Answer Sheet

Q1)

A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance.

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

● The user can directly attach an elastic IP to the instance
✓ The user would need to create an internet gateway and then attach an elastic IP to the instance to connect from internet
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 the user is launching an instance he needs to select an option which attaches a public IP to the instance. If the user has not selected the option to attach the public IP then it will only have a private IP when launched. The user cannot connect to the instance from the internet. If the user wants an elastic IP to connect to the instance from the internet he should create an internet gateway and assign an elastic IP to instance.
● The instance will never launch if the public IP is not assigned
● The instance will always have a public DNS attached to the instance by default

Q2)

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

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

The user has also setup a NAT instance (i-123456) to allow traffic to the internet from the VPN subnet.

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

● Destination: 0.0.0.0/0 and Target: i-12345
● Destination: 172.28.0.0/12 and Target: vgw-12345
● Destination: 20.0.0.0/16 and Target: local
✓ Destination: 20.0.1.0/24 and Target: i-12345
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, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, it will create a virtual private gateway to route all traffic of the VPN subnet. If the user has setup a NAT instance to route all the internet requests then all requests to the internet should be routed to it. All requests to the organization's DC will be routed to the VPN gateway. Here are the valid entries for the main route table in this scenario:
Destination: 0.0.0.0/0 & Target: i-12345 (To route all internet traffic to the NAT Instance)
Destination: 172.28.0.0/12 & Target: vgw-12345 (To route all the organization's data centre traffic to the VPN gateway)
Destination: 20.0.0.0/16 & Target: local (To allow local routing in VPC)

Q3)

An organization is generating digital policy files which are required by the admins for verification. Once the files are verified they may not be required in the future unless there is some compliance issue.

If the organization wants to save them in a cost effective way, which is the best possible solution?

● AWS RRS
✓ AWS Glacier
Explanation:-Amazon S3 stores objects according to their storage class. There are three major storage classes: Standard, Reduced Redundancy and Glacier. Standard is for AWS S3 and provides very high durability. However, the costs are a little higher. Reduced redundancy is for less critical files. Glacier is for archival and the files which are accessed infrequently. It is an extremely low-cost storage service that provides secure and durable storage for data archiving and backup.
● AWS S3
● AWS RDS

Q4)

A root account owner has created an S3 bucket testmycloud. The account owner wants to allow everyone to upload the objects as well as enforce that the person who uploaded the object should manage the permission of those objects.

Which is the easiest way to achieve this?

● The root account owner should create a bucket policy which allows the IAM users to upload the object
● The root account should create the IAM users and provide them the permission to upload content to the bucket
● The root account owner should create the bucket policy which allows the other account owners to set the object policy of that bucket
✓ The root account should use ACL with the bucket to allow everyone to upload the object
Explanation:-Each AWS S3 bucket and object has an ACL (Access Control List) associated with it. An ACL is a list of grants identifying the grantee and the permission granted. The user can use ACLs to grant basic read/write permissions to other AWS accounts. ACLs use an Amazon S3–specific XML schema. The user cannot grant permissions to other users in his account. ACLs are suitable for specific scenarios. For example, if a bucket owner allows other AWS accounts to upload objects, permissions to these objects can only be managed using the object ACL by the AWS account that owns the object.

Q5)

A user has configured an SSL listener at ELB as well as on the back-end instances.

Which of the below mentioned statements helps the user understand ELB traffic handling with respect to the SSL listener?

✓ ELB will not modify the headers

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. SSL does not support sticky sessions. If the user has enabled a proxy protocol it adds the source and destination IP to the header.

● ELB will intercept the request to add the cookie details if sticky session is enabled
● ELB will modify headers to add requestor details
● It is not possible to have the SSL listener both at ELB and back-end instances

---

Q6)

A user is configuring the Multi AZ feature of an RDS DB. The user came to know that this RDS DB does not use the AWS technology, but uses server mirroring to achieve HA.

Which DB is the user using right now?

● PostgreSQL
● My SQL
● Oracle
✓ MS SQL

Explanation:-Amazon RDS provides high availability and failover support for DB instances using Multi AZ deployments. In a Multi AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. Multi AZ deployments for Oracle, PostgreSQL, and MySQL DB instances use Amazon technology, while SQL Server (MS SQL) DB instances use SQL Server Mirroring.

Q7)

A user has enabled the Multi AZ feature with the MS SQL RDS database server.

Which of the below mentioned statements will help the user understand the Multi AZ feature better?

● In a Multi AZ, AWS runs two DBs in parallel and copies the data synchronously to the replica copy
● In a Multi AZ, AWS runs two DBs in parallel and copies the data asynchronously to the replica copy
✓ In a Multi AZ, AWS runs just one DB but copies the data synchronously to the standby replica

Explanation:-Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Note that the high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a read replica.

● AWS MS SQL does not support the Multi AZ feature

Q8) An admin is planning to monitor the ELB. Which of the below mentioned services does not help the admin capture the monitoring information about the ELB activity?

● ELB Access logs
✓ ELB health check

Explanation:-The admin can capture information about Elastic Load Balancer using either:
CloudWatch Metrics
ELB Logs files which are stored in the S3 bucket
CloudTrail with API calls which can notify the user as well generate logs for each API calls
The health check is internally performed by ELB and does not help the admin get the ELB activity.

● CloudWatch metrics
● ELB API calls with CloudTrail

Q9)

A user is measuring the latency of an application every minute and storing data inside a file in the JSON format and wants to send all latency data to AWS CloudWatch.

