NEW PRACTICE TEST I

Attempt	1	**Completed on**	Sunday , 03 February 2019 , 12:18 AM
Marks Obtained	9 / 65	**Time Taken**	00 H 03 M 09 S
Your score is	13.85%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Design and implement hybrid IT network architectures at scale	11	2	5	4
2	Manage, optimize, and troubleshoot the network	11	0	2	9
3	Design and implement AWS networks	23	4	1	18
4	Configure network integration with application services	9	3	1	5
5	Design and implement for security and compliance	6	0	0	6
6	Automate AWS tasks	5	0	0	5

65	9	9	47
Questions	Correct	Incorrect	Unattempted

Show Answers All ▾

QUESTION 1 INCORRECT DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company is planning on setting up a VPN connection between a VPC hosted in AWS and their on-premise data center. There is a need to ensure the VPN connection is highly available and at the same time to ensure cost is kept to a minimum. What would you do to ensure these requirements are kept?

○ **A.** Create 2 VPN connections for high availability ✓

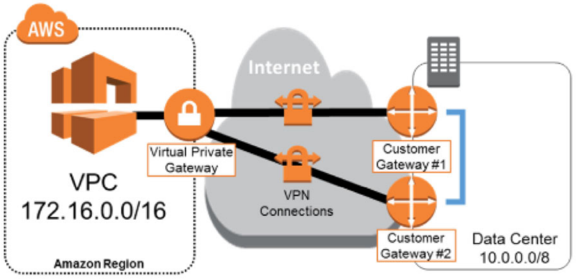
○ **B.** Create an additional Direct connect connection

○ **C.** Create an additional VPC peering connection ✖

○ **D.** VPN connections are already high available

Explanation :

Answer – A
########
As per AWS Docs,
To enable redundancy/high availability, each AWS Virtual Private Gateway (VGW) has two VPN endpoints (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#VPNTunnels) with capabilities for static and dynamic routing. Although statically routed VPN connections from a single customer gateway are sufficient for establishing remote connectivity to a VPC, this is not a highly available configuration. The best practice for making VPN connections highly available is to use redundant customer gateways and dynamic routing for automatic failover between AWS and customer VPN endpoints. For simplicity, the diagram in the next section depicts each VPN connection, consisting of two IPsec tunnels to both VGW endpoints, as a single line.



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

Ask our Experts

QUESTION 2 INCORRECT DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company needs to set up a VPN connection between their AWS VPC and their on-premise data center. There is a need to implement GRE VPN as the standard routing protocol. How would you implement this requirement?

○ **A.** Use AWS Managed VPN connections

○ **B.** Use CloudHub VPN to create a secure VPN connection

○ **C.** Create an EC2 instance and then use a software from the AWS Marketplace ✓

○ **D.** Use AWS Direct Connect ✖

Explanation :

Answer – C

Since there is a requirement to use a custom routing protocol instead of IPSec, the normal AWS VPN managed connections cannot be used. Instead, you have to decide on creating an EC2 instance and using a custom VPN software from the AWS Marketplace. The below diagram from the AWS Documentation shows how this can be set up

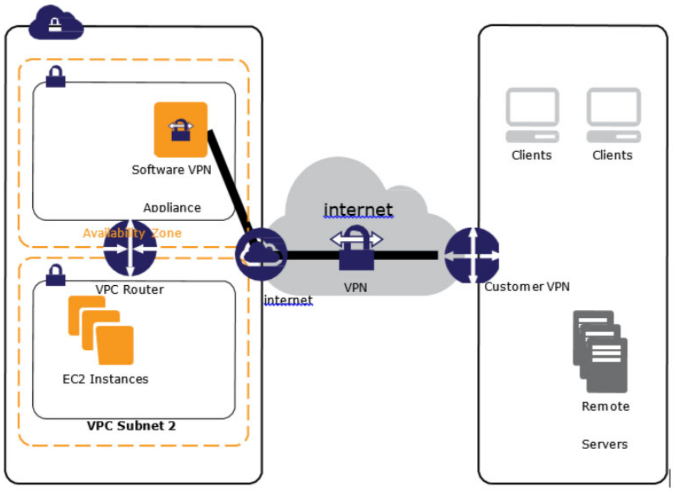


Figure: Software VPN

Options A and B are invalid because these don't support the GRE protocol for encryption

Option D is invalid because this should be used for direct connection between an AWS VPC and an on-premise data center

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

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/software-vpn-network-to-amazon.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/software-vpn-network-to-amazon.html)

Ask our Experts 👍 👎

QUESTION 3 INCORRECT DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company is planning on deploying an EC2 instance which will be used to route VPN traffic to an on-premise data center. In such a scenario what is the responsibility of AWS?

○ **A.** Ensuring high availability of the EC2 Instance ✖

○ **B.** Ensuring high availability of the VPN connection

○ **C.** Ensuring the health of the underlying physical host ✔

○ **D.** Configuration of the IPSec protocol

Explanation :

Answer – C
All other options are invalid because all of the underlying configuration is the responsibility of the customer.
In such a case since the customer is planning on now using an AWS Managed connection but instead planning on adopting a custom VPN solution, AWS is only responsible for Ensuring the health of the underlying physical host of the EC2 Instance
For more information on Custom VPN connections , please refer to the below URL:

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/software-vpn-network-to-amazon.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/software-vpn-network-to-amazon.html)

Ask our Experts 👍 👎

QUESTION 4 INCORRECT MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You are using a Windows Server 2012 in your on-premise location as a customer gateway. You've setup the Virtual Private gateway and the VPN connection. You have also setup the VPN configuration on the Windows Server 2012 machine. But when you check the status of the tunnel in the AWS Console , it still shows as down. What needs to be done to ensure that the tunnel is in the UP state.

○ **A.** Issue a ping command request from the Windows Server 2012 device ✔

○ **B.** From the AWS Console , choose the VPN connection , choose Actions->Bring uptunnel

○ **C.** From the AWS Console , choose the Virtual Private gateway , choose Actions->Bringup tunnel ✖

○ **D.** Ensure BGP routing protocol is setup on the Windows Server 2012 device

Explanation :

Answer – A
This is also given in the AWS Documentation. You have to initiate a request from the Customer gateway device
Step 6: Test the VPN Connection
"To test that the VPN connection is working correctly, launch an instance into your VPC, and ensure that it does not have an Internet connection. After you've launched the instance, ping its private IP address from your Windows server. The VPN tunnel comes up when traffic is generated from the customer gateway, therefore the ping command also initiates the VPN connection".
Option B and C are invalid because no such options are available

Option D is invalid because this is not the right setup
For more information on setting up Windows Server 2012 as the customer gateway , please refer to the below URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/customer-gateway-windows-2012.html (https://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/customer-gateway-windows-2012.html)

Ask our Experts

QUESTION 5 INCORRECT DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has a set of AWS Direct Connect connections. They want to aggregate the bandwidth of these connections to ensure that a large amount of data can be sent through the pipe. So a decision has been made to set up a link aggregation group. What are the factors that need to be considered when setting up the LAG group? Choose 2 answers from the options given below.

□ **A.** You have to ensure that the existing AWS Direct connect connections have the same bandwidth. ✔

☑ **B.** You have to ensure that a VPN connection is also in place to attach to the LAG group ✖

□ **C.** You have to ensure that all AWS Direct connect connections terminate at the same AWS endpoint ✔

☑ **D.** You have to ensure that all AWS Direct connect connections terminate at different AWS endpoint ✖

Explanation :

Answer – A and C

The clear requirements for setting up LAG is given in the AWS Documentation

The following rules apply:

- All connections in the LAG must use the same bandwidth. The following bandwidths are supported: 1 Gbps and 10 Gbps.
- You can have a maximum of 4 connections in a LAG. Each connection in the LAG counts towards your overall connection limit for the region.
- All connections in the LAG must terminate at the same AWS Direct Connect endpoint.

Options B and D are invalid because they break the rules for setting up a LAG group

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

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html)

Ask our Experts

QUESTION 6 INCORRECT MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your company has setup an AWS Direct Connect connection with the help of an AWS Partner. The customer gateway is in an on-premise data center. Your operations department needs to be informed whenever the Direct Connect connection is down. How can you achieve this?

○ **A.** Use the AWS Direct Connect tunnel logging facility to check for any failures ✖

○ **B.** Use Cloudwatch metrics to check for the state of the tunnel ✔

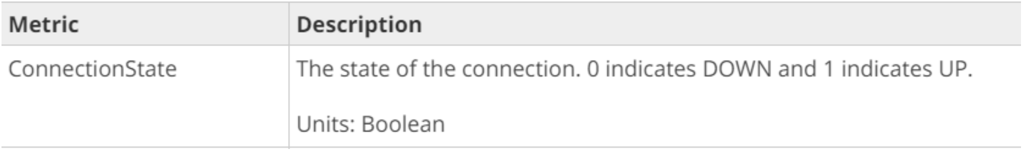
○ **C.** Use Cloudwatch logs to check for the state of the tunnel

○ **D.** You will anyway be notified if the AWS Direct Connect connection is down.

Explanation :

Answer – B

The AWS Direct Connect service now has a metric available in Cloudwatch called Connection State. You can design an alarm whenever the connection state is DOWN.



Metric	Description
ConnectionState	The state of the connection. 0 indicates DOWN and 1 indicates UP. Units: Boolean

Options A and C are invalid because no such entries are available for Direct Connect

Option D , even though a possibility is not the best suited way to check for when the connection is down.
For more information on monitoring for AWS Direct Connect , please refer to the below URL:

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

Ask our Experts 👍 👎

QUESTION 7 CORRECT DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You're in charge for setting up the AWS Direct Connect connection between your on-premise data center and an AWS Partner location. You need to ensure that your network can support the connection. What needs to be in check for this. Choose 3 answers from the options given below

☑ **A.** The network must have support for 802.1Q VLAN ✓

☑ **B.** The network device must support BGP ✓

□ **C.** The network device must support Static Routing

☑ **D.** Auto-negotiation for the port must be disabled for the network device ✓

Explanation :

Answer – A,B and D
Following are the requirements given in the AWS Documentation for AWS Direct Connect

· Your network must use single mode fiber with a 1000BASE-LX (1310nm) transceiver for 1 gigabit Ethernet, or a 10GBASE-LR (1310nm) transceiver for 10 gigabit Ethernet.

· Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be configured manually.

· 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices.

· Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.

· (Optional) You can configure Bidirectional Forwarding Detection (BFD) on your network. Asynchronous BFD is automatically enabled for AWS Direct Connect virtual interfaces, but will not take effect until you configure it on your router.

Option C is invalid because the network device must support BGP routing
For more information on AWS Direct Connect , please refer to the below URL:

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html)

Ask our Experts 👍 👎

QUESTION 8 CORRECT DESIGN AND IMPLEMENT AWS NETWORKS

A company is planning to setup an AWS Direct Connect connection to access resources in AWS via their on-premise data center. They are estimating the costs that would be involved. Which of the following should be taken into account from a costing aspect for AWS Direct Connect? Choose 3 answers from the options given below

☑ **A.** Number of port hours consumed ✓

□ **B.** Data transfer into AWS Direct Connect

☑ **C.** Data transfer from a S3 bucket via a public VIF ✓

☑ **D.** Data transfer from a VPC via a private VIF ✓

Explanation :

Answer – A,C and D
In AWS Direct Connect you pay for the port hours and data transfer out
Option B is incorrect since incoming data transfer is not charged
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

QUESTION 9 CORRECT DESIGN AND IMPLEMENT AWS NETWORKS

A company has a requirement to send large amounts of data that needs to be ingested into S3. This needs to be done on a regular basis. Also the data transfer needs to be encrypted. The data transfer line needs to be low latency and dependable. How could you accomplish this?

