Answer Sheet

Q1)

You are using a Windows Server 2012 in your on-premise location as a customer gateway.

You've setup the Virtual Private gateway and the VPN connection. You have also setup the VPN configuration on the Windows Server 2012 machine.

But when you check the status of the tunnel in the AWS Console, it still shows as down. What needs to be done to ensure that the tunnel is in the UP state. ?

- From the AWS Console, choose the VPN connection , choose Actions->Bring up tunnel
- Ensure BGP routing protocol is setup on the Windows Server 2012 device
- ✓ Issue a ping command request from the Windows Server 2012 device
- From the AWS Console, choose the Virtual Private gateway. choose Actions->Bring up tunnel

---

Q2)

You have created 3 VPC's , VPC , VPC B and VPC C. There is a VPC peering connection between VPC A and VPC B and a separate peering connection between VPC B and VPC C.

Which of the following is correct with regards to this VPC peering arrangement?

- Instances launched in VPC A can reach instances in VPC C if the right routing entries are present.
- ✓ Instances launched In VPC A can reach instances in VPC C via a proxy instance in VPC B
- Instances launched in VPC A can reach instances in VPC C if the right Security Groups
- Instances launched In VPC A can reach Instances In VPC C

Q3)

Your company is planning on setting up an AWS Direct Connect Connection and a VPN connection as a backup.

In case the AWS Direct Connect connection falls, then the traffic should be routed on the VPN line.

What can be done to ensure this fall over happens as smoothly as possible.

- Enable BGP Routing
- In AWS VPN , make AWS Direct Connect as the primary device
- In AWS Direct Connect, make the VPN as the secondary device.
- ✓ Enable Bidirectional Forwarding Detection

Q4)

Your company has setup an AWS Direct Connect connection with the help of an AWS Partner. The customer gateway Is In an on-premise data center.

Your operations department needs to be informed whenever the Direct Connect connection is down. How can you achieve this?

- You will anyway be notified if the AWS Direct Connect connection is down.
- ✓ Use Cloud watch metrics to check for the state of the tunnel
- Use the AWS Direct Connect tunnel logging facility to check for any failures
- Use Cloud watch logs to check for the state of the tunnel

Q5)

You have 2 VPC's , VPC A and VPC B. Both the VPC?s have been peered. You have configured the route tables in VPC A so that traffic can flow from VPCA to VPCB.

You try to ping an Instance In VPCB from VPCA, but are unable to do so. You have confirmed that the NACL's and Security Groups have been configured property.

What could be the reason for this issue?

- NACL's don't work in peered VPC'S hence the requests will not work.
- ✓ The route tables In VPCB have not been configured.
- Security Groups don' t work in peered VPC' S hence the requests will not work.
- The VPC's have overlapping CIDR blocks

Q6)

Your management is planning on using AWS Cloud front to speed up distribution of contents to users from an S3 bucket.

They are worried on the aspect on whether users will get the ideal response when they request for objects from Cloud front.

What would you communicate to them as to how users would get content from Cloud front?

- If a user requests an object. only when the entire object is available, it is sent to the user. This is to ensure a correct end user experience
- ✓ As soon as the first byte arrives from the origin. Cloud Front begins to forward the files to the user
- If a user requests an object. the user is directed to the origin location for retrieval of the object.

- Amazon Cloud Front will respond with an HTTP 404 error.

Q7)

Your team is using applications that are hosted in 2 different regions in AWS. There are EC2 Instances that are performing a replication processes between the applications across regions via their respective Elastic IP's.

It is noticed that the current MTU Is 1500 and there is a need to increase the throughput for the replication traffic. How can this be achieved?

- Create a VPN tunnel between the 2 VPCs and Increase the MTU on the instances
- Install the Enhanced Networking modules on the instances
- Increase the MTU on the Instances
- ✅ This Is not possible

Q8)

Your company is currently planning on using Route53 for managing Blue Green deployments.

They have already setup an 80%-20% for a new deployment. How can you ensure to stop sending traffic to the older setup once all testing is complete?

- Change the resource record weight to 100
- Delete the weighted resource record
- ✅ Change the resource record weight to 0
- Change the resource record to a simple routing policy

Q9)

You have just recently set up a web and database tier in a VPC and hosted the application.

When testing the application, you are not able to reach the home page for the app. You have verified the security groups.

