PRACTICE TEST IV

Attempt	1
Marks Obtained	0 / 80
Your score is	0.0%

Completed on	Sunday , 03 February 2019 , 11:09 PM
Time Taken	00 H 00 M 18 S
Result	Fail

Domains / Topics wise Quiz Performance Report

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

80	0	1	79
Questions	Correct	Incorrect	Unattempted

Show Answers

All	▼

QUESTION 1   UNATTEMPTED

Which of the following is a not a recommended Private IP range that should be used when defining your internal VPC's.

○   **A.**   10.0.0.0 - 10.255.255.255

○   **B.**   20.0.0.0 - 20.255.255.255   ✔

○   **C.**   172.16.0.0 - 172.31.255.255

○   **D.**   192.168.0.0 - 192.168.255.255

Explanation :

Answer - B

When the VPC is created, the following private IPv4 address ranges should be used as specified in RFC 1918 (http://www.faqs.org/rfcs/rfc1918.html)

·   10.0.0.0 - 10.255.255.255 (10/8 prefix)

·   172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

·   192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

For more information on VPC and Subnets, please visit 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 2   UNATTEMPTED

Your VPC currently has 2 subnets in AWS. The VPC has a CIDR block of 10.0.0.0/16 and the subnets have a CIDR block of 10.0.1.0/24 and 10.0.2.0/24 respectively. You decide on creating a custom route table for each subnet. When you initially create a custom route table , which of the following routes will be present in the route table automatically,

○   **A.**   A route for 10.0.0.0/16 as the destination   ✔

○   **B.**   A route for 10.0.1.0/24 as the destination

○   **C.**   A route for 10.0.2.0/24 as the destination

○   **D.** There will be no default route in the route table

Ask our Experts

👍 👎

QUESTION 3   UNATTEMPTED

You have a set of EC2 Instances which are part of a public subnet in a VPC. There is a requirement to ensure that administrators can only SSH from a workstation with an IP of 59.12.10.10. Which of the following CIDR blocks would be added to the Inbound Rules for the Security Group to fulfil this requirement

○   **A.** 59.12.10.10/28

○   **B.** 59.12.10.10/16

○   **C.** 59.12.10.10/32 ✔

○   **D.** 59.12.10.10/24

Explanation :

Answer – C

Since we just want to specify one IP address , the /32 CIDR notation specifies a single IP address and should be added accordingly to the Security Group

For more information on CIDR notation, please visit the below link:

- https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing (https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

Ask our Experts

👍 👎

QUESTION 4   UNATTEMPTED

You currently have a set of EC2 Instances in a private subnet that communicates to the internet via a NAT instance. You now plan to start using a NAT gateway and replace the usage of the NAT Instance. During the transition , which of the following needs to be noted

○ **A.** You can safely do the transition since during the transition , the existing connections will be moved from the NAT instance to the gateway.

○ **B.** The existing connections to the NAT instance will go through a connection draining period, hence there will be no disruptions to the existing service.

○ **C.** There will be a slight disruption which needs to be accounted for because the current connections to the NAT instance will be dropped. ✔

○ **D.** It is not possible to replace a NAT gateway with a NAT instance.

Explanation :

Answer - C
The AWS documentation mentions the following

If you change your routing from a NAT instance to a NAT gateway, or if you disassociate the Elastic IP address from your NAT instance, any current connections are dropped and have to be re-established. Ensure that you do not have any critical tasks (or any other tasks that operate through the NAT instance) running.

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

- 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 5   UNATTEMPTED

You have configured a web server listening on port 80 on an EC2 Instance. You are trying to reach the home page of the web server but are not able to do so. You've checked that the Internet gateway is attached to the VPC , and the route tables have been modified accordingly. You have also attached an Elastic IP address to the EC2 Instance. Which of the following could be the cause for the underlying issue.

- ○ **A.** Check the Outbound Security Group rules, this could be denying the traffic on port 80.

- ○ **B.** Check the Inbound Rules for the NACL , this could be denying the traffic ✔

- ○ **C.** You need to have a public IP defined for the EC2 Instance, since the Elastic IP will not work.

- ○ **D.** Change the Internet gateway as there could be an issue with the Internet gateway.

Explanation :

Answer – B
If you have a DENY rule as shown below for the port traffic which is lower in precedence for the

NACL, this could also be a reason as to why the traffic is being blocked.

Summary	Inbound Rules	Outbound Rules	Subnet Associations	Tags

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules ▼

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
95	HTTP (80)	TCP (6)	80	0.0.0.0/0	DENY
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

For more information on NACL, please visit the below link:

- 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 6   UNATTEMPTED

Which of the following statements is false when it comes to the Elastic Network Interface?

- ○ **A.** You can attach a network interface to an instance when it's running

- ○ **B.** You can detach the secondary network interface and attach it to another instance in the same subnet.

- ○ **C.** You can detach the Primary network interface and attach it to another instance in the same subnet. ✔

- ○ **D.** You have a secondary private IP for a Network Interface

Explanation :

Answer - C

The AWS documentation mentions the following on some of the points regarding Elastic Network Interfaces

1)   You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).

2)   You can detach secondary (eth*N*) network interfaces when the instance is running or stopped. However, you can't detach the primary (eth0) interface.

3)   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 the Elastic Network Interface, please visit 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

👍 👎

An application has been built with the appropriate AWS SDK. This application interacts with the S3 service in AWS. This application is going to be deployed in a private subnet. Which of the following should be done to ensure that the application can successfully interact with the S3 service

○   **A.** Make the subnet as a public subnet

○   **B.** Attach an Internet gateway to the VPC

○   **C.** Create a VPC S3 endpoint ✔

○   **D.** Attach a Virtual Private gateway to the VPC

Explanation :

Answer - C

One can use the S3 VPC endpoint

A VPC endpoint enables you to privately connect your VPC to an AWS service without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in other services. Traffic between your VPC and the AWS service does not leave the Amazon network.

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

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

Ask our Experts

👍 👎

QUESTION 8 UNATTEMPTED

Which are the 3 types of health checks that you can monitor using Route53 health checks. Choose 3 answers from the options given below

☐ A. Health checks that monitor an endpoint ✔

☐ B. Health checks that monitor CloudWatch alarms ✔

☐ C. Health checks that monitor CloudWatch logs

☐ D. Health checks that monitor other health checks ✔

Explanation :

Answer – A,B and D

The AWS documentation mentions the following

There are 3 types of health checks available in Route53

1) Health checks that monitor an endpoint - You can configure a health check that monitors an endpoint that you specify either by IP address or by domain name

2) Health checks that monitor CloudWatch alarms - You can create CloudWatch alarms that monitor the status of CloudWatch metrics, such as the number of throttled read events for a Amazon DynamoDB database or the number of Elastic Load Balancing hosts that are considered healthy

3) Health checks that monitor other health checks - You can create a health check that monitors whether Amazon Route 53 considers other health checks healthy or unhealthy

For more information on Route53 health checks, please visit the below link:

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-types.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-types.html)

Ask our Experts

👍 👎

QUESTION 9   UNATTEMPTED

Which of the following is not a protocol which can be used when monitoring an endpoint using Route53 health checks

○   **A.** HTTP

○   **B.** HTTPS

○   **C.** TCP

○   **D.** UDP ✔

Explanation :

Answer - D
The method that you want Amazon Route 53 to use to check the health of your endpoint:
·   HTTP – Amazon Route 53 tries to establish a TCP connection. If successful, Amazon Route 53 submits an HTTP request and waits for an HTTP status code of 200 or greater and less than 400.
·   HTTPS – Amazon Route 53 tries to establish a TCP connection. If successful, Amazon Route 53 submits an HTTPS request and waits for an HTTP status code of 200 or greater and less than 400.

