

- 🏠 (<https://www.whizlabs.com/learn>) > My Courses (<https://www.whizlabs.com/learn/my-courses>)
- > AWS Certified Advanced Networking Specialty (<https://www.whizlabs.com/learn/course/aws-cans-practice-tests#section-1>)
 - > Practice Test I (<https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14608>) > Report

PRACTICE TEST I

Attempt	1	Completed on	Sunday , 03 February 2019 , 10:29 PM
Marks Obtained	1 / 80	Time Taken	00 H 00 M 15 S
Your score is	1.25%	Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	80	1	0	79

80 Questions	1 Correct	0 Incorrect	79 Unattempted	Show Answers	All	▼
------------------------	---------------------	-----------------------	--------------------------	--------------	-----	---

QUESTION 1 CORRECT

What is the current limit on the number of BGP advertised routes can you have per route table?

- ☒ A. 100 ✓
- ☐ B. 50
- ☐ C. 200
- ☐ D. Unlimited

Explanation :

Answer – A

This is clearly provided in the AWS documentation

BGP advertised routes per route table (propagated routes)	100	You can have up to 100 propagated routes per route table. This limit cannot be increased. If you require more than 100 prefixes, advertise a default route.
---	-----	---

For more information on the VPC limits , please visit the below link:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html)

Ask our Experts



QUESTION 2 UNATTEMPTED

You have a web application hosted on a web server in AWS. You have a need for the moment to allow both HTTP and HTTPS Traffic for this application. Which of the following ports need to be configured in the security group to ensure that the traffic gets routed accordingly. Choose 2 answers from the options given below

- ☐ A. 22
- ☐ B. 80 ✓
- ☐ C. 443 ✓
- ☐ D. 25

Explanation :

Answer – B and C

The port used by HTTP traffic is port 80 and that by HTTPS is port 443.

For configuration of these ports on a load balancer, one can visit the below URL:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html> (<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html>)

Ask our Experts



QUESTION 3 UNATTEMPTED

Your company currently has a VPN connection between AWS and its on-premise infrastructure. There was a suggestion to use jumbo frames to get a larger set of network packets sent across the VPN connection. As a network specialist what would you recommend in this regard?

- ☐ A. Agree on this, since it would definitely help in sending more data across the VPN connection.
- ☐ B. Agree on this, but also make the suggestion to use larger instance types on the AWS side.
- ☐ C. Disagree on this, since using jumbo frames this could slow down the traffic ✓

☐ D. Disagree on this since using jumbo frames is not possible in AWS.

Explanation :

Answer - C

The AWS documentation mentions the following on jumbo frames

Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead.

Jumbo frames should be used with caution for Internet-bound traffic or any traffic that leaves a VPC.

Packets are fragmented by intermediate systems, which slows down this traffic.

Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead. Fewer packets are needed to send the same amount of usable data. However, outside of a given AWS region (EC2-Classic), a single VPC, or a VPC peering connection, you will experience a maximum path of 1500 MTU. VPN connections and traffic sent over an Internet gateway are limited to 1500 MTU. If packets are over 1500 bytes, they are fragmented, or they are dropped if the Don't Fragment flag is set in the IP header.

Jumbo frames should be used with caution for Internet-bound traffic or any traffic that leaves a VPC. Packets are fragmented by intermediate systems, which slows down this traffic. To use jumbo frames inside a VPC and not slow traffic that's bound for outside the VPC, you can configure the MTU size by route, or use multiple elastic network interfaces with different MTU sizes and different routes.

For instances that are colocated inside a cluster placement group, jumbo frames help to achieve the maximum network throughput possible, and they are recommended in this case.

For more information, see [Placement Groups](#).

For more information on jumbo frames, one can visit the below URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html)

Ask our Experts



QUESTION 4 UNATTEMPTED

Which of the following statements are false with regards to placement groups?

- ☐ A. You can merge placement groups ✓
- ☐ B. A placement group can span peered VPC's
- ☐ C. A cluster placement group can't span multiple Availability Zones.
- ☐ D. You can move an existing instance into a placement group

Explanation :

Answer – A

The AWS documentation mentions the following on placement groups

1. You can't merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement group.
2. A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs.
3. A placement group are of two types..
 1. Cluster Placement Groups - A cluster placement group can't span multiple Availability Zones.
 2. Spread Placement Groups - A spread placement group can span multiple Availability Zones

For more information, please check:

- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>
(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>)

4. You can move an existing instance to a placement group, move an instance from one placement group to another, or remove an instance from a placement group. Before you begin, the instance must be in the `stopped` state.

For more information on placement groups, one can visit the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>)

Ask our Experts



QUESTION 5 UNATTEMPTED

In order to enable Enhanced networking with the Elastic Network Adapter , which of the following pre-requisites should be met? Choose 3 answers from the options given below

- ☐ **A. Launch the Instance in a VPC** ✓
- ☐ **B. Use a para-virtual Instance Type**
- ☐ **C. Use a HVM Instance Type** ✓
- ☐ **D. Use Linux version 3.2 or greater** ✓

Explanation :

Answer – A,C and D

The AWS documentation mentions the following on enabling the Elastic Network Adapter

- Launch the instance from an HVM AMI using Linux kernel version of 3.2 or later. The latest Amazon Linux HVM AMIs have the modules required for enhanced networking installed and have the required attributes set. Therefore, if you launch an Amazon EBS-backed, enhanced networking-supported instance using a current Amazon Linux HVM AMI, ENA enhanced networking is already enabled for your instance.
- Launch the instance in a VPC. (You can't enable enhanced networking if the instance is in EC2-Classic.)

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena.html>)

Ask our Experts



QUESTION 6 UNATTEMPTED

Which of the following situations will cause a charge to be incurred when using an Elastic IP address? Choose 2 options

- ☐ A. When the Elastic IP is associated with a running instance.
- ☐ B. The instance has only one Elastic IP address attached to it.
- ☐ C. Elastic IP is associated with a stopped instance. ✓
- ☐ D. You have dissociated the Elastic IP address. ✓

Explanation :

Answer - C & D

The AWS documentation mentions the following on Elastic IP addresses

An Elastic IP address doesn't incur charges as long as the following conditions are true:

- The Elastic IP address is associated with an Amazon EC2 instance.
- The instance associated with the Elastic IP address is running.
- The instance has only one Elastic IP address attached to it.

If you've stopped or terminated an EC2 instance with an associated Elastic IP address and you don't need that Elastic IP address any more, consider disassociating or releasing the Elastic IP address

For more information, please visit the below URL:

- <https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/>
(<https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/>)

Ask our Experts



QUESTION 7 UNATTEMPTED

Which of the following are advantages to use multiple IP addresses on an EC2 Instance in AWS? Choose three answers

- ☐ A. Host multiple websites on a single server by using multiple SSL certificate ✓
- ☐ B. To support multiple network interfaces ✓
- ☐ C. To failover to a standby instance ✓
- ☐ D. To ensure broadcasting is possible on the subnet

Explanation :

Answer – A,B and C

It can be useful to assign multiple IP addresses to an instance in your VPC to do the following:

- For more information on multiple IP addresses, please visit the below URL:

- ## Ask our Experts

QUESTION 8 UNATTEMPTED

- ☐ A. 1
- ☒ B. 2 ✓
- ☐ C. 4
- ☐ D. 8

Explanation :

Answer – B

The AWS documentation mentions the following on DB Subnet Groups

Each DB subnet group should have subnets in at least two Availability Zones in a given region. When creating a DB instance in VPC, you must select a DB subnet group. Amazon RDS uses that DB subnet group and your preferred Availability Zone to select a subnet and an IP address within that subnet to associate with your DB instance. If the primary DB instance of a Multi-AZ deployment fails, Amazon RDS can promote the corresponding standby and subsequently create a new standby using an IP address of the subnet in one of the other Availability Zones.

For more information on multiple IP addresses, please visit the below URL:

- ## Ask our Experts



QUESTION 9 UNATTEMPTED

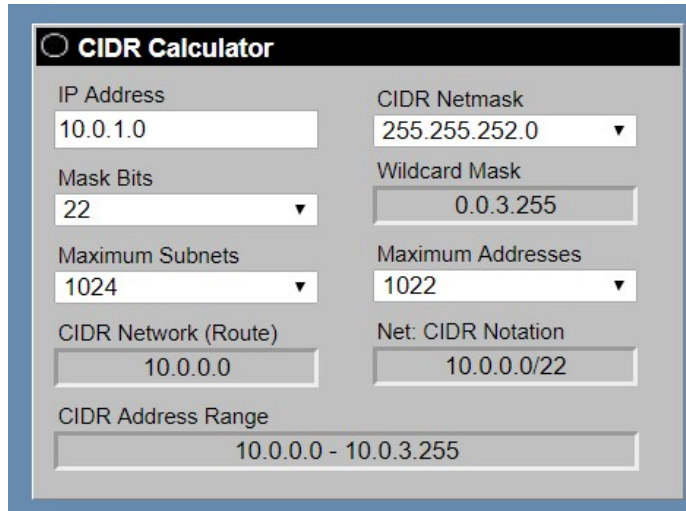
You have a requirement to create a subnet which will have the ability to host 1000 addresses. Which of the below network masks would you use to ensure that the ability to host this many IP addresses is as accurate as possible

- ☐ A. /21
- ☒ B. /22 ✓
- ☐ C. /23
- ☐ D. /24

Explanation :

Answer – B

You can use any CIDR calculator available online to see the number of subnets and host addresses when you use different network masks. A snapshot of one such site is given below



The screenshot shows a web-based CIDR Calculator. The title is "CIDR Calculator". It has several input fields and output displays. The "IP Address" field contains "10.0.1.0". The "Mask Bits" dropdown is set to "22". The "Maximum Subnets" dropdown is set to "1024". The "CIDR Netmask" dropdown is set to "255.255.252.0". The "Wildcard Mask" field displays "0.0.3.255". The "Maximum Addresses" dropdown is set to "1022". The "CIDR Network (Route)" field displays "10.0.0.0". The "Net: CIDR Notation" field displays "10.0.0.0/22". The "CIDR Address Range" field displays "10.0.0.0 - 10.0.3.255".

