

## AWS-SysOps Dumps

### Amazon AWS Certified SysOps Administrator - Associate

<https://www.certleader.com/AWS-SysOps-dumps.html>



**NEW QUESTION 1**

- (Topic 1)

Your team is excited about the use of AWS because now they have access to programmable Infrastructure. You have been asked to manage your AWS infrastructure in a manner similar to the way you might manage application code. You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development, test, QA, production).

Which approach addresses this requirement?

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

**Answer: B**

**Explanation:**

Reference:

<http://aws.amazon.com/opsworks/faqs/>

**NEW QUESTION 2**

- (Topic 1)

Your EC2-Based Multi-tier application includes a monitoring instance that periodically makes application-level read-only requests of various application components and if any of those fail more than three times in 30 seconds calls CloudWatch to fire an alarm, and the alarm notifies your operations team by email and SMS of a possible application health problem. However, you also need to watch the watcher -the monitoring instance itself - and be notified if it becomes unhealthy.

Which of the following is a simple way to achieve that goal?

- A. Run another monitoring instance that pings the monitoring instance and fires a CloudWatch alarm that notifies your operations team should the primary monitoring instance become unhealthy
- B. Set a CloudWatch alarm based on EC2 system and instance status checks and have the alarm notify your operations team of any detected problem with the monitoring instance
- C. Set a CloudWatch alarm based on the CPU utilization of the monitoring instance and have the alarm notify your operations team if the CPU usage exceeds 50% for more than one minute; then have your monitoring application go into a CPU-bound loop should it detect any application problem
- D. Have the monitoring instances post messages to an SQS queue and then dequeue those messages on another instance. Should the queue cease to have new messages, the second instance should first terminate the original monitoring instance, start another backup monitoring instance, and assume the role of the previous monitoring instance, beginning adding messages to the SQS queue

**Answer: D**

**NEW QUESTION 3**

- (Topic 1)

You are tasked with setting up a cluster of EC2 instances for a NoSQL database. The database requires random read IO disk performance up to a 100,000 IOPS at 4KB block size per node.

Which of the following EC2 instances will perform the best for this workload?

- A. A High-Memory Quadruple Extra Large (m2.4xlarge) with EBS-Optimized set to true and a Provisioned IOPS EBS volume
- B. A Cluster Compute Eight Extra Large (cc2.8xlarge) using instance storage
- C. High I/O Quadruple Extra Large (hi1.4xlarge) using instance storage
- D. A Cluster GPU Quadruple Extra Large (cg1.4xlarge) using four separate 4000 PIOPS EBS volumes in a RAID 0 configuration

**Answer: C**

**Explanation:**

Explanation: Reference:

<http://aws.amazon.com/ec2/instance-types/>

**NEW QUESTION 4**

- (Topic 1)

You have a web-style application with a stateless but CPU and memory-intensive web tier running on a cc2.8xlarge EC2 instance inside of a VPC. The instance when under load is having problems returning requests within the SLA as defined by your business. The application maintains its state in a DynamoDB table, but the data tier is properly provisioned and responses are consistently fast.

How can you best resolve the issue of the application responses not meeting your SLA?

- A. Add another cc2.8xlarge application instance, and put both behind an Elastic Load Balancer
- B. Move the cc2.8xlarge to the same Availability Zone as the DynamoDB table
- C. Cache the database responses in ElastiCache for more rapid access
- D. Move the database from DynamoDB to RDS MySQL in scale-out read-replica configuration

**Answer: B**

**Explanation:**

Reference:

<http://aws.amazon.com/elasticmapreduce/faqs/>

**NEW QUESTION 5**

- (Topic 1)

You have a server with a 500GB Amazon EBS data volume. The volume is 80% full. You need to back up the volume at regular intervals and be able to re-create

the volume in a new Availability Zone in the shortest time possible. All applications using the volume can be paused for a period of a few minutes with no discernible user impact.

Which of the following backup methods will best fulfill your requirements?

- A. Take periodic snapshots of the EBS volume
- B. Use a third party Incremental backup application to back up to Amazon Glacier
- C. Periodically back up all data to a single compressed archive and archive to Amazon S3 using a parallelized multi-part upload
- D. Create another EBS volume in the second Availability Zone attach it to the Amazon EC2 instance, and use a disk manager to mirror the two disks

**Answer: D**

**Explanation:**

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>

**NEW QUESTION 6**

- (Topic 1)

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

Which two mechanisms will allow the application to failover to new instances without the need for reconfiguration? Choose 2 answers

- A. Create an ELB to reroute traffic to a failover instance
- B. Create a secondary ENI that can be moved to a failover instance
- C. Use Route53 health checks to fail traffic over to a failover instance
- D. Assign a secondary private IP address to the primary ENI that can be moved to a failover instance

**Answer: AD**

**NEW QUESTION 7**

- (Topic 1)

You have decided to change the Instance type for instances running in your application tier that are using Auto Scaling.

In which area below would you change the instance type definition?

- A. Auto Scaling launch configuration
- B. Auto Scaling group
- C. Auto Scaling policy
- D. Auto Scaling tags

**Answer: A**

**Explanation:**

Reference:

<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/WhatIsAutoScaling.html>

**NEW QUESTION 8**

- (Topic 1)

You are designing a system that has a Bastion host. This component needs to be highly available without human intervention.

Which of the following approaches would you select?

- A. Run the bastion on two instances one in each AZ
- B. Run the bastion on an active Instance in one AZ and have an AMI ready to boot up in the event of failure
- C. Configure the bastion instance in an Auto Scaling group Specify the Auto Scaling group to include multiple AZs but have a min-size of 1 and max-size of 1
- D. Configure an ELB in front of the bastion instance

**Answer: C**

**NEW QUESTION 9**

- (Topic 1)

You have set up individual AWS accounts for each project. You have been asked to make sure your AWS Infrastructure costs do not exceed the budget set per project for each month.

Which of the following approaches can help ensure that you do not exceed the budget each month?

- A. Consolidate your accounts so you have a single bill for all accounts and projects
- B. Set up auto scaling with CloudWatch alarms using SNS to notify you when you are running too many Instances in a given account
- C. Set up CloudWatch billing alerts for all AWS resources used by each project, with a notification occurring when the amount for each resource tagged to a particular project matches the budget allocated to the project
- D. Set up CloudWatch billing alerts for all AWS resources used by each account, with email notifications when it hits 50%, 80% and 90% of its budgeted monthly spend

**Answer: C**

**NEW QUESTION 10**

- (Topic 1)

Your entire AWS infrastructure lives inside of one Amazon VPC. You have an Infrastructure monitoring application running on an Amazon instance in Availability Zone (AZ) A of the region, and another application instance running in AZ B. The monitoring application needs to make use of ICMP ping to confirm network reachability of the instance hosting the application.

Can you configure the security groups for these instances to only allow the ICMP ping to pass from the monitoring instance to the application instance and nothing else? If so how?

- A. No Two instances in two different AZ's can't talk directly to each other via ICMP ping as that protocol is not allowed across subnet (iebroadcast) boundaries
- B. Yes Both the monitoring instance and the application instance have to be a part of the same security group, and that security group needs to allow inbound ICMP
- C. Yes, The security group for the monitoring instance needs to allow outbound ICMP and the application instance's security group needs to allow Inbound ICMP
- D. Yes, Both the monitoring instance's security group and the application instance's security group need to allow both inbound and outbound ICMP ping packets since ICMP is not a connection-oriented protocol

**Answer: D**

#### NEW QUESTION 10

- (Topic 1)

You are running a web-application on AWS consisting of the following components an Elastic Load Balancer (ELB) an Auto-Scaling Group of EC2 instances running Linux/PHP/Apache, and Relational DataBase Service (RDS) MySQL.  
Which security measures fall into AWS's responsibility?

