Amazon

Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

NEW QUESTION 1
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 2
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 3
Your company runs an application for the US market in the us-east-1 AWS region. This application uses proprietary TCP and UDP protocols on Amazon Elastic Compute Cloud (EC2) instances. End users run a
real-time, front-end application on their local PCs. This front-end application knows the DNS hostname of the service.
You must prepare the system for global expansion. The end users must access the application with lowest latency.
How should you use AWS services to meet these requirements?

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

Answer: B

NEW QUESTION 4
A company has deployed a production environment in the AWS Cloud The environment is contained in a VPC and includes a virtual private gateway The company has established an AWS Direct Connect connection which includes a private virtual interface (VIF) and a VPN connection to the on-premises data center
For traffic originating in the VPC what is the order of BGP path selection from MOST preferred to LEAST preferred?

A. Direct Connect BGP routes static routes longest prefix match, VPN BGP routes
B. Static routes longest prefix match Direct Connect BGP route
C. VPN BGP routes
D. Longest prefix match static routes Direct Connect BGP routes VPN BGP routes
E. Longest prefix match VPN BGP routes, static route
F. Direct Connect BGP routes

Answer: B

NEW QUESTION 5
A company's application runs in a VPC and stores sensitive data in Amazon S3 The application's Amazon EC2 instances are located in a private subnet with a NAT gateway deployed in a public subnet to provide access to Amazon S3 The S3 bucket is located in the same AWS Region as the EC2 instances The company wants to ensure that this bucket can be accessed only from the VPC where the application resides
Which changes should a network engineer make to the architecture to meet these requirements?

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

Answer: B

NEW QUESTION 6
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 7
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 8
A company runs a large-scale application on a feel of Amazon EC2 instances that ate distributed across several VPCs A Network Load Balancer (NLB) in a separate VPC routes traffic to the EC2 instances The NLB's VPC is peered to all the application VPCs
The application must process millions of requests each minute during times of peak utilization Users are reporting that the connections to the application are failing during peak times Monitoring shows an increase in port allocation errors on the NLB.
Which action will solve this issue with the LEAST change to the architecture?

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

Answer: C

NEW QUESTION 9
Your company decides to use Amazon S3 to augment its on-premises data store. Instead of using the company's highly controlled, on-premises Internet gateway, a Direct Connect connection is ordered to provide high bandwidth, low latency access to S3. Since the company does not own a publically routable IPv4 address block, a request was made to AWS for an AWS-owned address for a Public Virtual Interface (VIF).
The security team is calling this new connection a “backdoor”, and you have been asked to clarify the risk to the company.
Which concern from the security team is valid and should be addressed?

A. AWS advertises its aggregate routes to the Internet allowing anyone on the Internet to reach the router.
B. Direct Connect customers with a Public VIF in the same region could directly reach the router.
C. EC2 instances in the same region with access to the Internet could directly reach the router.
D. The S3 service could reach the router through a pre-configured VPC Endpoint.

Answer: C

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/control-routes-direct-connect/

NEW QUESTION 10
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 10
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 13
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 17
A company uses AWS Direct Connect lo connect its corporate network to multiple VPCs in the same AWS account and the same AVVS 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 VPC
D. Configure a private VIF to connect to the corporate network
E. 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

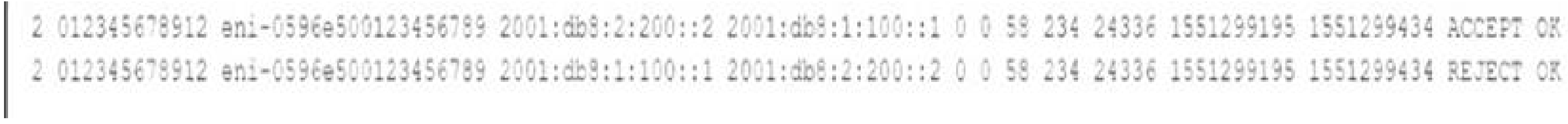
Answer: D

NEW QUESTION 19
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 21
A company is delivering web content from an Amazon EC2 instance in a public subnet with address 2001 db8 1 100 1 Users report they are unable to access the web content The VPC Flow Logs tor the subnet contain the following entries.



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

Which action will restore network reachability to the EC2 instance1?

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

Answer: C

NEW QUESTION 24
A company with several VPCs in the us-east-1 Region wants to reduce the cost of its workloads A network engineer has identified that all traffic bound to Amazon services is flowing through a NAT gateway. Additionally, all the VPCs are peered to a hub VPC for access to common services.

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

Answer: A

NEW QUESTION 29
You run a well-architected, multi-AZ application in the eu-central-1 (Frankfurt) AWS region. The application is hosted in a VPC and is only accessed from the corporate network. To support large volumes of data transfer and administration of the application, you use a single 10-Gbps AWS Direct Connect connection with multiple private virtual interfaces. As part of a review, you decide to improve the resilience of your connection to AWS and make sure that any additional connectivity does not share the same Direct Connect routers at AWS. You need to provide the best levels of resilience to meet the application's needs.
Which two options should you consider? (Select two.)