An example site for calculating CIDR blocks is given below

- <http://www.subnet-calculator.com/cidr.php> (<http://www.subnet-calculator.com/cidr.php>)

Ask our Experts



QUESTION 10 UNATTEMPTED

How many tunnels are provided for a VPN connection created between AWS and an on-premise infrastructure?

- ☐ A. 1
- ☒ B. 2 ✓
- ☐ C. 4
- ☐ D. 8

Explanation :

Answer - B

The AWS documentation mentions the following on VPN connections

You use a VPN connection to connect your network to a VPC. Each VPN connection has two tunnels, with each tunnel using a unique virtual private gateway public IP address. It is important to configure both tunnels for redundancy. When one tunnel becomes unavailable (for example, down for maintenance), network traffic is automatically routed to the available tunnel for that specific VPN connection.

For more information on VPC connections, please visit the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts



QUESTION 11 UNATTEMPTED

Which of the following features allows to aggregate multiple 1 gigabit or 10 gigabit connections at a single AWS Direct Connect and treat them as a single connection.

- ☐ A. Direct Connection Peering
- ☒ B. Link Aggregation Group ✓
- ☐ C. Connection Addition Group
- ☐ D. VPN connection peering

Explanation :

Answer - B

The AWS documentation mentions the following on link aggregation groups

A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple 1 gigabit or 10 gigabit connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.

For more information on LAG, please visit the below URL:

- <http://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html>
(<http://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html>)

Ask our Experts



QUESTION 12 UNATTEMPTED

Which of the following commands can be issued on your linux EC2 Instance to get the public IP of the instance while it is in the running state

- ☐ A. curl http://254.169.254.169/latest/meta-data/public-ipv4
- ☐ B. curl http://127.0.0.1/latest/meta-data/public-ipv4
- ☒ C. curl http://169.254.169.254/latest/meta-data/public-ipv4 ✓
- ☐ D. curl http://10.0.1.0/latest/meta-data/public-ipv4

Explanation :

Answer – C

The URL: for Instance metadata is

- <http://169.254.169.254/latest/meta-data/> (<http://169.254.169.254/latest/meta-data/>)

The different properties that can be retrieved via the Instance metadata is

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/

For more information on Instance metadata, please visit the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>)

Ask our Experts



QUESTION 13 UNATTEMPTED

You currently manage a set of web servers hosted on EC2 Servers with public IP addresses. These IP addresses are mapped to domain names. There was an urgent maintenance activity that had to be carried out on the servers and the servers had to be restarted. Now the web application hosted on these EC2 Instances is not accessible via the domain names configured earlier. Which of the following could be a reason for this.

- ☐ A. The Route53 hosted zone needs to be restarted.
- ☐ B. The network interfaces need to be initialized again.
- ☐ C. The public IP addresses need to be associated to the ENI again.
- ☒ D. The public IP addresses have changed after the instance was stopped and started ✓

Explanation :

Answer – D

By default the public IP address of an EC2 Instance is released after the instance is stopped and started. Hence the earlier IP address which were mapped to the domain names would have become invalid now.

For more information on public IP addressing, please visit the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-public-addresses>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-public-addresses>)

Ask our Experts



QUESTION 14 UNATTEMPTED

Which of the following features negates the need for you to manually enter VPN routes in your route table

- ☐ A. Peer Routing
- ☒ B. Route Propagation ✓
- ☐ C. Route Navigation
- ☐ D. Route Prepending

Explanation :

Answer - B

The AWS Documentation mentions the following on Route tables

Route propagation allows a virtual private gateway to automatically propagate routes to the route tables so that you don't need to manually enter VPN routes to your route tables. You can enable or disable route propagation.

For more information on Route Propagation, please visit the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#EnableDisableRouteProp
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#EnableDisableRouteProp)



Ask our Experts

QUESTION 15 UNATTEMPTED

Which of the following is true with regards to configuration of https for cloudfront with S3 as the origin. Choose 3 answers from the options given below.

- ☐ A. Even if an S3 bucket is configured as a website endpoint , https can be used between cloudfront and S3.
- ☐ B. CloudFront always forwards requests to S3 by using the protocol that viewers used to submit the requests ✓
- ☐ C. Amazon S3 provides the SSL/TLS certificate ✓
- ☐ D. If you want to require HTTPS for communication between CloudFront and Amazon S3, you must change the value of Viewer Protocol Policy to Redirect HTTP to HTTPS or HTTPS Only ✓

Explanation :

Answer – B,C and D

The AWS documentation provides the following information

Note the following about using HTTPS when the origin is an Amazon S3 bucket:

- If your Amazon S3 bucket is configured as a website endpoint, you can't configure CloudFront to use HTTPS to communicate with your origin because Amazon S3 doesn't support HTTPS connections in that configuration.
- Amazon S3 provides the SSL/TLS certificate, so you don't have to.

When your origin is an Amazon S3 bucket, CloudFront always forwards requests to S3 by using the protocol that viewers used to submit the requests

If you want to require HTTPS for communication between CloudFront and Amazon S3, you must change the value of Viewer Protocol Policy to Redirect HTTP to HTTPS or HTTPS Only.

For more information on using https with cloudfront as S3 as the origin, please visit the below URL:

- <http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-s3-origin.html>
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-s3-origin.html>)

Ask our Experts



QUESTION 16 UNATTEMPTED

Your company has the following Direct Connect and VPN Connections

Site A - VPN 10.1.0.0/24 AS 65000 65000

Site B - VPN 10.1.0.252/30 AS 65000

Site C - Direct Connect 10.0.0.0/8 AS 65000

Site D - Direct Connect 10.0.0.0/16 AS 65000 65000 65000

Which site will AWS choose to reach your network?

- ☐ A. Site A
- ☒ B. Site B ✓
- ☐ C. Site C
- ☐ D. Site D

Explanation :

Answer – B

AWS uses the most specific route in your route table that matches the traffic to determine how to route the traffic (longest prefix match). Hence the one that matches this is Site B.

For more information on route table priority, please visit the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-priority
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-priority)

Ask our Experts



QUESTION 17 UNATTEMPTED

You have 2 VPC's , VPC A and VPC B. Both the VPC's have been peered. You have configured the route tables in VPC A so that traffic can flow from VPCA to VPCB. You try to ping an instance in VPCB from VPCA , but are unable to do so. You have confirmed that the NACL's and Security Groups have been configured properly. What could be the reason for this issue?

- ☐ A. The VPC's have overlapping CIDR blocks
- ☐ B. Security Groups don't work in peered VPC's hence the requests will not work.
- ☐ C. NACL's don't work in peered VPC's hence the requests will not work.
- ☒ D. The route tables in VPCB have not been configured. ✓

Explanation :

Answer – D

The AWS Documentation mentions the following

To send traffic from your instance to an instance in a peer VPC using private IPv4 addresses, you must add a route to the route table that's associated with the subnet in which the instance resides. The route points to the CIDR block (or portion of the CIDR block) of the other VPC in the VPC peering connection.

The owner of the other VPC in the peering connection must also add a route to their subnet's route table to direct traffic back to your VPC.

For more information on VPC Peering routing, please visit the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-routing.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-routing.html>)

Ask our Experts



QUESTION 18 UNATTEMPTED

You have an EC2 Instance in a VPC which has 2 AZ's. The EC2 Instance has an ENI with a public and private IP address. The EC2 Instance is hosting a web server. This web server connects to a database RDS Instance. There is a backup web server available on another subnet. You have initiated a disaster recovery scenario and have moved the ENI on the original server to the backup server in the other subnet. But when you try to use the web application, it now seems that the web server cannot connect to the database server. Which of the following could be the underlying issue?

- ☐ A. The database server needs to get a new public IP to work with the ENI.
- ☐ B. The security group for the database is blocking the connection to the web server in the new subnet ✓
- ☐ C. The instance needs to be restarted so that it can start using the ENI
- ☐ D. It is not possible to move ENI's across subnets, hence the move operation would have failed.

Explanation :

Answer – B

When you move the ENI to a new subnet, the private IP of the ENI will change to reflect the IP range given from the CIDR block of the new subnet.

If you already had a Security Group that was allowing traffic from the original private IP of the ENI, this would not be in effect when the ENI is moved to the newer subnet.

Hence the Security Group for the database would ideally need to be modified to ensure the traffic can flow from the new web server to the database server.

For more information on Elastic Network interfaces, please refer to below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>)

Ask our Experts



QUESTION 19

UNATTEMPTED

You work for a company that has around 2,000 employees. There is a decision from senior management to start using AWS Workspaces. The data for the employees is already stored in the on-premise Active Directory. How can you ensure that authentication is applied in an effective manner, ensuring that the on-premise AD is used for authentication. Choose 2 answers from the options given below

- ☐ A. Deploy an AD Connector in AWS which will be used to connect to the on-premise AD ✓
- ☐ B. Deploy Hosted AD in AWS which will be used to connect to the on-premise AD
- ☐ C. Create a Direct Connect connection between the datacenter and AWS. ✓
- ☐ D. Create a VPN between the datacenter AWS and the on-premise environment.

Explanation :

Answer – A and C

The AWS Documentation mentions the following on AD Connectors

AD Connector is a directory gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory without caching any information in the cloud. AD Connector comes in two sizes, small and large. A small AD Connector is designed for smaller organizations of up to 500 users. A large AD Connector can support larger organizations of up to 5,000 users.

Once set up, AD Connector offers the following benefits:

- Your end users and IT administrators can use their existing corporate credentials to log on to AWS applications such as Amazon WorkSpaces, Amazon WorkDocs, or Amazon WorkMail.

For more information on the AD Connector, please refer to below URL:

- http://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html (http://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html)

For better performance and reliability consider using the Direct Connect Connection between AWS and the on-premise infrastructure.

For more information on Direct Connect, please refer to below URL:

- <https://aws.amazon.com/directconnect/> (<https://aws.amazon.com/directconnect/>)

Ask our Experts



QUESTION 20

UNATTEMPTED

You work for an organization that has a Direct Connect Connection and a backup VPN connection. This has been setup just recently. After setting it up, the traffic flow still prefers the VPN connection instead of the Direct connection. You have prepended a longer AS_PATH on the VPN connection , but even then this connection is being preferred. Which of the below steps can be used to ensure the Direct Connect connection is used.

