Amazon AWS-SysOps

AWS Certified SysOps Administrator – Associate

Version: 15.0

QUESTION NO: 1

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

QUESTION NO: 2

When preparing for a compliance assessment of your system built inside of AWS. what are three best-practices for you to prepare for an audit? (Choose three.)

A.
Gather evidence of your IT operational controls

B.
Request and obtain applicable third-party audited AWS compliance reports and certifications

C.
Request and obtain a compliance and security tour of an AWS data center for a pre-assessment security review

D.
Request and obtain approval from AWS to perform relevant network scans and in-depth penetration tests of your system's Instances and endpoints

E.
Schedule meetings with AWS's third-party auditors to provide evidence of AWS compliance that maps to your control objectives

Answer: A,B,D
Explanation:

QUESTION NO: 3

You have started a new job and are reviewing your company's infrastructure on AWS You notice one web application where they have an Elastic Load Balancer (&B) in front of web instances in an Auto Scaling Group When you check the metrics for the ELB in CloudWatch you see four healthy instances in Availability Zone (AZ) A and zero in AZ B There are zero unhealthy instances.

What do you need to fix to balance the instances across AZs?

A.
Set the ELB to only be attached to another AZ

B.
Make sure Auto Scaling is configured to launch in both AZs

C.
Make sure your AMI is available in both AZs

D.
Make sure the maximum size of the Auto Scaling Group is greater than 4

Answer: B
Explanation:

QUESTION NO: 4

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

Which option will provide the most scalable solution for communicating between the application and SQS?

A.
Ensure the application instances are properly configured with an Elastic Load Balancer

B.
Ensure the application instances are launched in private subnets with the EBS-optimized option enabled

C.
Ensure the application instances are launched in public subnets with the associate-public-IP-address=true option enabled

D.
Launch application instances in private subnets with an Auto Scaling group and Auto Scaling triggers configured to watch the SQS queue size

Answer: D

Explanation:

Bandwidth literally means network not IO Bandwidth. Having alerts to scale the Autoscaling is most sophisticated option.

QUESTION NO: 5

You have identified network throughput as a bottleneck on your m1.small EC2 instance when uploading data Into Amazon S3 In the same region.

How do you remedy this situation?

A.
Add an additional ENI

B.
Change to a larger Instance

C.
Use DirectConnect between EC2 and S3

D.
Use EBS PIOPS on the local volume

Answer: B
Explanation:

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

QUESTION NO: 6

When attached to an Amazon VPC, which two components provide connectivity with external networks? (Choose two.)

A.
Elastic IPS (EIP)

B.
NAT Gateway (NAT)

C.
Internet Gateway (IGW)

D.
Virtual Private Gateway (VGW)

Answer: C,D
Explanation:

QUESTION NO: 7

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

What should you do to avoid potential service disruptions during the ramp up in traffic?

A.
Ensure that you have pre-allocated 175 Elastic IP addresses so that each server will be able to obtain one as it launches

B.
Check the service limits in Trusted Advisor and adjust as necessary so the forecasted count remains within limits.

C.
Change your Auto Scaling configuration to set a desired capacity of 175 prior to the launch of the marketing campaign

D.
Pre-warm your Elastic Load Balancer to match the requests per second anticipated during peak demand prior to the marketing campaign

Answer: D

Explanation:

Amazon ELB is able to handle the vast majority of use cases for our customers without requiring "pre-warming" (configuring the load balancer to have the appropriate level of capacity based on

expected traffic).

Reference:

https://aws.amazon.com/articles/1636185810492479#pre-warming

QUESTION NO: 8

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

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

A.
Change the thresholds set on the Auto Scaling group health check

B.
Add an Elastic Load Balancing health check to your Auto Scaling group

C.
Increase the value for the Health check interval set on the Elastic Load Balancer

D.
Change the health check set on the Elastic Load Balancer to use TCP rather than HTTP checks

Answer: A

Explanation:

QUESTION NO: 9

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

A.
Amazon S3

B.
Amazon RDS

C.
Amazon EBS

D.
Amazon Red shift

Answer: B,D

Explanation:

By default, and 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.

QUESTION NO: 10

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

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

A.
Nothing, there are no single points of failure in this architecture.

B.
Create and attach a second IGW to provide redundant internet connectivity.

C.
Create and configure a second Elastic Load Balancer to provide a redundant load balancer.

D.
Create a second multi-AZ RDS instance in another Availability Zone and configure replication to provide a redundant database.

Answer: A

Explanation:

You need multiple ELB if you want HA across regions.

“AWS Load Balancer –Cross Network

Many times it happens that after setting up your ELB, you experience significant drops in your performance. The best way to handle this situation is to start with identifying whether your ELB is single AZ or multiple AZ, as single AZ ELB is also considered as one of the Single Points of Failures on AWS Cloud. Once you identify your ELB, it is necessary to make sure ELB loads are kept cross regions.”

Reference:

https://www.botmetric.com/blog/eliminating-single-points-of-failures-on-aws-cloud/

QUESTION NO: 11

Which of the following are characteristics of Amazon VPC subnets? (Choose two.)

A.
Each subnet maps to a single Availability Zone

B.
A CIDR block mask of /25 is the smallest range supported

C.
Instances in a private subnet can communicate with the internet only if they have an Elastic IP.

D.
By default, all subnets can route between each other, whether they are private or public

E.
V Each subnet spans at least 2 Availability zones to provide a high-availability environment

Answer: A,D

Explanation:

“Each subnet must reside entirely within one Availability Zone and cannot span zones.”

“Every subnet that you create is automatically associated with the main route table for the VPC.”

Reference:

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

QUESTION NO: 12

You are creating an Auto Scaling group whose Instances need to insert a custom metric into CloudWatch.

Which method would be the best way to authenticate your CloudWatch PUT request?

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

B.
Create an IAM user with the PutMetricData permission and modify the Auto Scaling launch configuration to inject the userscredentials into the instance User Data

C.
Modify the appropriate Cloud Watch metric policies to allow the Put MetricData permission to instances from the Auto Scaling group

D.
Create an IAM user with the PutMetricData permission and put the credentials in a private repository and have applications on the server pull the credentials as needed

Answer: A

Explanation:

Creates an IAM role is always the best practice to give permissions to EC2 instances in order to

interact with other AWS services

QUESTION NO: 13

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

A.
Data is automatically saved as an E8S volume.

B.
Data is automatically saved as an ESS snapshot.

C.
Data is automatically deleted.

D.
Data is unavailable until the instance is restarted.

Answer: C
Explanation:

We recommend that you use AMIs backed by Amazon EBS, because they launch faster and use persistent storage.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html#choose-an-ami-by-root-device

QUESTION NO: 14

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

What could you do to help alleviate the pressure on the infrastructure while maintaining availability

during these events? (Choose three.)

A.
Leverage CloudFront for the delivery of the articles.

B.
Add RDS read-replicas for the read traffic going to your relational database

C.
Leverage ElastiCache for caching the most frequently used data.

D.
Use SOS to queue up the requests for the technical posts and deliver them out of the queue.

E.
Use Route53 health checks to fail over to an S3 bucket for an error page.

Answer: A,B,C
Explanation:

QUESTION NO: 15

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

What option would you implement to successfully launch this application1?

A.
Create a second, independent LOAP server in AWS for your application to use for authentication

B.
Establish a VPN connection so your applications can authenticate against your existing on-premises LDAP servers

C.
Establish a VPN connection between your data center and AWS create a LDAP replica on AWS and configure your application to use the LDAP replica for authentication

D.
Create a second LDAP domain on AWS establish a VPN connection to establish a trust relationship between your new and existing domains and use the new domain for authentication

Answer: C

Explanation:

Create read replica(RODC) of main LDAP server so that LDAP read replica or RODC can authenticate with application locally.

Creating new domain and trust relationship would require lot of work and changes in exiting ldap configuration so D cannot be answer here.

QUESTION NO: 16

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

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

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

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

C.
Two public subnets for ELB two private subnets for the web-servers and two private subnets for RDS

D.
Two public subnets for ELB two public subnets for the web-servers, and two public subnets for RDS

Answer: C

Explanation:

While using ELB for web applications, ensure that you place all other EC2 instances in private subnets wherever possible. Except where there is an explicit requirement for instances requiring outside world access and Elastic IP attached, place all the instances in private subnets only. In the Amazon VPC environment, only ELBs must be in the public subnet as secure practice.

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balance

QUESTION NO: 17

An application that you are managing has EC2 instances & Dynamo OB tables deployed to several AWS Regions in order to monitor the performance of the application globally, you would like to see two graphs:

1) Avg CPU Utilization across all EC2 instances

2) Number of Throttled Requests for all DynamoDB tables.

How can you accomplish this?

A.
Tag your resources with the application name, and select the tag name as the dimension in the Cloudwatch Management console to view the respective graphs

B.
Use the Cloud Watch CLI tools to pull the respective metrics from each regional endpoint Aggregate the data offline & store it for graphing in CloudWatch.

C.
Add SNMP traps to each instance and DynamoDB table Leverage a central monitoring server to capture data from each instance and table Put the aggregate data into Cloud Watch for graphing.

D.
Add a CloudWatch agent to each instance and attach one to each DynamoDB table. When configuring the agent set the appropriate application name & view the graphs in CloudWatch.

Answer: B
Reference:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Tools.CLI.html

QUESTION NO: 18

When assessing an organization’s use of AWS API access credentials which of the following three credentials should be evaluated? (Choose three.)

A.
Key pairs

B.
Console passwords

C.
Access keys

D.
Signing certificates

E.
Security Group memberships

Answer: B,C,D

Explanation:

AWS provides a number of authentication mechanisms including a console, account IDs and secret keys, X.509 certificates, and MFA devices to control access to AWS APIs. Console authentication is the most appropriate for administrative or manual activities, account IDs and secret keys for accessing REST-based interfaces or tools, and X.509 certificates for SOAP-based interfaces and tools.

Your organization should consider the circumstances under which it will leverage access keys, x.509certificates, console passwords, or MFA devices.

QUESTION NO: 19

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

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

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

A.
Stop and start the instance so that it will be able to be redeployed on a healthy host system that most likely will fix the "impaired" system status

B.
Reboot your instance so that the operating system will have a chance to boot in a clean healthy state that most likely will fix the 'impaired" system status

C.
Add another dynamic private IP address to me instance and try to connect via mat new path, since the networking stack of the OS may be locked up causing the “impaired” system status.

D.
Add another Elastic Network Interface to the instance and try to connect via that new path since the networking stack of the OS may be locked up causing the "impaired" system status

E.
un-map and then re-map the EIP to the instance, since the IGWVNAT gateway may not be working properly, causing the "impaired" system status

Answer: A
Explanation:

QUESTION NO: 20

What is a placement group?

A.
A collection of Auto Scaling groups in the same Region

B.
Feature that enables EC2 instances to interact with each other via nigh bandwidth, low latency connections

C.
A collection of Elastic Load Balancers in the same Region or Availability Zone

D.
A collection of authorized Cloud Front edge locations for a distribution

Answer: B
Explanation:

QUESTION NO: 21

Your entire AWS infrastructure lives inside of one Amazon VPC. You have an Infrastructure monitoring application running on an Amazon instance in Availability Zone (AZ) A of the region, and another application instance running in AZ B. The monitoring application needs to make use of ICMP ping to confirm network reachability of the instance hosting the application.

Can you configure the security groups for these instances to only allow the ICMP ping to pass from the monitoring instance to the application instance and nothing else? If so how?

A.
No, two instances in two different AZ's can't talk directly to each other via ICMP ping as that protocol is not allowed across subnet (iebroadcast) boundaries

B.
Yes, both the monitoring instance and the application instance have to be a part of the same security group, and that security group needs to allow inbound ICMP

C.
Yes, the security group for the monitoring instance needs to allow outbound ICMP and the application instance's security group needs to allow Inbound ICMP

D.
Yes, both the monitoring instance's security group and the application instance's security group need to allow both inbound and outbound ICMP ping packets since ICMP is not a connection-oriented protocol

Answer: C
Explanation:

Even though ICMP is not a connection-oriented protocol, Security Groups are stateful. “Security groups are stateful — responses to allowed inbound traffic are allowed to flow outbound

regardless of outbound rules, and vice versa”.

Reference:

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

QUESTION NO: 22

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

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

A.
A network ACL that allows communication between the two subnets.

B.
Both instances are the same instance class and using the same Key-pair.

C.
That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.

D.
Security groups are set to allow the application host to talk to the database on the right port/protocol.

Answer: A,D

Explanation:

QUESTION NO: 23

Which services allow the customer to retain full administrative privileges of the underlying EC2 instances? (Choose two.)

A.
Amazon Elastic Map Reduce

B.
Elastic Load Balancing

C.
AWS Elastic Beanstalk

D.
Amazon Elasticache

E.
Amazon Relational Database service

Answer: A,C

Explanation:

Only the below services provide Root level access

- EC2

- Elastic Beanstalk

- Elastic MapReduce – Master Node

- Opswork

QUESTION NO: 24

You have a web-style application with a stateless but CPU and memory-intensive web tier running on a cc2 8xlarge EC2 instance inside of a VPC The instance when under load is having problems returning requests within the SLA as defined by your business The application maintains its state in a DynamoDB table, but the data tier is properly provisioned and responses are consistently fast.

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

A.
Add another cc2 8xlarge application instance, and put both behind an Elastic Load Balancer

B.
Move the cc2 8xlarge to the same Availability Zone as the DynamoDB table

C.
Cache the database responses in ElastiCache for more rapid access

D.
Move the database from DynamoDB to RDS MySQL in scale-out read-replica configuration

Answer: A
Explanation:

DynamoDB is automatically available across three facilities in an AWS Region. So moving in to a same AZ is not possible / necessary.

In this case the DB layer is not the issue, the EC2 8xlarge is the issue; so add another one with a ELB in-front of it.

See also: https://aws.amazon.com/dynamodb/faqs/

QUESTION NO: 25

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

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

A.
Create an ELB to reroute traffic to a failover instance

B.
Create a secondary ENI that can be moved to a failover instance

C.
Use Route53 health checks to fail traffic over to a failover instance

D.
Assign a secondary private IP address to the primary ENIO that can be moved to a failover instance

Answer: B,D

Explanation:

QUESTION NO: 26

You are designing a system that has a Bastion host. This component needs to be highly available without human intervention.

Which of the following approaches would you select?

A.
Run the bastion on two instances one in each AZ

B.
Run the bastion on an active Instance in one AZ and have an AMI ready to boot up in the event of failure

C.
Configure the bastion instance in an Auto Scaling group. Specify the Auto Scaling group to include multiple AZs but have a min-size of 1 and max-size of 1

D.
Configure an ELB in front of the bastion instance

Answer: C

Explanation:

QUESTION NO: 27

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

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

BrainDumps

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
Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

http://docs.aws.amazon.com/AmazonS3/latest/dev/amazon-s3-policy-keys.html

QUESTION NO: 28

Which of the following requires a custom CloudWatch metric to monitor?

A.
Data transfer of an EC2 instance

B.
Disk usage activity of an EC2 instance

C.
Memory Utilization of an EC2 instance

D.
CPU Utilization of an EC2 instance

Answer: C
Explanation:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/ec2-metricscollected.html

CPU, Disk I/O, Data Transfer are default metrics. Memory is not mentioned.

QUESTION NO: 29

You run a web application where web servers on EC2 Instances are in an Auto Scaling group. Monitoring over the last 6 months shows that 6 web servers are necessary to handle the minimum load During the day up to 12 servers are needed five to six days per year, the number of web servers required might go up to 15.

What would you recommend to minimize costs while being able to provide hill availability?

A.
6 Reserved instances (heavy utilization).

6 Reserved instances {medium utilization), rest covered by On-Demand instances

B.
6 Reserved instances (heavy utilization).

6 On-Demand instances, rest covered by Spot Instances

C.
6 Reserved instances (heavy utilization)

6 Spot instances, rest covered by On-Demand instances

D.
6 Reserved instances (heavy utilization)

6 Reserved instances (medium utilization) rest covered by Spot instances

Answer: B
Explanation:

QUESTION NO: 30

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

Which configuration would achieve that goal?

A.
Route53 record sets with weighted routing policy

B.
Route53 record sets with latency based routing policy

C.
Auto Scaling with scheduled scaling actions set

D.
Elastic Load Balancing with health checks enabled

Answer: A
Explanation:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

QUESTION NO: 31

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

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

A.
Consolidate your accounts so you have a single bill for all accounts and projects

B.
Set up auto scaling with CloudWatch alarms using SNS to notify you when you are running too many Instances in a given account

C.
Set up CloudWatch billing alerts for all AWS resources used by each project, with a notification occurring when the amount for each resource tagged to a particular project matches the budget allocated to the project.

D.
Set up CloudWatch billing alerts for all AWS resources used by each account, with email notifications when it hits 50%. 80% and 90% of its budgeted monthly spend

Answer: D
Explanation:

Consolidate your accounts so you have a single bill for all accounts and projects (Consolidation will

not help limit per account)

Set up auto scaling with CloudWatch alarms using SNS to notify you when you are running too many Instances in a given account (many instances do not directly map to cost and would not

give exact cost).

Set up CloudWatch billing alerts for all AWS resources used by each project, with a notification occurring when the amount for each resource tagged to a particular project matches the budget allocated to the project. (as each project already has an account, no need for resource tagging).

QUESTION NO: 32

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

A.
Cannot De detached or attached to an EC2 instance until me snapshot completes

B.
Can be used in read-only mode while me snapshot is in progress

C.
Can be used while me snapshot is in progress

D.
Cannot be used until the snapshot completes

Answer: C
Explanation:

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

QUESTION NO: 33

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

What two actions could you take to rectify this? (Choose two.)

A.
Increase the number of nodes in your cluster

B.
Tweak the max_item_size parameter

C.
Shrink the number of nodes in your cluster

D.
Increase the size of the nodes in the duster

Answer: A,D
Reference:

https://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/CacheMetrics.WhichShouldIMonitor.html

QUESTION NO: 34

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

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

A.
Move to an SSD backed instance

B.
Move the database to an EBS-Optimized Instance

C.
T Use Provisioned IOPs EBS

D.
Use the ephemeral storage on an m2 4xiarge Instance Instead

Answer: B,C
Explanation:

QUESTION NO: 35

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

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

A.
Run another monitoring instance that pings the monitoring instance and fires a could watch alarm mat notifies your operations team should the primary monitoring instance become unhealthy.

B.
Set a CloudWatch alarm based on EC2 system and instance status checks and have the alarm notify your operations team of any detected problem with the monitoring instance.

C.
Set a CloudWatch alarm based on the CPU utilization of the monitoring instance and have the alarm notify your operations team if C r the CPU usage exceeds 50% few more than one minute: then have your monitoring application go into a CPU-bound loop should it Detect any application problems.

D.
Have the monitoring instances post messages to an SOS queue and then dequeue those messages on another instance should the queue cease to have new messages, the second instance should first terminate the original monitoring instance start another backup monitoring instance and assume (he role of the previous monitoring instance and beginning adding messages to the SQSqueue.

Answer: B

Explanation:

QUESTION NO: 36

You have decided to change the Instance type for instances running in your application tier that are using Auto Scaling.

In which area below would you change the instance type definition?

A.
Auto Scaling launch configuration

B.
Auto Scaling group

C.
Auto Scaling policy

D.
Auto Scaling tags

Answer: A

Explanation:

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

QUESTION NO: 37

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

Which VPC component should you evaluate next?

A.
The configuration of a NAT instance

B.
The configuration of the Routing Table

C.
The configuration of the internet Gateway (IGW)

D.
The configuration of SRC/DST checking

Answer: B
Explanation:

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

QUESTION NO: 38

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

Which deployment option meets these requirements while minimizing administrative burden?

A.
Create a new stack within Opsworks add the appropriate layers to the stack and deploy the application

B.
Create a new application within Elastic Beanstalk and deploy this application to a new environment

C.
Launch a Mode JS server from a community AMI and manually deploy the application to the launched EC2 instance

D.
Launch and configure Chef Server on an EC2 instance and leverage the AWS CLI to launch application servers and configure those instances using Chef.

Answer: A
Explanation:

OpsWorks has integrated support for Chef and lifecycle events.

http://docs.aws.amazon.com/opsworks/latest/userguide/workingcookbook.html

QUESTION NO: 39

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

Which task would be best accomplished with a script?

A.
Creating daily EBS snapshots with a monthly rotation of snapshots

B.
Creating daily RDS snapshots with a monthly rotation of snapshots

C.
Automatically detect and stop unused or underutilized EC2 instances

D.
Automatically add Auto Scaled EC2 instances to an Amazon Elastic Load Balancer

Answer: A

Explanation:

QUESTION NO: 40

Your organization's security policy requires that all privileged users either use frequently rotated passwords or one-time access credentials in addition to username/password.

Which two of the following options would allow an organization to enforce this policy for AWS users? (Choose two.)

A.
Configure multi-factor authentication for privileged 1AM users

B.
Create 1AM users for privileged accounts

C.
Implement identity federation between your organization's Identity provider leveraging the 1AM Security Token Service

D.
Enable the 1AM single-use password policy option for privileged users

Answer: A,B

Explanation:

QUESTION NO: 41

What are characteristics of Amazon S3? (Choose two.)

