

[🏠 \(https://www.whizlabs.com/learn/\)](https://www.whizlabs.com/learn/) > [My Courses \(https://www.whizlabs.com/learn/my-courses\)](https://www.whizlabs.com/learn/my-courses)
> [AWS Certified Advanced Networking Specialty \(https://www.whizlabs.com/learn/course/aws-cans-practice-tests#section-1\)](https://www.whizlabs.com/learn/course/aws-cans-practice-tests#section-1)
> [Practice Test V \(https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14612\)](https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14612) > **Report**

PRACTICE TEST V

Attempt	1	Completed on	Sunday , 03 February 2019 , 11:12 PM
Marks Obtained	1 / 80	Time Taken	00 H 01 M 25 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	1	0	79
Questions	Correct	Incorrect	Unattempted

[Show Answers](#)

All



QUESTION 1 UNATTEMPTED

You have created a custom VPC(10.0.0.0/16) and subnet in AWS. You have are planning on hosting applications on EC2 instances that depend on IPV6 traffic. You need to ensure that the traffic goes through the internet gateway. Which of the following routes would you add to the route table to ensure that the traffic would flow as desired?

- ☐ A. 0.0.0.0/0 ->Internet gateway
- ☐ B. 10.0.0.0/16->Internet gateway
- ☒ C. ::/0->Internet gateway ✓
- ☐ D. 10.0.0.0/16->Internet gateway

Explanation :

Answer – C

This is given as an example in the AWS documentation

Routing for IPv6

If you associate an IPv6 CIDR block with your VPC and subnet, your route table must include separate routes for IPv6 traffic. The following table shows the custom route table for this scenario if you choose to enable IPv6 communication in your VPC. The second entry is the default route that's automatically added for local routing in the VPC over IPv6. The fourth entry routes all other IPv6 subnet traffic to the Internet gateway.

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

For more information on this scenario in the VPC, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html)

Ask our Experts



QUESTION 2 UNATTEMPTED

Your infrastructure in AWS which consist of EC2 instances is suddenly facing a DDos attack from a set of IP addresses. You need to mitigate this issue immediately. Which of the following steps can you perform to mitigate this issue?

- ☐ A. Add a deny rule to the Outbound traffic for the Security group attached to the EC2 Instances for the set of IP ranges.
- ☐ B. Ensure the IP ranges are removed to the route table of the subnet
- ☐ C. Enable VPC logs.
- ☐ D. Add a deny rule to the Inbound traffic for the NACL group attached to the subnet for the set of IP ranges. ✓

Explanation :

Answer – D

As a quick mitigation measure , a Deny rule can be added to the NACL for the subnet so that no Inbound traffic from the set of IP addresses makes it to the subnet

For more information on NACL's, please refer to the below URL:

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

Ask our Experts



QUESTION 3 UNATTEMPTED

Which of the following are 2 types of NAT devices provided by AWS?

- ☐ A. NAT Instance ✓
- ☐ B. NAT gateway ✓
- ☐ C. NAT connection
- ☐ D. NAT device

Explanation :

Answer – A and B

The AWS documentation mentions the following

AWS offers two kinds of NAT devices—a *NAT gateway* or a *NAT instance*. We recommend NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI. You can choose to use a NAT instance for special purposes.

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

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

Ask our Experts



QUESTION 4 UNATTEMPTED

You currently have a DHCP options set associated with a VPC. You need to ensure that some additional settings are placed and associated via the DHCP options set with the VPC. How can this be accomplished.

- ☐ A. Modify the current DHCP options set associated with the VPC
- ☐ B. Create a new DHCP options set. Add this to the VPC.

- ☐ C. Create a new DHCP options set. Replace the current DHCP options set with the new one. ✓
- ☐ D. This is not possible. Once the DHCP options set is associated with a VPC, it cannot be changed.

Explanation :

Answer - C

The AWS documentation mentions the following

After you create a set of DHCP options, you can't modify them. If you want your VPC to use a different set of DHCP options, you must create a new set and associate them with your VPC. You can also set up your VPC to use no DHCP options at all.

You can have multiple sets of DHCP options, but you can associate only one set of DHCP options with a VPC at a time. If you delete a VPC, the DHCP options set associated with the VPC are also deleted.

For more information on DHCP Options Set, please refer to the below URL:

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

Ask our Experts



QUESTION 5 UNATTEMPTED

You have an EC2 Instance located in a subnet in a VPC. You have installed a new application that works on the TCP protocol , port 80. You are trying to access the application from a workstation but are not able to do so. Which of the below steps would rectify the issue.

- ☐ A. Add an Inbound rule to the Security Group ✓
- ☐ B. Add an Inbound rule to the NACL Group
- ☐ C. Add an Outbound rule to the Security Group
- ☐ D. Add an Outbound rule to the NACL Group

Explanation :

Answer – A

The most likely reason is that the Security group attached to the EC2 Instance has not been opened up to the new application on the TCP protocol and port 80.

For more information on Security Groups , please refer to the below URL:

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

Ask our Experts



QUESTION 6 UNATTEMPTED

You are planning on creating a fault tolerant EC2 Instance by creating a secondary network interface and a backup EC2 Instance. Which of the following is a requirement to ensure the switch over can be done successfully. Choose 2 answers from the options given below

- ☐ A. The network interface must reside in the same Availability Zone ✓
- ☐ B. The network interface must reside in the same Region
- ☐ C. The instance must reside in the same Availability Zone ✓
- ☐ D. The instance must reside in the same Region

Explanation :

Answer – A and C

This is given in the AWS documentation

You can attach a network interface in one subnet to an instance in another subnet in the same VPC; however, both the network interface and the instance must reside in the same Availability Zone.

For more information on Elastic Network Interfaces , please refer 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



QUESTION 7 UNATTEMPTED

Which of the following protocols are currently supported as health checks for Route53. Choose 3 answers from the options given below

- ☐ A. UDP
- ☐ B. HTTP ✓
- ☐ C. HTTPS ✓
- ☐ D. TCP ✓

Explanation :

Answer – B,C and D

Route 53 supports health checks over HTTPS, HTTP or TCP.

For more information on Route53 , please refer to the below URL:

- <https://aws.amazon.com/route53/faqs/> (<https://aws.amazon.com/route53/faqs/>)

Ask our Experts

**QUESTION 8 UNATTEMPTED**

Which of the following statements is incorrect when it comes to the VPC gateway service

- ☐ A. Once can use the VPC gateway for S3 to establish a connection between private instances and S3
- ☐ B. You can have an endpoint for a VPC to connect to a service in any region ✓
- ☐ C. You cannot transfer an endpoint from one VPC to another, or from one service to another.
- ☐ D. Endpoint connections cannot be extended out of a VPC.

Explanation :

Answer - B

The AWS documentation mentions the following on the VPC gateway service

- Endpoints are supported within the same region only. You cannot create an endpoint between a VPC and a service in a different region.
- You cannot transfer an endpoint from one VPC to another, or from one service to another.
- Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, AWS Direct Connect connection, or ClassicLink connection in your VPC cannot use the endpoint to communicate with resources in the endpoint service.

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

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

Ask our Experts

**QUESTION 9 UNATTEMPTED**

When you plan to utilize a NAT gateway , which of the following are charges that you need to be wary about? Choose 2 answers from the options given below.

- ☐ A. There is a charge for each hour the NAT gateway is operational. ✓
- ☐ B. There is a charge for each instance which connects to the NAT gateway
- ☐ C. There is a charge for each destination workstation that connects to the NAT gateway.
- ☐ D. There is a data processing charge for each GB processed. ✓

Explanation :

Answer – A and D

If you choose to create a NAT gateway in your VPC, you are charged for each "NAT Gateway-hour" that your NAT gateway is provisioned and available. Data processing charges apply for each Gigabyte processed through the NAT gateway regardless of the traffic's source or destination.

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

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

Ask our Experts



QUESTION 10 UNATTEMPTED

You have established a VPN connection from AWS to your on-premise infrastructure. But the VPC connections keeps on going down. How can you ensure the connection is always active?

