Amazon

Exam Questions AWS-SysOps

Amazon AWS Certified SysOps Administrator - Associate

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 infrastructur
B. Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructur
C. Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructur
D. Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructur

Answer: B

Explanation:
Reference:
http://aws.amazon.com/opsworks/faqs/

NEW QUESTION 2
- (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 side 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 PIOPs 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 3
- (Topic 1)
When preparing for a compliance assessment of your system built inside of AWS. what are three best-practices for you to prepare for an audit?
Choose 3 answers

A. Gather evidence of your IT operational controls
B. Request and obtain applicable third-party audited AWS compliance reports and certifications
C. Request and obtain a compliance and security tour of an AWS data center for a pre-assessment security review
D. Request and obtain approval from AWS to perform relevant network scans and in-depth penetration tests of your system's Instances and endpoints
E. Schedule meetings with AWS's third-party auditors to provide evidence of AWS compliance that maps to your control objectives

Answer: ABD

NEW QUESTION 4
- (Topic 1)
You use S3 to store critical data for your company Several users within your group currently have lull permissions to your S3 buckets You need to come up with a solution mat does not impact your users and also protect against the accidental deletion of objects.
Which two options will address this issue? Choose 2 answers

A. Enable versioning on your S3 Buckets
B. Configure your S3 Buckets with MFA delete
C. Create a Bucket policy and only allow read only permissions to all users at the bucket level
D. Enable object life cycle policies and configure the data older than 3 months to be archived in Glacier

Answer: AB

NEW QUESTION 5
- (Topic 1)
You have a server with a 5O0GB 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 me two disks

Answer: D

Explanation:

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

NEW QUESTION 6
- (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 7
- (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 8
- (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 9
- (Topic 1)
You run a web application where web servers on EC2 Instances are In an Auto Scaling group Monitoring over the last 6 months shows that 6 web servers are necessary to handle the minimum load During the day up to 12 servers are needed Five to six days per year, the number of web servers required might go up to 15.
What would you recommend to minimize costs while being able to provide hill availability?

A. 6 Reserved instances (heavy utilization). 6 Reserved instances {medium utilization), rest covered by On-Demand instances
B. 6 Reserved instances (heavy utilization). 6 On-Demand instances, rest covered by Spot Instances
C. 6 Reserved instances (heavy utilization) 6 Spot instances, rest covered by On-Demand instances
D. 6 Reserved instances (heavy utilization) 6 Reserved instances (medium utilization) rest covered by Spot instances

Answer: B

NEW QUESTION 10
- (Topic 1)
What is a placement group?

A. A collection of Auto Scaling groups in the same Region
B. Feature that enables EC2 instances to interact with each other via nigh bandwidth, low latency connections
C. A collection of Elastic Load Balancers in the same Region or Availability Zone
D. A collection of authorized Cloud Front edge locations for a distribution

Answer: B

Explanation:
Reference:
http://aws.amazon.com/ec2/faqs/

NEW QUESTION 10
- (Topic 1)
Which of the following requires a custom CloudWatch metric to monitor?

A. Data transfer of an EC2 instance
B. Disk usage activity of an EC2 instance
C. Memory Utilization of an EC2 instance
D. CPU Utilization of an EC2 instance

Answer: C

Explanation:
Reference:
http://aws.amazon.com/cloudwatch/

NEW QUESTION 13
- (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 15
- (Topic 1)
Your organization's security policy requires that all privileged users either use frequently rotated passwords or one-time access credentials in addition to username/password.
Which two of the following options would allow an organization to enforce this policy for AWS users?
Choose 2 answers

A. Configure multi-factor authentication for privileged 1AM users
B. Create 1AM users for privileged accounts
C. Implement identity federation between your organization's Identity provider leveraging the 1AM Security Token Service
D. Enable the 1AM single-use password policy option for privileged users

Answer: CD

NEW QUESTION 20
- (Topic 1)
Your application currently leverages AWS Auto Scaling to grow and shrink as load Increases/ decreases and has been performing well Your marketing team expects a steady ramp up in traffic to follow an upcoming campaign that will result in a 20x growth in traffic over 4 weeks Your forecast for the approximate number of Amazon EC2 instances necessary to meet the peak demand is 175.
What should you do to avoid potential service disruptions during the ramp up in traffic?

