Answer Sheet

Q1)

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

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 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 a NAT instance with an elastic IP. If the user is trying to delete the VPC it will not allow as the NAT instance is still running.

- It will not allow to delete the VPC since it has a running route instance

---

Q2)

A user has configured an HTTPS listener on an ELB. The user has not configured any security policy which can help to negotiate SSL between the client and ELB.

What will ELB do in this scenario?

- It is not required to have a security policy since SSL is already installed
- By default ELB will select the latest version of the policy
- ELB creation will fail without a security policy
- ✅ By default ELB will select the first version of the security policy

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. If the user has created an HTTPS/SSL listener without associating any security policy, Elastic Load Balancing will, by default, associate the latest version of the ELBSecurityPolicy-YYYY-MM with the load balancer.

Q3)

A user is observing the EC2 CPU utilization metric on CloudWatch. The user has observed some interesting patterns while filtering over the 1 week period for a particular hour.

The user wants to zoom that data point to a more granular period.

How can the user do that easily with CloudWatch?

- The user can zoom a particular period by specifying the aggregation data for that period
- The user can zoom a particular period by specifying the period in the Time Range
- ✅ The user can zoom a particular period by selecting that period with the mouse and then releasing the mouse

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 AWS CloudWatch console provides the option to change the granularity of a graph and zoom in to see data over a shorter time period. To zoom, the user has to click in the graph details pane, drag on the graph area for selection, and then release the mouse button.

- The user can zoom a particular period by double clicking on that period with the mouse

---

Q4)

A user has enabled detailed CloudWatch metric monitoring on an Auto Scaling group.

Which of the below mentioned metrics will help the user identify the total number of instances in an Auto Scaling group including pending, terminating and running instances.

- GroupSumInstances
- It is not possible to get a count of all the three metrics together. The user has to find the individual number of running, terminating and pending instances and sum it
- ✅ GroupInstancesCount

Explanation:-CloudWatch is used to monitor AWS as well as the custom services. For Auto Scaling, CloudWatch provides various metrics to get the group information, such as the Number of Pending, Running or Terminating instances at any moment. If the user wants to get the total number of Running, Pending and Terminating instances at any moment, he can use the GroupTotalInstances metric.

- GroupTotalInstances

Q5)

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

Which of the below mentioned SSL protocols is not supported by the security policy?

- ✅ TLS 1.3

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. Elastic Load Balancing supports the following versions of the SSL protocol:
TLS 1.2
TLS 1.1

TLS 1.0
SSL 3.0
SSL 2.0
- SSL 2.0
- TLS 1.2
- SSL 3.0

Q6) Which of the below mentioned AWS RDS logs cannot be viewed from the console for MySQL?

- Slow Query Log
- ✅ Transaction Log

Explanation:-The user can view, download, and watch the database logs using the Amazon RDS console, the Command Line Interface (CLI), or the Amazon RDS API. For the MySQL RDS, the user can view the error log, slow query log, and general logs. RDS does not support viewing the transaction logs.

- General Log
- Error Log

Q7)

A user is trying to configure the CloudWatch billing alarm.

Which of the below mentioned steps should be performed by the user for the first time alarm creation in the AWS Account Management section?

- ✅ Enable Receiving Billing Alerts

Explanation:-AWS CloudWatch supports enabling the billing alarm on the total AWS charges. Before the user can create an alarm on the estimated charges, he must enable monitoring of the estimated AWS charges, by selecting the option “Enable receiving billing alerts”. It takes about 15 minutes before the user can view the billing data. The user can then create the alarms.

- Enable CloudWatch Billing Threshold
- Enable AWS billing utility
- Enable Receiving Billing Reports

Q8)

A user has enabled session stickiness with ELB. The user does not want ELB to manage the cookie; instead he wants the application to manage the cookie.

What will happen when the server instance, which is bound to a cookie, crashes?

- The session will be sticky and ELB will route requests to another server as ELB keeps replicating the cookie
- The response will have a cookie but stickiness will be deleted
- ✅ The session will not be sticky until a new cookie is inserted

Explanation:-With Elastic Load Balancer, if the admin has enabled a sticky session with application controlled stickiness, the load balancer uses a special cookie generated by the application to associate the session with the original server which handles the request. ELB follows the lifetime of the application-generated cookie corresponding to the cookie name specified in the ELB policy configuration. The load balancer only inserts a new stickiness cookie if the application response includes a new application cookie. The load balancer stickiness cookie does not update with each request. If the application cookie is explicitly removed or expires, the session stops being sticky until a new application cookie is issued.

- ELB will throw an error due to cookie unavailability

Q9)

A user has setup a CloudWatch alarm on an EC2 action when the CPU utilization is above 75%.

The alarm sends a notification to SNS on the alarm state.

If the user wants to simulate the alarm action how can he achieve this?

- ✅ The user can set the alarm state to ‘Alarm’ using CLI

Explanation:-Amazon CloudWatch alarms watch 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. The user can test an alarm by setting it to any state using the SetAlarmState API (mon-set-alarm-state command). This temporary state change lasts only until the next alarm comparison occurs.

- From the AWS console change the state to ‘Alarm’
- Run the SNS action manually
- Run activities on the CPU such that its utilization reaches above 75%

Q10)

An organization has created 5 IAM users. The organization wants to give them the same login ID but different passwords.

How can the organization achieve this?

- The organization should create a separate login ID but give the IAM users the same alias so that each one can login with their alias
- It is not possible to have the same login ID for multiple IAM users of the same account
- The organization should create various groups and add each user with the same login ID to different groups. The user can login with their own group ID
- ✅ The organization should create each user in a separate region so that they have their own URL to login

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Whenever the organization is creating an IAM user, there should be a unique ID for each user. It is not possible to have the same login ID for multiple users. The names of users, groups, roles, instance profiles must be alphanumeric, including the following common characters: plus (+), equal (=), comma (,), period (.), at (@), and dash (-).

