PRACTICE TEST II

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

Completed on	Sunday , 03 February 2019 , 11:06 PM
Time Taken	00 H 00 M 57 S
Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	80	0	2	78

80 Questions	**0** Correct	**2** Incorrect	**78** Unattempted

Show Answers

All

QUESTION 1 INCORRECT

When implementing AWS Cloudhub for multiple VPN connections which of the following statements about the implementation is false

○ **A.** AWS Cloudhub can be used to provide secure communication between sites ✖

- **B.** You need to create a virtual private gateway on the AWS side
- **C.** You need to create a single customer gateway at the main site ✔
- **D.** You need to use the Border gateway protocol

Explanation :

Answer - C
The AWS documentation mentions the following
If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub.
To use the AWS VPN CloudHub, you must create a virtual private gateway with multiple customer gateways. You must use a unique Border Gateway Protocol (BGP) Autonomous System Number (ASN) for each customer gateway. Customer gateways advertise the appropriate routes (BGP prefixes) over their VPN connections.
For more information on AWS VPN Cloudhub , please refer to the below link:

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

Ask our Experts

QUESTION 2 UNATTEMPTED

There is a request from the networking team in your organization to create the below VPC in AWS

172.168.128.128/28

How many subnets would be allowed with this configuration?

- **A.** 1 ✔
- **B.** 16
- **C.** 20
- **D.** 24

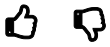
Explanation :

Answer – A
Smallest allowable CIDR range for a VPC is /28 so it cannot be subnetted any further.
With a AWS VPC would result in only 1 Subnet and 11 available hosts (16 - 5 reserved)

For more details, Please check the following AWS Docs

- 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 3 UNATTEMPTED

As per the TCP/IP model, which layer makes use of the core protocols of Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP)

- A. Session Layer
- B. Transport Layer ✔
- C. Network Layer
- D. Data-Link Layer

Explanation :

Answer - B
The Transport layer (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).
For more information on the TCP IP Model, one can visit the below URL:

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

Ask our Experts

QUESTION 4 UNATTEMPTED

What is the term given to the largest permissible packet that can be passed over a network connection?

- A. Maximum network unit
- B. Maximum connection unit
- C. Maximum received unit
- D. Maximum transmission unit ✔

Explanation :

Answer – D
The AWS documentation mentions the following on MTU
The maximum transmission unit (MTU) of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data that can be passed in a single packet. Ethernet packets consist of the frame, or the actual data you are sending, and the network overhead information that surrounds it.
For more information on MTU , one can visit the below URL:

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

Ask our Experts

QUESTION 5 UNATTEMPTED

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

- A. Autonomous System numbers ✔
- B. Internet System numbers

- C. Autonomous System locators
- D. Internet System locators

Explanation :

Answer - A
Autonomous System numbers are used to identify networks that present a clearly defined external routing policy to the Internet. AWS Direct Connect requires an ASN to create a public or private virtual interface. You may use a public ASN which you own, or you can pick any private ASN number between 64512 to 65535 range.
For more information on Autonomous System numbers, one can visit the below URL:

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

Ask our Experts

QUESTION 6 UNATTEMPTED

Which of the following attributes allow for instances launched in a VPC to receive a DNS hostname and ensure that DNS resolution is possible via Amazon DNS. Choose 2 answers from the options given below

- [ ] A. enableDnsHostnames ✔
- [ ] B. setDnsHostnames
- [ ] C. enableDnsSupport ✔
- [ ] D. enableDnsresolution

Explanation :

Answer - A and C
Your VPC has attributes that determine whether your instance receives public DNS hostnames, and whether DNS resolution through the Amazon DNS server is supported.
1. enableDnsHostnames - Indicates whether the instances launched in the VPC get public DNS hostnames.
2. enableDnsSupport - Indicates whether the DNS resolution is supported for the VPC.

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

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

Ask our Experts

QUESTION 7 UNATTEMPTED

You are the network administrator for a company. Your company currently has resources on-premise and in AWS. There is a requirement to create a VPN connection between AWS and the on-premise infrastructure. But there is also a compliance requirement that the connections should be managed by the company on both sides of the connection. Which of the below 2 options would suffice this requirement

- [ ] **A.** Create a customer gateway on the on-premise location ✔
- [ ] **B.** Use Direct Connect as the connectivity option
- [ ] **C.** Use a software VPN appliance in your VPC ✔
- [ ] **D.** Use the amazon virtual private interface

Explanation :

Answer – A and C
The AWS documentation mentions the following
Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network. This option is recommended if you must manage both ends of the VPN connection either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPC's
For more information on such networking options, one can visit the below URL:

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

Ask our Experts

QUESTION 8 UNATTEMPTED

You are the network administrator for a company. There is a requirement to connect VPC's which are located in different regions. Which of the following option cannot be used for connectivity

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

Explanation :

Answer - A
#Note: Question Outdated now. We have cross region VPC peering for specific regions now.
We are working on updating this question.
https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/ (https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/)

Ask our Experts

QUESTION 9 UNATTEMPTED

When connecting multiple VPCs in different AWS Regions which of the below is not a best principle to consider

- A. Ensure that your VPC network ranges (CIDR blocks) do not overlap.
- B. You should try to connect all VPC's is possible. ✔
- C. Ensure you implement a highly available (HA) design

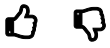
- **D.** Use network equipment that supports IPsec VPN tunnels and Border Gateway Protocol

Explanation :

Answer - B
The AWS documentation mentions the following
When connecting multiple VPCs in different AWS Regions, there are some universal network-design principles to consider:
1. Ensure that your VPC network ranges (CIDR blocks) do not overlap.
Make sure the solution you choose is able to scale according to your current and future VPC connectivity needs.
2. Ensure you implement a highly available (HA) design with no single point of failure.
3. Consider your data-transfer needs, as this will affect the solution you choose. Some solutions proposed below may prove to be more expensive than others based on the amount of data transferred.
4. Use network equipment that supports IPsec VPN tunnels and Border Gateway Protocol (BGP), when applicable.
5. Connect only those VPCs that really need to communicate with each other.
For more information on VPC connectivity across regions, one can visit the below URL:

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

Ask our Experts



QUESTION 10 UNATTEMPTED

You currently have 2 instances (c4.large) in a VPC. You plan to create a placement group because now there is a requirement for better network communication between the instances. You are planning to move the already created instances to this placement group. But you encounter an issue. Which of the below could be a legitimate issue

- **A.** The Instance type of the instances are not supported in the placement group.
- **B.** You can't have Linux Instances in a placement group
- **C.** You can't move an existing instance into a placement group ✔

- **D.** You can't have Instances with EBS volumes in a placement group

Explanation :

Answer - C
The AWS documentation mentions the following
You can't move an existing instance into a placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group.
For more information on placement groups, one can visit the below URL:

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

Ask our Experts

QUESTION 11 UNATTEMPTED

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

- **A.** You can assign a secondary private IPv4 address to any network interface.
- **B.** You can assign multiple IPv6 addresses to a network interface that's in a subnet that has an associated IPv6 CIDR block.
- **C.** Multiple IP addresses can be only be assigned to network interfaces on stopped instances. ✔
- **D.** Security groups apply to network interfaces, not to IP addresses. Therefore, IP addresses are subject to the security group of the network interface in which they're specified.

Explanation :

Answer – C
Multiple IP addresses can be assigned and unassigned to network interfaces attached to running or stopped instances.
The AWS documentation mentions the following
1. You can assign a secondary private IPv4 address to any network interface. The network interface can be attached to or detached from the instance.
2. You can assign multiple IPv6 addresses to a network interface that's in a subnet that has an

associated IPv6 CIDR block.
3. You must choose the secondary IPv4 from the IPv4 CIDR block range of the subnet for the network interface.
4. Security groups apply to network interfaces, not to IP addresses
For more information on IP addressing, one can visit the below URL:

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

Ask our Experts

QUESTION 12 UNATTEMPTED

You had an Elastic IP address associated with an instance that was running for a period of 3 months. Now you have disassociated the Elastic IP address. But you can see that you are still being charged for the Elastic IP address. What can you do to ensure that you don't get charged for the Elastic IP address? Choose 2 answers from the options given below

- [ ] **A.** Explicitly release the Elastic IP from your account. ✔
- [ ] **B.** Quickly associate it with any stopped instance
- [ ] **C.** Quickly associate it with any running instance ✔
- [ ] **D.** Associate it with an un-attached network interface

Explanation :

Answer - A and C
The AWS documentation mentions the following
A disassociated Elastic IP address remains allocated to your account until you explicitly release it.
To ensure efficient use of Elastic IP addresses, we impose a small hourly charge if an Elastic IP address is not associated with a running instance, or if it is associated with a stopped instance or an unattached network interface. While your instance is running, you are not charged for one Elastic IP address associated with the instance, but you are charged for any additional Elastic IP addresses associated with the instance.
For more information on Elastic IP's , one can visit the below URL:

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

Ask our Experts

QUESTION 13 UNATTEMPTED

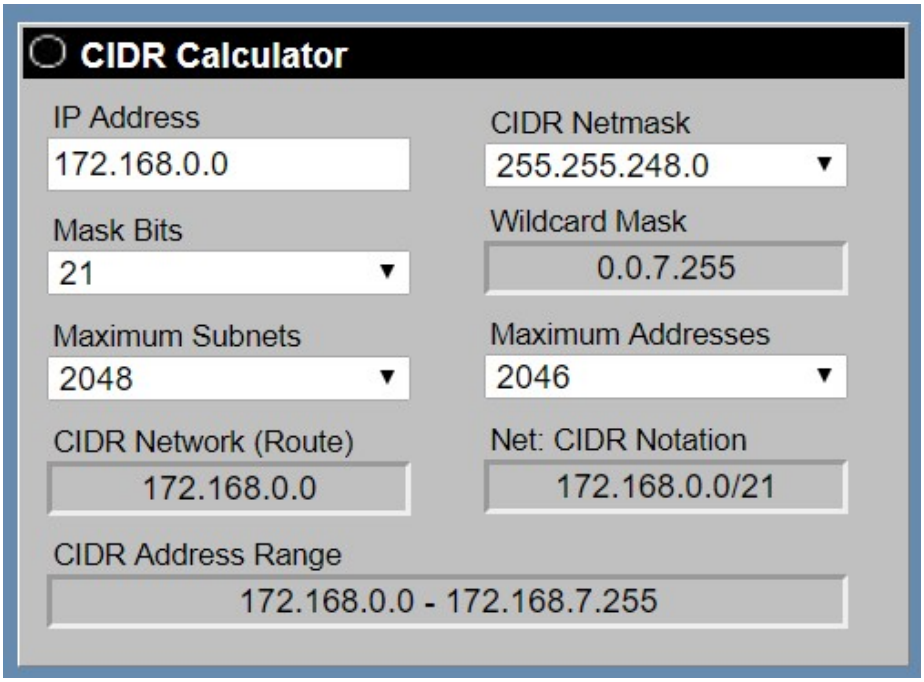
You have a requirement to create a subnet which will have the ability to host 2000 addresses. Which of the below network masks would you use to ensure that the ability to host this many IP addresses is as accurate as possible

- A. /21 ✔
- B. /22
- C. /23
- D. /24

Explanation :

Answer – A

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



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

Ask our Experts

QUESTION 14 UNATTEMPTED

The IPSec protocol is used to end-to-end security of data in which of the following layers of the Internet protocol suite

- A. Application Layer
- B. Transport Layer
- C. Internet layer ✔
- D. Link Layer

Explanation :

Answer - C
IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at the Transport Layer (TLS) and the Application layer (SSH). IPsec can automatically secure applications at the IP layer.
For more information on the IPSec protocol , one can visit the below URL:

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

Ask our Experts

QUESTION 15 UNATTEMPTED

You have 2 VPC's VPCA(172.16.0.0/16) and VPCB(10.0.0.0/16). You are planning on establishing VPC connecting peering. Which of the following routes need to be added to the route table for both VPC's to ensure communication across VPC's. Choose 2 answers from the options given below. Assume that the Target for the VPC Peering connection has an ID of pcx-1122

- [ ] **A.** In the Route table for VPCA add a route of 172.16.0.0/16 and Target as pcx-1122
- [ ] **B.** In the Route table for VPCA add a route of 10.0.0.0/16 and Target as pcx-1122 ✔
- [ ] **C.** In the Route table for VPCB add a route of 172.16.0.0/16 and Target as pcx-1122 ✔
- [ ] **D.** In the Route table for VPCB add a route of 10.0.0.0/16 and Target as pcx-1122

Explanation :

Answer - B and C
An example is given on the AWS documentation on this as per the snapshots below. And this also gives the Route table configurations

Two VPCs Peered Together

You have a VPC peering connection (`pcx-11112222`) between VPC A and VPC B, which are in the same AWS account, and do not have overlapping CIDR blocks.

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

Route table	Destination	Target
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-11112222
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-11112222

For more information on this example , one can visit the below URL:

- http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html (http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html)

Ask our Experts

QUESTION 16 UNATTEMPTED

You currently have setup a VPC and subnets in AWS. You have setup routes in the route table for traffic on the CIDR block of 0.0.0.0/0. You just want to establish communication across all hosts. But you notice that some applications are not working as desired. These are Ipv6 based applications that are sitting across subnets in the VPC. What must be done to alleviate this issue?

- **A.** Ensure that the route of 0.0.0.0/0 is removed and a more specific route is placed.
- **B.** Remove the route of 0.0.0.0/0 and add the route of ::/0 instead to allow all communication.
- **C.** Add a route for ::/0 to the route table as well. ✔
- **D.** Add the default route of 172.132.0.0/16 to the Route table

Explanation :

Answer - C
CIDR blocks for IPv4 and IPv6 are treated separately. For example, a route with a destination CIDR of 0.0.0.0/0 (all IPv4 addresses) does not automatically include all IPv6 addresses. You must create a route with a destination CIDR of ::/0 for all IPv6 addresses.
For more information on Route propagation , one can visit the below URL:

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

Ask our Experts

QUESTION 17 UNATTEMPTED

Which of the following can be used to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different regions

- A. AWS Direct Connect connector
- B. AWS Direct Connect replicator
- C. AWS Direct Connect interface
- D. AWS Direct Connect gateway ✔

Explanation :

Answer – D
The AWS documentation mentions the following
You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different regions. You associate a Direct Connect gateway with the virtual private gateway for the VPC, and then create a private virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. You can attach multiple private virtual interfaces to your Direct Connect gateway.
For more information on Direct Connect gateways , one can visit the below URL:

- http://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways.html (http://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways.html)

Ask our Experts

QUESTION 18 UNATTEMPTED

Which of the following is not a type of subnet that you can host in a VPC

- A. Public
- B. Private
- C. Direct Connect only ✔

D. VPN-only

Explanation :

Answer - C
The following types of subnets can be configured
1. Public Subnet - In order to set up a public subnet, you have to configure its routing table so that traffic from that subnet to the Internet is routed through an Internet gateway associated with the VPC
2. Private Subnets - For private subnets, traffic to the Internet can be routed through a special network address translation (NAT) instance
3. VPN-only - By attaching a virtual private gateway to your VPC, you can create a VPN connection between your VPC and your own data center
For more information on extending VPC's , one can visit the below URL:

- https://d0.awsstatic.com/whitepapers/extend-your-it-infrastructure-with-amazon-vpc.pdf (https://d0.awsstatic.com/whitepapers/extend-your-it-infrastructure-with-amazon-vpc.pdf)

Ask our Experts

QUESTION 19 UNATTEMPTED

Your company has the following Direct Connect and VPN Connections

Site A - VPN 10.1.0.0/28 AS 65000 65000

Site B - VPN 10.1.0.252/24 AS 65000

Site C - Direct Connect 10.0.0.0/8 AS 65000

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

Which site will AWS choose to reach your network?

A. Site A ✔

B. Site B

C. Site C

D. Site D

Explanation :

Answer – A
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 A.
For more information on route table priority, please visit the below URL:

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

Ask our Experts

QUESTION 20 UNATTEMPTED

Which of the following can help to create dual-homed instances with workloads/roles on distinct subnets

- **A.** Multiple EBS Volumes
- **B.** Multiple VPC's
- **C.** Multiple network interfaces ✔
- **D.** Multiple S3 buckets

Explanation :

Answer – C
The AWS documentation mentions the following
Attaching multiple network interfaces to an instance is useful when you want to:

- Create a management network.
- Use network and security appliances in your VPC.
- Create dual-homed instances with workloads/roles on distinct subnets.
- Create a low-budget, high-availability solution.

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

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

Ask our Experts

QUESTION 21 UNATTEMPTED

When automating the creation of a network using cloudformation , which of the following types would normally be assigned a property of a private IP address?

- A. AWS::EC2::Subnet
- B. AWS::EC2::NetworkInterface ✔
- C. AWS::EC2::VPC
- D. AWS::EC2::SubnetCidrBlock

Explanation :

