Answer Sheet

Q1) Which of the below options is recommended to provide an auditor who needs access to the logs of account activity related to actions across your AWS infrastructure?

- 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.
- ✓ 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.

- Create a role that has the full permissions to access the resources for the auditor.
- The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.

Q2) Which of the following are Lifecycle events available in Opswork? Choose 3 options from the below:

- ✓ Shutdown
- ✓ Deploy
- ✓ Setup
- Decommision

Q3)

You are an architect for a new sharing mobile application. Anywhere in the world, your users can see local news on topics they chose. They can post pictures and videos from inside the application.

Since the application is being used on a mobile phone, connection stability is required for uploading content and delivery should be quick.

Content is accessed a lot in the first minutes after it has been posted but is quickly replaced by new content before disappearing.

The local nature of the news means that 90% of the uploaded content is then read locally.

What solution will optimize the user experience when users upload and view content (by minimizing page load times and minimizing upload times)?

- ✓ Use CloudFront for uploading the content to S3 bucket and for content delivery.

Explanation:-it uses CloudFront for both uploading as well as distributing the content (not just distributing) which is the most efficient use of the service.

- Upload to EC2 in regions closer to the user, send content to S3, use CloudFront.
- Upload and store in S3, and use CloudFront.
- Upload and store in S3 in the region closest to the user and then use multiple distributions of CloudFront.

Q4)

An application is composed of multiple components. Currently, all the components are hosted on a single EC2 instance. Due to security reasons, the organization wants to implement 2 separate SSL for the separate modules.

How can the organization achieve this with a single instance? Choose an answer from the below options:

- 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 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 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. 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.

- Create an EC2 instance with a NAT address.

Q5)

You're migrating an existing application to the AWS cloud. The application will be primarily using EC2 instances. This application needs to be built with the highest availability architecture available.

The application currently relies on hardcoded hostnames for intercommunication between the three tiers.

You've migrated the application and configured the multi-tiers using the internal Elastic Load Balancer for serving the traffic.

The load balancer hostname is demo-app.us-east-1.elb.amazonaws.com.

The current hard-coded hostname in your application used to communicate between your multi-tier application is demolayer.example.com.

What is the best method for architecting this setup to have as much high availability as possible? Choose the correct answer from the below options:

- Create a public resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com.
- Create an environment variable passed to the EC2 instances using user-data with the ELB hostname, demo-app.us-east-1.elb.amazonaws.com.
- Add a cname record to the existing on-premise DNS server with a value of demo-app.us-east-1.elb.amazonaws.com. Create a public resource

record set using Route 53 with a hostname of applayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com.
✅ Create a private resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com.
Explanation:-Since demolayer.example.com is an internal DNS record, the best way is Route 53 to create an internal resource record. One can then point the resource record to the create ELB. While ordinary Amazon Route 53 resource record sets are standard DNS resource record sets, alias resource record sets provide an Amazon Route 53–specific extension to DNS functionality. Instead of an IP address or a domain name, an alias resource record set contains a pointer to a CloudFront distribution, an Elastic Beanstalk environment, an ELB Classic or Application Load Balancer, an Amazon S3 bucket that is configured as a static website, or another Amazon Route 53 resource record set in the same hosted zone. it creates an internal ALIAS record set where it defines the mapping between the hard-coded host name and the ELB host name that is to be used.

Q6)

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16.

The public subnet uses CIDR 20.0.1.0/24.

The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306.

The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp).

Which of the below-mentioned entries is required in the private subnet database security group DBSecGrp?

- Allow Outbound on port 3306 for destination Web Server Security Group WebSecGrp.
- Allow Inbound on port 3306 from source 20.0.0.0/16.
- ✅ Allow Inbound on port 3306 for the source Web Server Security Group WebSecGrp.

Explanation:-The important point in this question is to allow the incoming traffic to the private subnet on port 3306 only for the instances in the private subnet. (a) it allows the inbound traffic only for the required port 3306, and (b) it allows only the traffic from the instances in the public subnet (WebSecGrp).

- Allow Outbound on port 80 for destination NAT instance IP.

Q7)

A user has setup Auto Scaling with ELB on the EC2 instances. The user wants to configure that whenever the CPU utilization is below 10%, Auto Scaling should remove one instance.

How can the user configure this?

- Use CloudWatch to monitor the data and Auto Scaling to remove the instances using scheduled actions.
- The user can get an email using SNS when the CPU utilization is less than 10%. The user can use the desired capacity of Auto Scaling to remove the instance.
- ✅ Configure CloudWatch to send a notification to the Auto Scaling group when the CPU Utilization is less than 10% and configure the Auto Scaling policy to remove the instance.

Explanation:-The notification is sent to Auto Scaling Group which then removes an instance from the running instances. More information on Auto Scaling, Scheduled Actions: Auto Scaling helps you maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Auto Scaling to help ensure that you are running your desired number of Amazon EC2 instances. Auto Scaling can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.

- Configure CloudWatch to send a notification to Auto Scaling Launch configuration when the CPU utilization is less than 10% and configure the Auto Scaling policy to remove the instance.

