PRACTICE TEST III

Attempt	1
Marks Obtained	0 / 80
Your score is	0.0%
Completed on	Sunday , 03 February 2019 , 11:07 PM
Time Taken	00 H 00 M 07 S
Result	Fail

Domains / Topics wise Quiz Performance Report

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

80 Questions	**0** Correct	**0** Incorrect	**80** Unattempted

Show Answers

All

QUESTION 1 UNATTEMPTED

Which of the following are supported bandwidths for the Link Aggregation Group when it comes to Direct Connect. Choose 2 answers from the options given below

- [ ] **A.** 500 Mbps
- [ ] **B.** 1 Gbps ✔

- [ ] **C.** 10 Gbps ✔
- [ ] **D.** 20 Gbps

Explanation :

Answer – B and C
The AWS documentation mentions the following on link aggregation group
· 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.
For more information on link aggregation group , please refer to the below link

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

Ask our Experts

QUESTION 2 UNATTEMPTED

Your company has a highly available Direct Connect solution that utilizes two datacenters. Each data center contains one two-connection LAG and one standard DX connection. How many LOAs will be filled out in total if your company completes an order to add a new connection to each one of the LAGs?

- ○ **A.** 1
- ○ **B.** 4 ✔
- ○ **C.** 6
- ○ **D.** 10

Explanation :

Answer – B
AWS documentation and LOA is used for DX, interconnect and Link Aggregation **Group**

- https://docs.aws.amazon.com/cli/latest/reference/directconnect/describe-loa.html (https://docs.aws.amazon.com/cli/latest/reference/directconnect/describe-loa.html)

So in this example each data centre would have 2 LOAs (1 DX and 1 LAG) = 4 and adding more connection to the LAGs will not increase the number of LOAs.
The AWS documentation mentions the following on link aggregation group
When you create a LAG, you can download the Letter of Authorization and Connecting Facility Assignment (LOA-CFA) for each new physical connection individually from the AWS Direct Connect console
For more information on link aggregation group , please refer to the below link

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

Ask our Experts

QUESTION 3 UNATTEMPTED

Which of the following are best practices when creating VPN connections with on-premise data centers. Choose 3 answers from the options given below

- [ ] **A.** Ensure to limit the traffic that flows through the VPN ✔
- [ ] **B.** Ensure to implement non-overlapping network ranges for your private networks ✔
- [ ] **C.** Consider using static routed network connections for better performance
- [ ] **D.** Consider using dynamic routed network connections for better performance ✔

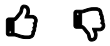
Explanation :

Answer – A,B and D
The AWS documentation mentions the following
When configuring VPN connections to any computer network, there are some universal network-design principles to consider. For example, whenever possible, limit the amount of traffic that must traverse VPN connections. This will reduce VPN network contention and latency, which can improve application performance. It is also best to implement non-overlapping network ranges for your private

networks to simplify the ability to route between remote networks. Finally, use dynamically routed network connections to create highly available, resilient, more scalable links to resources in your corporate network.
For more information on VPC-VPN connection sharing , please refer to the below link

- https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing/ (https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing/)

Ask our Experts



QUESTION 4 UNATTEMPTED

A company currently has a number of VPC's hosted in AWS. They also have a VPN connection between their on-premise data center and AWS. They want to limit the number of VPN connections they would need to create in order to ensure that the VPC's hosted in AWS can talk to the on-premise services. Which of the below is a way that this can be achieved.

- **A.** Peer the VPC's together and then forward the traffic through one of the VPC's
- **B.** Create a shared services VPC and route all requests to the other VPC's via this VPC ✔
- **C.** There is no way, you need to ensure there is a VPN connection between each VPC and the on-premise infrastructure
- **D.** Make use of an AWS storage Gateway to integrate AWS Cloud with existing on-premise infrastructure.

Explanation :

Answer – B
The AWS documentation mentions the following

Shared Services VPC

This approach creates a shared services VPC which contains replicated services, and also application proxies for requests to remote resources that cannot be directly replicated as a shared service. This approach eliminates the need to create VPN connections for additional VPCs because all required on-premises resources will be accessed either directly or indirectly through the shared services VPC.

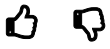
This option is best suited for customers with the following use case/requirements:

- The majority of their infrastructure is (or will be) on AWS
- The required on-premises resources are easy to replicate or proxy (e.g., Active Directory)
- They prefer to limit VPN traffic
- Strong security or compliance programs require additional application-level controls and proxy servers between their AWS and on-premises resources (e.g., application-layer firewalls)

For more information on VPC-VPN connection sharing , please refer to the below link

- https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing/ (https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing/)

Ask our Experts



QUESTION 5 UNATTEMPTED

You have created a NAT gateway to ensure that instances in your private subnet can download updates from the internet. But the instances are still not able to reach the internet even after the gateway has been created. Which of the following is not a right verification that needs to be carried out to diagnose the issue?

- A. Verify that the destination is reachable by pinging the destination from another source using a public IP address
- B. Verify that the NAT gateway is in the Available state
- C. Verify that the NAT gateway has been created in the private subnet ✔
- D. Make sure that the private subnet's route table has a default route pointing to the NAT gateway

Explanation :

Answer - C
The NAT gateway needs to be created in the public subnet and not the private subnet
The AWS documentation mentions some of the below points which can be used to diagnose internet connectivity issues for EC2 Instances
To troubleshoot instances that can't connect to the Internet from a private subnet using a NAT gateway, check the following:

- Verify that the destination is reachable by pinging the destination from another source using a public IP address.
- Verify that the NAT gateway is in the Available state. Note: A NAT gateway in the Failed state is automatically deleted after about an hour.
- Make sure that you've created your NAT gateway in a public subnet, and that that the public route table has a default route pointing to an Internet gateway.
- Make sure that the private subnet's route table has a default route pointing to the NAT gateway.

Check that you have allowed the required protocols and ports for outbound traffic to the Internet.

For more information on EC2 Internet connectivity , please refer to the below link

- https://aws.amazon.com/premiumsupport/knowledge-center/ec2-internet-connectivity/ (https://aws.amazon.com/premiumsupport/knowledge-center/ec2-internet-connectivity/)

Ask our Experts

QUESTION 6 UNATTEMPTED

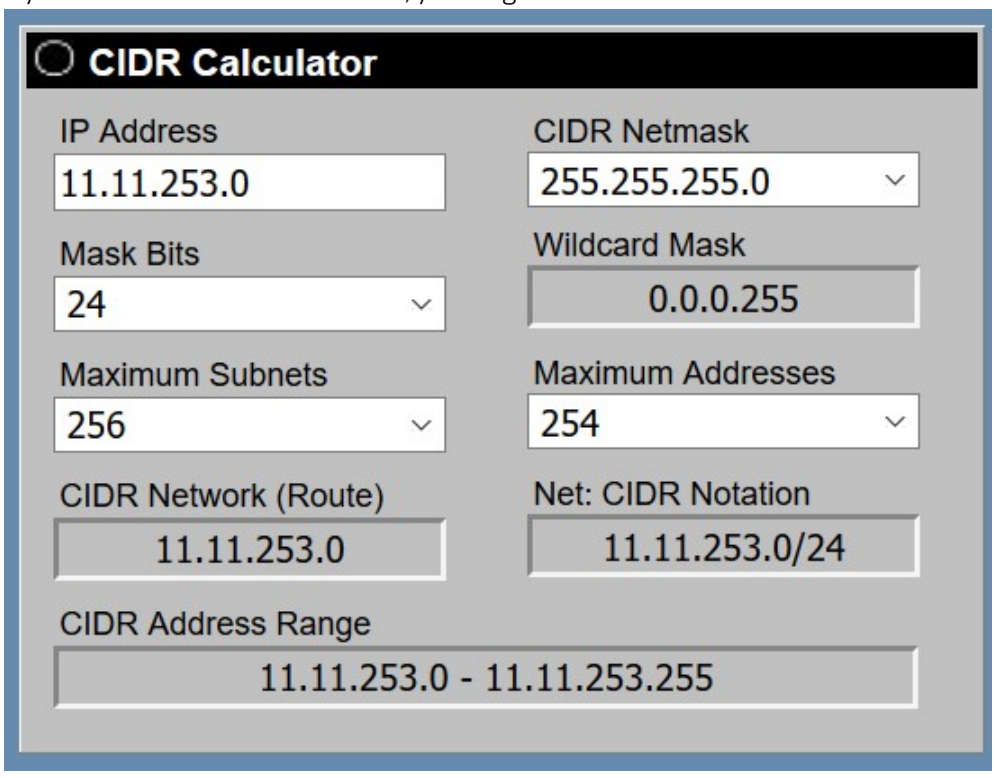
You have instructed to create a presence on the AWS Cloud. The IP address range 11.11.253.0/24 has been allocated for the cloud. Which of the following is the right number of subnets and hosts available for this CIDR range. Do not consider the reserved IP addresses for subnets.