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

Answer: AE

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

NEW QUESTION 34
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 35
Your company's policy requires that all VPCs peer with a "common services: VPC. This VPC contains a fleet of layer 7 proxies and an Internet gateway. No other VPC is allowed to provision an Internet gateway. You configure a new VPC and peer with the common service VPC as required by policy. You launch an Amazon EC2. Windows instance configured to forward all traffic to the layer 7 proxies in the common services VPC. The application on this server should successfully interact with Amazon S3 using its properly configured AWS Identity and Access Management (IAM) role. However, Amazon S3 is returning 403 errors to the application.
Which step should you take to enable access to Amazon S3?

A. Update the S3 bucket policy with the private IP address of the instance.
B. Exclude 169.254.169.0/24 from the instance's proxy configuration.
C. Configure a VPC endpoint for Amazon S3 in the same subnet as the instance.
D. Update the CORS configuration for Amazon S3 to allow traffic from the proxy.

Answer: B

NEW QUESTION 37
A company provisions an AWS Direct Connect connection to permit access to Amazon EC2 resources in several Amazon VPCs and to data stored in private Amazon S3 buckets. The Network Engineer needs to configure the company's on-premises router for this Direct Connect connection.

Which of the following actions will require the LEAST amount of configuration overhead on the customer router?

A. Configure private virtual interfaces for the VPC resources and for Amazon S3.
B. Configure private virtual interfaces for the VPC resources and a public virtual interface for Amazon S3.
C. Configure a private virtual interface to a Direct Connect gateway for the VPC resources and for Amazon S3.
D. Configure a private virtual interface to a Direct Connect gateway for the VPC resources and a public virtual interface for Amazon S3.

Answer: A

NEW QUESTION 41
An architecture is being designed to support an Amazon WorkSpaces deployment of 1,000 desktops. Which architecture will support this deployment while allowing for future expansion?

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

Answer: B

NEW QUESTION 45
Your company maintains an Amazon Route 53 private hosted zone. DNS resolution is restricted to a single, pre-existing VPC. For a new application deployment, you create an additional VPC in the same AWS account. Both this new VPC and your on-premises DNS infrastructure must resolve records in the existing private hosted zone.
Which two activities are required to enable DNS resolution both within the new VPC and from the on-premises infrastructure? (Select two.)

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

Answer: BD

NEW QUESTION 50
A company has lwo on-premises data center locations. There is a company-managed router at earn data center. Each data center has a dedicated AWS Direct Connect connection to a Direct Connect gateway through a private virtual interface The router for the first location is advertising 110 routes to the Direct Connect gateway by using BGP and the router tor the second location is advertising 60 routes to the Direct Connect gateway by using BGP The Direct Connect gateway is attached to a company VPC through a virtual private gateway
A network engineer receives reports that resources In the VPC are not reachable from various locations in either data center. The network engineer checks the VPC route table and sees that the routes from the first data center. location are not being populated into the route table The network engineer must resolve this issue in the most operationally efficient manner
What should the network engineer do to meet these requirements'

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

Answer: D

NEW QUESTION 55
Your company runs an HTTPS application using an Elastic Load Balancing (ELB) load balancer/PHP on nginx server/RDS in multiple Availability Zones. You need to apply Geographic Restriction and identify the client’s IP address in your application to generate dynamic content.
How should you utilize AWS services in a scalable fashion to perform this task?

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

Answer: D

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

NEW QUESTION 60
Your company has a 1-Gbps AWS Direct Connect connection to AWS. Your company needs to send traffic from on-premises to a VPC owned by a partner company. The connectivity must have minimal latency at the lowest price.
Which of the following connectivity options should you choose?

A. Create a new Direct Connect connection, and set up a new circuit to connect to the partner VPC using a private virtual interface.
B. Create a new Direct Connect connection, and leverage the existing circuit to connect to the partner VPC.
C. Create a new private virtual interface, and leverage the existing connection to connect to the partner VPC.
D. Enable VPC peering and use your VPC as a transitive point to reach the partner VPC.

Answer: C

Explanation:
https://docs.aws.amazon.com/vpc/latest/peering/create-vpc-peering-connection.html#create-vpc-peering-connec

NEW QUESTION 65
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 67
A VPC is deployed with a 10 0 0.0/16 CIDR block. The engineering team is reviewing DHCP options and there is disagreement about the valid DNS addresses available for the VPC Which addresses are valid IP addresses provided by Amazon for this subnet' (Select TWO.)

A. 8.8.8.8
B. 10.00.2
C. 10.1.0.2
D. 169.254.169.253
E. 169.254.169.254

Answer: BE

NEW QUESTION 70
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 72
You need to set up an Amazon Elastic Compute Cloud (EC2) instance for an application that requires the lowest latency and the highest packet-per-second network performance. The application will talk to other servers in a peered VPC.
Which two of the following components should be part of the design? (Select two.)

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

Answer: AE

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

NEW QUESTION 77
Changes made to a security group attached to an Application Load Balancer resulted in connectivity issues for a company's production web application. The Network Engineer needs to lock down permissions for the company's AWS account, automate auditing for any changes, and set up notifications.
What actions should accomplish this?

