

# Exam Questions AWS-SysOps

Amazon AWS Certified SysOps Administrator - Associate

<https://www.2passeasy.com/dumps/AWS-SysOps/>



### NEW QUESTION 1

- (Topic 1)

What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment of the primary OB instance fails?

- A. The IP of the primary DB instance is switched to the standby OB instance
- B. The RDS (Relational Database Service) DB instance reboots
- C. A new DB instance is created in the standby availability zone
- D. The canonical name record (CNAME) is changed from primary to standby

**Answer: D**

### NEW QUESTION 2

- (Topic 1)

Which of the following statements about this S3 bucket policy is true?

```
{
  "Id": "IPAllowPolicy",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "192.168.100.0/24"
        },
        "NotIpAddress": {
          "aws:SourceIp": "192.168.100.188/32"
        }
      }
    }
  ],
  "Principal": {
    "AWS": [
      "*"
    ]
  }
}
```

- A. Denies the server with the IP address 192 168 100 0 full access to the "mybucket" bucket
- B. Denies the server with the IP address 192 168 100 188 full access to the "mybucket" bucket
- C. Grants all the servers within the 192 168 100 0/24 subnet full access to the "mybucket" bucket
- D. Grants all the servers within the 192 168 100 188/32 subnet full access to the "mybucket" bucket

**Answer: B**

### NEW QUESTION 3

- (Topic 1)

A customer has a web application that uses cookie Based sessions to track logged in users It Is deployed on AWS using ELB and Auto Scaling The customer observes that when load increases. Auto Scaling launches new Instances but the load on the easting Instances does not decrease, causing all existing users to have a sluggish experience.

Which two answer choices independently describe a behavior that could be the cause of the sluggish user experience? Choose 2 answers

- A. ELB's normal behavior sends requests from the same user to the same backend instance
- B. ELB's behavior when sticky sessions are enabled causes ELB to send requests in the same session to the same backend instance
- C. A faulty browser is not honoring the TTL of the ELB DNS nam
- D. The web application uses long polling such as comet or websocket
- E. Thereby keeping a connection open to a web server tor a long time
- F. The web application uses long polling such as comet or websocket
- G. Thereby keeping a connection open to a web server for a long tim

**Answer: BD**

### NEW QUESTION 4

- (Topic 1)

You need to design a VPC for a web-application consisting of an Elastic Load Balancer (ELB). a fleet of web/application servers, and an RDS database The entire Infrastructure must be distributed over 2 availability zones.

Which VPC configuration works while assuring the database is not available from the Internet?

- A. One public subnet for ELB one public subnet for the web-servers, and one private subnet for the database
- B. One public subnet for ELB two private subnets for the web-servers, two private subnets for RDS
- C. Two public subnets for ELB two private subnets for the web-servers and two private subnets for RDS
- D. Two public subnets for ELB two public subnets for the web-servers, and two public subnets for RDS

**Answer: A**

#### NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (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 I
- 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 9

- (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-pai
- C. That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicat
- D. Security groups are set to allow the application host to talk to the database on the right port/protoco

**Answer: AD**

#### NEW QUESTION 10

- (Topic 1)

You are creating an Auto Scaling group whose Instances need to insert a custom metric into CloudWatch. Which method would be the best way to authenticate your CloudWatch PUT request?

- A. Create an IAM role with the Put MetricData permission and modify the Auto Scaling launch configuration to launch instances in that role
- B. Create an IAM user with the PutMetricData permission and modify the Auto Scaling launch configuration to inject the userscredentials into the instance User

Data

- C. Modify the appropriate Cloud Watch metric policies to allow the Put MetricData permission to instances from the Auto Scaling group
- D. Create an IAM user with the PutMetricData permission and put the credentials in a private repository and have applications on the server pull the credentials as needed

**Answer:** A

#### NEW QUESTION 10

- (Topic 1)

If you want to launch Amazon Elastic Compute Cloud (EC2) Instances and assign each Instance a predetermined private IP address you should:

- A. Assign a group or sequential Elastic IP address to the instances
- B. Launch the instances in a Placement Group
- C. Launch the instances in the Amazon virtual Private Cloud (VPC).
- D. Use standard EC2 instances since each instance gets a private Domain Name Service (DNS) already
- E. Launch the Instance from a private Amazon Machine image (Mil)

**Answer:** C

#### Explanation:

Reference:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html>

#### NEW QUESTION 11

- (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 15

- (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 20

- (Topic 2)

A user has created a VPC with CIDR 20.0.0.0/16 with only a private subnet and VPN connection using the VPC wizard. The user wants to connect to the instance in a private subnet over SSH. How should the user define the security rule for SSH?