Q11)

A user runs the command "dd if=/dev/xvdf of=/dev/null bs=1M" on an EBS volume created from a snapshot and attached to a Linux instance.

Which of the below mentioned activities is the user performing with the step given above?

- Copying the data from a snapshot to the device
- ✓ Pre warming the EBS volume

Explanation:-When the user creates an EBS volume and is trying to access it for the first time it will encounter reduced IOPS due to wiping or initiating of the block storage. To avoid this as well as achieve the best performance it is required to pre warm the EBS volume. For a volume created from a snapshot and attached with a Linux OS, the "dd" command pre warms the existing data on EBS and any restored snapshots of volumes that have been previously fully pre warmed. This command maintains incremental snapshots; however, because this operation is read-only, it does not pre warm unused space that has never been written to on the original volume. In the command "dd if=/dev/xvdf of=/dev/null bs=1M" , the parameter "if=input file" should be set to the drive that the user wishes to warm. The "of=output file" parameter should be set to the Linux null virtual device, /dev/null. The "bs" parameter sets the block size of the read operation; for optimal performance, this should be set to 1 MB.

- Formatting the volume
- Initiating the device to mount on the EBS volume

Q12)

A user has configured an ELB to distribute the traffic among multiple instances. The user instances are facing some issues due to the back-end servers.

Which of the below mentioned CloudWatch metrics helps the user understand the issue with the instances?

- HTTPCode_Backend_4XX
- ✓ HTTPCode_Backend_5XX

Explanation:-CloudWatch is used to monitor AWS as well as the custom services. For ELB, CloudWatch provides various metrics including error code by ELB as well as by back-end servers (instances). It gives data for the count of the number of HTTP response codes generated by the back-end instances. This metric does not include any response codes generated by the load balancer. These metrics are:
The 2XX class status codes represents successful actions
The 3XX class status code indicates that the user agent requires action
The 4XX class status code represents client errors
The 5XX class status code represents back-end server errors

- HTTPCode_Backend_2XX
- HTTPCode_Backend_3XX

Q13)

A user has launched multiple EC2 instances for the purpose of development and testing in the same region.

The user wants to find the separate cost for the production and development instances.

How can the user find the cost distribution?

- ✓ The user should use Cost Allocation Tags and AWS billing reports

Explanation:-AWS provides cost allocation tags to categorize and track the AWS costs. When the user applies tags to his AWS resources (such as Amazon EC2 instances or Amazon S3 buckets), AWS generates a cost allocation report as a comma-separated value (CSV file) with the usage and costs aggregated by those tags. The user can apply tags which represent business categories (such as cost centres, application names, or instance type – Production/Dev) to organize usage costs across multiple services.

- It is not possible to get the AWS cost usage data of single region instances separately
- The user should download the activity report of the EC2 services as it has the instance ID wise data
- The user should use Cost Distribution Metadata and AWS detailed billing

---

Q14)

An organization is planning to create 5 different AWS accounts considering various security requirements.

The organization wants to use a single payee account by using the consolidated billing option.

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

- Each AWS account needs to create an AWS billing policy to provide permission to the payee account
- Master (Payee) account will get only the total bill and cannot see the cost incurred by each account
- It is not recommended to use consolidated billing since the payee account will have access to the linked accounts
- ✓ Master (Payee) account can view only the AWS billing details of the linked accounts

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. Consolidated billing enables the organization to see a combined view of the AWS charges incurred by each account as well as obtain a detailed cost report for each of the individual AWS accounts associated with the paying account. The payee account will not have any other access than billing data of linked accounts.
http://docs.aws.amazon.com/awsaccountbilling/latest/about/consolidatedbilling.html

---

Q15)

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

Which of the below mentioned security policies is supported by ELB?

- Dynamic Security Policy

- Default Security Policy
- ✅ Predefined Security Policy

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. ELB supports two policies:
1. Predefined Security Policy, which comes with predefined cipher and SSL protocols;
2. Custom Security Policy, which allows the user to configure a policy.

- All the other options

Q16)

A user has created a mobile application which makes calls to DynamoDB to fetch certain data.

The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile.

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 role with DynamoDB and EC2 access. Attach the role with EC2 and route all calls from the mobile through EC2
- Create an IAM Role with DynamoDB access and attach it with the mobile application
- ✅ The application should use an IAM role with web identity federation which validates calls to DynamoDB with identity providers, such as Google, Amazon, and Facebook

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. If the user is creating an app that runs on a mobile phone and makes requests to AWS, the user should not create an IAM user and distribute the user's access key with the app. Instead, he should use an identity provider, such as Login with Amazon, Facebook, or Google to authenticate the users, and then use that identity to get temporary security credentials.

- The user should create a separate IAM user for each mobile application and provide DynamoDB access with it

---

Q17) A sys admin has enabled a log on ELB. Which of the below mentioned activities are not captured by the log?

- Response processing time
- ✅ Front end processing time

Explanation:-Elastic Load Balancing access logs capture detailed information for all the requests made to the load balancer. Each request will have details, such as client IP, request path, ELB IP, time, and latencies. The time will have information, such as Request Processing time, Backend Processing time and Response Processing time.

- Request processing time
- Backend processing time

Q18) A sys admin is trying to understand the sticky session algorithm. Please select the correct sequence of steps, both when the cookie is present and when it is not, to help the admin understand the implementation of the sticky session:
1. ELB inserts the cookie in the response
2. ELB chooses the instance based on the load balancing algorithm
3. Check the cookie in the service request
4. The cookie is found in the request
5. The cookie is not found in the request

- 3,2,5,4 [Cookie is not Present] & 3,2,4,5 [Cookie is Present]
- 3,1,4,2 [Cookie is not Present] & 3,1,5,2 [Cookie is Present]
- 3,4,1,2 [Cookie is not Present] & 3,5,1,2 [Cookie is Present]
- ✅ 3,5,2,1 [Cookie is not Present] & 3,4,2,1 [Cookie is Present]

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. The load balancer uses a special load-balancer-generated cookie to track the application instance for each request. When the load balancer receives a request, it first checks to see if this cookie is present in the request. If so, the request is sent to the application instance specified in the cookie. If there is no cookie, the load balancer chooses an application instance based on the existing load balancing algorithm. A cookie is inserted into the response for binding subsequent requests from the same user to that application instance.

