination at the edge.
C. Configure the CloudFront Cache Behavior to require HTTPS and to forward requests to the origin via AWS Direct Connect.
D. Configure the CloudFront Cache Behavior to redirect HTTP requests to HTTPS and to forward request to the origin via the Amazon private network.

Answer: A

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#

NEW QUESTION 57
A company is deploying a critical application on two Amazon EC2 instances in a VPC Failed client connections to the EC2 instances must be logged according to company policy.
What is the MOST cost-effective solution to meet these requirements'?

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

Answer: D

NEW QUESTION 62
An application runs on a fleet of Amazon EC2 instances in a VPC. All instances can reach one another using private IP addresses. The application owner has a new requirement that the domain name received via DHCP should be different for a particular set of instances that are currently in one particular subnet.
What changes should be made to meet this requirement while continuing to support the existing application requirements?

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

Answer: D

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

NEW QUESTION 66
A company has two redundant AWS Direct Connect connections to a VPC. The VPC is configured using BGP metrics so that one Direct Connect connection is used as the primary traffic path. The company wants the primary Direct Connect connection to fail to the secondary in less than one second.
What should be done to meet this requirement?

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

Answer: B

NEW QUESTION 70
A company has a hybrid IT architecture with two AWS Direct Connect connections to provide high availability. The services hosted on-premises are accessible using public IPs, and are also on the 172.16.0.0/16 range. The AWS resources are on the 192.168.0.0/18 range. The company wants to use Amazon Elastic Load Balancing for SSL offloading, health checks, and sticky sessions.
What should be done to meet these requirements?

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

Answer: D

NEW QUESTION 71

A department in your company has created a new account that is not part of the organization’s consolidated billing family. The department has also created a VPC for its workload. Access is restricted by network access control lists to the department’s on-premises private IP allocation. An AWS Direct Connect private virtual interface for this VPC advertises a default route to the company network. When the department downloads data from an Amazon Elastic Compute Cloud(EC2) instance in its new VPC, what are the associated charges?

A. The company pays Internet Data Out charges.
B. The company pays AWS Direct Connect Data Out charges.
C. The department pays Internet Data Out charges.
D. The department pays AWS Direct Connect Data Out charges.

Answer: D

NEW QUESTION 74
A company's IT Security team needs to ensure that all servers within an Amazon VPC can communicate with a list of five approved external IPs only. The team also wants to receive a notification every time any server tries to open a connection with a non-approved endpoint.
What is the MOST cost-effective solution that meets these requirements?

A. Add allowed IPs to the network ACL for the application server subnet
B. Enable VPC Flow Logs with a filter set to AL
C. Create an Amazon CloudWatch Logs filter on the VPC Flow Logs log group filtered by REJEC
D. Create an alarm for this metric to notify the Security team.
E. Enable Amazon GuardDuty on the account and the specific regio
F. Upload a list of allowed IPs to Amazon S3 and link the S3 object to the GuardDuty trusted IP lis
G. Configure an Amazon CloudWatch Events rule on all GuardDuty findings to trigger an Amazon SNS notification to the Security team.
H. Add allowed IPs to the network ACL for the application server subnet
I. Enable VPC Flow Logs with a filter set to REJEC
J. Set an Amazon CloudWatch Logs filter for the log group on every even
K. Create an alarm for this metric to notify the Security team.
L. Enable Amazon GuardDuty on the account and specific regio
M. Upload a list of allowed IPs to Amazon S3 and link the S3 object to the GuardDuty threat IP lis
N. Integrate GuardDuty with a compatible SIEM to report on every alarm from GuardDuty.

Answer: C

NEW QUESTION 79
A company wants to migrate its production and development applications to the AWS Cloud across multiple VPCs in three AWS Regions us-east-1 (N Virginia), eu-west-1 (Ireland), and ap-southeast-1 (Singapore) The company needs a scalable solution that provides connectivity between all three Regions The solution also must provide private connectivity to the company's on-premises data center in Northern Virginia Data that is transferred from on premises and data that is transferred between Regions must be encrypted in transit The company requires predictable network performance and must minimize cost
The company has initiated a solution by deploying a transit gateway with two route tables in each Region One route table is for the production environment, and one route table is for the development environment
What else must the company do to meet its requirements with the LOWEST latency?

A. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center On each transit gateway, create a VPN attachment over the public VIF for the production and development route tables Create transit gateway peenng connections to route traffic between Regions
B. Deploy an AWS Direct Connect connection in us-east-1 and a transit VIF to the on-premises data center Associate all transit gateways and the transit VIF with a different Direct Connect gatewa
C. Create transit gateway peering connections to route traffic between Regions
D. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center.On each transit gateway, create a VPN attachment over the public VIF for the production and development route table
E. Route traffic between Regions through the VPN connections.
F. Deploy an AWS Direct Connect connection in us-east-1 to the on-premises data center Create one transit VIF for each transit gateway route table, and associate each transit VIF with a Direct Connect gateway Associate all transit gateways with the Direct Connect gateway Create transit gateway peering connections to route traffic between Regions.

Answer: B

NEW QUESTION 80
The Web Application Development team is worried about malicious activity from 200 random IP addresses. Which action will ensure security and scalability from this type of threat?

A. Use inbound security group rules to block the IP addresses.
B. Use inbound network ACL rules to block the IP addresses.
C. Use AWS WAF to block the IP addresses.
D. Write iptables rules on the instance to block the IP addresses.

Answer: C

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

NEW QUESTION 81
You have a global corporate network with 153 individual IP prefixes in your internal routing table. You establish a private virtual interface over AWS Direct Connect to a VPC that has an Internet gateway (IGW). All instances in the VPC must be able to route to the Internet via an IGW and route to the global corporate network via the VGW.
How should you configure your on-premises BGP peer to meet these requirements?

A. Configure AS-Prepending on your BGP session
B. Summarize your prefix announcement to less than 100

C. Announce a default route to the VPC over the BGP session
D. Enable route propagation on the VPC route table

Answer: B

NEW QUESTION 83
You have multiple Amazon Elastic Compute Cloud (EC2) instances running a web server in a VPC configured with security groups and NACL. You need to ensure layer 7 protocol level logging of all network traffic (ACCEPT/REJECT) on the instances. What should be enabled to complete this task?

A. CloudWatch Logs at the VPC level
B. Packet sniffing at the instance level
C. VPC flow logs at the subnet level
D. Packet sniffing at the VPC level

Answer: B

NEW QUESTION 87
You deploy an Amazon EC2 instance that runs a web server into a subnet in a VPC. An Internet gateway is attached, and the main route table has a default route (0.0.0.0/0) configured with a target of the Internet gateway.
The instance has a security group configured to allow as follows:
Protocol: TCP
Port: 80 inbound, nothing outbound
The Network ACL for the subnet is configured to allow as follows:
Protocol: TCP
Port: 80 inbound, nothing outbound
When you try to browse to the web server, you receive no response. Which additional step should you take to receive a successful response?

A. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 80
B. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 1024-65535
C. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 80
D. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 1024-65535

Answer: B

NEW QUESTION 92
A company is building a hybrid PCI-DSS compliant application that runs in the us-west-2 Region and
on-premises. The application sends access logs from all locations to a single Amazon S3 bucket in us-west-2 To protect this sensitive data, the bucket policy is configured to deny access from public IP addresses
How should an engineer configure the network to meet these requirements?

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

Answer: C

NEW QUESTION 96
A financial company is designing a secure AWS network architecture to support a hybrid cloud strategy. Systems deployed in the AWS Cloud are mission critical and have strict availability requirements. The
company anticipates the need for hundreds of VPCs. Instances will be transient and rely heavily on DNS resolution The applications must be designed to have Availability Zone isolation and tolerate the loss of an Availability Zone
What is the MOST reliable way to implement DNS in this scenario?