A. Ensure that you have pre-allocated 175 Elastic IP addresses so that each server will be able to obtain one as it launches
B. Check the service limits in Trusted Advisor and adjust as necessary so the forecasted count remains within limit
C. Change your Auto Scaling configuration to set a desired capacity of 175 prior to the launch of the marketing campaign
D. Pre-warm your Elastic Load Balancer to match the requests per second anticipated during peak demand prior to the marketing campaign

Answer: D

NEW QUESTION 25
- (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 28
- (Topic 1)
You have started a new job and are reviewing your company's infrastructure on AWS You notice one web application where they have an Elastic Load Balancer (&B) in front of web instances in an Auto Scaling Group When you check the metrics for the ELB in CloudWatch you see four healthy instances In Availability Zone (AZ) A and zero in AZ B There are zero unhealthy instances.
What do you need to fix to balance the instances across AZs?

A. Set the ELB to only be attached to another AZ
B. Make sure Auto Scaling is configured to launch in both AZs

C. Make sure your AMI is available in both AZs
D. Make sure the maximum size of the Auto Scaling Group is greater than 4

Answer: B

NEW QUESTION 32
- (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 33
- (Topic 2)
A user is planning to setup infrastructure on AWS for the Christmas sales. The user is planning to use Auto Scaling based on the schedule for proactive scaling. What advise would you give to the user?

A. It is good to schedule now because if the user forgets later on it will not scale up
B. The scaling should be setup only one week before Christmas
C. Wait till end of November before scheduling the activity
D. It is not advisable to use scheduled based scaling

Answer: C

Explanation:

Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. The user can specify any date in the future to scale up or down during that period. As per Auto Scaling the user can schedule an action for up to a month in the future. Thus, it is recommended to wait until end of November before scheduling for Christmas.

NEW QUESTION 34
- (Topic 2)
A user is trying to understand the ACL and policy for an S3 bucket. Which of the below mentioned policy permissions is equivalent to the WRITE ACL on a bucket?

A. s3:GetObjectAcl
B. s3:GetObjectVersion
C. s3:ListBucketVersions
D. s3:DeleteObject

Answer: D

Explanation:

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

NEW QUESTION 39
- (Topic 2)
An application is generating a log file every 5 minutes. The log file is not critical but may be required only for verification in case of some major issue. The file should be accessible over the internet whenever required. Which of the below mentioned options is a best possible storage solution for it?

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

Answer: D

Explanation:

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

NEW QUESTION 41
- (Topic 2)
A user is trying to connect to a running EC2 instance using SSH. However, the user gets a connection time out error. Which of the below mentioned options is not a possible reason for rejection?

A. The access key to connect to the instance is wrong
B. The security group is not configured properly

C. The private key used to launch the instance is not correct
D. The instance CPU is heavily loaded

Answer: A

Explanation:

If the user is trying to connect to a Linux EC2 instance and receives the connection time out error the probable reasons are: Security group is not configured with the SSH port The private key pair is not right The user name to login is wrong The instance CPU is heavily loaded, so it does not allow more connections

NEW QUESTION 46
- (Topic 2)
A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24. and VPN only subnets CIDR (20.0.1.0/24. along with the VPN gateway (vgw-12345. to connect to the user's data centre. Which of the below mentioned options is a valid entry for the main route table in this scenario?

A. Destination: 20.0.0.0/24 and Target: vgw-12345
B. Destination: 20.0.0.0/16 and Target: ALL
C. Destination: 20.0.1.0/16 and Target: vgw-12345
D. Destination: 0.0.0.0/0 and Target: vgw-12345

Answer: D

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. Here are the valid entries for the main route table in this scenario: Destination: 0.0.0.0/0 & Target: vgw-12345 (To route all internet traffic to the VPN gateway. Destination: 20.0.0.0/16 & Target: local (To allow local routing in VPC.

