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
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 3
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 4
An organization has created a web application inside a VPC and wants to make it available to 200 client VPCs. The client VPCs are in the same region but are owned by other business units within the organization.
What is the best way to meet this requirement, without making the application publicly available?

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

Answer: A

NEW QUESTION 5
A company hosts several applications in the AWS Cloud across multiple VPCs that are connected to a transit gateway Redundant AWS Direct Connect connections and a Direct Connect gateway provide private network connectivity lo the company's on-premises environment
During a maintenance window, the networking team adds eight VPCs The application management team notices that there is no reachability between the newly created VPCs and the on-premises environment Connectivity between all VPCs through the transit gateway is working as expected.
Which of the following are possible causes of the connectivity issues? (Choose TWO)

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

Answer: AD

NEW QUESTION 6
A company is deploying a non-web application on an AWS load balancer. All targets are servers located
on-premises that can be accessed by using AWS Direct Connect. The company wants to ensure that the source IP addresses of clients connecting to the application are passed all the way to the end server.
How can this requirement be achieved?

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

Answer: C

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

NEW QUESTION 7
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 8
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 9
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 10
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 10
The Security department has mandated that all outbound traffic from a VPC toward an on-premises datacenter must go through a security appliance that runs on an Amazon EC2 instance.
Which of the following maximizes network performance on AWS? (Choose two.)

A. Support for the enhanced networking drivers
B. Support for sending traffic over the Direct Connect connection
C. The instance sizes and families supported by the security appliance
D. Support for placement groups within the VPC
E. Security appliance support for multiple elastic network interfaces

Answer: AC

NEW QUESTION 15
An organization wants to process sensitive information using the Amazon EMR service. The information is stored in on-premises databases. The output of processing will be encrypted using AWS KMS before it is uploaded to a customer-owned Amazon S3 bucket. The current configuration includes a VPS with public and private subnets, with VPN connectivity to the on-premises network. The security organization does not allow Amazon EC2 instances to run in the public subnet.
What is the MOST simple and secure architecture that will achieve the organization's goal?

A. Use the existing VPC and configure Amazon EMR in a private subnet with an Amazon S3 endpoint.
B. use the existing VPS and a NAT gateway, and configure Amazon EMR in a private subnet with an Amazon S3 endpoint.
C. Create a new VPS without an IGW and configure the VPN and Amazon EMR in a private subnet with an Amazon S3 endpoint.
D. Create a new VPS without an IGW and configure the VPN and Amazon EMR in a private subnet with an Amazon S3 endpoint and a NAT gateway.

Answer: A

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

NEW QUESTION 19
You are building an application that provides real-time audio and video services to customers on the Internet. The application requires high throughput. To ensure proper audio and video transmission, minimal latency is required.
Which of the following will improve transmission quality?

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

Answer: A

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

NEW QUESTION 23
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 25
Your company needs to leverage Amazon Simple Storage Solution (S3) for backup and archiving. According to company policy, data should not flow on the public Internet even if data is encrypted. You have set up two S3 buckets in us-east-1 and us-west-2. Your company data center is located on the West Coast of the United States. The design must be cost-effective and enable minimal latency.
Which design should you set up?

A. An AWS Direct Connect connection to us-east-1 and a Direct Connect connection to us-west-2.
B. An AWS Direct Connect connection to us-east-1.

C. An AWS Direct Connect connection to us-west-2.
D. An AWS Direct Connect connection to us-west-2 and a VPN connection to us-east-1.

Answer: C

NEW QUESTION 26
A Network Engineer is troubleshooting a network connectivity issue for an instance within a public subnet that cannot connect to the internet. The first step the Engineer takes is to SSH to the instance via a local bastion within the VPC and runs an ifconfig command to inspect the IP addresses configured on the instance. The output is as follows:

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

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

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

Answer: D

NEW QUESTION 30
A company's web application is deployed on Amazon EC2 instances behind a public Application Load Balancer. The application flags malicious requests and uses an AWS Lambda function to add the offending IP addresses to the network ACL to block any further request for 24 hours. Recently, the application has been receiving more malicious requests, which causes the network ACL to reach its limit of allowed entries.
Which action should be taken to block more IP addresses, without compromising the existing security requirements?

A. Update the AWS Lambda function to remove blocked entries from the network ACL after 2 hours.
B. Update the AWS Lambda function to block malicious IPs in security groups rather than the network ACL.
C. Update the AWS Lambda function to block malicious IPs in AWS WAF attached to the Application Load Balancer.
D. Update the AWS Lambda function to add an additional network ACL to the subnets once the limit for the previous ones has been reached.

Answer: C

NEW QUESTION 32
A company is using AWS to host all of its applications. Each application is isolated in its own Amazon VPC. Different environments such as Development, Test, and Production are also isolated in their own VPCs. The Network Engineer needs to automate VPC creation to enforce the company's network and security standards. Additionally, the CIDR range used in each VPC needs to be unique.
Which solution meets all of these requirements?

A. Use AWS CloudFormation to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.
B. Use AWS OpsWorks to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.
C. Use the VPC wizard in the AWS Management Consol
D. Type in the CIDR blocks for the VPC and subnets.
E. Create the VPCs using AWS CLI and use the dry-run flag to validate if the current CIDR range is in use.

Answer: A

NEW QUESTION 36
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 40
An IT company wants to securely perform an on-off migration of its on-premises VMs to the AWS Cloud by using AWS Server Migration Service {AWS SMS) For the first phase of the migration, the company must migrate 50 development VMs m batches during non-peak times over the next 7 days The VMs are between 2

GB and 5 GB in size The company has 1 Gbps of available bandwidth over the internet
Which network connectivity option meets these requirements MOST cost-effectively?