A.
Objects are directly accessible via a URL

B.
S3 should be used to host a relational database

C.
S3 allows you to store objects or virtually unlimited size

D.
S3 allows you to store virtually unlimited amounts of data

E.
S3 offers Provisioned IOPS

Answer: A,D
Explanation:

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

Reference:

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

QUESTION NO: 42

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

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

A.
Multi-AZ RDS

B.
RDS snapshots

C.
RDS read replicas

D.
RDS automated backup

Answer: D
Explanation:

References:

https://aws.amazon.com/rds/details/#ha

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html

QUESTION NO: 43

A media company produces new video files on-premises every day with a total size of around 100 GBS 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/

QUESTION NO: 44

You are running a web-application on AWS consisting of the following components an Elastic Load Balancer (ELB) an Auto-Scaling Group of EC2 instances running Linux/PHP/Apache, and Relational DataBase Service (RDS) MySQL.

Which security measures fall into AWS's responsibility?

A.
Protect the EC2 instances against unsolicited access by enforcing the principle of least-privilege access

B.

Protect against IP spoofing or packet sniffing

C.
Assure all communication between EC2 instances and ELB is encrypted

D.
Install latest security patches on ELB. RDS and EC2 instances

Answer: B
Reference:

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

QUESTION NO: 45

You use S3 to store critical data for your company. Several users within your group currently have lull permissions to your S3 buckets. You need to come up with a solution mat does not impact your users and also protect against the accidental deletion of objects.

Which two options will address this issue? (Choose two.)

A.
Enable versioning on your S3 Buckets

B.
Configure your S3 Buckets with MFA delete

C.
Create a Bucket policy and only allow read only permissions to all users at the bucket level

D.
Enable object life cycle policies and configure the data older than 3 months to be archived in Glacier

Answer: A,B
Explanation:

Versioning allows easy recovery of previous file version.

MFA delete requires additional MFA authentication to delete files.

Won’t impact the users current access.

Reference:

http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html

http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html

QUESTION NO: 46

An organization's security policy requires multiple copies of all critical data to be replicated across at least a primary and backup data center. The organization has decided to store some critical data on Amazon S3.

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

A.
Use the S3 copy API to replicate data between two S3 buckets in different regions

B.
You do not need to implement anything since S3 data is automatically replicated between regions

C.
Use the S3 copy API to replicate data between two S3 buckets in different facilities within an AWS Region

D.
You do not need to implement anything since S3 data is automatically replicated between multiple facilities within an AWS Region

Answer: D
Explanation:

You specify a region when you create your Amazon S3 bucket. Within that region, your objects are redundantly stored on multiple devices across multiple facilities. Please refer to Regional Products and Services for details of Amazon S3 service availability by region.

Reference:

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

QUESTION NO: 47

You are tasked with setting up a cluster of EC2 Instances for a NoSQL database. The database

requires random read I/O disk performance up to a 100,000 IOPS at 4KB block side per node.

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

A.
A High-Memory Quadruple Extra Large (m2.4xlarge) with EBS-Optimized set to true and a PIOPs EBS volume

B.
A Cluster Compute Eight Extra Large (cc2.8xlarge) using instance storage

C.
High I/O Quadruple Extra Large (hi1.4xlarge) using instance storage

D.
A Cluster GPU Quadruple Extra Large (cg1.4xlarge) using four separate 4000 PIOPS EBS volumes in a RAID 0 configuration

Answer: C
Explanation:

The SSD storage is local to the instance. Using PV virtualization, you can expect 120,000 random read IOPS (Input/Output Operations Per Second) and between 10,000 and 85,000 random write IOPS, both with 4K blocks.

For HVM and Windows AMIs, you can expect 90,000 random read IOPS and 9,000 to 75,000 random write IOPS.

Reference:

https://aws.amazon.com/blogs/aws/new-high-io-ec2-instance-type-hi14xlarge/

QUESTION NO: 48

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

A.
Data will be deleted and win no longer be accessible

B.
Data is automatically saved in an EBS volume.

C.
Data is automatically saved as an EBS snapshot

D.
Data is unavailable until the instance is restarted

Answer: A
Explanation:

However, data in the instance store is lost under the following circumstances:

The underlying disk drive fails

The instance stops

The instance terminates

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-lifetime

QUESTION NO: 49

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

Which approach addresses this requirement?

A.
Use cost allocation reports and AWS OpsWorks to deploy and manage your infrastructure.

B.
Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructure.

C.
Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructure.

D.
Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure.

Answer: D
Explanation:

OpsWorks for Chef Automate automatically performs updates for new Chef minor versions.

OpsWorks for Chef Automate does not perform major platform version updates automatically (for example, a major new platform version such as Chef Automate 13) because these updates might include backward-incompatible changes and require additional testing. In these cases, you must manually initiate the update.

Reference: https://aws.amazon.com/opsworks/chefautomate/faqs/

QUESTION NO: 50

You have a server with a 5O0GB Amazon EBS data volume. The volume is 80% full. You need to back up the volume at regular intervals and be able to re-create the volume in a new Availability Zone in the shortest time possible. All applications using the volume can be paused for a period of a few minutes with no discernible user impact.

Which of the following backup methods will best fulfill your requirements?

A.
Take periodic snapshots of the EBS volume

B.
Use a third party Incremental backup application to back up to Amazon Glacier

C.
Periodically back up all data to a single compressed archive and archive to Amazon S3 using a parallelized multi-part upload

D.
Create another EBS volume in the second Availability Zone attach it to the Amazon EC2 instance, and use a disk manager to mirror me two disks

Answer: A
Explanation:

EBS volumes can only be attached to EC2 instances within the same Availability Zone.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-restoring-volume.html

QUESTION NO: 51

Your company Is moving towards tracking web page users with a small tracking

Image loaded on each page Currently you are serving this image out of US-East, but are starting to get concerned about the time it takes to load the image for users on the west coast.

What are the two best ways to speed up serving this image? (Choose two.)

A.
Use Route 53's Latency Based Routing and serve the image out of US-West-2 as well as US-East-1

B.
Serve the image out through CloudFront

C.
Serve the image out of S3 so that it isn't being served oft of your web application tier

D.
Use EBS PIOPs to serve the image faster out of your EC2 instances

Answer: A,B

Explanation:

Cloudfront gets the image closer to the user and Route53 ensures the best connection based on network latency.

QUESTION NO: 52

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

A.
Assign a group or sequential Elastic IP address to the instances

B.
Launch the instances in a Placement Group

C.
Launch the instances in the Amazon virtual Private Cloud (VPC).

D.
Use standard EC2 instances since each instance gets a private Domain Name Service (DNS) already

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

Answer: C
Explanation:

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html

QUESTION NO: 53

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

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

A.
ELB's normal behavior sends requests from the same user to the same backend instance

B.
ELB's behavior when sticky sessions are enabled causes ELB to send requests in the same session to the same backend instance

C.
A faulty browser is not honoring the TTL of the ELB DNS name

D.

The web application uses long polling such as comet or websockets. Thereby keeping a connection open to a web server tor a long time

Answer: B,D

Explanation:

QUESTION NO: 54

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

A.
By using an AAAA record

B.
By using an A record

C.
By using an Amazon Route 53 CNAME record

D.
By using an Amazon Route 53 Alias record

Answer: D

Explanation:

Alias resource record sets are virtual records that work like CNAME records. But they differ from CNAME records in that they are not visible to resolvers. Resolvers only see the A record and the resulting IP address of the target record. As such, unlike CNAME records, alias resource record sets are available to configure a zone apex (also known as a root domain or naked domain) in a dynamic environment.

Reference: http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html

QUESTION NO: 55

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

A.
The organization should create a separate login ID but give the IAM users the same alias so that each one can login with their alias

B.
The organization should create each user in a separate region so that they have their own URL to login

C.
It is not possible to have the same login ID for multiple IAM users of the same account

D.
The organization should create various groups and add each user with the same login ID to different groups. The user can login with their own group ID

Answer: C

Explanation:

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

QUESTION NO: 56

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

A.
AWS S3 with 1 GB of storage

B.
AWS micro instance running 24 hours daily

C.
AWS ELB running 24 hours a day

D.
AWS PIOPS volume of 10 GB size

Answer: D

Explanation:

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

QUESTION NO: 57

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

A.
AWS Simple Notification Service

B.
AWS Simple Workflow

C.
AWS Simple Queue Service

D.
AWS Simple Query Service

Answer: C

Explanation:

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

QUESTION NO: 58

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

A.
Use the IAM groups and add users as per their role to different groups and apply policy to group

B.
The user can create a policy and apply it to multiple users in a single go with the AWS CLI

C.
Add each user to the IAM role as per their organization role to achieve effective policy setup

D.
Use the IAM role and implement access at the role level

Answer: A
Explanation:

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

QUESTION NO: 59

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

A.
Parameters

B.
Outputs

C.
Template version

D.

Resources

Answer: D

Explanation:

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

QUESTION NO: 60

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

A.
Public IP address

B.
Internet gateway

C.
Elastic IP

D.
Private IP address

Answer: C

Explanation:

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

instances to connect to the internet through the Amazon EC2 network edge.

QUESTION NO: 61

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

A.
Notify the Auto Scaling launch config to scale up

B.
Send an SMS using SNS

C.
Notify the Auto Scaling group to scale down

D.
Stop the EC2 instance

Answer: A
Explanation:

Q: What actions can I take from a CloudWatch Alarm?

When you create an alarm, you can configure it to perform one or more automated actions when the metric you chose to monitor exceeds a threshold you define. For example, you can set an alarm that sends you an email, publishes to an SQS queue, stops or terminates an Amazon EC2 instance, or executes an Auto Scaling policy.

Since Amazon CloudWatch alarms are integrated with answer is A.

https://aws.amazon.com/cloudwatch/faqs/

Amazon Simple Notification Service, you can also use any notification type supported by SNS

QUESTION NO: 62

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

A.
Terminate the instances with the ec2-terminate-instance command

B.
Terminate the Auto Scaling instances with the as-terminate-instance command

C.
Set the minimum size and desired capacity to 0

D.
There is no need to change the capacity. Run the as-delete-group command and it will reset all values to 0

Answer: C
Explanation:

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

QUESTION NO: 63

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

A.
Master (Payee. account will get only the total bill and cannot see the cost incurred by each account

B.
Master (Payee. account can view only the AWS billing details of the linked accounts

C.
It is not recommended to use consolidated billing since the payee account will have access to the linked accounts

D.
Each AWS account needs to create an AWS billing policy to provide permission to the payee account

Answer: B

Explanation:

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

QUESTION NO: 64

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

A.
None because the user infrastructure is in the private cloud/

B.
AWS SNS

C.
AWS SES

D.
AWS SMS

Answer: B

Explanation:

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

QUESTION NO: 65

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

A.
Add a new instance manually by 8 AM Thursday and terminate the same by 6 PM Friday

B.
Schedule Auto Scaling to scale up by 8 AM Thursday and scale down after 6 PM on Friday

C.
Schedule a policy which may scale up every day at 8 AM and scales down by 6 PM

D.
Configure a batch process to add an instance by 8 AM and remove it by Friday 6 PM

Answer: B

Explanation:

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

QUESTION NO: 66

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

A.
Run activities on the CPU such that its utilization reaches above 75%

B.
From the AWS console change the state to ‘Alarm’

C.
The user can set the alarm state to ‘Alarm’ using CLI

D.
Run the SNS action manually

Answer: C

Explanation:

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

QUESTION NO: 67

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

A.
Maximum size

B.
Auto Scaling group name

C.
End time

D.
Recurrence value

Answer: A

Explanation:

When you update a stack with an Auto Scaling group and scheduled action, AWS CloudFormation always sets the min size, max size, and desired capacity properties of your Auto Scaling group to the values that are defined in the AWS::AutoScaling::AutoScalingGroup resource of your template, even if a scheduled action is in effect.

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

Reference:

http://docs.aws.amazon.com/es_es/AWSCloudFormation/latest/UserGuide/aws-resource-as-scheduledaction.html

QUESTION NO: 68

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

A.
Create a new alarm of $400 and link it with the first alarm

B.
It is not possible to modify the alarm once it has crossed the usage limit

C.
Update the alarm to set the limit at $400 instead of $200

D.
Create a new alarm for the additional $200 amount

Answer: C
Explanation:

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

QUESTION NO: 69

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

```
"Statement": [{
"Sid": "Stmt1388811069831",
"Effect": "Allow",
"Principal": {"AWS": "*"},
"Action": ["s3:GetObjectAcl", "s3:ListBucket", "s3:GetObject"],
"Resource": ["arn:aws:s3:::cloudacademy/*.jpg"]
}]
```

BrainDumps

A.
It is not possible to define a policy at the object level

B.
It will make all the objects of the bucket cloudacademy as public

C.
It will make the bucket cloudacademy as public

D.
the aws.jpg object as public

Answer: A

Explanation:

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

QUESTION NO: 70

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

A.
Delete the unutilized EBS volumes once the instance is terminated

B.
Delete the AutoScaling launch configuration after the instances are terminated

C.
Release the elastic IP if not required once the instance is terminated

D.

Delete the AWS ELB after the instances are terminated

Answer: B

Explanation:

AWS bills the user on as pay as you go model. AWS will charge the user once the AWS resource is allocated. Even though the user is not using the resource, AWS will charge if it is in service or allocated. Thus, it is advised that once the user's work is completed he should:

Terminate the EC2 instance Delete the EBS volumes Release the unutilized Elastic IPs Delete ELB The AutoScaling launch configuration does not cost the user. Thus, it will not make any difference to the cost whether it is deleted or not.

QUESTION NO: 71

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

A.
Aggregate

B.
Sum

C.
Sample data

D.
Average

Answer: A

Explanation:

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

QUESTION NO: 72

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

A.
AWS Elastic Beanstalk

B.
AWS Cloudfront

C.
AWS Cloudformation

D.
AWS DevOps

Answer: C
Explanation:

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

QUESTION NO: 73

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

A.
Elastic IP

B.
Private IP

C.
Public IP

D.
Internet gateway

Answer: B

Explanation:

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

QUESTION NO: 74

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

A.
Programmatic access

B.
AWS bucket to hold the billing report

C.
AWS billing alerts

D.
Monthly Billing report

Answer: C

Explanation:

AWS provides an option to have programmatic access to billing. Programmatic Billing Access leverages the existing Amazon Simple Storage Service (Amazon S3. APIs. Thus, the user can

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

QUESTION NO: 75

A user has configured the Auto Scaling group with the minimum capacity as 3 and the maximum capacity as 5. When the user configures the AS group, how many instances will Auto Scaling launch?

A.
3

B.
0

C.
5

D.
2

Answer: A
Explanation:

QUESTION NO: 76

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

A.
ELB Access logs

B.
ELB health check

C.
CloudWatch metrics

D.
ELB API calls with CloudTrail

Answer: B

Explanation:

The admin can capture information about Elastic Load Balancer using either:

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

QUESTION NO: 77

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

A.
Cloudformation follows the DevOps model for the creation of Dev & Test

B.
AWS Cloudfromation does not charge the user for its service but only charges for the AWS resources created with it

C.
Cloudformation works with a wide variety of AWS services, such as EC2, EBS, VPC, IAM, S3, RDS, ELB, etc.

D.
CloudFormation provides a set of application bootstrapping scripts which enables the user to install Software

Answer: A

Explanation:

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

provision and manage the AWS resources in an orderly way.

QUESTION NO: 78

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

A.
View the Auto Scaling CPU metrics

B.
Aggregate the data over the instance AMI ID

C.
The user has to use the CloudWatchanalyser to find the average data across instances

D.
It is not possible to see the average CPU utilization of the same AMI ID since the instance ID is different

Answer: A
Explanation:

You can aggregate statistics for the EC2 instances in an Auto Scaling group. Note that Amazon CloudWatch cannot aggregate data across regions. Metrics are completely separate between regions.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GetMetricAutoScalingGroup.html

QUESTION NO: 79

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

A.
Email JSON

B.
HTTP

C.
AWS SQS

D.
AWS SES

Answer: D

Explanation:

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

QUESTION NO: 80

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

A.
It is not possible to setup detailed monitoring for Auto Scaling

B.
In this case, Auto Scaling will send data every minute and will charge the user extra

C.
Detailed monitoring will send data every minute without additional charges

D.
Auto Scaling sends data every minute only and does not charge the user

Answer: B

Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points

to CloudWatch every minute. Auto Scaling includes 7 metrics and 1 dimension, and sends data to CloudWatch every 5 minutes by default. The user can enable detailed monitoring for Auto Scaling, which sends data to CloudWatch every minute. However, this will have some extra-costs.

QUESTION NO: 81

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

A.
AWS SES

B.
AWS Cloudtrail

C.
AWS Cloudwatch

D.
AWS SNS

Answer: D

Explanation:

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

QUESTION NO: 82

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

A.
It is not possible to do this with SQS

B.

You can use sequencing information on each message

C.
You can do this with SQS but you also need to use SWF

D.
Messages will arrive in the same order by default

Answer: B

Explanation:

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

QUESTION NO: 83

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

A.
AWS MFA with EBS

B.
AWS EBS encryption

C.
Multi-tier encryption with Redshift

D.
AWS S3 server side storage

Answer: B

Explanation:

AWS EBS supports encryption of the volume while creating new volumes. It also supports creating volumes from existing snapshots provided the snapshots are created from encrypted volumes. The data at rest, the I/O as well as all the snapshots of EBS will be encrypted. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves

between the EC2 instances and EBS storage. EBS encryption is based on the AES-256 cryptographic algorithm, which is the industry standard

QUESTION NO: 84

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

A.
The user can only disable connection draining from CLI

B.
It is not possible to disable the connection draining feature once enabled

C.
The user can disable the connection draining feature from EC2 -> ELB console or from CLI

D.
The user needs to stop all instances before disabling connection draining

Answer: C
Explanation:

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

QUESTION NO: 85

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

A.
The user needs to use AWS CLI or API to upload the data

B.

The user can use the AWS Import Export facility to import data to CloudWatch

C.
The user will upload data from the AWS console

D.
The user cannot upload data to CloudWatch since it is not an AWS service metric

Answer: A

Explanation:

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

QUESTION NO: 86

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

A.
The folders support only ACL

B.
Both the object and bucket can have an Access Policy but folder cannot have policy

C.
Folders can have a policy

D.
Both the object and bucket can have ACL but folders cannot have ACL

Answer: D

Explanation:

Amazon S3 Access Control Lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify the requester has the necessary access permissions.

Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html

QUESTION NO: 87

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

A.
3

B.
5

C.
2

D.
1

Answer: C
Explanation:

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

QUESTION NO: 88

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

A.
The organization has to create a special password policy and attach it to each user

B.
The root account owner has to use CLI which forces each IAM user to change their password on first login

C.
By default each IAM user can modify their passwords

D.
The root account owner can set the policy from the IAM console under the password policy screen

Answer: D
Explanation:

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

QUESTION NO: 89

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

A.
AWS Glacier

B.
AWS Elastic Transcoder

C.
AWS Simple Notification Service

D.
AWS Simple Queue Service

Answer: D
Explanation:

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

QUESTION NO: 90

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

A.
AWS S3

B.
AWS Glacier

C.
AWS RDS

D.
AWS RRS

Answer: D
Explanation:

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

QUESTION NO: 91

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

A.
It will not allow the user to create the private subnet due to a CIDR overlap

B.
It will allow the user to create a private subnet with CIDR as 20.0.0.128/25

C.
This statement is wrong as AWS does not allow CIDR 20.0.0.0/25

D.
It will not allow the user to create a private subnet due to a wrong CIDR range

Answer: B

Explanation:

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

QUESTION NO: 92

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

A.
The user should select all objects from the console and apply a single policy to mark them public

B.
The user can write a program which programmatically makes all objects public using S3 SDK

C.
Set the AWS bucket policy which marks all objects as public

D.
Make the bucket ACL as public so it will also mark all objects as public

Answer: C

Explanation:

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

QUESTION NO: 93

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

A.
Increase the desired capacity of the Auto Scaling group

B.
Increase the maximum limit of the Auto Scaling group

C.
Launch an instance manually and register it with ELB on the fly

D.
Decrease the minimum limit of the Auto Scaling group

Answer: A
Explanation:

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

QUESTION NO: 94

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

A.
https:// 999988887777.signin.aws.amazon.com/console/

B.
https:// signin.aws.amazon.com/cloudacademy/

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

D.
https:// 999988887777.aws.amazon.com/ cloudacademy/

Answer: A
Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Once the organization has created the IAM users, they will have a separate AWS console URL to login to the AWS console. The console login URL for the IAM user will be https:// AWS_Account_ID.signin.aws.amazon.com/console/. It uses only the AWS account ID and does not depend on the group or user ID.

QUESTION NO: 95

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

A.
600 seconds

B.
3600 seconds

C.
300 seconds

D.
0 seconds

Answer: C

Explanation:

The Elastic Load Balancer connection draining feature causes the load balancer to stop sending new requests to the back-end instances when the instances are deregistering or become unhealthy, while ensuring that inflight requests continue to be served. The user can specify a maximum time (3600 seconds. for the load balancer to keep the connections alive before reporting the instance as deregistered. If the user does not specify the maximum timeout period, by default, the load balancer will close the connections to the deregistering instance after 300 seconds.