How can the user achieve this?

● The user has to parse the file before uploading data to CloudWatch
✓ The user can supply the file as an input to the CloudWatch command

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 part of the request. If the user wants to upload the custom data from a file, he can supply file name along with the parameter –metric-data to command put-metric-data.

● It is not possible to upload the custom data to CloudWatch
● The user can use the CloudWatch Import command to import data from the file to CloudWatch

---

Q10)

A user has launched an EBS backed EC2 instance. The user has rebooted the instance.

Which of the below mentioned statements is not true with respect to the reboot action?

● The Elastic IP remains associated with the instance
● The private and public address remains the same

● The volume is preserved

✓ The instance runs on a new host computer

Explanation:-A user can 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. However, it is recommended that the user use the Amazon EC2 to reboot the instance instead of running the operating system reboot command from the instance. The instance remains on the same host computer and maintains its public DNS name, private IP address, and any data on its instance store volumes. It typically takes a few minutes for the reboot to complete, but the time it takes to reboot depends on the instance configuration.

Q11)

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AddToLoadBalancer (which adds instances to the load balancer) process for a while.

What will happen to the instances launched during the suspension period?

● It is not possible to suspend only the AddToLoadBalancer process

✓ The instances will not be registered with ELB and the user has to manually register when the process is resumed

Explanation:-Auto Scaling performs various processes, such as Launch, Terminate, add to Load Balancer etc. The user can also suspend the individual process. The AddToLoadBalancer process type adds instances to the load balancer when the instances are launched. If this process is suspended, Auto Scaling will launch the instances but will not add them to the load balancer. When the user resumes this process, Auto Scaling will resume adding new instances launched after resumption to the load balancer. However, it will not add running instances that were launched while the process was suspended; those instances must be added manually.

● Auto Scaling will not launch the instance during this period due to process suspension

● The instances will be registered with ELB only once the process has resumed

---

Q12)

An organization is planning to use AWS for 5 different departments. The finance department is responsible to pay for all the accounts.

However, they want the cost separation for each account to map with the right cost centre.

How can the finance department achieve this?

● Create 5 separate accounts and use the IAM cross account access with the roles for better management

● Create 5 separate IAM users and set a different policy for their access

✓ Create 5 separate accounts and make them a part of one consolidate 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. 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.

● Create 5 separate IAM groups and add users as per the department's employees

---

Q13)

A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance.

The user has 3 elastic IPs and is trying to assign one of the Elastic IPs to the VPC instance from the console.

The console does not show any instance in the IP assignment screen.

What is a possible reason that the instance is unavailable in the assigned IP console?

● The IP address belongs to a different zone than the subnet zone

✓ The IP addresses belong to EC2 Classic; so they cannot be assigned to VPC

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 the user is launching an instance he needs to select an option which attaches a public IP to the instance. If the user has not selected the option to attach the public IP then it will only have a private IP when launched. If the user wants to connect to an instance from the internet he should create an elastic IP with VPC. If the elastic IP is a part of EC2 Classic it cannot be assigned to a VPC instance.

● The IP address may be attached to one of the instances

● The user has not created an internet gateway

Q14)

A user has setup an EBS backed instance and attached 2 EBS volumes to it. The user has setup a CloudWatch alarm on each volume for the disk data.

The user has stopped the EC2 instance and detached the EBS volumes.

What will be the status of the alarms on the EBS volume?

● Alarm

● OK

● The EBS cannot be detached until all the alarms are removed

✓ Insufficient Data

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. Alarms invoke actions only for sustained state changes. There are three states of the alarm: OK, Alarm and Insufficient data. In this case since the EBS is detached and inactive the state will be Insufficient.

Q15)

A user has launched an EBS backed EC2 instance in the US-East-1a region. The user stopped the instance and started it back

after 20 days.

AWS throws up an ‘InsufficientInstanceCapacity’ error.

What can be the possible reason for this?

● AWS zone mapping is changed for that user account
● The user account has reached the maximum EC2 instance limit
● There is some issue with the host capacity on which the instance is launched
✓ AWS does not have sufficient capacity in that availability zone
Explanation:-When the user gets an ‘InsufficientInstanceCapacity’ error while launching or starting an EC2 instance, it means that AWS does not currently have enough available capacity to service the user request. If the user is requesting a large number of instances, there might not be enough server capacity to host them. The user can either try again later, by specifying a smaller number of instances or changing the availability zone if launching a fresh instance.

Q16)

A user has setup an EBS backed instance and a CloudWatch alarm when the CPU utilization is more than 65%. The user has setup the alarm to watch it for 5 periods of 5 minutes each.

The CPU utilization is 60% between 9 AM to 6 PM.

The user has stopped the EC2 instance for 15 minutes between 11 AM to 11:15 AM.

What will be the status of the alarm at 11:30 AM?

● Error
✓ OK
Explanation:-Amazon CloudWatch alarm watches a single metric over a time period 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 state of the alarm will be OK for the whole day. When the user stops the instance for three periods the alarm may not receive the data.
● Alarm
● Insufficient Data

Q17)

A user has launched an EC2 instance from an instance store backed AMI. The infrastructure team wants to create an AMI from the running instance.

Which of the below mentioned steps will not be performed while creating the AMI?