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

Answer: D

NEW QUESTION 44
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 48
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 51
A company has Iwo on-premises data center locations. There is a company-managed router at earn data center. Each data center has a dedicated AWS Direct Connect connection to a Direct Connect gateway through a private virtual interface The router for the first location is advertising 110 routes to the Direct Connect gateway by using BGP and the router tor the second location is advertising 60 routes to the Direct Connect gateway by using BGP The Direct Connect gateway is attached to a company VPC through a virtual private gateway
A network engineer receives reports that resources In the VPC are not reachable from various locations in either data center. The network engineer checks the VPC route table and sees that the routes from the first data center. location are not being populated into the route table The network engineer must resolve this issue in the most operationally efficient manner
What should the network engineer do to meet these requirements'

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

Answer: D

NEW QUESTION 56
You are designing the network infrastructure for an application server in Amazon VPC. Users will access all the application instances from the Internet and from an on-premises network. The on-premises network is connected to your VPC over an AWS Direct Connect link.
How should you design routing to meet these requirements?

A. Configure a single routing table with two default routes: one to the Internet via an IGW, the other to the on-premises network via the VG
B. Use this routing table across all subnets in your VPC.
C. Configure two routing tables: one that has a default route via the IGW, and another that has a default route via the VG
D. Associate both routing tables with each VPC subnet.
E. Configure a single routing table with a default route via the IG
F. Propagate a default route via BGP on the AWS Direct Connect customer route
G. Associate the routing table with all VPC subnet.
H. Configure a single routing table with a default route via the IG
I. Propagate specific routes for theon-premises networks via BGP on the AWS Direct Connect customer route
J. Associate the routing table with all VPC subnets.

Answer: D

NEW QUESTION 61
An organization has ordered a new AWS Direct Connect connection. The AWS Management Console reports that the connection is available and BGP status is up. However, the networking team is not able to reach instances in the VPC using ping on the organization's private IP address
What could cause this connectivity issue? (Choose two.)

A. The VGW is not advertising the correct CIDR range back on-premises.
B. The instance security group does not allow ICMP traffic.
C. A public virtual interface must be configured for Amazon EC2 connectivity.
D. The on-premises router is not advertising the correct CIDR range to AWS.

E. There is a misconfiguration of the bi-directional forwarding detection.

Answer: BD

NEW QUESTION 62
An organization has multiple applications running in VPCs across multiple AWS accounts. The network engineer has deployed a central VPC with a pair of software VPN instances that run IPSec tunnels with dynamic routing to VGWs of all application VPCs. This central VPC is connected to on-premises resources via a Direct Connect connection using a private VIF.
What additional configuration is required to enable the applications in VPCs to communicate with each other and access on-premises resources?

A. Configure each application VPC with a static route entry pointing the on-premises CIDR block to the software VPN instances.
B. Configure the central VPC with a static route entry pointing the on-premises CIDR block to local VGWs.
C. Advertise all application VPC CIDR blocks to on-premises resources via the VGW in the central VPC.
D. Configure IPSec tunnels from the on-premises router into the software VPN instances with dynamic routing.

Answer: D

NEW QUESTION 65
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 68
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 71
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 74
A company is running services in a VPC with a CIDR block of 10.5.0.0/22 End users report that they no longer can provision new resources because some ot the subnets in theVPC have run out of IP addresses
How should a network engineer resolve this issue?

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

Answer: D

NEW QUESTION 77
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 78
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 82
A company needs to allow its remote users to access company resources in the AWS Cloud. The company has two VPCs that are connected through VPC peering. The remote users must be able to access resources in both VPCs by using secure connections from their laptop computers The company does not want to implement an access management solution that requires additional costs or effort.
Which solution meets these requirements?

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

Answer: B

NEW QUESTION 84
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 85
Your company operates a single AWS account. A common services VPC is deployed to provide shared services, such as network scanning and compliance tools. Each AWS workload uses its own VPC, and each VPC must peer with the common services VPC. You must choose the most efficient and cost effective approach.
Which approach should be used to automate the required VPC peering?

A. AWS CloudTrail integration with Amazon CloudWatch Logs to trigger a Lambda function.
B. An OpsWorks Chef recipe to execute a command-line peering request.
C. Cfn-init with AWS CloudFormation to execute a command-line peering request.
D. An AWS CloudFormation template that includes a peering request.

Answer: D

Explanation:
https://cloakable.irdeto.com/2017/10/11/how-to-implement-vpc-peering-between-2-vpcs-in-the-same-aws-accou

NEW QUESTION 88
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 92
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 95
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 98
A legacy, on-premises web application cannot be load balances effectively. There are both planned and unplanned events that cause usage spikes to millions of concurrent users. The existing infrastructure cannot handle the usage spikes. The CIO has mandated that the application be moved to the cloud to avoid further disruptions, with the additional requirement that source IP addresses be unaltered to support network traffic-monitoring needs. Which of the following designs will meet these requirements?

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

Answer: D

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

NEW QUESTION 100
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 104
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 105
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 108
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 109
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 114
An organization with a growing e-commerce presence uses the AWS CloudHSM to offload the SSL/TLS processing of its web server fleet. The company leverages Amazon EC2 Auto Scaling for web servers to handle the growth. What architectural approach is optimal to scale the encryption operation?

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

D. Use multiple CloudHSM instances, and load balance them using an Application Load Balancer.

Answer: B

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

NEW QUESTION 119
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 121
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 122
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 127
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 132
.....

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