- A. Allow Inbound traffic on port 22 from the user's network
- B. The user has to create an instance in EC2 Classic with an elastic IP and configure the security group of a private subnet to allow SSH from that elastic IP
- C. The user can connect to a instance in a private subnet using the NAT instance
- D. Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the Internet

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 23

- (Topic 2)

A system admin is managing buckets, objects and folders with AWS S3. Which of the below mentioned statements is true and should be taken in consideration by the sysadmin?

- A. The folders support only ACL
- B. Both the object and bucket can have an Access Policy but folder cannot have policy
- C. Folders can have a policy
- D. Both the object and bucket can have ACL but folders cannot have ACL

**Answer:** A

**Explanation:**

A sysadmin can grant permission to the S3 objects or the buckets to any user or make objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket. It cannot be applied at the object level. The folders are similar to objects with no content. Thus, folders can have only ACL and cannot have a policy.

**NEW QUESTION 28**

- (Topic 2)

A user has received a message from the support team that an issue occurred 1 week back between 3 AM to 4 AM and the EC2 server was not reachable. The user is checking the CloudWatch metrics of that instance. How can the user find the data easily using the CloudWatch console?

- A. The user can find the data by giving the exact values in the time Tab under CloudWatch metrics
- B. The user can find the data by filtering values of the last 1 week for a 1 hour period in the Relative tab under CloudWatch metrics
- C. It is not possible to find the exact time from the console
- D. The user has to use CLI to provide the specific time
- E. The user can find the data by giving the exact values in the Absolute tab under CloudWatch metrics

**Answer:** D

**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.

**NEW QUESTION 31**

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

Amazon CloudWatch is basically a metrics repository. Either the user can send the custom data or an AWS product can put metrics into the repository, and the user can retrieve the statistics based on those metrics. The statistics are metric data aggregations over specified periods of time. Aggregations are made using the namespace, metric name, dimensions, and the data point unit of measure, within the time period that is specified by the user. To aggregate the data across instances launched with AMI, the user should select the AMI ID under EC2 metrics and select the aggregate average to view the data.

**NEW QUESTION 36**

- (Topic 2)

A user is running one instance for only 3 hours every day. The user wants to save some cost with the instance. Which of the below mentioned Reserved Instance categories is advised in this case?

- A. The user should not use RI; instead only go with the on-demand pricing
- B. The user should use the AWS high utilized RI
- C. The user should use the AWS medium utilized RI
- D. The user should use the AWS low utilized RI

**Answer:** A

**Explanation:**

The AWS Reserved Instance provides the user with an option to save some money by paying a one-time fixed amount and then save on the hourly rate. It is advisable that if the user is having 30% or more usage of an instance per day, he should go for a RI. If the user is going to use an EC2 instance for more than 2200-2500 hours per year, RI will help the user save some cost. Here, the instance is not going to run for less than 1500 hours. Thus, it is advisable that the user should use the on-demand pricing.

**NEW QUESTION 40**

- (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 45

- (Topic 2)

An organization is setting up programmatic billing access for their AWS account. Which of the below mentioned services is not required or enabled when the organization wants to use programmatic access?

- A. Programmatic access
- B. AWS bucket to hold the billing report
- C. AWS billing alerts
- D. Monthly Billing report

**Answer:** C

**Explanation:**

AWS provides an option to have programmatic access to billing. Programmatic Billing Access leverages the existing Amazon Simple Storage Service (Amazon S3. APIs. Thus, the user can build applications that reference his billing data from a CSV (comma-separated value. file stored in an Amazon S3 bucket. To enable programmatic access, the user has to first enable the monthly billing report. Then the user needs to provide an AWS bucket name where the billing CSV will be uploaded. The user should also enable the Programmatic access option.