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

Answer: C

NEW QUESTION 97
A computing team is evaluating whether to place a high performance computing (HPC) application in AWS. The team is concerned about application performance and wants to know what options are available to increase networking performance.
Which of the following changes would increase performance for this application? (Choose two.)

A. Place the application across many smaller instances to achieve higher total throughput.
B. Increase the MTU of the VPC to 9001.
C. Enable an MTU of 9001 in the application's operating system.
D. Enable enhanced networking on the instances.
E. Deploy the application in two Availability Zones and insert them in one placement group.

Answer: CD

NEW QUESTION 100
DNS name resolution must be provided for services in the following four zones: company.private.
emea.company.private. apac.company.private. amer.company.private.
The contents of these zones is not considered sensitive, however, the zones only need to be used by services hosted in these VPCs, one per geographic region. Each VPC should resolve the names in all zones.
How can you use Amazon route 53 to meet these requirements?

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

Answer: A

NEW QUESTION 102
A company uses a newly provisioned 1-Gbps AWS Direct Connect connection to configure a virtual interface for access to Amazon S3
Which configuration values is the network engineer required to provide? (Select TWO.)

A. Connection speed
B. VLAN ID
C. IP prefixes to advertise
D. Direct Connect location
E. Virtual private gateway

Answer: BE

NEW QUESTION 106
An organization runs a consumer-facing website on AWS. The Amazon EC2-based web fleet is load balanced using the AWS Application Load Balancer, Amazon Route 53 is used to provide the public DNS services.
The following URLs need to server content to end users: test.example.com
web.example.com example.com
Based on this information, what combination of services must be used to meet the requirement? (Select two.)

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

Answer: BC

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

NEW QUESTION 110
An organization processes consumer information submitted through its website. The organization’s security policy requires that personally identifiable information (PII) elements are specifically encrypted at all times and as soon as feasible when received. The front-end Amazon EC2 instances should not have access to decrypted PII. A single service within the production VPC must decrypt the PII by leveraging an iAM role.
Which combination of services will support these requirement? (Select two.)

A. Amazon Aurora in a private subnet
B. Amazon CloudFront using AWS Lambda@Edge
C. Customer-managed MySQL with Transparent Data Encryption
D. Application Load Balancer using HTTPS listeners and targets
E. AWS Key Management Services

Answer: BE

NEW QUESTION 113
A company deployed its production Amazon VPC using CIDR block 33.16.0.0/16. The company has nearly depleted its addresses and now needs to extend the VPC network.
Which CIDR blocks meet the company’s requirement to extend the VPC network with a secondary CIDR? (Choose two.)

A. 33.17.0.0/16
B. 172.16.0.0/18
C. 100.70.0.0/17
D. 192.168.1.0/24
E. 10.0.0.0/8

Answer: AC

NEW QUESTION 114
A company has applications running in a single AWS Region and its on premises data center in a hybrid mode The company has a 1Gbps AWS Direct Connect connection from the data center to AWS that is 65% utilized. The company has an AWS Enterprise Support plan
The company is planning to deploy a new critical application on AWS that will connect with existing applications running in the data center. The application SLA requires a minimum ot 99.9% network uptime between the data center and AWS.

What is the MOST cost-effective way to meet this SLA requirement?

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

Answer: A

NEW QUESTION 116
A company wants to use thin clients running virtual desktops to replace 500 desktop computers used by its call center employees The company is evaluating Amazon Workspaces as a solution
A network engineer who is testing with a thin client is unable to conned to Amazon Workspaces After entering credentials the network engineer receives the following error:
"An error occurred while launching your Workspace Please try again" What should the network engineer do to resolve this issue?

