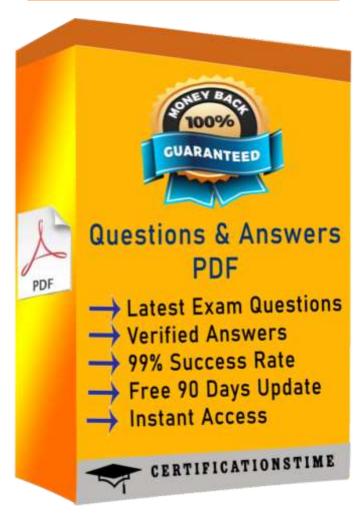# Exam Questions ANS-C00

AWS Certified Advanced Networking Specialty

https://certificationstime.com/

QUESTION 1

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.

Correct Answer: A

QUESTION 2

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? (Choose two.)

A. Use BGP AS prepend attribute to prepend additional AS numbers while advertising routers from R1 to VGW.
B. Use BGP local preference attribute to assign R1 to a lower local preference number than R2.
C. Use BGP local preference attribute to assign R1 a higher local preference number than R2.
D. Use BGP MED attribute to assign a higher MED value to the routes advertised R1 to VGW.
E. Use BGP MED attribute to assign a higher MED value to the routes advertised from R2 to VGW.

Correct Answer: A,C

QUESTION 3

A Network Engineer is designing a new system on AWS that will take advantage of Amazon CloudFront for

both content caching and for protecting the underlying origin. There is concern that an external agency might be
able to access the IP addresses for the application's origin and then attack the origin despite it being served by
CloudFront. Which of the following solutions provides the strongest level of protection to the origin?

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

Correct Answer: A

QUESTION 4

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

Correct Answer: D

QUESTION 5

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.

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.

Correct Answer: B

Explanation/Reference:

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.

QUESTION 6

Which two statements about placement groups are correct? (Choose two.)

A. A placement group can span multiple VPCs.
B. A placement group can span multiple Availability Zones.
C. You cannot merge placement groups.
D. It is best to use the same instance types in a placement group.

Correct Answer: A,C

Explanation/Reference:

A placement group can span multiple VPCs but may not experience the full performance benefit. The only way
to add instances from one placement group to another is to create AMIs out of the instances and spin them all
up into one placement group.

QUESTION 7

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

Correct Answer: C

Explanation/Reference:

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

QUESTION 8

Your company wishes to improve the performance of its EC2 instances. They require low latency and high
throughput. They are currently deployed on T2.medium. It is imperative that you experience as little downtime
as possible, but cost and performance are most important. How should you accomplish this?

A. Create AMIs from the instances, create new instances on t2.medium, and start those instances in aplacement group.
B. Create AMIs from the instances, deploy the instances as i3.large, and start those instances in a placementgroup.
C. Stop the instances and restart them in a placement group.
D. Add an extra ENI to the instances and team them to provide greater throughput.

Correct Answer: B

Explanation/Reference:

T2. medium is not compatible with placement groups. You cannot team ENIs to add more throughput on AWS.

QUESTION 9

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? (Choose two.)

A. Internet gateway
B. VPC Flow Logs
C. AWS CloudTrail
D. Lambda
E. AWS Inspector

Correct Answer: C,D

Explanation/Reference:

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

QUESTION 10

Which is not a valid Route 53 record?

A. SPF
B. NAPTR
C. AAAA
D. BFD

Correct Answer: D

Explanation/Reference:

BFD stands for Bi-directional Forwarding Detection and has nothing to do with Route 53.

QUESTION 11

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

Correct Answer: C

Explanation/Reference:

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

QUESTION 12

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

Correct Answer: C

Explanation/Reference:

Explanation:
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_exampleevents.html

QUESTION 13

A multinational organization has applications deployed in three different AWS regions. These applications must
securely communicate with each other by VPN. According to the organization's security team, the VPN must

meet the following requirements:
AES 128-bit encryption
SHA-1 hashing
User access via SSL VPN
PFS using DH Group 2
Ability to maintain/rotate keys and passwords
Certificate-based authentication
Which solution should you recommend so that the organization meets the requirements?

A. AWS hardware VPN between the virtual private gateway and customer gateway
B. A third-party VPN solution deployed from AWS Marketplace
C. A private MPLS solution from an international carrier
D. AWS hardware VPN between the virtual private gateways in each region

Correct Answer: D

QUESTION 14

Your company has placement groups in two different availability zones. There is a large project coming up and,
although resilience is important, cost and speed are the most important factors. The servers in each placement
group need to be able to achieve the highest speed possible.
How can this be achieved?

