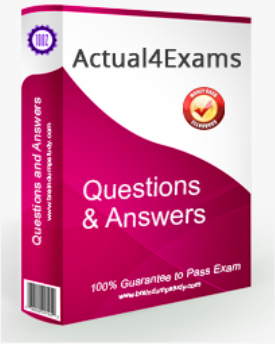
[Actual4Exams]



Try before you buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

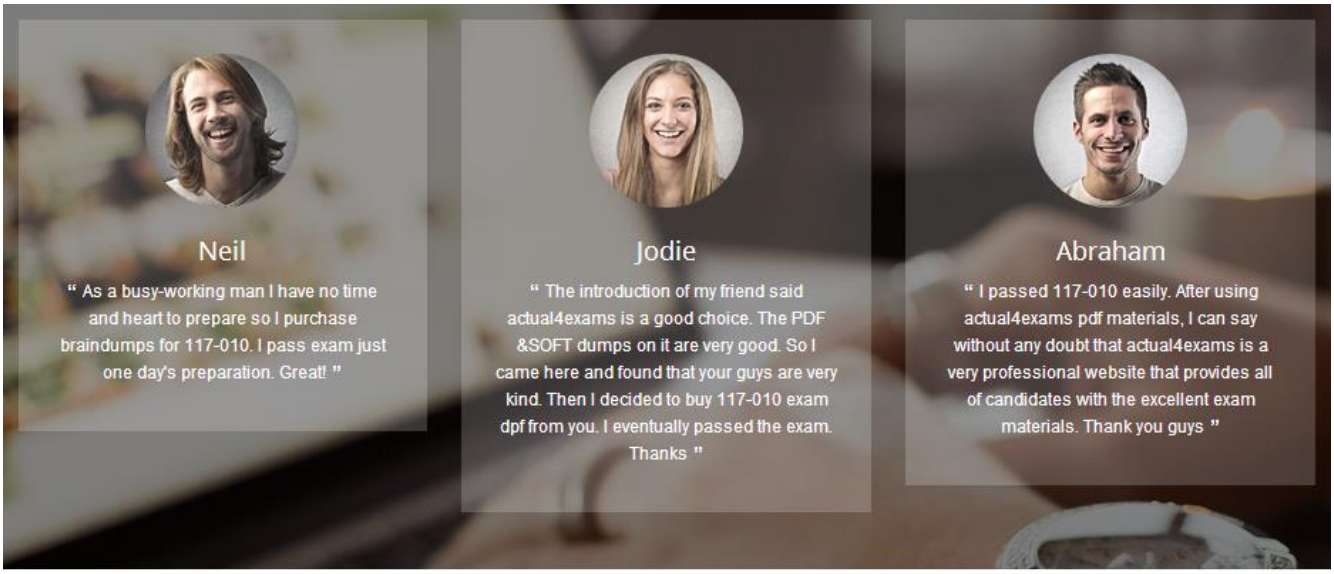
Choose an exam to sample

Select a vendor...

Select an exam...

Your email address

Download Now



Why Choose Actual4Exams

Quality and Value

Actual4Exams Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all vce.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our Actual4Exams testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

Actual4Exams offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

Exam : **AWS-Advanced-Networking-Specialty**

Title : AWS Certified Advanced Networking Specialty (ANS-C00) Exam

Vendor : Amazon

Version : DEMO

NO.1 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 new connection through your AWS Management Console and wait for an email from AWS with information.
B. Create a support ticket. Provide your AWS account number and telecommunications company's name and where you need the Direct Connect connection to terminate.
C. Ask your telecommunications provider to contact AWS through an AWS Partner Channel. Provide your AWS account number.
D. 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.
Answer: A
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/provision-direct-connection/
https://docs.aws.amazon.com/directconnect/latest/UserGuide/getting_started.html

NO.2 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 the VPC wizard in the AWS Management Console. Type in the CIDR blocks for the VPC and subnets.
B. Use AWS OpsWorks to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.
C. Use AWS CloudFormation to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.
D. Create the VPCs using AWS CLI and use the dry-run flag to validate if the current CIDR range is in use.
Answer: C

NO.3 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. A public virtual interface must be configured for Amazon EC2 connectivity.
D. The VGW is not advertising the correct CIDR range back on-premises.
E. There is a misconfiguration of the bi-directional forwarding detection.
Answer: A,B

NO.4 The Security department has mandated that all outbound traffic from a VPC toward an on-premises datacenter must go through a security appliance that runs on an Amazon EC2 instance.
Which of the following maximizes network performance on AWS? (Choose two.)
A. Security appliance support for multiple elastic network interfaces
B. Support for sending traffic over the Direct Connect connection
C. The instance sizes and families supported by the security appliance
D. Support for the enhanced networking drivers
E. Support for placement groups within the VPC
Answer: C,D