NEW QUESTION 51
- (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 56
- (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 61
- (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 consol
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 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 (Paye
B. account will get only the total bill and cannot see the cost incurred by each account
C. Master (Paye
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 68
- (Topic 2)
A sys admin is maintaining an application on AWS. The application is installed on EC2 and user has configured ELB and Auto Scaling. Considering future load increase, the user is planning to launch new servers proactively so that they get registered with ELB. How can the user add these instances with Auto Scaling?

A. Increase the desired capacity of the Auto Scaling group
B. Increase the maximum limit of the Auto Scaling group
C. Launch an instance manually and register it with ELB on the fly
D. Decrease the minimum limit of the Auto Scaling grou

Answer: A

Explanation:

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

NEW QUESTION 70
- (Topic 2)
A user has created a photo editing software and hosted it on EC2. The software accepts requests from the user about the photo format and resolution and sends a message to S3 to enhance the picture accordingly.Which of the below mentioned AWS services will help make a scalable software with the AWS infrastructure in this scenario?

A. AWS Glacier
B. AWS Elastic Transcoder
C. AWS Simple Notification Service
D. AWS Simple Queue Service

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 configure SQS, which will decouple the call between the EC2 application and S3. Thus, the application does not keep waiting for S3 to provide the data.

NEW QUESTION 73
- (Topic 2)
A root AWS account owner is trying to understand various options to set the permission to AWS S3. Which of the below mentioned options is not the right option to grant permission for S3?

A. User Access Policy
B. S3 Object Access Policy
C. S3 Bucket Access Policy
D. S3 ACL

Answer: B

Explanation:

Amazon S3 provides a set of operations to work with the Amazon S3 resources. Managing S3 resource access refers to granting others permissions to work with S3. There are three ways the root account owner can define access with S3: S3 ACL: The user can use ACLs to grant basic read/write permissions to other AWS accounts. S3 Bucket Policy: The policy is used to grant other AWS accounts or IAM users permissions for the bucket and the objects in it. User Access Policy: Define an IAM user and assign him the IAM policy which grants him access to S3.

NEW QUESTION 78
- (Topic 2)
A user has launched an ELB which has 5 instances registered with it. The user deletes the ELB by mistake. What will happen to the instances?

A. ELB will ask the user whether to delete the instances or not
B. Instances will be terminated
C. ELB cannot be deleted if it has running instances registered with it
D. Instances will keep running

Answer: D

Explanation:

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

NEW QUESTION 83
- (Topic 2)
An organization has setup consolidated billing with 3 different AWS accounts. Which of the below mentioned advantages will organization receive in terms of the AWS pricing?

A. The consolidated billing does not bring any cost advantage for the organization
B. All AWS accounts will be charged for S3 storage by combining the total storage of each account
C. The EC2 instances of each account will receive a total of 750*3 micro instance hours free
D. The free usage tier for all the 3 accounts will be 3 years and not a single year

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. For billing purposes, AWS treats all the accounts on the consolidated bill as one account. Some services, such as Amazon EC2 and Amazon S3 have volume pricing tiers across certain usage dimensions that give the user lower prices when he uses the service more.

NEW QUESTION 87
- (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 92
- (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 manuall
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. I t 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 96

- (Topic 2)
A user is planning to setup notifications on the RDS DB for a snapshot. Which of the below mentioned event categories is not supported by RDS for this snapshot source type?

A. Backup
B. Creation
C. Deletion
D. Restoration

Answer: A

Explanation:

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

NEW QUESTION 97
- (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 terminat
instances, respectively. Some other actions performed by Auto Scaling are:
AddToLoadbalancer,
AlarmNotification, HealthCheck, AZRebalance, ReplaceUnHealthy, and ScheduledActions.

NEW QUESTION 102
- (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 104
- (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 inflight requests continue to be served.

NEW QUESTION 108
- (Topic 2)
A user has launched an EBS backed instance. The user started the instance at 9 AM in the morning. Between 9 AM to 10 AM, the user is testing some script. Thus, he stopped the instance twice and restarted it. In the same hour the user rebooted the instance once. For how many instance hours will AWS charge the user?

