Amazon AWS-SysOps

AWS Certified SysOps Administrator – Associate

Topic 1, Volume A

QUESTION NO: 1

You are currently hosting multiple applications in a VPC and have logged numerous port scans coming in from a specific IP address block. Your security team has requested that all access from the offending IP address block be denied tor the next 24 hours.

Which of the following is the best method to quickly and temporarily deny access from the specified IP address block?

A. Create an AD policy to modify Windows Firewall settings on all hosts in the VPC to deny access from the IP address block
B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP address block
C. Add a rule to all of the VPC 5 Security Groups to deny access from the IP address block
D. Modify the Windows Firewall settings on all Amazon Machine Images (AMIs) that your organization uses in that VPC to deny access from the IP address block

Answer: C
Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

QUESTION NO: 2

When preparing for a compliance assessment of your system built inside of AWS. what are three best-practices for you to prepare for anaudit?

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: B,D,E
Explanation:

QUESTION NO: 3

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
Explanation:

QUESTION NO: 4

You have been asked to leverage Amazon VPC BC2 and SOS to implement an application that submits and receives millions of messages per second to a message queue. You want to ensure your application has sufficient bandwidth between your EC2 instances and SQS

Which option will provide (he most scalable solution for communicating between the application and SOS?

A. Ensure the application instances are properly configured with an Elastic Load Balancer
B. Ensure the application instances are launched in private subnets with the EBS-optimized option enabled
C. Ensure the application instances are launched in public subnets with the associate-public-IP-address=true option enabled
D. Launch application instances in private subnets with an Auto Scaling group and Auto Scaling triggers configured to watch the SOS queue size

Answer: C
Reference:

http://www.cardinalpath.com/autoscaling-your-website-with-amazon-web-services-part-2/

QUESTION NO: 5

You have identified network throughput as a bottleneck on your ml small EC2 instance when uploading data Into Amazon S3 In the same region.

How do you remedy this situation?

A. Add an additional ENI
B. Change to a larger Instance
C. Use DirectConnect between EC2 and S3
D. Use EBS PIOPS on the local volume

Answer: B
Reference:

https://media.amazonwebservices.com/AWS_Amazon_EMR_Best_Practices.pdf

QUESTION NO: 6

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: C,D
Explanation:

QUESTION NO: 7

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 limits.
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
Explanation:

QUESTION NO: 8

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

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

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

Answer: B
Explanation:
Reference:

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

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

For information about EC2 instance status checks, see Monitor Instances With Status Checks in

the Amazon EC2 User Guide for Linux Instances. For information about Elastic Load Balancing health checks, see Health Check in the Elastic Load Balancing Developer Guide.

This topic shows you how to add an Elastic Load Balancing health check to your Auto Scaling

group, assuming that you have created a load balancer and have registered the load balancer with your Auto Scaling group. If you have not registered the load balancer with your Auto Scaling group, see Set Up a Scaled and Load-Balanced Application.

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

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

QUESTION NO: 9

Which two AWS services provide out-of-the-box user configurable automatic backup-as-a-service and backup rotation options?

Choose 2 answers

A. Amazon S3
B. Amazon RDS
C. Amazon EBS
D. Amazon Red shift

Answer: C,D
Explanation:

QUESTION NO: 10

An organization has configured a VPC with an Internet Gateway (IGW). pairs of public and private subnets (each with one subnet per Availability Zone), and an Elastic Load Balancer (ELB) configured to use the public subnets The application s web tier leverages the ELB. Auto Scaling and a mum-AZ RDS database instance The organization would like to eliminate any potential

single points ft failure in this design.

What step should you take to achieve this organization's objective?

A. Nothing, there are no single points of failure in this architecture.
B. Create and attach a second IGW to provide redundant internet connectivity.
C. Create and configure a second Elastic Load Balancer to provide a redundant load balancer.
D. Create a second multi-AZ RDS instance in another Availability Zone and configurereplication to provide a redundant database.

Answer: C
Explanation:

QUESTION NO: 11

Which of the following are characteristics of Amazon VPC subnets?

Choose 2 answers

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

Answer: C,E
Explanation:

QUESTION NO: 12

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: B
Explanation:

QUESTION NO: 13

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

A. Data is automatically saved as an E8S volume.
B. Data is automatically saved as an ESS snapshot.
C. Data is automatically deleted.
D. Data is unavailable until the instance is restarted.

Answer: D
Explanation:
Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html

QUESTION NO: 14

You have a web application leveraging an Elastic Load Balancer (ELB) In front of the web servers deployed using an Auto Scaling Group Your database is running on Relational Database Service (RDS) The application serves out technical articles and responses to them in general there are more views of an article than there are responses to the article. On occasion, an article on the site becomes extremely popular resulting in significant traffic Increases that causes the site to go down.

What could you do to help alleviate the pressure on the infrastructure while maintaining availability during these events?

Choose 3 answers

A. Leverage CloudFront for the delivery of the articles.
B. Add RDS read-replicas for the read traffic going to your relational database
C. Leverage ElastiCache for caching the most frequently used data.

D. Use SOS to queue up the requests for the technical posts and deliver them out of the queue.
E. Use Route53 health checks to fail over to an S3 bucket for an error page.

Answer: A,C,E
Explanation:

QUESTION NO: 15

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

What option would you implement to successfully launch this application1?

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

Answer: D
Explanation:
Reference:

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

QUESTION NO: 16

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

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

A. One public subnet for ELB one public subnet for the web-servers, and one private subnet for the database

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

Answer: A
Explanation:

QUESTION NO: 17

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

How can you accomplish this?

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

Answer: C
Explanation:

QUESTION NO: 18

When assessing an organization s use of AWS API access credentials which of the following three credentials should be evaluated?

Choose 3 answers

A. Key pairs
B. Console passwords

C. Access keys
D. Signing certificates
E. Security Group memberships

Answer: A,C,D
Explanation:
Reference:

http://media.amazonwebservices.com/AWS_Operational_Checklists.pdf

QUESTION NO: 19

You have a Linux EC2 web server instance running inside a VPC The instance is In a public subnet and has an EIP associated with it so you can connect to It over the Internet via HTTP or SSH The instance was also fully accessible when you last logged in via SSH. and was also serving web requests on port 80.

Now you are not able to SSH into the host nor does it respond to web requests on port 80 that were working fine last time you checked You have double-checked that all networking configuration parameters (security groups route tables. IGW'EIP. NACLs etc) are properly configured {and you haven't made any changes to those anyway since you were last able to reach the Instance). You look at the EC2 console and notice that system status check shows "impaired."

Which should be your next step in troubleshooting and attempting to get the instance back to a healthy state so that you can log in again?

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

Answer: B
Explanation:

QUESTION NO: 20

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: C
Explanation:
Reference:

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

QUESTION NO: 21

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 monitoringinstance 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
Explanation:

QUESTION NO: 22

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

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

Choose 2 answers

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

Answer: A,C
Explanation:

QUESTION NO: 23

Which services allow the customer to retain full administrative privileges of the underlying EC2 instances?

Choose 2 answers

A. Amazon Elastic Map Reduce
B. Elastic Load Balancing
C. AWS Elastic Beanstalk
D. I" Amazon Elasticache
E. Amazon Relational Database service

Answer: B,C
Explanation:

QUESTION NO: 24

You have a web-style application with a stateless but CPU and memory-intensive web tier running

on a cc2 8xlarge EC2 instance inside of a VPC The instance when under load is having

problems returning requests within the SLA as defined by your business The application maintains its state in a DynamoDB table, but the data tier is properly provisioned and responses are consistently fast.

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

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

Answer: B
Explanation:
Reference:

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

QUESTION NO: 25

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

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

Choose 2 answers

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

Answer: A,D
Explanation:

QUESTION NO: 26

You are designing a system that has a Bastion host. This component needs to be highly available

without human intervention.

Which of the following approaches would you select?

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

Answer: C
Explanation:

QUESTION NO: 27

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

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

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

Answer: C
Explanation:

QUESTION NO: 28

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 EC2mstance

Answer: B
Explanation:
Reference:

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

QUESTION NO: 29

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: C
Explanation:

QUESTION NO: 30

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

Which configuration would achieve that goal?

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

Answer: D
Explanation:
Reference:

http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyCo
ncepts.html

QUESTION NO: 31

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

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

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

notifications when it hits 50%. 80% and 90% of its budgeted monthly spend

Answer: C

Explanation:

QUESTION NO: 32

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

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

Answer: C
Explanation:
Reference:

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

QUESTION NO: 33

You are using ElastiCache Memcached to store session state and cache database queries in your infrastructure You notice in Cloud Watch that Evictions and GetMisses are Doth very high.

What two actions could you take to rectify this?

Choose 2 answers

A. Increase the number of nodes in your cluster
B. Tweak the max-item-size parameter
C. Shrink the number of nodes in your cluster
D. Increase the size of the nodes in the duster

Answer: B,D
Explanation:

QUESTION NO: 34

You are running a database on an EC2 instance, with the data stored on Elastic Block Store (EBS) for persistence At times throughout the day, you are seeing large variance in the response times of the database queries Looking into the instance with the isolate command you see a lot of wait time on the disk volume that the database's data is stored on.

What two ways can you improve the performance of the database's storage while maintaining the current persistence of the data?

Choose 2 answers

A. Move to an SSD backed instance
B. Move the database to an EBS-Optimized Instance
C. T Use Provisioned IOPs EBS
D. Use the ephemeral storage on an m2 4xiarge Instance Instead

Answer: A,B
Explanation:

QUESTION NO: 35

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

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

A. Run another monitoring instance that pings the monitoring instance and fires a could watch alarm mat notifies your operations teamshould the primary monitoring instance become unhealthy.
B. Set a Cloud Watch alarm based on EC2 system and instance status checks and have the alarm notify your operations team of anydetected problem with the monitoring instance.
C. Set a Cloud Watch alarm based on the CPU utilization of the monitoring instance and nave the alarm notify your operations team if C r the CPU usage exceeds 50% few more than one minute: then have your monitoring application go into a CPU-bound loop should itDetect any application problems.
D. Have the monitoring instances post messages to an SOS queue and then dequeue those messages on another instance should D c- the queue cease to have new messages, the second instance should first terminate the original monitoring instance start anotherbackup monitoring instance and assume (he role of the previous monitoring instance and beginning adding messages to the SOSqueue.

Answer: D
Explanation:

QUESTION NO: 36

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: B
Explanation:
Reference:

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

QUESTION NO: 37

You are attempting to connect to an instance in Amazon VPC without success You have already verified that the VPC has an Internet Gateway (IGW) the instance has an associated Elastic IP (EIP) and correct security group rules are in place.

Which VPC component should you evaluate next?

