Amazon

Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

NEW QUESTION 1
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 2
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 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
You manage a web service that is used by client applications deployed in 300 offices worldwide. The web service architecture is an Elastic Load balancer (ELB) distributing traffic across four application servers deployed in an autoscaling group across two availability zones.
The ELB is configured to use round robin, and sticky sessions are disabled. You have configured the NACLs and Security Groups to allow port 22 from your bastion host, and port 80 from 0.0.0.0/0. The client configuration is managed by each regional IT team.
Upon inspection you find that a large amount of requests from incorrectly configured sites are causing a single application server to degrade. The remainder of the requests are equally distributed across all servers with no negative effects.
What should you do to remedy the situation and prevent future occurrences?

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

Answer: C

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

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

Answer: AD

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

NEW QUESTION 8
A company wants to migrate its workloads to the AWS Cloud. The company has two web applications and wants to run them in separate, isolated VPCs. The company needs to use Elastic Load Balancing to distribute requests between application instances.
For security reasons, internet gateways must not be attached to the application VPCs. Inbound HTTP requests to the application must be routed through a centralized VPC. and the application VPCs must not be exposed to any other inbound traffic The application VPCs cannot be allowed to initiate any outbound connections
What should a network engineer do to meet these requirements?

A. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
B. Create a public Network Load Balancer (NLB) in the centralized VP
C. Create target groups for the private DNS names of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.
D. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
E. Create a public Network Load Balancer (NLB) in the centralized VP
F. Create target groups for the private IP addresses of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.
G. Run the applications behind private Network Load Balancers (NLBs) in separate VPC
H. Create VPC peering connections between the application VPCs and the centralized VP
I. Create a public Application Load Balancer (ALB) in the centralized VP
J. Create target groups for the private DNS names of the NLB
K. Configure host-based routing to route application traffic between individual applications though the ALB.
L. Run the applications behind private Network Load Balancers (NLBs) inseparate VPC
M. Configure each NLB as an AWS PrivateLink endpoint service with associated VPC endpoints in the centralized VPC Create target groups that include the private IP addresses of each endpoin
N. Create a public Application Load Balancer (ALB) in the centralized VP
O. Configurehost-based routing to route application traffic to the corresponding target group through the ALB.

Answer: D

NEW QUESTION 9
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 10
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 10
A financial services company receives real-time stock quotes in its ingestion VPC. The company plans to perform customer-specific data analysis on the stock quotes in various VPCs. The stock quotes must be distributed simultaneously from Amazon EC2 instances in the ingestion VPC to EC2 instances in the data analysis VPCs
Which set of configuration steps should the company lake to meet these requirements?

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

Answer: D

NEW QUESTION 11
An insurance company is planning the migration of workloads from its on-premises data center to the AWS Cloud The company requires end-to-end domain name resolution Bidirectional DNS resolution between AWS
and the existing on-premises environments must be established The workloads will be migrated into multiple VPCs. The workloads also have dependencies on each other, and not all the workloads will be migrated at the same time
Which solution meets these requirements? Which solution meets these requirements?

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

Answer: B

NEW QUESTION 15
A company is connecting to a VPC over an AWS Direct Connect using a private VIF, and a dynamic VPN connection as a backup. The company's Reliability Engineering team has been running failover and resiliency tests on the network and the existing VPC by simulating an outage situation on the Direct Connect connection. During the resiliency tests, traffic failed to switch over to the backup VPN connection.
How can this failure be troubleshot?

A. Ensure that Bidirectional Forwarding Detection is enabled on the Direct Connect connection
B. Confirm that the same routes are being advertised over both the VPN and Direct Connect.
C. Reconfigure the Direct Connect session from static routes to Border Gateway Protocol (BGP) peering.
D. Configure a virtual private gateway for the VPN and another virtual private gateway for Direct Connect.

Answer: B

NEW QUESTION 19
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 21
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 25
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 29
Your organization’s corporate website must be available on www.acme.com and acme.com. How should you configure Amazon Route 53 to meet this requirement?