- ☐ A. Remove the prepended AS_PATH.
- ☐ B. Reconfigure the VPN as a static VPN instead of dynamic.
- ☐ C. Increase the MED property on the VPN connection.
- ☒ D. Advertise a less specific prefix on the VPN connection ✓

Explanation :

Answer – D

It could be that the route being specified for the routing table is more specific for the VPN connection , hence this is being preferred.

The AWS Documentation clearly states that the most specific route in your route table that matches the traffic to determine how to route the traffic is used.

Hence it is better to ensure the VPN connection has a less specific route to ensure that it is not the preferred route which is taken.

For more information on Routing, please refer to below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-vgw
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-vgw)

Ask our Experts



QUESTION 21 UNATTEMPTED

Your company currently has a Link Aggregation Group to AWS with two 1Gbps connections. What is the best way to increase throughput on this Link Aggregation Group?

- ☐ A. Add one 10Gbps connections to the Link Aggregation Group
- ☐ B. Add two 10Gbps connections to the Link Aggregation Group
- ☒ C. Add two 1Gbps connections to the Link Aggregation Group ✓
- ☐ D. Add three 1Gbps connections to the Link Aggregation Group

Explanation :

Answer – C

As per the AWS documentation, the Link Aggregation Group has the following rules, hence only option C can be used in this instance

You can create a LAG from existing connections or provide new connections. After creating the LAG, you can assign existing connections (independent as well as connections that are part of another LAG).

The following rules apply:

- All connections in the LAG must have the same bandwidth. The following bandwidths are supported: 1 Gbit / s and 10 Gbit / s.
- A LAG can contain a maximum of 4 connections. Each link in the LAG must be considered individually for the overall connection limit for the region.
- All connections in the LAG must run at the same AWS DirectConnect endpoint.

For more information on Link Aggregation Group, please refer to below URL:

- <http://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html>
(<http://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html>)

Ask our Experts



QUESTION 22 UNATTEMPTED

Which of the following is a key pre-requisite required to ensure MFA can be used along with AWS Workspaces

- ☒ **A. A RADIUS Server deployed in the on-premise environment** ✓
- ☐ **B. An MFA Server deployed in the on-premise environment**
- ☐ **C. An MFA Server deployed in AWS**
- ☐ **D. An MFA Server deployed in AWS and in the on-premise environment**

Explanation :

Answer - A

To enable MFA for AWS services such as Amazon WorkSpaces and QuickSight, a key requirement is an MFA solution that is a Remote Authentication Dial-In User Service (RADIUS) server or a plugin to a RADIUS server already implemented in your on-premises infrastructure. RADIUS is an industry-standard client/server protocol that provides authentication, authorization, and accounting management to enable users to connect network services.

For more information on enabling MFA for AWS Workspaces, please refer to below URL:

- <https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/> (<https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/>)

Ask our Experts



You are configuring a Direct Connect Connection from AWS to your on-premise environment. You have configured a 1 GB Ethernet connection. You have verified with your AWS account manager and your colocation provider that everything is connected, and all of your information is correct. But the link is still not working as expected. Which of the following could be an issue?

- ☐ A. Your network supports BGP which is an issue.
- ☐ B. The connection must be 10 GB's or greater
- ☒ C. Auto Negotiation for the port is not disabled. ✓
- ☐ D. The connections have support for 802.1Q VLANs which is an issue

Explanation :

Answer - C

The AWS Documentation mentions the following requirements for AWS Direct Connect connections.

1. Connections to AWS Direct Connect require single mode fiber, 1000BASE-LX (1310nm) for 1 gigabit Ethernet, or 10GBASE-LR (1310nm) for 10 gigabit Ethernet.
2. Auto Negotiation for the port must be disabled.
3. You must support 802.1Q VLANs across these connections.
4. Your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication.

For more information on Direct Connect, please refer to below URL:

- <http://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf>
(<http://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf>)

Ask our Experts



Which of the following protocols are used for dynamically routed VPN Connections

- ☐ A. TCP
- ☐ B. UDP
- ☐ C. ICMP
- ☒ D. BGP ✓

Explanation :

Answer – D

The AWS Documentation mentions the following

Dynamically routed VPN connections use the Border Gateway Protocol (BGP) to exchange routing information between your customer gateways and the virtual private gateways. Statically routed VPN connections require you to enter static routes for the network on your side of the customer gateway. For more information on VPN Connections, please refer to below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts



QUESTION 25 UNATTEMPTED

Which of the following services can be used for monitoring VPN connections

- ☐ A. VPC Flow Logs
- ☐ B. AWS WAF
- ☐ C. AWS Config
- ☒ D. AWS Cloudwatch ✓

Explanation :

Answer - D

The AWS Documentation mentions the following

You can monitor VPN tunnels using CloudWatch, which collects and processes raw data from the VPN service into readable, near real-time metrics. These statistics are recorded for a period of 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. VPN metric data is automatically sent to CloudWatch as it becomes available.

For more information on monitoring VPN Connections, please refer to below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/monitoring-cloudwatch-vpn.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/monitoring-cloudwatch-vpn.html>)

Ask our Experts



QUESTION 26 UNATTEMPTED

Your company currently has a 100 Mbps line and needs to have a Direct Connect connection in place. How can the company achieve this?

- ☐ A. This is not possible with a 100 Mbps line.
- ☐ B. This is possible only if you upgrade to a 200 Mbps line
- ☐ C. This is possible only if you upgrade to a 500 Mbps line

☐ **D. You can contact an AWS Partner for this requirement** ✓

Explanation :

Answer - D

The AWS Documentation mentions the following

1Gbps and 10Gbps ports are available. Speeds of 50Mbps, 100Mbps, 200Mbps, 300Mbps, 400Mbps, and 500Mbps can be ordered from any APN partners supporting AWS Direct Connect.

For more information on AWS Direct Connect, please refer to below URL:

- <https://aws.amazon.com/directconnect/faqs/> (<https://aws.amazon.com/directconnect/faqs/>)

Ask our Experts



QUESTION 27 **UNATTEMPTED**

In Cloudfront what is the Origin Protocol policy that must be chosen to ensure that the communication with the origin is done either via http or https. Choose an answer from the options below

- ☐ **A. HTTP**
- ☐ **B. HTTPS**
- ☐ **C. Match Viewer** ✓
- ☐ **D. None of the above**

Explanation :

Answer – C

Its clearly given in the aws documentation that the Origin Protocol Policy should be set accordingly.

Origin Protocol Policy (Amazon EC2 and Other Custom Origins Only)

The protocol policy that you want CloudFront to use when fetching objects from your origin server.

Important

If your Amazon S3 bucket is configured as a website endpoint, you must specify HTTP Only. Amazon S3 doesn't support HTTPS connections in that configuration.

Choose the applicable value:

- **HTTP Only:** CloudFront uses only HTTP to access the origin.
- **HTTPS Only:** CloudFront uses only HTTPS to access the origin.
- **Match Viewer:** CloudFront communicates with your origin using HTTP or HTTPS, depending on the protocol of the viewer request. CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.

Important

For HTTPS viewer requests that CloudFront forwards to this origin, one of the domain names in the SSL certificate on your origin server must match the domain name that you specify for **Origin Domain Name**. Otherwise, CloudFront responds to the viewer requests with an HTTP status code 502 (Bad Gateway) instead of the requested object.

For more information, see [Requirements for Using SSL/TLS Certificates with CloudFront](#).

For more information on Cloudfront CDN please see the below link:

- <http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html>
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html>)

Ask our Experts



QUESTION 28 UNATTEMPTED

There are 2 company's that have their own AWS accounts. How can they connect to a central VPC for identity validation? How would you best design this solution? Choose an answer from the options below

- ☐ A. Migrate each VPC resources to the central VPC using migration tools such as Import/Export, Snapshot, AMI Copy, and S3 sharing.
- ☒ B. Create a VPC peering connection with the central VPC. ✓
- ☐ C. Create a Direct Connect connection from each VPC endpoint to the central VPC.
- ☐ D. Create an OpenVPN instance in central VPC and establish an IPSec tunnel between VPCs.

Explanation :

Answer – B

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. For more information on VPC Peering please see the below link:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>)

Ask our Experts



QUESTION 29 UNATTEMPTED

A legacy software is hosted on an EC2 instance which has the license tied to the MAC address. So from your experience with AWS you know that every time an instance is restarted it will almost certainly lose its MAC address. What would be a possible solution to this given the options below? Choose an answer from the options below

- ☐ A. Make sure any EC2 Instance that you deploy has a static IP address that is mapped to the MAC address.
- ☐ B. Use a VPC with a private subnet for the license and a public subnet for the EC2.
- ☐ C. Use a VPC with a private subnet and configure the MAC address to be tied to that subnet.
- ☒ D. Use a VPC with an elastic network interface that has a fixed MAC Address. ✓

Explanation :

Answer – D

There is a good example in the AWS documentation which supports option D.

Create a Low Budget High Availability Solution

If one of your instances serving a particular function fails, its network interface can be attached to a replacement or hot standby instance pre-configured for the same role in order to rapidly recover the service. For example, you can use a network interface as your primary or secondary network interface to a critical service such as a database instance or a NAT instance. If the instance fails, you (or more likely, the code running on your behalf) can attach the network interface to a hot standby instance. Because the interface maintains its private IP addresses, Elastic IP addresses, and MAC address, network traffic begins flowing to the standby instance as soon as you attach the network interface to the replacement instance. Users experience a brief loss of connectivity between the time the instance fails and the time that the network interface is attached to the standby instance, but no changes to the VPC route table or your DNS server are required.

For more information on elastic network interfaces please visit the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>)



QUESTION 30 UNATTEMPTED

Your company has just set up a new document server on its AWS VPC, and it has four very important clients that it wants to give access to. These clients also have VPCs on AWS and it is through these VPCs that they will be given accessibility to the document server. In addition, each of the clients should not have access to any of the other clients' VPCs. Choose the correct answer from the options below

- ☒ **A. Set up VPC peering between your company's VPC and each of the clients' VPCs.**
✓
- ☐ **B. Set up VPC peering between your company's VPC and each of the clients' VPCs, but block the IPs from CIDR of the clients' VPCs to deny them access to each other.**
- ☐ **C. Set up VPC peering between your company's VPC and each of the clients' VPC. Each client should have VPC peering set up between each other to speed up access time.**
- ☐ **D. Set up all the VPCs with the same CIDR but have your company's VPC as a centralized VPC.**

Explanation :

Answer – A

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. There is no need to setup client VPC peering between each other because this is a clear requirement in the question, hence option C is wrong.