Q19)

A user has two EC2 instances running in two separate regions. The user is running an internal memory management tool, which captures the data and sends it to CloudWatch in US East, using a CLI with the same namespace and metric.

Which of the below mentioned options is true with respect to the above statement?

- CloudWatch will take the data of the server, which sends the data first
- The setup will not work as CloudWatch cannot receive data across regions
- CloudWatch will give an error since the data will conflict due to two sources
- ✅ CloudWatch will receive and aggregate the data based on the namespace and metric

Explanation:-Amazon CloudWatch does not differentiate the source of a metric when receiving custom data. If the user is publishing a metric with the same namespace and dimensions from different sources, CloudWatch will treat them as a single metric. If the data is coming with the same timezone within a minute, CloudWatch will aggregate the data. It treats these as a single metric, allowing the user to get the statistics, such as minimum, maximum, average, and the sum of all across all servers.

Q20)

An application is generating a log file every 5 minutes. The log file is not critical but may be required only for verification in case of some major issue.

The file should be accessible over the internet whenever required.

Which of the below mentioned options is a best possible storage solution for it?

- AWS S3
- AWS RDS
- AWS Glacier
- ✅ AWS S3 RRS

Explanation:-Amazon S3 stores objects according to their storage class. There are three major storage classes: Standard, Reduced Redundancy Storage and Glacier. Standard is for AWS S3 and provides very high durability. However, the costs are a little higher. Glacier is for archival and the files are not available over the internet. Reduced Redundancy Storage is for less critical files. Reduced Redundancy is little cheaper as it provides less durability in comparison to S3. In this case since the log files are not mission critical files, RRS will be a better option.

Q21) An organization has created one IAM user and applied the below mentioned policy to the user. What entitlements do the IAM users avail with this policy?

```
{
“Version”: “2012-10-17”,
“Statement”: [
{
“Effect”: “Allow”,
“Action”: “ec2:Describe*”,
“Resource”: “*”
},
{
“Effect”: “Allow”
“Action”: [
“cloudwatch:ListMetrics”,
“cloudwatch:GetMetricStatistics”,
“cloudwatch:Describe*”
],
“Resource”: “*”
},
{
“Effect”: “Allow”,
“Action”: “autoscaling:Describe*”,
“Resource”: “*”
}
]
}
```

- The policy will allow the user to perform all read and write activities on the EC2 services
- The policy will allow the user to list all the EC2 resources except EBS
- ✅ The policy will allow the user to perform all read only activities on the EC2 services except load balancing

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If an organization wants to setup read only access to EC2 for a particular user, they should mention the action in the IAM policy which entitles the user for Describe rights for EC2, CloudWatch, Auto Scaling and ELB. In the policy shown below, the user will have read only access for EC2 and EBS, CloudWatch and Auto Scaling. Since ELB is not mentioned as a part of the list, the user will not have access to ELB.AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If an organization wants to setup read only access to EC2 for a particular user, they should mention the action in the IAM policy which entitles the user for Describe rights for EC2, CloudWatch, Auto Scaling and ELB. In the policy shown below, the user will have read only access for EC2 and EBS, CloudWatch and Auto Scaling. Since ELB is not mentioned as a part of the list, the user will not have access to ELB.

```
{
“Version”: “2012-10-17”,
“Statement”: [
{
“Effect”: “Allow”,
“Action”: “ec2:Describe*”,
“Resource”: “*”
},
{
“Effect”: “Allow”,
“Action”: [
“cloudwatch:ListMetrics”,
“cloudwatch:GetMetricStatistics”,
“cloudwatch:Describe*”
],
“Resource”: “*”
},
{
“Effect”: “Allow”,
“Action”: “autoscaling:Describe*”,
“Resource”: “*”
}
]
}
```

- The policy will allow the user to perform all read only activities on the EC2 services

---

Q22)

A user is trying to pre-warm a blank EBS volume attached to a Linux instance.

Which of the below mentioned steps should be performed by the user?

- Contact AWS support to pre-warm
- There is no need to pre-warm an EBS volume
- Format the device

✅ Unmount the volume before pre-warming

Explanation:-When the user creates a new EBS volume or restores a volume from the snapshot, the back-end storage blocks are immediately allocated to the user EBS. However, the first time when the user is trying to access a block of the storage, it is recommended to either be wiped from the new volumes or instantiated from the snapshot (for restored volumes) before the user can access the block. This preliminary action takes time and can cause a 5 to 50 percent loss of IOPS for the volume when the block is accessed for the first time. To avoid this it is required to pre warm the volume. Pre-warming an EBS volume on a Linux instance requires that the user should unmount the blank device first and then write all the blocks on the device using a command, such as “dd”.

Q23)

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), which of the below mentioned statements is true?

✅ It is possible to have different encryption keys for different versions of the same object

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). If the bucket is versioning-enabled, each object version uploaded by the user using the SSE-C feature can have its own encryption key. The user is responsible for tracking which encryption key was used for which object’s version

- The user should use the same encryption key for all versions of the same object
- AWS S3 does not allow the user to upload his own keys for server side encryption
- The SSE-C does not work when versioning is enabled

Q24)

A user has enabled termination protection on an EC2 instance. The user has also set Instance initiated shutdown behaviour to terminate.

When the user shuts down the instance from the OS, what will happen?