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

Answer: A

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

NEW QUESTION 31
An application runs on a fleet of Amazon EC2 instances in a VPC. All instances can reach one another using private IP addresses. The application owner has a new requirement that the domain name received via DHCP should be different for a particular set of instances that are currently in one particular subnet.
What changes should be made to meet this requirement while continuing to support the existing application requirements?

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

Answer: D

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

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

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

Answer: B

NEW QUESTION 38
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 41
A Network Engineer needs to create a public virtual interface on the company's AWS Direct Connect connection and only import routes which originated from the same region as the Direct Connect location.
What action should accomplish this?

A. Configure a prefix list on the customer router containing the AWS IP address ranges for the specific region.
B. Configure a filter on the company's router to only import routes with the 7224:8100 BGP community attribute.
C. Configure a filter on the company's router to only import routes without a BGP community attribute and a maximum path length of 3.
D. Configure a filter in the console and only allow routes advertised by AWS without a BGP community attribute and a maximum path length of 3.

Answer: B

NEW QUESTION 43
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 44
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 45
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 49
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 54
An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used.
Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: "There are not enough free addresses in subnet 'subnet-12345677' to satisfy the requested number of instances."
What action will resolve the availability problem?

A. Create a new subnet using a VPC secondary IPv6 CIDR, and associate an IPv6 CID
B. Include the new subnet in the Auto Scaling group.
C. Create a new subnet using a VPC secondary IPv4 CIDR, and associate an IPv6 CID
D. Include the new subnet in the Auto Scaling group.
E. Resize the IPv6 CIDR on each of the existing subnet
F. Modify the Auto Scaling group maximum number of instances.
G. Add a secondary IPv4 CIDR to the Amazon VP
H. Assign secondary IPv4 address space to each of the existing subnets.

Answer: B

NEW QUESTION 55
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 59
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 61
A company uses an Application Load Balancer (ALB) to provide access to a multi-tenant web application for 25 customers The company creates a unique hostname for each customer to use to access the application Hostnames use the format customer-name example.com.
Each customer has a dedicated group of Amazon EC2 instances that run their own version of the web application. When a customer visits customer-name example com, the ALB should route the request to the correct group of EC2 instances The company requires a highly available solution that is easy to maintain
Which solution meets these requirements at the LOWEST cost?

A. Create one ALB for all customers Create a listener rule that includes an HTTP header condition to match the URL Add a forward action to route the request to

the customer target group Use Amazon Route 53 to create an alias record for each customer-name example com hostname that points to the ALB
B. Create one ALB for each customer Configure the listener to route requests to the customer target group Configure an NGINX proxy server to manageconnections to each ALB Use Amazon Route 53 to create a CNAME record for each customer-name example com hostname that points to the NGINX proxy server
C. Create one ALB for ail customers Create a listener rule that includes a Host header condition to match the hostname Add a forward action to route the request to the customer target group Use Amazon Route 53 to create an alias record for each customer-name example com hostname that points to the ALB
D. Create one ALB for each customer Configure the listener to route requests to the customer target group Create an Amazon CloudFront distribution Add each ALB to the distribution as a custom origin Use Amazon Route 53 to create an alias for each customer-name example com hostname that points to the CloudFront distribution

Answer: A

NEW QUESTION 64
A financial company is designing a secure AWS network architecture to support a hybrid cloud strategy. Systems deployed in the AWS Cloud are mission critical and have strict availability requirements. The
company anticipates the need for hundreds of VPCs. Instances will be transient and rely heavily on DNS resolution The applications must be designed to have Availability Zone isolation and tolerate the loss of an Availability Zone
What is the MOST reliable way to implement DNS in this scenario?

