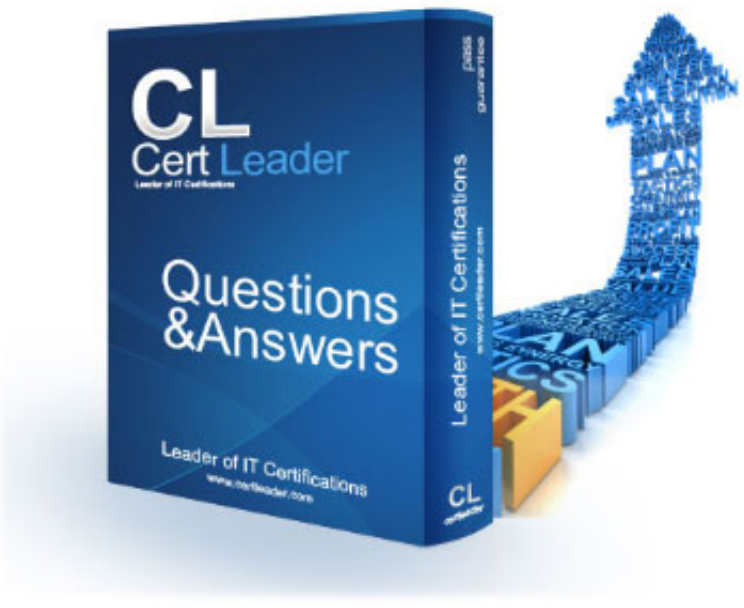
AWS-SysOps Dumps

Amazon AWS Certified SysOps Administrator - Associate

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



NEW QUESTION 1
- (Topic 1)
Your team Is excited about the use of AWS because now they have access to programmable Infrastructure" You have been asked to manage your AWS infrastructure In a manner similar to the way you might manage application code You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development test QA. production).
Which approach addresses this requirement?

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

Answer: B

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

NEW QUESTION 2
- (Topic 1)
You 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 the most scalable solution for communicating between the application and SQS?

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 SQS queue size

Answer: B

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

NEW QUESTION 3
- (Topic 1)
You have decided to change the Instance type for instances running In your application tier that are using Auto Scaling.
In which area below would you change the instance type definition?

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

Answer: A

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

NEW QUESTION 4
- (Topic 1)
You are designing a system that has a Bastion host. This component needs to be highly available without human intervention.
Which of the following approaches would you select?

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

Answer: C

NEW QUESTION 5
- (Topic 1)
You have set up Individual AWS accounts for each project. You have been asked to make sure your AWS Infrastructure costs do not exceed the budget set per project for each month.
Which of the following approaches can help ensure that you do not exceed the budget each month?

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

Answer: C

NEW QUESTION 6
- (Topic 1)
Your entire AWS infrastructure lives inside of one Amazon VPC You have an Infrastructure monitoring application running on an Amazon instance in Availability Zone (AZ) A of the region, and another application instance running in AZ B. The monitoring application needs to make use of ICMP ping to confirm network reachability of the instance hosting the application.
Can you configure the security groups for these instances to only allow the ICMP ping to pass from the monitoring instance to the application instance and nothing else" If so how?

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

Answer: D

NEW QUESTION 7
- (Topic 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 for 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: B

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

NEW QUESTION 8
- (Topic 1)
Which of the following are characteristics of Amazon VPC subnets?
Choose 2 answers

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

Answer: CE

NEW QUESTION 9
- (Topic 1)
You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database. You want to confirm that they can talk to each other for your application to work properly.
Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC? Choose 2 answers

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

Answer: AD

NEW QUESTION 10
- (Topic 1)
You are creating an Auto Scaling group whose Instances need to insert a custom metric into CloudWatch.
Which method would be the best way to authenticate your CloudWatch PUT request?

A. Create an IAM role with the Put MetricData permission and modify the Auto Scaling launch configuration to launch instances in that role
B. Create an IAM user with the PutMetricData permission and modify the Auto Scaling launch configuration to inject the userscredentials into the instance User Data
C. Modify the appropriate Cloud Watch metric policies to allow the Put MetricData permission to instances from the Auto Scaling group
D. Create an IAM user with the PutMetricData permission and put the credentials in a private repository and have applications on the server pull the credentials as needed

Answer: A

NEW QUESTION 10
- (Topic 1)
You have started a new job and are reviewing your company's infrastructure on AWS You notice one web application where they have an Elastic Load Balancer (&B) in front of web instances in an Auto Scaling Group When you check the metrics for the ELB in CloudWatch you see four healthy instances In Availability Zone (AZ) A and zero in AZ B There are zero unhealthy instances.
What do you need to fix to balance the instances across AZs?