- The OS will shutdown but the instance will not be terminated due to protection
- It will not allow the user to shutdown the instance from the OS

✅ It will terminate the instance

Explanation:-It is always possible that someone can terminate an EC2 instance using the Amazon EC2 console, command line interface or API by mistake. If the admin wants to prevent the instance from being accidentally terminated, he can enable termination protection for that instance. The user can also setup shutdown behaviour for an EBS backed instance to guide the instance on what should be done when he initiates shutdown from the OS using Instance initiated shutdown behaviour. If the instance initiated behaviour is set to terminate and the user shuts off the OS even though termination protection is enabled, it will still terminate the instance.

- It is not possible to set the termination protection when an Instance initiated shutdown is set to terminate

---

Q25)

A user is measuring the CPU utilization of a private data centre machine every minute. The machine provides the aggregate of data every hour, such as Sum of data”, “Min value”, “Max value, and “Number of Data points”.

The user wants to send these values to CloudWatch.

How can the user achieve this?

- Send the data using the put-metric-data command with the aggregate –data parameter
- Send the data using the put-metric-data command with the aggregate-values parameter
- Send the data using the put-metric-data command with the average-values parameter

✅ Send the data using the put-metric-data command with the statistic-values parameter

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 user can publish the data to CloudWatch as single data points or as an aggregated set of data points called a statistic set using the command put-metric-data. When sending the aggregate data, the user needs to send it with the parameter statistic-values:
aws cloudwatch put-metric-data –metric-name –namespace –timestamp –statistic-values Sum=XX,Minimum=YY,Maximum=AA,SampleCount=BB –unit Milliseconds

---

Q26)

A user has deployed an application on his private cloud. The user is using his own monitoring tool. He wants to configure that whenever there is an error, the monitoring tool should notify him via SMS.

Which of the below mentioned AWS services will help in this scenario?

- None because the user infrastructure is in the private cloud/
- AWS SES
- AWS SMS

✅ AWS SNS

Explanation:-Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, and fully managed push messaging service. Amazon SNS can be used to make push notifications to mobile devices. Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS) queues or to any HTTP endpoint. In this case user can use the SNS apis to send SMS.

Q27)

A user has created a VPC with a public subnet. The user has terminated all the instances which are part of the subnet.

Which of the below mentioned statements is true with respect to this scenario?

- The subnet to which the instances were launched with will be deleted
- ✓ All network interface attached with the instances will be deleted

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. When an instance is launched it will have a network interface attached with it. The user cannot delete the subnet until he terminates the instance and deletes the network interface. When the user terminates the instance all the network interfaces attached with it are also deleted.

- When the user launches a new instance it cannot use the same subnet
- The user cannot delete the VPC since the subnet is not deleted

---

Q28)

A user has developed an application which is required to send the data to a NoSQL database. The user wants to decouple the data sending such that the application keeps processing and sending data but does not wait for an acknowledgement of DB.

Which of the below mentioned applications helps in this scenario?

- AWS Simple Notification Service
- ✓ AWS Simple Queue Service

Explanation:-Amazon Simple Queue Service (SQS) is a fast, reliable, scalable, and fully managed message queuing service. SQS provides a simple and cost-effective way to decouple the components of an application. In this case, the user can use AWS SQS to send messages which are received from an application and sent to DB. The application can continue processing data without waiting for any acknowledgement from DB. The user can use SQS to transmit any volume of data without losing messages or requiring other services to always be available.

- AWS Simple Workflow
- AWS Simple Query Service

Q29)

An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%. The higher CPU usage triggers an event for Auto Scaling as per the scaling policy.

If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

- It is not possible to find the root cause from that instance without triggering scaling
- Stop the scaling process until research is completed
- Delete Auto Scaling until research is completed
- ✓ Suspend the scaling process until research is completed

Explanation:-Auto Scaling allows the user to suspend and then resume one or more of the Auto Scaling processes in the Auto Scaling group. This is very useful when the user wants to investigate a configuration problem or some other issue, such as a memory leak with the web application and then make changes to the application, without triggering the Auto Scaling process.

Q30)

A user has launched 10 instances from the same AMI ID using Auto Scaling. The user is trying to see the average CPU utilization across all instances of the last 2 weeks under the CloudWatch console.

How can the user achieve this?

- It is not possible to see the average CPU utilization of the same AMI ID since the instance ID is different
- The user has to use the CloudWatch analyser to find the average data across instances
- View the Auto Scaling CPU metrics
- ✓ Aggregate the data over the instance AMI ID

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. To aggregate the data across instances launched with AMI, the user should select the AMI ID under EC2 metrics and select the aggregate average to view the data.

Q31)

An organization has configured Auto Scaling with ELB. One of the instance health check returns the status as Impaired to Auto Scaling.

What will Auto Scaling do in this scenario?

- Notify ELB to stop sending traffic to the impaired instance
- Notify the user using SNS for the failed state
- Perform a health check until cool down before declaring that the instance has failed
- ✓ Terminate the instance and launch a new instance

Explanation:-The Auto Scaling group determines the health state of each instance periodically by checking the results of the Amazon EC2 instance status checks. If the instance status description shows any other state other than "running" or the system status description shows impaired, Auto Scaling considers the instance to be unhealthy. Thus, it terminates the instance and launches a replacement.

Q32)

A user is trying to understand AWS SNS.

To which of the below mentioned end points is SNS unable to send a notification?

- AWS SQS
- ✓ AWS SES

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 select one the following transports as part of the subscription requests: “HTTP”, “HTTPS”,”Email”, “Email-JSON”, “SQS”, “and SMS”.

- HTTP
- Email JSON

Q33)

A sys admin is trying to understand EBS snapshots.

Which of the below mentioned statements will not be useful to the admin to understand the concepts about a snapshot?