- ☐ A. Ensure a public IP is provided for the customer gateway
- ☐ B. Ensure a public IP is provided for the virtual private gateway
- ☐ C. Ensure a networking monitoring tool is in place to generate traffic ✓
- ☐ D. Ensure the attribute of keep-alive is set for the VPC connection

Explanation :

Answer – C

The AWS documentation mentions the following

The VPN tunnel comes up when traffic is generated from your side of the VPN connection. The virtual private gateway is not the initiator; your customer gateway must initiate the tunnels. If your VPN connection experiences a period of idle time (usually 10 seconds, depending on your configuration), the tunnel may go down. To prevent this, you can use a network monitoring tool to generate keepalive pings; for example, by using IP SLA.

For more information on VPN connections, please refer to 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

You have a classic load balancer that have backend instances that have instances that communicate on the TCP protocol. If there was a need to get connection information such as the source IP address , which of the following configurations needs to be carried out?

- ☐ A. Configure connection draining
- ☐ B. Configure sticky sessions
- ☒ C. Configure Proxy protocol ✓
- ☐ D. Configure Cross-Zone Load balancing

Explanation :

Answer - C

The AWS documentation mentions the following

By default, when you use Transmission Control Protocol (TCP) for both front-end and back-end connections, your Classic Load Balancer forwards requests to the instances without modifying the request headers. If you enable Proxy Protocol, a human-readable header is added to the request header with connection information such as the source IP address, destination IP address, and port numbers. The header is then sent to the instance as part of the request.

For more information on Proxy protocol, please refer to the below URL:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-proxy-protocol.html>
(<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-proxy-protocol.html>)

Ask our Experts



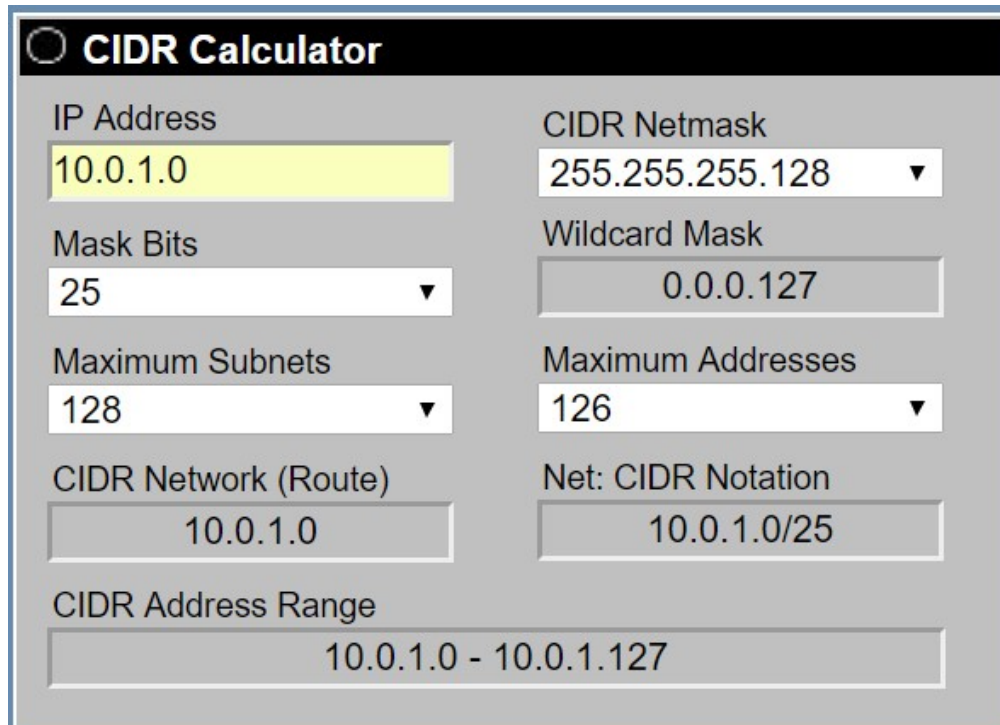
You are planning to use the CIDR block of 10.0.1.0/25 for designing the subnets in AWS. What is the range of addresses with this CIDR configuration?

- ☒ A. 128 ✓
- ☐ B. 256
- ☐ C. 1028
- ☐ D. 2056

Explanation :

Answer - A

The snapshot from a CIDR calculator shows how this would look like



The screenshot shows a web-based CIDR Calculator interface. It has a dark header with the title 'CIDR Calculator'. Below the header, there are several input fields and dropdown menus arranged in two columns. The left column contains 'IP Address' (10.0.1.0), 'Mask Bits' (25), 'Maximum Subnets' (128), 'CIDR Network (Route)' (10.0.1.0), and 'CIDR Address Range' (10.0.1.0 - 10.0.1.127). The right column contains 'CIDR Netmask' (255.255.255.128), 'Wildcard Mask' (0.0.0.127), 'Maximum Addresses' (126), and 'Net: CIDR Notation' (10.0.1.0/25). The 'IP Address' field is highlighted in yellow.

Field	Value
IP Address	10.0.1.0
Mask Bits	25
Maximum Subnets	128
CIDR Network (Route)	10.0.1.0
CIDR Address Range	10.0.1.0 - 10.0.1.127
CIDR Netmask	255.255.255.128
Wildcard Mask	0.0.0.127
Maximum Addresses	126
Net: CIDR Notation	10.0.1.0/25

Please refer to the below site for the CIDR calculator

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

Ask our Experts



A company has a direct connect connection from AWS to their on-premise location. Which of the following can be used as a backup to the existing Direct Connect connection to establish high availability. Choose 2 answers from the options given below

- ☐ A. Another direct connect connection from the same AWS partner
- ☐ B. Another direct connect connection from a different AWS partner ✓
- ☐ C. A AWS VPN Connection ✓
- ☐ D. A Virtual private gateway

Explanation :

Answer – B and C

This is given in the AWS documentation

Many AWS customers establish private connectivity between AWS and their data center, office, or colocation environment with AWS Direct Connect to reduce network costs, increase bandwidth throughput, or provide a more consistent network experience than Internet-based connections.

Because each dedicated, physical connection is in one AWS Direct Connect location, multiple dynamically routed AWS Direct Connect connections are necessary to achieve high availability. Architectures with the highest levels of availability will leverage different AWS Direct Connect partner networks to ensure network-provider redundancy.

And the AWS VPN connection can also be used as a backup to the existing AWS Direct Connect connection.

For more information on data center high availability, please refer to the below URL:

- <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 14 UNATTEMPTED

You are in charge of setting up a Direct Connect connection between your company's AWS account and their on-premise infrastructure. Your senior management has asked for the cost parameters for the Direct Connect connection. Which of the following contribute to the cost of the AWS Direct Connect connection. Choose 2 answers from the options given below

- ☐ A. Initial upfront charges

- ☐ B. Port-hours charges ✓
- ☐ C. Data Transfer In charges
- ☐ D. Data Transfer Out charges ✓

Explanation :

Answer – B and D

This is given in the AWS documentation

AWS Direct Connect has two separate charges: port-hours and Data Transfer. Pricing is per port-hour consumed for each port type. Partial port-hours consumed are billed as full hours.

Data Transfer In is \$0.00 per GB in all locations.

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

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

Ask our Experts



QUESTION 15 UNATTEMPTED

You have an EC2 Instance with the following Security configured

- a) Inbound allowed for ICMP
- b) Outbound denied for ICMP
- c) Network ACL allowed for ICMP
- d) Network denied for ICMP

If Flow logs is enabled for the instance , which of the following flow records will be recorded. Choose 3 answers from the options give below

- ☐ A. An ACCEPT record for the request based on the Security Group ✓
- ☐ B. An ACCEPT record for the request based on the NACL ✓
- ☐ C. A REJECT record for the response based on the Security Group
- ☐ D. A REJECT record for the response based on the NACL ✓

Explanation :

Answer – A,B and D

This example is given in the AWS documentation as well

For example, you use the ping command from your home computer (IP address is 203.0.113.12) to your instance (the network interface's private IP address is 172.31.16.139). Your security group's inbound rules allow ICMP traffic and the outbound rules do not allow ICMP traffic; however, because security groups are stateful, the response ping from your instance is allowed. Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic. Because network ACLs are stateless, the response ping is dropped and will not reach your home computer. In a flow log, this is displayed as 2 flow log records:

- An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance.
- A REJECT record for the response ping that the network ACL denied.