- **A.** 256 maximum number of subnets and 254 number of hosts ✔
- **B.** 128 maximum number of subnets and 254 number of hosts
- **C.** 256 maximum number of subnets and 128 number of hosts
- **D.** 256 maximum number of subnets and 256 number of hosts

Explanation :

Answer – A

If you use an online CIDR calculator , you will get the number of subnets and hosts allowed



For the link on the CIDR calculator, please refer to the below link

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

Ask our Experts

QUESTION 7 UNATTEMPTED

Which of the following is not used as a VPC to VPC connectivity option

- A. VPC Peering
- B. Software VPN
- C. AWS VPN CloudHub ✔
- D. Hardware VPN

Explanation :

Answer – C
AWS VPN Cloudhub is used for connecting on-premise data centers to AWS VPC
The AWS documentation mentions the following on VPC to VP connectivity options

Amazon VPC–to–Amazon VPC Connectivity Options	
VPC Peering	Describes the AWS-recommended approach for connecting multiple Amazon VPCs within a region using the Amazon VPC peering feature.
Software VPN	Describes connecting multiple Amazon VPCs using VPN connections established between user-managed software VPN appliances running inside of each Amazon VPC.
Software-to-Hardware VPN	Describes connecting multiple Amazon VPCs with a VPN connection established between a user-managed software VPN appliance in one Amazon VPC and AWS-managed network equipment attached to the other Amazon VPC.
Hardware VPN	Describes connecting multiple Amazon VPCs, leveraging multiple hardware VPN connections between your remote network and each of your Amazon VPCs.
AWS Direct Connect	Describes connecting multiple Amazon VPCs, leveraging logical connections on customer-managed AWS Direct Connect routers.

For more information on the VPC connectivity options, please visit the below link

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

Ask our Experts

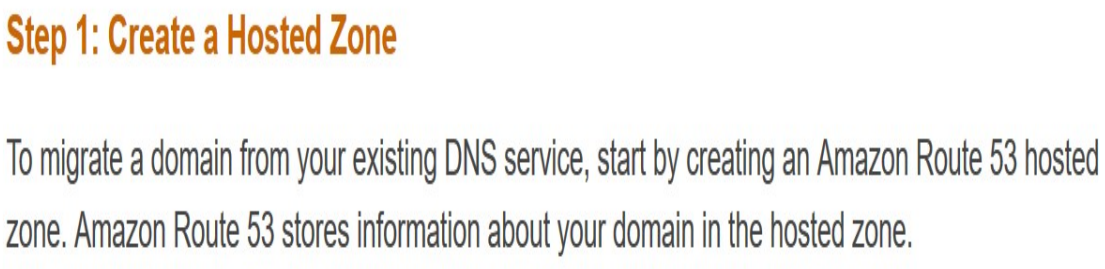
QUESTION 8 UNATTEMPTED

You are considering on migrating your existing DNS service to AWS Route53. Which of the following is the first thing you should do in Route53 for this.

- A. Create a CNAME record
- B. Create a AAA record
- C. Create a hosted zone ✔
- D. Create a new domain name

Explanation :

Answer – C
This is given in the AWS documentation



For more information on migrating DNS, please visit the below link

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

Ask our Experts

QUESTION 9 UNATTEMPTED

What does it mean when one want to configure white label servers in AWS.

- **A.** This is when you want to configure EC2 Instances for the first time
- **B.** This is when you want to configure placement groups for the first time.
- **C.** This is when you to configure AMI's for EC2 Instances
- **D.** This is when you want to have name servers in Route53 to be the same as the domain name of your hosted zone ✔

Explanation :

Answer - D
This is given in the AWS documentation
Each Amazon Route 53 hosted zone is associated with four name servers, known collectively as a delegation set. By default, the name servers have names like ns-2048.awsdns-64.com. If you want the domain name of your name servers to be the same as the domain name of your hosted zone, for example, ns1.example.com, you can configure white label name servers, also known as vanity name servers or private name servers.
For more information on migrating DNS, please visit the below link

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/white-label-name-servers.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/white-label-name-servers.html)

Ask our Experts

QUESTION 10 UNATTEMPTED

You have the requirement to get a snapshot of the current configuration of the resources in your AWS Account. Which of the following services can be used for this purpose

- A. AWS CodeDeploy
- B. AWS Trusted Advisor
- C. AWS Config ✔
- D. AWS IAM

Explanation :

Answer - C
The AWS Documentation mentions the following
With AWS Config, you can do the following:

- Evaluate your AWS resource configurations for desired settings.
- Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.
- Retrieve configurations of one or more resources that exist in your account.
- Retrieve historical configurations of one or more resources.
- Receive a notification whenever a resource is created, modified, or deleted.
- View relationships between resources. For example, you might want to find all resources that use a particular security group.

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

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

Ask our Experts

QUESTION 11 UNATTEMPTED

An audit is going to be conducted for your company's AWS account. Which of the following steps will ensure that the auditor has the right access to the logs of your AWS account

- **A.** Enable S3 and ELB logs. Send the logs as a zip file to the IT Auditor.
- **B.** Ensure that Cloudtrail is enabled. Create a role for read only access to Cloudtrail. Create a user for the IT Auditor and attach the role to the user. ✔
- **C.** Ensure that Cloudtrail is enabled. Create a user for the IT Auditor and ensure that full control is given to the user for Cloudtrail.
- **D.** Enable Cloudwatch logs. Create a user for the IT Auditor and ensure that full control is given to the user for the Cloudwatch logs.

Explanation :

Answer – B
The AWS Documentation clearly mentions the below
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
For more information on Cloudtrail, please visit the below URL:

- http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)

Ask our Experts

QUESTION 12 UNATTEMPTED

Your company has an on-premise Active Directory setup in place. The company has extended their footprint on AWS , but still want to have the ability to use their on-premise Active Directory for authentication. Which of the following AWS services can be used to ensure that AWS resources such as AWS Workspaces can continue to use the existing credentials stored in the on-premise Active Directory.

- **A.** Use the Active Directory service on AWS
- **B.** Use the AWS Simple AD service

- C. Use the Active Directory connector service on AWS ✔
- D. Use the ClassicLink feature on AWS

Explanation :

Answer – C
The AWS Documentation mentions the following
AD Connector is a directory gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory without caching any information in the cloud. AD Connector comes in two sizes, small and large. A small AD Connector is designed for smaller organizations of up to 500 users. A large AD Connector can support larger organizations of up to 5,000 users.
For more information on the AD connector, please refer to the below URL:

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

Ask our Experts

QUESTION 13 UNATTEMPTED

Which of the below 3 things can you achieve with the Cloudwatch logs service

- [ ] A. Record API calls for your AWS account and delivers log files containing API calls to your Amazon S3 bucket
- [ ] B. Send the log data to AWS Lambda for custom processing or to load into other systems ✔
- [ ] C. Stream the log data to Amazon Kinesis ✔
- [ ] D. Stream the log data into Amazon Elasticsearch in near real-time with CloudWatch Logs subscriptions. ✔

Explanation :

Answer - B,C and D
You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, and other sources. You can then retrieve the associated log data from CloudWatch Logs.
For more information on Cloudwatch logs, please visit the below URL:

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

Ask our Experts

QUESTION 14 UNATTEMPTED

Which of the following commands can be used to get the detailed of the ENI's in a particular region

- A. get-network-cards
- B. get-network-interfaces
- C. describe-ENI
- D. describe-network-interfaces ✔

Explanation :

Answer - D
This command can be used to get the details of one or more network interfaces
For more information on the command, please visit the below URL:

- http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-network-interfaces.html (http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-network-interfaces.html)

Ask our Experts

QUESTION 15 UNATTEMPTED

A Classic load balancer has been setup in AWS where the backend instances listen on the TCP protocol. There is a requirement to get the client IP's which hit the load balancer. Which of the following can be used to fulfil this requirement

- A. Use the Proxy Protocol Header ✔
- B. Configure sticky sessions
- C. Configure connection draining
- D. Configure Cross-Zone Load balancing

Explanation :

Answer - A
The AWS documentation mentions the following
The Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections. Because load balancers intercept traffic between clients and your instances, the access logs from your instance contain the IP address of the load balancer instead of the originating client. You can parse the first line of the request to retrieve your client's IP address and the port number.
For more information on Proxy protocol please visit the below URL:

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

Ask our Experts

QUESTION 16 UNATTEMPTED

Which of the following is the mode in which connections in a Link Aggregation Group operate in

- A. Active/Passive mode
- B. Passive/Active mode
- C. Active/Active mode ✔
- D. Passive/Passive mode

Explanation :

Answer – C
The AWS documentation mentions the following
All LAGs have an attribute that determines the minimum number of connections in the LAG that must be operational for the LAG itself to be operational. By default, new LAGs have this attribute set to 0. You can update your LAG to specify a different value—doing so means that your entire LAG becomes non-operational if the number of operational connections falls below this threshold. This attribute can be used to prevent over-utilization of the remaining connections.
All connections in a LAG operate in Active/Active mode.
For more information on link aggregation group , please refer to the below link:

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

Ask our Experts

QUESTION 17 UNATTEMPTED

Which of the following is incorrect when it comes to the NAT gateway

- A. You can associate a security group with the NAT gateway ✔
- B. A NAT gateway supports bursts of up to 10 Gbps of bandwidth
- C. You can associate exactly one Elastic IP address with a NAT gateway
- D. A NAT gateway supports the following protocols: TCP, UDP, and ICMP

Explanation :

Answer - A
The AWS documentation mentions the following
A NAT gateway has the following characteristics:

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

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

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

Ask our Experts

QUESTION 18 UNATTEMPTED

Apart from the below 2 aspects , what other requirements need to be in place to ensure that instances from a VPC subnet can access the Internet.