○ **A.** Use an AWS VPN Managed connection

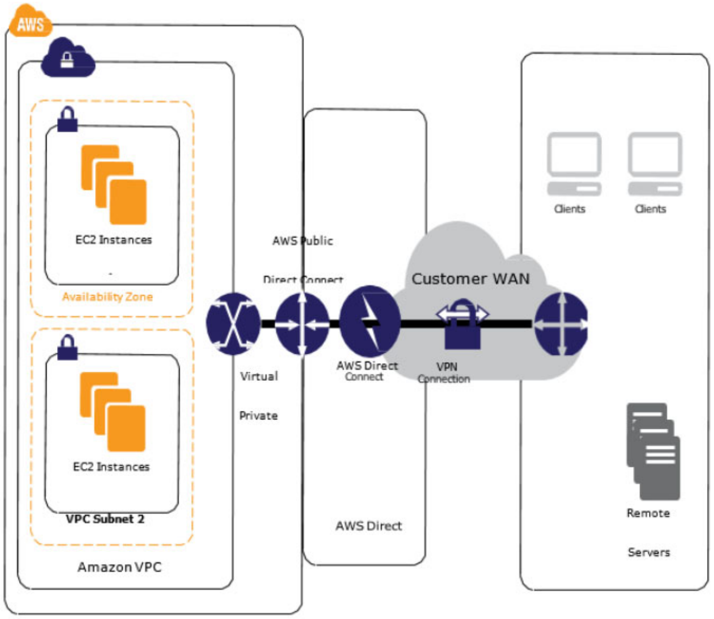
○ **B.** Use an AWS Direct Connect connection

○ **C.** Use an AWS Managed VPN over AWS Direct Connect ✔

○ **D.** Use AWS Direct Connect over an AWS Managed VPN

Explanation :

Answer – C
One can utilize an AWS VPN over AWS Direct connect to get all features of a low latency and encrypted connection. The below diagram from the AWS Documentation shows the architecture of such a setup



Option A is incorrect because this alone with not guarantee a low latency network connection

Option B is incorrect because this alone will not guarantee encryption of the connection
Option D is incorrect because this is an incorrect configuration
For more information on AWS Direct Connect plus VPN , please refer to the below URL:

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html)

Ask our Experts

QUESTION 10 INCORRECT DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on setting up an AWS Direct Connect Connection and a VPN connection as a backup. Incase the AWS Direct Connect connection fails , then the traffic should be routed on the VPN line. What can be done to ensure this failover happens as smoothly as possible.

○ **A.** In AWS Direct Connect , make the VPN as the secondary device. ✖

○ **B.** In AWS VPN , make AWS Direct Connect as the primary device

○ **C.** Enable Bidirectional Forwarding Detection ✓

○ **D.** Enable BGP Routing

Explanation :

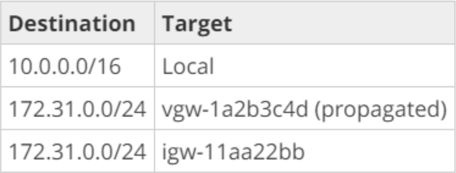
Answer – C
The AWS Documentation mentions the following
Bidirectional Forwarding Detection (BFD) is a network fault detection protocol that provides fast failure detection times, which facilitates faster re-convergence time for dynamic routing protocols. It is independent of media, routing protocol, and data. We recommend enabling BFD when configuring multiple AWS Direct Connect connections or when configuring a single AWS Direct Connect connection and a VPN connection as a back up to ensure fast detection and failover. You can configure BFD to detect link or path failures and update dynamic routing as Direct Connect quickly terminates BGP peering so that backup routes can kick in
Options A and B are incorrect since these are not valid options
Option D is incorrect since BGP routing is a pre-requisite for AWS Direct Connect
For more information on BFD , please refer to the below URL:

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

Ask our Experts

QUESTION 11 INCORRECT DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your trying out a AWS VPN managed connection. You have created the VPN to your on-premise location. You earlier were also using an Internet gateway. You've added the VPN connection to your routing table and enabled propagation. Below is the Route table.



Destination	Target
10.0.0.0/16	Local
172.31.0.0/24	vgw-1a2b3c4d (propagated)
172.31.0.0/24	igw-11aa22bb

Based on the route table , which of the following is TRUE?

○ **A.** Traffic destined for 172.31.0.0/24 will go through the Virtual Private gateway

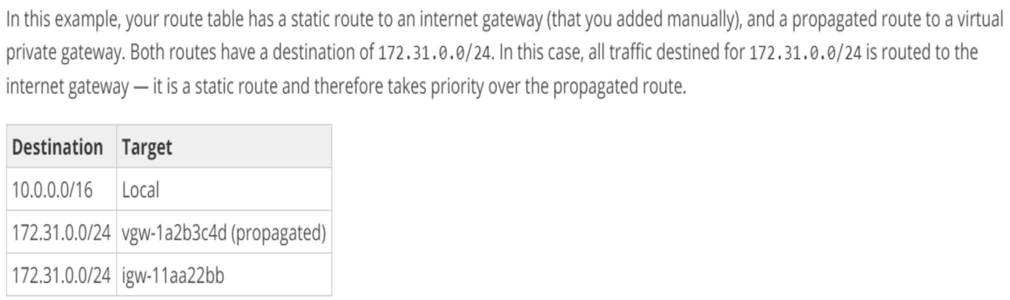
○ **B.** Traffic destined for 172.31.0.0/24 will go through the Internet gateway ✓

○ **C.** Traffic destined for 172.31.0.0/24 will go through the local router

○ **D.** This is not possible , you cannot have 2 routes with the same destination. ✖

Explanation :

Answer – B
Such an example is given in the AWS Documentation



In this example, your route table has a static route to an internet gateway (that you added manually), and a propagated route to a virtual private gateway. Both routes have a destination of `172.31.0.0/24`. In this case, all traffic destined for `172.31.0.0/24` is routed to the internet gateway — it is a static route and therefore takes priority over the propagated route.

Destination	Target
10.0.0.0/16	Local
172.31.0.0/24	vgw-1a2b3c4d (propagated)
172.31.0.0/24	igw-11aa22bb

Option A is incorrect because of the way traffic is routed based on priority.

Option C is incorrect because there is no route defined for such routing
Option D is incorrect because you can have multiple routes with the same destination
For more information on VPN Routing priority , please refer to the below URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-route-priority (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-route-priority)

Ask our Experts

QUESTION 12 INCORRECT CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company is planning on creating a private hosted zone in AWS. They need to ensure that on-premise devices can reach the resources defined in the private hosted zone. How can this be achieved , ensuring least effort is put into setting this up.

○ **A.** Consider using Simple AD for resolving DNS requests. ✓

○ **B.** Convert the private hosted zone to a public one

○ **C.** Create an EC2 instance and install a DNS resolver

○ **D.** Create an EC2 instance and install AD Domain services ✖

Explanation :

Answer – A
This is also mentioned in the AWS Documentation
Simple AD forwards DNS requests to the IP address of the Amazon-provided DNS servers for your VPC. These DNS servers will resolve names configured in your Route 53 private hosted zones. By pointing your on-premises computers to your Simple AD, you can now resolve DNS requests to the private hosted zone.
Option B is incorrect because it is specifically mentioned to use a private hosted zone.
Options C and D are incorrect because this would add a maintenance overhead
For more information on Simple AD and DNS , please refer to the below URL:

- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/simple_ad_dns.html (https://docs.aws.amazon.com/directoryservice/latest/admin-guide/simple_ad_dns.html)

Ask our Experts

QUESTION 13 CORRECT DESIGN AND IMPLEMENT AWS NETWORKS

You are designing an online shopping application for your company. This application will be running in a VPC on EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application tier must read and write data to a customer managed database cluster. There should be no access to the database from the Internet, but the cluster must be able to obtain software patches from the Internet. Which VPC design meets these requirements completely?

○ **A.** Public subnets for both the application tier and the database cluster

○ **B.** Public subnets for the application tier, and private subnets for the database cluster and NAT Instance.

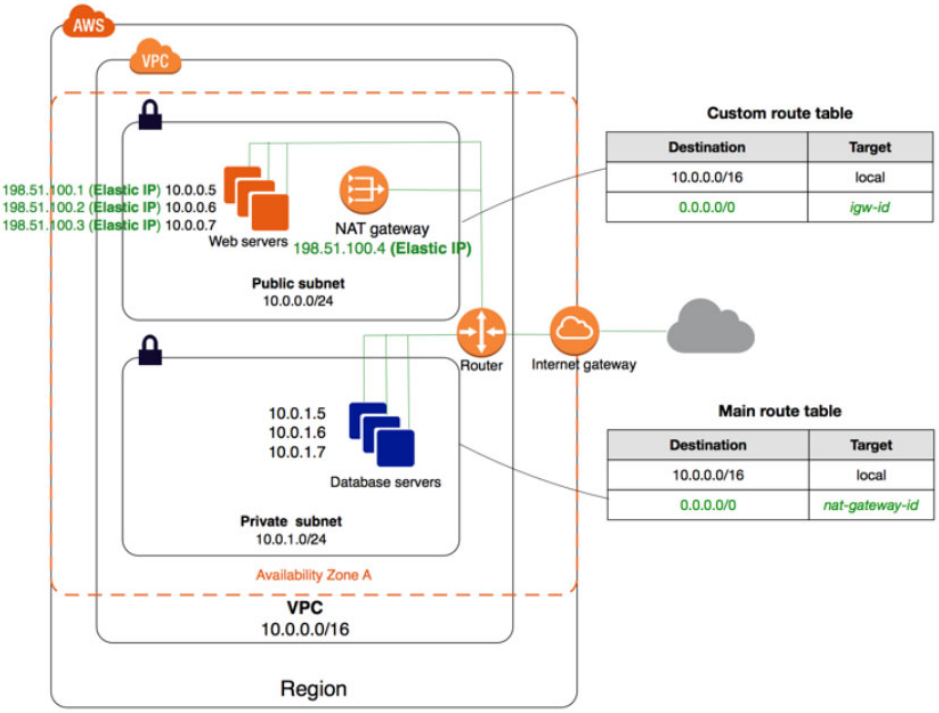
○ **C.** Public subnets for the application tier and NAT Gateway, and private subnets for the database cluster ✔

○ **D.** Public subnets for the application tier, and private subnets for the database cluster and NAT Gateway

Explanation :

Answer – C

The following diagram from the AWS Documentation shows the right setup for this.



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

Option A is incorrect because the database tier should not be in the public subnet.
Options B and D are incorrect because the NAT gateway needs to be in the public subnet
For more information on this setup, please refer to the below URL:

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

Ask our Experts

QUESTION 14 CORRECT DESIGN AND IMPLEMENT AWS NETWORKS

A company has a set of resources hosted in a VPC. They have acquired another company and they have their own set of resources hosted in AWS. The requirement now is to ensure that resources in the VPC of the parent company can access the resources in the VPC of the child company. What is the best way to accomplish this with minimum costing involved.

○ **A.** Usea Direct Connect connection with a private VIF

○ **B.** Establish a NAT gateway to establish communication across VPC's

○ **C.** Use a VPN connection to peer both VPC's

○ **D.** Use VPC Peering to peer both VPC's ✔

Explanation :

Answer – D

VPC Peering allows you to connect VPC's together. The VPC's themselves can be in different regions and different AWS accounts.

Option A is incorrect since this would bear a high cost

Options B and C are incorrect since you should use VPC peering

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

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

Ask our Experts

QUESTION 15 CORRECT CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

An architecture consists of the following

a) A primary and secondary infrastructure hosted in AWS.

b) Both infrastructures consists of ELB, Autoscaling and EC2 resources

How should Route53 be configured to ensure proper failover incase the primary infrastructure goes down.

○ **A.** Configure a primary routing policy

○ **B.** Configure a weighted routing policy

○ **C.** Configure a Multi-Answer routing policy

○ **D.** Configure a failover routing policy ✔

Explanation :

Answer - D

The AWS Documentation mentions the following

You can create an active-passive failover configuration by using failover records. You create a primary and a secondary failover record that have the same name and type, and you associate a health check with each.

For more information on DNS failover using Route53, please visit the following URL:

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring-options.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring-options.html)

Ask our Experts

QUESTION 16 CORRECT CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your management is planning on using AWS Cloudfront to speed up distribution of contents to users from an S3 bucket. They are worried on the aspect on whether users will get the ideal response when they request for objects from Cloudfront. What would you communicate to them as to how users would get content from Cloudfront?

○ **A.** If a user requests an object , only when the entire object is available , it is sent to the user. This is to ensure a correct end user experience

○ **B.** If a user requests an object , the user is directed to the origin location for retrieval of the object.

○ **C.** As soon as the first byte arrives from the origin, CloudFront begins to forward the files to the user ✓

○ **D.** Amazon CloudFront will respond with an HTTP 404 error.