For more information on Flow Logs, please refer to the below URL:

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

Ask our Experts



QUESTION 16 UNATTEMPTED

Which of the following statements are incorrect when it comes to VPC's, Subnets and Route tables

- ☐ A. A VPC comes with an implicit router
- ☐ B. The VPC comes with a main route table
- ☐ C. Each subnet can be associated with multiple route tables ✓
- ☐ D. Custom route tables can be created for a VPC

Explanation :

Answer - C

The AWS documentation mentions the following

- 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

For more information on VPC and 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



You have VPC's in AWS in the following configuration

- a) VPC A which is peered to VPC B
- b) VPC A is connected to an on-premise location via a VPN connection
- c) VPC B is peered to VPC C

The route tables for VPC peering and the VPN connection are setup appropriately. Which of the following statements are true. Give 2 answers from the options given below

- ☐ A. Instances in VPC A can access VPC B if the Security Groups and NACL permit ✓
- ☐ B. Instances in VPC B can access VPC A if the Security Groups and NACL permit ✓
- ☐ C. Instances in VPC B can access resources in the on-premise location if the Security Groups and NACL permit
- ☐ D. Instances in VPC C can access VPC A if the Security Groups and NACL permit

Explanation :

Answer – A and B

This scenario is given in the AWS documentation

If either VPC in a peering relationship has one of the following connections, you cannot extend the peering relationship to that connection:

- A VPN connection or an AWS Direct Connect connection to a corporate network
- An internet connection through an internet gateway
- An internet connection in a private subnet through a NAT device
- A VPC endpoint to an AWS service; for example, an endpoint to Amazon S3.
- (IPv6) A ClassicLink connection. You can enable IPv4 communication between a linked EC2-

Classic instance and instances in a VPC on the other side of a VPC peering connection. However, IPv6 is not supported in EC2-Classic, so you cannot extend this connection for IPv6 communication.

For example, if VPC A and VPC B are peered, and VPC A has any of these connections, then instances in VPC B cannot use the connection to access resources on the other side of the connection. Similarly, resources on the other side of a connection cannot use the connection to access VPC B.

Also transitive peering is not allowed

For more information on Invalid Peering configurations, please refer to the below URL:

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

QUESTION 18

UNATTEMPTED

Which of the following statements is true with regards to the Default VPC? Choose 2 answers from the options given below

- ☐ A. You can delete the default VPC. ✓
- ☐ B. You can restore a deleted default VPC
- ☐ C. You can mark an existing custom VPC as the default VPC
- ☐ D. You can create a default VPC if the original one is deleted ✓

Explanation :

Answer – A and D

The AWS documentation mentions the following

If you delete your default VPC, you can create a new one. You cannot restore a previous default VPC that you deleted, and you cannot mark an existing nondefault VPC as a default VPC.

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

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

Ask our Experts



QUESTION 19

UNATTEMPTED

When configuring Security Groups for AWS Workspaces, which of the following should be allowed in the security group. Choose 3 answers from the options given below

- ☐ A. Outbound traffic on ports 80 ✓
- ☐ B. Outbound traffic on ports 22
- ☐ C. Outbound traffic on ports 443 ✓
- ☐ D. Traffic to all destinations ✓

Explanation :

Answer – A,C and D

The recommendation for Internet access is provided in the AWS documentation

We recommend that you launch your WorkSpaces in private subnets in your virtual private cloud (VPC) and use one of the following options to allow your WorkSpaces to access the Internet:

- 1) Configure a NAT gateway in your VPC.
- 2) Configure automatic assignment of public IP addresses.
- 3) Manually assign public IP addresses to your WorkSpaces.

With any of these options, you must ensure that the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0).

For more information on workspaces and Internet access, please refer to the below URL:

· (<http://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-internet-access.html>)<http://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-internet-access.html> (<http://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-internet-access.html>)

Ask our Experts



QUESTION 20

UNATTEMPTED

At which layer of the Internet protocol suite does the DNS and DHCP protocol operate at?

- ☒ A. Application ✓
- ☐ B. Transport
- ☐ C. Internet
- ☐ D. Link

Explanation :

Answer - A

Below is the snapshot of the Internet Protocol Suite

Internet protocol suite

Application layer

BGP · DHCP · DNS · FTP · HTTP · IMAP ·
LDAP · MGCP · NNTP · NTP · POP ·
ONC/RPC · RTP · RTSP · RIP · SIP · SMTP ·
SNMP · SSH · Telnet · TLS/SSL · XMPP ·
more...

Transport layer

TCP · UDP · DCCP · SCTP · RSVP · *more...*

Internet layer

IP (IPv4 · IPv6) · ICMP · ICMPv6 · ECN ·
IGMP · **IPsec** · *more...*

Link layer

ARP · NDP · OSPF · Tunnels (L2TP) · PPP ·
MAC (Ethernet · DSL · ISDN · FDDI) · *more...*

V · T · E

For more information on the Internet protocol suite, please refer to the below URL:

- https://en.wikipedia.org/wiki/Internet_protocol_suite
(https://en.wikipedia.org/wiki/Internet_protocol_suite)

Ask our Experts



QUESTION 21 UNATTEMPTED

Which of the following determines what is the maximum supported MTU for an Instance

- ☐ A. The AMI
- ☒ B. The Instance Type ✓
- ☐ C. The VPC the instance is hosted in
- ☐ D. The subnet the instance is hosted in

Explanation :

Answer - B

The AWS documentation mentions the following

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. The maximum supported MTU for an instance depends on its instance type. For more information on network MTU, please refer to 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 22 UNATTEMPTED

Which of the following commands can be used to check the path MTU between two hosts?

- ☒ A. tracepath ✓
- ☐ B. ping
- ☐ C. traceroot
- ☐ D. traceping

Explanation :

Answer - A

The AWS documentation mentions the following

You can check the path MTU between two hosts using the tracepath command, which is part of the iputils package that is available by default on many Linux distributions, including Amazon Linux. For more information on network MTU, please refer to 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 23 UNATTEMPTED

You are planning on using the Elastic Network Adapter for Enhanced Networking. Which of the following is not a pre-requisite that needs to be met to work with Enhanced Networking.

- ☐ 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 – B

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.)

For more information on Enhanced Networking, please refer to the below URL:

- <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 24 UNATTEMPTED

You are planning on hosting an email server on an EC2 Instance. Which of the following should ideally be carried out to ensure the email server would function as intended. Choose 3 answers from the options given below

- ☐ A. Ensure an elastic IP is assigned to the server ✓
- ☐ B. Ensure a static reverse DNS record is created for the Elastic IP ✓
- ☐ C. Ensure AWS is provided with the Elastic IP ✓
- ☐ D. Ensure a CNAME record is created for the mail server

Explanation :

Answer – A,B and C

The AWS documentation mentions the following

If you intend to send email to third parties from an instance, we suggest you provision one or more Elastic IP addresses and provide them to us. AWS works with ISPs and Internet anti-spam organizations to reduce the chance that your email sent from these addresses will be flagged as spam. In addition, assigning a static reverse DNS record to your Elastic IP address used to send email can help avoid having email flagged as spam by some anti-spam organizations.

For more information on Elastic IP addresses, please refer to the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>)

Ask our Experts



QUESTION 25 UNATTEMPTED

When working with the costing for a classic load balancer, which of the following are parameters which determine the cost of using a classic load balancer.

- ☐ A. The number of connections established with the load balancer
- ☐ B. The data transferred via the load balancer ✓
- ☐ C. The amount of time the load balancer is running ✓
- ☐ D. The number of backend instances

Explanation :

Answer – B and C

The AWS documentation mentions the following

You are charged for each hour or partial hour that a Classic Load Balancer is running and for each GB of data transferred through your load balancer.

For more information on the load balancer, please refer to the below URL:

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

Ask our Experts



QUESTION 26 UNATTEMPTED

Which of the following is not an advantage of using multiple IP addresses on an EC2 Instance in AWS.

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

Explanation :

Answer – D

The AWS documentation mentions the following on multiple IP addresses

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

- Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address.
- Operate network appliances, such as firewalls or load balancers, that have multiple IP addresses for each network interface.
- Redirect internal traffic to a standby instance in case your instance fails, by reassigning the secondary IP address to the standby instance.