Q8)

As an IT administrator, you have been tasked to develop a reliable and durable logging solution to track changes made to your EC2, IAM and RDS resources.

The solution must ensure the integrity and confidentiality of your log data.

Which of these solutions would you implement?

- 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 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 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. (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 option to apply the trail to all regions (global).

Q9) How can you configure the backups of an Oracle RAC configuration which is hosted on the AWS public cloud?

- Enable automated backups on the RDS RAC cluster; enable auto snapshot copy to a backup region to reduce RPO and RTO.
- Create manual snapshots of the RDS backup and write a script that runs the manual snapshot.
- Enable Multi-AZ failover on the RDS RAC cluster to reduce the RPO and RTO in the event of disaster or failure.
- ✅ Create a script that runs snapshots against the EBS volumes to create backups and durability.

Explanation:-Currently, Oracle Real Application Cluster (RAC) is not supported as per the AWS documentation. However, you can deploy scalable RAC on Amazon EC2 using the recently-published tutorial and Amazon Machine Images (AMI). So, in order to take the backups, you need to take the backup in the form of EBS volume snapshots of the EC2 that is deployed for RAC. 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.

Q10)

A user is accessing RDS from an application.

The user has enabled the Multi-AZ feature with the MS SQL RDS DB.

During a planned outage how will AWS ensure that a switch from DB to a standby replica will not affect access to the application?

- The switch over changes hardware so RDS does not need to worry about access
- RDS will have both the DBs running independently and the user has to manually switch over
- RDS will have an internal IP which will redirect all requests to the new DB
- ✅ RDS uses DNS to switch over to stand by replica for seamless transition

Explanation:-Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure (for example, instance hardware failure, storage failure, or network disruption), Amazon RDS performs an automatic failover to the standby by changing the CNAME for the DB instance to point to the standby, so that you can resume database operations as soon as the failover is complete. as mentioned above, RDS performs automatic failover by flipping the CNAME for the DB instance from primary to standby instance.

Q11) Which of the following are techniques to stop DDoS attacks on your AWS architecture? Choose 3 answers from the below options:

- ✅ Use an Amazon CloudFront distribution for both static and dynamic content.
- Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
- ✅ Add alert Amazon CloudWatch to look for high Network in and CPU utilization.
- Use dedicated instances to ensure that each instance has the maximum performance possible.
- ✅ Use an Elastic Load Balancer with auto scaling groups at the web, App. Restricting direct internet traffic to Amazon Relational Database Service (RDS) tiers.
- Create processes and capabilities to quickly add and remove rules to the instance OS firewall.

Q12)

An organization has added 3 of his AWS accounts to consolidated billing. One of the AWS accounts has purchased a Reserved Instance (RI) of a small instance size in the US-East-1a zone.

All other AWS accounts are running instances of a small size in the same zone.

What will happen in this case for the RI pricing?

- If there are more than one instances of a small size running across multiple accounts in the same zone no one will get the benefit of RI.
- One instance of a small size and running in the US-East-1a zone of each AWS account will get the benefit of RI pricing.
- ✅ Any single instance from all the three accounts can get the benefit of AWS RI pricing if they are running in the same zone and are of the same size.

Explanation:-the reserved price benefit will be applied to a single EC2 instance across all the accounts.

- Only the account that has purchased the RI will get the advantage of RI pricing.

Q13)

You have just developed a new mobile application that handles analytics workloads on large-scale datasets that are stored on Amazon Redshift.

Consequently, the application needs to access Amazon Redshift tables.

Which of the below methods would be the best for both practically and security-wise to access the tables? Choose the correct answer from the below options:

- Create a RedShift read-only access policy in IAM and embed those credentials in the application.
- Create a HSM client certificate in Redshift and authenticate using this certificate.
- Create an IAM user and generate encryption keys for that user. Create a policy for RedShift read-only access. Embed the keys in the application.
- ✅ Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary credentials.

Explanation:-For access to any AWS service, the ideal approach for any application is to use Roles. This is the first preference. This along with the usage of roles is highly stressed in the AWS documentation.

Q14) Which of the following must be done while generating a pre-signed URL in S3 in order to ensure that the user who is given the pre-signed URL has the permission to upload the object?

- Ensure the user has write permission to S3.
- Create a Cloudfront distribution.
- Ensure the user has read permission to S3.
- ✅ Ensure that the person who has created the pre-signed URL has the permission to upload the object to the appropriate S3 bucket.

Explanation:-in order to successfully upload an object to S3, the pre-signed URL must be created by someone who has permission to perform the operation that the pre-signed URL is based upon.

Q15)

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 by mistake.

The user is trying to create another subnet of CIDR 20.0.1.0/24.

How can the user create the second subnet?

- The user can modify the first subnet CIDR with AWS CLI.
- ✅ It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created.

Explanation:-Once you create a subnet, you cannot modify it, you have to delete it.

- There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet's CIDR.
- The user can modify the first subnet CIDR from the console.

Q16)

A mobile application has been developed which stores data in DynamoDB. The application needs to scale to handle millions of views.

The customer also needs access to the data in the DynamoDB table as part of the application.