· TCP – Amazon Route 53 tries to establish a TCP connection.

For more information on creating route53 health checks, please visit the below link:

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-creating.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-creating.html)

Ask our Experts

👍 👎

QUESTION 10   UNATTEMPTED

Which of the following is a type of record set that cannot be created for a private hosted zone in Route53.

○ **A.** Geolocation ✔

○ **B.** Simple

○ **C.** Failover

○ **D.** Weighted

Explanation :

Answer - A

You can use the following routing policies when you create resource record sets in a private hosted zone:

- Simple

- Failover

- Weighted

For more information on Private hosted zones, please visit the below link:

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html)

👍 👎

QUESTION 11   UNATTEMPTED

You are planning to use the AWS classic load balancer in AWS. You are preparing the subnets which will be used in the load balancer. Which of the following bitmask is the minimum which is required for the subnet in order to be used with the Load Balancer

○   A. /30

○   B. /29

○   C. /28

○   D. /27 ✔

Explanation :

Answer – D
This is mentioned in the AWS documentation
To ensure that your load balancer can scale properly, verify that each subnet for your load balancer has a CIDR block with at least a /27 bitmask (for example, 10.0.0.0/27) and has at least 8 free IP addresses. Your load balancer uses these IP addresses to establish connections with the instances.
For more information on setting up the instances in an ELB, please visit the below link:

• http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-backend-instances.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-backend-instances.html)

👍 👎

You have just set up a classic load balancer with EC2 Instances distributed over 2 subnets. The first subnet has one instance and the other subnet has 3 instances. You have noticed that the load is high on the single instance located in the first subnet. Which of the following settings can be set on the load balancer to ensure even distribution of traffic across all of the instances

- ○   **A.** Configure connection draining
- ○   **B.** Configure sticky sessions
- ○   **C.** Configure Proxy protocol
- ○   **D.** Configure Cross-Zone Load balancing ✔

Explanation :

Answer - D
The AWS documentation mentions the following
If the load balancer nodes for your Classic Load Balancer can distribute requests regardless of Availability Zone, this is known as *cross-zone load balancing*. With cross-zone load balancing enabled, your load balancer nodes distribute incoming requests evenly across the Availability Zones enabled for your load balancer
For more information on cross zone load balancing, please visit the below link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-crosszone-lb.html
(http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-crosszone-lb.html)

Ask our Experts

👍 👎

You are planning to use the CIDR block of 10.0.1.0/27 for designing the subnets in AWS. How many maximum possible subnets are possible with this CIDR configuration?

○   A. 1 * 27

○   B. 2 * 28   ✔

○   C. 2 * 32

○   D. 4 * 16

Explanation :

Answer - B

In AWS, a VPC is limited to /28 CIDR range to the maximum number of subnets is actually 2.

Ex: 1 x /27 CIDR can be split into 2 x /28 subnets.

CIDR Calculator

IP Address	CIDR Netmask
10.0.1.0	255.255.255.224 ▼

Mask Bits	Wildcard Mask
27 ▼	0.0.0.31

Maximum Subnets	Maximum Addresses
32 ▼	30 ▼

CIDR Network (Route)	Net: CIDR Notation
10.0.1.0	10.0.1.0/27

CIDR Address Range

10.0.1.0 - 10.0.1.31

Ask our Experts

👍 👎

QUESTION 14   UNATTEMPTED

Which of the following cannot be used to enable the Proxy protocol for the classic load balancer

○   A. The AWS API

○   B. A Script which uses the AWS CLI

○   C. The AWS CLI

○   **D.** The AWS Management Console ✔

Explanation :

Answer - D

The AWS Management Console does not support enabling Proxy Protocol.

For more information on the 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

👍 👎

QUESTION 15   UNATTEMPTED

When you want to create an AWS Direct Connect connection in the AWS console, what are the 2 artefacts which are required? Choose 2 answers from the options given below

☐   **A.** AWS Direct Connection location ✔

☐   **B.** The Virtual Private gateway

☐   **C.** The Customer gateway

☐   **D.** The port speed ✔

Explanation :

Answer – A and D

The AWS documentation mentions the following

To create an AWS Direct Connect connection, you need the following information

1) AWS Direct Connect location - Work with a partner in the AWS Partner Network (APN) to help you establish network circuits between an AWS Direct Connect location and your data center, office, or colocation environment, or to provide colocation space within the same facility as the AWS Direct Connect location

2) Port speed - 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.
 For more information on working with AWS Direct Connect connections, please refer to 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 16   UNATTEMPTED

Which of the following features of S3 allows for the bucket owner not liable to be charged for the objects requests and downloads from a bucket from users

○   **A.** Transfer acceleration

○   **B.** Requester Pays ✔

○   **C.** Billing request

○   **D.** Reduced S3 costs

Explanation :

Answer - B
The AWS documentation mention
In general, bucket owners pay for all Amazon S3 storage and data transfer costs associated with their bucket. A bucket owner, however, can configure a bucket to be a Requester Pays bucket. With Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket. The bucket owner always pays the cost of storing data.
For more information on requester pays, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/RequesterPaysBuckets.html
  (http://docs.aws.amazon.com/AmazonS3/latest/dev/RequesterPaysBuckets.html)

Ask our Experts

👍 👎

QUESTION 17   UNATTEMPTED

Which of the following statements on VPC Flow Logs is incorrect

- ○ **A.** After you've created a flow log, you cannot change its configuration
- ○ **B.** You can create a flow log for a VPC, a subnet, or a network interface
- ○ **C.** Flow log data is published to a log group in CloudWatch Log
- ○ **D.** The log data is captured in real time. ✔

Explanation :

Answer - D
The AWS documentation mentions the following on VPC Flow Logs
A flow log record represents a network flow in your flow log. Each record captures the network flow for a specific 5-tuple, for a specific capture window. A 5-tuple is a set of 5 different values that specify the source, destination, and protocol for an Internet protocol (IP) flow. The capture window is a duration of time during which the flow logs service aggregates data before publishing flow log records. The capture window is approximately 10 minutes, but can take up to 15 minutes.
For more information on VPC 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

Which of the following statements on the egress-only Internet gateway is incorrect

○ **A.** An egress-only Internet gateway is stateful

○ **B.** You can associate a security group with an egress-only Internet gateway ✔

○ **C.** You can use a network ACL to control the traffic to and from the subnet for which the egress-only Internet gateway routes traffic

○ **D.** An egress-only Internet gateway is for use with IPv6 traffic only

---

Explanation :

Answer - B
The AWS documentation mentions the following on egress-only Internet gateway
An egress-only Internet gateway is stateful: it forwards traffic from the instances in the subnet to the Internet or other AWS services, and then sends the response back to the instances.
An egress-only Internet gateway has the following characteristics:

• You cannot associate a security group with an egress-only Internet gateway. You can use security groups for your instances in the private subnet to control the traffic to and from those instances.

• You can use a network ACL to control the traffic to and from the subnet for which the egress-only Internet gateway routes traffic.