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

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

Ask our Experts



QUESTION 27 UNATTEMPTED

You are planning on using the AWS RDS service to host a database. You need to have the database with the Multi-AZ option enabled. Which of the following is the minimum requirement for the DB Subnet Group for this implementation.

- ☐ A. A subnet group with one subnet in one Availability Zone
- ☐ B. A subnet group with one subnet in one Region
- ☐ C. A subnet group with two subnets each in a separate Availability Zone ✓
- ☐ D. A subnet group with two subnets each in a separate Region

Explanation :

Answer – C

The AWS documentation mentions the following

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 DB Subnet groups, please visit the below URL:

- http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html
(http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html)

Ask our Experts



QUESTION 28 UNATTEMPTED

What is the term given to a hosted interface used by an account that is different from the account that owns the AWS Direct Connect connection?

- ☐ A. Private Virtual Interface
- ☐ B. Public Virtual Interface
- ☐ C. Secondary Virtual Interface
- ☐ D. Hosted Virtual Interface ✓

Explanation :

Answer - D

The AWS documentation mentions the following

Hosted virtual interfaces (VIF) can connect to public resources or a VPC in the same way as standard VIFs, except that the account that owns the hosted VIF is different from the connection owner.

Bandwidth is shared across all virtual interfaces on the parent connection

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

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

Ask our Experts



QUESTION 29 UNATTEMPTED

Which of the following is a connection that can be provided by an AWS partner when providing a sub-1G Direct Connect connection.

- ☒ A. Hosted connection ✓
- ☐ B. Private connection
- ☐ C. Public Connection
- ☐ D. Shared Connection

Explanation :

Answer - A

The AWS documentation mentions the following

A Hosted connection allows an APN partner to create a Direct Connect sub-1G connection for you, allocating dedicated bandwidth for that connection rather than having multiple VIFs on the same parent connection competing for bandwidth

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

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

Ask our Experts



QUESTION 30 UNATTEMPTED

Which of the below is a least expensive Active Directory option provided by AWS which is sufficient when you have 5000 users or less.

- ☐ A. AWS Directory Service for Microsoft Active Directory
- ☐ B. Shared AD
- ☒ C. Simple AD ✓
- ☐ D. AD Connector

Explanation :

Answer - C

The following AD options are provided by AWS

- AWS Directory Service for Microsoft Active Directory is a feature-rich managed Microsoft Active Directory hosted on the AWS cloud. Microsoft AD is your best choice if you have more than 5,000 users and need a trust relationship set up between an AWS hosted directory and your on-premises directories.
 - AD Connector simply connects your existing on-premises Active Directory to AWS. AD Connector is your best choice when you want to use your existing on-premises directory with AWS services.
 - Simple AD is an inexpensive Active Directory-compatible service with the common directory features. In most cases, Simple AD is the least expensive option and your best choice if you have 5,000 or fewer users and don't need the more advanced Microsoft Active Directory features
- For more information on AD options from AWS, please visit the below URL:
- http://docs.aws.amazon.com/directoryservice/latest/admin-guide/best_practices.html
(http://docs.aws.amazon.com/directoryservice/latest/admin-guide/best_practices.html)

Ask our Experts



QUESTION 31 UNATTEMPTED

Which of the following is not supported for AWS VPN connections.

- ☐ A. NAT traversal
- ☐ B. Cloudwatch metrics
- ☐ C. 128 bit encryption ✓
- ☐ D. 4-byte ASN

Explanation :

Answer - C

The AWS documentation mentions the following features enabled on AWS VPN connections

- NAT traversal
- 4-byte ASN (in addition to 2-byte ASN)
- CloudWatch metrics
- Reusable IP addresses for your customer gateways
- Additional encryption options; including AES 256-bit encryption, SHA-2 hashing, and additional Diffie-Hellman groups
- Configurable tunnel options
- Custom private ASN for the Amazon side of a BGP session

For more information on AWS VPN 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 32 UNATTEMPTED

Which of the following statements about AWS Direct Connect connections is incorrect.

- ☐ A. AWS Direct Connect supports 1 Gbps: 1000BASE-LX
- ☐ B. AWS Direct Connect support 10 Gbps: 10GBASE-LR
- ☐ C. You can change the port speed of an existing connection ✓
- ☐ D. AWS Direct connect gives a private connection between AWS and on-premise infrastructure

Explanation :

Answer - C

AWS Direct Connect supports two port speeds: 1 Gbps: 1000BASE-LX (1310nm) over single-mode fiber and 10 Gbps: 10GBASE-LR (1310nm) over single-mode fiber. You cannot change the port speed after you've created the connection request. If you need to change the port speed, you must create and configure a new connection.

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

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

Ask our Experts



QUESTION 33 UNATTEMPTED

Which of the following can be used to connect an existing Active Directory setup to Amazon Workspaces. Choose 2 answers from the options given below

- ☐ A. Simple AD
- ☐ B. Samba AD
- ☐ C. AWS Microsoft AD ✓
- ☐ D. AD connector ✓

Explanation :

Answer – C and D

This snapshot is given in the AWS documentation

Q: Can I connect to my existing Active Directory with my Amazon WorkSpaces?

Yes. You can use AD Connector or AWS Microsoft AD to integrate with your existing on-premises Active Directory.

For more information on AWS Workspaces, please visit the below URL:

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

Ask our Experts



QUESTION 34 UNATTEMPTED

Which of the following services can be used to log API calls made to the Cloudfront service?

- ☒ A. Cloudtrail ✓
- ☐ B. Cloudwatch
- ☐ C. Cloudwatch logs
- ☐ D. AWS config

Explanation :

Answer - A

The AWS documentation mentions the following

CloudFront is integrated with CloudTrail, an AWS service that captures information about every request that is sent to the CloudFront API by your AWS account, including your IAM users. CloudTrail periodically saves log files of these requests to an Amazon S3 bucket that you specify. CloudTrail captures information about all requests, whether they were made using the CloudFront console, the CloudFront API, the AWS SDKs, the CloudFront CLI, or another service, for example, AWS CloudFormation.

For more information on logging using Cloudtrail, please visit the below URL:

- http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/logging_using_cloudtrail.html (http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/logging_using_cloudtrail.html)

Ask our Experts



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



Which of the following is incorrect with regards to Security Groups

- ☐ A. By default, security groups allow all outbound traffic.
- ☒ B. Security groups are stateless ✓
- ☐ C. You can't create rules that deny access
- ☐ D. Rules are applied immediately to instances

Explanation :

Answer - B

The AWS documentation mentions the following

The following are the characteristics of security group rules:

- 1) By default, security groups allow all outbound traffic.
- 2) Security group rules are always permissive; you can't create rules that deny access.
- 3) Security groups are stateful – if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules.
- 4) You can add and remove rules at any time. Your changes are automatically applied to the instances associated with the security group after a short period.

For more information on Security Groups, please refer to below URL:

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

Ask our Experts



QUESTION 37 UNATTEMPTED

Which of the following services cannot be used to help protect against DDos attacks on your AWS infrastructure?

- ☒ A. AWS Config ✓
- ☐ B. AWS WAF
- ☐ C. AWS Shield
- ☐ D. AWS Shield Advanced

Explanation :

Answer – A

Option A, AWS Config cannot be used to help protect against DDos attacks on your AWS infrastructure. All other options can be used in this scenario.

The AWS documentation mentions the following

You can use AWS WAF web access control lists (web ACLs) to help minimize the effects of a distributed denial of service (DDoS) attack. AWS also provides AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services. For added protection against DDoS attacks, AWS offers AWS Shield Advanced. AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, and Amazon Route 53 hosted zones.

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

- <http://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>
(<http://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>)



QUESTION 38 UNATTEMPTED

You are designing Internet connectivity for your VPC. The Web servers must be available on the Internet. The application must have a highly available architecture. Which alternatives should you consider? Choose 2 answers from the options below

- ☐ A. Configure a NAT instance in your VPC Create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address.
- ☐ B. Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.
- ☐ C. Place all your web servers behind ELB. Configure a Route53 CNAME to point to the ELB DNS name. ✓
- ☐ D. Assign EIP's to all web servers. Configure a Route53 record set with all EIPs with health checks and DNS failover. ✓
- ☐ E. Configure ELB with an EIP. Place all your Web servers behind ELB Configure a Route53 A record that points to the EIP.

