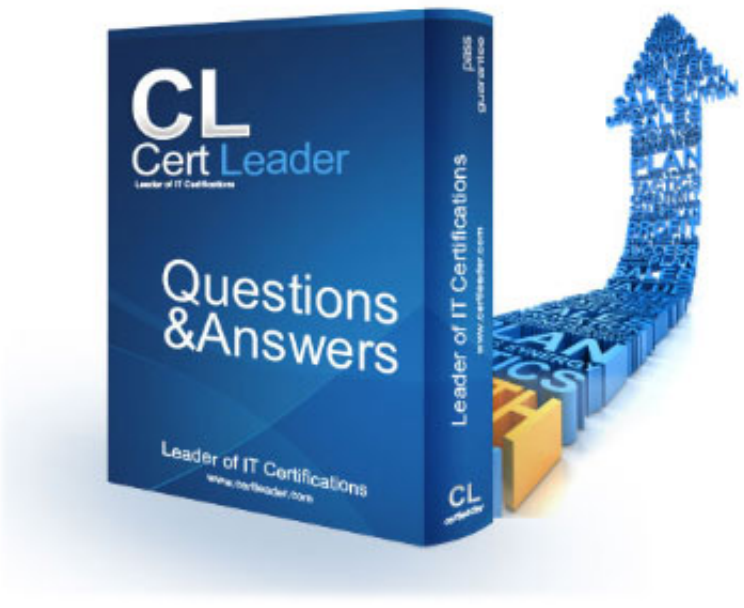
SOA-C01 Dumps

AWS Certified SysOps Administrator - Associate

https://www.certleader.com/SOA-C01-dumps.html



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

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

Answer: B

Explanation:
As the EC2 limit per region is max 20. You will need to fill an Amazon EC2 instance request form to increase the EC2 instances to 175.
http://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2
I don??t think the answer can be D, as the question says ??expects a steady ramp up in traffic to follow an upcoming campaign that will result in a 20x growth in traffic over 4 weeks??. To pre-warm your ELB, you have to put in a request to AWS. You can??t do it.
Q: How do I reserve capacity for an existing, running instance?
To reserve capacity for a running instance, you can purchase a Reserved Instance or modify an existing reservation so it matches your instance's specifications. You can purchase Reserved Instances via the Amazon EC2 Console or by using the PurchaseReservedInstancesOffering API. You can modify existing Reserved Instances via the Amazon EC2 Console or by using the ModifyReservedInstances API call.
In both cases, the reservation must match the following attributes of the running instance you want to cover:
Availability Zone (e.g., us-east-1a) Instance type (e.g., m3.large)
Platform (e.g., Linux/UNIX (Amazon VPC)) Tenancy (e.g., default)
Q: How do I control which instances are billed at the lower rate?
The RunInstances API command does not distinguish between On-Demand instances and the reservations that can be applied to them. When computing your bill, our system will automatically optimize which instances are charged at the lower rate to ensure you always pay the lowest amount. For information about hourly billing, and how it applies to Reserved Instances, see Billing Benefits and Payment Options.
Q: How many Reserved Instances can I purchase?
You can purchase up to 20 Reserved Instances per Availability Zone each month. If you need additional Reserved Instances, complete the form found here. Information about previous generation Reserved Instance types can be found here.
Q: Can I reassign my Reserved Instance from one instance type (e.g., c1.xlarge) to another (e.g., m1.large)?
No. A Reserved Instance is associated with a specific instance type for the duration of its term; however, you can change from one instance size (e.g., c3.large) to another (e.g., c3.xlarge) in the same type, if it is a Linux/UNIX Reserved Instance.
Q: Can I move a Reserved Instance from one region to another?
No. A Reserved Instance is associated with a specific region, which is fixed for the duration of the reservation's term.
Q: Can I modify a Reserved Instance?
Yes. You can request to modify active reservations that you own in one of the following ways: Move between Availability Zones within the same region. Change the network platform from EC2-Classic to EC2-VPC (for EC2-Classic-enabled customers). Change the instance type of your Linux/UNIX Reserved Instances to a larger or smaller size in the same instance type (e.g., convert 8 m1.smalls into 4 m1.mediums, or vice versa).
Instance type modifications are only supported for Linux/UNIX platform reservations. However, due to licensing differences Linux Reserved Instances cannot be modified to RedHat or SUSE Linux Reserved Instances.
The reservations that you modify must have been purchased on the same day, be the same instance type, and in the same Availability Zone and region. It is not possible to combine reservations. However, if you have multiple instances in the same reservation (i.e., the reservation was purchased to apply to 10 instances), you can modify each of these instances either individually or as a whole.
Q: How do I request changes or modifications?
You can submit a modification request from the Amazon EC2 Console or by using the ModifyReservedInstances API. We process your requests as soon as possible, depending on available capacity. There is no additional cost for modifying your Reserved Instances.
To learn more about modification, see the Amazon EC2 User Guide.

