Answer Sheet

Q1)

A gaming company adopted AWS Cloud Formation to automate load-testing of their games. They have created an AWS Cloud Formation template for each gaming environment including one for the load-testing stack.

The load-testing stack creates an Amazon Relational Database Service (RDS) Postgres database and two web servers running on Amazon Elastic Compute Cloud (EC2) that send HTTP requests, measure response times, and write the results into the database.

A test run usually takes between 15 and 30 minutes. Once the tests are done, the AWS Cloud Formation stacks are torn down immediately.

The test results written to the Amazon RDS database must remain accessible for visualization and analysis.

Select possible solutions that allow access to the test results after the AWS Cloud Formation load -testing stack is deleted. Choose 2 options from the below:.

● Define an Amazon RDS Read-Replica in the load-testing AWS CloudFormation stack and define a dependency relation between master and replica via the DependsOn attribute.

✓ Define a deletion policy of type Retain for the Amazon RDS resource to assure that the RDS database is not deleted with the AWS CloudFormation stack.

Explanation:-Retain deletion policy, the RDS resources would be preserved for the visualization and analysis after the stack gets deleted.

✓ Define a deletion policy of type Snapshot for the Amazon RDS resource to assure that the RDS database can be restored after the AWS CloudFormation stack is deleted.

Explanation:-the Snapshot deletion policy, a snapshot of the RDS instance would get created for visualization and analysis later after the stack gets deleted.

● Define automated backups with a backup retention period of 30 days for the Amazon RDS database and perform point-in-time recovery of the database after the AWS CloudFormation stack is deleted.

● Define an update policy to prevent deletion of the Amazon RDS database after the AWS CloudFormation stack is deleted.

Q2)

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?

● 20.0.0.122

✓ 20.0.0.255

Explanation:-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.

● 20.0.0.55

● 20.0.0.132

Q3) Which of the following authentication method is used when an account manager needs to login into CloudHSM?

● IAM Role

✓ SSH Keys

● Console password

● IAM password

Q4) Why will the following CloudFormation template fail to deploy a stack? Choose the correct answer from the below options: { "AWSTemplateFormatVersion" : "2010-09-09", "Parameters" : { "VPCId" : { "Type": "String", "Description" : "Enter current VPC Id" }, "SubnetId : { "Type": "String", "Description" : "Enter a subnet Id" } }, "Outputs" : { "InstanceId" : { "Value" : { "Ref" : "MyInstance" }, "Description" : "Instance Id" } } }

● A template description is mandatory but is not included

✓ A “Resources” section is mandatory but is not included

Explanation:-As per the documentation, the resources part is mandatory for the CloudFormation template

● A “Conditions” section is mandatory but is not included

● CloudFormation templates do not use a “Parameters” section

Q5)

The DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure.

To inspect all HTTP requests, WAFs sit in-line with your application traffic.

Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck.

To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes.

This type of scaling for WAF is done via a WAF sandwich.

Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below

● The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the Internet.
● The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
● The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
✓ The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.
Explanation:-As shown in the "WAF Sandwich" diagram, the WAF EC2 instances are placed in an auto-scaling group, thus it can scale according to the increase in the incoming traffic load. The ELB on the left of the WAF is a public facing ELB which accepts the incoming traffic and sends to the WAF, which inspects and filters the malicious traffic, and forwards the safe traffic to the ELB on its right side - which is an internal ELB. This ELB then distributes the traffic among the EC2 instances for further processing. It has the WAF EC2 instance is placed in an autoscaling group and between two ELBs.

Q6)

You want to set up a public website on AWS. The things that you require are as follows:

- You want the database and the application server running on AWS VPC.

- You want the database to be able to connect to the Internet, specifically for any patch upgrades.

- You do not want to receive any incoming requests from the Internet to the database.

Which of the following solutions would be the best to satisfy all the above requirements for your planned public website on AWS? Choose the correct answer from the options below

✓ Set up the public website on a public subnet and set up the database in a private subnet which connects to the Internet via a NAT instance.
Explanation:-You should set up the data server in private subnet as it needs only the traffic from NAT instance or NAT Gateway, and not from the internet.
● Set up the database in a private subnet with a security group which only allows outbound traffic.
● Set up the database in a public subnet with a security group which only allows inbound traffic.
● Set up the database in a local data center and use a private gateway to connect the application to the database.

Q7)

You are working as a consultant for a company designing a new hybrid architecture to manage part of their application infrastructure in the cloud and on-premise.

As part of the infrastructure, they need to consistently transfer high amounts of data.

They require a low latency and high consistency traffic to AWS.

The company is looking to keep costs as low possible and is willing to accept slow traffic in the event of primary failure.

Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

✓ Provision a Direct Connect connection to an AWS region using a Direct Connect partner. Provision a VPN connection as a backup in the event of Direct Connect connection failure.
Explanation:-It sets up a Direct Connect as the primary connection which provides consistent bandwidth for transferring high amounts of data, and in case of failure, sets up a VPN which is a low-cost solution.
● Provision a Direct Connect connection which has automatic failover and backup built into the service.
● Create a dual VPN tunnel for private connectivity, which increases network consistency and reduces latency. The dual tunnel provides a backup VPN in the case of primary failover.
● Provision a Direct Connect connection to an AWS region using a Direct Connect provider. Provision a secondary Direct Connect connection as a failover.