For more information on the egress only internet gateway , please refer to 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

In order to create VPC Flow logs, which of the following are required. Choose 3 answers from the options given below

- ☐ **A.** The resource for which the log needs to be created. ✔
- ☐ **B.** An IAM Role with privilege to publish the logs to Cloudwatch ✔
- ☐ **C.** A Cloudwatch Log Group ✔
- ☐ **D.** A Cloudwatch Log Stream

Explanation :

Answer – A,B and C
To create a flow log, you specify the resource for which you want to create the flow log, the type of traffic to capture (accepted traffic, rejected traffic, or all traffic), the name of a log group in CloudWatch Logs to which the flow log will be published, and the ARN of an IAM role that has sufficient permission to publish the flow log to the CloudWatch Logs log group.
For more information on VPC 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

👍 👎

Which of the following protocol+port is used by Amazon Workspaces for authentication

- ○ **A.** TCP/80
- ○ **B.** UDP/443

○   **C.** HTTP/80

○   **D.** HTTPS/443 ✔

Explanation :

Answer - D

Client applications use HTTPS over port 443 for all authentication and session-related information

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

- http://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html (http://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html)

Ask our Experts

👍   👎

QUESTION 21   UNATTEMPTED

Which of the following types of protocols is the BGP protocol normally classified as?

○   **A.** Link state

○   **B.** Distance vector

○   **C.** Path Vector ✔

○   **D.** Link Vector

Explanation :

Answer – C

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol

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

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

Ask our Experts

👍 👎

QUESTION 22 UNATTEMPTED

If a VPN connection exists between an on-premise facility and AWS , and Workspaces are being used. What is the minimum amount of MTU which should be supported by the connection?

- ○ **A.** 500
- ○ **B.** 900
- ○ **C.** 1200 ✔
- ○ **D.** 1500

Explanation :

Answer - C
This is given in the AWS documentation
If users will access their WorkSpaces through a virtual private network (VPN), the connection must support a maximum transmission unit (MTU) of at least 1200 bytes.
For more information on AWS Workspaces networking requirements, please refer to the below URL:

- http://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-network-requirements.html
  (http://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-network-requirements.html)

QUESTION 23   UNATTEMPTED

A VPN has been setup between AWS and the on-premise network. An EC2 Instance is launched in the VPC to test the connection via the ping command. Which of the below must be done to ensure the test works as desired. Choose 3 answers from the options given below.

☐   **A.** Ensure the Security Groups allow Inbound ICMP traffic ✔

☐   **B.** Ensure the Security Groups allow Outbound ICMP traffic

☐   **C.** Ensure that the Network Group allows Inbound ICMP traffic ✔

☐   **D.** Ensure that the Network Group allows Outbound ICMP traffic ✔

Explanation :

Answer – A,C and D
After you create the VPN connection and configure the customer gateway, you can launch an instance and test the connection by pinging the instance. You need to use an AMI that responds to ping requests, and you need to ensure that your instance's security group is configured to enable inbound ICMP.
Remember that Security Groups are stateful in nature, so you don't need to ensure that Outbound traffic is allowed.
For more information on test VPN connections, please refer to the below URL:

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

Ask our Experts

👍 👎

When using the AWS Direct Connect connection , what is the pricing for Inbound Traffic.

- ○ **A.** $0.02 per GB in all locations
- ○ **B.** It depends on the region for the Direct Connect connection
- ○ **C.** It depends on the AZ for the Direct Connect connection
- ○ **D.** $0.00 per GB in all locations ✔

Explanation :

Answer - D

This is mentioned in the AWS documentation

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

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

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

Ask our Experts

👍 👎

You are currently using Route53 for DNS routing. Your application is hosted on EC2 Instances across multiple regions in an effort to ensure that users across the globe get the best user experience. Which of the below will also help to ensure the user experience is even better.

- ○ **A.** Configure Geolocation routing policies in Route53
- ○ **B.** Configure latency based routing policies in Route53 ✔

○ **C.** Configure weighted based routing policies in Route53

○ **D.** Configure failover based routing policies in Route53

Explanation :

Answer – B

This is mentioned in the AWS documentation

If your application is hosted in multiple Amazon EC2 regions, you can improve performance for your users by serving their requests from the Amazon EC2 region that provides the lowest latency.

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

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Ask our Experts

👍 👎

You have a requirement to host both a private and public hosted zone for the same domain name in Route53. How can this be achieved?

○ **A.** This is not possible in Route53

○ **B.** Create different resources records in the same hosted zone

○ **C.** Configure split-view DNS in Route53 ✔

○ **D.** Create one hosted zone with both the private and public option

---

Explanation :

Answer - C

This is mentioned in the AWS documentation

You can use Amazon Route 53 to configure split-view DNS, also known as split-horizon DNS. If you want to maintain internal and external versions of the same website or application (for example, for testing changes before you make them public), you can configure public and private hosted zones to return different internal and external IP addresses for the same domain name. Just create a public hosted zone and a private hosted zone that have the same domain name, and create the same subdomains in both hosted zones

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

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html)

Ask our Experts

👍 👎

QUESTION 27   UNATTEMPTED

A company currently has 50 employees and would like to use a directory service in AWS. Which of the following would be best suited

○ **A.** Simple AD ✔

○ **B.** AD Connector

○ **C.** Microsoft AD hosted on an EC2 Instance

○ **D.** Microsoft AD

Explanation :

Answer - A
Since the foot print is small , the Simple AD service should suffice.
The AWS documentation mentions the following on the Simple AD
Simple AD is a standalone managed directory that is powered by a Samba 4 Active Directory Compatible Server. It is available in two sizes.
·   Small - Supports up to 500 users (approximately 2,000 objects including users, groups, and computers).
·   Large - Supports up to 5,000 users (approximately 20,000 objects including users, groups,

and computers).

For more information on Simple AD, 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 28   UNATTEMPTED

Which of the following can be used as a means of classifying and managing network traffic and of providing quality of service (QoS) in modern Layer 3 IP networks

○ **A.** BFD

○ **B.** BGP

○ **C.** DSCP ✔

○ **D.** MEP

Explanation :

Answer - C
Differentiated Services Code Point (DSCP) is a means of classifying and managing network traffic and of providing quality of service (QoS) in modern Layer 3 IP networks. It uses the 6-bit Differentiated Services (DS) field in the IP header for the purpose of packet classification. Differentiated services (DiffServ) is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.
For more information please refer to the below URL:

- https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html (https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html)

Ask our Experts

👍 👎

QUESTION 29   UNATTEMPTED

What is the name of the label applied to packets to allow routers to know where to forward in an MPLS network

○ **A.** BFD

○ **B.** BGP

○ **C.** DSCP

○ **D.** FEC ✔

Explanation :

Answer - D
A Forwarding Equivalence Class (FEC) is a term used in Multiprotocol Label Switching (MPLS) to describe a set of packets with similar and / or identical characteristics which may be forwarded the same way; that is, they may be bound to the same MPLS label.
For more information please refer to the below URL:

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

Ask our Experts

👍 👎

There is a requirement to monitor the HTTPS traffic that is being directed to the Cloudfront setup you have in AWS. Which of the following services can be used for this

○ **A.** AWS Shield

○ **B.** AWS Cloudfront logs

○ **C.** AWS WAF ✔

○ **D.** AWS Cloudwatch

Explanation :

Answer – C

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.

For more information on AWS WAF please refer to the below URL:

- http://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html (http://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html)

Ask our Experts

👍 👎

Which of the following is a not an application/implementation for creating a hybrid network between on-premise and AWS?

