Answer Sheet

Q1)

A user has created a queue named “myqueue” with SQS. There are four messages published to queue which are not received by the consumer yet.

If the user tries to delete the queue, what will happen?

- It will ask user to delete the messages first
- It will initiate the delete but wait for four days before deleting until all messages are deleted automatically.
- A user can never delete a queue manually. AWS deletes it after 30 days of inactivity on queue
- ✅ It will delete the queue

Explanation:-SQS allows the user to move data between distributed components of applications so they can perform different tasks without losing messages or requiring each component to be always available. The user can delete a queue at any time, whether it is empty or not. It is important to note that queues retain messages for a set period of time. By default, a queue retains messages for four days.

Q2)

A user had aggregated the CloudWatch metric data on the AMI ID. The user observed some abnormal behaviour of the CPU utilization metric while viewing the last 2 weeks of data.

The user wants to share that data with his manager.

How can the user achieve this easily with the AWS console?

- The user has to find the period and data and provide all the aggregation information to the manager
- The user can use the export data option from the CloudWatch console to export the current data point
- The user can use the CloudWatch data copy functionality to copy the current data points
- ✅ The user can use the copy URL functionality of CloudWatch to share the exact details

Explanation:-Amazon CloudWatch provides the functionality to graph the metric data generated either by the AWS services or the custom metric to make it easier for the user to analyse. The console provides the option to save the URL or bookmark it so that it can be used in the future by typing the same URL. The Copy URL functionality is available under the console when the user selects any metric to view.

Q3)

An AWS account wants to be part of the consolidated billing of his organization’s payee account.

How can the owner of that account achieve this?

- The owner of the linked account requests the payee account to add his account to consolidated billing
- The payee account has to request AWS support to link the other accounts with his account
- The owner of the linked account should add the payee account to his master account list from the billing console
- ✅ The payee account will send a request to the linked account to be a part of consolidated billing

Explanation:-AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. To add a particular account (linked) to the master (payee) account, the payee account has to request the linked account to join consolidated billing. Once the linked account accepts the request henceforth all charges incurred by the linked account will be paid by the payee account.

Q4)

A user has launched an EC2 instance store backed instance in the US-East-1a zone. The user created AMI #1 and copied it to the Europe region.

After that, the user made a few updates to the application running in the US-East-1a zone. The user makes an AMI#2 after the changes.

If the user launches a new instance in Europe from the AMI #1 copy, which of the below mentioned statements is true?

- The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI
- The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copying. Thus, the copied AMI will have all the updated data
- ✅ The new instance in the EU region will not have the changes made after the AMI copy

Explanation:-Within EC2, when the user copies an AMI, the new AMI is fully independent of the source AMI; there is no link to the original (source) AMI. The user can modify the source AMI without affecting the new AMI and vice a versa. Therefore, in this case even if the source AMI is modified, the copied AMI of the EU region will not have the changes. Thus, after copy the user needs to copy the new source AMI to the destination region to get those changes.

- It is not possible to copy the instance store backed AMI from one region to another

---

Q5)

A user has configured the Auto Scaling group with the minimum capacity as 3 and the maximum capacity as 5.

When the user configures the AS group, how many instances will Auto Scaling launch?

- ✅ 3

Explanation:-When the user configures the launch configuration and the Auto Scaling group, the Auto Scaling group will start instances by launching the minimum number (or the desired number, if specified) of EC2 instances. If there are no other scaling conditions attached to the Auto Scaling group, it will maintain the minimum number of running instances at all times.

- TRUE

- 5
- 2

Q6)

An organization has created a Queue named “modularqueue” with SQS.

The organization is not performing any operations such as SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermission, and RemovePermission on the queue.

What can happen in this scenario?

- ✅ AWS SQS can delete queue after 30 days without notification

Explanation:-Amazon SQS can delete a queue without notification if one of the following actions hasn’t been performed on it for 30 consecutive days: SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermission, and RemovePermission.

- AWS SQS notifies the user after 2 weeks and deletes the queue after 3 weeks.
- AWS SQS sends notification after 15 days for inactivity on queue
- AWS SQS marks queue inactive after 30 days

Q7)

A sys admin is using server side encryption with AWS S3.

Which of the below mentioned statements helps the user understand the S3 encryption functionality?

- The user can use the AWS console, SDK and APIs to encrypt or decrypt the content for server side encryption with the user supplied key
- The user can upload his own encryption key to the S3 console
- The user must send an AES-128 encrypted key
- ✅ The server side encryption with the user supplied key works when versioning is enabled

Explanation:-AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key. The encryption with the user supplied key (SSE-C) does not work with the AWS console. The S3 does not store the keys and the user has to send a key with each request. The SSE-C works when the user has enabled versioning.

Q8)

A user has created a web application with Auto Scaling. The user is regularly monitoring the application and he observed that the traffic is highest on Thursday and Friday between 8 AM to 6 PM.

What is the best solution to handle scaling in this case?

- Add a new instance manually by 8 AM Thursday and terminate the same by 6 PM Friday
- Configure a batch process to add a instance by 8 AM and remove it by Friday 6 PM
- ✅ Schedule Auto Scaling to scale up by 8 AM Thursday and scale down after 6 PM on Friday

Explanation:-Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. In this case the load increases by Thursday and decreases by Friday. Thus, the user can setup the scaling activity based on the predictable traffic patterns of the web application using Auto Scaling scale by Schedule.

- Schedule a policy which may scale up every day at 8 AM and scales down by 6 PM

Q9)

A sys admin has enabled logging on ELB.

Which of the below mentioned fields will not be a part of the log file name?