QUESTION NO: 96

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

A.
User Access Policy

B.
S3 Object Access Policy

C.
S3 Bucket Access Policy

D.
S3 ACL

Answer: B

Explanation:

Amazon S3 provides a set of operations to work with the Amazon S3 resources. Managing S3 resource access refers to granting others permissions to work with S3. There are three ways the root account owner can define access with S3:

S3 ACL: The user can use ACLs to grant basic read/write permissions to other AWS accounts.

S3 Bucket Policy: The policy is used to grant other AWS accounts or IAM users permissions for the bucket and the objects in it.

User Access Policy: Define an IAM user and assign him the IAM policy which grants him access to S3.

QUESTION NO: 97

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

A.
Enable ELB cross zone load balancing

B.
Enable ELB cookie setup

C.
Enable ELB sticky session

D.
Enable ELB connection draining

Answer: C
Explanation:

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

QUESTION NO: 98

A user has configured ELB with three instances. The user wants to achieve High Availability as well as redundancy with ELB. Which of the below mentioned AWS services helps the user achieve this for ELB?

A.
Route 53

B.
AWS Mechanical Turk

C.
Auto Scaling

D.
AWS EMR

Answer: A

Explanation:

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

QUESTION NO: 99

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

A.
AWS Cost Manager

B.
AWS Cost Explorer

C.
AWS CloudWatch

D.
AWS Consolidated Billing

Answer: B

Explanation:

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

QUESTION NO: 100

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

A.
ELB will ask the user whether to delete the instances or not

B.
Instances will be terminated

C.
ELB cannot be deleted if it has running instances registered with it

D.
Instances will keep running

Answer: D

Explanation:

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

QUESTION NO: 101

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

A.
Backup

B.
Creation

C.
Deletion

D.
Restoration

Answer: A

Explanation:

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

QUESTION NO: 102

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

A.
Create a stack

B.
Configure a service

C.
Create and upload the template

D.
Provide the parameters configured as part of the template

Answer: B
Explanation:

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

QUESTION NO: 103

A user has configured the AWS CloudWatch alarm for estimated usage charges in the US East

region. Which of the below mentioned statements is not true with respect to the estimated charges?

A.
It will store the estimated charges data of the last 14 days

B.
It will include the estimated charges of every AWS service

C.
The metric data will represent the data of all the regions

D.
The metric data will show data specific to that region

Answer: D
Explanation:

When the user has enabled the monitoring of estimated charges for the AWS account with AWS CloudWatch, the estimated charges are calculated and sent several times daily to CloudWatch in the form of metric data. This data will be stored for 14 days. The billing metric data is stored in the US East (Northern Virginia. Region and represents worldwide charges. This data also includes the estimated charges for every service in AWS used by the user, as well as the estimated overall AWS charges.

QUESTION NO: 104

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

A.
RDS will have an internal IP which will redirect all requests to the new DB

B.
RDS uses DNS to switch over to stand by replica for seamless transition

C.
The switch over changes Hardware so RDS does not need to worry about access

D.
RDS will have both the DBs running independently and the user has to manually switch over

Answer: B

Explanation:

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

QUESTION NO: 105

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

A.
AWS RRS

B.
AWS S3

C.
AWS RDS

D.
AWS Glacier

Answer: D

Explanation:

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

QUESTION NO: 106

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

A.
3 hours

B.
4 hours

C.
2 hours

D.
1 hour

Answer: A
Explanation:

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

QUESTION NO: 107

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

A.
The user can enable logging with CloudWatch which logs all the activities

B.
Use CloudTrail to monitor the API calls

C.
Create an IAM user and allow each user to log the data using the S3 bucket

D.
Enable detailed monitoring with CloudWatch

Answer: B

Explanation:

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

QUESTION NO: 108

A user has created a queue named "myqueue" with SQS. There are four messages published to queue which are not received by the consumer yet. If the user tries to delete the queue, what will happen?

A.
A user can never delete a queue manually. AWS deletes it after 30 days of inactivity on queue

B.
It will delete the queue

C.
It will initiate the delete but wait for four days before deleting until all messages are deleted automatically.

D.
It will ask user to delete the messages first

Answer: B

Explanation:

SQS allows the user to move data between distributed components of applications so they can perform different tasks without losing messages or requiring each component to be always available. The user can delete a queue at any time, whether it is empty or not. It is important to note that queues retain messages for a set period of time. By default, a queue retains messages for four days.

QUESTION NO: 109

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

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

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

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

D.
Use the “Launch more like this” option to copy the instance from one region to another

Answer: B
Explanation:

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

QUESTION NO: 110

A user has created numerous EBS volumes. What is the general limit for each AWS account for the maximum number of EBS volumes that can be created?

A.
10000

B.
5000

C.
100

D.
1000

Answer: B

Explanation:

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

QUESTION NO: 111

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

A.
Destination: 20.0.0.0/24 and Target: vgw-12345

B.
Destination: 20.0.0.0/16 and Target: ALL

C.
Destination: 20.0.1.0/16 and Target: vgw-12345

D.
Destination: 0.0.0.0/0 and Target: vgw-12345

Answer: D

Explanation:

The main route table came with the VPC, and it also has a route for the VPN-only subnet. A custom route table is associated with the public subnet. The custom route table has a route over the Internet gateway (the destination is 0.0.0.0/0, and the target is the Internet gateway).

If you create a new subnet in this VPC, it's automatically associated with the main route table, which routes its traffic to the virtual private gateway. If you were to set up the reverse configuration (the main route table with the route to the Internet gateway, and the custom route table with the route to the virtual private gateway), then a new subnet automatically has a route to the Internet gateway.

Reference:

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

QUESTION NO: 112

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

A.
Create an AMI from the volume and share the AMI

B.
Copy the data to an unencrypted volume and then share

C.
Take a snapshot and share the snapshot with a friend

D.
If both the accounts are using the same encryption key then the user can share the volume directly

Answer: B

Explanation:

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

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

QUESTION NO: 113

A user has enabled the Multi AZ feature with the MS SQL RDS database server. Which of the below mentioned statements will help the user understand the Multi AZ feature better?

A.
In a Multi AZ, AWS runs two DBs in parallel and copies the data asynchronously to the replica copy

B.
In a Multi AZ, AWS runs two DBs in parallel and copies the data synchronously to the replica copy

C.
In a Multi AZ, AWS runs just one DB but copies the data synchronously to the standby replica

D.
AWS MS SQL does not support the Multi AZ feature

Answer: C
Explanation:

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

QUESTION NO: 114

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

A.
InstanceName is a reserved tag for AWS. Thus, AWS will not allow this tag

B.
AWS will not allow the tags as the value is the same for different keys

C.
AWS will allow tags but will not show correctly in the cost allocation report due to the same value of the two separate keys

D.

AWS will allow both the tags and show properly in the cost distribution report

Answer: D

Explanation:

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

QUESTION NO: 115

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

A.
The user can use the CloudWatch Import tool

B.
The user should be able to see the data in the console after around 15 minutes

C.
If the user is uploading the custom data, the user must supply the namespace, timezone, and metric name as part of the command

D.
The user can view as well as upload data using the console, CLI and APIs

Answer: B

Explanation:

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

QUESTION NO: 116

A user is launching an EC2 instance in the US East region. Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

A.
Always select the US-East-1-a zone for HA

B.
Do not select the AZ; instead let AWS select the AZ

C.
The user can never select the availability zone while launching an instance

D.
Always select the AZ while launching an instance

Answer: B

Explanation:

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

QUESTION NO: 117

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

A.
Allow Inbound traffic on port 22 from the user's network

B.
The user has to create an instance in EC2 Classic with an elastic IP and configure the security group of a private subnet to allow SSH from that elastic IP

C.
The user can connect to a instance in a private subnet using the NAT instance

D.
Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the Internet

Answer: A
Explanation:

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

QUESTION NO: 118

A user has created an ELB with the availability zone US-East-1.

The user wants to add more zones to ELB to achieve High Availability. How can the user add more zones to the existing ELB?

A.
It is not possible to add more zones to the existing ELB

B.
The only option is to launch instances in different zones and add to ELB

C.
The user should stop the ELB and add zones and instances as required

D.
The user can add zones on the fly from the AWS console

Answer: B
Explanation:

QUESTION NO: 119

A user has configured an Auto Scaling group with ELB. The user has enabled detailed

CloudWatch monitoring on Elastic Load balancing. Which of the below mentioned statements will help the user understand this functionality better?

A.
ELB sends data to CloudWatch every minute only and does not charge the user

B.
ELB will send data every minute and will charge the user extra

C.
ELB is not supported by CloudWatch

D.
It is not possible to setup detailed monitoring for ELB

Answer: A

Explanation:

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

QUESTION NO: 120

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

A.
The client can connect over IPV4 or IPV6 using Dualstack

B.
ELB DNS supports both IPV4 and IPV6

C.
Communication between the load balancer and back-end instances is always through IPV4

D.
The ELB supports either IPV4 or IPV6 but not both

Answer: D

Explanation:

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

QUESTION NO: 121

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

A.
The user can find the data by giving the exact values in the time Tab under CloudWatch metrics

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

C.
It is not possible to find the exact time from the console. The user has to use CLI to provide the specific time

D.
The user can find the data by giving the exact values in the Absolute tab under CloudWatch metrics

Answer: D

Explanation:

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

QUESTION NO: 122

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

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

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

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

D.
Configure CloudWatch to send a notification to the Auto Scaling group when the CPU Utilization is less than 10% and configure the Auto Scaling policy to remove the instance

Answer: D
Explanation:

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

QUESTION NO: 123

A user has enabled detailed CloudWatch metric monitoring on an Auto Scaling group. Which of the below mentioned metrics will help the user identify the total number of instances in an Auto Scaling group including pending, terminating and running instances?

A.
GroupTotalInstances

B.
GroupSumInstances

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

D.
GroupInstancesCount

Answer: A

Explanation:

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

QUESTION NO: 124

A user is trying to configure the CloudWatch billing alarm. Which of the below mentioned steps should be performed by the user for the first time alarm creation in the AWS Account Management section?

A.
Enable Receiving Billing Reports

B.
Enable Receiving Billing Alerts

C.
Enable AWS billing utility

D.
Enable CloudWatch Billing Threshold

Answer: B

Explanation:

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

QUESTION NO: 125

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 time zone so that CloudWatch shows the data only in the local time zone

B.
In the CloudWatch console select the local time zone 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 time zone while uploading the data so that CloudWatch will show the data only in the local time zone

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 time zone under the time range caption in the console because the time range tab allows the user to change the time zone.

QUESTION NO: 126

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

```
"Statement": [
{
"Sid": "AllowUsersAllActionsForCredentials",
"Effect": "Allow",
"Action": [
"iam:*AccessKey*",
],
"Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]
}
]
```

BrainDumps

A.
The policy allows the IAM user to modify all IAM users' access keys using the console, SDK, CLI or APIs

B.
The policy allows the IAM user to modify all IAM users' credentials using the console, SDK, CLI or APIs

C.
The policy allows the IAM user to modify all credentials using only the console

D.
The policy allows the IAM user to modify the IAM user's own credentials using the console, SDK, CLI or APIs

Answer: A

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (Account ID 123412341234. wants some of their users to manage keys (access and secret access keys. of all IAM users, the organization should set the below mentioned policy which entitles the IAM user to modify keys of all IAM users with CLI, SDK or API.

```
"Statement": [
{
"Sid": "AllowUsersAllActionsForCredentials",
"Effect": "Allow",
"Action": [
"iam:*AccessKey*",
],
"Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]
}
]
```

BrainDumps

QUESTION NO: 127

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

A.
The access key to connect to the instance is wrong

B.
The security group is not configured properly

C.
The private key used to launch the instance is not correct

D.
The instance CPU is heavily loaded

Answer: A
Explanation:

If the user is trying to connect to a Linux EC2 instance and receives the connection time out error the probable reasons are:

Security group is not configured with the SSH port

The private key pair is not right

The user name to login is wrong

The instance CPU is heavily loaded, so it does not allow more connections

QUESTION NO: 128

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

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

A.
SSL Protocols

B.
Client Order Preference

C.
SSL Ciphers

D.
Server Order Preference

Answer: B

Explanation:

Elastic Load Balancing uses a Secure Socket Layer (SSL) negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. A security policy is a combination of SSL Protocols, SSL Ciphers, and the Server Order Preference option.

QUESTION NO: 129

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

A.
DiskReadBytes

B.
NetworkIn

C.
NetworkOut

D.
CPUUtilization

Answer: A

Explanation:

CloudWatch is used to monitor AWS as the well custom services. For EC2 when the user is monitoring the EC2 instances, it will capture the 7 Instance level and 3 system check parameters for the EC2 instance. Since this is an EBS backed instance, it will not have ephemeral storage attached to it. Out of the 7 EC2 metrics, the 4 metrics DiskReadOps, DiskWriteOps,

DiskReadBytes and DiskWriteBytes are disk related data and available only when there is ephemeral storage attached to an instance. For an EBS backed instance without any additional device, this data will be 0.

QUESTION NO: 130

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

A.
For restart it does not charge for an extra hour, while every stop/start it will be charged as a separate hour

B.
Every restart is charged by AWS as a separate hour, while multiple start/stop actions during a single hour will be counted as a single hour

C.
For every restart or start/stop it will be charged as a separate hour

D.
For restart it charges extra only once, while for every stop/start it will be charged as a separate hour

Answer: A
Explanation:

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

QUESTION NO: 131

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

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

B.
http://sqs.amazonaws.com/123456789012/myqueue

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

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

Answer: A
Explanation:

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

Reference:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-general-identifiers.html

QUESTION NO: 132

A sys admin is trying to understand the Auto Scaling activities. Which of the below mentioned processes is not performed by Auto Scaling?

A.
Reboot Instance

B.
Schedule Actions

C.
Replace Unhealthy

D.
Availability Zone Balancing

Answer: A
Explanation:

Reboot Instance is not performed by AS. Only termination.

Reference:

http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html

QUESTION NO: 133

A sys admin is trying to understand EBS snapshots. Which of the below mentioned statements will not be useful to the admin to understand the concepts about a snapshot?

A.
The snapshot is synchronous

B.
It is recommended to stop the instance before taking a snapshot for consistent data

C.
The snapshot is incremental

D.
The snapshot captures the data that has been written to the hard disk when the snapshot command was executed

Answer: A
Explanation:

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

QUESTION NO: 134

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

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

B.
The root account owner should create the bucket policy which allows the other account owners to set the object policy of that bucket

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

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

Answer: C
Explanation:

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

QUESTION NO: 135

An organization has setup consolidated billing with 3 different AWS accounts. Which of the below mentioned advantages will organization receive in terms of the AWS pricing?

A.
The consolidated billing does not bring any cost advantage for the organization

B.
All AWS accounts will be charged for S3 storage by combining the total storage of each account

C.
The EC2 instances of each account will receive a total of 750*3 micro instance hours free

D.
The free usage tier for all the 3 accounts will be 3 years and not a single year

Answer: B
Explanation:

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS. accounts within a single organization by making a single paying account. For billing purposes, AWS treats all the accounts on the consolidated bill as one account. Some services, such as Amazon EC2 and Amazon S3 have volume pricing tiers across certain usage dimensions that give the user lower prices when he uses the service more.

QUESTION NO: 136

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

A.
Stop one of the instances and change the availability zone

B.
The zone can only be modified using the AWS CLI

C.
From the AWS EC2 console, select the Actions - > Change zones and specify new zone

D.
Create an AMI of the running instance and launch the instance in a separate AZ

Answer: D
Explanation:

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

QUESTION NO: 137

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

A.
AWS CloudWatch + AWS SES

B.
AWS CloudWatch + AWS SNS

C.
None. It is not possible to configure the light with the AWS infrastructure services

D.
AWS CloudWatch and a dedicated software turning on the light

Answer: B
Explanation:

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

QUESTION NO: 138

An organization has added 3 of his AWS accounts to consolidated billing. One of the AWS accounts has purchased a Reserved Instance (RI. of a small instance size in the US-East-1a zone. All other AWS accounts are running instances of a small size in the same zone. What will happen in this case for the RI pricing?

A.
Only the account that has purchased the RI will get the advantage of RI pricing

B.
One instance of a small size and running in the US-East-1a zone of each AWS account will get the benefit of RI pricing

C.
Any single instance from all the three accounts can get the benefit of AWS RI pricing if they are running in the same zone and are of the same size

D.
If there are more than one instances of a small size running across multiple accounts in the same zone no one will get the benefit of RI

Answer: C
Explanation:

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

QUESTION NO: 139

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

A.
Create 5 separate accounts and make them a part of one consolidate billing

B.
Create 5 separate accounts and use the IAM cross account access with the roles for better management

C.
Create 5 separate IAM users and set a different policy for their access

D.
Create 5 separate IAM groups and add users as per the department’s employees

Answer: A

Explanation:

AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS. accounts within a single organization by making a single paying account. Consolidated billing enables the organization to see a combined view of the AWS charges incurred by each account as well as obtain a detailed cost report for each of the individual AWS accounts associated with the paying account.

QUESTION NO: 140

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

A.
Alarm

B.
OK

C.
Insufficient Data

D.
Error

Answer: B

Explanation:

Amazon CloudWatch alarm watches a single metric over a time period the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The state of the alarm will be OK for the whole day. When the user stops the instance for three periods the alarm may not receive the data

QUESTION NO: 141

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

A.
The user should not use RI; instead only go with the on-demand pricing

B.
The user should use the AWS high utilized RI

C.
The user should use the AWS medium utilized RI

D.
The user should use the AWS low utilized RI

Answer: A

Explanation:

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

QUESTION NO: 142

A user has setup an RDS DB with Oracle. The user wants to get notifications when someone modifies the security group of that DB. How can the user configure that?

A.
It is not possible to get the notifications on a change in the security group

B.
Configure SNS to monitor security group changes

C.
Configure event notification on the DB security group

D.
Configure the CloudWatch alarm on the DB for a change in the security group

Answer: C

Explanation:

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

QUESTION NO: 143

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

A.
Auto Scaling will execute both processes but will add just one instance on the 1st

B.
Auto Scaling will add two instances on the 1st of the month

C.
Auto Scaling will schedule both the processes but execute only one process randomly

D.
Auto Scaling will throw an error since there is a conflict in the schedule of two separate Auto Scaling Processes

Answer: D

Explanation:

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

QUESTION NO: 144

A user is planning to setup infrastructure on AWS for the Christmas sales. The user is planning to use Auto Scaling based on the schedule for proactive scaling. What advice would you give to the user?

A.
It is good to schedule now because if the user forgets later on it will not scale up

B.
The scaling should be setup only one week before Christmas

C.
Wait till end of November before scheduling the activity

D.
It is not advisable to use scheduled based scaling

Answer: C
Explanation:

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

QUESTION NO: 145

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

A.
s3:GetObjectAcl

B.
s3:GetObjectVersion

C.
s3:ListBucketVersions

D.
s3:DeleteObject

Answer: D

Explanation:

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

QUESTION NO: 146

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

A.
ELB sticky session

B.
ELB deregistration check

C.
ELB connection draining

D.
ELB auto registration Off

Answer: C

Explanation:

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

QUESTION NO: 147

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

performed while creating the AMI?

A.
Define the AMI launch permissions

B.
Upload the bundled volume

C.
Register the AMI

D.
Bundle the volume

Answer: A

Explanation:

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

QUESTION NO: 148

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

A.
The user should create a separate IAM user for each employee and provide access to them as per the policy

B.
The user should create an IAM role and attach STS with the role. The user should attach that role to the EC2 instance and setup AWS authentication on that server

C.
The user should create IAM groups as per the organization’s departments and add each user to the group for better access control

D.
Attach an IAM role with the organization’s authentication service to authorize each user for various

AWS services

Answer: D

Explanation:

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

QUESTION NO: 149

A user has configured a VPC with a new subnet. The user has created a security group. The user wants to configure that instances of the same subnet communicate with each other. How can the user configure this with the security group?

A.
There is no need for a security group modification as all the instances can communicate with each other inside the same subnet

B.
Configure the subnet as the source in the security group and allow traffic on all the protocols and ports

C.
Configure the security group itself as the source and allow traffic on all the protocols and ports

D.
The user has to use VPC peering to configure this

Answer: C

Explanation:

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

select all the protocols and ports for that source.

QUESTION NO: 150

A user is launching an instance. He is on the “Tag the instance” screen. Which of the below mentioned information will not help the user understand the functionality of an AWS tag?

A.
Each tag will have a key and value

B.
The user can apply tags to the S3 bucket

C.
The maximum value of the tag key length is 64 unicode characters

D.
AWS tags are used to find the cost distribution of various resources

Answer: C
Explanation:

AWS provides cost allocation tags to categorize and track the AWS costs. When the user applies tags to his AWS resources, AWS generates a cost allocation report as a comma-separated value (CSV file. with the usage and costs aggregated by those tags. Each tag will have a key-value and can be applied to services, such as EC2, S3, RDS, EMR, etc. The maximum size of a tag key is 128 unicode characters.