○ **A.** AWS Direct Connect

○ **B.** VPC Peering ✔

○ **C.** Hardware VPN

○ **D.** Software VPN

Explanation :

Answer – B
VPC Peering is used for peering VPC's and is not used for creating a hybrid solution.
For more information on AWS 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 32   **UNATTEMPTED**

Which of the following metrics can help understand if your infrastructure in AWS (EC2+ELB) is under a DDos attack. Choose 2 answers from the options given below.

☐ **A.** EC2 CPU utilization ✔

☐ **B.** ELB SurgeQueueLength ✔

☐ **C.** HealthyHostCount

☐ **D.** UnHealthyHostCount

Explanation :

Answer – A and B
Definitely the CPU utilization of the backend instances can give an indication of whether the backend instances are under tremendous load.

Surge queue length is defined by the number of requests that are queued by Elastic Load Balancing (ELB). These requests are queued when back-end systems are unable to process incoming requests as fast as the requests are being received

For more information on ELB troubleshooting please refer to the below URL:

- https://aws.amazon.com/premiumsupport/knowledge-center/elb-capacity-troubleshooting/ (https://aws.amazon.com/premiumsupport/knowledge-center/elb-capacity-troubleshooting/)

Ask our Experts

👍 👎

QUESTION 33   UNATTEMPTED

Which of the following is required when creating a VPN connection in AWS.

☐   **A.** Customer gateway ✔

☐   **B.** Internet gateway

☐   **C.** Virtual Private gateway ✔

☐   **D.** BGP

Explanation :

Answer – A and C

The AWS documentation mentions the following

A virtual private *gateway* is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the VPN connection.

A customer gateway is a physical device or software application on your side of the VPN connection.

For more information on AWS VPN 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 34   UNATTEMPTED

When AWS claims that VPC's can operate in dual stack mode , what does that mean?

○ **A.** The VPC has operate on both the TCP and UDP protocol at the same time

○ **B.** The VPC can have an Internet gateway and Customer gateway attached at the same time

○ **C.** The VPC can operate in both IPv4 and IPv6 ✔

○ **D.** The VPC can have an Internet gateway and Virtual private gateway attached at the same time

Explanation :

Answer - C
The AWS documentation mentions the following
Your VPC can operate in dual-stack mode — your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other.
For more information on VPC and IPv6 please refer to the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html)

Ask our Experts

👍 👎

QUESTION 35   UNATTEMPTED

What is the bandwidth limitation of the Internet gateway provided by AWS?

○ **A.** 50Mbps

○ **B.** 100Mbps

○ **C.** 200 Mbps

○ **D.** There is no limit ✔

Explanation :

Answer – D

This is mentioned in the AWS documentation

An Internet gateway is horizontally-scaled, redundant, and highly available. It imposes no bandwidth constraints.

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

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

Ask our Experts

👍 👎

QUESTION 36   UNATTEMPTED

Which of the below CIDR notation mask is assigned to a subnet which holds IPv6 IP addresses ?

○ **A.** /32

○ **B.** /48

○ **C.** /56

○ **D.** /64 ✔

Explanation :

Answer - D
For IPv6, the subnet size is fixed to be a /64. Only one IPv6 CIDR block can be allocated to a subnet

Q. Is there a limit on how large or small a subnet can be?

The minimum size of a subnet is a /28 (or 14 IP addresses.) for IPv4. Subnets cannot be larger than the VPC in which they are created.

For IPv6, the subnet size is fixed to be a /64. Only one IPv6 CIDR block can be allocated to a subnet.

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

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

Ask our Experts

👍 👎

QUESTION 37   UNATTEMPTED

Which of the below mentioned services can be used to monitor the account activity in your AWS account

○   **A.** AWS Cloudtrail ✔

○   **B.** AWS Cloudwatch

○   **C.** AWS Cloudwatch logs

○   **D.** Account Reports

Explanation :

Answer – A

The AWS documentation mentions the following

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 the below URL:

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

Ask our Experts

👍 👎

QUESTION 38   UNATTEMPTED

Which of the below mentioned services can be used to monitor changes to your infrastructure.

○ **A.** AWS Cloudtrail

○ **B.** AWS Cloudwatch

○ **C.** AWS Cloudwatch logs

○ **D.** AWS Config ✔

Explanation :

Answer - D

The AWS documentation mentions the following

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

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

- http://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html (http://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html)

👍 👎

QUESTION 39   UNATTEMPTED

You have enabled logs for a classic load balancer. There is a need to perform SQL queries on the log files. Which of the below actions would you perform. Choose 2 answers from the options given below

- ☐ **A.** Configure the logs to be copied to S3 ✔
- ☐ **B.** Configure the logs to be copied to Athena
- ☐ **C.** Use the Athena service to query the logs ✔
- ☐ **D.** Use the EMR service to query the logs

Explanation :

Answer – A and C
Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.
So first ensure the logs are copied to S3.
For more information on ELB access log collection, please refer to the below URL:

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

👍 👎

Which of the following record types in Route53 is used for IPv6 addresses?

○ **A.** A

○ **B.** AAAA ✔

○ **C.** CNAME

○ **D.** PTR

Explanation :

Answer - B

The value for a AAAA record is an IPv6 address in colon-separated hexadecimal format

For more information on the resource record types in Route53, please refer to 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 41   UNATTEMPTED

You currently have an application hosted on an ELB with EC2 Instances running in AWS. Route53 is used as the DNS Service. You are planning on deploying a new version of the application which will have a new ELB with EC2 Instances. But you want this transition to be phased out so that a percentage of users get access to the new application. Once the new application is confirmed as working that the entire user base can be switched over. How would you configure Route53 in this case?

○ **A.** Configure Route53 with the Weighted routing policy ✔

○ **B.** Configure Route53 with the Failover routing policy

○ **C.** Configure Route53 with the Latency routing policy

○ **D.** Configure Route53 with the Simple routing policy

Explanation :

Answer – A

The AWS documentation mentions the following

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software

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

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Ask our Experts

👍 👎

QUESTION 42   UNATTEMPTED

Which of the following allows private EC2 Instances in your VPC have the ability to work with AWS resources without the need of an an internet gateway, NAT device, public IP address, or VPN connection

○ **A.** PublicLink

○ **B.** VPCLink

○ **C.** PrivateLink ✔

○ **D.** AWSLink

Explanation :

Answer - C
The AWS documentation mentions the following
AWS PrivateLink is a highly available, scalable technology that enables you to privately access some AWS services from your VPC. You do not require an internet gateway, NAT device, public IP address, or VPN connection to communicate with the supported AWS service. Traffic between your VPC and the service does not leave the Amazon network.
For more information on the PrivateLink, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html#what-is-privatelink
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html#what-is-privatelink)

Ask our Experts

👍 👎

QUESTION 43   UNATTEMPTED

You have created a custom VPC and create a subnet. You have launched an EC2 in that subnet. You have noticed that the EC2 Instance is not being assigned a public IP address. What changes need to be done to ensure the EC2 Instance can get a public IP address. Choose 2 answers from the options given below

- [ ] **A.** Ensure an Internet gateway is attached to the VPC
- [ ] **B.** Ensure the Auto-assign attribute for the subnet is marked as 'Yes' ✔
- [ ] **C.** Ensure that when the EC2 Instance is launched
- [ ] **D.** Ensure that when the wizard is used during launch time of the EC2 Instance , the setting is marked as enabled for Public IP for the EC2 Instance. ✔

Explanation :

Answer – B and D

By default, nondefault subnets have the IPv4 public addressing attribute set to false, and default subnets have this attribute set to true. An exception is a nondefault subnet created by the Amazon EC2 launch instance wizard — the wizard sets the attribute to true

For more information on public IP adressing, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#subnet-public-ip (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#subnet-public-ip)

Ask our Experts

👍 👎

QUESTION 44   UNATTEMPTED

Which of the following are ways that Direct Connect connection can be setup. Choose 3 answers from the options given below

☐ **A.** At an AWS Direct Connect location ✔

☐ **B.** Via an AWS Partner Network ✔

☐ **C.** Via an existing VPN connection

☐ **D.** Through a hosted connection provided by a member of the APN ✔

Explanation :

Answer – A,B and D

The AWS documentation mentions the following

You can set up an AWS Direct Connect connection in one of the following ways:

· At an AWS Direct Connect location.