What can help you diagnose the issue,

- Use AWS WAF to analyze the traffic
- Use the AWS Trusted Advisor to see what can be done.
- Use AWS Guard Duty to analyze the traffic
- ✅ Use VPC Flow logs to diagnose the traffic

Q10)

Your company is planning on creating a private hosted zone in AWS.

They need to ensure that on-premise devices can reach the resources defined in the private hosted zone.

How can this be achieved, ensuring least effort Is put Into setting this up?

- Create an EC2 instance and install a DNS resolver
- ✅ Consider using Simple AD for resolving DNS requests
- Create an EC2 instance and install AD Domain services
- Convert the private hosted zone to a public one

Q11)

Your company is planning on deploying an EC2 instance which will be used to route VPN traffic to an on- premise data center.

In such a scenario what is the responsibility of AWS?

- ✅ Ensuring high availability of the VPN connection
- Ensuring the health of the underlying physical host
- Ensuring high availability of the EC2 Instance
- Configuration of the IPSec protocol

Q12)

Your architecture team has recommended the following for the VPC's in your AWS Account "A shared services VPC which would provide services to other VPCs " A hosted VPC that will be accessible to the customer The hosted VPC will also interact with the shared services VPC.

Which of the following should also be considered as part of the design. Choose 2 answers from the options given below.

Each answer is an independent design solution?

- ✅ Ensure a virtual private link is available for accessing the Shared services VPC.
- Create a VPN between each VPC. Ensure the Virtual private gateway is in place for the other VPCs
- ✅ Put the shared services VPC as public. Ensure the right security measures are in place for accessing the shared services.
- Use VPC peering between the shared services VPC and other VPC's

Q13)

You work for an organization that has a Direct Connect Connection and a backup VPN connection. This has been setup Just

recently.

After setting it up, the traffic flow still prefers the VPN connection Instead of the Direct connection. You have pretended a longer AS_PATH on the VPN connection, but even then this connection is being preferred.

Which of the below steps can be used to ensure the Direct Connect connection is used?.

- Remove the pretended AS_PATH.
- ✓ Advertise a less specific prefix on the VPN connection
- Reconfigure the VPN as a static VPN instead of dynamic.
- In crease the MED property on the VPN connection.

Q14)

You've setup a set of EC2 Linux based instances in a placement group. You've chosen instances with Enhanced Networking enabled.

You want to ensure that the maximum number of packets can be sent across the network interfaces.

How could you achieve this.?

- Change the jumbo frame setting on the ethernet interface for each instance
- Set the Network Access Control List to the maximum network packet size
- Set the Placement Group settings to the maximum network packet size
- ✓ Change the MTU setting on the ethernet interface for each instance

---

Q15)

Your company is planning on hosting their own VPN server in AWS. This will be hosted on an EC2 instance and using a software from the AWS Marketplace.

You are tasked with ensuring optimal performance of the underlying VPN server.

Which of the following aspects would you consider? Choose 2 answers from the options given below

- ✓ Ensure that the instance is using Enhanced Networking
- Use a Network load balancer for scaling
- Ensure that the instance is using EBS optimized Volumes
- ✓ Understand the packet limitations In the infrastructure

Q16)

You have a Lambda function that is designed to probe for events on an EC2

Instance. After the probe is complete, the lambda function needs to send requests to an SQS queue.

How can this be achieved? Select 2 Answers.

- Ensure that the Lambda function details are added to the VPC configuration
- ✓ Ensure that the VPC configuration Is added to the Lambda function
- Ensure that IpV6 is enabled for the subnet hosting the Lambda function
- ✓ Create a NAT instance in the VPC

Q17)

Your company is planning on using an EC2 instance for handling voice related traffic.

A custom application will be installed on a Linux based instance.

Which of the following is an ideal implementation step to ensure Quality of Service for the voice based software?

- Use an Application load balancer in front of the EC2 instance
- Use a Network load balancer In front of the EC2 Instance
- Use a placement group for the EC2 Instance
- ✓ Enable Enhanced networking on the instance

Q18)

You currently manage a set of web servers hosted on EC2 Servers with public IP addresses. **These IP addresses are mapped to domain names.**

There was an urgent maintenance activity that had to be carried out on the servers and the servers had to be restarted.

Now the web application hosted on these EC2 Instances is not accessible via the domain names configured earlier.

Which of the following could be a reason for this?