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

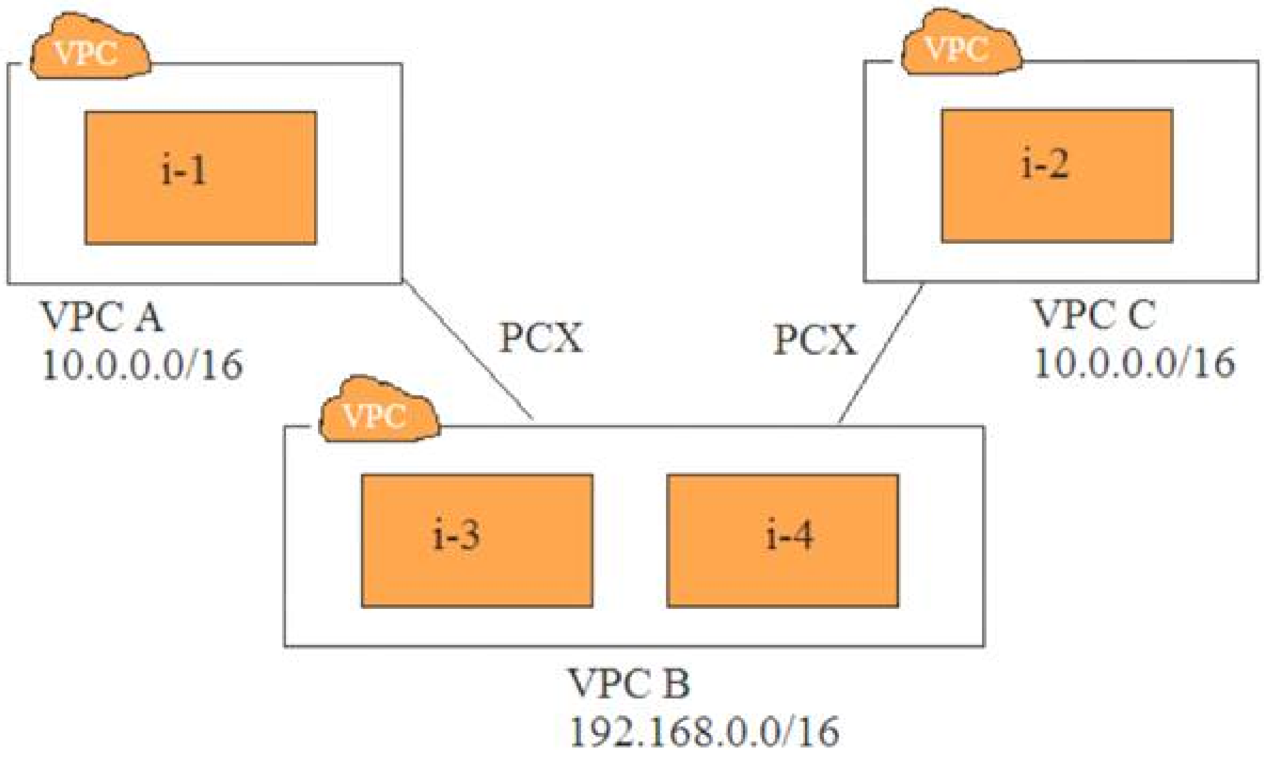
Answer: C

NEW QUESTION 120
A Network Engineer needs to be automatically notified when a certain TCP port is accessed on a fleet of Amazon EC2 instances running in an Amazon VPC. Which of the following is the MOST reliable solution?

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

Answer: A

NEW QUESTION 121
Refer to the image.



You have three VPCs: A, B, and C. VPCs A and C are both peered with VPC B. The IP address ranges are as follows:
VPC A: 10.0.0.0/16
VPC B: 192.168.0.0/16
VPC C: 10.0.0.0/16
Instance i-1 in VPC A has the IP address 10.0.0.10. Instance i-2 in VPC C has the IP address 10.0.0.10. Instances i-3 and i-4 in VPC B have the IP addresses 192.168.1.10 and 192.168.1.20, respectively, i-3 and i-4 are in the subnet 192.168.1.0/24.

i-3 must be able to communicate with i-1
i-4 must be able to communicate with i-2
i-3 and i-4 are able to communicate with i-1, but not with i-2.
Which two steps will fix this problem? (Select two.)