1. Ensure that your subnet's route table points to the Internet gateway

2. Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance

Choose 2 answers from the options given below

- [ ] **A.** Attach an Internet gateway to your VPC. ✔
- [ ] **B.** Attach an Internet gateway to your subnet.
- [ ] **C.** Ensure the instance in the subnet has a private IP

☐ **D.** Ensure the instance in the subnet has a public IP ✔

Explanation :

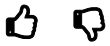
Answer – A and D
The AWS documentation mentions the following on Internet gateways
To enable access to or from the Internet for instances in a VPC subnet, you must do the following:

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

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

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

Ask our Experts



QUESTION 19 UNATTEMPTED

What are the 2 types of endpoints available in a VPC for accessing public AWS resources

☐ **A.** Primary
☐ **B.** Interface ✔
☐ **C.** Gateway ✔
☐ **D.** Internal

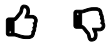
Explanation :

Answer – B and C
The AWS documentation mentions the following
1. Interface - An elastic network interface with a private IP address that serves as an entry point for

traffic destined to a supported AWS service.
2. Gateway - A gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service
For more information on VPC endpoints, please refer to the below link:

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

Ask our Experts



QUESTION 20 UNATTEMPTED

Which of the following are valid origins for Cloudfront Web distributions. Choose 2 answers from the options given below

- [ ] **A.** An HTTP Server ✔
- [ ] **B.** An S3 bucket ✔
- [ ] **C.** An SQS queue
- [ ] **D.** An SNS topic

Explanation :

Answer – A and B
The AWS documentation mentions that the origin for a cloudfront distribution can be an Amazon S3 bucket or HTTP server from which CloudFront gets the files that it distributes.
For more information on the distributions, please refer to the below link:

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

Ask our Experts

QUESTION 21 UNATTEMPTED

Which of the following can be used to change the cache behavior for objects stored in Cloudfront. Choose 3 answers from the below options.

- [x] **A.** Minimum TTL ✔
- [ ] **B.** Cache TTL
- [x] **C.** Maximum TTL ✔
- [x] **D.** Default TTL ✔

Explanation :

Answer – A,C and D
To change the cache duration for all objects that match the same path pattern, you can change the CloudFront settings for Minimum TTL, Maximum TTL, and Default TTL for a cache behavior.
For more information on Cloudfront Cache, please refer to the below link:

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

Ask our Experts

QUESTION 22 UNATTEMPTED

In order to serve private content , which of the following can be used with Cloudfront. Choose 2 answers from the options shown below

- [x] **A.** Use Signed URL's ✔
- [ ] **B.** Use Signed Objects
- [ ] **C.** Use Signed Distributions

☐ **D.** Use Signed Cookies ✔

Explanation :

Answer – A and D
You can configure CloudFront to require that users access your objects using either signed URLs or signed cookies
For more information on serving private content, please refer to the below link:

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

Ask our Experts

QUESTION 23 UNATTEMPTED

Your application server instances reside in the private subnet of your VPC. These instances need to access a Git repository on the Internet. You create a NAT gateway in the public subnet of your VPC. The NAT gateway can reach the Git repository, but instances in the private subnet cannot. You confirm that a default route in the private subnet route table points to the NAT gateway. The security group for your application server instances permits all traffic to the NAT gateway.

What configuration change should you make to ensure that these instances can reach the patch server?

○ **A.** Assign public IP addresses to the instances and route 0.0.0.0/0 to the Internet gateway.

- **B.** Configure an outbound rule on the application server instance security group for the Git repository. ✔
- **C.** Configure inbound network access control lists (network ACLs) to allow traffic from the Git repository to the public subnet.
- **D.** Configure an inbound rule on the application server instance security group for the Git repository.

Explanation :

Answer – B
The traffic leaves the instance destined for the Git repository; at this point, the security group must allow it through. The route then directs that traffic (based on the IP) to the NAT gateway.
Option A is wrong because it removes the private aspect of the subnet and would have no effect on the blocked traffic anyway.
Option C is wrong because the problem is that outgoing traffic is not getting to the NAT gateway.
Option D is wrong because to allow outgoing traffic to the Git repository requires an outgoing security group rule
For more information on security groups, please refer to the below link:

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

Ask our Experts

QUESTION 24 UNATTEMPTED

If you want to have a cluster of EC2 Instances which would need to have low network latency between them , which of the following would you ideally do.

- **A.** Launch all of the Instances as t2.micro instances
- **B.** Launch all of the instances with Security Groups which allows all network traffic
- **C.** Launch all of the instances with NACL's which allows all network traffic
- **D.** Launch all of the instances in a placement group ✔

Explanation :

Answer – D
The AWS documentation mentions the following
A *placement group* is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking. For more information on placement groups, please refer to the below link:

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

Ask our Experts

QUESTION 25 UNATTEMPTED

You are responsible for several EC2 instances deployed from Amazon AMIs that are required to upload information to an S3 bucket. This information must not traverse the public internet. You must also be able to update the instances. Which option is your best solution?

- **A.** Consider using a VPN with an IP addresses specified in the AWS official S3 prefix list
- **B.** Use an S3 endpoint along with a NAT gateway.
- **C.** Use an S3 endpoint along with a NAT Instance.
- **D.** Use an S3 end point associated with the VPC. ✔

Explanation :

Answer – D
Option A is incorrect. VPN is not a solution for this case
Option B and C are incorrect - Because both NAT gateway and NAT instance are used for private instances to communicate with the internet.
Option D is correct. Tha main requirement of the question is that we need to upload information to S3

with out using internet. S3 is a service residing outside the VPC. We also need to update the server with the latest patches.
NAT Gateway is not required since AWS hosts YUM repository on S3 can be accessed using S3 VPC GATEWAY endpoint, and doesn't need to go across the internet to get the server updates.
We need to create an S3 end point for the VPC and select the route table.
Subnets associated with selected route tables will be able to access this endpoint. When we use an S3 end point to connect we will be using Amazon's internal network to communicate with the S3 rather than internet.

Ask our Experts

QUESTION 26 UNATTEMPTED

Which of the following can be used to monitor the traffic that is reaching your EC2 Instances

- A. Security groups
- B. NACL's
- C. VPC Flow Logs ✔
- D. Subnet Flow Logs

Explanation :

Answer - C
The AWS documentation mentions the following
Flow logs can help you with a number of tasks; for example, to troubleshoot why specific traffic is not reaching an instance, which in turn can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.
For more information on VPC FlowLogs, please refer to the below link:

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

Ask our Experts

QUESTION 27 UNATTEMPTED

Which of the following is false when it comes to DHCP Options Set.

- **A.** You can modify the DHCP options set after they have been created. ✔
- **B.** You can have multiple sets of DHCP options
- **C.** One DHCP options can be associated with one VPC at a time
- **D.** If you delete a VPC, the DHCP options set associated with the VPC are also deleted.

Explanation :

Answer – A
The AWS documentation mentions the following
After you create a set of DHCP options, you can't modify them. If you want your VPC to use a different set of DHCP options, you must create a new set and associate them with your VPC. You can also set up your VPC to use no DHCP options at all.
You can have multiple sets of DHCP options, but you can associate only one set of DHCP options with a VPC at a time. If you delete a VPC, the DHCP options set associated with the VPC are also deleted.
For more information on DHCP Options Set, please refer to the below link:

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

Ask our Experts

QUESTION 28 UNATTEMPTED

Which of the following are used to ensure instances in the private subnet can communicate with the Internet. Choose 2 answers from the options below.