Q8) When it comes to KMS, which of the following best describes how the AWS Key Management Service works? Choose the correct answer from the options below

● AWS KMS supports two kinds of keys - master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The master keys are then used to encrypt and decrypt customer data.
● AWS KMS supports two kinds of keys - master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The data keys are then used to encrypt the customer data and the master keys are used to decrypt the customer data.
✓ AWS KMS supports two kinds of keys - master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The data keys are then used to encrypt and decrypt customer data.
Explanation:-AWS KMS supports two types of keys - Master Keys and Data Keys. A Data Key is used to encrypt and decrypt the actual data; whereas, the Master Key is used to protect (encrypt and decrypt) the data key as well as some data upto 4Kib.
● AWS KMS supports two kinds of keys - master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The data keys are then used to decrypt the customer data, and the master keys are used to encrypt the customer data.

Q9)

A legacy application with licensing is attached to a single MAC address. Since an EC2 instance can receive a new MAC address while launching new instances.

How can you ensure that your EC2 instance can maintain a single MAC address for licensing? Choose the correct answer from the options below:

● AWS cannot have a fixed MAC address; the best solution is to create a dedicated VPN/VGW gateway to serve data from the legacy application.

● Private subnets have static MAC addresses. Launch the EC2 instance in a private subnet and, if required, use a NAT to serve data over the internet.
● Configure a manual MAC address for each EC2 instance and report that to the licensing company.
✓ Create an ENI and assign it to the EC2 instance. The ENI will have a static MAC address and can be detached and reattached to a new instance if the current instance becomes unavailable.
Explanation:-Whenever a question has a scenario where you need to use fixed MAC address for EC2 instances, always think about using Elastic Network Interface (ENI). If a static MAC address is assigned to an ENI, it remains unchanged. As long as the EC2 has that ENI, it's MAC address will not change. As mentioned above, as ENI with static MAC address can be assigned to the EC2 instance. If the instance becomes unavilable or needs to be replaced, the ENI can be detached and re-attached to another EC2 while maintaining the same MAC address.

Q10)

You are setting up a video streaming service with the main components of the set up being S3, CloudFront, and Transcoder.

Your video content will be stored on AWS S3 and it should only be viewed by the subscribers who have paid for the service.

Your first job is to upload 10 videos to S3 and make sure they are secure before you even begin to start thinking of streaming the videos.

The 10 videos have just finished uploading to S3, so you now need to secure them with encryption at rest.

Which of the following would be the best way to do this? Choose the correct answer from the options below:

● Use AWS CloudHSM appliance with both physical and logical tamper detection and response mechanisms that trigger zeroization of the appliance.
● Set an API flag, or check a box in the AWS Management Console, to have data encrypted in Amazon S3. Create IAM Users to access the videos from S3.
✓ Use KMS to encrypt source data and decrypt resulting output. Also, use Origin Access Identity on your CloudFront distribution, so the content is only able to be served via CloudFront, not S3 URLs.
Explanation:-(a) it uses KMS for encrypting and decrypting the data, and (b) it ensures that only the authenticated users will have access to the videos by using the Origin Access Identity (OAI) on the CloudFront distribution and disabling the access via S3 URLs.
● Encrypt your data using AES-256. After the object is encrypted, the encryption key you used needs to be stored on AWS CloudFront so that only authenticated users can stream the videos.

Q11)

Suppose you are hosting a website in an S3 bucket. Your users load the website endpoint https://website.s3-website-us-east-1.amazonaws.com.

Now you want to use CSS on the web pages that are stored in a different bucket which is also public.

But layout on the client browser is not loading properly.

What might have gone wrong? Choose the correct option from given below

● This is not possible
● Modify bucket policy on css bucket to able to access website bucket
● Modify bucket policy on website bucket to able to access css bucket
✓ You can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.
Explanation:-Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support in Amazon S3, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.

Q12)

You have created a VPC with CIDR block 10.0.0.0/24, which supports 256 IP addresses.

Now, you want to split this into two subnets, each supporting 128 IP addresses.

Can this be done and if so how will the allocation of IP addresses be configured? Choose the correct answer from the options below:

● One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.1.0/25 (for addresses 10.0.1.0 - 10.0.1.127).
✓ One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).
Explanation:-One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).
● This is not possible.
● One subnet will use CIDR block 10.0.0.0/127 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/255 (for addresses 10.0.0.128 - 10.0.0.255).

Q13)

You have been given the task of designing a backup strategy for your organization's AWS resources with the only caveat being that you must use the AWS Storage Gateway.

Which of the following is the correct/appropriate statement surrounding the backup strategy on the AWS Storage Gateway? Choose the correct answer from the options below

● It doesn't matter whether you use Gateway-Cached Volumes or Gateway-Stored Volumes as long as you also combine either of these solutions with the Gateway-Virtual Tape Library (VTL).
● You should use the Gateway-Virtual Tape Library (VTL) since the Gateway-Cached Volumes and Gateway-Stored Volumes cannot be used for

backups.

✓ You should use Gateway-Stored Volumes as it is preferable to Gateway-Cached Volumes as a backup storage medium.

Explanation:-(a) the scenario in the question is asking you to design a backup (not a storage) strategy, (b) Gateway-Stored Volume backs up the data on Amazon S3 while keeping the data on the on-premises server, and (c) Gateway-Cached Volume only keeps the frequently accessed data on the on-premises server and stores the data on Amazon S3.

● You should use Gateway-Cached Volumes. You will have quicker access to the data, and it is a more preferred backup solution than Gateway-Stored Volumes.

Q14)

An auditor has been advised to go through the artifacts in your AWS account.

Which of the below options should be carried out so that the auditor can carry out the audit? Choose the correct answer from the options below.