- Load Balancer IP
- ✅ EC2 instance IP

Explanation:-Elastic Load Balancing access logs capture detailed information for all the requests made to the load balancer. Elastic Load Balancing publishes a log file from each load balancer node at the interval that the user has specified. The load balancer can deliver multiple logs for the same period. Elastic Load Balancing creates log file names in the following format:
“{Bucket}/{Prefix}/AWSLogs/{AWS AccountID}/elasticloadbalancing/{Region}/{Year}/{Month}/{Day}/{AWS Account ID}_elasticloadbalancing_{Region}_{Load Balancer Name}_{End Time}_{Load Balancer IP}_{Random String}.log“

- Random string
- S3 bucket name

Q10)

A user has scheduled the maintenance window of an RDS DB on Monday at 3 AM.

Which of the below mentioned events may force to take the DB instance offline during the maintenance window?

- Enabling Read Replica
- DB password change
- ✅ Security patching

Explanation:-Amazon RDS performs maintenance on the DB instance during a user-definable maintenance window. The system may be offline or experience lower performance during that window. The only maintenance events that may require RDS to make the DB instance offline are:
Scaling compute operations
Software patching. Required software patching is automatically scheduled only for patches that are security and durability related. Such patching occurs infrequently (typically once every few months) and seldom requires more than a fraction of the maintenance window.

- Backing up the database

Q11)

A user has created an Auto Scaling group with default configurations from CLI. The user wants to setup the CloudWatch alarm on the EC2 instances, which are launched by the Auto Scaling group.

The user has setup an alarm to monitor the CPU utilization every minute.

Which of the below mentioned statements is true?

- The alarm creation will fail since the user has not enabled detailed monitoring on the EC2 instances
- It will fetch the data at every minute but the four data points [corresponding to 4 minutes] will not have value since the EC2 basic monitoring metrics are collected every five minutes
- ✅ It will fetch the data at every minute as detailed monitoring on EC2 will be enabled by the default launch configuration of Auto Scaling

Explanation:-CloudWatch is used to monitor AWS as well as the custom services. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates an Auto Scaling launch config using CLI, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. Thus, by default detailed monitoring will be enabled for Auto Scaling as well as for all the instances launched by that Auto Scaling group.

- The user has to first enable detailed monitoring on the EC2 instances to support alarm monitoring at every minute

---

Q12)

A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet.

How can the instances in the private subnet connect to the internet?

- Use the internet gateway with a private IP
- ✅ Use NAT with an elastic IP

Explanation:-A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created two subnets (one private and one public), they would need a Network Address Translation (NAT) instance with the elastic IP address. This enables the instances in the private subnet to send requests to the internet (for example, to perform software updates).

- Allow outbound traffic in the security group for port 80 to allow internet updates
- The private subnet can never connect to the internet

Q13)

The CFO of a company wants to allow one of his employees to view only the AWS usage report page.

Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?

- ✅ "Effect": "Allow", "Action": ["aws-portal:ViewUsage"], "Resource": "*"