There is no need to block IP's hence Option B is wrong.

VPC peering needs to have the basic functionality that the CIDR's should not overlap, hence option D is wrong.

For more information on VPC Peering please see the below link:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>)



QUESTION 31 UNATTEMPTED

Your company has an AWS Direct Connect connection from a VPC to an on-premise location. Which of the following can be used as a backup incase the Direct Connect connection fails for any reason. Choose 2 answers from the options given below

- ☐ A. There is no need to configure this as AWS will fall back to a secondary Direct Connect connection as per their SLA.
- ☐ B. Setup a secondary Direct Connect connection. ✓
- ☐ C. Setup a VPN connection ✓
- ☐ D. Setup a peering connection

Explanation :

Answer – B and C

The AWS Documentation mentions the following

If you have established a second AWS Direct Connect connection, traffic will failover to the second link automatically. We recommend enabling Bidirectional Forwarding Detection (BFD) when configuring your connections to ensure fast detection and failover. If you have configured a back-up IPsec VPN connection instead, all VPC traffic will failover to the VPN connection automatically. Traffic to/from public resources such as Amazon S3 will be routed over the Internet.

For more information on Direct Connect please see the below link:

- <https://aws.amazon.com/directconnect/faqs/> (<https://aws.amazon.com/directconnect/faqs/>)

Ask our Experts



QUESTION 32 UNATTEMPTED

Which of the following are configuration recommendations when configuring high availability for VPN connections to AWS? Choose 2 answers from the options given below

- ☐ A. Configure redundant customer gateways ✓
- ☐ B. Configure static routing
- ☐ C. Configure dynamic routing ✓
- ☐ D. Configure Direct Connect

Explanation :

Answer – A and C

The AWS Documentation mentions the following

Many AWS customers choose to implement VPN connections because they can be a quick, easy, and cost-effective way to set up remote connectivity to a VPC. To enable redundancy, each AWS Virtual Private Gateway (VGW) has two VPN endpoints (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#VPNTunnels) with capabilities for static and dynamic routing. Although statically routed VPN connections from a single customer gateway are sufficient for establishing remote connectivity to a VPC, this is not a highly available configuration. The best practice for making VPN connections highly available is to use redundant customer gateways and dynamic routing for automatic failover between AWS and customer VPN endpoints.

For more information on high availability for network connections please see the below link:

- <https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/> (<https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/>)

Ask our Experts



QUESTION 33 UNATTEMPTED

You have 2 VPN connections established between AWS and your on-premise location. You need to ensure that one VPN is preferred over the other.

Which of the following configurations can allow you to do this?

- ☒ A. Use more specific routes ✓
- ☐ B. Use less specific routes
- ☐ C. Use AS-path prepending
- ☐ D. Use BGP priority

Explanation :

Answer - A

The AWS Documentation mentions the following

AWS will use the more specific routes to send traffic to the appropriate data center, and will fail back to the other data center following the summarized route if the more specific route becomes temporarily unavailable.

For more information on high availability for network connections please see the below link:

- <https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/> (<https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/>)

Ask our Experts



QUESTION 34 UNATTEMPTED

How is it possible to ensure that the same set of nameservers can be used for multiple hosted zones in Route53?

- ☐ A. This is not possible
- ☒ B. In the API, create a Reusable Delegation Set. ✓
- ☐ C. In the console, create a Reusable Delegation Set.
- ☐ D. Import the domain in Route53

Explanation :

Answer – B

The AWS Documentation mentions the following

Creates a delegation set (a group of four name servers) that can be reused by multiple hosted zones. If a hosted zone ID is specified, CreateReusableDelegationSet marks the delegation set associated with that zone as reusable

For more information on CreateReusableDelegationSet please see the below link:

- http://docs.aws.amazon.com/Route53/latest/APIReference/API_CreateReusableDelegationSet.html (http://docs.aws.amazon.com/Route53/latest/APIReference/API_CreateReusableDelegationSet.html)

Ask our Experts



QUESTION 35 UNATTEMPTED

When you create a subnet, you specify the CIDR block for the subnet. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset (to enable multiple subnets). The allowed block size is between a /28 netmask and /16 netmask. You decide to you create a VPC with CIDR block 10.0.0.0/24. Therefore what is the maximum allowed number of IP addresses and the minimum allowed number of IP addresses according to AWS and what is the number of IP addresses supported by the VPC you created? Choose the correct answer from the options below

- ☐ **A. Maximum is 28 and the minimum is 16 and the one created supports 24 IP addresses**
- ☐ **B. Maximum is 256 and the minimum is 16 and the one created supports 24 IP addresses**
- ☐ **C. Maximum is 65,536 and the minimum is 24 and the one created supports 28 IP addresses**
- ☐ **D. Maximum is 65,536 and the minimum is 16 and the one created supports 256 IP addresses ✓**

Explanation :

Answer – D

This is clearly given in the aws documentation

VPC and Subnet Sizing for IPv4

You can assign a single CIDR block to a VPC. The allowed block size is between a /16 netmask and /28 netmask. In other words, the VPC can contain from 16 to 65,536 IP addresses.

For more information on VPC and subnets please see the below link:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Ask our Experts



QUESTION 36 UNATTEMPTED

Your company needs an inexpensive solution to host their AD data in the cloud. They do not need all of the features of AD but do need to be able to use it with WorkSpaces. Which of the following is the best recommended solution

- ☐ A. Use Hosted Microsoft AD
- ☒ B. Use the Simple AD service ✓
- ☐ C. Use the AD Connector
- ☐ D. Deploy an AD server on a large EC2 instance

Explanation :

Answer – B

The AWS documentation mentions the following on Simple AD

Simple AD provides a subset of the features offered by Microsoft AD, including the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO).

For more information on Simple AD please see the below link:

- http://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html
(http://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html)

Ask our Experts



QUESTION 37 UNATTEMPTED

You have created a VPC with CIDR block 10.0.0.0/24, which supports 256 IP addresses. You want to now split this into two subnets, each supporting 128 IP addresses. Can this be done and if so how will the allocation of IP addresses be configured? Choose the correct answer from the options below

- ☐ A. One subnet will use CIDR block 10.0.0.0/127 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/255 (for addresses 10.0.0.128 - 10.0.0.255).
- ☐ B. One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.1.0/25 (for addresses 10.0.1.0 - 10.0.1.127).

- ☐ C. One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255). ✓
- ☐ D. This is not possible.

Explanation :

Answer – C

This is clearly given in the aws documentation

For example, if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).

For more information on VPC and subnets please see the below link:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Ask our Experts



QUESTION 38 UNATTEMPTED

A company is building an AWS Cloud Environment for a financial regulatory firm. Part of the requirements are being able to monitor all changes in an environment and all traffic sent to and from the environment. What suggestions would you make to ensure all the requirements for monitoring the financial architecture are satisfied? Choose the 2 correct answers from the options below

- ☐ A. Configure an IPS/IDS in promiscuous mode, which will listen to all packet traffic and API changes.
- ☐ B. Configure an IPS/IDS system, such as Palo Alto Networks, using promiscuous mode that monitors, filters, and alerts of all potential hazard traffic leaving the VPC.
- ☐ C. Configure an IPS/IDS to listen and block all suspected bad traffic coming into and out of the VPC. Configure CloudTrail with CloudWatch Logs to monitor all changes within an environment. ✓
- ☐ D. Configure an IPS/IDS system, such as Palo Alto Networks, that monitors, filters, and alerts of all potential hazard traffic leaving the VPC. ✓

Explanation :

Answer – C and D

Promiscuous mode is not supported in AWS hence the options of A and B are automatically out.

Please find the below developer forums thread on the same.

- <https://forums.aws.amazon.com/thread.jspa?threadID=35683>
(<https://forums.aws.amazon.com/thread.jspa?threadID=35683>)

Please find the below URL: to a good slide deck from AWS for getting IDS in place.

- <https://awsmedia.s3.amazonaws.com/SEC402.pdf>
(<https://awsmedia.s3.amazonaws.com/SEC402.pdf>)

Ask our Experts



QUESTION 39 UNATTEMPTED

You currently have 9 EC2 instances running in a Placement Group. All these 9 instances were initially launched at the same time and seem to be performing as expected. You decide that you need to add 2 new instances to the group; however, when you attempt to do this you receive a 'capacity error'. Which of the following actions will most likely fix this problem? Choose the correct answer from the options below

- ☐ A. Make a new Placement Group and launch the new instances in the new group. Make sure the Placement Groups are in the same subnet.
- ☒ B. Stop and restart the instances in the Placement Group and then try the launch again. ✓
- ☐ C. Request a capacity increase from AWS as you are initially limited to 10 instances per Placement Group.
- ☐ D. Make sure all the instances are the same size and then try the launch again.

Explanation :

Answer – B

AWS recommends to try and launch the instances again

Error: InsufficientInstanceCapacity

If you get an `InsufficientInstanceCapacity` error when you try to launch an instance or start a stopped instance, AWS does not currently have enough available capacity to service your request. Try the following:

- Wait a few minutes and then submit your request again; capacity can shift frequently.
- Submit a new request with a reduced number of instances. For example, if you're making a single request to launch 15 instances, try making 3 requests for 5 instances, or 15 requests for 1 instance instead.
- If you're launching an instance, submit a new request without specifying an Availability Zone.
- If you're launching an instance, submit a new request using a different instance type (which you can resize at a later stage). For more information, see [Resizing Your Instance](#).
- Try purchasing Reserved Instances. Reserved Instances are a long-term capacity reservation. For more information, see: [Amazon EC2 Reserved Instances](#).

For more information on this error , just browse to the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-capacity.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-capacity.html>)

Ask our Experts



QUESTION 40 UNATTEMPTED

A company is running data application on-premise that requires large amounts of data to be transferred to a VPC containing EC2 instances in an AWS region. The company is concerned about the total overall transfer costs required for this application and is potentially not going to deploy a hybrid environment for the customer-facing part of the application to run in a VPC. Given that the data transferred to AWS is new data every time, what suggestions could you make to the company to help reduce the overall cost of data transfer to AWS? Choose the correct answer from the options below

- ☐ A. Provision a VPN connection between the on-premise data center and the AWS region using the VPN section of a VPC.
- ☐ B. Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region. ✓
- ☐ C. Suggest using AWS import/export to transfer the TBs of data while synchronizing the new data as it arrives
- ☐ D. Suggest leaving the data required for the application on-premise and use a VPN to query the on-premise database data from EC2 when required.