● Create an IAM user with full VPC access but set a condition that will not allow the auditor to modify anything if the request is from any IP other than their own.

● Give the auditor root access to your AWS Infrastructure, because an auditor will always need access to every service.

● Create an IAM user tied to an administrator role. Also provide an additional level of security with MFA.

✓ Create an IAM Role with the read only permissions to access the AWS VPC infrastructure and assign that role to the auditor.

Explanation:-IAM Role gives just the minimum required permissions (read-only) to audit the VPC infrastructure to the auditor.

Q15) Which of the following is NOT a way to minimize the attack surface area as a DDOS minimization strategy in AWS? Choose the correct answer from the options below

● Reduce the number of necessary Internet entry points.

✓ Configure services such as Elastic Load Balancing and Auto Scaling to automatically scale.

Explanation:-It is used for mitigating the DDoS attack where the system scales to absorb the application layer traffic in order to keep it responsive.

● Eliminate non-critical Internet entry points.

● Separate end user traffic from management traffic.

Q16)

A company is running a web application that has a high amount of dynamic content.

The company is looking to reduce load time by implementing a caching solution that will help reduce load times for clients requesting the application.

What is the best possible solution and why? Choose the correct answer from the options below

✓ Create a CloudFront distribution, enable query string forwarding, set the TTL to 0: This will keep TCP connections open from CloudFront to origin, reducing the time it takes for TCP handshake to occur.

Explanation:-(a) it uses CloudFront distribution which is AWS managed highly available and scalable service, (b) it sets the TTL to 0, so that whenever the content changes at the origin, the updated content immediately gets cached at all the edge locations, giving users the latest content, and (c) it uses query string forwarding to get the custom or dynamic content generated at the origin server using the query string parameters. See the image below for the CloudFront settings.

● Offload the DNS to Route 53; Route 53 has DNS servers all around the world and routes the request to the closest region which reduces DNS latency.

● Create an ElastiCache cluster, write code that caches the correct dynamic content and places it in front of the RDS dynamic content. This will reduce the amount of time it takes to request the dynamic content since it is cached.

● Create a CloudFront distribution; disable query string forwarding, set the TTL to 0. This will keep TCP connections open from CloudFront to origin, reducing the time it takes for TCP handshake to occur

---

Q17)

Your company has an e-commerce platform which is expanding all over the globe, you have EC2 instances deployed in multiple regions you want to monitor the performance of all of these EC2 instances.

How will you setup CloudWatch to monitor EC2 instances in multiple regions?

● Create separate dashboards in every region

✓ Have one single dashboard to report metrics to CloudWatch from different region

Explanation:-You can monitor AWS resources in multiple regions using a single CloudWatch dashboard. For example, you can create a dashboard that shows CPU utilization for an EC2 instance located in the us-west-2 region with your billing metrics, which are located in the us-east-1 region.

● This is not possible

● Register instances running on different regions to CloudWatch

---

Q18)

You currently have 9 EC2 instances running in a Placement Group.

All these nine instances were initially launched at the same time and seemed to be performing as expected.

You decide that you need to add two 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

✓ Stop and restart the instances in the Placement Group and then try the launch again.

Explanation:-The most likely reason for the "Capacity Error" is that the underlying hardware may not have the capacity to launch any additional instances on it. If the instances are stopped and restarted, AWS may move the instances to a hardware that has capacity for all the requested instances.

● 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.

Q19)

A legacy software is hosted on an EC2 instance which has the license tied to the MAC address.

From your experience with AWS, you know that every time an instance is restarted, it will almost certainly lose it's MAC address.

What will be a possible solution to this? Choose an answer from the options below

● Use a VPC with a private subnet and configure the MAC address to be tied to that subnet.
● Make sure that EC2 Instance you deploy has a static IP address that is mapped to the MAC address.
✓ Use a VPC with an elastic network interface that has a fixed MAC Address.
Explanation:-You should use Elastic Network Interface that is associated with a fixed MAC address. This will ensure that the legacy license based software would always work and not lose the MAC address any point in future.
● Use a VPC with a private subnet for the license and a public subnet for the EC2.

Q20)

You are setting up a VPN for a customer to connect his remote network to his Amazon VPC environment.

There are many ways to accomplish this. Also, you have given a list of the things that the customer has specified that the network needs to be able to do.

They are as follows:

- Predictable network performance

- Support for BGP peering and routing policies

- A secure IPsec VPN connection but not over the Internet

Which of the following VPN options would best satisfy the customer's requirements? Choose the correct answer from the options below

● AWS VPN CloudHub
● Software appliance-based VPN connection with IPsec
● AWS Direct Connect with AWS VPN CloudHub
✓ AWS Direct Connect and IPsec Hardware VPN connection over private lines
Explanation:-(a) with AWS Direct Connect, you would always get the predictable network performance without using the internet, and (b) it uses Hardware VPN Connection which is a secure way of logging into the AWS platform. Option C is incorrect because CloudHub is used when your remote sites want to communicate with each other, and not just with the AWS VPC. AWS Direct Connect with Hardware VPN is the best architectural solution here. There is a good read on different connection options for AWS.

Q21)

You have two teams to analyze data of a massive application using Redshift, each query issued by the first team takes approximately 1-2 hours to analyze the data while other team takes very short time to analyze the data.

You don't want the second team's queries to wait until the already running long queries are completed.

How will you solve the problem in the most economical way? Choose an answer from the options below.