NEW QUESTION 2
You have an Auto Scaling group associated with an Elastic Load Balancer (ELB). You have noticed that instances launched via the Auto Scaling group are being marked unhealthy due to an ELB health check, but these unhealthy instances are not being terminated.
What do you need to do to ensure trial instances marked unhealthy by the ELB will be terminated and replaced?

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

Answer: B

Explanation:
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-add-elb-healthcheck.html
Add an Elastic Load Balancing Health Check to your Auto Scaling Group
By default, an Auto Scaling group periodically reviews the results of EC2 instance status to determine the health state of each instance. However, if you have associated your Auto Scaling group with an Elastic Load Balancing load balancer, you can choose to use the Elastic Load Balancing health check. In this case, Auto Scaling determines the health status of your instances by checking the results of both the EC2 instance status check and the Elastic Load Balancing instance health check.
For information about EC2 instance status checks, see Monitor Instances With Status Checks in the Amazon EC2 User Guide for Linux Instances. For information about Elastic Load Balancing health checks, see Health Check in the Elastic Load Balancing Developer Guide.
This topic shows you how to add an Elastic Load Balancing health check to your Auto Scaling group, assuming that you have created a load balancer and have registered the load balancer with your Auto Scaling group. If you have not registered the load balancer with your Auto Scaling group, see Set Up a Scaled and Load-Balanced Application.
Auto Scaling marks an instance unhealthy if the calls to the Amazon EC2 action DescribeInstanceStatus return any state other than running, the system status shows impaired, or the calls to Elastic Load Balancing action DescribeInstanceHealth returns OutOfService in the instance state field.
If there are multiple load balancers associated with your Auto Scaling group, Auto Scaling checks the health state of your EC2 instances by making health check calls to each load balancer. For each call, if the Elastic Load Balancing action returns any state other than InService, the instance is marked as

unhealthy. After Auto Scaling marks an instance as unhealthy, it remains in that state, even if subsequent calls from other load balancers return an InService state for the same instance.

NEW QUESTION 3
An application that you are managing has EC2 instances & Dynamo OB tables deployed to several AWS Regions. In order to monitor the performance of the application globally, you would like to see two graphs: 1) Avg CPU Utilization across all EC2 instances and 2) Number of Throttled Requests for all DynamoDB tables.
How can you accomplish this?

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

Answer: A

Explanation:
Correct answer should be A. When you turn on detailed monitoring in CloudWatch, you can get 1) Avg CPU Utilization across all EC2 instances and 2) Number of Throttled Requests for all DynamoDB tables
Reference: http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/GetSingleMetricAllDimen sions.html

NEW QUESTION 4
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. N
B. 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 (i.e., broadcast) boundaries
C. Ye
D. 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
E. Ye
F. The security group for the monitoring instance needs to allow outbound ICMP and the application instance's security group needs to allow Inbound ICMP
G. 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: C

NEW QUESTION 5
You have a web-style application with a stateless but CPU and memory-intensive web tier running on
a cc2 8xlarge EC2 instance inside of a VPC The instance when under load is having problems returning requests within the SLA as defined by your business The application maintains its state in a DynamoDB table, but the data tier is properly provisioned and responses are consistently fast.
How can you best resolve the issue of the application responses not meeting your SLA?

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

Answer: C

Explanation:
But it is possibly A as DynamoDB is automatically available across three facilities in an AWS Region. So moving in to a same AZ is not possible / necessary.
In this case the DB layer is not the issue, the EC2 8xlarge is the issue; so add another one with a ELB in-frond of it.
See also: https://aws.amazon.com/dynamodb/faqs/

NEW QUESTION 6
You are managing a legacy application Inside VPC with hard coded IP addresses in its configuration. Which two mechanisms will allow the application to failover to new instances without the need for reconfiguration? Choose 2 answers

A. Create an ELB to reroute traffic to a failover instance
B. Create a secondary ENI that can be moved to a failover instance
C. Use Route53 health checks to fail traffic over to a failover instance
D. Assign a secondary private IP address to the primary ENI0 that can be moved to a failover instance

Answer: BD

Explanation:
This is an odd question. First of all, option A cannot be right because ELB does not failover. Cannot be C because Route 53 does work with hard coded IP. Only B & D cannot be rule out so best answer.

NEW QUESTION 7
Your EC2-Based Multi-tier application includes a monitoring instance that periodically makes application -level read only requests of various application components and if any of those fail more than three times 30 seconds calls CloudWatch lo fire an alarm, and the alarm notifies your operations team by email and SMS of a possible application health problem. However, you also need to ??watch the watcher?? --the monitoring instance itself - and be notified if it becomes

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

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

Answer: B

NEW QUESTION 8
You are attempting to connect to an instance in Amazon VPC without success. You have already verified that the VPC has an Internet Gateway (IGW) the instance has an associated Elastic IP (EIP) and correct security group rules are in place.
Which VPC component should you evaluate next?

