Amazon.ANS-C00.v2022-06-30.q165

Exam Code:	ANS-C00
Exam Name:	AWS Certified Advanced Networking Specialty (ANS-C00) Exam
Certification Provider:	Amazon
Free Question Number:	165
Version:	v2022-06-30
# of views:	1504
# of Questions views:	5547
https://www.dumpsfiles.com/files/Amazon/ANS-C00/Amazon.ANS-C00.v2022-06-30.q165	

NEW QUESTION: 1
Your on-premises network has an IP address range of 11.11.0.0/16. Only IPs within this network range can be used for inter-server communication. The IP address range 11.11.253.0/24 has been allocated for the cloud.
You need to design a VPC in AWS. The servers within the VPC should be able to communicate with hosts both on the Internet and on-premises through a VPN connection.
What combination of configuration steps meets your needs? (Choose 2)
A. Set up the VPC with an IP address range of 11.11.253.0/24.
B. Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set up a NAT gateway to do translation between 10.10.10.0/24 and 11.11.253.0/24 for all outbound traffic.
C. Set up a VPN connection between a VGW and an on-premises router, set the VGW as the default gateway for all traffic, and configure the on-premises router to forward traffic to the Internet.
D. Set up a VPN connection between a VGW and an on-premises router, set the VGW as the default gateway for traffic destined to 11.11.0.0/24, and add a VPC subnet route to point the default gateway to an Internet gateway for Internet traffic.
E. Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set the VGW to do a source IP translation of all outbound packets to 11.11.0.0/16.
Answer: (SHOW ANSWER)
The VPC needs to use a CIDR block in the assigned range (and be non-overlapping with the data center). All traffic not destined for the VPC is routed to the VGW (that route is assumed) and must then be forwarded to the Internet when it arrives on-premises. B and E are wrong because they are not in the assigned range (you can use non-RFC 1918 addresses in a VPC). D is wrong because it directs traffic to the Internet through the Internet gateway.

NEW QUESTION: 2

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: (SHOW ANSWER)
https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html

NEW QUESTION: 3
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 Route 53 private hosted zone's VPC associations to include the new VPC.
B. Launch Amazon EC2-based DNS proxies in the new VPC. Specify the proxies in the DHCP options set.
C. Update the DHCP options set for the new VPC with the Route 53 nameserver IP addresses.
D. Launch Amazon EC2-based DNS proxies in the new VPC. Specify the proxies as forwarders in the onpremises DNS.
E. Update the on-premises DNS to include forwarders to the Route 53 nameserver IP addresses.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 4
You can use the ____ page of the AWS Config console to look up resources that AWS Config has discovered, including deleted resources and resources that are not currently being recorded.
A. snapshot listing
B. configuration history
C. resource inventory

D. resource database

Answer: (SHOW ANSWER)

You can use the AWS Config console, AWS CLI, and AWS Config API to look up the resources that AWS Config has taken an inventory of, or discovered, including deleted resources and resources that AWS Config is not currently recording. AWS Config discovers supported resource types only. You can use the AWS Config console in the AWS Management console to look up these resources. The Resource Inventory page lets you perform this search.

Reference:

http://docs.aws.amazon.com/config/latest/developerguide/looking-up-discovered-resources.html

NEW QUESTION: 5

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 using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.

B. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.

C. Configure acme.com with an A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.

D. Configure acme.com with an ALIAS record targeting the ELB. www.acme.com with an ALIAS record targeting the ELB.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 6

You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems. Which two AWS Services cloud you leverage to build an automated notification system? (Select two.)

A. Internet gateway

B. VPC Flow Logs

C. AWS CloudTrail

D. Lambda

E. AWS Inspector

Answer: B,D (LEAVE A REPLY)

References: https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-by-using-aws-cloudtrail-amazon-sns-and-aws-lambda/

NEW QUESTION: 7

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 ELB. www.acme.com with an ALIAS record targeting the ELB.
B. Configure acme.com with an A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
C. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
D. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.
Answer: D (LEAVE A REPLY)
https://aws.amazon.com/blogs/security/how-to-manage-amazon-guardduty-security-findings-across-multiple-accounts/

NEW QUESTION: 8
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 OpsWorks to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.
B. Create the VPCs using AWS CLI and use the dry-run flag to validate if the current CIDR range is in use.
C. Use the VPC wizard in the AWS Management Console. Type in the CIDR blocks for the VPC and subnets.
D. 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.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
Your organization uses a VPN to connect to your VPC but must upgrade to a 1-G AWS Direct Connect connection for stability and performance. Your telecommunications provider has provisioned the circuit from your data center to an AWS Direct Connect facility and needs information on how to cross-connect (e.g., which rack/port to connect).
What is the AWS-recommended procedure for providing this information?
A. Create a support ticket. Provide your AWS account number and telecommunications company's name and where you need the Direct Connect connection to terminate.
B. Ask your telecommunications provider to contact AWS through an AWS Partner Channel. Provide your AWS account number.

C. Contact an AWS Account Manager and provide your AWS account number, telecommunications company's name, and where you need the Direct Connect connection to terminate.
D. Create a new connection through your AWS Management Console and wait for an email from AWS with information.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
Your organization has a newly installed 1-Gbps AWS Direct Connect connection. You order the cross- connect from the Direct Connect location provider to the port on your router in the same facility. To enable the use of your first virtual interface, your router must be configured appropriately.
What are the minimum requirements for your router?
A. 1-Gbps Multi Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
B. IPsec Parameters, Pre-Shared key, Peer IP Address, BGP Session with MD5
C. BGP Session with MD5, 802.1Q VLAN, Route-Map, Prefix List, IPsec encrypted GRE Tunnel
D. 1-Gbps Single Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
Answer: (SHOW ANSWER)

NEW QUESTION: 11
An organization delivers high-resolution, dynamic web content. Internet users access the content from a variety of platforms, including mobile, tablet and desktop. Each platform receives a customized experience to account for the differences in viewing modes. A dedicated, automatic-scaling fleet of Amazon EC2 instances is used for each platform to server content based on path-based headers.
Which combination of services will MINIMIZE cost and MAXIMIZE performance? (Select two.)
A. Amazon CloudFront with Lambda@Edge
B. Network Load Balancer
C. Amazon S3 static websites
D. Amazon Route 53 with traffic flow policies
E. Application Load Balancer
Answer: A,E (LEAVE A REPLY)
Explanation
References: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html

NEW QUESTION: 12
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. ABC Telecom creates a support ticket with AWS to exchange MPLS labels and include the AWS port as part of their MPLS network.
B. The customer performs Q-in-Q tunneling, with the AWS-required VLAN tag in the inside and VLAN 100 as the outside tag.
C. Create a support ticket with AWS to request the removal of the outer VLAN tag 100 as the traffic reaches AWS routers.
D. ABC Telecom removes the other tag before sending the packet to AWS.
E. 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.
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 13
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 (LEAVE A REPLY)
Explanation
https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-us

NEW QUESTION: 14
The Web Application Development team is worried about malicious activity from 200 random IP addresses.
Which action will ensure security and scalability from this type of threat?
A. Write iptables rules on the instance to block the IP addresses.
B. Use inbound network ACL rules to block the IP addresses.
C. Use inbound security group rules to block the IP addresses.
D. Use AWS WAF to block the IP addresses.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15

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 (LEAVE A REPLY)
https://medium.com/faun/aws-network-load-balancer-and-client-source-ip-410bfeded6df

NEW QUESTION: 16
You are managing a VPC with 4 AZs. There is a load balancer managing the public accessibility to your servers. You have a secondary ENI with a private IPv4 address on an instance that is serving public web traffic. Your server communicates over private addresses to a database in another subnet. Security is a major concern for your company and whitelisting is in effect. You have to bring the web server down for maintenance, what two things should you do? Choose the 2 correct answers:
A. Reboot the instance.
B. Move the ENI from one server to the other.
C. Associate the new ENI with the database security group.
D. Configure a secondary ENI on the standby instance.
Answer: (SHOW ANSWER)
You must configure a secondary ENI on the standby instance with an IP address that can access the data subnet. This may require modification of the security group for the database.

NEW QUESTION: 17
You use a VPN to extend your corporate network into a VPC. Instances in the VPC are able to resolve resource records in an Amazon Route 53 private hosted zone. Your on-premises DNS

server is configured with a forwarder to the VPC DNS server IP address. On-premises users are unable to resolve names in the private hosted zone, although instances in a peered VPC can. What should you do to provide on-premises users with access to the private hosted zone?
A. Create a proxy resolver within the VPC. Point the on-premises forwarder to the proxy resolver.
B. Modify the network access control list on the VPC to allow DNS queries from on-premises systems.
C. Configure the on-premises server as a secondary DNS for the private zone. Update the NS records.
D. Update the on-premises forwarders with the four name servers assigned to the private hosted zone.
Answer: (SHOW ANSWER)
Explanation
References:
https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-by

NEW QUESTION: 18
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 instance security group does not allow ICMP traffic.
B. The on-premises router is not advertising the correct CIDR range to AWS.
C. The VGW is not advertising the correct CIDR range back on-premises.
D. A public virtual interface must be configured for Amazon EC2 connectivity.
E. There is a misconfiguration of the bi-directional forwarding detection.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 19
Which two choices can serve as a directory service for WorkSpaces? Choose the 2 correct answers:
A. Simple AD
B. Enhanced AD
C. Direct Connection
D. AWS Microsoft AD
Answer: A,D (LEAVE A REPLY)
There is no such thing as "Enhanced AD" and DX is not a directory service.

NEW QUESTION: 20
A company is about to migrate an application from its on-premises data center to AWS. As part of the planning process, the following requirements involving DNS have been identified.

On-premises systems must be able to resolve the entries in an Amazon Route 53 private hosted zone.
Amazon EC2 instances running in the organization's VPC must be able to resolve the DNS names of on-premises systems The organization's VPC uses the CIDR block 172.16.0.0/16.
Assuming that there is no DNS namespace overlap, how can these requirements be met?
A. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxies. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to 172.16.0.2. Change the DHCP options set for the VPC to use the new DNS proxies. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 as authoritative for the Route 53 private hosted zone.
B. Change the DHCP options set for the VPC to use both the on-premises DNS systems. Configure the on-premises DNS systems with a stub-zone, delegating the Route 53 private hosted zone's name servers as authoritative for the Route 53 private hosted zone.
C. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxies. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to the Amazon-provided DNS server (172.16.0.2). Change the DHCP options set for the VPC to use the new DNS proxies. Configure the on-premises DNS systems with a stub- zone, delegating the proxies as authoritative for the Route 53 private hosted zone.
D. Change the DHCP options set for the VPC to use both the Amazon-provided DNS server and the on- premises DNS systems. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 as authoritative for the Route 53 private hosted zone.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
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. Deploy an IPsec VPN over a public virtual interface on a new 10-Gbps Direct Connect connection.
B. Install a second 10-Gbps Direct Connect connection to a Direct Connect location in eu-west-1.
C. Install a second 10-Gbps Direct Connect connection to the same Direct Connection location.
D. Install a second 10-Gbps Direct Connect connection to a second Direct Connect location for eu-central-1.
E. Deploy an IPsec VPN over the Internet to the eu-west-1 region for diversity.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 22
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. cfn-init scripts
B. instance meta-data
C. DHCP Options Set
D. instance user-data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
The Payment Card Industry Data Security Standard (PCI DSS) merchants that handle credit card data must use strong cryptography. These merchants must also use security protocols to protect sensitive data during transmission over public networks.
You are migrating your PCI DSS application from on-premises SSL appliance and Apache to a VPC behind Amazon CloudFront.
How should you configure CloudFront to meet this requirement?
A. Configure the CloudFront Cache Behavior to require HTTPS and the CloudFront Origin's Protocol Policy to 'Match Viewer'.
B. Configure the CloudFront Cache Behavior to allow TCP connections and to forward all requests to the origin without TLS termination at the edge.
C. Configure the CloudFront Cache Behavior to require HTTPS and to forward requests to the origin via AWS Direct Connect.
D. Configure the CloudFront Cache Behavior to redirect HTTP requests to HTTPS and to forward request to the origin via the Amazon private network.
Answer: A (LEAVE A REPLY)
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesOriginProtocolPolicy

NEW QUESTION: 24
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. 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.
B. 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.
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: (SHOW ANSWER)

NEW QUESTION: 25
You need to set up a VPN between AWS VPC and your on-premises network. You create a VPN connection in the AWS Management Console, download the configuration file, and install it on your on- premises router. The tunnel is not coming up because of firewall restrictions on your router. Which two network traffic options should you allow through the firewall? (Select two.)
A. UDP port 500
B. IP protocol 50
C. IP protocol 5
D. TCP port 50
E. TCP port 500
Answer: (SHOW ANSWER)
Explanation/Reference:
References: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html

NEW QUESTION: 26
You need to quickly view inbound traffic to an instance to determine why it isn't reaching the instance properly. What is the best tool for this? Choose the correct answer:
A. Wireshark
B. CloudWatch
C. CloudTrail
D. Flow Logs
Answer: D (LEAVE A REPLY)
CloudWatch only shows the amount of data in. Wireshark cannot see anything inside AWS infrastructure. You can only use it to view instance traffic.

NEW QUESTION: 27
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. Update the Security Groups to only allow port 80 to the application servers from the ELB.
B. Update the NACL to only allow port 80 to the application servers from the ELB servers.
C. Terminate the affected instance and allow Auto Scaling to create a new instance.
D. Mark the affected instance as degraded in the ELB and raise it with the client application team.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
When an AWS Config rule is triggered a JSON object known as an AWS Config Event is created. This object contains another JSON string in its ____ parameter, which describes the event that triggered the rule.
A. resultToken
B. eventLeftScope
C. invokingEvent
D. configRuleName
Answer: (SHOW ANSWER)
The JSON object for an AWS Config event contains an invoking Event attribute, which describes the event that triggers the evaluation for a rule. If the event is published in response to a resource configuration change, the value for this attribute is a string that contains a JSON configuration Item or a configuration Item Summary (for oversized configuration items). The configuration item represents the state of the resource at the moment that AWS Config detected the change. If the event is published for a periodic evaluation, the value is a string that contains a JSON object. The object includes information about the evaluation that was triggered. For each type of event, a function must parse the string with a JSON parser to be able to evaluate its contents.
Reference:
http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_example-events.html

NEW QUESTION: 29
A network engineer has configured a private hosted zone using Amazon Route 53. The engineer needs to configure health checks for record sets within the zone that are associated with instances.
How can the engineer meet the requirements?
A. Create a CloudWatch metric that checks the status of the EC2 StatusCheckFailed metric, add an alarm to the metric, and then create a health check that is based on the state of the alarm.

B. Configure a Route 53 health check pointing to an Amazon SNS topic that notifies an Amazon CloudWatch alarm when the Amazon EC2 StatusCheckFailed metric fails.
C. Create a CloudWatch alarm for the StatusCheckFailed metric and choose Recover this instance, selecting a threshold value of 1.
D. Configure a Route 53 health check to a private IP associated with the instances inside the VPC to be checked.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
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 outbound ICMP.
B. The security group is denying inbound ICMP.
C. The network ACL is denying outbound ICMP.
D. The network ACL is denying inbound ICMP.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
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: B (LEAVE A REPLY)
Explanation
https://aws.amazon.com/answers/networking/vpc-network-management-and-monitoring/ VPC Flow Logs capture network flow information for a VPC, subnet, or network interface in Amazon CloudWatch Logs. Flow logs can help you with a number of tasks, such as troubleshooting why specific traffic is not reaching an instance, which in turn can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance, to profile your network traffic, and to look for abnormal traffic behaviors. A common use of VPC flow logs is to watch for abnormal and unexpected denied outbound connection requests, which could be an indication of a misconfigured or compromised EC2 instance. CloudWatch Alerts can provide rudimentary network alerting on VPC Flow Logs, however AWS APN members provide third-party log management systems that provide extensive reporting, visualization, and alerting capabilities based on VPC Flow Log data.

NEW QUESTION: 32
Which service would you use to see CPU usage?
Choose the correct answer:
A. None of the above
B. Config
C. CloudWatch
D. CloudTrail
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
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. VPC flow logs at the subnet level
C. Packet sniffing at the instance level
D. Packet sniffing at the VPC level
Answer: A (LEAVE A REPLY)

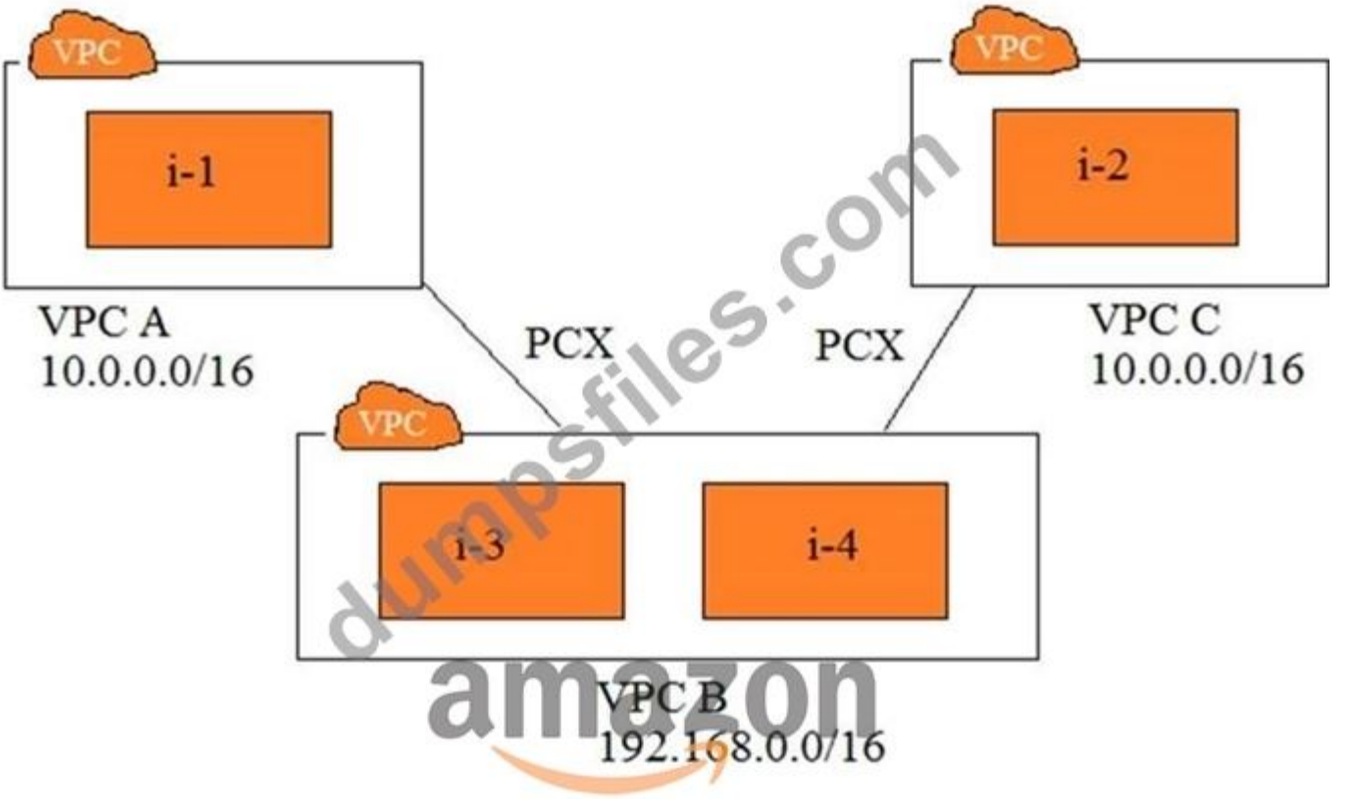
NEW QUESTION: 34
You are building an application that provides real-time audio and video services to customers on the Internet. The application requires high throughput. To ensure proper audio and video transmission, minimal latency is required.
Which of the following will improve transmission quality?
A. Enable enhanced networking
B. Select G2 instance types
C. Enable jumbo frames
D. Use multiple elastic network interfaces
Answer: A (LEAVE A REPLY)

With G3 instances, Enhanced Networking using the Elastic Network Adapter (ENA) with 25 Gbps of aggregate network bandwidth within a Placement Group.
https://aws.amazon.com/ec2/instance-types/
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

NEW QUESTION: 35
A network engineer deploys an application in a private subnet in a VPC that connects to many external video feed providers using RTMP over the internet. A NAT gateway has been deployed in a public subnet and is working as expected. From the Amazon EC2 instance, the application is able to connect to all feed providers except one, which hangs when connecting. Manually testing a connection from an Amazon EC2 instance in the public subnet to the problem feed indicates that the feed works as expected.
What is causing this issue?
A. The NAT gateway does not support fragmented packets.
B. An Amazon EC2 instance expects to communicate with an MTU of 9001.
C. The internet gateway only supports an MTU of 1500 bytes.
D. The security group on the instances does not allow PMTUD.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
You have a hybrid environment in which your VPC queries your on-premises DNS server for up resources in your environment. The EC2 instances in your VPC are unable to resolve on-premises resources. What are two possible reasons for this problem? Choose the 2 correct answers:
A. Your NACL is blocking UDP port 53 outbound
B. Your security group is blocking port 53 inbound
C. Your NACL is blocking TCP port 53 outbound.
D. Your on-premises firewall is blocking port 443
Answer: A,C (LEAVE A REPLY)
DNS requires TCP and UDP port 53.

NEW QUESTION: 37
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 two route tables: one with a route for destination VPC A, and another for destination VPC C.
B. Create a new route table for VPC B, with unique route entries for destination VPC A and destination VPC C.
C. Change the IP address of i-2 to 10.0.0.100. Assign it an elastic IP address.
D. Create subnets 192.168.1.0/27 and 192.168.1.16/27. Move i-3 and i-4 to these subnets, respectively.
E. Create subnets 192.168.1.0/28 and 192.168.1.16/28. Move i-3 and i-4 to these subnets, respectively.

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 38
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. 10.0.0.0/8
B. 192.168.1.0/24
C. 100.70.0.0/17
D. 172.16.0.0/18
E. 33.17.0.0/16
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 39
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 (LEAVE A REPLY)
Explanation
https://cloakable.irdeto.com/2017/10/11/how-to-implement-vpc-peering-between-2-vpcs-in-the-same-aws-accou

NEW QUESTION: 40
Which of the following types of contents cannot serve over HTTP or HTTPS in Amazon CloudFront?
A. Apple HTTP Live Streaming
B. Static and dynamic download content
C. Adobe Flash multimedia content
D. CloudFront RTMP distribution
Answer: C (LEAVE A REPLY)
In Amazon CloudFront, you can use web distributions to serve the following content over HTTP or HTTPS:
Static and dynamic download content, for example, .html, .css, .php, and image files, using HTTP or HTTPS.