- ✓ The public IP addresses have changed after the instance was stopped and started
- The public IP addresses need to be associated to the ENI again.
- The network interfaces need to be initialized again.
- The Route53 hosted zone needs to be restarted.

Q19)

Your IT Security department has deployed a firewall on an AWS EC2 Instance.

They have mandated at all traffic from certain applications needs to move through the firewall.

In such a case what considerations should be made for the EC2 instance for maximum performance?

- Consider using NACL's
- Consider using an Amazon Linux AMI only
- Driver support for the Intel Virtual function and Elastic Network Adapter (ENA)
- ✓ The underlying Instance type

Q20)

You're planning on hosting an application on an Amazon Linux EC2 Instance.

You have a requirement to reduce the amount of time it takes to process packets on the EC2 instance.

Which of the following can be used for this requirement?

- ✓ Consider using the Data Plane Development Kit
- Consider using an MTU of 12.000
- Consider using Jumbo frames for packet transmission
- Use an Instance which supports the Windows AMI

Q21)

A company is planning on using a Cloud front Distribution.

The origin will be an 53 bucket They want to ensure that users cannot access the objects in the 53 bucket via the public URL of the bucket objects.

How can you accomplish this? Please select:

- ✓ Create a Cloud front Origin identity which has access via the bucket policy
- Place an IAM policy which ensures that users cannot access the objects
- Create a Cloud front Origin identity which has access via the AM policy
- Create a separate IAM user that has access via the bucket policy

---

Q22)

You have a VPC and EC2 Instances hosted in the subnet. You need to diagnose layer 4 traffic and see which requests are ACCEPTED and REJECTED.

Which of the following would help in fulfilling this requirement?

- Installing IDS on each Instance
- Enabling Cloud Trail
- ✓ Enabling VPC Flow Logs

Explanation:-Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. Operating at the connection level (Layer 4), Network Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) and is capable of handling millions of requests per second while maintaining ultra-low latencies. Network Load Balancer is also optimized to handle sudden and volatile traffic patterns. Refer: https://aws.amazon.com/elasticloadbalancing/

- Using Cloud watch logs

Q23) Which one of the following is not true about Amazon Cloud Front cache behaviors?

- Forward query strings to the origin, and cache based on specified parameters in the query string.
- ✓ For RTMP distributions, you can configure Cloud Front to forward query string parameters to your origin.
- Don't forward query strings to the origin at all then Cloud Front doesn?t cache based on query string parameters.
- Forward query strings to the origin, and cache based on all parameters in the query string.

Q24)

You have been requested to use Cloud Formation to maintain version control and achieve automation for the applications In your organization.

The environment will consist of several networking components and application services.

What Is the best way to design the template.

- Use Cloud Formation custom resources to handle dependencies between stacks
- Create multiple templates in one Cloud Formation stack.
- ✓ Create separate templates based on functionality, create nested stacks with Cloud formation.
- Combine all resources into one template for version control 3nc1 3utrr3tI

Q25)

A company has setup an application on an EC2 Instance in a private subnet. This Instance is used to process videos.

The Instance has been enabled with Enhanced Networking. The Instance now needs to get videos from an S3 bucket for processing.

An IAM Role has been assigned to the Instance to access S3. But when the EC2 Instance tries to access the S3 bucket, a 403 error is returned.

What needs to be done to ensure that the error gets resolved?

- Ensure that the CIDR range for the S3 bucket is added to the Security Groups for the EC2 Instance
- Ensure that a VPC endpoint is created and attached to the EC2 Instance
- ✓ Ensure that a VPC endpoint is created and attached to the subnet
- Ensure that the CIDR range for the 53 bucket is added to the NACL's for the subne

---

Q26)

Your company is planning on deploying EC2 Instances across multiple regions. These instances will make calls to the Simple Storage service.

You are trying to understand the data transfer costs which are Incurred in such an implementation.

Which of the following is not charged by AWS?

- From an Elastic Compute Cloud (Amazon EC2) in eu-west-i to Amazon Simple Storage Service (Amazon S3) in us-east-i
- From Amazon EC2 in eu-west-i to your on-premises data center
- ✓ From your on-premises data center to Amazon S3 in us-east-i
- From Amazon 53 In us-east-i to Amazon EC2 in eu-west-

Q27)

Your team has created a cloud formation template. The template consists of a creation of a Virtual private gateway, Customer gateway and a VPN connection based on the created artifacts.

The templates sometimes gives errors because the routes are not being added because of the missing Virtual private gateway resource.