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

Answer: B

Explanation:
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/UserScenariosForVPC.ht ml

NEW QUESTION 9
You are tasked with the migration of a highly trafficked Node JS application to AWS In order to comply with organizational standards Chef recipes must be used to configure the application servers that host this application and to support application lifecycle events.
Which deployment option meets these requirements while minimizing administrative burden?

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

Answer: A

Explanation:
OpsWorks has integrated support for Chef and lifecycle events.
See: http://docs.aws.amazon.com/opsworks/latest/userguide/workingcookbook.html

NEW QUESTION 10
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 10
An organization's security policy requires multiple copies of all critical data to be replicated across at least a primary and backup data center. The organization has decided to store some critical data on Amazon S3.
Which option should you implement to ensure this requirement is met?

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

Answer: D

Explanation:
It seems that this question wants to emphasize below (S3 Faq ?V https://aws.amazon.com/s3/faqs/) You specify a region when you create your Amazon S3 bucket. Within that region, your objects are redundantly stored on multiple devices across multiple facilities. Please refer to Regional Products and Services for details of Amazon S3 service availability by region.

NEW QUESTION 13
You are tasked with setting up a cluster of EC2 Instances for a NoSQL database. The database requires random read IO disk performance up to a 100,000 IOPS at 4KB block side per node.

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

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

Answer: C

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

NEW QUESTION 16
When an EC2 EBS-backed (EBS root) instance is stopped, what happens to the data on any ephemeral store volumes?

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

Answer: A

Explanation:
See: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store- lifetime
However, data in the instance store is lost under the following circumstances:
?V The underlying disk drive fails
?V The instance stops
?V The instance terminates

NEW QUESTION 21
A user has developed an application which is required to send the data to a NoSQL database. The user wants to decouple the data sending such that the application keeps processing and sending data but does not wait for an acknowledgement of DB. Which of the below mentioned applications helps in this scenario?

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

Answer: C

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

NEW QUESTION 22
A user has recently started using EC2. The user launched one EC2 instance in the default subnet in EC2-VPC Which of the below mentioned options is not attached or available with the EC2 instance when it is launched?

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

Answer: C

Explanation:
A Virtual Private Cloud (VPC. is a virtual network dedicated to a user??s AWS account. A subnet is a range of IP addresses in the VPC. The user can launch the AWS resources into a subnet. There are two supported platforms into which a user can launch instances: EC2-Classic and EC2-VPC (default subnet. A default VPC has all the benefits of EC2-VPC and the ease of use of EC2-Classic. Each instance that the user launches into a default subnet has a private IP address and a public IP address. These instances can communicate with the internet through an internet gateway. An internet gateway enables the EC2 instances to connect to the internet through the Amazon EC2 network edge.

NEW QUESTION 23
A user has launched an EC2 instance. The user is planning to setup the CloudWatch alarm. Which of the below mentioned actions is not supported by the CloudWatch alarm?

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

Answer: A

Explanation:

A user can create a CloudWatch alarm that takes various actions when the alarm changes state. An alarm watches a single metric over the time period that the user has specified, and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The actions could be sending a notification to an Amazon Simple Notification Service topic (SMS, Email, and HTTP end point notifying the Auto Scaling policy or changing the state of the instance to Stop/Terminate.
CloudWatch cannot change the auto-scaling launch configuration.
B ?V It can send an SMS with SNS
C ?V Auto-scaling uses CloudWatch metrics to scale up and down.
D ?V CloudWatch can stop instances

NEW QUESTION 25
A user has deployed an application on his private cloud. The user is using his own monitoring tool. He wants to configure that whenever there is an error, the monitoring tool should notify him via SMS. Which of the below mentioned AWS services will help in this scenario?

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

Answer: B

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

NEW QUESTION 30
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.
http://docs.aws.amazon.com/cli/latest/reference/opsworks/set-time-based-auto-scaling.html

NEW QUESTION 33
A user has setup a CloudWatch alarm on an EC2 action when the CPU utilization is above 75%. The alarm sends a notification to SNS on the alarm state. If the user wants to simulate the alarm action how can he achieve this?

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

Answer: C

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

NEW QUESTION 37
A sysadmin 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

NEW QUESTION 41
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 46
An organization is planning to use AWS for their production roll out. The organization wants to implement automation for deployment such that it will automatically create a LAMP stack, download the latest PHP installable from S3 and setup the ELB. Which of the below mentioned AWS services meets the requirement for making an orderly deployment of the software?

A. AWS Elastic Beanstalk
B. AWS CloudFront
C. AWS CloudFormation
D. AWS DevOps

Answer: C

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

NEW QUESTION 51
An organization is setting up programmatic billing access for their AWS account. Which of the below mentioned services is not required or enabled when the organization wants to use programmatic access?

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

Answer: C

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

NEW QUESTION 55
An admin is planning to monitor the ELB. Which of the below mentioned services does not help the admin capture the monitoring information about the ELB activity?

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

Answer: B

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

NEW QUESTION 57
A user is planning to use AWS CloudFormation. Which of the below mentioned functionalities does not help him to correctly understand CloudFormation?