● Upload the bundled volume
✓ Define the AMI launch permissions
Explanation:-When the user has launched an EC2 instance from an instance store backed AMI, it will need to follow certain steps, such as “Bundling the root volume”, “Uploading the bundled volume” and “Register the AMI”. Once the AMI is created the user can setup the launch permission. However, it is not required to setup during the launch.
● Register the AMI
● Bundle the volume

Q18)

A user has deployed an application on an EBS backed EC2 instance. For a better performance of application, it requires dedicated EC2 to EBS traffic.

How can the user achieve this?

● Launch the EC2 instance as EBS dedicated with PIOPS EBS
✓ Launch the EC2 instance as EBS optimized with PIOPS EBS
Explanation:-Any application which has performance sensitive workloads and requires minimal variability with dedicated EC2 to EBS traffic should use provisioned IOPS EBS volumes, which are attached to an EBS-optimized EC2 instance or it should use an instance with 10 Gigabit network connectivity. Launching an instance that is EBS-optimized provides the user with a dedicated connection between the EC2 instance and the EBS volume.
● Launch the EC2 instance as EBS dedicated with PIOPS EBS
● Launch the EC2 instance as EBS enhanced with PIOPS EBS

Q19)

You are managing the AWS account of a big organization. The organization has more than 1000+ employees and they want to provide access to the various services to most of the employees.

Which of the below mentioned options is the best possible solution in this case?

● The user should create an IAM role and attach STS with the role. The user should attach that role to the EC2 instance and setup AWS authentication on that server
● The user should create a separate IAM user for each employee and provide access to them as per the policy
● The user should create IAM groups as per the organization’s departments and add each user to the group for better access control
✓ Attach an IAM role with the organization’s authentication service to authorize each user for various AWS services
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 is managing an AWS account for an organization that already has an identity system, such as the login system for the corporate network (SSO). In this case, instead of creating individual IAM users or groups for each user who need AWS access, it may be more practical to use a proxy server to translate the user identities from the organization network into the temporary AWS security credentials. This proxy server will attach an IAM role to the user after authentication.

Q20)

A user has launched an EC2 Windows instance from an instance store backed AMI. The user has also set the Instance initiated shutdown behaviour to stop.

What will happen when the user shuts down the OS?

● The instance will stay running but the OS will be shutdown

● The instance will be terminated

● It will not allow the user to shutdown the OS when the shutdown behaviour is set to Stop

✓ It is not possible to set the termination behaviour to Stop for an Instance store backed AMI instance

Explanation:-When the EC2 instance is launched from an instance store backed AMI, it will not allow the user to configure the shutdown behaviour to "Stop". It gives a warning that the instance does not have the EBS root volume.

Q21)

An organization has configured Auto Scaling for hosting their application.

The system admin wants to understand the Auto Scaling health check process.

If the instance is unhealthy, Auto Scaling launches an instance and terminates the unhealthy instance.

What is the order execution?

✓ Auto Scaling terminates the instance first and then launches a new instance

Explanation:-Auto Scaling keeps checking the health of the instances at regular intervals and marks the instance for replacement when it is unhealthy. The ReplaceUnhealthy process terminates instances which are marked as unhealthy and subsequently creates new instances to replace them. This process first terminates the instance and then launches a new instance.

● Auto Scaling performs the launch and terminate processes in a random order

● Auto Scaling launches a new instance first and then terminates the unhealthy instance

● Auto Scaling launches and terminates the instances simultaneously

Q22)

A system admin is planning to encrypt all objects being uploaded to S3 from an application.

The system admin does not want to implement his own encryption algorithm; instead he is planning to use server side encryption by supplying his own key (SSE-C).

Which parameter is not required while making a call for SSE-C?

● x-amz-server-side-encryption-customer-key

● x-amz-server-side-encryption-customer-key-MD5

✓ x-amz-server-side-encryption-customer-key-AES-256

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). When the user is supplying his own encryption key, the user has to send the below mentioned parameters as a part of the API calls:
x-amz-server-side-encryption-customer-algorithm: Specifies the encryption algorithm
x-amz-server-side-encryption-customer-key: To provide the base64-encoded encryption key
x-amz-server-side-encryption-customer-key-MD5: To provide the base64-encoded 128-bit MD5 digest of the encryption key

● x-amz-server-side-encryption-customer-algorithm

Q23)

A user is using the AWS SQS to decouple the services.

Which of the below mentioned operations is not supported by SQS?

● SendMessageBatch

● CreateQueue

✓ DeleteMessageQueue

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. The user can perform the following set of operations using the Amazon SQS: CreateQueue, ListQueues, DeleteQueue, SendMessage, SendMessageBatch, ReceiveMessage, DeleteMessage, DeleteMessageBatch, ChangeMessageVisibility, ChangeMessageVisibilityBatch, SetQueueAttributes, GetQueueAttributes, GetQueueUrl, AddPermission and RemovePermission. Operations can be performed only by the AWS account owner or an AWS account that the account owner has delegated to.

● DeleteMessageBatch

Q24)

A user has setup Auto Scaling with ELB on the EC2 instances.

The user wants to configure that whenever the CPU utilization is below 10%, Auto Scaling should remove one instance.

How can the user configure this?