Which of the below methods would help to fulfill this requirement?

- Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in a server-side language using the AWS SDK and host the application in an S3 bucket for scalability.
- Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWith API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket.
- Configure an on-premise AD server utilizing SAML 2.0 to manage the application users inside of the on-premise AD server and write code that authenticates against the LD serves. Grant a role assigned to the STS token to allow the end-user to access the required data in the DynamoDB table.
- ✅ Let the users sign in to the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket.

Explanation:-The AssumeRolewithWebIdentity returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider.

Q17)

A user is using CloudFormation to launch an EC2 instance and then planning to configure an application after the instance is launched.

The user wants the stack creation of ELB and AutoScaling to wait until the EC2 instance is launched and configured properly.

How can the user configure this?

- The user can use the HoldCondition resource to wait for the creation of the other dependent resources.
- ✅ The user can use the WaitCondition resource to hold the creation of the other dependent resources.

Explanation:-You can use a wait condition for situations like the following: To coordinate stack resource creation with configuration actions that are external to the stack creation To track the status of a configuration process

- It is not possible that the stack creation will wait until one service is created and launched.
- The user can use the DependentCondition resource to hold the creation of the other dependent resources.

Q18)

A document storage company is deploying their application to AWS and changing their business model to support both Free Tier and Premium Tier users.

The premium Tier users will be allowed to store up to 200GB of data and Free Tier customers will be allowed to store only 5GB.

The customer expects that billions of files will be stored.

All users need to be alerted when approaching 75 percent quota utilization and again at 90 percent quota use.

To support the Free Tier and Premium Tier users, how should they architect their application?

- The company should write both the content length and the username of the files owner as S3 metadata for the object. They should then create a file watcher to iterate over each object and aggregate the size for each user and send a notification via Amazon Simple Queue Service to an emailing service if the storage threshold is exceeded.
- The company should deploy an Amazon Relational Database Service (RDS) relational database with a stored objects table that has a row for each stored object along with the size of each object. The upload server will query the aggregate consumption of the user in question (by first determining the files stored by the user, and then querying the stored objects table for respective file sizes) and send an email via Amazon Simple Email Service if the thresholds are breached.
- ✅ The company should utilize an Amazon Simple Workflow Service activity worker that updates the user's used data counter in Amazon DynamoDB. The Activity Worker will use Simple Email Service to send an email if the counter increases above the appropriate thresholds.

Explanation:-DynamoDB which is highly scalable service is best suitable in this scenario.

- The company should create two separate Amazon Simple Storage Service buckets, one for date storage for Free Tier Users, and another for data storage for Premium Tier users. An Amazon Simple Workflow Service activity worker will query all objects for a given user based on the bucket the data is stored in and aggregate storage. The activity worker will notify the user via Amazon Simple Notification Service when necessary.

Q19)

A user has launched a large EBS backed EC2 instance in the US-East-1a region. The user wants to achieve Disaster Recovery (DR) for that instance by creating another small instance in Europe.

How can the user achieve DR?

- Copy the instance from the US East region to the EU region.
- Use the “Launch more like this” option to copy the instance from one region to another.
- Copy the running instance using the “Instance Copy” command to the EU region.
- ✅ Create an AMI of the instance and copy the AMI to the EU region. Then launch the instance from the EU AMI.

Explanation:-If you need an AMI across multiple regions, then you have to copy the AMI across regions. Note that by default AMI’s that you have created will not be available across all regions. To copy AMI's, follow the below steps Step 1) The first step is to create an AMI from your running instance by choosing on Image->Create Image. Step 2) Once the Image has been created, go to the AMI section in the EC2 dashboard and click on the Copy AMI option. Step 3) In the next screen , you can specify where to copy the AMI to. For the entire details to copy AMI's,

---

Q20)

You are writing an AWS CloudFormation template and you want to assign values to properties that will not be available until runtime.

You know that you can use intrinsic functions to do this but are unsure as to which part of the template they can be used in.

Which of the following is correct in describing how you can currently use intrinsic functions in an AWS CloudFormation template? Choose an option from the below:

- You can use intrinsic functions in any part of a template.
- You can use intrinsic functions in any part of a template, except AWSTemplateFormatVersion and Description.
- ✅ You can only use intrinsic functions in specific parts of a template. You can use intrinsic functions in resource properties, metadata attributes, and update policy attributes.

Explanation:-As per AWS documentation: You can use intrinsic functions only in specific parts of a template. Currently, you can use intrinsic functions in resource properties, outputs, metadata attributes, and update policy attributes. You can also use intrinsic functions to conditionally create stack resources.

- You can use intrinsic functions only in the resource properties part of a template.

Q21) If an on-premise application is dependent on multicast and is required to be moved on to AWS, which of the below steps need to be carried out on the Operating system hosting that app so that it can be moved to AWS?

- Create all the subnets on a different VPC and use VPC peering between them.
- ✅ 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).

- Provide Elastic Network Interfaces between the subnets.
- All of the answers listed will help in deploying applications that require multicast on AWS.