How can you resolve this?

- ✓ Add a Depends On attribute to the Route Table entry on the VPGW
- Change the order of the creation of the resources in the template
- Add a custom resource to the template for the Route Table entry
- Add a Depends On attribute to the VPGW on the Route table

Q28)

You have a team that is trying to ingest data in Amazon 53. They are trying to ingest 1 TB of data using a large instance.

Enhanced Networking has been enabled on the instance. But the data ingestion process is Quiz n still running slowly.

What can be done to rectify the issue?

- Use an AWS Direct Connect connection between S3 and the instance
- Create a VPN connection from the instance to S3
- ✓ Consider using 2 instances and splitting the ingestion of data
- Create a VPC endpoint from the instance to 53

Q29)

Your company is planning on opening an AWS Direct Connect connection.

They need to ensure that their router has the required capabilities to support this connection.

Which of the following needs to be supported by the router. Choose 3 answers from the options given below ?

- ✓ Single Mode Fiber
- ✓ BGP and BGP MDS authentication
- 802.lad
- ✓ 802.1QVLAN

Q30)

You need to create a Private VIF for an existing AWS Direct Connect connection.

Which of the following is required during the configuration process?

- Prefixes to advertise
- The Peer Public IP
- ✓ Virtual Gateway
- ✓ VLAN ID

Q31)

You've just setup an Amazon Red shift cluster and started loading tables using the COPY command.

You've noticed that the Internet Is being utilized for the data being copied.

You want to ensure that the internet is not used during the copy operation. How can you achieve this?

- Ensure the NACL's are set on the Subnets hosting the Red shift cluster
- Ensure the Security Groups are set on the EC2 Instances hosting the Red shift cluster
- ✓ Ensure Enhanced VPC routing Is enabled for the Red shift cluster
- Ensure the routing table points to a VPN instead of the Internet gateway

---

Q32)

Your team has setup a testing environment using a VPC and EC2 Instances. An application is being hosted on these Instances.

Some housekeeping scripts are being developed using AWS Lambda that would need to delete files created by these Ec2 Instances on their respective EBS volumes.

What Is the Initial configuration that needs to be put in place?

- Ensure an Internet gateway Is attached to the VPC
- ✓ Ensure to use the vpc -config when creating the AWS Lambda function
- Ensure the VPC has a route entry to the Lambda function
- Ensure to use the --vpc- conflg when creating the Ec2 instance

---

Q33)

You have an on-premise application that needs access to the Simple Storage Service.

Some of the key requirements are high bandwidth for the connection, low jitter and high availability.

Which of the following option would you consider in the design?

- Using AWS Direct Connect with a private VIF
- Using an IPSec VPN connection to a Virtual Private gateway
- Use the public Internet to access the S3 service
- ✓ Using AWS Direct Connect with a public VIF

Q34)

Your production team has created a Multi-AZ Amazon RDS instance. The application connects to the instance via a custom DNS A record.

There was an instance wherein the primary database failed and the application could no longer connect to the database.

What needs to be done to ensure this same issue does not happen in the future?

- Ensure the primary database is quickly swapped with the secondary one
- Ensure that the application is using the IP address of secondary database instance
- Ensure that the application is using the IP address of primary database instance
- ✓ Ensure that the application Is using the Amazon RDS hostname

---

Q35)

Your company has an AWS Direct connect connection in the us-west region. They want to use a VPC via the AWS Direct Connect connection.

The VPC is located in another region. How can you achieve this connectivity?

Choose 2 answers from the options given below.

- Create a private VIF and then a VPN connection over that to the remote VPC
- ✓ Create a Public VIF and then a VPN connection over that to the remote VPC
- ✓ Create a Direct Connect gateway in a public region
- Create a private VIF from the current AWS Direct Connect Connection. With Inter-region peering this is possible.

Q36)

You want to automated the VPC Peering connections that occurs in your AWS Account.

Which of the following methods can be used to automate the VPC peering connections

- Use Cloud watch metrics along with a Lambda function
- Use cloud trail along with a Lambda function
- Use an Ops work stack to peer the VPCs
- ✓ Use a Cloud formation template to peer the VPC5

Q37)

Your team has created a cloud formation template.

It creates a VPC and a subnet with a CIDR block of 10.0.0.0/16 and you have created another subnet with in the VPC with a CIDR block of 10.1.0.0/24.

What will happen when you try to deploy the template?