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

Answer: AE

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

NEW QUESTION 124
You use a VPN to extend your corporate network into a VPC. Instances in the VPC are able to resolve resource records in an Amazon Route 53 private hosted zone. Your on-premises DNS server is configured with a forwarder to the VPC DNS server IP address. On-premises users are unable to resolve names in the private hosted zone, although instances in a peered VPC can.
What should you do to provide on-premises users with access to the private hosted zone?

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

Answer: A

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

NEW QUESTION 125
Under increased cybersecurity concerns, a company is deploying a near real-time intrusion detection system (IDS) solution. A system must be put in place as soon as possible. The architecture consists of many AWS accounts, and all results must be delivered to a central location.
Which solution will meet this requirement, while minimizing downtime and costs?

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

Answer: D

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

NEW QUESTION 126
A network engineer is managing two AWS Direct Connect connections. Each connection has a public virtual interface configured with a private ASN. The engineer wants to configure active/passive routing between the Direct Connect connections to access Amazon public endpoints. What BGP configuration is required for the on-premises equipment? (Select two.)

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

Answer: AE

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

NEW QUESTION 131
Your application is hosted behind an Elastic Load Balancer (ELB) within an autoscaling group. The autoscaling group is configured with a minimum of 2, a maximum of 14, and a desired value of 2. The autoscaling cooldown and the termination policies are set to the default value.
CloudWatch reports that the site typically requires just two servers, but spikes at the start and end of the business day can require eight to ten servers. You receive intermittent reports of timeouts and partially loaded web pages.
Which configuration change should you make to address this issue?

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

Answer: A

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

NEW QUESTION 132
A legacy, on-premises web application cannot be load balances effectively. There are both planned and unplanned events that cause usage spikes to millions of concurrent users. The existing infrastructure cannot handle the usage spikes. The CIO has mandated that the application be moved to the cloud to avoid further disruptions, with the additional requirement that source IP addresses be unaltered to support network traffic-monitoring needs. Which of the following designs will meet these requirements?

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

Answer: D

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

NEW QUESTION 136
A space exploration company owns a series of telescopes that capture a large number of images and data of the night sky. The images and data are processed on an application hosted on AWS Fargate in a target group assigned to an Application Load Balancer (ALB). The application is made available through the address https:/'space example com
Scientists require another custom-built application hosted on several Amazon EC2 instances within an Auto Scaling group. This application will be made available from the address https://space.example.com/meteor. The company needs a solution that can automatically scale from a small number of requests overnight to a large number of requests for a future meteor shower.
What is the MOST operationally efficient solution that meets these requirements?

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

Answer: A

NEW QUESTION 139
A company has 225 mobile and desktop devices and 300 partner VPNs that need access to an AWS VPC. VPN users should not be able to reach one another. Which approach will meet the technical and security requirements while minimizing costs?

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

Answer: D

NEW QUESTION 144
A company's network engineer needs to evaluate and monitor DNS traffic The company uses Amazon Route 53 as the DNS service for its public hosted zone All DNS queries must be captured for future analysis.
What should the network engineer do to meet these requirements?

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

Answer: A

NEW QUESTION 146
Your organization has a newly installed 1-Gbps AWS Direct Connect connection. You order the cross-connect from the Direct Connect location provider to the port on your router in the same facility. To enable the use of your first virtual interface, your router must be configured appropriately.

What are the minimum requirements for your router?

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

Answer: B

NEW QUESTION 150
A company wants to conduct a proof of concept for an SAP HANA application with a hey objective to automate the provisioning of infrastructure and the application. The company operates a hybrid cloud infrastructure with AWS Direct Connect between its data center and VPC. Security policy dictates that all traffic from AWS be routed through on-premises data center firewalls. Security policy also prohibits the use of a VPC internet gateway for internet access The company enforces use of a forward proxy server for all outbound network traffic All resources inside the VPC are able to reach on-premises servers.
All Amazon EC2 Linux instances require package updates over the internet. However, the updates are failing and sending errors.
What would cause these errors?