A. Create AMIs from all of the instances, terminate them, and deploy them all into one placement group.
B. In the CLI, run the command "aws ec2 set-placement-group 1 " for all of the instances.
C. Duplicate the VPC, peer the new VPC, create AMIs of the instances, terminate them, and redeploy them in two separate placement groups between the two VPCs.
D. Peer the two placement groups using AWS PG Peering.

Correct Answer: A

Explanation/Reference:

There is no AWS PG Peering option, Duplicating the VPC does not align with the cost concern, there is no "aws
ec2 set-placement-group" command.

QUESTION 15

What are two reasons that could cause an HTTP health check to fail? (Choose two.)

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

Correct Answer: A,B

Explanation/Reference:

A load balancer does not perform health checks through the internet gateway, so it is not necessary and 443 is
HTTPS not HTTP

QUESTION 16

Your organization leverages an IP Address Management (IPAM) product to manage IP address distribution.
The IPAM exposes an API. Development teams use CloudFormation to provision approved reference architectures. At deployment time, IP addresses must be allocated to the VPC. When the VPC is deleted, the
IPAM must reclaim the VPC's IP allocation.
Which method allows for efficient, automated integration of the IPAM with CloudFormation?

 A. AWS CloudFormation parameters using the "Ref::" intrinsic function
 B. AWS CloudFormation custom resource using an AWS Lambda invocation.
 C. CloudFormation::OpsWorks::Stack with custom Chef configuration.
 D.   AWS CloudFormation parameters using the "Fn::FindInMap" intrinsic function.

Correct Answer: A

QUESTION 17

You wish to have a sub-1G connection to AWS to save on costs. How can you achieve this?

 A. Just set your router to the speed you want and AWS will charge you based on the actual speed of the port.
 B. Contact AWS, they will put you in contact with a technical account manager who can help you get this setup.
 C. You can't. The only speeds available for Direct Connect are 1G and 10G.
 D. Contact an AWS partner, AWS does not provide sub-1G connection speeds.

Correct Answer: D

Explanation/Reference:

Sub-1G service is only available through AWS partners.

QUESTION 18

You have a hybrid infrastructure, and you need AWS resources to be able to resolve your on-premises DNS
names. You have configured a DNS server on an EC2 instance in your 10.1.3.0/24 subnet. This subnet resides
on the VPC 10.1.0.0/16. What step should you take to accomplish this?

A. Configure your DNS server to forward queries for the private hosted zone to 10.1.3.2.
B. Configure the DHCP option set in the VPC to point to the EC2 DNS server.
C. Configure your DNS server to forward queries for the private hosted zone to 10.1.0.2.
D. Disable the source/destination check flag for the DNS instance.

Correct Answer: B

Explanation/Reference:

Your DNS server will forward queries to your on-premises DNS. You must configure the DHCP option set so
the instances will forward queries to your on-premises DNS instead of the VPC DNS.

QUESTION 19

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

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

D. Update the CORS configuration for Amazon S3 to allow traffic from the proxy.

Correct Answer: D

QUESTION 20

You need to create a baseline of normal traffic flow in order to implement some security changes to your
organization.
What two items would be best to use? (Choose two.)

A. Wireshark
B. CloudTrail
C. An IDS
D. CloudWatch

Correct Answer: A,D

QUESTION 21

You have two placement groups in a VPC. What communication speed can be expected between the two
placement groups?

A. 5Gbps
B. 10Gbps
C. 20Gbps
D. You cannot communicate between two placement groups.

Correct Answer: A

Explanation/Reference:

5Gbps is the maximum speed for traffic outside of a placement group.

QUESTION 22

A Network Engineer is troubleshooting a network connectivity issue for an instance within a public subnet that
cannot connect to the internet. The first step the Engineer takes is to SSH to the instance via a local

bastion

within the VPC and runs an ifconfig command to inspect the IP addresses configured on the instance. The

output is as follows:

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

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

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

Correct Answer: B

QUESTION 23

With respect to Amazon CloudFront, which one of the following statements is correct?

A. For HTTPS web distributions, you cannot forward cookies to your origin.
B. For both HTTP and HTTPS web distributions, you can choose to forward cookies to your origin.
C. For HTTP web distributions, you cannot forward cookies to your origin.
D. For Real Time Messaging Protocol (RTMP) distributions, you can configure CloudFront to process cookies.

Correct Answer: B

Explanation/Reference:

With respect to Amazon CloudFront, for HTTP and HTTPS web distributions, you can choose whether you want
CloudFront to forward cookies to your origin. For RTMP distributions, you cannot configure CloudFront to
process cookies.
Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

QUESTION 24

You need to create a subnet in a VPC that supports 14 hosts. You need to be as accurate as possible since
you run a very large company. What CIDR should you use?