A. The configuration of a MAT instance
B. The configuration of the Routing Table
C. The configuration of the internet Gateway (IGW)
D. The configuration of SRC'DST checking

Answer: C
Explanation:
Reference:

http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/UserScenariosForVPC.

html

QUESTION NO: 38

You are tasked with the migration of a highly trafficked Node JS application to AWS In order to comply with organizational standards Chef recipes must be used to configure the application servers that host this application and to support application lifecycle events.

Which deployment option meets these requirements while minimizing administrative burden?

A. Create a new stack within Opsworks add the appropriate layers to the stack and deploy the application
B. Create a new application within Elastic Beanstalk and deploy this application to a new environment
C. Launch a Mode JS server from a community AMI and manually deploy the application to the launched EC2 instance
D. Launch and configure Chef Server on an EC2 instance and leverage the AWS CLI to launch application servers and configure those instances using Chef.

Answer: B
Explanation:
Reference:

http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deployment.html

QUESTION NO: 39

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

Which task would be best accomplished with a script?

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

Answer: C
Explanation:

QUESTION NO: 40

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: C,D
Explanation:

QUESTION NO: 41

What are characteristics of Amazon S3?

Choose 2 answers

A. Objects are directly accessible via a URL
B. S3 should be used to host a relational database
C. S3 allows you to store objects or virtually unlimited size
D. S3 allows you to store virtually unlimited amounts of data
E. S3 offers Provisioned IOPS

Answer: B,C
Explanation:

QUESTION NO: 42

You receive a frantic call from a new DBA who accidentally dropped a table containing all your customers.

Which Amazon RDS feature will allow you to reliably restore your database to within 5 minutes of when the mistake was made?

A. Multi-AZ RDS

B. RDS snapshots
C. RDS read replicas
D. RDS automated backup

Answer: B
Explanation:
Reference:

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.BackingUpAndRestoringAm
azonRDSInstances.html

QUESTION NO: 43

A media company produces new video files on-premises every day with a total size of around
100GBS after compression All files have a size of 1 -2 GB and need to be uploaded to Amazon
S3 every night in a fixed time window between 3am and 5am Current upload takes almost 3
hours, although less than half of the available bandwidth is used.

What step(s) would ensure that the file uploads are able to complete in the allotted time window?

A. Increase your network bandwidth to provide faster throughput to S3
B. Upload the files in parallel to S3
C. Pack all files into a single archive, upload it to S3, then extract the files in AWS
D. Use AWS Import/Export to transfer the video files

Answer: D
Explanation:
Reference:

http://aws.amazon.com/importexport/faqs/

QUESTION NO: 44

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 ELB. RDS and EC2 instances

Answer: B
Explanation:

QUESTION NO: 45

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: B,C
Explanation:

QUESTION NO: 46

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

data on Amazon S3.

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

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

Answer: C
Explanation:

QUESTION NO: 47

You are tasked with setting up a cluster of EC2 Instances for a NoSOL database The database requires random read 10 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 (hil 4xiarge) 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: B
Reference:

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

QUESTION NO: 48

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 volume.
C. Data Is automatically saved as an E8S snapshot
D. Data is unavailable until the instance is restarted

Answer: D
Explanation:

QUESTION NO: 49

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

Which approach addresses this requirement?

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

Answer: B
Reference:

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

QUESTION NO: 50

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 **28** 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
Reference:

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

QUESTION NO: 51

Your company Is moving towards tracking web page users with a small tracking Image loaded on each page Currently you are serving this image out of US-East, but are starting to get concerned about the time It takes to load the image for users on the west coast.

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

Choose 2 answers

A. Use Route 53's Latency Based Routing and serve the image out of US-West-2 as well as US-East-1
B. Serve the image out through CloudFront
C. Serve the image out of S3 so that it isn't being served oft of your web application tier
D. Use EBS PIOPs to serve the image faster out of your EC2 instances

Answer: A,B
Explanation:

QUESTION NO: 52

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

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

already
E. Launch the Instance from a private Amazon Machine image (Mil)

Answer: C
Reference:

QUESTION NO: 53

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

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

Choose 2 answers

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

Answer: B,D
Explanation:

QUESTION NO: 54

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

A. The IP of the primary DB instance is switched to the standby OB instance
B. The RDS (Relational Database Service) DB instance reboots
C. A new DB instance is created in the standby availability zone

D. The canonical name record (CNAME) is changed from primary to standby

Answer: B
Explanation:

QUESTION NO: 55

How can the domain's zone apex for example "myzoneapexdomain com" be pointed towards an Elastic Load Balancer?

A. By using an AAAA record
B. By using an A record
C. By using an Amazon Route 53 CNAME record
D. By using an Amazon Route 53 Alias record

Answer: C
Reference:

http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

Topic 2, Volume B

QUESTION NO: 56

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

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

Answer: C
Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage

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

QUESTION NO: 57

A user is planning to evaluate AWS for their internal use. The user does not want to incur any charge on his account during the evaluation. Which of the below mentioned AWS services would incur a charge if used?

A. AWS S3 with 1 GB of storage
B. AWS micro instance running 24 hours daily
C. AWS ELB running 24 hours a day
D. AWS PIOPS volume of 10 GB size

Answer: D
Explanation:

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

QUESTION NO: 58

A user has developed an application which is required to send the data to a NoSQL database. The user wants to decouple the data sending such that the application keeps processing and sending data but does not wait for an acknowledgement of DB. Which of the below mentioned applications helps in this scenario?

A. AWS Simple Notification Service
B. AWS Simple Workflow
C. AWS Simple Queue Service

D. AWS Simple Query Service

Answer: C
Explanation:

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

QUESTION NO: 59

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

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

Answer: A
Explanation:

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

QUESTION NO: 60

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

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

Answer: D
Explanation:

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

QUESTION NO: 61

A user has recently started using EC2. The user launched one EC2 instance in the default subnet in EC2-VPC Which of the below mentioned options is not attached or available with the EC2 instance when it is launched?

A. Public IP address
B. Internet gateway
C. Elastic IP
D. Private IP address

Answer: C
Explanation:

A Virtual Private Cloud (VPC. is a virtual network dedicated to a user's AWS account. A subnet is a range of IP addresses in the VPC. The user can launch the AWS resources into a subnet. There are two supported platforms into which a user can launch instances: EC2-Classic and EC2-VPC

(default subnet.. A default VPC has all the benefits of EC2-VPC and the ease of use of EC2-Classic. Each instance that the user launches into a default subnet has a private IP address and a public IP address. These instances can communicate with the internet through an internet gateway. An internet gateway enables the EC2 instances to connect to the internet through the Amazon EC2 network edge.

QUESTION NO: 62

A user has launched an EC2 instance. The user is planning to setup the CloudWatch alarm. Which of the

below mentioned actions is not supported by the CloudWatch alarm?

A. Notify the Auto Scaling launch config to scale up
B. Send an SMS using SNS
C. Notify the Auto Scaling group to scale down
D. Stop the EC2 instance

Answer: B
Explanation:

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

QUESTION NO: 63

A user is trying to delete an Auto Scaling group from CLI. Which of the below mentioned steps are to be performed by the user?

A. Terminate the instances with the ec2-terminate-instance command
B. Terminate the Auto Scaling instances with the as-terminate-instance command
C. Set the minimum size and desired capacity to 0
D. There is no need to change the capacity. Run the as-delete-group command and it will reset all values to 0

Answer: C
Explanation:

If the user wants to delete the Auto Scaling group, the user should manually set the values of the minimum and desired capacity to 0. Otherwise Auto Scaling will not allow for the deletion of the group from CLI. While trying from the AWS console, the user need not set the values to 0 as the Auto Scaling console will automatically do so.

QUESTION NO: 64

An organization is planning to create 5 different AWS accounts considering various security requirements. The organization wants to use a single payee account by using the consolidated billing option. Which of the below mentioned statements is true with respect to the above information?

A. Master (Payee. account will get only the total bill and cannot see the cost incurred by each account
B. Master (Payee. account can view only the AWS billing details of the linked accounts
C. It is not recommended to use consolidated billing since the payee account will have access to the linked accounts
D. 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.

QUESTIONNO: 10
A user has deployed an application on his private cloud. The user is using his own monitoring tool. He wants to configure that whenever there is an error, the monitoring tool should notify him via

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

A. None because the user infrastructure is in the private cloud/
B. AWS SNS
C. AWS SES
D. AWS SMS

Answer: B

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

QUESTION NO: 65

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

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

Answer: B
Explanation:

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

QUESTION NO: 66

A user has setup a CloudWatch alarm on an EC2 action when the CPU utilization is above 75%.
The alarm sends a notification to SNS on the alarm state. If the user wants to simulate the alarm
action how can he achieve this?

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

Answer: C
Explanation:

Amazon CloudWatch alarms watch a single metric over a time period that the user specifies and
performs one or more actions based on the value of the metric relative to a given threshold over
a number of time periods.The user can test an alarm by setting it to any state using the
SetAlarmState API (mon-set-alarm-state command.. This temporary state change lasts only until
the next alarm comparison occurs.

QUESTION 13

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

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

Answer: A

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

QUESTION NO: 67

A user has setup a billing alarm using CloudWatch for $200. The usage of AWS exceeded $200 after some days. The user wants to increase the limit from $200 to $400? What should the user do?

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

Answer: C
Explanation:

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

QUESTION NO: 68

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

"Statement": [{

"Sid": "Stmt1388811069831",

"Effect": "Allow",

"Principal": { "AWS": "*"},

"Action": ["s3:GetObjectAcl", "s3:ListBucket", "s3:GetObject"],

"Resource": ["arn:aws:s3:::cloudacademy/*.jpg"]

}]

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

Answer: A
Explanation:

A system admin can grant permission to the S3 objects or buckets to any user or make objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if the user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket. It cannot be applied at the object level.

QUESTION NO: 69

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

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

Answer: B
Explanation:

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

QUESTION NO: 70

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

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

Answer: A
Explanation:

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

QUESTION NO: 71

An organization is planning to use AWS for their production roll out. The organization wants to implement

automation for deployment such that it will automatically create a LAMP stack, download the latest PHP

installable from S3 and setup the ELB. Which of the below mentioned AWS services meets the quirement for making an orderly deployment of the software?

A. AWS Elastic Beanstalk
B. AWS Cloudfront
C. AWS Cloudformation
D. AWS DevOps

Answer: C
Explanation:

AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. Cloudformation provides an easy way to create and delete the collection of related AWS resources and provision them in an orderly way. AWS CloudFormation automates and simplifies the task of repeatedly and predictably creating groups of related resources that power the user's applications. AWS Cloudfront is a CDN; Elastic Beanstalk does quite a few of the required tasks. However, it is a PAAS which uses a ready AMI. AWS Elastic Beanstalk provides an environment to easily develop and run applications in the cloud.

QUESTION NO: 72

A user has created a subnet with VPC and launched an EC2 instance in that subnet with only default settings.Which of the below mentioned options is ready to use on the EC2 instance as soon as it is launched?