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

Answer: C

NEW QUESTION 66
You ping an Amazon Elastic Compute Cloud (EC2) instance from an on-premises server. VPC Flow Logs record the following:
2 123456789010 eni-1235b8ca 10.123.234.78 172.11.22.33 0 0 1 8 672 1432917027
1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.11.22.33 10.123.234.78 0 0 1 4 336 1432917027
1432917082 ACCEPT OK
2 123456789010 eni-1235b8ca 172.11.22.33 10.123.234.78 0 0 1 4 336 1432917094
1432917142 REJECT OK
Why are ICMP responses not received by the on-premises system?

A. The inbound network access control list is blocking the traffic
B. The outbound network access control list is blocking the traffic
C. The inbound security group is blocking the traffic.
D. The outbound security group is blocking the traffic.

Answer: B

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html

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 75
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 78
A customer has set up multiple VPCs for Dev, Test, Prod, and Management. You need to set up AWS Direct Connect to enable data flow from on-premises to

each VPC. The customer has monitoring software running in the Management VPC that collects metrics from the instances in all the other VPCs. Due to budget requirements, data transfer charges should be kept at minimum.
Which design should be recommended?

A. Create a total of four private VIFs, one for each VPC owned by the customer, and route traffic between VPCs using the Direct Connect link.
B. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs.
C. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs, enable source/destination NAT in the Management VPC.
D. Create a total of four private VIFs, and enable VPC peering between all VPCs.

Answer: A

NEW QUESTION 82
A company uses a single connection to the internet when connecting its on-premises location to AWS. It has selected an AWS Partner Network (APN) Partner to provide a point-to-point circuit for its first-ever 10 Gbps AWS Direct Connect connection.
What steps must be taken to order the cross-connect at the Direct Connect location?

A. Obtain the LOA/CFA from the APN Partner when ordering connectivit
B. Upload it to the AWS Management Console when creating a new Direct Connect connectio
C. AWS will ensure that the cross-connect is installed.
D. Obtain the LOA/CFA from the AWS Management Console when ordering the Direct Connect connectio
E. Provide it to the APN Partner when ordering connectivit
F. The Direct Connect partner will ensure that the cross-connect is installed.
G. Obtain the LOA/CFA each from the AWS Management Console and the APN Partne
H. Provide both tothe Facility Operator of the Direct Connect locatio
I. The Facility Operator will ensure that the cross-connect is installed.
J. Identify the APN Partner in the AWS Management Console when creating the Direct Connect connectio
K. Provide the resulting Connection ID to the APN Partner, who will ensure that the cross-connect is installed.

Answer: B

NEW QUESTION 83
All IP addresses within a 10.0.0.0/16 VPC are fully utilized with application servers across two Availability Zones. The application servers need to send frequent UDP probes to a single central authentication server on the Internet to confirm that is running up-to-date packages. The network is designed for application servers to use a single NAT gateway for internal access. Testing reveals that a few of the servers are unable to communicate with the authentication server.

A. The NAT gateway does not support UDP traffic.
B. The authentication server is not accepting traffic.
C. The NAT gateway cannot allocate more ports.
D. The NAT gateway is launched in a private subnet.

Answer: C

Explanation:
Ref: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
"A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. This limit also applies if you create approximately 900 connections per second to a single destination (about 55,000 connections per minute). If the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, you can create an additional 55,000 connections. For more than 55,000 connections, there is an increased chance of connection errors due to port allocation errors. These errors can be monitored by viewing the ErrorPortAllocation CloudWatch metric for your NAT gateway. For more information, see Monitoring NAT Gateways Using Amazon CloudWatch."

NEW QUESTION 86
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 87
Your company uses an NTP server to synchronize time across systems. The company runs multiple versions of Linux and Windows systems. You discover that the NTP server has failed, and you need to add an alternate NTP server to your instances.
Where should you apply the NTP server update to propagate information without rebooting your running instances?

A. DHCP Options Set
B. instance user-data
C. cfn-init scripts
D. instance meta-data

Answer: A

Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-dhcp-options.html

NEW QUESTION 92
A Network Engineer has enabled VPC Flow Logs to troubleshoot an ICMP reachability issue for an echo reply from an Amazon EC2 instance. The flow logs reveal an ACCEPT record for the request from the client to the EC2 instance, and a REJECT record for the response from the EC2 instance to the client.
What is the MOST likely reason for there to be a REJECT record?