- [ ] **A.** Internet gateway
- [ ] **B.** NAT Instances ✔
- [ ] **C.** NAT Gateway ✔
- [ ] **D.** AWS Direct Connect

Explanation :

Answer – B and C
The AWS documentation mentions the following
Customer EC2 instances in a private subnet sometimes need to communicate with the public Internet. A NAT device enables this connection, replacing internal servers' private IP addresses with public IP addresses on the way out of the network, and retranslating response IP addresses on the way back in. AWS offers two types of NAT options: NAT gateways and NAT instances. NAT gateways are AWS managed while customers are responsible for managing NAT instances. NAT gateways provide better availability and bandwidth over individual NAT instances, however customers can leverage multiple NAT instances to increase availability and network performance
For more information on VPC egress traffic, please refer to the below link:

- https://aws.amazon.com/answers/networking/controlling-vpc-egress-traffic/ (https://aws.amazon.com/answers/networking/controlling-vpc-egress-traffic/)

Ask our Experts

QUESTION 29 UNATTEMPTED

Which of the following services can be used to mitigate DDos attacks to your application hosted in AWS. Choose 3 answers from the options given below

- [ ] **A.** Route53 ✔
- [ ] **B.** Cloudfront ✔
- [ ] **C.** Elastic Load balancer ✔
- [ ] **D.** SQS

Explanation :

Answer-A,B & C
The AWS documentation mentions the following
1. Route53- One of the most common targets of DDoS attacks is the Domain Name System (DNS). Amazon Route 53 is a highly available and scalable DNS service designed to route end users to infrastructure running inside or outside of AWS. Route 53 makes it possible to manage traffic globally through a variety of routing types, and provides out-of-the-box shuffle sharding and Anycast routing capabilities to protect domain names from DNS-based DDoS attacks.
2. Cloudfront - Amazon CloudFront distributes traffic across multiple Points of Presence (PoP) locations and filters requests to ensure that only valid HTTP(S) requests will be forwarded to backend hosts.
3. Elastic Load Balancing (ELB) enables the automatic distribution of application traffic to several Amazon Elastic Compute Cloud (Amazon EC2) instances across multiple Availability Zones, which minimizes the risk of overloading a single EC2 instance. Elastic Load Balancing, like CloudFront, only supports valid TCP requests, so DDoS attacks such as UDP and SYN floods are not able to reach EC2 instances

For more information on mitigation of DDos attacks, please refer to the below link:

- https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/ (https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/)

Ask our Experts

QUESTION 30 UNATTEMPTED

As an AWS professional you have been told to ensure that traffic to an application is evenly balanced. The application has multiple web servers that host the application? Choose an answer from the options below which will fulfil the above requirement.

- **A.** Configure a NAT instance in your VPC Create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address.
- **B.** Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.

- **C.** Place all your web servers behind ELB. Configure a Route53 CNAME to point to the ELB DNS name. ✔
- **D.** Configure ELB with an EIP. Place all your Web servers behind ELB Configure a Route53 A record that points to the EIP.

Explanation :

Answer – C
Option A is wrong because a NAT instance is ideally used to route traffic from a private subnet to the internet via a public subnet.
Option B is wrong because you don't want to point Cloudfront to private IP Addresses.
You can use an ELB, assign the web servers and have a Route 53 entry to the ELB.
For more information on how to use ELB, please visit the below link:

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

Ask our Experts

QUESTION 31 UNATTEMPTED

Your company was recently acquired and a Direct Connection connection was extended from your new parent corporation to your AWS VPC using a hosted Virtual Interface. What data charges are billed to your account for that connection?

- **A.** You are not charged anything.
- **B.** You are responsible for all data transfer in.
- **C.** You are only responsible for the port hours of the Virtual Interface.
- **D.** You are responsible for all data transfer out. ✔

Explanation :

Answer – D

This is given in the AWS documentation
Data Transfer via AWS Direct Connect will be billed in the same month in which the usage occurred. If you have a hosted virtual interface, you will only be charged for the data transferred out of that virtual interface at the applicable Data Transfer rates
For more information on AWS Direct Connect, please visit the below link:

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

Ask our Experts

QUESTION 32 UNATTEMPTED

Your network utilizes jumbo frames on its servers and your router. You are trying to access your AWS resources, and you are having issues with packet loss. Which of the following can be thought of to rectify the issue.

- A. Considering Lowering the MTU for your network.
- B. Remove the "Do not Fragment" flag on the packets. ✔
- C. Consider using Direct Connect
- D. Call AWS support.

Explanation :

Answer – B
IP fragmentation can cause excessive retransmissions when fragments encounter packet loss and reliable protocols such as TCP must retransmit all of the fragments in order to recover from the loss of a single fragment
For more information on IP Fragmentation, please visit the below link:

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

Ask our Experts

QUESTION 33 UNATTEMPTED

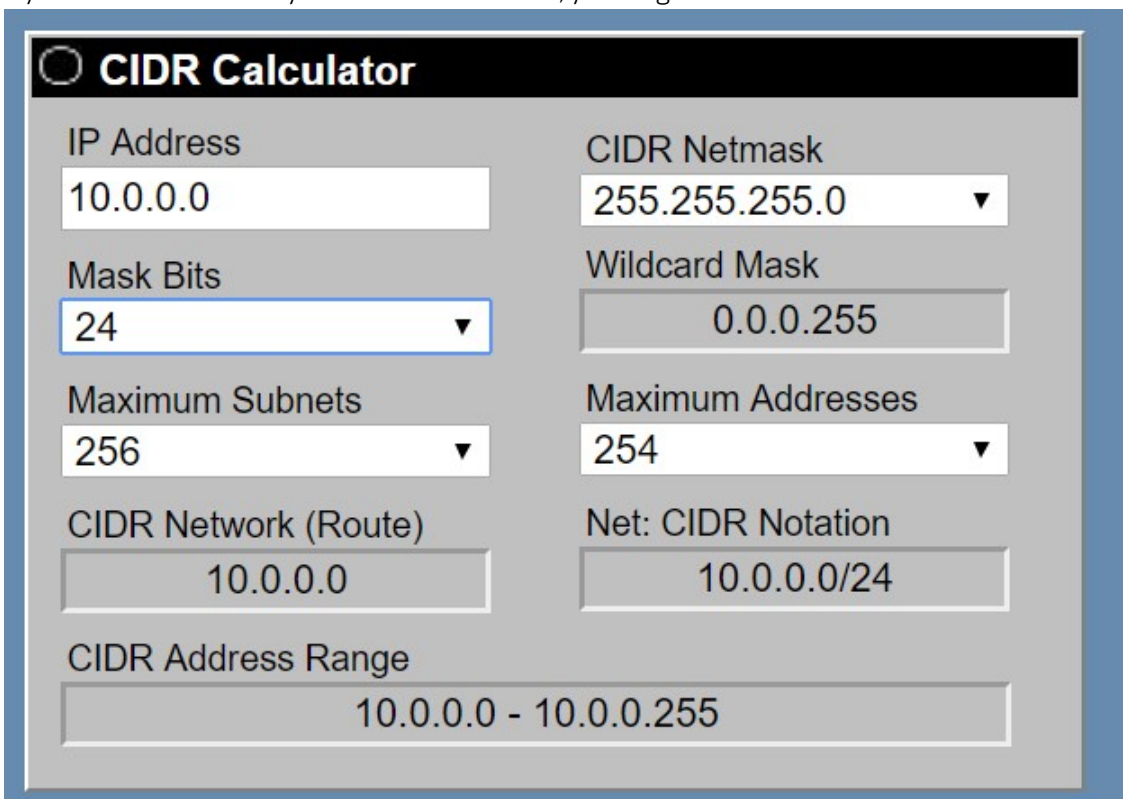
You have been told to define a VPC with a CIDR block as 10.0.0.0/24. What is the equivalent Network mask for this block?

- A. 255.255.254.0
- B. 255.255.252.0
- C. 255.255.255.0 ✔
- D. 255.255.250.0

Explanation :

Answer – C

If you see the result of any online CIDR calculator , you will get this result



For trying out the CIDR calculator, please visit the following URL:

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

Ask our Experts

QUESTION 34 UNATTEMPTED

Which of the following is not an item which is captured via VPC Flow Logs

- A. Source Address
- B. Destination Port
- C. Packets
- D. Frames ✔

Explanation :

Answer – D
The Frames element is not captured.
The below snapshot from the documentation shows a segment of elements which are captured

Field	Description
version	The VPC flow logs version.
account-id	The AWS account ID for the flow log.
interface-id	The ID of the network interface for which the log stream applies.
srcaddr	The source IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
dstaddr	The destination IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
srcport	The source port of the traffic.
dstport	The destination port of the traffic.
protocol	The IANA protocol number of the traffic. For more information, go to Assigned Internet Protocol Numbers.
packets	The number of packets transferred during the capture window.

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

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html#flow-log-records (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html#flow-log-records)

Ask our Experts

QUESTION 35 UNATTEMPTED

Which of the following statements about VPC and IP addressing is false.

- A. You can enable IPv6 support for your VPC and resources
- B. You cannot disable IPv4 support for your VPC
- C. You can only operate VPC's in only one mode at a time , either IPv4 or IPv6 ✔
- D. The default IP addressing for Amazon VPC and Amazon EC2 is IPv4

Explanation :

Answer - C
The AWS documentation mentions the following
If you have an existing VPC that supports IPv4 only, and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resources. Your VPC can operate in dual-stack mode — your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other.
You cannot disable IPv4 support for your VPC and subnets; this is the default IP addressing system for Amazon VPC and Amazon EC2.
For more information on VPC and IP addressing , please visit the below URL:

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

Ask our Experts

QUESTION 36 UNATTEMPTED

Which of the below services can be used to protect your web applications from common web exploits

- A. AWS Config
- B. AWS WAF ✔
- C. AWS Cloudtrail
- D. AWS SQS

Explanation :

Answer – B
The AWS documentation mentions the following
AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns. Also, AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of web security rules.
For more information on the Web application firewall , please visit the below URL:

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

Ask our Experts

QUESTION 37 UNATTEMPTED

There is a requirement to get the IP address and port of the backend instances which serve traffic sent via an AWS ELB. How can this be achieved.