#### NEW QUESTION 46

- (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 51

- (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-Classik. 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 55

- (Topic 2)

An organization has added 3 of his AWS accounts to consolidated billing. One of the AWS accounts has purchased a Reserved Instance (RI. of a small instance size in the US-East-1a zone. All other AWS accounts are running instances of a small size in the same zone. What will happen in this case for the RI pricing?

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

**Answer:** C

**Explanation:**

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. For billing purposes, consolidated billing treats all the accounts on the consolidated bill as one account. This means that all accounts on a consolidated bill can receive the hourly cost benefit of the Amazon EC2 Reserved Instances purchased by any other account. In this case only one Reserved Instance has been purchased by one account. Thus, only a single instance from any of the accounts will get the advantage of RI. AWS will implement the blended rate for each instance if more than one instance is running concurrently.

#### NEW QUESTION 57

- (Topic 2)

A user is trying to save some cost on the AWS services. Which of the below mentioned options will not help him save cost?

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

**Answer:** B

**Explanation:**

AWS bills the user on a pay as you go model. AWS will charge the user once the AWS resource is allocated. Even though the user is not using the resource, AWS will charge if it is in service or allocated. Thus, it is advised that once the user's work is completed he should: Terminate the EC2 instance Delete the EBS volumes Release the unutilized Elastic IPs Delete ELB The AutoScaling launch configuration does not cost the user. Thus, it will not make any difference to the cost whether it is deleted or not.

#### NEW QUESTION 59

- (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 62

- (Topic 2)

A user has created an ELB with Auto Scaling. Which of the below mentioned offerings from ELB helps the user to stop sending new requests traffic from the load balancer to the EC2 instance when the instance is being deregistered while continuing in-flight requests?

- A. ELB sticky session
- B. ELB deregistration check
- C. ELB connection draining
- D. ELB auto registration Off

**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.

#### NEW QUESTION 65

- (Topic 2)

A user has setup a web application on EC2. The user is generating a log of the application performance at every second. There are multiple entries for each second. If the user wants to send that data to CloudWatch every minute, what should he do?

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 66

- (Topic 2)

An organization has created 50 IAM users. The organization has introduced a new policy which will change the access of an IAM user. How can the organization implement this effectively so that there is no need to apply the policy at the individual user level?

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

**Answer:** A

#### Explanation:

With AWS IAM, a group is a collection of IAM users. A group allows the user to specify permissions for a collection of users, which can make it easier to manage the permissions for those users. A group helps an organization manage access in a better way; instead of applying at the individual level, the organization can apply at the group level which is applicable to all the users who are a part of that group.

#### NEW QUESTION 69

- (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 71

- (Topic 2)

An organization wants to move to Cloud. They are looking for a secure encrypted database storage option. Which of the below mentioned AWS functionalities helps them to achieve this?

- A. AWS MFA with EBS
- B. AWS EBS encryption
- C. Multi-tier encryption with Redshift
- D. AWS S3 server side storage

**Answer:** B

#### Explanation:

AWS EBS supports encryption of the volume while creating new volumes. It also supports creating volumes from existing snapshots provided the snapshots are created from encrypted volumes. The data at rest, the I/O as well as all the snapshots of EBS will be encrypted. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between the EC2 instances and EBS storage. EBS encryption is based on the AES-256 cryptographic algorithm, which is the industry standard

#### NEW QUESTION 74

- (Topic 2)

A user is publishing custom metrics to CloudWatch. Which of the below mentioned statements will help the user understand the functionality better?

- A. The user can use the CloudWatch Import tool
- B. The user should be able to see the data in the console after around 15 minutes
- C. If the user is uploading the custom data, the user must supply the namespace, timezone, and metric name as part of the command
- D. The user can view as well as upload data using the console, CLI and APIs

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

#### NEW QUESTION 79

- (Topic 2)

You are building an online store on AWS that uses SQS to process your customer orders. Your backend system needs those messages in the same sequence the customer orders have been put in. How can you achieve that?