Explanation :

Answer – C and D

Option A is wrong because a NAT instance is ideally used to route traffic from a private subnet to the internet via a public subnet.

Option B is wrong because you don't want to point Cloudfront to private IP Addresses.

Option E is wrong because AWS does not recommend to assign IP Addresses to ELB. The public IP Addresses get automatically assigned to the ELB's.

You can either use an ELB , assign the web servers and have a Route 53 entry to the ELB. Or you can have Route53 route requests to the instances via Elastic IP's.

For more information on how to use ELB , please visit the below link:

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



QUESTION 39 UNATTEMPTED

A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an iPsec VPN. The application must authenticate against the on-premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user. Which two approaches can satisfy these objectives? Choose 2 answers from the options below

- ☐ A. Develop an identity broker that authenticates against IAM security Token service to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.
- ☐ B. The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket. ✓
- ☐ C. Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket. ✓
- ☐ D. The application authenticates against LDAP the application then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials the application can use the IAM temporary credentials to access the appropriate S3 bucket.

Explanation :

Answer – B and C

Option A is incorrect because we need to authenticate against LDAP.

Option D is incorrect because we cannot login to AWS IAM using LDAP credentials.

When you have the need for an in-premise environment to work with a cloud environment, you would normally have 2 artefacts for authentication purposes

- An identity store – So this is the on-premise store such as Active Directory which stores all the information for the user's and the groups they belong to.
- An identity broker – This is used as an intermediate agent between the on-premise location and the cloud environment. In Windows you have a system known as Active Directory Federation services to provide this facility.

For more information on federated access, please visit the below link:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html)

Ask our Experts



QUESTION 40 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 41 UNATTEMPTED

You have used the VPC Wizard to create a VPC with the private and public subnet option along with the NAT instance. You been told that the VPC is no longer required. You are trying to delete the VPC but are not able to do so. Why is this the case?

- ☐ A. It's because the VPC needs to be dissociated from the subnets first
- ☐ B. The NAT instance needs to be deleted first ✓
- ☐ C. The Internet gateway needs to be detached first
- ☐ D. The route tables need to be deleted first

Explanation :

Answer – B

To delete the VPC and the subnets, no instances should be present in the subnet. Since there is a NAT instance, this needs to be deleted first, before the VPC can be deleted.

For more information on working with VPC's, please refer to below URL:

- <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/working-with-vpcs.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/working-with-vpcs.html>)

Ask our Experts



QUESTION 42 UNATTEMPTED

What is the minimum and maximum allowed block size for a VPC? Choose 2 answers from the options given below

- ☐ A. Minimum - /16 ✓
- ☐ B. Minimum - /8
- ☐ C. Maximum - /24
- ☐ D. Maximum - /28 ✓

Explanation :

Answer – A and D

This is given in the AWS documentation

When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)

For more information on VPC's and subnets, please refer to below URL:

- 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 43 UNATTEMPTED

When configuring AWS Cloudhub, which of the below implementation steps would you carry out. Choose 2 answers from the options given below

- ☐ A. Create multiple customer gateways each with a public IP address ✓

- ☐ B. Create multiple customer gateways each with the same public IP address
- ☐ C. Create a VPN connection between each customer gateway and an individual virtual private gateway
- ☐ D. Create a VPN connection between each customer gateway and a common virtual private gateway ✓

Explanation :

Answer – A and D

The steps are given in the AWS documentation

To configure the AWS VPN CloudHub, you use the AWS Management Console to create multiple customer gateways, each with the public IP address of the gateway and the ASN. Next, you create a VPN connection from each customer gateway to a common virtual private gateway.

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

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

Ask our Experts



QUESTION 44 UNATTEMPTED

Which of the below record sets can be used to point to a classic Load Balancer DNS name created in AWS?

- ☐ A. CNAME
- ☐ B. A
- ☐ C. TXT
- ☐ D. Alias ✓

Explanation :

Answer - D

This is given in the AWS documentation

While ordinary Amazon Route 53 resource record sets are standard DNS resource record sets, *alias resource record sets* provide an Amazon Route 53–specific extension to DNS functionality. Instead of an IP address or a domain name, an alias resource record set contains a pointer to a CloudFront distribution, an Elastic Beanstalk environment, an ELB Classic, Application, or Network Load Balancer, an Amazon S3 bucket that is configured as a static website, or another Amazon Route 53 resource record set in the same hosted zone

For more information on alias and non-alias records, please refer to below URL:

- <http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>
(<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>)

Ask our Experts



QUESTION 45 UNATTEMPTED

You currently have 2 EC2 Instances that host a web application. One is a primary server and the other is a backup server. What would you configure in Route53 to ensure that if the primary server goes down for any reason, the users will be directed to the backup server? Choose 2 answers from the options given below

- ☐ A. Configure the latency based routing policy
- ☐ B. Configure health checks ✓
- ☐ C. Configure DNS failover ✓
- ☐ D. Configure server failover

Explanation :

Answer – B and C

If you have multiple resources that perform the same function, you can configure DNS failover so that Amazon Route 53 will route your traffic from an unhealthy resource to a healthy resource. For example, if you have two web servers and one web server becomes unhealthy, Amazon Route 53 can route traffic to the other web server

For more information on DNS failover, please refer to below URL:

- <http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>
(<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>)

Ask our Experts



QUESTION 46 UNATTEMPTED

What are the general steps carried out when enabling Origin access identity in Cloudfront? Choose 2 answers from the options given below

- ☐ A. Create a special Cloudfront group

- ☐ B. Create a special Cloudfront user ✓
- ☐ C. Apply read only permission for the identity to the bucket via Bucket ACL
- ☐ D. Apply read only permission for the identity to the bucket via Bucket policies ✓

Explanation :

Answer – B and D

The general steps for enabling Origin access identity in Cloudfront is

- 1) Create an origin access identity, which is a special CloudFront user, and associate the origin access identity with your distribution
- 2) Change the permissions either on your Amazon S3 bucket or on the objects in your bucket so only the origin access identity has read permission

For more information on Cloudfront private content, please refer to below URL:

- <http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>)

Ask our Experts



QUESTION 47 UNATTEMPTED

Which of the following HTTP methods are not cached by Cloudfront?

- ☒ A. PUT ✓
- ☐ B. GET
- ☐ C. HEAD
- ☐ D. OPTIONS

Explanation :

Answer – A

CloudFront caches responses to GET and HEAD requests and, optionally, OPTIONS requests.

CloudFront does not cache responses to requests that use the other methods.

For more information on Cloudfront web distributions, please refer to below URL:

- <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 48 UNATTEMPTED

If you need to set up HTTPS on Cloudfront which uses S3 as the origin, which of the following Viewer protocol policy's can be used. Choose 2 answers from the options given below.

- ☐ A. Match Viewer
- ☐ B. Redirect HTTP to HTTPS ✓
- ☐ C. HTTPS Only ✓
- ☐ D. HTTP Only

Explanation :

Answer – B and C

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 Cloudfront and S3, please refer to 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 49 UNATTEMPTED

You are planning on setting up Cloudfront with a custom origin. For the moment , the performance of the requests is not on priority , but rather the costs associated with Cloudfront. Which of the below costing options for Cloudfront can be utilized to reduce the costs if this is the case.

- ☐ A. Price class ✓
- ☐ B. Spot requests
- ☐ C. Reserved pricing

☐ D. On-demand pricing

Explanation :

Answer - A

The AWS documentation mentions the following

By default, CloudFront responds to requests for your objects based only on performance: objects are served from the edge location for which latency is lowest for that viewer. If you're willing to accept higher latency for your viewers in some geographic regions in return for lower cost, you can choose a price class that doesn't include all CloudFront regions.