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

● Use CloudWatch to monitor the data and Auto Scaling to remove the instances using scheduled actions

● The user can get an email using SNS when the CPU utilization is less than 10%. The user can use the desired capacity of Auto Scaling to remove the instance

✓ Configure CloudWatch to send a notification to the Auto Scaling group when the CPU Utilization is less than 10% and configure the Auto Scaling policy to remove the instance

Explanation:-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 setup to receive a notification on the Auto Scaling group with the CloudWatch alarm when the CPU utilization is below a certain threshold. The user can configure the Auto Scaling policy to take action for removing the instance. When the CPU utilization is below 10% CloudWatch will send an alarm to the Auto Scaling group to execute the policy.

Q25)

A user want's to configure a CloudWatch alarm on RDS to receive a notification when the CPU utilization of RDS is higher than 50%. Currently – at the time the user wants to create the alarm, there is some activity on RDS, such as RDS unavailability.

How must the user procede?

● Setup the notification when the CPU is more than 75% on RDS
● It is not possible to setup the alarm on RDS under the circumstances
● Setup the notification when the CPU utilization is less than 10%
✓ Setup the notification when the state is Insufficient Data

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 alarm has three states: Alarm, OK and Insufficient data. The Alarm will change to Insufficient Data when any of the three situations arise: when the alarm has just started, when the metric is not available or when enough data is not available for the metric to determine the alarm state. If the user wants to find that RDS is not available, he can setup to receive the notification when the state is in Insufficient data.

Q26) A user has configured Auto Scaling with the minimum capacity as 2 and the desired capacity as 2. The user is trying to terminate one of the existing instance with the command:
as-terminate-instance-in-auto-scaling-group –decrement-desired-capacity
What will Auto Scaling do in this scenario?

✓ Throws an error

Explanation:-The Auto Scaling command as-terminate-instance-in-auto-scaling-group will terminate the specific instance ID. The user is required to specify the parameter as –decrement-desired-capacity. Then Auto Scaling will terminate the instance and decrease the desired capacity by 1. In this case since the minimum size is 2, Auto Scaling will not allow the desired capacity to go below 2. Thus, it will throw an error.

● Terminates the instance and updates the desired capacity and minimum size to 1
● Terminates the instance and does not launch a new instance
● Terminates the instance and updates the desired capacity to 1

Q27)

A user is planning to evaluate AWS for their internal use. The user does not want to incur any charge on his account during the evaluation.

Which of the below mentioned AWS services would incur a charge if used?

● AWS S3 with 1 GB of storage
● AWS micro instance running 24 hours daily
● AWS ELB running 24 hours a day
✓ AWS PIOPS volume of 10 GB size

Explanation:-AWS is introducing a free usage tier for one year to help the new AWS customers get started in Cloud. The free tier can be used for anything that the user wants to run in the Cloud. AWS offers a handful of AWS services as a part of this which includes 750 hours of free micro instances and 750 hours of ELB. It includes the AWS S3 of 5 GB and AWS EBS general purpose volume upto 30 GB. PIOPS is not part of free usage tier.

Q28)

An organization has configured the custom metric upload with CloudWatch. The organization has given permission to its employees to upload data using CLI as well SDK.

How can the user track the calls made to CloudWatch?

● Create an IAM user and allow each user to log the data using the S3 bucket
✓ Use CloudTrail to monitor the API calls

Explanation:-AWS CloudTrail is a web service which will allow the user to monitor the calls made to the Amazon CloudWatch API for the organization's account, including calls made by the AWS Management Console, Command Line Interface (CLI), and other services. When CloudTrail logging is turned on, CloudWatch will write log files into the Amazon S3 bucket, which is specified during the CloudTrail configuration.

● The user can enable logging with CloudWatch which logs all the activities
● Enable detailed monitoring with CloudWatch

Q29)

An organization, which has the AWS account ID as 999988887777, has created 50 IAM users. All the users are added to the same group cloudacademy.

If the organization has enabled that each IAM user can login with the AWS console, which AWS login URL will the IAM users use??

✓ https:// 999988887777.signin.aws.amazon.com/console/

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Once the organization has created the IAM users, they will have a separate AWS console URL to login to the AWS console. The console login URL for the IAM user will be https:// AWS_Account_ID.signin.aws.amazon.com/console/. It uses only the AWS account ID and does not depend on the group or user ID.

● https:// signin.aws.amazon.com/cloudacademy/
● https:// cloudacademy.signin.aws.amazon.com/999988887777/console/
● https:// 999988887777.aws.amazon.com/ cloudacademy/

Q30)

A user has created a Cloudformation stack. The stack creates AWS services, such as EC2 instances, ELB, AutoScaling, and RDS.

While creating the stack it created EC2, ELB and AutoScaling but failed to create RDS.

What will Cloudformation do in this scenario?

● Cloudformation can never throw an error after launching a few services since it verifies all the steps before launching
● It will warn the user about the error and ask the user to manually create RDS
● It will wait for the user's input about the error and correct the mistake after the input
✓ Rollback all the changes and terminate all the created services

Explanation:-AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. The AWS Cloudformation stack is a collection of AWS resources which are created and managed as a single unit when AWS CloudFormation instantiates a template. If any of the services fails to launch, Cloudformation will rollback all the changes and terminate or delete all the created services.

Q31)

A user is trying to send custom metrics to CloudWatch using the PutMetricData APIs.

Which of the below mentioned points should the user needs to take care while sending the data to CloudWatch?