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the CFO wants to allow only AWS usage report page access, the policy for that IAM user will be as given below:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"aws-portal:ViewUsage"
],
"Resource": "*"
}
]
}
```

- "Effect": "Allow", "Action": ["aws-portal: ViewBilling"], "Resource": "*"
- "Effect": "Allow", "Action": ["Describe"], "Resource": "Billing"
- "Effect": "Allow", "Action": ["AccountUsage], "Resource": "*"

Q14)

A sys admin is planning to subscribe to the RDS event notifications.

For which of the below mentioned source categories the subscription cannot be configured?

- DB parameter group
- DB security group
- DB snapshot
- ✅ DB options group

Explanation:-Amazon RDS uses the Amazon Simple Notification Service (SNS) to provide a notification when an Amazon RDS event occurs. These events can be configured for source categories, such as DB instance, DB security group, DB snapshot and DB parameter group.

Q15)

A user has setup a web application on EC2. The user is generating a log of the application performance at every second.

There are multiple entries for each second.

If the user wants to send that data to CloudWatch every minute, what should he do?

- The user should send only the data of the 60th second as CloudWatch will map the receive data timezone with the sent data timezone
- Calculate the average of one minute and send the data to CloudWatch
- It is not possible to send the custom metric to CloudWatch every minute
- ✅ Give CloudWatch the Min, Max, Sum, and SampleCount of a number of every minute

Explanation:-Amazon CloudWatch aggregates statistics according to the period length that the user has specified while getting data from CloudWatch. The user can publish as many data points as he wants with the same or similar time stamps. CloudWatch aggregates them by the period length when the user calls get statistics about those data points. CloudWatch records the average (sum of all items divided by the number of items) of the values received for every 1-minute period, as well as the number of samples, maximum value, and minimum value for the same time period. CloudWatch will aggregate all the data which have time stamps within a one-minute period.

Q16)

A user has created an S3 bucket which is not publicly accessible. The bucket is having thirty objects which are also private.

If the user wants to make the objects public, how can he configure this with minimal efforts?

- The user should select all objects from the console and apply a single policy to mark them public
- ✅ Set the AWS bucket policy which marks all objects as public

Explanation:-A system admin can grant permission of the S3 objects or buckets to any user or make the objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if the user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket.

- The user can write a program which programmatically makes all objects public using S3 SDK
- Make the bucket ACL as public so it will also mark all objects as public

---

Q17)

A sys admin has created a shopping cart application and hosted it on EC2. The EC2 instances are running behind ELB.

The admin wants to ensure that the end user request will always go to the EC2 instance where the user session has been created.

How can the admin configure this?

- Enable ELB cookie setup
- ✅ Enable ELB sticky session

Explanation:-Generally AWS ELB routes each request to a zone with the minimum load. The Elastic Load Balancer provides a feature called sticky session which binds the user's session with a specific EC2 instance. If the sticky session is enabled the first request from the user will be redirected to any of the EC2 instances. But, henceforth, all requests from the same user will be redirected to the same EC2 instance. This ensures that all requests coming from the user during the session will be sent to the same application instance.

- Enable ELB cross zone load balancing
- Enable ELB connection draining

Q18)

A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer.

The ELB security policy supports various ciphers.

Which of the below mentioned options helps identify the matching cipher at the client side to the ELB cipher list when client is requesting ELB DNS over SSL?

- Client Configuration Preference
- Load Balancer Preference
- Cipher Protocol
- ✅ Server Order Preference

Explanation:-Elastic Load Balancing uses a Secure Socket Layer (SSL) negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. When client is requesting ELB DNS over SSL and if the load balancer is configured to support the Server Order Preference, then the load balancer gets to select the first cipher in its list that matches any one of the ciphers in the client's list. Server Order Preference ensures that the load balancer determines which cipher is used for the SSL connection.

Q19)

A user has created a VPC with the public subnet. The user has created a security group for that VPC.

Which of the below mentioned statements is true when a security group is created?

- It can connect to the AWS services, such as S3 and RDS by default
- ✅ It will have all the outbound traffic by default but block all inbound traffic.

Explanation:-A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. AWS provides two features the user can use to increase security in VPC: security groups and network ACLs. Security groups work at the instance level while ACLs work at the subnet level. When a user creates a security group with AWS VPC, by default it will allow all the outbound traffic but block all inbound traffic.

- It will have all the inbound traffic by default
- It will by default allow traffic to the internet gateway

Q20)

A user has setup a CloudWatch alarm on the EC2 instance for CPU utilization. The user has setup to receive a notification on email when the CPU utilization is higher than 60%. The user is running a virus scan on the same instance at a particular time.

The user wants to avoid receiving an email at this time.

What should the user do?

- Remove the alarm
- Disable the alarm for a while using the console
- Modify the CPU utilization by removing the email alert
- ✅ Disable the alarm for a while using CLI

Explanation:-Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. When the user has setup an alarm and it is know that for some unavoidable event the status may change to Alarm, the user can disable the alarm using the DisableAlarmActions API or from the command line mon-disable-alarm-actions.

Q21)

A user is launching an EC2 instance in the US East region.

Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

- Always select the AZ while launching an instance
- Always select the US-East-1-a zone for HA
- The user can never select the availability zone while launching an instance
- ✅ Do not select the AZ; instead let AWS select the AZ

Explanation:-When launching an instance with EC2, AWS recommends not to select the availability zone (AZ). AWS specifies that the default Availability Zone should be accepted. This is because it enables AWS to select the best Availability Zone based on the system health and available capacity. If the user launches additional instances, only then an Availability Zone should be specified. This is to specify the same or different AZ from the running instances.

Q22)

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

The private subnet uses CIDR 20.0.0.0/24 .

The NAT instance ID is i-a12345.

Which of the below mentioned entries are required in the main route table attached with the private subnet to allow instances to connect with the internet?

- Destination: 20.0.0.0/0 and Target: i-a12345