For more information on the price class, please refer to below URL:

- <http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PriceClass.html>
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PriceClass.html>)

Ask our Experts



QUESTION 50 UNATTEMPTED

Which of the following are deployment strategies that can be employed for placement groups. Choose 2 answers from the options given below

- ☐ A. Cluster ✓
- ☐ B. Primary
- ☐ C. Spread ✓
- ☐ D. Low Network

Explanation :

Answer – A and C

You can launch instances in a placement group, which determines how instances are placed on underlying hardware. When you create a placement group, you specify one of the following strategies for the group:

- Cluster—clusters instances into a low-latency group in a single Availability Zone
- Spread—spreads instances across underlying hardware

For more information on placement groups, please refer to 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 51 UNATTEMPTED

Which of the following are some steps that can be used to troubleshoot AWS Direct connect connections. Choose 3 answers from the options given below

- ☐ A. Ensure AWS Direct Connect cross connects are established ✓
- ☐ B. Check if Auto Negotiation is turned off ✓
- ☐ C. Verify that your device is supported by AWS Direct Connect ✓
- ☐ D. Check the status of the Virtual private gateway

Explanation :

Answer – A,B and C

Some of the recommendations from AWS for troubleshooting AWS Direct Connect connections

1) Verify that your AWS Direct Connect cross connects are established

2) Ask your service provider to turn off Auto Negotiation on their device, to set their device to Full Duplex, and to set their device to the correct speed.

3) Verify that your device is supported by AWS Direct Connect

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

- http://docs.aws.amazon.com/directconnect/latest/UserGuide/ts_remote_connect_text.html
(http://docs.aws.amazon.com/directconnect/latest/UserGuide/ts_remote_connect_text.html)

Ask our Experts



QUESTION 52 UNATTEMPTED

You have just peered 2 VPC's. You plan to host instances in these VPC's that need to communicate with each other. Which of the following would you do to ensure that optimal network communication can be in place between the instances?

- ☐ A. Ensure the instances are chosen with the Instance type that supports Enhanced Networking ✓
- ☐ B. Set the MTU of the instances to 1500
- ☐ C. Create two subnets in the same AZ and create a placement group. ✓

- ☐ D. Create two subnets in different AZs and create a placement group.

Explanation :

Answer – A and C

The AWS documentation mentions the following

A cluster 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 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 53 UNATTEMPTED

You have an instance inside a VPC that needs to communicate with other instances inside the VPC and also across the Internet. The best network transmission rates need to be in place. How can this be accomplished. Choose 2 answers from the options given below

- ☐ A. Configure two ENIs, one for internal traffic and one for external traffic ✓
- ☐ B. Configure one ENI with 2 private IP's
- ☐ C. Configure the external ENI with an MTU of 1500 and the internal ENI with an MTU of 9001. ✓
- ☐ D. Configure the external ENI with an MTU of 9001 and the internal ENI with an MTU of 1500.

Explanation :

Answer - A and C

The AWS documentation mentions the following

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. The maximum supported MTU for an instance depends on its instance type. All Amazon EC2 instance types support 1500 MTU, and many current instance sizes support 9001 MTU, or jumbo frame

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.

For more information on network MTU, please refer to 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 54 UNATTEMPTED

Your company's infrastructure currently includes EC2 Instances , an ELB and Cloudfront for Content Distribution. In order to protect the infrastructure from Internet attacks which of the following options would you employ. Choose 2 answers from the options given below

- ☐ A. Enable WAF to be placed in front of the ELB ✓
- ☐ B. Enable WAF to be placed in front of Cloudfront ✓
- ☐ C. Put DENY rules for all traffic in the NACL
- ☐ D. Ensure no traffic passed with the help of the Security Groups

Explanation :

Answer – A and B

The AWS documentation mentions the following

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront or an Application Load Balancer responds to requests either with the requested content or with an HTTP 403 status code (Forbidden).

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

- <http://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>
(<http://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>)

Ask our Experts



QUESTION 55 UNATTEMPTED

Your company has decided to use AWS WorkSpaces for its hosted desktop solution. Your company has an existing AD of about 60,000 users, and you want to minimize authentication traffic from AWS to your datacenter. What steps would you take to ensure the above requirement can be fulfilled? Choose 2 options.

- ☐ A. Create a VPN between the datacenter AWS.
- ☐ B. Deploy an AD Connector in AWS.
- ☐ C. Create a Direct Connect connection between the datacenter and AWS. ✓
- ☐ D. Use the Microsoft AD in AWS. ✓

Explanation :

Answer – C and D

Since the number of users is more , using AD connector would not be ideal. And also for a large number of users it is better to use AWS Direct Connect.

For more information on the Directory Service option, please refer to below URL:

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

Ask our Experts



QUESTION 56 UNATTEMPTED

Your company has two Direct Connect locations. You need to configure one link as passive. What should you configure in your router to set that link as the passive link? How can this be accomplished.

- ☒ A. Configure AS_PATH for the passive link ✓
- ☐ B. Set a higher MED for the active link
- ☐ C. Advertise a network with a higher CIDR.
- ☐ D. Advertise a network with a higher BGP.

Explanation :

Answer – A

The AWS documentation provides the following

Active/Passive (failover). One connection is handling traffic, and the other is on standby. If the active connection becomes unavailable, all traffic is routed through the passive connection. You will need to AS path prepend the routes on one of your links for it to be the passive link
For more information on Active Passive Direct Connect, please refer to below URL:

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

Ask our Experts



QUESTION 57 UNATTEMPTED

Which of the following contains the current IP address ranges published by AWS

- ☐ A. ip-ranges.xml
- ☒ B. ip-ranges.json ✓
- ☐ C. ip-addresses.xml
- ☐ D. ip-addresses.json

Explanation :

Answer - B

The AWS documentation mentions the following

Amazon Web Services (AWS) publishes its current IP address ranges in JSON format. To view the current ranges, download the .json file. To maintain history, save successive versions of the .json file on your system

For more information on AWS IP ranges, please refer to below URL:

- <http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>
(<http://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>)

Ask our Experts



QUESTION 58 UNATTEMPTED

Which of the following features enables immediate failover of AWS Direct Connect connections from primary to secondary

- ☐ A. AS_PATH

- ☐ B. MED
- ☒ C. BFD ✓
- ☐ D. IPSec

Explanation :

Answer - 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

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 59 UNATTEMPTED

Which of the following is not part of the Rule definition for Inbound Rules for Network ACL's

- ☐ A. Protocol
- ☐ B. Port Number
- ☐ C. Source IP Address
- ☒ D. Destination IP Address ✓

Explanation :

Answer - D

The parts of the Inbound Rules for Network ACL's are

1) Rule number - Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that may contradict it.

2) Protocol - You can specify any protocol that has a standard protocol number. For more information,

3) Protocol Numbers - If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.

4) The source of the traffic (CIDR range) and the destination (listening) port or port range.

Choice of ALLOW or DENY for the specified traffic.

For more information on Network ACL's, please refer to below URL:

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

Ask our Experts



QUESTION 60 UNATTEMPTED

You have an on-premise DNS server. One of the EC2 Instances in your VPC is trying to communicate with the DNS server via the VPN connection. But the communication is being blocked. Which of the following can be reasons for this. Choose 2 answers from the options given below

- ☐ A. The NACL is blocking Outbound traffic for TCP – port 53 ✓
- ☐ B. The NACL is blocking Outbound traffic for UDP – port 53 ✓
- ☐ C. The NACL is blocking Outbound traffic for TCP – port 443
- ☐ D. The NACL is blocking Outbound traffic for UDP – port 443

Explanation :

Answer – A and B

The ports used by DNS is TCP and UDP on port 53

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

- [https://technet.microsoft.com/en-us/library/dd197515\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd197515(v=ws.10).aspx)
([https://technet.microsoft.com/en-us/library/dd197515\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd197515(v=ws.10).aspx))

Ask our Experts



QUESTION 61 UNATTEMPTED

Which of the following protocols are used for AWS VPN connections?

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

Explanation :

Answer - A

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

For more information on VPN Connections, please refer to 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 62 UNATTEMPTED

Which of the following are required for having virtual interfaces in AWS. Choose 2 answers from the options given below

- ☐ A. A customer gateway
- ☐ B. A VLAN ID ✓
- ☐ C. Compliance with Ethernet 802.1Q standard ✓
- ☐ D. A Virtual Private gateway

Explanation :

Answer – B and C

The AWS documentation mentions the following

Each virtual interface must be tagged with a new, unused customer-provided tag (VLAN ID) that complies with the Ethernet 802.1Q standard. This tag is required for any traffic traversing the AWS Direct Connect connection. The number must be between 1 and 4094.