QUESTION NO: 151

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

QUESTION NO: 152

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

A.
20.0.0.255

B.
20.0.0.132

C.
20.0.0.122

D.
20.0.0.55

Answer: A

Explanation:

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

QUESTION NO: 153

A user has launched an EBS backed EC2 instance. The user has rebooted the instance. Which of the below mentioned statements is not true with respect to the reboot action?

A.
The private and public address remains the same

B.
The Elastic IP remains associated with the instance

C.
The volume is preserved

D.
The instance runs on a new host computer

Answer: D

Explanation:

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

QUESTION NO: 154

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

A.
The user should send only the data of the 60th second as CloudWatch will map the receive data timezone with the sent data timezone

B.
It is not possible to send the custom metric to CloudWatch every minute

C.
Give CloudWatch the Min, Max, Sum, and SampleCount of a number of every minute

D.
Calculate the average of one minute and send the data to CloudWatch

Answer: C
Explanation:

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

QUESTION NO: 155

An AWS root account owner is trying to create a policy to access RDS. Which of the below mentioned statements is true with respect to the above information?

A.
Create a policy, which allows the users to access RDS and apply it to the RDS instances

B.
The user cannot access the RDS database if he is not assigned the correct IAM policy

C.

The root account owner should create a policy for the IAM user and give him access to the RDS services

D.
The policy should be created for the user and provide access for RDS

Answer: C
Explanation:

AWS Identity and Access Management is a web service, which allows organizations to manage users and user permissions for various AWS services. If the account owner wants to create a policy for RDS, the owner has to create an IAM user and define the policy, which entitles the IAM user with various RDS services such as Launch Instance, Manage security group, Manage parameter group etc.

QUESTION NO: 156

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

A.
Schedule the automated back up in non-working hours

B.
Use a large or higher size instance

C.
Use PIOPS

D.
Take a snapshot from standby Replica

Answer: D
Explanation:

An RDS DB instance which has enabled Multi AZ deployments may experience increased write and commit latency compared to a Single AZ deployment, due to synchronous data replication. The user may also face changes in latency if deployment fails over to the standby replica. For production workloads, AWS recommends the user to use provisioned IOPS and DB instance classes (m1.large and larger. as they are optimized for provisioned IOPS to give a fast, and

consistent performance. With Multi AZ feature, the user can not have option to take snapshot from replica.

QUESTION NO: 157

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

A.
It is not possible to show multiple metrics with the different units on the same graph

B.
Add a third Y-axis with the console to show all the data in proportion

C.
Change the axis of Network by using the Switch command from the graph

D.
Change the units of CPU utilization so it can be shown in proportion with Network

Answer: C
Explanation:

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

QUESTION NO: 158

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

A.

Set up programmatic billing access. Download and parse the bill as per the requirement

B.
It is not possible for the user to create his own billing management service with AWS

C.
Enable the AWS CloudWatch alarm which will provide APIs to download the alarm data

D.
Use AWS billing APIs to download the usage report of each service from the AWS billing console

Answer: A
Explanation:

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

QUESTION NO: 159

A user is planning to schedule a backup for an EBS volume. The user wants security of the snapshot data. How can the user achieve data encryption with a snapshot?

A.
Use encrypted EBS volumes so that the snapshot will be encrypted by AWS

B.
While creating a snapshot select the snapshot with encryption

C.
By default, the snapshot is encrypted by AWS

D.
Enable server side encryption for the snapshot using S3

Answer: A
Explanation:

AWS EBS supports encryption of the volume. It also supports creating volumes from existing snapshots provided the snapshots are created from encrypted volumes. The data at rest, the I/O

as well as all the snapshots of the encrypted EBS will also be encrypted. EBS encryption is based on the AES-256 cryptographic algorithm, which is the industry standard.

QUESTION NO: 160

A user has created a public subnet with VPC and launched an EC2 instance within it. The user is trying to delete the subnet. What will happen in this scenario?

A.
It will delete the subnet and make the EC2 instance as a part of the default subnet

B.
It will not allow the user to delete the subnet until the instances are terminated

C.
It will delete the subnet as well as terminate the instances

D.
The subnet can never be deleted independently, but the user has to delete the VPC first

Answer: B
Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When an instance is launched it will have a network interface attached with it. The user cannot delete the subnet until he terminates the instance and deletes the network interface.

QUESTION NO: 161

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

A.
OK

B.
Insufficient Data

C.
Alarm

D.
The EBS cannot be detached until all the alarms are removed

Answer: B

Explanation:

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

QUESTION NO: 162

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

A.
AWS account ID

B.
X.509 certificate and private key

C.
AWS login ID to login to the console

D.
Access key and secret access key

Answer: C

Explanation:

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

AWS account ID;

AWS access and secret access key;

X.509 certificate with private key.

QUESTION NO: 163

A user has configured an SSL listener at ELB as well as on the back-end instances. Which of the below mentioned statements helps the user understand ELB traffic handling with respect to the SSL listener?

A.
It is not possible to have the SSL listener both at ELB and back-end instances

B.
ELB will modify headers to add requestor details

C.
ELB will intercept the request to add the cookie details if sticky session is enabled

D.
ELB will not modify the headers

Answer: D
Explanation:

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

QUESTION NO: 164

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

A.

Cloudformation can never throw an error after launching a few services since it verifies all the steps before launching

B.
It will warn the user about the error and ask the user to manually create RDS

C.
Rollback all the changes and terminate all the created services

D.
It will wait for the user's input about the error and correct the mistake after the input

Answer: C
Explanation:

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

QUESTION NO: 165

A user is trying to launch an EBS backed EC2 instance under free usage. The user wants to achieve encryption of the EBS volume. How can the user encrypt the data at rest?

A.
Use AWS EBS encryption to encrypt the data at rest

B.
The user cannot use EBS encryption and has to encrypt the data manually or using a third party tool

C.
The user has to select the encryption enabled flag while launching the EC2 instance

D.
Encryption of volume is not available as a part of the free usage tier

Answer: B
Explanation:

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

QUESTION NO: 166

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

A.
It will not allow to delete the VPC as it has subnets with route tables

B.
It will not allow to delete the VPC since it has a running route instance

C.
It will terminate the VPC along with all the instances launched by the wizard

D.
It will not allow to delete the VPC since it has a running NAT instance

Answer: D
Explanation:

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

QUESTION NO: 167

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

A.
The user has to parse the file before uploading data to CloudWatch

B.
It is not possible to upload the custom data to CloudWatch

C.
The user can supply the file as an input to the CloudWatch command

D.
The user can use the CloudWatch Import command to import data from the file to CloudWatch

Answer: C
Explanation:

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

QUESTION NO: 168

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 new host computer

Answer: C
Explanation:

A user can always stop/start an EBS backed EC2 instance. When the user stops the instance, it

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

QUESTION NO: 169

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

A.
AWS will not allow to update the DB until the maintenance window is configured

B.
AWS will select the default maintenance window if the user has not provided it

C.
AWS will ask the user to specify the maintenance window during the update

D.
It is not possible to change the DB size from micro to large with RDS

Answer: B
Explanation:

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

QUESTION NO: 170

A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance. The user has 3 elastic IPs and is trying to assign one of the Elastic IPs to the VPC instance from the console. The console does not show any instance in the IP assignment screen. What is a possible reason that

the instance is unavailable in the assigned IP console?

A.
The IP address may be attached to one of the instances

B.
The IP address belongs to a different zone than the subnet zone

C.
The user has not created an internet gateway

D.
The IP addresses belong to EC2 Classic; so they cannot be assigned to VPC

Answer: D

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When the user is launching an instance he needs to select an option which attaches a public IP to the instance. If the user has not selected the option to attach the public IP, then it will only have a private IP when launched. If the user wants to connect to an instance from the Internet, he should create an elastic IP with VPC. If the elastic IP is a part of EC2 Classic, it cannot be assigned to a VPC instance.

QUESTION NO: 171

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 centers, application names, or instance type – Production/Dev. to organize usage costs across multiple services.

QUESTION NO: 172

A user has created a VPC with CIDR 20.0.0.0/16 using VPC Wizard. The user has created a public CIDR (20.0.0.0/24. and a VPN only subnet CIDR (20.0.1.0/24. along with the hardware VPN access to connect to the user's data center. Which of the below mentioned components is not present when the VPC is setup with the wizard?

A.
Main route table attached with a VPN only subnet

B.
A NAT instance configured to allow the VPN subnet instances to connect with the internet

C.
Custom route table attached with a public subnet

D.
An internet gateway for a public subnet

Answer: B

Explanation:

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

QUESTION NO: 173

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 allow by default traffic to the internet gateway

Answer: C
Explanation:

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

QUESTION NO: 174

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

A.
Auto Scaling will keep trying to launch the instance for 72 hours

B.
Auto Scaling will suspend the scaling process

C.
Auto Scaling will start an instance in a separate region

D.
The Auto Scaling group will be terminated automatically

Answer: B
Explanation:

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

QUESTION NO: 175

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

A.
Availability zone outage

B.
A manual failover of the DB instance using Reboot with failover option

C.
Region outage

D.
When the user changes the DB instance’s server type

Answer: C
Explanation:

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

QUESTION NO: 176

An organization has configured Auto Scaling with ELB. One of the instance health check returns the status as Impaired to Auto Scaling. What will Auto Scaling do in this scenario?

A.
Perform a health check until cool down before declaring that the instance has failed

B.
Terminate the instance and launch a new instance

C.
Notify the user using SNS for the failed state

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

Answer: B

Explanation:

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

QUESTION NO: 177

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

A.
It is not possible that the stack creation will wait until one service is created and launched

B.
The user can use the HoldCondition resource to wait for the creation of the other dependent resources

C.
The user can use the DependentCondition resource to hold the creation of the other dependent resources

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

Answer: D

Explanation:

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

QUESTION NO: 178

An organization has configured two single availability zones. The Auto Scaling groups are configured in separate zones. The user wants to merge the groups such that one group spans across multiple zones. How can the user configure this?

A.
Run the command as-join-auto-scaling-group to join the two groups

B.
Run the command as-update-auto-scaling-group to configure one group to span across zones and delete the other group

C.
Run the command as-copy-auto-scaling-group to join the two groups

D.
Run the command as-merge-auto-scaling-group to merge the groups

Answer: B

Explanation:

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

QUESTION NO: 179

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

A.
The payee account has to request AWS support to link the other accounts with his account

B.
The owner of the linked account should add the payee account to his master account list from the billing console

C.
The payee account will send a request to the linked account to be a part of consolidated billing

D.
The owner of the linked account requests the payee account to add his account to consolidated billing

Answer: C
Explanation:

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

QUESTION NO: 180

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

```
"Statement": [{
"Sid": "Stmt1388811069831",
"Effect": "Allow",
"Principal": {"AWS": "*"},
"Action": ["s3:GetObjectAcl", "s3:ListBucket"],
"Resource": ["arn:aws:s3:::cloudacademy]
}]
```

BrainDumps

A.
It will make the cloudacademy bucket as well as all its objects as public

B.
It will allow everyone to view the ACL of the bucket

C.
It will give an error as no object is defined as part of the policy while the action defines the rule about the object

D.
It will make the cloudacademy bucket as public

Answer: C
Explanation:

Tested and got an error while saving the above S3 bucket policy:" Action does not apply to any resource(s) in statement – Action "s3:GetObject" in Statement "Stmt123456788" "

QUESTION NO: 181

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.
Create an AMI of the running instance and launch the instance in a separate AZ

C.
Stop one of the instances and change the availability zone

D.
From the AWS EC2 console, select the Actions - > Change zones and specify the new zone

Answer: B

Explanation:

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

QUESTION NO: 182

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

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

BrainDumps

A.
The IAM policy will throw an error due to an invalid resource name

B.
The IAM policy will allow the user to subscribe to any IAM group

C.
Allow the IAM user to update the membership of the group called TestingGroup

D.
Allow the IAM user to delete the TestingGroup

Answer: C

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (account ID

123412341234) wants their users to manage their subscription to the groups, they should create a relevant policy for that. The below mentioned policy allows the respective IAM user to update the membership of the group called MarketingGroup.

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

BrainDumps

QUESTION NO: 183

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

A.
There is no way to register the stopped instances with ELB

B.
The user cannot stop the instances if they are registered with ELB

C.
If the instances have the same Elastic IP assigned after reboot they will be registered with ELB

D.
The instances will automatically get registered with ELB

Answer: D
Reference:

https://aws.amazon.com/about-aws/whats-new/2015/12/support-for-automatic-re-registration-of-ec2-back-end-instances-when-stopped-and-restarted/

QUESTION NO: 184

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

A.
The user has provided the wrong user name for the OS login

B.
The instance CPU is heavily loaded

C.
The security group is not configured properly

D.
The access key to connect to the instance is wrong

Answer: A
Explanation:

If the user is trying to connect to a Linux EC2 instance and receives the Host Key not found error the probable reasons are:

The private key pair is not right

The user name to login is wrong

QUESTION NO: 185

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

A.
5 minutes

B.
1 hour

C.
30 minutes

D.
2 hours

Answer: B
Explanation:

When you enable connection draining, you can specify a maximum time for the load balancer to keep connections alive before reporting the instance as de-registered. The maximum timeout value can be set between 1 and 3,600 seconds (the default is 300 seconds). When the maximum time limit is reached, the load balancer forcibly closes connections to the de-registering instance.

Reference:

http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/config-conn-drain.html

QUESTION NO: 186

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

A.
AWS CloudWatch + Cloudformation

B.
AWS CloudWatch + AWS AutoScaling + AWS ELB

C.
AWS CloudWatch + AWS VPC

D.
AWS CloudWatch + AWS SNS

Answer: D
Explanation:

Amazon SNS can deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS) queues or to any HTTP endpoint. The user can configure a web service (HTTP End point) in his data center which receives data and launches an instance in the private cloud. The user should configure the CloudWatch alarm to send a notification to SNS when the "StatusCheckFailed" metric is true for the EC2 instance. The SNS topic can be configured to send

a notification to the user's HTTP endpoint which launches an instance in the private cloud.

QUESTION NO: 187

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

A.
Load Balancer IP

B.
EC2 instance IP

C.
S3 bucket name

D.
Random string

Answer: B

Explanation:

Elastic Load Balancing access logs capture detailed information for all the requests made to the load balancer. Elastic Load Balancing publishes a log file from each load balancer node at the interval that the user has specified. The load balancer can deliver multiple logs for the same period. Elastic Load Balancing creates log file names in the following format:

"{Bucket}/{Prefix}/AWSLogs/{AWS AccountID}/elasticloadbalancing/{Region}/{Year}/{Month}/{Day}/{AWS

Account ID}_elasticloadbalancing_{Region}_{Load Balancer Name}_{End Time}_{Load Balancer IP}_{Random

String}.log"

QUESTION NO: 188

A user has created a queue named "awsmodule" with SQS. One of the consumers of queue is

down for 3 days and then becomes available. Will that component receive message from queue?

A.
Yes, since SQS by default stores message for 4 days

B.
No, since SQS by default stores message for 1 day only

C.
No, since SQS sends message to consumers who are available that time

D.
Yes, since SQS will not delete message until it is delivered to all consumers

Answer: A

Explanation:

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

QUESTION NO: 189

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

A.
Create an IAM policy with the security group and use that security group for AWS console login

B.
Create an IAM policy with a condition which denies access when the IP address range is not from the organization

C.
Configure the EC2 instance security group which allows traffic only from the organization’s IP range

D.
Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

Answer: B

Explanation:

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

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

BrainDumps

QUESTION NO: 190

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

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

BrainDumps

A.
The policy will allow the user to perform all read only activities on the EC2 services

B.
The policy will allow the user to list all the EC2 resources except EBS

C.
The policy will allow the user to perform all read and write activities on the EC2 services

D.
The policy will allow the user to perform all read only activities on the EC2 services except load

Balancing

Answer: D

Explanation:

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

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

BrainDumps

QUESTION NO: 191

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

A.
The response will have a cookie but stickiness will be deleted

B.
The session will not be sticky until a new cookie is inserted

C.
ELB will throw an error due to cookie unavailability

D.
The session will be sticky and ELB will route requests to another server as ELB keeps replicating the Cookie

Answer: B

Explanation:

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

QUESTION NO: 192

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

A.
The user can zoom a particular period by selecting that period with the mouse and then releasing the mouse

B.
The user can zoom a particular period by double clicking on that period with the mouse

C.
The user can zoom a particular period by specifying the aggregation data for that period

D.
The user can zoom a particular period by specifying the period in the Time Range

Answer: A
Explanation:

QUESTION NO: 193

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

A.

It will fetch the data at every minute but the four data points [corresponding to 4 minutes] will not have value since the EC2 basic monitoring metrics are collected every five minutes

B.
It will fetch the data at every minute as detailed monitoring on EC2 will be enabled by the default launch configuration of Auto Scaling

C.
The alarm creation will fail since the user has not enabled detailed monitoring on the EC2 instances

D.
The user has to first enable detailed monitoring on the EC2 instances to support alarm monitoring at every minute

Answer: B

Explanation:

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

QUESTION NO: 194

A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is not true in this scenario?

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

B.
The VPC will create two subnets

C.
The VPC will create one internet gateway and attach it to VPC

D.
The VPC will launch one NAT instance with an elastic IP

Answer: A

Explanation:

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

QUESTION NO: 195

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

A.
If the end user is requesting behind a proxy server then the user should not enable a proxy protocol on ELB

B.
ELB does not support a proxy protocol when it is listening on both the load balancer and the back-end instances

C.
Whether the end user is requesting from a proxy server or directly, it does not make a difference for the proxy protocol

D.
If the end user is requesting behind the proxy, then the user should add the “isproxy” flag to the ELB Configuration

Answer: A

Explanation:

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

another header to the request which already has a header from the proxy server. This duplication may result in errors.

QUESTION NO: 196

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

A.
The user has to request AWS to increase the number of elastic IPs associated with the account

B.
AWS allows 10 EC2 Classic IPs per region; so it will allow to allocate new Elastic IPs to the same region

C.
The AWS will not allow to create a new elastic IP in VPC; it will throw an error

D.
The user can allocate a new IP address in VPC as it has a different limit than EC2

Answer: D

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. A user can have 5 IP addresses per region with EC2 Classic. The user can have 5 separate IPs with VPC in the same region as it has a separate limit than EC2 Classic.

QUESTION NO: 197

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

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

B.
The user can directly attach an elastic IP to the instance

C.
The instance will never launch if the public IP is not assigned

D.
The user would need to create an Internet gateway and then attach an elastic IP to the instance to connect from internet

Answer: D

Explanation:

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

QUESTION NO: 198

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": "*"
}
]
}
```

BrainDumps

A.
The policy is not created correctly. It will throw an error for wrong resource name

B.
The policy is for the group. Thus, the IAM user cannot have any entitlement to this

C.
It allows full access to all AWS services for the IAM users who are a part of this group

D.
If this policy is applied to the EC2 resource, the users of the group will have full access to the EC2 Resources

Answer: C
Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The IAM group allows the organization to specify permissions for a collection of users. With the below mentioned policy, it will allow the group full access (Admin to all AWS services).

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
]
}
```

BrainDumps

QUESTION NO: 199

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

A.
Setup the notification when the CPU is more than 75% on RDS

B.
Setup the notification when the state is Insufficient Data

C.
Setup the notification when the CPU utilization is less than 10%

D.
It is not possible to setup the alarm on RDS

Answer: B
Explanation:

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

QUESTION NO: 200

George has shared an EC2 AMI created in the US East region from his AWS account with Stefano. George copies the same AMI to the US West region. Can Stefano access the copied AMI of George's account from the US West region?

A.
No, copy AMI does not copy the permission

B.
It is not possible to share the AMI with a specific account

C.
Yes, since copy AMI copies all private account sharing permissions

D.
Yes, since copy AMI copies all the permissions attached with the AMI

Answer: A
Explanation:

Within EC2, when the user copies an AMI, the new AMI is fully independent of the source AMI; there is no link to the original (source. AMI. AWS does not copy launch the permissions, user-defined tags or the Amazon S3 bucket permissions from the source AMI to the new AMI. Thus, in this case by default Stefano will not have access to the AMI in the US West region.

QUESTION NO: 201

A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance. The

Internet gateway has also been created. What can be the reason for the error?

A.
The internet gateway is not configured with the route table

B.
The private IP is not present

C.
The outbound traffic on the security group is disabled

D.
The internet gateway is not configured with the security group

Answer: A

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. AWS provides two features the user can use to increase security in VPC: security groups and network ACLs. Security groups work at the instance level. When a user launches an instance and wants to connect to an instance, he needs an internet gateway. The Internet gateway should be configured with the route table to allow traffic from the Internet.

QUESTION NO: 202

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

A.
ELBSecurity Policy-2014-01

B.
ELBSecurity Policy-2011-08

C.
ELBDefault Negotiation Policy

D.
ELBSample- OpenSSLDefault Cipher Policy

Answer: A

Explanation:

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

QUESTION NO: 203

A user has configured ELB with Auto Scaling. The user suspended the Auto Scaling AlarmNotification which notifies Auto Scaling for CloudWatch alarms. process for a while. What will Auto Scaling do during this period?