A. Set the ELB to only be attached to another AZ
B. Make sure Auto Scaling is configured to launch in both AZs
C. Make sure your AMI is available in both AZs
D. Make sure the maximum size of the Auto Scaling Group is greater than 4

Answer: B

NEW QUESTION 15
- (Topic 1)
You have identified network throughput as a bottleneck on your m1.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

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

NEW QUESTION 18
- (Topic 1)
You are using ElastiCache Memcached to store session state and cache database queries in your infrastructure. You notice in CloudWatch 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: BD

NEW QUESTION 20
- (Topic 1)
You have been asked to propose a multi-region deployment of a web-facing application where a controlled portion of your traffic is being processed by an alternate region.
Which configuration would achieve that goal?

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

Answer: D

Explanation:
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html

NEW QUESTION 21
- (Topic 1)
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: AD

NEW QUESTION 25
- (Topic 1)
You have a Linux EC2 web server instance running inside a VPC The instance is In a public subnet and has an EIP associated with it so you can connect to It over the Internet via HTTP or SSH The instance was also fully accessible when you last logged in via SSH. and was also serving web requests on port 80.
Now you are not able to SSH into the host nor does it respond to web requests on port 80 that were working fine last time you checked You have double-checked

that all networking configuration parameters (security groups route tables. IGW'EIP. NACLs etc) are properly configured {and you haven't made any changes to those anyway since you were last able to reach the Instance). You look at the EC2 console and notice that system status check shows "impaired."
Which should be your next step in troubleshooting and attempting to get the instance back to a healthy state so that you can log in again?

A. Stop and start the instance so that it will be able to be redeployed on a healthy host system that most likely will fix the "impaired" system status
B. Reboot your instance so that the operating system will have a chance to boot in a clean healthy state that most likely will fix the 'impaired" system status
C. Add another dynamic private IP address to 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 statu
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: A

NEW QUESTION 30
- (Topic 2)
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 rol
C. The user should attach that role to the EC2 instance and setup AWS authentication on that server
D. The user should create IAM groups as per the organization's departments and add each user to the group for better access control
E. 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.

NEW QUESTION 32
- (Topic 2)
A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24. and VPN only subnets CIDR (20.0.1.0/24. along with the VPN gateway (vgw-12345. to connect to the user's data centre. Which of the below mentioned options is a valid entry for the main route table in this scenario?

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

Answer: D

Explanation:

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

NEW QUESTION 33
- (Topic 2)
An organization is generating digital policy files which are required by the admins for verification. Once the files are verified they may not be required in the future unless there is some compliance issue. If the organization wants to save them in a cost effective way, which is the best possible solution?

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

Answer: D

Explanation:

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

NEW QUESTION 36
- (Topic 2)
A user has received a message from the support team that an issue occurred 1 week back between 3 AM to 4 AM and the EC2 server was not reachable. The user is checking the CloudWatch metrics of that instance. How can the user find the data easily using the CloudWatch console?

A. The user can find the data by giving the exact values in the time Tab under CloudWatch metrics
B. The user can find the data by filtering values of the last 1 week for a 1 hour period in the Relative tab under CloudWatch metrics

C. It is not possible to find the exact time from the consol
D. The user has to use CLI to provide the specific time
E. The user can find the data by giving the exact values in the Absolute tab under CloudWatch metrics

Answer: D

Explanation:

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

NEW QUESTION 41
- (Topic 2)
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.

NEW QUESTION 46
- (Topic 2)
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.

