Amazon-Web-Services

Exam Questions SOA-C01

AWS Certified SysOps Administrator - Associate

NEW QUESTION 1
You are currently hosting multiple applications in a VPC and have logged numerous port scans coming in from a specific IP address block. Your security team has requested that all access from the offending IP address block be denied for the next 24 hours.
Which of the following is the best method to quickly and temporarily deny access from the specified IP address block?

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

Answer: B

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

NEW QUESTION 2
When attached to an Amazon VPC which two components provide connectivity with external networks? Choose 2 answers

A. Elastic IPS (EIP)
B. NAT Gateway (NAT)
C. Internet Gateway {IGW)
D. Virtual Private Gateway (VGW)

Answer: CD

NEW QUESTION 3
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 4
Which two AWS services provide out-of-the-box user configurable automatic backup-as-a-service and backup rotation options? Choose 2 answers

A. Amazon S3
B. Amazon RDS
C. Amazon EBS
D. Amazon Redshift

Answer: BD

Explanation:
By default: at no additional charge, Amazon RDS enables automated backups of your DB Instance with a 1-day retention period. By default: Amazon Redshift enables automated backups of your data warehouse cluster with a 1- day retention period.

NEW QUESTION 5
You are creating an Auto Scaling group whose Instances need to insert a custom metric into CloudWatch.
Which method would be the best way to authenticate your CloudWatch PUT request?

A. Create an IAM role with the Put MetricData permission and modify the Auto Scaling launch configuration to launch instances in that role

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

Answer: A

NEW QUESTION 6
The majority of your Infrastructure is on premises and you have a small footprint on AWS Your company has decided to roll out a new application that is heavily dependent on low latency connectivity to LOAP for authentication Your security policy requires minimal changes to the company's existing application user management processes.
What option would you implement to successfully launch this application1?

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

Answer: C

Explanation:
Since it requires no changes to the authentication infrastructure as requested in the question. Option D creates a new LDAP, trusts, etc.

NEW QUESTION 7
Which services allow the customer to retain full administrative privileges of the underlying EC2 instances?
Choose 2 answers

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

Answer: AC

Explanation:
The below services provide Root level access:
* EC2
* Elastic Beanstalk
* Elastic MapReduce ?V Master Node
* Opswork

NEW QUESTION 8
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

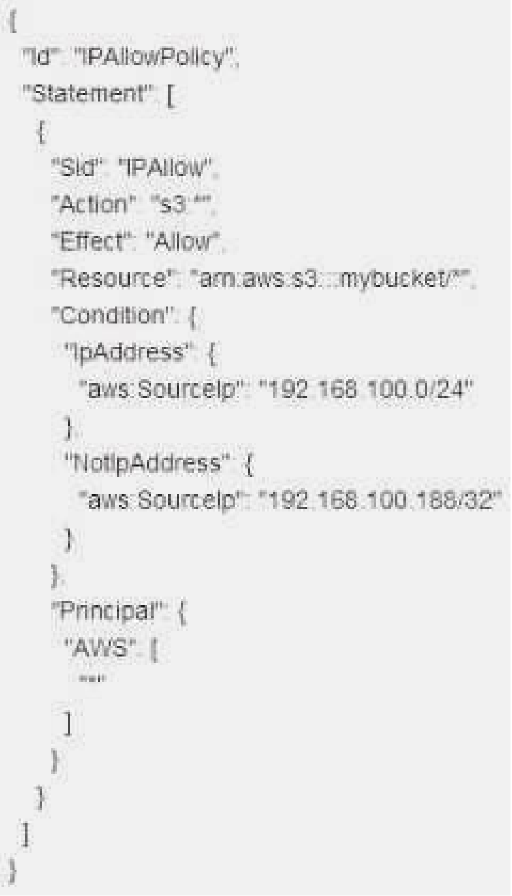
Explanation:
This is an odd question. First of all, option A cannot be right because ELB does not failover. Cannot be C because Route 53 does work with hard coded IP. Only B & D cannot be rule out so best answer.

NEW QUESTION 9
You are designing a system that has a Bastion host. This component needs to be highly available without human intervention.
Which of the following approaches would you select?

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

Answer: C

NEW QUESTION 10
Which of the following statements about this S3 bucket policy is true?



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

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

Answer: B

NEW QUESTION 10
You run a web application where web servers on EC2 Instances are In an Auto Scaling group Monitoring over the last 6 months shows that 6 web servers are necessary to handle the minimum load During the day up to 12 servers are needed Five to six days per year, the number of web servers required might go up to 15.
What would you recommend to minimize costs while being able to provide hill availability?

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

Answer: A

Explanation:
The only plausible answer is A because all other answers include Spot Instances that can be removed without warning and that would not be highly available.

NEW QUESTION 15
You have been asked to propose a multi-region deployment of a web-facing application where a controlled portion of your traffic is being processed by an alternate region.
Which configuration would achieve that goal?

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

Answer: A

Explanation:
The question is asking ??a controlled portion of your traffic??, that would be established with weighted routing policy.
See: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

NEW QUESTION 19
A media company produces new video files on-premises every day with a total size of around 100GBS after compression All files have a size of 1 - 2 GB and need to be uploaded to Amazon S3 every night in a fixed time window between 3am and 5am Current upload takes almost 3 hours, although less than half of the available bandwidth is used.
What step(s) would ensure that the file uploads are able to complete in the allotted time window?

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

Answer: B

Explanation:
Reference:
https://aws.amazon.com/blogs/aws/amazon-s3-multipart-upload/

NEW QUESTION 20
What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment of the primary OB instance fails?

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

Answer: D

Explanation:
https://aws.amazon.com/rds/faqs/

NEW QUESTION 24
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 29
An organization is planning to create 5 different AWS accounts considering various security requirements. The organization wants to use a single payee account by using the consolidated billing option. Which of the below mentioned statements is true with respect to the above information?

A. Master (Paye
B. account will get only the total bill and cannot see the cost incurred by each account
C. Master (Paye
D. account can view only the AWS billing details of the linked accounts
E. It is not recommended to use consolidated billing since the payee account will have access to the linked accounts
F. Each AWS account needs to create an AWS billing policy to provide permission to the payee account

Answer: B

Explanation:
AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS. accounts within a single organization by making a single paying account. Consolidated billing enables the organization to see a combined view of the AWS charges incurred by each account as well as obtain a detailed cost report for each of the individual AWS accounts associated with the paying account. The payee account will not have any other access than billing data of linked accounts.

NEW QUESTION 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 31
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 35
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 38
A user is trying to understand AWS SNS. To which of the below mentioned end points is SNS unable to send a notification?

A. Email JSON
B. HTTP
C. AWS SQS
D. AWS SES

Answer: D

Explanation:
Amazon Simple Notification Service (Amazon SNS. is a fast, flexible, and fully managed push messaging service. Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS. queues or to any HTTP endpoint. The user can select one the following transports as part of the subscription requests: ??HTTP??, ??HTTPS??,??Email??, ??Email-JSON??, ??SQS??, ??and SMS??.

NEW QUESTION 39
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 43
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 48

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

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

Answer: D

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

NEW QUESTION 51
A root AWS account owner is trying to understand various options to set the permission to AWS S3. Which of the below mentioned options is not the right option to grant permission for S3?

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

Answer: B

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

NEW QUESTION 53
An organization is using AWS since a few months. The finance team wants to visualize the pattern of AWS spending. Which of the below AWS tool will help for this requirement?

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

Answer: B

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

NEW QUESTION 54
A user has launched an ELB which has 5 instances registered with it. The user deletes the ELB by mistake. What will happen to the instances?

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

Answer: D

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

NEW QUESTION 58
A user is accessing RDS from an application. The user has enabled the Multi AZ feature with the MS SQL RDS DB. During a planned outage how will AWS ensure that a switch from DB to a standby replica will not affect access to the application?

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

Answer: B

Explanation:
In the event of a planned or unplanned outage of a DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone if the user

has enabled Multi AZ. The automatic failover mechanism simply changes the DNS record of the DB instance to point to the standby DB instance. As a result, the user will need to re-establish any existing connections to the DB instance. However, as the DNS is the same, the application can access DB seamlessly.

NEW QUESTION 60
An organization is using cost allocation tags to find the cost distribution of different departments and projects. One of the instances has two separate tags with the key/ value as ??InstanceName/HR??, ??CostCenter/HR??. What will AWS do in this case?

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

Answer: D

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

NEW QUESTION 61
A user has created an ELB with the availability zone US-East-1

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

Answer: D

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

NEW QUESTION 62
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 64
A user has launched an EBS backed EC2 instance. What will be the difference while performing the
restart or stop/start options on that instance?

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

Answer: A

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

NEW QUESTION 66
A user has created a queue named ??myqueue?? in US-East region with AWS SQS. The user??s AWS account ID is 123456789012. If the user wants to perform some action on this queue, which of the below Queue URL should he use?

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

E. http:// 123456789012.sq
F. us-east-1.amazonaws.com/myqueue

Answer: A

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

NEW QUESTION 68
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 69
A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

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

Answer: D

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

NEW QUESTION 73
A user wants to make so that whenever the CPU utilization of the AWS EC2 instance is above 90%, the redlight of his bedroom turns on. Which of the below mentioned AWS services is helpful for this purpose?

A. AWS CloudWatch + AWS SES
B. AWS CloudWatch + AWS SNS
C. Non
D. It is not possible to configure the light with the AWS infrastructure services
E. AWS CloudWatch and a dedicated software turning on the light

Answer: B

Explanation:
Amazon Simple Notification Service (Amazon SNS. is a fast, flexible, and fully managed push messaging service. Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS. queues or to any HTTP endpoint. The user can configure some sensor devices at his home which receives data on the HTTP end point (REST calls. and turn on the red light. The user can configure the CloudWatch alarm to send a notification to the AWS SNS HTTP end point (the sensor device. and it will turn the light red when there is an alarm condition.

NEW QUESTION 76
A user has setup an EBS backed instance and a CloudWatch alarm when the CPU utilization is more than 65%. The user has setup the alarm to watch it for 5 periods of 5 minutes each. The CPU utilization is 60% between 9 AM to 6 PM. The user has stopped the EC2 instance for 15 minutes between 11 AM to 11:15 AM. What will be the status of the alarm at 11:30 AM?

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

Answer: B

Explanation:
Amazon CloudWatch alarm watches a single metric over a time period the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The state of the alarm will be OK for the whole day. When the user stops the instance for three periods

the alarm may not receive the data

NEW QUESTION 77
A user has created an ELB with Auto Scaling. Which of the below mentioned offerings from ELB helps the user to stop sending new requests traffic from the load balancer to the EC2 instance when the instance is being deregistered while continuing in-flight requests?

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

Answer: C

Explanation:
The Elastic Load Balancer connection draining feature causes the load balancer to stop sending new requests to the back-end instances when the instances are deregistering or become unhealthy, while ensuring that inflight requests continue to be served.

NEW QUESTION 79
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 80
A user has setup an EBS backed instance and attached 2 EBS volumes to it. The user has setup a CloudWatch alarm on each volume for the disk data. The user has stopped the EC2 instance and detached the EBS volumes. What will be the status of the alarms on the EBS volume?

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

Answer: B

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

NEW QUESTION 82
A user has launched an EBS backed instance with EC2-Classic. The user stops and starts the instance. Which of the below mentioned statements is not true with respect to the stop/start action?

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

Answer: C

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

NEW QUESTION 87
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 88
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 89
A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

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

Answer: B

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

NEW QUESTION 91
A user has hosted an application on EC2 instances. The EC2 instances are configured with ELB and Auto Scaling. The application server session time out is 2 hours. The user wants to configure connection draining to ensure that all in-flight requests are supported by ELB even though the instance is being deregistered. What time out period should the user specify for connection draining?

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

Answer: B

NEW QUESTION 93
A user has created a queue named ??awsmodule?? with SQS. One of the consumers of queue is down for 3 days and then becomes available. Will that component receive message from queue?

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

Answer: A

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

NEW QUESTION 98
A user has configured ELB with a TCP listener at ELB as well as on the back-end instances. The user wants to enable a proxy protocol to capture the source and destination IP information in the header. Which of the below mentioned statements helps the user understand a proxy protocol with TCP configuration?

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

Answer: A

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

NEW QUESTION 99
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 103
A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned SSL protocols is not supported by the security policy?

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

Answer: A

Explanation:
Elastic Load Balancing uses a Secure Socket Layer (SSL. negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. Elastic Load Balancing supports the following versions of the SSL protocol:
TLS 1.2
TLS 1.1
TLS 1.0
SSL 3.0
SSL 2.0

NEW QUESTION 105
A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80. and a DB server in the private subnet (port 3306.. The user is configuring a security group for the public subnet (WebSecGrp. and the private subnet (DBSecGrp.. Which of the below mentioned entries is required in the private subnet database security group (DBSecGrp.?

A. Allow Inbound on port 3306 for Source Web Server Security Group (WebSecGrp.
B. Allow Inbound on port 3306 from source 20.0.0.0/16
C. Allow Outbound on port 3306 for Destination Web Server Security Group (WebSecGrp.
D. Allow Outbound on port 80 for Destination NAT Instance IP

Answer: A

Explanation:
A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the private subnet can receive inbound traffic from the public subnet on the DB port. Thus, configure port 3306 in Inbound with the source as the Web Server Security Group (WebSecGrp.. The user should configure ports 80 and 443 for Destination 0.0.0.0/0 as the route table directs traffic to the NAT instance from the private subnet.

NEW QUESTION 107
A user has launched an EC2 Windows instance from an instance store backed AMI. The user has also set the Instance initiated shutdown behavior to stop. What will happen when the user shuts down the OS?

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

Answer: B

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

NEW QUESTION 110
A user has created a VPC with public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24 . The NAT instance ID is i-a12345. Which of the below mentioned entries are required in the main route table attached with the private subnet to allow instances to connect with the internet?

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

Answer: A

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

NEW QUESTION 114
An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%. The higher CPU usage triggers an event for Auto Scaling as per the scaling policy. If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

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

Answer: D

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

NEW QUESTION 119
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 123
A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services does not provide detailed monitoring with CloudWatch?

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

D. AWS Route53

Answer: A

Explanation:
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, EC2, Auto Scaling, ELB, and Route 53 can provide the monitoring data every minute.