A.
AWS will not receive the alarms from CloudWatch

B.
AWS will receive the alarms but will not execute the Auto Scaling policy

C.
Auto Scaling will execute the policy but it will not launch the instances until the process is resumed

D.
It is not possible to suspend the AlarmNotification process

Answer: B
Explanation:

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

QUESTION NO: 204

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

A.
The instances of George and Ray will be running in the same data center

B.
All the instances of George and Ray can communicate over a private IP with a minimal cost

C.
All the instances of George and Ray can communicate over a private IP without any cost

D.
The US-East-1a region of George and Ray can be different availability zones

Answer: D

Explanation:

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

QUESTION NO: 205

A user had aggregated the CloudWatch metric data on the AMI ID. The user observed some abnormal behavior of the CPU utilization metric while viewing the last 2 weeks of data. The user wants to share that data with his manager. How can the user achieve this easily with the AWS console?

A.
The user can use the copy URL functionality of CloudWatch to share the exact details

B.
The user can use the export data option from the CloudWatch console to export the current data point

C.

The user has to find the period and data and provide all the aggregation information to the manager

D.
The user can use the CloudWatch data copy functionality to copy the current data points

Answer: A

Explanation:

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

QUESTION NO: 206

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

A.
Remove the alarm

B.
Disable the alarm for a while using CLI

C.
Modify the CPU utilization by removing the email alert

D.
Disable the alarm for a while using the console

Answer: B

Explanation:

Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. When the user has setup an alarm and it is known that for some unavoidable event the status may change to Alarm, the user can disable the alarm using the

DisableAlarmActions API or from the command line mon-disable-alarm-actions.

QUESTION NO: 207

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

A.
TLS 1.3

B.
TLS 1.2

C.
SSL 2.0

D.
SSL 3.0

Answer: A
Explanation:

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

TLS 1.2

TLS 1.1

TLS 1.0

SSL 3.0

SSL 2.0

QUESTION NO: 208

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

A.
Allow Inbound on port 3306 for Source Web Server Security Group (WebSecGrp)

B.
Allow Inbound on port 3306 from source 20.0.0.0/16

C.
Allow Outbound on port 3306 for Destination Web Server Security Group (WebSecGrp)

D.
Allow Outbound on port 80 for Destination NAT Instance IP

Answer: A
Explanation:

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

QUESTION NO: 209

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created public and VPN only subnets along with hardware VPN access to connect to the user's data center. The user has not yet launched any instance as well as modified or deleted any setup. He wants to delete this VPC from the console. Will the console allow the user to delete the VPC?

A.
Yes, the console will delete all the setups and also delete the virtual private gateway

B.
No, the console will ask the user to manually detach the virtual private gateway first and then allow deleting the VPC

C.
Yes, the console will delete all the setups and detach the virtual private gateway

D.
No, since the NAT instance is running

Answer: C
Explanation:

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

QUESTION NO: 210

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

A.
The ratio between IOPS and the EBS volume is higher than 30

B.
The maximum IOPS supported by EBS is 3000

C.
The ratio between IOPS and the EBS volume is lower than 50

D.
PIOPS is supported for EBS higher than 500 GB size

Answer: A
Explanation:

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

QUESTION NO: 211

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

A.
The user can get the aggregate data of the numbers generated over a minute and send it to CloudWatch

B.
The user has to supply the time zone with each data point

C.
CloudWatch will not truncate the number until it has an exponent larger than 126 (i.e. (1 x 10^126))

D.
The user can create a file in the JSON format with the metric name and value and supply it to CloudWatch

Answer: B
Explanation:

QUESTION NO: 212

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 behavior is set to Stop

B.
It is not possible to set the termination behavior 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 behavior to “Stop”. It gives a warning that the instance does not have the EBS root volume.

QUESTION NO: 213

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

A.
The user should use the same encryption key for all versions of the same object

B.
It is possible to have different encryption keys for different versions of the same object

C.
AWS S3 does not allow the user to upload his own keys for server side encryption

D.
The SSE-C does not work when versioning is enabled

Answer: B

Explanation:

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

QUESTION NO: 214

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

A.
The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range

B.
It is not possible to create a subnet with the same CIDR as VPC

C.
The second subnet will be created

D.
It will throw a CIDR overlaps error

Answer: D
Explanation:

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

QUESTION NO: 215

A user has launched an RDS MySQL DB with the Multi AZ feature. The user has scheduled the scaling of instance storage during maintenance window. What is the correct order of events during maintenance window?

Perform maintenance on standby

Promote standby to primary

Perform maintenance on original primary

Promote original master back as primary

A.
1, 2, 3, 4

B.
1, 2, 3

C.
2, 3, 1, 4

Answer: B
Explanation:

Running MySQL on the RDS DB instance as a Multi-AZ deployment can help the user reduce the impact of a maintenance event, as the Amazon will conduct maintenance by following the steps in the below mentioned order:

QUESTION NO: 216

A sys admin is using server side encryption with AWS S3. Which of the below mentioned statements helps the user understand the S3 encryption functionality?

A.
The server side encryption with the user supplied key works when versioning is enabled

B.
The user can use the AWS console, SDK and APIs to encrypt or decrypt the content for server side encryption with the user supplied key

C.
The user must send an AES-128 encrypted key

D.
The user can upload his own encryption key to the S3 console

Answer: A
Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key. The encryption with the user supplied key (SSE-C. does not work with the AWS console. The S3 does not store the keys and the user has to send a key with each request. The SSE-C works when the user has enabled versioning.

QUESTION NO: 217

A root account owner is trying to understand the S3 bucket ACL. Which of the below mentioned options cannot be used to grant ACL on the object using the authorized predefined group?

A.
Authenticated user group

B.
All users group

C.
Log Delivery Group

D.
Canonical user group

Answer: D
Explanation:

An S3 bucket ACL grantee can be an AWS account or one of the predefined Amazon S3 groups. Amazon S3 has a set of predefined groups. When granting account access to a group, the user can specify one of the URLs of that group instead of a canonical user ID. AWS S3 has the following predefined groups:

Authenticated Users group: It represents all AWS accounts. All Users group: Access permission to this group allows anyone to access the resource. Log Delivery group: WRITE permission on a bucket enables this group to write server access logs to the bucket.

QUESTION NO: 218

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user's data center. The user's data center has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-123456) to allow traffic to the internet from the VPN subnet. Which of the below mentioned options is not a valid entry for the main route table in this scenario?

A.

Destination: 20.0.1.0/24 and Target: i-12345

B.
Destination: 0.0.0.0/0 and Target: i-12345

C.
Destination: 172.28.0.0/12 and Target: vgw-12345

D.
Destination: 20.0.0.0/16 and Target: local

Answer: A
Explanation:

The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data center, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data center. When the user has configured this setup with Wizard, it will create a virtual private gateway to route all traffic of the VPN subnet. If the user has setup a NAT instance to route all the Internet requests, then all requests to the internet should be routed to it. All requests to the organization's DC will be routed to the VPN gateway.

Here are the valid entries for the main route table in this scenario:

Destination: 0.0.0.0/0 & Target: i-12345 (To route all internet traffic to the NAT Instance.

Destination: 172.28.0.0/12 & Target: vgw-12345 (To route all the organization's data center traffic to the VPN gateway).

Destination: 20.0.0.0/16 & Target: local (To allow local routing in VPC).

QUESTION NO: 219

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

A.
Destination: 0.0.0.0/0 and Target: i-a12345

B.
Destination: 20.0.0.0/0 and Target: 80

C.
Destination: 20.0.0.0/0 and Target: i-a12345

D.
Destination: 20.0.0.0/24 and Target: i-a12345

Answer: A
Explanation:

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

QUESTION NO: 220

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

A.
He can just view the content of the bucket

B.
He can do all the operations on the bucket

C.
It is not possible to give access to an IAM user using ACL

D.
The IAM user can perform all operations on the bucket using only API/SDK

Answer: C
Explanation:

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

QUESTION NO: 221

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

A.
Stop the scaling process until research is completed

B.
It is not possible to find the root cause from that instance without triggering scaling

C.
Delete Auto Scaling until research is completed

D.
Suspend the scaling process until research is completed

Answer: D
Explanation:

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

QUESTION NO: 222

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

A.
DB security group

B.
DB snapshot

C.

DB options group

D.
DB parameter group

Answer: C
Explanation:

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

QUESTION NO: 223

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

A.
The user account has reached the maximum EC2 instance limit

B.
The snapshot is corrupt

C.
The AMI is missing. It is the required part

D.
The user account has reached the maximum volume limit

Answer: A
Explanation:

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

QUESTION NO: 224

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

A.
AWS EMR

B.
AWS RDS

C.
AWS ELB

D.
AWS Route53

Answer: A

Explanation:

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

QUESTION NO: 225

A user is measuring the CPU utilization of a private data center machine every minute. The machine provides the aggregate of data every hour, such as Sum of data", "Min value", "Max value, and "Number of Data points".

The user wants to send these values to CloudWatch. How can the user achieve this?

A.
Send the data using the put-metric-data command with the aggregate-values parameter

B.
Send the data using the put-metric-data command with the average-values parameter

C.
Send the data using the put-metric-data command with the statistic-values parameter

D.
Send the data using the put-metric-data command with the aggregate –data parameter

Answer: C
Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user can publish the data to CloudWatch as single data points or as an aggregated set of data points called a statistic set using the command put-metric-data. When sending the aggregate data, the user needs to send it with the parameter statistic-values:

```
awscloudwatch put-metric-data--metric-name <Name>--namespace
<Custom namespace>--timestamp
<UTC Format>--statistic-values
Sum=XX,Minimum=YY,Maximum=AA,SampleCount=BB--unit Milliseconds
```

QUESTION NO: 226

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

A.
SNS will send data every minute after configuration

B.
There is no need to enable since SNS provides data every minute

C.
AWS CloudWatch does not support monitoring for SNS

D.
SNS cannot provide data every minute

Answer: D
Explanation:

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

QUESTION NO: 227

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 center has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data center, what will happen?

A.
It will allow traffic communication on both the CIDRs of the data center

B.
It will not allow traffic with data center 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 center CIDRs

D.
It will allow traffic with data center 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 center. If the user has an IP address prefix in the VPC that overlaps with one of the networks' prefixes, any traffic to the network's prefix is dropped. In this case CIDR 20.0.54.0/24 falls in the VPC's CIDR range of 20.0.0.0/16. Thus, it will not allow traffic on that IP. In the case of 20.1.0.0/24, it does not fall in the VPC's CIDR range. Thus, traffic will be allowed on it.

QUESTION NO: 228

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

A.
It is not possible to get the log files for MySQL RDS

B.
Find all the transaction logs and query on those records

C.
Direct the logs to the DB table and then query that table

D.
Download the log file to DynamoDB and search for the record

Answer: C

Explanation:

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

QUESTION NO: 229

A user is trying to send custom metrics to CloudWatch using the PutMetricData APIs. Which of the below mentioned points should the user needs to take care while sending the data to CloudWatch?

A.
The size of a request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests

B.
The size of a request is limited to 128KB for HTTP GET requests and 64KB for HTTP POST requests

C.
The size of a request is limited to 40KB for HTTP GET requests and 8KB for HTTP POST requests

D.
The size of a request is limited to 16KB for HTTP GET requests and 80KB for HTTP POST requests

Answer: A

Explanation:

With AWS CloudWatch, the user can publish data points for a metric that share not only the same time stamp, but also the same namespace and dimensions. CloudWatch can accept multiple data

points in the same PutMetricData call with the same time stamp. The only thing that the user needs to take care of is that the size of a PutMetricData request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests.

QUESTION NO: 230

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

A.
It is not possible to stop the instance using the CloudWatch alarm

B.
CloudWatch will stop the instance when the action is executed

C.
The user cannot set an alarm on EC2 since he does not have the permission

D.
The user can setup the action but it will not be executed if the user does not have EC2 rights

Answer: D
Explanation:

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

QUESTION NO: 231

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

A.
Auto Scaling will not launch or terminate any instances

B.
Auto Scaling will allow the instances to grow more than the maximum size

C.
Auto Scaling will keep launching instances till the maximum instance size

D.
It is not possible to suspend the terminate process while keeping the launch active

Answer: B
Explanation:

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

QUESTION NO: 232

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

A.
The user should create a separate IAM user for each mobile application and provide DynamoDB access with it

B.
The user should create an IAM role with DynamoDB and EC2 access. Attach the role with EC2 and route all calls from the mobile through EC2

C.
The application should use an IAM role with web identity federation which validates calls to DynamoDB with identity providers, such as Google, Amazon, and Facebook

D.
Create an IAM Role with DynamoDB access and attach it with the mobile application

Answer: C
Explanation:

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

QUESTION NO: 233

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

A.
My SQL

B.
Oracle

C.
MS SQL

D.
PostgreSQL

Answer: C
Explanation:

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

QUESTION NO: 234

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

A.
Change the Disable button for notification to “Yes” in the RDS console

B.
Set the send mail flag to false in the DB event notification console

C.
The only option is to delete the notification from the console

D.
Change the Enable button for notification to “No” in the RDS console

Answer: D
Explanation:

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

QUESTION NO: 235

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

A.
There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet’s CIDR

B.
The user can modify the first subnet CIDR from the console

C.
It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created

D.
The user can modify the first subnet CIDR with AWS CLI

Answer: C
Explanation:

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

QUESTION NO: 236

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

A.
Configure Destination as DB Security group ID (DbSecGrp) for port 3306 Outbound

B.
80 for Destination 0.0.0.0/0 Outbound

C.
Configure port 3306 for source 20.0.0.0/24 InBound

D.
Configure port 80 InBound for source 20.0.0.0/16

Answer: A
Explanation:

A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the public subnet can receive inbound traffic directly from the internet. Thus, the user should configure port 80 with source 0.0.0.0/0 in InBound. The user should configure that the instance in the public subnet can send traffic to the private subnet instances on the DB port. Thus, the user should configure the DB security group of the private subnet (DbSecGrp) as the destination for port 3306 in Outbound.

QUESTION NO: 237

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

A.
AWS Auto Scaling

B.
AWS Route 53

C.
AWS EMR

D.
AWS SNS

Answer: B
Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, ELB, OpsWorks, and Route 53 can provide the monitoring data every minute without charging the user.

QUESTION NO: 238

A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the

user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?

A.
AWS/StorageGateway

B.
AWS/CloudTrail

C.
AWS/ElastiCache

D.
AWS/SWF

Answer: B

Explanation:

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

QUESTION NO: 239

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

A.
x-amz-server-side-encryption-customer-key-AES-256

B.
x-amz-server-side-encryption-customer-key

C.
x-amz-server-side-encryption-customer-algorithm

D.
x-amz-server-side-encryption-customer-key-MD5

Answer: A
Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along with each API call to supply his own encryption key (SSE-C). When the user is supplying his own encryption key, the user has to send the below mentioned parameters as a part of the API calls:

x-amz-server-side-encryption-customer-algorithm: Specifies the encryption algorithm

x-amz-server-side-encryption-customer-key: To provide the base64-encoded encryption key

x-amz-server-side-encryption-customer-key-MD5: To provide the base64-encoded 128-bit MD5 digest of the encryption key

QUESTION NO: 240

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.

QUESTION NO: 241

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

A.
as-delete-instance-in-auto-scaling-group <Instance ID> --no-decrement-desired-capacity

B.
as-terminate-instance-in-auto-scaling-group <Instance ID> --update-desired-capacity

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

D.
as-terminate-instance-in-auto-scaling-group <Instance ID> --no-decrement-desired-capacity

Answer: D
Explanation:

The Auto Scaling command as-terminate-instance-in-auto-scaling-group <Instance ID> will terminate the specific instance ID. The user is required to specify the parameter as –no-decrement-desired-capacity to ensure that it launches a new instance from the launch config after terminating the instance. If the user specifies the parameter --decrement-desired-capacity, then Auto Scaling will terminate the instance and decrease the desired capacity by 1.

QUESTION NO: 242

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

A.
All the data will be erased but the ephemeral storage will stay connected

B.
All data will be erased and the ephemeral storage is released

C.
It is not possible to restart an instance launched from an instance store backed AMI

D.
The data is preserved

Answer: D

Explanation:

A user can reboot an EC2 instance using the AWS console, the Amazon EC2 CLI or the Amazon EC2 API. Rebooting an instance is equivalent to rebooting an operating system. However, it is recommended that the user use Amazon EC2 to reboot the instance instead of running the operating system reboot command from the instance. When an instance launched from an instance store backed AMI is rebooted all the ephemeral storage data is still preserved.

QUESTION NO: 243

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: B

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”.

Reference:

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

QUESTION NO: 244

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

A.
The user can delete all the instances of the subnet. Change the size of the subnets to 20.0.0.0/32 and 20.0.1.0/32, respectively. Then the user can increase the size of the VPC using CLI

B.
It is not possible to change the size of the VPC once it has been created

C.
The user can add a subnet with a higher range so that it will automatically increase the size of the VPC

D.
The user can delete the subnets first and then modify the size of the VPC

Answer: B

Explanation:

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

QUESTION NO: 245

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

A.
Dynamic Security Policy

B.
All the other options

C.
Predefined Security Policy

D.
Default Security Policy

Answer: C
Explanation:

Elastic Load Balancing uses a Secure Socket Layer (SSL. negotiation configuration which is known as a Security Policy. It is used to negotiate the SSL connections between a client and the load balancer. ELB supports two policies:

Predefined Security Policy, which comes with predefined cipher and SSL protocols;

Custom Security Policy, which allows the user to configure a policy.

QUESTION NO: 246

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

A.
IAM User ID

B.
S3 Secure ID

C.
Access ID

D.

Canonical user ID

Answer: D

Explanation:

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

QUESTION NO: 247

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

A.
HTTPCode_Backend_3XX

B.
HTTPCode_Backend_4XX

C.
HTTPCode_Backend_2XX

D.
HTTPCode_Backend_5XX

Answer: D

Explanation:

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

The 2XX class status codes represents successful actions

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

The 4XX class status code represents client errors

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

QUESTION NO: 248

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

A.
The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copying. Thus, the copied AMI will have all the updated data

B.
The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI

C.
It is not possible to copy the instance store backed AMI from one region to another

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

Answer: D
Explanation:

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

QUESTION NO: 249

A user runs the command “dd if=/dev/zero of=/dev/xvdfbs=1M” on a fresh blank EBS volume attached to a Linux instance. Which of the below mentioned activities is the user performing with the command given above?

A.
Creating a file system on the EBS volume

B.
Mounting the device to the instance

C.
Pre warming the EBS volume

D.
Formatting the EBS volume

Answer: C
Explanation:

When the user creates a new EBS volume and is trying to access it for the first time it will encounter reduced IOPS due to wiping or initiating of the block storage. To avoid this as well as achieve the best performance it is required to pre warm the EBS volume. For a blank volume attached with a Linux OS, the “dd” command is used to write to all the blocks on the device. In the command “dd if=/dev/zero of=/dev/xvdfbs=1M” the parameter “if =import file” should be set to one of the Linux virtual devices, such as /dev/zero. The “of=output file” parameter should be set to the drive that the user wishes to warm. The “bs” parameter sets the block size of the write operation; for optimal performance, this should be set to 1 MB.

QUESTION NO: 250

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

A.
When the user sets an alarm on the Auto Scaling group, it automatically enables detail monitoring

B.
By default detailed monitoring is enabled for Auto Scaling

C.
Auto Scaling does not support detailed monitoring

D.

Enable detail monitoring from the AWS console

Answer: B

Explanation:

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

QUESTION NO: 251

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

A.
The user cannot delete the VPC since the subnet is not deleted

B.
All network interface attached with the instances will be deleted

C.
When the user launches a new instance it cannot use the same subnet

D.
The subnet to which the instances were launched with will be deleted

Answer: B

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When an instance is launched it will have a network interface attached with it. The user cannot delete the subnet until he terminates the instance and deletes the network interface. When the user terminates the instance all the network interfaces attached with it are also deleted.