A. 3 hours
B. 4 hours
C. 2 hours

D. 1 hour

Answer: A

Explanation:

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

NEW QUESTION 113
- (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 regio
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 114
- (Topic 2)
A user has configured the Auto Scaling group with the minimum capacity as 3 and the maximum capacity as 5. When the user configures the AS group, how many instances will Auto Scaling launch?

A. 3
B. 0
C. 5
D. 2

Answer: C

NEW QUESTION 115
- (Topic 2)
A user has created numerous EBS volumes. What is the general limit for each AWS account for the maximum number of EBS volumes that can be created?

A. 10000
B. 5000
C. 100
D. 1000

Answer: B

Explanation:

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

NEW QUESTION 118
- (Topic 2)
An organization is using AWS since a few months. The finance team wants to visualize the pattern of AWS spending. Which of the below AWS tool will help for this requirement?

A. AWS Cost Manager
B. AWS Cost Explorer
C. AWS CloudWatch
D. AWS Consolidated Billing

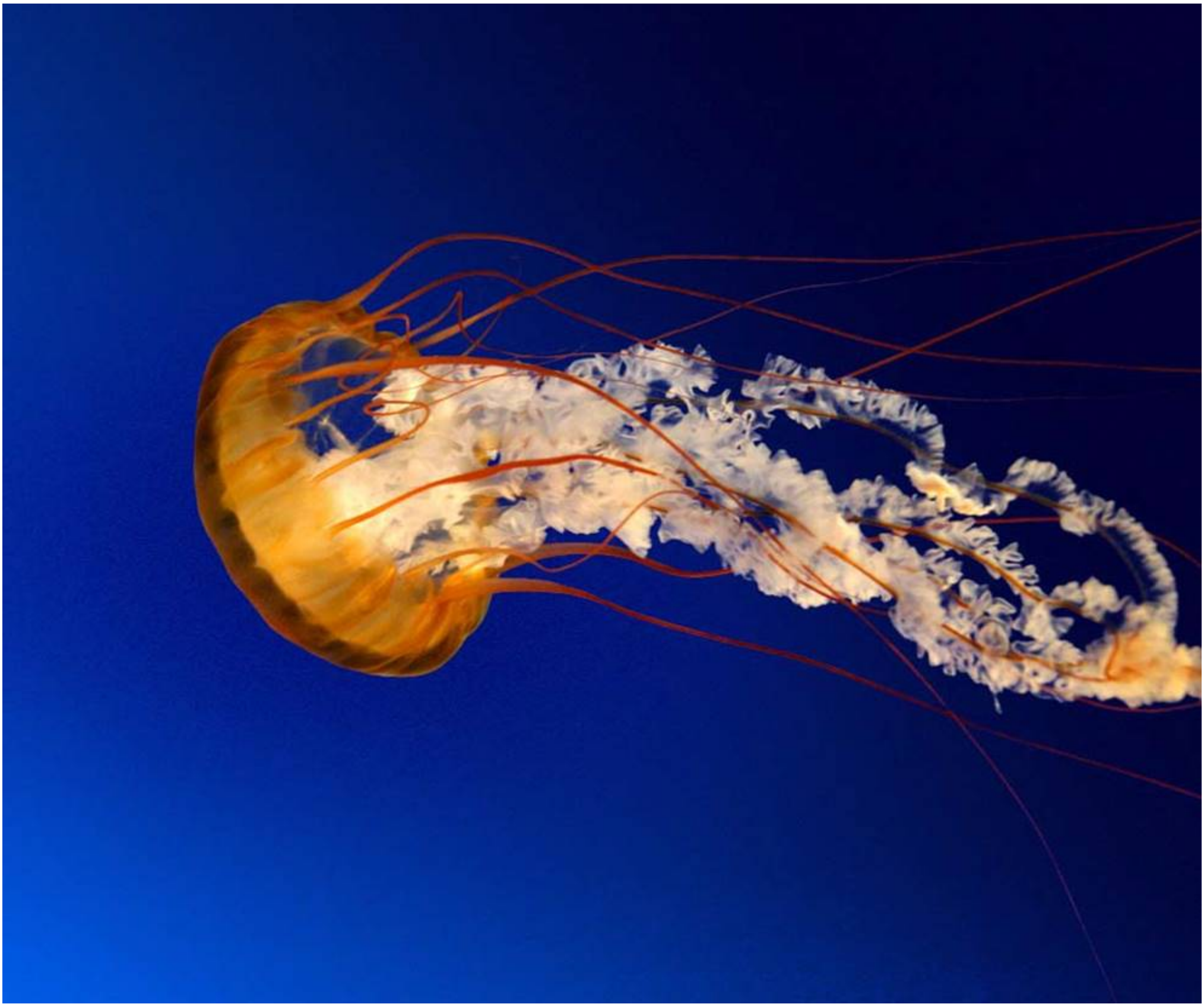
Answer: B

Explanation:

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

NEW QUESTION 123

- (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 125
- (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 the following transports as part of the subscription requests: “HTTP”, “HTTPS”,”Email”, “Email-JSON”, “SQS”, “and SMS”.

NEW QUESTION 130
- (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 135
- (Topic 2)
A system admin is planning to setup event notifications on RDS. Which of the below mentioned services will help the admin setup notifications?

A. AWS SES
B. AWS Cloudtrail
C. AWS Cloudwatch
D. AWS SNS

Answer: D

Explanation:

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

NEW QUESTION 139
- (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 ephermal 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 143
- (Topic 3)
A user has launched 5 instances in EC2-CLASSIC and attached 5 elastic IPs to the five different instances in the US East region. The user is creating a VPC in the same region. The user wants to assign an elastic IP to the VPC instance. How can the user achieve this?

A. The user has to request AWS to increase the number of elastic IPs associated with the account
B. AWS allows 10 EC2 Classic IPs per region; so it will allow to allocate new Elastic IPs to the same region
C. The AWS will not allow to create a new elastic IP in VPC; it will throw an error
D. The user can allocate a new IP address in VPC as it has a different limit than EC2

Answer: D

Explanation:
Section: (none)