A. /28
B. /24
C. /25
D. /27

Correct Answer: D

Explanation/Reference:

/27 supports 27 hosts since AWS reserves 5 addresses. /25 supports 123 hosts, /28 supports 11, /24
supports
251.

QUESTION 25

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
onpremises 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. Change the DHCP options set for the VPC to use both the Amazon-provided DNS server and the
   onpremises 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.
B. 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.
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 on-premises DNS systems. Configure the
   onpremises 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.

Correct Answer: C

QUESTION 26

In the "start using the AWS Direct Connect steps," when can you complete the Cross Connect step?

A. After verifying your virtual interface
B. After you have received your Letter of Authorization and Connecting Facility Assignment (LOA-CFA) fromAWS
C. 72 hours after submitting your request for AWS Direct Connect Connection
D. Immediately after submitting your request for AWS Direct Connect Connection

Correct Answer: B

Explanation/Reference:

To complete the steps of "start using the AWS Direct Connect," after submitting your request for AWS Direct
Connect connection, AWS will send you an email within 72 hours with a Letter of Authorization and Connecting
Facility Assignment (LOA-CFA). After you have received your LOA-CFA, you need to complete your crossnetwork connection, also known as a cross connect.
Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Colocation.html

QUESTION 27

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.C
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.

Correct Answer: C

QUESTION 28

Which CloudWatch attributes are used for the statistics generation?

A. All the options are used
B. Dimension
C. Data point unit
D. NameSpace

Correct Answer: A

Explanation/Reference:

Statistics represents data aggregation of the metric data values over a specific period of time. These aggregations are made using the namespace, metric name, dimensions and the data point unit of measure
within the time period that the user has specified.
Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API_MetricDatum.html

QUESTION 29

Imagine you are using AWS Direct Connect with just one connection from your router to the AWS Direct
Connect router. If your connection becomes unavailable, the communication with AWS cloud is lost. What is
the best method to prevent this from happening?

A. AWS Direct Connect neither provides BGP nor provides the failover.
B. AWS Direct Connect recommends to have the same configuration set up in a multi AZ zone to prevent suchloss in connections.
C. AWS Direct Connect recommends that you request and configure two dedicated connections to AWS eitherusing BGP Multipath (Active/Active) connection or the failover (Active/Passive) connection.
D. AWS Direct connect does not have a provision to prevent the situation but when you design the system, it isrecommended to request a back-up instance to which the traffic can be re-routed.

Correct Answer: C

Explanation/Reference:

When configuring redundant connections with the AWS Direct Connect, and to provide for failover, we recommend that you request and configure two dedicated connections to the AWS. There are different
configuration choices available when you provision two dedicated connections. You can either use Active/Active
(BGP multipath) connection or Active/Passive (failover) connection to configure the two dedicated connections.
Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/
getstarted.html#RedundantConnections

QUESTION 30

From the following options, select the answer that correctly describes the implementation of the HTTP protocol

A. By definition, HTTP is a connection-less oriented protocol and therefore utilises TCP
B. By definition, HTTP is a connection orientated protocol and therefore utilises TCP
C. By definition, HTTP is a connection-less oriented protocol and therefore utilises UDP
D. By definition, HTTP can be configured to be either connection or connection-less oriented – by specifyingthe appropriate HTTP header.

Correct Answer: B

Explanation/Reference:

HTTP is a connection orientated protocol and therefore utilizes TCP
Reference: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

QUESTION 31

You need to create a subnet in a VPC that supports 1000 hosts. You need to be as accurate as possible since
you run a very large company. What CIDR should you use?

A. /16
B. /24
C. /7
D. /22

Correct Answer: D

Explanation/Reference:

/22 supports 1019 hosts since AWS reserves 5 addresses.

QUESTION 32

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? (Choose two.)

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

Correct Answer: C,E

QUESTION 33

You have 3 VPCs that need to be able to pass traffic. In what two ways can you achieve this? (Choose two.)

A. Peer each VPC to every other VPC to create a full mesh peering.
B. Peer them, VPC peering allows transitive peering as of December 2017.
C. Call AWS to enable transitive peering.
D. Create VPNs between them and adjust the routing tables accordingly.

Correct Answer: A,D

Explanation/Reference:

VPN instances can be used to create transitive peering. Full mesh peering is the only way to use peering to
allow all VPCs to communicate with all other VPCs. Transitive peering is not possible.

QUESTION 34

Which port range must be allowed through a NACL to ensure all return traffic is successful?

A. 1024 – 65,535
B. 22
C. 65,000 – 65,535
D. 80 – 443

Correct Answer: A

Explanation/Reference:

1024 – 65,535 is the full "ephemeral port" range.