Explanation :

Answer – B

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

For more information on AWS direct connect, just browse to the below URL:

- <https://aws.amazon.com/directconnect/> (<https://aws.amazon.com/directconnect/>)

Ask our Experts



QUESTION 41 UNATTEMPTED

Your company has an EC2 Instance hosted in AWS. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring? Which one of the below steps can help address this issue.

- ☐ A. Use the VPC Flow Logs.
- ☐ B. Use a network monitoring tool provided by an AWS partner. ✓
- ☐ C. Use another instance. Setup a port to “promiscuous mode” and sniff the traffic to analyze the packets.
- ☐ D. Use Cloudwatch metric

Explanation :

Answer - B

Since here you need to sniff the actual network packets , the ideal approach would be to use a network monitoring tool provided by an AWS partner.

The AWS documentation mentions the following

Multiple AWS Partner Network members offer virtual firewall appliances that can be deployed as an in-line gateway for inbound or outbound network traffic. Firewall appliances provide additional application-level filtering, deep packet inspection, IPS/IDS, and network threat protection features.

For more information on the security capabilities, please visit the below URL:

- <https://aws.amazon.com/answers/networking/vpc-security-capabilities/>
(<https://aws.amazon.com/answers/networking/vpc-security-capabilities/>)

Ask our Experts



QUESTION 42 UNATTEMPTED

There are currently 3 VPC's.

VPC A - CIDR Block - 10.111.0.0/16

There are 14 servers in this VPC in the range 10.111.2.101 – 10.111.2.114

VPC B - CIDR Block - 10.111.2.0/24

There are 16 servers in this VPC in the range 10.111.2.120 – 10.111.2.136

VPC C - 172.31.0.0/16

You need to access VPC A and VPC B from VPC C. How can you achieve this? Choose 2 answers from the options below

- ☐ A. From VPC C, create a peering connection and add a route to VPC A's peering connection for 10.111.2.96/28
- ☐ B. From VPC C, create a peering connection and add a route to VPC A's peering connection for 10.111.2.96/27 ✓
- ☐ C. From VPC C, create a peering connection and add a route to VPC B's peering connection for 10.111.2.0/24. ✓

- ☐ **D. Change the CIDR block of VPC B since this would overlap and hence you would not be able to peer the VPC's**

Explanation :

Answer - B and C

Again here if you use the CIDR calculator, if you add a more specific route of 10.111.2.96/27 for VPC A and 10.111.2.0/24 for VPC B, this would work.

Also note that VPC Peering would be possible from VPC C to VPC B and from VPC C to VPC A

For more information on VPC Peering, please visit the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.html>)

Ask our Experts



QUESTION 43 UNATTEMPTED

Which of the commands can be used to list the metrics for Direct Connect connections in AWS

- ☐ **A. AWS cloudwatch list-metrics --namespace "AWS/Direct"**
- ☐ **B. AWS cloudwatch list-metrics --namespace "AWS/DirectConnect"**
- ☐ **C. AWS cloudwatch list-metrics --namespace "AWS/DC"**
- ☐ **D. AWS cloudwatch list-metrics --namespace "AWS/DX" ✓**

Explanation :

Answer – D

This is given in the AWS documentation

To view metrics using the AWS CLI

- At a command prompt, use the following command:

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```



The following metrics are available from AWS Direct Connect. Metrics are currently available for AWS Direct Connect physical connections only.

For more information on monitoring Direct Connect connections, please visit the below URL:

- <http://docs.aws.amazon.com/directconnect/latest/UserGuide/monitoring-cloudwatch.html>
(<http://docs.aws.amazon.com/directconnect/latest/UserGuide/monitoring-cloudwatch.html>)

Ask our Experts



QUESTION 44 UNATTEMPTED

Which of the following statements on NAT gateways is incorrect?

- ☐ A. A NAT gateway supports bursts of up to 10 Gbps of bandwidth
- ☐ B. You can associate exactly one Elastic IP address with a NAT gateway
- ☒ C. You can associate a security group with a NAT gateway. ✓
- ☐ D. A NAT gateway supports the TCP and UDP protocol

Explanation :

Answer - C

The AWS documentation mentions the following on NAT gateways

A NAT gateway has the following characteristics:

- A NAT gateway supports bursts of up to 10 Gbps of bandwidth. If you require more than 10 Gbps bursts, you can distribute the workload by splitting your resources into multiple subnets, and creating a NAT gateway in each subnet.
- You can associate exactly one Elastic IP address with a NAT gateway. You cannot disassociate an Elastic IP address from a NAT gateway after it's created. To use a different Elastic IP address for your NAT gateway, you must create a new NAT gateway with the required address, update your route tables, and then delete the existing NAT gateway if it's no longer required.
- A NAT gateway supports the following protocols: TCP, UDP, and ICMP.
- You cannot associate a security group with a NAT gateway. You can use security groups for your instances in the private subnets to control the traffic to and from those instances.

For more information on NAT gateways, please visit the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html>)

Ask our Experts



QUESTION 45 UNATTEMPTED

Which of the following can be used to ensure that resources from the internet cannot initiate an IPv6 connection to instances in your public subnet

- ☐ A. Internet gateway
- ☒ B. egress-only Internet gateway ✓
- ☐ C. ingress-only Internet gateway
- ☐ D. NAT gateway

Explanation :

Answer - B

The AWS documentation mentions the following on egress-only Internet gateway

An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet, and prevents the Internet from initiating an IPv6 connection with your instances.

For more information on egress-only Internet gateway, please visit the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/egress-only-internet-gateway.html> (<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/egress-only-internet-gateway.html>)

Ask our Experts



QUESTION 46 UNATTEMPTED

Your company currently has 5 EC2 Instances that use Instance store volumes. The Instances have been placed in the stopped state for a week now. But you notice that you are still being charged for AWS EC2 service. Which of the following could be a possible reason for this?

- ☐ A. Instances in stopped state still incur a charge within AWS.
- ☐ B. Instance store Instances incur a charge no matter which state they are in
- ☐ C. You are being charged for the EBS volumes.
- ☒ D. You have Elastic IPs associated with those instances. ✓

Explanation :

Answer – D

The AWS documentation mentions the following on Elastic IP addresses

An Elastic IP address doesn't incur charges as long as the following conditions are true:

- The Elastic IP address is associated with an Amazon EC2 instance.
- The instance associated with the Elastic IP address is running.
- The instance has only one Elastic IP address attached to it.

If you've stopped or terminated an EC2 instance with an associated Elastic IP address and you don't need that Elastic IP address any more, consider disassociating or releasing the Elastic IP address. Hence the most feasible reason will be that there were Elastic IP's associated with these instances.

For more information, please visit the below URL:

- <https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/> (<https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/>)

Ask our Experts



QUESTION 47

UNATTEMPTED

You need to find the subnet, the security group and the VPC that your instance is associated with. Which of the following would be part of the set of commands that you would use first.

- ☐ A. AWS vpc describe-all
- ☐ B. AWS ec2 describe-security-groups
- ☒ C. AWS ec2 describe-instances ✓
- ☐ D. AWS ec2 describe-network-acl

Explanation :

Answer - C

This command will give you the entire details about your instance which includes the subnet, VPC and security group associated with your instance

For more information on the command, please visit the below URL:

- <http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html>
(<http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html>)

Ask our Experts



QUESTION 48

UNATTEMPTED

Which of the following is the most recommended encryption standard used for a VPN connection in AWS.

- ☐ A. Twofish
- ☒ B. AES ✓
- ☐ C. Blowfish
- ☐ D. TripleDES

Explanation :

Answer – B

Note that in the AWS Documentation, when you look at the configuration of a VPN connection, below are the minimum and recommended encryption protocols.

Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2. You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups.

For more information on this, please visit the below URL:

- <https://aws.amazon.com/vpc/faqs/> (<https://aws.amazon.com/vpc/faqs/>)

Ask our Experts



QUESTION 49 UNATTEMPTED

You want to ensure you have the absolute best transmission rates for an EC2 Instance both inside and outside of the VPC. Which of the following would help fulfil this requirement. Choose 2 answers from the options given below

- ☐ A. Configure an ENI for the instance for both internal and external traffic
- ☐ B. Configure two ENI's for the instance, one for internal traffic and the other for external traffic ✓
- ☐ C. Configure the single ENI for an MTU transmission rate of 9001
- ☐ D. Configure the external ENI with an MTU of 1500 and the internal ENI with an MTU of 9001 ✓

Explanation :

Answer - B and D

Ethernet frames can come in different formats, and the most common format is the standard Ethernet v2 frame format. It supports 1500 MTU, which is the largest Ethernet packet size supported over most of the Internet.

Most Instance types also support an MTU of 9001 which can be used for internal VPC communication. For more information on Network MTU settings, please visit the below URL:

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html)

Ask our Experts



QUESTION 50 UNATTEMPTED

Which of the following features on AWS Direct Connect can assist to provide faster failure detection times.

- ☐ A. Peering
- ☐ B. BFD ✓
- ☐ C. BGP

☐ D. VPN

Explanation :

Answer - B

The AWS documentation mentions the following on BFD

Bidirectional Forwarding Detection (BFD) is a network fault detection protocol that provides fast failure detection times, which facilitates faster re-convergence time for dynamic routing protocols. It is independent of media, routing protocol, and data. We recommend enabling BFD when configuring multiple AWS Direct Connect connections or when configuring a single AWS Direct Connect connection and a VPN connection as a back up to ensure fast detection and failover. You can configure BFD to detect link or path failures and update dynamic routing as Direct Connect quickly terminates BGP peering so that backup routes can kick in. This ensures that the Bidirectional Forwarding Detection (BGP) neighbor relationship is quickly torn down instead of waiting for 3 keep-alives to fail at a hold-down time of 90sec.