- ✅ Destination: 0.0.0.0/0 and Target: i-a12345

Explanation:-A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create two route tables and attach to the subnets. The main route table will have the entry “Destination: 0.0.0.0/0 and Target: i-a12345”, which allows all the instances in the private subnet to connect to the internet using NAT.

- Destination: 20.0.0.0/24 and Target: i-a12345
- Destination: 20.0.0.0/0 and Target: 80

Q23)

A user is displaying the CPU utilization, and Network in and Network out CloudWatch metrics data of a single instance on the same graph.

The graph uses one Y-axis for CPU utilization and Network in and another Y-axis for Network out.

Since Network in is too high, the CPU utilization data is not visible clearly on graph to the user.

How can the data be viewed better on the same graph?

- It is not possible to show multiple metrics with the different units on the same graph
- Add a third Y-axis with the console to show all the data in proportion
- ✅ Change the axis of Network by using the Switch command from the graph

Explanation:-Amazon CloudWatch provides the functionality to graph the metric data generated either by the AWS services or the custom metric to make it easier for the user to analyse. It is possible to show the multiple metrics with different units on the same graph. If the graph is not plotted properly due to a difference in the unit data over two metrics, the user can change the Y-axis of one of the graph by selecting that graph and clicking on the Switch option.

- Change the units of CPU utilization so it can be shown in proportion with Network

---

Q24)

A user has launched an EC2 instance from an instance store backed AMI. The user has attached an additional instance store volume to the instance.

The user wants to create an AMI from the running instance.

Will the AMI have the additional instance store volume data?

- It is not possible to attach an additional instance store volume to the existing instance store backed AMI instance
- No, since this is ephermal storage it will not be a part of the AMI
- No, since the instance store backed AMI can have only the root volume bundled
- ✅ Yes, the block device mapping will have information about the additional instance store volume

Explanation:-When the user has launched an EC2 instance from an instance store backed AMI and added an instance store volume to the instance in addition to the root device volume, the block device mapping for the new AMI contains the information for these volumes as well. In addition, the block device mappings for the instances those are launched from the new AMI will automatically contain information for these volumes.

Q25)

A user has a refrigerator plant. The user is measuring the temperature of the plant every 15 minutes.

If the user wants to send the data to CloudWatch to view the data visually, which of the below mentioned statements is true with respect to the information given above?

- ✅ The user needs to use AWS CLI or API to upload the data

Explanation:-AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. While sending the data the user has to include the metric name, namespace and timezone as part of the request.

- The user cannot upload data to CloudWatch since it is not an AWS service metric
- The user will upload data from the AWS console
- The user can use the AWS Import Export facility to import data to CloudWatch

---

Q26)

An organization has been using AWS for a few months.

The finance team wants to visualize the pattern of AWS spending.

Which of the below AWS tools will help for this requirement?

- AWS CloudWatch
- AWS Cost Manager
- ✅ AWS Cost Explorer

Explanation:-The AWS Billing and Cost Management console includes the Cost Explorer tool for viewing AWS cost data as a graph. It does not charge extra to user for this service. With Cost Explorer the user can filter graphs using resource tags or with services in AWS. If the organization is using Consolidated Billing it helps generate report based on linked accounts. This will help organization to identify areas that require further inquiry. The organization can view trends and use that to understand spend and to predict future costs.

- AWS Consolidated Billing

Q27)

A user is trying to aggregate all the CloudWatch metric data of the last 1 week.

Which of the below mentioned statistics is not available for the user as a part of data aggregation?

- ✅ Aggregate

Explanation:-Amazon CloudWatch is basically a metrics repository. Either the user can send the custom data or an AWS product can put metrics into the repository, and the user can retrieve the statistics based on those metrics. The statistics are metric data aggregations over specified periods of time. Aggregations are made using the namespace, metric name, dimensions, and the data point unit of measure, within the time period that is specified by the user. CloudWatch supports Sum, Min, Max, Sample Data and Average statistics aggregation.

- Sum
- Sample data
- Average

Q28)

A user has setup a custom application which generates a number in decimals. The user wants to track that number and setup the alarm whenever the number is above a certain limit.

The application is sending the data to CloudWatch at regular intervals for this purpose.

Which of the below mentioned statements is not true with respect to the above scenario?

- CloudWatch will not truncate the number until it has an exponent larger than 126 (i.e. (1 x 10^126)
- The user can get the aggregate data of the numbers generated over a minute and send it to CloudWatch
- The user can create a file in the JSON format with the metric name and value and supply it to CloudWatch
- ✅ The user has to supply the timezone with each data point

Explanation:-AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The metric value parameter is acceptable as Double but CloudWatch will truncate values with very large exponents. E.g. If the values with base-10 exponents are greater than 126 (1 x 10^126) then it will be truncated. The user can also send data with values in a JSON format with the metric-data parameter. CloudWatch also supports the aggregate data with the statistic set parameter, such as Sum, Min, Max, Sample Data and Average statistics.

Q29)

A user is receiving a notification from the RDS DB whenever there is a change in the DB security group.

The user does not want to receive these notifications for only a month.

Thus, he does not want to delete the notification. How can the user configure this?

- ✅ Change the Enable button for notification to “No” in the RDS console

Explanation:-Amazon RDS uses the Amazon Simple Notification Service to provide a notification when an Amazon RDS event occurs. Event notifications are sent to the addresses that the user has provided while creating the subscription. The user can easily turn off the notification without deleting a subscription by setting the Enabled radio button to No in the Amazon RDS console or by setting the Enabled parameter to false using the CLI or Amazon RDS API.

- Set the send mail flag to false in the DB event notification console
- Change the Disable button for notification to “Yes” in the RDS console
- The only option is to delete the notification from the console

Q30)

A user is planning to use AWS services for his web application.

If the user is trying to set up his own billing management system for AWS, how can he configure it?

- Use AWS billing APIs to download the usage report of each service from the AWS billing console
- It is not possible for the user to create his own billing management service with AWS
- ✅ Set up programmatic billing access. Download and parse the bill as per the requirement