A. Inbound security groups are configured incorrectly on the EC2 instances running in the VPC.
B. The VPC route table does not have entries for the proxy server in the data center
C. The EC2 instances are not configured to use the proxy running in the data center for traffic on TCP port 80.
D. The data center firewall is blocking all traffic sent from the VPC CIDR range destined for 0.0.0.0/0.

Answer: B

NEW QUESTION 154
A network architect is designing an internet website. It has web, application, and database tiers that will run in AWS. The website uses Amazon DynamoDB.
Which architecture will minimize public exposure of the back-end instances?

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

Answer: B

NEW QUESTION 159
You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a
self-referencing rule using the cluster security group’s group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions. How should you enable secure cluster communication while deploying additional cluster members in another AWS region?

A. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other’s security group-id in each region.
B. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
C. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
D. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other’s security group-id in each region.

Answer: B

NEW QUESTION 161
A company is about to migrate an application from its on-premises data center to AWS. As part of the planning process, the following requirements involving DNS have been identified.
The organization’s VPC uses the CIDR block 172.16.0.0/16.
Assuming that there is no DNS namespace overlap, how can these requirements be met?

A. Change the DHCP options set for the VPC to use both the Amazon-provided DNS server and theon-premises DNS system
B. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 as authoritative for the Route 53 private hosted zone.
C. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxie
D. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to 172.16.0.2. Change the DHCP options set for the VPC to use the new DNS proxie
E. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 as authoritative for the Route 53 private hosted zone.
F. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxie
G. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to the Amazon-provided DNS server (172.16.0.2). Change the DHCP options set for the VPC to use the new DNS proxie
H. Configure the on-premises DNS systems with a stub-zone, delegating the proxies as authoritative for the Route 53 private hosted zone.
I. Change the DHCP options set for the VPC to use both the on-premises DNS system
J. Configure theon-premises DNS systems with a stub-zone, delegating the Route 53 private hosted zone’s name servers as authoritative for the Route 53 private hosted zone.

Answer: C

NEW QUESTION 162

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

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

Answer: D

NEW QUESTION 165
Your organization needs to resolve DNS entries stored in an Amazon Route 53 private zone "awscloud:internal" from the corporate network. An AWS Direct Connect connection with a private virtual interface is configured to provide access to a VPC with the CIDR block 192.168.0.0/16. A DNS Resolver (BIND) is configured on an Amazon Elastic Compute Cloud (EC2) instance with the IP address 192.168.10.5 within the VPC. The DNS Resolver has standard root server hints configured and conditional forwarding for "awscloud.internal" to the IP address 192.168.0.2.
From your PC on the corporate network, you query the DNS server at 192.168.10.5 for www.amazon.com. The query is successful and returns the appropriate response. When you query for "server.awscloud.internal", the query times out. You receive no response.
How should you enable successful queries for "server.awscloud.internal"?

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

Answer: B

NEW QUESTION 169
A network engineer deploys an application in a private subnet in a VPC that connects to many external video feed providers using RTMP over the internet. A NAT gateway has been deployed in a public subnet and is working as expected. From the Amazon EC2 instance, the application is able to connect to all feed providers except one, which hangs when connecting. Manually testing a
connection from an Amazon EC2 instance in the public subnet to the problem feed indicates that the feed works as expected.
What is causing this issue?

A. The NAT gateway does not support fragmented packets.
B. The internet gateway only supports an MTU of 1500 bytes.
C. An Amazon EC2 instance expects to communicate with an MTU of 9001.
D. The security group on the instances does not allow PMTUD.

Answer: A

NEW QUESTION 172
You are building an application in AWS that requires Amazon Elastic MapReduce (Amazon EMR). The application needs to resolve hostnames in your internal, on-premises Active Directory domain. You update your DHCP Options Set in the VPC to point to a pair of Active Directory integrated DNS servers running in your VPC.
Which action is required to support a successful Amazon EMR cluster launch?

