Answer Sheet

Q1)

You have created an Elastic Load Balancer with Duration-Based sticky sessions enabled in front of your six EC2 web application instances in US-West-2.

For High Availability, there are three web application instances in Availability Zone 1 and three web application instances in Availability Zone 2.

To load test, you set up a software-based load tester in Availability Zone 2 to send traffic to the Elastic Load Balancer, as well as letting several hundred users browse to the ELB’s hostname. After a while, you notice that the users’ sessions are spread evenly across the EC2 instances in both AZ’s, but the software-based load tester’s traffic is hitting only the instances in Availability Zone 2.

What steps can you take to resolve this problem? Choose the 2 correct answer from the options below:

✓ Use a third party load-testing service to send requests from globally distributed clients.
Explanation:-"If you do not ensure that DNS is re-resolved or use multiple test clients to simulate increased load, the test may continue to hit a single IP address when Elastic Load Balancing has actually allocated many more IP addresses. Because your end users will not all be resolving to that single IP address, your test will not be a realistic sampling of real-world behavior.”
● Create a software-based load tester in US-East-1 and test from there.
✓ Force the software-based load tester to re-resolve DNS before every request.
Explanation:-"If you do not ensure that DNS is re-resolved or use multiple test clients to simulate increased load, the test may continue to hit a single IP address when Elastic Load Balancing has actually allocated many more IP addresses. Because your end users will not all be resolving to that single IP address, your test will not be a realistic sampling of real-world behavior.”
● Switch to Application-Controlled sticky sessions.

Q2)

You are running a news website in the EU-west-1 region that updates every 15 minutes. The website has a worldwide audience.

It uses an Auto Scaling group behind an Elastic Load Balancer and an Amazon RDS database. Static content resides on Amazon S3 and is distributed through Amazon CloudFront.

Your Auto Scaling group is set to trigger a scale up event at 60% CPU utilization, you use an Amazon RDS extra large DB instance with 10,000 Provisioned IOPS. Its CPU utilization is around 80%. While freeable memory is in the 2 GB range.

Web analytics reports show that the average load time of your web pages is around 1.5 to 2 seconds but your SEO consultant wants to bring down the average load time to under 0.5 seconds.

How would you improve page load times for your users? Choose 3 options from the below

✓ Switch Amazon RDS database to the high memory extra-large Instance type
Explanation:-In this scenario, there are major points of consideration: (1) news website updtes every 15 minutes, (2) current average load time is high, and (3) the performance of the use of the website should be improved (i.e. read performance needs improvement). When the questions asks for performance improving solution for read heavy application, always see if any of the options contain caching solution such as ElastiCache, CloudFront, or Read Replicas. scaling up the RDS instance helps improving its read and write performance.
● Set up a second installation in another region, and use the Amazon Route 53 latency-based routing feature to select the right region.
✓ Add an Amazon ElastiCache caching layer to your application for storing sessions and frequent DB queries
Explanation:-In this scenario, there are major points of consideration: (1) news website updtes every 15 minutes, (2) current average load time is high, and (3) the performance of the use of the website should be improved (i.e. read performance needs improvement). When the questions asks for performance improving solution for read heavy application, always see if any of the options contain caching solution such as ElastiCache, CloudFront, or Read Replicas. it uses ElastiCache for storing sessions as well as frequent DB queries; hence reducing the load on the database. This should help increasing the read performance.
✓ Configure Amazon CloudFront dynamic content support to enable caching of re-usable content from your site
Explanation:-In this scenario, there are major points of consideration: (1) news website updtes every 15 minutes, (2) current average load time is high, and (3) the performance of the use of the website should be improved (i.e. read performance needs improvement). When the questions asks for performance improving solution for read heavy application, always see if any of the options contain caching solution such as ElastiCache, CloudFront, or Read Replicas. it uses CloudFront which is a network of globally distributed "edge-locations" that caches the content and improves the user experience.
● Lower the scale up trigger of your Auto Scaling group to 30% so it scales more aggressively.

Q3) A company wants to integrate their AD on-premise with the AWS services. They specifically want to set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? Choose 3 answers from the below options:

● Tagging each folder in the bucket.
● Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket.
✓ Setting up a federation proxy or identity provider.
✓ Using AWS Security Token Service to generate temporary tokens.
✓ Configuring IAM role.

Q4) Which of the following can be done by Auto scaling? Choose 2 answers from the options given below:

✓ Start up EC2 instances when CPU utilization is above threshold.
Explanation:-As per the AWS documentation, below is what can be done with Auto Scaling. You can only scale horizontally and not vertically. Scale-out Amazon EC2 instances seamlessly and automatically when demand increases. Shed unneeded Amazon EC2 instances automatically and save money when demand subsides. Scale dynamically based on your Amazon CloudWatch metrics, or predictably according to a schedule that you define. Replace unhealthy or unreachable instances to maintain the higher availability of your applications. Receive notifications via Amazon Simple Notification Service (Amazon SNS) to be alerted when you use Amazon CloudWatch alarms to initiate Auto Scaling actions, or when Auto Scaling

completes an action. Run On-Demand or Spot Instances, including those inside your virtual private cloud (VPC) or high performance computing (HPC) clusters. If you're signed up for the Amazon EC2 service, you're already registered to use Auto Scaling and can begin using the feature via the API or command line interface.

● Increase the instance size when utilization is above threshold.
● Decrease the instance size when utilization is below threshold.
✓ Release EC2 instances when CPU utilization is below threshold.

Explanation:-As per the AWS documentation, below is what can be done with Auto Scaling. You can only scale horizontally and not vertically. Scale-out Amazon EC2 instances seamlessly and automatically when demand increases. Shed unneeded Amazon EC2 instances automatically and save money when demand subsides. Scale dynamically based on your Amazon CloudWatch metrics, or predictably according to a schedule that you define. Replace unhealthy or unreachable instances to maintain the higher availability of your applications. Receive notifications via Amazon Simple Notification Service (Amazon SNS) to be alerted when you use Amazon CloudWatch alarms to initiate Auto Scaling actions, or when Auto Scaling completes an action. Run On-Demand or Spot Instances, including those inside your virtual private cloud (VPC) or high performance computing (HPC) clusters. If you're signed up for the Amazon EC2 service, you're already registered to use Auto Scaling and can begin using the feature via the API or command line interface.

Q5) What are the steps that get carried out by Opswork when you attach a loadbalancer to a layer in Opswork? Choose 3 options from the below:

✓ Automatically activates and deactivates the instances' Availability Zones.
✓ Automatically registers the layer's instance's when they come online and deregisters instances when they leave the online state, including load-based and time-based instances.
● Terminates the EC2 Instances.
✓ Deregisters any currently registered instances.

Q6)

You have an application running on an EC2 Instance access an S3 bucket.

How should the application use AWS credentials to access the S3 bucket securely?

● Create an IAM user for the application with permissions that allow list access to the S3 bucket. The application retrieves the IAM user credentials from a temporary directory with permissions that allow read access only to the application user.
✓ Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata

Explanation:-An IAM role is similar to a user. In that, it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user. You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. Whenever the question presents you with a scenario where an application, user, or service wants to access another service, always prefer creating IAM Role over IAM User. The reason being that when an IAM User is created for the application, it has to use the security credentials such as access key and secret key to use the AWS resource/service. This has security concerns. Whereas, when an IAM Role is created, it has all the necessary policies attached to it. So, the use of access key and secret key is not needed. This is the preferred approach. Option A is incorrect because you should not use the account access keys , instead you should use the IAM Role. Option B is incorrect because instead of IAM User, you should use the IAM Role. See the given above. Option C is CORRECT because, (a) it creates the IAM Role with appropriate permissions, and (b) the application accesses the AWS Resource using that role. Option D is incorrect because instead of IAM User, you should use the IAM Role. See the given above. For more information on IAM roles, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html The correct answer is: Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata

● Use the AWS account access Keys. The application retrieves the credentials from the source code of the application.
● Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application. Create a new access and secret key for the user and provide these credentials to the SaaS provider.