Answer - B

This would be the network interface. An example is given below

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Description" : "Simple Standalone ENI",
  "Resources" : {
      "myENI" : {
          "Type" : "AWS::EC2::NetworkInterface",
          "Properties" : {
          "Tags": [{"Key":"foo","Value":"bar"}],
          "Description": "A nice description.",
          "SourceDestCheck": "false",
          "GroupSet": ["sg-75zzz219"],
          "SubnetId": "subnet-3z648z53",
          "PrivateIpAddress": "10.0.0.16"
      }
    }
  }
}
```

For more information on the AWS::EC2::NetworkInterface type, please visit the below URL:

- http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-network-interface.html

(http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-network-interface.html)

Ask our Experts

QUESTION 22 UNATTEMPTED

Which of the following is not part of the logs which can be achieved from the requests made to Route53

- A. The client IP address ✔
- B. Domain that was requested
- C. The DNS record type
- D. DNS Response code

Explanation :

Answer - A
The AWS documentation mentions the following
You can configure Amazon Route53 to log information about the queries that Amazon Route 53 receives, such as the following:

- The domain or subdomain that was requested
- The date and time of the request
- The DNS record type (such as A or AAAA)
- The Amazon Route 53 edge location that responded to the DNS query
- The DNS response code, such as NoError or ServFail

For more information on Route53 logging, please visit the below URL:

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

Ask our Experts

QUESTION 23 UNATTEMPTED

Which of the following records are automatically created when you create a hosted zone in Route53. Choose 2 answers from the options given below

- [ ] **A.** AAA
- [ ] **B.** Name Server ✔
- [ ] **C.** SOA ✔
- [ ] **D.** CNAME

Explanation :

Answer - B and C
When you create a hosted zone, Amazon Route 53 automatically creates four name server (NS) records and a start of authority (SOA) record for the zone
For more information on DNS migration to Route53, please visit the below URL:

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

Ask our Experts

QUESTION 24 UNATTEMPTED

Which of the following allows for Simple AD to resolve names using both DNS servers within your VPC and private DNS servers outside of your VPC

- ○ **A.** DNSName Resolution
- ○ **B.** DNSNameSet
- ○ **C.** DHCP options set ✔
- ○ **D.** Route53

Explanation :

Answer - C
If you want your Simple AD to resolve names using both DNS servers within your VPC and private DNS servers outside of your VPC, you can do this using a DHCP options set
For more information on DNS with Simple AD please visit the below URL:

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

Ask our Experts

QUESTION 25 UNATTEMPTED

Which of the following services allows you to run Microsoft Active Directory (AD) as a managed service

- A. Simple AD
- B. AD Connector
- C. AWS Directory Service ✔
- D. Amazon Cloud directory

Explanation :

Answer - C
The AWS documentation mentions the following
AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. AWS Directory Service for Microsoft Active Directory, also referred to as Microsoft AD, is powered by Windows Server 2012 R2. When you select and launch this directory type, it is created as a highly available pair of domain controllers connected to your virtual private cloud (VPC). The domain controllers run in different Availability Zones in a region of your choice. Host monitoring and recovery, data replication, snapshots, and software updates are automatically configured and managed for you.
For more information on the AWS Directory Service please visit the below URL:

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

Ask our Experts

QUESTION 26 UNATTEMPTED

You are planning to setup a load balancing solution in AWS. There is a requirement for using HTTPS for the back end instances and using path based routing. Which of the below types of load balancers should be used for this purpose

- A. Classic Load balancer
- B. Application Load balancer ✔
- C. Network Load balancer
- D. Secondary Load balancer

Explanation :

Answer - B
Some of the key points of the Application Load balancer over the classic load balancer is
1. Support for path-based routing. You can configure rules for your listener that forward requests based on the URL in the request. This enables you to structure your application as smaller services, and route requests to the correct service based on the content of the URL.
2. Support for host-based routing. You can configure rules for your listener that forward requests based on the host field in the HTTP header. This enables you to route requests to multiple domains using a single load balancer.
For more information on load balancing solutions please visit the below URL:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html)

Ask our Experts

QUESTION 27 UNATTEMPTED

You have an application hosted on an EC2 Instance. To distribute content you are planning to use the Content Delivery service. Before going to production there is a requirement to perform a load test. Which of the following should be considered when conducting a load test which involves the CDN service. Choose 3 answers from the options given below

- [ ] **A.** Send client requests from multiple geographic regions. ✔
- [ ] **B.** Configure your test so each client makes an independent DNS request ✔
- [ ] **C.** Ensure that the request goes to the first IP returned by the DNS
- [ ] **D.** spread your client requests across the set of IP addresses that are returned by DNS ✔

Explanation :

Answer - A,B and D
The following should be considered
· Send client requests from multiple geographic regions.
· Configure your test so each client makes an independent DNS request; each client will then receive a different set of IP addresses from DNS.
· For each client that is making requests, spread your client requests across the set of IP addresses that are returned by DNS, which ensures that the load is distributed across multiple servers in a CloudFront edge location.
For more information on load testing the CDN service please visit the below URL:

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

Ask our Experts

QUESTION 28 UNATTEMPTED

Which of the following is recommended to use when accessing AWS resources from EC2 Instances

- ○ **A.** Use the root access keys

- **B.** Define an IAM user and use the access keys attached to the user
- **C.** Consider implementing IAM Roles ✔
- **D.** Segregate IAM users into groups

Explanation :

Answer - C
IAM roles and temporary security credentials address these use cases. An IAM role lets you define a set of permissions to access the resources that a user or service needs, but the permissions are not attached to a specific IAM user or group. Instead, IAM users, mobile and EC2-based applications, or AWS services (like Amazon EC2) can programmatically assume a role
For more information on IAM Roles please visit the below URL:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)

Ask our Experts

QUESTION 29 UNATTEMPTED

Which of the below mentioned ways can be used to provide additional layers of protection to all your EC2 resources. Choose the correct answer from the options below

- **A.** Add policies which have deny and/or allow permissions on tagged resources
- **B.** Ensure that the proper tagging strategies have been implemented to identify all of your EC2 resources.
- **C.** Add an IP address condition to policies that specify that requests to EC2 instances should come from a specific IP address or CIDR block range.
- **D.** All actions listed here would provide additional layers of protection. ✔

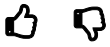
Explanation :

Answer – D

Option B is correct because tagging can allow one to understand which resources below to test, development and production environment if done properly.Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define Option A is right because it adds on top on that. If you have tagging, you can then also allow permissions based on the tagging.
For more information on tagging please see the below link:

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

Ask our Experts



QUESTION 30 UNATTEMPTED

An auditor needs read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS. What is the best way for creating this sort of access? Choose the correct answer from the options below

- **A.** One should contact AWS as part of the shared responsibility model, and AWS will grant required access.
- **B.** Create a role that has the required permissions.
- **C.** Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs. ✔
- **D.** Create an SNS notification that sends the CloudTrail log files.

Explanation :

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

For more information on Cloudtrail please see the below link:

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

Ask our Experts

QUESTION 31 UNATTEMPTED

When BGP is used for routing within an autonomous system which of the below annotation is this normally referred to

- A. pBGP
- B. iBGP ✔
- C. eBGP
- D. sBGP

Explanation :

Answer - B
BGP may be used for routing within an autonomous system. In this application it is referred to as Interior Border Gateway Protocol, Internal BGP, or iBGP. In contrast, the Internet application of the protocol may be referred to as Exterior Border Gateway Protocol, External BGP, or eBGP
For more information on the Border gateway protocol please see the below link:

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

Ask our Experts

QUESTION 32 UNATTEMPTED

Which of the following statements is false when it comes to AWS Direct Connect

- A. It is a private connection that is separate from the internet
- B. It can help have a consistent network performance