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. A user can have 5 IP addresses per region with EC2 Classic. The user can have 5 separate IPs with VPC in the same region as it has a separate limit than EC2 Classic.

NEW QUESTION 144
- (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 149
- (Topic 3)
A user is sending the data to CloudWatch using the CloudWatch API. The user is sending data 90 minutes in the future. What will CloudWatch do in this case?

A. CloudWatch will accept the data
B. It is not possible to send data of the future
C. It is not possible to send the data manually to CloudWatch
D. The user cannot send data for more than 60 minutes in the future

Answer: A

Explanation:

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

NEW QUESTION 154
- (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 157
- (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 160
- (Topic 3)
Your mission is to create a lights-out datacenter environment, and you plan to use AWS OpsWorks to accomplish this. First you created a stack and added an App Server layer with an instance running in it. Next you added an application to the instance, and now you need to deploy a MySQL RDS database instance.
Which of the following answers accurately describe how to add a backend database server to an OpsWorks stack? Choose 3 answers

A. Add a new database layer and then add recipes to the deploy actions of the database and App Server layer
B. Use OpsWorks' "Clone Stack" feature to create a second RDS stack in another Availability Zone for redundancy in the event of a failure in the Primary A
C. To switch to the secondary RDS instance, set the [:database] attributes to values that are appropriate for your server which you can do by using custom JSO
D. The variables that characterize the RDS database connection—host, user, and so on—are set using the corresponding values from the deploy JSON's [:depioy][:app_name][:database] attribute
E. Cookbook attributes are stored in a repository, so OpsWorks requires that the "password": "your_password" attribute for the RDS instance must be encrypted using at least a 256-bit ke
F. Set up the connection between the app server and the RDS layer by using a custom recip
G. The recipe configures the app server as required, typically by creating a configuration fil
H. The recipe gets the connection data such as the host and database name from a set of attributes in the stack configuration and deployment JSON that AWS OpsWorks installs on every instanc

Answer: BCE

NEW QUESTION 162
- (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 165
- (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 170
- (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 private subnet database security group (DBSecGrp.?