Q7)

A media company produces new video files on-premises every day with a total size of around 100GB after compression. All files have a size of 1 -2 GB and need to be uploaded to Amazon S3 every night in a fixed time window between 3 AM and 5 AM.

Current upload takes almost 3 hours, although less than half of the available bandwidth is used.

What step(s) would ensure that the file uploads are able to complete in the allotted time window?

● Pack all files into a single archive, upload it to S3, and then extract the files in AWS
✓ Upload the files in parallel to S3
● Increase your network bandwidth to provide faster throughput to S3
● Use AWS Import/Export to transfer the video files

Q8) Which of the below-mentioned methods is the best to stop a series of attacks coming from a set of determined IP ranges?

● Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)
● Change the EIP (Elastic IP Address) of the NAT instance in the web tier subnet and update the Main Route Table with the new EIP
● Create 15 Security Group rules to block the attacking IP addresses over port 80
✓ Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses

Explanation:-In this scenario, the attack is coming from a set of certain IP addresses over specific port from a specific country. You are supposed to defend against this attack. In such questions, always think about two options: Security groups and Network Access Control List (NACL). Security Groups operate at the individual instance level, whereas NACL operates at subnet level. You should always fortify the NACL first, as it is encounter first during the communication with the instances in the VPC. Option A is incorrect because IP addresses cannot be blocked using route table or IGW. Option B is incorrect because changing the EIP of NAT instance cannot block the incoming traffic from a particular IP address. Option C is incorrect because (a) you cannot deny port access using security groups, and (b) by default all requests are denied; you open access for particular IP address or range. You cannot deny access for particular IP addresses using security groups. Option D is CORRECT because (a) you can add deny rules in NACL and block access to certain IP addresses. See an example below: The correct answer is: Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses

Q9)

You have an application running on an EC2 Instance accesses an SQS queue.

How should the application use AWS credentials to access the SQS queue securely?

● Create an IAM user for the application with permissions that allows access to the SQS queue. The application retrieves the IAM user credentials from a temporary directory with permissions that allow access only to the application user.
✅ Create an IAM role for EC2 that allows access to the SQS queue. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata
Explanation:-An IAM role is similar to a user. In that, it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user. You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. Whenever the question presents you with a scenario where an application, user, or service wants to access another service, always prefer creating IAM Role over IAM User. The reason being that when an IAM User is created for the application, it has to use the security credentials such as access key and secret key to use the AWS resource/service. This has security concerns. Whereas, when an IAM Role is created, it has all the necessary policies attached to it. So, the use of access key and secret key is not needed. This is the preferred approach. Option A is incorrect because you should not use the account access keys , instead you should use the IAM Role. Option B is incorrect because instead of IAM User, you should use the IAM Role. See the given above. Option C is CORRECT because, (a) it creates the IAM Role with appropriate permissions, and (b) the application accesses the AWS Resource using that role. Option D is incorrect because instead of IAM User, you should use the IAM Role. See the given above. For more information on IAM roles, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html The correct answer is: Create an IAM role for EC2 that allows access to the SQS queue. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata
● Use the AWS account access Keys the application retrieves the credentials from the source code of the application.
● Create an IAM user for the application with permissions that allow access to the SQS queue launch the instance as the IAM user and retrieve the IAM user's credentials from the EC2 instance user data

Q10) Which of the following cache engines does Amazon Elastic Cache Support?

● Memcache Only
● Redis Only
● Wincache and Redis
✅ Memcache and Redis
Explanation:-AWS Elastic cache has support for the following: Redis - a fast, open source, in-memory data store, and cache. Amazon ElastiCache for Redis is a Redis-compatible in-memory service that delivers the ease-of-use and power of Redis along with the availability, reliability, and performance suitable for the most demanding applications. Both single-node and up to 15-shard clusters are available, enabling scalability to up to 3.55 TiB of in-memory data. ElastiCache for Redis is fully managed, scalable, and secure - making it an ideal candidate to power high-performance use cases such as Web, Mobile Apps, Gaming, Ad-Tech, and IoT. Memcached - a widely adopted memory object caching system. ElastiCache is protocol-compliant with Memcached, so popular tools that you use today with existing Memcached environments will work seamlessly with the service. For more information on Elastic cache, please refer to the below link https://aws.amazon.com/elasticache/ The correct answer is: Memcache and Redis

Q11)

You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site.

At some point you find out that other sites have been linking to the photos on your site, causing loss to your business.

What is an effective method to mitigate this? Choose the correct answer from the below options:

● Store photos on an EBS volume of the web server.
✅ Remove public read access and use signed URLs with expiry dates.
Explanation:-You can distribute private content using a signed URL that is valid for only a short time—possibly for as little as a few minutes. Signed URLs that are valid for such a short period are good for distributing content on-the-fly to a user for a limited purpose, such as distributing movie rentals or music downloads to customers on demand. Option A is incorrect because using CloudFront is an expensive option compared to using signed URLs. Option B is incorrect because the website is hosted on S3. Option C is CORRECT because, as mentioned above, it will ensure that only the trusted/authenticated users get access to the content. Option D is incorrect because the website is hosted on S3 which does not have any security group setting. For more information on Signed URL's please visit the below link http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html The correct answer is: Remove public read access and use signed URLs with expiry dates.
● Use CloudFront distributions for static content.
● Block the IPs of the offending websites in Security Groups.

Q12)

An organization is generating digital policy files which are required by the admins for verification.

Once the files are verified they may not be required in the future unless there is some compliance issue.

Which is the best possible solution if the organization wants to save them in a cost-effective way?

● AWS RRS
● AWS S3
● AWS RDS
✅ AWS Glacier
Explanation:-This question is basically asking you to choose a cost-effective archival solution. Amazon Glacier is most suited for such scenarios.

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. With Amazon Glacier, customers can reliably store their data for as little as $0.004 per gigabyte per month. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so that they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations. Option A and B are incorrect because they are used for real time storage. Option C is incorrect because this is a database service not an archival one. Option D is , as mentioned above, CORRECT. For more information on Glacier please visit the link – https://aws.amazon.com/glacier/details/ The correct answer is: AWS Glacier

Q13)

An application, basically a mobile application needs access for each user to store data in a DynamoDB table.

What is the best method for granting each mobile device that ensures the application has access DynamoDB tables for storage when required? Choose the correct options from the below:

● 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.
✓ 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.
● 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 only 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.

Q14) A company is running a MySQL RDS instance inside of 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 option from the below:

● Create an IPSec VPN connection using either OpenVPN or VPN/VGW through the Virtual Private Cloud service.
✓ Create a Data Pipeline that exports the MySQL data each night and securely downloads the data from an S3 HTTPS endpoint.
● 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.
● Configure the RDS instance as the master and enable replication over the open internet using a secure SSL endpoint to the on-premise server.