Multimedia content on demand using progressive download and Apple HTTP Live Streaming (HLS). A live event, such as a meeting, conference, or concert, in real time. You can't serve Adobe Flash multimedia content over HTTP or HTTPS.
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-overview.html

NEW QUESTION: 41
Over which of the following Ethernet standards does AWS Direct Connect link your internal network to an AWS Direct Connect location?
A. Copper backplane cable
B. Twisted pair cable
C. Single mode fiber-optic cable
D. Shielded balanced copper cable
Answer: C (LEAVE A REPLY)
AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet single mode fiber-optic cable.
Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

NEW QUESTION: 42
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 both the web and application tiers, setting session stickiness at the target group level for both tiers.
B. Deploy a web node and an application node as separate containers on the same host, using task linking to create a relationship between the pair. Add an Application Load Balancer with session stickiness in front of all web node containers.
C. 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.
D. Use an Application Load Balancer at the web tier and a Classic Load Balancer at the application tier.
Set session stickiness on both, but update the application code to create an application-controlled cookie on the Classic Load Balancer.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
A Lambda function needs to access the private address of an Amazon ElastiCache cluster in a VPC. The Lambda function also needs to write messages to Amazon SQS. The Lambda function has been configured to run in a subnet in the VPC.
Which of the following actions meet the requirements? (Select two.)
A. The Lambda function needs an IAM role to access Amazon SQS
B. The Lambda function must route through a NAT gateway or NAT instance in another subnet to access the public SQS API.
C. The Lambda function must be assigned a public IP address to access the public Amazon SQS API.
D. The ElastiCache server outbound security group rules must be configured to permit the Lambda function's security group.
E. The Lambda function must consume auto-assigned public IP addresses but not elastic IP addresses.
Answer: A,C (LEAVE A REPLY)
Explanation
References: https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/

NEW QUESTION: 44
Your organization requires strict adherence to a change control process for its Amazon Elastic Compute Cloud (EC2) and VPC environments. The organization uses AWS CloudFormation as the AWS service to control and implement changes. Which combination of three services provides an alert for changes made outside of AWS CloudFormation? (Select three.)
A. AWS Identify and Access Management
B. AWS CloudWatch metrics
C. AWS Simple Notification Service
D. AWS CloudFormation
E. AWS Lambda
F. AWS Config
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Your company has two DX locations. You need to configure one link as passive. What should you configure in your router to set that link as the passive link.
Choose the correct answer:
A. Set a higher MED.
B. Configure AS_PATH Prepending on the link.
C. Advertise a network with a higher CIDR.

D. Call your service provider and have the ASN changed for that link.

Answer: B (LEAVE A REPLY)

You should configure AS_PATH prepending on the link. A higher CIDR is the same as a more specific prefix, which will make the link more preferred. A higher MED will make the path less preferred, but this is not the preferred method to accomplish this. Changing your ASN will not help. Configuring AS_PATH Prepending is the preferred method of AWS to configure an Active-Passive configuration with Direct Connect.

NEW QUESTION: 46

Which of the following does not configure Amazon CloudFront cache behaviors to forward cookies to an origin for web distributions?

A. Origin server

B. AWS CLI

C. Amazon EMR

D. Amazon S3

Answer: D (LEAVE A REPLY)

Amazon S3 and some HTTP servers do not process cookies. Do not configure Amazon CloudFront cache behaviors to forward cookies to an origin that doesn't process cookies or you'll adversely affect cache ability and consequently performance.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

NEW QUESTION: 47

Which statement about VPC endpoints is incorrect?

Choose the correct answer:

A. Endpoints are transitive for Direct Connect connections.

B. Endpoints cannot be extended out of a VPC.

C. Endpoints cannot be tagged.

D. An S3 endpoint allows Amazon AMIs to install some software.

Answer: A (LEAVE A REPLY)

Endpoints are not transitive for Direct Connect connections or any other connections. To access S3 resources through an endpoint from outside of a VPC, an EC2 proxy must be used.

NEW QUESTION: 48
Under increased cybersecurity concerns, a company is deploying a near real-time intrusion detection system (IDS) solution. A system must be put in place as soon as possible. The architecture consists of many AWS accounts, and all results must be delivered to a central location.
Which solution will meet this requirement, while minimizing downtime and costs?
A. Enable Amazon GuardDuty on each account as members of a central account.
B. Enable Amazon Macie on each AWS account and configure central reporting.
C. Enable VPV Flow Logs on each VPC. Set up a stream of the flow logs to a central Amazon Elasticsearch cluster.
D. Deploy a third-party vendor solution to perform deep packet inspection in a transit VPC.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
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. The EC2 instances are not configured to use the proxy running in the data center for traffic on TCP port
80.
B. Inbound security groups are configured incorrectly on the EC2 instances running in the VPC.
C. The VPC route table does not have entries for the proxy server in the data center
D. The data center firewall is blocking all traffic sent from the VPC CIDR range destined for 0.0.0.0/0.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
A Network Engineer needs to be automatically notified when a certain TCP port is accessed on a fleet of Amazon EC2 instances running in an Amazon VPC.
Which of the following is the MOST reliable solution?
A. Create VPC Flow Logs that write to Amazon CloudWatch Logs, with a metric filter matching connections on the required port. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

B. Create an inbound rule in the VPC's network ACL that matches the TCP port. Create an Amazon CloudWatch alarm on the NetworkPackets metric for the ACL that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
C. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to notify the Administrator with Amazon SNS each time the TCP port is accessed.
D. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to publish to a custom Amazon CloudWatch metric each time the TCP port is accessed. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
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: (SHOW ANSWER)
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html#vpc-endpoints-policies-s3

NEW QUESTION: 52
You have two Direct Connect connections and two VPN connections to your network. Site A is VPN 10.1.0.0/24 AS 65000 65000, Site B is VPN 10.1.0.252/30 AS 65000, Site C is DX 10.0.0.0/8 AS 65000 and Site D is DX 10.0.0.0/16 AS 65000 65000 65000. Which site will AWS choose to reach your network?
Choose the correct answer:
A. Site A: VPN 10.0.1.0/24 AS 65000 65000
B. Site B: VPN 10.0.1.252/30 AS 65000 65000 65000
C. Site C: DX 10.0.0.0/8 AS 65000
D. Site D: DX 10.0.0.0/16
Answer: (SHOW ANSWER)
Site B, the most specific prefix always wins.

NEW QUESTION: 53
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. There is a misconfiguration of the bi-directional forwarding detection.
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. The VGW is not advertising the correct CIDR range back on-premises.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 54
Which one of the following options is not true about WorkSpaces? Choose the correct answer:
A. WorkSpaces can query on-premises domains for authentication.
B. WorkSpaces allows integration with Microsoft AD.
C. WorkSpaces is a fully managed, secure desktop computing service.
D. WorkSpaces is great for running Linux applications.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
In Amazon CloudFront, if you need to quickly remove objects from a distribution, you can:
A. delete the objects from cache.
B. invalidate the objects.
C. remove your Amazon S3 bucket.
D. delete your distribution and recreate it.
Answer: (SHOW ANSWER)
In Amazon CloudFront, if you need to quickly remove objects from a distribution, you can invalidate them.
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AddRemoveReplaceObjects.html

NEW QUESTION: 56
You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems. Which two AWS Services cloud you leverage to build an automated notification system? (Select two.)
A. Internet gateway
B. VPC Flow Logs

C. AWS CloudTrail
D. Lambda
E. AWS Inspector
Answer: (SHOW ANSWER)
Explanation
References:
https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-byusing- aws-cloudtrail-amazon-sns-and-aws-lambda/

NEW QUESTION: 57
The Web Application Development team is worried about malicious activity from 200 random IP addresses.
Which action will ensure security and scalability from this type of threat?
A. Use inbound network ACL rules to block the IP addresses.
B. Write iptables rules on the instance to block the IP addresses.
C. Use inbound security group rules to block the IP addresses.
D. Use AWS WAF to block the IP addresses.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
The Payment Card Industry Data Security Standard (PCI DSS) merchants that handle credit card data must use strong cryptography. These merchants must also use security protocols to protect sensitive data during transmission over public networks.
You are migrating your PCI DSS application from on-premises SSL appliance and Apache to a VPC behind Amazon CloudFront.
How should you configure CloudFront to meet this requirement?
A. Configure the CloudFront Cache Behavior to require HTTPS and the CloudFront Origin's Protocol Policy to 'Match Viewer'.
B. Configure the CloudFront Cache Behavior to allow TCP connections and to forward all requests to the origin without TLS termination at the edge.
C. Configure the CloudFront Cache Behavior to require HTTPS and to forward requests to the origin via AWS Direct Connect.
D. Configure the CloudFront Cache Behavior to redirect HTTP requests to HTTPS and to forward request to the origin via the Amazon private network.
Answer: A (LEAVE A REPLY)
Explanation
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#D

NEW QUESTION: 59
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 ELB. www.acme.com with an ALIAS record targeting the ELB.
B. Configure acme.com with an A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
C. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
D. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.
Answer: A (LEAVE A REPLY)
Explanation
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

NEW QUESTION: 60
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. 172.16.0.0/18
B. 10.0.0.0/8
C. 100.70.0.0/17
D. 192.168.1.0/24
E. 33.17.0.0/16
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 61
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 filter on the company's router to only import routes with the 7224:8100 BGP community attribute.
B. Configure a prefix list on the customer router containing the AWS IP address ranges for the specific region.
C. 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.
D. Configure a filter on the company's router to only import routes without a BGP community attribute and a maximum path length of 3.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
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 AWS Direct Connect Data Out charges.
B. The company pays Internet Data Out charges.
C. The department pays Internet Data Out charges.
D. The department pays AWS Direct Connect Data Out charges.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
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: A,B (LEAVE A REPLY)
Explanation/Reference:
References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

NEW QUESTION: 64
An organization will be extending its existing on-premises infrastructure into the cloud. The design consists of a transit VPC that contains stateful firewalls that will be deployed in a highly available configuration across two Availability Zones for automatic failover.
What MUST be configured for this design to work? (Select two.)
A. A different Autonomous System Number (ASN) for each firewall.