● Pause long queries and resume the queries afterwards
● Create a read replica of the Red shift instance and run second team's queries on read replica
● Start another Redshift cluster from snapshot for the second team if current Redshift cluster is busy processing long queries
✓ Create two separate workload management groups and assign them to respective teams
Explanation:-The best solution - without any effect on performance - is to create two separate workload management groups - one for each department and run the queries on them.

Q22)

Your company has just set up a new document server on its AWS VPC, and it has four very important clients that it wants to give access to.

These clients also have VPCs on AWS and it is through these VPCs that they will be given access to the document server.

In addition, each of the clients should not have access to any of the other clients' VPCs. Choose the correct answer from the options below

● Set up VPC peering between your company's VPC and each of the clients' VPCs, but block the IPs from CIDR of the clients' VPCs to deny access between each other.
✓ Set up VPC peering between your company's VPC and each of the clients' VPCs.
Explanation:-In this scenario, you are asked how resources from 4 VPCs can access resources from another VPC. This is a use case of "Star-Shaped" VPC peering shown in the image below. In this configuration, VPCs that have non-overlapping CIDR with your VPC, are peered for the intent of accessing the resources using their private IP addresses. As mentioned above, the peered VPCs can share and access the resources within each other via their private IP addresses.
● Set up all the VPCs with the same CIDR but have your company's VPC as a centralized VPC.
● Set up VPC peering between your company's VPC and each of the clients' VPC. Each client should have VPC peering set up between each other to speed up access time.

Q23)

A company has many employees who need to run internal applications that access the company's AWS resources.

These employees already have user credentials in the company's current identity authentication system, which does not support SAML 2.0.

The company does not want to create a separate IAM user for each company employee.

How should the SSO setup be designed? Choose the 2 correct answers from the options below

● Create an IAM user to share based off of employee roles in the company.
● Configure an AD server which synchronizes from the company's current Identity Provide and configures SAML-based single sign-on which will then use the AssumeRoleWithSAML API calls to generate credentials for the employees.
✓ Create a custom identity broker application which authenticates employees using the existing system and uses the AssumeRole API call to gain temporary, role-based access to AWS.
Explanation:-(a) it creates custom identity broker application for authenticating the users using their existing credentials, and (b) it uses AssumeRole API for accessing the resources using temporary role.
✓ Create a custom identity broker application which authenticates the employees using the existing system, uses the GetFederationToken API call and passes a permission policy to gain temporary access credentials from STS.
Explanation:-(a) it creates custom identity broker application for authenticating the users using their existing credentials, and (b) it uses AssumeRole API for accessing the resources using temporary role.

Q24)

When you create a subnet, you specify the CIDR block for the subnet. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset (to enable multiple subnets).

The allowed block size is between a /28 netmask and /16 netmasks.

You decide to you create a VPC with CIDR block 10.0.0.0/24.

Therefore, what is the maximum and the minimum number of IP addresses according to AWS and what is the number of IP addresses supported by the created VPC? Choose the correct answer from the options below:

● Maximum is 256 and the minimum is 16 and the created VPC supports 24 IP addresses
● Maximum is 65,536 and the minimum is 24 and the created VPC supports 28 IP addresses
● Maximum is 28 and the minimum is 16 and the created VPC supports 24 IP addresses
✓ Maximum is 65,536 and the minimum is 16 and the created VPC supports 256 IP addresses
Explanation:-First let us calculate the current number of IP addresses. The CIDR block is 10.0.0.0/24. Hence, out of 32 bits of address, 24 bits are set/masked. Hence, the remaining 8 bits indicate the remaining available IP addresses. Hence, the total number of current available instances is 2^(32-24) = 2^8 = 256. Now, the maximum allowed block size is a /16 netmask. i.e. Out of 32, first 16 bits are set/masked, leaving 16 bits available. Hence, the total number of maximum available instances = 2^(32-16) = 2^16 = 65,536. Now, the minimum allowed block size is a /28 netmask. i.e Out of 32, first 28 bits are set/masked, leaving 4 bits available. Hence, the total number of minimum available instances = 2^(32-28) = 2^4 = 16.

Q25)

BCJC is running Oracle DB workloads on AWS. Currently, they are running the Oracle RAC configuration on the AWS public cloud.

You've been tasked with configuring backups on the RAC cluster to enable durability.

What is the best method for configuring backups? Choose the correct answer from the options below

● Enable Multi-AZ failover on the RDS RAC cluster to reduce the RPO and RTO in the event of disaster or failure.
● Create manual snapshots of the RDS backup and write a script that runs the manual snapshot.
✓ Create a script that runs snapshots against the EBS volumes to create backups and durability.
Explanation:-Oracle RAC is supported via the deployment using Amazon EC2. Hence, for the data backup, you can create a script that takes the snapshots of the EBS volumes.
● Enable automated backups on the RDS RAC cluster; enable auto snapshot copy to a backup region to reduce RPO and RTO.

Q26) Regarding encryption on data stored on your databases, namely Amazon RDS, which of the following statements is the true? Choose the correct answer from the options below

✓ Encryption can be enabled on RDS instances to encrypt the underlying storage, and this will by default also encrypt snapshots as they are created. No additional configuration needs to be made on the client side for this to work.
Explanation:-Once the encryption is enabled, its automated backups, read replicas, and snapshots are automatically encrypted without need of any addition settings.
● Encryption can be enabled on RDS instances to encrypt the underlying storage, but you cannot encrypt snapshots as they are created.
● Encryption can be enabled on RDS instances to encrypt the underlying storage, and this will by default also encrypt snapshots as they are created. However, some additional configuration needs to be made on the client side for this to work.
● Encryption cannot be enabled on RDS instances unless the keys are not managed by KMS.