QUESTION NO: 252

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

A.
Cipher Protocol

B.
Client Configuration Preference

C.
Server Order Preference

D.
Load Balancer Preference

Answer: C
Explanation:

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

QUESTION NO: 253

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

A.
For Inbound allow Source: 20.0.1.0/24 on port 80

B.
For Outbound allow Destination: 0.0.0.0/0 on port 80

C.
For Inbound allow Source: 20.0.0.0/24 on port 80

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

Answer: C

Explanation:

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

QUESTION NO: 254

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

A.
The user should attach an IAM role with DynamoDB access to the EC2 instance

B.
The user should create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB

C.
The user should create an IAM role, which has EC2 access so that it will allow deploying the application

D.
The user should create an IAM user with DynamoDB and EC2 access. Attach the user with the application so that it does not use the root account credentials

Answer: A

Explanation:

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

QUESTION NO: 255

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

```
{
"Version": "2012-10-17",
"Statement": [{
"Sid": "AllowUsersAllActionsForCredentials",
"Effect": "Allow",
"Action": [
"iam:*LoginProfile",
"iam:*AccessKey*",
"iam:*SigningCertificate*"
],
"Resource": ["arn:aws:iam:: 123412341234:user/${aws:username}"]
}]
}
```

BrainDumps

A.
The policy allows the IAM user to modify all IAM user’s credentials using the console, SDK, CLI or APIs

B.
The policy will give an invalid resource error

C.
The policy allows the IAM user to modify all credentials using only the console

D.
The policy allows the user to modify all IAM user’s password, sign in certificates and access keys using only CLI, SDK or APIs

Answer: D

Explanation:

WS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (Account ID 123412341234) wants some of their users to manage credentials (access keys, password, and sing in certificates. of all IAM users, they should set an applicable policy to that user or group of users. The below mentioned policy allows the IAM user to modify the credentials of all IAM user's using only CLI, SDK or APIs. The user cannot use the AWS console for this activity since he does not have list permission for the IAM users.

```
{
"Version": "2012-10-17",
"Statement": [{
"Sid": "AllowUsersAllActionsForCredentials",
"Effect": "Allow"
"Action": [
"iam:*LoginProfile",
"iam:*AccessKey*",
"iam:*SigningCertificate*"
],
"Resource": ["arn:aws:iam::123412341234:user/${aws:username}"]
}]
}
```

BrainDumps

QUESTION NO: 256

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

ELB inserts the cookie in the response

ELB chooses the instance based on the load balancing algorithm

Check the cookie in the service request

The cookie is found in the request

The cookie is not found in the request

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

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

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

D.
3,2,5,4 [Cookie is not Present] & 3,2,4,5 [Cookie is Present]

Answer: C
Explanation:

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

QUESTION NO: 257

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

A.
Value

B.
Namespace

C.
Metric Name

D.
Time zone

Answer: B
Explanation:

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

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

QUESTION NO: 258

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

A.
Auto Scaling launches a new instance first and then terminates the unhealthy instance

B.
Auto Scaling performs the launch and terminate processes in a random order

C.
Auto Scaling launches and terminates the instances simultaneously

D.
Auto Scaling terminates the instance first and then launches a new instance

Answer: D
Explanation:

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

QUESTION NO: 259

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

A.
The private key file has the wrong file permission

B.
The ppk file used for SSH is read only

C.
The public key file has the wrong permission

D.
The user has provided the wrong user name for the OS login

Answer: A
Explanation:

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

chmod 0400 /path/to/private.key

QUESTION NO: 260

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

A.
The application does not have enough IO for the volume

B.
The instance is EBS optimized

C.
The EC2 instance has 10 Gigabit Network connectivity

D.
The volume size is too large

Answer: D
Explanation:

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

QUESTION NO: 261

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

A.
The admin should upload his secret key to the AWS console and let S3 decrypt the objects

B.
The admin should use CLI or API to upload the encryption key to the S3 bucket. When making a call to the S3 API mention the encryption key URL in each request

C.
S3 does not support client supplied encryption keys for server side encryption

D.
The admin should send the keys and encryption algorithm with each API call

Answer: D
Explanation:

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

QUESTION NO: 262

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: A
Explanation:

QUESTION NO: 263

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

A.
Enabling Read Replica

B.
Making the DB Multi AZ

C.
DB password change

D.
Security patching

Answer: D
Explanation:

Amazon RDS performs maintenance on the DB instance during a user-definable maintenance window. The system may be offline or experience lower performance during that window. The only maintenance events that may require RDS to make the DB instance offline are:

Scaling compute operations

Software patching. Required software patching is automatically scheduled only for patches that are security and durability related. Such patching occurs infrequently (typically once every few months) and seldom requires more than a fraction of the maintenance window.

QUESTION NO: 264

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?

A.
Launch the test and production instances in separate regions and allow region wise access to the group

B.
Define the IAM policy which allows access based on the instance ID

C.
Create an IAM policy with a condition which allows access to only small instances

D.
Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

Answer: D

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The user can add conditions as a part of the IAM policies. The condition can be set on AWS Tags, Time, and Client IP as well as on various parameters. If the organization wants the user to access only specific instances he should define proper tags and add to the IAM policy condition. The sample policy is shown below.

```
"Statement": [
{
"Action": "ec2:*",
"Effect": "Allow",
"Resource": "*",
"Condition": {
"StringEquals": {
"ec2:ResourceTag/InstanceType": "Production"
}
}
}
]
```

BrainDumps

QUESTION NO: 265

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

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

What will Auto Scaling do in this scenario?

A.
Terminates the instance and does not launch a new instance

B.
Terminates the instance and updates the desired capacity to 1

C.
Terminates the instance and updates the desired capacity and minimum size to 1

D.
Throws an error

Answer: D

Explanation:

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

QUESTION NO: 266

A user is collecting 1000 records per second. The user wants to send the data to CloudWatch using the custom namespace. Which of the below mentioned options is recommended for this activity?

A.
Aggregate the data with statistics, such as Min, max, Average, Sum and Sample data and send the data to CloudWatch

B.
Send all the data values to CloudWatch in a single command by separating them with a comma. CloudWatch will parse automatically

C.
Create one csv file of all the data and send a single file to CloudWatch

D.
It is not possible to send all the data in one call. Thus, it should be sent one by one. CloudWatch will aggregate the data automatically

Answer: A
Explanation:

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

QUESTION NO: 267

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

A.
124

B.
150

C.
134

D.
128

Answer: C
Explanation:

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

QUESTION NO: 268

An organization is trying to create various IAM users. Which of the below mentioned options is not a valid IAM username?

A.
John.cloud

B.
john@cloud

C.
John=cloud

D.
john#cloud

Answer: D
Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Whenever the organization is creating an IAM user, there should be a unique ID for each user. The names of users, groups, roles, instance profiles must be alphanumeric, including the following common characters:

plus (+., equal (=., comma (,., period (.., at (@., and dash (-..

QUESTION NO: 269

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 randomness. Which of the below mentioned options is a recommended option for this case?

A.
For the period when there is no data, the user should not send the data at all

B.
For the period when there is no data the user should send a blank value

C.
For the period when there is no data the user should send the value as 0

D.
The user must upload the data to CloudWatch as having no data for some period will cause an error at CloudWatch monitoring

Answer: C
Explanation:

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

QUESTION NO: 270

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

A.
CloudWatch will accept the data

B.
It is not possible to send data of the future

C.
It is not possible to send the data manually to CloudWatch

D.
The user cannot send data for more than 60 minutes in the future

Answer: A
Explanation:

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

QUESTION NO: 271

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 a folder, Amazon S3 uploads all the files and subfolders from the specified folder to the user's bucket. It then assigns a key value that is a combination of the uploaded file name and the folder name.

QUESTION NO: 272

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

A.
Error Log

B.
Slow Query Log

C.
Transaction Log

D.
General Log

Answer: C
Explanation:

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

QUESTION NO: 273

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

A.
AWS does not have sufficient capacity in that availability zone

B.
AWS zone mapping is changed for that user account

C.
There is some issue with the host capacity on which the instance is launched

D.
The user account has reached the maximum EC2 instance limit

Answer: A

Explanation:

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

QUESTION NO: 274

A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is true in this scenario?

A.
The AWS VPC will automatically create a NAT instance with the micro size

B.
VPC bounds the main route table with a private subnet and a custom route table with a public subnet

C.
The user has to manually create a NAT instance

D.
VPC bounds the main route table with a public subnet and a custom route table with a private subnet

Answer: B

Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance of a smaller or higher size, respectively. The VPC has an implied router and the VPC wizard updates the main route table used with the private subnet, creates a custom route table and associates it with the public subnet.

QUESTION NO: 275

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": "*"
}
]
}
```

BrainDumps

QUESTION NO: 276

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

A.
Define the group policy and add a condition which allows the access based on the IAM name

B.
Create a DynamoDB table with the same name as the IAM user name and define the policy rule which grants access based on the DynamoDB ARN using a variable

C.
Create a separate DynamoDB database for each user and configure a policy in the group based on the DB variable

D.
It is not possible to have a group level policy which allows different IAM users to different DynamoDB Tables

Answer: B

Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. AWS DynamoDB has only tables and the organization cannot make separate databases. The organization should create a table with the same name as the IAM user name and use the ARN of DynamoDB as part of the group policy. The sample policy is shown below:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"aws-portal:ViewUsage"
],
"Resource": "*"
}
]
}
```

BrainDumps

QUESTION NO: 277

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

A.
By default, ELB will select the first version of the security policy

B.
By default, ELB will select the latest version of the policy

C.
ELB creation will fail without a security policy

D.
It is not required to have a security policy since SSL is already installed

Answer: B

Explanation:

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

QUESTION NO: 278

A user is creating a Cloudformation stack. Which of the below mentioned limitations does not hold true for Cloudformation?

A.
One account by default is limited to 100 templates

B.
The user can use 60 parameters and 60 outputs in a single template

C.
The template, parameter, output, and resource description fields are limited to 4096 characters

D.
One account by default is limited to 20 stacks

Answer: A

Explanation:

AWS Cloudformation is an application management tool which provides application modelling, deployment, configuration, management and related activities. The limitations given below apply to the Cloudformation template and stack. There are no limits to the number of templates but each AWS CloudFormation account is limited to a maximum of 20 stacks by default. The Template,

Parameter, Output, and Resource description fields are limited to 4096 characters. The user can include up to 60 parameters and 60 outputs in a template.

QUESTION NO: 279

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 time zone within a minute, CloudWatch will aggregate the data. It treats these as a single metric, allowing the user to get the statistics, such as minimum, maximum, average, and the sum of all across all servers.

QUESTION NO: 280

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

A.
AWS SQS sends notification after 15 days for inactivity on queue

B.
AWS SQS can delete queue after 30 days without notification

C.
AWS SQS marks queue inactive after 30 days

D.
AWS SQS notifies the user after 2 weeks and deletes the queue after 3 weeks.

Answer: B
Explanation:

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

QUESTION NO: 281

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

A.
Update the Auto Scaling group to ignore the instance reboot event

B.
It is not possible to change the status once it is marked for replacement

C.
Manually add that instance to the Auto Scaling group after reboot to avoid replacement

D.
Change the health of the instance to healthy using the Auto Scaling commands

Answer: D
Explanation:

After an instance has been marked unhealthy by Auto Scaling, as a result of an Amazon EC2 or

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

QUESTION NO: 282

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

A.
elb-enable-zones-for-lb

B.
elb-add-zones-for-lb

C.
It is not possible to add more zones to the existing ELB

D.
elb-configure-zones-for-lb

Answer: A
Explanation:

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

QUESTION NO: 283

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

A.
One IAM user can be a part of a maximum of 5 groups

B.
The organization can create 100 groups per AWS account

C.
One AWS account can have a maximum of 5000 IAM users

D.
One AWS account can have 250 roles

Answer: A
Explanation:

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The default maximums for each of the IAM entities is given below:

Groups per AWS account: 100

Users per AWS account: 5000

Roles per AWS account: 250

Number of groups per user: 10 (that is, one user can be part of these many groups).

QUESTION NO: 284

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

A.
Setup the scaling policy to scale up and down based on the CloudWatch alarms

B.
The user should increase the desired capacity at 8 AM and decrease it by 7 PM manually

C.
The user should setup a batch process which launches the EC2 instance at a specific time

D.
Setup scheduled actions to scale up or down at a specific time

Answer: D

Explanation:

Scale based on a schedule

Sometimes you know exactly when you will need to increase or decrease the number of instances in your group, simply because that need arises on a predictable schedule. Scaling by schedule means that scaling actions are performed automatically as a function of time and date.

For more information, see Scheduled Scaling.

Reference:

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

QUESTION NO: 285

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

A.
Use the internet gateway with a private IP

B.
Allow outbound traffic in the security group for port 80 to allow internet updates

C.
The private subnet can never connect to the internet

D.
Use NAT with an elastic IP

Answer: D

Explanation:

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

QUESTION NO: 286

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

A.
monitoring.us-east-1.amazonaws.com

B.
monitoring.us-east-1-a.amazonaws.com

C.
monitoring.us-east-1a.amazonaws.com

D.
cloudwatch.us-east-1a.amazonaws.com

Answer: A
Explanation:

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

QUESTION NO: 287

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

A.
The instances will not be registered with ELB and the user has to manually register when the process is resumed

B.
The instances will be registered with ELB only once the process has resumed

C.
Auto Scaling will not launch the instance during this period due to process suspension

D.

It is not possible to suspend only the AddToLoadBalancer process

Answer: A

Explanation:

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

QUESTION NO: 288

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

A.
Response processing time

B.
Front end processing time

C.
Backend processing time

D.
Request processing time

Answer: B

Explanation:

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

QUESTION NO: 289

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

A.
The archive will be available as an object for the duration specified by the user during the restoration request

B.
The restored object's storage class will be RRS

C.
The user can modify the restoration period only by issuing a new restore request with the updated period

D.
The user needs to pay storage for both RRS (restored) and Glacier (Archive. Rates)

Answer: B

Explanation:

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

QUESTION NO: 290

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

A.
Setup the CloudWatch action to terminate the instance when the CPU utilization is less than 5%

B.

Setup the CloudWatch with Auto Scaling to terminate all the instances

C.
Setup a job which terminates all instances after 600 minutes

D.
It is not possible to terminate instances automatically

Answer: A
Explanation:

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

QUESTION NO: 291

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

A.
The user should not use his own security key as it is not secure

B.
Configure S3 to rotate the user's encryption key at regular intervals

C.
Configure S3 to store the user's keys securely with SSL

D.
Keep rotating the encryption key manually at the client side

Answer: D
Explanation:

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

keep rotating them regularly at the client side version.

QUESTION NO: 292

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

A.
Pre warming the EBS volume

B.
Initiating the device to mount on the EBS volume

C.
Formatting the volume

D.
Copying the data from a snapshot to the device

Answer: A
Explanation:

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

QUESTION NO: 293

A user has launched an EC2 Windows instance from an instance store backed AMI. The user

wants to convert the AMI to an EBS backed AMI. How can the user convert it?

A.
Attach an EBS volume to the instance and unbundle all the AMI bundled data inside the EBS

B.
A Windows based instance store backed AMI cannot be converted to an EBS backed AMI

C.
It is not possible to convert an instance store backed AMI to an EBS backed AMI

D.
Attach an EBS volume and use the copy command to copy all the ephemeral content to the EBS Volume

Answer: B

Explanation:

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

QUESTION NO: 294

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

A.
Destination : 20.0.0.0/24 and Target : VPC

B.
Destination : 20.0.0.0/16 and Target : ALL

C.
Destination : 20.0.0.0/0 and Target : ALL

D.
Destination : 20.0.0.0/24 and Target : Local

Answer: D

Explanation:

Option A doesn't use standard AWS terminology (you don't route to "VPC"), and because the mask is /24, it would only allow the instances in the private subnet to communicate with each other, not all the instances in the VPC as the question asked. Here's an example VPC route table for a public subnet (i.e. it routes to the IGW). Option D is the correct one.

QUESTION NO: 295

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

```
"Statement": [{
"Sid": "Stmt1388811069831",
"Effect": "Allow",
"Principal": { "AWS": "*"},
"Action": [ "s3:GetObjectAcl", "s3:ListBucket", "s3:GetObject"],
"Resource": [ "arn:aws:s3:::cloudacademy/*.jpg]
}]
```

BrainDumps

A.
It will make all the objects as well as the bucket public

B.
It will throw an error for the wrong action and does not allow to save the policy

C.
It will make the AWS.jpg object as public

D.
It will make the AWS.jpg as well as the cloudacademy bucket as public

Answer: B

Explanation:

A sysadmin can grant permission to the S3 objects or the buckets to any user or make objects public using the bucket policy and user policy. Both use the JSON-based access policy language.

Generally, if user is defining the ACL on the bucket, the objects in the bucket do not inherit it and

vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well

as the bucket to be public with a single policy applied to that bucket. In the below policy the action

says "S3:ListBucket" for effect Allow and when there is no bucket name mentioned as a part of the resource, it will throw an error and not save the policy.

QUESTION NO: 296

A user has launched an EC2 instance and deployed a production application in it. The user wants to prohibit any mistakes from the production team to avoid accidental termination. How can the user achieve this?

A.
The user can the set DisableApiTermination attribute to avoid accidental termination

B.
It is not possible to avoid accidental termination

C.
The user can set the Deletion termination flag to avoid accidental termination

D.
The user can set the InstanceInitiatedShutdownBehavior flag to avoid accidental termination

Answer: A
Explanation:

It is always possible that someone can terminate an EC2 instance using the Amazon EC2 console, command line interface or API by mistake. If the admin wants to prevent the instance from being accidentally terminated, he can enable termination protection for that instance. The DisableApiTermination attribute controls whether the instance can be terminated using the console, CLI or API. By default, termination protection is disabled for an EC2 instance. When it is set it will not allow the user to terminate the instance from CLI, API or the console.

QUESTION NO: 297

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

A.
Update the Launch config with CLI to set InstanceMonitoringDisabled = false

B.
The user should change the Auto Scaling group from the AWS console to enable detailed monitoring

C.
Update the Launch config with CLI to set InstanceMonitoring.Enabled = true

D.
Create a new Launch Config with detail monitoring enabled and update the Auto Scaling group

Answer: D

Explanation:

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

Create a new Launch config with detailed monitoring enabled

Update the Auto Scaling group with a new launch config

Enable detail monitoring on each EC2 instance

QUESTION NO: 298

A user is trying to pre-warm a blank EBS volume attached to a Linux instance. Which of the below mentioned steps should be performed by the user?

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

B.
Contact AWS support to pre-warm

C.
Unmount the volume before pre-warming

D.
Format the device

Answer: C

Explanation:

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

QUESTION NO: 299

A user has launched an EC2 instance from an instance store backed AMI. The user has attached an additional instance store volume to the instance. The user wants to create an AMI from the running instance. Will the AMI have the additional instance store volume data?

A.
Yes, the block device mapping will have information about the additional instance store volume

B.
No, since the instance store backed AMI can have only the root volume bundled

C.
It is not possible to attach an additional instance store volume to the existing instance store backed AMI instance

D.
No, since this is ephemeral storage it will not be a part of the AMI

Answer: A

Explanation:

When the user has launched an EC2 instance from an instance store backed AMI and added an instance store volume to the instance in addition to the root device volume, the block device mapping for the new AMI contains the information for these volumes as well. In addition, the block device mappings for the instances those are launched from the new AMI will automatically contain information for these volumes.

QUESTION NO: 300

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

A.
The volume will show a size of 8 GB

B.
The volume will show a loss of the IOPS performance the first time

C.
The volume will be blank

D.
If the EBS is mounted it will ask the user to create a file system

Answer: B
Explanation:

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

QUESTION NO: 301

A user has enabled termination protection on an EC2 instance. The user has also set Instance initiated shutdown behavior to terminate. When the user shuts down the instance from the OS, what will happen?

A.
The OS will shutdown but the instance will not be terminated due to protection

B.

It will terminate the instance

C.
It will not allow the user to shutdown the instance from the OS

D.
It is not possible to set the termination protection when an Instance initiated shutdown is set to Terminate

Answer: B

Explanation:

It is always possible that someone can terminate an EC2 instance using the Amazon EC2 console, command line interface or API by mistake. If the admin wants to prevent the instance from being accidentally terminated, he can enable termination protection for that instance. The user can also setup shutdown behavior for an EBS backed instance to guide the instance on what should be done when he initiates shutdown from the OS using Instance initiated shutdown behavior. If the instance initiated behavior is set to terminate and the user shuts off the OS even though termination protection is enabled, it will still terminate the instance.

QUESTION NO: 302

A user has deployed an application on an EBS backed EC2 instance. For a better performance of application, it requires dedicated EC2 to EBS traffic. How can the user achieve this?

A.
Launch the EC2 instance as EBS dedicated with PIOPS EBS

B.
Launch the EC2 instance as EBS enhanced with PIOPS EBS

C.
Launch the EC2 instance as EBS dedicated with PIOPS EBS

D.
Launch the EC2 instance as EBS optimized with PIOPS EBS

Answer: D

Explanation:

Any application which has performance sensitive workloads and requires minimal variability with

dedicated EC2 to EBS traffic should use provisioned IOPS EBS volumes, which are attached to an EBS-optimized EC2 instance or it should use an instance with 10 Gigabit network connectivity. Launching an instance that is EBS optimized provides the user with a dedicated connection between the EC2 instance and the EBS volume.

QUESTION NO: 303

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.