Explanation :

Answer – C
The AWS Documentation mentions the following which is done incase the files are not present in the Edge location
In the edge location, CloudFront checks its cache for the requested files. If the files are in the cache, CloudFront returns them to the user. If the files are *not* in the cache, it does the following:
a. CloudFront compares the request with the specifications in your distribution and forwards the request for the files to the applicable origin server for the corresponding file type—for example, to your Amazon S3 bucket for image files and to your HTTP server for the HTML files.
b. The origin servers send the files back to the CloudFront edge location.
c. As soon as the first byte arrives from the origin, CloudFront begins to forward the files to the user. CloudFront also adds the files to the cache in the edge location for the next time someone requests those files
Options A and D are incorrect since when the first bytes are received by Cloudfront , it is delivered to the user
Option B is incorrect since the content will be delivered by an Edge location
For more information on how Cloudfront works, please visit the following URL:

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html)

Ask our Experts

QUESTION 17 CORRECT CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company has setup a Cloudfront distribution. They are using multiple EC2 Instances as the origin. There is a requirement to ensure that cookies can be monitored in the requests. Based on the cookies , different sites can be relayed back to the users. Which of the following would help fulfil this requirement?

○ **A.** Consider using multiple origins

○ **B.** Consider using Lambda at the edge ✓

○ **C.** Consider using proxy protocol

○ **D.** Consider using RTMP distributions

Explanation :

Answer - B
This is also given in the AWS Documentation
There are many uses for Lambda@Edge processing. For example:

- A Lambda function can inspect cookies and rewrite URLs so that users see different versions of a site for A/B testing.
- CloudFront can return different objects to viewers based on the device they're using by checking the User-Agent header, which includes information about the devices. For example, CloudFront can return different images based on the screen size of their device. Similarly, the function could consider the value of the Referer header and cause CloudFront to return the images to bots that have the lowest available resolution.
- Or you could check cookies for other criteria. For example, on a retail website that sells clothing, if you use cookies to indicate which color a user chose for a jacket, a Lambda function can change the request so that CloudFront returns the image of a jacket in the selected color.
- A Lambda function can generate HTTP responses when CloudFront viewer request or origin request events occur.

- A function can inspect headers or authorization tokens, and insert a header to control access to your content before CloudFront forwards the request to your origin.
- A Lambda function can also make network calls to external resources to confirm user credentials, or fetch additional content to customize a response.

Option A is incorrect since multiple origins will not help in the requirement
Option C is incorrect since proxy protocol is normally used with the Elastic Load Balancer
Option D is incorrect since this is used for media streaming distributions
For more information on using Lambda at the edge, please visit the following URL:

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html)

Ask our Experts 👍 👎

QUESTION 18 UNATTEMPTED CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

A company is planning on using a Cloudfront Distribution. The origin will be an S3 bucket. They want to ensure that users cannot access the objects in the S3 bucket via the public URL of the bucket objects. How can you accomplish this?

○ **A.** Create a Cloudfront Origin Identity which has access via the bucket policy ✔

○ **B.** Place an IAM policy which ensures that users cannot access the objects

○ **C.** Create a Cloudfront Origin Identity which has access via the IAM policy

○ **D.** Create a separate IAM user that has access via the bucket policy

Explanation :

Answer – A
Options B and C is invalid because you need to set a bucket policy and not an IAM policy for this sort of access
Option D is invalid because you need to set a Cloudfront Origin Identity and not a separate IAM user
The AWS Documentation mentions the following
When you create or update a distribution, you can add an origin access identity and automatically update the bucket policy to give the origin access identity permission to access your bucket. Alternatively, you can choose to manually change the bucket policy or change ACLs, which control permissions on individual objects in your bucket.
Whichever method you use, you should still review the bucket policy for your bucket and review the permissions on your objects to ensure that:

· CloudFront can access objects in the bucket on behalf of users who are requesting your objects through CloudFront.
· Users can't use Amazon S3 URL:s to access your objects.

For more information on using Cloudfront Origin Access Indentity, please visit the following URL:

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

Ask our Experts 👍 👎

QUESTION 19 UNATTEMPTED CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company is planning on using Route53 as the DNS provider. They want to ensure that their company domain name points to an existing Cloudfront distribution. How this could be achieved.

○ **A.** Create an Alias record which points to the Cloudfront distribution ✔

○ **B.** Create a host record which points to the Cloudfront distribution

○ **C.** Create a CNAME record which points to the Cloudfront distribution

○ **D.** Create a non-alias record which points to the Cloudfront distribution

Explanation :

Answer - A
The AWS Documentation mentions the following
While ordinary Amazon Route 53 records are standard DNS records, *alias records* provide a Route 53–specific extension to DNS functionality. Instead of an IP address or a domain name, an alias record 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 Route 53 record in the same hosted zone. When Route 53 receives a DNS query that matches the name and type in an alias record, Route 53 follows the pointer and responds with the applicable value
For more information on Route53 Alias records, please visit the following URL:

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

Ask our Experts

QUESTION 20 UNATTEMPTED CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

A company currently hosts their architecture in the US region. They now need to duplicate that architecture to the Europe region and extend the application hosted on this architecture to the new region. In order to ensures that users across the globe get the same seamless experience from either setup, what needs to be done?

○ **A.** Create a classic Elastic Load Balancer is setup to route traffic to both locations

○ **B.** Create a weighted Route53 policy to route the policy based on the weightage for each location

○ **C.** Create an Application Elastic Load Balancer is setup to route traffic to both locations

○ **D.** Create a geolocation Route53 policy to route the policy based on the location. ✓

Explanation :

Answer - D
The AWS Documentation mentions the following to support this requirement
Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from
For more information on AWS Route53 Routing policies, please visit the following URL:

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

Ask our Experts

QUESTION 21 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company has the requirement to host a set of High performance computing nodes. These nodes will be used to process images and videos. Which of the following should be considered during the implementation process? Choose 2 answers from the options given below.

□ **A.** Consider using t2.large instances

□ **B.** Consider using C5 instances ✓

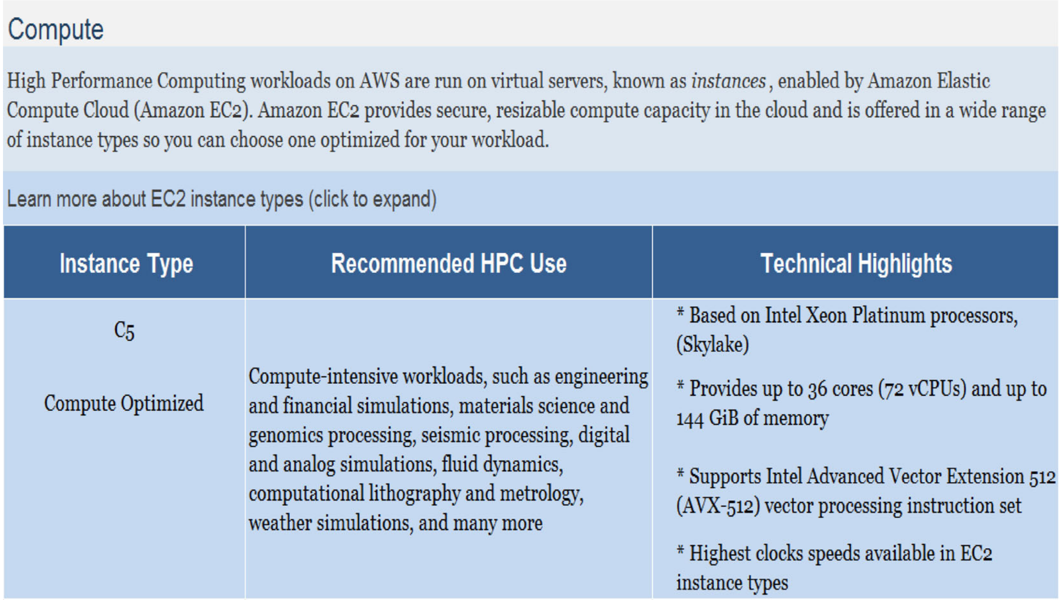
□ **C.** Consider placing the instances in a placement group. ✓

□ **D.** Consider using Linux based AMI's

Explanation :

Answer – B and C

The specifics for high performance computing is given in the AWS Documentation

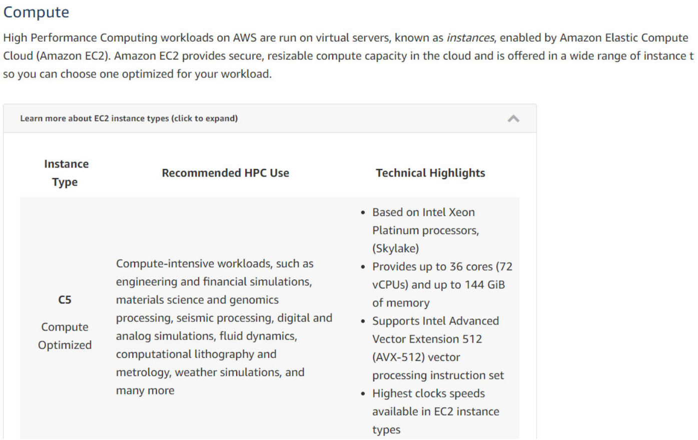


Compute

High Performance Computing workloads on AWS are run on virtual servers, known as *instances*, enabled by Amazon Elastic Compute Cloud (Amazon EC2). Amazon EC2 provides secure, resizable compute capacity in the cloud and is offered in a wide range of instance types so you can choose one optimized for your workload.

Learn more about EC2 instance types (click to expand)

Instance Type	Recommended HPC Use	Technical Highlights
C5 Compute Optimized	Compute-intensive workloads, such as engineering and financial simulations, materials science and genomics processing, seismic processing, digital and analog simulations, fluid dynamics, computational lithography and metrology, weather simulations, and many more	* Based on Intel Xeon Platinum processors, (Skylake) * Provides up to 36 cores (72 vCPUs) and up to 144 GiB of memory * Supports Intel Advanced Vector Extension 512 (AVX-512) vector processing instruction set * Highest clocks speeds available in EC2 instance types



Compute

High Performance Computing workloads on AWS are run on virtual servers, known as *instances*, enabled by Amazon Elastic Compute Cloud (Amazon EC2). Amazon EC2 provides secure, resizable compute capacity in the cloud and is offered in a wide range of instance t so you can choose one optimized for your workload.

Learn more about EC2 instance types (click to expand)

Instance Type	Recommended HPC Use	Technical Highlights
C5 Compute Optimized	Compute-intensive workloads, such as engineering and financial simulations, materials science and genomics processing, seismic processing, digital and analog simulations, fluid dynamics, computational lithography and metrology, weather simulations, and many more	• Based on Intel Xeon Platinum processors, (Skylake) • Provides up to 36 cores (72 vCPUs) and up to 144 GiB of memory • Supports Intel Advanced Vector Extension 512 (AVX-512) vector processing instruction set • Highest clocks speeds available in EC2 instance types

Option A is invalid because this will not give you the desired high performance capabilities

Option D is invalid because this is not a core design requirement.

For more information on high performance computing, please visit the following URL:

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

Ask our Experts

QUESTION 22 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You've setup a set of EC2 Linux based instances in a placement group. You've chosen instances with Enhanced Networking enabled. You want to ensure that the maximum number of packets can be sent across the network interfaces. How could you achieve this.?

○ **A.** Set the Network Access Control List to the maximum network packet size

○ **B.** Set the Placement Group settings to the maximum network packet size

○ **C.** Change the MTU setting on the ethernet interface for each instance ✔

○ **D.** Change the Jumbo frame setting on the ethernet interface for each instance

Explanation :

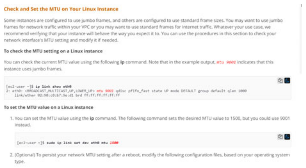
Answer – C
The AWS Documentation mentions on the MTU can be set for Linux based instances

Check and Set the MTU on Your Linux Instance

Some instances are configured to use jumbo frames, and others are configured to use standard frame sizes. You may want to use jumbo frames for network traffic within your VPC or you may want to use standard frames for Internet traffic. Whatever your use case, we recommend verifying that your instance will behave the way you expect it to. You can use the procedures in this section to check your network interface's MTU setting and modify it if needed.

To check the MTU setting on a Linux instance

You can check the current MTU value using the following ip command. Note that in the example output, mtu 9001 indicates that this instance uses jumbo frames.



Check and Set the MTU on Your Linux Instance

Some instances are configured to use jumbo frames, and others are configured to use standard frame sizes. You may want to use jumbo frames for network traffic within your VPC or you may want to use standard frames for Internet traffic. Whatever your use case, we recommend verifying that your instance will behave the way you expect it to. You can use the procedures in this section to check your network interface's MTU setting and modify it if needed.