NEW QUESTION 126
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 130
A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24. and a public subnet (20.0.0.0/24.. The user??s data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?

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

Answer: D

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

NEW QUESTION 133
A user has created a mobile application which makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

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

Answer: C

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

NEW QUESTION 138
A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services provides detailed monitoring with CloudWatch without charging the user extra?

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

Answer: B

Explanation:
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic

monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, ELB, OpsWorks, and Route 53 can provide the monitoring data every minute without charging the user.

NEW QUESTION 141
A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the
user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?

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

Answer: B

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

NEW QUESTION 145
A user is using the AWS SQS to decouple the services. Which of the below mentioned operations is not supported by SQS?

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

Answer: D

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

NEW QUESTION 149
A user has launched an EC2 instance. However, due to some reason the instance was terminated. If the user wants to find out the reason for termination, where can he find the details?

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

Answer: D

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

NEW QUESTION 151
A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned security policies is supported by ELB?

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

Answer: C

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

NEW QUESTION 155
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 157
A user has created an Auto Scaling group using CLI. The user wants to enable CloudWatch detailed monitoring for that group. How can the user configure this?

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

Answer: B

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

NEW QUESTION 158
A user is trying to create a PIOPS EBS volume with 8 GB size and 200 IOPS. Will AWS create the volume?

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

Answer: C

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

NEW QUESTION 161
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 165
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 168

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

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

Answer: D

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

NEW QUESTION 170
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 174
A user has two EC2 instances running in two separate regions. The user is running an internal memory management tool, which captures the data and sends it to CloudWatch in US East, using a CLI with the same namespace and metric. Which of the below mentioned options is true with respect to the above statement?

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

Answer: B

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

NEW QUESTION 177
A sys admin has enabled a log on ELB. Which of the below mentioned activities are not captured by the log?

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

Answer: B

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

NEW QUESTION 178
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 181
A user is running a batch process on EBS backed EC2 instances. The batch process starts a few instances to process hadoop Map reduce jobs which can run between 50 ?V 600 minutes or sometimes for more time. The user wants to configure that the instance gets terminated only when the process is completed. How can the user configure this with CloudWatch?

A. Setup the CloudWatch action to terminate the instance when the CPU utilization is less than 5%
B. Setup the CloudWatch with Auto Scaling to terminate all the instances
C. Setup a job which terminates all instances after 600 minutes
D. It is not possible to terminate instances automatically

Answer: D

Explanation:
Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which terminates the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action.

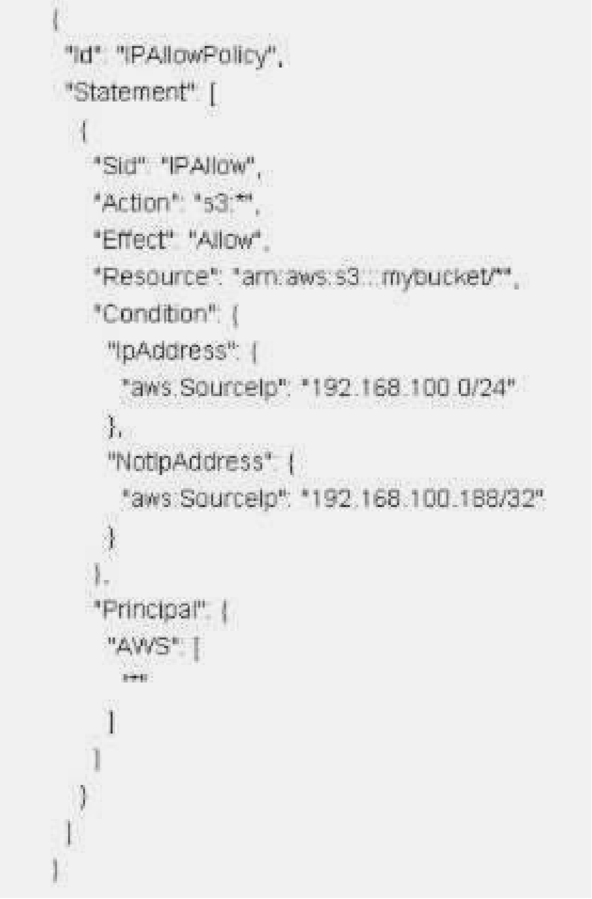
NEW QUESTION 186
A user has launched a Windows based EC2 instance. However, the instance has some issues and the user wants to check the log. When the user checks the Instance console output from the AWS console, what will it display?

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

Answer: D

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

NEW QUESTION 191
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 193
Your business is building a new application that will store its entire customer database on a RDS MySQL database, and will have various applications and users that will query that data for different purposes.
Large analytics jobs on the database are likely to cause other applications to not be able to get the query results they need to, before time out. Also, as your data grows, these analytics jobs will start to take more time, increasing the negative effect on the other applications.
How do you solve the contention issues between these different workloads on the same data?

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

Answer: B

Explanation:
Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory caching system, instead of relying entirely on slower disk-based databases. The service simplifies and offloads the management, monitoring and operation of in-memory cache environments, enabling your engineering resources to focus on developing applications. Using Amazon ElastiCache, you can not only improve load and response times to user actions and queries, but also reduce the cost associated with scaling web applications.
Amazon ElastiCache automates common administrative tasks required to operate a distributed cache environment. Using Amazon ElastiCache, you can add a caching layer to your application architecture in a matter of minutes via a few clicks of the AWS Management Console. Once a cache cluster is provisioned, Amazon ElastiCache automatically detects and replaces failed cache nodes, providing a resilient system that mitigates the risk of overloaded databases, which slow website and application load times. Through integration with Amazon CloudWatch monitoring, Amazon ElastiCache provides enhanced visibility into key performance metrics associated with your cache nodes. Amazon ElastiCache is protocol-compliant with Memcached and Redis, so code, applications, and popular tools that you use today with your existing Memcached or Redis environments will work seamlessly with the service. As with all Amazon Web Services,

NEW QUESTION 194
When you put objects in Amazon S3, what is the indication that an object was successfully stored?

A. Each S3 account has a special bucket named_s3_log
B. Success codes are written to this bucket with a timestamp and checksum.
C. A success code is inserted into the S3 object metadata.
D. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
E. Amazon S3 is engineered for 99.999999999% durabilit
F. Therefore, there is no need to confirm that data was inserted.

Answer: C

Explanation:
To ensure that data is not corrupted traversing the network, use the Content-MD5 form field. When you use this form field, Amazon S3 checks the object against the provided MD5 value. If they do not match, Amazon S3 returns an error.
success_action_status
The status code returned to the client upon successful upload if success_action_redirectis not specified.
Accepts the values 200, 201, or 204 (default).
If the value is set to 200 or 204, Amazon S3 returns an empty document with a 200 or 204 status code.
If the value is set to 201, Amazon S3 returns an XML document with a 201 status code.
If the value is not set or if it is set to an invalid value, Amazon S3 returns an empty document with a 204 status code.
Type: String Default: None Note
Some versions of the Adobe Flash player do not properly handle HTTP responses with an empty body. To support uploads through Adobe Flash, we recommend setting success_action_statusto 201.
Source: http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html

NEW QUESTION 196
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 197
An application you maintain consists of multiple EC2 instances in a default tenancy VPC. This application has undergone an internal audit and has been determined to require dedicated hardware for one instance. Your compliance team has given you a week to move this instance to single-tenant hardware.
Which process will have minimal impact on your application while complying with this requirement?

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

Answer: D

Explanation:
Reference:
See: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated- instance.html#dedicated-apichanges
You cannot change the tenancy of a default instance after you??ve launched it. You can change the tenancy of an instance from ??dedicated?? to ??host?? after you??ve launched it, and vice versa.

NEW QUESTION 200
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 202
Which features can be used to restrict access to data in S3? Choose 2 answers

A. Set an S3 ACL on the bucket or the object.
B. Create a CloudFront distribution for the bucket.
C. Set an S3 bucket policy.
D. Enable IAM Identity Federation
E. Use S3 Virtual Hosting

Answer: AC

Explanation:
https://aws.amazon.com/s3/faqs/

NEW QUESTION 204
A photo-sharing service stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider. Which AWS Security Token Service approach to temporary access should you use for the Amazon S3 operations?

A. SAML-based Identity Federation
B. Cross-Account Access
C. AWS Identity and Access Management roles
D. Web Identity Federation

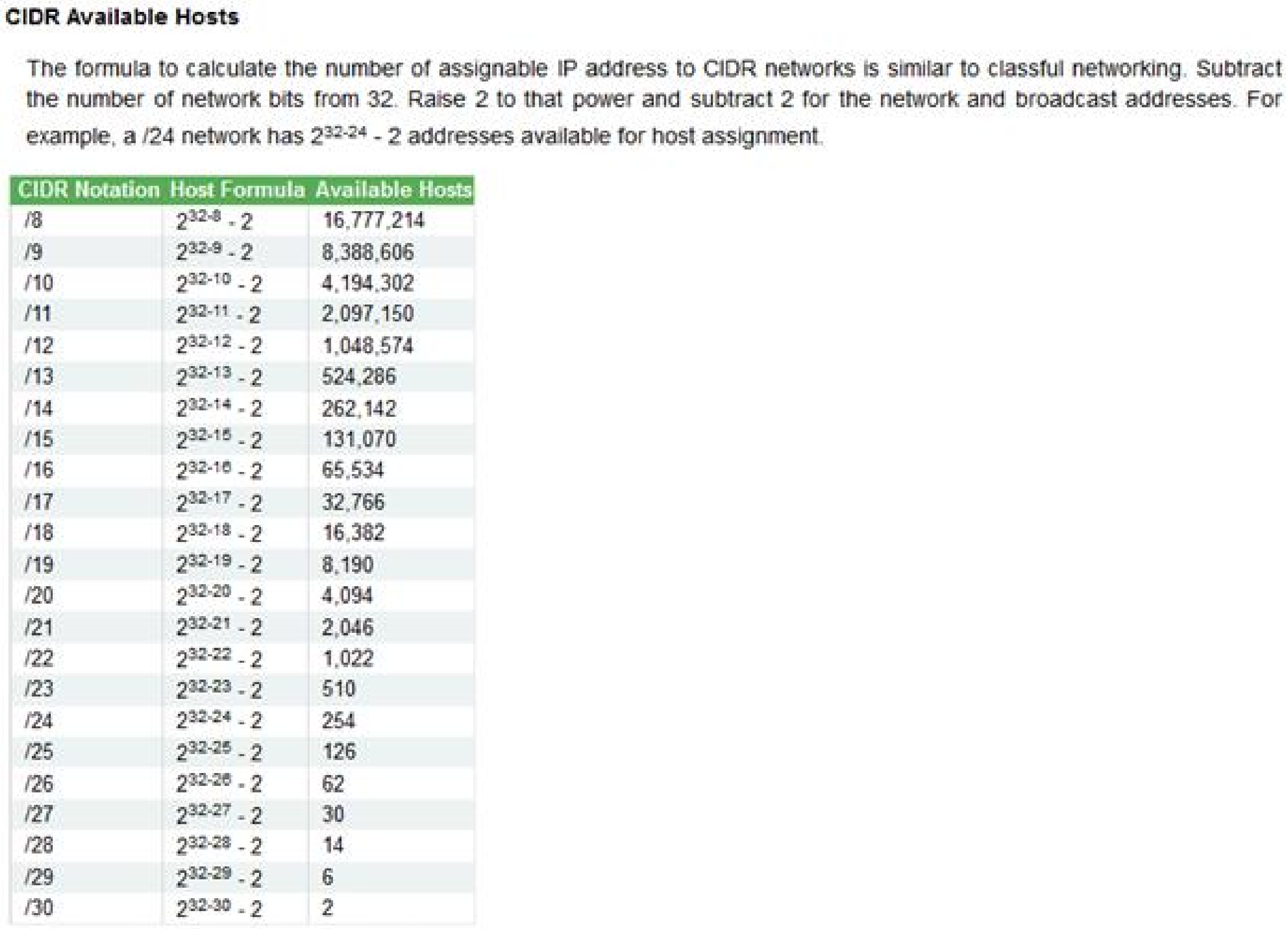
Answer: D

NEW QUESTION 209
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 210
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 214
The Security tram is connect because the number of AWS identity and access Management (IAM) policies being in the environment is increasing. The tasked a SysOps Administrator to report on the number of IAM policies in use and use the total IAM policies.
Which AWS service should the Administrator use to check how current IAM policy compares to current limits?

A. MWS Trusted Advisor
B. Amazon Inspector
C. AWS Config
D. Organizations

Answer: C

Explanation:
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

NEW QUESTION 218
A SysOps Administrator has attempted to copy an Marketplace AMI an associated billing Product code that was shared another account. When the copy process is attempted, it fails.
What action can be taken to successfully copy the AMI to the target destination?

A. Use an EC2 instance in the account by using the shared AMI and then created an AMI from the instance
B. Launch an EC2 instance in the account by using the shared AMI and then create an AMI from the instance
C. Use the AWS CLI with the --nobillingProduct flag to execute the copy and ignore the billingProductcode.
D. Create a VPC peering connection between the source and target account to facilitate the AMI copy process.

Answer: D

NEW QUESTION 222
A SysOps Administrator must take a team's single existing AWS CloudFormation template and split it into smaller, service specific template. All of the service in the template reference a single, shared Amazon S3 bucket.
What should the Administrator do to ensure that this S3 bucket can be referenced by all the service templates?

A. Include the S3 bucket as a mapping in each template
B. Add the S3 bucket as a resource in each template
C. Create the S3 bucket in its own template and export it
D. Generate the S3 bucket using StackSets

Answer: D

NEW QUESTION 226
A SysOps Administrator supports a legacy application that is hardcoded to service example.com. The application has recently been moved to AWS. The external DNS are managed by a third-party provider. The Administrator has set up an internal domain for example.com and configured this record using Amazon Route.
What solution offers the MOST efficient way to have instances in the same account resolve to the Route 53 service instead of the provider?