B. Border Gateway Protocol (BGP) routing
C. Autonomous system (AS) path prepending
D. Static routing
E. Equal-cost multi-path routing (ECMP)
Answer: B,C (LEAVE A REPLY)
Explanation
https://docs.aws.amazon.com/solutions/latest/cisco-based-transit-vpc/appendix-a.html

NEW QUESTION: 65
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: (SHOW ANSWER)
Explanation
References: https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html

NEW QUESTION: 66
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. Update the NACL to only allow port 80 to the application servers from the ELB servers.
B. Update the Security Groups to only allow port 80 to the application servers from the ELB.
C. Mark the affected instance as degraded in the ELB and raise it with the client application team.
D. Terminate the affected instance and allow Auto Scaling to create a new instance.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67

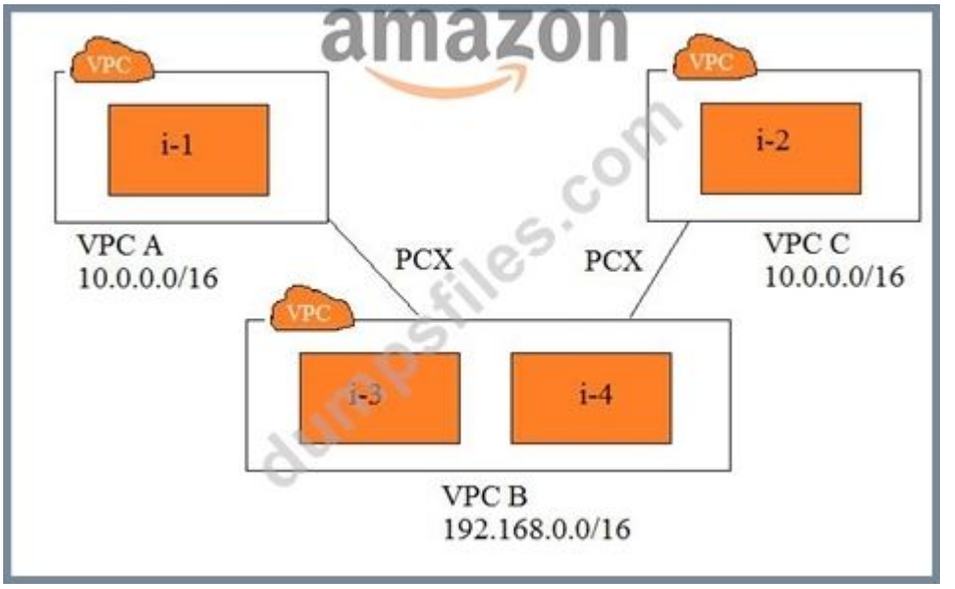
You deploy an Amazon EC2 instance that runs a web server into a subnet in a VPC. An Internet gateway is attached, and the main route table has a default route (0.0.0.0/0) configured with a target of the Internet gateway.
The instance has a security group configured to allow as follows:
* Protocol: TCP
* Port: 80 inbound, nothing outbound
The Network ACL for the subnet is configured to allow as follows:
* Protocol: TCP
* Port: 80 inbound, nothing outbound
When you try to browse to the web server, you receive no response.
Which additional step should you take to receive a successful response?
A. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 80
B. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 1024-65535
C. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 1024-65535
D. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 80
Answer: (SHOW ANSWER)

NEW QUESTION: 68
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 ENAs.
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: A,B (LEAVE A REPLY)
Explanation
References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

NEW QUESTION: 69
You are configuring a CloudFront distribution, and when you try to attach an SSL, you do not see your SSL listed. What is the most likely reason for this? Choose the correct answer:
A. You requested an SSL for the wrong region.
B. Sometimes, it won't show, and you need to retrieve the ARN for the SSL and enter it manually.
C. You must configure an https record in Route 53 first.
D. You didn't wait 48 hours after approving the SSL.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70

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: (SHOW ANSWER)
https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-partial-access.html#one-to-two-vpcs-simple-hub

NEW QUESTION: 71

Your organization requires strict adherence to a change control process for its Amazon Elastic Compute Cloud (EC2) and VPC environments. The organization uses AWS CloudFormation as the AWS service to control and implement changes. Which combination of three services provides an alert for changes made outside of AWS CloudFormation? (Select three.)

A. AWS Config

B. AWS Simple Notification Service

C. AWS CloudWatch metrics

D. AWS Lambda

E. AWS CloudFormation

F. AWS Identify and Access Management

Answer: A,B,D (LEAVE A REPLY)

Explanation

aws.amazon.com/about-aws/whats-new/2018/03/aws-config-notifications-are-now-integrated-with-amazon-clou

NEW QUESTION: 72

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 both VPCs, associate subnets, and define a target network. Add a rule to authorize client access to each target VPC. Update resource security groups in both VPCs to allow traffic from the security groups of each VPC for the subnet associations. 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.

B. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target network. Add a rule to authorize client access to the target VPC. and add a rule to authorize client access to the peered VPC. Update resource security groups in both VPCs to allow traffic from the security group for the subnet association. Instruct the users to sign in to the AWS Management Console and navigate to Client VPN to connect to the Client VPN endpoint.

C. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target network. Add a rule to authorize client access to the target VPC. and add a rule to authorize client access to the peered VPC. Update resource security groups in both VPCs to allow traffic from the security group for the subnet association. Securely send the users the configuration options, and instruct the users to install Client VPN on their laptops. Instruct the users to connect to the Client VPN endpoint to gain access to the resources.

D. Deploy a Network Load Balancer in front of the company resources. Set up security groups that contain the IP addresses of each of the user laptops. Instruct the users to connect to the application securely over TCP.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 73
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. Update the CORS configuration for Amazon S3 to allow traffic from the proxy.
D. Configure a VPC endpoint for Amazon S3 in the same subnet as the instance.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
Your VPC has a DX connection that is advertising 99 routes. You have two more prefixes to add: 10.223.1.0/24 and 10.223.2.0/24. You have several locations, so you need to be as exact as possible with your routing. How would you do this? Choose the correct answer:
A. Add the prefixes; AWS allows for as many BGP routes as you need but not static.
B. Contact AWS to extend the number of prefixes you are allowed to advertise. .
C. Summarize the routes into a 10.223.0.0/22 and advertise that route instead.
D. Summarize the routes into a 10.223.0.0/12 and advertise that route instead.
Answer: C (LEAVE A REPLY)
BGP has a strict 100 prefix limit. 10.223.0.0/12 includes both routes but is not very specific. 10.223.0.0/22 is the proper summarization of both routes.

NEW QUESTION: 75
A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven't yet upgraded.
What design will allow the company to serve both newer and earlier clients in the MOST efficient way?
A. Use an Application Load Balancer for the new application. Register both the new and earlier application backends as separate target groups. Use header-based routing to route traffic based on the application version.

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

NEW QUESTION: 76
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 block malicious IPs in AWS WAF attached to the Application Load Balancer.
B. Update the AWS Lambda function to add an additional network ACL to the subnets once the limit for the previous ones has been reached.
C. Update the AWS Lambda function to block malicious IPs in security groups rather than the network ACL.
D. Update the AWS Lambda function to remove blocked entries from the network ACL after 2 hours.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
A company has a hybrid IT architecture with two AWS Direct Connect connections to provide high availability. The services hosted on-premises are accessible using public IPs, and are also on the

172.16.0.0/16 range. The AWS resources are on the 192.168.0.0/18 range. The company wants to use Amazon Elastic Load Balancing for SSL offloading, health checks, and sticky sessions. What should be done to meet these requirements?
A. Create a Network Load Balancer pointing to the on-premises server's public IP address.
B. Create an Application Load Balancer pointing to the on-premises server's private IP address.
C. Create an Amazon CloudFront distribution for the on-premises service and use the public IPs of the on-premises servers as the origin.
D. Create a Network Load Balancer pointing to the on-premises server's private IP address.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
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 (LEAVE A REPLY)
Explanation
aws.amazon.com/premiumsupport/knowledge-center/internal-version-website/

NEW QUESTION: 79
What are two reasons that could cause an HTTP health check to fail? Choose the 2 correct answers:
A. Security group blocking port 80 to the instance
B. HTTP server not running
C. No Internet Gateway
D. NACL blocking port 443 to the instance
Answer: (SHOW ANSWER)
A load balancer does not perform health checks through the internet gateway, so it is not necessary and 443 is HTTPS not HTTP

NEW QUESTION: 80

Your organization runs a popular e-commerce application deployed on AWS that uses autoscaling in conjunction with an Elastic Load balancing (ELB) service with an HTTPS listener. Your security team reports that an exploitable vulnerability has been discovered in the encryption protocol and cipher that your site uses.
Which step should you take to fix this problem?
A. Generate new SSL certificates for all web servers and replace current certificates.
B. Generate new SSL certificates and use ELB to front-end the encrypted traffic for all web servers.
C. Change the security policy on the ELB to disable vulnerable protocols and ciphers.
D. Leverage your current configuration management system to update SSL policy on all web servers.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
You need to find the subnet, the security group and the VPC that your instance is associated with. You only have access to the terminal of an instance with an admin role attached. What is the first part of the command you would use?
Choose the correct answer:
A. aws ec2 describe-network-acl
B. aws ec2 describe-instances
C. aws vpc describe-all
D. aws ec2 describe-security-groups
Answer: (SHOW ANSWER)
aws ec2 describe-instances will tell a significant amount of information about the instances in your account. Apply a filter to be able to see information about your instance. Describe-security-groups and describe-network-acl would not allow you to see which group is associated with your instance and aws vpc describe-all doesn't exist.

NEW QUESTION: 82
Which other AWS service is used to track `Related Events' within the Configuration Item?
A. AWS WAF
B. SQS
C. AWS CloudTrail
D. S3
Answer: C (LEAVE A REPLY)
`Related Events' displays the AWS CloudTrail event ID that is related to the change that triggered the creation of the CI. There is a new CI made for every change made against a resource. As a result a different CloudTrail event IDs will be created. This allows you you to deep-dive into who or what and when made the change that triggered this CI. A great feature allowing for some great analysis to be taken, specifically when this affects security resources.
Reference:

http://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html#config-item-table

NEW QUESTION: 83
To connect to public AWS products such as Amazon EC2 and Amazon S3 through the AWS Direct Link, which step is NOT required?
A. Provide public IP address (/31) for each Border Gateway Protocol (BGP) session.
B. Allocate a Private IP address to your network in 172.x.x.x range.
C. Provide the public routes that you will advertise over Border Gateway Protocol (BGP).
D. Provide a public Autonomous System Number (ASN) that you own or a private one to identify your network on the Internet.
Answer: B (LEAVE A REPLY)
To connect to public AWS products such as Amazon EC2 and Amazon S3 through the AWS Direct Connect, you need to provide the following:
A public Autonomous System Number (ASN) that you own (preferred) or a private ASN. Public IP addresses (/30) (that is, one for each end of the BGP session) for each BGP session. The public routes that you will advertise over BGP.
Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

NEW QUESTION: 84
The Web Application Development team is worried about malicious activity from 200 random IP addresses.
Which action will ensure security and scalability from this type of threat?
A. Use inbound security group rules to block the IP addresses.
B. Use inbound network ACL rules to block the IP addresses.
C. Use AWS WAF to block the IP addresses.
D. Write iptables rules on the instance to block the IP addresses.
Answer: (SHOW ANSWER)
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html

NEW QUESTION: 85
You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems.
Which two AWS Services cloud you leverage to build an automated notification system? (Select two.)
A. Internet gateway
B. VPC Flow Logs
C. AWS CloudTrail
D. Lambda

E. AWS Inspector

Answer: C,D (LEAVE A REPLY)

Explanation

References:

https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-by-using-aws-cloudt

NEW QUESTION: 86

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 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.