- A. Protect the EC2 instances against unsolicited access by enforcing the principle of least-privilege access
- B. Protect against IP spoofing or packet sniffing
- C. Assure all communication between EC2 instances and ELB is encrypted
- D. Install latest security patches on EL
- E. RDS and EC2 instances

**Answer: B**

#### NEW QUESTION 11

- (Topic 1)

You have a web application leveraging an Elastic Load Balancer (ELB) In front of the web servers deployed using an Auto Scaling Group Your database is running on Relational Database Service (RDS) The application serves out technical articles and responses to them in general there are more views of an article than there are responses to the article. On occasion, an article on the site becomes extremely popular resulting in significant traffic Increases that causes the site to go down. What could you do to help alleviate the pressure on the infrastructure while maintaining availability during these events?  
Choose 3 answers

- A. Leverage CloudFront for the delivery of the article
- B. Add RDS read-replicas for the read traffic going to your relational database
- C. Leverage ElastiCache for caching the most frequently used dat
- D. Use SOS to queue up the requests for the technical posts and deliver them out of the queu
- E. Use Route53 health checks to fail over to an S3 bucket for an error pag

**Answer: ACE**

#### NEW QUESTION 13

- (Topic 1)

An application that you are managing has EC2 instances & Dynamo DB tables deployed to several AWS Regions In order to monitor the performance of the application globally, you would like to see two graphs 1) Avg CPU Utilization across all EC2 instances and 2) Number of Throttled Requests for all DynamoDB tables.  
How can you accomplish this?

- A. Tag your resources with the application name, and select the tag name as the dimension in the Cloudwatch Management console to view the respective graphs
- B. Use the Cloud Watch CLI tools to pull the respective metrics from each regional endpoint Aggregate the data offline & store it for graphing in CloudWate
- C. Add SNMP traps to each instance and DynamoDB table Leverage a central monitoring server to capture data from each instance and table Put the aggregate data into Cloud Watch for graphin
- D. Add a CloudWatch agent to each instance and attach one to each DynamoDB tabl
- E. When configuring the agent set the appropriate application name & view the graphs in CloudWate

**Answer: C**

#### NEW QUESTION 16

- (Topic 1)

When an EC2 EBS-backed (EBS root) instance is stopped, what happens to the data on any ephemeral store volumes?

- A. Data will be deleted and win no longer be accessible
- B. Data is automatically saved in an EBS volum
- C. Data is automatically saved as an EBS snapshot
- D. Data is unavailable until the instance is restarted

**Answer: D**

#### NEW QUESTION 18

- (Topic 1)

The majority of your Infrastructure is on premises and you have a small footprint on AWS Your company has decided to roll out a new application that is heavily dependent on low latency connectivity to LOAP for authentication Your security policy requires minimal changes to the company's existing application user management processes.  
What option would you implement to successfully launch this application1?

- A. Create a second, independent LOAP server in AWS for your application to use for authentication
- B. Establish a VPN connection so your applications can authenticate against your existing on-premises LDAP servers
- C. Establish a VPN connection between your data center and AWS create a LDAP replica on AWS and configure your application to use the LDAP replica for authentication

D. Create a second LDAP domain on AWS establish a VPN connection to establish a trust relationship between your new and existing domains and use the new domain for authentication

**Answer:** D

**Explanation:**

Reference:  
<http://msdn.microsoft.com/en-us/library/azure/jj156090.aspx>

**NEW QUESTION 22**

- (Topic 1)

Which of the following are characteristics of Amazon VPC subnets?

Choose 2 answers

- A. Each subnet maps to a single Availability Zone
- B. A CIDR block mask of /25 is the smallest range supported
- C. Instances in a private subnet can communicate with the internet only if they have an Elastic IP
- D. By default, all subnets can route between each other, whether they are private or public
- E. V Each subnet spans at least 2 Availability zones to provide a high-availability environment

**Answer:** CE

**NEW QUESTION 27**

- (Topic 1)

You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database. You want to confirm that they can talk to each other for your application to work properly.

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

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

**Answer:** AD

**NEW QUESTION 30**

- (Topic 1)

You have an Auto Scaling group associated with an Elastic Load Balancer (ELB). You have noticed that instances launched via the Auto Scaling group are being marked unhealthy due to an ELB health check, but these unhealthy instances are not being terminated

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

- A. Change the thresholds set on the Auto Scaling group health check
- B. Add an Elastic Load Balancing health check to your Auto Scaling group
- C. Increase the value for the Health check interval set on the Elastic Load Balancer
- D. Change the health check set on the Elastic Load Balancer to use TCP rather than HTTP checks

**Answer:** B

**Explanation:**

Reference:  
<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-add-elb-healthcheck.html>

Add an Elastic Load Balancing Health Check to your Auto Scaling Group

By default, an Auto Scaling group periodically reviews the results of EC2 instance status to determine the health state of each instance. However, if you have associated your Auto Scaling group with an Elastic Load Balancing load balancer, you can choose to use the Elastic Load Balancing health check. In this case, Auto Scaling determines the health status of your instances by checking the results of both the EC2 instance status check and the Elastic Load Balancing instance health check.

For information about EC2 instance status checks, see *Monitor Instances With Status Checks* in the *Amazon EC2 User Guide for Linux Instances*. For information about Elastic Load Balancing health checks, see *Health Check* in the *Elastic Load Balancing Developer Guide*.

This topic shows you how to add an Elastic Load Balancing health check to your Auto Scaling group, assuming that you have created a load balancer and have registered the load balancer with your Auto Scaling group. If you have not registered the load balancer with your Auto Scaling group, see *Set Up a Scaled and Load-Balanced Application*.

Auto Scaling marks an instance unhealthy if the calls to the Amazon EC2 action `DescribeInstanceStatus` return any state other than `running`, the system status shows `impaired`, or the calls to Elastic Load Balancing action `DescribeInstanceHealth` returns `OutOfService` in the instance state field.

If there are multiple load balancers associated with your Auto Scaling group, Auto Scaling checks the health state of your EC2 instances by making health check calls to each load balancer. For each call, if the Elastic Load Balancing action returns any state other than `InService`, the instance is marked as unhealthy. After Auto Scaling marks an instance as unhealthy, it remains in that state, even if subsequent calls from other load balancers return an `InService` state for the same instance.

**NEW QUESTION 35**

- (Topic 1)

Your company is moving towards tracking web page users with a small tracking

image loaded on each page. Currently you are serving this image out of US-East, but are starting to get concerned about the time it takes to load the image for users on the west coast.

What are the two best ways to speed up serving this image?

Choose 2 answers

- A. Use Route 53's Latency Based Routing and serve the image out of US-West-2 as well as US-East-1
- B. Serve the image out through CloudFront

- C. Serve the image out of S3 so that it isn't being served off of your web application tier
- D. Use EBS PIOPs to serve the image faster out of your EC2 instances

**Answer:** AD

#### NEW QUESTION 37

- (Topic 1)

An organization's security policy requires multiple copies of all critical data to be replicated across at least a primary and backup data center. The organization has decided to store some critical data on Amazon S3.

Which option should you implement to ensure this requirement is met?