A. Hardcode the name server record to the internal Route 53 IP address tor each instance
B. Enable DNS resolution in the subnets as required
C. Ensure that DNS resolution is enabled on the VPC
D. Create an OS-specific hardcoded entry tor DNS resolution to the private URL

Answer: C

Explanation:
Using DNS with Your VPC
Domain Name System (DNS) is a standard by which names used on the Internet are resolved to their corresponding IP addresses. A DNS hostname is a name that uniquely and absolutely names a computer; it's composed of a host name and a domain name. DNS servers resolve DNS hostnames to their corresponding IP addresses.
Public IPv4 addresses enable communication over the Internet, while private IPv4 addresses enable communication within the network of the instance (either EC2-Classic or a VPC). For more information, see IP Addressing in Your VPC.
We provide an Amazon DNS server. To use your own DNS server, create a new set of DHCP options for your VPC. For more information, see DHCP Options Sets.
Contents
DNS Hostnames
DNS Support in Your VPC DNS Limits
Viewing DNS Hostnames for Your EC2 Instance Updating DNS Support for Your VPC
Using Private Hosted Zones

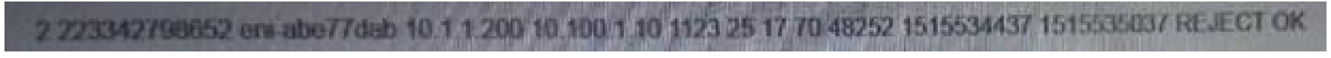
NEW QUESTION 230
A SysOps Administrator must run a script on production servers to fix an issue. The company has a policy block all remote interface access to production servers. The Based on this situation how should the Administrator execute the script?

A. Share and use the Amazon EC2 key pairs to gain access to the servers and run the script
B. Put the script into the user data of the instances
C. Configure the script to run as a cron job or scheduled task on the EC2 instances
D. Use Amazon EC2 Systems Manager to run the script

Answer: A

Explanation:
https://aws.amazon.com/getting-started/tutorials/deploy-code-vm/

NEW QUESTION 235
An Amazon EC2 instance is unable to connect to an SMTP server in a different subnet. Other instances are successfully communication with the SMTP servers, however Flow Logs have been enabled on the SMTP server's network interface and show the following information



```
2 223342798652 eni-abe77dab 10.1.1.200 10.100.1.10 1123 25 17 70 48252 1515534437 1515535037 REJECT OK
```

A. Add the instance to the security group for the SMTP server and ensure that it is permitted to communicate over TCP port 25.
B. Disable the iptables server on the SMTP server so that the instance can properly communicate over the network.
C. Install an email on the instance to ensure that it communicates correctly on TCP port 25 to theSMTP server.
D. Add a rule to the security group for the instance to explicit permit TCP port 25 outbound to any address.

Answer: D

NEW QUESTION 240
A company has created a separate AWS account for all development work to protect the production environment in this development account, developers have permission to manipulate IAM policies and roles. Corporate policies require that developers and blocked from accessing some services. What is the BEST way to grant the developers privileges in the development account while still complying with corporate policies?

A. Create a service control policy in AWS Organizations and apply it to the development account
B. Create a customer managed policy in IAM and apply it to all users within the development account
C. Create a job function policy in IAM and apply it to all users within the development account
D. Create an IAM policy and apply it in API Gateway to restrict the development account

Answer: A

Explanation:
https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-in-aws-organizations/

NEW QUESTION 242
An application stores data in an Amazon RDS database instance. Automated RDS snapshots are taken during specified backup windows every night. In addition, a SysOps Administrator takes monthly manual RDS snapshots. During a maintenance window, the RDS instance was accidentally deleted. How can the Administrator restore the DRS database instance?

A. Restore the instance from the last available automated snapshot.
B. Restore the instance from the last available manual snapshot.
C. Restore the instance from the last full RDS snapshot and subsequent incremental snapshots
D. Restore the instance from the RDS in the secondary Availability Zone

Answer: A

Explanation:
Creating a Final Snapshot and Retaining Automated Backups
When you delete a DB instance, you can choose whether to create a final snapshot of the DB instance. You can also choose to retain automated backups after the DB instance is deleted. To be able to restore the DB instance at a later time, create a final snapshot or retain automated backups.
How to To be able to restore To delete a DB instance quickly, Instead of creating a snapshot, you choose your deleted DB you can skip creating a final DB can choose to enable Retain
instance at a later snapshot. time, create a final DB Important
automated backups when you delete a DB instance. These backups
snapshot.
If you skip the snapshot, to are still subject to the retention restore your DB instance you period of the DB instance and age
need one of the following:
out the same way systems
You have to use an earlier snapshots do. manual snapshot of the DB instance to restore the DB instance to that snapshot's point in time.
You have to choose to retain automated backups; you can use those to restore it to any point in time within your retention period.
Automated backups
Automated backups are retained for All automated backups All automated backups are a set period of time, regardless of are deleted and can't deleted and can't be whether you chose to create a final be recovered, unless recovered, unless you choose snapshot. They are retained for to retain automated backups you enable Retain automated backups.
when you delete the DB retention period that was set on the
DB instance at the time you deleted Manual instance.
Earlier manual Earlier manual snapshots it.
snapshots
snapshots aren't aren't deleted. No snapshots are deleted. deleted.
You can't create a final snapshot of your DB instance if it has the status creating, failed, incompatible- restore, or incompatible-network. For more information about DB instance statuses, see DB Instance Status.

NEW QUESTION 243
An errant process is known to use in an entire processor and run at 100%. A SysOps Administrator wants to automate restarting the instance once the problem occurs for more than minutes.
How can this be accomplished?

A. Create an Amazon CloudWatch alarm or the Amazon EC2 instance with basic monitoring Enable an action to restart the instance
B. Create a CloudWatch alarm for the EC2 instance with detailed monitoring Enable an action to restart the instance
C. Create an AWS Lambda function to restart the EC2 instance triggered on a scheduled basis every 2 minutes
D. Create a Lambda function start the EC2 instance triggered by EC2 health

Answer: D

Explanation:
You can use CloudWatch Events to trigger an AWS Lambda function to start and stop your EC2 instances at scheduled intervals.
Note: This article provides an example for a simple solution. For a more robust solution, see AWS Instance Scheduler.
Resolution
CloudWatch Events allows you to create an event that is triggered at a specified time or interval in response to events that take place in your account. For example, you can create an event using CloudWatch Events for a specific time of day, or you can create an alarm when CPU utilization for an instance reaches a specific threshold. You can also configure a Lambda function to start and stop instances when triggered by these events.
In this example, we use Lambda functions to start and stop EC2 instances, and then we use CloudWatch Events to start instances in the morning and stop the instances at night.
1. Open the AWS Lambda console, and choose Create function.
2. Choose Author from scratch.
3. Enter a Name for your function, such as "StopEC2Instances."
4. From the Runtime drop-down menu, choose Python2.7.
5. Expand the Role drop-down menu, and then choose Create a custom role. This opens a new tab or window in your browser.
6. In the IAM Role drop-down menu, choose Create a new IAM Role, and enter a Role Name, such as ??lambda_start_stop_ec2."
7. Expand View Policy Document, choose Edit, and then choose Ok when prompted to read the documentation.

NEW QUESTION 244
A company is running an Oracle database engine that handles heavy online transaction processing (OLTP) structured data traffic.
How can a SysOps administrator ensure that the database has high availability?

A. Use Amazon DynamoOB to store the data
B. Use Amazon RDS Multi -AZ deployment to store the data
C. Use Amazon RDS read replicas in a different region to store the data
D. Use an Amazon Redshift cluster to store the data

Answer: B

NEW QUESTION 249
A company is migrating an application to AWS that requires access to a legacy system, which remain in the company's data centre. The application runs inside a VPC in the company's AWS account. The application must offer a consistent and low-latency response to its users
How can these requirements be met?

A. Create a software-based VPN connection between the Amazon VPC and the on-premises network
B. Create an AWS Direct Connect connection between AWS and the on-premises network and then use a private virtual interface
C. Create a hardware-based IPsec VPN connection between the VPC in AWS and the on-premises network
D. Create an overlay network by using third-party software and use that to connect the X/PC back to the on-premises network

Answer: B

Explanation:
Private Connectivity to your Amazon VPC. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network connection between your network and your VPC.

NEW QUESTION 251
After a particularly high bill, an organization wants to review the use of AWS services.
What AWS service will allow the SysOps Administrator to quickly view this information to shared it, and will also forest expenses for the billing period?

A. AWS Trusted Advisor
B. Amazon QuickSight
C. AWS Cost and Usage Report
D. AWS Cost Explorer

Answer: C

NEW QUESTION 252
A SysOps Administrator has set up a new Application Load Balancer (ALB) in front of a pair of private web server in multiple Availability Zones. After deployment an updates CloudFormation template with many changes, user now goes to one web server only.
What is the NOST likely reason that the traffic is not being balanced between both servers?

A. The faulty is returning HTTP 200 has been removed.
B. Sticky session have been disabled in the ALB for the working sever.
C. The ALB using a custom ping path that is not found on the faulty server.
D. The web client are using HTTP/2, which is terminated at the ALB.

Answer: B

Explanation:
Until now, the behavior of load balancers has been to route each request independently to the Amazon EC2 instance with the least load. With the stickiness feature, you can configure the load balancer to bind user sessions to specific application instances. All requests coming from the user during the session will be sent to the same application instance. Elastic Load Balancing supports two mechanisms to provide session stickiness: load balancer-generated HTTP cookies, which allow browser-based session lifetimes, and application-generated HTTP cookies, which allow application- specific session lifetimes. You can learn more about this feature by visiting the ELB Developers Guide.

NEW QUESTION 256
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 260
A company has a new requirement stating that all resources in AWS must be tagged according to a set policy. Which AWS service should to enforce and continually identify all resources that are not in compliance with the policy?

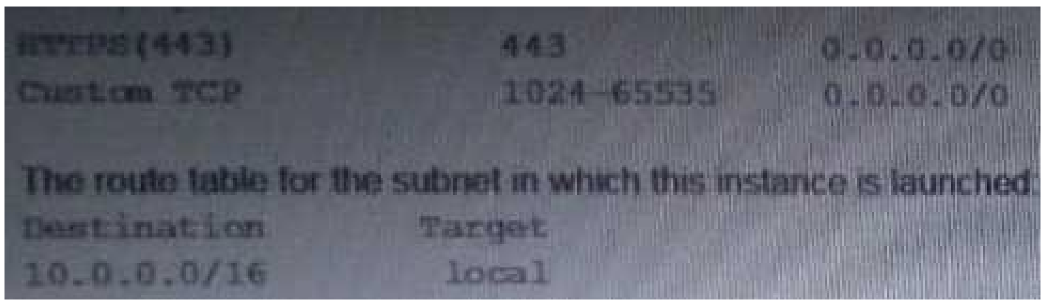
A. AWS CloudTrail
B. Amazon Inspector
C. AWS Config
D. AWS Systems Manager

Answer: C

Explanation:

AWS Config
TRACK RESOURCE INVENTORY AND CHANGES
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

NEW QUESTION 265
Exhibit:



HTTPS(443)	443	0.0.0.0/0
Custom TCP	1024-65535	0.0.0.0/0

The route table for the subnet in which this instance is launched:

Destination	Target
10.0.0.0/16	local

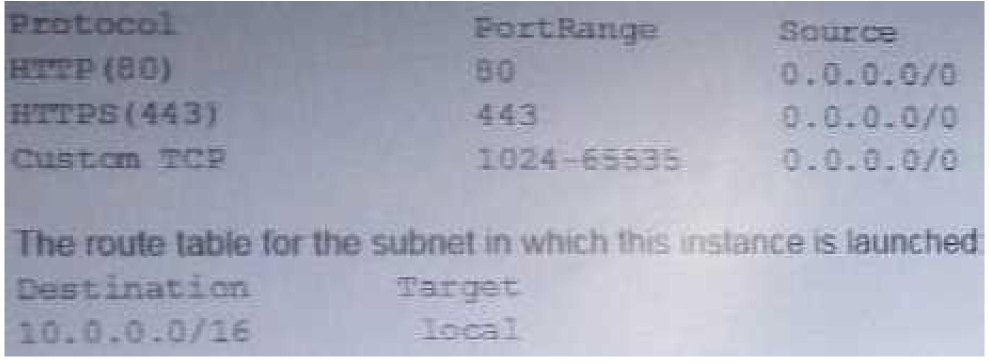
Based on the information provided what is causing the lack of access to S3 from the instance?

A. The instance profile does not have explicit permissions to write objects to the S3 bucket.
B. The route table does not have a rule tor all traffic to pass through a NAT gateway.
C. The route table does not have a rule for all traffic to pass through an internet gateway
D. The security group does not allow all TCP and all UDP traffic.

Answer: C

Explanation:
In practice, to cover the different types of clients that might initiate traffic to public-facing instances in your VPC, you can open ephemeral ports 1024-65535. However, you can also add rules to the ACL to deny traffic on any malicious ports within that range. Ensure that you place the DENY rules earlier in the table than the ALLOW rules that open the wide range of ephemeral ports.