To check the MTU setting on a Linux instance

You can check the current MTU value using the following **ip** command. Note that in the example output, `mtu 9001` indicates that this instance uses jumbo frames.

```
[ec2-user ~]$ ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

To set the MTU value on a Linux instance

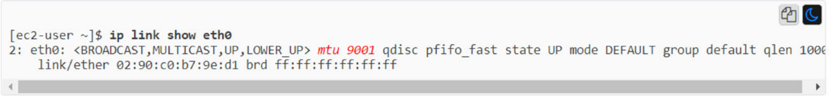
1. You can set the MTU value using the **ip** command. The following command sets the desired MTU value to 1500, but you could use 9001 instead.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

2. (Optional) To persist your network MTU setting after a reboot, modify the following configuration files, based on your operating system type.

To set the MTU value on a Linux instance

1. You can set the MTU value using the ip command. The following command sets the desired MTU value to 1500, but you could use 9001 instead.



```
[ec2-user ~]$ ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode DEFAULT group default qlen 100
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

2. (Optional) To persist your network MTU setting after a reboot, modify the following configuration files, based on your operating system type.

Options A,B and D are all invalid because no such settings exist.
For more information on network MTU, please visit the following URL:

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

Ask our Experts

QUESTION 23 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

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

○ **A.** The Route53 hosted zone needs to be restarted.

○ **B.** The network interfaces need to be initialized again.

○ **C.** The public IP addresses need to be associated to the ENI again.

○ **D.** The public IP addresses have changed after the instance was stopped and started ✓

Explanation :

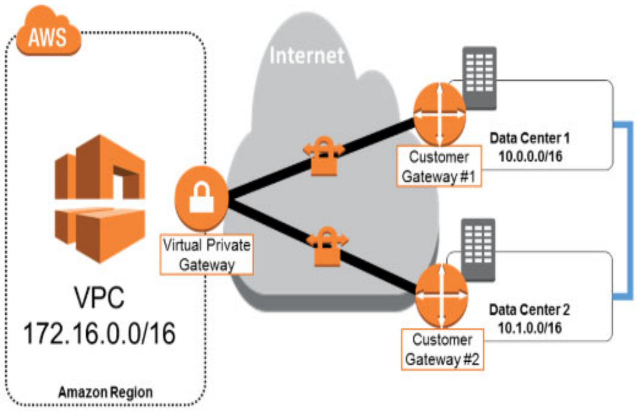
Answer – D
By default the public IP address of an EC2 Instance is released after the instance is stopped and started. Hence the earlier IP address which were mapped to the domain names would have become invalid now.
Options A,B and C are all invalid because these operations are not allowed in AWS
For more information on public IP addressing, please visit the below URL:

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

Ask our Experts

QUESTION 24 UNATTEMPTED DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

A company has setup the following for connecting their on-premise data center to AWS.



They require that in the event the primary connection to DataCenter1 goes down , traffic should be directed to Data Center2. Which of the following should be done in the implementation phase? Select 2 answers.

☐ **A.** Ensure static routes are in place. Ensure the routes are changed incase of a failover

☐ **B.** Ensure DataCenter2 advertises less specific routes. ✔

☐ **C.** Make use of AS-PATH prepending ✔

☐ **D.** Make use of AWS Direct Connect as well

Explanation :

Answer – B and C

The AWS Documentation mentions this use case and how the routes should be configured

· More specific routes: With this approach, both Customer Gateway 1 and Customer Gateway 2 advertise a summary route of 10.0.0.0/15. In addition, Customer Gateway 1 advertises 10.0.0.0/16 and Customer Gateway 2 advertises 10.1.0.0/16. AWS will use the more specific routes to send traffic to the appropriate data center, and will fail back to the other data center following the summarized route if the more specific route becomes temporarily unavailable.

· AS-path prepending: With this approach, both Customer Gateway 1 and Customer Gateway 2 advertise 10.0.0.0/16 and 10.1.0.0/16. However, Customer Gateway 1 uses AS-path prepending when advertising the 10.1.0.0/16 network to make this route less preferred. Likewise, Customer Gateway 2 uses AS-path prepending when advertising the 10.0.0.0/16 network to make this route less preferred. AWS will use the preferred routes to send traffic to the appropriate data center, and will fail back to the other data center following the less preferred routes when necessary.

Option A is incorrect because you should use dynamic routes

Option D is incorrect because we already have 2 VPN connections

For more information on Data center high availability, please visit 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 25 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the application , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.

○ **A.** Use the AWS Trusted Advisor to see what can be done.

○ **B.** Use VPC Flow logs to diagnose the traffic ✓

○ **C.** Use AWS WAF to analyze the traffic

○ **D.** Use AWS Guard Duty to analyze the traffic

Explanation :

Answer – B
The AWS Documentation mentions the following
VPC Flow Logs capture network flow information for a VPC, subnet, or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security tool to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviours
Option A is invalid because this can be used to check for security issues in your account , but not verify as to why you cannot reach the home page for your application
Option C is invalid because this used to protect your app against application layer attacks , but not verify as to why you cannot reach the home page for your application
Option D is invalid because this used to protect your instance against attacks , but not verify as to why you cannot reach the home page for your application
For more information on VPC Security, please visit the following URL:

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

Ask our Experts

QUESTION 26 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on using an EC2 instance for handling voice related traffic. A custom application will be installed on a Linux based instance. Which of the following implementation will help to achieve higher bandwidth for the application?

○ **A.** Enable Enhanced networking on the instance ✓

○ **B.** Use a Network load balancer in front of the EC2 instance

○ **C.** Use a placement group for the EC2 Instance

○ **D.** Use an Application load balancer in front of the EC2 instance

Explanation :

Answer - A
The best choice is to use Enhanced Networking. The AWS Documentation mentions the following on Enhanced Networking
Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. There is no additional charge for using enhanced networking.
Options B,C and D are used for multiple instances ideally
For more information on Enhanced Networking, please visit the following URL:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html)

Ask our Experts 👍 👎

QUESTION 27 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have a database that is running on a large instance type. From a monitoring perspective it seems that the packets are getting lost and the instance is not delivering requests as desired. Initially a test was done to check the capacity of the server. At that time , the database server was able to take on the load. What could be the issue at this point in time.

○ **A.** The right AMI was not chosen for the underlying instance

○ **B.** The instance was using accumulated network credits during the testing phase

○ **C.** There are internal database errors which are causing the timeouts. ✔

○ **D.** The instance is not using a VPN tunnel for communication

Explanation :

Answer – C
The most probable reason in this case is that now the database is not performing under the load and hence is giving TCP errors.
Option A is invalid because the AMI will not be the issue
Option B is invalid because the Instance will still get the network credits during normal operations time
Option D is invalid because the mode of transport is not given in the question
For more information on troubleshooting databases on AWS, please visit the following URL:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html)

Ask our Experts 👍 👎

QUESTION 28 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your team is using applications that are hosted in 2 different regions in AWS. There are EC2 Instances that are performing a replication processes between the applications across regions via their respective Elastic IP's. It is noticed that the current MTU is 1500 and there is a need to increase the throughput for the replication traffic. How can this be achieved?

○ **A.** Create a VPN tunnel between the 2 VPC's and increase the MTU on the instances

○ **B.** Increase the MTU on the Instances

○ **C.** Install the Enhanced Networking modules on the instances

○ **D.** This is not possible ✔

Explanation :

Answer – D
You are already working at the maximum allowable MTU of 1500 that is available for traffic traversing via the Internet. If you are in a VPC , then you can use Jumbo frames. This is also given in the AWS Documentation
Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead. Fewer packets are needed to send the same amount of usable data. However, outside of a given AWS region (EC2-Classic), a single VPC, or a VPC peering connection, you will experience a maximum path of 1500 MTU. VPN connections and traffic sent over an Internet gateway are limited to 1500 MTU
Option A is invalid because still the maximum MTU in a VPN tunnel is 1,500
Options B and C are invalid because still this will not affect the overall MTU
For more information on Network MTU, please visit the following URL:

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

Ask our Experts

QUESTION 29 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your team is planning on hosting an application in AWS. This application will be using a MySQL database hosted on an EC2 Instance. It is anticipated that the disk performance might take a hit due to the high Input/Output activity. How can you ensure baseline performance with low latency for the database tier?

○ **A.** Ensure to use an Instance with Enhanced Networking enabled

○ **B.** Ensure to use EBS IOPS volumes ✓

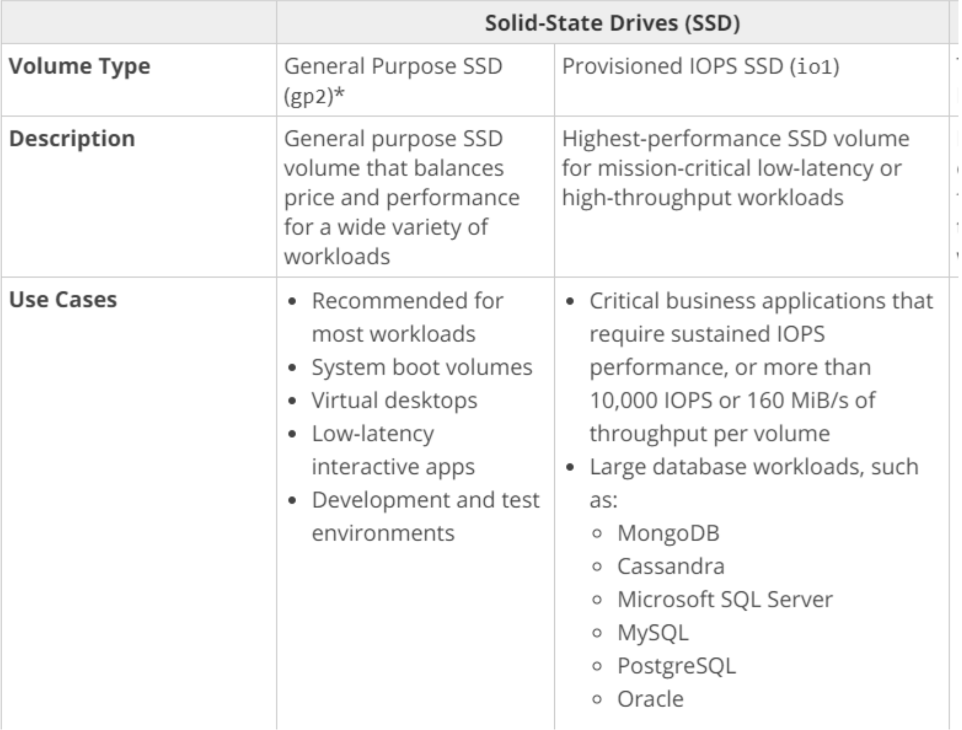
○ **C.** Ensure to use the EFS file system

○ **D.** Ensure to use Amazon S3 for storage

Explanation :

Answer – B

This is also given in the AWS Documentation wherein EBS IOPS volumes should be used for database workloads



	Solid-State Drives (SSD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume • Large database workloads, such as: ○ MongoDB ○ Cassandra ○ Microsoft SQL Server ○ MySQL ○ PostgreSQL ○ Oracle

Option A is invalid because the question is mentioning on disk performance

Options C and D are invalid because these should not be used for storing databases

For more information on EBS volume types, please visit the following URL:

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

Ask our Experts

QUESTION 30 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

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

○ **A.** The VPC's have overlapping CIDR blocks

○ **B.** Security Groups don't work in peered VPC's hence the requests will not work.

○ **C.** NACL's don't work in peered VPC's hence the requests will not work.

○ **D.** The route tables in VPCB have not been configured. ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
To send traffic from your instance to an instance in a peer VPC using private IPv4 addresses, you must add a route to the route table that's associated with the subnet in which the instance resides. The route points to the CIDR block (or portion of the CIDR block) of the other VPC in the VPC peering connection.
The owner of the other VPC in the peering connection must also add a route to their subnet's route table to direct traffic back to your VPC.
Option A is invalid because you would not have been able to create the VPC peering relationship if here were overlapping CIDR blocks
Options B and C are invalid because Security Groups and NACL's are still valid in Peering relationships
For more information on VPC Peering routing, please visit the below URL:

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

Ask our Experts

QUESTION 31 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your production team had earlier created a VPC with the CIDR block of 192.168.0.0./16. Instances were launched in the VPC. Now there is a decision to ensure the instances have an address space for 10.0.0.0/16. How can this be achieved?