A. Elastic IP
B. Private IP
C. Public IP
D. I nternet gateway

Answer: B
Explanation:

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

QUESTION NO: 73

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

programmatic access?

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

Answer: C
Explanation:

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

QUESTION NO: 74

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
Explanation:

When the user configures the launch configuration and the Auto Scaling group, the Auto Scaling group will start instances by launching the minimum number (or the desired number, if specified. of EC2 instances. If there are no other scaling conditions attached to the Auto Scaling group, it will maintain the minimum number of running instances at all times.

QUESTION NO: 75

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

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

Answer: B
Explanation:

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

QUESTION NO: 76

A user is planning to use AWS Cloudformation. Which of the below mentioned functionalities does not help him to correctly understand Cloudfromation?

A. Cloudformation follows the DevOps model for the creation of Dev & Test
B. AWS Cloudfromation does not charge the user for its service but only charges for the AWS resources
created with it
C. Cloudformation works with a wide variety of AWS services, such as EC2, EBS, VPC, IAM, S3, RDS,
ELB, etc
D. CloudFormation provides a set of application bootstrapping scripts which enables the user to install
Software

Answer: A
Explanation:

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

QUESTION NO: 77

A user has launched 10 instances from the same AMI ID using Auto Scaling. The user is trying to see the

average CPU utilization across all instances of the last 2 weeks under the CloudWatch console. How can the user achieve this?

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

Answer: B
Explanation:

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

QUESTION NO: 78

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".

QUESTION NO: 79

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.

QUESTION NO: 80

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

QUESTION NO: 81

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

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

Answer: B
Explanation:

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

QUESTION NO: 82

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

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

Answer: B
Explanation:

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

QUESTION NO: 83

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

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

Answer: C
Explanation:

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

QUESTION NO: 84

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

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

Answer: A
Explanation:

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

QUESTION NO: 85

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

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

C. Folders can have a policy
D. Both the object and bucket can have ACL but folders cannot have ACL

Answer: A
Explanation:

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

QUESTION NO: 86

A user has created an ELB with three instances. How many security groups will ELB create by default?

A. 3
B. 5
C. 2
D. 1

Answer: C
Explanation:

Elastic Load Balancing provides a special Amazon EC2 source security group that the user can use to ensure that back-end EC2 instances receive traffic only from Elastic Load Balancing. This feature needs two security groups: the source security group and a security group that defines the ingress rules for the back-end instances. To ensure that traffic only flows between the load balancer and the back-end instances, the user can add or modify a rule to the back-end security group which can limit the ingress traffic. Thus, it can come only from the source security group provided by Elastic load Balancing.

QUESTION NO: 87

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

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

Answer: D
Explanation:

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

QUESTION NO: 88

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.

QUESTION NO: 89

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.

QUESTION NO: 90

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

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

Answer: B
Explanation:

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

QUESTION NO: 91

A user has created an S3 bucket which is not publicly accessible. The bucket is having thirty objects which are also private. If the user wants to make the objects public, how can he configure this with minimal efforts?

A. The user should select all objects from the console and apply a single policy to mark them public
B. The user can write a program which programmatically makes all objects public using S3 SDK
C. Set the AWS bucket policy which marks all objects as public
D. Make the bucket ACL as public so it will also mark all objects as public

Answer: C
Explanation:

A system admin can grant permission of the S3 objects or buckets to any user or make the objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if the user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket.

QUESTION NO: 92

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.

QUESTION NO: 93

An organization, which has the AWS account ID as 999988887777, has created 50 IAM users. All the users are added to the same group cloudacademy. If the organization has enabled that each IAM user can login with the AWS console, which AWS login URL will the IAM users use?

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

Answer: A
Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Once the organization has created the IAM users, they will have a separate AWS console URL to login to the AWS console. The console login URL for the IAM user will be https:// AWS_Account_ID.signin.aws.amazon.com/console/. It uses

only the AWS account ID and does not depend on the group or user ID.

QUESTION NO: 94

A user has setup connection draining with ELB to allow in-flight requests to continue while the instance is being deregistered through Auto Scaling. If the user has not specified the draining time, how long will ELB allow inflight requests traffic to continue?

A. 600 seconds
B. 3600 seconds
C. 300 seconds
D. 0 seconds

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. The user can specify a maximum time (3600 seconds. for the load balancer to keep the connections alive before reporting the instance as deregistered. If the user does not specify the maximum timeout period, by default, the load balancer will close the connections to the deregistering instance after 300 seconds.

QUESTION NO: 95

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.

QUESTION NO: 96

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

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

Answer: C
Explanation:

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

QUESTION NO: 97

A user has configured ELB with three instances. The user wants to achieve High Availability as well as

redundancy with ELB. Which of the below mentioned AWS services helps the user achieve this for

ELB?

A. Route 53
B. AWS Mechanical Turk
C. Auto Scaling
D. AWS EMR

Answer: A
Explanation:

The user can provide high availability and redundancy for applications running behind Elastic Load Balancer by enabling the Amazon Route 53 Domain Name System (DNS. failover for the load balancers. Amazon Route 53 is a DNS service that provides reliable routing to the user's infrastructure.

QUESTION NO: 98

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.

QUESTION NO: 99

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.

QUESTION NO: 100

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.

QUESTION NO: 101

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

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

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

Answer: B
Explanation:

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

QUESTION NO: 102

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.

QUESTION NO: 103

A user is accessing RDS from an application. The user has enabled the Multi AZ feature with the

MS SQL RDS DB. During a planned outage how will AWS ensure that a switch from DB to a standby replica will not affect access to the application?

A. RDS will have an internal IP which will redirect all requests to the new DB
B. RDS uses DNS to switch over to stand by replica for seamless transition
C. The switch over changes Hardware so RDS does not need to worry about access
D. RDS will have both the DBs running independently and the user has to manually switch over

Answer: B
Explanation:

In the event of a planned or unplanned outage of a DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone if the user has enabled Multi AZ. The automatic failover mechanism simply changes the DNS record of the DB instance to point to the standby DB instance. As a result, the user will need to re-establish any existing connections to the DB instance. However, as the DNS is the same, the application can access DB seamlessly.

QUESTION NO: 104

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.

QUESTION NO: 105

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.

QUESTION NO: 106

An organization has configured the custom metric upload with CloudWatch. The organization has given permission to its employees to upload data using CLI as well SDK. How can the user track the calls made to CloudWatch?

A. The user can enable logging with CloudWatch which logs all the activities
B. Use CloudTrail to monitor the API calls
C. Create an IAM user and allow each user to log the data using the S3 bucket
D. Enable detailed monitoring with CloudWatch

Answer: B

Explanation:

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

QUESTION NO: 107

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 manually. AWS deletes it after 30 days of inactivity on queue
B. It will delete the queue
C. It will initiate the delete but wait for four days before deleting until all messages are deleted automatically.
D. 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.

QUESTION NO: 108

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

How can the user achieve DR?

A. Copy the running instance using the "Instance Copy" command to the EU region

B. Create an AMI of the instance and copy the AMI to the EU region. Then launch the instance from the EU AMI

C. Copy the instance from the US East region to the EU region

D. 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.

QUESTION NO: 109

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.

QUESTION NO: 110

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.

QUESTION NO: 111

A user has stored data on an encrypted EBS volume. The user wants to share the data with his friend's AWS account. How can user achieve this?

A. Create an AMI from the volume and share the AMI
B. Copy the data to an unencrypted volume and then share
C. Take a snapshot and share the snapshot with a friend
D. If both the accounts are using the same encryption key then the user can share the volume directly

Answer: B
Explanation:

AWS EBS supports encryption of the volume. It also supports creating volumes from existing snapshots

provided the snapshots are created from encrypted volumes. If the user is having data on an encrypted volume and is trying to share it with others, he has to copy the data from the encrypted volume to a new unencrypted volume. Only then can the user share it as an encrypted volume data. Otherwise the snapshot cannot be shared.

QUESTION NO: 112

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

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

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

Answer: C
Explanation:

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.Note that the high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a read replica.

QUESTION NO: 113

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

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

Answer: D
Explanation:

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

QUESTION NO: 114

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

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

Answer: B
Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and

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

QUESTION NO: 115

A user is launching an EC2 instance in the US East region. Which of the below mentioned options is

recommended by AWS with respect to the selection of the availability zone?

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

Answer: B
Explanation:

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

QUESTION NO: 116

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

A. Allow Inbound traffic on port 22 from the user's network
B. The user has to create an instance in EC2 Classic with an elastic IP and configure the security group
of a private subnet to allow SSH from that elastic IP

C. The user can connect to a instance in a private subnet using the NAT instance
D. Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the Internet

Answer: A
Explanation:

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

QUESTION NO: 117

A user has created an ELB with the availability zone US-East-1A. The user wants to add more zones to ELB to achieve High Availability. How can the user add more zones to the existing ELB?

A. It is not possible to add more zones to the existing ELB
B. The only option is to launch instances in different zones and add to ELB
C. The user should stop the ELB and add zones and instances as required
D. The user can add zones on the fly from the AWS console

Answer: D
Explanation:

The user has created an Elastic Load Balancer with the availability zone and wants to add more zones to the existing ELB. The user can do so in two ways:
From the console or CLI, add new zones to ELB;
Launch instances in a separate AZ and add instances to the existing ELB.

QUESTION NO: 118

A user has configured an Auto Scaling group with ELB. The user has enabled detailed CloudWatch monitoring on Elastic Load balancing. Which of the below mentioned statements will help the user understand this functionality better?

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

Answer: A
Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed
monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Elastic Load Balancing includes 10 metrics and 2 dimensions, and sends data to CloudWatch every minute. This does not cost extra.

QUESTION NO: 119

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

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

Answer: D
Explanation:

Elastic Load Balancing supports both Internet Protocol version 6 (IPv6. and Internet Protocol version 4 (IPv4.. Clients can connect to the user's load balancer using either IPv4 or IPv6 (in EC2-Classic. DNS. However, communication between the load balancer and its back-end instances uses only IPv4. The user can use the Dualstack-prefixed DNS name to enable IPv6 support for

communications between the client and the load balancers. Thus, the clients are able to access the load balancer using either IPv4 or IPv6 as their individual connectivity needs dictate.

QUESTION NO: 120

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

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

QUESTION NO: 121

A user has setup Auto Scaling with ELB on the EC2 instances. The user wants to configure that whenever the CPU utilization is below 10%, Auto Scaling should remove one instance. How can the user configure this?

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

B. Use CloudWatch to monitor the data and Auto Scaling to remove the instances

using scheduled
actions
C. Configure CloudWatch to send a notification to Auto Scaling Launch configuration when the CPU
utilization is less than 10% and configure the Auto Scaling policy to remove the instance
D. Configure CloudWatch to send a notification to the Auto Scaling group when the CPU Utilization is
less than 10% and configure the Auto Scaling policy to remove the instance

Answer: D
Explanation:

Amazon CloudWatch alarms watch a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup to receive a notification on the Auto Scaling group with the CloudWatch alarm when the CPU utilization is below a certain threshold. The user can configure the Auto Scaling policy to take action for removing the instance. When the CPU utilization is below 10% CloudWatch will send an alarm to the Auto Scaling group to execute the policy.