NEW QUESTION 270
A System Administrator is trying to identify why Put Object calls are not made from an Amazon EC2 instance to an Amazon bucket in the same region. The instance is launched in a subnet with CIDR range 10.1.0.24 and 'Auto assign public IP set to yes. The instance profile tied to this instance has AmazonS3Access policy.
Security group rules for the instance:



Protocol	PortRange	Source
HTTP(80)	80	0.0.0.0/0
HTTPS(443)	443	0.0.0.0/0
Custom TCP	1024-65535	0.0.0.0/0

The route table for the subnet in which this instance is launched:

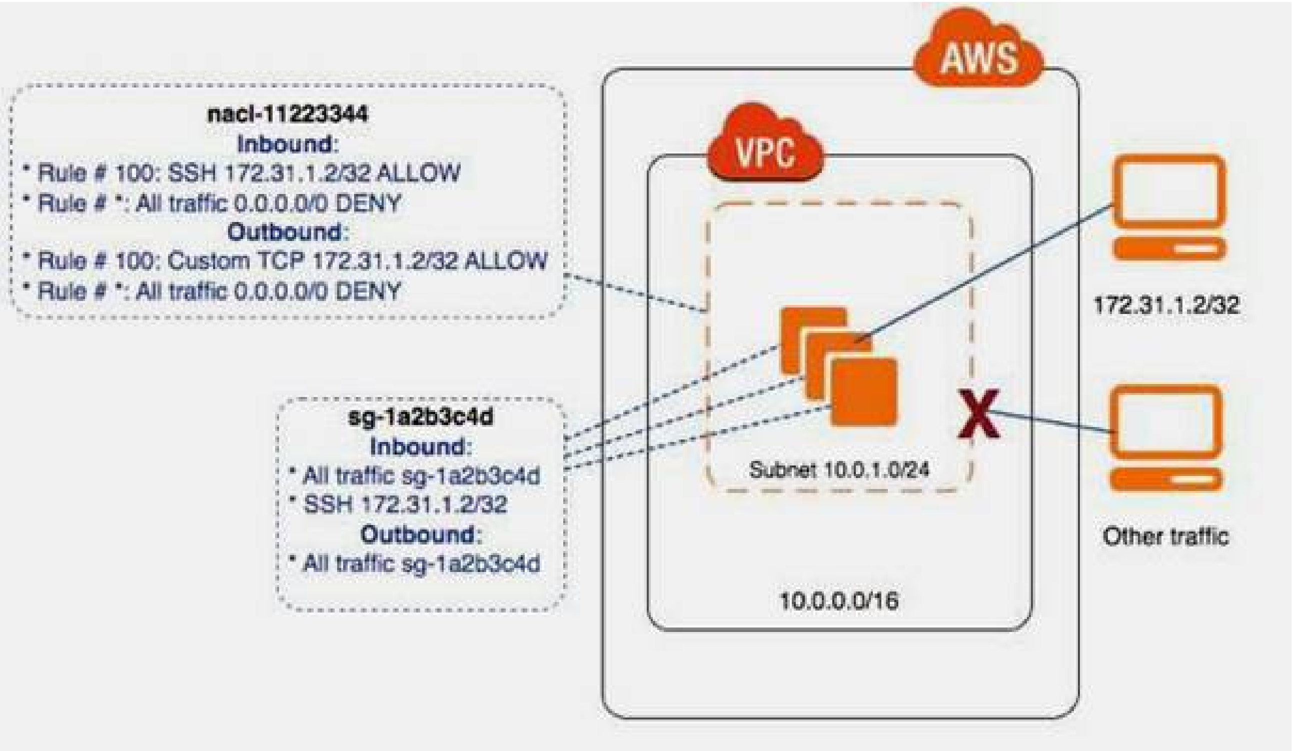
Destination	Target
10.0.0.0/16	local

Based on the information provided what is causing the lack of access to S3 from the instance?

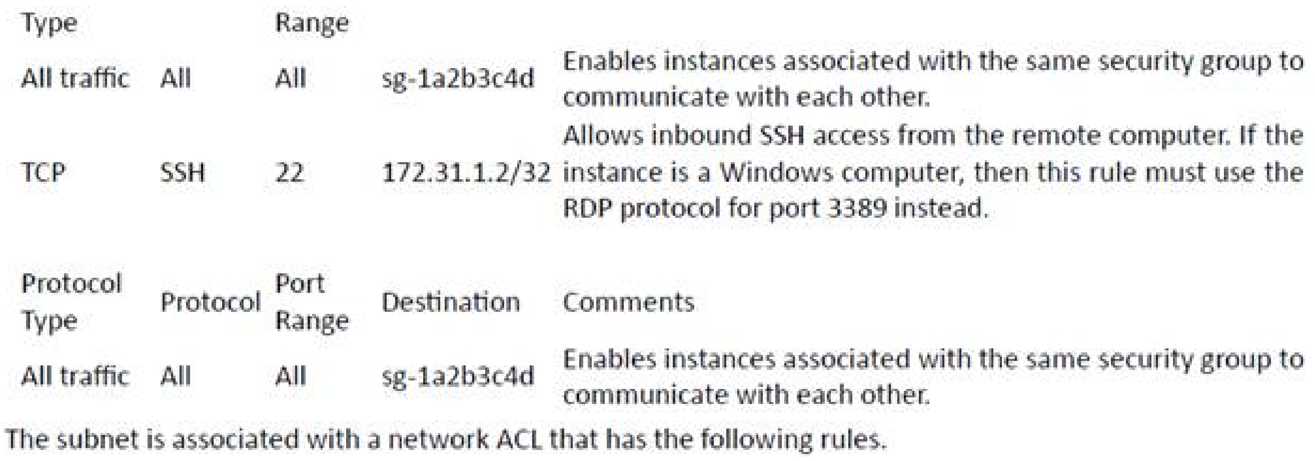
A. The instance profile does not have explicit permissions to write objects to the S3 bucket.
B. The route table does not have a rule for all traffic to pass through a NAT gateway.
C. The route table does not have rule for all traffic to pass through an internet gateway

Answer: B

Explanation:
Controlling Access to Instances in a Subnet
In this example, instances in your subnet can communicate with each other, and are accessible from a trusted remote computer. The remote computer may be a computer in your local network or an instance in a different subnet or VPC that you use to connect to your instances to perform administrative tasks. Your security group rules and network ACL rules allow access from the IP address of your remote computer (172.31.1.2/32). All other traffic from the Internet or other networks is denied.


AWS
VPC
nacl-11223344
Inbound:
* Rule # 100: SSH 172.31.1.2/32 ALLOW
* Rule # *: All traffic 0.0.0.0/0 DENY
Outbound:
* Rule # 100: Custom TCP 172.31.1.2/32 ALLOW
* Rule # *: All traffic 0.0.0.0/0 DENY
sg-1a2b3c4d
Inbound:
* All traffic sg-1a2b3c4d
* SSH 172.31.1.2/32
Outbound:
* All traffic sg-1a2b3c4d
Subnet 10.0.1.0/24
10.0.0.0/16
172.31.1.2/32
X
Other traffic

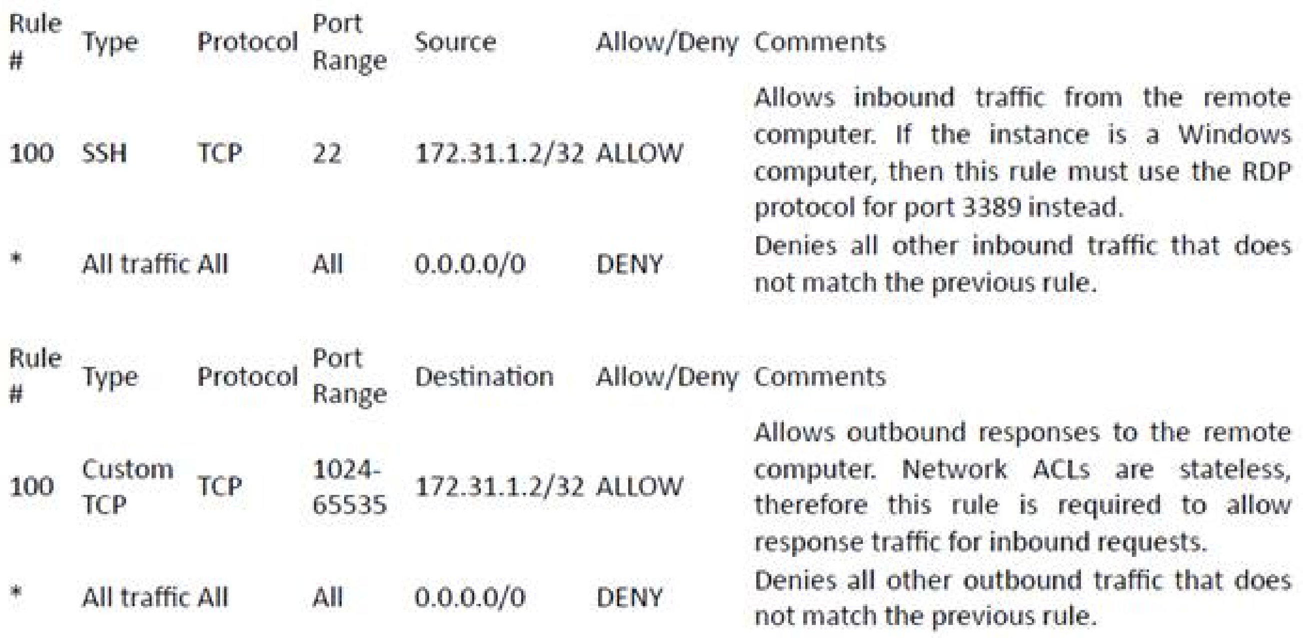
All instances use the same security group (sg-1a2b3c4d), with the following rules.
Protocol Protocol Port Source Comments



Type		Range		
All traffic	All	All	sg-1a2b3c4d	Enables instances associated with the same security group to communicate with each other.
TCP	SSH	22	172.31.1.2/32	Allows inbound SSH access from the remote computer. If the instance is a Windows computer, then this rule must use the RDP protocol for port 3389 instead.

Protocol Type	Protocol	Port Range	Destination	Comments
All traffic	All	All	sg-1a2b3c4d	Enables instances associated with the same security group to communicate with each other.

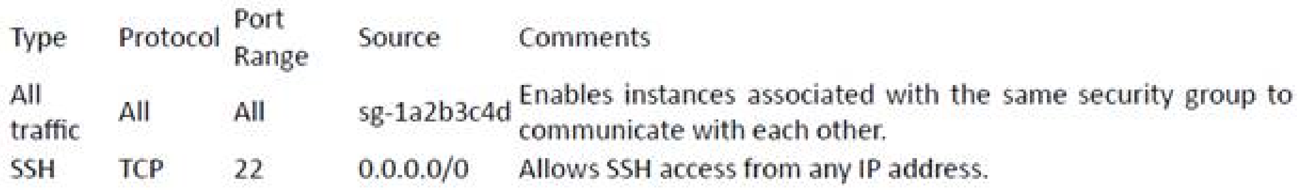
The subnet is associated with a network ACL that has the following rules.



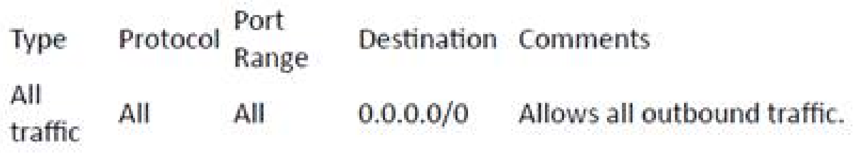
Rule #	Type	Protocol	Port Range	Source	Allow/Deny	Comments
100	SSH	TCP	22	172.31.1.2/32	ALLOW	Allows inbound traffic from the remote computer. If the instance is a Windows computer, then this rule must use the RDP protocol for port 3389 instead.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all other inbound traffic that does not match the previous rule.

Rule #	Type	Protocol	Port Range	Destination	Allow/Deny	Comments
100	Custom TCP	TCP	1024-65535	172.31.1.2/32	ALLOW	Allows outbound responses to the remote computer. Network ACLs are stateless, therefore this rule is required to allow response traffic for inbound requests.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all other outbound traffic that does not match the previous rule.

This scenario gives you the flexibility to change the security groups or security group rules for your instances, and have the network ACL as the backup layer of defense. The network ACL rules apply to all instances in the subnet, so if you accidentally make your security group rules too permissive, the network ACL rules continue to permit access only from the single IP address. For example, the following rules are more permissive than the earlier rules ?X they allow inbound SSH access from any IP address.



Type	Protocol	Port Range	Source	Comments
All traffic	All	All	sg-1a2b3c4d	Enables instances associated with the same security group to communicate with each other.
SSH	TCP	22	0.0.0.0/0	Allows SSH access from any IP address.



Type	Protocol	Port Range	Destination	Comments
All traffic	All	All	0.0.0.0/0	Allows all outbound traffic.

However, only other instances within the subnet and your remote computer are able to access this instance. The network ACL rules still prevent all inbound traffic to the subnet except from your remote computer.

NEW QUESTION 271
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 274
A SysOps Administrator has been tasked with deploying a company infrastructure as code. The administrator wants to write a single template that can be reused for multiple environment in a sale, repeatable manner.
What is the recommended way to use AWS CloudFormation to meet this requirement?

A. Use parameters to provision the resource.
B. Use rested stack to provision the resources.
C. Use Amazon EC2 user data to provision the resources.
D. Use stack policies to provision the resources.

Answer: D

NEW QUESTION 277
A SysOps Administrator has an AWS Lambda function that performs maintenance on versions AWS resources. This function must be run nightly.
Which is the MOST cost-effective solution?

A. Launch a single l2.nano Amazon EC2 instance and create a Linux corn job to invoke the Lambda function at the same every right.
B. Set up an Amazon CloudWatch metric alarm to invoke the Lambda function at the same time every night.
C. Schedule a CloudWatch event to invoke the Lambda function at the same time every night.
D. Implement a Chef recipe in Opsworks stack to invoke the Lambda function at the same time every night

Answer: C

Explanation:
Using AWS Lambda with Amazon CloudWatch Events
You can create a Lambda function and direct AWS Lambda to execute it on a regular schedule. You can specify a fixed rate (for example, execute a Lambda function every hour or 15 minutes), or you can specify a Cron expression. For more information on expressions schedules, see Schedule Expressions Using Rate or Cron.
This functionality is available when you create a Lambda function using the AWS Lambda console or the AWS CLI. To configure it using the AWS CLI, see Run an AWS Lambda Function on a Schedule Using the AWS CLI. The console provides CloudWatch Events as an event source. At the time of creating a Lambda function, you choose this event source and specify a time interval.
If you have made any manual changes to the permissions on your function, you may need to reapply
the scheduled event access to your function. You can do that by using the following CLI command.

```
$ aws lambda add-permission --function-name function_name\
--action 'lambda:InvokeFunction' --principal events.amazonaws.com \
--statement-id 'statement_id' \
--source-arn arn:aws:events:region:account-id:rule/rule_name
```

Each AWS account can have up to 100 unique event sources of the CloudWatch Events- Schedule source type. Each of these can be the event source for up to five Lambda functions. That is, you can have up to 500 Lambda functions that can be executing on a schedule in your AWS account.
The console also provides a blueprint (lambda-canary) that uses the CloudWatch Events - Schedule source type. Using this blueprint, you can create a sample Lambda function and test this feature. The example code that the blueprint provides checks for the presence of a specific webpage and specific text string on the webpage. If either the webpage or the text string is not found, the Lambda function throws an error.