A. Add a conditional forwarder to the Amazon-provided DNS server.
B. Enable seamless domain join for the Amazon EMR cluster.
C. Launch an AD connector for the internal domain.
D. Configure an Amazon Route 53 private zone for the EMR cluster.

Answer: A

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

NEW QUESTION 174
You are moving a two-tier application into an Amazon VPC. An Elastic Load Balancing (ELB) load balancer is configured in front of the application tier. The application tier is driven through RESTful interfaces. The data tier uses relational database service (RDS) MySQL. Company policy requires end-to-end encryption of all data in transit. in front
What ELB configuration complies with the corporate encryption policy?

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

Answer: B

Explanation:

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

NEW QUESTION 177
An AWS CloudFormation template is being used to create a VPC peering connection between two existing operational VPCs, each belonging to a different AWS account. All necessary components in the ‘Remote’ (receiving) account are already in place.
The template below creates the VPC peering connection in the Originating account. It contains these components:
AWSTemplateFormation Version: 2010-09-09 Parameters:
Originating VCId: Type: String RemoteVPCId: Type: String
RemoteVPCAccountId: Type: String Resources:
newVPCPeeringConnection:
Type: ‘AWS::EC2::VPCPeeringConnection’ Properties:
VpcdId: !Ref OriginatingVPCId PeerVpcId: !Ref RemoteVPCId PeerOwnerId: !Ref RemoteVPCAccountId
Which additional AWS CloudFormation components are necessary in the Originating account to create an operational cross-account VPC peering connection with AWS CloudFormation? (Select two.)

A. Resources:NewEC2SecurityGroup:Type: AWS::EC2::SecurityGroup
B. Resources:NetworkInterfaceToRemoteVPC:Type: “AWS::EC2NetworkInterface”
C. Resources:newEC2Route:Type: AWS::EC2::Route
D. Resources:VPCGatewayToRemoteVPC:Type: “AWS::EC2::VPCGatewayAttachment”
E. Resources:newVPCPeeringConnection:Type: ‘AWS::EC2VPCPeeringConnection’PeerRoleArn: !Ref PeerRoleArn

Answer: CE

Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_EC2.html

NEW QUESTION 178
A Network Engineer is provisioning a subnet for a load balancer that will sit in front of a fleet of application servers in a private subnet. There is limited IP space left in the VPC CIDR. The application has few users now but is expected to grow quickly to millions of users.
What design will use the LEAST amount of IP space, while allowing for this growth?

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

Answer: C

NEW QUESTION 180
A Lambda function needs to access the private address of an Amazon ElastiCache cluster in a VPC. The Lambda function also needs to write messages to Amazon SQS. The Lambda function has been configured to run in a subnet in the VPC.
Which of the following actions meet the requirements? (Select two.)

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

Answer: AB

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

NEW QUESTION 183
You operate a production VPC with both a public and a private subnet. Your organization maintains a restricted Amazon S3 bucket to support this production workload. Only Amazon EC2 instances in the private subnet should access the bucket. You implement VPC endpoints(VPC-E) for Amazon S3 and remove the NAT that previously provided a network path to Amazon S3. The default VPC-E policy is applied. Neither EC2 instances in the public or private subnets are able to access the S3 bucket.
What should you do to enable Amazon S3 access from EC2 instances in the private subnet?

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

Answer: B

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

NEW QUESTION 188
Your security team implements a host-based firewall on all of your Amazon Elastic Compute Cloud (EC2) instances to block all outgoing traffic. Exceptions must be requested for each specific requirement. Until you request a new rule, you cannot access the instance metadata service. Which firewall rule should you request to be added to your instances to allow instance metadata access?

A. Inbound; Protocol tcp; Source [Instance's EIP]; Destination 169.254.169.254
B. Inbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
C. Outbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
D. Outbound; Protocol tcp; Destination 169.254.169.254; Destination port 443

Answer: C

NEW QUESTION 193
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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

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

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

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

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

100% Actual & Verified — Instant Download, Please Click
Order The AWS-Certified-Advanced-Networking-Specialty Practice Test Here