Explanation:-AWS provides an option to have programmatic access to billing. Programmatic Billing Access leverages the existing Amazon Simple Storage Service (Amazon S3) APIs. Thus, the user can build applications that reference his billing data from a CSV (comma-separated value) file stored in an Amazon S3 bucket. AWS will upload the bill to the bucket every few hours and the user can download the bill CSV from the bucket, parse it and create a billing system as per the requirement.

- Enable the AWS CloudWatch alarm which will provide APIs to download the alarm data

---

Q31)

A user is trying to save some cost on the AWS services.

Which of the below mentioned options will not help him save cost?

- Release the elastic IP if not required once the instance is terminated
- Delete the AWS ELB after the instances are terminated
- Delete the unutilized EBS volumes once the instance is terminated
- ✅ Delete the AutoScaling launch configuration after the instances are terminated

Explanation:-AWS bills the user on a as pay as you go model. AWS will charge the user once the AWS resource is allocated. Even though the user is not using the resource, AWS will charge if it is in service or allocated. Thus, it is advised that once the user's work is completed he should:
1. Terminate the EC2 instance
2. Delete the EBS volumes
3. Release the unutilized Elastic IPs
4. Delete ELB

The AutoScaling launch configuration does not cost the user. Thus, it will not make any difference to the cost whether it is deleted or not.

Q32)

A user is trying to launch an EBS backed EC2 instance under free usage. The user wants to achieve encryption of the EBS volume.

How can the user encrypt the data at rest?

- Use AWS EBS encryption to encrypt the data at rest
- The user has to select the encryption enabled flag while launching the EC2 instance
- ✅ The user cannot use EBS encryption and has to encrypt the data manually or using a third party tool

Explanation:-AWS EBS supports encryption of the volume while creating new volumes. It supports encryption of the data at rest, the I/O as well as all the snapshots of the EBS volume. The EBS supports encryption for the selected instance type and the newer generation instances, such as m3, c3, cr1, r3, g2. It is not supported with a micro instance.

- Encryption of volume is not available as a part of the free usage tier

---

Q33)

An organization has created 50 IAM users. The organization has introduced a new policy which will change the access of an IAM user.

How can the organization implement this effectively so that there is no need to apply the policy at the individual user level?

- Add each user to the IAM role as per their organization role to achieve effective policy setup
- ✅ Use the IAM groups and add users as per their role to different groups and apply policy to group
- The user can create a policy and apply it to multiple users in a single go with the AWS CLI
- Use the IAM role and implement access at the role level

Q34)

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 in this VPC.

The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24.

What will happen in this scenario?

- The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range
- It is not possible to create a subnet with the same CIDR as VPC
- The second subnet will be created
- ✅ It will throw a CIDR overlaps error

Explanation:-A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet.

Q35)

A user wants to disable connection draining on an existing ELB.

Which of the below mentioned statements helps the user disable connection draining on the ELB?

- The user needs to stop all instances before disabling connection draining
- The user can only disable connection draining from CLI
- ✅ The user can disable the connection draining feature from EC2 -> ELB console or from CLI

Explanation:-The Elastic Load Balancer connection draining feature causes the load balancer to stop sending new requests to the back-end instances when the instances are deregistering or become unhealthy, while ensuring that in-flight requests continue to be served. The user can enable or disable connection draining from the AWS EC2 console -> ELB or using CLI.

- It is not possible to disable the connection draining feature once enabled

---

Q36)

A user has enabled detailed CloudWatch monitoring with the AWS Simple Notification Service.

Which of the below mentioned statements helps the user understand detailed monitoring better?

- There is no need to enable since SNS provides data every minute
- ✅ SNS cannot provide data every minute

Explanation:-CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. The AWS SNS service sends data every 5 minutes. Thus, it supports only the basic monitoring. The user cannot enable detailed monitoring with SNS.

- SNS will send data every minute after configuration
- AWS CloudWatch does not support monitoring for SNS

Q37)

A user has launched an ELB which has 5 instances registered with it. The user deletes the ELB by mistake.

What will happen to the instances?

- ELB cannot be deleted if it has running instances registered with it
- ELB will ask the user whether to delete the instances or not
- Instances will be terminated
- ✅ Instances will keep running

Explanation:-When the user deletes the Elastic Load Balancer, all the registered instances will be deregistered. However, they will continue to run. The user will incur charges if he does not take any action on those instances.

Q38)

An AWS root account owner is trying to create a policy to access RDS.

Which of the below mentioned statements is true with respect to the above information?

- The user cannot access the RDS database if he is not assigned the correct IAM policy
- The policy should be created for the user and provide access for RDS
- ✅ The root account owner should create a policy for the IAM user and give him access to the RDS services

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the account owner wants to create a policy for RDS, the owner has to create an IAM user and define the policy which entitles the IAM user with various RDS services such as Launch Instance, Manage security group, Manage parameter group etc.

- Create a policy which allows the users to access RDS and apply it to the RDS instances

---

Q39)

A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the user should first understand the namespace for the AWS services.

Which of the below mentioned is not a valid namespace for the AWS services?

- AWS/ElastiCache
- AWS/SWF
- ✅ AWS/CloudTrail

Explanation:-Amazon CloudWatch is basically a metrics repository. The AWS product puts metrics into this repository, and the user can retrieve the data or statistics based on those metrics. To distinguish the data for each service, the CloudWatch metric has a namespace. Namespaces are containers for metrics. All AWS services that provide the Amazon CloudWatch data use a namespace string, beginning with “AWS/”. All the services which are supported by CloudWatch will have some namespace. CloudWatch does not monitor CloudTrail. Thus, the namespace “AWS/CloudTrail” is incorrect.

- AWS/StorageGateway

Q40)

A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25 and a private subnet with CIDR 20.0.0.128/25.

The user has launched one instance each in the private and public subnets.

Which of the below mentioned options cannot be the correct IP address (private IP) assigned to an instance in the public or private subnet?

- 20.0.0.132

✅ 20.0.0.255