· Through a member of the AWS Partner Network (APN) or a network carrier.

· Through a hosted connection provided by a member of the APN.

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

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

👍 👎

QUESTION 45   UNATTEMPTED

Once you have created an AWS Direct Connect connection, how can you start working with connecting to resources in your VPC and other public resources? Choose 2 answers from the options given below

- ☐ **A. Create a VPC Peering connection**
- ☐ **B. Create a private virtual interface** ✔
- ☐ **C. Create a privatelink connection**
- ☐ **D. Create a public virtual interface** ✔

Explanation :

Answer – B and D
The AWS documentation mentions the following
After you have placed an order for an AWS Direct Connect connection, you must create a virtual interface to begin using it. 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. For more information on AWS Direct Connect getting started, please refer to the below URL:

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

👍 👎

Your AWS infrastructure currently has 4 VPC's. Your company has established an AWS Direct Connect connection from the on-premise to the AWS infrastructure. How many private interfaces would you configure?

- ○ **A.** None. You can use the resources in the VPC in the normal way.

- ○ **B.** One. One Virtual Interface is enough for accessing the VPC's

- ○ **C.** Four. One Virtual Interface for each VPC ✔

- ○ **D.** Eight. Two Virtual Interface(One for Incoming and one for Outgoing) for each VPC.

Explanation :

Answer - C
For private virtual interfaces, you need one private virtual interface for each VPC to connect to from the AWS Direct Connect connection.
For more information on working with 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

👍 👎

When working with AWS Workspaces , what is the recommendation for the Subnets required.

- ○ **A.** Have one private and one public subnet

○ **B.** Have two private and one public subnet ✔

○ **C.** Have one private and two public subnet

○ **D.** Have two private and two public subnet

Explanation :

Answer - B
The AWS documentation mentions the following
Amazon WorkSpaces launches your WorkSpaces in a virtual private cloud (VPC). If you use
AWS Directory Service to create a Microsoft AD or a Simple AD, we recommend that you
configure the VPC with one public subnet and two private subnets. Configure your directory to
launch your WorkSpaces in the private subnets.
For more information on Amazon Workspaces and VPC, please refer to the below URL:

- http://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-
  vpc.html (http://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-
  workspaces-vpc.html)

Ask our Experts

👍 👎

QUESTION 48   UNATTEMPTED

How many network interfaces does an AWS workspace have?

○ **A.** 1

○ **B.** 2 ✔

○ **C.** 3

○ **D.** 4

Explanation :

Answer - B

The AWS documentation mentions the following

· The primary network interface provides connectivity to the resources within your VPC as well as the Internet, and is used to join the WorkSpace to the directory.

· The management network interface is connected to a secure Amazon WorkSpaces management network. It is used for interactive streaming of the WorkSpace desktop to Amazon WorkSpaces clients, and to allow Amazon WorkSpaces to manage the WorkSpace.

For more information on Amazon Workspaces port requirements, please refer to the below URL:

- http://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-port-requirements.html
  (http://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-port-requirements.html)

Ask our Experts

👍 👎

QUESTION 49   UNATTEMPTED

If you wanted to add an expiration date to the URL's which are provided by Cloudfront, how would you go about doing that.

○ **A.** Set an expiration date for the Cloudfront distribution. This would then add the same date to the URL's

○ **B.** Use a signed URL' ✔

○ **C.** Use cookies to embed the expiration date.

○ **D.** This is not possible with Cloudfront

Explanation :

Answer - B

A signed URL includes additional information, for example, an expiration date and time, that gives you more control over access to your content.

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

- http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html
(http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html)

Ask our Experts

👍 👎

QUESTION 50   UNATTEMPTED

Which one of the following settings on the Classic load balancer helps define the amount of time between health checks of an individual backend instance

○   **A.** HealthCheck Interval ✔

○   **B.** Unhealthy Threshold

○   **C.** Response timeout

○   **D.** Healthy Threshold

Explanation :

Answer - A
The HealthCheck Interval is the amount of time between health checks of an individual instance
For more information on health checks, 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

👍 👎

You have 3 EC2 Instances that have public IP's addresses that are mapped to DNS names in Route53. A peer administrator has advised that this may not be the ideal setup and that the DNS names could point to invalid IP addresses in the future. Which of the following can help ensure that this issue does not happen. Choose 2 answers from the options given below. Each option forms part of the solution.

- ☐ **A.** Map the DNS names to the private IP addresses
- ☐ **B.** Create Elastic IP's and assign them to the EC2 Instances. ✔
- ☐ **C.** Map the DNS names to the Elastic IP's ✔
- ☐ **D.** Ensure the Instances receive private IP addresses.

Explanation :

Answer – B and C
When the instance is stopped and started , the public IP assigned to the instance will change and hence this can result in broken DNS links. The ideal scenario is to have Elastic IP addresses and map them to the DNS host names
For more information on Elastic IP, 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

👍 👎

You have created 5 VPC's in the Ireland region and attached an Internet gateway to them. When you try to create another Internet gateway, you are not able to do so. Which of the following could be a reason for this.

○   **A.** You need to create a VPC before you create an Internet gateway

○   **B.** You need to ensure the VPC is public before you can create an Internet gateway

○   **C.** You have crossed the threshold of 4 internet gateways

○   **D.** You have crossed the threshold of 5 internet gateways ✔

Explanation :

Answer - D

The below snapshot from the AWS documentation shows the limitation. Also remember that there is the default gateway already created which is part of the default VPC.

Internet gateways per region	5	This limit is directly correlated with the limit on VPCs per region. You cannot increase this limit individually; the only way to increase this limit is to increase the limit on VPCs per region. Only one internet gateway can be attached to a VPC at a time.