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

Answer: A

Explanation:
AWS CloudFormation is an application management tool which provides application modelling, deployment, configuration, management and related activities. It supports a wide variety of AWS services, such as EC2, EBS, AS, ELB, RDS, VPC, etc. It also provides application bootstrapping scripts which enable the user to

install software packages or create folders. It is free of the cost and only charges the user for the services created with it. The only challenge is that it does not follow any model, such as DevOps; instead customers can define templates and use them to provision and manage the AWS resources in an orderly way.

NEW QUESTION 60
A system admin is planning to setup event notifications on RDS. Which of the below mentioned services will help the admin setup notifications?

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

Answer: D

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

NEW QUESTION 61
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 65
A system admin is managing buckets, objects and folders with AWS S3. Which of the below mentioned statements is true and should be taken in consideration by the sysadmin?

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

Answer: A

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

NEW QUESTION 69
An organization has created 50 IAM users. The organization wants that each user can change their password but cannot change their access keys. How can the organization achieve this?

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

Answer: D

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

NEW QUESTION 72
A user has created a photo editing software and hosted it on EC2. The software accepts requests from the user about the photo format and resolution and sends a message to S3 to enhance the picture accordingly. Which of the below mentioned AWS services will help make a scalable software with the AWS infrastructure in this scenario?

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

Answer:

D

Explanation:
Amazon Simple Queue Service (SQS. is a fast, reliable, scalable, and fully managed message queuing service. SQS provides a simple and cost-effective way to decouple the components of an application. The user can configure SQS, which will decouple the call between the EC2 application and S3. Thus, the application does not keep waiting for S3 to provide the data.

NEW QUESTION 77
A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25. The user is trying to create the private subnet with CIDR 20.0.0.128/25. Which of the below mentioned statements is true in this scenario?

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

Answer: B

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

NEW QUESTION 82
A sys admin is maintaining an application on AWS. The application is installed on EC2 and user has configured ELB and Auto Scaling. Considering future load increase, the user is planning to launch new servers proactively so that they get registered with ELB. How can the user add these instances with Auto Scaling?

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

Answer: A

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

NEW QUESTION 86
A sysadmin has created a shopping cart application and hosted it on EC2. The EC2 instances are running behind ELB. The admin wants to ensure that the end user request will always go to the EC2 instance where the user session has been created. How can the admin configure this?

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

Answer: C

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

NEW QUESTION 91
A user is planning to setup notifications on the RDS DB for a snapshot. Which of the below mentioned event categories is not supported by RDS for this snapshot source type?

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

Answer: A

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

NEW QUESTION 94
A customer is using AWS for Dev and Test. The customer wants to setup the Dev environment with Cloudformation. Which of the below mentioned steps are not required while using Cloudformation?

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

Answer: B

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

NEW QUESTION 98
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 101
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 106
A user is checking the CloudWatch metrics from the AWS console. The user notices that the CloudWatch data is coming in UTC. The user wants to convert the data to a local time zone. How can the user perform this?

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

Answer: B

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

NEW QUESTION 108
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 112
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?Vspecific 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 116
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 118
A user has setup an RDS DB with Oracle. The user wants to get notifications when someone modifies the security group of that DB. How can the user configure that?

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

Answer: C

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

NEW QUESTION 121
A user is trying to understand the ACL and policy for an S3 bucket. Which of the below mentioned policy permissions is equivalent to the WRITE ACL on a bucket?

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

Answer: D

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

NEW QUESTION 126
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. Setting 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 128
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 132
A user has launched multiple EC2 instances for the purpose of development and testing in the same region. The user wants to find the separate cost for the production and development instances. How can the user find the cost distribution?

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

Answer: D

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

NEW QUESTION 133
A user has created a VPC with the public subnet. The user has created a security group for that VPC. Which of the below mentioned statements is true when a security group is created?

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

Answer: C

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

NEW QUESTION 135
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 137
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 138
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 143
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 146
A user has enabled session stickiness with ELB. The user does not want ELB to manage the cookie; instead he wants the application to manage the cookie. What will happen when the server instance, which is bound to a cookie, crashes?

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

Answer: B

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

NEW QUESTION 151

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

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

Answer: D

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

NEW QUESTION 155
An organization has applied the below mentioned policy on an IAM group which has selected the IAM users. What entitlements do the IAM users avail with this policy?
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
]
}

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

Answer: C

Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The IAM group allows the organization to specify permissions for a collection of users. With the below mentioned policy, it will allow the group full access (Admin. to all AWS services.
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
]
}

NEW QUESTION 158
A user is configuring a CloudWatch alarm on RDS to receive a notification when the CPU utilization of RDS is higher than 50%. The user has setup an alarm when there is some inactivity on RDS, such as RDS unavailability. How can the user configure this?

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

Answer: B

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

NEW QUESTION 161
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 166
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 167
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 171
A user is measuring the CPU utilization of a private data centre machine every minute. The machine provides the aggregate of data every hour, such as Sum of data??, ??Min value??, ??Max value, and ??Number of Data points??.
The user wants to send these values to CloudWatch. How can the user achieve this?