A. Allow Inbound on port 3306 for Source Web Server Security Group (WebSecGr
B. Allow Inbound on port 3306 from source 20.0.0.0/16
C. Allow Outbound on port 3306 for Destination Web Server Security Group (WebSecGr
D. Allow Outbound on port 80 for Destination NAT Instance 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 to host the web server and DB server respectively, the user should configure that the instances in the private subnet can receive inbound traffic from the public subnet on the DB port. Thus, configure port 3306 in Inbound with the source as the Web Server Security Group (WebSecGrp.. The user should configure ports 80 and 443 for Destination 0.0.0.0/0 as the route table directs traffic to the NAT instance from the private subnet.

NEW QUESTION 172
- (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 andomness. 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 175
- (Topic 3)
An organization has configured Auto Scaling with ELB. One of the instance health check returns the status as Impaired to Auto Scaling. What will Auto Scaling do in this scenario?

A. Perform a health check until cool down before declaring that the instance has failed
B. Terminate the instance and launch a new instance
C. Notify the user using SNS for the failed state

D. Notify ELB to stop sending traffic to the impaired instance

Answer: B

Explanation:

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

NEW QUESTION 177
- (Topic 3)
A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?

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

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. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet.

NEW QUESTION 180
- (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 afolder, 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 182
- (Topic 3)
A user is collecting 1000 records per second. The user wants to send the data to CloudWatch using the custom namespace. Which of the below mentioned options is recommended for this activity?

A. Aggregate the data with statistics, such as Min, max, Average, Sum and Sample data and send the data to CloudWatch
B. Send all the data values to CloudWatch in a single command by separating them with a comm
C. CloudWatch will parse automatically
D. Create one csv file of all the data and send a single file to CloudWatch
E. It is not possible to send all the data in one cal
F. Thus, it should be sent one by on
G. CloudWatch will aggregate the data automatically

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. The user can publish data to CloudWatch as single data points or as an aggregated set of data points called a statistic set using the command put-metric-data. It is recommended that when the user is having multiple data points per minute, he should aggregate the data so that it will minimize the number of calls to put-metric-data. In this case it will be single call to CloudWatch instead of 1000 calls if the data is aggregated.

NEW QUESTION 186
- (Topic 3)
Which services allow the customer to retain run administrative privileges or the undertying 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 190
- (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 194
- (Topic 3)
A root account owner has given full access of his S3 bucket to one of the IAM users using the bucket ACL. When the IAM user logs in to the S3 console, which actions can he perform?

A. He can just view the content of the bucket
B. He can do all the operations on the bucket
C. It is not possible to give access to an IAM user using ACL
D. The IAM user can perform all operations on the bucket using only API/SDK

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 (IAM users. in his account.

NEW QUESTION 197
- (Topic 3)
A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AlarmNotification (which notifies Auto Scaling for CloudWatch alarms. process for a while. What will Auto Scaling do during this period?

A. AWS will not receive the alarms from CloudWatch
B. AWS will receive the alarms but will not execute the Auto Scaling policy
C. Auto Scaling will execute the policy but it will not launch the instances until the process is resumed
D. It is not possible to suspend the AlarmNotification process

Answer: B

Explanation:

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

NEW QUESTION 198
- (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 201
- (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 205
- (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 208
- (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 212
- (Topic 3)
A user is configuring a CloudWatch alarm on RDS to receive a notification when the CPU utilization of RDS is higher than 50%. The user has setup an alarm when there is some inactivity on RDS, such as RDS unavailability. How can the user configure this?