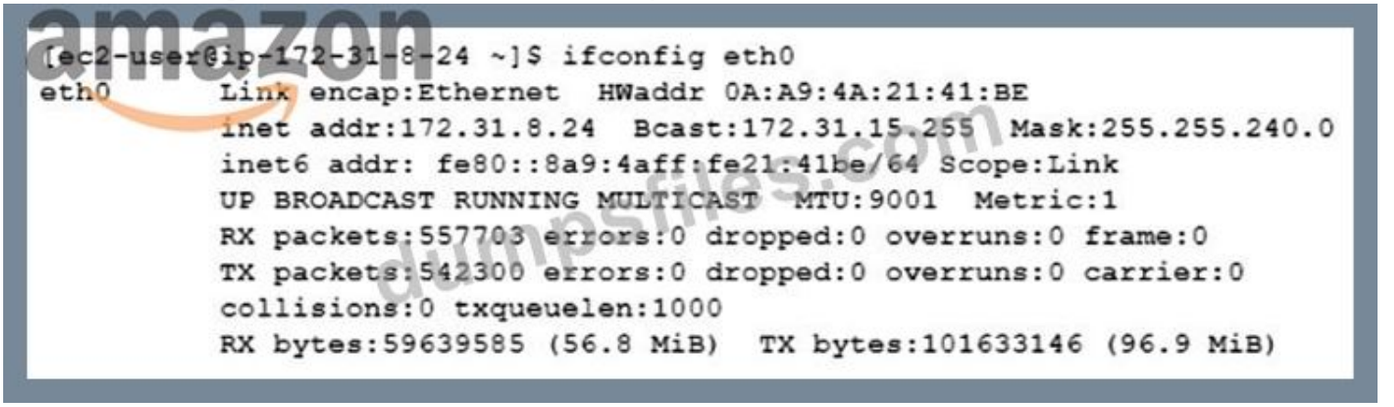
C. Set the Elastic Load Balancing (ELB) load balancer in front of the hosts of the service, and register the ELB name of the main service host as an ALIAS record with a latency-based routing policy in Route 53.

D. 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.

Answer: (SHOW ANSWER)

NEW QUESTION: 87

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:



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

NEW QUESTION: 88
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: A,E (LEAVE A REPLY)
References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

NEW QUESTION: 89
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 ENAs.
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: (SHOW ANSWER)
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

NEW QUESTION: 90
A Network Engineer is designing a new system on AWS that will take advantage of Amazon CloudFront for both content caching and for protecting the underlying origin. There is concern that an external agency might be able to access the IP addresses for the application's origin and then

attack the origin despite it being served by CloudFront. Which of the following solutions provides the strongest level of protection to the origin?
A. Configure CloudFront to use a custom header and configure an AWS WAF rule on the origin's Application Load Balancer to accept only traffic that contains that header.
B. Configure an AWS Lambda@Edge function to validate that the traffic to the Application Load Balancer originates from CloudFront.
C. Use an IP whitelist rule in AWS WAF within CloudFront to ensure that only known-client IPs are able to access the application.
D. Attach an origin access identity to the CloudFront origin that allows traffic to the origin that originates from only CloudFront.
Answer: C (LEAVE A REPLY)

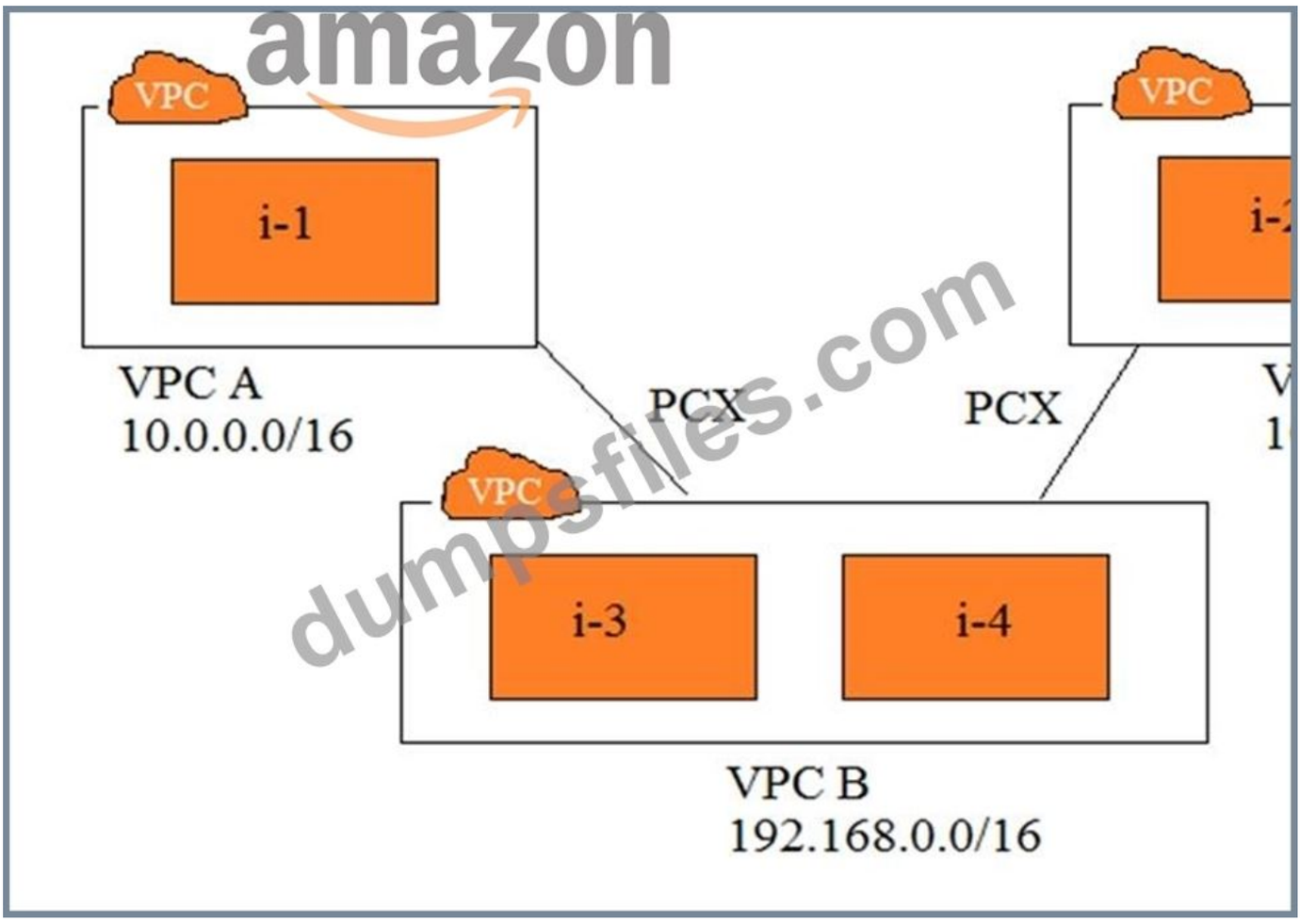
NEW QUESTION: 91
A logistics company has deployed a hybrid environment that has multiple VPCs in both the us-east-1 Region and the af-south-1 Region The on-premises data center is connected to us-east-1 through an AWS Direct Connect connection The Direct Connect connection is connected to a Direct Connect gateway that is associated with a transit gateway The transit gateway is attached to all the VPCs in us-east-1 An application that is deployed in af-south-1 requires access to a database in the data center The application also requires access to file storage in a VPC in us-east-1 Which solution will meet these requirements with the LOWEST latency?
A. Create a Direct Connect connection in af-south-1, and attach the VPCs with a Direct Connect gateway and a transit gateway Create an AWS Site-to-Site VPN connection over the internet between the Direct Connect connections.
B. Create a transit gateway in af-south-1 and attach the VPCs Associate the transit gateway in af-south-1 with the Direct Connect gateway tn us-east-1
C. Create inter-Region VPC peering connections between the VPCs in each Region Use the transit gateway attachments in us-east-1 to access the database in the data center
D. Create a transit gateway in af-south-1, and attach the VPCs Create a transit gateway peering connection between the transit gateways
Answer: (SHOW ANSWER)

NEW QUESTION: 92

You have deployed a website that utilizes CloudFront, Elastic Loadbalancer, and S3 to serve content. When users access your site, they receive a "mixed content" security warning. What is most likely the problem?
Choose the correct answer:
A. There is no rule in your bucket policy allowing public access.
B. You have applied your SSL to your Elastic Loadbalancer but not your CDN.
C. Your S3 Bucket permissions are incorrect.
D. You are using an SSL from an external CA.
Answer: B (LEAVE A REPLY)
You must apply the SSL to your Elastic Loadblanacer and your CDN to encrypt all aspects of your site.

NEW QUESTION: 93
A company has an application running on Amazon EC2 instances in a VPC The application must publish custom metrics to Amazon CloudWatch in the same AWS Region The metrics include proprietary information All connectivity must be over private IP addresses.
Which solution will meet these requirements'?
A. Connect to CloudWatch through an interface endpoint
B. Connect to CloudWatch through a NAT gateway
C. Connect to CloudWatch through a gateway endpoint
D. Connect to CloudWatch through an internet gateway
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
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. Change the IP address of i-2 to 10.0.0.100. Assign it an elastic IP address.

C. Create subnets 192.168.1.0/27 and 192.168.1.16/27. Move i-3 and i-4 to these subnets, respectively.

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: (SHOW ANSWER)

NEW QUESTION: 95
Your company currently has a LAG to AWS with two 1Gbps connections. What is the best way to increase throughput on this LAG?
Choose the correct answer:
A. Add three 1Gbps connections to the LAG.
B. Add one 10Gbps connections to the LAG.
C. Configure your router to use "jumbo frames" with an MTU of 9001.
D. Add two 1Gbps connections to the LAG.
Answer: D (LEAVE A REPLY)
Add two 1Gbps connections to the LAG. DX does not support jumbo frames, a LAG only supports 4 connections, and adding a 10Gbps connection will be limited to the lowest speed of 1Gbps.

NEW QUESTION: 96
In AWS Direct Connect, which of the following is true of configuring your router to connect to the AWS Direct Connect router?
A. After creating a virtual interface for your AWS Direct Connect connection, you can download the router configuration file from the available link
B. After Completing the Cross Connect step, the download link for router configuration will be available
C. After submitting your AWS Direct Connect connection request, you will receive the router configuration details by email within 72 hours
D. In Create a Virtual Interface step, the general configuration of your router would be available for downloading.
Answer: (SHOW ANSWER)
To use the AWS Direct Connect, after you have created a virtual interface for your AWS Direct Connect connection, you can download the router configuration file. This configuration helps your router connect to AWS Direct Connect router. This configuration is related to your created virtual interface details and vendor, platform, and software of your router.
Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#routerconfig

NEW QUESTION: 97
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 A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
B. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.
C. Configure acme.com with an ALIAS record targeting the ELB. www.acme.com with an ALIAS record targeting the ELB.
D. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
A company has a hybrid environment across its on-premises network and the AWS Cloud The company wants to use Amazon Elastic File System (Amazon EFS) to store and share data between on-premises services that are required to resolve DNS queries through on-premises DNS servers The company wants to use a custom domain name to connect to Amazon EFS The company also wants to avoid using the Amazon EFS target IP address.
What should a network engineer do to meet these requirements?
A. Create an Amazon Route 53 Resolver outbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone, and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 Resolver
B. Create an Amazon Route 53 Resolver inbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone, and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 Resolver
C. Create an Amazon Route 53 Resolver outbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 public hosted zone, and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 public hosted zone
D. Create an Amazon Route 53 Resolver inbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone, and add a new PTR record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 private hosted zone
Answer: C (LEAVE A REPLY)

NEW QUESTION: 99
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 OpsWorks 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 CloudFormation to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.
C. Create the VPCs using AWS CLI and use the dry-run flag to validate if the current CIDR range is in use.
D. Use the VPC wizard in the AWS Management Console. Type in the CIDR blocks for the VPC and subnets.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 100
A company installed an AWS Site-to-Site VPN and configured it to use two tunnels The company has learned that the VPN connectivity is unstable During a ping test from the on-premises data center to AWS: a network engineer notices that the first few ICMP replies time out but that subsequent requests are successful The AWS Management Console shows that the status for both tunnels last changed at the same time the ping responses were successfully received Which steps should the network engineer take to resolve the instability*? (Select TWO)
A. Send ICMP requests to an instance in the VPC every 5 seconds from the on-premises network
B. Change the tunnel configuration to active/standby on the virtual private gateway
C. Use AS PATH prepending on one path to cause all traffic to prefer that tunnel
D. Enable dead peer detection (DPD) on the customer gateway device
E. Use a higher multi-exit discriminator (MED) value on the preferred path to prefer that tunnel
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 101
Due to security requirements, all traffic must be encrypted between your VPC and your on-premises data center. You also want to maintain reliability.
What two options will allow you to achieve this?
Choose the 2 correct answers:
A. A Direct Connect connection with a Private VIF
B. A VPN connection
C. A Direct Connect connection with a Hosted VIF
D. A Direct Connect connection with a Public VIF
Answer: B,D (LEAVE A REPLY)
To run VPN over DX, you need to have a public VIF to access the VPN endpoints.