- A. Use the S3 copy API to replicate data between two S3 buckets in different regions
- B. You do not need to implement anything since S3 data is automatically replicated between regions
- C. Use the S3 copy API to replicate data between two S3 buckets in different facilities within an AWS Region
- D. You do not need to implement anything since S3 data is automatically replicated between multiple facilities within an AWS Region

**Answer:** D

#### NEW QUESTION 38

- (Topic 1)

You have been asked to propose a multi-region deployment of a web-facing application where a controlled portion of your traffic is being processed by an alternate region.

Which configuration would achieve that goal?

- A. Route53 record sets with weighted routing policy
- B. Route53 record sets with latency based routing policy
- C. Auto Scaling with scheduled scaling actions set
- D. Elastic Load Balancing with health checks enabled

**Answer:** D

#### Explanation:

Reference:

<http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html>

#### NEW QUESTION 40

- (Topic 1)

When attached to an Amazon VPC which two components provide connectivity with external networks? Choose 2 answers

- A. Elastic IPS (EIP)
- B. NAT Gateway (NAT)
- C. Internet Gateway (IGW)
- D. Virtual Private Gateway (VGW)

**Answer:** CD

#### NEW QUESTION 45

- (Topic 1)

You have been asked to automate many routine systems administrator backup and recovery activities. Your current plan is to leverage AWS-managed solutions as much as possible and automate the rest with the AWS CLI and scripts.

Which task would be best accomplished with a script?

- A. Creating daily EBS snapshots with a monthly rotation of snapshots
- B. Creating daily RDS snapshots with a monthly rotation of snapshots
- C. Automatically detect and stop unused or underutilized EC2 instances
- D. Automatically add Auto Scaled EC2 instances to an Amazon Elastic Load Balancer

**Answer:** A

#### NEW QUESTION 50

- (Topic 1)

When creation of an EBS snapshot is initiated but not completed the EBS volume?

- A. Cannot be detached or attached to an EC2 instance until the snapshot completes
- B. Can be used in read-only mode while the snapshot is in progress
- C. Can be used while the snapshot is in progress
- D. Cannot be used until the snapshot completes

**Answer:** C

#### Explanation:

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html>

#### NEW QUESTION 55

- (Topic 1)

You have a Linux EC2 web server instance running inside a VPC. The instance is in a public subnet and has an EIP associated with it so you can connect to it over the Internet via HTTP or SSH. The instance was also fully accessible when you last logged in via SSH, and was also serving web requests on port 80. Now you are not able to SSH into the host nor does it respond to web requests on port 80 that were working fine last time you checked. You have double-checked that all networking configuration parameters (security groups, route tables, IGW/EIP, NACLs, etc) are properly configured (and you haven't made any changes to those anyway since you were last able to reach the instance). You look at the EC2 console and notice that system status check shows "impaired." Which should be your next step in troubleshooting and attempting to get the instance back to a healthy state so that you can log in again?

- A. Stop and start the instance so that it will be able to be redeployed on a healthy host system that most likely will fix the "impaired" system status
- B. Reboot your instance so that the operating system will have a chance to boot in a clean healthy state that most likely will fix the "impaired" system status
- C. Add another dynamic private IP address to the instance and try to connect via that new path, since the networking stack of the OS may be locked up causing the "impaired" system status
- D. Add another Elastic Network Interface to the instance and try to connect via that new path since the networking stack of the OS may be locked up causing the "impaired" system status
- E. un-map and then re-map the EIP to the instance, since the IGW/VNAT gateway may not be working properly, causing the "impaired" system status

**Answer:** A

#### NEW QUESTION 56

- (Topic 2)

A user wants to disable connection draining on an existing ELB. Which of the below mentioned statements helps the user disable connection draining on the ELB?

- A. The user can only disable connection draining from CLI
- B. It is not possible to disable the connection draining feature once enabled
- C. The user can disable the connection draining feature from EC2 -> ELB console or from CLI
- D. The user needs to stop all instances before disabling connection draining

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 57

- (Topic 2)

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?

- A. It is not possible to setup detailed monitoring for Auto Scaling
- B. In this case, Auto Scaling will send data every minute and will charge the user extra
- C. Detailed monitoring will send data every minute without additional charges
- D. Auto Scaling sends data every minute only and does not charge the user

**Answer:** B

#### 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.

#### NEW QUESTION 60

- (Topic 2)

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?

- A. AWS RRS
- B. AWS S3
- C. AWS RDS
- D. AWS Glacier

**Answer:** D

#### 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.

#### NEW QUESTION 63

- (Topic 2)

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?

- A. Master (Payee) account will get only the total bill and cannot see the cost incurred by each account
- B. account will get only the total bill and cannot see the cost incurred by each account

- C. Master (Payee
- D. account can view only the AWS billing details of the linked accounts
- E. It is not recommended to use consolidated billing since the payee account will have access to the linked accounts
- F. Each AWS account needs to create an AWS billing policy to provide permission to the payee account

**Answer:** B

**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.

#### NEW QUESTION 67

- (Topic 2)

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?

- A. ELB Access logs
- B. ELB health check
- C. CloudWatch metrics
- D. ELB API calls with CloudTrail

**Answer:** B

**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.

#### NEW QUESTION 69

- (Topic 2)

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?

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

**Answer:** C

**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 (-).

#### NEW QUESTION 74

- (Topic 2)

A sys admin has created the below mentioned policy and applied to an S3 object named aws.jpg. The aws.jpg is inside a bucket named cloudacademy. What does this policy define?

```
"Statement": [{
  "Sid": "Stmnt1388811069831",
  "Effect": "Allow",
  "Principal": { "AWS": "*" },
  "Action": [ "s3:GetObjectAcl", "s3:ListBucket", "s3:GetObject" ],
  "Resource": [ "arn:aws:s3:::cloudacademy/*.jpg" ]
}]
```

- A. It is not possible to define a policy at the object level
- B. It will make all the objects of the bucket cloudacademy as public
- C. It will make the bucket cloudacademy as public
- D. the aws.jpg object as public

**Answer:** A

**Explanation:**

A system admin can grant permission to the S3 objects or 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 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. It cannot be applied at the object level.

#### NEW QUESTION 77

- (Topic 2)

A user is planning to use AWS Cloud formation for his automatic deployment requirements. Which of the below mentioned components are required as a part of the template?

- A. Parameters
- B. Outputs
- C. Template version
- D. Resources

**Answer: D**

**Explanation:**

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

#### **NEW QUESTION 80**

- (Topic 2)

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?

- A. Create a new alarm of \$400 and link it with the first alarm
- B. It is not possible to modify the alarm once it has crossed the usage limit
- C. Update the alarm to set the limit at \$400 instead of \$200
- D. Create a new alarm for the additional \$200 amount

**Answer: C**

**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.

#### **NEW QUESTION 81**

- (Topic 2)

A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25. The user is trying to create the private subnet with CIDR 20.0.0.128/25. Which of the below mentioned statements is true in this scenario?

- A. It will not allow the user to create the private subnet due to a CIDR overlap
- B. It will allow the user to create a private subnet with CIDR as 20.0.0.128/25
- C. This statement is wrong as AWS does not allow CIDR 20.0.0.0/25
- D. It will not allow the user to create a private subnet due to a wrong CIDR range

**Answer: B**

**Explanation:**

When the user creates a subnet in VPC, he specifies the CIDR block for the subnet. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC., or a subset (to enable multiple subnets.. If the user creates more than one subnet in a VPC, the CIDR blocks of the subnets must not overlap. Thus, in this case the user has created a VPC with the CIDR block 20.0.0.0/24, which supports 256 IP addresses (20.0.0.0 to 20.0.0.255.. The user can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses the CIDR block 20.0.0.0/25 (for addresses 20.0.0.0 - 20.0.0.127. and the other uses the CIDR block 20.0.0.128/25 (for addresses 20.0.0.128 - 20.0.0.255..