- C. Each connection can be used across multiple AWS regions ✔
- D. Both the 1-gigabit or 10-gigabit speed options are available

Explanation :

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

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

Ask our Experts

QUESTION 33 UNATTEMPTED

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

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

Explanation :

Answer - A
The AWS documentation mentions the following
A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple 1 gigabit or 10 gigabit connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.
You can associate an existing connection with a LAG. The connection can be standalone, or it can be part of another LAG. The connection must be on the same AWS device and must use the same bandwidth as the LAG. If the connection is already associated with another LAG, you cannot re-associate it if removing the connection causes the original LAG to fall below its threshold for minimum number of operational connections.
For more information on link aggregation group please see the below link:

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

Ask our Experts

QUESTION 34 UNATTEMPTED

Which of the following is not an ideal design recommendation of encrypting data in transit in AWS

- A. Limit the number of public subnets
- B. Route egress traffic through a NAT instance
- C. When using ELB terminate the TLS connection at the back end instances ✔
- D. Ensure that security groups and NACLs are configured to address the requirements of the PCI DSS.

Explanation :

Answer - C
The following design recommendations from the AWS documentation is present for encrypting data in transit
1. Limit the number of public subnets. Public subnets within Amazon VPC are similar to the demilitarized zone (DMZ) referred to in the PCI DSS.

2. Route egress traffic to the Internet through a network address translation (NAT) located in the public subnet and deploy all other hosts in private subnets.
3. Enable source/destination checks at the instance level to provide additional safeguards around isolation of network traffic.
4. Ensure that security groups and NACLs are configured to address the requirements of the PCI DSS.
5. Consider terminating the TLS connections at the front-end ELB layer or the WAF layer in the public subnet of Amazon VPC, and configuring non-TLS connections for traffic between private subnets.
For more information on this please see the below link:

- https://aws.amazon.com/blogs/security/how-to-address-the-pci-dss-requirements-for-data-encryption-in-transit-using-amazon-vpc/ (https://aws.amazon.com/blogs/security/how-to-address-the-pci-dss-requirements-for-data-encryption-in-transit-using-amazon-vpc/)

Ask our Experts

QUESTION 35 UNATTEMPTED

You are trying to connect to your instance from the internet and get an error message Network error: Connection timed out or Error connecting to [instance], reason: -> Connection timed out: connect.

Which of the below are valid checkpoints to diagnose the error. Choose 2 answers from the options given below

- ☐ **A.** Check the Inbound Security Group Rules ✔
- ☐ **B.** Check the route table for the VPC ✔
- ☐ **C.** Check if a private IP address has been assigned to the instance
- ☐ **D.** Check if the instance has been assigned a private DNS name

Explanation :

Answer - A and B
The AWS documentation mentions the following for troubleshooting EC2 Instance connectivity
1. Check your security group rules. You need a security group rule that allows inbound traffic from your public IPv4 address on the proper port.
2. Check the route table for the subnet. You need a route that sends all traffic destined outside the

VPC to the internet gateway for the VPC.
For more information on troubleshooting EC2 Instances please see the below link:

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

Ask our Experts

QUESTION 36 UNATTEMPTED

You have a web server hosted on an EC2 Instance. The subnet hosting the EC2 Instance has the following NACL attached

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	HTTP (80)	TCP (6)	80	10.1.0.0/16	ALLOW
101	HTTPS (443)	TCP (6)	443	10.1.0.0/16	ALLOW
200	HTTP (80)	TCP (6)	80	0.0.0.0/0	DENY
201	HTTPS (443)	TCP (6)	443	0.0.0.0/0	DENY
1000	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

What happens when a request comes from the internet to the web server on port 80

- A. The request will be allowed because of Rule no 100 which matches the request ✔
- B. The request will be allowed because of Rule no 1000 which matches the request
- C. The request will be denied because of Rule no 200
- D. The request will be denied because of Rule no *

Explanation :

Answer – A

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

Hence when the request comes from the internet , Rule no 100 will match for the port 80 request.

As a packet comes to the subnet, we evaluate it against the ingress rules of the ACL the subnet is associated with (starting at the top of the list of rules, and moving to the bottom). Here's how the evaluation goes if the packet is destined for the SSL port (443). The packet doesn't match the first rule evaluated (rule 100). It does match the second rule (110), which allows the packet into the subnet. If the packet had been destined for port 139 (NetBIOS), it doesn't match any of the rules, and the * rule ultimately denies the packet.

You might want to add a DENY rule in a situation where you legitimately need to open a wide range of ports, but there are certain ports within that range you want to deny. Just make sure to place the DENY rule earlier in the table than the rule that allows the wide range of port traffic.

Inbound						
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**	**Comments**
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	SSH	TCP	22	192.0.2.0/24	ALLOW	Allows inbound SSH traffic from your home network's public IPv4 address range (over the Internet gateway).
130	RDP	TCP	3389	192.0.2.0/24	ALLOW	Allows inbound RDP traffic to the web servers from your home network's public IPv4 address range (over the Internet gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW	Allows inbound return IPv4 traffic from the Internet (that is, for requests that originate in the subnet).

Outbound						
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny	Comments
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows outbound IPv4 HTTP traffic from the subnet to the Internet.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows outbound IPv4 HTTPS traffic from the subnet to the Internet.
120	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW	Allows outbound IPv4 responses to clients on the Internet (for example, serving web pages to people visiting the web servers in the subnet). This range is an example only. For more information about how to select the appropriate ephemeral port range, see Ephemeral Ports.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable).

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

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

Ask our Experts

QUESTION 37 UNATTEMPTED

You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database. You want to confirm that they can talk to each other for your application to work properly. Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC? Choose 2 answers.

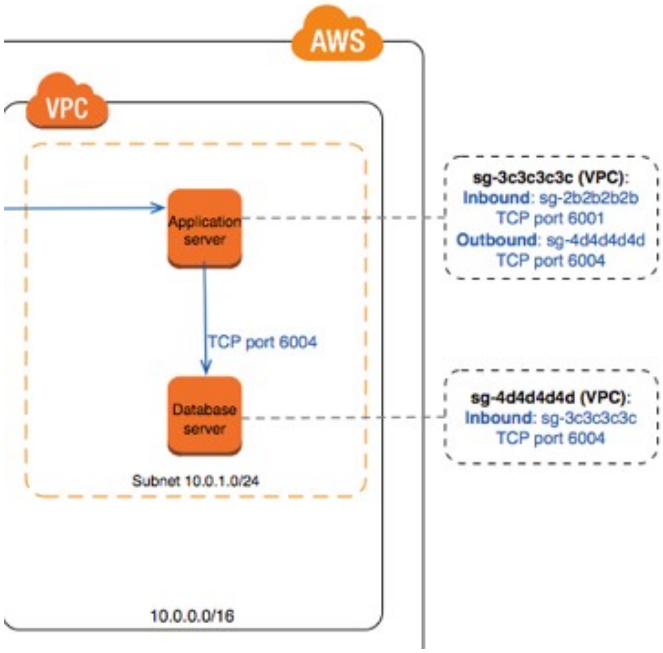
- ☐ **A.** A network ACL that allows communication between the two subnets. ✔
- ☐ **B.** Both instances are the same instance class and using the same Key-pair.

- [ ] **C.** That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.
- [ ] **D.** Security groups are set to allow the application host to talk to the database on the right port/protocol. ✔

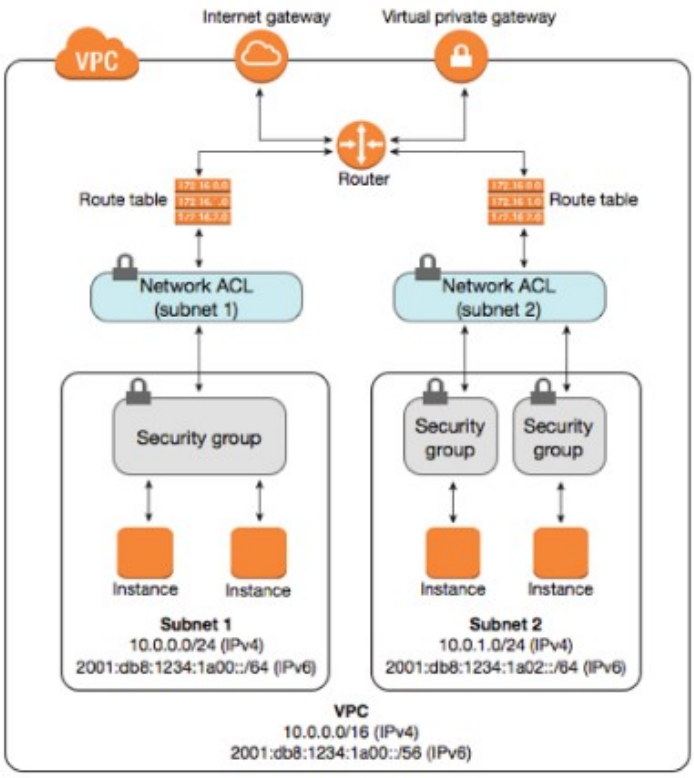
Explanation :

Answer - A and D

When you design a web server and database server, the security groups must be defined so that the web server can talk to the database server. An example image from the AWS documentation is given below



Also when communicating between subnets you need to have the NACL's defined



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

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

Ask our Experts

QUESTION 38 UNATTEMPTED

A company has setup a DirectConnect connection between their on-premise location and their AWS VPC. They want to setup redundancy incase the DirectConnect connection fails. What can they do in this regard? Choose all the options that apply

- [ ] **A.** Setup another DirectConnect connection ✔
- [ ] **B.** Setup an IPSec VPN Connection ✔
- [ ] **C.** Setup S3 connection

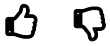
☐ **D.** Setup a connection via EC2 instances

Explanation :

Answer – A and B
This is clearly mentioned in the AWS FAQ's.
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. If you do not have a backup AWS Direct Connect link or a IPsec VPN link, then Amazon VPC traffic will be dropped in the event of a failure. Traffic to/from public resources will be routed over the Internet.
For more information on DirectConnect FAQ's , please visit the below URL:

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

Ask our Experts



QUESTION 39 UNATTEMPTED

A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25 and a private subnet with CIDR 20.0.0.128/25. The user has launched one instance each in the private and public subnets. Which of the below mentioned options cannot be the correct IP address (private IP. assigned to an instance in the public or private subnet?

○ **A.** 20.0.0.255 ✔

○ **B.** 20.0.0.132

○ **C.** 20.0.0.122

○ **D.** 20.0.0.55

Explanation :

Answer – A

As per the AWS documentation there is a reservation of IP addresses. Hence option A is right because this IP address will be reserved by AWS.
The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