A. The security group is denying inbound ICMP.
B. The network ACL is denying inbound ICMP.
C. The security group is denying outbound ICMP.
D. The network ACL is denying outbound ICMP.

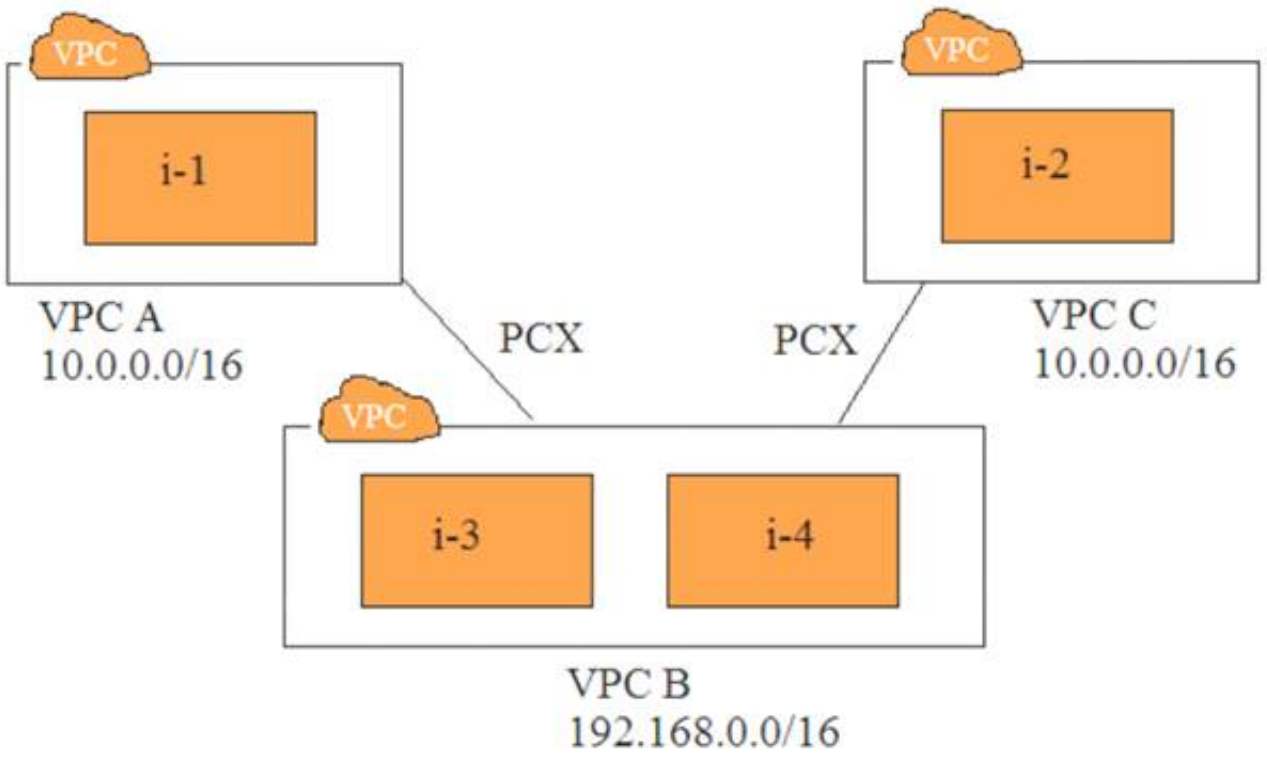
Answer: D

NEW QUESTION 95
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 96
Refer to the image.