#### **NEW QUESTION 82**

- (Topic 2)

A user is checking the CloudWatch metrics from the AWS console. The user notices that the CloudWatch data is coming in UTC. The user wants to convert the data to a local time zone. How can the user perform this?

- A. In the CloudWatch dashboard the user should set the local timezone so that CloudWatch shows the data only in the local time zone
- B. In the CloudWatch console select the local timezone under the Time Range tab to view the data as per the local timezone
- C. The CloudWatch data is always in UTC; the user has to manually convert the data
- D. The user should have send the local timezone while uploading the data so that CloudWatch will show the data only in the local timezone

**Answer: B**

**Explanation:**

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

#### **NEW QUESTION 83**

- (Topic 2)

A user has created a queue named "myqueue" with SQS. There are four messages published to queue which are not received by the consumer yet. If the user tries to delete the queue, what will happen?

- A. A user can never delete a queue manual

- B. AWS deletes it after 30 days of inactivity on queue
- C. It will delete the queue
- D. It will initiate the delete but wait for four days before deleting until all messages are deleted automaticall
- E. It will ask user to delete the messages first

**Answer:** B

**Explanation:**

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

**NEW QUESTION 87**

- (Topic 2)

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?

- A. Create a stack
- B. Configure a service
- C. Create and upload the template
- D. Provide the parameters configured as part of the template

**Answer:** B

**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.

**NEW QUESTION 91**

- (Topic 2)

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?

- A. In a Multi AZ, AWS runs two DBs in parallel and copies the data asynchronously to the replica copy
- B. In a Multi AZ, AWS runs two DBs in parallel and copies the data synchronously to the replica copy
- C. In a Multi AZ, AWS runs just one DB but copies the data synchronously to the standby replica
- D. AWS MS SQL does not support the Multi AZ feature

**Answer:** C

**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.

**NEW QUESTION 96**

- (Topic 2)

A user has created a web application with Auto Scaling. The user is regularly monitoring the application and he observed that the traffic is highest on Thursday and Friday between 8 AM to 6 PM. What is the best solution to handle scaling in this case?

- A. Add a new instance manually by 8 AM Thursday and terminate the same by 6 PM Friday
- B. Schedule Auto Scaling to scale up by 8 AM Thursday and scale down after 6 PM on Friday
- C. Schedule a policy which may scale up every day at 8 AM and scales down by 6 PM
- D. Configure a batch process to add a instance by 8 AM and remove it by Friday 6 PM

**Answer:** B

**Explanation:**

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

**NEW QUESTION 101**

- (Topic 2)

A user has launched an EC2 instance. The user is planning to setup the CloudWatch alarm. Which of the below mentioned actions is not supported by the CloudWatch alarm?

- A. Notify the Auto Scaling launch config to scale up
- B. Send an SMS using SNS
- C. Notify the Auto Scaling group to scale down

D. Stop the EC2 instance

**Answer:** B

**Explanation:**

A user can create a CloudWatch alarm that takes various actions when the alarm changes state. An alarm watches a single metric over the time period that the user has specified, 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 actions could be sending a notification to an Amazon Simple Notification Service topic (SMS, Email, and HTTP end point), notifying the Auto Scaling policy or changing the state of the instance to Stop/Terminate.

#### **NEW QUESTION 104**

- (Topic 2)

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?

- A. The root account owner should create a bucket policy which allows the IAM users to upload the object
- B. The root account owner should create the bucket policy which allows the other account owners to set the object policy of that bucket
- C. The root account should use ACL with the bucket to allow everyone to upload the object
- D. The root account should create the IAM users and provide them the permission to upload content to the bucket

**Answer:** C

**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.

#### **NEW QUESTION 107**

- (Topic 2)

A user has configured ELB with two EBS backed EC2 instances. The user is trying to understand the DNS access and IP support for ELB. Which of the below mentioned statements may not help the user understand the IP mechanism supported by ELB?

- A. The client can connect over IPV4 or IPV6 using Dualstack
- B. ELB DNS supports both IPV4 and IPV6
- C. Communication between the load balancer and back-end instances is always through IPV4
- D. The ELB supports either IPV4 or IPV6 but not both

**Answer:** D

**Explanation:**

Elastic Load Balancing supports both Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4). Clients can connect to the user's load balancer using either IPv4 or IPv6 (in EC2-Classic DNS). However, communication between the load balancer and its back-end instances uses only IPv4. The user can use the Dualstack-prefixed DNS name to enable IPv6 support for communications between the client and the load balancers. Thus, the clients are able to access the load balancer using either IPv4 or IPv6 as their individual connectivity needs dictate.

#### **NEW QUESTION 111**

- (Topic 2)

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?

- A. Run activities on the CPU such that its utilization reaches above 75%
- B. From the AWS console change the state to 'Alarm'
- C. The user can set the alarm state to 'Alarm' using CLI
- D. Run the SNS action manually

**Answer:** C

**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.

#### **NEW QUESTION 114**

- (Topic 2)

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?

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

**Answer:** A

**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.

**NEW QUESTION 118**

- (Topic 2)

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?

- A. Enable Receiving Billing Reports
- B. Enable Receiving Billing Alerts
- C. Enable AWS billing utility
- D. Enable CloudWatch Billing Threshold

**Answer: B**

**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.

**NEW QUESTION 119**

- (Topic 2)

A sys admin is trying to understand the Auto Scaling activities. Which of the below mentioned processes is not performed by Auto Scaling?

- A. Reboot Instance
- B. Schedule Actions
- C. Replace Unhealthy
- D. Availability Zone Balancing

**Answer: A**

**Explanation:**

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

**NEW QUESTION 124**

- (Topic 2)

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?

- A. The private and public address remains the same
- B. The Elastic IP remains associated with the instance
- C. The volume is preserved
- D. The instance runs on a new host computer

**Answer: D**

**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.

**NEW QUESTION 125**

- (Topic 2)

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

- A. Copy the running instance using the "Instance Copy" command to the EU region
- B. Create an AMI of the instance and copy the AMI to the EU region
- C. Then launch the instance from the EU AMI
- D. Copy the instance from the US East region to the EU region
- E. Use the "Launch more like this" option to copy the instance from one region to another

**Answer: B**

**Explanation:**

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

**NEW QUESTION 130**

- (Topic 2)

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?

- A. DiskReadBytes
- B. NetworkIn
- C. NetworkOut
- D. CPUUtilization

**Answer:** A

**Explanation:**

CloudWatch is used to monitor AWS as well as 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 ephemeral 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 ephemeral storage attached to an instance. For an EBS backed instance without any additional device, this data will be 0.

**NEW QUESTION 133**

- (Topic 2)

A user is trying to aggregate all the CloudWatch metric data of the last 1 week. Which of the below mentioned statistics is not available for the user as a part of data aggregation?

- A. Aggregate
- B. Sum
- C. Sample data
- D. Average

**Answer:** A

**Explanation:**

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

**NEW QUESTION 134**

- (Topic 2)

A user is launching an EC2 instance in the US East region. Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 138**

- (Topic 2)

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?