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

For more information on IP Reservation, please visit the link:

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

Ask our Experts

QUESTION 40 UNATTEMPTED

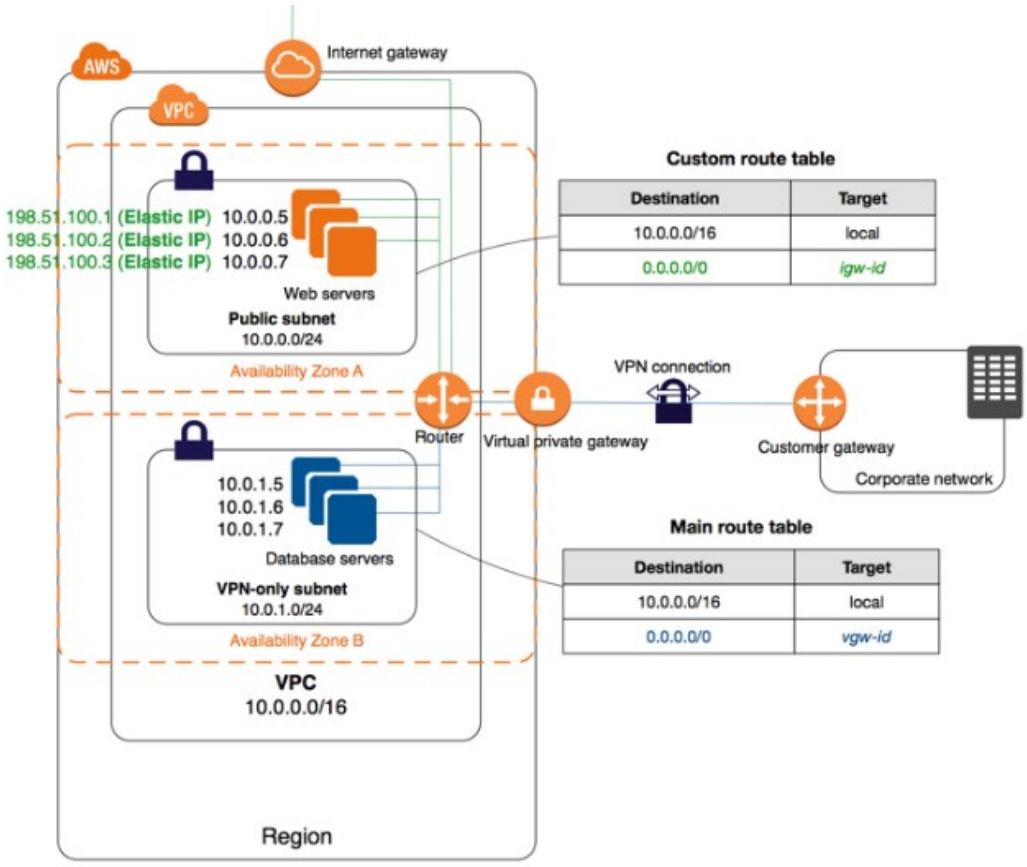
A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user's data centre. The user's data centre has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-123456) to allow traffic to the internet from the VPN subnet. Which of the below mentioned options is not a valid entry for the main route table in this scenario?

- A. Destination: 20.0.1.0/24 and Target: i-12345 ✔
- B. Destination: 0.0.0.0/0 and Target: i-12345
- C. Destination: 172.28.0.0/12 and Target: vgw-12345
- D. Destination: 20.0.0.0/16 and Target: local

Explanation :

Answer – A

The below diagram shows how a typical setup for a VPC with VPN and Internet gateway would look like. The only routing option which should have access to the internet gateway should be the 0.0.0.0/0 address. So Option A is the right answer.



For more information on VPC with the option of VPN, please visit the link:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html)

Ask our Experts

QUESTION 41 UNATTEMPTED

In order to ensure that alternate domains names can be used with your cloudfront distribution , which of the following must be done to ensure this works.

- A. Ensure the CNAME is created for the zone apex record.

- **B.** Ensure an AAA record is created along with the CNAME record.
- **C.** Ensure a reverse pointer record is created along with the CNAME record.
- **D.** Ensure that you own the domain name and create a CNAME record with the DNS service. ✔

Explanation :

Answer - D
The AWS documentation mentions the following
When you add an alternate domain name to a distribution, you need to create a CNAME record in your DNS configuration to route DNS queries for the domain name to your CloudFront distribution.
For more information on CNAME in Cloudfront, please visit the link:

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

Ask our Experts

QUESTION 42 UNATTEMPTED

Which of the following aspects of the AWS Config service is a collection of the configuration items for a given resource over any time

- **A.** Configuration Recorder
- **B.** Configuration History ✔
- **C.** Configuration Stream
- **D.** Configuration Snapshot

Explanation :

Answer - B
The AWS documentation mentions the following
A configuration history is a collection of the configuration items for a given resource over any time period. A configuration history can help you answer questions about, for example, when the resource was first created, how the resource has been configured over the last month, and what configuration changes were introduced yesterday at 9 AM. The configuration history is available to

you in multiple formats. AWS Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify. You can select a given resource in the AWS Config console and navigate to all previous configuration items for that resource using the timeline. Additionally, you can access the historical configuration items for a resource from the API.
For more information on the concepts of AWS config, please visit the link:

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

Ask our Experts

QUESTION 43 UNATTEMPTED

Which of the following request to Cloudfront will not the request directly back to the origin server?

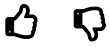
- A. GET ✔
- B. POST
- C. PUT
- D. OPTIONS

Explanation :

Answer – A
Apart from the GET method , the other methods will send the request directly back to the origin server. The GET request will first allow to poll the edge locations for content. Only of the content is not available , the request will be sent to the origin server to get the content.
For more information on the update HTTP requests for Cloudfront, please visit the link:

- https://aws.amazon.com/about-aws/whats-new/2013/10/15/amazon-cloudfront-now-supports-put-post-and-other-http-methods/ (https://aws.amazon.com/about-aws/whats-new/2013/10/15/amazon-cloudfront-now-supports-put-post-and-other-http-methods/)

Ask our Experts



QUESTION 44 UNATTEMPTED

Which of the following protocols are no longer supported for SSL on the classic load balancer?

- A. SSL 2.0 ✔
- B. SSL 3.0
- C. TLS 1.2
- D. TLS 1.1

Explanation :

Answer - A
The AWS documentation mentions the following on the protocols supported for the classic load balancer
The following versions of the SSL protocol are supported:

- TLS 1.2
- TLS 1.1
- TLS 1.0
- SSL 3.0

Deprecated SSL Protocol
If you previously enabled the SSL 2.0 protocol in a custom policy, we recommend that you update your security policy to the default predefined security policy.
For more information on the ELB security policy, please visit the link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-ssl-security-policy.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-ssl-security-policy.html)

Ask our Experts

QUESTION 45 UNATTEMPTED

What is the maximum allowable time available for connection draining on a class load balancer?

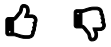
- A. 30 minutes
- B. 1 hour ✔
- C. 2 hours
- D. 5 hours

Explanation :

Answer - B
The AWS documentation mentions the following on the specifics of connection draining
When you enable connection draining, you can specify a maximum time for the load balancer to keep connections alive before reporting the instance as de-registered. The maximum timeout value can be set between 1 and 3,600 seconds (the default is 300 seconds). When the maximum time limit is reached, the load balancer forcibly closes connections to the de-registering instance.
For more information on the ELB connection draining, please visit the link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/config-conn-drain.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/config-conn-drain.html)

Ask our Experts



QUESTION 46 UNATTEMPTED

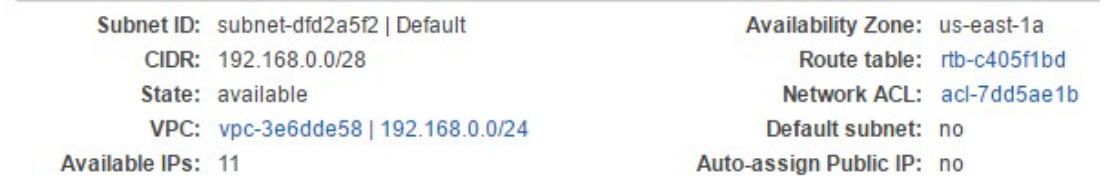
A user has created a subnet with VPC and launched an EC2 instance in that subnet with only default settings. Which of the below mentioned options is ready to use on the EC2 instance as soon as it is launched?

- A. Elastic IP
- B. Private IP ✔
- C. Public IP
- D. Internet gateway

Explanation :

Answer – B

When you create a subnet with the default settings, only the Private IP gets populated for EC2 instances. For Public IP, this is not possible because the Auto-assign Public IP will be 'no' by default. Also the Elastic IP and Internet gateway have to manually configured.



For more information on VPC, please visit the link:

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

Ask our Experts

QUESTION 47 UNATTEMPTED

A user has configured Elastic Load Balancing by enabling a Secure Socket Layer - SSL. Negotiation Configuration known as a Security Policy. Which of the below mentioned options is not part of this secure policy while negotiating the SSL connection between the user and the client?

- A. SSL Protocols
- B. Client Order Preference ✔
- C. SSL Ciphers
- D. Server Order Preference

Explanation :

Answer – B
If you see the AWS documentation for all possible SSL options in the below link you will see that SSL Protocols, SSL Ciphers and Server Order Preference are all part of the pre-defined policies. Only Client Order Preference is not present.

Security Policy	2016-08	2015-05	2015-03	2015-02	2014-10	2014-01	2011-08
SSL Protocols							
Protocol-SSLv3						♦	♦
Protocol-TLSv1	♦	♦	♦	♦	♦	♦	♦
Protocol-TLSv1.1	♦	♦	♦	♦	♦	♦	
Protocol-TLSv1.2	♦	♦	♦	♦	♦	♦	
SSL Options							
Server Order Preference	♦	♦	♦	♦	♦	♦	
SSL Ciphers							
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦	♦	

For more information on Secure ELB, please visit the link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-table.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-table.html)

Ask our Experts

QUESTION 48 UNATTEMPTED

A company is running a stateless web application with the following components

An Elastic Load Balancer.
4 Web/Application servers on EC2.
A MySQL RDS database with 2000 provisioned IOPS.
After observing the cloudwatch metrics , it is observed that the CPU of the web servers is reaching around 92% and the CPU of the database server is around 20%.
Which of the below 2 options can be used to alleviate the load on the entire infrastructure

- [ ] **A.** Create a read replica for the database
- [ ] **B.** Enable Multi-AZ for the database

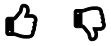
- [ ] **C.** Make use of Autoscaling and launch more Web/Application servers ✔
- [ ] **D.** Consider increasing the instance type of the Web/Application Servers ✔

Explanation :

Answer – C and D
Since the load on the Web/Application servers is high , it should be considered to make use of Autoscaling and increase the number of Web/Application servers or just increase the Instance type of the existing Web/Application servers
For more information on Autoscaling, please visit the link:

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

Ask our Experts



QUESTION 49 UNATTEMPTED

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

- [ ] **A.** Configuration Changes ✔
- [ ] **B.** Periodic ✔
- [ ] **C.** Templates
- [ ] **D.** Monitoring

Explanation :

Answer – A and B
1. Configuration Changes - AWS Config runs evaluations for the rule when certain types of resources are created, changed, or deleted.
2. Periodic - AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).
For more information on AWS config rules, please visit the link:

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

Ask our Experts

QUESTION 50 UNATTEMPTED

In Cloudtrail what is the component that marks the record of an activity in an AWS account?

- A. Cloudtrail workflow
- B. Cloudtrail Event ✔
- C. Cloudtrail logs
- D. Cloudtrail alarms

Explanation :

Answer - B