NO.5 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. Customer-managed MySQL with Transparent Data Encryption
B. Amazon Aurora in a private subnet
C. AWS Key Management Services
D. Amazon CloudFront using AWS Lambda@Edge
E. Application Load Balancer using HTTPS listeners and targets
Answer: C,D
Explanation:
https://aws.amazon.com/blogs/networking-and-content-delivery/serving-sse-kms-encrypted-content-from-s3-using-cloudfront/
https://aws.amazon.com/blogs/security/how-to-protect-sensitive-data-for-its-entire-lifecycle-in-aws/

NO.6 A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2 instances now use a NAT gateway tor internet access After the migration, some long-running database queries from private EC2 instances to a publicly accessible third-party database no longer receive responses The database query logs reveal that the queries successfully completed after 7 minutes but that the client EC2 instances never received the response.
Which configuration change should a network engineer implement to resolve this issue''
A. Configure the NAT gateway timeout to allow connections for up to 600 seconds
B. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds
C. Enable enhanced networking on the client EC2 instances
D. Close idle TCP connections though the NAT gateway
Answer: B
Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-troubleshooting.html#nat-gateway-troubleshooting-timeout To prevent the connection from being dropped, you can initiate more traffic over the connection. Alternatively, you can enable TCP keepalive on the instance with a

value less than 350 seconds.

NO.7 A company has applications running in a single AWS Region and its on premises data center in a hybrid mode The company has a 1Gbps AWS Direct Connect connection from the data center to AWS that is 65% utilized. The company has an AWS Enterprise Support plan The company is planning to deploy a new critical application on AWS that will connect with existing applications running in the data center. The application SLA requires a minimum ot 99.9% network uptime between the data center and AWS.
What is the MOST cost-effective way to meet this SLA requirement?
A. Set up two new hosted Direct Connect connections of 500 Mbps each through an AWS Direct Connect partner. Provision two virtual interfaces (VIFs) to the existing VPC on both Direct Connect connections, and use BGP for load balancing Terminate the existing 1Gbps Direct Connect connection
B. Purchase an additional 1Gbps Direct Connect connection from AWS in the existing cross-connect location Ask AWS to terminate this new connection in a different router Provision two virtual interfaces (VIFs) to the same VPC on both Direct Connect connections, and use BGP for load balancing
C. Purchase an additional 1Gbps Direct Connect connection from AWS In a different cross-connect location terminated in the associated Region Provision a new virtual interface (VIF) to the existing VPC. and use BGP for load balancing
D. Create a second virtual interface (VIF) on the existing Direct Connect connection, and terminate this VIF in the existing VPC Use BGP for load balancing between the VIFs in active/active mode.
Answer: C
Explanation:
https://aws.amazon.com/directconnect/sla/
99.9% - Included Resource uses virtual interfaces on Dedicated Connections at a minimum of 2 Direct Connect locations, and at least one of those Direct Connect locations uses the Associated AWS Region (described here) in which your workload is located.
99.99% - Included Resource uses virtual interfaces on at least 4 Dedicated Connections across a minimum of 2 Direct Connect locations (with no fewer than 2 connections in a single location), and at least one of the Direct Connect locations uses the Associated AWS Region in which your workload is located.

NO.8 Changes made to a security group attached to an Application Load Balancer resulted in connectivity issues for a company's production web application. The Network Engineer needs to lock down permissions for the company's AWS account, automate auditing for any changes, and set up notifications.
What actions should accomplish this?
A. Configure IAM user policies to lock down permissions for specific users. Enable AWS CloudTrail to identify the API calls from users. Configure Amazon Macie to use machine learning to identify any configuration changes, and configure Amazon SNS to send notifications.
B. Configure IAM user policies to lock down permissions for specific users. Enable AWS CloudTrail to identify API calls from users. Use AWS Config to audit any changes, and configure Amazon SNS to send notifications.
C. Configure IAM user policies to lock down permissions for specific users. Enable AWS CloudTrail to identify the API calls from users. Configure AWS CodeCommit to audit any changes in configurations,

and configure Amazon SNS to send notifications.

D. Configure IAM role policies to lock down permissions for specific users. Configure Amazon GuardDuty to audit and monitor configuration changes, and configure Amazon SNS to send notifications.

Answer: B

NO.9 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 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.

B. 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.

C. Use a Classic Load Balancer and upload the client certificate private keys to it. Perform SSL mutual authentication of the client-side certificate there.

D. 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.

Answer: A

NO.10 An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used.

Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: "There are not enough free addresses in subnet 'subnet-12345677' to satisfy the requested number of instances." What action will resolve the availability problem?

A. Create a new subnet using a VPC secondary IPv4 CIDR, and associate an IPv6 CIDR. Include the new subnet in the Auto Scaling group.

B. Create a new subnet using a VPC secondary IPv6 CIDR, and associate an IPv6 CIDR. Include the new subnet in the Auto Scaling group.

C. Resize the IPv6 CIDR on each of the existing subnets. Modify the Auto Scaling group maximum number of instances.

D. Add a secondary IPv4 CIDR to the Amazon VPC. Assign secondary IPv4 address space to each of the existing subnets.

Answer: A