Q27)

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 possible manner.

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

✓ 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.
Explanation:-It configures only one S3 bucket for all the CloudTrail log events on the account across all the regions. It also restricts the access to the security officer only via the bucket policy.
● 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.
● 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.
● 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.

Q28)

You have developed an application that processes massive amount of process logs generated by web site and mobile app.

This application requires the ability to analyze petabytes of unstructured data using Amazon Elastic MapReduce.

The resultant data is stored on Amazon S3.

You have deployed c4.8xlarge Instance type, whose CPUs are mostly idle during the data processing.

Which of the below options would be the most cost-efficient way to reduce the runtime of the log processing job?

● Create log files with smaller size and store them on Amazon S3. Apply the life cycle policy to the S3 bucket such that the files would be first moved to RRS and then to Amazon Glacier vaults.
● Create fewer, larger log files. Compress and store them on Amazon S3 bucket. Apply the life cycle policy to the S3 bucket such that the files would be first moved to RRS and then to Amazon Glacier vaults.
✓ Use smaller instances that have higher aggregate I/O performance.
Explanation:-Since the CPU's are mostly idle, it means that you have provisioned a larger instance which is under-utilized. A better cost-efficient solution would be to use smaller instances. For batch processing jobs such as the one mentioned in this scenario, you can use multiple t2 instances - which support the concept of CPU bursts - are ideal for situations where there are bursts of CPU during certain periods of time only.
● Add additional c4.8xlarge instances by introducing a task instance group. The network performance of 10 Gigabit per EC2 instance would increase the processing speed; thus reducing the load on the EMR cluster.

Q29) In Cloudfront, what is the Origin Protocol policy that must be chosen to ensure that the communication with the origin is done either via HTTP or HTTPS? Choose an answer from the options below

● HTTP
✓ Match Viewer
Explanation:-If the Origin Protocol Policy is set to Match Viewer, the CloudFront communicates with the origin using HTTP or HTTPS depending upon the protocol of the viewer request.
● HTTPS
● None of these

Q30)

A company has two batch processing applications that consume financial data about the day's stock transactions. Each transaction needs to be stored durably and guarantee that a record of each application is delivered so the audit and billing batch processing applications can process the data.

However, the two applications run separately and several hours apart and need access to the same transaction information.

After reviewing the transaction information for the day, the information no longer needs to be stored.

What is the best way to architect this application? Choose the correct answer from the options below

● Use Kinesis to store the transaction information. The billing application will consume data from the stream, the audit application can consume the same data several hours later.
● Store the transaction information in a DynamoDB table. The billing application can read the rows while the audit application will read the rows them remove the data.
● Use SQS for storing the transaction messages; when the billing batch process performs first and consumes the message, write the code in a way that does not remove the message after consumed, so it is available for the audit application several hours later. The audit application can consume the SQS message and remove it from the queue when completed.
✓ Use SQS for storing the transaction messages. When the billing batch process consumes each message, have the application create an identical message and place it in a different SQS for the audit application to use several hours later.
Explanation:-The main architectural considerations in this scenario are: (1) each transaction needs to be stored durably (no loss of any transaction, (2) guaranteed delivery of each record to the audit and billing batch processing, and (3) the processing of the record by two application is done with a time gap of several hours (should support asynchronous processing). Based on the considerations above, it seems that we must use an AWS service which helps in asynchronous processing of data with guaranteed delivery of each task. The most suited option for this is Amazon SQS. However, in SQS, the message can be duplicated (albeit guaranteed). Since there is no restriction about duplicated record is given in this scenario, use of SQS is most suited.
As mentioned above, SQS can store the transaction records in a queue. Once each record is processed, it stores it in a separate queue which will be processed by audit application several hours later. Thus enabling the asynchronous processing of the records. Also, the use of second queue ensures that the same records are not processed multiple times.

Q31)

A company has developed a Ruby on Rails content management platform. Currently, OpsWorks with several stacks for dev, staging, and production is being used to deploy and manage the application.

Now, the company wants to start using Python instead of Ruby.

How should the company manage the new deployment such that it should be able to revert back to the old application with

Ruby if the new deployment starts adversely impacting the existing customers? Choose the correct answer from the options below

✓ Create a new stack that contains a new layer with the Python code. Route only a small portion of the production traffic to use the new deployment stack. Once the application is validated, slowly increase the production traffic to the new stack using the Blue Green Deployment. Revert to the old stack, if the new stack deployment fails or does not work.
Explanation:-It deploys the new stack via the Blue/Green deployment method where the new stack is tested only on a small portion production traffic first. If the new deployment has any errors it reverses back to the old deployment stack.
● Update the existing host instances of the application with the new Python code. This will save the cost of having to maintain two stacks, hence cutting down on the costs.
● Create a new stack that contains the Python application code. Route all the traffic to the new stack at once so that all the customers get to access the updated application.
● Create a new stack that contains the Python application code and manages separate deployments of the application via the secondary stack using the deploy lifecycle action to implement the application code.

Q32)

A company is running a MySQL RDS instance inside AWS; however, a new requirement for disaster recovery is keeping a read replica of the production RDS instance in an on-premise data center.

What is the securest way of performing this replication? Choose the correct answer from the options below

✓ Create an IPSec VPN connection using either OpenVPN or VPN/VGW through the Virtual Private Cloud service.
Explanation:-It is feasible to setup the secure IPSec VPN connection between the on premise server and AWS VPC using the VPN/Gateways.
● Create a Data Pipeline that exports the MySQL data each night and securely downloads the data from an S3 HTTPS endpoint.
● Configure the RDS instance as the master and enable replication over the open internet using a secure SSL endpoint to the on-premise server.
● RDS cannot replicate to an on-premise database server. Instead, first configure the RDS instance to replicate to an EC2 instance with core MySQL, and then configure replication over a secure VPN/VPG connection.