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

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

Ask our Experts

👍   👎

Which of the following techniques can be used to reduce the surface of DDos attacks on your AWS infrastructure. Choose 3 answers from the options given below

- ☐ **A.** Use SQS queues to absorb the requests from the attack
- ☐ **B.** Deploy a load balancer in front of your computational resource ✔
- ☐ **C.** Deploy a cloudfront distribution in front of your computational resource ✔
- ☐ **D.** Use NACL's to control the flow of traffic. ✔

Explanation :

Answer – B,C and D
The AWS documentation mentions the following
One of the first techniques to mitigate DDoS attacks is to minimize the surface area that can be attacked thereby limiting the options for attackers and allowing you to build protections in a single place. We want to ensure that we do not expose our application or resources to ports, protocols or applications from where they do not expect any communication. Thus, minimizing the possible points of attack and letting us concentrate our mitigation efforts. In some cases, you can do this by placing your computation resources behind Content Distribution Networks (CDNs) or Load Balancers and restricting direct Internet traffic to certain parts of your infrastructure like your database servers. In other cases, you can use firewalls or Access Control Lists (ACLs) to control what traffic reaches your applications.
For more information on DDos attack prevention, please refer to the below URL:

- https://aws.amazon.com/shield/ddos-attack-protection/ (https://aws.amazon.com/shield/ddos-attack-protection/)

Ask our Experts

👍 👎

QUESTION 54   UNATTEMPTED

Your company has just set up a new document server on it's 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.
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

👍   👎

You have acquired a new contract from a client to move all of his existing infrastructure onto AWS. You notice that he is running some of his applications using multicast, and he needs to keep it running as such when it is migrated to AWS. You discover that multicast is not available on AWS, as you cannot manage multiple subnets on a single interface on AWS and a subnet can only belong to one availability zone. Which of the following would enable you to deploy legacy applications on AWS that require multicast? Choose the correct answer from the options below

- ○ **A.** Provide Elastic Network Interfaces between the subnets.
- ○ **B.** Create a virtual overlay network that runs on the OS level of the instance. ✔
- ○ **C.** All of the answers listed will help in deploying applications that require multicast on AWS.
- ○ **D.** Create all the subnets on a different VPC and use VPC peering between them.

Explanation :

Answer – B
The recommended solution is to use virtual overlay network. Please find the link to the below articles which has more information on the implementation of this method.

- https://aws.amazon.com/articles/6234671078671125 (https://aws.amazon.com/articles/6234671078671125)

Ask our Experts

👍 👎

Which of the following implementation steps can be used to ensure high availability of a NAT instance in AWS. Choose 2 answers from the options given below. Each answer forms part of the solution.

- [ ] **A.** Deploy 2 NAT instances
- [ ] **B.** Place the NAT instances behind an ELB
- [ ] **C.** Create a script to monitor the primary NAT Instance ✔
- [ ] **D.** Deploy one more NAT instance and ensure that this secondary instance will take over when the Primary NAT instance fails. ✔

Explanation :

Answer – C and D

For an example on high availability for a NAT instance , one can refer to the below URL:

- https://aws.amazon.com/articles/high-availability-for-amazon-vpc-nat-instances-an-example/ (https://aws.amazon.com/articles/high-availability-for-amazon-vpc-nat-instances-an-example/)

Ask our Experts

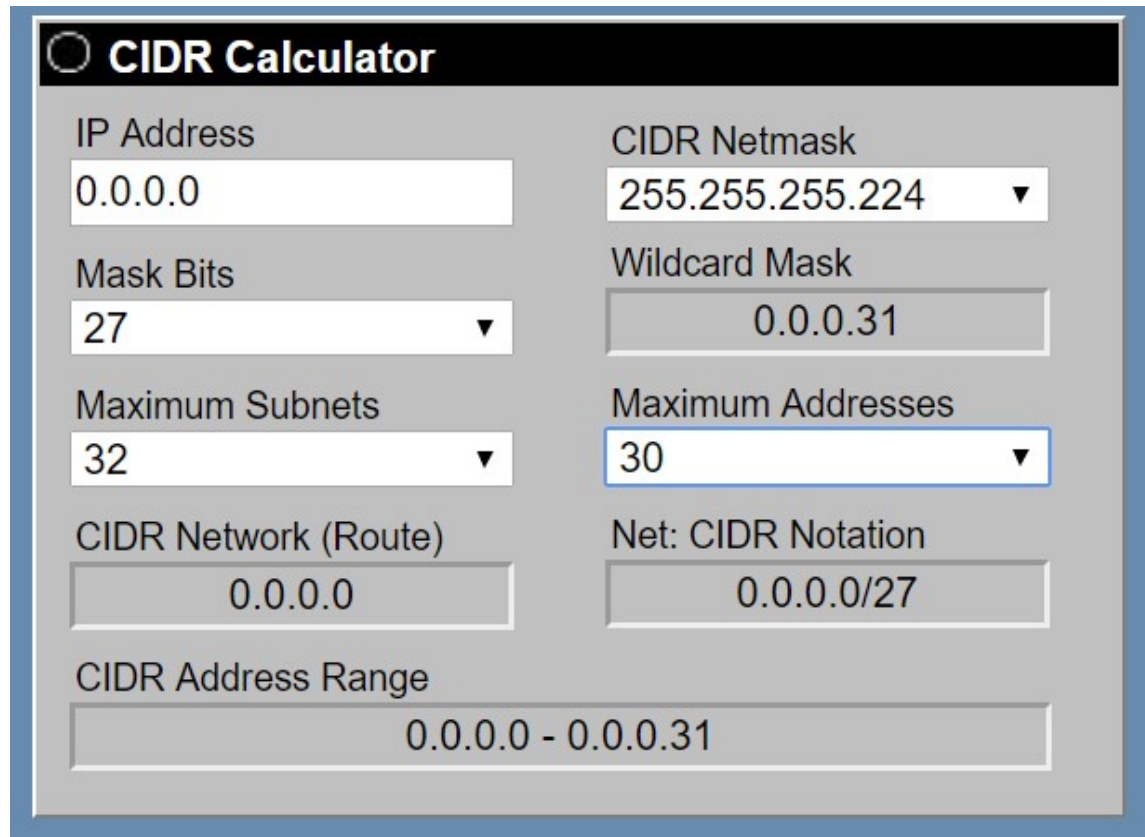👍 👎

QUESTION 57   UNATTEMPTED

You need to create a subnet in a VPC that supports 20 hosts. You need to be as accurate as possible. What CIDR should you use?

- ⭕ **A.** /27 ✔
- ⭕ **B.** /24
- ⭕ **C.** /28
- ⭕ **D.** /25

Explanation :

Answer – A

This can be seen by using an online CIDR calculator

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

Ask our Experts

QUESTION 58   UNATTEMPTED

You have linux EC2 Instances hosted in AWS. You want to create scripts that can use the tracepath command. Which of the following protocols need to be opened up in the Security groups

○ A. TCP

○ B. UDP ✔

○ C. ICMP

○ D. SSL

Explanation :

Answer – B
Tracepath works on the UDP protocol
For more information on the command , please refer to the below URL:

- https://linux.die.net/man/8/tracepath (https://linux.die.net/man/8/tracepath)

Ask our Experts

👍 👎

QUESTION 59   UNATTEMPTED

Which of the following services can be used along with the AWS WAF service.
Choose 2 answers from the options given below

☐ A. AWS SQS

☐ B. AWS ELB ✔

☐ C. AWS Cloudfront ✔

☐ D. AWS Lambda

Explanation :

Answer – B and C
The AWS documentation mentions the following

You use AWS WAF to control how Amazon CloudFront or an Application Load Balancer responds to web requests. You start by creating conditions, rules, and web access control lists (web ACLs). You define your conditions, combine your conditions into rules, and combine the rules into a web ACL.

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

• http://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html (http://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html)

Ask our Experts

👍 👎

QUESTION 60   UNATTEMPTED

If you wanted to ensure that the same set of nameservers are used across multiple domains in Route53 , what would you do?