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

Answer: C

Explanation:
AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user can publish the data to CloudWatch as single data points or as an aggregated set of data points called a statistic set using the command put- metric-data. When sending the aggregate data, the user needs to send it with the parameter statistic-values:
awscloudwatch put-metric-data --metric-name <Name> --namespace <Custom namespace -- timestamp
<UTC Format> --statistic-values Sum=XX,Minimum=YY,Maximum=AA,SampleCount=BB --unit Milliseconds

NEW QUESTION 176
A user wants to find the particular error that occurred on a certain date in the AWS MySQL RDS DB. Which of the below mentioned activities may help the user to get the data easily?

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

Answer: C

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

NEW QUESTION 179

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 20.0.0.1/24. How can the user create the second subnet?

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

Answer: D

Explanation:
A Virtual Private Cloud (VPC. is a virtual network dedicated to the user??s AWS account. A user can create a subnet with VPC and launch instances inside the subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet. The user cannot modify the CIDR of a subnet once it is created. Thus, in this case if required, the user has to delete the subnet and create new subnets.

NEW QUESTION 182
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 186
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 188
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 192
A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public subnet (port 80. and a DB server in the private subnet (port 3306.. The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required for the NAT security group?

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

D. For Outbound allow Destination: 0.0.0.0/0 on port 443

Answer: C

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

NEW QUESTION 197
A sys admin is trying to understand the sticky session algorithm. Please select the correct sequence of steps, both when the cookie is present and when it is not, to help the admin understand the implementation of the sticky session:
ELB inserts the cookie in the response
ELB chooses the instance based on the load balancing algorithm Check the cookie in the service request
The cookie is found in the request
The cookie is not found in the request

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

Answer: C

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

NEW QUESTION 200
A user has scheduled the maintenance window of an RDS DB on Monday at 3 AM. Which of the below mentioned events may force to take the DB instance offline during the maintenance window?

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

Answer: D

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

NEW QUESTION 204
A user is having data generated randomly based on a certain event. The user wants to upload that data to CloudWatch. It may happen that event may not have data generated for some period due to andomness. Which of the below mentioned options is a recommended option for this case?

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

Answer: C

Explanation:
AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. When the user data is more random and not generated at regular intervals, there can be a period which has no associated data. The user can either publish the zero (0. Value for that period or not publish the data at all. It is recommended that the user should publish zero instead of no value to monitor the health of the application. This is helpful in an alarm as well as in the generation of the sample data count.

NEW QUESTION 206
A user is sending the data to CloudWatch using the CloudWatch API. The user is sending data 90 minutes in the future. What will CloudWatch do in this case?

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

Answer: A

Explanation:

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

NEW QUESTION 209
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 211
The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?

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

Answer: C

Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the CFO wants to allow only AWS usage report page access, the policy for that IAM user will be as given below:
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow", "Action": [
"aws-portal:ViewUsage"
],
"Resource": "*"
}
]
}

NEW QUESTION 213
An organization has created 10 IAM users. The organization wants each of the IAM users to have access to a separate DyanmoDB table. All the users are added to the same group and the organization wants to setup a group level policy for this. How can the organization achieve this?

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

Answer: D

Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. AWS DynamoDB has only tables and the organization cannot makeseparate databases. The organization should create a table with the same name as the IAM user name and use the ARN of DynamoDB as part of the group policy. The sample policy is shown below:
{
"Version": "2012-10-17",
"Statement": [{
"Effect": "Allow",
"Action": ["dynamodb:*"],
"Resource": "arn:aws:dynamodb:region:account-number-without-hyphens:table/${aws:username}"
}
]
}

NEW QUESTION 214
An organization has setup Auto Scaling with ELB. Due to some manual error, one of the instances got rebooted. Thus, it failed the Auto Scaling health check. Auto Scaling has marked it for replacement. How can the system admin ensure that the instance does not get terminated?

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

Answer: D

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

NEW QUESTION 216
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 217
A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AddToLoadBalancer
(which adds instances to the load balancer. process for a while. What will happen to the instances launched during the suspension period?

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

Answer: A

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

NEW QUESTION 221
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 224
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 225
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 230
Which services allow the customer to retain run administrative privileges or the undertying EC2 instances? Choose 2 answers

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

Answer: AB

NEW QUESTION 233
You have a proprietary data store on-premises that must be backed up daily by dumping the data store contents to a single compressed 50GB file and sending the file to AWS. Your SLAs state that any dump file backed up within the past 7 days can be retrieved within 2 hours. Your compliance department has stated that all data must be held indefinitely. The time required to restore the data store from a backup is approximately 1 hour. Your on-premise network connection is capable of sustaining 1gbps to AWS.
Which backup methods to AWS would be most cost-effective while still meeting all of your requirements?

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

Answer: D

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

NEW QUESTION 236
Which method can be used to prevent an IP address block from accessing public objects in an S3 bucket?