Q33)

You have acquired a new contract from a client to move all of his existing infrastructures onto AWS.

You notice that he is running some of his applications using multicast, and he needs to keep it running as such when it is migrated to AWS.

You discover that multicast is not available on AWS, as you cannot manage multiple subnets on a single interface on AWS and a subnet can only belong to one availability zone.

Which of the following would enable you to deploy legacy applications on AWS that require multicast? Choose the correct answer from the options below

● Create all the subnets on a different VPC and use VPC peering between them.
● Provide Elastic Network Interfaces between the subnets.
● All of the answers listed will help in deploying applications that require multicast on AWS.
✓ Create a virtual overlay network that runs on the OS level of the instance.
Explanation:-overlay multicast is a method of building IP level multicast across a network fabric supporting unicast IP routing, such as Amazon Virtual Private Cloud (Amazon VPC).

Q34)

You are setting up a website for a small company. This website serves up images and is very resource intensive.

You have decided to serve up the images using Cloudfront.

There is a requirement though, that the content should be served up using a custom domain and should work with https.

What can you do to ensure this requirement is fulfilled?

● You must provision and configure an ALIAS in Route 53 and associate it to your CloudFront distribution
● You must create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket where the images are stored.
● You must provision and configure your own SSL certificate in Route 53 and associate it to your CloudFront distribution.
✓ You must provision and configure your own SSL certificate in IAM and associate it to your CloudFront distribution.
Explanation:-Third party/custom SSL certificate can be associated with CloudFront using IAM or ACM.

Q35)

Your company asked you to create a mobile application.

The application is built to work with DynamoDB as the backend and Javascript as the frontend.

During the usage of the application, you notice that there are spikes in the application, especially in the DynamoDB area.

Which option provides the most cost-effective and scalable architecture for this application? Choose an answer from the options below.

● Launch DynamoDB in Multi-AZ configuration with a global index to balance writes
● Increase write capacity of Dynamo db to meet the peak loads
✓ Create a service that pulls SQS messages and writes these to DynamoDB to handle sudden spikes in dynamo db
Explanation:-When the idea comes to scalability then SQS is the best option. Normally DynamoDB is scalable, but since one is looking for a cost-effective solution, the messaging in SQS can assist in managing the situation mentioned in the question. You can only adjust the provisioned capacity as needed. SQS is a scalable and very cost effective solution where it can store the data as messages in a queue for DynamoDB to be processed later when it has the sufficient capacity. This way the application would not lose any data due to sudden increase in the traffic.

● Autoscale Dynamo db to meet the requirements

Q36)

You're building a mobile application game. The application needs permission for each user to communicate and store data in DynamoDB tables.

What is the best method for granting each mobile device (that installs your application) to access DynamoDB tables for storage when required? Choose the correct answer from the options below

● During the install and game configuration process, have each user create an IAM credential and assign the IAM user to a group with proper permissions to communicate with DynamoDB.

● Create an IAM group that gives access to your application and to the DynamoDB tables. Then, when writing to DynamoDB, simply include the unique device ID to associate the data with that specific user.

✓ Create an IAM role with the proper permission policy to communicate with the DynamoDB table. Use web identity federation, which assumes the IAM role using AssumeRoleWithWebIdentity, when the user signs in, granting temporary security credentials using STS.

Explanation:-It (a) creates an IAM Role with the needed permissions to connect to DynamoDB, (b) it authenticates the users with Web Identity Federation, and (c) the application accesses the DynamoDB with temporary credentials that are given by STS.

● Create an Active Directory server and an AD user for each mobile application user. When the user signs in to the AD sign-on, allow the AD server to federate using SAML 2.0 to IAM and assign a role to the AD user which is the assumed with AssumeRoleWithSAML.

Q37) What does the below cloud formation template achieve when created as a custom policy. { "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": ["ec2:TerminateInstances", "ec2:StartInstances", "ec2:RunInstances", "ec2:StopInstances"], "Resource": "arn:aws:ec2:*:*:instance/*" }, { "Sid": "VisualEditor1", "Effect": "Allow", "Action": "ec2:DescribeInstances", "Resource": "*" }] }

● Permits the user to launch a new instance as well as start, stop, and terminate the existing instances.

● None of these.

● Permits the user to only describe the instances (read only), and will not be able to start, stop, or terminate instances, since it overrides the allowed actions of TerminateInstances, RunInstances, StartInstances, and StopInstances in the policy.

✓ Permits the user start, stop, and terminate the existing instances.

Explanation:-Although the policy given in the question allows the access to launch the EC2 instance by including "ec2:RunInstances" in the Actions, it will not allow the user to launch the EC2 instances. (Try creating the same policy, attach it to a new user. You can login using that user credentials and see if you can launch any EC2 instance. You will not be able to do so. You will get the error shown below.). In order to allow users to launch an instance, the policy needs to be updated to grant the user more privileges: access to launch using an EC2 key pair, a security group, an Elastic Block Store (EBS) volume, and an Amazon Machine Image (AMI). To do this, you will have to create a separate statement for the RunInstances action.

Q38)

After configuring a whole site CDN on CloudFront you receive the following error:

This distribution is not configured to allow the HTTP request method that was used for this request. The distribution supports only cachable requests.