● The size of a request is limited to 40KB for HTTP GET requests and 8KB for HTTP POST requests
● The size of a request is limited to 128KB for HTTP GET requests and 64KB for HTTP POST requests
✓ The size of a request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests

Explanation:-With AWS CloudWatch, the user can publish data points for a metric that share not only the same time stamp, but also the same namespace and dimensions. CloudWatch can accept multiple data points in the same PutMetricData call with the same time stamp. The only thing that the user needs to take care of is that the size of a PutMetricData request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests.

● The size of a request is limited to 16KB for HTTP GET requests and 80KB for HTTP POST requests

Q32)

A system admin is planning to setup event notifications on RDS.

Which of the below mentioned services will help the admin setup notifications?

✓ AWS SNS

Explanation:-Amazon RDS uses the Amazon Simple Notification Service to provide a notification when an Amazon RDS event occurs. These notifications can be in any notification form supported by Amazon SNS for an AWS region, such as an email, a text message or a call to an HTTP endpoint.

● AWS Cloudtrail
● AWS SES
● AWS Cloudwatch

Q33)

A user has created a VPC with CIDR 20.0.0.0/16 using VPC Wizard. The user has created a public CIDR (20.0.0.0/24) and a VPN only subnet CIDR (20.0.1.0/24) along with the hardware VPN access to connect to the user's data centre.

Which of the below mentioned components is not present when the VPC is setup with the wizard?

● Main route table attached with a VPN only subnet
● Custom route table attached with a public subnet
✓ A NAT instance configured to allow the VPN subnet instances to connect with the internet

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, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, 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. The wizard does not create a NAT instance by default. The user can create it manually and attach it with a VPN only subnet.

● An internet gateway for a public subnet

Q34)

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.

Which of the below mentioned entries are required in the main route table to allow the instances in VPC to communicate with each other?

● Destination : 20.0.0.0/16 and Target : Local
✓ Destination : 20.0.0.0/24 and Target : Local

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: 20.0.0.0/24 and Target: Local", which allows all instances in the VPC to communicate with each other.

● Destination : 20.0.0.0/16 and Target : ALL
● Destination : 20.0.0.0/0 and Target : ALL

Q35)

You are building an online store on AWS that uses SQS to process your customer orders.

Your backend system needs those messages in the same sequence the customer orders have been put in.

How can you achieve that?

● It is not possible to do this with SQS
✓ You can use sequencing information on each message

Explanation:-Amazon SQS is engineered to always be available and deliver messages. One of the resulting tradeoffs is that SQS does not guarantee first in, first out delivery of messages. For many distributed applications, each message can stand on its own, and as long as all messages are delivered, the order is not important. If your system requires that order be preserved, you can place sequencing information in each message, so that you can reorder the messages when the queue returns them.

● You can do this with SQS but you also need to use SWF
● Messages will arrive in the same order by default

Q36)

A user has setup a billing alarm using CloudWatch for $200.

The usage of AWS exceeded $200 after some days.

The user wants to increase the limit from $200 to $400?

What should the user do?

● Create a new alarm for the additional $200 amount
● It is not possible to modify the alarm once it has crossed the usage limit
✓ Update the alarm to set the limit at $400 instead of $200

Explanation:-AWS CloudWatch supports enabling the billing alarm on the total AWS charges. The estimated charges are calculated and sent several times daily to CloudWatch in the form of metric data. This data will be stored for 14 days. This data also includes the estimated charges for every service in AWS used by the user, as well as the estimated overall AWS charges. If the user wants to increase the limit, the user can modify the alarm and specify a new threshold.

● Create a new alarm of $400 and link it with the first alarm

---

Q37)

A user is planning to use AWS Cloudformation.

Which of the below mentioned functionalities does not help him to correctly understand Cloudformation?

● Cloudformation works with a wide variety of AWS services, such as EC2, EBS, VPC, IAM, S3, RDS, ELB, etc
● AWS Cloudfromation does not charge the user for its service but only charges for the AWS resources created with it
✓ Cloudformation follows the DevOps model for the creation of Dev & Test

Explanation:-AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. It supports a wide variety of AWS services, such as EC2, EBS, AS, ELB, RDS, VPC, etc. It also provides application bootstrapping scripts which enable the user to install software packages or create folders. It is free of the cost and only charges the user for the services created with it. The only challenge is that it does not follow any model, such as DevOps; instead customers can define templates and use them to provision and manage the AWS resources in an orderly way.

● CloudFormation provides a set of application bootstrapping scripts which enables the user to install software

---

Q38)

A user has launched an EC2 instance from an instance store backed AMI. The infrastructure team wants to create an AMI from the running instance.

Which of the below mentioned credentials is not required while creating the AMI?

● X.509 certificate and private key
✓ AWS login ID to login to the console

Explanation:-When the user has launched an EC2 instance from an instance store backed AMI and the admin team wants to create an AMI from it, the user needs to setup the AWS AMI or the API tools first. Once the tool is setup the user will need the following credentials:
AWS account ID;
AWS access and secret access key;
X.509 certificate with private key.

● Access key and secret access key
● AWS account ID

Q39)

A customer is using AWS for Dev and Test. The customer wants to setup the Dev environment with Cloudformation.

Which of the below mentioned steps are not required while using Cloudformation?

● Provide the parameters configured as part of the template
✓ Configure a service

Explanation:-AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. AWS CloudFormation introduces two concepts: the template and the stack. The template is a JSON-format, text-based file that describes all the AWS resources required to deploy and run an application. The stack is a collection of AWS resources which are created and managed as a single unit when AWS CloudFormation instantiates a template. While creating a stack, the user uploads the template and provides the data for the parameters if required.