NEW QUESTION 50
- (Topic 2)
A sys admin has created the below mentioned policy and applied to an S3 object named aws.jpg. The aws.jpg is inside a bucket named cloudacademy. What does this policy define?

```
"Statement": [{
"Sid": "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.

NEW QUESTION 53
- (Topic 2)

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

A. View the Auto Scaling CPU metrics
B. Aggregate the data over the instance AMI ID
C. The user has to use the 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.

NEW QUESTION 55
- (Topic 2)
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.

NEW QUESTION 60
- (Topic 2)
A root AWS account owner is trying to understand various options to set the permission to AWS S3. Which of the below mentioned options is not the right option to grant permission for S3?

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

Answer: B

Explanation:

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

NEW QUESTION 62
- (Topic 2)
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.

NEW QUESTION 66
- (Topic 2)
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.

NEW QUESTION 70
- (Topic 2)
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.

NEW QUESTION 72
- (Topic 2)
A user has enabled the Multi AZ feature with the MS SQL RDS database server. Which of the below mentioned statements will help the user understand the Multi AZ feature better?

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

Answer: C

Explanation:

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

NEW QUESTION 77
- (Topic 2)
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.

NEW QUESTION 79
- (Topic 2)
A user has created a web application with Auto Scaling. The user is regularly monitoring the application and he observed that the traffic is highest on Thursday and Friday between 8 AM to 6 PM. What is the best solution to handle scaling in this case?

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

Answer: B

Explanation:

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

NEW QUESTION 83
- (Topic 2)
A root account owner has created an S3 bucket testmycloud. The account owner wants to allow everyone to upload the objects as well as enforce that the person who uploaded the object should manage the permission of those objects. Which is the easiest way to achieve this?

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

Answer: C

Explanation:

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

NEW QUESTION 84
- (Topic 2)
A user has configured ELB with two EBS backed EC2 instances. The user is trying to understand the DNS access and IP support for ELB. Which of the below mentioned statements may not help the user understand the IP mechanism supported by ELB?

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

Answer: D

Explanation:

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

NEW QUESTION 85
- (Topic 2)
A user is trying to save some cost on the AWS services. Which of the below mentioned options will not help him save cost?

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

Answer: B

Explanation:

AWS bills the user on a 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.

NEW QUESTION 87
- (Topic 2)
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. Non
D. It is not possible to configure the light with the AWS infrastructure services
E. 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.

NEW QUESTION 91
- (Topic 2)
A user has launched an EBS backed EC2 instance. The user has rebooted the instance. Which of the below mentioned statements is not true with respect to the reboot action?

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

Answer: D

Explanation:

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

NEW QUESTION 96
- (Topic 2)
A user has launched a large EBS backed EC2 instance in the US-East-1a region. The user wants to achieve Disaster Recovery (DR. for that instance by creating another small instance in Europe. How can the user achieve DR?

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

Answer: B

Explanation:

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

NEW QUESTION 98
- (Topic 2)
A user has configured CloudWatch monitoring on an EBS backed EC2 instance. If the user has not attached any additional device, which of the below mentioned metrics will always show a 0 value?

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

Answer: A

Explanation:

CloudWatch is used to monitor AWS as 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.

NEW QUESTION 101
- (Topic 2)
An organization has created 50 IAM users. The organization has introduced a new policy which will change the access of an IAM user. How can the organization implement this effectively so that there is no need to apply the policy at the individual user level?

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

Answer: A

Explanation:

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

NEW QUESTION 106

- (Topic 2)
A user has configured an Auto Scaling group with ELB. The user has enabled detailed CloudWatch monitoring on Elastic Load balancing. Which of the below mentioned statements will help the user understand this functionality better?

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

Answer: A

Explanation:

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

NEW QUESTION 111
- (Topic 2)
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.

NEW QUESTION 115
- (Topic 2)
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.

NEW QUESTION 118
- (Topic 2)
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 capacit
E. 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.

NEW QUESTION 120
- (Topic 2)
An organization wants to move to Cloud. They are looking for a secure encrypted database storage option. Which of the below mentioned AWS functionalities

helps them to achieve this?

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

Answer: B

Explanation:

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

NEW QUESTION 124
- (Topic 2)
A user is publishing custom metrics to CloudWatch. Which of the below mentioned statements will help the user understand the functionality better?

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

Answer: B

Explanation:

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

NEW QUESTION 129
- (Topic 2)
A user has configured a VPC with a new subnet. The user has created a security group. The user wants to configure that instances of the same subnet communicate with each other. How can the user configure this with the security group?

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

Answer: C

Explanation:

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

NEW QUESTION 131
- (Topic 2)
A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

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

Answer: D

Explanation:

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

NEW QUESTION 133
- (Topic 3)
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.

NEW QUESTION 136
- (Topic 3)
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.

NEW QUESTION 137
- (Topic 3)
What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment if the primary DB instance fails?

A. The IP of the primary DB Instance is switched to the standby DB Instanc
B. A new DB instance is created in the standby availability zon
C. The canonical name record (CNAME) is changed from primary to standb
D. The RDS (Relational Database Service) DB instance reboot

Answer: D

Explanation:
Reference:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RebootInstance.html

NEW QUESTION 139
- (Topic 3)
A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling terminate process only for a while. What will happen to the availability zone rebalancing process (AZRebalance. during this period?

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

Answer: B

Explanation:

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

NEW QUESTION 142
- (Topic 3)
A sys admin has enabled logging on ELB. Which of the below mentioned fields will not be a part of the log file name?

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

Answer: B

Explanation:

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

NEW QUESTION 144
- (Topic 3)
A user is trying to connect to a running EC2 instance using SSH. However, the user gets an Unprotected Private Key File error. Which of the below mentioned options can be a possible reason for rejection?

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

Answer: A

Explanation:

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

NEW QUESTION 147
- (Topic 3)
A user has launched an EC2 instance store backed instance in the US-East-1a zone. The user created AMI #1 and copied it to the Europe region. After that, the user made a few updates to the application running in the US-East-1a zone. The user makes an AMI#2 after the changes. If the user launches a new instance in Europe from the AMI #1 copy, which of the below mentioned statements is true?

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

Answer: D

Explanation:

Within EC2, when the user copies an AMI, the new AMI is fully independent of the source AMI; there is no link to the original (source. AMI. The user can modify the source AMI without affecting the new AMI and vice 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.

NEW QUESTION 151
- (Topic 3)
A system admin is planning to encrypt all objects being uploaded to S3 from an application. The system admin does not want to implement his own encryption algorithm; instead he is planning to use server side encryption by supplying his own key (SSE-C.. Which parameter is not required while making a call for SSE-C?

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

Answer: A

Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key (SSE-C.. When the user is supplying his own encryption key, the user has to send the below mentioned parameters as a part of the API calls: x-amz-server-side-encryption-customer-algorithm: Specifies the encryption algorithm x-amz-server-side-encryption-customer-key: To provide the base64-encoded encryption key x-amz-server-side-encryption-customer-key-MD5: To provide the base64-encoded 128-bit MD5 digest of the encryption key

NEW QUESTION 155
- (Topic 3)
Which of the following statements about this S3 bucket policy is true?

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


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

Answer: C

NEW QUESTION 159
- (Topic 3)
A user has created an Auto Scaling group with default configurations from CLI. The user wants to setup the CloudWatch alarm on the EC2 instances, which are launched by the Auto Scaling group. The user has setup an alarm to monitor the CPU utilization every minute. Which of the below mentioned statements is true?

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

Answer: B

Explanation:

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

NEW QUESTION 162
- (Topic 3)
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.

NEW QUESTION 164
- (Topic 3)
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.

NEW QUESTION 167
- (Topic 3)
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.

NEW QUESTION 168
- (Topic 3)
A user has enabled detailed CloudWatch monitoring with the AWS Simple Notification Service. Which of the below mentioned statements helps the user understand detailed monitoring better?

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

Answer: D

Explanation:

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

NEW QUESTION 173
- (Topic 3)
A user has created a VPC with public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24 . 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.

NEW QUESTION 175
- (Topic 3)
A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?

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

D. It will throw a CIDR overlaps error

Answer: D

Explanation:

A Virtual Private Cloud (VPC. is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet.

NEW QUESTION 179
- (Topic 3)
A user wants to upload a complete folder to AWS S3 using the S3 Management console. How can the user perform this activity?

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

Answer: D

Explanation:

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

NEW QUESTION 184
- (Topic 3)
A user is collecting 1000 records per second. The user wants to send the data to CloudWatch using the custom namespace. Which of the below mentioned options is recommended for this activity?