○ **A.** Add a new address space to the VPC. Then ensure that the instances use the new address space

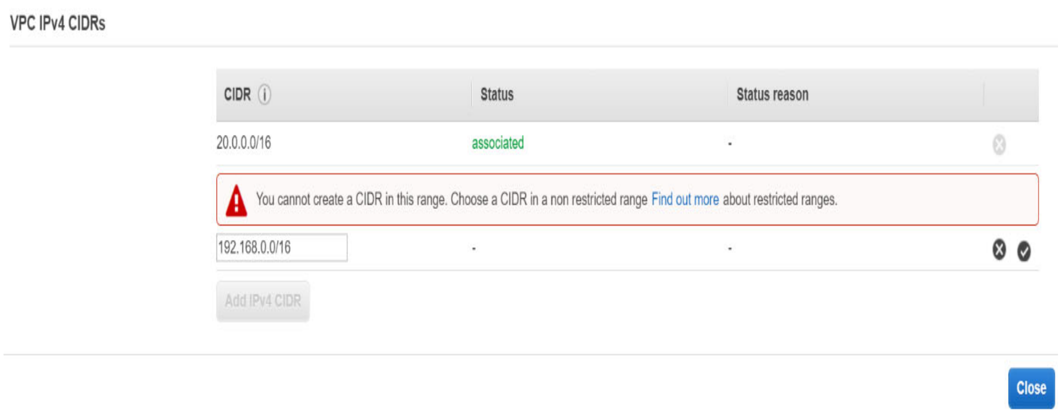
○ **B.** Create a new VPC with the address block of 10.0.0.0/16. Migrate all of the instances to the new VPC. ✔

○ **C.** Change the address block of the VPC from 192.168.0.0./16 to 10.0.0.0/16. All of the instances will now use the new address space.

○ **D.** Launch a NAT Instance. Ensure that the instance performs Network address translation onto the CIDR range of 10.0.0.0/16

Explanation :

Answer – B
Since the initial CIDR block is 192.168.0.0./16 , the additional CIDR blocks should correspond to the similar ranges. The below snapshot shows when you try to add a different CIDR block to an existing VPC which is different from the main CIDR block. You will get an error.



VPC IPv4 CIDRs

CIDR	Status	Status reason
20.0.0.0/16	associated	-
192.168.0.0/16	-	-

You cannot create a CIDR in this range. Choose a CIDR in a non restricted range Find out more about restricted ranges.

Option A is invalid because of the above mentioned error

Option C is invalid because you can't change the existing CIDR block
Option D is invalid because using a NAT instance is not the right approach
For more information on VPC and Subnet sizing , please visit the below URL:

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

Ask our Experts

QUESTION 32 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your architecture team has recommended the following for the VPC's in your AWS Account

- A shared services VPC which would provide services to other VPC's
- A hosted VPC that will be accessible to the customer
- The hosted VPC will also interact with the shared services VPC.

Which of the following should also be considered as part of the design. Choose 2 answers from the options given below. Each answer is an independent design solution

☐ **A. Ensurea virtual private link is available for accessing the Shared services VPC.** ✔

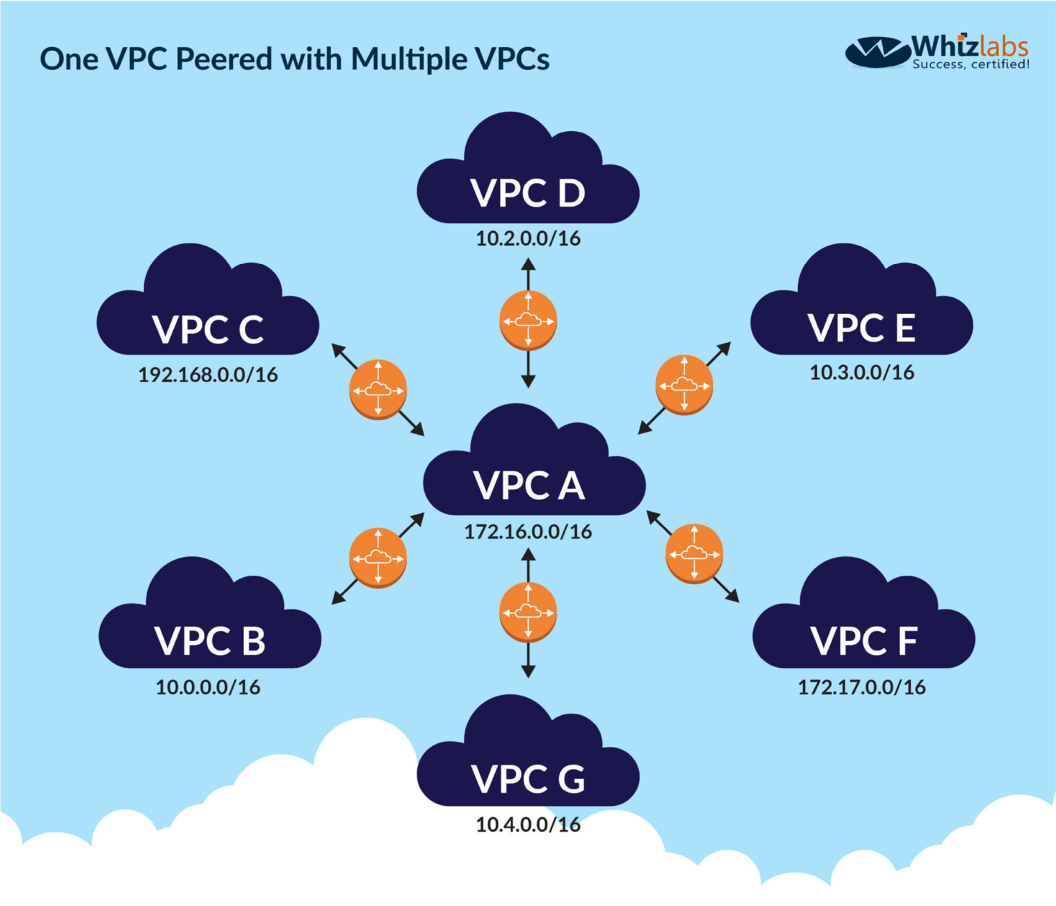
☐ **B. UseVPC peering between the shared services VPC and other VPC's**

☐ **C. Putthe shared services VPC as public. Ensure the right security measures are inplace for accessing the shared services.** ✔

☐ **D. Createa VPN between each VPC. Ensure the Virtual private gateway is in place for theother VPC's**

Explanation :

Answer - A and C
One option is to create a VPC privatelink which can be used to access the services in the AWS shared VPC. The below is also mentioned from the AWS Documentation to support this
You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an *endpoint service*). Other AWS principals can create a connection from their VPC to your endpoint service using an interface VPC endpoint. You are the *service provider*, and the AWS principals that create connections to your service are *service consumers*.
And the other option is to make the VPC as public. But the right security measures need to be put in place.
Option B is invalid because in VPC peering it states that,You may want to use this spoke configuration when you have resources on a central VPC, such as a repository of services, that other VPCs need to access. The other VPCs do not need access to each others' resources; they only need access to resources on the central VPC.



Option D is invalid because this option should only be used for a transit VPC
For more information on VPC and Subnet sizing , please visit the below URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/endpoint-service.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/endpoint-service.html)

Ask our Experts

QUESTION 33 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have created 3 VPC's , VPC A , VPC B and VPC C. There is a VPC peering connection between VPC A and VPC B and a separate peering connection between VPC B and VPC C. Which of the following is true with regards to this VPC peering arrangement?

○ **A.** Instances launched in VPC A can reach instances in VPC C

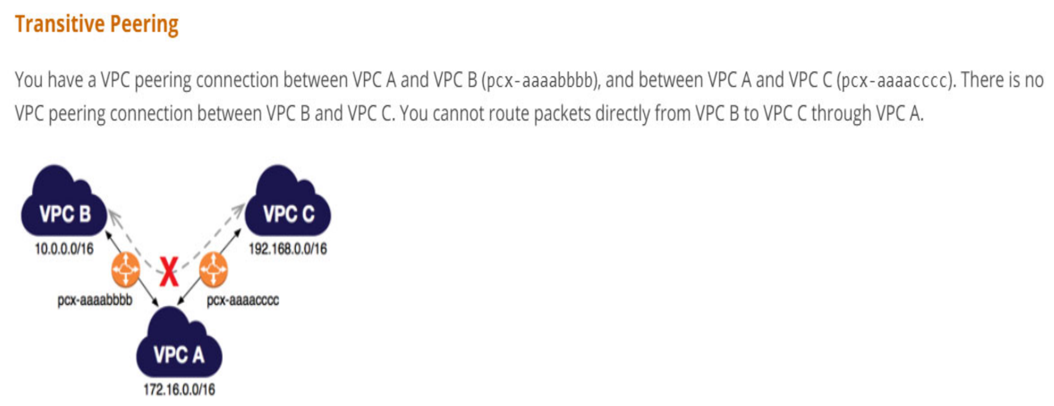
○ **B.** Instances launched in VPC A can reach instances in VPC C if the right routing entries are present.

○ **C.** Instances launched in VPC A can reach instances in VPC C if the right Security Groups rules are present for the instances

○ **D.** Instances launched in VPC A can reach instances in VPC C via a proxy instance in VPC B ✔

Explanation :

Answer – D
Since transitive peering is not allowed, you can use a proxy instance to forward the requests.
Options A,B and C are all invalid , because as per the AWS Documentation, this is the rule of transitive peering



Transitive Peering

You have a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb), and between VPC A and VPC C (pcx-aaaacccc). There is no VPC peering connection between VPC B and VPC C. You cannot route packets directly from VPC B to VPC C through VPC A.

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

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

Ask our Experts

QUESTION 34 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your VPC consists of public and private subnets. The private subnets make use of a NAT instance to download updates from the internet. The Instances are trying to download updates from a server which listens on port 8090. But the instances are not able to reach the external server for updates. Which of the following could be relevant issues with this. Choose 2 answers from the options given below

□ **A.** The NAT instance is blocking traffic on port 8090 ✓

□ **B.** The Inbound NACL is blocking traffic on port 8090

□ **C.** The Inbound Security Groups are blocking traffic on port 8090

□ **D.** There mote server firewall is blocking traffic ✓

Explanation :

Answer - A and D
The NAT instance could be blocking Outbound Traffic on port 8090 which is not allowing traffic to flow outwards.
The remote server could also be blocking traffic from the instances.
Options B and C are invalid because the traffic is Outbound on port 8090 and not Inbound on port 8090.
For more information on NAT Instances , please visit the below URL:

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

Ask our Experts

QUESTION 35 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your company has a set of instances hosted in a private subnet. These instances need to make calls to the Simple Storage Service. You have setup the Endpoint but are still not able to access the S3 buckets from the instances in the private subnet. Which of the following could be issues for the access? Choose 2 answers from the options given below

□ **A.** You should be using an interface instead of a gateway for accessing the S3 service.

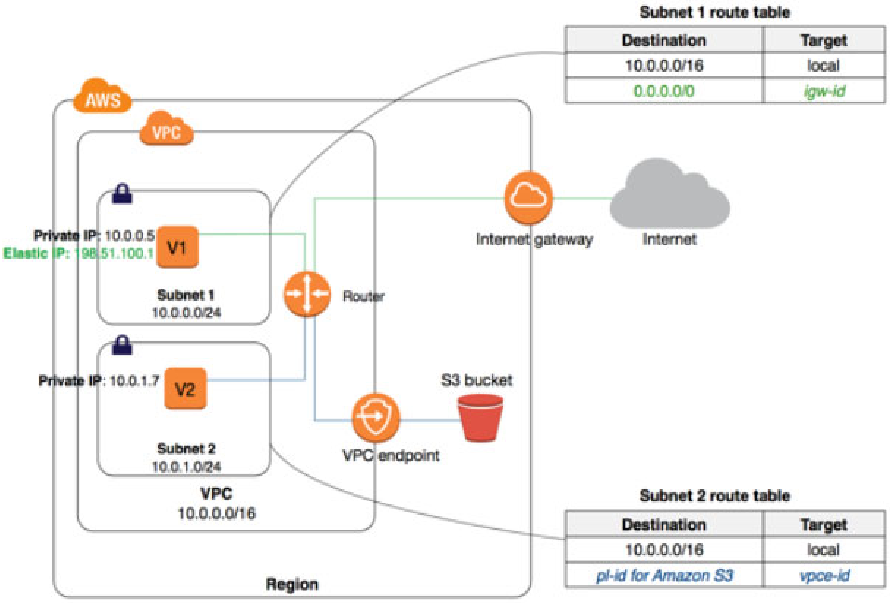
□ **B.** The prefix for the endpoint is not attached to the Route table ✓

□ **C.** The prefix for the endpoint is not attached to the Security Group

□ **D.** The endpoint is attached to the wrong VPC ✓

Explanation :

Answer - B and D
The prefix for the gateway endpoint needs to be added to the Route table
The below diagram from the AWS Documentation shows the design of an endpoint



Subnet 1 route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Subnet 2 route table

Destination	Target
10.0.0.0/16	local
pl-id for Amazon S3	*vpce-id*

Option A is incorrect because you should use a gateway for S3

Option C is incorrect because the prefix should be attached to the Route table and not the Security Group.
For more information on VPC gateway endpoints , please visit the below URL:

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

Ask our Experts

QUESTION 36 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on hosting their own VPN server in AWS. This will be hosted on an EC2 instance and using a software from the AWS Marketplace. You are tasked with ensuring optimal performance of the underlying VPN server. Which of the following aspects would you consider? Choose 2 answers from the options given below

□ **A.** Ensure that the instance is using EBS optimized Volumes

□ **B.** Ensure that the instance is using Enhanced Networking ✓

□ **C.** Under standthe packet limitations in the infrastructure ✓

□ **D.** Use a Network load balancer for scaling

Explanation :

Answer – B and C
Ensure that the Instance is using Enhanced Networking for better network throughput
Also conduct the necessary initial tests on the system to understand the overall performance of the system and see if there are any limitations.
Option A is incorrect since this has to do with storage and not network performance
Option D is incorrect since this has to do more with scalability.
For more information on tests that can be done on an underlying instance for network performance, please visit the below URL:

- https://aws.amazon.com/premiumsupport/knowledge-center/low-bandwidth-vpn/ (https://aws.amazon.com/premiumsupport/knowledge-center/low-bandwidth-vpn/)

Ask our Experts

QUESTION 37 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on deploying an application to AWS. There is a requirement for high availability and low latency between the underlying instances that support the application. Which of the following would you not consider in your design?