QUESTION NO: 304

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": [
       "*"
     ]
   }
  }
 ]
}
```

BrainDumps

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

Explanation:

QUESTION NO: 305

Which services allow the customer to retain run administrative privileges or the underlying EC2 instances? (Choose two.)

A.
AWS Elastic Beanstalk

B.
Amazon Elastic Map Reduce

C.
Elastic Load Balancing

D.
Amazon Relational Database Service

E.
Amazon Elastic Cache

Answer: A,B
Explanation:

QUESTION NO: 306

When an EC2 instance mat is backed by an S3-Based AMI is terminated, what happens to the data on the root volume?

A.
Data is automatically deleted

B.
Data is automatically saved as an EBS snapshot.

C.
Data is unavailable until the instance is restarted

D.
Data is automatically saved as an EBS volume.

Answer: A
Explanation:

QUESTION NO: 307

How can you secure data at rest on an EBS volume?

A.
Encrypt the volume using the S3 server-side encryption service.

B.
Attach the volume to an instance using EC2's SSL interface.

C.
Create an IAM policy that restricts read and write access to the volume.

D.
Write the data randomly instead of sequentially.

E.
Use an encrypted file system m top of the EBS volume.

Answer: C
Explanation:

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/policies_examples.html

QUESTION NO: 308

In order to optimize performance for a compute cluster that requires low inter-node latency, which feature in the following list should you use?

A.
AWS Direct Connect

B.
Placement Groups

C.
VPC private subnets

D.
EC2 Dedicated Instances

E.
Multiple Availability Zones

Answer: B

Explanation:

A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gigabits per second (Gbps) network. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.

QUESTION NO: 309

Amazon EBS snapshots have which of the following two characteristics? (Choose two.)

A.
EBS snapshots only save incremental changes from snapshot to snapshot

B.
EBS snapshots can be created in real-time without stopping an EC2 instance

C.
EBS snapshots can only be restored to an EBS volume of the same size or smaller

D.
EBS snapshots can only be restored and mounted to an instance in the same Availability Zone as the original EBS volume

Answer: A,B

Explanation:

QUESTION NO: 310

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

Which backup methods to AWS would be most cost-effective while still meeting all of your

requirements?

A.
Send the daily backup files to Glacier immediately after being generated

B.
Transfer the daily backup files to an EBS volume in AWS and take daily snapshots of the volume

C.
Transfer the daily backup files to S3 and use appropriate bucket lifecycle policies to send to Glacier

D.
Host the backup files on a Storage Gateway with Gateway-Cached Volumes and take daily snapshots

Answer: C
Explanation:

Because in the stored volume mode, you are storing data locally, the binary-compressed format is already available, and the bandwidth of your AWS connection meets the 7days/2hour SLA.

QUESTION NO: 311

You run a web application with the following components Elastic Load Balancer (EL8), 3 Web/Application servers, 1 MySQL RDS database with read replicas, and Amazon Simple Storage Service (Amazon S3) for static content. Average response time for users is increasing slowly.

What three CloudWatch RDS metrics will allow you to identify if the database is the bottleneck? (Choose three.)

A.
The number of outstanding IOs waiting to access the disk.

B.
The amount of write latency.

C.
The amount of disk space occupied by binary logs on the master.

D.
The amount of time a Read Replica DB Instance lags behind the source DB Instance

E.
The average number of disk I/O operations per second.

Answer: A,B,D
Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/rds-metricscollected.html

QUESTION NO: 312

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

A.
Create a bucket policy and apply it to the bucket

B.
Create a NACL and attach it to the VPC of the bucket

C.
Create an ACL and apply it to all objects in the bucket

D.
Modify the IAM policies of any users that would access the bucket

Answer: A
Explanation:

Reference:

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

QUESTION NO: 313

Your organization is preparing for a security assessment of your use of AWS.

In preparation for this assessment, which two IAM best practices should you consider implementing? (Choose two.)

A.
Create individual IAM users for everyone in your organization

B.
Configure MFA on the root account and for privileged IAM users

C.
Assign IAM users and groups configured with policies granting least privilege access

D.
Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

Answer: B,C

Explanation:

Reference:

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

QUESTION NO: 314

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: C
Reference:

https://aws.amazon.com/rds/details/read-replicas/

QUESTION NO: 315

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

A.
The IP of the primary DB Instance is switched to the standby DB Instance.

B.
A new DB instance is created in the standby availability zone.

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

D.
The RDS (Relational Database Service) DB instance reboots.

Answer: C
Explanation:

Failover Process for Amazon RDS:

In the event of a planned or unplanned outage of your DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone if you have enabled Multi-AZ. The time it takes for the failover to complete depends on the database activity and other conditions at the time the primary DB instance became unavailable.

The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance. As a result, you will need to re-establish any existing connections to your DB instance.

Reference:

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

QUESTION NO: 316

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_logs. Success codes are written to this bucket with a timestamp and checksum.

B.
A success code is inserted into the S3 object metadata.

C.
A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.

D.
Amazon S3 is engineered for 99.999999999% durability. Therefore, there is no need to confirm that data was inserted.

Answer: C
Explanation:

There are two opportunities for a copy request to return an error. One can occur when Amazon S3 receives the copy request and the other can occur while Amazon S3 is copying the files. If the error occurs before the copy operation starts, you receive a standard Amazon S3 error. If the error occurs during the copy operation, the error response is embedded in the 200 OK response. This means that a 200 OK response can contain either a success or an error. Make sure to design your application to parse the contents of the response and handle it appropriately.

If the copy is successful, you receive a response that contains the information about the copied object.

QUESTION NO: 317

How can an EBS volume that is currently attached to an EC2 instance be migrated from one Availability Zone to another?

A.
Simply create a new volume in the other AZ and specify the original volume as the source.

B.
Detach the volume, then use the ec2-migrate-volume command to move it to another AZ.

C.
Create a snapshot of the volume, and create a new volume from the snapshot in the other AZ.

D.
Detach the volume and attach it to another EC2 instance in the other AZ.

Answer: C
Explanation:

These snapshots can be used to create multiple new EBS volumes, expand the size of a volume, or move volumes across Availability Zone

Reference:

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

QUESTION NO: 318

You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from pre-defined customer IP addresses.

Which two options meet this security requirement? (Choose two.)

A.
Configure web server VPC security groups to allow traffic from your customers' IPs

B.
Configure your web servers to filter traffic based on the ELB's "X-forwarded-for" header

C.
Configure ELB security groups to allow traffic from your customers' IPs and deny all outbound traffic

D.
Configure a VPC NACL to allow web traffic from your customers' IPs and deny all outbound traffic

Answer: A,B
Explanation:

QUESTION NO: 319

How can software determine the public and private IP addresses of the Amazon EC2 instance that it is running on?

A.
Query the local instance metadata.

B.
Query the appropriate Amazon CloudWatch metric.

C.
Query the local instance userdata.

D.
Use ipconfig or ifconfig command.

Answer: A
Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.htm

QUESTION NO: 320

The compliance department within your multi-national organization requires that all data for your customers that reside in the European Union (EU) must not leave the EU and also data for customers that reside in the US must not leave the US without explicit authorization.

What must you do to comply with this requirement for a web based profile management application running on EC2?

A.
Run EC2 instances in multiple AWS Availability Zones in single Region and leverage an Elastic Load Balancer with session stickiness to route traffic to the appropriate zone to create their profile

B.
Run EC2 instances in multiple Regions and leverage Route 53's Latency Based Routing capabilities to route traffic to the appropriate region to create their profile

C.
Run EC2 instances in multiple Regions and leverage a third party data provider to determine if a user needs to be redirect to the appropriate region to create their profile

D.
Run EC2 instances in multiple AWS Availability Zones in a single Region and leverage a third party data provider to determine if a user needs to be redirect to the appropriate zone to create their profile

Answer: C
Explanation:

QUESTION NO: 321

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database.

Which configuration will allow you to securely serve private content to your users?

A.
Generate pre-signed URLs for each user as they request access to protected S3 content

B.
Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user

C.
Create an S3 bucket policy that limits access to your private content to only your subscribed users' credentials

D.
Create a CloudFront Origin Identity user for your subscribed users and assign the GetObject permission to this user

Answer: A
Explanation:

“You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn’t required to use signed URLs, but we recommend it.”

Reference:

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html

QUESTION NO: 322

In AWS, which security aspects are the customer's responsibility? (Choose four.)

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: B,C,D,F
Explanation:

QUESTION NO: 323

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:

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.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated-instance.html#dedicated-apichanges

QUESTION NO: 324

A .NET application that you manage is running in Elastic Beanstalk. Your developers tell you they will need access to application log files to debug issues that arise. The infrastructure will scale up and down.

How can you ensure the developers will be able to access only the log files?

A.
Access the log files directly from Elastic Beanstalk

B.
Enable log file rotation to S3 within the Elastic Beanstalk configuration

C.
Ask your developers to enable log file rotation in the applications web.config file

D.
Connect to each Instance launched by Elastic Beanstalk and create a Windows Scheduled task to rotate the log files to S3.

Answer: D

Explanation:

Reference:

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

QUESTION NO: 325

Your mission is to create a lights-out datacenter environment, and you plan to use AWS OpsWorks to accomplish this. First you created a stack and added an App Server layer with an instance running in it. Next you added an application to the instance, and now you need to deploy a MySQL RDS database instance.

Which of the following answers accurately describe how to add a backend database server to an OpsWorks stack? (Choose three.)

A.
Add a new database layer and then add recipes to the deploy actions of the database and App Server layers.

B.
Use OpsWorks' "Clone Stack" feature to create a second RDS stack in another Availability Zone for redundancy in the event of a failure in the Primary AZ. To switch to the secondary RDS instance, set the [:database] attributes to values that are appropriate for your server which you can do by using custom JSON.

C.
The variables that characterize the RDS database connection—host, user, and so on—are set using the corresponding values from the deploy JSON's [:depioy][:app_name][:database] attributes.

D.
Cookbook attributes are stored in a repository, so OpsWorks requires that the "password": "your_password" attribute for the RDS instance must be encrypted using at least a 256-bit key.

E.
Set up the connection between the app server and the RDS layer by using a custom recipe. The recipe configures the app server as required, typically by creating a configuration file. The recipe gets the connection data such as the host and database name from a set of attributes in the stack configuration and deployment JSON that AWS OpsWorks installs on every instance.

Answer: A,C,E

Explanation:

QUESTION NO: 326

A user needs to put sensitive data in an Amazon S3 bucket that can be accessed through an S3 VPC endpoint only. The user must ensure that resources in the VPC can only access the single S3 bucket.

Which combination of actions will meet the requirements? (Choose two.)

A.
Configure the bucket policy to only allow access through the S3 Private Endpoint.

B.
Modify the VPC endpoint policy on the bucket to only allow the VPC to access it.

C.
Modify the VPC peering configuration to only allow access to the S3 private Endpoint.

D.
Configure the VPC endpoint policy to only allow the VPC to access the specific S3 bucket.

E.
Configure the IAM policy attached to the S3 bucket to only allow access from the specific VPC.

Answer: B,D
Reference: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

QUESTION NO: 327

A corporate website is hosted on several Amazon EC2 instances across multiple regions around the globe.

How should an Administrator configure the website to maintain high availability with minimal downtime if one of the regions has network connectivity congestion for an extended period of time?

A.
Create an Elastic Load Balancer in front of all the Amazon EC2 instances.

B.
Create an Elastic Load Balancer that fails over to the secondary site when the primary site is not reachable.

C.
Create an Amazon Route 53 Latency Based Routing Record Set that resolves to an Elastic Load Balancer in each region. Set an appropriate health check on each ELB.

D.
Create an Amazon Route 53 latency Based Routing Record Set that resolves to Elastic Load Balancers I each region and has the Evaluate Target Health flag set to “true”.

Answer: D
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html

QUESTION NO: 328

A database running on Amazon EC2 requires sustained IOPS performance.

Which kind of Amazon EBS volume should an Administrator choose for this solution?

A.
Cloud HDD

B.
General Purpose SSD

C.
Provisioned IOPS SSD

D.
Throughput Optimized HDD

Answer: C
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

QUESTION NO: 329

What does the “configure” command allow an Administrator to do when setting up the AWS CLI? (Choose two.)

A.
Decide which VPC to create instances in.

B.
Designate the format of the response to CLI commands.

C.
Choose the default EC2 instance.

D.
Encrypt the CLI commands.

E.
Designate the default region.

Answer: B,E

Explanation:

QUESTION NO: 330

An Administrator has an Amazon EC2 instance with an IPv6 address. The Administrator needs to prevent direct access to this instance from the Internet.

The Administrator should place the EC2 instance in a:

A.
Private Subnet with an egress-only Internet Gateway attached to the subnet and placed in the subnet Route Table.

B.
Public subnet with an egress-only Internet Gateway attached to the VPC and placed in the VPC Route Table.

C.
Private subnet with an egress-only Internet Gateway attached to the VPC and placed in the subnet Route Table.

D.
Public subnet and a security group that blocks inbound IPv6 traffic attached to the interface.

Answer: B

Explanation:

QUESTION NO: 331

As part of an operational audit, an Administrator is tasked with showing that all security responsibilities under the customer's control are properly executed.

Which of the following items is the customer responsible for providing to the auditor? (Choose two.)

A.
Physical data center access logs

B.
AWS CloudTrail logs showing API calls

C.
Amazon EC2 instance system logs

D.
Storage device destruction records

E.
Xen Hypervisor system logs

Answer: C,D

Explanation:

QUESTION NO: 332

A colleague is attempting to launch several new CloudFormation stacks, and receives the following error response:

```
<Error>
        <Type> Sender</Type>
        <Code>Throttling</Code>
        <Message>Rate exceeded</Message>
</Error>
```

What should be done to address the error?

A.
Add a Pause to the CloudFormation templates.

B.
Add an exponential backoff between CreateStack API calls.

C.
Run the CloudFormation API calls from a larger Amazon EC2 instance.

D.
Combine stack templates into one, and retry the CreateStack API call.

Answer: B
Reference: https://forums.aws.amazon.com/thread.jspa?threadID=100414

QUESTION NO: 333

A security policy allows instances in the Production and Development accounts to write application logs to an Amazon S3 bucket belonging to the Security team's account. Only the Security team should be allowed to delete logs from the S3 bucket.

Using the "myAppRole" EC2 role, the production and development teams report that the application servers are not able to write to the S3 bucket.

Which changes need to be made to the policy to allow the application logs to be written to the S3 bucket?

Production Account: 111111111111

Dev Account: 222222222222

Security Account: 555555555555