- A. It is not possible to do this with SQS
- B. You can use sequencing information on each message
- C. You can do this with SQS but you also need to use SWF
- D. Messages will arrive in the same order by default

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 83

- (Topic 2)

An organization is using cost allocation tags to find the cost distribution of different departments and projects. One of the instances has two separate tags with the key/ value as "InstanceName/HR", "CostCenter/HR". What will AWS do in this case?

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 84

- (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 and a private subnet with CIDR 20.0.0.128/25. The user has launched one instance each in the private and public subnets. Which of the below mentioned options cannot be the correct IP address (private IP. assigned to an instance in the public or private subnet?

- A. 20.0.0.255
- B. 20.0.0.132
- C. 20.0.0.122
- D. 20.0.0.55

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 89

- (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 91

- (Topic 3)

A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?

- A. AWS/StorageGateway
- B. AWS/CloudTrail
- C. AWS/ElastiCache
- D. AWS/SWF

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 96

- (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 97

- (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 99

- (Topic 3)

When an EC2 instance mat is backed by an S3-Dased 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 snapsho
- C. Data is unavailable until the instance is restarted
- D. Data is automatically saved as an EBS volum

**Answer: A**

#### NEW QUESTION 100

- (Topic 3)

A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24. and a public subnet (20.0.0.0/24.. The user's data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?

- A. It will allow traffic communication on both the CIDRs of the data centre
- B. It will not allow traffic with data centre on CIDR 20.1.0.0/24 but allows traffic communication on 20.0.54.0/24
- C. It will not allow traffic communication on any of the data centre CIDRs
- D. It will allow traffic with data centre on CIDR 20.1.0.0/24 but does not allow on 20.0.54.0/24

**Answer:** D

**Explanation:**

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

**NEW QUESTION 105**

- (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 109**

- (Topic 3)

Which of the following statements about this S3 bucket policy is true?

```
{
  "Id": "IPAllowPolicy",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "192.168.100.0/24"
        },
        "NotIpAddress": {
          "aws:SourceIp": "192.168.100.188/32"
        }
      }
    }
  ],
  "Principal": {
    "AWS": [
      "*"
    ]
  }
}
```

- A. Denies the server with the IP address 192.166 100.0 full access to the "mybucket" bucket
- B. Denies the server with the IP address 192.166 100.188 full access to the "mybucket bucket
- C. Grants all the servers within the 192 168 100 0/24 subnet full access to the "mybucket" bucket
- D. Grants all the servers within the 192 168 100 188/32 subnet full access to the "mybucket" bucket

**Answer:** C

**NEW QUESTION 113**

- (Topic 3)

A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is true in this scenario?

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

**Answer:** B

**Explanation:**

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance of a smaller or higher size, respectively. The VPC has an implied router and the VPC wizard updates the main route table used with the private subnet, creates a custom route table and associates it with the public subnet.

#### NEW QUESTION 117

- (Topic 3)

A user is planning to scale up an application by 8 AM and scale down by 7 PM daily using Auto Scaling. What should the user do in this case?

- A. Setup the scaling policy to scale up and down based on the CloudWatch alarms
- B. The user should increase the desired capacity at 8 AM and decrease it by 7 PM manually
- C. The user should setup a batch process which launches the EC2 instance at a specific time
- D. Setup scheduled actions to scale up or down at a specific time

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 118

- (Topic 3)

A user wants to upload a complete folder to AWS S3 using the S3 Management console. How can the user perform this activity?

- A. Just drag and drop the folder using the flash tool provided by S3
- B. Use the Enable Enhanced Folder option from the S3 console while uploading objects
- C. The user cannot upload the whole folder in one go with the S3 management console
- D. Use the Enable Enhanced Uploader option from the S3 console while uploading objects

**Answer:** D

#### Explanation:

AWS S3 provides a console to upload objects to a bucket. The user can use the file upload screen to upload the whole folder in one go by clicking on the Enable Enhanced Uploader option. When the user uploads a folder, Amazon S3 uploads all the files and subfolders from the specified folder to the user's bucket. It then assigns a key value that is a combination of the uploaded file name and the folder name.