NEW QUESTION 281
......

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
You are currently hosting multiple applications in a VPC and have logged numerous port scans coming in from a specific IP address block. Your security team has requested that all access from the offending IP address block be denied for the next 24 hours.
Which of the following is the best method to quickly and temporarily deny access from the specified IP address block?

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

Answer: B

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

NEW QUESTION 2
When attached to an Amazon VPC which two components provide connectivity with external networks? Choose 2 answers

A. Elastic IPS (EIP)
B. NAT Gateway (NAT)
C. Internet Gateway {IGW)
D. Virtual Private Gateway (VGW)

Answer: CD

NEW QUESTION 3
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 4
Which two AWS services provide out-of-the-box user configurable automatic backup-as-a-service and backup rotation options? Choose 2 answers

A. Amazon S3
B. Amazon RDS
C. Amazon EBS
D. Amazon Redshift

Answer: BD

Explanation:
By default: at no additional charge, Amazon RDS enables automated backups of your DB Instance with a 1-day retention period. By default: Amazon Redshift enables automated backups of your data warehouse cluster with a 1- day retention period.

NEW QUESTION 5
You are creating an Auto Scaling group whose Instances need to insert a custom metric into CloudWatch.
Which method would be the best way to authenticate your CloudWatch PUT request?

A. Create an IAM role with the Put MetricData permission and modify the Auto Scaling launch configuration to launch instances in that role

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

Answer: A

NEW QUESTION 6
The majority of your Infrastructure is on premises and you have a small footprint on AWS Your company has decided to roll out a new application that is heavily dependent on low latency connectivity to LOAP for authentication Your security policy requires minimal changes to the company's existing application user management processes.
What option would you implement to successfully launch this application1?

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

Answer: C

Explanation:
Since it requires no changes to the authentication infrastructure as requested in the question. Option D creates a new LDAP, trusts, etc.

NEW QUESTION 7
Which services allow the customer to retain full administrative privileges of the underlying EC2 instances?
Choose 2 answers

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

Answer: AC

Explanation:
The below services provide Root level access:
* EC2
* Elastic Beanstalk
* Elastic MapReduce ?V Master Node
* Opswork

NEW QUESTION 8
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

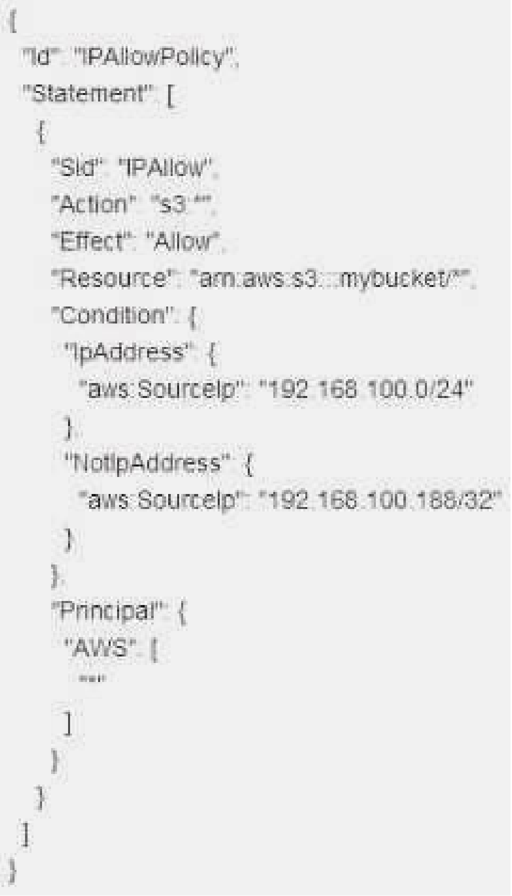
Explanation:
This is an odd question. First of all, option A cannot be right because ELB does not failover. Cannot be C because Route 53 does work with hard coded IP. Only B & D cannot be rule out so best answer.

NEW QUESTION 9
You are designing a system that has a Bastion host. This component needs to be highly available without human intervention.
Which of the following approaches would you select?

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

Answer: C

NEW QUESTION 10
Which of the following statements about this S3 bucket policy is true?



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

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

Answer: B

NEW QUESTION 10
You run a web application where web servers on EC2 Instances are In an Auto Scaling group Monitoring over the last 6 months shows that 6 web servers are necessary to handle the minimum load During the day up to 12 servers are needed Five to six days per year, the number of web servers required might go up to 15.
What would you recommend to minimize costs while being able to provide hill availability?

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

Answer: A

Explanation:
The only plausible answer is A because all other answers include Spot Instances that can be removed without warning and that would not be highly available.

NEW QUESTION 15
You have been asked to propose a multi-region deployment of a web-facing application where a controlled portion of your traffic is being processed by an alternate region.
Which configuration would achieve that goal?

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

Answer: A

Explanation:
The question is asking ??a controlled portion of your traffic??, that would be established with weighted routing policy.
See: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

NEW QUESTION 19
A media company produces new video files on-premises every day with a total size of around 100GBS after compression All files have a size of 1 - 2 GB and need to be uploaded to Amazon S3 every night in a fixed time window between 3am and 5am Current upload takes almost 3 hours, although less than half of the available bandwidth is used.
What step(s) would ensure that the file uploads are able to complete in the allotted time window?

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

Answer: B

Explanation:
Reference:
https://aws.amazon.com/blogs/aws/amazon-s3-multipart-upload/

NEW QUESTION 20
What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment of the primary OB instance fails?

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

Answer: D

Explanation:
https://aws.amazon.com/rds/faqs/

NEW QUESTION 24
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 29
An organization is planning to create 5 different AWS accounts considering various security requirements. The organization wants to use a single payee account by using the consolidated billing option. Which of the below mentioned statements is true with respect to the above information?

A. Master (Paye
B. account will get only the total bill and cannot see the cost incurred by each account
C. Master (Paye
D. account can view only the AWS billing details of the linked accounts
E. It is not recommended to use consolidated billing since the payee account will have access to the linked accounts
F. Each AWS account needs to create an AWS billing policy to provide permission to the payee account

Answer: B

Explanation:
AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS. accounts within a single organization by making a single paying account. Consolidated billing enables the organization to see a combined view of the AWS charges incurred by each account as well as obtain a detailed cost report for each of the individual AWS accounts associated with the paying account. The payee account will not have any other access than billing data of linked accounts.

NEW QUESTION 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 31
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 35
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 38
A user is trying to understand AWS SNS. To which of the below mentioned end points is SNS unable to send a notification?

A. Email JSON
B. HTTP
C. AWS SQS
D. AWS SES

Answer: D

Explanation:
Amazon Simple Notification Service (Amazon SNS. is a fast, flexible, and fully managed push messaging service. Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS. queues or to any HTTP endpoint. The user can select one the following transports as part of the subscription requests: ??HTTP??, ??HTTPS??,??Email??, ??Email-JSON??, ??SQS??, ??and SMS??.

NEW QUESTION 39
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 43
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 48

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

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

Answer: D

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

NEW QUESTION 51
A root AWS account owner is trying to understand various options to set the permission to AWS S3. Which of the below mentioned options is not the right option to grant permission for S3?

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

Answer: B

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

NEW QUESTION 53
An organization is using AWS since a few months. The finance team wants to visualize the pattern of AWS spending. Which of the below AWS tool will help for this requirement?

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

Answer: B

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

NEW QUESTION 54
A user has launched an ELB which has 5 instances registered with it. The user deletes the ELB by mistake. What will happen to the instances?

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

Answer: D

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

NEW QUESTION 58
A user is accessing RDS from an application. The user has enabled the Multi AZ feature with the MS SQL RDS DB. During a planned outage how will AWS ensure that a switch from DB to a standby replica will not affect access to the application?

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

Answer: B

Explanation:
In the event of a planned or unplanned outage of a DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone if the user

has enabled Multi AZ. The automatic failover mechanism simply changes the DNS record of the DB instance to point to the standby DB instance. As a result, the user will need to re-establish any existing connections to the DB instance. However, as the DNS is the same, the application can access DB seamlessly.

NEW QUESTION 60
An organization is using cost allocation tags to find the cost distribution of different departments and projects. One of the instances has two separate tags with the key/ value as ??InstanceName/HR??, ??CostCenter/HR??. What will AWS do in this case?

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

Answer: D

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

NEW QUESTION 61
A user has created an ELB with the availability zone US-East-1

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

Answer: D

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

NEW QUESTION 62
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 64
A user has launched an EBS backed EC2 instance. What will be the difference while performing the
restart or stop/start options on that instance?

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

Answer: A

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

NEW QUESTION 66
A user has created a queue named ??myqueue?? in US-East region with AWS SQS. The user??s AWS account ID is 123456789012. If the user wants to perform some action on this queue, which of the below Queue URL should he use?

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

E. http:// 123456789012.sq
F. us-east-1.amazonaws.com/myqueue

Answer: A

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

NEW QUESTION 68
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 69
A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

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

Answer: D

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

NEW QUESTION 73
A user wants to make so that whenever the CPU utilization of the AWS EC2 instance is above 90%, the redlight of his bedroom turns on. Which of the below mentioned AWS services is helpful for this purpose?

A. AWS CloudWatch + AWS SES
B. AWS CloudWatch + AWS SNS
C. Non
D. It is not possible to configure the light with the AWS infrastructure services
E. AWS CloudWatch and a dedicated software turning on the light

Answer: B

Explanation:
Amazon Simple Notification Service (Amazon SNS. is a fast, flexible, and fully managed push messaging service. Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS. queues or to any HTTP endpoint. The user can configure some sensor devices at his home which receives data on the HTTP end point (REST calls. and turn on the red light. The user can configure the CloudWatch alarm to send a notification to the AWS SNS HTTP end point (the sensor device. and it will turn the light red when there is an alarm condition.

NEW QUESTION 76
A user has setup an EBS backed instance and a CloudWatch alarm when the CPU utilization is more than 65%. The user has setup the alarm to watch it for 5 periods of 5 minutes each. The CPU utilization is 60% between 9 AM to 6 PM. The user has stopped the EC2 instance for 15 minutes between 11 AM to 11:15 AM. What will be the status of the alarm at 11:30 AM?

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

Answer: B

Explanation:
Amazon CloudWatch alarm watches a single metric over a time period the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The state of the alarm will be OK for the whole day. When the user stops the instance for three periods

the alarm may not receive the data

NEW QUESTION 77
A user has created an ELB with Auto Scaling. Which of the below mentioned offerings from ELB helps the user to stop sending new requests traffic from the load balancer to the EC2 instance when the instance is being deregistered while continuing in-flight requests?

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

Answer: C

Explanation:
The Elastic Load Balancer connection draining feature causes the load balancer to stop sending new requests to the back-end instances when the instances are deregistering or become unhealthy, while ensuring that inflight requests continue to be served.

NEW QUESTION 79
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 80
A user has setup an EBS backed instance and attached 2 EBS volumes to it. The user has setup a CloudWatch alarm on each volume for the disk data. The user has stopped the EC2 instance and detached the EBS volumes. What will be the status of the alarms on the EBS volume?

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

Answer: B

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

NEW QUESTION 82
A user has launched an EBS backed instance with EC2-Classic. The user stops and starts the instance. Which of the below mentioned statements is not true with respect to the stop/start action?

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

Answer: C

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

NEW QUESTION 87
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 88
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 89
A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

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

Answer: B

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

NEW QUESTION 91
A user has hosted an application on EC2 instances. The EC2 instances are configured with ELB and Auto Scaling. The application server session time out is 2 hours. The user wants to configure connection draining to ensure that all in-flight requests are supported by ELB even though the instance is being deregistered. What time out period should the user specify for connection draining?

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

Answer: B

NEW QUESTION 93
A user has created a queue named ??awsmodule?? with SQS. One of the consumers of queue is down for 3 days and then becomes available. Will that component receive message from queue?

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

Answer: A

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

NEW QUESTION 98
A user has configured ELB with a TCP listener at ELB as well as on the back-end instances. The user wants to enable a proxy protocol to capture the source and destination IP information in the header. Which of the below mentioned statements helps the user understand a proxy protocol with TCP configuration?

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

Answer: A

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

NEW QUESTION 99
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 103
A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned SSL protocols is not supported by the security policy?

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

Answer: A

Explanation:
Elastic Load Balancing uses a Secure Socket Layer (SSL. negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. Elastic Load Balancing supports the following versions of the SSL protocol:
TLS 1.2
TLS 1.1
TLS 1.0
SSL 3.0
SSL 2.0

NEW QUESTION 105
A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80. and a DB server in the private subnet (port 3306.. The user is configuring a security group for the public subnet (WebSecGrp. and the private subnet (DBSecGrp.. Which of the below mentioned entries is required in the private subnet database security group (DBSecGrp.?

A. Allow Inbound on port 3306 for Source Web Server Security Group (WebSecGrp.
B. Allow Inbound on port 3306 from source 20.0.0.0/16
C. Allow Outbound on port 3306 for Destination Web Server Security Group (WebSecGrp.
D. Allow Outbound on port 80 for Destination NAT Instance IP

Answer: A

Explanation:
A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the private subnet can receive inbound traffic from the public subnet on the DB port. Thus, configure port 3306 in Inbound with the source as the Web Server Security Group (WebSecGrp.. The user should configure ports 80 and 443 for Destination 0.0.0.0/0 as the route table directs traffic to the NAT instance from the private subnet.

NEW QUESTION 107
A user has launched an EC2 Windows instance from an instance store backed AMI. The user has also set the Instance initiated shutdown behavior to stop. What will happen when the user shuts down the OS?

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

Answer: B

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

NEW QUESTION 110
A user has created a VPC with public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24 . The NAT instance ID is i-a12345. Which of the below mentioned entries are required in the main route table attached with the private subnet to allow instances to connect with the internet?

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

Answer: A

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

NEW QUESTION 114
An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%. The higher CPU usage triggers an event for Auto Scaling as per the scaling policy. If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

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

Answer: D

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

NEW QUESTION 119
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 123
A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services does not provide detailed monitoring with CloudWatch?

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

D. AWS Route53

Answer: A

Explanation:
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, EC2, Auto Scaling, ELB, and Route 53 can provide the monitoring data every minute.