For more information on Bidirectional Forwarding Detection, please visit the below URL:

- <https://aws.amazon.com/premiumsupport/knowledge-center/enable-bfd-direct-connect/> (<https://aws.amazon.com/premiumsupport/knowledge-center/enable-bfd-direct-connect/>)

Ask our Experts



QUESTION 51 UNATTEMPTED

Your company has just launched an application that uses Cloudfront to serve image content which is stored in S3. But after the deployment, it is noticed that the images are not appearing on the web page. You have verified that the Cloudfront service is configured to use your domain name which is `cdn.demo.com`. Which of the following could be a likely reason for this issue?

- ☐ A. A policy has not been set for shared access to the bucket
- ☐ B. Use Elastic Cache to serve images instead of S3
- ☐ C. There is no record in Route 53 pointing to `cdn.demo.com` as the ALIAS ✓
- ☐ D. There is no host record created in Route53 pointing to `cdn.demo.com`

Explanation :

Answer - C

The AWS Documentation mentions the following which should be followed when using a Cloudfront distribution with your own domain name

If you want to use your own domain name, use Amazon Route 53 to create an alias resource record set (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>) that points to your CloudFront distribution. An alias resource record set is an Amazon Route 53 extension to DNS. It's similar to a CNAME resource record set, but you can create an alias resource record set both for the root domain, such as `example.com`, and for subdomains, such as `www.example.com` (<http://www.example.com>)

For more information on Cloudfront distribution and Route53, please refer to below URL:

- <http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html> (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>)

Ask our Experts



QUESTION 52 UNATTEMPTED

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below

- ☐ A. Amazon Cloudwatch Logs ✓
- ☐ B. Amazon VPC Flow Logs
- ☐ C. Amazon AWS Config
- ☐ D. Amazon Cloudtrail ✓

Explanation :

Answer – A and D

The AWS Documentation mentions the following about these services

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

For more information on Cloudtrail, please refer to below URL:

- <https://aws.amazon.com/cloudtrail/> (<https://aws.amazon.com/cloudtrail/>)

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.

For more information on Cloudwatch logs, please refer to below URL:

- <http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html> (<http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>)

Ask our Experts



QUESTION 53 UNATTEMPTED

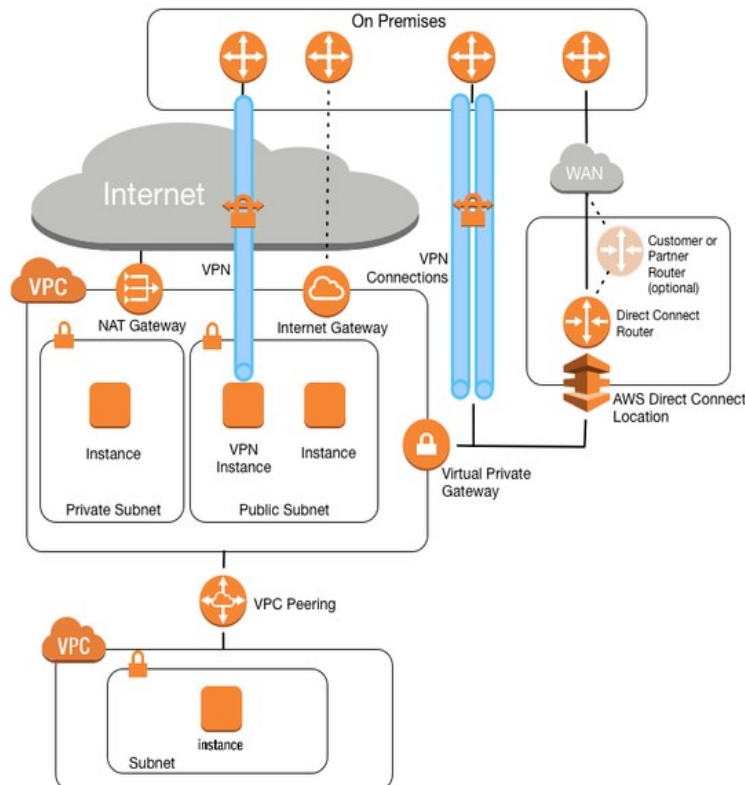
A new client may use your company to move all their existing Data Center applications and infrastructure to AWS. This is going to be a huge contract for your company, and you have been handed the entire contract and need to provide an initial scope to this possible new client. One of the things you notice concerning the existing infrastructure is that it has a small amount of legacy applications that you are almost certain will not work on AWS. Which of the following would be the best strategy to employ regarding the migration of these legacy applications? Choose the correct answer from the options below

- ☐ A. Create two VPCs. One containing all the legacy applications and the other containing all the other applications. Make a connection between them with VPC peering.
- ☐ B. Move the legacy applications onto AWS first, before you build any infrastructure. There is sure to be an AWS Machine Image that can run this legacy application.
- ☐ C. Create a hybrid cloud by configuring a VPN tunnel to the on-premises location of the Data Center ✓
- ☐ D. Convince the client to look for another solution by de-commissioning these applications and seeking out new ones that will run on AWS.

Explanation :

Answer – C

The best option is to have a dual mode wherein you have the legacy apps running on-premise and start migrating the apps which have compatibility in the cloud. Have a VPN connection from the on-premise to the cloud for ensuring communication can happen from each environment to the other.



For the full fundamentals on aws networking options, please visit the URL:

- <https://aws.amazon.com/blogs/apn/amazon-vpc-for-on-premises-network-engineers-part-one/> (<https://aws.amazon.com/blogs/apn/amazon-vpc-for-on-premises-network-engineers-part-one/>)

Ask our Experts



QUESTION 54 UNATTEMPTED

If one needs to establish a low latency dedicated connection to an S3 public endpoint over the Direct Connect dedicated low latency connection, what steps need to be taken to accomplish configuring a direct connection to a public S3 endpoint? Choose the correct answer from the options below

- ☒ **A. Configure a public virtual interface to connect to a public S3 endpoint resource.**
✓
- ☐ **B. Establish a VPN connection from the VPC to the public S3 endpoint.**
- ☐ **C. Configure a private virtual interface to connect to the public S3 endpoint via the Direct Connect connection.**
- ☐ **D. Add a BGP route as part of the on-premise router; this will route S3 related traffic to the public S3 endpoint to dedicated AWS region.**

Explanation :

Answer – A

You can create a public virtual interface to connect to public resources, or a private virtual interface to connect to your VPC. You can configure multiple virtual interfaces on a single AWS Direct Connect connection, and you'll need one private virtual interface for each VPC to connect to. Each virtual interface needs a VLAN ID, interface IP address, ASN, and BGP key.

For more information on virtual interfaces, please visit the below URL:

- <http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html> (<http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html>)

Ask our Experts



QUESTION 55 UNATTEMPTED

You're working as a consultant for a company that has a three tier application. The application layer of this architecture sends over 20Gbps of data per seconds during peak hours to and from Amazon S3. Currently, you're running two NAT gateways in two subnets to transfer the data from your private application layer to Amazon S3.

You will also need to ensure that the instances receive software patches from a third party repository. What architecture changes should be made, if any? Choose the correct answer from the options below.

- ☐ A. NAT gateways support 10Gbps and two are running: Add a third to a third subnet to allow for any increase in demand.
- ☐ B. Keep the NAT gateway and create a VPC S3 endpoint which allows for higher bandwidth throughput as well as tighter security. ✓
- ☐ C. NAT gateways support 10Gbps and two are running: No changes are required to improve this architecture.
- ☐ D. Remove the NAT gateway and create a VPC S3 endpoint which allows for higher bandwidth throughput as well as tighter security.

Explanation :

Answer – B

VPC endpoints alleviate the need for everything to go through the NAT instance

New VPC Endpoint for S3

Today we are simplifying access to S3 resources from within a VPC by introducing the concept of a VPC Endpoint. These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances.

EC2 instances running in private subnets of a VPC can now have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets.

For more information on VPC endpoints please refer to the below URL:

- <https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/>
(<https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/>)

Ask our Experts



QUESTION 56 UNATTEMPTED

Which of the following is incorrect when it comes to public IP addressing in AWS

- ☐ A. A public IP address is assigned from Amazon's pool of public IP addresses
- ☐ B. When an IP is disassociated from the instance, it is added back to the pool
- ☐ C. The Public IP allows the instance to be reachable from the internet
- ☐ D. You can manually associate or disassociate a public IP address ✓

Explanation :

Answer - D

The AWS documentation mentions the following on public IP addressing

A public IP address is assigned from Amazon's pool of public IP addresses; it's not associated with your account. When a public IP address is disassociated from your instance, it's released back into the pool, and is no longer available for you to use. You cannot manually associate or disassociate a public IP address.

For more information on IP addressing please refer to the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html>)

Ask our Experts



QUESTION 57 UNATTEMPTED

You have configured a dynamic VPN between your datacenter and your VPC. But you are not able to see the routes for the connection. What could be the possible reason for this?

- ☐ A. The NACL's are not configured properly
- ☐ B. The internal firewall is blocking the routes
- ☒ C. The route propagation is not set in the Route table ✓
- ☐ D. You have not set BFD for the connection

Explanation :

Answer - C

For routes to be dynamically setup , you needed to have route propagation setup on your routing table

The AWS documentation in addition mentions the following

If you've attached a virtual private gateway to your VPC and enabled route propagation on your route table, routes representing your VPN connection automatically appear as propagated routes in your route table

For more information on Route tables please refer to the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)

Ask our Experts



QUESTION 58 UNATTEMPTED

Your company has asked you to connect their on-premise environment to AWS. The traffic must be encrypted and reliability should be ensured. There is a requirement to access S3 resources in AWS from the on-premise environment. Which of the below ways can be used to fulfil this requirement. Choose 2 answers from the options given below

- ☐ A. Create a VPN connection ✓
- ☐ B. Create a Direct Connect connection with a private virtual interface
- ☐ C. Create a Direct Connect connection with a hosted virtual interface
- ☐ D. Create a Direct Connect connection with a public virtual interface ✓

Explanation :

Answer - A and D

The AWS documentation mentions the following

You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a *virtual private gateway* provides two VPN endpoints (tunnels) for automatic failover. You configure your *customer gateway* on the remote side of the VPN connection. You must create a virtual interface to begin using your AWS Direct Connect connection. You can create a private virtual interface to connect to your VPC, or you can create a public virtual interface to connect to AWS services that aren't in a VPC, such as Amazon S3 and Amazon Glacier. You can configure multiple virtual interfaces on a single AWS Direct Connect connection

For more information on VPN connections please refer to the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>)

For more information on Virtual interfaces please refer to the below URL:

- <http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html>
(<http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html>)

Ask our Experts



QUESTION 59 UNATTEMPTED

There is a requirement to ensure optimal performance for instances that are launched in two VPC's have that been peered? Which of the below are two steps that can be taken to achieve this.