- **A.** Check the VPC Flow Logs
- **B.** Check Cloudwatch metrics
- **C.** Check the ELB Console. The data is present in the log section.
- **D.** Enable ELB Access logs. Check the logs ✔

Explanation :

Answer – D
The AWS documentation mentions the following
Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.
For more information on the ELB Log files , please visit the below URL:

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

Ask our Experts

QUESTION 38 UNATTEMPTED

You have created a number of VPC's in a region. You are trying to create a 6th VPC, but are not able to do so. What could be the underlying issue?

- A. There is a limit of 5 VPC's per region. Submit a request to get the limit increased. ✔
- B. The region does no support creating of VPC's
- C. There is a already a VPC with the same name already defined
- D. There is already a VPC present with the same CIDR block range

Explanation :

Answer - A
The AWS documentation specifies this limitation

Resource	Default limit	Comments
VPCs per region	5	To increase this limit, submit a request. The limit for internet gateways per region is directly correlated to this one. Increasing this limit increases the limit on internet gateways per region by the same amount.

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

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

Ask our Experts

QUESTION 39 UNATTEMPTED

What are the 2 separate charges for AWS Direct Connect?

- [ ] **A.** VPC's in the region
- [ ] **B.** port-hours ✔
- [ ] **C.** Data transfer ✔
- [ ] **D.** Subnets in VPC

Explanation :

Answer – B and C
The AWS documentation mentions the following
AWS Direct Connect has two separate charges: port-hours and Data Transfer. Pricing is per port-hour consumed for each port type. Partial port-hours consumed are billed as full hours.
For more information on the AWS Direct Connect , please visit the below URL:

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

Ask our Experts

QUESTION 40 UNATTEMPTED

You are under a DDoS attack and you have added a deny all TCP rule to your NACL, but traffic is still coming. What could be the underlying issue?

- A. You configured the rule number to be too low.
- B. You need to add a deny rule outbound to the NACL
- C. A NACL can't protect against a DDos attacks
- D. The DDoS isn't a TCP attack ✔

Explanation :

Answer D
There are different types of DDos attacks, it can also be a UDP attack.
For more information on the types of DDos attacks , please refer to the below link:

- https://www.incapsula.com/ddos/ddos-attacks/ (https://www.incapsula.com/ddos/ddos-attacks/)

Ask our Experts

QUESTION 41 UNATTEMPTED

Which of the following are traffic types which are not captured by VPC flow logs. Choose 3 answers from the options given below

- [ ] A. DHCP traffic ✔
- [ ] B. IP traffic going to and from network interfaces
- [ ] C. Traffic to and from 169.254.169.254 ✔
- [ ] D. Traffic generated by instances when they contact the Amazon DNS server ✔

Explanation :

Answer – A, C and D

The AWS documentation mentions the following on the types of traffic not captured by VPC flow logs
1. Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
2. Traffic generated by a Windows instance for Amazon Windows license activation.
3. Traffic to and from 169.254.169.254 for instance metadata.
4. DHCP traffic.
5. Traffic to the reserved IP address for the default VPC router
For more information on VPC flow logs captured traffic , please refer to the below link:

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

Ask our Experts

QUESTION 42 UNATTEMPTED

Your company needs an inexpensive solution to host their AD data in the cloud. They do not need all of the features of AD but do need to be able to use it with WorkSpaces. What is the best solution from the below that can be used

- **A.** Deploy an AD server on an M3.large instance
- **B.** Use the Hosted Microsoft AD solution
- **C.** Use the Simple AD solution ✔
- **D.** Consider using the AD Connector

Explanation :

Answer – C
Simple AD is the least expensive with the required feature set to work with AWS Workspaces
Amazon WorkSpaces uses directories to store and manage information for your WorkSpaces and users. For your directory, you can choose from Simple AD, AD Connector, or AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as Microsoft AD. In addition, you can establish a trust relationship between your Microsoft AD directory and your on-premises domain.
For more information on Workspaces and Simple AD , please refer to the below link:

- http://docs.aws.amazon.com/workspaces/latest/adminguide/launch-workspace-simple-ad.html (http://docs.aws.amazon.com/workspaces/latest/adminguide/launch-workspace-simple-ad.html)

Ask our Experts

QUESTION 43 UNATTEMPTED

Which of the following are valid VPC CIDR's? Choose 2 answers from the options given below

- [ ] **A.** 10.0.0.0/24 ✔
- [ ] **B.** 10.0.0.0/29
- [ ] **C.** 20.0.0.0/10
- [ ] **D.** 20.0.0.0/27 ✔

Explanation :

Answer – A and D
The AWS documentation mentions the following
When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)
For more information on VPC Sizing , please refer to the below link:

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

Ask our Experts

QUESTION 44 UNATTEMPTED

Which of the below is not an option in the DHCP options set

- A. domain-name-servers
- B. domain-name
- C. IP-Range ✔
- D. ntp-servers

Explanation :

Answer - C
The following are the supported options
1. domain-name-servers
2. domain-name
3. ntp-servers
4. netbios-name-servers
5. netbios-node-type

For more information on DHCP Options set , please refer to the below link:

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

Ask our Experts

QUESTION 45 UNATTEMPTED

You have a static VPN connecting your data center and your VPC. You currently have 50 routes added to your route table. You want to add more, which of the following you would do to achieve this.

- [ ] A. Convert your VPN to a dynamic VPN ✔
- [ ] B. Consider using BGP ✔
- [ ] C. Increase the number of Route tables

☐ **D.** Increase the number of VPC's

Explanation :

Answer – A and B
A dynamic routing table can support 100 routes. A static can only support 50 per IPv4 and 50 per IPv6.
For more information on VPC and VPN , please refer to the below link:

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

Ask our Experts

QUESTION 46 UNATTEMPTED

If a VPN in AWS is created via the VPC wizard , what is the default value of the ASN assigned for the connection

- ○ **A.** 64000
- ○ **B.** 65000 ✔
- ○ **C.** 66000
- ○ **D.** 67000

Explanation :

Answer - B
This is given in the AWS documentation

(Dynamic routing only) Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the customer gateway.	You can use an existing ASN assigned to your network. If you don't have one, you can use a private ASN (in the 64512–65534 range). If you use the VPC wizard in the console to set up your VPC, we automatically use 65000 as the ASN.

For more information on VPC and VPN , please refer to the below link:

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

Ask our Experts

QUESTION 47 UNATTEMPTED

Which of the following is the valid IPv6 address which covers all addresses

- **A.** 0.0.0.0.0.0.0.0
- **B.** ::/0 ✔
- **C.** 0.0.0.0
- **D.** 0.0.0.0:/0

Explanation :

Answer - B
::/0 – The default route address (corresponding to 0.0.0.0/0 in IPv4) covering all addresses (unicast, multicast and others).
For more information on IPv6 addressing , please refer to the below link:

- https://en.wikipedia.org/wiki/IPv6_address (https://en.wikipedia.org/wiki/IPv6_address)

Ask our Experts

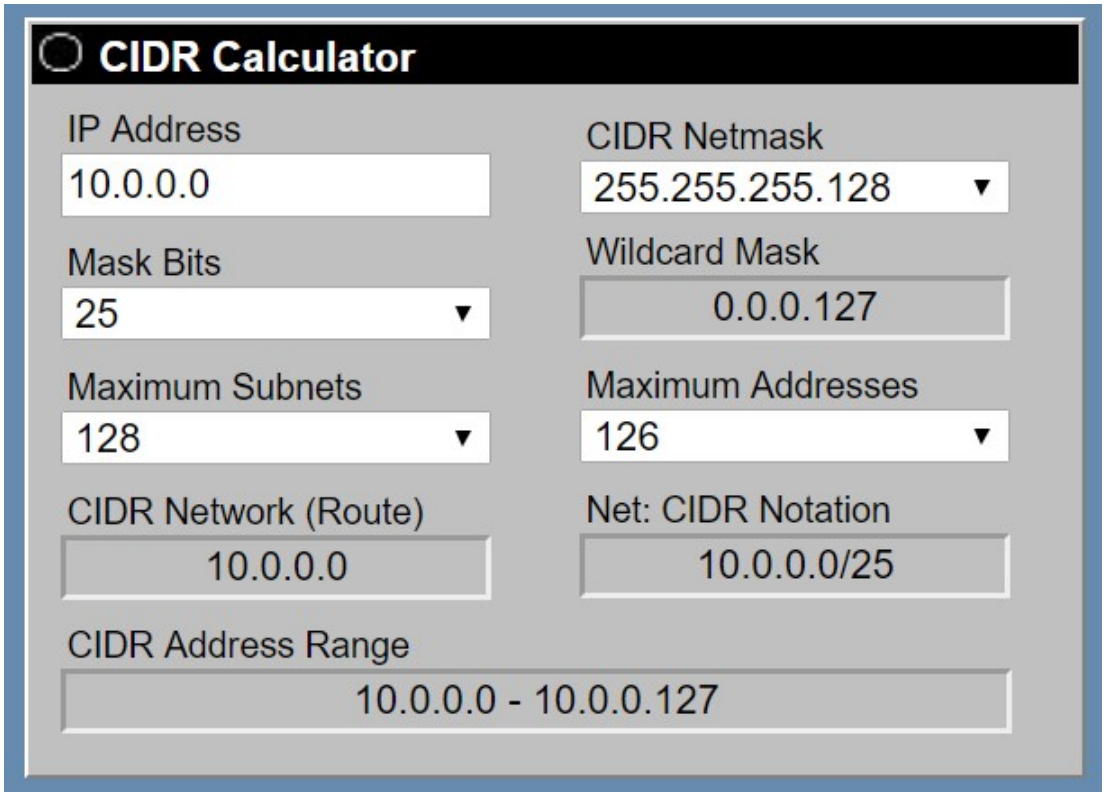
QUESTION 48 UNATTEMPTED

For the given network , 10.0.0.0/25 , what is the first and last address (network and broadcast)?