#### NEW QUESTION 123

- (Topic 3)

A user has configured an EC2 instance in the US-East-1a zone. The user has enabled detailed monitoring of the instance. The user is trying to get the data from CloudWatch using a CLI. Which of the below mentioned CloudWatch endpoint URLs should the user use?

- A. monitoring.us-east-1.amazonaws.com
- B. monitoring.us-east-1-a.amazonaws.com
- C. monitoring.us-east-1a.amazonaws.com
- D. cloudwatch.us-east-1a.amazonaws.com

**Answer:** A

#### Explanation:

The CloudWatch resources are always region specific and they will have the end point as region specific. If the user is trying to access the metric in the US-East-1 region, the endpoint URL will be: monitoring.us-east-1.amazonaws.com

#### NEW QUESTION 127

- (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 128

- (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 130**

- (Topic 3)

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

- A. Response processing time
- B. Front end processing time
- C. Backend processing time
- D. Request processing time

**Answer:** B

**Explanation:**

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

**NEW QUESTION 131**

- (Topic 3)

A user has created an EBS volume of 10 GB and attached it to a running instance. The user is trying to access EBS for first time. Which of the below mentioned options is the correct statement with respect to a first time EBS access?

- A. The volume will show a size of 8 GB
- B. The volume will show a loss of the IOPS performance the first time
- C. The volume will be blank
- D. If the EBS is mounted it will ask the user to create a file system

**Answer:** B

**Explanation:**

A user can create an EBS volume either from a snapshot or as a blank volume. If the volume is from a snapshot it will not be blank. The volume shows the right size only as long as it is mounted. This shows that the file system is created. When the user is accessing the volume the AWS EBS will wipe out the block storage or instantiate from the snapshot. Thus, the volume will show a loss of IOPS. It is recommended that the user should pre warm the EBS before use to achieve better IO.

**NEW QUESTION 135**

- (Topic 3)

An organization has configured Auto Scaling for hosting their application. The system admin wants to understand the Auto Scaling health check process. If the instance is unhealthy, Auto Scaling launches an instance and terminates the unhealthy instance. What is the order execution?

- A. Auto Scaling launches a new instance first and then terminates the unhealthy instance
- B. Auto Scaling performs the launch and terminate processes in a random order
- C. Auto Scaling launches and terminates the instances simultaneously
- D. Auto Scaling terminates the instance first and then launches a new instance

**Answer:** D

**Explanation:**

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

**NEW QUESTION 138**

- (Topic 3)

An application you maintain consists of multiple EC2 instances in a default tenancy VPC. This application has undergone an internal audit and has been determined to require dedicated hardware for one instance. Your compliance team has given you a week to move this instance to single-tenant hardware. Which process will have minimal impact on your application while complying with this requirement?

- A. Create a new VPC with tenancy=dedicated and migrate to the new VPC
- B. Use ec2-reboot-instances command line and set the parameter "dedicated=true"
- C. Right click on the instance, select properties and check the box for dedicated tenancy
- D. Stop the instance, create an AMI, launch a new instance with tenancy=dedicated, and terminate the old instance

**Answer:** A

**Explanation:**

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/CommandLineReference/ApiReference-cmd-CreateVpc.html>

**NEW QUESTION 140**

- (Topic 3)

A root account owner is trying to understand the S3 bucket ACL. Which of the below mentioned options cannot be used to grant ACL on the object using the authorized predefined group?

- A. Authenticated user group
- B. All users group
- C. Log Delivery Group
- D. Canonical user group

**Answer:** D

**Explanation:**

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

**NEW QUESTION 141**

- (Topic 3)

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below mentioned entries is required in the web server security group (WebSecGrp)?

- A. Configure Destination as DB Security group ID (DbSecGr
- B. for port 3306 Outbound
- C. 80 for Destination 0.0.0.0/0 Outbound
- D. Configure port 3306 for source 20.0.0.0/24 InBound
- E. Configure port 80 InBound for source 20.0.0.0/16

**Answer:** A

**Explanation:**

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the public subnet can receive inbound traffic directly from the internet. Thus, the user should configure port 80 with source 0.0.0.0/0 in InBound. The user should configure that the instance in the public subnet can send traffic to the private subnet instances on the DB port. Thus, the user should configure the DB Amazon AWS-SysOps : Practice Test security group of the private subnet (DbSecGrp) as the destination for port 3306 in Outbound.