For more information on Virtual Interfaces, please refer to 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 63 UNATTEMPTED

When a NAT gateway is created , which of the following needs to be specified for the NAT gateway.

- ☐ A. Public IP address
- ☐ B. Private IP address
- ☐ C. Static IP address
- ☐ D. Elastic IP address ✓

Explanation :

Answer - D

The AWS documentation mentions the following

To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside.

You must also specify an Elastic IP address to associate with the NAT gateway when you create it

For more information on the NAT gateway, please refer to 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 64 UNATTEMPTED

For EC2 Instances to be able to communicate with the Internet , which of the following is not a right requirement.

- ☐ A. The VPC must have an Internet gateway attached.
- ☐ B. The Instance should be placed in a private subnet ✓
- ☐ C. The Instance should be placed in a public subnet
- ☐ D. Ensure that your subnet's route table points to the Internet gateway.

Explanation :

Answer - B

The AWS documentation mentions the following

To enable access to or from the Internet for instances in a VPC subnet, you must do the following:

- 1) Attach an Internet gateway to your VPC.
- 2) Ensure that your subnet's route table points to the Internet gateway.
- 3) Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- 4) Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.

For more information on the Internet gateway, please refer to below URL:

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

Ask our Experts



QUESTION 65 UNATTEMPTED

What is the term used to identify networks that present a clearly defined external routing policy to the Internet

- ☒ A. Autonomous System numbers ✓
- ☐ B. Internet System numbers
- ☐ C. Autonomous System locators
- ☐ D. Internet System locators

Explanation :

Answer - A

Autonomous System numbers are used to identify networks that present a clearly defined external routing policy to the Internet. AWS Direct Connect requires an ASN to create a public or private virtual interface. You may use a public ASN which you own, or you can pick any private ASN number between 64512 to 65535 range.

For more information on Autonomous System numbers, one can visit the below URL:

- [https://en.wikipedia.org/wiki/Autonomous_system_\(Internet\)](https://en.wikipedia.org/wiki/Autonomous_system_(Internet))
([https://en.wikipedia.org/wiki/Autonomous_system_\(Internet\)](https://en.wikipedia.org/wiki/Autonomous_system_(Internet)))

Ask our Experts



QUESTION 66 UNATTEMPTED

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

- ☐ A. /28
- ☒ B. /27 ✓
- ☐ C. /25

☐ D. /24

Explanation :

Answer – B

We need to keep in mind that AWS reserves 5 IP addresses in each subnet, so we would only end up with 11 usable IP addresses in this scenario.

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block **10.0.0.0/24** (<http://10.0.0.0/24>) , the following five IP addresses are reserved:

- **10.0.0.0** (<http://10.0.0.0/24>) : Network address.
- **10.0.0.1** (<http://10.0.0.0/24>) : Reserved by AWS for the VPC router.
- **10.0.0.2** (<http://10.0.0.0/24>) : Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. For more information, see Amazon DNS Server.
- **10.0.0.3** (<http://10.0.0.0/24>) : Reserved by AWS for future use.
- **10.0.0.255** (<http://10.0.0.0/24>) : Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

For more information , please visit the link:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#vpc-sizing-ipv4 (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#vpc-sizing-ipv4)

Ask our Experts



QUESTION 67 UNATTEMPTED

Which of the following attributes of the VPC allow for Instances launched in a VPC to receive public DNS names

- ☐ A. enableDnsSupport
- ☐ B. enablepublicdns

- ☐ C. enableDnsHostnames ✓
- ☐ D. enabledns

Explanation :

Answer - C

Your VPC has attributes that determine whether your instance receives public DNS hostnames, and whether DNS resolution through the Amazon DNS server is supported.

1. enableDnsHostnames - Indicates whether the instances launched in the VPC get public DNS hostnames.

2. enableDnsSupport - Indicates whether the DNS resolution is supported for the VPC.

For more information on VPC DNS, one can visit the below URL:

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

Ask our Experts



QUESTION 68 UNATTEMPTED

You are the network administrator for a company. There is a requirement to connect VPC's which are located in different regions. Which of the following options can be used to fulfil this requirement. Choose 3 answers from the options given below

- ☐ A. VPC Peering
- ☐ B. Software VPN ✓
- ☐ C. Software to Hardware VPN ✓
- ☐ D. Internet based VPN ✓

Explanation :

Answer – B,C and D

VPC Peering connections can only be used if the VPC's are in the same region

For more information on such networking options, one can visit the below URL:

- https://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf
(https://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf)

Note: Question is outdated now. It will be replaced ASAP.

Reinvent 2017 update: AWS does support peering across regions

from . <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

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

"internet based VPN" is not a term

QUESTION 69

UNATTEMPTED

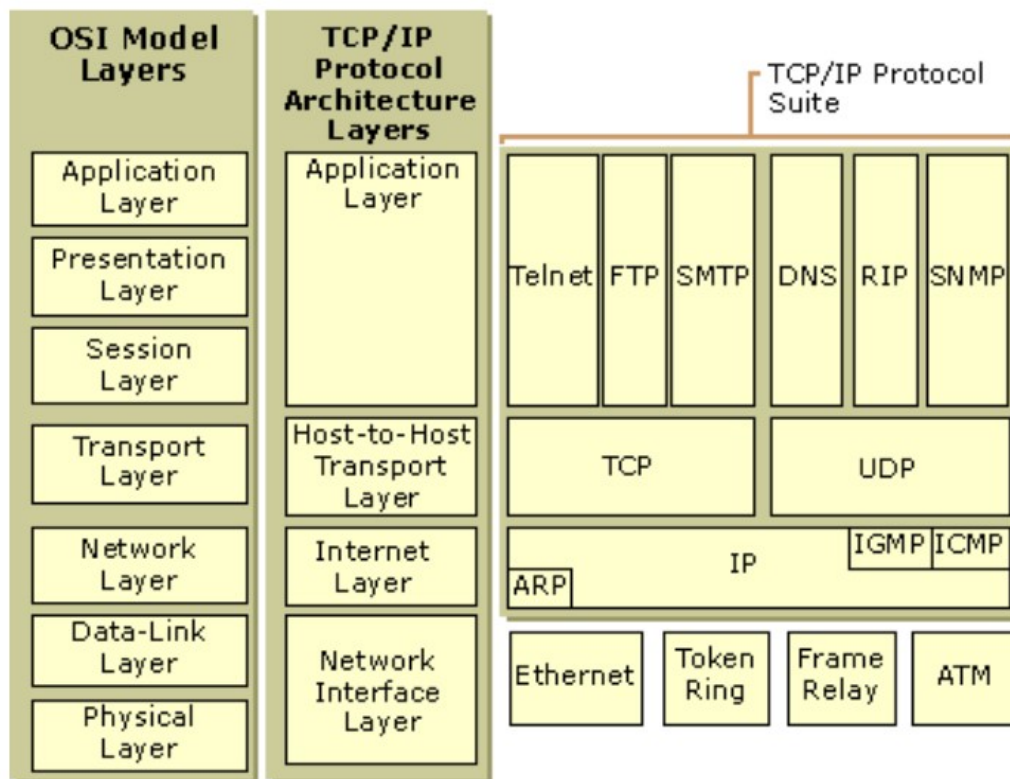
As per the TCP/IP model, which layer makes use of the protocols such as FTP and SMTP

- ☐ A. Session Layer
- ☐ B. Transport Layer
- ☐ C. Application Layer ✓
- ☐ D. Data-Link Layer

Explanation :

Answer - C

The below diagram shows the TCP/IP Model



For more information on the TCP IP Model, one can visit the below URL:

- <https://technet.microsoft.com/en-us/library/cc958821.aspx>
(<https://technet.microsoft.com/en-us/library/cc958821.aspx>)

Ask our Experts



QUESTION 70

UNATTEMPTED

Which of the following are correct when it comes to IP addressing in AWS. Choose 3 answers from the options given below

- ☐ A. You can assign a secondary private IPv4 address to any network interface. ✓
- ☐ B. You can assign multiple IPv6 addresses to a network interface that's in a subnet that has an associated IPv6 CIDR block. ✓
- ☐ C. You can assign a secondary IPv4 from the IPv4 CIDR block range of the VPC to any network interface.
- ☐ D. Security groups apply to network interfaces, not to IP addresses ✓

Explanation :

Answer – A,B and D

The AWS documentation mentions the following

1. You can assign a secondary private IPv4 address to any network interface. The network interface can be attached to or detached from the instance.
2. You can assign multiple IPv6 addresses to a network interface that's in a subnet that has an associated IPv6 CIDR block.
3. You must choose the secondary IPv4 from the IPv4 CIDR block range of the subnet for the network interface.
4. Security groups apply to network interfaces, not to IP addresses

For more information on IP addressing, one can visit the below URL:

- <http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/MultipleIP.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/MultipleIP.html>)

Ask our Experts



QUESTION 71

UNATTEMPTED

Which of the following is not a resource record type in Route53?