● Create and upload the template
● Create a stack

Q40)

A user has a weighing plant. The user measures the weight of some goods every 5 minutes and sends data to AWS CloudWatch for monitoring and tracking.

Which of the below mentioned parameters is mandatory for the user to include in the request list?

● Metric Name
● Value
● Timezone
✓ Namespace

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. The user has to always include the namespace as part of the request. The user can supply a file instead of the metric name. If the user does not supply the timezone, it accepts the current time. If the user is sending the data as a single data point it will have parameters, such as value. However, if the user is sending as an aggregate it will have parameters, such as statistic-values.

Q41)

A user has launched an EBS backed EC2 instance.

What will be the difference while performing the restart or stop/start options on that instance?

● For restart it charges extra only once, while for every stop/start it will be charged as a separate hour
● Every restart is charged by AWS as a separate hour, while multiple start/stop actions during a single hour will be counted as a single hour
✓ For restart it does not charge for an extra hour, while every stop/start it will be charged as a separate hour

Explanation:-For an EC2 instance launched with an EBS backed AMI, each time the instance state is changed from stop to start/ running, AWS charges a full instance hour, even if these transitions happen multiple times within a single hour. Anyway, rebooting an instance AWS does not charge a new instance billing hour.

● For every restart or start/stop it will be charged as a separate hour

---

Q42)

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

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

● The VPC will launch one NAT instance with an elastic IP
✓ The VPC will create a routing instance and attach it with a public subnet

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 a NAT instance with an elastic IP. Wizard will also create two subnets with route tables. It will also create an internet gateway and attach it to the VPC.

● The VPC will create one internet gateway and attach it to VPC
● The VPC will create two subnets

Q43)

A storage admin wants to encrypt all the objects stored in S3 using server side encryption. The user does not want to use the AES 256 encryption key provided by S3.

How can the user achieve this?

● S3 does not support client supplied encryption keys for server side encryption
● The admin should use CLI or API to upload the encryption key to the S3 bucket. When making a call to the S3 API mention the encryption key URL in each request
● The admin should upload his secret key to the AWS console and let S3 decrypt the objects
✓ The admin should send the keys and encryption algorithm with each API call

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. Amazon S3 never stores the user's encryption key. The user has to supply it for each encryption or decryption call.

Q44)

A user has created numerous EBS volumes.

What is the general limit for each AWS account for the maximum number of EBS volumes that can be created?

● 10000

✓ 5000

Explanation:-A user can attach multiple EBS volumes to the same instance within the limits specified by his AWS account. Each AWS account has a limit on the number of Amazon EBS volumes that the user can create, and the total storage available. The default limit for the maximum number of volumes that can be created is 5000.

● 1000

● 100

Q45)

A user is collecting 1000 records per second. The user wants to send the data to CloudWatch using the custom namespace.

Which of the below mentioned options is recommended for this activity?

● It is not possible to send all the data in one call. Thus, it should be sent one by one. CloudWatch will aggregate the data automatically

● Create one csv file of all the data and send a single file to CloudWatch

● Send all the data values to CloudWatch in a single command by separating them with a comma. CloudWatch will parse automatically

✓ Aggregate the data with statistics, such as Min, max, Average, Sum and Sample data and send the data to CloudWatch

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 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. It is recommended that when the user is having multiple data points per minute, he should aggregate the data so that it will minimize the number of calls to put-metric-data. In this case it will be single call to CloudWatch instead of 1000 calls if the data is aggregated.

Q46)

An organization is trying to create various IAM users.

Which of the below mentioned options is not a valid IAM username?

● John.cloud

✓ john#cloud

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. The names of users, groups, roles, instance profiles must be alphanumeric, including the following common characters: plus (+), equal (=), comma (,), period (.), at (@), and dash (-).

● john@cloud

● John=cloud

Q47)

A user has configured Elastic Load Balancing by enabling a Secure Socket Layer (SSL) negotiation configuration known as a Security Policy.

Which of the below mentioned options is not part of this secure policy while negotiating the SSL connection between the user and the client?

● Server Order Preference

✓ Client 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. A security policy is a combination of SSL Protocols, SSL Ciphers, and the Server Order Preference option.

● SSL Ciphers

● SSL Protocols

Q48)

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

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

● It is not possible to setup detailed monitoring for ELB

● ELB will send data every minute and will charge the user extra

✓ ELB sends data to CloudWatch every minute only and does not charge the user

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. Elastic Load Balancing includes 10 metrics and 2 dimensions, and sends data to CloudWatch every minute. This does not cost extra.

● ELB is not supported by CloudWatch

Q49)

George has shared an EC2 AMI created in the US East region from his AWS account with Stefano. George copies the same AMI to the US West region.

Can Stefano access the copied AMI of George’s account from the US West region?

● Yes, since copy AMI copies all the permissions attached with the AMI

● Yes, since copy AMI copies all private account sharing permissions

✓ No, copy AMI does not copy the permission

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. AWS does not copy launch the permissions, user-defined tags or the Amazon S3 bucket permissions from the source AMI to the new AMI. Thus, in this case by default Stefano will not have access to the AMI in the US West region.

● It is not possible to share the AMI with a specific account

Q50)

An organization wants to move to Cloud. They are looking for a secure encrypted database storage option.

Which of the below mentioned AWS functionalities helps them to achieve this?