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

Answer: A

Explanation:

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

NEW QUESTION 189
- (Topic 3)
A user has configured an EC2 instance in the US-East-1a zone. The user has enabled detailed monitoring of the instance. The user is trying to get the data from CloudWatch using a CLI. Which of the below mentioned CloudWatch endpoint URLs should the user use?

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

Answer: A

Explanation:

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

NEW QUESTION 191
- (Topic 3)
How can an EBS volume that is currently attached to an EC2 instance be migrated from one Availability Zone to another?

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

Answer: D

Explanation:

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

NEW QUESTION 195
- (Topic 3)
A root account owner has given full access of his S3 bucket to one of the IAM users using the bucket ACL. When the IAM user logs in to the S3 console, which actions can he perform?

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

Answer: C

Explanation:

Each AWS S3 bucket and object has an ACL (Access Control List. associated with it. An ACL is a list of grants identifying the grantee and the permission granted. The user can use ACLs to grant basic read/write permissions to other AWS accounts. ACLs use an Amazon S3–specific XML schema. The user cannot grant permissions to other users (IAM users. in his account.

NEW QUESTION 198
- (Topic 3)
A user has created a VPC with public and private subnets using the VPC wizard. The user has not launched any instance manually and is trying to delete the VPC. What will happen in this scenario?

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

Answer: D

Explanation:

A Virtual Private Cloud (VPC. is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance with an elastic IP. If the user is trying to delete the VPC it will not allow as the NAT instance is still running.

NEW QUESTION 203
- (Topic 3)
A user is observing the EC2 CPU utilization metric on CloudWatch. The user has observed some interesting patterns while filtering over the 1 week period for a particular hour. The user wants to zoom that data point to a more granular period. How can the user do that easily with CloudWatch?

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

Answer: A

NEW QUESTION 207
- (Topic 3)
A user is trying to setup a security policy for ELB. The user wants ELB to meet the cipher supported by the client by configuring the server order preference in ELB security policy. Which of the below mentioned
preconfigured policies supports this feature?

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

Answer: A

Explanation:

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

NEW QUESTION 208
- (Topic 3)
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

NEW QUESTION 210
- (Topic 3)
A user has launched an EBS backed EC2 instance in the US-East-1a region. The user stopped the instance and started it back after 20 days. AWS throws up an 'InsufficientInstanceCapacity' error. What can be the possible reason for this?

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

Answer: A

Explanation:

When the user gets an 'InsufficientInstanceCapacity' error while launching or starting an EC2 instance, it means that AWS does not currently have enough available capacity to service the user request. If the user is requesting a large number of instances, there might not be enough server capacity to host them. The user can either try again later, by specifying a smaller number of instances or changing the availability zone if launching a fresh instance.

NEW QUESTION 215
- (Topic 3)
You run a web application with the following components Elastic Load Balancer (EL8), 3 Web/Application servers, 1 MySQL RDS database with read replicas, and Amazon Simple Storage Service (Amazon S3) for static content. Average response time for users is increasing slowly.
What three CloudWatch RDS metrics will allow you to identify if the database is the bottleneck? Choose 3 answers

A. The number of outstanding IOs waiting to access the dis
B. The amount of write latenc
C. The amount of disk space occupied by binary logs on the maste
D. The amount of time a Read Replica DB Instance lags behind the source DB Instance
E. The average number of disk I/O operations per secon

Answer: ABD

NEW QUESTION 216
- (Topic 3)
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.

NEW QUESTION 218
- (Topic 3)
A user has created an EBS volume of 10 GB and attached it to a running instance. The user is trying to access EBS for first time. Which of the below mentioned options is the correct statement with respect to a first time EBS access?

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

Answer: B

Explanation:

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

better IO.

NEW QUESTION 221
- (Topic 3)
A user is creating a Cloudformation stack. Which of the below mentioned limitations does not hold true for Cloudformation?

A. One account by default is limited to 100 templates
B. The user can use 60 parameters and 60 outputs in a single template
C. The template, parameter, output, and resource description fields are limited to 4096 characters
D. One account by default is limited to 20 stacks

Answer: A

Explanation:

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

NEW QUESTION 226
- (Topic 3)
An organization has configured Auto Scaling for hosting their application. The system admin wants to understand the Auto Scaling health check process. If the instance is unhealthy, Auto Scaling launches an instance and terminates the unhealthy instance. What is the order execution?

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

Answer: D

Explanation:

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

NEW QUESTION 228
- (Topic 3)
An organization is planning to create a user with IAM. They are trying to understand the limitations of IAM so that they can plan accordingly. Which of the below mentioned statements is not true with respect to the limitations of IAM?

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

Answer: A