NEW QUESTION: 102

Your application is hosted behind an Elastic Load Balancer (ELB) within an autoscaling group. The autoscaling group is configured with a minimum of 2, a maximum of 14, and a desired value of 2. The autoscaling cooldown and the termination policies are set to the default value. CloudWatch reports that the site typically requires just two servers, but spikes at the start and end of the business day can require eight to ten servers. You receive intermittent reports of timeouts and partially loaded web pages.
Which configuration change should you make to address this issue?
A. Configure connection draining on the ELB.
B. Configure the autoscaling cooldown to 600 seconds.
C. Configure the termination policy to oldest instance.
D. Configure a Terminating: Wait lifecycle hook on a scale in event.
Answer: (SHOW ANSWER)
References: https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html

NEW QUESTION: 103
Convert the following IPv4 address in presented in binary form, into dotted decimal form
10101100.01111011.00001101.10011101
A. 172.123.13.157
B. 173.13.13.157
C. 172.122.13.15
D. 172.124.13.57
Answer: A (LEAVE A REPLY)
An IPv4 address in dotted decimal format is constructed using binary arithmetic. In binary arithmetic, each bit within a group represents a power of two. Specifically, the first bit in a group represents 2 to the power of 0, the second bit represents 2 to the power of 1, the third bit represents 2 to the power of 2, and so on. Binary format is simple because each successive bit in a group is exactly twice the value of the previous bit.
The first octet is 128+32+8+4=172
The second octet 64+32+16+8+2+1=123
The third octet 8+4+1= 13
The fourth octet is 128+16+8+4+1= 157
Reference: https://en.wikipedia.org/wiki/IPv4

NEW QUESTION: 104
A company wants to use thin clients running virtual desktops to replace 500 desktop computers used by its call center employees The company is evaluating Amazon Workspaces as a solution
A network engineer who is testing with a thin client is unable to conned to Amazon Workspaces
After entering credentials the network engineer receives the following error:
"An error occurred while launching your Workspace Please try again"
What should the network engineer do to resolve this issue?

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

NEW QUESTION: 105
You are auditing an AWS infrastructure after you noticed some abnormal charges on the bill. You use AWS Config to monitor your changes. What else is required to find out who made the change? Choose the correct answer:
A. There is no information to find this. You will need to sign up for Config Premium.
B. Use the eventID of the change and reference it with your Flow Logs.
C. Use the eventId of the change and reference it with CloudTrail to find the culprit.
D. Use the eventID of the change and reference it with CloudWatch to find the culprit.
Answer: C (LEAVE A REPLY)
CloudTrail is for finding "who" performed an action.

NEW QUESTION: 106
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 CORS configuration for Amazon S3 to allow traffic from the proxy.
B. Configure a VPC endpoint for Amazon S3 in the same subnet as the instance.
C. Update the S3 bucket policy with the private IP address of the instance.
D. Exclude 169.254.169.0/24 from the instance's proxy configuration.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 107
Which AWS service is used within an AWS Config Rule to perform the logic evaluation of that rule?
A. Inspector
B. WAF
C. Lambda
D. SWF
Answer: C (LEAVE A REPLY)
AWS Config Rules are a great way to help you enforce specific compliance controls and checks across your resources and allows for you to adopt an `ideal' deployment specification for each of your resource types. Each Rule is simply a Lambda function that when called upon evaluates the resource and carries out some simply logic to determine the compliance result with the rule.
Reference:
http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_nodejs-sample.html

NEW QUESTION: 108
Which statement about placement groups is incorrect? Choose the correct answer:
A. A placement group is a logical grouping of instances in a single AZ.
B. If you stop an instance and restart it, it will always return to the same placement group.
C. To help ensure capacity in a placement group, deploy all instances at once.
D. There is no charge for creating a placement group.
Answer: B (LEAVE A REPLY)
There may not be sufficient capacity in the placement group.

NEW QUESTION: 109
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 (LEAVE A REPLY)
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html

NEW QUESTION: 110
An organization will be expanding its current network design. When fully built out, there will be 99 VPCs spread across 11 AWS accounts (9 VPCs per account). There is currently an AWS Direct Connect connection into one account with 9 VPCs, each with a virtual network interface (VIF) per VPC.
Which of the following designs will minimize cost while allowing the organization to expand?
A. Order 10 new Direct Connect connections, one from each of the accounts that will be provisioned.
Create private VIFs in each account. Attach one private VIF per VPC.
B. Create a transit VPC in the existing account that consists of two routers in separate Availability Zones.
Connect each VPC to the two routers in the transit VPC by using VPN.
C. Create hosted private VIFs in the existing account. Connect a private VIF to an AWS Direct Connect gateway in each account. Connect the gateway in each account to the VPCs.
D. Create a public VIF on the Direct Connect connection. Leverage the public VIF to create a VPN connection to each VPC.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 111
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 ELB. www.acme.com with an ALIAS record targeting the ELB.
B. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
C. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.
D. Configure acme.com with an A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
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. 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.
B. 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.
C. Enable Bidirectional Forwarding Detection (BFD) echo mode on the company's router and disable sending the Internet Control Message Protocol (ICMP) IP packet requests.
D. Configure BGP on the company's router with a keep-alive to 300 ms and the BGP hold timer to 900 ms.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
You are configuring a virtual interface for access to your VPC on a newly provisioned 1-Gbps AWS Direct Connect connection. Which two configuration values do you need to provide? (Select two.)
A. Public AS number
B. VLAN ID
C. IP prefixes to advertise
D. Direct Connect location
E. Virtual private gateway
Answer: (SHOW ANSWER)
Explanation
References: https://aws.amazon.com/directconnect/faqs/

NEW QUESTION: 114
A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2 instances now use a NAT gateway tor internet access After the migration, some long-running database queries from private EC2 instances to a publicly accessible third-party database no longer receive responses The database query logs reveal that the queries successfully completed after 7 minutes but that the client EC2 instances never received the response.
Which configuration change should a network engineer implement to resolve this issue"
A. Configure the NAT gateway timeout to allow connections for up to 600 seconds
B. Close idle TCP connections though the NAT gateway
C. Enable enhanced networking on the client EC2 instances
D. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds

Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
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 CloudTrail to log information to Amazon CloudWatch Logs Insights about the queries that Route 53 receives
B. Use AWS WAF to log information to Amazon CloudWatch Logs about the queries that Route 53 receives
C. Use VPC Flow Logs to log information to Amazon CloudWatch Logs Insights about the queries that Route 53 receives
D. Use Route 53 query logging to log information to Amazon CloudWatch Logs about the queries that Route 53 receives
Answer: B (LEAVE A REPLY)

NEW QUESTION: 116
Which service would you use to see who changed your infrastructure? Choose the correct answer:
A. CloudTrail
B. Config
C. Flow Logs
Answer: (SHOW ANSWER)

NEW QUESTION: 117
A company runs a large-scale application on a feel of Amazon EC2 instances that ate distributed across several VPCs A Network Load Balancer (NLB) in a separate VPC routes traffic to the EC2 instances The NLB's VPC is peered to all the application VPCs The application must process millions of requests each minute during times of peak utilization Users are reporting that the connections to the application are failing during peak times Monitoring shows an increase in port allocation errors on the NLB.
Which action will solve this issue with the LEAST change to the architecture?
A. Add a new target group to the same NLB listener
B. Increase the number of EC2 instances in the target group
C. Create an Application Load Balancer for the target group
D. Change the target group type to 'instance"
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118

You have a website hosted on EC2 that is not serving web pages. You have ensured that the server is running and the site is configured properly. What could be the problem? Choose the correct answer:

A. Your NACL does not allow port 80 outbound.

B. Your NACL does not allow ports 1024 ?65535 outbound.

C. Your NACL does not allow ports 1024 ?65535 inbound.

D. Your security group does not allow outbound traffic.

Answer: B (LEAVE A REPLY)

The ephemeral ports 1024 ?65535 are required outbound for return traffic. For the server to access websites, those same ports need to be allowed inbound.

NEW QUESTION: 119

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

A. Create a proxy resolver within the VPC. Point the on-premises forwarder to the proxy resolver.

B. Modify the network access control list on the VPC to allow DNS queries from on-premises systems.

C. Configure the on-premises server as a secondary DNS for the private zone. Update the NS records.

D. Update the on-premises forwarders with the four name servers assigned to the private hosted zone.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 120

A company has recently established an AWS Direct Connect connection from its on-premises data center to AWS. A Network Engineer has blocked all traffic destined for Amazon S3 over the company's gateway to the internet from its on-premises firewall. S3 traffic should only traverse the Direct Connect connection.

Currently, no one in the on-premises data center can access Amazon S3.

Which solution will resolve this connectivity issue?

A. Configure a private virtual interface on the Direct Connect connection. Update the on-premises routing tables to choose Direct Connect as the preferred next hop for traffic destined for Amazon S3.