● Multi-tier encryption with Redshift

✓ AWS EBS encryption

Explanation:-AWS EBS supports encryption of the volume while creating new volumes. 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 EBS will be encrypted. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between the EC2 instances and EBS storage. EBS encryption is based on the AES-256 cryptographic algorithm, which is the industry standard.

● AWS MFA with EBS

● AWS S3 server side storage

Q51)

A user is having data generated randomly based on a certain event. The user wants to upload that data to CloudWatch.

It may happen that event may not have data generated for some period due to randomness.

Which of the below mentioned options is a recommended option for this case?

● For the period when there is no data, the user should not send the data at all

✓ For the period when there is no data the user should send the value as 0

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. When the user data is more random and not generated at regular intervals, there can be a period which has no associated data. The user can either publish the zero (0) value for that period or not publish the data at all. It is recommended that the user should publish zero instead of no value to monitor the health of the application. This is helpful in an alarm as well as in the generation of the sample data count.

● The user must upload the data to CloudWatch as having no data for some period will cause an error at CloudWatch monitoring

● For the period when there is no data the user should send a blank value

Q52)

An AWS account owner has setup multiple IAM users. One IAM user only has CloudWatch access.

He has setup the alarm action which stops the EC2 instances when the CPU utilization is below the threshold limit.

What will happen in this case?

✓ The user can setup the action but it will not be executed if the user does not have EC2 rights

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 setup an action which stops the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action. If the IAM user has read/write permissions for Amazon CloudWatch but not for Amazon EC2, he can still create an alarm. However, the stop or terminate actions will not be performed on the Amazon EC2 instance.

● The user cannot set an alarm on EC2 since he does not have the permission

● It is not possible to stop the instance using the CloudWatch alarm

● CloudWatch will stop the instance when the action is executed

Q53)

A user has configured the AWS CloudWatch alarm for estimated usage charges in the US East region.

Which of the below mentioned statements is not true with respect to the estimated charges?

● The metric data will represent the data of all the regions

✓ The metric data will show data specific to that region

Explanation:-When the user has enabled the monitoring of estimated charges for the AWS account with AWS CloudWatch, the estimated charges are calculated and sent several times daily to CloudWatch in the form of metric data. This data will be stored for 14 days. The billing metric data is stored in the US East (Northern Virginia) region and represents worldwide charges.

Hence, the metric data will not show data specific to that region.

This data also includes the estimated charges for every service in AWS used by the user, as well as the estimated overall AWS charges.

● It will include the estimated charges of every AWS service

● It will store the estimated charges data of the last 14 days

Q54)

A user has configured CloudWatch monitoring on an EBS backed EC2 instance.

If the user has not attached any additional device, which of the below mentioned metrics will always show a 0 value?

● NetworkIn

✓ DiskReadBytes

Explanation:-CloudWatch is used to monitor AWS as the well custom services. For EC2 when the user is monitoring the EC2 instances, it will capture the 7 Instance level and 3 system check parameters for the EC2 instance. Since this is an EBS backed instance, it will not have ephermal storage attached to it. Out of the 7 EC2 metrics, the 4 metrics DiskReadOps, DiskWriteOps, DiskReadBytes and DiskWriteBytes are disk related data and available only when there is ephermal storage attached to an instance. For an EBS backed instance without any additional device, this data will be 0.

● CPUUtilization
● NetworkOut

Q55)

A sys admin is maintaining an application on AWS. The application is installed on EC2 and user has configured ELB and Auto Scaling.

Considering future load increase, the user is planning to launch new servers proactively so that they get registered with ELB.

How can the user add these instances with Auto Scaling?

● Decrease the minimum limit of the Auto Scaling group
● Increase the maximum limit of the Auto Scaling group
✓ Increase the desired capacity of the Auto Scaling group

Explanation:-A user can increase the desired capacity of the Auto Scaling group and Auto Scaling will launch a new instance as per the new capacity. The newly launched instances will be registered with ELB if Auto Scaling group is configured with ELB. If the user decreases the minimum size the instances will be removed from Auto Scaling. Increasing the maximum size will not add instances but only set the maximum instance cap.

● Launch an instance manually and register it with ELB on the fly

Q56)

A user has created photo editing software and hosted it on EC2. The software accepts requests from the user about the photo format and resolution and sends a message to S3 to enhance the picture accordingly.

Which of the below mentioned AWS services will help make a scalable software with the AWS infrastructure in this scenario?

● AWS Simple Notification Service
● AWS Elastic Transcoder
● AWS Glacier
✓ 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. The user can configure SQS, which will decouple the call between the EC2 application and S3. Thus, the application does not keep waiting for S3 to provide the data.

Q57)

An organization has created 50 IAM users. The organization wants that each user can change their password but cannot change their access keys.

How can the organization achieve this?

● The root account owner has to use CLI which forces each IAM user to change their password on first login
● By default each IAM user can modify their passwords
● The organization has to create a special password policy and attach it to each user
✓ The root account owner can set the policy from the IAM console under the password policy screen

Explanation:-With AWS IAM, organizations can use the AWS Management Console to display, create, change or delete a password policy. As a part of managing the password policy, the user can enable all users to manage their own passwords. If the user has selected the option which allows the IAM users to modify their password, he does not need to set a separate policy for the users. This option in the AWS console allows changing only the password.