QUESTION NO: 122

A user has enabled detailed CloudWatch metric monitoring on an Auto Scaling group. Which of the below

mentioned metrics will help the user identify the total number of instances in an Auto Scaling group cluding pending, terminating and running instances?

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

Answer: A
Explanation:

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

QUESTION NO: 123

A user is trying to configure the CloudWatch billing alarm. Which of the below mentioned steps should be

performed by the user for the first time alarm creation in the AWS Account Management section?

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

Answer: B
Explanation:

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

QUESTION NO: 124

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 72 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.

QUESTION NO: 125

An organization (Account ID 123412341234. has attached the below mentioned IAM policy to a
user. What does this policy statement entitle the user to perform?

"Statement": [

{

"Sid": "AllowUsersAllActionsForCredentials",

"Effect": "Allow",

"Action": [

"iam:*AccessKey*",

],

"Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]

}

]

A. 0
B. 0
C. 0
D. 0

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. If the organization (Account ID 123412341234. wants some of their users to manage keys (access and secret access keys. of all IAM users, the organization should set the below mentioned policy which entitles the IAM user to modify keys of all IAM users with CLI, SDK or API.
"Statement": [
{
"Sid": "AllowUsersAllActionsForCredentials",
"Effect": "Allow",
"Action": [
"iam:*AccessKey*",
],
"Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]
}
]

QUESTION NO: 126

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

QUESTION NO: 127

A user has configured Elastic Load Balancing by enabling a Secure Socket Layer
(SSL. negotiation

configuration known as a Security Policy. Which of the below mentioned options is not part of this
secure policy while negotiating the SSL connection between the user and the client?

A. SSL Protocols
B. Client Order Preference
C. SSL Ciphers
D. Server Order Preference

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

QUESTION NO: 128

A user has configured CloudWatch monitoring on an EBS backed EC2 instance. If the user has
not attached any additional device, which of the below mentioned metrics will always show a 0
value?

A. DiskReadBytes

B. NetworkIn
C. NetworkOut
D. CPUUtilization

Answer: A
Explanation:

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

QUESTION NO: 129

A user has launched an EBS backed EC2 instance. What will be the difference while performing the restart or stop/start options on that instance?

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

Answer: A
Explanation:

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

QUESTION NO: 130

A user has created a queue named "myqueue" in US-East region with AWS SQS. The user's AWS account ID is 123456789012. If the user wants to perform some action on this queue, which of the below Queue URL should he use?

A. http://sqs.us-east-1.amazonaws.com/123456789012/myqueue
B. http://sqs.amazonaws.com/123456789012/myqueue
C. http://sqs. 123456789012.us-east-1.amazonaws.com/myqueue
D. http:// 123456789012.sqs. us-east-1.amazonaws.com/myqueue

Answer: A
Explanation:

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

QUESTION NO: 131

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.

QUESTION NO: 132

A sys admin is trying to understand EBS snapshots. Which of the below mentioned statements will not be

useful to the admin to understand the concepts about a snapshot?

A. The snapshot is synchronous
B. It is recommended to stop the instance before taking a snapshot for consistent data
C. The snapshot is incremental
D. The snapshot captures the data that has been written to the hard disk when the snapshot command
was executed

Answer: A
Explanation:

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

QUESTION NO: 133

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

A. The root account owner should create a bucket policy which allows the IAM users to upload the object
B. The root account owner should create the bucket policy which allows the other account owners

to set

the object policy of that bucket

C. The root account should use ACL with the bucket to allow everyone to upload the object

D. The root account should create the IAM users and provide them the permission to upload content to the bucket

Answer: C
Explanation:

Each AWS S3 bucket and object has an ACL (Access Control List. associated with it. An ACL is a list of grants identifying the grantee and the permission granted. The user can use ACLs to grant basic read/write permissions to other AWS accounts. ACLs use an Amazon S3–specific XML schema. The user cannot grant permissions to other users in his account. ACLs are suitable for specific scenarios. For example, if a bucket owner allows other AWS accounts to upload objects, permissions to these objects can only be managed using the object ACL by the AWS account that owns the object.

QUESTION NO: 134

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.

QUESTION NO: 135

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

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

Answer: D
Explanation:

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

QUESTION NO: 136

A user wants to make so that whenever the CPU utilization of the AWS EC2 instance is above 90%, the redlight of his bedroom turns on. Which of the below mentioned AWS services is helpful for this purpose?

A. AWS CloudWatch + AWS SES
B. AWS CloudWatch + AWS SNS
C. None. It is not possible to configure the light with the AWS infrastructure services
D. AWS CloudWatch and a dedicated software turning on the light

Answer: B
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 configure some sensor devices at his home which receives data on the HTTP end point (REST calls. and turn on

the red light. The user can configure the CloudWatch alarm to send a notification to the AWS SNS HTTP end point (the sensor device. and it will turn the light red when there is an alarm condition.

QUESTION NO: 137

An organization has added 3 of his AWS accounts to consolidated billing. One of the AWS accounts has

purchased a Reserved Instance (RI. of a small instance size in the US-East-1a zone. All other AWS accounts are running instances of a small size in the same zone. What will happen in this case for the RI pricing?

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

Answer: C
Explanation:

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

QUESTION NO: 138

An organization is planning to use AWS for 5 different departments. The finance department is responsible to pay for all the accounts. However, they want the cost separation for each account to map with the right cost centre. How can the finance department achieve this?

A. Create 5 separate accounts and make them a part of one consolidate billing
B. Create 5 separate accounts and use the IAM cross account access with the roles for better management
C. Create 5 separate IAM users and set a different policy for their access
D. Create 5 separate IAM groups and add users as per the department's employees

Answer: A
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.

QUESTION NO: 139

A user has setup an EBS backed instance and a CloudWatch alarm when the CPU utilization is more than 65%. The user has setup the alarm to watch it for 5 periods of 5 minutes each. The CPU utilization is 60% between 9 AM to 6 PM. The user has stopped the EC2 instance for 15 minutes between 11 AM to 11:15 AM. What will be the status of the alarm at 11:30 AM?

A. Alarm
B. OK
C. Insufficient Data
D. Error

Answer: B
Explanation:

Amazon CloudWatch alarm watches a single metric over a time period the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a

number of time periods. The state of the alarm will be OK for the whole day. When the user stops the instance for three periods the alarm may not receive the data

QUESTION NO: 140

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

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

Answer: A
Explanation:

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

QUESTION NO: 141

A user has setup an RDS DB with Oracle. The user wants to get notifications when someone modifies the

security group of that DB. How can the user configure that?

A. It is not possible to get the notifications on a change in the security group
B. Configure SNS to monitor security group changes
C. Configure event notification on the DB security group
D. Configure the CloudWatch alarm on the DB for a change in the security group

Answer: C
Explanation:

Amazon RDS uses the Amazon Simple Notification Service to provide a notification when an Amazon RDS event occurs. These events can be configured for source categories, such as DB instance, DB security group, DB snapshot and DB parameter group. If the user is subscribed to a Configuration Change category for a DB security group, he will be notified when the DB security group is changed.

QUESTION NO: 142

A user is trying to setup a recurring Auto Scaling process. The user has setup one process to scale up every day at 8 am and scale down at 7 PM. The user is trying to setup another recurring process which scales up on the 1st of every month at 8 AM and scales down the same day at 7 PM. What will Auto Scaling do in this scenario?

A. Auto Scaling will execute both processes but will add just one instance on the 1st
B. Auto Scaling will add two instances on the 1st of the month
C. Auto Scaling will schedule both the processes but execute only one process randomly
D. Auto Scaling will throw an error since there is a conflict in the schedule of two separate Auto Scaling
Processes

Answer: D
Explanation:

Auto Scaling based on a schedule allows the user to scale the application in response to predictable load
changes. The user can also configure the recurring schedule action which will follow the Linux cron format. As per Auto Scaling, a scheduled action must have a unique time value. If the user attempts to schedule an activity at a time when another existing activity is already scheduled, the call will be rejected with an error message noting the conflict.

QUESTION NO: 143

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.

QUESTION NO: 144

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.

QUESTION NO: 145

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.

QUESTION NO: 146

A user has launched an EC2 instance from an instance store backed AMI. The infrastructure team wants to create an AMI from the running instance. Which of the below mentioned steps will not be performed while creating the AMI?

A. Define the AMI launch permissions
B. Upload the bundled volume
C. Register the AMI
D. Bundle the volume

Answer: A
Explanation:

When the user has launched an EC2 instance from an instance store backed AMI, it will need to follow certain steps, such as "Bundling the root volume", "Uploading the bundled volume" and "Register the AMI". Once the AMI is created the user can setup the launch permission. However, it is not required to setup during the launch.

QUESTION NO: 147

You are managing the AWS account of a big organization. The organization has more than 1000+ employees and they want to provide access to the various services to most of the employees. Which of the below mentioned options is the best possible solution in this case?

A. The user should create a separate IAM user for each employee and provide access to them as per
the policy
B. The user should create an IAM role and attach STS with the role. The user should attach that role to
the EC2 instance and setup AWS authentication on that server
C. The user should create IAM groups as per the organization's departments and add each user to the
group for better access control
D. Attach an IAM role with the organization's authentication service to authorize each user for various
AWS services

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 is managing an AWS account for an organization that already has an identity system, such as the login system for the corporate network (SSO.. In this case, instead of creating individual IAM users or groups for each user who need AWS access, it may be more practical to use a proxy server to translate the user identities from the organization network into the temporary AWS security credentials. This proxy server will attach an IAM role to the user after authentication.

QUESTION NO: 148

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.

QUESTION NO: 149

A user is launching an instance. He is on the "Tag the instance" screen. Which of the below mentioned

information will not help the user understand the functionality of an AWS tag?

A. Each tag will have a key and value
B. The user can apply tags to the S3 bucket
C. The maximum value of the tag key length is 64 unicode characters
D. AWS tags are used to find the cost distribution of various resources

Answer: C
Explanation:

AWS provides cost allocation tags to categorize and track the AWS costs. When the user applies tags to his AWS resources, AWS generates a cost allocation report as a comma-separated value (CSV file. with the usage and costs aggregated by those tags. Each tag will have a key-value and can be applied to services, such as EC2, S3, RDS, EMR, etc. The maximum size of a tag key is

128 unicode characters.

QUESTION NO: 150

A user has created a VPC with CIDR 20.0.0.0/16. The user has created public and VPN only subnets along with hardware VPN access to connect to the user's datacenter. The user wants to make so that all traffic coming to the public subnet follows the organization's proxy policy. How can the user make this happen?