- A. <https://999988887777.signin.aws.amazon.com/console/>
- B. <https://signin.aws.amazon.com/cloudacademy/>
- C. <https://cloudacademy.signin.aws.amazon.com/999988887777/console/>
- D. <https://999988887777.aws.amazon.com/cloudacademy/>

**Answer:** A

**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/](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.

**NEW QUESTION 141**

- (Topic 2)

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?

- A. ELB sends data to CloudWatch every minute only and does not charge the user
- B. ELB will send data every minute and will charge the user extra
- C. ELB is not supported by CloudWatch
- D. It is not possible to setup detailed monitoring for ELB

**Answer:** A

**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.

**NEW QUESTION 146**

- (Topic 2)

A sys admin has created a shopping cart application and hosted it on EC2. The EC2 instances are running behind ELB. The admin wants to ensure that the end user request will always go to the EC2 instance where the user session has been created. How can the admin configure this?

- A. Enable ELB cross zone load balancing
- B. Enable ELB cookie setup
- C. Enable ELB sticky session
- D. Enable ELB connection draining

**Answer:** C

**Explanation:**

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

**NEW QUESTION 149**

- (Topic 2)

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?

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

**Answer:** D

**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.

**NEW QUESTION 152**

- (Topic 2)

A user has a refrigerator plant. The user is measuring the temperature of the plant every 15 minutes. If the user wants to send the data to CloudWatch to view the data visually, which of the below mentioned statements is true with respect to the information given above?

- A. The user needs to use AWS CLI or API to upload the data
- B. The user can use the AWS Import Export facility to import data to CloudWatch
- C. The user will upload data from the AWS console
- D. The user cannot upload data to CloudWatch since it is not an AWS service metric

**Answer:** A

**Explanation:**

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

**NEW QUESTION 157**

- (Topic 2)

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?

Exhibit:



- A. It will store the estimated charges data of the last 14 days
- B. It will include the estimated charges of every AWS service
- C. The metric data will represent the data of all the regions
- D. The metric data will show data specific to that region

**Answer:** D

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

**NEW QUESTION 161**

- (Topic 2)

A user is trying to understand AWS SNS. To which of the below mentioned end points is SNS unable to send a notification?

- A. Email JSON
- B. HTTP
- C. AWS SQS
- D. AWS SES

**Answer:** D

**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 of the following transports as part of the subscription requests: "HTTP", "HTTPS", "Email", "Email-JSON", "SQS", "and SMS".

**NEW QUESTION 165**

- (Topic 2)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 166**

- (Topic 2)

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?

- A. Stop one of the instances and change the availability zone
- B. The zone can only be modified using the AWS CLI
- C. From the AWS EC2 console, select the Actions - > Change zones and specify new zone
- D. Create an AMI of the running instance and launch the instance in a separate AZ

**Answer: D**

**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.

**NEW QUESTION 171**

- (Topic 2)

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?

- A. For restart it does not charge for an extra hour, while every stop/start it will be charged as a separate hour
- B. 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
- C. For every restart or start/stop it will be charged as a separate hour
- D. For restart it charges extra only once, while for every stop/start it will be charged as a separate hour

**Answer: A**

**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.

**NEW QUESTION 173**

- (Topic 3)

A user has launched an EC2 instance from an instance store backed AMI. The user has attached an additional instance store volume to the instance. The user wants to create an AMI from the running instance. Will the AMI have the additional instance store volume data?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 177**

- (Topic 3)

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling terminate process only for a while. What will happen to the availability zone rebalancing process (AZRebalance) during this period?

- A. Auto Scaling will not launch or terminate any instances
- B. Auto Scaling will allow the instances to grow more than the maximum size
- C. Auto Scaling will keep launching instances till the maximum instance size

D. It is not possible to suspend the terminate process while keeping the launch active

**Answer:** B

**Explanation:**

Auto Scaling performs various processes, such as Launch, Terminate, Availability Zone Rebalance (AZRebalance, etc. 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.

#### NEW QUESTION 182

- (Topic 3)

An organization has created a Queue named "modularqueue" with SQS. The organization is not performing any operations such as SendMessage, ReceiveMessage, DeleteMessage, GetQueueAttributes, SetQueueAttributes, AddPermission, and RemovePermission on the queue. What can happen in this scenario?

- A. AWS SQS sends notification after 15 days for inactivity on queue
- B. AWS SQS can delete queue after 30 days without notification
- C. AWS SQS marks queue inactive after 30 days
- D. AWS SQS notifies the user after 2 weeks and deletes the queue after 3 week

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 184

- (Topic 3)

A sys admin has enabled logging on ELB. Which of the below mentioned fields will not be a part of the log file name?

- A. Load Balancer IP
- B. EC2 instance IP
- C. S3 bucket name
- D. Random string

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 189

- (Topic 3)

A user is trying to connect to a running EC2 instance using SSH. However, the user gets an Unprotected Private Key File error. Which of the below mentioned options can be a possible reason for rejection?

- A. The private key file has the wrong file permission
- B. The ppk file used for SSH is read only
- C. The public key file has the wrong permission
- D. The user has provided the wrong user name for the OS login

**Answer:** A

**Explanation:**

While doing SSH to an EC2 instance, if you get an Unprotected Private Key File error it means that the private key file's permissions on your computer are too open. Ideally the private key should have the Unix permission of 0400. To fix that, run the command: `chmod 0400 /path/to/private.key`

#### NEW QUESTION 191

- (Topic 3)

A user has created a VPC with CIDR 20.0.0.0/24. The user has used all the IPs of CIDR and wants to increase the size of the VPC. The user has two subnets: public (20.0.0.0/28. and private (20.0.1.0/28.. How can the user change the size of the VPC?

- A. The user can delete all the instances of the subne
- B. Change the size of the subnets to 20.0.0.0/32 and 20.0.1.0/32, respective
- C. Then the user can increase the size of the VPC using CLI
- D. It is not possible to change the size of the VPC once it has been created
- E. The user can add a subnet with a higher range so that it will automatically increase the size of the VPC
- F. The user can delete the subnets first and then modify the size of the VPC

**Answer:** B

**Explanation:**

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

**NEW QUESTION 194**

- (Topic 3)

A user has launched an EC2 instance store backed instance in the US-East-1a zone. The user created AMI #1 and copied it to the Europe region. After that, the user made a few updates to the application running in the US-East-1a zone. The user makes an AMI#2 after the changes. If the user launches a new instance in Europe from the AMI #1 copy, which of the below mentioned statements is true?

- A. The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copyin
- B. Thus, the copied AMI will have all the updated data
- C. The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI
- D. It is not possible to copy the instance store backed AMI from one region to another
- E. The new instance in the EU region will not have the changes made after the AMI copy

**Answer:** D

**Explanation:**

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

**NEW QUESTION 198**

- (Topic 3)

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?

- A. It is not possible to stop the instance using the CloudWatch alarm
- B. CloudWatch will stop the instance when the action is executed
- C. The user cannot set an alarm on EC2 since he does not have the permission
- D. The user can setup the action but it will not be executed if the user does not have EC2 rights

**Answer:** D

**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.

**NEW QUESTION 202**

- (Topic 3)

When an EC2 instance that is backed by an S3-based AMI is terminated, what happens to the data on the root volume?

- A. Data is automatically deleted
- B. Data is automatically saved as an EBS snapshot
- C. Data is unavailable until the instance is restarted
- D. Data is automatically saved as an EBS volume

**Answer:** A

**NEW QUESTION 204**

- (Topic 3)

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?