Q58) Best practice is to pre-warm:
Choose the correct answer:

● Elastic load balancers that you are expecting will experience a large increase in traffic. Pre-warm using the read and write back method.
● EBS volumes that were created from scratch. Pre-warm using the read and then write back method.
✓ Newly created EBS volumes. Pre-warm using the read and then write back method.

Explanation:-Newly created EBS volumes. Pre-warm using the read and then write back method. The read and write back method is used to pre-warm EBS volumes created from a snapshot. Fresh EBS volumes do require read or write back during pre-warming. Elastic load balancers should be pre-warmed prior to an anticipated large spike in traffic, but this is done by contacting AWS to provision additional back-end resources, not by a read and write back command.

● Elastic load balancers that recently experienced a large increase in traffic.

Q59) Your AWS application is set up to use Auto Scaling with an ELB. To be sure that your application is performing its best and the page loads quickly what, precisely, could you monitor in CloudWatch? Choose the correct answer:

● Monitor the Hard Drive IOPS
● Monitor the CPU utilization
● Set up a third-party monitoring solution
✓ Monitor your ELB latency using CloudWatch metrics

Explanation:-CloudWatch provides latency metrics which monitor the time it takes for the request to go from the Elastic Load Balancer to the instance and back. Latency is a good metric to determine if our Elastic Load Balancer is healthy

Q60)

A user wants to upload a complete folder to AWS S3 using the S3 Management console.

How can the user perform this activity?

● Just drag and drop the folder using the flash tool provided by S3
● The user cannot upload the whole folder in one go with the S3 management console
✓ Use the Enable Enhanced Uploader option from the S3 console while uploading objects
Explanation:-AWS S3 provides a console to upload objects to a bucket. The user can use the file upload screen to upload the whole folder in one go by clicking on the Enable Enhanced Uploader option. When the user uploads a folder, Amazon S3 uploads all the files and subfolders from the specified folder to the user's bucket. It then assigns a key value that is a combination of the uploaded file name and the folder name.
● Use the Enable Enhanced Folder option from the S3 console while uploading objects

---

Q61)

A user has created an EBS volume of 10 GB and attached it to a running instance. The user is trying to access EBS for first time.

Which of the below mentioned options is the correct statement with respect to a first time EBS access?

✓ The volume will show a loss of the IOPS performance the first time
Explanation:-The volume will show a loss of the IOPS performance the first time
● If the EBS is mounted it will ask the user to create a file system
● The volume will show a size of 8 GB
● The volume will be blank

Q62) A sysadmin has created the below mentioned policy on an S3 bucket named cloudacademy. What does this policy define?
"Statement": [{
"Sid": "Stmt1388811069831",
"Effect": "Allow",
"Principal": { "AWS": "*"},
"Action": ["s3:GetObjectAcl", "s3:ListBucket"],
"Resource": ["arn:aws:s3:::cloudacademy]
}]

✓ It will make the cloudacademy bucket as public
Explanation:-A sysadmin can grant permission to the S3 objects or the buckets to any user or make 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. In the sample policy the action says "S3:ListBucket" for effect Allow on Resource arn:aws:s3:::cloudacademy. This will make the cloudacademy bucket public.
"Statement": [{
"Sid": "Stmt1388811069831",
"Effect": "Allow",
"Principal": { "AWS": "*" },
"Action": ["s3:GetObjectAcl", "s3:ListBucket"],
"Resource": ["arn:aws:s3:::cloudacademy]
}]
● It will make the cloudacademy bucket as well as all its objects as public
● It will give an error as no object is defined as part of the policy while the action defines the rule about the object
● It will allow everyone to view the ACL of the bucket

Q63)

user has launched an EC2 instance. The instance got terminated as soon as it was launched.

Which of the below mentioned options is not a possible reason for this?

✓ The user account has reached the maximum EC2 instance limit
Explanation:-When the user account has reached the maximum number of EC2 instances, it will not be allowed to launch an instance. AWS will throw an 'InstanceLimitExceeded' error. For all other reasons, such as "AMI is missing part", "Corrupt Snapshot" or "Volume limit has reached" it will launch an EC2 instance and then terminate it.
● The snapshot is corrupt
● The user account has reached the maximum volume limit
● The AMI is missing. It is the required part

Q64)

A user is planning to setup notifications on the RDS DB for a snapshot.

Which of the below mentioned event categories is not supported by RDS for this snapshot source type?

● Creation
● Deletion
● Restoration
✓ Backup
Explanation:-Amazon RDS uses the Amazon Simple Notification Service to provide a notification when an Amazon RDS event occurs. Event categories for a snapshot source type include: Creation, Deletion, and Restoration. The Backup is a part of DB instance source type.

Q65) An organization has applied the below mentioned policy on an IAM group which has a few IAM users. What entitlements do the IAM users of that group avail with this policy?
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",

```
“NotAction”: “iam:*”,
“Resource”: “*”
}
]
}
```

● It allows full access to all AWS services except IAM services for the IAM users who are part of this group
● The policy cannot be applied to a group since it is for IAM access
● It allows full access to all IAM services for the IAM users who are part of this group
✓ The policy is not created correctly. It will throw an error for wrong action

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The IAM group allows the organization to specify permissions for a collection of users. With the below mentioned policy, it will allow the group full access (Admin) to all AWS services except IAM management. The user part of this group will not be able to create or manage the IAM users, groups or roles.

```
{
“Version”: “2012-10-17”,
“Statement”: [
{
“Effect”: “Allow”,
“NotAction”: “iam:*”,
“Resource”: “*”
}
]
}
```