**NEW QUESTION 146**

- (Topic 3)

Amazon EBS snapshots have which of the following two characteristics? (Choose 2.) Choose 2 answers

- A. EBS snapshots only save incremental changes from snapshot to snapshot
- B. EBS snapshots can be created in real-time without stopping an EC2 instance
- C. EBS snapshots can only be restored to an EBS volume of the same size or smaller
- D. EBS snapshots can only be restored and mounted to an instance in the same Availability Zone as the original EBS volume

**Answer:** AD

**NEW QUESTION 147**

- (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 148**

- (Topic 3)

A user has moved an object to Glacier using the life cycle rules. The user requests to restore the archive after 6 months. When the restore request is completed the user accesses that archive. Which of the below mentioned statements is not true in this condition?

- A. The archive will be available as an object for the duration specified by the user during the restoration request
- B. The restored object's storage class will be RRS
- C. The user can modify the restoration period only by issuing a new restore request with the updated period
- D. The user needs to pay storage for both RRS (restore and Glacier (Archiv
- E. Rates
- F. Rates

**Answer: B**

**Explanation:**

AWS Glacier is an archival service offered by AWS. AWS S3 provides lifecycle rules to archive and restore objects from S3 to Glacier. Once the object is archived their storage class will change to Glacier. If the user sends a request for restore, the storage class will still be Glacier for the restored object. The user will be paying for both the archived copy as well as for the restored object. The object is available only for the duration specified in the restore request and if the user wants to modify that period, he has to raise another restore request with the updated duration.

**NEW QUESTION 151**

- (Topic 3)

A user has created a Cloudformation stack. The stack creates AWS services, such as EC2 instances, ELB, AutoScaling, and RDS. While creating the stack it created EC2, ELB and AutoScaling but failed to create RDS. What will Cloudformation do in this scenario?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 154**

- (Topic 3)

A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is not true in this scenario?

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

**Answer: A**

**Explanation:**

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance with an elastic IP. Wizard will also create two subnets with route tables. It will also create an internet gateway and attach it to the VPC.

**NEW QUESTION 155**

- (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 160**

- (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 165

- (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 168

- (Topic 3)

A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required for the NAT security group?

- A. For Inbound allow Source: 20.0.1.0/24 on port 80
- B. For Outbound allow Destination: 0.0.0.0/0 on port 80
- C. For Inbound allow Source: 20.0.0.0/24 on port 80
- D. For Outbound allow Destination: 0.0.0.0/0 on port 443

**Answer: C**

**Explanation:**

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the private subnet can connect to the internet using the NAT instances. The user should first configure that NAT can receive traffic on ports 80 and 443 from the private subnet. Thus, allow ports 80 and 443 in Inbound for the private subnet 20.0.1.0/24. Now to route this traffic to the internet configure ports 80 and Amazon AWS-SysOps : Practice Test 443 in Outbound with destination 0.0.0.0/0. The NAT should not have an entry for the public subnet CIDR.

#### NEW QUESTION 172

- (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 175

- (Topic 3)

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

- A. The ratio between IOPS and the EBS volume is higher than 30
- B. The maximum IOPS supported by EBS is 3000

- C. The ratio between IOPS and the EBS volume is lower than 50
- D. PIOPS is supported for EBS higher than 500 GB size

**Answer:** A

**Explanation:**

A provisioned IOPS EBS volume can range in size from 10 GB to 1 TB and the user can provision up to 4000 IOPS per volume. The ratio of IOPS provisioned to the volume size requested should be a maximum of 30; for example, a volume with 3000 IOPS must be at least 100 GB.

#### NEW QUESTION 176

- (Topic 3)

An organization is trying to create various IAM users. Which of the below mentioned options is not a valid IAM username?