You have three VPCs: A, B, and C. VPCs A and C are both peered with VPC B. The IP address ranges are as follows:
VPC A: 10.0.0.0/16
VPC B: 192.168.0.0/16
VPC C: 10.0.0.0/16
Instance i-1 in VPC A has the IP address 10.0.0.10. Instance i-2 in VPC C has the IP address 10.0.0.10. Instances i-3 and i-4 in VPC B have the IP addresses 192.168.1.10 and 192.168.1.20, respectively, i-3 and i-4 are in the subnet 192.168.1.0/24.
i-3 must be able to communicate with i-1
i-4 must be able to communicate with i-2
i-3 and i-4 are able to communicate with i-1, but not with i-2.
Which two steps will fix this problem? (Select two.)

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

Answer: AE

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

NEW QUESTION 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 105
A team implements a highly available solution using Amazon AppStream 2.0. The AppStream 2.0 fleet needs to communicate with resources both in an existing VPC and on-premises. The VPC is connected to the on-premises environment using an AWS Direct Connect private virtual interface.
What implementation enables on-premises users to connect to AppStream and existing VPC resources?

A. Deploy two subnets into the existing VP
B. Add a public virtual interface to the Direct Connect connection for users to access the AppStream endpoint
C. Deploy two subnets into the existing VP
D. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.
E. Deploy a new VPC with two subnet
F. Create a VPC peering connection between the two VPCs for users to access the AppStream endpoint.
G. Deploy one subnet into the existing VP
H. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.

Answer: B

NEW QUESTION 110
An organization is using a VPC endpoint for Amazon S3. When the security group rules for a set of instances were initially configured, access was restricted to allow traffic only to the IP addresses of the Amazon S3 API endpoints in the region from the published JSON file. The application was working properly, but now is logging a growing number of timeouts when connecting with Amazon S3. No internet gateway is configured for the VPC.
Which solution will fix the connectivity failures with the LEAST amount of effort?

A. Create a Lambda function to update the security group based on AmazonIPSpaceChanged notifications.
B. Update the VPC routing to direct Amazon S3 prefix-list traffic to the VPC endpoint using the route tableAPIs.
C. Update the application server’s outbound security group to use the prefix-list for Amazon S3 in the same region.
D. Create an additional VPC endpoint for Amazon S3 in the same route table to scale the concurrent connections to Amazon.

Answer: C

Explanation:
https://aws.amazon.com/blogs/aws/subscribe-to-aws-public-ip-address-changes-via-amazon-sns/

NEW QUESTION 114
A customer is using ABC Telecom as a network provider. The customer has 10 different offices connected to ABC Telecom’s MPLS backbone. The customer is setting up an AWS Direct Connect connection to AWS and has provided the LOA-CFA to ABC Telecom. ABC Telecom has terminated the Direct Connect circuit into their MPLS backbone. To uniquely identify the customer’s traffic over the MPLS backbone, the customer must encapsulate all traffic with VLAN tag 100. The customer wants to send traffic to multiple VPCs.
Which two steps should be taken to meet the customer’s requirement? (Select two.)

A. The customer performs Q-in-Q tunneling, with the AWS-required VLAN tag in the inside and VLAN 100 as the outside tag.
B. Create a support ticket with AWS to request the removal of the outer VLAN tag 100 as the traffic reaches AWS routers.
C. Send the traffic for all VPCs with the same VLAN tag 100 and use BGP to ensure that proper routing takes place to the appropriate VPC.
D. ABC Telecom removes the other tag before sending the packet to AWS.
E. ABC Telecom creates a support ticket with AWS to exchange MPLS labels and include the AWS port as part of their MPLS network.

Answer: AD

NEW QUESTION 119
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 121
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 125
You operate a production VPC with both a public and a private subnet. Your organization maintains a restricted Amazon S3 bucket to support this production workload. Only Amazon EC2 instances in the private subnet should access the bucket. You implement VPC endpoints(VPC-E) for Amazon S3 and remove the NAT that previously provided a network path to Amazon S3. The default VPC-E policy is applied. Neither EC2 instances in the public or private subnets are able to access the S3 bucket.
What should you do to enable Amazon S3 access from EC2 instances in the private subnet?

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

Answer: B

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

NEW QUESTION 126
.....

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