Q22)

You are deploying your first EC2 instance in AWS and are using the AWS console to do this. You have chosen your AMI and your instance type and have now come to the screen where you configure your instance details.

One of the things that you need to decide is whether you want to auto-assign a public IP address or not.

You assume that if you do not choose this option you will be able to assign an Elastic IP address later, which happens to be a correct assumption.

Which of the below options best describes why an Elastic IP address would be preferable to a public IP address? Choose the correct option from the below:

- ✅ With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.

Explanation:-in case of an instance failure, you can reassign the EIP to a new instance, thus you do not need to change any reference to the IP address in your application.

- An Elastic IP address is free, whilst you must pay for a public IP address.
- You can have an unlimited amount of Elastic IP addresses, however public IP addresses are limited in number.
- An Elastic IP address cannot be accessed from the internet like a public IP address and hence is safer from a security standpoint.

Q23) Which of the following reports in CloudFront can help find out the most popular requested objects at an edge location? Choose an answer from the options given below

- Cache Statistics
- Top Referrers
- ✅ Popular Object

Explanation:-The Amazon CloudFront console can display a list of the 50 most popular objects for a distribution during a specified date range in the previous 60 days. Data for the Popular Objects report is drawn from the same source as CloudFront access logs. To get an accurate count of the top 50 objects, CloudFront counts the requests for all of your objects in 10-minute intervals beginning at midnight and keeps a running total of the top 150 objects for the next 24 hours.

- Most requested
- Most Referred

Q24)

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user’s data center.

The user's data center has CIDR 172.28.0.0/12.

The user has also setup a NAT instance (i-12345) to allow traffic to the internet from the VPN subnet.

Which of the below-mentioned options is not a valid entry for the main route table in this scenario?

- Destination: 20.0.0.0/16 and Target: local
- ✅ Destination: 20.0.1.0/24 and Target: i-12345

Explanation:-the destination of private subnet with NAT instance as target is not needed in the route table. This is an invalid entry.

- Destination: 0.0.0.0/0 and Target: i-12345
- Destination: 172.28.0.0/12 and Target: vgw-12345

Q25)

You are having trouble maintaining session states on some of your applications that are using an Elastic Load Balancer(ELB).

There does not seem to be an even distribution of sessions across your ELB.

Which of the following is the recommended method by AWS to try and rectify the issues to overcome this problem that you are having? Choose the correct option from the below:

- If your application does not have its own session cookie, then you can configure Elastic Load Balancing to create a session cookie by specifying your own stickiness duration.
- Use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance.
- ✅ Use ElastiCache, which is a web service that makes it easy to set up, manage, and scale a distributed in-memory cache environment in the cloud.

Explanation:-ElastiCache can be utilized to store the session state in cache rather than in any database. It also improves the performance by allowing you to quickly retrieve the session state information.

- Use a special cookie to track the instance for each request to each listener. When the load balancer receives a request, it will then check to see if this cookie is present in the request.

Q26) Which of the following is the most recommended approach to replicate an RDS instance to an on-premise location to AWS in the most secure manner?

- ✅ 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.

- Configure the RDS instance as the master and enable replication over the open internet using a secure SSL endpoint to the on-premise server.
- 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.

Q27)

You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets.

One instance is running a database and the other instance an application that will interface with the database.

You want to confirm that they can talk to each other for your application to work properly.

Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC? Choose 2 options from the below:

- Both instances are the same instance class and using the same Key-pair.
- ✅ A network ACL that allows communication between the two subnets.
- ✅ Security groups are set to allow the application host to talk to the database on the right port/protocol.
- That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.

Q28)

You have an ELB on AWS which has a set of web servers behind them.

There is a requirement that the SSL key used to encrypt data is always kept secure.

Secondly, the logs of ELB should only be decrypted by a subset of users.

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. 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, 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.

Explanation:-it uses CloudHSM for performing the SSL transaction without requiring any additional way of storing or managing the SSL private key. This is the most secure way of ensuring that the key will not be moved outside of the AWS environment. Also, it uses the highly available and durable S3 service for storing the logs.

- 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.

Q29)

You have been asked to leverage Amazon VPC EC2 and SQS to implement an application that submits and receives millions of messages per second to a message queue.

You want to ensure that your application has sufficient bandwidth between your EC2 instances and SQS.

Which option will provide the most scalable solution for communicating between the application and SQS?

- Ensure the application instances are launched in private subnets with the associate-public-IP-address=true option enabled. Remove any NAT instance from the public subnet, if any.
- Ensure the application instances are properly configured with an Elastic Load Balancer.
- Ensure the application instances are launched in private subnets with the EBS-optimized option enabled.
- ✅ Ensure the application instances are launched in public subnets with an Auto Scaling group and Auto Scaling triggers are configured to watch the SQS queue size.

Explanation:-For the exam, remember that Amazon SQS is an Internet-based service. To connect to the Amazon SQS Endpoint (sqs.us-east-1.amazonaws.com), the Amazon EC2 instance requires access to the Internet. Hence, either it should be in a public subnet or be in a private subnet with a NAT instance/gateway in the public subnet. (a) it uses Auto Scaling for ensuring scalability of the application, and (b) it has instances in the public subnet so they can access the SQS service over the internet.