Explanation:-When the user creates a subnet in VPC, he specifies the CIDR block for the subnet. In this case the user has created a VPC with the CIDR block 20.0.0.0/24, which supports 256 IP addresses (20.0.0.0 to 20.0.0.255). The public subnet will have IP addresses between 20.0.0.0 – 20.0.0.127 and the private subnet will have IP addresses between 20.0.0.128 – 20.0.0.255. AWS reserves the first four IP addresses and the last IP address in each subnet's CIDR block. These are not available for the user to use. Thus, the instance cannot have an IP address of 20.0.0.255.

- 20.0.0.122
- 20.0.0.55

Q41)

A user has created an Auto Scaling group using CLI. The user wants to enable CloudWatch detailed monitoring for that group.

How can the user configure this?

✅ By default detailed monitoring is enabled for Auto Scaling

Explanation:-CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates an Auto Scaling launch config as the first step for creating an Auto Scaling group, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. Thus, the user does not need to set this flag if he wants detailed monitoring.

- When the user sets an alarm on the Auto Scaling group, it automatically enables detail monitoring
- Auto Scaling does not support detailed monitoring
- Enable detail monitoring from the AWS console

Q42)

A user is trying to setup a recurring Auto Scaling process. The user has setup one process to scale up every day at 8 am and scale down at 7 PM.

The user is trying to setup another recurring process which scales up on the 1st of every month at 8 AM and scales down the same day at 7 PM.

What will Auto Scaling do in this scenario?

- Auto Scaling will add two instances on the 1st of the month
- Auto Scaling will execute both processes but will add just one instance on the 1st

✅ Auto Scaling will throw an error since there is a conflict in the schedule of two separate Auto Scaling processes

Explanation:-Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. The user can also configure the recurring schedule action which will follow the Linux cron format. As per Auto Scaling, a scheduled action must have a unique time value. If the user attempts to schedule an activity at a time when another existing activity is already scheduled, the call will be rejected with an error message noting the conflict.

- Auto Scaling will schedule both the processes but execute only one process randomly

---

Q43)

A user has created an application which will be hosted on EC2. The application makes calls to DynamoDB to fetch certain data.

The application is using the DynamoDB SDK to connect with from the EC2 instance.

Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

- The user should create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB
- The user should create an IAM role, which has EC2 access so that it will allow deploying the application

✅ The user should attach an IAM role with DynamoDB access to the EC2 instance

Explanation:-With AWS IAM a user is creating an application which runs on an EC2 instance and makes requests to AWS, such as DynamoDB or S3 calls. Here it is recommended that the user should not create an IAM user and pass the user's credentials to the application or embed those credentials inside the application. Instead, the user should use roles for EC2 and give that role access to DynamoDB /S3. When the roles are attached to EC2, it will give temporary security credentials to the application hosted on that EC2, to connect with DynamoDB / S3.

- The user should create an IAM user with DynamoDB and EC2 access. Attach the user with the application so that it does not use the root account credentials

---

Q44)

An organization has setup consolidated billing with 3 different AWS accounts.

Which of the below mentioned advantages will organization receive in terms of the AWS pricing?

- The free usage tier for all the 3 accounts will be 3 years and not a single year
- The EC2 instances of each account will receive a total of 750*3 micro instance hours free

✅ There is really no cost advantage with consolidated billing. The advantage is rather the convenience and simplicity of a single bill.

Explanation:-AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. For billing purposes, AWS treats all the accounts on the consolidated bill as one account. Some services, such as Amazon EC2 and Amazon S3 have volume pricing tiers across certain usage dimensions that give the user lower prices when he uses the service more.

- The consolidated billing does not bring any cost advantage for the organization

---

Q45)

A user is planning to schedule a backup for an EBS volume. The user wants security of the snapshot data.

How can the user achieve data encryption with a snapshot?

- By default the snapshot is encrypted by AWS
- ✅ Use encrypted EBS volumes so that the snapshot will be encrypted by AWS

Explanation:-AWS EBS supports encryption of the volume. It also supports creating volumes from existing snapshots provided the snapshots are created from encrypted volumes. The data at rest, the I/O as well as all the snapshots of the encrypted EBS will also be encrypted. EBS encryption is based on the AES-256 cryptographic algorithm, which is the industry standard.

- While creating a snapshot select the snapshot with encryption
- Enable server side encryption for the snapshot using S3

Q46)

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 20.0.0.1/24.

How can the user create the second subnet?

- The user can modify the first subnet CIDR from the console
- 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 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:-A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside the subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet. The user cannot modify the CIDR of a subnet once it is created. Thus, in this case if required, the user has to delete the subnet and create new subnets.

Q47)

A user has setup an Auto Scaling group. The group has failed to launch a single instance for more than 24 hours.

What will happen to Auto Scaling in this condition?

- ✅ Auto Scaling will suspend the scaling process

Explanation:-If Auto Scaling is trying to launch an instance and if the launching of the instance fails continuously, it will suspend the processes for the Auto Scaling groups since it repeatedly failed to launch an instance. This is known as an administrative suspension. It commonly applies to the Auto Scaling group that has no running instances which is trying to launch instances for more than 24 hours, and has not succeeded in that to do so.

- Auto Scaling will start an instance in a separate region
- The Auto Scaling group will be terminated automatically
- Auto Scaling will keep trying to launch the instance for 72 hours

---

Q48)

A user is planning to use AWS Cloudformation for his automatic deployment requirements.

Which of the below mentioned components are required as a part of the template?

- Parameters
- ✅ Resources

Explanation:-AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. The template is a JSON-format, text-based file that describes all the AWS resources required to deploy and run an application. It can have option fields, such as Template Parameters, Output, Data tables, and Template file format version. The only mandatory value is Resource. The user can define the AWS services which will be used/ created by this template inside the Resource section.

- Template version
- Outputs

Q49)

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 uses DNS to switch over to stand by replica for seamless transition

Explanation:-In the event of a planned or unplanned outage of a DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone if the user has enabled Multi AZ. The automatic failover mechanism simply changes the DNS record of the DB instance to point to the standby DB instance. As a result, the user will need to re-establish any existing connections to the DB instance. However, as the DNS is the same, the application can access DB seamlessly.