- The snapshot is incremental
- The snapshot captures the data that has been written to the hard disk when the snapshot command was executed
- ✅ The snapshot is synchronous

Explanation:-The AWS snapshot is a point in time backup of an EBS volume. When the snapshot command is executed it will capture the current state of the data that is written on the drive and take a backup. For a better and consistent snapshot of the root EBS volume, AWS recommends stopping the instance. For additional volumes it is recommended to unmount the device. The snapshots are asynchronous and incremental.

- It is recommended to stop the instance before taking a snapshot for consistent data

---

Q34)

An organization is setting up programmatic billing access for their AWS account.

Which of the below mentioned services will not be required when the organization wants to use programmatic access?

- Monthly Billing report
- Programmatic access
- AWS bucket to hold the billing report
- ✅ AWS billing alerts

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. To enable programmatic access, the user has to first enable the monthly billing report. Then the user needs to provide an AWS bucket name where the billing CSV will be uploaded. The user should also enable the Programmatic access option.

Q35) You have created a VPC with CIDR 20.0.0.0/16, along with a public and VPN only subnets. You have hardware VPN access to connect to the your datacenter.
What do you need to do so that all traffic coming to the public subnet follows the organization’s proxy policy?

- Set up a NAT with the proxy protocol and configure that the public subnet receives traffic from NAT
- It is not possible to setup the proxy policy for a public subnet
- ✅ Set the route table and security group of the public subnet which receives traffic from a virtual private gateway

Explanation:-The user can create subnets within a VPC. If the user wants to connect to VPC from his own data centre, he can setup public and VPN only subnets which uses hardware VPN access to connect with his data centre. When the user has configured this setup, it will update the main route table used with the VPN-only subnet, create a custom route table and associate it with the public subnet. It also creates an internet gateway for the public subnet. By default the internet traffic of the VPN subnet is routed to a virtual private gateway while the internet traffic of the public subnet is routed through the internet gateway. The user can set up the route and security group rules. These rules enable the traffic to come from the organization’s network over the virtual private gateway to the public subnet to allow proxy settings on that public subnet.

- Set up a proxy policy in the internet gateway connected with the public subnet

---

Q36)

A user is trying to understand the detailed CloudWatch monitoring concept.

Which of the below mentioned services provides detailed monitoring with CloudWatch without charging the user extra?

- AWS EMR
- ✅ AWS Route 53

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. Services, such as RDS, ELB, OpsWorks, and Route 53 can provide the monitoring data every minute without charging the user.

- AWS Auto Scaling
- AWS SNS

Q37)

A user has created a queue named “myqueue” in US-East region with AWS SQS. The user’s AWS account ID is 123456789012.

If the user wants to perform some action on this queue, which of the below Queue URL should he use?

- http://sqs. 123456789012.us-east-1.amazonaws.com/myqueue
- http://sqs.amazonaws.com/123456789012/myqueue
- ✅ http://sqs.us-east-1.amazonaws.com/123456789012/myqueue

Explanation:-When creating a new queue in SQS, the user must provide a queue name that is unique within the scope of all queues of user’s account. If the user creates queues using both the latest WSDL and a previous version, he will have a single namespace for all his queues. Amazon SQS assigns each queue created by user an identifier called a queue URL, which includes the queue name and other components that Amazon SQS determines. Whenever the user wants to perform an action on a queue, he must provide its queue URL. The queue URL for the account id 123456789012 & queue name “myqueue” in US-East-1 region will be http://sqs.us-east-1.amazonaws.com/123456789012/myqueue.

- http:// 123456789012.sqs. us-east-1.amazonaws.com/myqueue

Q38)

A root account owner is trying to understand the S3 bucket ACL.

Which of the below mentioned options cannot be used to grant ACL on the object using the authorized predefined group?

- All users group
- Log Delivery Group
- Authenticated user group
- ✅ Canonical user group

Explanation:-An S3 bucket ACL grantee can be an AWS account or one of the predefined Amazon S3 groups. Amazon S3 has a set of predefined groups. When granting account access to a group, the user can specify one of the URLs of that group instead of a canonical user ID. AWS S3 has the following predefined groups:
Authenticated Users group: It represents all AWS accounts.
All Users group: Access permission to this group allows anyone to access the resource.
Log Delivery group: WRITE permission on a bucket enables this group to write server access logs to the bucket.

Q39)

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling terminate process only for a while.

What might the Availability Zone Rebalancing process (AZRebalance) consequently cause during this period?

- Auto Scaling will keep launching instances till the maximum instance size
- It is not possible to suspend the terminate process while keeping the launch active
- Auto Scaling will not launch or terminate any instances
- ✅ Auto Scaling might allow the number instances in an Availability Zone to remain higher than the maximum size

Explanation:-Auto Scaling performs various processes, such as Launch, Terminate, and Availability Zone Rebalance (AZRebalance). The AZRebalance process type seeks to maintain a balanced number of instances across Availability Zones within a region. If the user suspends the Terminate process, the AZRebalance process can cause the Auto Scaling group to grow up to ten percent larger than the maximum size. This is because Auto Scaling allows groups to temporarily grow larger than the maximum size during rebalancing activities. If Auto Scaling cannot terminate instances, the Auto Scaling group could remain up to ten percent larger than the maximum size until the user resumes the Terminate process type.

Q40)

A user has created a subnet with VPC and launched an EC2 instance in that subnet with only default settings.

Which of the below mentioned options is ready to use on the EC2 instance as soon as it is launched?

- Public IP
- ✅ Private IP

Explanation:-A Virtual Private Cloud (VPC) is a virtual network dedicated to a user's AWS account. A subnet is a range of IP addresses in the VPC. The user can launch the AWS resources into a subnet. There are two supported platforms into which a user can launch instances: EC2-Classic and EC2-VPC. When the user launches an instance which is not a part of the non-default subnet, it will only have a private IP assigned to it. The instances part of a subnet can communicate with each other but cannot communicate over the internet or to the AWS services, such as RDS / S3.

- Elastic IP
- Internet gateway

Q41)

A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24) and a public subnet (20.0.0.0/24).