- **A.** 10.0.0.0 and 10.0.0.127 ✔
- **B.** 10.0.0.0 and 10.0.0.128
- **C.** 10.0.0.1 and 10.0.0.255
- **D.** 10.0.0.0 and 10.0.0.255

Explanation :

Answer – A
This can be determined using the CIDR calculator



Reference the below link for the CIDR calculator

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

Ask our Experts

QUESTION 49 UNATTEMPTED

You have 3 VPCs: VPC-A (10.0.0.0/16), VPC-B (10.1.0.0/16) and VPC-C (10.1.0.0/16). How can you ensure that VPC-A can communicate with the other VPC's. Choose 2 answers from the options below with each answer forming part of the solution

- [ ] **A.** Create a VPC peering relationship between VPC-A and VPC-B and between VPC-A and VPC-C ✔
- [ ] **B.** Create a VPC peering relationship between VPC-A and VPC-B and between VPC-B and VPC-C

- [ ] **C.** Ensure the route tables are modified with the new peering connections ✔
- [ ] **D.** This cannot be done because of the overlapping CIDR blocks

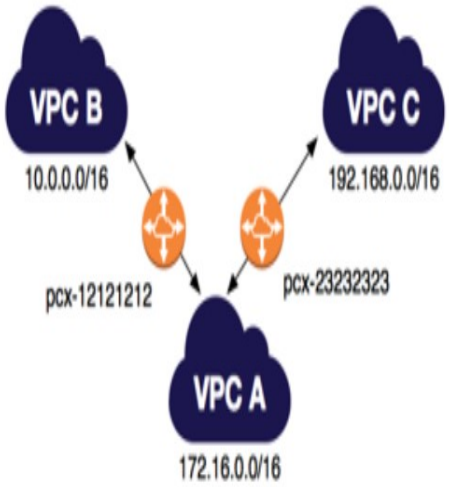
Explanation :

Answer – A and C
You can access the following link to see the configuration between 3 VPC's

- http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html#one-to-two-vpcs-full-access (http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html#one-to-two-vpcs-full-access)

One VPC Peered with Two VPCs

You have a central VPC (VPC A), and you have a VPC peering connection between VPC A and VPC B (pcx-12121212), and between VPC A and VPC C (pcx-23232323). The VPCs are in the same AWS account, and do not have overlapping CIDR blocks.



Ask our Experts

QUESTION 50 UNATTEMPTED

You need to ensure that a subnet can get requests from all destinations. Which of the following would you use in the route table?

- A. 255.255.255.255/32
- B. 255.255.255.255/0
- C. 0.0.0.0/0 ✔
- D. 0.0.0.0/32

Explanation :

Answer – C
This is the default route. For more information on the default route , please refer to the below link:

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

Ask our Experts

QUESTION 51 UNATTEMPTED

Which of the following can directly serve as authentication services for Amazon Workspaces? Choose 3 answers from the options given below

- A. AD Connector ✔
- B. Microsoft AD hosted on AWS ✔
- C. Simple AD ✔
- D. DirectConnect

Explanation :

Answer – A,B and C

The AWS documentation mentions the following
Amazon WorkSpaces uses a directory to store and manage information for your WorkSpaces and users. You can use one of the following options:

- AD Connector — Use your existing on-premises Microsoft Active Directory. Users can sign into their WorkSpaces using their on-premises credentials and access on-premises resources from their WorkSpaces.
- Microsoft AD — Create a Microsoft Active Directory hosted on AWS.
- Simple AD — Create a directory that is compatible with Microsoft Active Directory, powered by Samba 4, and hosted on AWS.
- Cross trust — Create a trust relationship between your Microsoft AD directory and your on-premises domain.

For more information on AWS Workspaces and Active Directory, please visit the below link:

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

Ask our Experts

QUESTION 52 UNATTEMPTED

Which of the following port numbers are used by the HTTPS protocol

- A. 80
- B. 22
- C. 23
- D. 443 ✔

Explanation :

Answer - D
HTTPS URLs begin with "https://" and use port 443 by default, whereas HTTP URLs begin with "http://" and use port 80 by default.
For more information on the HTTPs protocol, please visit the below link:

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

Ask our Experts

QUESTION 53 UNATTEMPTED

Which of the following port numbers have to be open for AWS workspaces to function properly. Choose 3 answers from the options below

- [ ] **A.** Port 443 ✔
- [ ] **B.** Port 22
- [ ] **C.** Port 53 ✔
- [ ] **D.** Port 80 ✔

Explanation :

Answer – A ,C and D
The following major ports need to be open for AWS Workspaces
1. Port 443 (TCP) - This port is used for client application updates, registration, and authentication. The desktop client applications support the use of a proxy server for port 443 (HTTPS) traffic.

2. Port 53 (UDP) - This port is used to access DNS servers
3. Port 80 (UDP and TCP) - This port is used for initial connections to http://clients/amazonworkspaces.com, which then switch to HTTPS
For more information on the port requirements, please visit the below link:

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

Ask our Experts

QUESTION 54 UNATTEMPTED

Which of the following is not an attribute associated with the Elastic Network Interface

- A. NACL ✔
- B. Security Groups
- C. MAC address
- D. source/destination check flag

Explanation :

Answer - A
A network interface can include the following attributes:

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

For more information on the Elastic Network Interface, please visit the below link:

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

Ask our Experts

QUESTION 55 UNATTEMPTED

Which of the following protocols are supported for AWS VPN connections

- **A.** IPSec ✔
- **B.** OpenSSL
- **C.** AES
- **D.** DES

Explanation :

Answer - A
The AWS documentation mentions the following
Although the term *VPN connection* is a general term, in the Amazon VPC documentation, a VPN connection refers to the connection between your VPC and your own network. AWS supports Internet Protocol security (IPsec) VPN connections.
For more information on VPN connections, please visit the below link:

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

Ask our Experts

QUESTION 56 UNATTEMPTED

When configuring a virtual interface with Direct Connect , which of the following is false when it comes to the configuration of BGP with the virtual interface

- **A.** If a public ASN is being used , then it must be ensured that you own the ASN.
- **B.** If a private ASN is used , it must be in the 64512 to 65535 range
- **C.** A BGP session needs to have a public or private ASN number at the customer side.
- **D.** Autonomous System (AS) prepending can work even if you use a private ASN for a public virtual interface. ✔

Explanation :

Answer - D
The AWS documentation mentions the following
A virtual interface must have a public or private Border Gateway Protocol (BGP) Autonomous System Number (ASN) for your side of the BGP session. If you are using a public ASN, you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range. Autonomous System (AS) prepending does not work if you use a private ASN for a public virtual interface. You can provide your own MD5 BGP authentication key, or you can let Amazon generate one for you.
For more information on Virtual interfaces, please visit the below link:

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

Ask our Experts

QUESTION 57 UNATTEMPTED

How many DHCP options set can be assigned to a VPC at a time. Choose an answer from the options given below

- **A.** 1 ✔
- **B.** 2
- **C.** 4
- **D.** 8

Explanation :

Answer – A
This is given in the AWS documentation
You can have multiple sets of DHCP options, but you can associate only one set of DHCP options with a VPC at a time
For more information on DHCP Options set, please visit the below link:

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

Ask our Experts

QUESTION 58 UNATTEMPTED

What are the 2 types of MTU supported by Instances types in AWS? Choose 2 answers from the options given below

- [ ] **A.** 1500 ✔
- [ ] **B.** 2001
- [ ] **C.** 5001
- [ ] **D.** 9001 ✔

Explanation :

Answer – A and D
This is given in the AWS documentation
All Amazon EC2 instance types support 1500 MTU, and many current instance sizes support 9001 MTU, or jumbo frames.
For more information on Network MTU, please visit the below link:

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

Ask our Experts

QUESTION 59 UNATTEMPTED

Which of the following is the container for resource records in Route53

- A. Domain Name
- B. Name Server
- C. Hosted Zone ✔
- D. Delegation Set

Explanation :

Answer - C
This is given in the AWS documentation
A container for resource record sets, which include information about how you want to route traffic for a domain (such as example.com) and all of its subdomains (such as www.example.com, retail.example.com, and seattle.accounting.example.com). A hosted zone has the same name as the corresponding domain
For more information on the concepts of Route53 , please visit the below link:

- http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/route-53-concepts.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/route-53-concepts.html)

Ask our Experts

QUESTION 60 UNATTEMPTED

If you wanted to have network speeds of upto 25 Gbps for supported instance types, which of the following would you consider using?