○ **A.** Deploy instances across multiple availability zones

○ **B.** Enable Enhanced Networking on the instances

○ **C.** Use a Network load balancer in front of the instances

○ **D.** Place the instances in a cluster placement group ✓

Explanation :

Answer – D
If you place the instances in a placement group , then they need to be placed in a single availability zone. This would not meet the requirement of high availability.
As per AWS docs:
"Launching instances in a spread placement group reduces the risk of simultaneous failures that might occur when instances share the same underlying hardware. Spread placement groups provide access to distinct hardware, and are therefore suitable for mixing instance types or launching instances over time. A spread placement group can span multiple Availability Zones, and you can have a maximum of seven running instances per Availability Zone per group."
Options A and C are incorrect because this would provide high availability as required
Options B is incorrect because this would help in better network performance
For more information on Placement groups, please visit the below URL:

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

Ask our Experts

QUESTION 38 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You're planning on hosting an application on an Amazon Linux EC2 Instance. You have a requirement to reduce the amount of time it takes to process packets on the EC2 instance. Which of the following can be used for this requirement?

○ **A.** Use an Instance which supports the Windows AMI

○ **B.** Consider using the Data Plane Development Kit ✓

○ **C.** Consider using Jumbo frames for packet transmission

○ **D.** Consider using an MTU of 12,000

Explanation :

Answer - B
DPDK is the Data Plane Development Kit that consists of libraries to accelerate packet processing workloads running on a wide variety of CPU architectures.
For more information on the Data Plane Development Kit, please visit the below URL:

- https://www.dpdk.org/ (https://www.dpdk.org/)

Ask our Experts

QUESTION 39 UNATTEMPTED DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your IT Security department has deployed a firewall on an AWS EC2 Instance. They have mandated at all traffic from certain applications needs to move through the firewall. In such a case, what considerations should be made for the EC2 instance for maximum performance? Choose 2 answers.

□ **A.** Consider using an Amazon Linux AMI only

□ **B.** The underlying Instance type ✔

□ **C.** Driver support for the Intel Virtual Function and Elastic Network Adapter (ENA) ✔

□ **D.** Consider using NACL's

Explanation :

Answer - B and C
Yes , if you choose a higher instance type , you will get better performance , so consider using a higher instance type
Also use Enhanced Networking for better networking support
Option A is invalid because it is not necessary to only use an Amazon Linux AMI only
Option D is invalid because this is good from a security aspect but not a performance aspect
For more information on Enhanced Networking, please visit the below URL:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html)

Ask our Experts

QUESTION 40 UNATTEMPTED DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

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

○ **A.** Removethe prepended AS_PATH.

○ **B.** Reconfigurethe VPN as a static VPN instead of dynamic.

○ **C.** Increasethe MED property on the VPN connection.

○ **D.** Advertisea less specific prefix on the VPN connection ✔

Explanation :

Answer – D
It could be that the route being specified for the routing table is more specific for the VPN connection , hence this is being preferred.
The AWS Documentation clearly states that the most specific route in your route table that matches the traffic to determine how to route the traffic is used.

Hence it is better to ensure the VPN connection has a less specific route to ensure that it is not the preferred route which is taken.
Option A is invalid because this would not an affect
Options B and C are invalid because this would make the VPN more preferable
For more information on Routing using Route tables, please refer to below URL:

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

Ask our Experts

QUESTION 41 UNATTEMPTED DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company is planning on hosting an application on a set of EC2 Instances. There is a requirement for complete end to end encryption for the data to ensure that the application is (HIPAA) compliant. How can you achieve this?

○ **A.** Ensure that the traffic is encrypted using KMS

○ **B.** Setup a VPN connection between the EC2 Instance and the Internet

○ **C.** Setup a Direct Connect connection between the EC2 Instance and the Internet

○ **D.** Use SSL to encrypt all the data at the application layer ✓

Explanation :

Answer – D
Since the data needs to be encrypted end to end, use an SSL certificate which can be mapped to the application.
Option A is incorrect because this can be used to encrypt data at rest
Option B is incorrect because this will not encrypt traffic end to end
Option C is incorrect because this is not a feasible option for this scenario
Below is an example on how to use SSL with an Apache Instance on EC2

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/SSL-on-an-instance.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/SSL-on-an-instance.html)

Ask our Experts

QUESTION 42 UNATTEMPTED AUTOMATE AWS TASKS

Your company is currently planning on using Route53 for managing Blue Green deployments. They have already setup an 80%-20% for a new deployment. How can you ensure to stop sending traffic to the older setup once all testing is complete?

○ **A.** Delete the weighted resource record

○ **B.** Change the resource record to a simple routing policy

○ **C.** Change the resource record weight to 100

○ **D.** Change the resource record weight to 0 ✓

Explanation :

Answer – D
The AWS Documentation mentions the following to support this answer
Enter an integer between 0 and 255. To disable routing to a resource, set Weight to 0. If you set Weight to 0 for all of the records in the group, traffic is routed to all resources with equal probability. This ensures that you don't accidentally disable routing for a group of weighted records.
Options A and B are incorrect since you need to first mark the resource record as 0
Option C is incorrect because this will cause the reverse and all traffic will flow to the application

For more information on setting values for the weighted resource records , please refer to the below URL:

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-values-weighted.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-values-weighted.html)

Ask our Experts 👍 👎

QUESTION 43 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have a set of instances setup in an AWS VPC. You need to ensure that instances in the VPC receive host names from the AWS DNS. You have set the enableDnsHostname attribute set to true for your VPC. But the instances are still not receiving the host names when they are being launched. What could be the underlying issue.

○ **A.** The Auto-Assign Public IP is not set for the Subnet in which the Instance is launched

○ **B.** The enable DnsSupport is not set to true for the VPC ✔

○ **C.** You need to configure a Route 53 private hosted zone first

○ **D.** You need to configure a Route 53 public hosted zone first

Explanation :

Answer – B
You need to set both values for instances to receive DNS hostnames. This is also given in the AWS Documentation
If both attributes are set to true, the following occurs:

- Your instance receives a public DNS hostname.
- The Amazon-provided DNS server can resolve Amazon-provided private DNS hostnames.

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

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

Ask our Experts 👍 👎

QUESTION 44 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have setup a Cloudfront distribution in AWS. You want to use the AWS Certification Manager along with Cloudfront. You are setting up Cloudfront, but you cannot see the ACM certificate that you created at an earlier stage to associate with the distribution. What could be the underlying issue?

○ **A.** You have not uploaded or created the certificate in the right region ✔

○ **B.** You need to upload the certificate directly to Cloudfront after the distribution is created

○ **C.** You need to ensure that a CNAME record is created in Route 53 first

○ **D.** You need to ensure that an alias record is created in Route 53 first

Explanation :

Answer – A
The certificate needs to be configured in the North Virginia region. This is also given in the AWS Documentation
Supported Regions
Visit AWS Regions and Endpoints in the AWS General Reference or the AWS Region Table to see the regional availability for ACM.

Like most AWS resources, certificates in ACM are regional resources. To use a certificate with Elastic Load Balancing for the same fully qualified domain name (FQDN) or set of FQDNs in more than one AWS region, you must request or import a certificate for each region. For certificates provided by ACM, this means you must revalidate each domain name in the certificate for each region. You cannot copy a certificate between regions.
To use an ACM Certificate with Amazon CloudFront, you must request or import the certificate in the US East (N. Virginia) region. ACM Certificates in this region that are associated with a CloudFront distribution are distributed to all the geographic locations configured for that distribution.
For more information on regions for ACM , please refer to the below URL:

- https://docs.aws.amazon.com/acm/latest/userguide/acm-regions.html (https://docs.aws.amazon.com/acm/latest/userguide/acm-regions.html)

Ask our Experts 👍 👎

QUESTION 45 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have launched a couple of EC2 Instances in separate subnets. You are transferring data via the Public IP's of the EC2 Instances. Both Instances are located in the same AZ. Instances are located in the us-east-1 region. What would the data transfer charges?

○ **A.** There are no data transfer charges for instances in the same region

○ **B.** The reare no data transfer charges for instances in the same AZ

○ **C.** There will be a data transfer charge of $0.01/GB ✔

○ **D.** There is no data transfer charge for the internet

Explanation :

Answer – C
The below information is given in the AWS Documentation for data transfer for EC2 Instances
· Data transferred "in" to and "out" of Amazon EC2, Amazon RDS, Amazon Redshift , Amazon DynamoDB Accelerator (DAX), and Amazon ElastiCache instances or Elastic Network Interfaces across VPC peering connections in the same AWS region is charged at $0.01/GB.
· Data transferred "in" to and "out" of Amazon Elastic Load Balancing is priced equivalent to Amazon EC2. Data processed by Amazon Elastic Load Balancing will incur charges in addition to Amazon EC2 data transfer charges.
· Using a public or Elastic IPv4 address is charged at $0.01/GB.
· Using an IPv6 address from a different VPC is charged at $0.01/GB.
· Amazon EC2, Amazon RDS, Amazon Redshift and Amazon ElastiCache instances or Elastic Network Interfaces in the same Availability Zone is $0.00/GB.

Options A,B and D are incorrect since there are charges which will be incurred
For more information on demand pricing , please refer to the below URL:

- https://aws.amazon.com/ec2/pricing/on-demand/ (https://aws.amazon.com/ec2/pricing/on-demand/)

Ask our Experts 👍 👎

QUESTION 46 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have been put in charge for setting up a network architecture for a company. The architecture consists of an application that will exchange a lot of information and hence will need a high bandwidth consideration. There will be other B2B customers that will access this application as separate tenants. What consideration will you provide in the design.

○ **A.** Consider using a Virtual private gateway for each customer as this will provide the least latency

○ **B.** Consider using AWS Direct Connect for each customer. But this will also depend on the availability of an AWS partner in that location of the customer. ✓

○ **C.** Consider using AWS VPN for each customer. But this will also depend on the availability of an AWS partner in that location of the customer.

○ **D.** Allow each customer to connect via the Internet. Setup the right security groups and NACL's for the application.

Explanation :

Answer - B
AWS Direct connect will offer a dedicated and high bandwidth connection for each customer.
But then there has to be an AWS Partner also available to ensure connection from the customer location
Options A and C are invalid since this will not ensure high bandwidth
Option D is invalid because separate tenancy would be an issue
For more information on AWS Direct Connect, please refer to below URL:

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html)

Ask our Experts 👍 👎

QUESTION 47 UNATTEMPTED AUTOMATE AWS TASKS

Your team has created a cloudformation template. It creates a VPC and a subnet with a CIDR block of 10.0.0.0/16 and you have created another subnet with in the VPC with a CIDR block of 10.0.1.0/24. What will happen when you try to deploy the template?