- ☐ A. Ensure the instances are launched in subnets in different AZ's and create a placement group.
- ☐ B. Ensure the instances are launched in subnets in the same AZ and create a placement group. ✓

- ☐ C. Ensure that the instance type support enhanced networking ✓
- ☐ D. Ensure the MTU for the ENI is set to 1500 for the instances

Explanation :

Answer - B and C

The AWS documentation mentions the following on placement groups

A *placement group* is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking

For more information on placement groups please refer to the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>)

Ask our Experts



QUESTION 60 UNATTEMPTED

When connecting your VPC to remote networks via VPN, what are some of the options available to you. Choose 3 answers from the options given below

- ☐ A. AWS Managed VPN ✓
- ☐ B. VPC Peering
- ☐ C. AWS VPN CloudHub ✓
- ☐ D. Third party software VPN appliance ✓

Explanation :

Answer – A,C and D

The AWS documentation mentions the following on the type of VPN connections

1. AWS Managed VPN - You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a *virtual private gateway* provides two VPN endpoints (tunnels) for automatic failover. You configure your *customer gateway* on the remote side of the VPN connection.
2. AWS VPN Cloudhub - If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks
3. Third party software VPN appliance - You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open source communities.

For more information on VPN connections please refer to the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>)

Ask our Experts



QUESTION 61 UNATTEMPTED

Your company has a web server hosted on an EC2 Instance. This is being used along with the AWS Application Load Balancer, Cloudfront and S3. There is a requirement to get the IP addresses accessing the web site. How can this be managed if no access has been provided to the AWS console or the API.

- ☐ A. Use the local metadata on the server to access the logs
- ☐ B. The access logs should already have this information
- ☒ C. Add "X-Forwarded For" to the access logs and view the access logs ✓
- ☐ D. Convert the Application Load balancer to a classic load balancer

Explanation :

Answer – C

The AWS documentation mentions the following on X-Forwarded headers

The X-Forwarded-For request header helps you identify the IP address of a client when you use an HTTP or HTTPS load balancer. Because load balancers intercept traffic between clients and servers, your server access logs contain only the IP address of the load balancer. To see the IP address of the client, use the X-Forwarded-For request header. Elastic Load Balancing stores the IP address of the client in the X-Forwarded-For request header and passes the header to your server.

For more information on X-Forwarded headers please refer to the below URL:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html>
(<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html>)

Ask our Experts



QUESTION 62 UNATTEMPTED

An Elastic Load balancer has just been setup with the following settings

HealthCheck Interval - 5 seconds

Healthy threshold -5

UnHealthy threshold -6

How long will an instance take to become healthy with the above settings?

- ☐ A. 30 seconds

- ☐ B. 5 seconds
- ☐ C. 60 seconds
- ☐ D. 25 seconds ✓

Explanation :

Answer – D

If the instance checks pass through and the all ELB health pings work, then the Instance would be marked as healthy after HealthCheck Interval* Healthy threshold time interval.

For more information on configuring health checks for the ELB please refer to the below URL:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>
(<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>)

Ask our Experts



QUESTION 63 UNATTEMPTED

Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below

- ☐ A. AWS Cloudfront ✓
- ☐ B. AWS Lambda
- ☐ C. AWS Application Load Balancer ✓
- ☐ D. AWS Classic Load Balancer

Explanation :

Answer – A and C

The AWS documentation mentions the following on the Application Load Balancer

AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it can be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.

For more information on the web application firewall please refer to the below URL:

- <https://aws.amazon.com/waf/faq/> (<https://aws.amazon.com/waf/faq/>)

Ask our Experts



QUESTION 64 UNATTEMPTED

Your website utilizes EC2, S3, ELB-Classical, and CloudFront. How can you implement the right security measures for this configuration? Choose 2 answers from the options given below

- ☐ A. An NACL that blocks all ports to your subnets.
- ☒ B. A restricted bucket policy on S3 ✓
- ☒ C. A WAF on your CloudFront distribution. ✓
- ☐ D. A WAF on the load balancer.

Explanation :

Answer - B and C

The NACL would not be the right approach to block all ports , because then the application hosted on the instances in the subnet might not work with this approach.

WAF are supported on the Application Load Balancer and not the classic load balancer

For more information on the web application firewall please refer to the below URL:

- <https://aws.amazon.com/waf/faq/> (<https://aws.amazon.com/waf/faq/>)

For more information on bucket policies please refer to the below URL:

- <http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>)

Ask our Experts



QUESTION 65 UNATTEMPTED

There are 3 VPC's that need instances to be able to pass traffic between each other. How can this be achieved.

- ☐ A. Peer the VPC's , transitive peering is now allowed in AWS
- ☐ B. Peer the VPC's and then Contact AWS support to enable transitive peering
- ☒ C. Peer the VPC's to each other in a full mesh configuration. ✓
- ☐ D. Peer the VPC's , enable transitive peering via the route tables

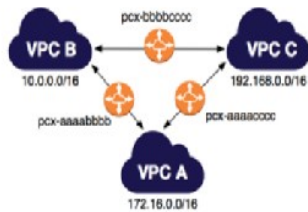
Explanation :

Answer - C

This is clearly given in the AWS documentation

You have peered three VPCs together in a full mesh configuration. The VPCs are in the same AWS account and do not have overlapping CIDR blocks:

- VPC A is peered to VPC B through VPC peering connection `p-cx-aaaabbbb`
- VPC A is peered to VPC C through VPC peering connection `p-cx-aaaacccc`
- VPC B is peered to VPC C through VPC peering connection `p-cx-bbbbbbcc`



You may want to use this full mesh configuration when you have separate VPCs that need to share resources with each other without restriction; for example, as a file sharing system.

The route tables for each VPC point to the relevant VPC peering connection to access the entire CIDR block of the peer VPCs.

For more information on VPC Peering please refer to the below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>)

Ask our Experts



QUESTION 66 UNATTEMPTED

You are trying to connect your on-premise AD Microsoft Exchange Email server with the Simple AD service provided by AWS but are not able to do so? Which of the following could be a reason for this.

- ☐ A. The firewall is blocking the necessary ports.
- ☐ B. The NACL's are blocking the necessary ports.
- ☒ C. Simple AD does not work with many Microsoft products ✓
- ☐ D. You need to implement SSL before using Simple AD with Exchange Server.

Explanation :

Answer – C

The AWS documentation mentions the following on the Simple AD service

Simple AD provides a subset of the features offered by Microsoft AD, including the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO). However, note that Simple AD does not support features such as trust relationships with other domains, Active Directory Administrative Center, PowerShell support, Active Directory recycle bin, group managed service accounts, and schema extensions for POSIX and Microsoft applications

For more information on the Simple AD service please refer to the below URL:

- http://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html
(http://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html)

Ask our Experts



QUESTION 67 UNATTEMPTED

You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient. Which of the following options would you consider for configuring the web server infrastructure? Choose 2 answers from the options below

- ☐ **A. Configure ELB with TCP listeners on TCP/443. And place the Web servers behind it. ✓**
- ☐ **B. Configure your Web servers with EIP's. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers. ✓**
- ☐ **C. Configure ELB with HTTPS listeners, and place the Web servers behind it.**
- ☐ **D. Configure your web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution.**

Explanation :

Answer - A and B

Option A is correct because end instance will handle SSL Authentication. TLS connection does not terminate on the ELB and on the backend servers its decrypted while passing through it.

Option B is correct because we can use Web Servers directly along with Route 53 and ELB can be removed.

Option C is incorrect because Client side certifications is not supported by ELB with HTTPs

Option D is incorrect because Cloudfront does not support Client side certification.

Ask our Experts



QUESTION 68 UNATTEMPTED

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPsec tunnels over the internet. You will be using

VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways. Which of the following objectives would you achieve by implementing an IPsec tunnel as outlined above? Choose 4 answers from the options below

- ☐ A. End-to-end protection of data in transit
- ☐ B. End-to-end Identity authentication
- ☒ C. Data encryption across the Internet ✓
- ☒ D. Protection of data in transit over the Internet ✓
- ☒ E. Peer identity authentication between VPN gateway and customer gateway ✓
- ☒ F. Data integrity protection across the Internet ✓

Explanation :

Answer – C,D,E and F

The below link provides an article on the general working of an IPsec tunnel which outlines the advantages of an IPsec tunnel which includes

- <http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>
(<http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>)

- 1) Data encryption across the Internet
- 2) Protection of data in transit over the Internet
- 3) Peer identity authentication between source and destination (in aws that is the VPN gateway and customer gateway)
- 4) Data integrity protection across the Internet

Ask our Experts



QUESTION 69 UNATTEMPTED

You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks. Which of the below are viable mitigation techniques? Choose 3 answers from the options below

- ☐ A. Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
- ☐ B. Use dedicated instances to ensure that each instance has the maximum performance possible.
- ☒ C. Use an Amazon CloudFront distribution for both static and dynamic content. ✓
- ☒ D. Use an Elastic Load Balancer with auto scaling groups at the web, App and Amazon Relational Database Service (RDS) tiers ✓
- ☒ E. Add alert Amazon CloudWatch to look for high Network in and CPU utilization. ✓
- ☐ F. Create processes and capabilities to quickly add and remove rules to the instance OS firewall.

Explanation :

Answer – C,D and E

The below snapshot from the AWS documentation shows the best architecture practises for avoiding DDos attacks.