- The template will give an error during the design stage

- The template will give a deployment error when creating the subnet and leave the VPC as created
- ✓ The template will give a deployment error and all resources will be rolled back
- The template will deploy successfully

Q38)

You have a set of EC2 Instances in a VPC. You need to have optimal network performance on these Instances.

These Instances will talk to Instances In another VPC via VPC peering. Which of the following should be carried out to ensure maximum network performance?

Choose 2 answers from the options given below.

- Create 2 availability zones for the instances in the primary VPC and place them in a placement group
- ✓ Enable Enhanced Networking on the Instances
- Set the MTU on the Instances to 9001
- ✓ Ensure the operating system supports Enhanced networking

Q39)

You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication.

The solution must be resilient. Which of the following options would you consider for configuring the web server infrastructure?

Choose 2 answers from the options below

- ✓ Configure ELB with HTTPS listeners, and place the Web servers behind it.
- Configure your Web servers with EIP?s. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers.
- Configure your web servers as the origins for a Cloud Front distribution.
- ✓ Configure ELB with TCP listeners on TCP/443. And place the Web servers behind it.

Q40)

Your company has an AWS Direct connect connection in the us-west region.

They are currently using a public VIF to access an S3 bucket in the us-west region.

They now want to make use of AWS Direct Connect to access an 53 bucket in the us-east region.

How can this be achieved In the most economical way?

- Create another Private VIF from your current AWS Direct connect connection
- ✓ Create another Public VIF from your current AWS Direct connect connection
- Create another AWS Direct connect connection from your on-premise network in the us-east region.
- Create an VPN IPsec connection

Q41)

A company has setup a set of EC2 Instances behind an Application Load Balancer.

There seems to be a barrage of requests from a series of URL's, You need to have these URL's blacklisted.

How can you achieve this on an ongoing manner?

- Deny the URLS via the Security Groups for the Instance
- Use AWS VPC Flow logs to prevent the attacks from the URL's
- Deny the URL?s via the NACL?s for the subnet
- ✓ Put a WAF in front of the Application Load Balancer

Q42)

You currently have 9 EC2 instances running in a Placement Group. All these 9 instances were initially launched at the same time and seem to be performing as expected.

You decide that you need to add 2 new instances to the group; however, when you attempt to do this you receive a capacity error.

Which of the following actions will most likely fix this problem? Choose the correct answer from the options below Please select:

- Make sure all the instances are the same size and then try the launch again.
- Request a capacity Increase from AWS as you are initially limited to 10 instances per Placement Group.
- Make a new Placement Group and launch the new instances in the new group. Make sure the Placement Groups are in the same subnet.
- ✓ Stop and restart the instances in the Placement Group and then try the launch again.

Q43)

You have a My SQL cluster which is hosted in AWS. The nodes in the cluster currently work with the private IP addresses.

There is a self-referencing security group which is used for securing access across the nodes of the cluster.

There Is now a requirement to ensure disaster recovery for these nodes in another region.

How can you achieve communication across the nodes in different regions securely?

- [x] Create a VPN IPSec tunnel. Ensure the nodes in the different region reference the VPC CIDR block in their security groups
- [ ] Use the private IP addresses of the nodes and use SSL certificates for secure communication across the nodes
- [ ] Create a VPN IPSec tunnel. Ensure the nodes in the different region reference the security groups assigne to the nodes in the primary region
- [ ] Use public IP addresses and use SSL certificates for secure communication across the nodes

---

Q44)

Your company has an AWS Direct Connect connection from a VPC to an on-premise location.

Which of the following can be used as a backup incase the Direct Connect connection fails for any reason?

Choose 2 answers from the options given below ?

- [x] Set up a VPN connection
- [ ] There is no need to configure this as AWS will fall back to a secondary Direct Connect connection as per their SLA.
- [x] Setup a peering connection
- [ ] Setup a secondary Direct Connect connection.

Q45)

Your company has the following Direct Connect and VPN Connections

Site A - VPN 10.1.0.0/24 AS 65000 65000

Site B - VPN 10.1.0.252/30 AS 65000

Site C - Direct Connect 10.0.0.0/8 AS 65000

Site D - Direct Connect 10.0.0.0/16 AS 65000 SI

Which site will AWS choose to reach your network' SI Please select:

- [x] Site B
- [ ] Site D
- [ ] Site C
- [ ] Site A

Q46)

Your company has an EC2 Instance hosted in AWS. This EC2 Instance hosts an application.