What is the most likely cause of this? Choose the correct answer from the options below

● The CloudFront distribution is configured to the wrong origin

● Allowed HTTP methods on that specific origin is only accepting GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

✓ Allowed HTTP methods on that specific origin is only accepting GET, HEAD

Explanation:-When the CloudFront Distribution supports only "cacheable requests", it means that it supports only GET and HEAD HTTP requests (read only). For the HTTP requests such as OPTIONS, PUT, POST, PATCH AND DELETE, the CloudFront will give an error "The distribution supports only cacheable requests".

● Allowed HTTP methods on that specific origin is only accepting GET, HEAD, OPTIONS

Q39)

A company is designing a high availability solution for a customer. This customer requires that their application needs to be able to handle an unexpected amount of load and allow site visitors to read data from a DynamoDB table, which contains the results of an online polling system.

Given this information, what would be the best and most cost-saving method for architecting and developing this application? Choose the correct answer from the options below

● Create a Lamba script, which pulls the most recent DynamoDB polling results and creates a custom HTML page, inside of Amazon S3 and use CloudFront and Route 53 to serve the static website.

● Deploy an Auto Scaling application with Elastic Load Balancer pointing to EC2 instances that use a server-side SDK to communicate with the DynamoDB table.

✓ Use the JavaScript SDK and build a static HTML page, hosted inside of an Amazon S3 bucket; use CloudFront and Route 53 to serve the website, which uses JavaScript client-side language to communicate with DynamoD

Explanation:-(a) to show the polling results, a static HTML page that is stored in S3 bucket is sufficient as well as cost-effective, (b) CloudFront and Route53 are AWS managed services that are highly available and scalable, and (c) it uses the JavaScript to communicate with DynamoDB.

● Create a CloudFront distribution that serves the HTML web page, but send the visitors to an Auto Scaling ELB application pointing to EC2 instances.

Q40)

You're running a financial application on an EC2 instance. Data is stored in the instance is critical and in the event of a failure of an EBS volume, the RTO and RPO are less than 1 minute.

How would you architect this application given the RTO and RPO requirements? Choose the correct answer from the options

below

● Stripe multiple EBS volumes together with RAID 0, which provides fault tolerance on EBS volumes.
● Nothing is required since EBS volumes are durability backed up to additional hardware in the same availability zone.
✓ Mirror the data using RAID 1 configuration, which provides fault tolerance on EBS volumes.
Explanation:-RAID 1 configuration maintains the exact copy of the data (via mirroring) in a backup EBS volume which can be used in case of the failure of the main volume, providing redundancy and fault tolerance. In case of failure, the old EBS volume can quickly be replaced with the backup volume and the RTO and RPO requirement can be met within a minute.
● Write a script to create automated snapshots of the EBS volumes every minute. In the event of failure have an automated script that detects failure and launches a new volume from the most recent snapshot.

Q41)

A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that will occur on AWS.

How can the company meet the auditor's requirements without comprising with the security in the AWS environment? Choose the correct answer from the options below

● The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
● Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
● Create a role that has the required permissions for the auditor.
✓ 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.
Explanation:-You need to enable the CloudTrail logging in order to generate the logs with information about all the activities related to the AWS account and resources. It also creates an IAM user that has permissions to read the logs that are stored in the S3 bucket. More information on AWS CloudTrail 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.

Q42) If one 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

● 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.
● Establish a VPN connection from the VPC to the public S3 endpoint.
✓ Configure a public virtual interface to connect to a public S3 endpoint resource.
Explanation:-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.
● Configure a private virtual interface to connect to the public S3 endpoint via the Direct Connect connection.

Q43)

A company has three consolidated billing accounts; development, staging, and production.

The development account has purchased three reserved instances with instance type of m4.large in Availability Zone us-east-1a.

However, no instance is running on the development account, but has five m4.large instances running in the staging account which is also in Availability Zone 1a.

Who can receive the benefit of the reserved instance pricing? Choose the correct answer from the options below

✓ The reserved instance pricing will be applied to the instances in the staging account because the staging account is running an instance that matches the reserved instance type.
Explanation:-The reserved instance pricing be applied to the staging account as it is part of the Consolidated Billing group and only three EC2 instances will be charged with the reserved instance price. Option D is incorrect because the reserved Consolidated Billing advantage is applied to all the accounts that are linked to the primary account, not just the primary account.
● No account will receive the reservation pricing because the reservation was purchased on the development account and no instances that match the reservation are running in the development account.
● All the instances in all the accounts running the m4.large will receive the pricing even if there is only one reserved instance purchase.
● Only the primary account (the consolidated billing primary account) will receive the discounted pricing if the instance is running in the primary billing account.

Q44)

You're working as a consultant for a company that has a three-tier application. The application layer of this architecture sends over 20Gbps of data per seconds during peak hours to and from Amazon S3.

Currently, you're running two NAT gateways in two subnets to transfer the data from your private application layer to Amazon S3.

You will also need to ensure that the instances receive software patches from a third party repository.

What architecture changes should be made, if any? Choose the correct answer from the options below.

● Remove the NAT gateways and create a VPC S3 endpoint which allows for higher bandwidth throughput as well as tighter security.
● NAT gateways support 10Gbps and two are running: Add a third to a third subnet to allow for any increase in demand.

● NAT gateways support 10Gbps and two are running: No changes are required to improve this architecture.

✓ Keep the NAT gateways and create a VPC S3 endpoint which allows for higher bandwidth throughput as well as tighter security

Explanation:-(a) you can securely connect with S3 via the S3 endpoint, and (2) even though you can connect to S3 endpoint without requiring a NAT gateway, you still need to keep it because the instances in the VPC needs to receive the software patches from the third party repository.