○ **A.** The template will give an error during the design stage

○ **B.** The template will give a deployment error when creating the subnet and leave the VPC as created

○ **C.** The template will give a deployment error and all resources will be rolled back ✓

○ **D.** The template will deploy successfully

Explanation :

Answer - C
Here since there are overlapping CIDR blocks , the template deployment will fail and all resources will be rolled back
Option A is invalid because if the JSON template is valid in syntax it will proceed ahead
Option B is invalid because when an error occurs all resources will be rolled back by default
Option D is invalid because it will give an error because of overlapping CIDR blocks
For more information on Cloudformation key concepts, please refer to below URL:

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis-concepts.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis-concepts.html)

Ask our Experts 👍 👎

QUESTION 48 UNATTEMPTED AUTOMATE AWS TASKS

Your team has created a clouformation template. The template consists of a creation of a Virtual private gateway , Customer gateway and a VPN connection based on the created artefacts. The templates sometimes gives errors because the routes are not being added because of the missing Virtual private gateway resource. How can you resolve this?

○ **A.** Change the order of the creation of the resources in the template

○ **B.** Add a Depends On attribute to the VPGW on the Route table

○ **C.** Add a Depends On attribute to the Route Table entry on the VPGW ✓

○ **D.** Add a custom resource to the template for the Route Table entry

Explanation :

Answer - C
The AWS Documentation mentions the following
With the DependsOn attribute you can specify that the creation of a specific resource follows another. When you add a DependsOn attribute to a resource, that resource is created only after the creation of the resource specified in the DependsOn attribute.
Option A is invalid because the order will not resolve the problem
Option B is invalid because it should be the other way around , there should be a DependsOn attribute to the RouteTable entry on the VPGW
Option D is invalid because a custom resource will not resolve the problem
For more information on Cloudformation DependsOn attribute, please refer to below URL:

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-dependson.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-dependson.html)

Ask our Experts 👍 👎

QUESTION 49 UNATTEMPTED AUTOMATE AWS TASKS

Your team has setup a testing environment using a VPC and EC2 Instances. An application is being hosted on these instances. Some housekeeping scripts are being developed using AWS Lambda that would need to delete files created by these Ec2 Instances on their respective EBS volumes. What is the initial configuration that needs to be put in place?

○ **A.** Ensure to use the --vpc-config when creating the AWS Lambda function ✓

○ **B.** Ensure to use the --vpc-config when creating the Ec2 instance

○ **C.** Ensure the VPC has a route entry to the Lambda function

○ **D.** Ensure an Internet gateway is attached to the VPC

Explanation :

Answer – A
The AWS Documentation mentions the following
AWS Lambda runs your function code securely within a VPC by default. However, to enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function to connect securely to other resources within your private VPC.
Options B and C are incorrect since these are not valid configurations
Option D is invalid since you would ideally want to keep the VPC private.
For more information on using AWS lambda in your own private VPC, please refer to below URL:

- https://docs.aws.amazon.com/lambda/latest/dg/vpc.html (https://docs.aws.amazon.com/lambda/latest/dg/vpc.html)

Ask our Experts 👍 👎

QUESTION 50 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You're AWS Admin team has created an AWS workspace. Users on the on-premise environment don't seem to have the ability to use the AWS created workspaces. What could be the primary underling issue.

○ **A.** The AWS Workspaces have not been created properly. They need to be recreated.

○ **B.** The ports on the company firewall are not open ✓

○ **C.** The NACL's on the AWS Workspaces are not allowing incoming traffic

○ **D.** The Security Groups on AWS Workspaces are not allowing outbound traffic

Explanation :

Answer – B
The AWS Documentation mentions the following
To connect to your WorkSpaces, the network that your Amazon WorkSpaces clients are connected to must have certain ports open to the IP address ranges for the various AWS services (grouped in subsets). These address ranges vary by AWS region. These same ports must also be open on any firewall running on the client.
Options A,C and D are all invalid since the primary concern will be the ports on the company firewall
For more information on the AWS workspaces port requirements, please refer to below URL:

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

Ask our Experts 👍 👎

QUESTION 51 UNATTEMPTED DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

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

□ **A.** There is no need to configure this as AWS will fall back to a secondary Direct Connect connection as per their SLA.

□ **B.** Setup a secondary Direct Connect connection. ✓

□ **C.** Setup a VPN connection ✓

□ **D.** Setup a peering connection

Explanation :

Answer – B and C
The AWS Documentation mentions the following
If you have established a second AWS Direct Connect connection, traffic will failover to the second link automatically. We recommend enabling Bidirectional Forwarding Detection (BFD) when configuring your connections to ensure fast detection and failover. If you have configured a back-up IPsec VPN connection instead, all VPC traffic will failover to the VPN connection automatically. Traffic to/from public resources such as Amazon S3 will be routed over the Internet.
Option A is invalid because AWS will not fall back to a secondary connection. You have to ensure high availability.
Option D is invalid because this is only used for connecting 2 VPC's together.
For more information on high availability of Network connections, please refer to 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 52 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

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
This is also given in the AWS DocumentationInsufficient Instance Capacity

Description

You get the InsufficientInstanceCapacity error when you try to launch a new instance or restart a stopped instance.

Cause

If you get an InsufficientInstanceCapacity error when you try to launch an instance or restart a stopped instance, AWS does not currently have enough available On-Demand capacity to service your request.

Solution

To resolve the issue, try the following:

- Wait a few minutes and then submit your request again; capacity can shift frequently.
- Submit a new request with a reduced number of instances. For example, if you're making a single request to launch 15 instances, try making 3 requests for 5 instances, or 15 requests for 1 instance instead.
- If you're launching an instance, submit a new request without specifying an Availability Zone.
- If you're launching an instance, submit a new request using a different instance type (which you can resize at a later stage). For more information, see Changing the Instance Type.
- If you are launching instances into a cluster placement group, you can get an insufficient capacity error. For more information, see Placement Group Rules and Limitations.
- Try purchasing Reserved Instances, which are a long-term capacity reservation. For more information, see Amazon EC2 Reserved Instances.

Options A,C and D are all invalid because none of these options will help resolve the error

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

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

Ask our Experts

QUESTION 53 UNATTEMPTED DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You've just setup an Amazon Redshift cluster and started loading tables using the COPY command. You've noticed that the Internet is being utilized for the data being copied. You want to ensure that the internet is not used during the copy operation. How can you achieve this?

○ **A.** Ensure the NACL's are set on the Subnets hosting the Redshift cluster

○ **B.** Ensure Enhanced VPC routing is enabled for the Redshift cluster ✓

○ **C.** Ensure the Security Groups are set on the EC2 Instances hosting the Redshift cluster

○ **D.** Ensure the routing table points to a VPN instead of the Internet gateway

Explanation :

Answer – B
The AWS Documentation mentions the following
When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY and UNLOAD traffic between your cluster and your data repositories through your Amazon VPC. You can now use standard VPC features, such as VPC security groups, network access control lists (ACLs), VPC endpoints, VPC endpoint policies, Internet gateways, and Domain Name System (DNS) servers, to tightly manage the flow of data between your Amazon Redshift cluster and other resources. When you use Enhanced VPC Routing to route traffic through your VPC, you can also use VPC flow logs to monitor COPY and UNLOAD traffic.
If Enhanced VPC Routing is not enabled, Amazon Redshift routes traffic through the Internet, including traffic to other services within the AWS network.
Options A and C are invalid because this has more to do with the Security aspect
Option D would just be the same solution and not avoid traffic flowing via the Internet
For more information on Enhanced VPC Routing , just browse to the below URL:

- https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html (https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html)

Ask our Experts 👍 👎

QUESTION 54 UNATTEMPTED MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your production team has created a Multi-AZ Amazon RDS instance. The application connects to the instance via a custom DNS A record. There was an instance wherein the primary database failed and the application could no longer connect to the database. What needs to be done to ensure this same issue does not happen in the future.

○ **A.** Ensure that the application is using the Amazon RDS hostname ✔

○ **B.** Ensure the primary database is quickly swapped with the secondary one

○ **C.** Ensure that the application is using the IP address of primary database instance

○ **D.** Ensure that the application is using the IP address of secondary database instance

Explanation :

Answer – A
You need to ensure that the application connects using the Amazon RDS hostname. In the case of a primary instance issue , automatically in the backend the swap will occur to the secondary instance.
Option B is invalid because the switch over is done by AWS
Options C and D are invalid because you should never point to the IP address of the databases
For more information on MultiAZ for databases , just browse to the below URL:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html)

Ask our Experts 👍 👎

QUESTION 55 UNATTEMPTED DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

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

○ **A.** Use VPC Flow Logs.

○ **B.** Use a network monitoring tool provided by an AWS partner. ✔

○ **C.** Use another instance. Setup a port to “promiscuous mode” and sniff the traffic toanalyze the packets.

○ **D.** Use Cloudwatch metric

Explanation :

Answer – B
Since here you need to sniff the actual network packets , the ideal approach would be to use a network monitoring tool provided by an AWS partner.
The AWS documentation mentions the following
Multiple AWS Partner Network members offer virtual firewall appliances that can be deployed as an in-line gateway for inbound or outbound network traffic. Firewall appliances provide additional application-level filtering, deep packet inspection, IPS/IDS, and network threat protection features.
Options A and D are invalid because these cannot be used for packet inspection
Option C is invalid because promiscuous mode is not supported in AWS
For more information on the security capabilities, please visit the below URL:

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

Ask our Experts

QUESTION 56 UNATTEMPTED DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You have an on-premise application that needs access to the Simple Storage Service. Some of the key requirements are high bandwidth for the connection , low jitter and high availability. Which of the following option would you consider in the design.

○ **A.** Use the public internet to access the S3 service

○ **B.** Using AWS Direct Connect with a private VIF

○ **C.** Using AWS Direct Connect with a public VIF ✓

○ **D.** Using an IPSec VPN connection to a Virtual Private gateway

Explanation :

Answer – C
The AWS Documentation mentions the following
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
Options A and D are invalid because this would now be a ideal solution for low jitter
Option B is invalid because you need a public VIF for accessing public services such as S3
For more information on AWS Direct Connect, please visit the below URL:

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

Ask our Experts

QUESTION 57 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on hosting an Active Directory Domain server in a VPC. Resources in other VPC' will need to access the domain server for authentication and DNS routing. What is the core implementation steps you would consider in such a design? Choose 2 answers from the options given below

□ **A.** Consider a Hub and Spoke Model VPC Design ✓

□ **B.** Make use of VPC peering ✓

□ **C.** Consider a Transit VPC Design

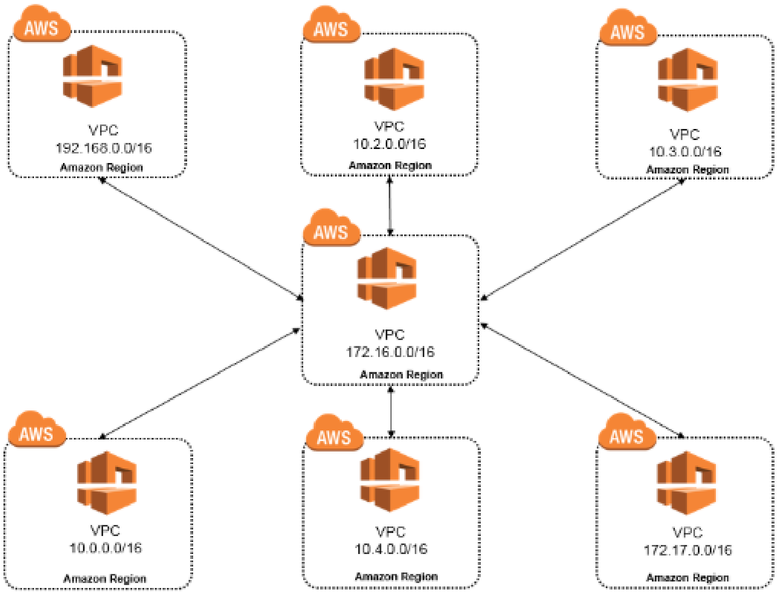
□ **D.** Make use of a VPN connection

Explanation :

Answer – A and B

A mention of such a design is given in the AWS Documentation

This is best suited when you have a shared service that needs to be shared across multiple other VPC's



Option C is invalid because this is when you want to relay information via a VPC

Option D is invalid because you need to make use of VPC Peering

For more information on Multi-VPC connectivity, please visit the below URL:

- https://aws.amazon.com/answers/networking/aws-single-region-multi-vpc-connectivity/ (https://aws.amazon.com/answers/networking/aws-single-region-multi-vpc-connectivity/)

Ask our Experts

QUESTION 58 UNATTEMPTED DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

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

□ **A.** Configure ELB with TCP listeners on TCP/443. And place the Web servers behind it. ✔

□ **B.** Configure your Web servers with EIP's. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers. ✔

□ **C.** Configure ELB with HTTPS listeners, and place the Web servers behind it.