- ☒ A. IPv6 ✓
- ☐ B. CNAME

☐ C. TXT

☐ D. MX

Explanation :

Answer A

The following record types can be created in Route53

- 1) A
- 2) AAAA
- 3) CAA
- 4) CNAME
- 5) MX
- 6) NAPTR
- 7) NS
- 8) PTR
- 9) SOA
- 10) SPF
- 11) SRV
- 12) TXT

For more information on Resource record types, one can visit the below URL:

- <http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/ResourceRecordTypes.html>
(<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/ResourceRecordTypes.html>)

Ask our Experts



QUESTION 72 UNATTEMPTED

You are planning to setup a load balancing solution in AWS. There is a requirement for using TCP Routing for the back end instances which has Configurable idle connection timeout. Which of the below types of load balancers should be used for this purpose

- ☒ A. Classic Load balancer ✓
- ☐ B. Application Load balancer
- ☐ C. Network Load balancer
- ☐ D. Secondary Load balancer

Explanation :

Answer – A

The AWS documentation mentions the following

Feature	Application Load Balancer	Network Load Balancer	Classic Load Balancer
Protocols	HTTP, HTTPS	TCP	TCP, SSL, HTTP, HTTPS
Platforms	VPC	VPC	EC2-Classic, VPC
Health checks	✓	✓	✓
CloudWatch metrics	✓	✓	✓
Logging	✓	✓	✓
Zonal fail-over	✓	✓	✓
Connection draining (deregistration delay)	✓	✓	✓
Load Balancing to multiple ports on the same instance	✓	✓	
WebSockets	✓	✓	
IP addresses as targets	✓	✓	
Load balancer deletion protection	✓	✓	
Path-Based Routing	✓		
Host-Based Routing	✓		
Native HTTP/2	✓		
Configurable idle connection timeout	✓		✓
Cross-zone load balancing	✓	✓	✓
SSL offloading	✓		✓
Server Name Indication (SNI)	✓		
Sticky sessions	✓		✓
Back-end server encryption	✓		✓
Static IP		✓	
Elastic IP address		✓	
Preserve Source IP address		✓	

- <https://aws.amazon.com/elasticloadbalancing/details/#details>
(<https://aws.amazon.com/elasticloadbalancing/details/#details>)

Ask our Experts



QUESTION 73 UNATTEMPTED

Which of the following statements are true when it comes to AWS Direct Connect?
Choose 3 answers from the options given below.

- ☐ A. It is a private connection that is separate from the internet ✓

- ☐ B. It can help have a consistent network performance ✓
- ☐ C. Each connection can be used across multiple AWS regions ✓
- ☐ D. Both 10 gigabit and 100 gigabit speed options are available

Explanation :

Answer – A,B and C

The AWS documentation mentions the following

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1-gigabit or 10-gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing Internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the region with which it is associated, and you can use a single connection in a public region or AWS GovCloud (US) to access public AWS services in all other public regions.

For more information on AWS Direct connect please see the below link

<http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

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

Ask our Experts



QUESTION 74 UNATTEMPTED

Which of the following statements are true when it comes to associating a link aggregation group with an AWS direct connect connection

- ☐ A. The connection can be on a different AWS device
- ☐ B. You can associate an existing connection with a LAG ✓
- ☐ C. The connection can be standalone, or it can be part of another LAG ✓
- ☐ D. It can be used to aggregate multiple 1 gigabit or 10 gigabit connections at a single AWS Direct Connect endpoint ✓

Explanation :

Answer – B,C and D

The AWS documentation mentions the following

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.

You can associate an existing connection with a LAG. The connection can be standalone, or it can be part of another LAG. The connection must be on the same AWS device and must use the same bandwidth as the LAG. If the connection is already associated with another LAG, you cannot re-associate it if removing the connection causes the original LAG to fall below its threshold for minimum number of operational connections.

For more information on link aggregation group please see the below link:

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

Ask our Experts



QUESTION 75 UNATTEMPTED

When defining a subnet in AWS , how many IP addresses are reserved by AWS.

- ☐ A. 1
- ☐ B. 3
- ☐ C. 4
- ☒ D. 5 ✓

Explanation :

Answer - D

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

For more information on IP Reservation, please visit the 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



What is the default time interval period for the logs collected by the Classic Load Balancer in AWS?

- ☐ A. 5 minutes
- ☐ B. 20 minutes
- ☒ C. 60 minutes ✓
- ☐ D. 90 minutes

Explanation :

Answer - C

The AWS documentation mentions the following

Elastic Load Balancing publishes a log file for each load balancer node at the interval you specify. You can specify a publishing interval of either 5 minutes or 60 minutes when you enable the access log for your load balancer. By default, Elastic Load Balancing publishes logs at a 60-minute interval

For more information on ELB access logs, please visit the link:

- <http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html>
(<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html>)

Ask our Experts



When using AWS config to monitor your resources what are the 2 types of triggers that can be setup?

- ☒ A. Configuration Changes ✓
- ☒ B. Periodic ✓
- ☐ C. Templates
- ☐ D. Monitoring

Explanation :

Answer – A and B

1. Configuration Changes - AWS Config runs evaluations for the rule when certain types of resources are created, changed, or deleted.
2. Periodic - AWS Config runs evaluations for the rule at a frequency that you choose (for example,

every 24 hours).

For more information on AWS config rules, please visit the link:

- <http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>
(<http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>)

Ask our Experts



QUESTION 78 UNATTEMPTED

For which of the below components can VPC Flow logs be enabled for? Choose 3 answers for the options given below

- ☐ A. VPC ✓
- ☐ B. Elastic IP
- ☐ C. Subnet ✓
- ☐ D. Network interface ✓

Explanation :

Answer – A,C and D

You can create a flow log for a VPC, a subnet, or a network interface

For more information on VPC Flow Logs, please visit the link:

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

Ask our Experts



QUESTION 79 UNATTEMPTED

Which of the following statements are true with regards to Security Groups which can be defined for EC2 Instances. Choose 3 answers from the options given below.

- ☐ A. In Security Groups you can define both allow and deny rules
- ☐ B. You can specify separate rules for inbound and outbound traffic. ✓
- ☐ C. When you create a security group, it has no inbound rules ✓
- ☐ D. Security groups are stateful in nature ✓

Explanation :

Answer – B,C and D

The AWS documentation mentions the following on Security groups

1. You can specify allow rules, but not deny rules.
2. You can specify separate rules for inbound and outbound traffic.
3. When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
4. Security groups are stateful – if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules

For more information on Security Groups, please refer to below URL:

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

Ask our Experts



QUESTION 80

CORRECT

You have a subnet with a CIDR block of 10.0.1.0/24. Which of the following can be IP address which would be assigned to an EC2 Instance launched in this subnet.

Choose 3 answers from the options given below.

- ☒ A. 10.0.1.4 ✓
- ☒ B. 10.0.1.253 ✓
- ☐ C. 10.0.1.3
- ☒ D. 10.0.1.254 ✓

Explanation :

Answer – A,B and D

The AWS Documentation mentions the following

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. For more information, see Amazon DNS Server

(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#AmazonDNS).

- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

For more information on subnets and VPC's, please refer to below URL:

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

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14612>)

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/>)

Company

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

Mobile App



Android Coming Soon



iOS Coming Soon

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>)