Q15) Which of the following are the ways to minimize the attack surface area as a DDOS minimization strategy in AWS? Choose 3 options from the below:

✓ Eliminate non-critical Internet entry points.
Explanation:-Some important consideration when architecting on AWS is to limit the opportunities that an attacker may have to target your application. For example, if you do not expect an end user to directly interact with certain resources you will want to make sure that those resources are not accessible from the Internet. Similarly, if you do not expect end-users or external applications to communicate with your application on certain ports or protocols, you will want to make sure that traffic is not accepted. This concept is known as attack surface reduction. Option A is incorrect because it is used for mitigating the DDoS attack where the system scales to absorb the application layer traffic in order to keep it responsive. Option B, C and D are all CORRECT as they all are used for reducing the DDoS attack surface. For more information on DDoS attacks in AWS, please visit the below URL https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf The correct answers are: Reduce the number of necessary Internet entry points., Separate end user traffic from management traffic., Eliminate non-critical Internet entry points.
✓ Separate end user traffic from management traffic.
Explanation:-Some important consideration when architecting on AWS is to limit the opportunities that an attacker may have to target your application. For example, if you do not expect an end user to directly interact with certain resources you will want to make sure that those resources are not accessible from the Internet. Similarly, if you do not expect end-users or external applications to communicate with your application on certain ports or protocols, you will want to make sure that traffic is not accepted. This concept is known as attack surface reduction. Option A is incorrect because it is used for mitigating the DDoS attack where the system scales to absorb the application layer traffic in order to keep it responsive. Option B, C and D are all CORRECT as they all are used for reducing the DDoS attack surface. For more information on DDoS attacks in AWS, please visit the below URL https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf The correct answers are: Reduce the number of necessary Internet entry points., Separate end user traffic from management traffic., Eliminate non-critical Internet entry points.
● Configure services such as Elastic Load Balancing and Auto Scaling to automatically scale.
✓ Reduce the number of necessary Internet entry points.
Explanation:-Some important consideration when architecting on AWS is to limit the opportunities that an attacker may have to target your application. For example, if you do not expect an end user to directly interact with certain resources you will want to make sure that those resources are not accessible from the Internet. Similarly, if you do not expect end-users or external applications to communicate with your application on certain ports or protocols, you will want to make sure that traffic is not accepted. This concept is known as attack surface reduction. Option A is incorrect because it is used for mitigating the DDoS attack where the system scales to absorb the application layer traffic in order to keep it responsive. Option B, C and D are all CORRECT as they all are used for reducing the DDoS attack surface. For more information on DDoS attacks in AWS, please visit the below URL https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf The correct answers are: Reduce the number of necessary Internet entry points., Separate end user traffic from management traffic., Eliminate non-critical Internet entry points.

Q16) Which of the following features ensures even distribution of traffic to Amazon EC2 instances in multiple Availability Zones registered with a load balancer?

✓ Elastic Load Balancing cross-zone load balancing
● An Amazon Route 53 weighted routing policy
● Elastic Load Balancing request routing
● An Amazon Route 53 latency routing policy

Q17)

A customer is deploying an SSL enabled Web application on AWS and would like to implement a separation of roles between the EC2 service administrators that are entitled to login to Instances as well making API calls and the security officers who will maintain and have exclusive access to the application's X.509 certificate that contains the private key.

Which configuration option would satisfy the above requirements?

● Configure the web servers to retrieve the certificate upon boot from an CloudHSM that is managed by the security officers.
● Upload the certificate on an S3 bucket owned by the security officers and accessible only by the EC2 role of the web servers
● Configure system permissions on the web servers to restrict access to the certificate only to the authorized security officers.
✓ Configure IAM policies authorizing access to the certificate store only to the security officer's and terminate SSL on the ELB.

Q18)

A web application is currently hosted on an on-premise location. There is ad-campaign underway and there is a probability that the influx of traffic on the website is going to increase.

The company does not have the time to migrate this application to AWS.

Which scenario below will provide full site functionality, while helping to improve the ability of your application to take the influx of traffic in the short timeframe required?

● Migrate to AWS because this is the only option. Use VM import ‘Export to quickly convert an on-premises web server to an AMI create an Auto Scaling group which uses the imported AMI to scale the web tier based on incoming traffic.
● Create an S3 bucket and configure it tor website hosting. Migrate your DNS to Route53 using zone import and leverage Route53 DNS failover to failover to the S3 hosted website.
● Create an AMI which can be used of launch web servers in EC2. Create an Auto Scaling group which uses the AMI’s to scale the web tier based on incoming traffic. Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted in AWS.
✓ Offload traffic from on-premises environment by setting up a CloudFront distribution and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behaviour and select a TTL that objects should exist in cache.
Explanation:-In this scenario, the major points of consideration are: (1) your application may get unpredictable bursts of traffic, (b) you need to improve the current infrastructure in shortest period possible, and (3) your web servers are on premise. Since the time period in hand is short, instead of migrating the app to AWS, you need to consider different ways where the performance would improve without doing much modification to the existing infrastructure. Option A is CORRECT because (a) CloudFront is AWS’s highly scalable, highly available content delivery service, where it can perform excellently even in case of sudden unpredictable burst of traffic, (b) the only change you need to make is make the on-premises load balancer as the custom origin of the CloudFront distribution. Option B is incorrect because you are supposed to improve the current situation in shortest time possible. Migrating to AWS would be more time consuming than simply setting up the CloudFront distribution. Option C is incorrect because you cannot host dynamic web sites on S3 bucket. Also, this option provides insufficient infrastructure set up options. Option D is incorrect because ELB cannot do balancing between AWS EC2 instances and on-premise instances. More information on CloudFront: You can have CloudFront sit in front of your on-premise web environment, via a custom origin. This would protect against unexpected bursts in traffic by letting CloudFront handle the traffic from the cache, thus removing some of the load from the on-premise web servers. Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long-term. commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations. If you have dynamic content, then it is best to have the TTL set to 0. For more information on CloudFront, please visit the below URL: https://aws.amazon.com/cloudfront/ The correct answer is: Offload traffic from on-premises environment by setting up a CloudFront distribution and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behaviour and select a TTL that objects should exist in cache.

Q19)

You are designing an application and are considering how to mitigate distributed denial-of-service (DDoS) attacks.

Which of the below are viable mitigation techniques? Choose 3 options from the below:

✓ Add alert Amazon CloudWatch to look for high Network in and CPU utilization.
Explanation:-This question is asking you to select some of the most recommended and widely used DDoS mitigation techniques. What is a DDoS Attack? A Distributed Denial of Service (DDoS) attack is an attack orchestrated by distributed multiple sources that makes your web application unresponsive and unavailable for the end users. DDoS Mitigation Techniques Some of the recommended techniques for mitigating the DDoS attacks are (i) build the architecture using the AWS services and offerings that have the capabilities to protect the application from such attacks. e.g. CloudFront, WAF, Autoscaling, Route53, VPC etc. (ii) defend the infrastructure layer by over-provisioning capacity, and deploying DDoS mitigation systems. (iii) defend the application layer by using WAF, and operating at scale by using autoscale so that the application can withstand the attack by scaling and absorbing the traffic. (iv) minimizing the surface area of attack (v) obfuscating the AWS resources Option A is incorrect because ENIs do not help in increasing the network bandwidth. Option B is incorrect because having dedicated instances performing at maximum capacity will not help mitigating the DDoS attack. What is needed is instances behind auto-scaling so that the traffic can be absorbed while actions are being taken on the attack and the application can continue responding to the clients. Option C is CORRECT because (a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming from IPs from specific location, such requests can be blocked. Option D is CORRECT because (a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack. Option E is CORRECT because CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities. Option F is incorrect because adding and removing rules of firewall is not going to mitigate the DDoS attack. It is very important to read the AWS Whitepaper on Best Practices for DDoS Resiliency. https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf The correct answers are: Use an Amazon CloudFront distribution for both static and dynamic content., Use an Elastic Load Balancer with auto scaling groups at the web, App tiers; also use Amazon Relational Database Service (RDS) , Add alert Amazon CloudWatch to look for high Network in and CPU utilization.
✓ Use an Elastic Load Balancer with auto scaling groups at the web, App tiers; also use Amazon Relational Database Service (RDS)
Explanation:-This question is asking you to select some of the most recommended and widely used DDoS mitigation techniques. What is a DDoS Attack? A Distributed Denial of Service (DDoS) attack is an attack orchestrated by distributed multiple sources that makes your web application unresponsive and unavailable for the end users. DDoS Mitigation Techniques Some of the recommended techniques for mitigating the DDoS attacks are (i) build the architecture using the AWS services and offerings that have the capabilities to protect the application from such attacks. e.g. CloudFront, WAF, Autoscaling, Route53, VPC etc. (ii) defend the infrastructure layer by over-provisioning capacity, and deploying DDoS mitigation systems. (iii) defend the application layer by using WAF, and operating at scale by using autoscale so that the application can withstand the attack by scaling and absorbing the traffic. (iv) minimizing the surface area of attack (v) obfuscating the AWS resources Option A is incorrect because ENIs do not help in increasing the network bandwidth. Option B is incorrect because having dedicated instances performing at maximum capacity will not help mitigating the DDoS attack. What is needed is instances behind auto-scaling so that the traffic can be absorbed while actions are being taken on the attack and the application can continue responding to the clients. Option C is CORRECT because (a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming

from IPs from specific location, such requests can be blocked. Option D is CORRECT because (a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack. Option E is CORRECT because CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities. Option F is incorrect because adding and removing rules of firewall is not going to mitigate the DDoS attack. It is very important to read the AWS Whitepaper on Best Practices for DDoS Resiliency. https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf The correct answers are: Use an Amazon CloudFront distribution for both static and dynamic content., Use an Elastic Load Balancer with auto scaling groups at the web, App tiers; also use Amazon Relational Database Service (RDS) , Add alert Amazon CloudWatch to look for high Network in and CPU utilization.

● Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
● Use dedicated instances to ensure that each instance has the maximum performance possible.
✓ Use an Amazon CloudFront distribution for both static and dynamic content.

Explanation:-This question is asking you to select some of the most recommended and widely used DDoS mitigation techniques. What is a DDoS Attack? A Distributed Denial of Service (DDoS) attack is an attack orchestrated by distributed multiple sources that makes your web application unresponsive and unavailable for the end users. DDoS Mitigation Techniques Some of the recommended techniques for mitigating the DDoS attacks are (i) build the architecture using the AWS services and offerings that have the capabilities to protect the application from such attacks. e.g. CloudFront, WAF, Autoscaling, Route53, VPC etc. (ii) defend the infrastructure layer by over-provisioning capacity, and deploying DDoS mitigation systems. (iii) defend the application layer by using WAF, and operating at scale by using autoscale so that the application can withstand the attack by scaling and absorbing the traffic. (iv) minimizing the surface area of attack (v) obfuscating the AWS resources Option A is incorrect because ENIs do not help in increasing the network bandwidth. Option B is incorrect because having dedicated instances performing at maximum capacity will not help mitigating the DDoS attack. What is needed is instances behind auto-scaling so that the traffic can be absorbed while actions are being taken on the attack and the application can continue responding to the clients. Option C is CORRECT because (a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming from IPs from specific location, such requests can be blocked. Option D is CORRECT because (a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack. Option E is CORRECT because CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities. Option F is incorrect because adding and removing rules of firewall is not going to mitigate the DDoS attack. It is very important to read the AWS Whitepaper on Best Practices for DDoS Resiliency. https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf The correct answers are: Use an Amazon CloudFront distribution for both static and dynamic content., Use an Elastic Load Balancer with auto scaling groups at the web, App tiers; also use Amazon Relational Database Service (RDS) , Add alert Amazon CloudWatch to look for high Network in and CPU utilization.

Q20)

An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the web server on a single VPC instance such that it allows the internet traffic as well as the back-end management traffic.

The organization wants to make sure that the back end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing web server will have an IP address which can receive traffic from all the internet IPs.

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

● The organization should create 2 EC2 instances as this is not possible with one EC2 instance
✓ The organization should create 2 network interfaces, one for the internet traffic and the other for the backend traffic

Explanation:-An Elastic Network Interface (ENI) is a virtual network interface that you can attach to an instance in a VPC. Network interfaces are available only for instances running in a VPC. A network interface can include the following attributes: A primary private IPv4 address One or more secondary private IPv4 addresses One Elastic IP address (IPv4) per private IPv4 address One public IPv4 address One or more IPv6 addresses One or more security groups A MAC address A source/destination check flag A description See an example below how the route table can be configured to allow the IP based access via multiple ENIs. For more information on ENI , please refer to the below link http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html The correct answer is: The organization should create 2 network interfaces, one for the internet traffic and the other for the backend traffic

● It is not possible to have 2 IP addresses for a single instance
● This is not possible

Q21) Does an AWS Direct Connect location provide access to Amazon Web Services in the region it is associated with, as well as other US regions?

● Incorrect , it only pertains to the region it is associated with
✓ Correct

Explanation:-Correct, this is possible. Please refer to the below link for more information https://aws.amazon.com/about-aws/whats-new/2013/12/19/aws-direct-connect-inter-region/ The correct answer is: Yes

Q22)

You've created a temporary application that accepts image uploads, stores them in S3, and records the information about the images in RDS.

After building this architecture and accepting the images for the duration required, it's time to delete the CloudFormation template.

However, your manager has informed you that, for some reason, they need to ensure that a backup is taken of the RDS when the CloudFormation template is deleted.

Which of the options below will fulfill the above requirement?

● For both the RDS and S3 resource types on the CloudFormation template, set the DeletionPolicy to Retain.
✓ Set the DeletionPolicy on the RDS resource to snapshot.

Explanation:-The main point in this scenario is that even if the CloudFormation stack is deleted there should be a way to able to restore the RDS data if needed. Option A is incorrect because the DeletionPolicy of the RDS instance should be set to snapshot. If delete is used, the resource would get deleted and the dat cannot be restored in the future. Option B is incorrect because DeletionPolicy attribute for RDS should be snapshot, not retain because with snapshot option, the backup of the RDS instance would be stored in the form of snapshots (which is the requirement). With retain option, CF will keep the RDS instance alive which is unwanted. There is such no requirement on S3. Option C is CORRECT because it correctly sets the DeletionPolicy of the RDS to snapshot so that the data can be restored from the snapshot if needed. Option D is incorrect because it sets the DeletionPolicy of the RDS to retain which will keep the RDS instance alive. It just needs to take the snapshot. More information on

DeletionPolicy on CloudFront DeletionPolicy options include: Retain: You retain the resource in the event of a stack deletion. Snapshot: You get a snapshot of the resource before it’s deleted. This option is available only for resources that support snapshots. Delete: You delete the resource along with the stack. This is the default outcome if you don’t set a DeletionPolicy. To keep or copy resources when you delete a stack, you can specify either the Retain or Snapshot policy options. With the DeletionPolicy attribute, you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default. For more information on Cloudformation deletion policy, please visit the below URL http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html The correct answer is: Set the DeletionPolicy on the RDS resource to snapshot.

● Enable S3 bucket replication on the source bucket to a destination bucket to maintain a copy of all the S3 objects, set the deletion policy for the RDS instance to delete.

● Set the DeletionPolicy on the RDS resource to retain.

Q23)

An application runs on-premise as well as on AWS to achieve the minimum recovery time objective(RTO).

Which of the below-mentioned configurations will not meet the requirements of the multi-site solution scenario?