A . Setting up a NAT with the proxy protocol and configure that the public subnet receives traffic from NAT
B . Settin up a proxy policy in the internet gateway connected with the public subnet
C . It is not possible to setup the proxy policy for a public subnet
D . Setting the route table and security group of the public subnet which receives traffic from a virtual private gateway

Answer: D
Explanation:

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

QUESTION NO: 151

A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25 and a private subnet with CIDR 20.0.0.128/25. The user has launched one instance each in the private and public subnets. Which of the below mentioned options cannot be the correct IP address (private IP. assigned to an instance in the public or private subnet?

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

Answer: A
Explanation:

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

QUESTION NO: 152

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.

QUESTION NO: 153

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

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

Answer: C
Explanation:

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

Topic 3, Volume C

QUESTION NO: 154

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.

QUESTION NO: 155

A user is using a small MySQL RDS DB. The user is experiencing high latency due to the Multi AZ feature.Which of the below mentioned options may not help the user in this situation?

A. Schedule the automated back up in non-working hours
B. Use a large or higher size instance
C. Use PIOPS
D. Take a snapshot from standby Replica

Answer: D
Explanation:

An RDS DB instance which has enabled Multi AZ deployments may experience increased write and commit latency compared to a Single AZ deployment, due to synchronous data replication. The user may also face changes in latency if deployment fails over to the standby replica. For production workloads, AWS recommends the user to use provisioned IOPS and DB instance classes (m1.large and larger. as they are optimized for provisioned IOPS to give a fast, and consistent performance. With Multi AZ feature, the user can not have option to take snapshot from replica.

QUESTION NO: 156

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.

QUESTION NO: 157

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

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

Answer: A
Explanation:

AWS provides an option to have programmatic access to billing. Programmatic Billing Access

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

QUESTION NO: 158

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.

QUESTION NO: 159

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

delete the subnet. What will happen in this scenario?

A. It will delete the subnet and make the EC2 instance as a part of the default subnet
B. It will not allow the user to delete the subnet until the instances are terminated
C. It will delete the subnet as well as terminate the instances
D. The subnet can never be deleted independently, but the user has to delete the VPC first

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

QUESTION NO: 160

A user has setup an EBS backed instance and attached 2 EBS volumes to it. The user has setup a

CloudWatch alarm on each volume for the disk data. The user has stopped the EC2 instance and detached the EBS volumes. What will be the status of the alarms on the EBS volume?

A. OK
B. Insufficient Data
C. Alarm
D. The EBS cannot be detached until all the alarms are removed

Answer: B
Explanation:

Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. Alarms invoke actions only for sustained state changes. There are three states of the alarm: OK, Alarm and Insufficient data. In this case since the EBS is detached and inactive the state will be Insufficient.

QUESTION NO: 161

A user has launched an EC2 instance from an instance store backed AMI. The infrastructure team wants to create an AMI from the running instance. Which of the below mentioned credentials is not

required while creating the AMI?

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

Answer: C
Explanation:

When the user has launched an EC2 instance from an instance store backed AMI and the admin team wants to create an AMI from it, the user needs to setup the AWS AMI or the API tools first. Once the tool is setup the user will need the following credentials:

AWS account ID;

AWS access and secret access key;

X.509 certificate with private key.

QUESTION NO: 162

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

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

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

Answer: D
Explanation:

When the user has configured Transmission Control Protocol (TCP. or Secure Sockets Layer (SSL. for both front-end and back-end connections of the Elastic Load Balancer, the load balancer forwards the request to the back-end instances without modifying the request headers unless the proxy header is enabled. SSL does not support sticky sessions. If the user has enabled a proxy

protocol it adds the source and destination IP to the header.

QUESTION NO: 163

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

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

Answer: C
Explanation:

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

QUESTION NO: 164

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.

QUESTION NO: 165

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.

QUESTION NO: 166

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 file, he can supply file name along with the parameter -- metric-data to command put-metric-data.

QUESTION NO: 167

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.

QUESTION NO: 168

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.

QUESTION NO: 169

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.

QUESTION NO: 170

A user has launched multiple EC2 instances for the purpose of development and testing in the same region. The user wants to find the separate cost for the production and development instances. How can the user find the cost distribution?

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

Answer: D
Explanation:

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

QUESTION NO: 171

A user has created a VPC with CIDR 20.0.0.0/16 using VPC Wizard. The user has created a public CIDR

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

A. Main route table attached with a VPN only subnet
B. A NAT instance configured to allow the VPN subnet instances to connect with the internet

C. Custom route table attached with a public subnet
D. An internet gateway for a public subnet

Answer: B
Explanation:

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

QUESTION NO: 172

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.

QUESTION NO: 173

A user has setup an Auto Scaling group. The group has failed to launch a single instance for more than 24 hours. What will happen to Auto Scaling in this condition?

A. Auto Scaling will keep trying to launch the instance for 72 hours
B. Auto Scaling will suspend the scaling process
C. Auto Scaling will start an instance in a separate region
D. The Auto Scaling group will be terminated automatically

Answer: B
Explanation:

If Auto Scaling is trying to launch an instance and if the launching of the instance
fails continuously, it will
suspend the processes for the Auto Scaling groups since it repeatedly failed to launch an
instance. This is known as an administrative suspension. It commonly applies to the Auto Scaling
group that has no running instances which is trying to launch instances for more than 24 hours,
and has not succeeded in that to do so.

QUESTION NO: 174

A user is planning to set up the Multi AZ feature of RDS. Which of the below mentioned conditions
won't take advantage of the Multi AZ feature?

A. Availability zone outage
B. A manual failover of the DB instance using Reboot with failover option
C. Region outage
D. When the user changes the DB instance's server type

Answer: C
Explanation:

Amazon RDS when enabled with Multi AZ will handle failovers automatically. Thus, the user can
resume
database operations as quickly as possible without administrative intervention. The primary DB
instance
switches over automatically to the standby replica if any of the following conditions occur:

An Availability Zone outage

The primary DB instance fails

The DB instance's server type is changed

The DB instance is undergoing software patching

A manual failover of the DB instance was initiated using Reboot with failover

QUESTION NO: 175

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.

QUESTION NO: 176

A user is using Cloudformation to launch an EC2 instance and then configure an application after the instance is launched. The user wants the stack creation of ELB and AutoScaling to wait until the EC2 instance is launched and configured properly. How can the user configure this?

A. It is not possible that the stack creation will wait until one service is created and launched
B. The user can use the HoldCondition resource to wait for the creation of the other dependent resources
C. The user can use the DependentCondition resource to hold the creation of the other dependent resources

D. The user can use the WaitCondition resource to hold the creation of the other

dependent resources

Answer: D
Explanation:

AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. AWS CloudFormation provides a WaitCondition resource which acts as a barrier and blocks the creation of other resources until a completion signal is received from an external source, such as a user application or management system.

QUESTION NO: 177

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

separate zones. The user wants to merge the groups such that one group spans across multiple zones. How can the user configure this?

A. Run the command as-join-auto-scaling-group to join the two groups
B. Run the command as-update-auto-scaling-group to configure one group to span across zones and
delete the other group
C. Run the command as-copy-auto-scaling-group to join the two groups
D. Run the command as-merge-auto-scaling-group to merge the groups

Answer: B
Explanation:

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

QUESTION NO: 178

An AWS account wants to be part of the consolidated billing of his organization's payee account. How can the owner of that account achieve this?

A. The payee account has to request AWS support to link the other accounts with his account
B. The owner of the linked account should add the payee account to his master account list from the
billing console
C. The payee account will send a request to the linked account to be a part of consolidated billing
D. The owner of the linked account requests the payee account to add his account to consolidated billing

Answer: C
Explanation:

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS. accounts within a single organization by making a single paying account. To add a particular account (linked. to the master (payee. account, the payee account has to request the linked account to join consolidated billing. Once the linked account accepts the request henceforth all charges incurred by the linked account will be paid by the payee account.

QUESTION NO: 179

A sysadmin has created the below mentioned policy on an S3 bucket named cloudacademy. What does this policy define?

"Statement": [{

"Sid": "Stmt1388811069831",

"Effect": "Allow",

"Principal": { "AWS": "*"},

"Action": ["s3:GetObjectAcl", "s3:ListBucket"],

"Resource": ["arn:aws:s3:::cloudacademy]

}]

A. It will make the cloudacademy bucket as well as all its objects as public
B. It will allow everyone to view the ACL of the bucket
C. It will give an error as no object is defined as part of the policy while the action defines the rule about
the object
D. It will make the cloudacademy bucket as public

Answer: D
Explanation:

A sysadmin can grant permission to the S3 objects or the buckets to any user or make objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if the user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket. In the sample policy the action says "S3:ListBucket" for effect Allow on Resource arn:aws:s3:::cloudacademy. This will make the cloudacademy bucket public.
"Statement": [{
"Sid": "Stmt1388811069831",
"Effect": "Allow",
"Principal": { "AWS": "*" },
"Action": ["s3:GetObjectAcl", "s3:ListBucket"],
"Resource": ["arn:aws:s3:::cloudacademy]
}]

QUESTION NO: 180

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

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

Answer: B
Explanation:

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

QUESTION NO: 181

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 "
}]

QUESTION NO: 182

A user has configured ELB with two EBS backed instances. The user has stopped the instances for 1 week to save costs. The user restarts the instances after 1 week. Which of the below mentioned statements will help the user to understand the ELB and instance registration better?

A. There is no way to register the stopped instances with ELB
B. The user cannot stop the instances if they are registered with ELB
C. If the instances have the same Elastic IP assigned after reboot they will be registered with ELB
D. The instances will automatically get registered with ELB

Answer: C
Explanation:

Elastic Load Balancing registers the user's load balancer with his EC2 instance using the associated IP
address. When the instances are stopped and started back they will have a different IP address. Thus, they will not get registered with ELB unless the user manually registers them. If the instances are assigned the same Elastic IP after reboot they will automatically get registered with ELB.

QUESTION NO: 183

A user is trying to connect to a running EC2 instance using SSH. However, the user gets a Host key not found error. Which of the below mentioned options is a possible reason for rejection?

A. The user has provided the wrong user name for the OS login
B. The instance CPU is heavily loaded
C. The security group is not configured properly
D. The access key to connect to the instance is wrong

Answer: A
Explanation:

If the user is trying to connect to a Linux EC2 instance and receives the Host Key not found error the probable reasons are: The private key pair is not right The user name to login is wrong

QUESTION NO: 184

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

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

Answer: B
Explanation:

QUESTION NO: 185

A user is using the AWS EC2. The user wants to make so that when there is an issue in the EC2 server, such as instance status failed, it should start a new instance in the user's private cloud. Which AWS service helps to achieve this automation?