- A. Intel 82599 Virtual Function (VF) interface
- B. Route propagation
- C. Elastic Network Adapter ✔
- D. VPC Peering

Explanation :

Answer – C

This is given in the AWS documentation
The Elastic Network Adapter (ENA) supports network speeds of up to 25 Gbps for supported instance types.
For more information on Enhanced Networking , please visit the below link:

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

Ask our Experts

QUESTION 61 UNATTEMPTED

How many public IP addresses can be assigned to an Elastic Network interface? Choose one answer from the options given below

- A. 1 ✔
- B. 2
- C. 4
- D. 5

Explanation :

Answer – A
A network interface can include the following attributes:

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

For more information on the Elastic Network Interface, please visit the below link:

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

Ask our Experts

QUESTION 62 UNATTEMPTED

You have a requirement to create a subnet which will have the ability to host 512 addresses. Which of the below network masks would you use to ensure that the ability to host this many IP addresses is as accurate as possible

- A. /21
- B. /22 ✔
- C. /23
- D. /24

Explanation :

Answer – B
If you have the subnet mask of /23, you will have exactly 512 hosts; out of this 5 IPs are not available to use, because those are reserved IPs. So, you will end up with 507 hosts which is not meeting our requirement.
Hence, the correct answer would be option B.
The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

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

10.0.0.3: Reserved by AWS for future use.
10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.
Please check the below link to know more about it:

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

Ask our Experts

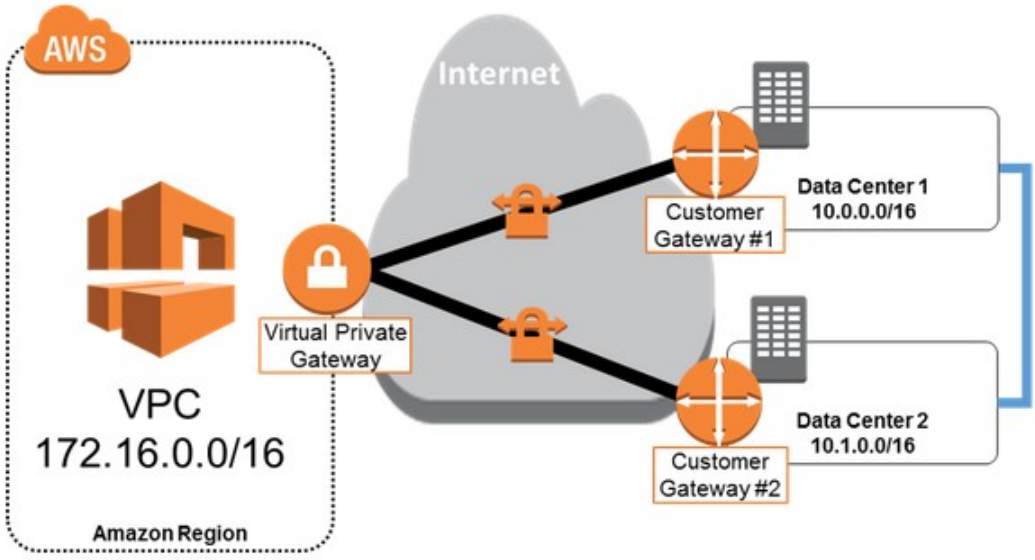
QUESTION 63 UNATTEMPTED

Your company has a data center on-premise. They want to establish a VPN connection to AWS. But they also want the connection to be highly available. Which of the below options can fulfil this requirement. Choose 2 answers from the options below. Each option presents part of the option.

- [ ] **A.** Create 2 customer gateways. ✔
- [ ] **B.** Create 2 Virtual private gateways
- [ ] **C.** Create a Virtual private gateway ✔
- [ ] **D.** Create a customer gateway

Explanation :

Answer – A and C
The below diagram shows a high available architecture for AWS VPN connections.



For more information on High Availability of VPN connections , please refer to the below link:

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

Ask our Experts

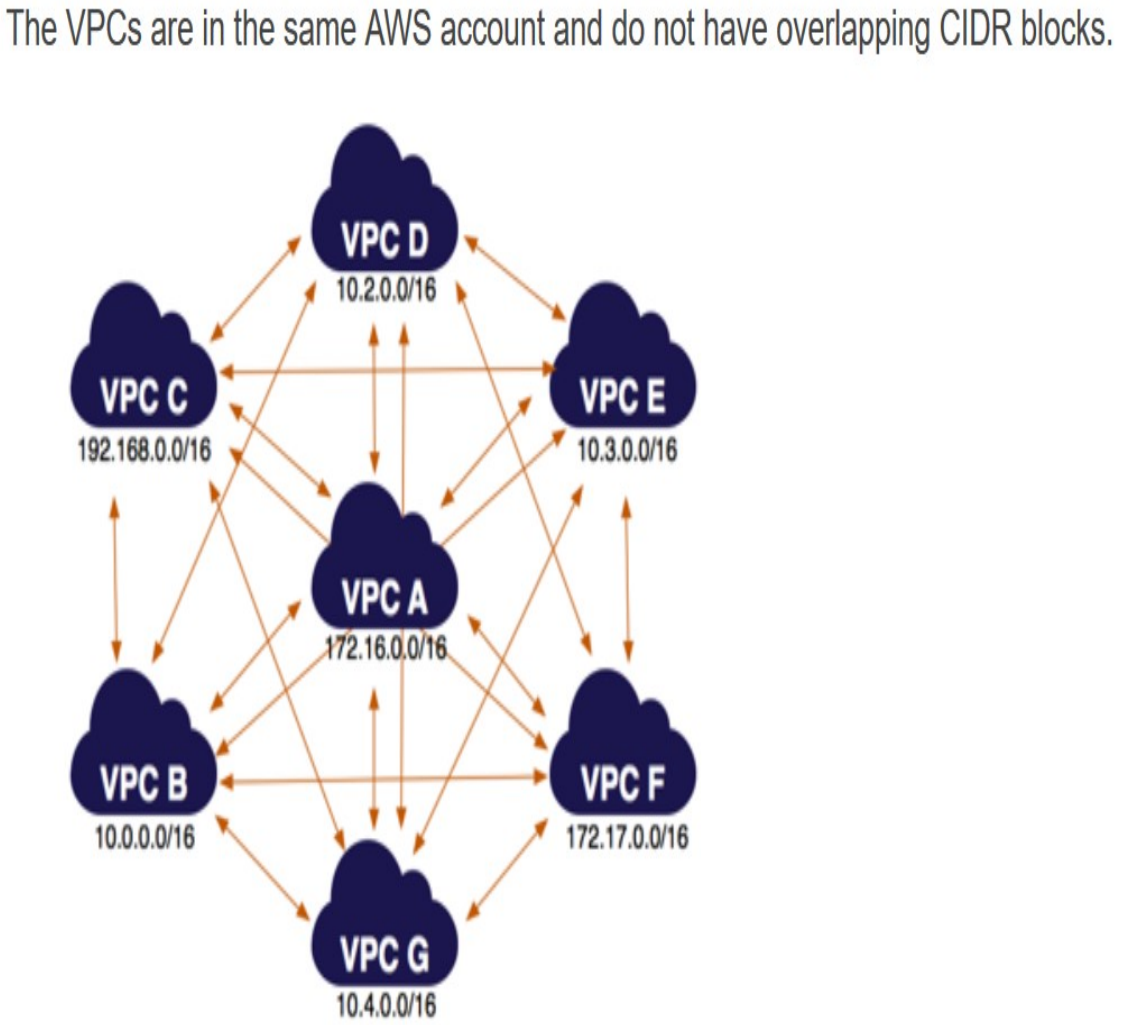
QUESTION 64 UNATTEMPTED

You have 5 VPC's in AWS. There is a file sharing server in 2 VPC's. There is a need for this file sharing service to be available across the other VPC's. How can this be accomplished. Choose 2 answers from the options below. Each answer forms part of the solution.

- ☐ **A.** Create Instances with Enhanced networking to share the files across
- ☐ **B.** Create a full mesh configuration of VPC Peering with the VPC's ✔
- ☐ **C.** Modify the Route tables of each VPC with the peering configuration ✔
- ☐ **D.** Modify the VPC configuration of each VPC with the peering configuration

Explanation :

Answer – B and C
The below diagram from the AWS documentation shows the full mesh configuration of multiple VPC's



For more information on VPC Peering for multiple VPC's , please refer to the below link:
http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html#many-vpcs-full-access
(http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html#many-vpcs-full-access)

Ask our Experts

QUESTION 65 UNATTEMPTED

What are the pre-requisites for using the AD connector which is available in AWS? Choose 3 answers from the options below

- [ ] **A.** There should be at least 2 subnets in the VPC with each in a different Availability Zone. ✔
- [ ] **B.** The VPC must be connected to your on-premises network ✔
- [ ] **C.** The VPC must have shared tenancy
- [ ] **D.** The VPC must have default hardware tenancy ✔

Explanation :

Answer – A,B and D
The AWS documentation mentions this clearly
Set up a VPC with the following:

- At least two subnets. Each of the subnets must be in a different Availability Zone.
- The VPC must be connected to your on-premises network through a virtual private network (VPN) connection or AWS Direct Connect.
- The VPC must have default hardware tenancy.