Q30)

A company is making extensive use of S3. They have a strict security policy and require that all artifacts are stored securely in S3.

Which of the following request headers, when specified in an API call, will cause an object to be SSE? Choose the correct option from the below:

- amz-server-side-encryption
- AES256
- server-side-encryption
- ✅ x-amz-server-side-encryption

Explanation:-Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. The object creation REST APIs (see Specifying Server-Side Encryption Using the REST API) provides a request header, x-amz-server-side-encryption that you can use to request server-side encryption. To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS. The following code example shows a Put request using SSE-S3. PUT /example-object HTTP/1.1 Host: myBucket.s3.amazonaws.com Date: Wed, 8 Jun 2016 17:50:00 GMT Authorization: authorization string Content-Type: text/plain Content-Length: 11434 x-amz-meta-author: Janet Expect: 100-continue x-amz-server-side-encryption: AES256 [11434 bytes of object data] In order to enforce object encryption, create an S3 bucket policy that denies any S3 Put request that does not include the x-amz-server-side-encryption header. There are two possible values for the x-amz-server-side-encryption header: AES256, which tells S3 to use S3-managed keys, and aws:kms, which tells S3 to use AWS KMS–managed keys.

Q31)

A user has created a VPC with public and private subnets using the VPC wizard.

Which of the below-mentioned statements is not true in this scenario?

- ✅ The VPC will create a routing instance and attach it with a public subnet.
- The VPC will create one internet gateway and attach it to VPC.
- The VPC will create two subnets.
- The VPC will launch one NAT Gateway with an elastic IP.

Q32) Which of the following benefits does adding Multi-AZ deployment in RDS provide? Choose answers from the options given below:

- Decrease latencies if app servers accessing database are in multiple Availability zones.
- ✅ Make database more available during maintenance tasks.

Explanation:-Some of the advantages of Multi-AZ rds deployments are given below If an Availability Zone failure or DB Instance failure occurs, your availability impact is limited to the time automatic failover takes to complete The availability benefits of Multi-AZ deployments also extend to planned maintenance and backups. In the case of system upgrades like OS patching or DB Instance scaling, these operations are applied first on the standby, prior to the automatic failover. As a result, your availability impact is, again, only the time required for automatic failover to complete. If a storage volume on your primary fails in a Multi-AZ deployment, Amazon RDS automatically initiates a failover to the up-to-date standby For more information on Multi-AZ rds deployments please visit the link https://aws.amazon.com/rds/details/multi-az/ The correct answers are: Multi-AZ deployed database can tolerate an Availability Zone failure., Make database more available during maintenance tasks.

- ✅ Multi-AZ deployed database can tolerate an Availability Zone failure.

Explanation:-Some of the advantages of Multi-AZ rds deployments are given below If an Availability Zone failure or DB Instance failure occurs, your availability impact is limited to the time automatic failover takes to complete The availability benefits of Multi-AZ deployments also extend to planned maintenance and backups. In the case of system upgrades like OS patching or DB Instance scaling, these operations are applied first on the standby, prior to the automatic failover. As a result, your availability impact is, again, only the time required for automatic failover to complete. If a storage volume on your primary fails in a Multi-AZ deployment, Amazon RDS automatically initiates a failover to the up-to-date standby For more information on Multi-AZ rds deployments please visit the link https://aws.amazon.com/rds/details/multi-az/ The correct answers are: Multi-AZ deployed database can tolerate an Availability Zone failure., Make database more available during maintenance tasks.

- Make database access times faster for all app servers.

Q33)

You are the new IT architect in a company that operates a mobile sleep tracking application. When activated at night, the mobile app is sending collected data points of 1 KB every 5 minutes to your middleware.

The middleware layer takes care of authenticating the user and writing the data points into an Amazon DynamoDB table.

Every morning, you scan the table to extract and aggregate last night's data on a per-user basis, and store the results in Amazon S.

Users are notified via Amazon SMS mobile push notifications that new data is available, which is parsed and visualized by the mobile app.

Currently, you have around 100k users.

You have been tasked to optimize the architecture of the middleware system to lower the cost. What would you recommend? Choose 2 options from below:

- Write data directly into an Amazon Redshift cluster replacing both Amazon DynamoDB and Amazon S3.
- . Introduce Amazon Elasticache to cache reads from the Amazon DynamoDB table and reduce provisioned read throughput.
- ✅ Create a new Amazon DynamoDB table each day and drop the one for the previous day after its data is on Amazon S3.

Explanation:-(a) The data stored would be old/obsolete anyways and need not be stored; hence, lowering the cost, and (b) Storing the data in DynamoDB is expensive; hence, you should not keep the tables with the data not needed.

- ✅ Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput.

Explanation:-(a) it uses SQS which reduce the provisioned output cutting down on the costs, and (b) acts as a buffer that absorbs sudden higher load, eliminating going over the provisioned capacity.

- Have the mobile app access Amazon DynamoDB directly instead of JSON files stored on Amazon S3.

Q34)

You are designing a photo-sharing mobile app.