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The default maximums for each of the IAM entities is given below: Groups per AWS account: 100 Users per AWS account: 5000 Roles per AWS account: 250 Number of groups per user: 10 (that is, one user can be part of these many groups.

NEW QUESTION 229
- (Topic 3)
Your business is building a new application that will store its entire customer database on a RDS MySQL database, and will have various applications and users that will query that data for different purposes.
Large analytics jobs on the database are likely to cause other applications to not be able to get the query results they need to, before time out. Also, as your data grows, these analytics jobs will start to take more time, increasing the negative effect on the other applications.
How do you solve the contention issues between these different workloads on the same data?

A. Enable Multi-AZ mode on the RDS instance
B. Use ElastiCache to offload the analytics job data
C. Create RDS Read-Replicas for the analytics work
D. Run the RDS instance on the largest size possible

Answer: B

NEW QUESTION 234
- (Topic 3)
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.

NEW QUESTION 238
- (Topic 3)
An organization (account ID 123412341234. has configured the IAM policy to allow the user to modify his credentials. What will the below mentioned statement allow the user to perform?

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 241
- (Topic 3)
An application you maintain consists of multiple EC2 instances in a default tenancy VPC. This application has undergone an internal audit and has been determined to require dedicated hardware for one instance. Your compliance team has given you a week to move this instance to single-tenant hardware. Which process will have minimal impact on your application while complying with this requirement?

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

Answer: A

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

NEW QUESTION 243
- (Topic 3)
When you put objects in Amazon S3, what is the indication that an object was successfully stored?

A. Each S3 account has a special bucket named_s3_log
B. Success codes are written to this bucket with a timestamp and checksu
C. A success code is inserted into the S3 object metadat

D. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successfu
E. Amazon S3 is engineered for 99.999999999% durabilit
F. Therefore there is no need to confirm that data was inserte

Answer: B

Explanation:
Reference:
http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPUT.html

NEW QUESTION 248
- (Topic 3)
A user has launched an RDS postgreSQL DB with AWS. The user did not specify the maintenance window during creation. The user has configured RDS to update the DB instance type from micro to large. If the user wants to have it during the maintenance window, what will AWS do?

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

Answer: B

Explanation:

AWS RDS has a compulsory maintenance window which by default is 30 minutes. If the user does not specify the maintenance window during the creation of RDS then AWS will select a 30-minute maintenance window randomly from an 8-hour block of time per region. In this case, Amazon RDS assigns a 30-minute maintenance window on a randomly selected day of the week.

NEW QUESTION 250
- (Topic 3)
A user has a weighing plant. The user measures the weight of some goods every 5 minutes and sends data to AWS CloudWatch for monitoring and tracking. Which of the below mentioned parameters is mandatory for the user to include in the request list?

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

Answer: B

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user can publish the data to CloudWatch as single data points or as an aggregated set of data points called a statistic set. The user has to always include the namespace as part of the request. The user can supply a file instead of the metric name. If the user does not supply the timezone, it accepts the current time. If the user is sending the data as a single data point it will have parameters, such as value. However, if the user is sending as an aggregate it will have parameters, such as statistic-values.

NEW QUESTION 255
- (Topic 3)
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.

NEW QUESTION 256
- (Topic 3)
A user has launched an EC2 instance from an instance store backed AMI. The infrastructure team wants to create an AMI from the running instance. Which of the below mentioned credentials is not required while creating the AMI?

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

Answer: C

Explanation:

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

NEW QUESTION 259
- (Topic 3)
A user has moved an object to Glacier using the life cycle rules. The user requests to restore the archive after 6 months. When the restore request is completed the user accesses that archive. Which of the below mentioned statements is not true in this condition?

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

Answer: B

Explanation:

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

NEW QUESTION 263
- (Topic 3)
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.

NEW QUESTION 265
- (Topic 3)
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.

NEW QUESTION 270
- (Topic 3)
A user has configured an HTTPS listener on an ELB. The user has not configured any security policy which can help to negotiate SSL between the client and ELB. What will ELB do in this scenario?

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

Answer: B

Explanation:

Elastic Load Balancing uses a Secure Socket Layer (SSL. negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. If the user has created an HTTPS/SSL listener without associating any security policy, Elastic Load Balancing will, bydefault, associate the latest version of the ELBSecurityPolicy-YYYY-MM with the load balancer.

NEW QUESTION 274
- (Topic 3)
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.

NEW QUESTION 278
- (Topic 3)
A user is receiving a notification from the RDS DB whenever there is a change in the DB security group. The user does not want to receive these notifications for only a month. Thus, he does not want to delete the notification. How can the user configure this?