For more information on the pre-requisites for AD connector , please refer to the below link:

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

Ask our Experts

QUESTION 66 UNATTEMPTED

You want to monitor any changes to the network configuration of the VPC's and subnets in AWS. Which of the below services can help accomplish this. Choose 3 answers from the options given below

- [x] **A.** AWS Cloudtrail ✔
- [x] **B.** AWS Cloudwatch Logs ✔
- [x] **C.** AWS Config ✔
- [ ] **D.** AWS Direct Connect

Explanation :

Answer – A,B and C
The AWS documentation mentions the following
AWS CloudTrail provides a history of AWS API calls for an account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). This AWS API call history enables security analysis, resource change tracking, and compliance auditing. Customers can also deliver CloudTrail data to CloudWatch Logs to store, monitor, and process API calls for network-specific changes and to send appropriate notifications
AWS Config creates an AWS network resource inventory, including configuration history and configuration change notification
For more information on Networking monitoring in AWS , please refer to the below link:

- https://aws.amazon.com/answers/networking/vpc-network-management-and-monitoring/ (https://aws.amazon.com/answers/networking/vpc-network-management-and-monitoring/)

Ask our Experts

QUESTION 67 UNATTEMPTED

Which of the following is false with regards to AWS Load Balancers

- ○ **A.** The nodes of an Internet-facing load balancer have private IP addresses ✔
- ○ **B.** The DNS name of an Internet-facing load balancer is publicly resolvable to the public IP addresses of the nodes

- C. The nodes of an internal load balancer have only private IP addresses
- D. The nodes of an internal load balancer have only private IP addresses

Explanation :

Answer - A
The AWS Documentation mentions the following
The nodes of an Internet-facing load balancer have public IP addresses. The DNS name of an Internet-facing load balancer is publicly resolvable to the public IP addresses of the nodes. Therefore, Internet-facing load balancers can route requests from clients over the Internet
The nodes of an internal load balancer have only private IP addresses. The DNS name of an internal load balancer is publicly resolvable to the private IP addresses of the nodes. Therefore, internal load balancers can only route requests from clients with access to the VPC for the load balancer.
For more information on Load Balancers , please refer to the below link:

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

Ask our Experts

QUESTION 68 UNATTEMPTED

You want to get the list of IP addresses of the Edge Server locations for Cloudfront. How can you get this easily?

- A. Check the Cloudfront Console.
- B. Use the Cloudfront API to query the IP addresses.
- C. Download the ip-ranges.json file available from AWS. ✔
- D. Contact AWS

Explanation :

Answer – C
Amazon Web Services (AWS) publishes its current IP address ranges in JSON format. To view the

current ranges, download ip-ranges.json

- https://ip-ranges.amazonaws.com/ip-ranges.json (https://ip-ranges.amazonaws.com/ip-ranges.json)

For more information on location of Edge servers , please refer to the below link:

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

Ask our Experts

QUESTION 69 UNATTEMPTED

What is the current limit on the data transfer per distribution in Cloudfront?

- **A.** 40 Gbps ✔
- **B.** 100 Gbps
- **C.** 200 Gbps
- **D.** 500 Gbps

Explanation :

Answer - A
This is given in the AWS documentation

General Limits

Entity	Limit
Data transfer rate per distribution	40 Gbps Request a higher limit

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

- http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cloudfront-limits.html#limits-general (http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cloudfront-limits.html#limits-general)

Ask our Experts

QUESTION 70 UNATTEMPTED

Which AWS service is best suited to work on its own to help mitigate a large scale global DDOS attack?

- A. AWS ELB
- B. AWS Cloudfront ✔
- C. AWS SQS
- D. AWS EC2

Explanation :

Answer – B
The AWS documentation mentions the following

Amazon CloudFront distributes traffic across multiple Points of Presence (PoP) locations and filters requests to ensure that only valid HTTP(S) requests will be forwarded to backend hosts. CloudFront also supports geo restriction, also known as *geoblocking*, which can be useful for isolating attacks originating from a particular geographic location
For more information on DDos attack mitigation , please refer to the below link:

- https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/ (https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/)

Ask our Experts

QUESTION 71 UNATTEMPTED

Which of following assists in setting a Active/Passive Direct Connect connection to AWS?

- **A.** Use VPC Peering
- **B.** Use a Virtual private gateway
- **C.** Use Route Propagation
- **D.** Use AS_PATH prepending ✔

Explanation :

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

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

Ask our Experts

QUESTION 72 UNATTEMPTED

Which of the following can be used for outbound communication over IPv6 from instances in your VPC to the Internet

- A. Egress only Internet gateway ✔
- B. Customer gateway
- C. Virtual Private Gateway
- D. Virtual Private connection

Explanation :

Answer – A
The AWS documentation mentions the following
An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet, and prevents the Internet from initiating an IPv6 connection with your instances.
For more information on Egress only Internet gateways , please refer to the below link:

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

Ask our Experts

QUESTION 73 UNATTEMPTED

Which of the following is the Elastic IP a property of?

- A. Elastic Network Interface ✔
- B. Subnet

C. CloudTrail

D. MAC Address

Explanation :

Answer - A
The AWS documentation mentions the following
An Elastic IP address is a property of network interfaces. You can associate an Elastic IP address with an instance by updating the network interface attached to the instance.
For more information on Elastic IP's, please refer to the below link:

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

Ask our Experts

QUESTION 74 UNATTEMPTED

What is the default CIDR range provided for the default VPC's setup in AWS?

A. 10.0.0.0/16

B. 172.31.0.0/16 ✔

C. 20.0.0.0/16

D. 192.168.0.0/16

Explanation :

Answer – B
This is mentioned in the AWS documentation
Default VPCs are assigned a CIDR range of 172.31.0.0/16. Default subnets within a default VPC are assigned /20 netblocks within the VPC CIDR range.
For more information on VPC's, please refer to the below link:

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

Ask our Experts

QUESTION 75 UNATTEMPTED

What is the fixed size allocated to a VPC for IPv6 CIDR blocks?

- A. /64
- B. /56 ✔
- C. /40
- D. /32

Explanation :

Answer - B
This is mentioned in the AWS documentation
For IPv6, the VPC is a fixed size of /56 (in CIDR notation). A VPC can have both IPv4 and IPv6 CIDR blocks associated to it.
For more information on VPC's, please refer to the below link:

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

Ask our Experts

QUESTION 76 UNATTEMPTED

What is the minimum size of a subnet that can be present in a VPC in AWS?

- A. /30

- B. /29
- C. /28 ✔
- D. /27

Explanation :

Answer - C
This is mentioned in the AWS documentation
The minimum size of a subnet is a /28
For more information on VPC's, please refer to the below link:

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

Ask our Experts

QUESTION 77 UNATTEMPTED

Which of the below mentioned options is the best option to avoid SQL Injection attacks against your infrastructure in aws?

- A. Create a DirectConnect connection so that your have a dedicated connection line.
- B. Create NACL rules for the subnet hosting the application.
- C. Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group ✔
- D. Remove all but TLS 1 & 2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

Explanation :

Answer – C
AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns.
For more information on WAF, please visit the below URL:

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

Ask our Experts

QUESTION 78 UNATTEMPTED

Which of the below mentioned methods is the best to stop a series of attacks coming from a set of determined IP ranges?

- **A.** Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)
- **B.** Create web Security Group rules to block the attacking IP addresses over port 80
- **C.** Put the application on the private subnet.
- **D.** Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses ✔

Explanation :

Answer – D
A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC
For more information on NACL please visit the below URL:

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

Ask our Experts

QUESTION 79 UNATTEMPTED

A company currently has an on-premise location connecting to a VPC. The company wants to have a dedicated network connection from the on-premise location to the VPC? Choose the correct answer from the options below which would help fulfil the above requirement

- **A.** Provision a VPN connection between the on-premise data center and the AWS region using the VPN section of a VPC.
- **B.** Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region. ✔
- **C.** Use a hardware VPN to connect both locations.
- **D.** Use a software VPN to connect both locations.

Explanation :

Answer – B
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
For more information on aws direct connect, just browse to the below URL:

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

Ask our Experts

QUESTION 80 UNATTEMPTED

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?

- A. It will throw a CIDR overlap error ✔
- B. It is not possible to create a subnet with the same CIDR as the VPC
- C. The second subnet will be created
- D. The VPC will modify the first subnet to allow this IP range

Explanation :

Answer - A
Since the CIDR overlaps for the first the second subnet, an overlap error will occur
For more information on VPC subnets, please refer to the below link:

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

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14621)

- PM Certification (https://www.whizlabs.com/project-management-certifications/)
- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

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)