The application will store all pictures in a single Amazon S3 bucket.

Users will upload pictures from their mobile device directly to Amazon S3 and will be able to view and download their own pictures directly from Amazon S3.

You want to configure security to handle potentially millions of users in the most secure manner possible.

What should be done by your server-side application, when a new user registers on the photo-sharing mobile application?

- Create an IAM user. Update the bucket policy with appropriate permissions for the IAM user. Generate an access Key and secret Key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
- Create a set of long-term credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app and use them to access Amazon S3.
- Record the user's Information In Amazon DynamoDB. When the user uses their mobile app create temporary credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.
- ✅ Record the user's Information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app create temporary credentials using the AWS Security Token Service 'AssumeRole' function, store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.

Explanation:-(a) it creates an IAM Role with appropriate permissions, (b) it generates temporary security credentials using STS "AssumeRole" function, and (c) it generates new credentials when the user runs the app the next time.

- Create IAM user. Assign appropriate permissions to the IAM user Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.

Q35) Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

- Use an IAM policy that references the LDAP account identifiers and the AWS credentials.
- Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.
- ✅ Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.

Explanation:-The SAML protocol is used to integrate on-premise IDAP servers with AWS services.

- Use the LDAP credentials to restrict a group of users from launching specific EC2 instance types.
- Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.

Q36)

There is a requirement to create EMR jobs that shift through all of the web server logs and error logs to pull statistics on click stream and errors based off of client IP address.

Given the requirements what would be the best method for collecting the log data and analyzing it automatically? Choose the correct answer from the below options:

- If the application is using HTTP, you need to configure proxy protocol to pass the client IP address in a new HTTP header. If the application is using TCP, modify the application code to pull the client IP into the x-forward-for header so the web servers can parse it.
- ✅ If the application is using TCP, configure proxy protocol to pass the client IP address in a new TCP header. If the application is using, HTTP modify the application code to pull the client IP into the x-forward-for header so the web servers can parse it.

Explanation:-If the application is using TCP, configure proxy protocol to pass the client IP address in a new TCP header. If the application is using, HTTP modify the application code to pull the client IP into the x-forward-for header so the web servers can parse it.

- Configure ELB error logs then create a Data Pipeline job which imports the logs from an S3 bucket into EMR for analyzing and outputs the EMR data into a new S3 bucket.
- Configure ELB access logs then create a Data Pipeline job which imports the logs from an S3 bucket into EMR for analyzing and output the EMR data into a new S3 bucket.

Q37)

You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3. An Elastic Map Reduce job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO.

You recently improved the overall performance of the website using Cloud Front for dynamic content delivery and your website as the origin.

After this architectural change, the usage dashboard shows that the traffic on your website dropped by an order of magnitude.

How will you fix your usage dashboard?

- Turn on Cloud Trail and use trail log tiles on S3 as input of the Elastic Map Reduce job
- Use Elastic Beanstalk “Rebuild Environment” option to update log delivery to the Elastic Map Reduce job.
- Use Elastic Beanstalk ‘Restart App server(s)” option to update log delivery to the Elastic Map Reduce job.
- ✅ Enable Cloud Front to deliver access logs to S3 and use them as input of the Elastic Map Reduce job.

Explanation:-In this scenario, you have a web site that is set up using Elastic Beanstalk. This web site delivers logs to S3, which is used by the EMR job to show the usage dashboard. Now, the architecture is changed, where CloudFront is used to deliver the dynamic content, and is using web site as the origin. The effect that is seen is that the dashboard now shows that the trafic to the website is reduced. The most likely reason for this is that the dashboard is not getting the true data of the traffic. Since it is unlikely that EMR failed to get the entire data, the most likely cause could be that the S3 may not have the logs of the entire traffic to the website. Hence, most likely reason is that the CloudFront is not sending the logs to S3. if CloudFront delivers the logs to S3, the EMR job will pick those logs and update the dashboard.

- Change your log collection process to use Cloud Watch ELB metrics as input of the Elastic Map Reduce job

---

Q38)

Your company is hosting a web application on AWS. According to the architectural best practices, the application must be highly available, scalable, cost effective, with high-performance and should require minimal human intervention.

You have deployed the web servers and database servers in public and private subnet of the VPC respectively.

While testing the application via web browser, you noticed that the application is not accessible.

Which configuration settings you must do to tackle this problem? Choose 2 options from below:

- ✅ Assign EIP's to all web servers. Configure a Route53 A-Record set with all EIPs with health checks and DNS failover.

Explanation:-(a) if the web servers are behind an ELB, the load on the web servers will be uniformly distributed. Hence, if any of the web servers goes offline or becomes non-responsive, the traffic would be routed to other online web servers; making the application highly available, (b) In Route53, you can either resolve the DNS query via creating an ALIAS record pointing to the ELB endpoint or an A record pointing to the IP Addresses of the application. As the EIPs are static (will not be changed) and can be assigned to new web servers if any of the web servers becomes offline, the EIPs can be used in the A record. The health check would ensure that Route53 checks the health of the record set before the failover to other web servers.