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

Answer: D

Explanation:

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

NEW QUESTION 283
- (Topic 3)
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

NEW QUESTION 285
- (Topic 3)
A user has launched an EC2 Windows instance from an instance store backed AMI. The user has also set the Instance initiated shutdown behavior to stop. What will happen when the user shuts down the OS?

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

Answer: B

Explanation:

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

NEW QUESTION 288
- (Topic 3)
A user has created a VPC with public and private subnets using the VPC Wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24. Which of the below mentioned entries are required in the main route table to allow the instances in VPC to communicate with each other?

A. Destination : 20.0.0.0/24 and Target : VPC

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

Answer: D

NEW QUESTION 289
- (Topic 3)
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.

NEW QUESTION 294
- (Topic 3)
A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. The ELB security policy supports various ciphers. Which of the below mentioned options helps identify the matching cipher at the client side to the ELB cipher list when client is requesting ELB DNS over SSL?

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

Answer: C

Explanation:

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

NEW QUESTION 295
- (Topic 3)
A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet. How can the instances in the private subnet connect to 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..

NEW QUESTION 297
- (Topic 3)
Which of the below mentioned AWS RDS logs cannot be viewed from the console for MySQL?

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

Answer: C

Explanation:

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

NEW QUESTION 299
- (Topic 3)
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.

NEW QUESTION 300
- (Topic 3)
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

NEW QUESTION 305
- (Topic 3)
A user is trying to create a PIOPS EBS volume with 4000 IOPS and 100 GB size. AWS does not allow the user to create this volume. What is the possible root cause for this?

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

Answer: A

Explanation:

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

NEW QUESTION 310
- (Topic 3)
A user has created a queue named "awsmodule" with SQS. One of the consumers of queue is down for 3 days and then becomes available. Will that component receive message from queue?

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

Answer: A

Explanation:

SQS allows the user to move data between distributed components of applications so they can perform different tasks without losing messages or requiring each component to be always available. Queues retain messages for a set period of time. By default, a queue retains messages for four days. However, the user can configure a queue to retain messages for up to 14 days after the message has been sent.

NEW QUESTION 315
- (Topic 3)
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

NEW QUESTION 317
- (Topic 3)
A user is configuring the Multi AZ feature of an RDS DB. The user came to know that this RDS DB does not use the AWS technology, but uses server mirroring to achieve HA. Which DB is the user using right now?

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

Answer: C

Explanation:

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

NEW QUESTION 319
- (Topic 3)
In order to optimize performance for a compute cluster that requires low inter-node latency, which feature in the following list should you use?

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

Answer: D

NEW QUESTION 321
- (Topic 3)
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.

NEW QUESTION 324
- (Topic 3)
A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption (SSE-C., 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

NEW QUESTION 328
- (Topic 3)
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.

NEW QUESTION 330
- (Topic 3)
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]
}]

NEW QUESTION 333
- (Topic 3)
An organization is measuring the latency of an application every minute and storing data inside a file in the JSON format. The organization wants to send all latency data to AWS CloudWatch. How can the organization achieve this?

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

Answer: C

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user has to always include the namespace as part of the request. If the user wants to upload the custom data from a Amazon AWS-SysOps : Practice Test file, he can supply file name along with the parameter -- metric-data to command put-metric-data.

NEW QUESTION 336
- (Topic 3)
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.

NEW QUESTION 341
- (Topic 3)
A user has granted read/write permission of his S3 bucket using ACL. Which of the below mentioned options is a valid ID to grant permission to other AWS accounts (grantee. using ACL?

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

Answer: D

Explanation:

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

NEW QUESTION 346
- (Topic 3)
A user has launched a Windows based EC2 instance. However, the instance has some issues and the user wants to check the log. When the user checks the Instance console output from the AWS console, what will it display?

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

Answer: D

Explanation:

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

NEW QUESTION 350
- (Topic 3)
An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

A. Create an IAM policy with the security group and use that security group for AWS console login
B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization
C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
D. Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

Answer: B

Explanation:

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

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

NEW QUESTION 352
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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