A. AWS CloudWatch + Cloudformation
B. AWS CloudWatch + AWS AutoScaling + AWS ELB
C. AWS CloudWatch + AWS VPC
D. AWS CloudWatch + AWS SNS

Answer: D
Explanation:

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 configure a web service (HTTP End point. in his data centre which receives data and launches an instance in the private cloud. The user should configure the CloudWatch alarm to send a notification to SNS when the "StatusCheckFailed" metric is true for the EC2 instance. The SNS topic can be configured to send a notification to the user's HTTP end point which launches an instance in the private cloud.

QUESTION NO: 186

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

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

Answer: B
Explanation:

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

QUESTION NO: 187

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.

QUESTION NO: 188

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"]
}
}
}]

QUESTION NO: 189

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

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": "ec2:Describe*",

"Resource": "*"

},

{

"Effect": "Allow"

"Action": [

"cloudwatch:ListMetrics",

"cloudwatch:GetMetricStatistics",

"cloudwatch:Describe*"

],

"Resource": "*"

},

{

"Effect": "Allow",

"Action": "autoscaling:Describe*",

"Resource": "*"

}

]

}

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

Answer: D
Explanation:

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

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

QUESTION NO: 190

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

instance, which is bound to a cookie, crashes?

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

Answer: B
Explanation:

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

QUESTION NO: 191

A user is observing the EC2 CPU utilization metric on CloudWatch. The user has observed some interesting patterns while filtering over the 1 week period for a particular hour. The user wants to zoom that data point to a more granular period. How can the user do that easily with CloudWatch?

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

Answer: A
Explanation:

QUESTION NO: 192

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

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

Answer: B
Explanation:

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

QUESTION NO: 193

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

mentioned statements is not true in this scenario?

A. The VPC will create a routing instance and attach it with a public subnet

B. The VPC will create two subnets

C. The VPC will create one internet gateway and attach it to VPC
D. The VPC will launch one NAT instance with an elastic IP

Answer: A
Explanation:

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

QUESTION NO: 194

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.

QUESTION NO: 195

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. A W S   a l l o w s   1 0   E C 2   C l a s s i c   I P s   p e r   r e g i o n ;   s o   i t
w i l l   a l l o w   t o   a l l o c a t e   n e w   E l a s t i c   I P s   t o   t h e   s a m e
r e g i o n
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.

QUESTION NO: 196

A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance. Which of the below mentioned statements is true with respect to this scenario?

A. The instance will always have a public DNS attached to the instance by default

B. The user can directly attach an elastic IP to the instance
C. The instance will never launch if the public IP is not assigned
D. The user would need to create an internet gateway and then attach an elastic IP to the

instance to
connect from internet

Answer: D
Explanation:

A Virtual Private Cloud (VPC. is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When the user is launching an instance he needs to select an option which attaches a public IP to the instance. If the user has not selected the option to attach the public IP then it will only have a private IP when launched. The user cannot connect to the instance from the internet. If the user wants an elastic IP to connect to the instance from the internet he should create an internet gateway and assign an elastic IP to instance.

QUESTION NO: 197

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 correctly. It will throw an error for wrong resource name
B. The policy is for the group. Thus, the IAM user cannot have any entitlement to this
C. It allows full access to all AWS services for the IAM users who are a part of this group
D. 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": "*"
}
]
}

QUESTION NO: 198

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.

QUESTION NO: 199

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.

QUESTION NO: 200

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.

QUESTION NO: 201

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

preconfigured policies supports this feature?

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

Answer: A
Explanation:

Elastic Load Balancing uses a Secure Socket Layer (SSL. negotiation configuration which is known as a
Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. If the load balancer is configured to support the Server Order Preference, then the load balancer gets to select the first cipher in its list that matches any one of the ciphers in the client's list. When the user verifies the preconfigured policies supported by ELB, the policy "ELBSecurity Policy-2014-01" supports server order preference.

QUESTION NO: 202

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.

QUESTION NO: 203

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

launched two EC2 instances in the US-East-1a zone with his AWS account. Which of the below
entioned statements will help George and Ray understand the availability zone (AZ. concept
better?

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

Answer: D

Explanation:

Each AWS region has multiple, isolated locations known as Availability Zones. To ensure that the AWS

resources are distributed across the Availability Zones for a region, AWS independently maps the Availability Zones to identifiers for each account. In this case the Availability Zone US-East-1a where George's EC2 instances are running might not be the same location as the US-East-1a zone of Ray's EC2 instances. There is no way for the user to coordinate the Availability Zones between accounts.

QUESTION NO: 204

A user had aggregated the CloudWatch metric data on the AMI ID. The user observed some abnormal

behaviour of the CPU utilization metric while viewing the last 2 weeks of data. The user wants to share that data with his manager. How can the user achieve this easily with the AWS console?

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

Answer: A
Explanation:

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

A user has setup a CloudWatch alarm on the EC2 instance for CPU utilization. The user has setup to receive a notification on email when the CPU utilization is higher than 60%. The user is running a virus scan on the same instance at a particular time. The user wants to avoid receiving an email at this time. What should the user do?

A. Remove the alarm
B. Disable the alarm for a while using CLI
C. Modify the CPU utilization by removing the email alert
D. Disable the alarm for a while using the console

Answer: B
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. When the user has setup an alarm and it is know that for some unavoidable event the status may change to Alarm, the user can disable the alarm using the DisableAlarmActions API or from the command line mon-disable-alarm-actions.

QUESTION NO: 206

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

QUESTION NO: 207

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 (WebSecGrp.

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 (WebSecGrp.

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.

QUESTION NO: 208

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created public

and VPN only subnets along with hardware VPN access to connect to the user's data centre. The

user has not yet launched any instance as well as modified or deleted any setup. He wants to delete this VPC from the console. Will the console allow the user to delete the VPC?

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

Answer: C
Explanation:

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

QUESTION NO: 209

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

A. The ratio between IOPS and the EBS volume is higher than 30
B. The maximum IOPS supported by EBS is 3000
C. The ratio between IOPS and the EBS volume is lower than 50
D. PIOPS is supported for EBS higher than 500 GB size

Answer: A
Explanation:

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

QUESTION NO: 210

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

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

Answer: B
Explanation:

QUESTION NO: 211

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

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

Answer: B
Explanation:

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

QUESTION NO: 212

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption (SSE-C., which of the below mentioned statements is true?

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

Answer: B
Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key (SSE-C.. If the bucket is versioning-enabled, each object version uploaded by the user using the SSE-C feature can have its own encryption key. The user is responsible for tracking which encryption key was used for which object's version

QUESTION NO: 213

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.

QUESTION NO: 214

A user has launched an RDS MySQL DB with the Multi AZ feature. The user has scheduled the scaling of

instance storage during maintenance window. What is the correct order of events
during maintenance window?

Perform maintenance on standby

Promote standby to primary

Perform maintenance on original primary

Promote original master back as primary

A. 1, 2, 3, 4
B. 1, 2, 3
C. 2, 3, 1, 4

Answer: B
Explanation:

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

QUESTION NO: 215

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.

QUESTION NO: 216

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.

QUESTION NO: 217

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

172.28.0.0/12. The user has also setup a NAT instance (i-123456. to allow traffic to the internet from the VPN subnet. Which of the below mentioned options is not a valid entry for the main route table in this scenario?

A. Destination: 20.0.1.0/24 and Target: i-12345
B. Destination: 0.0.0.0/0 and Target: i-12345
C. Destination: 172.28.0.0/12 and Target: vgw-12345
D. Destination: 20.0.0.0/16 and Target: local

Answer: A
Explanation:

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

QUESTION NO: 218

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 . The NAT instance ID is i-a12345. Which of the below mentioned entries are required in the main route table attached with the private subnet to allow instances to connect with the internet?

A. Destination: 0.0.0.0/0 and Target: i-a12345
B. Destination: 20.0.0.0/0 and Target: 80
C. Destination: 20.0.0.0/0 and Target: i-a12345
D. Destination: 20.0.0.0/24 and Target: i-a12345

Answer: A
Explanation:

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create two route tables and attach to the subnets. The main route table will have the entry "Destination: 0.0.0.0/0 and Target: ia12345", which allows all the instances in the private subnet to connect to the internet using NAT.

QUESTION NO: 219

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.

QUESTION NO: 220

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.

QUESTION NO: 221

A sys admin is planning to subscribe to the RDS event notifications. For which of the below mentioned source categories the subscription cannot be configured?

A. DB security group
B. DB snapshot
C. DB options group
D. DB parameter group

Answer: C
Explanation:

Amazon RDS uses the Amazon Simple Notification Service (SNS. to provide a notification when an Amazon RDS event occurs. These events can be configured for source categories, such as DB instance, DB security group, DB snapshot and DB parameter group.

QUESTION NO: 222

A user has launched an EC2 instance. The instance got terminated as soon as it was launched. Which of the below mentioned options is not a possible reason for this?

A. The user account has reached the maximum EC2 instance limit
B. The snapshot is corrupt
C. The AMI is missing. It is the required part
D. The user account has reached the maximum volume limit

Answer: A
Explanation:

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

QUESTION NO: 223

A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services does not provide detailed monitoring with CloudWatch?

A. AWS EMR
B. AWS RDS
C. AWS ELB
D. AWS Route53

Answer: A
Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed

monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, EC2, Auto Scaling, ELB, and Route 53 can provide the monitoring data every minute.

QUESTION NO: 224

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

QUESTION NO: 225

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

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

Answer: D
Explanation:

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

QUESTION NO: 226

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

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

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

Answer: D
Explanation:

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

QUESTION NO: 227

A user wants to find the particular error that occurred on a certain date in the AWS MySQL RDS DB. Which of the below mentioned activities may help the user to get the data easily?

A. It is not possible to get the log files for MySQL RDS
B. Find all the transaction logs and query on those records
C. Direct the logs to the DB table and then query that table
D. Download the log file to DynamoDB and search for the record

Answer: C
Explanation:

The user can view, download, and watch the database logs using the Amazon RDS console, the Command Line Interface (CLI. or the Amazon RDS API. For the MySQL RDS, the user can view the error log, slow query log, and general logs. The user can also view the MySQL logs easily by directing the logs to a database table in the main database and querying that table.

QUESTION NO: 228

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

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

A. The size of a request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests
B. The size of a request is limited to 128KB for HTTP GET requests and 64KB for HTTP POST requests
C. The size of a request is limited to 40KB for HTTP GET requests and 8KB for HTTP POST requests
D. The size of a request is limited to 16KB for HTTP GET requests and 80KB for HTTP POST requests

Answer: A
Explanation:

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

QUESTION NO: 229

An AWS account owner has setup multiple IAM users. One IAM user only has CloudWatch access. He has setup the alarm action which stops the EC2 instances when the CPU utilization is below the threshold limit. What will happen in this case?

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

Answer: D
Explanation:

Amazon CloudWatch alarms watch a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which stops the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action. If the IAM user has read/write permissions for Amazon CloudWatch but not for Amazon EC2, he can still create an alarm. However, the stop or terminate actions will not be performed on the Amazon EC2 instance.