B. Configure a public virtual interface on the Direct Connect connection. Update the on-premises routing tables to choose Direct Connect as the preferred next hop for traffic destined for Amazon S3.
C. Establish an S3 VPC endpoint for the company's Amazon VPC. Configure a private virtual interface on the Direct Connect connection. Update the on-premises routing tables to choose Direct Connect as the preferred next hop
D. Configure a public virtual interface on the Direct Connect connection. Establish an AWS managed VPN over the connection. Update the on-premises routing tables to choose the VPN connection as the preferred next hop.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
You need to set up a VPN between AWS VPC and your on-premises network. You create a VPN connection in the AWS Management Console, download the configuration file, and install it on your on-premises router. The tunnel is not coming up because of firewall restrictions on your router. Which two network traffic options should you allow through the firewall? (Select two.)
A. UDP port 500
B. IP protocol 50
C. IP protocol 5
D. TCP port 50
E. TCP port 500
Answer: A,B (LEAVE A REPLY)
Explanation/Reference:
References: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html

NEW QUESTION: 122
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. 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.
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. 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.
D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
A network engineer is deploying an application on an Amazon EC2 instance. The instance is reachable within the VPC through its private IP address and from the internet using an elastic IP address. Clients are connecting to the instance over the Internet and within the VPC, and the application needs to be identified by a single custom Fully Qualified Domain Name that is publicly resolvable -'app.example.com'.
Instances within the VPC should always connect to the private IP to minimize data transfer costs.
How should the engineer configure DNS to support these requirements?
A. Create a CNAME for 'app' in the DNS zone 'example.com' to the public DNS name for the Amazon EC2 instance.
B. Use Amazon Route 53 to create a geo-based routing entry for the hostname 'app' in the DNS zone 'example.com'.
C. Create two A record entries for 'app' in the DNS zone 'example.com' - one for the public IP and one for the private IP.
D. Use Route 53 to create an ALIAS record to the public DNS name for the instance.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
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 (LEAVE A REPLY)
100 prefix is the limit on BGP over direct connect.

https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

NEW QUESTION: 125
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: /28 per subnetWeb: /27 per subnet
B. Network Load Balancer: /29 per subnetWeb: /26 per subnet
C. Network Load Balancer: /28 per subnetWeb: /25 per subnet
D. Network Load Balancer: /28 per subnetWeb: /26 per subnet
Answer: (SHOW ANSWER)

NEW QUESTION: 126
You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a self- referencing rule using the cluster security group's group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions.
How should you enable secure cluster communication while deploying additional cluster members in another AWS region?
A. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other's security group-id in each region.
B. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
C. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
D. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other's security group-id in each region.
Answer: B (LEAVE A REPLY)
https://aws.amazon.com/blogs/database/how-to-configure-a-private-network-environment-for-amazon-dynamodb-using-vpc-endpoints/ So, it's possible to create a more secure environment using private routing, and CDIR based security group references can be created:

https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html

NEW QUESTION: 127
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. Application Load Balancer using HTTPS listeners and targets
B. AWS Key Management Services
C. Customer-managed MySQL with Transparent Data Encryption
D. Amazon CloudFront using AWS Lambda@Edge
E. Amazon Aurora in a private subnet
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 128
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 network ACL associated with the subnet to permit outbound traffic
B. Update the network ACL associated with the subnet to permit inbound traffic
C. Update the security group associated with eni-0596e500l23456789 to permit inbound traffic
D. Update the security group associated with eni-0596e500i234 56~89 to permit outbound traffic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
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: /28 per subnetWeb: /25 per subnet
B. Network Load Balancer: /28 per subnetWeb: /26 per subnet
C. Network Load Balancer: /29 per subnetWeb: /26 per subnet

D. Network Load Balancer: /28 per subnetWeb: /27 per subnet
Answer: B (LEAVE A REPLY)

NEW QUESTION: 130
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 (LEAVE A REPLY)
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html#vpc-endpoints-policies-s3

NEW QUESTION: 131
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: B (LEAVE A REPLY)
Explanation
https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html

NEW QUESTION: 132

To get started using AWS Direct Connect, in which of the following steps do you configure Border Gateway Protocol (BGP)?

A. Complete the Cross Connect

B. Verify your Virtual Interface

C. Create a Virtual Interface

D. Submit AWS Direct Connect Connection Request

Answer: C (LEAVE A REPLY)

In AWS Direct Connect, your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication, and you need to provide a private Autonomous System Number (ASN) for that to connect to Amazon Virtual Private Cloud (VPC). To connect to public AWS products such as Amazon EC2 and Amazon S3, you will also need to provide a public ASN that you own (preferred) or a private ASN. You have to configure BGP in the Create a Virtual Interface step.

Reference:

http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#createvirtualinterface

NEW QUESTION: 133

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

A. Enable the private DNS name for the SQS endpoint. Create an Amazon Route 53 private hosted zone for the domain us-east-1 .sqs.amazonaws.com. Create an alias record to the DNS name of the SQS endpoint. Share the private hosted zone with all other VPCs.

B. Disable the private DNS name for the SOS endpoint. Create an Amazon Route 53 private hosted zone for the domain sqs.us-east-1 .amazonaws.com. Create an alias record to the DNS name of the SOS endpoint. Share the private hosted zone with all other VPCs

C. Disable the private DNS name for the SQS endpoint. Create an Amazon Route 53 private hosted zone for the domain us-east-1.sqs.amazonaws.com. Create a CNAME record to the DNS name of the SQS endpoint Share the private hosted zone with ail other VPCs

D. Enable the private DNS name for the SOS endpoint Create an Amazon Route 53 private hosted zone for the domain SQS.us-east-t.amazonaws.com. Create a CNAME record to the DNS name of the SQS endpoint. Share the private hosted zone with all other VPCs.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 134

You have just peered two VPCs, and you need to improve performance for instances you plan on deploying. What are two steps you would take to do this? Choose the 2 correct answers:

A. Create two subnets in the same AZ and create a placement group.

B. Set the MTU of your instances to 1500.

C. Create two subnets in different AZs and create a placement group.

D. Ensure you choose instances that use enhanced networking.

Answer: (SHOW ANSWER)
A placement group can only be deployed in the same AZ and is only useful with enhanced networking instances.

NEW QUESTION: 135
An AWS CloudFormation template is being used to create a VPC peering connection between two existing operational VPCs, each belonging to a different AWS account. All necessary components in the 'Remote' (receiving) account are already in place.
The template below creates the VPC peering connection in the Originating account. It contains these components:
AWSTemplateFormation Version: 2010-09-09
Parameters:
Originating VCId:
Type: String
RemoteVPCId:
Type: String
RemoteVPCAccountId:
Type: String
Resources:
newVPCPeeringConnection:
Type: 'AWS::EC2::VPCPeeringConnection'
Properties:
VpcdId: !Ref OriginatingVPCId
PeerVpcId: !Ref RemoteVPCId
PeerOwnerId: !Ref RemoteVPCAccountId
Which additional AWS CloudFormation components are necessary in the Originating account to create an operational cross-account VPC peering connection with AWS CloudFormation? (Select two.)
A. Resources:NewEC2SecurityGroup:Type: AWS::EC2::SecurityGroup
B. Resources:NetworkInterfaceToRemoteVPC:Type: "AWS::EC2NetworkInterface"
C. Resources:newEC2Route:Type: AWS::EC2::Route
D. Resources:VPCGatewayToRemoteVPC:Type: "AWS::EC2::VPCGatewayAttachment"
E. Resources:newVPCPeeringConnection:Type:
'AWS::EC2VPCPeeringConnection'PeerRoleArn: !Ref PeerRoleArn
Answer: (SHOW ANSWER)
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_EC2.html

NEW QUESTION: 136
In the context of CloudFront RTMP Distribution, the Adobe Flash Media Server _____ file specifies which domains can access media files in a particular domain.
A. accessdomain.JSON

B. crossdomain.xml
C. accessdomain.xml
D. crossdomain.JSON
Answer: B (LEAVE A REPLY)
In the context of CloudFront RTMP Distribution, the Adobe Flash Media Server crossdomain.xml file specifies which domains can access media files in a particular domain.
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Streaming_CrossDomain.html

NEW QUESTION: 137
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 (LEAVE A REPLY)
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: 138
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. Use an Amazon Route 53 geolocation routing policy to navigate traffic to the closest Region
B. Configure AWS Global Accelerator in front of all the Regions
C. Create an Amazon CloudFront distribution in front of all the Regions
D. Use an Amazon Route 53 geoproximity routing policy to navigate traffic to the closest Region
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
Your company has set up AWS Direct Connect to connect on-premises to an Amazon VPC instance. Two Direct Connect connections terminate at two different Direct Connect locations. You are using two routers, R1 and R2, at your end (one of each Direct Connect connection). R1 and R2 do NOT have connectivity between them. Both routers advertise the same routers over BGP to the VGW. You have a stateful firewall on each router. The routers drop some of the traffic coming from the VPC.
Which two actions should you take to fix this problem? (Select two.)
A. Use BGP MED attribute to assign a higher MED value to the routes advertised from R2 to VGW.
B. Use BGP local preference attribute to assign R1 to a lower local preference number than R2.
C. Use BGP MED attribute to assign a higher MED value to the routes advertised R1 to VGW.
D. Use BGP AS prepend attribute to prepend additional AS numbers while advertising routers from R1 to VGW.
E. Use BGP local preference attribute to assign R1 a higher local preference number than R2.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 140
You are configuring a virtual interface for access to your VPC on a newly provisioned 1-Gbps AWS Direct Connect connection. Which two configuration values do you need to provide? (Select two.)
A. Public AS number
B. VLAN ID
C. IP prefixes to advertise
D. Direct Connect location
E. Virtual private gateway
Answer: B,E (LEAVE A REPLY)
References: https://aws.amazon.com/directconnect/faqs/

NEW QUESTION: 141
The Web Application Development team is worried about malicious activity from 200 random IP addresses.
Which action will ensure security and scalability from this type of threat?
A. Use inbound security group rules to block the IP addresses.
B. Use inbound network ACL rules to block the IP addresses.
C. Use AWS WAF to block the IP addresses.
D. Write iptables rules on the instance to block the IP addresses.
Answer: C (LEAVE A REPLY)
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html

NEW QUESTION: 142
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 Route 53 private hosted zone's VPC associations to include the new VPC.
B. Update the on-premises DNS to include forwarders to the Route 53 nameserver IP addresses.
C. Update the DHCP options set for the new VPC with the Route 53 nameserver IP addresses.
D. Launch Amazon EC2-based DNS proxies in the new VPC. Specify the proxies in the DHCP options set.
E. Launch Amazon EC2-based DNS proxies in the new VPC. Specify the proxies as forwarders in the on-premises DNS.
Answer: (SHOW ANSWER)

NEW QUESTION: 143
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 single Route 53 Public Hosted Zone for the zone company.private and configure the VPS DNS Resolver to forward

B. Create a single Route 53 Private Hosted Zone for the zone company.private and associate it with the three 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 Route 53 Private Hosted Zone for each of the four zones and associate them with the three VPCs.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144
You are a holdings company that buys many businesses and must integrate their VPCs into your network. You are constantly encountering networks with similar or overlapping subnets. What is the best way to manage this.
Choose the correct answer:
A. BFD
B. VRF
C. A standby router for the overlapping subnets.
D. A strict IP addressing policy that forces new companies to change the IP addresses of their VPCs.
Answer: (SHOW ANSWER)
VRF, or Virtual Routing and Forwarding will allow you to have multiple routing tables on your router.

NEW QUESTION: 145
You are using the CLI to assign multiple IP addresses to interfaces. The operation fails. What is the most likely reason?
Choose the correct answer:
A. You cannot assign IP addresses in the CLI.
B. You can only assign 5 IP addresses at a time through the CLI.
C. One or more of the IP addresses could not be assigned.
D. All of the IP addresses could not be assigned.
Answer: C (LEAVE A REPLY)
One more of the IP addresses could not be assigned. It only takes one failed assignment for the entire operation to fail.

NEW QUESTION: 146
An organization is deploying an application in a VPC that requires SSL mutual authentication with a client-side certificate, as that is the primary method of identifying clients. The Network Engineer has been tasked with defining the mechanism used within AWS to provide the SSL mutual authentication.
Which of the following options meets the organization's requirements?