The user's data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24.

If the private subnet wants to communicate with the data centre, what will happen?

- It will not allow traffic communication on any of the data centre CIDRs
- It will not allow traffic with data centre on CIDR 20.1.0.0/24 but allows traffic communication on 20.0.54.0/24
- ✅ It will allow traffic with data centre on CIDR 20.1.0.0/24 but does not allow on 20.0.54.0/24

Explanation:-VPC allows the user to set up a connection between his VPC and corporate or home network data centre. If the user has an IP address prefix in the VPC that overlaps with one of the networks' prefixes, any traffic to the network's prefix is dropped. In this case CIDR 20.0.54.0/24 falls in the VPC's CIDR range of 20.0.0.0/16. Thus, it will not allow traffic on that IP. In the case of 20.1.0.0/24, it does not fall in the VPC's CIDR range. Thus, traffic will be allowed on it.

- It will allow traffic communication on both the CIDRs of the data centre

---

Q42)

George has launched three EC2 instances inside the US-East-1a zone with his AWS account.

Ray has launched two EC2 instances in the US-East-1a zone with his AWS account.

Which of the below mentioned statements will help George and Ray understand the availability zone (AZ) concept better?

- The instances of George and Ray will be running in the same data centre
- All the instances of George and Ray can communicate over a private IP without any cost
- All the instances of George and Ray can communicate over a private IP with a minimal cost
- ✅ The US-East-1a region of George and Ray can be different availability zones

Explanation:-Each AWS region has multiple, isolated locations known as Availability Zones. To ensure that the AWS resources are distributed across the Availability Zones for a region, AWS independently maps the Availability Zones to identifiers for each account. In this case the Availability

Zone US-East-1a where George's EC2 instances are running might not be the same location as the US-East-1a zone of Ray's EC2 instances. There is no way for the user to coordinate the Availability Zones between accounts.

Q43)

An organization is using cost allocation tags to find the cost distribution of different departments and projects.

One of the instances has two separate tags with the key/ value as "InstanceName/HR", "CostCenter/HR".

What will AWS do in this case?

- AWS will allow tags but will not show correctly in the cost allocation report due to the same value of the two separate keys
- InstanceName is a reserved tag for AWS. Thus, AWS will not allow this tag
- AWS will not allow the tags as the value is the same for different keys
- ✅ AWS will allow both the tags and show properly in the cost distribution report

Explanation:-AWS provides cost allocation tags to categorize and track the AWS costs. When the user applies tags to his AWS resources, AWS generates a cost allocation report as a comma-separated value (CSV file) with the usage and costs aggregated by those tags. Each tag will have a key-value and can be applied to services, such as EC2, S3, RDS, EMR, etc. It is required that the key should be different for each tag. The value can be the same for different keys. In this case since the value is different, AWS will properly show the distribution report with the correct values.

Q44)

A user is trying to setup a scheduled scaling activity using Auto Scaling. The user wants to setup the recurring schedule.

Which of the below mentioned parameters is not required in this case?

- End time
- ✅ Maximum size

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. If the user is setting a recurring event, it is required that the user specifies the Recurrence value (in a cron format), end time (not compulsory but recurrence will stop after this) and the Auto Scaling group for which the scaling activity is to be scheduled.

- Recurrence value
- Auto Scaling group name

Q45)

A user runs the command "dd if=/dev/zero of=/dev/xvdf bs=1M" on a fresh blank EBS volume attached to a Linux instance.

Which of the below mentioned activities is the user performing with the command given above?

- ✅ Pre warming the EBS volume

Explanation:-When the user creates a new EBS volume and is trying to access it for the first time it will encounter reduced IOPS due to wiping or initiating of the block storage. To avoid this as well as achieve the best performance it is required to pre warm the EBS volume. For a blank volume attached with a Linux OS, the "dd" command is used to write to all the blocks on the device. In the command "dd if=/dev/zero of=/dev/xvdf bs=1M" the parameter "if =import file" should be set to one of the Linux virtual devices, such as /dev/zero. The "of=output file" parameter should be set to the drive that the user wishes to warm. The "bs" parameter sets the block size of the write operation; for optimal performance, this should be set to 1 MB.

- Creating a file system on the EBS volume
- Formatting the EBS volume
- Mounting the device to the instance

Q46) A user has launched an RDS MySQL DB with the Multi AZ feature. The user has scheduled the scaling of instance storage during maintenance window. What is the correct order of events during maintenance window?
1. Perform maintenance on standby
2. Promote standby to primary
3. Perform maintenance on original primary
4. Promote original master back as primary

- 2, 3, 1, 4
- ✅ 1, 2, 3

Explanation:-Running MySQL on the RDS DB instance as a Multi-AZ deployment can help the user reduce the impact of a maintenance event, as the Amazon will conduct maintenance by following the steps in the below mentioned order:
1. Perform maintenance on standby
2. Promote standby to primary
3. Perform maintenance on original primary, which becomes the new standby.

- 2, 3, 1
- 1, 2, 3, 4

Q47)

An organization is planning to create a user with IAM. They are trying to understand the limitations of IAM so that they can plan accordingly.

Which of the below mentioned statements is not true with respect to the limitations of IAM?

- One AWS account can have a maximum of 5000 IAM users
- ✅ One IAM user can be a part of as many groups as is needed

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The default maximums for each of the IAM entities is given below:

Groups per AWS account: 100
Users per AWS account: 5000
Roles per AWS account: 250
Number of groups per user: 10 (that is, one user can be part of these many groups)

- One AWS account can have 250 roles
- The organization can create 100 groups per AWS account

Q48)

An organization has configured two single availability zones. The Auto Scaling groups are configured in separate zones.

The user wants to merge the groups such that one group spans across multiple zones.

How can the user configure this?