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

Answer: A

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

NEW QUESTION 239
You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from pre-defined customer IP addresses.
Which two options meet this security requirement? Choose 2 answers

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

Answer: CD

NEW QUESTION 244
In AWS, which security aspects are the customer??s responsibility? Choose 4 answers

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

Answer: BCDF

Explanation:
Decommissioning is AWS responsibility not Customer.

NEW QUESTION 246
A .NET application that you manage is running in Elastic Beanstalk. Your developers tell you they will need access to application log files to debug issues that arise. The infrastructure will scale up and down.
How can you ensure the developers will be able to access only the log files?

A. Access the log files directly from Elastic Beanstalk
B. Enable log file rotation to S3 within the Elastic Beanstalk configuration
C. Ask your developers to enable log file rotation in the applications web.config file
D. Connect to each Instance launched by Elastic Beanstalk and create a Windows Scheduled task to rotate the log files to S3.

Answer: A

Explanation:
Reference:
http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.loggingS3.title.html

NEW QUESTION 247
A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region.
Test is peered to both Prod and Dev. All VPCs have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to Prod to speed up time to market. Which of the following options helps the company accomplish this?

A. Create a new peering connection Between Prod and Dev along with appropriate routes.
B. Create a new entry to Prod in the Dev route table using the peering connection as the target.
C. Attach a second gateway to De
D. Add a new entry in the Prod route table identifying the gateway as the target.
E. The VPCs have non-overlapping CIDR blocks in the same accoun
F. The route tables contain local routes for all VPCs.

Answer: A

Explanation:
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-pg.pdf

NEW QUESTION 249
An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group is configured to allow SSH from any IP address and deny all outbound traffic. What changes need to be made to allow SSH access to the instance?

A. The outbound security group needs to be modified to allow outbound traffic.
B. The outbound network ACL needs to be modified to allow outbound traffic.
C. Nothing, it can be accessed from any IP address using SSH.
D. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.

Answer: B

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

NEW QUESTION 252
Which of the following are true regarding encrypted Amazon Elastic Block Store (EBS) volumes? Choose 2 answers

A. Supported on all Amazon EBS volume types
B. Snapshots are automatically encrypted
C. Available to all instance types
D. Existing volumes can be encrypted
E. shared volumes can be encrypted

Answer: AB

Explanation:
This feature is supported on all Amazon EBS volume types (General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic). You can access encrypted Amazon EBS volumes the same way you access existing volumes; encryption and decryption are handled transparently and they require no additional action from you, your Amazon EC2 instance, or your application. Snapshots of encrypted Amazon EBS volumes are automatically encrypted, and volumes that are created from encrypted Amazon EBS snapshots are also automatically encrypted.
Reference: http://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

NEW QUESTION 254
A customer needs to capture all client connection information from their load balancer every five minutes. The company wants to use this data for analyzing traffic patterns and troubleshooting their applications. Which of the following options meets the customer requirements?

A. Enable AWS CloudTrail for the load balancer.
B. Enable access logs on the load balancer.
C. Install the Amazon CloudWatch Logs agent on the load balancer.
D. Enable Amazon CloudWatch metrics on the load balancer.

Answer: A

NEW QUESTION 258
An Auto-Scaling group spans 3 AZs and currently has 4 running EC2 instances. When Auto Scaling needs to terminate an EC2 instance by default, AutoScaling will:
Choose 2 answers

A. Allow at least five minutes for Windows/Linux shutdown scripts to complete, before terminating the instance.
B. Terminate the instance with the least active network connection
C. If multiple instances meet this criterion, one will be randomly selected.
D. Send an SNS notification, if configured to do so.
E. Terminate an instance in the AZ which currently has 2 running EC2 instances.
F. Randomly select one of the 3 AZs, and then terminate an instance in that AZ.

Answer: CD

Explanation:
http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-termination.html

NEW QUESTION 263
The Database Administrator learn is interested in performing manual backups of Amazon DRS Oracle DB instance.
What step be taken to perform the backups?

A. Attach an Amazon EBS volume with Oracle RMAN installed to the RDS instance
B. Take a snapshot of the EBS volume that is attached to the DB instance.
C. Install Oracle Secure Backup on the RDS instance and back up the Oracle database to Amazon S3
D. Take a snapshot of the DB instance

Answer: D

NEW QUESTION 266
A company uses AWS Organization with a multi-account structure. A Syslog Administrator was notified that an IAM user with the System Administrator policy applied was not able to launch any Amazon EC2 instance using a public?
Why is this occurring?

A. The account is an AWS Organization master account, and by default it cannot provision EC2 instances.
B. The account is an AWS Organization member account, and a service control policy is denying provisioning of EC2 instances.
C. The account AWS Organization master account, and it does not have an access key activated for the IAM account.
D. The account is an AWS Organization master account, and it does not have an access key activated for the IAM account.

Answer: B

Explanation:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

NEW QUESTION 270
Based on the AWS Shared Responsibility Model, which of the following actions are the responsibility of the customer for an Aurora database?