○ **A.** Create a delegation set via the console

○ **B.** Create a dual hosted zone in Route53

○ **C.** Create a delegation set via the AWS CLI ✔

○ **D.** Create a primary hosted zone in Route53

Explanation :

Answer - C

The AWS documentation mentions the following

By default, each hosted zone that you create gets a different set of four name servers—a different delegation set. If you create a lot of hosted zones, maintaining different delegation sets can be difficult and time consuming. Amazon Route 53 lets you create a delegation set that you can reuse with multiple hosted zones.

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

• http://docs.aws.amazon.com/Route53/latest/APIReference/Welcome.html (http://docs.aws.amazon.com/Route53/latest/APIReference/Welcome.html)

👍 👎

QUESTION 61   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
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)

👍 👎

Which of the following are valid properties of Placement Groups? Choose 3 answers from the list of options given below.

- ☐ **A.** A cluster placement group can span across multiple AZ's.

- ☐ **B.** Placement groups can't be merged ✔

- ☐ **C.** An instance can be launched in one placement group at a time; it cannot span multiple placement groups ✔

- ☐ **D.** You can't move an existing instance into a Placement Group.

- ☐ **E.** If you want to delete a Placement Group you need to terminate or move all instances from it. ✔

Explanation :

Answer - B,C and E
Option A is Incorrect. A cluster placement group is a logical grouping of instances within a single Availability Zone.
Option D is Incorrect. You can move an existing instance into a Placement Group.

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

The limitations on placement groups are
1) A placement group can't span multiple Availability Zones
2) You can't merge placement groups
3) A placement group can span peered VPCs
For more information on placement groups , just browse 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

👍 👎

Which of the following services can be used to do a deep dive into the packets sent across to EC2 Instances.

- ○ **A.** Cloudwatch
- ○ **B.** Cloudtrail
- ○ **C.** FlowLogs
- ○ **D.** None of the above ✔

Explanation :

Answer – D
All of the services such as Flowlogs give you metadata on the traffic. It will not give a deep dive into the actual packets. You need to use a custom software for this.
An example of this is given in the below link:

- http://fmad.io/blog-aws-packet-capture-ec2.html (http://fmad.io/blog-aws-packet-capture-ec2.html)

Ask our Experts

👍 👎

Which of the following factors can determine the EC2 Network performance. Choose 3 answers from the options given below

- ☐ **A.** The EBS volume attached

☐ **B.** EC2 instance size ✔

☐ **C.** Location of the EC2 Instance ✔

☐ **D.** EC2 instance maximum transmission unit ✔

Explanation :

Answer – B,C and D
The following factors can determine the EC2 Network performance
1)   EC2 instance size. Larger instance sizes for an instance type typically provide better
network performance than smaller instance sizes of the same type.
2)   EC2 instance maximum transmission unit (MTU)
3)   Location of the EC2 Instance
For more information on this , please visit the below link:

- https://aws.amazon.com/premiumsupport/knowledge-center/network-throughput-
  benchmark-windows-ec2/ (https://aws.amazon.com/premiumsupport/knowledge-
  center/network-throughput-benchmark-windows-ec2/)

Ask our Experts

👍 👎

QUESTION 65   UNATTEMPTED

You've recently migrated an application from a customer's on-premise data
center to the AWS cloud. Currently, you're using the ELB to serve traffic to the
legacy application. The ELB is also using HTTP port 80 as the health check ping
port. The application is currently responding by returning a text file on port 80
when you test the IP address directly. However, the instance is not registering
as healthy even though the appropriate amount of time has passed for the
health check to register as healthy. How might the issue be resolved? Choose
the correct answer from the options below

○ **A.** Change the ELB listener port from ping port 80 to HTTPS port 80 for the instance to register as healthy

○ **B.** Change the ELB listener port from HTTP port 80 to TCP port 80 for the instance to register as healthy ✔

○ **C.** Change the ELB listener port from HTTP port 80 to HTTPS port 80 for the instance to register as healthy

○ **D.** Change the ELB listener port from HTTP port 80 to TCP port 443 for the instance to register as healthy

Explanation :

Answer – B

Since the application is a custom application and not a standard HTTP application, hence you need to have the TCP ports open.

Before you start using Elastic Load Balancing, you must configure one or more *listeners* for your Classic Load Balancer. A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instance) connections.

Elastic Load Balancing supports the following protocols:

· HTTP
· HTTPS (secure HTTP)
· TCP
· SSL (secure TCP)

For more information on listener configuration for ELB please see the below link:

• http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html)

Ask our Experts

👍 👎

Which of the following services can help you get a history of Classic Load Balancer API calls?

○　A.　Cloudtrail ✔

○　B.　Cloudwatch

○　C.　Cloudwatch logs

○　D.　AWS Config

Explanation :

Answer - A
This is given in the AWS documentation

Q: Can I get a history of Classic Load Balancer API calls made on my account for security analysis and operational troubleshooting purposes?

Yes. To receive a history of Classic Load Balancer API calls made on your account, simply turn on CloudTrail in the AWS Management Console.

For more information on the ELB FAQ's please see the below link:

- https://aws.amazon.com/elasticloadbalancing/faqs/ (https://aws.amazon.com/elasticloadbalancing/faqs/)

Ask our Experts

👍　👎

Which of the following is not part of the charges which can get acquired when using AWS Cloudfront?

○　A.　Data Transfer In ✔

○ **B.** Data Transfer Out

○ **C.** HTTP/HTTPS Requests

○ **D.** Invalidation Requests

Explanation :

Answer - A

This is mentioned in the AWS documentation

Amazon CloudFront charges are based on actual usage of the service in four areas: Data Transfer Out, HTTP/HTTPS Requests, Invalidation Requests, and Dedicated IP Custom SSL certificates associated with a CloudFront distribution.

For more information on Cloufront pricing please see the below link:

- https://aws.amazon.com/cloudfront/details/#faq (https://aws.amazon.com/cloudfront/details/#faq)

Ask our Experts

👍 👎

QUESTION 68   UNATTEMPTED

Which of the following tools can be used to check if the EC2 Linux Instance supports Enhanced Networking

○ **A.** eetworkping

○ **B.** ethtool ✔

○ **C.** awsnetwork

○ **D.** tracert

Explanation :

Answer - B

ethtool is a utility for Linux kernel-based operating system for displaying and modifying some parameters of network interface controllers (NICs) and their device drivers.
For more information on the tool please see the below link:

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

Ask our Experts

👍 👎

QUESTION 69 UNATTEMPTED

You have servers in your private subnet in a VPC which need to access the Internet.

How could you achieve this?

The solution needs to be highly available.

- ○ **A.** Convert the subnet to a public subnet
- ○ **B.** Deploy a NAT instance
- ○ **C.** Deploy a bastion host
- ○ **D.** Use the NAT gateway service ✔

Explanation :

Answer D
Since a highly available solution is required , it is advisable to use the NAT gateway option
For more information on the differences between the NAT instance and the NAT gateway please see the below link:

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

QUESTION 70   UNATTEMPTED

Which of the following statements are true about the default Network ACL assigned to the default VPC.

☐ **A.** The Network ACL Inbound Rules allow all traffic ✔

☐ **B.** The Network ACL Inbound Rules deny all traffic

☐ **C.** The Network ACL Outbound Rules allow all traffic ✔

☐ **D.** The Network ACL Outbound Rules deny all traffic

Explanation :

Answer – A and C

The AWS documentation mentions the following

The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated. Each network ACL also includes a rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule.

For more information on the default NACL please see the below link:

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

👍 👎

You have an EC2 Instance based out of the Amazon Linux AMI. You have created a secondary Network Interface and attached it to the running instance. What needs to be done to ensure that the new network interface is configured automatically?