- RDS will have an internal IP which will redirect all requests to the new DB

Q50)

A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance.

The internet gateway has also been created. What can be the reason for the error?

- The internet gateway is not configured with the security group

✅ The outbound traffic on the security group is disabled

Explanation:-A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. AWS provides two features the user can use to increase security in VPC: security groups and network ACLs. Security groups work at the instance level. When a user launches an instance and wants to connect to an instance, he needs an internet gateway. The internet gateway should be configured with the route table to allow traffic from the internet.

⚪ The private IP is not present

⚪ The internet gateway is not configured with the route table

---

Q51)

A user is trying to create a PIOPS EBS volume with 4000 IOPS and 100 GB size. AWS does not allow the user to create this volume.

What is the possible root cause for this?

⚪ The maximum IOPS supported by EBS is 3000

✅ The ratio between IOPS and the EBS volume is higher than 30

Explanation:-A Provisioned IOPS (SSD) volume can range in size from 4 GiB to 16 TiB and you can provision up to 20,000 IOPS per volume. The ratio of IOPS provisioned to the volume size requested should be a maximum of 30; for example, a volume with 3000 IOPS must be at least 100 GB.

⚪ PIOPS is supported for EBS higher than 500 GB size

⚪ The ratio between IOPS and the EBS volume is lower than 50

Q52) In the shared responsibility model at AWS, what two options are you responsible for instead of Amazon within an audit? Choose the 2 correct answers:

✅ The operating systems' administrators group

Explanation:-The operating systems' administrators group, An application that you have running within AWS EC2

⚪ The global infrastructure that hosts the virtualization hypervisors

⚪ Physical security to AWS data centers

✅ An application that you have running within AWS EC2

Explanation:-The operating systems' administrators group, An application that you have running within AWS EC2

Q53) Assuming you have kept the default settings and are using the automated backup services provided by AWS, which of the following will retain automated backups? Choose the correct answer:

⚪ An RDS database when the RDS instance is terminated

✅ None of these

Explanation:-Automated backups of RDS databases are deleted when an RDS instance is terminated. Only manual snapshots of an RDS database remain after the RDS instance is terminated. AWS does not offer an automated backup solution for volumes attached to EC2 instances.

⚪ An instance store root volume when the EC2 instance is terminated

⚪ An EBS root volume when the EC2 instance is terminated

Q54)

A user is creating a Cloudformation stack.

Which of the below mentioned limitations does not hold true for Cloudformation?

⚪ The user can use 60 parameters and 60 outputs in a single template

⚪ One account by default is limited to 20 stacks

⚪ The template, parameter, output, and resource description fields are limited to 4096 characters

✅ One account by default is limited to 100 templates

Explanation:-AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. The limitations given below apply to the Cloudformation template and stack. There are no limits to the number of templates but each AWS CloudFormation account is limited to a maximum of 20 stacks by default. The Template, Parameter, Output, and Resource description fields are limited to 4096 characters. The user can include up to 60 parameters and 60 outputs in a template.

Q55)

A user has received a message from the support team that an issue occurred 1 week back between 3 AM to 4 AM and the EC2 server was not reachable.

The user is checking the CloudWatch metrics of that instance.

How can the user find the data easily using the CloudWatch console?

⚪ The user can find the data by giving the exact values in the time Tab under CloudWatch metrics

⚪ The user can find the data by filtering values of the last 1 week for a 1 hour period in the Relative tab under CloudWatch metrics

⚪ It is not possible to find the exact time from the console. The user has to use CLI to provide the specific time

✅ The user can find the data by giving the exact values in the Absolute tab under CloudWatch metrics

Explanation:-If the user is viewing the data inside the CloudWatch console, the console provides options to filter values either using the relative period, such as days /hours or using the Absolute tab where the user can provide data with a specific date and time. The console also provides the option to search using the local timezone under the time range caption in the console.

Q56)

A user is checking the CloudWatch metrics from the AWS console. The user notices that the CloudWatch data is coming in UTC.

The user wants to convert the data to a local time zone.

How can the user perform this?

- In the CloudWatch dashboard the user should set the local timezone so that CloudWatch shows the data only in the local time zone
- The CloudWatch data is always in UTC; the user has to manually convert the data
- ✅ In the CloudWatch console select the local timezone under the Time Range tab to view the data as per the local timezone

Explanation:-If the user is viewing the data inside the CloudWatch console, the console provides options to filter values either using the relative period, such as days/hours or using the Absolute tab where the user can provide data with a specific date and time. The console also provides the option to search using the local timezone under the time range caption in the console because the time range tab allows the user to change the time zone.

- The user should have send the local timezone while uploading the data so that CloudWatch will show the data only in the local timezone

---

Q57)

An organization has setup Auto Scaling with ELB. Due to some manual error, one of the instances got rebooted.

Thus, it failed the Auto Scaling health check.

Auto Scaling has marked it for replacement.

How can the system admin ensure that the instance does not get terminated?

- It is not possible to change the status once it is marked for replacement
- Manually add that instance to the Auto Scaling group after reboot to avoid replacement
- Update the Auto Scaling group to ignore the instance reboot event
- ✅ Change the health of the instance to healthy using the Auto Scaling commands

Explanation:-After an instance has been marked unhealthy by Auto Scaling, as a result of an Amazon EC2 or ELB health check, it is almost immediately scheduled for replacement as it will never automatically recover its health. If the user knows that the instance is healthy then he can manually call the SetInstanceHealth action (or the as-set-instance-health command from CLI) to set the instance's health status back to healthy. Auto Scaling will throw an error if the instance is already terminating or else it will mark it healthy.

Q58)

A user has created a VPC with CIDR 20.0.0.0/16. The user has used all the IPs of CIDR and wants to increase the size of the VPC. The user has two subnets: public (20.0.0.0/20) and private (20.0.1.0/20).

How can the user change the size of the VPC?

- ✅ It is not possible to change the size of the VPC once it has been created