A. Configure IAM user policies to lock down permissions for specific user
B. Enable AWS CloudTrail to identify API calls from user
C. Use AWS Config to audit any changes, and configure Amazon SNS to send notifications.
D. Configure IAM user policies to lock down permissions for specific user
E. Enable AWS CloudTrail to identify the API calls from user
F. Configure AWS CodeCommit to audit any changes in configurations, and configure Amazon SNS to send notifications.
G. Configure IAM user policies to lock down permissions for specific user
H. Enable AWS CloudTrail to identify the API calls from user
I. Configure Amazon Macie to use machine learning to identify any configuration changes, and configure Amazon SNS to send notifications.
J. Configure IAM role policies to lock down permissions for specific user
K. Configure Amazon GuardDuty to audit and monitor configuration changes, and configure Amazon SNS to send notifications.

Answer: A

NEW QUESTION 78
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 83
A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven’t yet upgraded.
What design will allow the company to serve both newer and earlier clients in the MOST efficient way?

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

Answer: D

NEW QUESTION 84
A Systems Administrator is designing a hybrid DNS solution with spilt-view. The apex-domain “example.com” should be served through name servers across multiple top-level domains (TLDs). The name server for subdomain “dev.example.com” should reside on-premises. The administrator has decided to use Amazon Route 53 to achieve this scenario.
What procedurals steps must be taken to implement the solution?

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

Answer: A

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

NEW QUESTION 87
A company is deploying a new web application that uses a three-tier model with a public-facing Network Load Balancer and web servers in an Amazon VPC. The application servers are hosted in the company's data center. There is an AWS Direct Connect connection between the VPC and the company’s data center. Load testing results indicate that up to 100 servers, equally distributed across multiple Availability Zones, are required to handle peak loads.
The Network Engineer needs to design a VPC that has a /24 CIDR assigned to it.
How should the Engineer allocate subnets across three Availability Zones for each tier?

A. Network Load Balancer: /29 per subnetWeb: /26 per subnet
B. Network Load Balancer: /28 per subnetWeb: /25 per subnet
C. Network Load Balancer: /28 per subnetWeb: /27 per subnet
D. Network Load Balancer: /28 per subnetWeb: /26 per subnet

Answer: D

NEW QUESTION 90
A Network Engineer is designing a new system on AWS that will take advantage of Amazon CloudFront for both content caching and for protecting the underlying origin. There is concern that an external agency might be able to access the IP addresses for the application’s origin and then attack the origin despite it being served by CloudFront. Which of the following solutions provides the strongest level of protection to the origin?

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

Answer: B

NEW QUESTION 92
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 94
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 98
Your hybrid networking environment consists of two application VPCs, a shared services VPC, and your corporate network. The corporate network is connected to the shared services VPC via an IPsec VPN with dynamic (BGP) routing enabled.
The applications require access to a common authentication service in the shared services VPC. You need to enable native network access from the corporate network to both application VPCs.
Which step should you take to meet the requirements?

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

Answer: C

NEW QUESTION 102
A company has an AWS Direct Connect connection between its on-premises data center and Amazon VPC. An application running on an Amazon EC2 instance in the VPC needs to access confidential data stored in the on-premises data center with consistent performance For compliance purposes, data encryption is required.
What should the network engineer do to meet these requirements?

A. Configure a public virtual interface on the Direct Connect connectio
B. Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.
C. Configure a private virtual interface on the Direct Connect connectio
D. Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.
E. Configure an internet gateway in the VPC Set up a software VPN between the customer gateway and an EC2 instance in the VPC.
F. Configure an internet gateway in the VPC Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.

Answer: D

NEW QUESTION 105
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 110
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 114
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 117
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 118
You have been asked to monitor traffic flows on your Amazon EC2 instance. You will be performing deep packet inspection, looking for atypical patterns.
Which tool will enable you to look at this data?

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

Answer: A

NEW QUESTION 123
A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2 instances now use a NAT gateway tor internet access After the migration, some long-running database queries from private EC2 instances to a publicly accessible third-party database no longer receive responses The database query logs reveal that the queries successfully completed after 7 minutes but that the client EC2 instances never received the response.
Which configuration change should a network engineer implement to resolve this issue"

A. Configure the NAT gateway timeout to allow connections for up to 600 seconds
B. Enable enhanced networking on the client EC2 instances
C. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds

D. Close idle TCP connections though the NAT gateway

Answer: C

NEW QUESTION 124
An organization delivers high-resolution, dynamic web content. Internet users access the content from a variety of platforms, including mobile, tablet and desktop. Each platform receives a customized experience to account for the differences in viewing modes. A dedicated, automatic-scaling fleet of Amazon EC2 instances is used for each platform to server content based on path-based headers.
Which combination of services will MINIMIZE cost and MAXIMIZE performance? (Select two.)

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

Answer: AE

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

NEW QUESTION 128
You are configuring a virtual interface for access to your VPC on a newly provisioned 1-Gbps AWS Direct Connect connection. Which two configuration values do you need to provide? (Select two.)

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

Answer: BE

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

NEW QUESTION 130
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 132
......