- ○ **A.** Go ahead and add the interfaces to the network interfaces location on the instance
- ○ **B.** Use the AWS CLI to configure the network interface
- ○ **C.** The Amazon based instances do not accept secondary interfaces
- ○ **D.** This will configured automatically. ✔

Explanation :

Answer - D
The AWS documentation mentions the following
Launching an Amazon Linux or Windows Server instance with multiple network interfaces automatically configures interfaces, private IPv4 addresses, and route tables on the operating system of the instance
For more information on the Elastic Network Interface please see the below link:

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

Ask our Experts

👍 👎

When you launch an instance with the default settings in a default VPC, which of the below automatically get generated for the instance. Choose 3 answers from the options given below

☐ **A.** Private IP address ✔

☐ **B.** Elastic IP address

☐ **C.** Private DNS hostname ✔

☐ **D.** Public DNS hostname ✔

Explanation :

Answer – A,C and D

The AWS documentation mentions the following

When you launch an instance into a default VPC, we provide the instance with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance

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

- 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 73   UNATTEMPTED

Which of the following features of S3 can enable faster transfer of files over long distances.

○ **A.** Requester Pays

○ **B.** Transfer Acceleration ✔

○ **C.** Fast Transfer

○ **D.** Multi-part file upload

Explanation :

Answer - B

The AWS documentation mentions the following

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

For more information on S3 acceleration please see the below link:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html)

Ask our Experts

👍 👎

QUESTION 74   UNATTEMPTED

Which of the following are pre-requisites for enabling cross region replication between S3 buckets. Choose 2 answers from the options given below

☐ **A.** The source and destination buckets must have versioning enabled ✔

☐ **B.** The source and destination buckets must have MFA enabled

☐ **C.** The source and destination buckets must be in different AWS Regions ✔

☐ **D.** The source and destination buckets must be in different AWS AZ's

Explanation :

Answer – A and C

The AWS documentation mentions the following

Requirements for cross-region replication:

1)   The source and destination buckets must have versioning enabled.

2)   The source and destination buckets must be in different AWS Regions.

For more information on cross region replication please see the below link:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html
  (http://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html)

Ask our Experts

👍 👎

QUESTION 75   UNATTEMPTED

A user has configured an ELB to distribute the traffic among multiple instances. The user instances are facing some issues due to the back-end servers. Which of the below mentioned CloudWatch metrics helps the user understand the issue with the instances?

○ **A.** HTTPCode_Backend_3XX

○ **B.** HTTPCode_Backend_4XX

○ **C.** HTTPCode_Backend_2XX

○ **D.** HTTPCode_Backend_5XX ✔

Explanation :

Answer – D
The Either HTTPCode_Backend_5XX for the load balancer is caused by issues in the backend servers. The different sort of errors are given below
·   HTTP 502: Bad Gateway
·   HTTP 503: Service Unavailable
·   HTTP 504: Gateway Timeout
For more information on ELB errors visit the link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ts-elb-http-errors.html
  (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ts-elb-http-errors.html)

Ask our Experts

👍 👎

A user has created a VPC with a public subnet. The user has terminated all the instances which are part of the subnet. Which of the below mentioned statements is true with respect to this scenario?

- ○ **A.** The user cannot delete the VPC since the subnet is not deleted
- ○ **B.** All network interface attached with the instances will be deleted ✔
- ○ **C.** When the user launches a new instance it cannot use the same subnet
- ○ **D.** The subnet to which the instances were launched with will be deleted

Explanation :

Answer – B
When you delete an instance the elastic network interface which in the below example of eth0 will also be deleted.
For information on elastic network interfaces , please visit the 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

👍 👎

A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public

subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required for the NAT security group?

- A. For Inbound allow Source: 20.0.1.0/24 on port 80
- B. For Outbound allow Destination: 0.0.0.0/0 on port 80
- C. For Inbound allow Source: 20.0.0.0/24 on port 80 ✔
- D. For Outbound allow Destination: 0.0.0.0/0 on port 443

Explanation :

Answer – C

As per aws below are the recommended rules for a NAT instance.

NATSG: Recommended Rules

Inbound			
Source	Protocol	Port Range	Comments
10.0.1.0/24	TCP	80	Allow inbound HTTP traffic from servers in the private subnet
10.0.1.0/24	TCP	443	Allow inbound HTTPS traffic from servers in the private subnet
Public IP address range of your home network	TCP	22	Allow inbound SSH access to the NAT instance from your home network (over the Internet gateway)

Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet

For information on NAT security , please visit the link:

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

QUESTION 78   UNATTEMPTED

Your website is hosted on 10 EC2 instances in five regions around the globe, with two instances per region. How could you configure your site to maintain availability with minimum downtime if one of the five regions was to lose network connectivity for an extended period? Choose the correct answer from the options given below.

- ○ **A.** Establish VPN connections between the instances in each region. Rely on BGP to failover in the case of region-wide connectivity failure for an extended period.

- ○ **B.** Create a Route 53 Latency Based Routing Record Set that resolves to an Elastic Load Balancer in each region and has the Evaluate Target Health flag set to true. ✔

- ○ **C.** Create a Route 53 Latency Based Routing Record Set that resolves to an Elastic Load Balancer in each region. Set an appropriate health check on each ELB.

- ○ **D.** Create a Elastic Load Balancer to place in front of the EC2 instances. Set an appropriate health check on each ELB.

Explanation :

Answer – B

If your application is hosted on Amazon EC2 instances in multiple Amazon EC2 regions, you can reduce latency for your users by serving their requests from the Amazon EC2 region for which network latency is lowest. Amazon Route 53 latency-based routing lets you use DNS to route user requests to the Amazon EC2 region that will give your users the fastest response.

The Evaluate Target health check will ensure availability. If any one of the regions fails, since the evaluate target is set to true , the requests will be sent to another region.

For more information on latency based routing, please visit the link:

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency)

Ask our Experts

👍 👎

QUESTION 79   UNATTEMPTED

In order to optimize performance for a compute cluster that requires low inter-node latency, which feature in the following list should you use?

- ○ **A.** AWS Direct Connect
- ○ **B.** Placement Groups ✔
- ○ **C.** VPC private subnets
- ○ **D.** EC2 Dedicated Instances
- ○ **E.** Multiple Availability Zones

Explanation :

Answer – B
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 visit the 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 80   INCORRECT

You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from predefined customer IP addresses. Which two options meet this security requirement? Choose 2 answers

☑ **A.** Configure web server VPC security groups to allow traffic from your customers' IPs ✔

☐ **B.** Configure your web servers to filter traffic based on the ELB's "X-forwarded-for" header ✔

☑ **C.** Configure ELB security groups to allow traffic from your customers' IPs and deny all outbound traffic ✖

☐ **D.** Configure a VPC NACL to allow web traffic from your customers' IPs and deny all outbound traffic

Explanation :

Answer - A and B
The Web servers security group can help ensure that the requests come from the customer's IP via Rules in the security group.
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.
For more information on X-Forwarded-For request , please refer to the link:

• http://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/classic/x-forwarded-headers.html
(http://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/classic/x-forwarded-headers.html)
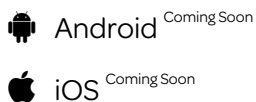
Ask our Experts

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/)

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

f
(https://www.facebook.com/whizlabs.software/)

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

𝕏

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

G+

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