NEW QUESTION 126
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 130
A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24. and a public subnet (20.0.0.0/24.. The user??s data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?

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

Answer: D

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

NEW QUESTION 133
A user has created a mobile application which makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

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

Answer: C

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

NEW QUESTION 138
A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services provides detailed monitoring with CloudWatch without charging the user extra?

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

Answer: B

Explanation:
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic

monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, ELB, OpsWorks, and Route 53 can provide the monitoring data every minute without charging the user.

NEW QUESTION 141
A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the
user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?

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

Answer: B

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

NEW QUESTION 145
A user is using the AWS SQS to decouple the services. Which of the below mentioned operations is not supported by SQS?

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

Answer: D

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

NEW QUESTION 149
A user has launched an EC2 instance. However, due to some reason the instance was terminated. If the user wants to find out the reason for termination, where can he find the details?

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

Answer: D

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

NEW QUESTION 151
A user has configured ELB with SSL using a security policy for secure negotiation between the client and load balancer. Which of the below mentioned security policies is supported by ELB?

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

Answer: C

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

NEW QUESTION 155
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 157
A user has created an Auto Scaling group using CLI. The user wants to enable CloudWatch detailed monitoring for that group. How can the user configure this?

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

Answer: B

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

NEW QUESTION 158
A user is trying to create a PIOPS EBS volume with 8 GB size and 200 IOPS. Will AWS create the volume?

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

Answer: C

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

NEW QUESTION 161
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 165
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 168

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

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

Answer: D

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

NEW QUESTION 170
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 174
A user has two EC2 instances running in two separate regions. The user is running an internal memory management tool, which captures the data and sends it to CloudWatch in US East, using a CLI with the same namespace and metric. Which of the below mentioned options is true with respect to the above statement?

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

Answer: B

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

NEW QUESTION 177
A sys admin has enabled a log on ELB. Which of the below mentioned activities are not captured by the log?

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

Answer: B

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

NEW QUESTION 178
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 181
A user is running a batch process on EBS backed EC2 instances. The batch process starts a few instances to process hadoop Map reduce jobs which can run between 50 ?V 600 minutes or sometimes for more time. The user wants to configure that the instance gets terminated only when the process is completed. How can the user configure this with CloudWatch?

A. Setup the CloudWatch action to terminate the instance when the CPU utilization is less than 5%
B. Setup the CloudWatch with Auto Scaling to terminate all the instances
C. Setup a job which terminates all instances after 600 minutes
D. It is not possible to terminate instances automatically

Answer: D

Explanation:
Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which terminates the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action.

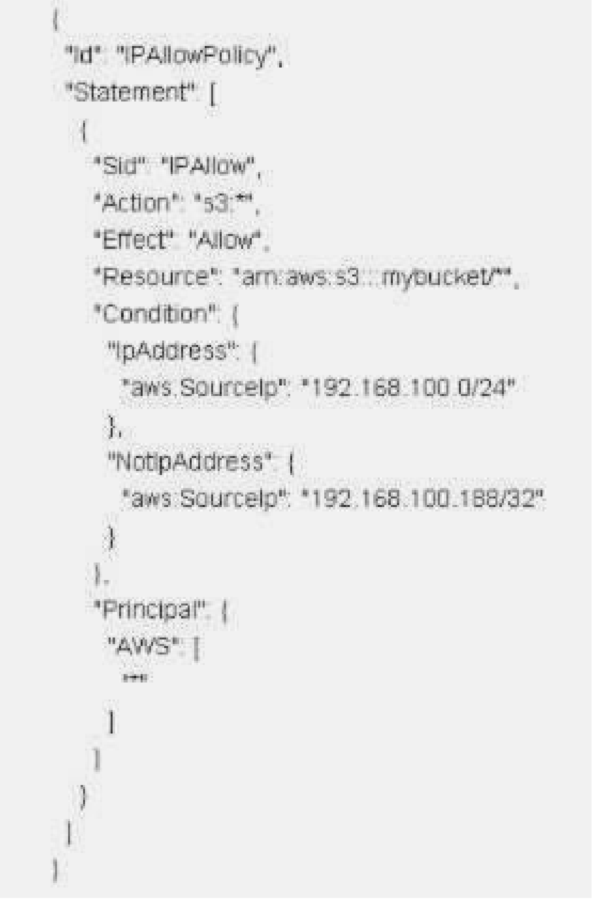
NEW QUESTION 186
A user has launched a Windows based EC2 instance. However, the instance has some issues and the user wants to check the log. When the user checks the Instance console output from the AWS console, what will it display?

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

Answer: D

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

NEW QUESTION 191
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 193
Your business is building a new application that will store its entire customer database on a RDS MySQL database, and will have various applications and users that will query that data for different purposes.
Large analytics jobs on the database are likely to cause other applications to not be able to get the query results they need to, before time out. Also, as your data grows, these analytics jobs will start to take more time, increasing the negative effect on the other applications.
How do you solve the contention issues between these different workloads on the same data?

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

Answer: B

Explanation:
Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory caching system, instead of relying entirely on slower disk-based databases. The service simplifies and offloads the management, monitoring and operation of in-memory cache environments, enabling your engineering resources to focus on developing applications. Using Amazon ElastiCache, you can not only improve load and response times to user actions and queries, but also reduce the cost associated with scaling web applications.
Amazon ElastiCache automates common administrative tasks required to operate a distributed cache environment. Using Amazon ElastiCache, you can add a caching layer to your application architecture in a matter of minutes via a few clicks of the AWS Management Console. Once a cache cluster is provisioned, Amazon ElastiCache automatically detects and replaces failed cache nodes, providing a resilient system that mitigates the risk of overloaded databases, which slow website and application load times. Through integration with Amazon CloudWatch monitoring, Amazon ElastiCache provides enhanced visibility into key performance metrics associated with your cache nodes. Amazon ElastiCache is protocol-compliant with Memcached and Redis, so code, applications, and popular tools that you use today with your existing Memcached or Redis environments will work seamlessly with the service. As with all Amazon Web Services,

NEW QUESTION 194
When you put objects in Amazon S3, what is the indication that an object was successfully stored?

A. Each S3 account has a special bucket named_s3_log
B. Success codes are written to this bucket with a timestamp and checksum.
C. A success code is inserted into the S3 object metadata.
D. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
E. Amazon S3 is engineered for 99.999999999% durabilit
F. Therefore, there is no need to confirm that data was inserted.

Answer: C

Explanation:
To ensure that data is not corrupted traversing the network, use the Content-MD5 form field. When you use this form field, Amazon S3 checks the object against the provided MD5 value. If they do not match, Amazon S3 returns an error.
success_action_status
The status code returned to the client upon successful upload if success_action_redirectis not specified.
Accepts the values 200, 201, or 204 (default).
If the value is set to 200 or 204, Amazon S3 returns an empty document with a 200 or 204 status code.
If the value is set to 201, Amazon S3 returns an XML document with a 201 status code.
If the value is not set or if it is set to an invalid value, Amazon S3 returns an empty document with a 204 status code.
Type: String Default: None Note
Some versions of the Adobe Flash player do not properly handle HTTP responses with an empty body. To support uploads through Adobe Flash, we recommend setting success_action_statusto 201.
Source: http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html

NEW QUESTION 196
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 197
An application you maintain consists of multiple EC2 instances in a default tenancy VPC. This application has undergone an internal audit and has been determined to require dedicated hardware for one instance. Your compliance team has given you a week to move this instance to single-tenant hardware.
Which process will have minimal impact on your application while complying with this requirement?

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

Answer: D

Explanation:
Reference:
See: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated- instance.html#dedicated-apichanges
You cannot change the tenancy of a default instance after you??ve launched it. You can change the tenancy of an instance from ??dedicated?? to ??host?? after you??ve launched it, and vice versa.

NEW QUESTION 200
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 202
Which features can be used to restrict access to data in S3? Choose 2 answers

A. Set an S3 ACL on the bucket or the object.
B. Create a CloudFront distribution for the bucket.
C. Set an S3 bucket policy.
D. Enable IAM Identity Federation
E. Use S3 Virtual Hosting

Answer: AC

Explanation:
https://aws.amazon.com/s3/faqs/

NEW QUESTION 204
A photo-sharing service stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider. Which AWS Security Token Service approach to temporary access should you use for the Amazon S3 operations?

A. SAML-based Identity Federation
B. Cross-Account Access
C. AWS Identity and Access Management roles
D. Web Identity Federation

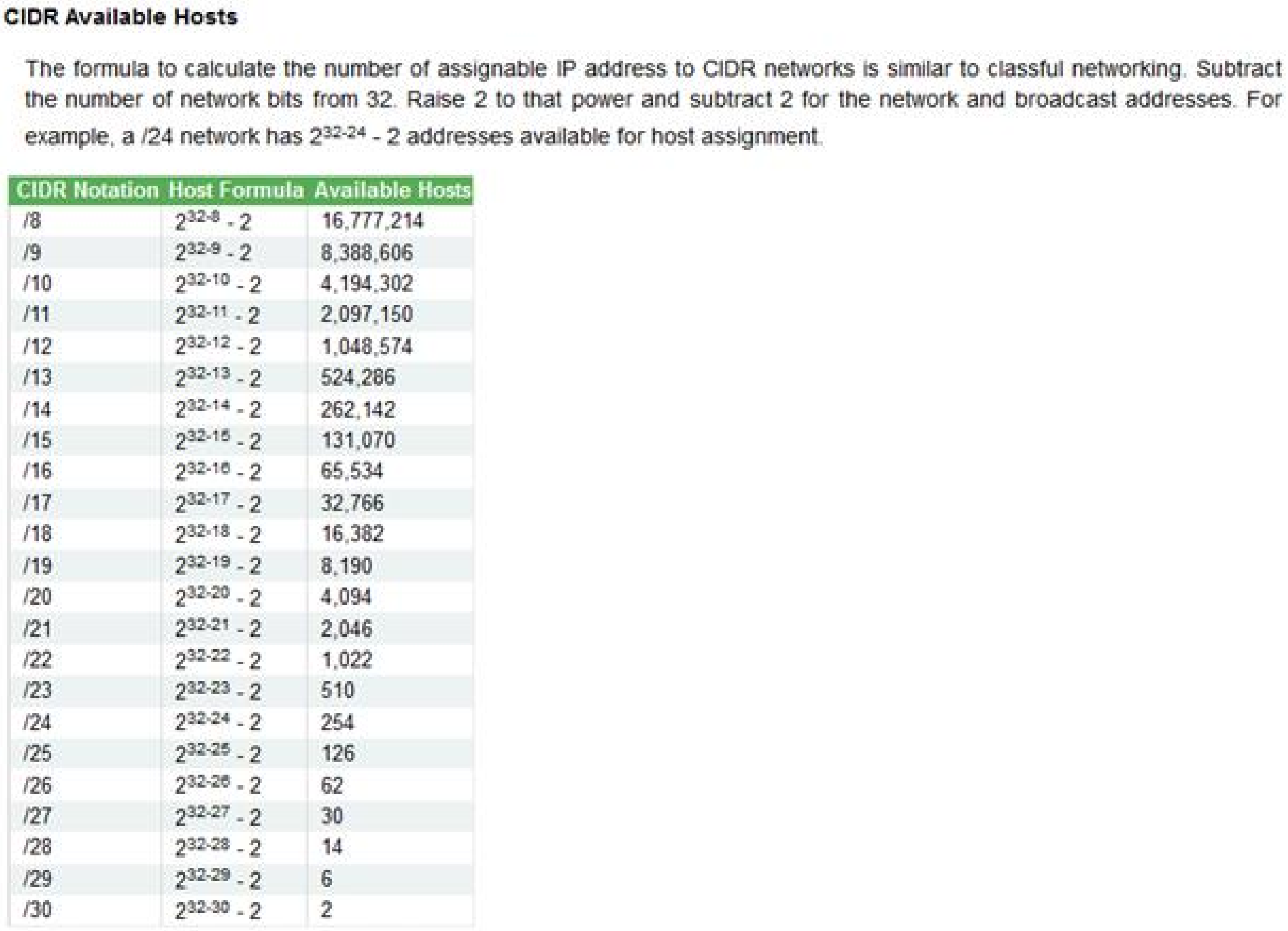
Answer: D

NEW QUESTION 209
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 210
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 214
The Security tram is connect because the number of AWS identity and access Management (IAM) policies being in the environment is increasing. The tasked a SysOps Administrator to report on the number of IAM policies in use and use the total IAM policies.
Which AWS service should the Administrator use to check how current IAM policy compares to current limits?

A. MWS Trusted Advisor
B. Amazon Inspector
C. AWS Config
D. Organizations

Answer: C

Explanation:
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

NEW QUESTION 218
A SysOps Administrator has attempted to copy an Marketplace AMI an associated billing Product code that was shared another account. When the copy process is attempted, it fails.
What action can be taken to successfully copy the AMI to the target destination?

A. Use an EC2 instance in the account by using the shared AMI and then created an AMI from the instance
B. Launch an EC2 instance in the account by using the shared AMI and then create an AMI from the instance
C. Use the AWS CLI with the --nobillingProduct flag to execute the copy and ignore the billingProductcode.
D. Create a VPC peering connection between the source and target account to facilitate the AMI copy process.

Answer: D

NEW QUESTION 222
A SysOps Administrator must take a team's single existing AWS CloudFormation template and split it into smaller, service specific template. All of the service in the template reference a single, shared Amazon S3 bucket.
What should the Administrator do to ensure that this S3 bucket can be referenced by all the service templates?

A. Include the S3 bucket as a mapping in each template
B. Add the S3 bucket as a resource in each template
C. Create the S3 bucket in its own template and export it
D. Generate the S3 bucket using StackSets

Answer: D

NEW QUESTION 226
A SysOps Administrator supports a legacy application that is hardcoded to service example.com. The application has recently been moved to AWS. The external DNS are managed by a third-party provider. The Administrator has set up an internal domain for example.com and configured this record using Amazon Route.
What solution offers the MOST efficient way to have instances in the same account resolve to the Route 53 service instead of the provider?