- Configure a NAT instance in your VPC and create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address.
- ✅ Place all your web servers behind ELB. Configure a Route53 ALIAS-Record to point to the ELB DNS name.

Explanation:-(a) if the web servers are behind an ELB, the load on the web servers will be uniformly distributed. Hence, if any of the web servers goes offline or becomes non-responsive, the traffic would be routed to other online web servers; making the application highly available, and (b) You can use Route53 to set the ALIAS record that points to the ELB endpoint.

- Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.
- Configure ELB with an EIP. Place all your Web servers behind ELB. Configure a Route53 A record that points to the EIP.

Q39) What are some of the best practices when managing permissions for Opswork? Choose 3 answers from the below options:

- ✅ Users should only have access permission to the resources they need as part of the Opswork stack.

Explanation:-The following are some general guidelines for providing access to your employees. First and foremost, we recommend that you do not use your account's root credentials to access AWS resources. Instead, create IAM users for your employees and attach policies that provide appropriate access. Each employee can then use their IAM user credentials to access resources. Employees should have permissions to access only those resources that they need to perform their jobs. For example, application developers need to access only the stacks that run their applications. Employees should have permissions to use only those actions that they need to perform their jobs. An application developer might need full permissions for a development stack and permissions to deploy their apps to the corresponding production stack.

- Use the root account for managing the resources attached to Opswork.
- ✅ Application developers need to access only the stacks that run their applications.

Explanation:-The following are some general guidelines for providing access to your employees. First and foremost, we recommend that you do not use your account's root credentials to access AWS resources. Instead, create IAM users for your employees and attach policies that provide appropriate access. Each employee can then use their IAM user credentials to access resources. Employees should have permissions to access only those resources that they need to perform their jobs. For example, application developers need to access only the stacks that run their applications. Employees should have permissions to use only those actions that they need to perform their jobs. An application developer might need full permissions for a development stack and permissions to deploy their apps to the corresponding production stack.

- ✅ Create IAM users for your users and attach policies that provide appropriate access.

Explanation:-The following are some general guidelines for providing access to your employees. First and foremost, we recommend that you do not use your account's root credentials to access AWS resources. Instead, create IAM users for your employees and attach policies that provide appropriate access. Each employee can then use their IAM user credentials to access resources. Employees should have permissions to access only those resources that they need to perform their jobs. For example, application developers need to access only the stacks that run their applications. Employees should have permissions to use only those actions that they need to perform their jobs. An application developer might need full permissions for a development stack and permissions to deploy their apps to the corresponding production stack.

Q40)

Your company is running a website on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance.

The site performs a high number of small reads and writes per second and relies on an eventual consistency model.

After comprehensive tests, you discover that there is read contention on RDS MySQL.

Which are the best approaches to meet these requirements? Choose 2 answers from the below options:

- Increase the RDS MySQL Instance size and Implement provisioned IOPS.
- ✅ Add an RDS MySQL read replica in each availability zone.

Explanation:-Implement Read Replicas and Elastic Cache Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.

- Implement sharding to distribute load to multiple RDS MySQL instances.
- ✅ Deploy ElasticCache in-memory cache running in each availability zone.

Explanation:-Implement Read Replicas and Elastic Cache Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.

Q41) What are some of the common types of content that are supported by a web distribution via CloudFront? Choose 3 options from the below:

- ✅ Static content

Explanation:-You can use web distributions to serve the following content over HTTP or HTTPS: Static and dynamic download content, for example, .html, .css, .php, and image files, using HTTP or HTTPS. Multimedia content on demand using progressive download and Apple HTTP Live Streaming (HLS). A live event, such as a meeting, conference, or concert, in real time. For live streaming, you create the distribution automatically by using an AWS CloudFormation Stack.

- ✅ Multimedia content

Explanation:-You can use web distributions to serve the following content over HTTP or HTTPS: Static and dynamic download content, for example, .html, .css, .php, and image files, using HTTP or HTTPS. Multimedia content on demand using progressive download and Apple HTTP Live Streaming (HLS). A live event, such as a meeting, conference, or concert, in real time. For live streaming, you create the distribution automatically by using an AWS CloudFormation Stack.

- ✅ Live events

Explanation:-You can use web distributions to serve the following content over HTTP or HTTPS: Static and dynamic download content, for example, .html, .css, .php, and image files, using HTTP or HTTPS. Multimedia content on demand using progressive download and Apple HTTP Live Streaming (HLS). A live event, such as a meeting, conference, or concert, in real time. For live streaming, you create the distribution automatically by using an AWS CloudFormation Stack.

- Peer to peer networking

Q42)

The company runs a complex customer system and consists of 10 different software components all backed up by RDS.

You adopted Opswork to simplify management and deployment of that application and created a stack and layers for each component.

A security policy requires that all instances should run on the latest AMI and that instances must be replaced within one month after the latest AMI has been released.

AMI replacements should be done without incurring application downtime or capacity problems.