The AWS documentation mentions the following
An event in CloudTrail is the record of an activity in an AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. CloudTrail events provide a history of both API and non-API account activity made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
For more information on AWS Cloudtrail concepts, please visit the link:

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

Ask our Experts

QUESTION 51 UNATTEMPTED

You are managing the AWS account of a big organization. The organization has more than 1000+ employees and they want to provide access to the various services to most of the employees. Which of the below mentioned options is the best possible solution in this case?

- **A.** The user should create a separate IAM user for each employee and provide access to them as per the policy
- **B.** The user should create an IAM role and attach STS with the role. The user should attach that role to the EC2 instance and setup AWS authentication on that server
- **C.** The user should create IAM groups as per the organization's departments and add each user to the group for better access control
- **D.** Attach an IAM role with the organization's authentication service to authorize each user for various AWS services ✔

Explanation :

Answer – D
The best practise for IAM is to create roles which has specific access to an AWS service and then give the user permission to the AWS service via the role.
For the best practises on IAM policies, please visit the link:

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

Ask our Experts

QUESTION 52 UNATTEMPTED

A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25 and a private subnet with CIDR 20.0.0.128/25. The user has launched one instance each in the private and public subnets. Which of the below mentioned options cannot be the correct IP address (private IP. assigned to an instance in the public or private subnet?

- A. 20.0.0.255 ✔
- B. 20.0.0.132
- C. 20.0.0.122
- D. 20.0.0.55

Explanation :

Answer – A
As per the AWS documentation there is a reservation of IP addresses. Hence option A is right because this IP address will be reserved by AWS.
The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

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

For more information on IP Reservation, please visit the link:

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

Ask our Experts

QUESTION 53 UNATTEMPTED

A user has launched an EBS backed EC2 instance. The user has rebooted the instance. Which of the below mentioned statements is not true with respect to the reboot action?

- A. The private and public address remains the same
- B. The Elastic IP remains associated with the instance

- C. The volume is preserved
- D. The instance runs on a new host computer ✔

Explanation :

Answer – D
When you reboot your instance, as per the AWS documentation the following actions occur
An instance reboot is equivalent to an operating system reboot. In most cases, it takes only a few minutes to reboot your instance. When you reboot an instance, it remains on the same physical host, so your instance keeps its public DNS name (IPv4), private IPv4 address, IPv6 address (if applicable), and any data on its instance store volumes.
From the above explanation it is pretty straightforward to understand that Option D is the right option.
For more information on rebooting instance, please visit the link:

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

Ask our Experts

QUESTION 54 UNATTEMPTED

Which of the following is false when comparing using NAT instances vs NAT gateways?

- A. The bandwidth of NAT gateways supports bursts of up to 10Gbps and for NAT instances it depends on the Instance type
- B. The NAT gateways are managed by AWS
- C. You can associate security groups with both the NAT instances and NAT gateways ✔
- D. NAT gateways are highly available by default

Explanation :

Answer – C
The following are the key distinctions between NAT Instances and NAT gateways

NAT Gateways	NAT Instances
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.
Supports bursts of up to 10Gbps.	Depends on the bandwidth of the instance type.
Managed by AWS.You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.
Cannot be associated with a NAT gateway. You can associate security groups with your resources behind the NAT gateway to control inbound and outbound traffic.	Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic.

For more information on the comparison, please visit the link:

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

Ask our Experts

QUESTION 55 UNATTEMPTED

You currently have EC2 Instances in a private subnets. There are applications based on IPv6 which are hosted on these instances. You have configured NAT instances in a public subnet to ensure that applications hosted on the instances in the private subnet can download the required updates. But after configuring the instances , the applications are still not able to download the updates. Which of the following could be the underlying issue.

- **A.** The NAT instance should not be configured in the public subnet , it should be configured in the private subnet
- **B.** The NAT instance is not configured with a private IP address.
- **C.** NAT is not supported for IPv6 traffic ✔

D. The NAT instance is not configured with a private DNS name.

Explanation :

Answer - C
The AWS documentation mentions the following
NAT is not supported for IPv6 traffic—use an egress-only Internet gateway instead.
For more information on NAT Instances, please visit the link:

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

Ask our Experts

QUESTION 56 UNATTEMPTED

A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is not true in this scenario?

A. The VPC will create a routing instance and attach it with a public subnet ✔

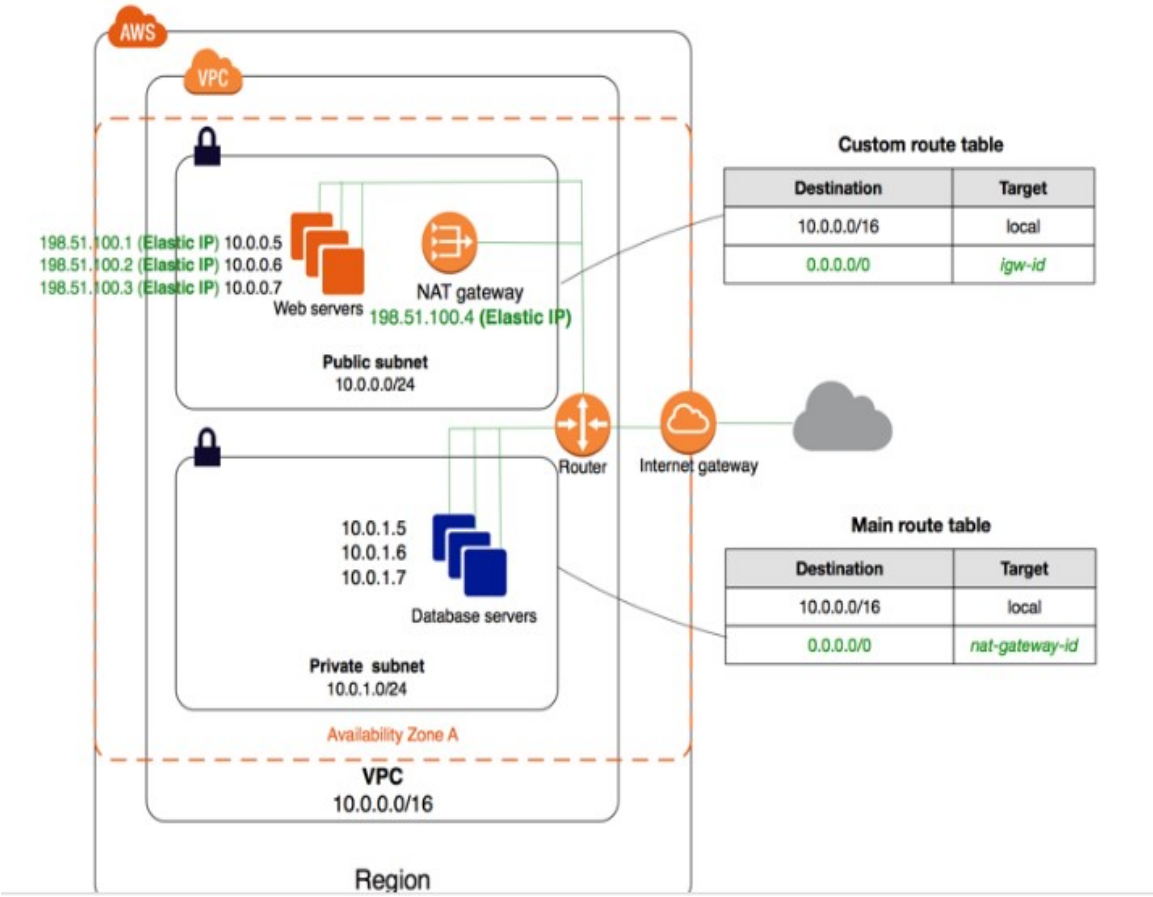
B. The VPC will create two subnets

C. The VPC will create one internet gateway and attach it to VPC

D. The VPC will launch one NAT instance with an elastic IP

Explanation :

Answer – A
Below is the general diagram of what is created when you have a private and public subnet used when using the VPC wizard. So you will get the below options
1) 2 subnets – one private and one public
2) One NAT instance to route traffic from the public to private subnet
3) One internet gateway attached to the VPC.



For more information on VPC and subnets , please visit the URL:

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

Ask our Experts

QUESTION 57 UNATTEMPTED

A user has created a subnet in VPC and launched an EC2 instance within it and is trying to access the instance through internet. The user has not selected the option to assign the IP address while launching the instance. Which of the below mentioned statements is true with respect to this scenario?

- A. The instance will always have a public DNS attached to the instance by default
- B. The user can directly attach an elastic IP to the instance
- C. The instance will never launch if the public IP is not assigned
- D. The user would need to create an internet gateway and then attach an elastic IP to the instance to connect from internet ✔

Explanation :

Answer – D
When you create a simple subnet and VPC , there is no internet gateway attached to the VPC. So to access it from the internet you need to ensure an Internet gateway is attached to the VPC and an elastic or public IP is assigned to the EC2 instance.
For more information on VPC and subnets , please visit the URL:

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

Ask our Experts

QUESTION 58 UNATTEMPTED

A user is trying to setup a security policy for ELB. The user wants ELB to meet the cipher supported by the client by configuring the server order preference in ELB security policy. Which of the below mentioned preconfigured policies supports this feature?

- A. ELBSecurity Policy-2014-01 ✔
- B. ELBSecurity Policy-2011-08
- C. ELBDefault Negotiation Policy
- D. ELBSample- OpenSSLDefault Cipher Policy

Explanation :

Answer – A
As per the AWS documentation the Server order preference is supported by the ELBSecurity Policy-2014-01 security policy.

Security Policy	2016-08	2015-05	2015-03	2015-02	2014-10	2014-01	2011-08
SSL Protocols							
Protocol-SSLv3						♦	♦
Protocol-TLSv1	♦	♦	♦	♦	♦	♦	♦
Protocol-TLSv1.1	♦	♦	♦	♦	♦	♦	
Protocol-TLSv1.2	♦	♦	♦	♦	♦	♦	
SSL Options							
Server Order Preference	♦	♦	♦	♦	♦	♦	

For more information on ELB security policies, please visit the link:

- http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-options.html (http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-options.html)

Ask our Experts

QUESTION 59 UNATTEMPTED

Due to a lot of your EC2 services going off line at least once a week for no apparent reason your security officer has told you that you need to tighten up the logging of all events that occur on your AWS account. He wants to be able to access all events that occur on the account across all regions quickly and in the simplest way possible. He also wants to make sure he is the only person that has access to these events in the most secure way possible. Which of the following would be the best solution to assure his requirements are met? Choose the correct answer from the options below

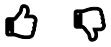
- **A.** Use CloudTrail to log all events to a separate S3 bucket in each region as CloudTrail cannot write to a bucket in a different region. Use MFA and bucket policies on all the different buckets.
- **B.** Use CloudTrail to send all API calls to CloudWatch and send an email to the security officer every time an API call is made. Make sure the emails are encrypted.
- **C.** Use CloudTrail to log all events to one S3 bucket. Make this S3 bucket only accessible by your security officer with a bucket policy that restricts access to his user only and also add MFA to the policy for a further level of security. ✔