- Run the command as-copy-auto-scaling-group to join the two groups
- Run the command as-join-auto-scaling-group to join the two groups
- ✅ Run the command as-update-auto-scaling-group to configure one group to span across zones and delete the other group

Explanation:-If the user has configured two separate single availability zone Auto Scaling groups and wants to merge them then he should update one of the groups and delete the other one. While updating the first group it is recommended that the user should increase the size of the minimum, maximum and desired capacity as a summation of both the groups.

- Run the command as-merge-auto-scaling-group to merge the groups

---

Q49)

A user is planning to scale up an application by 8 AM and scale down by 7 PM daily using Auto Scaling.

What should the user do in this case?

- Setup the scaling policy to scale up and down based on the CloudWatch alarms
- The user should increase the desired capacity at 8 AM and decrease it by 7 PM manually
- The user should increase the desired capacity at 8 AM and decrease it by 7 PM manually
- ✅ Setup scheduled actions to scale up or down at a specific time

Explanation:-Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. To configure the Auto Scaling group to scale based on a schedule, the user needs to create scheduled actions. A scheduled action tells Auto Scaling to perform a scaling action at a certain time in the future.

Q50)

A user has provisioned 2000 IOPS to the EBS volume. The application hosted on that EBS is experiencing less IOPS than provisioned.

Which of the below mentioned options does not affect the IOPS of the volume?

- The instance is EBS optimized
- The EC2 instance has 10 Gigabit Network connectivity
- ✅ The volume size is too large

Explanation:-When the application does not experience the expected IOPS or throughput of the PIOPS EBS volume that was provisioned, the possible root cause could be that the EC2 bandwidth is the limiting factor and the instance might not be either EBS-optimized or might not have 10 Gigabit network connectivity. Another possible cause for not experiencing the expected IOPS could also be that the user is not driving enough I/O to the EBS volumes. The size of the volume may not affect IOPS.

- The application does not have enough IO for the volume

Q51)

A user has launched a Windows based EC2 instance. However, the instance has some issues and the user wants to check the log.

When the user checks the Instance console output from the AWS console, what will it display?

- The Windows instance does not support the console output
- ✅ The last three system events' log errors

Explanation:-The AWS EC2 console provides a useful tool called Console output for problem diagnosis. It is useful to find out any kernel issues, termination reasons or service configuration issues. For a Windows instance it lists the last three system event log errors. For Linux it displays the exact console output.

- The last 10 system event log error
- All the event logs since instance boot

Q52)

A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances.

How can the user change it?

- ✅ Create an AMI of the running instance and launch the instance in a separate AZ

Explanation:-With AWS EC2, when a user is launching an instance he can select the availability zone (AZ) at the time of launch. If the zone is not selected, AWS selects it on behalf of the user. Once the instance is launched, the user cannot change the zone of that instance unless he creates an AMI of that instance and launches a new instance from it.

- From the AWS EC2 console, select the Actions - > Change zones and specify new zone

- The zone can only be modified using the AWS CLI
- Stop one of the instances and change the availability zone

Q53)

A user has launched an EBS backed instance. The user started the instance at 9 AM in the morning. Between 9 AM to 10 AM, the user is testing some script.

Thus, he stopped the instance twice and restarted it.

In the same hour the user rebooted the instance once.

For how many instance hours will AWS charge the user?

- 4 hours
- ✅ 3 hours

Explanation:-A user can stop/start or reboot an EC2 instance using the AWS console, the Amazon EC2 CLI or the Amazon EC2 API. Rebooting an instance is equivalent to rebooting an operating system. When the instance is rebooted AWS will not charge the user for the extra hours. In case the user stops the instance, AWS does not charge the running cost but charges only the EBS storage cost. If the user starts and stops the instance multiple times in a single hour, AWS will charge the user for every start and stop. In this case, since the instance was rebooted twice, it will cost the user for 3 instance hours.

- 2 hours
- 1 hour

Q54)

A user is publishing custom metrics to CloudWatch.

Which of the below mentioned statements will help the user understand the functionality better?

- The user can use the CloudWatch Import tool
- If the user is uploading the custom data, the user must supply the namespace, timezone, and metric name as part of the command
- ✅ The user should be able to see the data in the console after around 15 minutes

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 user has to always include the namespace as a part of the request. However, the other parameters are optional. If the user has uploaded data using CLI, he can view it as a graph inside the console. The data will take around 2 minutes to upload but can be viewed only after around 15 minutes.

- The user can view as well as upload data using the console, CLI and APIs

---

Q55)

An organization has created 10 IAM users. The organization wants each of the IAM users to have access to a separate DyanmoDB table.

All the users are added to the same group and the organization wants to setup a group level policy for this.

How can the organization achieve this?

- Define the group policy and add a condition which allows the access based on the IAM name
- Create a separate DynamoDB database for each user and configure a policy in the group based on the DB variable
- It is not possible to have a group level policy which allows different IAM users to different DynamoDB tables
- ✅ Create a DynamoDB table with the same name as the IAM user name and define the policy rule which grants access based on the DynamoDB ARN using a variable

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. AWS DynamoDB has only tables and the organization cannot make separate databases. The organization should create a table with the same name as the IAM user name and use the ARN of DynamoDB as part of the group policy. The sample policy is shown below:

```
{
“Version”: “2012-10-17”,
“Statement”: [{
“Effect”: “Allow”,
“Action”: [“dynamodb:*”],
“Resource”: “arn:aws:dynamodb:region:account-number-without-hyphens:table/${aws:username}”
}
]
}
```

Q56)

A user has created a public subnet with VPC and launched an EC2 instance within it. The user is trying to delete the subnet.

What will happen in this scenario?

- The subnet can never be deleted independently, but the user has to delete the VPC first
- It will delete the subnet as well as terminate the instances
- ✅ It will not allow the user to delete the subnet until the instances are terminated

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. When an instance is launched it will have a network interface attached with it. The user cannot delete the subnet until he terminates the instance and deletes the network interface.