Currently this application Is experiencing a number of Issues. You need to inspect the network packets to see what the ty of error that Is occurring?

Which one of the below steps can help address this issue?

- [ ] Use VPC Flow Logs.
- [x] Use a network mentioning tool provided by an AWS partner.
- [ ] Use another instance. Setup a port to promiscuous mode, and sniff the traffic to analyze the packets
- [ ] Use Cloud watch metric

Q47)

You have working on creating a VPN connection between AWS and your on-premise infrastructure.

You've created the Virtual private gateway and the customer gateway.

You need to ensure the firewall rules are set on your side.

Which of the following would you configure? Choose 2 answers from the options given below?

- [x] IP protocol 50
- [ ] TCP port SOO
- [x] UDP port 500
- [ ] TCP port SO

Q48)

You have setup an EC2 Instance that hosts a web application. You have set the following rules?

Security Group Rules o Allow Inbound Traffic on port 80 from 0.0.0.0/0 o Deny Outgoing Traffic?

NACL o Allow Inbound Traffic on port 80 from 0.0.0.0/0 o Deny Outgoing Traffic Users are complaining that they cannot access the web server.

How can you ensure that the issue gets resolved?

- [x] Allow Outgoing Traffic on the NACL for ephemeral ports
- [ ] Allow Outgoing Traffic on the Security groups for ephemeral ports
- [ ] Allow Outgoing Traffic on the NACL for port 80
- [ ] Allow Outgoing Traffic on the Security groups for port 80

Q49)

Your team is using a NAT instance on an Linux EC2 Instance. The private subnet has a route added for S 0.0.0.0/0 for the NAT Instance.

This NAT Instance Is being used to download updates from the Internet for instances In the private subnet.

But the IT administrators who are in charge of applying the updates complain of slow response times.

What can be done to rectify this issue? Choose 2 answers from the options given below

- ✅ Add another NAT instance. Add another route for 0.0.0.0/0 to the new NAT instance
- Move the NAT instance to the private subnet to be closer the instances
- ✅ Upgrade the NAT instance to a larger instance type
- Replace the NAT instance with a NAT gateway

Q50)

You are trying to diagnose a connection issue with a Linux instance. The instance is assigned a public IP and is in the public subnet.

You can also see that the Internet gateway is attached and the route tables are in place. You SSH into the Instance from a bastion host.

You then do an If config and see that the Interface does not have a public IP address.

What should be done next to check the issue ?

- ✅ Check the Security Groups for the instance
- Assign a private P to the interface
- Assign the public IP to the interface
- Assign an Elastic IP to the interface

Q51)

You need to perform a deep packet analysis for packets that are being sent to your EC2 Instance.

Which of the following can help you accomplish this?

- ✅ Wire shark
- AWS Cloud Watch
- AWS Cloud Trail
- AWS VPC Flow Logs

Q52)

You have an EC2 Instance that will act as a custom origin for a Cloud front web distribution.

You need to ensure that traffic is encryp

- Configure the Viewer protocol policy as HTTPS and ensure that the traffic flows via the Amazon Virtual Private Network
- ✅ Configure the Viewer protocol policy as Redirect HTTP to HTTPS and Change the Origin Protocol policy to Match Viewer
- Configure the Viewer protocol policy as HTTP and ensure that SSL certificate is installed on the EC2 Instance
- Configure the Viewer protocol policy as Redirect HTTP to HTTPS and ensure that the traffic flows via the

---

Q53)

You're AWS Admin team has created an AWS workspace.

Users on the on-premise environment don't seem to have the ability to use the AWS created workspaces.

What could be the primary underling issue. Please select:

- ✅ The AWS Workspaces have not been created properly. They need to be recreated
- The NACLS on the AWS Workspaces are not allowing incoming traffic
- The Security Groups on AWS Workspaces are not allowing outbound traffic
- The ports on the company firewall are not open

Q54)

Your company is planning on deploying an application to AWS.

There is a requirement for high availability and low latency between the underlying instances that support the application.

Which of the following would you not consider In your design?

- Deploy instances across multiple availability zones
- Use a Network load balancer in front of the instances
- Enable Enhanced Networking on the instances
- ✅ Place the instances in a placement group

Q55)

You have a database that is running on a large instance type. From a monitoring perspective it seems that the packets are

getting lost and the instance is not delivering requests as desired.