- A. The zone can only be modified using the AWS CLI
- B. It is not possible to change the zone of an instance after it is launched
- C. Stop one of the instances and change the availability zone
- D. From the AWS EC2 console, select the Actions -> Change zones and specify the new zone

**Answer:** B

**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.

**NEW QUESTION 207**

- (Topic 3)

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?

- A. x-amz-server-side-encryption-customer-key-AES-256
- B. x-amz-server-side-encryption-customer-key
- C. x-amz-server-side-encryption-customer-algorithm
- D. x-amz-server-side-encryption-customer-key-MD5

**Answer:** A

**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

**NEW QUESTION 210**

- (Topic 3)

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?

- A. The instance will always have a public DNS attached to the instance by default
- B. The user can directly attach an elastic IP to the instance
- C. The instance will never launch if the public IP is not assigned
- D. The user would need to create an internet gateway and then attach an elastic IP to the instance to connect from internet

**Answer:** D

**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.

**NEW QUESTION 215**

- (Topic 3)

A user has created an Auto Scaling group with default configurations from CLI. The user wants to setup the CloudWatch alarm on the EC2 instances, which are launched by the Auto Scaling group. The user has setup an alarm to monitor the CPU utilization every minute. Which of the below mentioned statements is true?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 216**

- (Topic 3)

You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from pre-defined customer IP addresses.

Which two options meet this security requirement? Choose 2 answers A. Configure web server VPC security groups to allow traffic from your customers' IPs

- A. Configure your web servers to filter traffic based on the ELB's "X-forwarded-for" header
- B. Configure ELB security groups to allow traffic from your customers' IPs and deny all outbound traffic
- C. Configure a VPC NACL to allow web traffic from your customers' IPs and deny all outbound traffic

**Answer:** AB

**NEW QUESTION 217**

- (Topic 3)

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": "*"
}
]
}
```

- A. The policy will allow the user to perform all read only activities on the EC2 services
- B. The policy will allow the user to list all the EC2 resources except EBS
- C. The policy will allow the user to perform all read and write activities on the EC2 services
- D. The policy will allow the user to perform all read only activities on the EC2 services except load Balancing

**Answer:** D

**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.

```
{
"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": "*"
}
]
}
```

**NEW QUESTION 221**

- (Topic 3)

Which method can be used to prevent an IP address block from accessing public objects in an S3 bucket?

- A. Create a bucket policy and apply it to the bucket
- B. Create a NACL and attach it to the VPC of the bucket
- C. Create an ACL and apply it to all objects in the bucket
- D. Modify the IAM policies of any users that would access the bucket

**Answer:** A

**Explanation:**

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

**NEW QUESTION 223**

- (Topic 3)

In AWS, which security aspects are the customer's responsibility? Choose 4 answers

- A. Controlling physical access to compute resources
- B. Patch management on the EC2 instance s operating system
- C. Encryption of EBS (Elastic Block Storage) volumes
- D. Life-cycle management of IAM credentials
- E. Decommissioning storage devices
- F. Security Group and ACL (Access Control List) settings

**Answer:** BCEF

**NEW QUESTION 224**

- (Topic 3)

A user is using the AWS SQS to decouple the services. Which of the below mentioned operations is not supported by SQS?

- A. SendMessageBatch
- B. DeleteMessageBatch
- C. CreateQueue
- D. DeleteMessageQueue

**Answer:** D

**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.

**NEW QUESTION 229**

- (Topic 3)

A user has enabled detailed CloudWatch monitoring with the AWS Simple Notification Service. Which of the below mentioned statements helps the user understand detailed monitoring better?

- A. SNS will send data every minute after configuration
- B. There is no need to enable since SNS provides data every minute
- C. AWS CloudWatch does not support monitoring for SNS
- D. SNS cannot provide data every minute

**Answer:** D

**Explanation:**

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

**NEW QUESTION 234**

- (Topic 3)

An organization has setup Auto Scaling with ELB. Due to some manual error, one of the instances got rebooted. Thus, it failed the Auto Scaling health check. Auto Scaling has marked it for replacement. How can the system admin ensure that the instance does not get terminated?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 238**

- (Topic 3)

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?

- A. For the period when there is no data, the user should not send the data at all
- B. For the period when there is no data the user should send a blank value
- C. For the period when there is no data the user should send the value as 0
- D. The user must upload the data to CloudWatch as having no data for some period will cause an error at CloudWatch monitoring

**Answer:** C

**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.

**NEW QUESTION 240**

- (Topic 3)

You have a proprietary data store on-premises that must be backed up daily by dumping the data store contents to a single compressed 50GB file and sending the file to AWS. Your SLAs state that any dump file backed up within the past 7 days can be retrieved within 2 hours. Your compliance department has stated that all data must be held indefinitely. The time required to restore the data store from a backup is approximately 1 hour. Your on-premise network connection is capable of sustaining 1gbps to AWS.

Which backup methods to AWS would be most cost-effective while still meeting all of your requirements?

- A. Send the daily backup files to Glacier immediately after being generated
- B. Transfer the daily backup files to an EBS volume in AWS and take daily snapshots of the volume
- C. Transfer the daily backup files to S3 and use appropriate bucket lifecycle policies to send to Glacier
- D. Host the backup files on a Storage Gateway with Gateway-Cached Volumes and take daily snapshots

**Answer:** D

**Explanation:**

Reference:

<http://aws.amazon.com/storagegateway/faqs/>

**NEW QUESTION 244**

- (Topic 3)

Which services allow the customer to retain run administrative privileges or the underlying EC2 instances? Choose 2 answers

- A. AWS Elastic Beanstalk
- B. Amazon Elastic Map Reduce
- C. Elastic Load Balancing
- D. Amazon Relational Database Service
- E. Amazon Elasti Cache

**Answer:** AB

**NEW QUESTION 246**

- (Topic 3)

How can an EBS volume that is currently attached to an EC2 instance be migrated from one Availability Zone to another?

- A. Simply create a new volume in the other AZ and specify the original volume as the source
- B. Detach the volume, then use the `ec2-migrate-volume` command to move it to another AZ
- C. Create a snapshot of the volume, and create a new volume from the snapshot in the other AZ
- D. Detach the volume and attach it to another EC2 instance in the other AZ

**Answer:** D

**Explanation:**

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html>

**NEW QUESTION 249**

- (Topic 3)

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?

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

**Answer:** D

**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.

**NEW QUESTION 254**

- (Topic 3)

A user runs the command `dd if=/dev/zero of=/dev/xvdfbs=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?

- A. Creating a file system on the EBS volume
- B. Mounting the device to the instance
- C. Pre warming the EBS volume
- D. Formatting the EBS volume

**Answer:** C

**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/xvdfbs=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.

**NEW QUESTION 256**

- (Topic 3)

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?

- A. No, copy AMI does not copy the permission
- B. It is not possible to share the AMI with a specific account
- C. Yes, since copy AMI copies all private account sharing permissions
- D. Yes, since copy AMI copies all the permissions attached with the AMI

**Answer:** A

**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.

**NEW QUESTION 260**

- (Topic 3)

An organization has applied the below mentioned policy on an IAM group which has selected the IAM users. What entitlements do the IAM users avail with this policy?

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

- A. The policy is not created correctl
- B. It will throw an error for wrong resource name
- C. The policy is for the grou
- D. Thus, the IAM user cannot have any entitlement to this
- E. It allows full access to all AWS services for the IAM users who are a part of this group
- F. If this policy is applied to the EC2 resource, the users of the group will have full access to the EC2 Resources

**Answer:** C

**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.

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

**NEW QUESTION 262**

- (Topic 3)

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?

- A. The user can zoom a particular period by selecting that period with the mouse and then releasing the mouse
- B. The user can zoom a particular period by double clicking on that period with the mouse
- C. The user can zoom a particular period by specifying the aggregation data for that period
- D. The user can zoom a particular period by specifying the period in the Time Range

**Answer:** A

**NEW QUESTION 266**

- (Topic 3)

A user is trying to setup a security policy for ELB. The user wants ELB to meet the cipher supported by the client by configuring the server order preference in ELB security policy. Which of the below mentioned preconfigured policies supports this feature?

- A. ELBSecurity Policy-2014-01
- B. ELBSecurity Policy-2011-08
- C. ELBDefault Negotiation Policy
- D. ELBSample- OpenSSLDefault Cipher Policy

**Answer:** A

**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 load balancer is configured to support the Server Order Preference, then the load balancer gets to select the first cipher in its list that matches any one of the ciphers in the client's list. When the user verifies the preconfigured policies supported by ELB, the policy "ELBSecurity Policy-2014-01" supports server order preference.

#### NEW QUESTION 271

- (Topic 3)

The compliance department within your multi-national organization requires that all data for your customers that reside in the European Union (EU) must not leave the EU and also

data for customers that reside in the US must not leave the US without explicit authorization.

What must you do to comply with this requirement for a web based profile management application running on EC2?

- A. Run EC2 instances in multiple AWS Availability Zones in single Region and leverage an Elastic Load Balancer with session stickiness to route traffic to the appropriate zone to create their profile
- B. Run EC2 instances in multiple Regions and leverage Route 53's Latency Based Routing capabilities to route traffic to the appropriate region to create their profile
- C. Run EC2 instances in multiple Regions and leverage a third party data provider to determine if a user needs to be redirect to the appropriate region to create their profile
- D. Run EC2 instances in multiple AWS Availability Zones in a single Region and leverage a third party data provider to determine if a user needs to be redirect to the appropriate zone to create their profile

**Answer:** C

#### NEW QUESTION 273

- (Topic 3)

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?

- A. AWS does not have sufficient capacity in that availability zone
- B. AWS zone mapping is changed for that user account
- C. There is some issue with the host capacity on which the instance is launched
- D. The user account has reached the maximum EC2 instance limit

**Answer:** A

**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.

#### NEW QUESTION 274

- (Topic 3)

A user is planning to use AWS services for his web application. If the user is trying to set up his own billing management system for AWS, how can he configure it?

- A. Set up programmatic billing access
- B. Download and parse the bill as per the requirement
- C. It is not possible for the user to create his own billing management service with AWS
- D. Enable the AWS CloudWatch alarm which will provide APIs to download the alarm data
- E. Use AWS billing APIs to download the usage report of each service from the AWS billing console

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 279

- (Topic 3)

A user is creating a CloudFormation stack. Which of the below mentioned limitations does not hold true for CloudFormation?

- A. One account by default is limited to 100 templates

- B. The user can use 60 parameters and 60 outputs in a single template
- C. The template, parameter, output, and resource description fields are limited to 4096 characters
- D. One account by default is limited to 20 stacks

**Answer:** A

**Explanation:**

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

**NEW QUESTION 283**

- (Topic 3)

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?

- A. One IAM user can be a part of a maximum of 5 groups
- B. The organization can create 100 groups per AWS account
- C. One AWS account can have a maximum of 5000 IAM users
- D. One AWS account can have 250 roles

**Answer:** A

**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).

**NEW QUESTION 285**

- (Topic 3)

An organization (account ID 123412341234. has configured the IAM policy to allow the user to modify his credentials. What will the below mentioned statement allow the user to perform?

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:AddUserToGroup",
      "iam:RemoveUserFromGroup",
      "iam:GetGroup"
    ],
    "Resource": "arn:aws:iam:: 123412341234:group/TestingGroup"
  }]
}
```