QUESTION NO: 230

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

A. Auto Scaling will not launch or terminate any instances
B. Auto Scaling will allow the instances to grow more than the maximum size
C. Auto Scaling will keep launching instances till the maximum instance size
D. It is not possible to suspend the terminate process while keeping the launch active

Answer: B
Explanation:

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

QUESTION NO: 231

A user has created a mobile application which makes calls to DynamoDB to fetch certain data.
The application is using the DynamoDB SDK and root account access/secret access key to
connect to DynamoDB from mobile. Which of the below mentioned statements is true with respect
to the best practice for security in this scenario?

A. The user should create a separate IAM user for each mobile application and
provide DynamoDB
access with it
B. The user should create an IAM role with DynamoDB and EC2 access. Attach the role with
EC2 and
route all calls from the mobile through EC2
C. The application should use an IAM role with web identity federation which validates calls
to DynamoDB with identity providers, such as Google, Amazon, and Facebook
D. Create an IAM Role with DynamoDB access and attach it with the mobile application

Answer: C
Explanation:

With AWS IAM a user is creating an application which runs on an EC2 instance and makes requests to AWS, such as DynamoDB or S3 calls. Here it is recommended that the user should not create an IAM user and pass the user's credentials to the application or embed those credentials inside the application. If the user is creating an app that runs on a mobile phone and makes requests to AWS, the user should not create an IAMuser and distribute the user's access key with the app. Instead, he should use an identity provider, such as Login with Amazon, Facebook, or Google to authenticate the users, and then use that identity to get temporary security credentials.

QUESTION NO: 232

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.

QUESTION NO: 233

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

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

Answer: D
Explanation:

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

QUESTION NO: 234

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 by mistake. The user is trying to create another subnet of CIDR 20.0.0.1/24. How can the user create the second subnet?

A. There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet
based on the second subnet's CIDR
B. The user can modify the first subnet CIDR from the console
C. It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been
created
D. The user can modify the first subnet CIDR with AWS CLI

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 the 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. The user cannot modify the CIDR of a subnet once it is created. Thus, in this case if required, the user has to delete the subnet and create new

subnets.

QUESTION NO: 235

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 (DbSecGrp. for port 3306 Outbound
B. 80 for Destination 0.0.0.0/0 Outbound
C. Configure port 3306 for source 20.0.0.0/24 InBound
D. 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 security group of the private subnet (DbSecGrp. as the destination for port 3306 in Outbound.

QUESTION NO: 236

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.

QUESTION NO: 237

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

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

Answer: B
Explanation:

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

QUESTION NO: 238

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

QUESTION NO: 239

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

supported by SQS?

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

145

Answer: D
Explanation:

Amazon Simple Queue Service (SQS. is a fast, reliable, scalable, and fully managed message queuing
service. SQS provides a simple and cost-effective way to decouple the components of an
application. The user can perform the following set of operations using the Amazon SQS:
CreateQueue, ListQueues, DeleteQueue, SendMessage, SendMessageBatch, ReceiveMessage,
DeleteMessage, DeleteMessageBatch, ChangeMessageVisibility, ChangeMessageVisibilityBatch,
SetQueueAttributes, GetQueueAttributes, GetQueueUrl, AddPermission and RemovePermission.
Operations can be performed only by the AWS account owner or an AWS account that the
account owner has delegated to.

QUESTION NO: 240

A user has configured Auto Scaling with 3 instances. The user had created a new AMI after
updating one of the instances. If the user wants to terminate two specific instances to ensure that
Auto Scaling launches an instances with the new launch configuration, which command should he
run?

A. as-delete-instance-in-auto-scaling-group <Instance ID> --no-decrement-desired-capacity
B. as-terminate-instance-in-auto-scaling-group <Instance ID> --update-desired-capacity
C. as-terminate-instance-in-auto-scaling-group <Instance ID> --decrement-desired-capacity
D. as-terminate-instance-in-auto-scaling-group <Instance ID> --no-decrement-desired-capacity

Answer: D
Explanation:

The Auto Scaling command as-terminate-instance-in-auto-scaling-group <Instance ID>
will terminate the
specific instance ID. The user is required to specify the parameter as –no-decrement-desired-
capacity to
ensure that it launches a new instance from the launch config after terminating the instance. If the
user
specifies the parameter --decrement-desired-capacity then Auto Scaling will terminate the instance
and

decrease the desired capacity by 1.

QUESTION NO: 241

A user has launched an EC2 instance from an instance store backed AMI. If the user restarts the instance, what will happen to the ephermal storage data?

A. All the data will be erased but the ephermal storage will stay connected
B. All data will be erased and the ephermal storage is released
C. It is not possible to restart an instance launched from an instance store backed AMI
D. The data is preserved

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 Amazon EC2 to reboot the instance instead of running the operating system reboot command from the instance. When an instance launched from an instance store backed AMI is rebooted all the ephermal storage data is still preserved.

QUESTION NO: 242

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

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

Answer: D
Explanation:

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

QUESTION NO: 243

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

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

Answer: B
Explanation:

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

QUESTION NO: 244

A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned security policies is supported by ELB?

A. Dynamic Security Policy
B. All the other options
C. Predefined Security Policy
D. Default Security Policy

Answer: C

Explanation:

Elastic Load Balancing uses a Secure Socket Layer (SSL. negotiation configuration which is known as a
Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. ELB
supports two policies:
Predefined Security Policy, which comes with predefined cipher and SSL protocols;
Custom Security Policy, which allows the user to configure a policy.

QUESTION NO: 245

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.

A user has configured an ELB to distribute the traffic among multiple instances. The user instances are facing some issues due to the back-end servers. Which of the below mentioned CloudWatch metrics helps the user understand the issue with the instances?

A. HTTPCode_Backend_3XX
B. HTTPCode_Backend_4XX
C. HTTPCode_Backend_2XX
D. HTTPCode_Backend_5XX

Answer: D
Explanation:

CloudWatch is used to monitor AWS as well as the custom services. For ELB, CloudWatch provides various metrics including error code by ELB as well as by back-end servers (instances.. It gives data for the count of the number of HTTP response codes generated by the back-end instances. This metric does not include any response codes generated by the load balancer. These metrics are:

The 2XX class status codes represents successful actions

The 3XX class status code indicates that the user agent requires action

The 4XX class status code represents client errors

The 5XX class status code represents back-end server errors

QUESTION NO: 247

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

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

D. The new instance in the EU region will not have the changes made after the AMI copy

Answer: D
Explanation:

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

QUESTION NO: 248

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.

QUESTION NO: 249

A user has created an Auto Scaling group using CLI. The user wants to enable CloudWatch detailed

monitoring for that group. How can the user configure this?

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

Answer: B
Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed

monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates an Auto Scaling launch config as the first step for creating an Auto Scaling group, each launch configuration contains a flag named
InstanceMonitoring.Enabled. The default value of this flag is true. Thus, the user does not need to set this flag if he wants detailed monitoring.

QUESTION NO: 250

A user has created a VPC with a public subnet. The user has terminated all the instances which are part of the subnet. Which of the below mentioned statements is true with respect to this scenario?

A. The user cannot delete the VPC since the subnet is not deleted
B. All network interface attached with the instances will be deleted
C. When the user launches a new instance it cannot use the same subnet
D. The subnet to which the instances were launched with will be deleted

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

QUESTION NO: 251

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

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

Answer: C
Explanation:

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

QUESTION NO: 252

A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The

153

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 443 in Outbound with destination 0.0.0.0/0. The NAT should not have an entry for the public subnet CIDR.

QUESTION NO: 253

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

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

Answer: A
Explanation:

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

QUESTION NO: 254

An organization (Account ID 123412341234. has attached the below mentioned IAM policy to a user. What does this policy statement entitle the user to perform?

{

"Version": "2012-10-17",

"Statement": [{

"Sid": "AllowUsersAllActionsForCredentials",

"Effect": "Allow",

"Action": [

"iam:*LoginProfile",

"iam:*AccessKey*",

"iam:*SigningCertificate*"

],

"Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]

}]

}

A. The policy allows the IAM user to modify all IAM user's credentials using the console, SDK, CLI or APIs
B. The policy will give an invalid resource error
C. The policy allows the IAM user to modify all credentials using only the console
D. The policy allows the user to modify all IAM user's password, sign in certificates and access

keys
using only CLI, SDK or APIs

Answer: D
Explanation:

WS 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 some of their users to manage credentials (access keys, password, and sing in certificates. of all IAM users, they should set an applicable policy to that user or group of users. The below mentioned policy allows the IAM user to modify the credentials of all IAM user's using only CLI, SDK or APIs. The user cannot use the AWS console for this activity since he does not have list permission for the IAM users.
{
"Version": "2012-10-17",
"Statement": [{
"Sid": "AllowUsersAllActionsForCredentials",
"Effect": "Allow"
"Action": [
"iam:*LoginProfile",
"iam:*AccessKey*",
"iam:*SigningCertificate*"
],
"Resource": ["arn:aws:iam::123412341234:user/${aws:username}"]
}]
}

QUESTION NO: 255

A sys admin is trying to understand the sticky session algorithm. Please select the correct sequence of steps, both when the cookie is present and when it is not, to help the admin understand the implementation of the sticky session:

ELB inserts the cookie in the response

ELB chooses the instance based on the load balancing algorithm

Check the cookie in the service request

The cookie is found in the request

The cookie is not found in the request

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

Answer: C
Explanation:

Generally AWS ELB routes each request to a zone with the minimum load. The Elastic Load Balancer provides a feature called sticky session which binds the user's session with a specific EC2 instance. The load balancer uses a special load-balancer-generated cookie to track the application instance for each request. When the load balancer receives a request, it first checks to see if this cookie is present in the request. If so, the request is sent to the application instance specified in the cookie. If there is no cookie, the load balancer chooses an application instance based on the existing load balancing algorithm. A cookie is inserted into the response for binding subsequent requests from the same user to that application instance.

QUESTION NO: 256

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.

QUESTION NO: 257

An organization has configured Auto Scaling for hosting their application. The system admin wants to

understand the Auto Scaling health check process. If the instance is unhealthy, Auto Scaling launches an

instance and terminates the unhealthy instance. What is the order execution?

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

Answer: D
Explanation:

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

QUESTION NO: 258

A user is trying to connect to a running EC2 instance using SSH. However, the user gets an Unprotected

Private Key File error. Which of the below mentioned options can be a possible reason for rejection?

A. The private key file has the wrong file permission

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

Answer: A
Explanation:

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

QUESTION NO: 259

A user has provisioned 2000 IOPS to the EBS volume. The application hosted on that EBS is experiencing less IOPS than provisioned. Which of the below mentioned options does not affect the IOPS of the volume?