□ **D.** Configure your web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution.

Explanation :

Answer - A and B

The AWS Documentation mentions the following

You can create a load balancer that uses the SSL/TLS protocol for encrypted connections (also known as *SSL offload*). This feature enables traffic encryption between your load balancer and the clients that initiate HTTPS sessions, and for connections between your load balancer and your EC2 instances.

Amazon CloudFront is a global content delivery network (CDN) service that accelerates delivery of your websites, APIs, video content or other web assets. It integrates with other Amazon Web Services products to give developers and businesses an easy way to accelerate content to end users with no minimum usage commitments.

Currently, ELBs cannot support authentication for the client side. SSL/TLS certificate is required for two-way SSL authentication to succeed.

The second way is to configure the webservers with Elastic IP address and have the web servers act as the endpoint for the traffic. Let Route53 DNS server send requests to these webservers in a round-robin fashion.

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

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html)

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

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

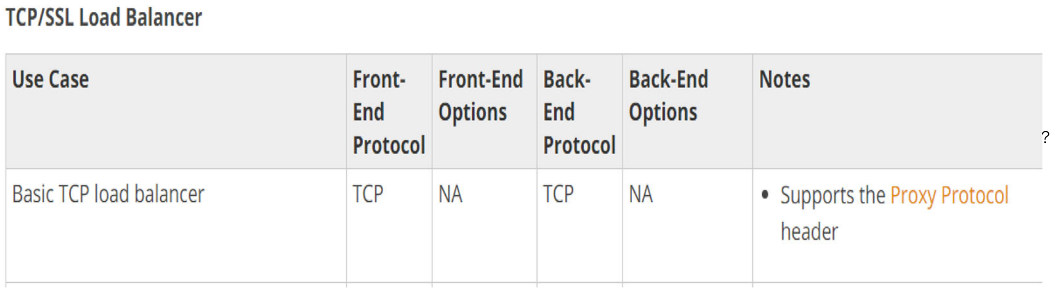
Option D is incorrect. CloudFront does not support client authentication with client-side SSL certificates. If an origin requests a client-side certificate, CloudFront drops the request.

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorCustomOrigin.html#RequestCustomClientSideS
(https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorCustomOrigin.html#RequestCustomClientSide

You can use API Gateway to generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway. This allows your HTTP backend to control and accept only requests originating from Amazon API Gateway, even if the backend is publicly accessible.

https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-client-side-ssl-authentication.html
(https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-client-side-ssl-authentication.html)

An ELB Classic Load Balancer cannot validate a client side certificate, so it must be passed through as standard TCP on port 443 to let the EC2 instance handle the validation.



TCP/SSL Load Balancer

Use Case	Front-End Protocol	Front-End Options	Back-End Protocol	Back-End Options	Notes
Basic TCP load balancer	TCP	NA	TCP	NA	• Supports the Proxy Protocol header

Proxy Protocol is an Internet protocol used to carry connection information from the source requesting the connection to the destination for which the connection was requested.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. So in this configuration Client side certificate can be used for authentication by the back end server.

So Option A seems to be correct.

Ask our Experts

QUESTION 59 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the webserver on a single EC2 instance of VPC such that it allows the internet traffic as well as the back-end management traffic. The organization wants to make so that the back-end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing webserver will have an IP address which can receive traffic from all the internet IPs.

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

○ **A.** It is not possible to have 2 IP addresses for a single instance

○ **B.** The organization should create 2 network interfaces , one for the internet traffic and the other for the backend traffic ✓

○ **C.** The organization should create 2 EC2 instances as this is not possible with one EC2 instance

○ **D.** This is not possible

Explanation :

Answer – B
You can attach 2 ENI's to the Instance. One ENI can be used to accept Internet traffic and the other can be used to interact with your instances in the private subnet.
Options A and D are invalid because a solution is possible
Option C is incorrect because you should have 2 Elastic Network Interfaces and not 2 EC2 Instances
For more information on Elastic Network Interfaces, please visit the below URL:

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

Ask our Experts 👍 👎

QUESTION 60 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on deploying EC2 Instances across multiple regions. These instances will make calls to the Simple Storage service. You are trying to understand the data transfer costs which are incurred in such an implementation. Which of the following is not charged by AWS?

○ **A.** From an Elastic Compute Cloud (Amazon EC2) in eu-west-1 to Amazon Simple Storage Service (Amazon S3) in us-east-1

○ **B.** From your on-premises data center to Amazon S3 in us-east-1 ✓

○ **C.** From Amazon EC2 in eu-west-1 to your on-premises data center

○ **D.** From Amazon S3 in us-east-1 to Amazon EC2 in eu-west-1

Explanation :

Answer - B
All data transfer into AWS via the Internet is not charged
The AWS Documentation mentions the following on data transfer rates
There is no Data Transfer charge for data transferred within an Amazon S3 Region via a COPY request. Data transferred via a COPY request between AWS Regions is charged at rates specified in the pricing section of the Amazon S3 detail page. There is no Data Transfer charge for data transferred between Amazon EC2 and Amazon S3 within the same region or for data transferred between the Amazon EC2 Northern Virginia Region and the Amazon S3 US East (Northern Virginia) Region. Data transferred between Amazon EC2 and Amazon S3 across all other regions (i.e. between the Amazon EC2 Northern California and Amazon S3 US East (Northern Virginia) is charged at rates specified on the Amazon S3 pricing page.
Options A,C and D are all invalid because all of the options will incur data charges
For more information on S3 pricing, please visit the below URL:

- https://aws.amazon.com/s3/pricing/ (https://aws.amazon.com/s3/pricing/)

For more information on EC2 pricing, please visit the below URL:

- https://aws.amazon.com/ec2/pricing/ (https://aws.amazon.com/ec2/pricing/)

Ask our Experts 👍 👎

QUESTION 61 UNATTEMPTED AUTOMATE AWS TASKS

You have been requested to use CloudFormation to maintain version control and achieve automation for the applications in your organization. The environment will consist of several networking components and application services. What is the best way to design the template.

○ **A.** Create separate templates based on functionality, create nested stacks with CloudFormation. ✓

○ **B.** Use CloudFormation custom resources to handle dependencies between stacks

○ **C.** Create multiple templates in one CloudFormation stack.

○ **D.** Combine all resources into one template for version control and automation.

Explanation :

Answer – A
Create separate stacks templates. So create a separate one for networking so that can be managed separately.
Option B is incorrect because custom resources is not the right option for managing multiple components.
Option C is incorrect because You can’t have multiple templates in one CloudFormation stack
Option D is incorrect because maintaining one template can become an issue.
For more information on Cloudformation best practises please refer to the below link:

- http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html (http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html)

Ask our Experts

QUESTION 62 UNATTEMPTED CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your team is using a NAT instance on an Linux EC2 Instance. The private subnet has a route added for 0.0.0.0/0 for the NAT instance. This NAT instance is being used to download updates from the Internet for instances in the private subnet. But the IT administrators who are in charge of applying the updates complain of slow response times. What can be done to rectify this issue? Choose 2 answers from the options given below

□ **A.** Add another NAT instance. Add another route for 0.0.0.0/0 to the new NAT instance

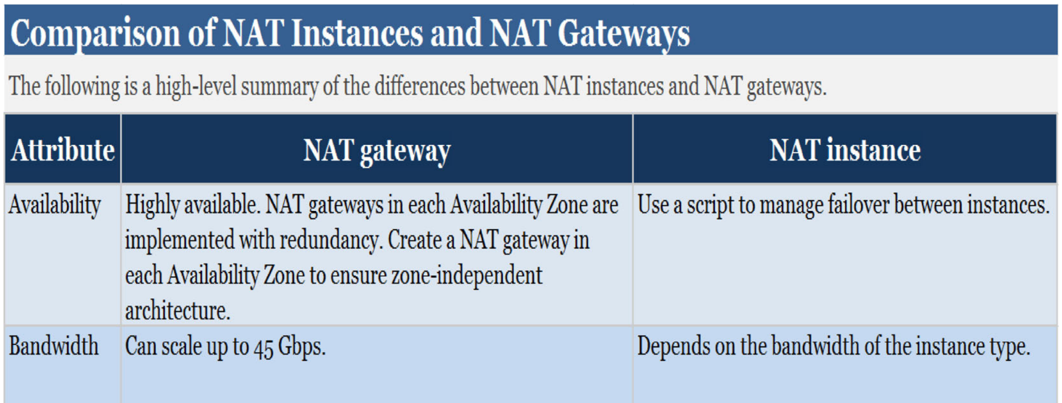
□ **B.** Replace the NAT instance with a NAT gateway ✓

□ **C.** Upgrade the NAT instance to a larger Instance type ✓

□ **D.** Move the NAT instance to the private subnet to be closer the instances

Explanation :

Answer - B and C
The bandwidth capability of the NAT instance depends on the Instance type. Below is a part of the comparison of NAT instances and NAT gateways from the AWS Documentation



Comparison of NAT Instances and NAT Gateways

The following is a high-level summary of the differences between NAT instances and NAT gateways.

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type.

So one option is to replace the NAT instance with a NAT gateway. The other option is to upgrade the instance type of the current NAT instance.

Option A is incorrect because this is not possible to add 2 routes for the same destination
Option D is incorrect because the NAT instance has to be in a public subnet
For more information on the comparison of NAT instances with NAT gateways, please refer to the below link:

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

Ask our Experts 👍 👎

QUESTION 63 UNATTEMPTED CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You have a team that is trying to ingest data in Amazon S3. They are trying to ingest 1 TB of data using a large instance. Enhanced Networking has been enabled on the instance. But the data ingestion process is still running slowly. What can be done to rectify the issue?

○ **A.** Use an AWS Direct Connect connection between S3 and the instance

○ **B.** Create a VPC endpoint from the instance to S3

○ **C.** Consider using 2 instances and splitting the ingestion of data ✓

○ **D.** Create a VPN connection from the instance to S3

Explanation :

Answer – C
Trying to upload a single large object might not be feasible and hence it is better to split the object across multiple instances and carry out the data ingestion process.
Option A,B and D are all incorrect since this is a limitation on the instance side
For more information on Amazon S3, please refer to the below link:

- https://aws.amazon.com/s3/faqs/ (https://aws.amazon.com/s3/faqs/)

Ask our Experts 👍 👎

QUESTION 64 UNATTEMPTED DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your current web application is hosted on a set of EC2 Instances which are placed behind an application load balancer. All the Security groups and NACL's have been put into place for tight security. What extra measure can be taken to ensure blocking of DDos attacks from malicious IP addresses

○ **A.** Consider placing the WAF service in front of the Application Load balancer ✓

○ **B.** Consider placing an AWS PrivateLink service in front of the Application Load balancer

○ **C.** Consider placing an AWS Shield service in front of the Application Load balancer

○ **D.** Consider adding the more restrictive rules to the Network ACL's

Explanation :

Answer – A
The AWS Documentation mentions the following
AWS WAF is a web application firewall that lets you monitor web requests that are forwarded to Amazon CloudFront distributions or an Application Load Balancer. You can also use AWS WAF to block or allow requests based on conditions that you specify, such as the IP addresses that requests originate from or values in the requests.
Option B is incorrect because AWS PrivateLink is used to provide an endpoint for a service
Option C is incorrect because AWS Shield is already a service present. You need AWS Shield Advanced for DDos protection
Option D is incorrect because you need a better effective mechanism for protecting against DDoS attacks
For more information on AWS WAF, please refer to the below link:

- https://aws.amazon.com/documentation/waf/ (https://aws.amazon.com/documentation/waf/)

Ask our Experts

QUESTION 65 CORRECT DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has the following Direct Connect and VPN Connections

Site A - VPN 10.1.0.0/24 AS 65000 65000

Site B - VPN 10.1.0.252/30 AS 65000

Site C - Direct Connect 10.0.0.0/8 AS 65000

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

You are trying to connect to an IP address of 10.1.0.254. Which of the following route will be chosen?

○ **A.** Site A

○ **B.** Site B ✓

○ **C.** Site C

○ **D.** Site D

Explanation :

Answer – B

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

Option A,C and D are all incorrect since the shortest prefix would be chosen.

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

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

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14775)

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)