Initially a test was done to check the capacity of the server. At that time, the database server was able to take on the load.

What could be the issue at this point in time?

- ✅ There are internal database errors which are causing the timeouts.
- There is not using a VPN tunnel for communication
- The instance was using accumulated network credits during the testing phase
- The right AMI was not chosen for the underlying instance

Q56)

You have a set of instances setup in an AWS VPC. You need to ensure that instances in the VPC receive host names from the AWS DNS.

You have set the enable DNs Hostname attribute set to true for your VPC.

But the instances are still not receiving the host names when they are being launched. What could be the underlying issue?

- The Auto-Assign Public P is not set for the Subnet in which the Instance is launched
- You need to configure a Route 53 private hosted zone first
- You need to configure a Route 53 public hosted zone first
- ✅ The enable DNs Support is not set to true for the VPC

Q57)

You have setup a Cloud front distribution in AWS. You want to use the AWS Certification Manager along with Cloud front.

You are setting up Cloud front, but you cannot see the ACM certificate that you created at an earlier stage to associate with the distribution.

What could be the underlying issue?

- You need to upload the certificate directly to Cloud front after the distribution is created
- You need to ensure that an alias record is created in Route 53 first
- You need to ensure that a CNAME record is created in Route 53 first
- ✅ You have not uploaded or created the certificate in the right region

---

Q58)

Your company is planning on using Route53 as the DNS provider.

They want to ensure that their company domain name points to an existing Cloud front distribution.

How this could be achieved. Please select:

- Create a CNAME record which points to the Cloud front distribution
- ✅ Create an Alias record which points to the Cloud front distribution
- Create a non-alias record which points to the Cloud front distribution
- Create a host record which points to the Cloud front distribution

---

Q59)

A company currently hosts their architecture in the US region.

They now need to duplicate that architecture to the Europe region and extend the application hosted on this architecture to the new region.

In order to ensures that users across the globe get the same seamless experience from either setup, what needs to be done?

- Create a weighted Route53 policy to route the policy based on the weight age for each location
- Create a classic Elastic Load Balancer is setup to route traffic to both locations
- ✅ Create a geolocation RouteS3 policy to route the policy based on the location.
- Create an Application Elastic Load Balancer is setup to route traffic to both locations

---

Q60)

You have launched a couple of EC2 Instances in separate subnets. You are transferring data via the Public IP?s of the EC2 Instances.

Both Instances are located in the same AZ. Instances are located in the us-east-i region. What would the data transfer charges?

- ✅ There will be a data transfer charge of $0.01/GB
- There are no data transfer charges for instances in the same region
- There are no data transfer charges for instances In the same AZ
- There is no data transfer charge for the internet

Q61)

Your company has a set of AWS Direct Connect connections. They want to aggregate the bandwidth of these connections to ensure that a large amount of data can be sent through the pipe.

So a decision has been made to set up a link aggregation group. What are the factors that need to be considered when setting up the LAG group?

Choose 2 answers from the options given below.

- [x] You have to ensure that the existing AWS Direct connect connections have the same bandwidth
- [x] You have to ensure that all AWS Direct connect connections terminate at the same AWS endpoint
- [ ] You have to ensure that all AWS Direct connect connections terminate at different AWS endpoint
- [ ] You have to ensure that a VPN connection is also in place to attach to the LAG group

---

Q62)

A company has a set of resources hosted in a VPC. They have acquired another company and they have their own set of resources hosted in AWS.

The requirement now is to ensure that resources in the VPC of the parent company can access the resources In the VPC of the child company.

What Is the best way to accomplish this with minimum costing involved?

- [ ] Use a Direct Connect connection with a private V1F
- [ ] Use VPC Peering to peer both VPC's
- [ ] Use a VPN connection to peer both VPCS
- [x] Establish a NAT gateway to establish communication across VPCs

---

Q63)

Your current web application is hosted on a set of EC2 Instances which are placed behind an application load balancer.

All the Security groups and NACL's have been put into place for tight security.

What extra measure can be taken to ensure blocking of DDS attacks from malicious IP addresses

- [ ] Consider placing an AWS Private Link service In front of the Application Load balancer
- [ ] Consider adding the more restrictive rules to the Network ACL's
- [ ] Consider placing an AWS Shield service in front of the Application Load balancer
- [x] Consider placing the WAF service in front of the Application Load balancer v'