	AWS Edge Locations			AWS Regions		
	Amazon CloudFront with AWS WAF (BP1, BP2)	Amazon API Gateway (BP4)	Amazon Route 53 (BP3)	Elastic Load Balancing (BP6)	Amazon VPC (BP5)	Amazon EC2 with Auto Scaling (BP7)
Layer 3 (e.g., UDP reflection) attack mitigation	✓	✓	✓	✓	✓	
Layer 4 (e.g., SYN flood) attack mitigation	✓	✓	✓	✓		
Layer 6 (e.g., SSL) attack mitigation	✓	✓	N/A	✓		
Reduce attack surface	✓	✓	✓	✓	✓	
Scale to absorb application layer traffic	✓	✓	✓	✓		✓
Layer 7 (application layer) attack mitigation	✓	✓	✓			
Geographic isolation and dispersion of excess traffic and larger DDoS attacks	✓	✓	✓			

For best practises against DDos attacks , please visit the below link:

- https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf
(https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf)

Ask our Experts



QUESTION 70 UNATTEMPTED

A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC. How should they architect their solution to achieve these goals?

- ☐ A. Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see all traffic across the VPC.
- ☐ B. Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides.

- ☐ C. Configure servers running in the VPC using the host-based 'route' commands to send all traffic through the platform to a scalable virtualized IDS/IPS.
- ☐ D. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection. ✓

Explanation :

Answer - D

Promiscuous mode is not supported in aws hence the options of A is out.

Please find the below developer forums thread on the same.

- <https://forums.aws.amazon.com/thread.jspa?threadID=35683>
(<https://forums.aws.amazon.com/thread.jspa?threadID=35683>)

Option B would just add an overhead to the infrastructure

Between Option C and D, an agent would do a better job than the route command.

Please find the below url to a good slide deck from AWS for getting IDS in place.

- <https://awsmedia.s3.amazonaws.com/SEC402.pdf>
(<https://awsmedia.s3.amazonaws.com/SEC402.pdf>)

Ask our Experts



QUESTION 71 UNATTEMPTED

You are currently experiencing an attack on your EC2 Instances located in a subnet. At the moment, the IT security department is to stop the attack. The default NACL's have been setup on the subnet. Which of the following commands would you issue to mitigate the attack for the moment?

- ☐ A. AWS ec2 delete-network-acl-entry ✓
- ☐ B. AWS ec2 create-network-acl-entry
- ☐ C. AWS ec2 rename-network-acl-entry
- ☐ D. AWS ec2 change-network-acl-entry

Explanation :

Answer - A

Since the default rules of the NACL is to allow all traffic, the best option first would be to delete the default rule from the NACL to block all traffic

An example of the command is shown below

`aws ec2 delete-network-acl-entry --network-acl-id acl-5fb85d36 --ingress --rule-number 100`

For more information on the command, please visit the below URL:

- <http://docs.aws.amazon.com/cli/latest/reference/ec2/delete-network-acl-entry.html>
(<http://docs.aws.amazon.com/cli/latest/reference/ec2/delete-network-acl-entry.html>)

Ask our Experts



QUESTION 72 UNATTEMPTED

Which of the following statements on VPC routing is false

- ☐ A. The VPC comes with an implicit router.
- ☐ B. You can delete the main route table with the VPC and replace it with a custom route table ✓
- ☐ C. You can create additional custom route tables for your VPC
- ☐ D. Each subnet in a VPC must be associated with a route table

Explanation :

Answer - B

The AWS documentation mentions the following on Route tables

The following are the basic things that you need to know about route tables:

- Your VPC has an implicit router.
 - Your VPC automatically comes with a main route table that you can modify.
 - You can create additional custom route tables for your VPC.
 - Each subnet must be associated with a route table, which controls the routing for the subnet. If you don't explicitly associate a subnet with a particular route table, the subnet is implicitly associated with the main route table.
 - You cannot delete the main route table, but you can replace the main route table with a custom table that you've created (so that this table is the default table each new subnet is associated with).
- For more information on VPC route tables , please visit the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)

Ask our Experts



QUESTION 73 UNATTEMPTED

Which of the below options is the most suited for connecting your on-premise Active directory services to AWS? Choose an answer from the options below

- ☐ A. Simple AD
- ☐ B. AWS Directory Service for Microsoft Active Directory (Enterprise Edition)
- ☐ C. AD Connector ✓
- ☐ D. Any of these options are acceptable to use as long as they configured correctly for 10,000 customers

This is clearly given as the limits in the AWS documentation where there is a limit of static routes for 50 routes. Hence the best option is to use dynamic routing.

Route Tables

Resource	Default limit	Comments
Route tables per VPC	200	Including the main route table. You can associate one route table to one or more subnets in a VPC. To increase this limit, submit a request .
Routes per route table (non-propagated routes)	50	This is the limit for the number of non-propagated entries per route table. You can submit a request for an increase of up to a maximum of 100; however, network performance may be impacted. This limit is enforced separately for IPv4 routes and IPv6 routes (you can have 50 each, and a maximum of 100 each).
BGP advertised routes per route table (propagated routes)	100	You can have up to 100 propagated routes per route table. This limit cannot be increased. If you require more than 100 prefixes, advertise a default route.

For more information on the limits, please visit the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html#vpc-limits-route-tables
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html#vpc-limits-route-tables)

Ask our Experts



QUESTION 75 UNATTEMPTED

An EC2 Instance has been setup in AWS. A software was successfully download and installed on the EC2 Instance. This software uses IPv6 for communication. After the software was installed, and you were trying to access the software via IPv6 on port 80, you were not able to do so. What needs to be done to alleviate this issue?

- ☒ A. Add an inbound rule to your security group that allows inbound traffic on port 80 for ::/0. ✓
- ☐ B. Add an internet gateway for the instance.
- ☐ C. Add an inbound rule to your security group that allows inbound traffic on port 80 for 0.0.0.0/0.
- ☐ D. Add an egress-only internet gateway.

Explanation :

Answer – A

Since the application works on IPv6, you need to ensure that the port is open for all Ipv6 addresses as ::/0

For more information on authorizing access to your instances , please visit the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html> (<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>)

Ask our Experts



QUESTION 76 UNATTEMPTED

Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement.

- ☒ **A. Set up VPC peering between the central server VPC and each of the teams VPCs.**
✓
- ☐ **B. Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.**
- ☐ **C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.**
- ☐ **D. None of the above options will work.**

Explanation :

Answer – A

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. VPC peering needs to have the basic functionality that the CIDR's should not overlap, hence option D is wrong.

For more information on VPC Peering please see the below link:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html> (<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>)

Ask our Experts



There is a requirement to host a database server. This server should not be able to connect to the internet except in the case of downloading the required database patches. Which of the following solutions would be the best to satisfy all the above requirements? Choose the correct answer from the options below

- ☐ A. Set up the database in a private subnet with a security group which only allows outbound traffic.
- ☐ B. Set up the database in a public subnet with a security group which only allows inbound traffic.
- ☐ C. Set up the database in a local data center and use a private gateway to connect the application to the database.
- ☐ D. Set up the database in a private subnet which connects to the Internet via a NAT instance. ✓

Explanation :

Answer – D

This sort of setup as per the aws documentation coincides with Scenario2 of setting up a VPC.

Scenario 2: VPC with Public and Private Subnets (NAT)

The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. We recommend this scenario if you want to run a public-facing web application, while maintaining back-end servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in a private subnet. You can set up security and routing so that the web servers can communicate with the database servers.

For more information on the VPC Scenario for public and private subnets please see the below link:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Ask our Experts



There is a requirement for a company to transfer large amounts of data between AWS and an on-premise location. There is an additional requirement for low latency and high consistency traffic to AWS. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

- ☐ A. Provision a Direct Connect connection to an AWS region using a Direct Connect partner. ✓

- ☐ B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
- ☐ C. Create an IPSec tunnel for private connectivity, which increases network consistency and reduces latency.
- ☐ D. This is not possible.

Explanation :

Answer – A

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

For more information on AWS direct connect, just browse to the below URL:

- <https://aws.amazon.com/directconnect/> (<https://aws.amazon.com/directconnect/>)

Ask our Experts



QUESTION 79 UNATTEMPTED

Which of the following is provided by AWS which allows the automation of network interface configuration on Linux instances

- ☐ A. AWS-net-utils
- ☒ B. ec2-net-utils ✓
- ☐ C. AWS-linux-utils
- ☐ D. ec2-linux-utils

Explanation :

Answer - B

The AWS Documentation mentions the following

Amazon Linux AMIs may contain additional scripts installed by AWS, known as ec2-net-utils. These scripts optionally automate the configuration of your network interfaces. These scripts are available for Amazon Linux only.

For more information on using Elastic network interfaces, just browse to the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>)

Ask our Experts



An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the webserver on a single VPC instance such that it allows the internet traffic as well as the back-end management traffic. The organization wants to make so that the back end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing webserver will have an IP address which can receive traffic from all the internet IPs.

How can the organization achieve this by running web server on a single instance?

- ☐ A. It is not possible to have 2 IP addresses for a single instance
- ☐ B. The organization should create 2 network interfaces , one for the internet traffic and the other for the backend traffic ✓
- ☐ C. The organization should create 2 EC2 instances as this is not possible with one EC2 instance
- ☐ D. This is not possible

Explanation :

Answer - B

An elastic network interface (referred to as a network interface in this documentation) is a virtual network interface that you can attach to an instance in a VPC. Network interfaces are available only for instances running in a VPC.

A network interface can include the following attributes:

- A primary private IPv4 address
- One or more secondary private IPv4 addresses
- One Elastic IP address (IPv4) per private IPv4 address
- One public IPv4 address
- One or more IPv6 addresses
- One or more security groups
- A MAC address
- A source/destination check flag
- A description

For more information on ENI , please refer to the below link:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>)


Ask our Experts



Certification

- ➔ Cloud Certification
(<https://www.whizlabs.com/cloud-certification-training-courses/>)
- ➔ Java Certification
(<https://www.whizlabs.com/oracle-java-certifications/>)
- ➔ PM Certification
(<https://www.whizlabs.com/project-management-certifications/>)
- ➔ Big Data Certification
(<https://www.whizlabs.com/big-data-certifications/>)

Mobile App

-  Android Coming Soon
-  iOS Coming Soon

Company

- ➔ Support
(<https://help.whizlabs.com/hc/en-us>)
- ➔ Discussions (<http://ask.whizlabs.com/>)
- ➔ Blog (<https://www.whizlabs.com/blog/>)

Follow us



(<https://www.facebook.com/whizlabs.software/>)



(<https://in.linkedin.com/company/whizlabs-software>)



(<https://twitter.com/whizlabs?lang=en>)



(<https://plus.google.com/+WhizlabsSoftware>)