A. Hardcode the name server record to the internal Route 53 IP address tor each instance
B. Enable DNS resolution in the subnets as required
C. Ensure that DNS resolution is enabled on the VPC
D. Create an OS-specific hardcoded entry tor DNS resolution to the private URL

Answer: C

Explanation:
Using DNS with Your VPC
Domain Name System (DNS) is a standard by which names used on the Internet are resolved to their corresponding IP addresses. A DNS hostname is a name that uniquely and absolutely names a computer; it's composed of a host name and a domain name. DNS servers resolve DNS hostnames to their corresponding IP addresses.
Public IPv4 addresses enable communication over the Internet, while private IPv4 addresses enable communication within the network of the instance (either EC2-Classic or a VPC). For more information, see IP Addressing in Your VPC.
We provide an Amazon DNS server. To use your own DNS server, create a new set of DHCP options for your VPC. For more information, see DHCP Options Sets.
Contents
DNS Hostnames
DNS Support in Your VPC DNS Limits
Viewing DNS Hostnames for Your EC2 Instance Updating DNS Support for Your VPC
Using Private Hosted Zones

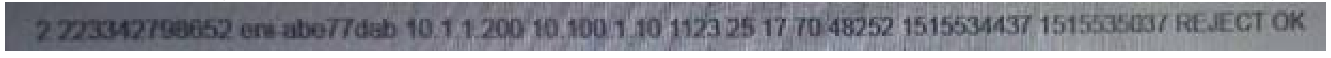
NEW QUESTION 230
A SysOps Administrator must run a script on production servers to fix an issue. The company has a policy block all remote interface access to production servers. The Based on this situation how should the Administrator execute the script?

A. Share and use the Amazon EC2 key pairs to gain access to the servers and run the script
B. Put the script into the user data of the instances
C. Configure the script to run as a cron job or scheduled task on the EC2 instances
D. Use Amazon EC2 Systems Manager to run the script

Answer: A

Explanation:
https://aws.amazon.com/getting-started/tutorials/deploy-code-vm/

NEW QUESTION 235
An Amazon EC2 instance is unable to connect to an SMTP server in a different subnet. Other instances are successfully communication with the SMTP servers, however Flow Logs have been enabled on the SMTP server's network interface and show the following information



```
2 223342798652 eni-abe77dab 10.1.1.200 10.100.1.10 1123 25 17 70 48252 1515534437 1515535037 REJECT OK
```

A. Add the instance to the security group for the SMTP server and ensure that it is permitted to communicate over TCP port 25.
B. Disable the iptables server on the SMTP server so that the instance can properly communicate over the network.
C. Install an email on the instance to ensure that it communicates correctly on TCP port 25 to theSMTP server.
D. Add a rule to the security group for the instance to explicit permit TCP port 25 outbound to any address.

Answer: D

NEW QUESTION 240
A company has created a separate AWS account for all development work to protect the production environment in this development account, developers have permission to manipulate IAM policies and roles. Corporate policies require that developers and blocked from accessing some services. What is the BEST way to grant the developers privileges in the development account while still complying with corporate policies?

A. Create a service control policy in AWS Organizations and apply it to the development account
B. Create a customer managed policy in IAM and apply it to all users within the development account
C. Create a job function policy in IAM and apply it to all users within the development account
D. Create an IAM policy and apply it in API Gateway to restrict the development account

Answer: A

Explanation:
https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-in-aws-organizations/

NEW QUESTION 242
An application stores data in an Amazon RDS database instance. Automated RDS snapshots are taken during specified backup windows every night. In addition, a SysOps Administrator takes monthly manual RDS snapshots. During a maintenance window, the RDS instance was accidentally deleted. How can the Administrator restore the DRS database instance?

A. Restore the instance from the last available automated snapshot.
B. Restore the instance from the last available manual snapshot.
C. Restore the instance from the last full RDS snapshot and subsequent incremental snapshots
D. Restore the instance from the RDS in the secondary Availability Zone

Answer: A

Explanation:
Creating a Final Snapshot and Retaining Automated Backups
When you delete a DB instance, you can choose whether to create a final snapshot of the DB instance. You can also choose to retain automated backups after the DB instance is deleted. To be able to restore the DB instance at a later time, create a final snapshot or retain automated backups.
How to To be able to restore To delete a DB instance quickly, Instead of creating a snapshot, you choose your deleted DB you can skip creating a final DB can choose to enable Retain
instance at a later snapshot. time, create a final DB Important
automated backups when you delete a DB instance. These backups
snapshot.
If you skip the snapshot, to are still subject to the retention restore your DB instance you period of the DB instance and age
need one of the following:
out the same way systems
You have to use an earlier snapshots do. manual snapshot of the DB instance to restore the DB instance to that snapshot's point in time.
You have to choose to retain automated backups; you can use those to restore it to any point in time within your retention period.
Automated backups
Automated backups are retained for All automated backups All automated backups are a set period of time, regardless of are deleted and can't deleted and can't be whether you chose to create a final be recovered, unless recovered, unless you choose snapshot. They are retained for to retain automated backups you enable Retain automated backups.
when you delete the DB retention period that was set on the
DB instance at the time you deleted Manual instance.
Earlier manual Earlier manual snapshots it.
snapshots
snapshots aren't aren't deleted. No snapshots are deleted. deleted.
You can't create a final snapshot of your DB instance if it has the status creating, failed, incompatible- restore, or incompatible-network. For more information about DB instance statuses, see DB Instance Status.

NEW QUESTION 243
An errant process is known to use in an entire processor and run at 100%. A SysOps Administrator wants to automate restarting the instance once the problem occurs for more than minutes.
How can this be accomplished?

A. Create an Amazon CloudWatch alarm or the Amazon EC2 instance with basic monitoring Enable an action to restart the instance
B. Create a CloudWatch alarm for the EC2 instance with detailed monitoring Enable an action to restart the instance
C. Create an AWS Lambda function to restart the EC2 instance triggered on a scheduled basis every 2 minutes
D. Create a Lambda function start the EC2 instance triggered by EC2 health

Answer: D

Explanation:
You can use CloudWatch Events to trigger an AWS Lambda function to start and stop your EC2 instances at scheduled intervals.
Note: This article provides an example for a simple solution. For a more robust solution, see AWS Instance Scheduler.
Resolution
CloudWatch Events allows you to create an event that is triggered at a specified time or interval in response to events that take place in your account. For example, you can create an event using CloudWatch Events for a specific time of day, or you can create an alarm when CPU utilization for an instance reaches a specific threshold. You can also configure a Lambda function to start and stop instances when triggered by these events.
In this example, we use Lambda functions to start and stop EC2 instances, and then we use CloudWatch Events to start instances in the morning and stop the instances at night.
1. Open the AWS Lambda console, and choose Create function.
2. Choose Author from scratch.
3. Enter a Name for your function, such as "StopEC2Instances."
4. From the Runtime drop-down menu, choose Python2.7.
5. Expand the Role drop-down menu, and then choose Create a custom role. This opens a new tab or window in your browser.
6. In the IAM Role drop-down menu, choose Create a new IAM Role, and enter a Role Name, such as ??lambda_start_stop_ec2."
7. Expand View Policy Document, choose Edit, and then choose Ok when prompted to read the documentation.

NEW QUESTION 244
A company is running an Oracle database engine that handles heavy online transaction processing (OLTP) structured data traffic.
How can a SysOps administrator ensure that the database has high availability?

A. Use Amazon DynamoOB to store the data
B. Use Amazon RDS Multi -AZ deployment to store the data
C. Use Amazon RDS read replicas in a different region to store the data
D. Use an Amazon Redshift cluster to store the data

Answer: B

NEW QUESTION 249
A company is migrating an application to AWS that requires access to a legacy system, which remain in the company's data centre. The application runs inside a VPC in the company's AWS account. The application must offer a consistent and low-latency response to its users
How can these requirements be met?

A. Create a software-based VPN connection between the Amazon VPC and the on-premises network
B. Create an AWS Direct Connect connection between AWS and the on-premises network and then use a private virtual interface
C. Create a hardware-based IPsec VPN connection between the VPC in AWS and the on-premises network
D. Create an overlay network by using third-party software and use that to connect the X/PC back to the on-premises network

Answer: B

Explanation:
Private Connectivity to your Amazon VPC. You can use AWS Direct Connect to establish a private virtual interface from your on-premise network directly to your Amazon VPC, providing you with a private, high bandwidth network connection between your network and your VPC.

NEW QUESTION 251
After a particularly high bill, an organization wants to review the use of AWS services.
What AWS service will allow the SysOps Administrator to quickly view this information to shared it, and will also forest expenses for the billing period?

A. AWS Trusted Advisor
B. Amazon QuickSight
C. AWS Cost and Usage Report
D. AWS Cost Explorer

Answer: C

NEW QUESTION 252
A SysOps Administrator has set up a new Application Load Balancer (ALB) in front of a pair of private web server in multiple Availability Zones. After deployment an updates CloudFormation template with many changes, user now goes to one web server only.
What is the NOST likely reason that the traffic is not being balanced between both servers?

A. The faulty is returning HTTP 200 has been removed.
B. Sticky session have been disabled in the ALB for the working sever.
C. The ALB using a custom ping path that is not found on the faulty server.
D. The web client are using HTTP/2, which is terminated at the ALB.

Answer: B

Explanation:
Until now, the behavior of load balancers has been to route each request independently to the Amazon EC2 instance with the least load. With the stickiness feature, you can configure the load balancer to bind user sessions to specific application instances. All requests coming from the user during the session will be sent to the same application instance. Elastic Load Balancing supports two mechanisms to provide session stickiness: load balancer-generated HTTP cookies, which allow browser-based session lifetimes, and application-generated HTTP cookies, which allow application- specific session lifetimes. You can learn more about this feature by visiting the ELB Developers Guide.

NEW QUESTION 256
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 260
A company has a new requirement stating that all resources in AWS must be tagged according to a set policy. Which AWS service should to enforce and continually identify all resources that are not in compliance with the policy?

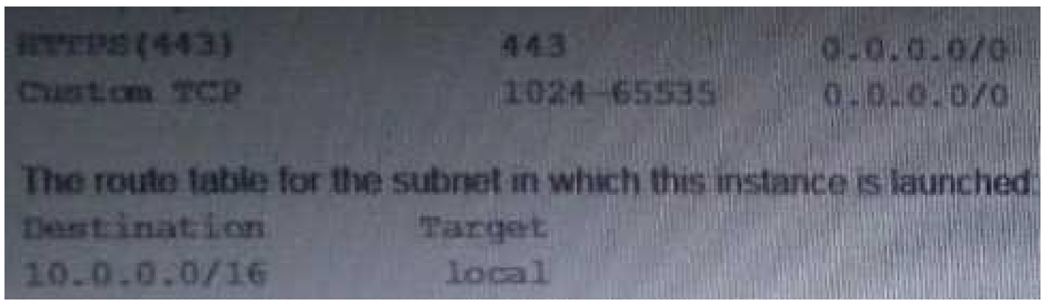
A. AWS CloudTrail
B. Amazon Inspector
C. AWS Config
D. AWS Systems Manager

Answer: C

Explanation:

AWS Config
TRACK RESOURCE INVENTORY AND CHANGES
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

NEW QUESTION 265
Exhibit:



HTTPS(443)	443	0.0.0.0/0
Custom TCP	1024-65535	0.0.0.0/0

The route table for the subnet in which this instance is launched:

Destination	Target
10.0.0.0/16	local

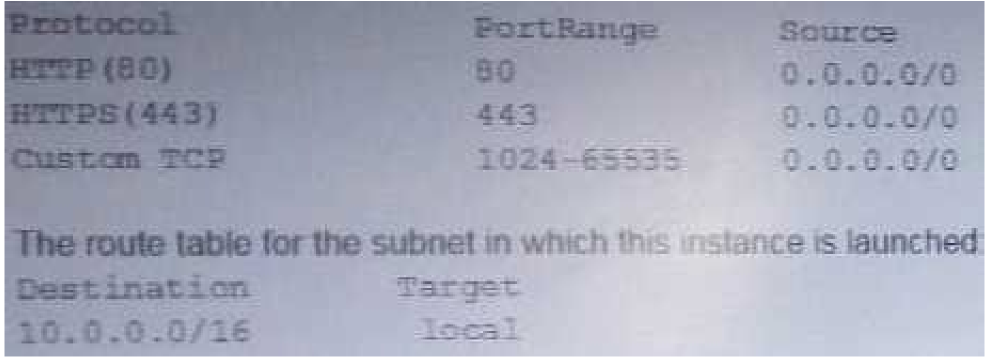
Based on the information provided what is causing the lack of access to S3 from the instance?

A. The instance profile does not have explicit permissions to write objects to the S3 bucket.
B. The route table does not have a rule tor all traffic to pass through a NAT gateway.
C. The route table does not have a rule for all traffic to pass through an internet gateway
D. The security group does not allow all TCP and all UDP traffic.

Answer: C

Explanation:
In practice, to cover the different types of clients that might initiate traffic to public-facing instances in your VPC, you can open ephemeral ports 1024-65535. However, you can also add rules to the ACL to deny traffic on any malicious ports within that range. Ensure that you place the DENY rules earlier in the table than the ALLOW rules that open the wide range of ephemeral ports.