You decide to write a script to be run as soon as the new AMI is released. Choose 2 options which meet your requirements:

- Assign a custom recipe to each layer which replaces the underlying AMI. Use OpsWorks life-cycle events to incrementally execute this custom recipe and update the instances with the new AMI.
- ✅ Add new instances with the latest Amazon AMI as a custom AMI to all OpsWork layers of your stack and terminate the old ones.

Explanation:-you can only add new instances at the layer level by specifying to use Custom AMI at the stack level. More information on Blue-Green Deployment: Blue-green deployment is a technique that reduces downtime and risk by running two identical production environments called Blue and Green. At any time, only one of the environments is live, with the live environment serving all production traffic.

- Specify the latest AMI as the custom AMI at the stack level terminates instances of the stack and let OpsWork launch new instances with the new AMI.
- Identify all EC2 instances of your OpsWork stack, stop each instance, replace the AMI ID property with the latest AMI ID, and restart the instance. To avoid down time, make sure no more than one instance is stopped at the same time.
- ✅ Create a new stack and layers with identical configuration, add instances with the latest AMI specified as a custom AMI to the new layers, switch DNS to the new stack, and tear down the old stack.

Explanation:-it represents a common practice of Blue-Green Deployment which is carried out for reducing the downtime and risk by running two identical production environments called Blue and Green. Please see "More information.." section for additional details.

Q43)

A marketing research company has developed a tracking system that collects user behavior during web marketing campaigns on behalf of the customers all over the world.

The tracking system consists of an auto-scaled group of EC2 instances behind an ELB. And the collected data is stored in DynamoDB.

After the campaign is terminated the tracking system is torn down and the data is moved to Amazon Redshift, where it is aggregated and used to generate detailed reports.

The company wants to be able to instantiate new tracking systems in any region without any manual intervention and therefore adopted CloudFormation.

What needs to be done to make sure that the AWS Cloudformation template works for every AWS region? Choose 2 options from the below:

✅ Use the built-in Mappings and FindInMap functions of AWS Cloudformation to refer to the AMI ID set in the ImageID attribute of the Autoscaling::LaunchConfiguration resource.

Explanation:-the AMI ID would be needed to launch the similar instances in the new region where the template would be used.

- The names of the DynamoDB tables must be different in every target region.
- IAM users with the right to start Cloudformation stacks must be defined for every target region.
- Avoid using Deletion Policies for the EBS snapshots.
- ✅ Use the built-in function of Cloudformation to set the AZ attribute of the ELB resource.

Explanation:-you need to get the name of the Availability Zone based on the region in which the template would be used.

Q44) Which is the following services can be used to deploy systems into AWS? Choose 3 answers from the options below.

- Amazon ElasticCache
- ✅ AWS Opsworks

Explanation:-With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

- ✅ AWS Cloudformation

Explanation:-With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

- Amazon Kinesis
- ✅ AWS beanstalk

Explanation:-With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

Q45)

A company has the requirement to transfer large datasets quite frequently from their on-premise location to AWS.

Which of the below connections should ideally be established to fulfill this requirement?

- Internet Gateway
- VPN connection
- Customer gateway
- ✅ DirectConnect

Explanation:-With AWS Direct Connect, you can transfer your business-critical data directly from your datacenter, office, or colocation environment into and from AWS bypassing your Internet service provider and removing network congestion. Further, AWS Direct Connect's simple pay-as-you-go pricing, and no minimum commitment means you pay only for the network ports you use and the data you transfer over the connection, which can greatly reduce your networking costs.

Q46)

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?

- ✅ Add an Elastic Load Balancing health check to your Auto Scaling group.

Explanation:-To discover the availability of your EC2 instances, a load balancer 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 The load balancer checks the health of the registered instances using either the default health check configuration provided by Elastic Load Balancing or a health check configuration that you configure. When configuring the Autoscaling group, you can choose either the option of EC2 or ELB health checks. Since Ec2 instances are being marked as unhealthy by ELB but not being terminated by Autoscaling it means that the check from the Autoscaling side is wrongly configured.

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

Q47)

A user has created a VPC with public and private subnets using the VPC wizard.

The user has not launched any instance manually and is trying to delete the VPC.

What will happen in this scenario?

- It will not allow to delete the VPC since it has a running route instance.
- It will terminate the VPC along with all the instances launched by the wizard.
- It will not allow to delete the VPC as it has subnets with route tables.
- ✅ It will not allow to delete the VPC since it has a running NAT instance.

Explanation:-Since the VPC will contain a NAT instance because of the private/public subnet combination, when you try to delete the VPC you will get the error message.

Q48)

By default, when an EBS volume is attached to a Windows instance, it may show up as any drive letter on the instance.

For which services can you use to change the settings of the drive letters of the EBS volumes per your specifications?

- AMIConfig Service
- ✓ Ec2Config Service

Explanation:-Windows AMIs include an optional service called the EC2Config service (EC2Config.exe). EC2Config starts when the instance boots and performs tasks during startup and each time you stop or start the instance. EC2Config can also perform tasks on demand. Some of these tasks are automatically enabled, while others must be enabled manually. Although optional, this service provides access to advanced features that aren't otherwise available. This service runs in the LocalSystem account.

- Ec2-AMIConfig Service
- EBSConfig Service