✓ Setup a single DB instance

Explanation:-Running a single DB instance is not ideal for a disaster recovery scenario. For more information on AWS disaster recovery, please refer to the below link https://aws.amazon.com/disaster-recovery/ The correct answer is: Setup a single DB instance

● Keep the application running on-premise and in AWS with full capacity

● Setup weighted DNS service like Route53 to route traffic accross sites

● Configure data replication

Q24) Which is the best option to avoid SQL Injection attacks against your infrastructure in AWS?

● Remove all but TLS 1 & 2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

✓ Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group

Explanation:-In such scenarios where you are designing a solution to prevent the DDoS attack, always think of using Web Access Firewall (WAF). AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns. Option A is incorrect because, although this option could work, the setup is very complex and it not a cost effective solution. Option B is incorrect because, (a) even though blocking certain IPs will mitigate the risk, the attacker could maneuver the IP address and circumvent the IP check by NACL, and (b) it does not prevent the attack from the new source of threat. Option C is CORRECT because (a) WAF Tiers acts as the first line of defense, it filters out the known sources of attack and blocks common attack patterns, such as SQL injection or cross-site scripting, (b) the ELB of the application is not exposed to the attack, and most importantly (c) this pattern - known as "WAF Sandwich" pattern - has WAF layer with EC2 instances are placed between two ELBs - one that faces the web, receives all the traffic, and sends them to WAF layer to filter out the malicious requests, and sends the filtered non-malicious requests, another ELB - which receives the non-malicious requests and send them to the EC2 instances for processing. See the image below: Option D is incorrect because there is no such thing as Advanced Protocol Filtering feature for ELB. For more information on WAF, please visit the below URL: https://aws.amazon.com/waf/ The correct answer is: Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group

● Create a DirectConnect connection so that your have a dedicated connection line.

● Create NACL rules for the subnet hosting the application

Q25) A company wants to utilize AWS storage. For them low storage cost is paramount, the data is rarely retrieved, and data retrieval times of several hours are acceptable for them. What is the best storage option to use?

● Reduced Redundancy Storage

✓ Glacier

Explanation:-With the above requirements, the best option is to opt for Amazon Glacier. Please refer to the Glacier FAQ’s https://aws.amazon.com/glacier/faqs/ The correct answer is: Glacier

● EBS backed storage connected to EC2

● Cloud Front

Q26)

You have large EC2 instances in your AWS infrastructure which you have recently setup. These instances carry out the task of creating JPEG files and store them on a S3 bucket and occasionally need to perform high computational tasks.

After close monitoring you see that the CPUs of these instances remain idle most of the time.

Which of the below solutions will ensure better utilization of resources?

● Ensure the application hosted on the EC2 instances uses larger files on S3 to handle more load.

✓ Use T2 instances if possible.

Explanation:-In this scenario the problem is that the large EC2 instances are mostly remaining unused. Hence, the solution should be to use instances that can cost less but still be able to carry out occasional high computational tasks. T2 instances are Burstable Performance Instances that provide a baseline level of CPU performance with the ability to burst above the baseline. The baseline performance and ability to burst are governed by CPU Credits. T2 instances accumulate CPU Credits when they are idle, and consume CPU Credits when they are active. T2 instances are the lowest-cost Amazon EC2 instance option designed to dramatically reduce costs for applications that benefit from the ability to burst to full core performance whenever required. Option A is incorrect because there is no issue with the current use of S3. Option B is incorrect because adding another large instance is, on the contrary, an expensive solution and would add to the existing cost. Option C is CORRECT because T2 instances are cost-effective and also provide a baseline level of CPU performance with the ability to burst above the baseline whenever required. Option D is incorrect because this option is not going to make efficient use of the current instances. It will not lower the cost of the architecture. For more information on Instances types, please visit the below URL: https://aws.amazon.com/ec2/instance-types/t2/

● Use Amazon glacier instead of S3.
● Add additional large instances by introducing a task group.

Q27)

You decide to configure a bucket for static website hosting. As per the AWS documentation, you create a bucket named 'mybucket.com' and then you enable website hosting with an index document of 'index.html' and you leave the error document as blank.

You then upload a file named 'index.html' to the bucket.

After clicking on the endpoint of mybucket.com.s3-website-us-east-1.amazonaws.com you receive 403 Forbidden error.

You then change the CORS configuration on the bucket so that everyone has access, however, you still receive the 403 Forbidden error.

What additional step do you need to do so that the endpoint is accessible to everyone? Choose the correct option from the below:

● Register mybucket.com on Route53
● Wait for the DNS change to propagate
● You need to add a name for the error document, because it is a required field
✓ Change the permissions on the index.html file also, so that everyone has access

Explanation:-You are receiving the 403 Forbidden Error because you do not have the permissions to view the index.html file. Option A is incorrect because this is an S3 hosted website, Route 53 does not come into picture. Option B is incorrect because it is a static website hosted on S3. This issue is not related to DNS resolution. Option C is incorrect because even if you add the error document, you will get the error, because you need to set the proper permissions. Option D is CORRECT because it sets the appropriate permissions so that the user has access to the index.html. For more information on web site hosting in S3, please visit the below link: http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html The correct answer is: Change the permissions on the index.html file also, so that everyone has access

Q28) Which of the below components is used by AWS Data Pipeline to poll for tasks and then performs those tasks?

● S3
✓ Task Runner

Explanation:-Task Runner is a task agent application that polls AWS Data Pipeline for scheduled tasks and executes them on Amazon EC2 instances, Amazon EMR clusters, or other computational resources, reporting status as it does so. For more information on the Taskrunner in AWS pipeline, please refer to the below link http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-using-task-runner.html The correct answer is: Task Runner

● Definition Syntax File
● AWS OpsWork

Q29)

An organization has created multiple components of a single application. Currently, all the components are hosted on a single EC2 instance.

Due to security reasons, the organization wants to implement 2 separate SSL certificates for the separate modules.

How can the organization achieve this with a single instance?

● Create an EC2 instance which has both an ACL and the security group attached to it and have separate rules for each IP address.
● Create an EC2 instance which has multiple subnets attached to it and each will have a separate IP address.
✓ Create an EC2 instance which has multiple network interfaces with multiple elastic IP addresses.

Explanation:-It can be useful to assign multiple IP addresses to an instance in your VPC to do the following: (1) Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address. (2) Operate network appliances, such as firewalls or load balancers, that have multiple IP addresses for each network interface. (3) Redirect internal traffic to a standby instance in case your instance fails, by reassigning the secondary IP address to the standby instance. Option A is CORRECT because, as mentioned above, if you have multiple elastic network interfaces (ENIs) attached to the EC2 instance, each network IP can have a component running with a separate SSL certificate. Option B is incorrect because having separate rules in security group as well as NACL does not mean that the instance supports multiple SSLs. Option C is incorrect because an EC2 instance cannot have multiple subnets. Option D is incorrect because NAT address is not related to supporting multiple SSLs. For more information on Multiple IP Addresses, please refer to the link below: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html The correct answer is: Create an EC2 instance which has multiple network interfaces with multiple elastic IP addresses.

● Create an EC2 instance with a NAT address.

Q30)

You are building a website that will retrieve and display highly sensitive information to users. The amount of traffic the site will receive is known and not expected to fluctuate. The site will leverage SSL to protect the communication between the clients and the web servers.

Due to the nature of the site you are very concerned about the security of your SSL private key and want to ensure that the key cannot be accidentally or intentionally moved outside your environment.

Additionally, while the data the site will display is stored on an encrypted EBS volume, you are also concerned that the web servers' logs might contain some sensitive information; therefore, the logs must be stored so that they can only be decrypted by employees of your company.

Which of these architectures meets all of the requirements?