A. Performing underlying OS updates
B. Provisioning of storage for database
C. Scheduling maintenance, patches and other updates
D. Executing maintenance, patches and other updates

Answer:

B

NEW QUESTION 274
A SysOps Administrator is asked to create an Amazon VPC IPv4 subnet that will support a minimum of 30 network resources simultaneously.
What is the minimum CIDR netmask that will sustain this requirement?

A. /25
B. /26
C. /27
D. /28

Answer: C

Explanation:

CIDR Available Hosts

The formula to calculate the number of assignable IP address to CIDR networks is similar to classful networking. Subtract the number of network bits from 32. Raise 2 to that power and subtract 2 for the network and broadcast addresses. For example, a /24 network has $2^{32-24} - 2$ addresses available for host assignment.

CIDR Notation	Host Formula	Available Hosts
/8	$2^{32-8} - 2$	16,777,214
/9	$2^{32-9} - 2$	8,388,606
/10	$2^{32-10} - 2$	4,194,302
/11	$2^{32-11} - 2$	2,097,150
/12	$2^{32-12} - 2$	1,048,574
/13	$2^{32-13} - 2$	524,286
/14	$2^{32-14} - 2$	262,142
/15	$2^{32-15} - 2$	131,070
/16	$2^{32-16} - 2$	65,534
/17	$2^{32-17} - 2$	32,766
/18	$2^{32-18} - 2$	16,382
/19	$2^{32-19} - 2$	8,190
/20	$2^{32-20} - 2$	4,094
/21	$2^{32-21} - 2$	2,046
/22	$2^{32-22} - 2$	1,022
/23	$2^{32-23} - 2$	510
/24	$2^{32-24} - 2$	254
/25	$2^{32-25} - 2$	126
/26	$2^{32-26} - 2$	62
/27	$2^{32-27} - 2$	30
/28	$2^{32-28} - 2$	14
/29	$2^{32-29} - 2$	6
/30	$2^{32-30} - 2$	2

NEW QUESTION 278
A SysOps Administrator needs to implement logging strategy that will allow of Linux-based Amazon EC2 instance to write log files into a single shared archive. An additional requirement is that log location must be accessible on all EC2 fleet instances using the local file system.
What service meets the requirements?

A. Amazon Elastic IV
B. Amazon EBS
C. Amazon Kinesis
D. AWS CloudTrail

Answer: C

Explanation:
Amazon Kinesis Firehose
Customers who have large amounts of log data to process can use Amazon Kinesis Firehose as a serverless log ingestion and delivery mechanism. Amazon Kinesis Firehose is a managed service that enables customers to deliver real-time streaming data to destinations such as Amazon ES, Amazon S3, and Amazon Redshift. Firehose is designed to handle large amounts of incoming data and can generate bulk indexing requests to an Amazon ES domain.
Unlike self-managed log processing components, such as a Logstash cluster, Firehose does not
require any servers, applications, or resource management. Customers configure individual data producers to send log data to a Firehose delivery stream continuously, and Firehose manages the rest.

NEW QUESTION 283
A company is running as production application in one region and is expanding to a second region. A SysOps Administrator has copied the requirement Amazon Machine images (AMIs) from the region to the second. An IAM user can list the copied AMIS in the AWS Management Console but when trying to launch an EC2 instance using one of the AMIs, the process fails.
What is the likely reason?

A. The destination AMI is corrupted because of copy process failure.
B. The user must first register the AMI before using it.
C. The AMI is stored in an encrypted Amazon Elastic Block Store (Amazon EBS) volume.
D. The launch permissions are not copied from the source AMI to the new AMI.

Answer: C

Explanation:
https://aws.amazon.com/blogs/security/how-to-create-a-custom-ami-with-encrypted-amazon-ebs- snapshots-and-share-it-with-other-accounts-and-regions/

NEW QUESTION 284
An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85baf1fc, and it is actively used by 10 Amazon EC2 hosts.
The organization has become concerned that the file system is not encrypted. How can this be resolved?

A. Enable encryption on each hosts connection to the Amazon EFS volume Each connection must be recreated for encryption to take effect
B. Enable encryption on the existing EFS volume by using the AWS Command Line Interface
C. Enable encryption on each host's local drive Restart each host to encrypt the drive
D. Enable encryption on a newly created volume and copy all data from the original volume Reconnect each host to the new volume

Answer: A

Explanation:
https://docs.aws.amazon.com/efs/latest/ug/encryption.html https://aws.amazon.com/premiumsupport/knowledge-center/encrypt-data-efs/

NEW QUESTION 288
A SysOps Administrator management a fleet of instance store-backed Amazon Linux EC2 instances. The SSH key used to access these instances has been lost.
How can SSH access be restored?