- It will delete the subnet and make the EC2 instance as a part of the default subnet

---

Q57)

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside.

How can it achieve this?

- Create an IAM policy with the security group and use that security group for AWS console login
- Create an IAM policy with VPC and allow a secure gateway between the organization and AWS console
- Configure the EC2 instance security group which allows traffic only from the organization's IP range
- ✅ Create an IAM policy with a condition which denies access when the IP address range is not from the organization

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The user can add conditions as a part of the IAM policies. The condition can be set on AWS Tags, Time, and Client IP as well as on many other parameters. If the organization wants the user to access only from a specific IP range, they should set an IAM policy condition which denies access when the IP is not in a certain range. E.g. The sample policy given below denies all traffic when the IP is not in a certain range.

```
"Statement": [{
"Effect": "Deny",
"Action": "*",
"Resource": "*",
"Condition": {
"NotIpAddress": {
"aws:SourceIp": ["10.10.10.0/24", "20.20.30.0/24"]
}
}
}]
```

Q58)

A user is trying to understand the ACL and policy for an S3 bucket.

Which of the below mentioned policy permissions is equivalent to the WRITE ACL on a bucket?

- s3:GetObjectAcl
- ✅ s3:DeleteObject

Explanation:-Amazon S3 provides a set of operations to work with the Amazon S3 resources. Each AWS S3 bucket can have an ACL (Access Control List) or bucket policy associated with it. The WRITE ACL list allows the other AWS accounts to write/modify to that bucket. The equivalent S3 bucket policy permission for it is s3:DeleteObject.

- s3:GetObjectVersion
- s3:ListBucketVersions

Q59)

A user is trying to understand the detailed CloudWatch monitoring concept.

Which of the below mentioned services does not provide detailed monitoring with CloudWatch?

- AWS Route53
- ✅ AWS EMR

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. Services, such as RDS, EC2, Auto Scaling, ELB, and Route 53 can provide the monitoring data every minute.

- AWS RDS
- AWS ELB

Q60)

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AlarmNotification (which notifies Auto Scaling for CloudWatch alarms) process for a while.

What will Auto Scaling do during this period?

- Auto Scaling will execute the policy but it will not launch the instances until the process is resumed
- It is not possible to suspend the AlarmNotification process
- ✅ AWS will receive the alarms but will not execute the Auto Scaling policy

Explanation:-Auto Scaling performs various processes, such as Launch, Terminate Alarm Notification etc. The user can also suspend individual process. The AlarmNotification process type accepts notifications from the Amazon CloudWatch alarms that are associated with the Auto Scaling group. If the user suspends this process type, Auto Scaling will not automatically execute the scaling policies that would be triggered by the alarms.

- AWS will not receive the alarms from CloudWatch

Q61)

A sys admin is trying to understand the Auto Scaling activities.

Which of the below mentioned processes is not performed by Auto Scaling?

- Availability Zone Balancing
- Replace Unhealthy
- Schedule Actions
- ✅ Reboot Instance

Explanation:-There are two primary types of Auto Scaling processes: Launch and Terminate, which launch or terminat instances, respectively. Some other actions performed by Auto Scaling are: AddToLoadbalancer, AlarmNotification, HealthCheck, AZRebalance, ReplaceUnHealthy, and

ScheduledActions.

Q62)

A user is sending the data to CloudWatch using the CloudWatch API. The user is sending data 90 minutes in the future.

What will CloudWatch do in this case?

- It is not possible to send data of the future
- ✓ CloudWatch will accept the data

Explanation:-With Amazon CloudWatch, each metric data point must be marked with a time stamp. The user can send the data using CLI but the time has to be in the UTC format. If the user does not provide the time, CloudWatch will take the data received time in the UTC timezone. The time stamp sent by the user can be up to two weeks in the past and up to two hours into the future.

- The user cannot send data for more than 60 minutes in the future
- It is not possible to send the data manually to CloudWatch

Q63)

A user has configured an Auto Scaling group with ELB. The user has enabled detailed CloudWatch monitoring on Auto Scaling.

Which of the below mentioned statements will help the user understand the functionality better?

- It is not possible to setup detailed monitoring for Auto Scaling
- Detailed monitoring will send data every minute without additional charges
- ✓ In this case, Auto Scaling will send data every minute and will charge the user extra

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. Auto Scaling includes 7 metrics and 1 dimension, and sends data to CloudWatch every 5 minutes by default. The user can enable detailed monitoring for Auto Scaling, which sends data to CloudWatch every minute. However, this will have some extra-costs.

- Auto Scaling sends data every minute only and does not charge the user

Q64)

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

Which of the below mentioned statements is true in this scenario?

- VPC bounds the main route table with a public subnet and a custom route table with a private subnet
- The user has to manually create a NAT instance
- The AWS VPC will automatically create a NAT instance with the micro size
- ✓ VPC bounds the main route table with a private subnet and a custom route table with a public subnet

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 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 a NAT instance of a smaller or higher size, respectively. The VPC has an implied router and the VPC wizard updates the main route table used with the private subnet, creates a custom route table and associates it with the public subnet.

Q65)

A user has launched an RDS postgreSQL DB with AWS. The user did not specify the maintenance window during creation.

The user has configured RDS to update the DB instance type from micro to large.

If the user wants to have it during the maintenance window, what will AWS do?

- It is not possible to change the DB size from micro to large with RDS
- AWS will not allow to update the DB until the maintenance window is configured
- AWS will ask the user to specify the maintenance window during the update
- ✓ AWS will select the default maintenance window if the user has not provided it

Explanation:-AWS RDS has a compulsory maintenance window which by default is 30 minutes. If the user does not specify the maintenance window during the creation of RDS then AWS will select a 30-minute maintenance window randomly from an 8-hour block of time per region. In this case, Amazon RDS assigns a 30-minute maintenance window on a randomly selected day of the week.