● Use Elastic Load Balancing to distribute traffic to a set of web servers. Configure the load balancer to perform TCP load balancing, use an AWS CloudHSM to perform the SSL transactions, and write your web server logs to an ephemeral volume that has been encrypted using a randomly generated AES key.
✓ Use Elastic Load Balancing to distribute traffic to a set of web servers, configure the load balancer to perform TCP load balancing, use an AWS CloudHSM to perform the SSL transactions, and write your web server logs to a private Amazon S3 bucket using Amazon S3 server-side encryption.
● Use Elastic Load Balancing to distribute traffic to a set of web servers. Use TCP load balancing on the load balancer and configure your web servers to retrieve the private key from a private Amazon S3 bucket on boot. Write your web server logs to a private Amazon S3 bucket using Amazon S3 server-side encryption.
● Use Elastic Load Balancing to distribute traffic to a set of web servers. To protect the SSL private key, upload the key to the load balancer and configure the load balancer to offload the SSL traffic. Write your web server logs to an ephemeral volume that has been encrypted using a randomly generated AES key.

Q31)

You have multiple Amazon EC2 instances running in a cluster across multiple Availability Zones within the same region.

What combination of the following should be used to ensure the highest network performance (packets per second), lowest latency, and lowest jitter? Choose 3 options from the below:

● Amazon PV AMI
✓ Enhanced networking
● Amazon EC2 placement groups
✓ Amazon HVM AMI
✓ Amazon VPC

Q32) A company has the requirement to analyze the clickstreams from a web application in real time? Which of the below AWS services will fulfill this requirement?

● Amazon SQS
✓ Amazon Kinesis
Explanation:-Kinesis Data Streams are extremely useful for rapid and continuous data intake and aggregation. The type of data used includes IT infrastructure log data, application logs, social media, market data feeds, and web clickstream data. Because the response time for the data intake and processing is in real time, the processing is typically lightweight. Option A is CORRECT because Amazon Kinesis Data Streams are very useful in processing website clickstreams in real time, and then analyzing using multiple different Kinesis Data Streams applications running in parallel. Option B is incorrect because SQS is used for storing messages/work items for asynchronous processing in the application, not the real time processing of clickstream data. Option C is incorrect because Redshift is a data warehouse solution that is used for Online Analytical Processing of data, and where complex analytic queries against petabytes of structured data. It is not used in real time processing of clickstream data. Option D is incorrect because AWS IoT is a platform that enables you to connect devices to AWS Services and other devices, secure data and interactions, process and act upon device data. It does not do the real time processing of the clickstream data. However, it can leverage Amazon Kinesis Analytics to do it. For more information on Kinesis , please visit the below link http://docs.aws.amazon.com/streams/latest/dev/introduction.html The correct answer is: Amazon Kinesis
● Amazon Redshift
● AWS IoT

Q33) Which of the following is a reliable and durable logging solution to track changes made to your AWS resources?

● Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs
● Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
● Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.
✓ Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
Explanation:-For the scenarios where the application is tracking (or needs to track) the changes made by any AWS service, resource, or API, always think about AWS CloudTrail service. AWS Identity and Access Management (IAM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account. CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets. The most important points in this question are (a) S3 bucket with global services option enabled, (b) Data integrity, and (c) Confidentiality. Option A is CORRECT because (a) it uses AWS CloudTrail with Global Option enabled, (b) a single new S3 bucket and IAM Roles so that it has the confidentiality, (c) MFA on Delete on S3 bucket so that it maintains the data integrity. See the AWS CloudTrail setting below which sets the Global Option. Options B is incorrect because (a) although it uses AWS CloudTrail, the Global Option is not enabled, and (b) SNS notifications can be a overhead in this situation. Option C is incorrect because (a) as an existing S3 bucket is used, it may already be accessed to the user, hence not maintaining the confidentiality, and (b) it is not using IAM roles. Option D is incorrect because (a) although it uses AWS CloudTrail, the Global Option is not enabled, and (b) three S3 buckets are not needed. For more information on Cloudtrail, please visit the below URL: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html The correct answer is: Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.

Q34) What is the type of replication that occurs between the instances when configuring an RDS environment for Multi-AZ in a particular region? Choose an option from the below:

● Asynchronous replication
✓ Synchronous replication
Explanation:-Multi-AZ deployments for the MySQL, MariaDB, Oracle, and PostgreSQL engines utilize synchronous physical replication to keep data on the standby up-to-date with the primary. Multi-AZ deployments for the SQL Server engine use synchronous logical replication to achieve the same result, employing SQL Server-native Mirroring technology. Both approaches safeguard your data in the event of a DB Instance failure or loss of an Availability Zone. For more information on Multi-AZ, please refer to the below URL: https://aws.amazon.com/rds/details/multi-az/ The correct answer

is: Synchronous replication

● Snapshot replication

● Default replication

Q35)

You have an Auto Scaling group associated with an Elastic Load Balancer (ELB).

You have noticed that instances launched via the Auto Scaling group are being marked unhealthy due to an ELB health check but these unhealthy instances are not being terminated.

What do you need to do to ensure trial instances marked unhealthy by the ELB will be terminated and replaced?

● Increase the value for the Health check interval set on the Elastic Load Balancer

✓ Add an Elastic Load Balancing health check to your Auto Scaling group

Explanation:-To discover the availability of your EC2 instances, an ELB periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks. The status of the instances that are healthy at the time of the health check is InService. The status of any instances that are unhealthy at the time of the health check is OutOfService. When you allow the Auto Scaling group (ASG) to receive the traffic from the ELB, it gets notified when the instance becomes unhealthy and then it terminates it. See the images in the "More information..." section for more details. Option A is incorrect because changing the threshold will not enable ASG to know about the unhealthy instances. Option B is CORRECT because when you associate the ELB with ASG, you allow the ASG to receive the traffic from that ELB. As a result, the ASG will get aware about the unhealthy instances and it terminates them. Option C is incorrect because increasing the interval will still not communicate the information about the unhealthy instances to the ASG. Option D is incorrect because this setting will not communicate the information about the unhealthy instances to the ASG either. More information on ELB with Auto Scaling Group: For more information on ELB, please visit the below URL: https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html The correct answer is: Add an Elastic Load Balancing health check to your Auto Scaling group

● Change the thresholds set on the Auto Scaling group health check

● Change the health check set on the Elastic Load Balancer to use TCP rather than HTTP checks

---

Q36)

You have a video transcoding application running on Amazon EC2. Each instance polls a queue to find out which video should be transcoded and then runs a transcoding process. If this process is interrupted, the videos will be transcoded by another instance based on the queuing system.

You have a large backlog of videos which need to be transcoded and would like to reduce this backlog by adding more instances.

You will need these instances only until the backlog is reduced.

Which type of Amazon EC2 instances should you use to reduce the backlog in the most cost-efficient way?

● Dedicated instances

✓ Spot instances

Explanation:-Since this is like a batch processing job, the best type of instance to use is a Spot instance. Since these jobs don't last for the entire duration of the year, they can bid upon and allocated and deallocated as requested. Option A and C are incorrect because the application need the instances only until the backlog is reduced. With reserved/dedicated instances, there is a possibility that the instances might get idle after the backlog reduction. So, this is a costly solution. Option B is CORRECT because (i) they are less expensive than reserved instances, (ii) interruption in the transcoding process is affordable since the videos will be transcoded by another instance based on the queuing system. Option D is incorrect because (i) on-demand instances are most expensive, (ii) you can afford interruption in the transcoding process, and (iii) on demand instances would have been suited if there was no alternate way of transcoding the videos and interruption was not affordable. For more information on Spot Instances, please visit the URL – https://aws.amazon.com/ec2/spot/ The correct answer is: Spot instances

● Reserved instances

● On-demand instances

Q37)

You are using DynamoDB to store data in your application. One of the tables named "Users", you have defined "UserID" as it primary key.