A. Contact AWS Support lo retrieve a backup of the SSH key after authentication
B. Create a new SSH key slop the EC2 instances apply the new key, and restart the EC2 instances
C. Create a new SSH key and apply the new key to the running EC2 instances
D. Launch a new fleet of EC2 instances wilt a newly created SSH key

Answer: A

Explanation:
Resolution
Warning: Do not perform this procedure if your EC2 instance is an instance store-backed instance. This recovery procedure requires a stop and start of your instance, which means that data on instance store volumes will be lost. For more information, see Determining the Root Device Type of Your Instance.
To recover access to your Linux instance using AWS Systems Manager (SSM) automation, run the AWSSupport-ResetAccess Automation automation document. For more information, see Reset Passwords and SSH Keys on Amazon EC2 Instances.
Or, to manually recover access to your Linux instance, create a new key pair to replace the lost key pair. For more information, see Connecting to Your Linux Instance If You Lose Your Private Key.

NEW QUESTION 292
A SysOps Administrator must monitor a fleet of Amazon EC2 Linux instance with the constraint that no agent be installed. The SysOps administrator Chooses Amazon CloudWatch as the monitoring tool.
Which metrics can be measured given the constraints? (Select THREE.)

A. CPU Utilization
B. Disk Read Operations
C. Memory Utilization
D. Network Packets in
E. Network Packets Dropped
F. CPU Ready Time

Answer: ABD

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html

NEW QUESTION 294
A company has a VoIP application deployed on AWS. The application is accessed by employees in a remote office and is extremely sensitive to any latency and packets loss. Minimize latency and packet loos is a higher priority than minimizing cost.
Employees are reporting occasional difficulties accessing the application. The Local Network Engineer has completed thorough troubleshooting on the LAN and unable to identify any signs of congestion or equipment failure that may be causing the issue.
What is the BEST way to address the connectivity issues between the remote office and the application?

A. Configure a VPN connection to the VPC Route all traffic to the application via the VPN connection over the public internet
B. Establish a Direct Connect to the VPC Route all traffic to the application via the direct connect connection
C. Enable VPC peering to decrease latency between instances Enable QoS on peering connection
D. Configure Amazon Trusted Advisor to give higher prioritization to the IP to assigned to the remote office over public internet traffic

Answer: C

Explanation:
https://docs.aws.amazon.com/vpc/latest/peering/create-vpc-peering-connection.html

NEW QUESTION 297
A company wants to send 70% of its inbound traffic to the us-east-1 region and 30% to the us-east region under normal; conditions. If all the servers go down in one of the regions, the company wants all the traffic to be re-routed to the other region.

A. Configure an Application Load Balancer Target Group with weighted rules and a health check enabled
B. Use a Network Load Balancer with sticky sessions enabled and weighted round room with a 70/30 ratio
C. Create two CNAMF records in Amazon Route R3 enable dynamic traffic shaping with a 7G730 ratio
D. Use a Route 53 weighted routing policy with a 70 /30 ratio and configure a heath check

Answer:

D

Explanation:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-values- weighted-alias.html

NEW QUESTION 302
A company operate a secure website running an Amazon EC2 instance behind a Classic Load Balancer. An SSL certificate from AWS Certificate Manager is deployment on the load balancer. The company's Marketing team has determined that too many customer using older browser are experiencing issues with the website has asked a SysOps Administrator to fix this issue.
What course of action should the administrator take?

A. Update the SSL negotiation configuration of the load balancer by creating a custom security polic
B. Ensure the appropriate cipher has been enabled so that the web application can support the webbrowser.
C. Create a separate Classic Load Balancer and install custom SSL certificate with a different domain name on it that support the web browse
D. Ask customer with the affected browser to use this domain name instead of the one they are accustomed to using.
E. Create a new SSL certificate in Certificate Manager and install this certificate on each of the servers to accommodates the web browsers.
F. Remove the load balancer from the configuration and instead install a custom SSL certificate on each of the web servers.

Answer: A

Explanation:
Update the SSL Negotiation Configuration of Your Classic Load Balancer
Elastic Load Balancing provides security policies that have predefined SSL negotiation configurations to use to negotiate SSL connections between clients and your load balancer. If you are using the HTTPS/SSL protocol for your listener, you can use one of the predefined security policies, or use your own custom security policy.
For more information about the security policies, see SSL Negotiation Configurations for Classic Load Balancers. For information about the configurations of the security policies provided by Elastic Load Balancing, see Predefined SSL Security Policies.
If you create an HTTPS/SSL listener without associating a security policy, Elastic Load Balancing associates the default predefined security policy, ELBSecurityPolicy-2016-08, with your load balancer. If you have an existing load balancer with an SSL negotiation configuration that does not use the latest protocols and ciphers, we recommend that you update your load balancer to use ELBSecurityPolicy-2016-08. If you prefer, you can create a custom configuration. We strongly recommend that you test the new security policies before you upgrade your load balancer configuration.
The following examples show you how to update the SSL negotiation configuration for an HTTPS/SSL listener. Note that the change does not affect requests that were received by a load balancer node and are pending routing to a healthy instance, but the updated configuration will be used with new requests that are received.

NEW QUESTION 307
.....

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 SOA-C01 Exam with Our Prep Materials Via below:

https://www.certleader.com/SOA-C01-dumps.html