- **D.** Use CloudTrail to log all events to an Amazon Glacier Vault. Make sure the vault access policy only grants access to the security officer's IP address.

Explanation :

Answer - C
Option B is invalid because you need Cloudtrail to monitor API calls and not send calls.
Option A is invalid because its not ideal to have different buckets for access to the one security officer. And you can have Cloudtrail deliver log calls to one S3 bucket.
Option D is wrong because Glacier is not the ideal option for retrieval for the security officier.
For more information on Cloudtrail please see the below link:

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

Ask our Experts



QUESTION 60 UNATTEMPTED

A company has placed a set of on-premise resources with an AWS Direct Connect provider. After establishing connections to a local AWS region in the US, the company needs to establish a low latency dedicated connection to an S3 public endpoint over the Direct Connect dedicated low latency connection. What steps need to be taken to accomplish configuring a direct connection to a public S3 endpoint? Choose the correct answer from the options below

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

Explanation :

Answer – C
You must create a virtual interface to begin using your AWS Direct Connect connection. You can create a public virtual interface to connect to public resources, or a private virtual interface to connect to your VPC. You can configure multiple virtual interfaces on a single AWS Direct Connect connection, and you'll need one private virtual interface for each VPC to connect to. Each virtual interface needs a VLAN ID, interface IP address, ASN, and BGP key.
For more information on virtual interfaces please see 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 61 UNATTEMPTED

Your company has a VPN connection between the on-premise data center and AWS. You need to monitor the VPN connection so that you can be notified whenever the connection was down. Which of the following steps would you take? Choose two answers from the options given below. Each answer forms part of the solution.

- A. Create a cloudwatch log

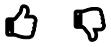
- [ ] **B.** Create a cloudwatch alarm that sends a notification whenever the state of the alarm is set to ALARM. ✔
- [ ] **C.** Ensure that cloudwatch metric being monitored is TunnelState for the VPN connection ✔
- [ ] **D.** Monitor the cloudwatch log being monitored is TunnelState for the VPN connection

Explanation :

Answer – B and C
For more information on monitoring VPN connections please see the below link:

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

Ask our Experts



QUESTION 62 UNATTEMPTED

You wanted to monitor the network interfaces for certain EC2 Instances. Which of the following would assist in this requirement Choose two answers from the options given below. Each answer forms part of the solution.

- [ ] **A.** Go to the necessary network interfaces in the AWS console. ✔
- [ ] **B.** Log into the EC2 Instances and choose the networking interfaces
- [ ] **C.** Enable Flow Logs ✔
- [ ] **D.** Enable Network interface logging

Explanation :

Answer – A and C

The AWS documentation mentions the following
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.
For more information on VPC flow logs please see 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 63 UNATTEMPTED

Which of the following can be used to restrict traffic to the subnets located in your VPC.

- A. Security Groups
- B. VPC Flow Logs
- C. Network Access Control Lists ✔
- D. Subnet security groups

Explanation :

Answer – C
The AWS documentation mentions the following
AWS provides two features that you can use to increase security in your VPC: security groups andnetwork *ACLs*. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets.
For more information on VPC's and subnets please see the below link:

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

Ask our Experts

QUESTION 64 UNATTEMPTED

There is a requirement to monitor API calls against your AWS account by different users and entities. There needs to be a history of those calls. The history of those calls are needed in in bulk for later review. Which 2 services can be used in this scenario

- A. AWS Config; AWS Inspector
- B. AWS CloudTrail; AWS Config
- C. AWS CloudTrail; CloudWatch Events ✔
- D. AWS Config; AWS Lambda

Explanation :

Answer – C
You can use AWS CloudTrail to get a history of AWS API calls and related events for your account. This history includes calls made with the AWS Management Console, AWS Command Line Interface, AWS SDKs, and other AWS services.
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)

Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. CloudWatch Events becomes aware of operational changes as they occur. CloudWatch Events responds to these operational changes and takes corrective action as necessary, by sending messages to respond to the environment, activating functions, making changes, and capturing state information.
For more information on Cloudwatch events, please visit the below URL:

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html (http://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html)

Ask our Experts

QUESTION 65 UNATTEMPTED

Your company currently has a Direct Connect connetion to AWS. There is a need for users to directly work with S3 buckets. There is also a requirement for private EC2 servers to access S3 content. Which of the following can be used to meet this requirement. Choose 2 answers from the options given below

- [x] **A.** A Private Virtual Interface ✔
- [ ] **B.** A Hosted Virtual Interface
- [ ] **C.** A Virtual private gateway
- [x] **D.** A Public Virtual Interface ✔

Explanation :

Answer – A and D
To connect to AWS public endpoints (for example, Amazon EC2 or Amazon S3) with dedicated network performance, use a public virtual interface.
To connect to private services such as an Amazon VPC with dedicated network performance, use a private virtual interface.
For more information on Virtual Interfaces, please refer to below URL:

- https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/ (https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/)

Ask our Experts

QUESTION 66 UNATTEMPTED

Your company is currently using a Cloudfront distribution to distribute content to users. Which of the following can be used to ensure that only authorized users can access content from the distribution. Choose 2 answers from the options below

- [ ] **A.** Configure an SSL on the distribution
- [ ] **B.** Configure Cloudfront OAI ✔
- [ ] **C.** Configure signed cookies ✔
- [ ] **D.** Configure Network Access Control Lists

Explanation :

Answer - B and C
The AWS Documentation mentions the following on Cloudfront signed cookies and OAI
CloudFront signed cookies allow you to control who can access your content when you don't want to change your current URLs or when you want to provide access to multiple restricted files, for example, all of the files in the subscribers' area of a website.
For more information on signed cookies, please refer to below URL:

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

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

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

Ask our Experts

QUESTION 67 UNATTEMPTED

Your company has an on-premise environment with Active Directory for authentication and a DNS Server. You are trying to make the EC2 Instances in your AWS VPC resolve the on-premise resources , but it does not seem to work. What could be the reason for this. Choose 2 answers from the options given below

- [ ] **A.** The NACL is blocking UDP port 53 outbound ✔
- [ ] **B.** The NACL is blocking TCP port 53 outbound ✔
- [ ] **C.** The Security Group is blocking port 80 Inbound.
- [ ] **D.** The Security Group is blocking port 80 Outbound.

Explanation :

Answer - A and B
The Network ports used by a DNS Server is port 53. Hence these ports need to be open in the Network Access Control Lists.
During DNS resolution, DNS messages are sent from DNS clients to DNS servers or between DNS servers. Messages are sent over UDP and DNS servers bind to UDP port 53. When the message length exceeds the default message size for a User Datagram Protocol (UDP) datagram (512 octets), the first response to the message is sent with as much data as the UDP datagram will allow, and then the DNS server sets a flag indicating a truncated response. The message sender can then choose to reissue the request to the DNS server using TCP (over TCP port 53)
For more information on NACL's, please refer to below URL:

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

Ask our Experts

QUESTION 68 UNATTEMPTED

Which of the following is false with regards to Security Groups which can be defined for EC2 Instances

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

Explanation :

Answer - A
The AWS documentation mentions the following on Security groups
1. You can specify allow rules, but not deny rules.
2. You can specify separate rules for inbound and outbound traffic.
3. When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
4. Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules
For more information on Security Groups, please refer to below URL:

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

Ask our Experts

QUESTION 69 UNATTEMPTED

You are creating an application which stores extremely sensitive financial information. All information in the system must be encrypted at rest and in transit. Which of these is a violation of this policy?

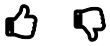
- A. ELB SSL termination. ✔
- B. ELB Using Proxy Protocol v1.
- C. CloudFront Viewer Protocol Policy set to HTTPS redirection.
- D. Telling S3 to use AES256 on the server-side.

Explanation :