A. Setup the notification when the CPU is more than 75% on RDS
B. Setup the notification when the state is Insufficient Data
C. Setup the notification when the CPU utilization is less than 10%
D. It is not possible to setup the alarm on RDS

Answer: B

Explanation:

Amazon CloudWatch alarms watch a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The alarm has three states: Alarm, OK and Insufficient data. The Alarm will change to Insufficient Data when any of the three situations arise: when the alarm has just started, when the metric is not available or when enough data is not available for the metric to determine the alarm state. If the user wants to find that RDS is not available, he can setup to receive the notification when the state is in Insufficient data.

NEW QUESTION 217
- (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 219
- (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 222
- (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 225
- (Topic 3)
A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services provides detailed monitoring with CloudWatch without charging the user extra?

A. AWS Auto Scaling
B. AWS Route 53
C. AWS EMR
D. AWS SNS

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

NEW QUESTION 226
- (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 231
- (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 Deletion termination 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 232
- (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 235
- (Topic 3)
A user has created a VPC with the public subnet. The user has created a security group for that VPC. Which of the below mentioned statements is true when a security group is created?

A. It can connect to the AWS services, such as S3 and RDS by default
B. It will have all the inbound traffic by default
C. It will have all the outbound traffic by default
D. It will by default allow traffic to the internet gateway

Answer: C

Explanation:

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

NEW QUESTION 236
- (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 237
- (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 242
- (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 244
- (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 245
- (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 247
- (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 252
- (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 255
- (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
E. and Glacier (Archiv
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 257
- (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. The user has 3 elastic IPs and is trying to assign one of the Elastic IPs to the VPC instance from the console. The console does not show any instance in the IP assignment screen. What is a possible reason that the instance is unavailable in the assigned IP console?

A. The IP address may be attached to one of the instances
B. The IP address belongs to a different zone than the subnet zone
C. The user has not created an internet gateway
D. The IP addresses belong to EC2 Classic; so they cannot be assigned to VPC

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

NEW QUESTION 260
- (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, bydefault, associate the latest version of the ELBSecurityPolicy-YYYY-MM with the load balancer.

NEW QUESTION 262
- (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 264
- (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 265
- (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 269
- (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 273
- (Topic 3)
An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%. The higher CPU usage triggers an event for Auto Scaling as per the scaling policy. If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

A. Stop the scaling process until research is completed
B. It is not possible to find the root cause from that instance without triggering scaling
C. Delete Auto Scaling until research is completed
D. Suspend the scaling process until research is completed

Answer: D

Explanation:

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

NEW QUESTION 277
- (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 280
- (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 284
- (Topic 3)
A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned SSL protocols is not supported by the security policy?

A. TLS 1.3
B. TLS 1.2
C. SSL 2.0
D. SSL 3.0

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. Elastic Load Balancing supports the following versions of the SSL protocol: TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.0 SSL 2.0

NEW QUESTION 285
- (Topic 3)
A user has two EC2 instances running in two separate regions. The user is running an internal memory
management tool, which captures the data and sends it to CloudWatch in US East, using a CLI with the same namespace and metric. Which of the below mentioned options is true with respect to the above statement?

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

Answer: B

Explanation:

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

NEW QUESTION 289
- (Topic 3)
A user has created a queue named “awsmodule” with SQS. One of the consumers of queue is down for 3 days and then becomes available. Will that component receive message from queue?

A. Yes, since SQS by default stores message for 4 days
B. No, since SQS by default stores message for 1 day only
C. No, since SQS sends message to consumers who are available that time
D. Yes, since SQS will not delete message until it is delivered to all consumers

Answer: A

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. Queues retain messages for a set period of time. By default, a queue retains messages for four days. However, the user can configure a queue to retain messages for up to 14 days after the message has been sent.

NEW QUESTION 293
- (Topic 3)
A user is configuring the Multi AZ feature of an RDS DB. The user came to know that this RDS DB does not use the AWS technology, but uses server mirroring to achieve HA. Which DB is the user using right now?

A. My SQL
B. Oracle
C. MS SQL
D. PostgreSQL

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. Multi AZ deployments for Oracle, PostgreSQL, and MySQL DB instances use Amazon technology, while SQL Server (MS SQL. DB instances use SQL Server Mirroring.