A. Use a Classic Load Balancer and upload the client certificate private keys to it. Perform SSL mutual authentication of the client-side certificate there.
B. Use a Network Load Balancer with a TCP listener on port 443, and pass the request through for the SSL mutual authentication to be handled by a backend instance.
C. Use an Application Load Balancer and upload the client certificate private keys to it by using the native server name indication (SNI) features with smart certificate selection to handle multiple calling applications.
D. Front the application with Amazon API Gateway, and use its client-side SSL mutual authentication feature that uses the backend instances to verify the source of the request.
Answer: (SHOW ANSWER)
References:

NEW QUESTION: 147
An organization will be extending its existing on-premises infrastructure into the cloud. The design consists of a transit VPC that contains stateful firewalls that will be deployed in a highly available configuration across two Availability Zones for automatic failover.
What MUST be configured for this design to work? (Select two.)
A. Autonomous system (AS) path prepending
B. Border Gateway Protocol (BGP) routing
C. Static routing
D. Equal-cost multi-path routing (ECMP)
E. A different Autonomous System Number (ASN) for each firewall.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 148
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: (SHOW ANSWER)
Explanation
References:
https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-conn

NEW QUESTION: 149

Your Amazon Kinesis application receives data streams from thousands of devices. The data is then stored in an on-premises Hadoop cluster. You are concerned about historical data that shows periods of sustained traffic between 1 Gbps and 2 Gbps during peaks. You must ensure that you have secure, fault- tolerant connectivity between Amazon Kinesis and your data center. What should you implement to address these needs?

A. Deploy a single 1-Gbps Direct Connect connection with a VPN backup.

B. Deploy three 1-Gbps Direct Connect connections.

C. Deploy two 1-Gbps Direct Connect connections.

D. Set up an IPsec VPN connection over Direct Connect with two tunnels.

Answer: B (LEAVE A REPLY)

Three connections are required to provide fault tolerance. All of the other options would be unable to handle the peak loads over 1 Gbps without exceeding the available bandwidth.

NEW QUESTION: 150

You are architecting an HPC solution in AWS. The system consists of a cluster of EC2 instances that require low-latency communications between them.

Which method should you use to set up a cluster to meet these requirements?

A. Create a VPC with one subnet in a single Availability Zone. Keep the size of the subnet equal to the number of instances required in the cluster. Launch instances for the cluster in this small subnet to guarantee low-latency network performance.

B. Create a placement group. Choose an EC2 instance type compatible with placement groups for the cluster. Launch instances for the cluster in the placement group.

C. Launch Amazon EC2 instances with the largest available number of cores and RAM. Attach all instances to an Amazon EBS PIOPS volume. Implement a shared memory system across all instances in the cluster, using this shared EBS volume to minimize latency of communication.

D. Choose an EC2 instance type that offers enhanced networking. Attach a 10-Gbps non-blocking elastic network interface to the instances. Configure the elastic network interface to optimize network performance to reduce latency.

Answer: B (LEAVE A REPLY)

Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. A is incorrect because the size of a subnet has no impact on network performance. C is incorrect because an EBS volume cannot be shared between EC2 instances. D is only half the solution because the enhanced networking affects the network behavior of an EC2 instance but not the network infrastructure between instances.

NEW QUESTION: 151

You have a server that serves www, FTP, and mail. You need to access this server using www.yourname.com, ftp.yourname.com, and mail.yourname.com. You want to ensure an IP change results in the least number of other changes. What is the best solution? Choose the correct answer:

A. Create PTR records and point the IP address of the server back to www, ftp, and mail.

B. Create an A record pointing to the server's IP address and create CNAME records for www, ftp, and mail and point those to the A record.
C. Create an A record for www, ftp and mail, and point it to the ALIAS of the server.
D. Create CNAME records for www, ftp, and mail and point those to the A record already provided to the instance by AWS.
Answer: B (LEAVE A REPLY)
There is no ALIAS record for an EC2 instance, CNAME records pointed to the A record provided by AWS won't work because if the IP changes, the A record will change also. A PTR record is not appropriate here and cannot point to more than one record. Having three CNAME records and one A record will result in only having to change the A record if the IP changes.

NEW QUESTION: 152
In Amazon CloudFront, you cannot configure CloudFront to process cookies for_____.
A. HTTPS web distributions
B. Web and RTMP distributions
C. RTMP distributions
D. HTTP web distributions
Answer: C (LEAVE A REPLY)
You cannot configure Amazon CloudFront to log cookies for RTMP distributions. For web distributions, CloudFront by default doesn't consider cookies when caching your objects in edge locations. If your origin returns two objects and they differ only by the values in the Set-Cookie header, CloudFront caches only one version of the object.
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

NEW QUESTION: 153
An organization has three AWS accounts with each containing VPCs in Virginia, Canada and the Sydney regions. The organization wants to determine whether all available Elastic IP addresses (EIPs) in these accounts are attached to Amazon EC2 instances or in use elastic network interfaces (ENIs) in all of the specified regions for compliance and cost-optimization purposes. Which of the following meets the requirements with the LEAST management overhead?

A. use an Amazon CloudWatch Events rule to schedule an AWS Lambda function in each account in all three regions to find the unattached and unused EIPs.
B. Use a CloudWatch event bus to schedule Lambda functions in each account in all three regions to find the unattached and unused EIPs.
C. Add an AWS managed, EIP-attached AWS Config rule in each region in all three accounts to find unattached and unused EIPs.
D. Use AWS CloudFormation StackSets to deploy an AWS Config EIP-attached rule in all accounts and regions to find the unattached and unused EIPs.
Answer: D (LEAVE A REPLY)
Explanation
https://docs.aws.amazon.com/config/latest/developerguide/eip-attached.html

NEW QUESTION: 154
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. ABC Telecom creates a support ticket with AWS to exchange MPLS labels and include the AWS port as part of their MPLS network.
B. The customer performs Q-in-Q tunneling, with the AWS-required VLAN tag in the inside and VLAN
100 as the outside tag.
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. Create a support ticket with AWS to request the removal of the outer VLAN tag 100 as the traffic reaches AWS routers.
E. ABC Telecom removes the other tag before sending the packet to AWS.
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 155
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. Configure a virtual private gateway for the VPN and another virtual private gateway for Direct Connect.

B. Confirm that the same routes are being advertised over both the VPN and Direct Connect.
C. Ensure that Bidirectional Forwarding Detection is enabled on the Direct Connect connection
D. Reconfigure the Direct Connect session from static routes to Border Gateway Protocol (BGP) peering.
Answer: (SHOW ANSWER)

NEW QUESTION: 156
You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems. Which two AWS Services cloud you leverage to build an automated notification system? (Select two.)
A. Internet gateway
B. VPC Flow Logs
C. AWS CloudTrail
D. Lambda
E. AWS Inspector
Answer: C,D (LEAVE A REPLY)
Explanation/Reference:
References: https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-by- using-aws-cloudtrail-amazon-sns-and-aws-lambda/

NEW QUESTION: 157
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 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.
B. 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
C. 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.
D. 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
Answer: B (LEAVE A REPLY)

NEW QUESTION: 158
You have two placement groups in a VPC. What communication speed can be expected between the two placement groups?
Choose the correct answer:
A. 5Gbps
B. 10Gbps
C. 20Gbps
D. You cannot communicate between two placement groups.
Answer: A (LEAVE A REPLY)
5Gbps is the maximum speed for traffic outside of a placement group.

NEW QUESTION: 159
You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a selfreferencing rule using the cluster security group's group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions. How should you enable secure cluster communication while deploying additional cluster members in another AWS region?
A. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
B. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other's security group-id in each region.
C. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other's security group-id in each region.
D. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 160
In the context of Amazon CloudFront, when you configure the media player, the path you specify to the media file must contain the characters _____.
A. flv/std just before the domain name
B. flv/std immediately after the domain name
C. cfx/st just before the domain name
D. cfx/st immediately after the domain name
Answer: (SHOW ANSWER)

In Amazon CloudFront, when you configure the media player, the path you specify to the media file must contain the characters cfx/st immediately after the domain name. For example: rtmp://s5c39gqb8ow64r.cloudfront.net/cfx/st/mediafile.flv Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Streaming_URLs.html

NEW QUESTION: 161
A company provisions an AWS Direct Connect connection to permit access to Amazon EC2 resources in several Amazon VPCs and to data stored in private Amazon S3 buckets. The Network Engineer needs to configure the company's on-premises router for this Direct Connect connection.
Which of the following actions will require the LEAST amount of configuration overhead on the customer router?
A. Configure a private virtual interface to a Direct Connect gateway for the VPC resources and a public virtual interface for Amazon S3.
B. Configure a private virtual interface to a Direct Connect gateway for the VPC resources and for Amazon S3.
C. Configure private virtual interfaces for the VPC resources and for Amazon S3.
D. Configure private virtual interfaces for the VPC resources and a public virtual interface for Amazon S3.
Answer: (SHOW ANSWER)

NEW QUESTION: 162
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. Use X-Forwarded-For with security groups to apply the Geographic Restriction.
B. Modify the nginx log configuration to record value in X-Forwarded-For and use CloudFront to apply the Geographic Restriction.
C. Enable ELB access logs to store the client IP address and parse these to dynamically modify a blacklist.
D. Modify the application code to use value of X-Forwarded-For and CloudFront to apply the Geographic Restriction.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
You are a network engineer at a company that just purchased a DX connection. You ensured your equipment met all of the technical requirements, you have verified with your AWS account manager and your colocation provider that everything is connected, and all of your information is correct. For some reason, the link does not operate correctly. What could be the problem? Choose the correct answer:

A. The CAT6 cable is frayed.
B. Autonegotiation is enabled.
C. You are using 802.1q VLANs instead of 802.1w.
D. BFD is disabled.
Answer: B (LEAVE A REPLY)
Autonegotiation is enabled. A DX connection uses single-mode fiber, not CAT6; BFD is optional, and 802.1q is the correct standard. Autonegotiation must be disabled for DX to work properly.

NEW QUESTION: 164
A network engineer deploys an application in a private subnet in a VPC that connects to many external video feed providers using RTMP over the internet. A NAT gateway has been deployed in a public subnet and is working as expected. From the Amazon EC2 instance, the application is able to connect to all feed providers except one, which hangs when connecting. Manually testing a connection from an Amazon EC2 instance in the public subnet to the problem feed indicates that the feed works as expected.
What is causing this issue?
A. The internet gateway only supports an MTU of 1500 bytes.
B. The security group on the instances does not allow PMTUD.
C. An Amazon EC2 instance expects to communicate with an MTU of 9001.
D. The NAT gateway does not support fragmented packets.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
A company wants to migrate its production and development applications to the AWS Cloud across multiple VPCs in three AWS Regions us-east-1 (N Virginia), eu-west-1 (Ireland), and ap-southeast-1 (Singapore) The company needs a scalable solution that provides connectivity between all three Regions The solution also must provide private connectivity to the company's on-premises data center in Northern Virginia Data that is transferred from on premises and data that is transferred between Regions must be encrypted in transit The company requires predictable network performance and must minimize cost The company has initiated a solution by deploying a transit gateway with two route tables in each Region One route table is for the production environment, and one route table is for the development environment What else must the company do to meet its requirements with the LOWEST latency?
A. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center. On each transit gateway, create a VPN attachment over the public VIF for the production and development route tables. Route traffic between Regions through the VPN connections.
B. Deploy an AWS Direct Connect connection in us-east-1 and a transit VIF to the on-premises data center Associate all transit gateways and the transit VIF with a different Direct Connect gateway. Create transit gateway peering connections to route traffic between Regions

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