However, you envision that, in some cases, you might need to query the table by "UserName" which cannot be set as primary key.

What changes would you do to this table to be able to query using UserName? Choose correct option from the below:

● Create a hash and range primary key.

✓ Create a secondary index.

Explanation:-Amazon DynamoDB provides fast access to items in a table by specifying primary key values. However, many applications might benefit from having one or more secondary (or alternate) keys available, to allow efficient access to data with attributes other than the primary key. To address this, you can create one or more secondary indexes on a table, and issue Query or Scan requests against these indexes. Option A is incorrect because creating another table is costly and unnecessary. Option B is incorrect because UserName cannot be primary key. Option C is CORRECT because, as mentioned above, creating a secondary index on UserName would allow the user to efficiently access the table via querying on this attribute rather than UserID which is the primary key. Option D is incorrect because DynamoDB tables are partitioned based on the primary key and you cannot make UserName as the primary key. http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GSI.html The correct answer is: Create a secondary index.

● Create a second table that contains all the information, but make UserName the primary key.

● Partition the table using UserName rather than UserID.

Q38)

Your team is excited about the use of AWS because now they have access to "programmable Infrastructure".

You have been asked to manage your AWS infrastructure in a manner similar to the way you might manage application code.

You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development, test, QA , and production).

Which approach addresses this requirement?

● Use cost allocation reports and AWS Opsworks to deploy and manage your infrastructure.
● Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructure.
● Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructure.
✓ Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure.

Explanation:-You can use AWS Cloud Formation’s sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don’t need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, in effect applying version control to your AWS infrastructure the same way you do with your software. You can also visualize your templates as diagrams and edit them using a drag-and-drop interface with the AWS CloudFormation Designer. Option A is incorrect because Cost Allocation Reports is not helpful for the purpose of the question. Option B is incorrect because CloudWatch is used for monitoring the metrics pertaining to different AWS resources. Option C is incorrect because it does not have the concept of programmable Infrastructure. Option D is CORRECT because AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. For more information on CloudFormation, please visit the link: https://aws.amazon.com/cloudformation/ The correct answer is: Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure.

Q39) Of the 6 available sections on a CloudFormation template (Template Description Declaration, Template Format Version Declaration, Parameters, Resources, Mappings, Outputs), which is the only one required for a CloudFormation template to be accepted? Choose an option from the below:

● Parameters
● Template Declaration
● Mappings
✓ Resources

Explanation:-Resources is the only mandatory field while creating the CloudFormation template. It specifies the stack resources and their properties, such as an Amazon Elastic Compute Cloud instance or an Amazon Simple Storage Service bucket. For more information on CloudFormation templates, please refer to the below link: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html The correct answer is: Resources

---

Q40)

Your supervisor is upset about the fact that SNS topics that he subscribed to are now cluttering up his email inbox.

How can he stop receiving the email from SNS without disrupting other users’ ability to receive the email from SNS? Choose 2 options from the below:

● You can delete the SNS topic responsible for the emails
✓ He can use the unsubscribe information provided in the emails

Explanation:-Every request has a unsubscribe URL which can be used. Also from the aws console , one can just delete the subscription Option A is CORRECT because deleting the subscription for the user from the SNS topic will ensure that he will not receive any notifications (basically just unsubscribe him). Option B is incorrect because you cannot delete the endpoint from the SNS subscription. Option C is incorrect because if you delete the topic then none of the subscribers will get any notifications. Option D is CORRECT because the notifications has an option to unsubscribe which the user can avail to stop receiving the notifications. For more information on SNS subscription please visit the below link http://docs.aws.amazon.com/sns/latest/api/API_Subscribe.html The correct answers are: You can delete the subscription from the SNS topic responsible for the emails, He can use the unsubscribe information provided in the emails

● You can delete the endpoint from the SNS subscription responsible for the emails
✓ You can delete the subscription from the SNS topic responsible for the emails

Explanation:-Every request has a unsubscribe URL which can be used. Also from the aws console , one can just delete the subscription Option A is CORRECT because deleting the subscription for the user from the SNS topic will ensure that he will not receive any notifications (basically just unsubscribe him). Option B is incorrect because you cannot delete the endpoint from the SNS subscription. Option C is incorrect because if you delete the topic then none of the subscribers will get any notifications. Option D is CORRECT because the notifications has an option to unsubscribe which the user can avail to stop receiving the notifications. For more information on SNS subscription please visit the below link http://docs.aws.amazon.com/sns/latest/api/API_Subscribe.html The correct answers are: You can delete the subscription from the SNS topic responsible for the emails, He can use the unsubscribe information provided in the emails

---

Q41)

You are managing a legacy application inside VPC with hard-coded IP addresses in its configuration.

Which mechanisms will allow the application to failover to new instances without the need for reconfiguration? Choose 2 options from the below:

✓ Assign a secondary private IP address to the primary ENI of the failover instance
● Use Route53 health checks to reroute the traffic to the failover instance
✓ Create a secondary ENI that can be moved to the failover instance
● Create an ELB to reroute traffic to the failover instance

Q42)

A company has a Direct Connect established between their on-premise location and AWS.

The applications hosted on the on-premise location are experiencing high latency when using S3.

What could be done to ensure that the latency to S3 can be reduced?

● Establish a VPN connection from the VPC to the public S3 endpoint.
● Configure a private virtual interface to connect to the public S3 endpoint via the Direct Connect connection.
● 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.
✓ 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. See the image below: Option A is CORRECT because, as mentioned above, it creates a public virtual interface to connect to S3 endpoint. Option B is incorrect because to connect to S3 endpoint, a public virtual interface needs to be created, not VPN. Option C is incorrect because to connect to S3 endpoint, a public virtual interface needs to be created, not private. Option D is incorrect because this setup will not help connecting to the S3 endpoint. For more information on virtual interfaces, please visit the below URL http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html The correct answer is: Configure a public virtual interface to connect to a public S3 endpoint resource.

Q43)

A company has a web application hosted on AWS. The IT Security Administrator has noticed that a lot of requests are coming from a set of IPs.

As an AWS professional, what can you do to ensure that this type of attack is limited?

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

Explanation:-In this scenario, the attack is coming from a set of certain IP addresses over specific port from a specific country. You are supposed to defend against this attack. In such questions, always think about two options: Security groups and Network Access Control List (NACL). Security Groups operate at the individual instance level, whereas NACL operates at subnet level. You should always fortify the NACL first, as it is encounter first during the communication with the instances in the VPC. Option A is incorrect because IP addresses cannot be blocked using route table or IGW. Option B is incorrect because (a) you cannot deny port access using security groups, and (b) by default all requests are denied; you open access for particular IP address or range. You cannot deny access for particular IP addresses using security groups. Option C is incorrect because if the application servers are put in the private subnet, the application will not be accessible from the internet, especially since the option does not mention any public facing ELB or Route 53 configuration. Option D is CORRECT because (a) you can add deny rules in NACL and block access to certain IP addresses. See an example below: The correct answer is: Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses

Q44)

You have created an Elastic Load Balancer with Duration-Based sticky sessions enabled in front of your six EC2 web application instances in US-West-2. For High Availability, there are three web application instances in Availability Zone 1 and three web application instances in Availability Zone 2. To load test, you set up a software-based load tester in Availability Zone 2 to send traffic to the Elastic Load Balancer, as well as letting several hundred users browse to the ELB's hostname.

After a while, you notice that the users' sessions are spread evenly across the EC2 instances in both AZ's, but the software-based load tester's traffic is hitting only the instances in Availability Zone 2.