Answer – A
If you use SSL termination, your servers will always get non-secure connections and will never know whether users used a more secure channel or not.
If you are using Elastic beanstalk to configure the ELB, you can use the below article to ensure end to end encryption.

- http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/configuring-https-endtoend.html (http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/configuring-https-endtoend.html)

Ask our Experts



QUESTION 70 UNATTEMPTED

You want to send a broadcast message to your 10.0.0.0/24 subnet, which one of these addresses should you use?

- **A.** 10.0.0.255
- **B.** 10.0.0.127
- **C.** 10.0.0.1
- **D.** Broadcast is not allowed in AWS ✔

Explanation :

Answer – D
This is given in the AWS Documentation that VPC's don't support broadcast or multicast.
For more information on VPC's, please refer to below URL:

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

Ask our Experts

QUESTION 71 UNATTEMPTED

Which of the following is a detailed list of the IP address ranges assigned to and used by AWS

- A. ip-ranges.json ✔
- B. aws.json
- C. aws-vpc.json
- D. There is no list. You need to contact AWS support for this.

Explanation :

Answer - A
The AWS Documentation mentions the following
Amazon Web Services (AWS) publishes its current IP address ranges in JSON format. To view the current ranges, download the .json file. To maintain history, save successive versions of the .json file on your system. To determine whether there have been changes since the last time that you saved the file, check the publication time in the current file and compare it to the publication time in the last file that you saved.
For more information on AWS reserved IP ranges, please refer to below URL:

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

Ask our Experts

QUESTION 72 UNATTEMPTED

You currently have deployed a set of t2.medium EC2 Instances. There is a requirement now mentioning that low latency and high throughput is established between these instances. How can you accomplish this whilst minimizing downtime? Choose 3 answers from the options given below.

- [ ] **A.** Stop and restart the instances in a placement group
- [x] **B.** Create AMI's from the instances ✔
- [ ] **C.** Launch new t2.medium instances from the AMI's
- [x] **D.** Launch new m4.large instances from the AMI's ✔
- [x] **E.** Ensure the new instances are launched in a placement group ✔

Explanation :

Answer – B,D and E
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 ensure minimum downtime, create AMI's out of the instances so that new instances can be launched faster.
There is a restriction on which instance types can be used for EC2 Instances in a placement group.
T2.medium instances cannot be used in a placement group.
For more information on placement groups, please refer to below URL:

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

Ask our Experts

QUESTION 73 UNATTEMPTED

Which of the following is not an attribute of a Elastic Network Interface

- ○ **A.** A primary private IPv4 address

- **B.** One or more secondary private IPv4 addresses
- **C.** One Elastic IP address (IPv4) per public IPv4 address ✔
- **D.** One public IPv4 address

Explanation :

Answer – C
The AWS Documentation mentions the following
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 Elastic Network interfaces, please refer to below URL:

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

Ask our Experts

QUESTION 74 UNATTEMPTED

You need the absolute highest possible network performance for a cluster computing application. You already selected homogeneous instance types supporting 10 gigabit enhanced networking, made sure that your workload was network bound, and put the instances in a placement group. What is the last optimization you can make?

- **A.** Use 9001 MTU instead of 1500 for Jumbo Frames, to raise packet body to packet overhead ratios. ✔

- **B.** Segregate the instances into different peered VPCs while keeping them all in a placement group, so each one has its own Internet Gateway.
- **C.** Bake an AMI for the instances and relaunch, so the instances are fresh in the placement group and do not have noisy neighbors.
- **D.** Turn off SYN/ACK on your TCP stack or begin using UDP for higher throughput.

Explanation :

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

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

Ask our Experts

QUESTION 75 UNATTEMPTED

You have a subnet with a CIDR block of 10.0.1.0/24. Which of the following is not an IP address which would be assigned to an EC2 Instance launched in this subnet

- **A.** 10.0.1.4
- **B.** 10.0.1.253
- **C.** 10.0.1.3 ✔
- **D.** 10.0.1.254

Explanation :

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

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

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

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

Ask our Experts

QUESTION 76 UNATTEMPTED

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?

- **A.** Use CloudTrail Log File Integrity Validation. ✔
- **B.** Use AWS Config SNS Subscriptions and process events in real time.
- **C.** Use CloudTrail backed up to AWS S3 and Glacier.

- **D.** Use AWS Config Timeline forensics.

Explanation :

Answer - A
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the AWS CLI to validate the files in the location where CloudTrail delivered them
Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.
For more information on Cloudtrail log file validation, please visit the below URL:

- http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html)

Ask our Experts

QUESTION 77 UNATTEMPTED

Which of the following are network requirements for establishing a Direct Connect connection. Choose 3 answers from the options given below

- [ ] **A.** Connections to AWS Direct Connect require single mode fiber, 1000BASE-LX (1310nm) for 1 gigabit Ethernet ✔
- [ ] **B.** Support Border Gateway Protocol (BGP) ✔
- [ ] **C.** Support for AES Encryption
- [ ] **D.** Support for BGP MD5 authentication ✔

Explanation :

Answer - A,B and D
The AWS Documentation mentions the following
To use AWS Direct Connect in an AWS Direct Connect location, your network must meet one of the following conditions:

- Your network is collocated with an existing AWS Direct Connect location.
- You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN). You are working with an independent service provider to connect to AWS Direct Connect.

In addition, your network must meet the following conditions:

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

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

- http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html#overview_requirements (http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html#overview_requirements)

Ask our Experts

QUESTION 78 UNATTEMPTED

Which of the following is not required for establishing Victual Interfaces in AWS

- A. VLAN ID
- B. BGP multi-exit discriminator ✔
- C. An ASN for the BGP Session
- D. Peer IP Address

Explanation :

Answer – B
The AWS Documentation mentions the following

The following information is needed for a virtual interface:
1) VLAN: Each virtual interface must be tagged with a new, unused customer-provided tag (VLAN ID) that complies with the Ethernet 802.1Q standard.
2) Peer IP addresses: The IP address ranges that are assigned to each end of the virtual interface for the BGP peering session
3) BGP information: A virtual interface must have a public or private Border Gateway Protocol (BGP) Autonomous System Number (ASN) for your side of the BGP session
For more information on Virtual Interface requirements, please refer to below URL:

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

Ask our Experts

QUESTION 79 UNATTEMPTED

Which of the following services can be used in conjunction with Cloudwatch Logs. Choose the 3 most viable services from the options given below

- [ ] **A.** Amazon Kinesis ✔
- [ ] **B.** Amazon S3 ✔
- [ ] **C.** Amazon SQS
- [ ] **D.** Amazon Lambda ✔

Explanation :

Answer - A,B and D
The AWS Documentation the following products which can be integrated with Cloudwatch logs
1) Amazon Kinesis - Here data can be fed for real time analysis
2) Amazon S3 - You can use CloudWatch Logs to store your log data in highly durable storage such as S3.
3) Amazon Lambda - Lambda functions can be designed to work with Cloudwatch logs
For more information on Cloudwatch Logs, please refer to the below link:

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

Ask our Experts

QUESTION 80 INCORRECT

There is a requirement for a vendor to have access to an S3 bucket in your account. The vendor already has an AWS account. How can you provide access to the vendor on this bucket.

- **A.** Create a new IAM user and grant the relevant access to the vendor on that bucket.
- **B.** Create a new IAM group and grant the relevant access to the vendor on that bucket.
- **C.** Create a cross-account role for the vendor account and grant that role access to the S3 bucket. ✔
- **D.** Create an S3 bucket policy that allows the vendor to read from the bucket from their AWS account. ✖

Explanation :

Answer – C
The AWS documentation mentions
You share resources in one account with users in a different account. By setting up cross-account access in this way, you don't need to create individual IAM users in each account. In addition, users don't have to sign out of one account and sign into another in order to access resources that are in different AWS accounts. After configuring the role, you see how to use the role from the AWS Management Console, the AWS CLI, and the API
For more information on Cross Account Roles Access, please refer to the below link:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14610)

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)