Q45)

You have a massive social networking application which is already deployed on N.Virginia region with around 100 EC2 instances, you want to deploy your application to multiple regions for better availability.

You don't want to handle multiple key pairs and want to reuse existing key pairs for N.Virginia region.

How will you accomplish this?

● Key pair is not a region level concept, all the keys are available globally

● Use copy key command line API to transfer key to different regions

✓ Using import key-pair feature using AWS web console

Explanation:-Import key pair functionality enables migrating an EC2 instance from one region to another and use the same PEM key.

● Copy AMI of your EC2 machine between regions and start an instance from that AMI

Q46)

A new client may use your company to move all their existing Data Center applications and infrastructure to AWS.

This is going to be a huge contract for your company, and you have been handed the entire contract and need to provide an initial scope to this possible new client.

One of the things you notice concerning the existing infrastructure is that it has few legacy applications that you are almost certain will not work on AWS.

Which of the following would be the best strategy to employ regarding the migration of these legacy applications? Choose the correct answer from the options below

● Convince the client to look for another solution by de-commissioning these applications and seeking out new ones that will run on AWS.

● Create two VPCs. One containing all the legacy applications and the other containing all the other applications. Make a connection between them with VPC peering.

● Move the legacy applications onto AWS first, before you build any infrastructure. There is sure to be an AWS Machine Image that can run this legacy application.

✓ Create a hybrid cloud by configuring a VPN tunnel to the on-premises location of the Data Center.

Explanation:-It uses hybrid approach - where the legacy application stays on-premises. It should definitely work as the remaining infrastructure would be on AWS. The communication between the two infrastructures would be taken care by establishing the VPN connection. This is certainly the most viable, time and cost saving solution among the given options.

Q47)

You have recently migrated an application from a customer's on-premise data center to the AWS cloud.

Currently, you're using the ELB to serve traffic to the legacy application. The ELB is also using HTTP port 80 as the health check ping port.

The application is currently responding by returning a website to port 80 when you test the IP address directly.

However, the instance is not registering as healthy even though the appropriate amount of time has passed for the health check to register as healthy.

How might the issue be resolved? Choose the correct answer from the options below

● Change the ELB listener port from HTTP port 80 to HTTPS port 80 for the instance to register as healthy

● Change the ELB listener port from HTTP port 80 to TCP port 443 for the instance to register as healthy

✓ Change the ELB listener port from HTTP port 80 to TCP port 80 for the instance to register as healthy

Explanation:-Since the application is a custom application and not a standard HTTP application, hence you need to have the TCP ports open. Before you start using Elastic Load Balancing, you must configure one or more listeners for your Classic Load Balancer. A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instance) connections. Elastic Load Balancing supports the following protocols: HTTP HTTPS (secure HTTP) TCP SSL (secure TCP)

● Change the ELB listener port from ping port 80 to HTTPS port 80 for the instance to register as healthy

Q48)

You are running an online gaming server, with one of its requirements being a need for 100,000 IOPS of write performance on its EBS volumes.

Given the fact that EBS volumes can only provision a maximum of up to 20,000 IOPS which of the following would be a reasonable solution if instance bandwidth is not an issue? Choose the correct answer from the options below

● Use Auto Scaling to use spot instances when required to increase the IOPS write performance when required.

● Create a Placement Group with five 20,000 IOPS EBS volumes.

✓ Create a RAID 0 configuration for five 20,000 IOPS EBS volumes.

Explanation:-Creating a RAID 0 array allows you to achieve a higher level of performance for a file system than you can provision on a single Amazon EBS volume and the resulting size of a RAID 0 array is the sum of the sizes of the volumes within it, and the bandwidth is the sum of the available bandwidth of the volumes within it.

● Use ephemeral storage which gives a much larger IOPS write performance.

Q49)

A company is running a production load Redshift cluster for a client. The client has an RTO objective of one hour and an RPO of one day.

While configuring the initial cluster what configuration would best meet the recovery needs of the client for this specific Redshift cluster configuration? Choose the correct answer from the options below

● Create the cluster configuration and enable Redshift replication from the cluster running in the primary region to the cluster running in the secondary region. In the event of a disaster, change the DNS endpoint to the secondary cluster's leader node.
● Enable automatic snapshots on the cluster in the production region FROM the disaster recovery region so snapshots are available in the disaster recovery region and can be launched in the event of a disaster.
● Enable automatic snapshots on a Redshift cluster. In the event of a disaster, a failover to the backup region is needed. Manually copy the snapshot from the primary region to the secondary region.
✓ Enable automatic snapshots and configure automatic snapshot copy from the current production cluster to the disaster recovery region.
Explanation:-It copies the snapshot from source region (production) to the destination region (disaster recovery region).

Q50)

You are maintaining an application that is spread across multiple web servers and has incoming traffic balanced by ELB. The application allows users to upload pictures.

Currently, each web server stores the image and a background task synchronizes the data between servers.

However, the synchronization task can no longer keep up with the number of images uploaded.

What change could you make so that all web servers have a place to store and read images at the same time? Choose an answer from the below options:

● Store the images on Amazon EBS
● Store the images on the ELB
● Store the images on Amazon Cloudfront
✓ Store the images in Amazon S3
Explanation:-Amazon Simple Storage Service is storage for the Internet. It is designed to make web-scale computing easier for developers. Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of websites. The service aims to maximize benefits of scale and to pass those benefits on to developers.