What steps can you take to resolve this problem? Choose 2 correct options from the below:

✓ Use a third party load-testing service to send requests from globally distributed clients

Explanation:-When you create an elastic load balancer, a default level of capacity is allocated and configured. As Elastic Load Balancing sees changes in the traffic profile, it will scale up or down. The time required for Elastic Load Balancing to scale can range from 1 to 7 minutes, depending on the changes in the traffic profile. When Elastic Load Balancing scales, it updates the DNS record with the new list of IP addresses. To ensure that clients are taking advantage of the increased capacity, Elastic Load Balancing uses a TTL setting on the DNS record of 60 seconds. It is critical that you factor this changing DNS record into your tests. If you do not ensure that DNS is re-resolved or use multiple test clients to simulate increased load, the test may continue to hit a single IP address when Elastic Load Balancing has actually allocated many more IP addresses. Because your end users will not all be resolving to that single IP address, your test will not be a realistic sampling of real-world behavior. Option A is incorrect because creating load tester in US-East-1 will face the same problem of traffic hitting only the instances in that AZ. Option B is CORRECT because if you do not ensure that DNS is re-resolved the test may continue to hit the single IP address. Option C is CORRECT because if the requests come from globally distributed users, the DNS will not be resolved to a single IP address and the traffic would be distributed evenly across multiple instances. Option D is incorrect because the traffic will be routed to the same back-end instances as the users continue to access your application. The load will not be evenly distributed across the AZs. Please refer to the below article for more information: http://aws.amazon.com/articles/1636185810492479 The correct answers are: Force the software-based load tester to re-resolve DNS before every request, Use a third party load-testing service to send requests from globally distributed clients

✓ Force the software-based load tester to re-resolve DNS before every request

Explanation:-When you create an elastic load balancer, a default level of capacity is allocated and configured. As Elastic Load Balancing sees changes in the traffic profile, it will scale up or down. The time required for Elastic Load Balancing to scale can range from 1 to 7 minutes, depending on the changes in the traffic profile. When Elastic Load Balancing scales, it updates the DNS record with the new list of IP addresses. To ensure that clients are taking advantage of the increased capacity, Elastic Load Balancing uses a TTL setting on the DNS record of 60 seconds. It is critical that you factor this changing DNS record into your tests. If you do not ensure that DNS is re-resolved or use multiple test clients to simulate increased load, the test may continue to hit a single IP address when Elastic Load Balancing has actually allocated many more IP addresses. Because your end users will not all be resolving to that single IP address, your test will not be a realistic sampling of real-world behavior. Option A is incorrect because creating load tester in US-East-1 will face the same problem of traffic hitting only the instances in that AZ. Option B is CORRECT because if you do not ensure that DNS is re-resolved the test may continue to hit the single IP address. Option C is CORRECT because if the requests come from globally distributed users, the DNS will not be resolved to a single IP address and the traffic would be distributed evenly across multiple instances. Option D is incorrect because the traffic will be routed to the same back-end instances as the users continue to access your application. The load will not be evenly distributed across the AZs. Please refer to the below article for more information: http://aws.amazon.com/articles/1636185810492479 The correct answers are: Force the software-based load tester to re-resolve DNS before every request, Use a third party load-testing service to send requests from globally distributed clients

● Create a software-based load tester in US-East-1 and test from there
● Switch to Application-Controlled sticky sessions

Q45) Which of the following AWS services can be used to define alarms to trigger on a certain activity in the AWS Data pipeline?

✓ SNS
Explanation:-Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push notification service that lets you send individual messages or to fan-out messages to large numbers of recipients. Amazon SNS makes it simple and cost effective to send push notifications to mobile device users, email recipients or even send messages to other distributed services. For more information on SNS, please refer to the below link https://aws.amazon.com/sns/ The correct answer is: SNS
● SQS
● SES
● CodeDeploy

Q46)

In Amazon Cognito, your mobile app authenticates with the Identity Provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito.

Which of the following is returned for the user to provide a set of temporary, limited-privilege AWS credentials?

● Cognito Key pair
✓ Cognito Identity ID
Explanation:-If you're allowing unauthenticated users, you can retrieve a unique Amazon Cognito identifier (identity ID) for your end user immediately. If you're authenticating users, you can retrieve the identity ID after you've set the login tokens in the credentials provider For more information on Cognito ID, please refer to the below link: http://docs.aws.amazon.com/cognito/latest/developerguide/getting-credentials.html The correct answer is: Cognito Identity ID
● Cognito SDK
● Cognito API

Q47)

You created three S3 buckets – "mydomain.com", "downloads.mydomain.com", and "www.mydomain.com". You uploaded your files, enabled static website hosting, specified both of the default documents under the "enable static website hosting" header, and set the "Make Public" permission for the objects in each of the three buckets.

All that's left for you to do is to create the Route 53 Aliases for the three buckets.

You are going to have your end users test your websites by browsing to http://mydomain.com/error.html, http://downloads.mydomain.com/index.html, and http://www.mydomain.com.

What problems will your testers encounter? Choose an option from the below:

● http://downloads.mydomain.com/index.html will not work because the "downloads" prefix is not a supported prefix for S3 websites using Route 53 aliases
✓ There will be no problems, all three sites should work
Explanation:-Previously only allowed domain prefix when we are creating AWS Route53 aliases for AWS S3 static websites was the "www". However, this is no longer the case. You can now use other sub-domains. For more information on S3 web site hosting please visit the below link: http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html The correct answer is: There will be no problems, all three sites should work
● http://mydomain.com/error.html will not work because you did not set a value for the error.html file
● http://www.mydomain.com will not work because the URL does not include a file name at the end of it

Q48)

An organization has the requirement to store 10TB worth of scanned files. There is a requirement to have a search application in place which can be used to search through the scanned files.

Which of the below is the best option for implementing the search facility?

● Use a single-AZ RDS MySQL instance to store the search index for the scanned files and use an EC2 instance with a custom application to search based on the index.
● Model the environment using CloudFormation. Use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the scanned files with a search index.
✓ Use S3 with standard redundancy to store and serve the scanned files. Use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.
Explanation:-This question presents following scenarios: (1) type of storage that can store large amount of data (10TB), (2) the commercial search product is at its end of life, (3) the architecture should be cost effective, highly available, and durable. Tip: Whenever a storage service that can store large amount of data with low cost, high availability, and high durability, always think about using S3. Option A is incorrect because even though it uses S3, it uses the commercial search software which is at its end of life. Option B is incorrect because striped EBS is not as durable solution as S3 and certainly not as cost effective as S3. Also, it has maintenance overhead. Option C is CORRECT because (a) it uses S3 to store the images, (b) instead of the commercial product that is at its end of life, it uses CloudSearch for query processing, and (c) with multi AZ implementation, it achieves high availability. Option D is incorrect because with single AZ RDS instance, it does not have high availability. Amazon CloudSearch With Amazon CloudSearch, you can quickly add rich search capabilities to your website or application. You don't need to become a search expert or worry about hardware provisioning, setup, and maintenance. With a few clicks in the AWS Management Console, you can create a search domain and upload the data that you want to make searchable, and Amazon CloudSearch will automatically provision the required resources and deploy a highly tuned search index. You can easily change your search parameters, fine tune search relevance, and apply new settings at any time. As your volume of data and traffic fluctuates, Amazon CloudSearch seamlessly scales to meet your needs. For more information on AWS CloudSearch, please visit the below link https://aws.amazon.com/cloudsearch/ The correct answer is: Use S3 with standard redundancy to store and serve the scanned files. Use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.
● Use S3 with reduced redundancy lo store and serve the scanned files. Install a commercial search application on EC2 Instances and configure with auto-scaling and an Elastic Load Balancer.