- A. John.cloud
- B. john@cloud
- C. John=cloud
- D. john#cloud

**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. Whenever the organization is creating an IAM user, there should be a unique ID for each user. The names of users, groups, roles, instance profiles must be alphanumeric, including the following common characters: plus (+), equal (=), comma (,), period (.), at (@), and dash (-).

#### NEW QUESTION 179

- (Topic 3)

A user has enabled session stickiness with ELB. The user does not want ELB to manage the cookie; instead he wants the application to manage the cookie. What will happen when the server instance, which is bound to a cookie, crashes?

- A. The response will have a cookie but stickiness will be deleted
- B. The session will not be sticky until a new cookie is inserted
- C. ELB will throw an error due to cookie unavailability
- D. The session will be sticky and ELB will route requests to another server as ELB keeps replicating the Cookie

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 181

- (Topic 3)

A user has hosted an application on EC2 instances. The EC2 instances are configured with ELB and Auto Scaling. The application server session time out is 2 hours. The user wants to configure connection draining to ensure that all in-flight requests are supported by ELB even though the instance is being deregistered. What time out period should the user specify for connection draining?

- A. 5 minutes
- B. 1 hour
- C. 30 minutes
- D. 2 hours

**Answer:** B

#### NEW QUESTION 185

- (Topic 3)

A user has configured ELB with a TCP listener at ELB as well as on the back-end instances. The user wants to enable a proxy protocol to capture the source and destination IP information in the header. Which of the below mentioned statements helps the user understand a proxy protocol with TCP configuration?

- A. If the end user is requesting behind a proxy server then the user should not enable a proxy protocol on ELB
- B. ELB does not support a proxy protocol when it is listening on both the load balancer and the back-end instances
- C. Whether the end user is requesting from a proxy server or directly, it does not make a difference for the proxy protocol
- D. If the end user is requesting behind the proxy then the user should add the "isproxy" flag to the ELB Configuration

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 187

- (Topic 3)

A user has created an application which will be hosted on EC2. The application makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK to connect with from the EC2 instance. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

- A. The user should attach an IAM role with DynamoDB access to the EC2 instance
- B. The user should create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB
- C. The user should create an IAM role, which has EC2 access so that it will allow deploying the application
- D. The user should create an IAM user with DynamoDB and EC2 access
- E. Attach the user with the application so that it does not use the root account credentials

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 190

- (Topic 3)

A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance. The internet gateway has also been created. What can be the reason for the error?

- A. The internet gateway is not configured with the route table
- B. The private IP is not present
- C. The outbound traffic on the security group is disabled
- D. The internet gateway is not configured with the security group

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 191

- (Topic 3)

A user has enabled termination protection on an EC2 instance. The user has also set Instance initiated shutdown behaviour to terminate. When the user shuts down the instance from the OS, what will happen?

- A. The OS will shutdown but the instance will not be terminated due to protection
- B. It will terminate the instance
- C. It will not allow the user to shutdown the instance from the OS
- D. It is not possible to set the termination protection when an Instance initiated shutdown is set to Terminate

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 195

- (Topic 3)

A user has created an Auto Scaling group using CLI. The user wants to enable CloudWatch detailed monitoring for that group. How can the user configure this?

- A. When the user sets an alarm on the Auto Scaling group, it automatically enables detail monitoring
- B. By default detailed monitoring is enabled for Auto Scaling
- C. Auto Scaling does not support detailed monitoring
- D. Enable detail monitoring from the AWS console

**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. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates an Auto Scaling launch config as the first step for creating an Auto Scaling group, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. Thus, the user does not need to set this flag if he wants detailed monitoring.

#### NEW QUESTION 197

- (Topic 3)

A user has granted read/write permission of his S3 bucket using ACL. Which of the below mentioned options is a valid ID to grant permission to other AWS accounts (grantee. using ACL)?

- A. IAM User ID
- B. S3 Secure ID
- C. Access ID
- D. Canonical user ID

**Answer: D**

#### Explanation:

An S3 bucket ACL grantee can be an AWS account or one of the predefined Amazon S3 groups. The user can grant permission to an AWS account by the email address of that account or by the canonical user ID. If the user provides an email in the grant request, Amazon S3 finds the canonical user ID for that account and adds it to the ACL. The resulting ACL will always contain the canonical user ID for the AWS account, and not the AWS account's email address.