A. The application does not have enough IO for the volume
B. The instance is EBS optimized
C. The EC2 instance has 10 Gigabit Network connectivity
D. The volume size is too large

Answer: D
Explanation:

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

QUESTION NO: 260

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

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

Answer: D
Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API callto supply his own encryption key. Amazon S3 never stores the user's encryption key. The user has to supply it for each encryption or decryption call.

QUESTION NO: 261

A user is trying to create a PIOPS EBS volume with 8 GB size and 200 IOPS. Will AWS create the volume?

A. Yes, since the ratio between EBS and IOPS is less than 30
B. No, since the PIOPS and EBS size ratio is less than 30
C. No, the EBS size is less than 10 GB
D. Yes, since PIOPS is higher than 100

Answer: C
Explanation:

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

QUESTION NO: 262

A user has scheduled the maintenance window of an RDS DB on Monday at 3 AM. Which of the below

mentioned events may force to take the DB instance offline during the maintenance window?

A. Enabling Read Replica
B. Making the DB Multi AZ
C. DB password change
D. Security patching

Answer: D
Explanation:

Amazon RDS performs maintenance on the DB instance during a user-definable maintenance window. The system may be offline or experience lower performance during that window. The only maintenance events that may require RDS to make the DB instance offline are:
Scaling compute operations
Software patching. Required software patching is automatically scheduled only for patches that are security
and durability related. Such patching occurs infrequently (typically once every few months. and seldom
requires more than a fraction of the maintenance window.

QUESTION NO: 263

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

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"
}
}
}
]

QUESTION NO: 264

A user has configured Auto Scaling with the minimum capacity as 2 and the desired capacity as 2. The user is trying to terminate one of the existing instance with the command:

as-terminate-instance-in-auto-scaling-group<Instance ID> --decrement-desired-capacity

What will Auto Scaling do in this scenario?

A. Terminates the instance and does not launch a new instance
B. Terminates the instance and updates the desired capacity to 1
C. Terminates the instance and updates the desired capacity and minimum size to 1
D. Throws an error

Answer: D
Explanation:

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

QUESTION NO: 265

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 comma.
CloudWatch will parse automatically
C. Create one csv file of all the data and send a single file to CloudWatch
D. It is not possible to send all the data in one call. Thus, it should be sent one by
one. CloudWatch will
aggregate the data automatically

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.

QUESTION NO: 266

A user is trying to create an EBS volume with the highest PIOPS supported by EBS. What is the minimum size of EBS required to have the maximum IOPS?

A. 124
B. 150
C. 134
D. 128

Answer: C
Explanation:

A provisioned IOPS EBS volume can range in size from 10 GB to 1 TB and the user can provision up to 4000 IOPS per volume. The ratio of IOPS provisioned to the volume size requested should be a maximum of 30.

QUESTION NO: 267

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 (-..

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.

QUESTION NO: 269

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.

QUESTION NO: 270

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.

QUESTION NO: 271

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

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

Answer: C
Explanation:

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

QUESTION NO: 272

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.

QUESTION NO: 273

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.

QUESTION NO: 274

The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?

A. "Effect": "Allow", "Action": ["Describe"], "Resource": "Billing"
B. "Effect": "Allow", "Action": ["AccountUsage], "Resource": "*"
C. "Effect": "Allow", "Action": ["aws-portal:ViewUsage"], "Resource": "*"
D. "Effect": "Allow", "Action": ["aws-portal: ViewBilling"], "Resource": "*"

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 CFO wants to allow only AWS usage report page access, the policy for that IAM user will be as given below:
{
"Version": "2012-10-17",
"Statement": [

```
{
"Effect": "Allow",
"Action": [
"aws-portal:ViewUsage"
],
"Resource": "*"
}
]
}
```

QUESTION NO: 275

An organization has created 10 IAM users. The organization wants each of the IAM users to have access to a separate DyanmoDB table. All the users are added to the same group and the organization wants to setup a group level policy for this. How can the organization achieve this?

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

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. AWS DynamoDB has only tables and the organization cannot makeseparate databases. The organization should create a table with the same name as the IAM user name and use the ARN of DynamoDB as part of the group policy. The sample policy is shown below:

```
{
"Version": "2012-10-17",
"Statement": [{
```

"Effect": "Allow",
"Action": ["dynamodb:*"],
"Resource": "arn:aws:dynamodb:region:account-number-without-hyphens:table/
${aws:username}" }
]
}

QUESTION NO: 276

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.

QUESTION NO: 277

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.

QUESTION NO: 278

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.

QUESTION NO: 279

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

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

Answer: B
Explanation:

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

QUESTION NO: 280

An organization has setup Auto Scaling with ELB. Due to some manual error, one of the instances got

rebooted. Thus, it failed the Auto Scaling health check. Auto Scaling has marked it for replacement. How can the system admin ensure that the instance does not get terminated?

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

Answer: D
Explanation:

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

QUESTION NO: 281

A system admin wants to add more zones to the existing ELB. The system admin wants to perform this activity from CLI. Which of the below mentioned command helps the system admin to add new zones to the existing ELB?

A. elb-enable-zones-for-lb
B. elb-add-zones-for-lb
C. It is not possible to add more zones to the existing ELB
D. elb-configure-zones-for-lb

Answer: A
Explanation:

The user has created an Elastic Load Balancer with the availability zone and wants to add more zones to the existing ELB. The user can do so in two ways:
From the console or CLI, add new zones to ELB;

QUESTION NO: 282

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.

QUESTION NO: 283

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

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

Answer: A
Explanation:

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

QUESTION NO: 284

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

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

Answer: D
Explanation:

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

QUESTION NO: 285

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:

QUESTION NO: 286

A user has configured ELB with Auto Scaling. The user suspended the Auto
Scaling AddToLoadBalancer

(which adds instances to the load balancer. process for a while. What will happen to the instances
launched during the suspension period?

A. The instances will not be registered with ELB and the user has to manually register when
the process
is resumed
B. The instances will be registered with ELB only once the process has resumed
C. Auto Scaling will not launch the instance during this period due to process suspension
D. It is not possible to suspend only the AddToLoadBalancer process

Answer: A
Explanation:

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

QUESTION NO: 287

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

A. Response processing time
B. Front end processing time
C. Backend processing time

D. Request processing time

Answer: B
Explanation:

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

QUESTION NO: 288

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 (restored. and Glacier (Archive. 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.

QUESTION NO: 289

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.

QUESTION NO: 290

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

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

Answer: D
Explanation:

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

QUESTION NO: 291

A user runs the command "dd if=/dev/xvdf of=/dev/null bs=1M" on an EBS volume created from a snapshot and attached to a Linux instance. Which of the below mentioned activities is the user performing with the step given above?

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

Answer: A
Explanation:

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

QUESTION NO: 292

A user has launched an EC2 Windows instance from an instance store backed AMI. The user wants to convert the AMI to an EBS backed AMI. How can the user convert it?

A. Attach an EBS volume to the instance and unbundle all the AMI bundled data inside the EBS
B. A Windows based instance store backed AMI cannot be converted to an EBS backed AMI
C. It is not possible to convert an instance store backed AMI to an EBS backed AMI
D. Attach an EBS volume and use the copy command to copy all the ephermal content to the EBS Volume

Answer: B
Explanation:

Generally when a user has launched an EC2 instance from an instance store backed AMI, it can be converted to an EBS backed AMI provided the user has attached the EBS volume to the instance and unbundles the AMI data to it. However, if the instance is a Windows instance, AWS does not allow this. In this case, since the instance is a Windows instance, the user cannot convert it to an EBS backed AMI.

QUESTION NO: 293

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 : 20.0.0.0/16 and Target : Local

Answer: A
Explanation:

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet cannot. If these subnets are

created with Wizard, AWS will create two route tables and attach to the subnets. The main route table will have the entry "Destination: 20.0.0.0/24 and Target:
Local", which allows all instances in the VPC to communicate with each other.

QUESTION NO: 294

A sysadmin has created the below mentioned policy on an S3 bucket named cloudacademy. The bucket has both AWS.jpg and index.html objects. What does this policy define?

"Statement": [{

"Sid": "Stmt1388811069831",

"Effect": "Allow",

"Principal": { "AWS": "*"},

"Action": ["s3:GetObjectAcl", "s3:ListBucket", "s3:GetObject"],

"Resource": ["arn:aws:s3:::cloudacademy/*.jpg]

}]

A. It will make all the objects as well as the bucket public
B. It will throw an error for the wrong action and does not allow to save the policy
C. It will make the AWS.jpg object as public
D. It will make the AWS.jpg as well as the cloudacademy bucket as public

Answer: B
Explanation:

A sysadmin can grant permission to the S3 objects or the buckets to any user or make objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket. In the below policy the action says "S3:ListBucket" for effect Allow and when there is no bucket name mentioned as a part of the resource, it will throw an error and not save the policy.
"Statement": [{
"Sid": "Stmt1388811069831",
"Effect": "Allow",

"Principal": { "AWS": "*"},

"Action": ["s3:GetObjectAcl", "s3:ListBucket", "s3:GetObject"],
"Resource": ["arn:aws:s3:::cloudacademy/*.jpg]
}]

QUESTION NO: 295

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.

QUESTION NO: 296

A user has created a launch configuration for Auto Scaling where CloudWatch detailed monitoring is disabled. The user wants to now enable detailed monitoring. How can the user achieve this?

A. Update the Launch config with CLI to set InstanceMonitoringDisabled = false
B. The user should change the Auto Scaling group from the AWS console to enable detailed monitoring
C. Update the Launch config with CLI to set InstanceMonitoring.Enabled = true
D. Create a new Launch Config with detail monitoring enabled and update the Auto Scaling group

Answer: D
Explanation:

CloudWatch is used to monitor AWS as well as the custom services. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates the AutoScaling launch config as the first step for creating an Auto Scaling group, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. When the user has created a launch configuration with InstanceMonitoring.Enabled = false it will involve multiple steps to enable detail monitoring. The steps are:
Create a new Launch config with detailed monitoring enabled
Update the Auto Scaling group with a new launch config
Enable detail monitoring on each EC2 instance

QUESTION NO: 297

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".

QUESTION NO: 298

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.

QUESTION NO: 299

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

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

Answer: B
Explanation:

A user can create an EBS volume either from a snapshot or as a blank volume. If the volume is from a

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

QUESTION NO: 300

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.

QUESTION NO: 301

A user has deployed an application on an EBS backed EC2 instance. For a better performance of

application, it requires dedicated EC2 to EBS traffic. How can the user achieve this?

A. Launch the EC2 instance as EBS dedicated with PIOPS EBS
B. Launch the EC2 instance as EBS enhanced with PIOPS EBS
C. Launch the EC2 instance as EBS dedicated with PIOPS EBS
D. Launch the EC2 instance as EBS optimized with PIOPS EBS

Answer: D
Explanation:

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

QUESTION NO: 302

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.