Explanation:-Once the user has created a VPC, he cannot change the CIDR of that VPC. The user has to terminate all the instances, delete the subnets and then delete the VPC. Create a new VPC with a higher size and launch instances with the newly created VPC and subnets.

- The user can delete the subnets first and then modify the size of the VPC
- The user can add a subnet with a higher range so that it will automatically increase the size of the VPC
- The user can delete all the instances of the subnet. Change the size of the subnets to 20.0.0.0/32 and 20.0.1.0/32, respectively. Then the user can increase the size of the VPC using CLI

Q59)

A user wants to make so that whenever the CPU utilization of the AWS EC2 instance is above 90%, some sort of notification is sent to him.

Which of the below mentioned AWS services is helpful for this purpose?

- AWS CloudWatch and a dedicated software turning on the light
- ✅ AWS CloudWatch + AWS SNS

Explanation:-Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, and fully managed push messaging service. Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS) queues or to any HTTP endpoint. The user can configure some sensor devices at his home which receives data on the HTTP end point (REST calls) and turn on the red light. The user can configure the CloudWatch alarm to send a notification to the AWS SNS HTTP end point (the sensor device) and it will turn the light red when there is an alarm condition.

- None. It is not possible to configure the light with the AWS infrastructure services
- AWS CloudWatch + AWS SES

Q60)

A user has configured a VPC with a new subnet. The user has created a security group. The user wants to configure that instances of the same subnet communicate with each other.

How can the user configure this with the security group?

- There is no need for a security group modification as all the instances can communicate with each other inside the same subnet
- The user has to use VPC peering to configure this
- ✅ Configure the security group itself as the source and allow traffic on all the protocols and ports

Explanation:-A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. AWS provides two features that the user can use to increase security in VPC: security groups and network ACLs. Security groups work at the instance level. If the user is using the default security group it will have a rule which allows the instances to communicate with other. For a new security group the user has to specify the rule, add it to define the source as the security group itself, and select all the protocols and ports for that source.

- Configure the subnet as the source in the security group and allow traffic on all the protocols and ports

---

Q61)

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?

✅ Create an AMI of the instance and copy the AMI to the EU region. Then launch the instance from the EU AMI

Explanation:-To launch an EC2 instance it is required to have an AMI in that region. If the AMI is not available in that region, then create a new AMI or use the copy command to copy the AMI from one region to the other region.

- Copy the running instance using the “Instance Copy” command to the EU region
- Use the “Launch more like this” option to copy the instance from one region to another
- Copy the instance from the US East region to the EU region

Q62)

A user has created a VPC with CIDR 20.0.0.0/16 with only a private subnet and VPN connection using the VPC wizard.

The user wants to connect to the instance in a private subnet over SSH.

How should the user define the security rule for SSH?

- Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the internet
- The user has to create an instance in EC2 Classic with an elastic IP and configure the security group of a private subnet to allow SSH from that elastic IP
- The user can connect to a instance in a private subnet using the NAT instance

✅ Allow Inbound traffic on port 22 from the user’s network

Explanation:-The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, the user can setup a case with a VPN only subnet (private) which uses VPN access to connect with his data centre. When the user has configured this setup with Wizard, all network connections to the instances in the subnet will come from his data centre. The user has to configure the security group of the private subnet which allows the inbound traffic on SSH (port 22) from the data centre’s network range.

Q63)

A user has hosted an application on EC2 instances. The EC2 instances are configured with ELB and Auto Scaling.

The application server session time out is 2 hours.

The user wants to configure connection draining to ensure that all in-flight requests are supported by ELB even though the instance is being deregistered.

What time out period should the user specify for connection draining?

- 2 hours

✅ 5 minutes

Explanation:-The Elastic Load Balancer connection draining feature causes the load balancer to stop sending new requests to the back-end instances when the instances are deregistering or become unhealthy, while ensuring that in-flight requests continue to be served. The user can specify a maximum time of 3600 seconds (1 hour) for the load balancer to keep the connections alive before reporting the instance as deregistered. If the user does not specify the maximum timeout period, by default, the load balancer will close the connections to the deregistering instance after 300 seconds.

- 30 minutes
- 1 hour

Q64) A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at rest. If the user is supplying his own keys for encryption (SSE-C), what is recommended to the user for the purpose of security?

- The user should not use his own security key as it is not secure

✅ Keep rotating the encryption key manually at the client side

Explanation:-AWS S3 supports client side or server side encryption to encrypt all data at Rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key (SSE-C). Since S3 does not store the encryption keys in SSE-C, it is recommended that the user should manage keys securely and keep rotating them regularly at the client side version.

- Configure S3 to store the user’s keys securely with SSL
- Configure S3 to rotate the user’s encryption key at regular intervals

---

Q65)

A user has configured ELB with a TCP listener at ELB as well as on the back-end instances.

The user wants to enable a proxy protocol to capture the source and destination IP information in the header.

Which of the below mentioned statements helps the user understand a proxy protocol with TCP configuration?

- Whether the end user is requesting from a proxy server or directly, it does not make a difference for the proxy protocol
- If the end user is requesting behind the proxy then the user should add the “isproxy” flag to the ELB configuration

✅ If the end user is requesting behind a proxy server then the user should not enable a proxy protocol on ELB

Explanation:-When the user has configured Transmission Control Protocol (TCP) or Secure Sockets Layer (SSL) for both front-end and back-end connections of the Elastic Load Balancer, the load balancer forwards the request to the back-end instances without modifying the request headers unless the proxy header is enabled. If the end user is requesting from a Proxy Protocol enabled proxy server, then the ELB admin should not enable the Proxy Protocol on the load balancer. If the Proxy Protocol is enabled on both the proxy server and the load balancer, the load balancer will add another header to the request which already has a header from the proxy server. This duplication may result in errors.

- ELB does not support a proxy protocol when it is listening on both the load balancer and the back-end instances

---