- A. The IAM policy will throw an error due to an invalid resource name
- B. The IAM policy will allow the user to subscribe to any IAM group
- C. Allow the IAM user to update the membership of the group called TestingGroup
- D. Allow the IAM user to delete the TestingGroup

**Answer:** C

**Explanation:**

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (account ID 123412341234. wants their users to manage their subscription to the groups, they should create a relevant policy for that. The below mentioned policy allows the respective IAM user to update the membership of the group called MarketingGroup.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:AddUserToGroup",
      "iam:RemoveUserFromGroup",
      "iam:GetGroup"
    ],
    "Resource": "arn:aws:iam:: 123412341234:group/ TestingGroup "
  }]
}
```

**NEW QUESTION 288**

- (Topic 3)

A user has launched an EC2 instance and deployed a production application in it. The user wants to prohibit any mistakes from the production team to avoid accidental termination.

How can the user achieve this?

- A. The user can the set DisableApiTermination attribute to avoid accidental termination
- B. It is not possible to avoid accidental termination

- C. The user can set the DeletionTermination flag to avoid accidental termination
- D. The user can set the InstanceInitiatedShutdownBehavior flag to avoid accidental termination

**Answer:** A

**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 DisableApiTermination attribute controls whether the instance can be terminated using the console, CLI or API. By default, termination protection is disabled for an EC2 instance. When it is set it will not allow the user to terminate the instance from CLI, API or the console.

**NEW QUESTION 292**

- (Topic 3)

When you put objects in Amazon S3, what is the indication that an object was successfully stored?

- A. Each S3 account has a special bucket named\_s3\_log
- B. Success codes are written to this bucket with a timestamp and checksum
- C. A success code is inserted into the S3 object metadata
- D. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful
- E. Amazon S3 is engineered for 99.999999999% durability
- F. Therefore there is no need to confirm that data was inserted

**Answer:** B

**Explanation:**

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPUT.html>

**NEW QUESTION 295**

- (Topic 3)

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

- A. The user should not use his own security key as it is not secure
- B. Configure S3 to rotate the user's encryption key at regular intervals
- C. Configure S3 to store the user's keys securely with SSL
- D. Keep rotating the encryption key manually at the client side

**Answer:** D

**Explanation:**

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

**NEW QUESTION 300**

- (Topic 3)

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database.

Which configuration will allow you to securely serve private content to your users?

- A. Generate pre-signed URLs for each user as they request access to protected S3 content
- B. Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user
- C. Create an S3 bucket policy that limits access to your private content to only your subscribed users' credentials
- D. Create a CloudFront Origin Identity user for your subscribed users and assign the GetObject permission to this user

**Answer:** C

**Explanation:**

Reference:

<https://java.awsblog.com/post/Tx1VE22EWFR4H86/Accessing-Private-Content-in-Amazon-CloudFront>

**NEW QUESTION 303**

- (Topic 3)

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?

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

**Answer:** B

**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.

**NEW QUESTION 307**

- (Topic 3)

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?

- A. Value
- B. Namespace
- C. Metric Name
- D. Timezone

**Answer: B**

**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.

**NEW QUESTION 308**

- (Topic 3)

A user has setup a custom application which generates a number in decimals. The user wants to track that number and setup the alarm whenever the number is above a certain limit. The application is sending the data to CloudWatch at regular intervals for this purpose. Which of the below mentioned statements is not true with respect to the above scenario?

- A. The user can get the aggregate data of the numbers generated over a minute and send it to CloudWatch
- B. The user has to supply the timezone with each data point
- C. CloudWatch will not truncate the number until it has an exponent larger than 126 (i.
- D.  $(1 \times 10^{126})$ .
- E. The user can create a file in the JSON format with the metric name and value and supply it to CloudWatch

**Answer: B**

**NEW QUESTION 309**

- (Topic 3)

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

- A. Launch the test and production instances in separate regions and allow region wise access to the group
- B. Define the IAM policy which allows access based on the instance ID
- C. Create an IAM policy with a condition which allows access to only small instances
- D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

**Answer: D**

**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 various parameters. If the organization wants the user to access only specific instances he should define proper tags and add to the IAM policy condition.

The sample policy is shown below.