#### NEW QUESTION 200

- (Topic 3)

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created public and VPN only subnets along with hardware VPN access to connect to the user's data centre. The user has not yet launched any instance as well as modified or deleted any setup. He wants to delete this VPC from the console. Will the console allow the user to delete the VPC?

- A. Yes, the console will delete all the setups and also delete the virtual private gateway
- B. No, the console will ask the user to manually detach the virtual private gateway first and then allow deleting the VPC
- C. Yes, the console will delete all the setups and detach the virtual private gateway
- D. No, since the NAT instance is running

**Answer: C**

#### Explanation:

The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, it will create a virtual private gateway to route all traffic of the VPN subnet. If the virtual private gateway is attached with VPC and the user deletes the VPC from the console it will first detach the gateway automatically and only then delete the VPC.

#### NEW QUESTION 205

- (Topic 3)

An AWS root account owner is trying to create a policy to access RDS. Which of the below mentioned statements is true with respect to the above information?

- A. Create a policy which allows the users to access RDS and apply it to the RDS instances
- B. The user cannot access the RDS database if he is not assigned the correct IAM policy
- C. The root account owner should create a policy for the IAM user and give him access to the RDS services
- D. The policy should be created for the user and provide access for RDS

**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 account owner wants to create a policy for RDS, the owner has to create an IAM user and define the policy which entitles the IAM user with various RDS services such as Launch Instance, Manage security group, Manage parameter group etc.

#### NEW QUESTION 209

- (Topic 3)

Your organization is preparing for a security assessment of your use of AWS.

In preparation for this assessment, which two IAM best practices should you consider implementing? Choose 2 answers

- A. Create individual IAM users for everyone in your organization
- B. Configure MFA on the root account and for privileged IAM users
- C. Assign IAM users and groups configured with policies granting least privilege access
- D. Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

**Answer: BC**

#### Explanation:

Reference:

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

#### NEW QUESTION 211

- (Topic 3)

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

- A. Create an IAM policy with the security group and use that security group for AWS console login
- B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization

- C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
- D. Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 214**

- (Topic 3)

A user has created a VPC with CIDR 20.0.0.0/16 using VPC Wizard. The user has created a public CIDR (20.0.0.0/24) and a VPN only subnet CIDR (20.0.1.0/24) along with the hardware VPN access to connect to the user's data centre. Which of the below mentioned components is not present when the VPC is setup with the wizard?

- A. Main route table attached with a VPN only subnet
- B. A NAT instance configured to allow the VPN subnet instances to connect with the internet
- C. Custom route table attached with a public subnet
- D. An internet gateway for a public subnet

**Answer:** B

**Explanation:**

The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, it will update the main route table used with the VPN-only subnet, create a custom route table and associate it with the public subnet. It also creates an internet gateway for the public subnet. The wizard does not create a NAT instance by default. The user can create it manually and attach it with a VPN only subnet.

**NEW QUESTION 217**

A user is trying to setup a scheduled scaling activity using Auto Scaling. The user wants to setup the recurring schedule. Which of the below mentioned parameters is not required in this case?

- A. Maximum size
- B. Auto Scaling group name
- C. End time
- D. Recurrence value

**Answer:** A

**Explanation:**

Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. The user can also configure the recurring schedule action which will follow the Linux cron format. If the user is setting a recurring event, it is required that the user specifies the Recurrence value (in a cron format), end time (not compulsory but recurrence will stop after this) and the Auto Scaling group for which the scaling activity is to be scheduled.

**NEW QUESTION 218**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-SysOps Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-SysOps Product From:

<https://www.2passeasy.com/dumps/AWS-SysOps/>

## Money Back Guarantee

### **AWS-SysOps Practice Exam Features:**

- \* AWS-SysOps Questions and Answers Updated Frequently
- \* AWS-SysOps Practice Questions Verified by Expert Senior Certified Staff
- \* AWS-SysOps Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* AWS-SysOps Practice Test Questions in Multiple Choice Formats and Updates for 1 Year