NEW QUESTION 294
- (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 299
- (Topic 3)
A user is trying to launch an EBS backed EC2 instance under free usage. The user wants to achieve encryption of the EBS volume. How can the user encrypt the data at rest?

A. Use AWS EBS encryption to encrypt the data at rest
B. The user cannot use EBS encryption and has to encrypt the data manually or using a third party tool
C. The user has to select the encryption enabled flag while launching the EC2 instance
D. Encryption of volume is not available as a part of the free usage tier

Answer: B

Explanation:

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

NEW QUESTION 300
- (Topic 3)
In order to optimize performance for a compute cluster that requires low inter-node latency, which feature in the following list should you use?

A. AWS Direct Connect
B. Placement Groups
C. VPC private subnets
D. EC2 Dedicated Instances
E. Multiple Availability Zones

Answer: D

NEW QUESTION 305
- (Topic 3)
A user is trying to pre-warm a blank EBS volume attached to a Linux instance. Which of the below mentioned steps should be performed by the user?

A. There is no need to pre-warm an EBS volume

B. Contact AWS support to pre-warm
C. Unmount the volume before pre-warming
D. Format the device

Answer: C

Explanation:

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

NEW QUESTION 307
- (Topic 3)
A user has launched an EBS backed instance with EC2-Classic. The user stops and starts the instance. Which of the below mentioned statements is not true with respect to the stop/start action?

A. The instance gets new private and public IP addresses
B. The volume is preserved
C. The Elastic IP remains associated with the instance
D. The instance may run on a anew host computer

Answer: C

Explanation:

A user can always stop/start an EBS backed EC2 instance. When the user stops the instance, it first enters the stopping state, and then the stopped state. AWS does not charge the running cost but charges only for the EBS storage cost. If the instance is running in EC2-Classic, it receives a new private IP address; as the Elastic IP address (EIP. associated with the instance is no longer associated with that instance.

NEW QUESTION 308
- (Topic 3)
A user is displaying the CPU utilization, and Network in and Network out CloudWatch metrics data of a single instance on the same graph. The graph uses one Y-axis for CPU utilization and Network in and another Y-axis for Network out. Since Network in is too high, the CPU utilization data is not visible clearly on graph to the user. How can the data be viewed better on the same graph?

A. It is not possible to show multiple metrics with the different units on the same graph
B. Add a third Y-axis with the console to show all the data in proportion
C. Change the axis of Network by using the Switch command from the graph
D. Change the units of CPU utilization so it can be shown in proportion with Network

Answer: C

Explanation:

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

NEW QUESTION 313
- (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 317
- (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 320
- (Topic 3)
An organization is measuring the latency of an application every minute and storing data inside a file in the JSON format. The organization wants to send all latency data to AWS CloudWatch. How can the organization achieve this?

A. The user has to parse the file before uploading data to CloudWatch
B. It is not possible to upload the custom data to CloudWatch
C. The user can supply the file as an input to the CloudWatch command
D. The user can use the CloudWatch Import command to import data from the file to CloudWatch

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 has to always include the namespace as part of the request. If the user wants to upload the custom data from a Amazon AWS-SysOps : Practice Test file, he can supply file name along with the parameter -- metric-data to command put-metric-data.

NEW QUESTION 324
- (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 328
- (Topic 3)
A sys admin is using server side encryption with AWS S3. Which of the below mentioned statements helps the user understand the S3 encryption functionality?

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

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. The encryption with the user supplied key (SSE-C. does not work with the AWS console. The S3 does not store the keys and the user has to send a key with each request. The SSE-C works when the user has enabled versioning.

NEW QUESTION 332
- (Topic 3)
A user has launched a Windows based EC2 instance. However, the instance has some issues and the user wants to check the log. When the user checks the Instance console output from the AWS console, what will it display?

A. All the event logs since instance boot
B. The last 10 system event log error
C. The Windows instance does not support the console output
D. The last three system events' log errors

Answer: D

Explanation:

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

NEW QUESTION 337
- (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 340
- (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 344
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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 FirstTry

* AWS-SysOps Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year