```
"Statement": [  
{  
  "Action": "ec2:*",  
  "Effect": "Allow",  
  "Resource": "*",  
  "Condition": {  
    "StringEquals": {  
      "ec2:ResourceTag/InstanceType": "Production"  
    }  
  }  
}]
```

**NEW QUESTION 311**

- (Topic 3)

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?

- A. AWS account ID
- B. X.509 certificate and private key
- C. AWS login ID to login to the console
- D. Access key and secret access key

**Answer:** C

**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.

**NEW QUESTION 312**

- (Topic 3)

A user had aggregated the CloudWatch metric data on the AMI ID. The user observed some abnormal behaviour of the CPU utilization metric while viewing the last 2 weeks of data. The user wants to share that data with his manager. How can the user achieve this easily with the AWS console?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 313**

- (Topic 3)

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?

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

**Answer:** B

**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.

**NEW QUESTION 316**

- (Topic 3)

A user is receiving a notification from the RDS DB whenever there is a change in the DB security group. The user does not want to receive these notifications for only a month. Thus, he does not want to delete the notification. How can the user configure this?

- A. Change the Disable button for notification to "Yes" in the RDS console
- B. Set the send mail flag to false in the DB event notification console
- C. The only option is to delete the notification from the console
- D. Change the Enable button for notification to "No" in the RDS console

**Answer:** D

**Explanation:**

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

**NEW QUESTION 320**

- (Topic 3)

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?

- A. Pre warming the EBS volume
- B. Initiating the device to mount on the EBS volume
- C. Formatting the volume
- D. Copying the data from a snapshot to the device

**Answer:** A

**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.

**NEW QUESTION 322**

- (Topic 3)

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?

- A. Send the data using the put-metric-data command with the aggregate-values parameter
- B. Send the data using the put-metric-data command with the average-values parameter
- C. Send the data using the put-metric-data command with the statistic-values parameter
- D. Send the data using the put-metric-data command with the aggregate –data parameter

**Answer: C**

**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: `awscloudwatch put-metric-data --metric-name <Name> --namespace <Custom namespace> --timestamp <UTC Format> --statistic-values Sum=XX,Minimum=YY,Maximum=AA,SampleCount=BB --unit Milliseconds`

**NEW QUESTION 326**

- (Topic 3)

A user is planning to schedule a backup for an EBS volume. The user wants security of the snapshot data. How can the user achieve data encryption with a snapshot?

- A. Use encrypted EBS volumes so that the snapshot will be encrypted by AWS
- B. While creating a snapshot select the snapshot with encryption
- C. By default the snapshot is encrypted by AWS
- D. Enable server side encryption for the snapshot using S3

**Answer: A**

**Explanation:**

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

**NEW QUESTION 327**

- (Topic 3)

A user has launched an EC2 Windows instance from an instance store backed AMI. The user has also set the Instance initiated shutdown behavior to stop. What will happen when the user shuts down the OS?

- A. It will not allow the user to shutdown the OS when the shutdown behaviour is set to Stop
- B. It is not possible to set the termination behaviour to Stop for an Instance store backed AMI instance
- C. The instance will stay running but the OS will be shutdown
- D. The instance will be terminated

**Answer: B**

**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.

**NEW QUESTION 328**

- (Topic 3)

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?

- A. Destination : 20.0.0.0/24 and Target : VPC
- B. Destination : 20.0.0.0/16 and Target : ALL
- C. Destination : 20.0.0.0/0 and Target : ALL
- D. Destination : 20.0.0.0/24 and Target : Local

**Answer: D**

**NEW QUESTION 331**

- (Topic 3)

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:

ELB inserts the cookie in the response ELB chooses the instance based on the load balancing algorithm Check the cookie in the service request The cookie is found in the request The cookie is not found in the request

- A. 3,1,4,2 [Cookie is not Present] & 3,1,5,2 [Cookie is Present]
- B. 3,4,1,2 [Cookie is not Present] & 3,5,1,2 [Cookie is Present]
- C. 3,5,2,1 [Cookie is not Present] & 3,4,2,1 [Cookie is Present]
- D. 3,2,5,4 [Cookie is not Present] & 3,2,4,5 [Cookie is Present]

**Answer: C**

**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.

### NEW QUESTION 332

- (Topic 3)

A user has launched an EC2 instance. However, due to some reason the instance was terminated. If the user wants to find out the reason for termination, where can he find the details?

- A. It is not possible to find the details after the instance is terminated
- B. The user can get information from the AWS console, by checking the Instance description under the State transition reason label
- C. The user can get information from the AWS console, by checking the Instance description under the Instance Status Change reason label
- D. The user can get information from the AWS console, by checking the Instance description under the Instance Termination reason label

**Answer: D**

**Explanation:**

An EC2 instance, once terminated, may be available in the AWS console for a while after termination. The user can find the details about the termination from the description tab under the label State transition reason. If the instance is still running, there will be no reason listed. If the user has explicitly stopped or terminated the instance, the reason will be "User initiated shutdown".

### NEW QUESTION 336

- (Topic 3)

A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. The ELB security policy supports various ciphers. Which of the below mentioned options helps identify the matching cipher at the client side to the ELB cipher list when client is requesting ELB DNS over SSL?

- A. Cipher Protocol
- B. Client Configuration Preference
- C. Server Order Preference
- D. Load Balancer Preference

**Answer: C**

**Explanation:**

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

### NEW QUESTION 338

- (Topic 3)

A user is running a batch process on EBS backed EC2 instances. The batch process starts a few instances to process hadoop Map reduce jobs which can run between 50 – 600 minutes or sometimes for more time. The user wants to configure that the instance gets terminated only when the process is completed. How can the user configure this with CloudWatch?

- A. Setup the CloudWatch action to terminate the instance when the CPU utilization is less than 5%
- B. Setup the CloudWatch with Auto Scaling to terminate all the instances
- C. Setup a job which terminates all instances after 600 minutes
- D. It is not possible to terminate instances automatically

**Answer: D**

**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. The user can setup an action which terminates 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.

### NEW QUESTION 340

- (Topic 3)

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

- A. Use the internet gateway with a private IP
- B. Allow outbound traffic in the security group for port 80 to allow internet updates
- C. The private subnet can never connect to the internet
- D. Use NAT with an elastic IP

**Answer:** D

**Explanation:**

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

**NEW QUESTION 342**

- (Topic 3)

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

- A. Error Log
- B. Slow Query Log
- C. Transaction Log
- D. General Log

**Answer:** C

**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.

**NEW QUESTION 347**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your AWS-SysOps Exam with Our Prep Materials Via below:**

<https://www.certleader.com/AWS-SysOps-dumps.html>