NEW QUESTION 270
A System Administrator is trying to identify why Put Object calls are not made from an Amazon EC2 instance to an Amazon bucket in the same region. The instance is launched in a subnet with CIDR range 10.1.0.24 and 'Auto assign public IP set to yes. The instance profile tied to this instance has AmazonS3Access policy.
Security group rules for the instance:



Protocol	PortRange	Source
HTTP(80)	80	0.0.0.0/0
HTTPS(443)	443	0.0.0.0/0
Custom TCP	1024-65535	0.0.0.0/0

The route table for the subnet in which this instance is launched:

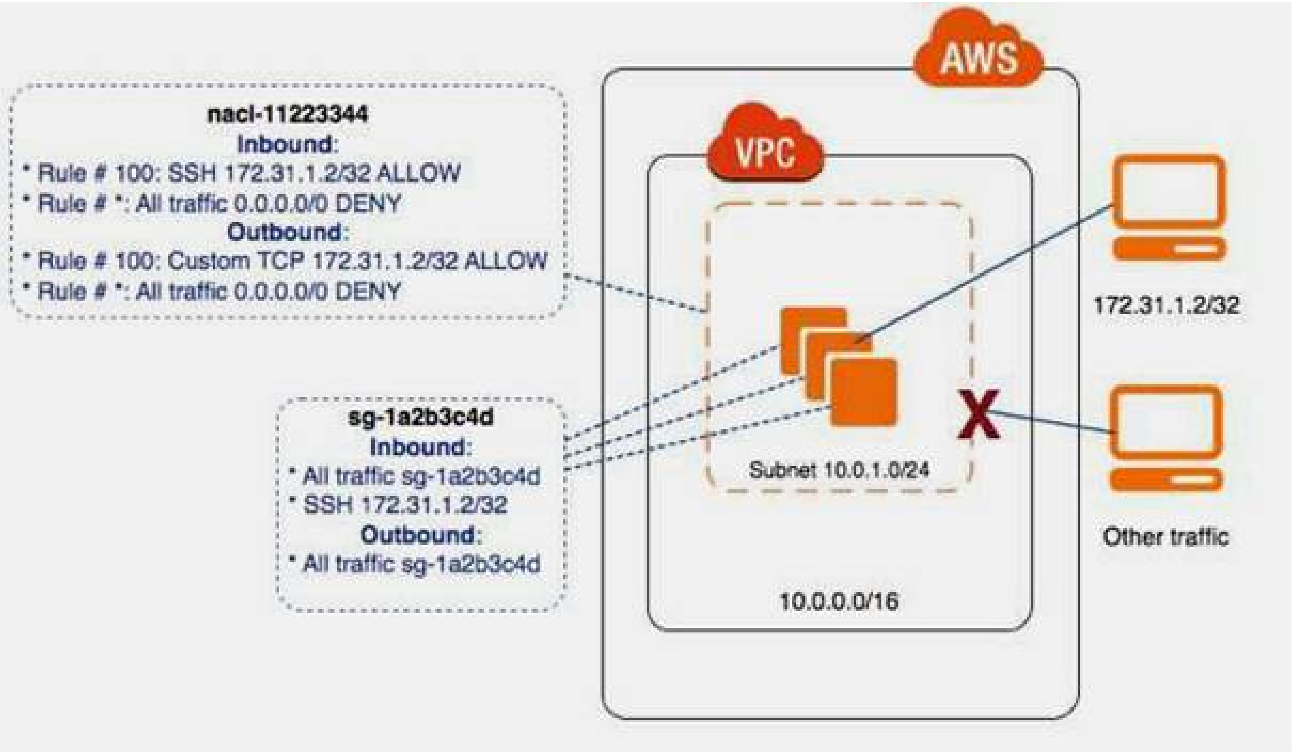
Destination	Target
10.0.0.0/16	local

Based on the information provided what is causing the lack of access to S3 from the instance?

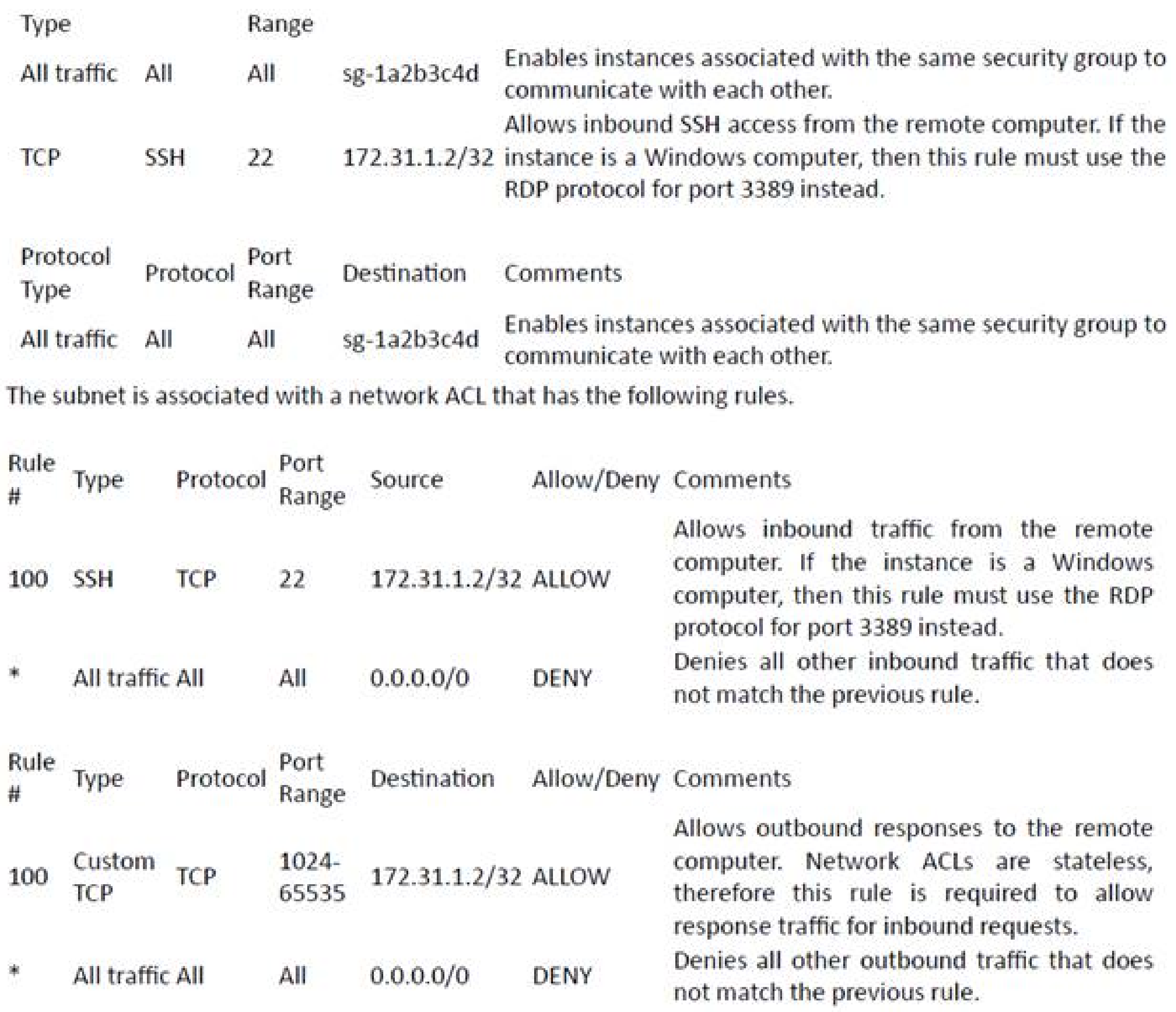
A. The instance profile does not have explicit permissions to write objects to the S3 bucket.
B. The route table does not have a rule for all traffic to pass through a NAT gateway.
C. The route table does not have rule for all traffic to pass through an internet gateway

Answer: B

Explanation:
Controlling Access to Instances in a Subnet
In this example, instances in your subnet can communicate with each other, and are accessible from a trusted remote computer. The remote computer may be a computer in your local network or an instance in a different subnet or VPC that you use to connect to your instances to perform administrative tasks. Your security group rules and network ACL rules allow access from the IP address of your remote computer (172.31.1.2/32). All other traffic from the Internet or other networks is denied.


nacl-11223344
Inbound:
* Rule # 100: SSH 172.31.1.2/32 ALLOW
* Rule # *: All traffic 0.0.0.0/0 DENY
Outbound:
* Rule # 100: Custom TCP 172.31.1.2/32 ALLOW
* Rule # *: All traffic 0.0.0.0/0 DENY
AWS
VPC
sg-1a2b3c4d
Inbound:
* All traffic sg-1a2b3c4d
* SSH 172.31.1.2/32
Outbound:
* All traffic sg-1a2b3c4d
Subnet 10.0.1.0/24
10.0.0.0/16
172.31.1.2/32
X
Other traffic

All instances use the same security group (sg-1a2b3c4d), with the following rules.
Protocol Protocol Port Source Comments



Type		Range		
All traffic	All	All	sg-1a2b3c4d	Enables instances associated with the same security group to communicate with each other.
TCP	SSH	22	172.31.1.2/32	Allows inbound SSH access from the remote computer. If the instance is a Windows computer, then this rule must use the RDP protocol for port 3389 instead.

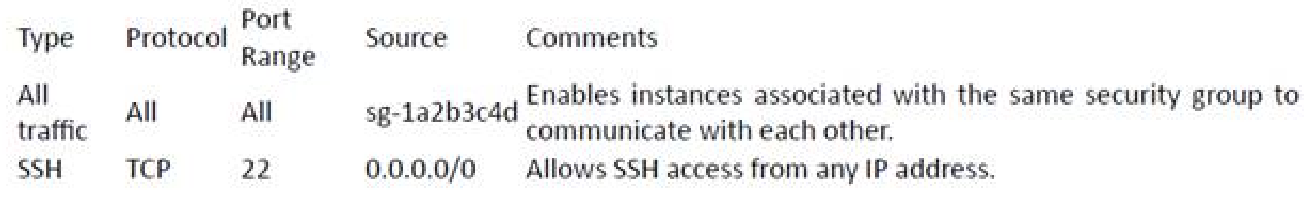
Protocol Type	Protocol	Port Range	Destination	Comments
All traffic	All	All	sg-1a2b3c4d	Enables instances associated with the same security group to communicate with each other.

The subnet is associated with a network ACL that has the following rules.

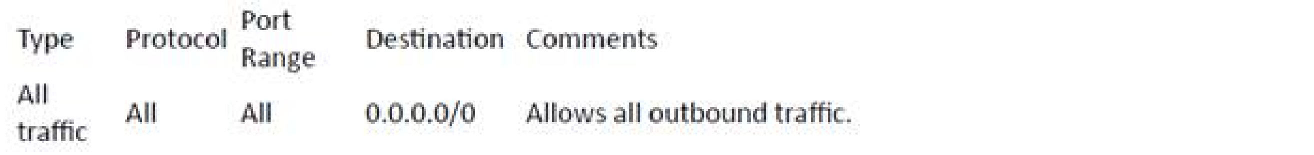
Rule #	Type	Protocol	Port Range	Source	Allow/Deny	Comments
100	SSH	TCP	22	172.31.1.2/32	ALLOW	Allows inbound traffic from the remote computer. If the instance is a Windows computer, then this rule must use the RDP protocol for port 3389 instead.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all other inbound traffic that does not match the previous rule.

Rule #	Type	Protocol	Port Range	Destination	Allow/Deny	Comments
100	Custom TCP	TCP	1024-65535	172.31.1.2/32	ALLOW	Allows outbound responses to the remote computer. Network ACLs are stateless, therefore this rule is required to allow response traffic for inbound requests.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all other outbound traffic that does not match the previous rule.

This scenario gives you the flexibility to change the security groups or security group rules for your instances, and have the network ACL as the backup layer of defense. The network ACL rules apply to all instances in the subnet, so if you accidentally make your security group rules too permissive, the network ACL rules continue to permit access only from the single IP address. For example, the following rules are more permissive than the earlier rules ?X they allow inbound SSH access from any IP address.



Type	Protocol	Port Range	Source	Comments
All traffic	All	All	sg-1a2b3c4d	Enables instances associated with the same security group to communicate with each other.
SSH	TCP	22	0.0.0.0/0	Allows SSH access from any IP address.



Type	Protocol	Port Range	Destination	Comments
All traffic	All	All	0.0.0.0/0	Allows all outbound traffic.

However, only other instances within the subnet and your remote computer are able to access this instance. The network ACL rules still prevent all inbound traffic to the subnet except from your remote computer.

NEW QUESTION 271
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 274
A SysOps Administrator has been tasked with deploying a company infrastructure as code. The administrator wants to write a single template that can be reused for multiple environment in a sale, repeatable manner.
What is the recommended way to use AWS CloudFormation to meet this requirement?

A. Use parameters to provision the resource.
B. Use rested stack to provision the resources.
C. Use Amazon EC2 user data to provision the resources.
D. Use stack policies to provision the resources.

Answer: D

NEW QUESTION 277
A SysOps Administrator has an AWS Lambda function that performs maintenance on versions AWS resources. This function must be run nightly.
Which is the MOST cost-effective solution?

A. Launch a single l2.nano Amazon EC2 instance and create a Linux corn job to invoke the Lambda function at the same every right.
B. Set up an Amazon CloudWatch metric alarm to invoke the Lambda function at the same time every night.
C. Schedule a CloudWatch event to invoke the Lambda function at the same time every night.
D. Implement a Chef recipe in Opsworks stack to invoke the Lambda function at the same time every night

Answer: C

Explanation:
Using AWS Lambda with Amazon CloudWatch Events
You can create a Lambda function and direct AWS Lambda to execute it on a regular schedule. You can specify a fixed rate (for example, execute a Lambda function every hour or 15 minutes), or you can specify a Cron expression. For more information on expressions schedules, see Schedule Expressions Using Rate or Cron.
This functionality is available when you create a Lambda function using the AWS Lambda console or the AWS CLI. To configure it using the AWS CLI, see Run an AWS Lambda Function on a Schedule Using the AWS CLI. The console provides CloudWatch Events as an event source. At the time of creating a Lambda function, you choose this event source and specify a time interval.
If you have made any manual changes to the permissions on your function, you may need to reapply
the scheduled event access to your function. You can do that by using the following CLI command.

```
$ aws lambda add-permission --function-name function_name\
--action 'lambda:InvokeFunction' --principal events.amazonaws.com \
--statement-id 'statement_id' \
--source-arn arn:aws:events:region:account-id:rule/rule_name
```

Each AWS account can have up to 100 unique event sources of the CloudWatch Events- Schedule source type. Each of these can be the event source for up to five Lambda functions. That is, you can have up to 500 Lambda functions that can be executing on a schedule in your AWS account.
The console also provides a blueprint (lambda-canary) that uses the CloudWatch Events - Schedule source type. Using this blueprint, you can create a sample Lambda function and test this feature. The example code that the blueprint provides checks for the presence of a specific webpage and specific text string on the webpage. If either the webpage or the text string is not found, the Lambda function throws an error.

NEW QUESTION 281
......

Relate Links

100% Pass Your SOA-C01 Exam with Exambible Prep Materials

https://www.exambible.com/SOA-C01-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/