```
{
     "Version": "2012-10-17",
     "Statement": [ [
        "Effect": "Allow",
        "Principal": [ {
           "AWS": [
               "arn: aws:iam: : 111111111111: role/myAppRole"
               "arn: aws:iam: : 222222222222: role/myAppRole"
            ]
         }],
         "Action": [
            "s3: *"
         ],
         "Resource": [
         ],
         "Condition" {
            "StringNotLike": {
               "aws: userID": [
                      "555555555555"
                }
            }
         }
     ]
}
```

BrainDumps

A.
Update the Action for the Allow policy from “s3:*” to “s3:PutObject”

B.
Change the order of the statements in the bucket policy, moving the Deny policy above the Allow policy.

C.
Update the Action for the Deny policy from “s3:*” to “s3: Delete*”.

D.
Remove the bucket policy, because the default security behavior will not allow objects to be deleted by non bucket owners.

Answer: A

Explanation:

QUESTION NO: 334

A company is auditing their infrastructure to obtain a compliance certification.

Which of the following options are the company’s responsibility within the Shared Responsibility Model? (Choose two.)

A.

AWS API endpoint SSL Certificates

B.
EC2 Instance Operating System updates

C.
EBS Encryption-at-result algorithms

D.
IAM user password policies

E.
AWS Hypervisor software updates

Answer: A,B

Explanation:

QUESTION NO: 335

Which instance characteristics are required if an Administrator wants to ensure use of the Amazon EC2 auto-recovery option? (Choose two.)

A.
The instance only has EBS volumes.

B.
The instance has EC2 Instance Store root volumes.

C.
The tenancy attribute is set to “default” (shred tenancy).

D.
The tenancy attribute is set to “Dedicated”.

E.
The instance type belongs to the d2, i2 or i3 instance type.

Answer: A,C
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html

QUESTION NO: 336

Which two steps are required to generate a report detailing specific cost allocation tags when creating a Monthly Cost Allocation report? (Choose two.)

A.
Use AWS CloudTrail to export the events for the specified resources.

B.
Use an AWS Lambda function to read the resources' metadata, and write the specified tags to a DynamoDB table.

C.
Activate the "requested" tags by clicking Manage report tags on the Billing Preferences page.

D.
Select the checkbox for Cost Allocation Report in the AWS account's Billing Management Console.

E.
Create a new Budget using the Billing Management Console, use the "Include costs related to Tags" feature, and select the requested tags.

Answer: B,D

Explanation:

QUESTION NO: 337

A company has a fleet of EC2 instances, and needs to remotely execute scripts for all of the instances.

Which Amazon EC2 Systems Manager feature allows this?

A.
System Manager Automation

B.
System Manager Run Command

C.
System Manager Parameter Store

D.
System Manager Inventory

Answer: B

Explanation:

QUESTION NO: 338

A corporate policy requires all new infrastructure deployments to use scalable and reusable resources to improve resources delivery times. The policy also restricts resource configuration management to the systems operations team. The development team requests the ability to deploy resources on demand in an effort to streamline their software development lifecycle.

What can the systems operations team do to ensure company policy is followed while also meeting the development team's requests?

A.
Create an AWS CloudFormation on template with the requested resources, and give it to the development team to adjust as needed.

B.
Provision the resources using the CLI, and create the necessary IAM permissions to allow the development team to modify them as needed.

C.
Create the AWS Service Catalog product and share with the development team through the Service Catalog.

D.
Grant the development team access to the AWS CloudFormation Design Template Editor to specify the needed resources and configurations. Once the templates are complete, the system operations team will launch the resources.

Answer: D

Explanation:

QUESTION NO: 339

An application hosted on AWS is going through an external compliance assessment. An Administrator has been tasked with providing proof of physical security at the facilities that are hosting the application.

What should the Administrator do?

A.
Work with AWS support to schedule a tour for the auditors.

B.
Send a copy of the AWS Security whitepaper to the auditors.

C.
Obtain a relevant report from AWS Artifact and share it with the auditors.

D.
Find the address for the AWS Direct Connect facility on the AWS Website.

Answer: B

Explanation:

QUESTION NO: 340

What can an Administrator do to monitor whether an organization's instances are compliant with corporate policies and guidelines?

A.
Check the instances' metadata to determine what software is running.

B.
Use AWS CloudTrail logs to identify the applications running on the instances.

C.
Set CloudWatch alarms that are triggered with any software change on the instances.

D.
Using Config Rules in the AWS Config service to check the instance's configuration and applications.

Answer: D

Explanation:

QUESTION NO: 341

Which of the following are the customer's responsibilities, according to the AWS Shared Responsibility Security Model? (Choose two.)

A.
Operating system, network, and firewall configuration

B.
Client-side data encryption and data integrity authentication

C.
AWS data center access logs

D.
Hypervisor updates and configuration

E.
Physical media destruction

Answer: A,B
Reference: https://cloudacademy.com/blog/aws-shared-responsibility-model-security/

QUESTION NO: 342

Elastic Load Balancing automatically distributes incoming traffic across multiple _____ instances.

A.
EC2

B.
RDS

C.
M3

D.
DB

Answer: A
Explanation:

AWS provides the Elastic Load Balancing service to automatically distribute the incoming traffic across multiple Amazon Elastic Compute Cloud (Amazon EC2) instances. The load balancer serves as a single point of contact for clients, which increases the availability of your application.

You can add and remove instances from your load balancer as your needs change, without disrupting the overall flow of requests to your application.

Reference:

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

QUESTION NO: 343

_____ is a task coordination and state management service for cloud applications.

A.
Amazon SWF

B.
Amazon FPS

C.
Amazon SES

D.
Amazon SNS

Answer: A
Explanation:

Amazon Simple Workflow (Amazon SWF) is a task coordination and state management service for cloud applications. With Amazon SWF, you can stop writing complex glue-code and state machinery and invest more in the business logic that makes your applications unique.

Reference: http://aws.amazon.com/swf/

QUESTION NO: 344

A block device is a storage device that moves data in sequences. How many types of block devices does Amazon EC2 support?

A.
2 -instance store volumes and EBS volumes

B.
5 -General Purpose SSD, Provisioned IOPS SSD, Throughput Optimized HDD, Cold HDD, and

Magnetic

C.
3 -SSD, HDD, and Magnetic

D.
1 -instance store volumes

Answer: A
Explanation:

A block device is a storage device that moves data in sequences of bytes or bits (blocks). These devices support random access and generally use buffered I/O. Examples include hard disks, CD-ROM drives, and flash drives. A block device can be physically attached to a computer or accessed remotely as if it were physically attached to the computer. Amazon EC2 supports two types of block devices:

Amazon EC2 supports two types of block devices.

Instance store volumes (virtual devices whose underlying hardware is physically attached to the host computer for the instance)

EBS volumes (remote storage devices)

The SSD, HDD and Magnetic choices are all options for the type of storage offered via EBS volumes. They are not types of block devices.

Reference:

http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html

QUESTION NO: 345

Do Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

A.
No, they are dependent.

B.
No, you cannot attach EBS volumes to an instance.

C.
Yes, they do but only if they are detached from the instance.

D.
Yes, they do, if the Delete on termination flag is unset.

Answer: D
Explanation:

An Amazon EBS volume behaves like a raw, unformatted, external block device that you can attach to a single instance. The volume persists independently from the running life of an Amazon EC2instance.

Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION NO: 346

Is it possible to access S3 objects from the Internet?

A.
Yes, but it has to pass through EC2.

B.
Yes, it is possible if proper public readable accesses and ACLs are set.

C.
No, there is no way to access any S3 objects from the Internet.

D.
No, only a general overview of S3 objects can be read from the Internet.

Answer: B
Explanation:

You must grant read permission on the specific objects to make them publicly accessible so that your users can view them on your website. You make objects publicly readable by using either the object ACL or by writing a bucket policy.

Reference: https://aws.amazon.com/articles/5050

QUESTION NO: 347

_____ is a fast, reliable, scalable, fully managed message queuing service.

A.
AWS Data Pipeline

B.
Amazon SES

C.
Amazon SQS

D.
Amazon SNS

Answer: C

Explanation:

Amazon Simple Queue Service (SQS) is a fast, reliable, scalable, fully managed message queuing service. SQS makes it simple and cost-effective to decouple the components of a cloud application.

Decoupling the components of an application -you have a queue of work items and want to track the successful completion of each item independently. Amazon SQS tracks the ACK/FAIL results, so the application does not have to maintain a persistent checkpoint or cursor. After a configured visibility timeout, Amazon SQS deletes acknowledged messages and redelivers failed messages.

Configuring individual message delay -you have a job queue and you need to schedule individual jobs with a delay. With standard queues, you can configure individual messages to have a delay of up to 15 minutes.

Dynamically increasing concurrency or throughput at read time -you have a work queue and want to add more consumers until the backlog is cleared. Amazon SQS requires no pre-provisioning.

Scaling transparently -your buffer requests and the load changes as a result of occasional load spikes or the natural growth of your business. Because Amazon SQS can process each buffered request independently, Amazon SQS can scale transparently to handle the load without any provisioning instructions from you.

Reference: http://aws.amazon.com/sqs/

QUESTION NO: 348

What does Amazon Route53 provide?

A.
A global Content Delivery Network

B.
A scalable DNS web service

C.
An SSH endpoint for Amazon EC2

D.
None of these

Answer: B
Explanation:

Amazon Route53 provides a scalable Domain Name System. Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

Reference: http://aws.amazon.com/route53/

QUESTION NO: 349

What does Amazon VPC stand for?

A.
Amazon Virtual Private Cloud

B.
Amazon Variable Power Cluster

C.
Amazon Virtual Private Computer

D.
Amazon Virtual Public Cloud

Answer: A

Explanation:

Amazon VPC stands for Amazon Virtual Private Cloud (Amazon VPC). Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can also create a hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.

Reference: http://aws.amazon.com/vpc/faqs/#G1

QUESTION NO: 350

Which of the following does Amazon S3 provide?

A.
A virtual server in the cloud

B.
A highly-scalable cloud storage

C.
A highly encrypted virtual disk in the cloud

D.
A transient storage in the cloud

Answer: B
Explanation:

Amazon S3 provides Scalable Storage in the Cloud. Amazon Simple Storage Service (Amazon S3) is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web. It is designed to deliver 99.999999999% durability, and scale past trillions of objects worldwide.

Reference: https://aws.amazon.com/s3/

QUESTION NO: 351

The billing process for Amazon EC2 instances was updated as of October 2, 2017. Which of the following statements is true regarding how you pay for Amazon EC2 instances? (Choose two.)

A.
Payment does not vary based on the instance AMI's operating system.

B.
You can pay per hour or per second, depending on the instance AMI's operating system.

C.
You pay for compute capacity by the day; hours are billed in proportion.

D.
You can pay per hour or per second, depending on the instance type.

Answer: B,D

Explanation:

Previously, if you launched an instance for 5 minutes, you would pay for 1 hour. If you launched an instance for 45 minutes, you would also pay for 1 hour. This means that partial hours cost as much as one full hour. Pricing is per instance-hour consumed for each instance, from the time an instance is launched until it is terminated or stopped. Each partial instance-hour consumed will be billed as a full hour.

With EC2 services now billed per-second in some cases, as well as per-hour in others as of October 2, 2017, there is more to consider. Amazon AWS is still based on the concept of pay-as-you-go. You pay Amazon EC2 instances by the second for all instance types except Dedicated Host, which is still billed per instance-hour. You are billed per second when using Linux operating systems with no separate hourly charge, and billed per hour when using Windows operating systems.

Reference: http://aws.amazon.com/ec2/pricing/

QUESTION NO: 352

When an instance terminates, Amazon EC2 uses the value of the _____ attribute for each attached Amazon EBS volume to determine whether to preserve or delete the volume.

A.
InstanceInitiatedShutdownBehavior

B.
DeleteOnTermination

C.
EC2ModifyInstance

D.
DisableApiTermination

Answer: B
Explanation:

When an instance terminates, Amazon EC2 uses the value of the DeleteOnTermination attribute for each attached Amazon EBS volume to determine whether to preserve or delete the volume.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

QUESTION NO: 353

What does Amazon RDS perform?

A.
It tests the functionalities in websites.

B.
It blocks users from creating DB instances.

C.
It manages the work involved in setting up a relational database.

D.
It provides sensory feedback.

Answer: C
Explanation:

Amazon RDS manages the work involved in setting up a relational database: from provisioning the infrastructure capacity you request to installing the database software.

Reference: http://aws.amazon.com/rds/faqs/#1

QUESTION NO: 354

What was the recommended use case for S3 Reduced Redundancy storage before its deprecation was planned?

A.
It was used to reduce storage costs by providing 500 times the durability of a typical disk drive at lower levels of redundancy.

B.
It was used to reduce storage costs for noncritical data at lower levels of redundancy.

C.
It was used to reduce storage costs by allowing you to destroy any copy of your files outside a specific jurisdiction.

D.
It was used to reduce storage costs for reproducible data at high levels of redundancy in a single facility.

Answer: B

Explanation:
Explanation

Reduced Redundancy Storage (RRS) was introduced in order to reduce storage costs. When first developed, you could use reduced redundancy storage for noncritical, reproducible data at lower levels of redundancy than Amazon S3 provides with standard storage. Now Standard is a more affordable from a cost perspective, because Amazon is deprecating RRS and has changed the pricing structure.

Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingRRS.html

QUESTION NO: 355

_____ is a fast, flexible, fully managed pub/sub messaging service.

A.
Amazon SQS

B.
Amazon SES

C.

Amazon FPS

D.
Amazon SNS

Answer: D
Explanation:

Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push messaging service. Amazon SNS makes it simple and cost-effective to push to mobile devices such as iPhone, iPad, Android, Kindle Fire, and internet connected smart devices, as well as pushing to other distributed services.

Reference: http://aws.amazon.com/sns/?nc1=h_l2_as

QUESTION NO: 356

Does AWS offer any web-based graphic user interface to access and manage EC2 instances?

A.
Yes, the AWS Application Clusters.

B.
No, you can only use the available software development kits.

C.
Yes, the AWS Management Console.

D.
No, you can only use the command line interface.

Answer: C
Explanation:

You can access and manage Amazon Web Services through a simple and intuitive web-based user interface known as the AWS Management Console.

Reference: http://aws.amazon.com/console/

QUESTION NO: 357

What is the maximum size of an object in Amazon S3?

A.
4 TB

B.
Unlimited

C.
5 TB

D.
500 MB

Answer: C
Explanation:

5TB is the maximum size of an object in Amazon S3.

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

Reference:

http://aws.amazon.com/s3/faqs/#How_much_data_can_I_store

QUESTION NO: 358

Amazon EBS provides the ability to create backups of any Amazon EC2 volume into what is known as _____.

A.
snapshots

B.
mirrors

C.
instance backups

D.
images

Answer: A

Explanation:

Amazon allows you to backup the data stored in your EBS volumes with snapshots that can later be used to create a new EBS volume.

Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION NO: 359

Which of the following size ranges is true of Individual Amazon S3 objects?

A.
5 gigabytes to 5 terabytes

B.
0 bytes to 5 terabytes

C.
100 megabytes to 5 gigabytes

D.
1 byte to 5 gigabytes

Answer: B

Explanation:

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from 0 bytes to 5 terabytes.

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

QUESTION NO: 360

What is a security group in Amazon AWS?

A.
A UNIX Group that gives permission to edit security settings

B.
An authorized group of instances that control access to other resources

C.
A virtual firewall that controls the traffic for one or more instances

D.
An Access Control List (ACL) for AWS resources

Answer: C
Explanation:

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION NO: 361

What does Amazon EBS stand for?

A.
Elastic Business Server

B.
Elastic Basic Storage

C.
Elastic Blade Server

D.
Elastic Block Store

Answer: D
Explanation:

Amazon EBS stands for Elastic Block Store. It is a persistent storage that allows you to store the data of the Amazon EC2 Instances in a separated virtual storage automatically replicated within its Availability Zone in order to prevent component failure; with Amazon EBS the customer can add more storage every time they need it, and also add more performances with Amazon EBS Provisioned IOPS.

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

QUESTION NO: 362

EBS (Elastic Block Store) can be best described as:

A.
persistent internet storage.

B.
persistent block storage.

C.
transient instance storage.

D.
transient block storage.

Answer: B
Explanation:

Amazon Elastic Block Store (Amazon EBS) provides block level (file system type) storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance.

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

QUESTION NO: 363

In Amazon RDS, which of the following provides enhanced availability and durability for Database (DB) Instances, making them to be a natural fit for production database workloads?

A.
Placement Groups

B.
Multi-Option Group deployment

C.
Multi-AZ deployment

D.
Multi-VPC deployment

Answer: C
Explanation:

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

Reference: http://aws.amazon.com/rds/multi-az/

QUESTION NO: 364

The Amazon Linux AMI is:

A.
a simple OS installation media.

B.
an instance package provided by the AWS.

C.
a refined, easy-to-use, up-to-date Linux desktop distribution.

D.
a supported and maintained Linux image provided by AWS.

Answer: D
Explanation:

The Amazon Linux AMI is a supported and maintained Linux image provided by AWS. It is

updated on a regular basis to include the latest components, and these updates are also made available in the yum repositories for installation on running instances. The Amazon Linux AMI also Includes packages that enable easy integration with AWS services, such as the AWS CLI, Amazon EC2 API and AMI tools, the Boto library for Python, and the Elastic Load Balancing tools.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html#amazon-linux

QUESTION NO: 365

_____ is a fully managed service for real-time processing of streaming data at massive scale.

A.
AWS Data Pipeline

B.
Amazon Kinesis

C.
AWS CloudHSM

D.
Amazon Elastic Compute Cloud

Answer: B

Explanation:

Amazon Kinesis is a fully managed service for real-time processing of streaming data at massive scale. Amazon Kinesis can collect and process hundreds of terabytes of data per hour from hundreds of thousands of sources, allowing you to easily write applications that process information in real-time from sources such as web site click-streams, marketing and financial information, manufacturing instrumentation and social media, and operational logs and metering data.

Reference: http://docs.aws.amazon.com/mobile/sdkforandroid/developerguide/kinesis.html

QUESTION NO: 366

In Amazon S3, what is the document that defines who can access a particular bucket or object called?

A.
Access Control Record

B.
Access Control Service

C.
Access Control List

D.
Access Control Server

Answer: C

Explanation:

Access Control List is the document that defines who can access a particular bucket or object in Amazon S3. Amazon S3 Access Control Lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access.

Reference:

http://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html

QUESTION NO: 367

Where is an object stored in Amazon S3?

A.
in a Bucket

B.
in a Collector

C.
in an Archive

D.
in a Vault

Answer: A

Explanation:

Every object in Amazon S3 is stored in a bucket. Before you can store data in Amazon S3, you must create a bucket.

Reference: http://docs.aws.amazon.com/AmazonS3/latest/gsg/CreatingABucket.html

QUESTION NO: 368

Which AWS service offers cost optimization by launching instances automatically only when needed?

A.
Elastic Load Balancing

B.
Elastic Compute Cloud

C.
Auto Scaling

D.
Relational Database Service

Answer: C

Explanation:

AWS Auto Scaling can launch instances based on certain criteria. This provides cost optimization to the user as it will only launch the instance when required, thereby resulting in cost saving.

Reference:

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

QUESTION NO: 369

What does Amazon SWF stand for?

A.
Simple Waveflow Service

B.
Simple WebFactor Service

C.
Simple Workflow Service

D.
Simple WebForm Service

Answer: C
Explanation:

Amazon Simple Workflow Service (SWF) provides the glue needed by your application to coordinate several tasks. These tasks are tackled by several instances coordinating aspects like the dependencies between them.

Reference: http://aws.amazon.com/swf/

QUESTION NO: 370

In Amazon EC2, can you create an EBS volume from a snapshot and attach it to another instance?

A.
No, you cannot attach EBS volumes to an instance.

B.
Yes, you can but only if the volume is larger than 2TB.

C.
No, you can't create an EBS volume from a snapshot.

D.
Yes, you can.

Answer: D
Explanation:

To keep a backup copy of your data, you can create a snapshot of an EBS volume, which is stored in Amazon S3. You can create an EBS volume from a snapshot, and attach it to another instance.

Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION NO: 371

Spot instances are ideally designed for which purpose below?

A.
Running database instances that can scale up and down based on a specific workload.

B.
Running long duration and highly transactional applications.

C.
For building distributed fault tolerant databases under a tight deadline.

D.
Taking advantage of excess EC2 capacity at prices below standard on-demand rates, for short duration jobs.

Answer: D

Explanation:

There are four general categories of time-flexible and interruption-tolerant tasks that work well with Spot Instances: Delayable tasks, Optional tasks, Tasks that can be sped up by adding additionalcomputing power and at the end, Tasks that require a large number of compute instances that you can't access any other way.

Reference: http://aws.amazon.com/ec2/spot-instances/

QUESTION NO: 372

What does Amazon EMR stand for?

A.
Elastic Magnetic Resonance

B.
Encrypted Machine Reads

C.
Elastic MapReduce

D.
Encrypted Machine Rendering

Answer: C
Explanation:

Amazon EMR stands for Elastic MapReduce (Amazon EMR.) Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoopand Apache Spark,

on AWS to process and analyze vast amounts of data. By using these frameworks and related open-

source projects, such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads.

Reference:

http://docs.aws.amazon.com/ElasticMapReduce/latest/DeveloperGuide/emr-what-is-emr.html

QUESTION NO: 373

What is the main use of EMR?

A.
Data-sensitive storage

B.
Encryption

C.
Data-intensive processing tasks

D.
authentication

Answer: C
Explanation:

Using Amazon EMR, you can instantly provision as much or as little capacity as you like to perform data-intensive tasks for applications such as web indexing, data mining, log file analysis,

machine learning, financial analysis, scientific simulation, and bioinformatics research. Amazon

EMR lets you focus on crunching or analyzing your data without having to worry about time-consuming set-up, management or tuning of Hadoop clusters or the compute capacity upon which they sit.

Reference: https://aws.amazon.com/elasticmapreduce/faqs/

QUESTION NO: 374

What cloud service does Amazon S3 offer?

A.
Atomic updates across keys over the Internet

B.
Messaging over the Internet

C.
Storage over the Internet

D.
Object locking over the Internet

Answer: C
Explanation:

Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web.

Reference:

http://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html

QUESTION NO: 375

A user is launching an instance with EC2. Which options below should the user consider before

launching an instance?

A.
Select the region where the instance is being launched.

B.
All choices are correct.

C.
Select the instance type.

D.
Select the OS of the AMI.

Answer: B
Explanation:

Regarding Amazon EC2, when launching an instance, the user needs to select the region the instance would be launched from. While launching, the user needs to plan for the instance type and the OS of the instance.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-instance_linux.html

QUESTION NO: 376

In regard to AWS CloudFormation, to pass values to your template at runtime you should use _____.

A.
parameters

B.
conditions

C.
resources

D.
mapping

Answer: A
Explanation:

Optional parameters are listed in the Parameters section. Parameters enable you to pass values

to your template at runtime, and can be dereferenced in the Resources and Outputs sections of the template.

Reference:

http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/concept-template.html

QUESTION NO: 377

What does Amazon S3 stand for?

A.
Social Storage Service

B.
Simple Storage Service

C.
Secure Storage Service

D.
Standard Storage Service

Answer: B

Explanation:

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. It provides a simple interface to manage scalable, reliable, and low latency data storage service over the Internet.

Reference: http://docs.aws.amazon.com/AmazonS3/latest/gsg/GetStartedWithS3.html

QUESTION NO: 378

What is Amazon WorkSpaces?

A.
Amazon WorkSpaces is a fully managed desktop computing service in the cloud, allowing end-users to access the documents, applications, and resources they need with the device of their choice.

B.
Amazon WorkSpaces is a flexible application management solution with automation tools that enable you to model and control your applications and their supporting infrastructure.

C.
Amazon WorkSpaces is a fully redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere on the web.

D.
Amazon WorkSpaces is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data.

Answer: A
Explanation:

Amazon WorkSpaces is a fully managed desktop computing service in the AWS cloud, allowing end-users to access the documents, applications, and resources they need with the device of their choice.

Amazon WorkSpaces offers a choice of service bundles. You can choose from Value, Standard, Performance, Power, or Graphics bundles that offer different CPU, GPU, memory, and storage resources (SSD volumes).

Reference: https://aws.amazon.com/workspaces/

QUESTION NO: 379

What does AMI stand for?

A.
Amazon Machine Image

B.
Advanced Machine Instance

C.
Amazon Micro Instance

D.
Advanced Machine Image

Answer: A

Explanation:

AMI stands for Amazon Machine Image.

An Amazon Machine Image (AMI) is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, you launch an instance, which is a copy of the AMI running as a virtual server in the cloud. You can launch multiple instances of an AMI, as shown in the following figure.

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

QUESTION NO: 380

Which of the following statements is true of tags and resource identifiers for EC2 instances?

A.
You can't select instances by their tags for stoppage, termination, or deletion

B.
You don't need to specify the resource identifier while terminating a resource.

C.
You don't need to specify the resource identifier while stopping a resource.

D.
You can select instances by their tags for stoppage, termination, or deletion

Answer: A

Explanation:

You can assign tags only to resources that already exist. You can't terminate, stop, or delete a resource based solely on its tags; you must specify the resource identifier. For example, to delete snapshots that you tagged with a tag key called DeleteMe, you must use the DeleteSnapshots action with the resource identifiers of the snapshots, such as snap-1234567890abcdef0. To identify resources by their tags, you can use the DescribeTags action to list all of your tags and their associated resources.

Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Using_Tags.html

QUESTION NO: 381

What does Amazon RDS stand for?

A.
Amazon Regional Data Server

B.
Amazon Regional Database Service

C.
Amazon Relative Data Service

D.
Amazon Relational Database Service

Answer: D

Explanation:

Amazon RDS stands for Relational Database Service, which offers easy to scale and manage relational databases on the Cloud.

It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks, freeing you up to focus on your applications and business. Amazon RDS provides you six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.

Reference: http://aws.amazon.com/rds/

QUESTION NO: 382

What does Amazon SES provide?

A.
A managed Email Server

B.
A scalable anti-spam service

C.
A scalable email sending and receiving service

D.
A managed drag-and-drop interface with the AWS CloudFormation Designer

Answer: C

Explanation:

Amazon SES or Simple Email Service offers a transactional and highly scalable email service.

Amazon SES is an email platform that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains. For example, you can send marketing emails such as special offers, transactional emails such as order confirmations, and other types of correspondence such as newsletters. When you use Amazon SES to receive mail, you can develop software solutions such as email auto responders, email unsubscribe systems, and applications that generate customer support tickets from incoming emails.

Reference: http://aws.amazon.com/ses/

QUESTION NO: 383

Pricing is ____ consumed for EC2 instances.

A.
per instance-hour only

B.
per instance-minute or instance-hour

C.
per instance-second or per instance-hour

D.
per instance-minute only

Answer: C

Explanation:

In AWS, you pay only for what you use.

EC2 pricing is per instance-second consumed, or per instance-hour consumed depending on the instance type and operating system for the AMI. For example, spot instances, reserved instances and on-demand instances are billed per-second, while Dedicated instances are billed per hour.

Linux instances can be billed per second, but Microsoft Windows instances are billed per hour.

Reference:

https://aws.amazon.com/blogs/aws/new-per-second-billing-for-ec2-instances-and-ebs-volumes/

QUESTION NO: 384

What does Amazon SES stand for?

A.
Simple Elastic Server

B.
Software Email Solution

C.
Software Enabled Server

D.
Simple Email Service

Answer: D
Explanation:

Amazon SES stands for Simple Email Service.

Amazon SES is an email platform that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains. For example, you can send marketing emails such as special offers, transactional emails such as order confirmations, and other types of correspondence such as newsletters. When you use Amazon SES to receive mail, you can develop software solutions such as email autoresponders, email unsubscribe systems, and applications that generate customer support tickets from incoming emails.

Reference: http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html

QUESTION NO: 385

What is a "vault" in Amazon Glacier?

A.
A unique ID that maps an AWS Region, plus a specific Amazon S3 bucket

B.
A way to group archives together in Amazon Glacier

C.

A container for storing S3 buckets

D.
A free tier available for 12 months following your AWS sign-up date

Answer: B
Explanation:

An Amazon Glacier vault is a container in which you can organize and manage your archives.

You store data in Amazon Glacier as an archive. Each archive is assigned a unique archive ID that can later be used to retrieve the data. An archive can represent a single file or you may choose to combine several files to be uploaded as a single archive. You upload archives into vaults. Vaults are collections of archives that you use to organize your data.

Reference: http://aws.amazon.com/glacier/faqs/#How_do_vaults_work

QUESTION NO: 386

A user has launched five instances and have registered them with an ELB. How can the user add the sixth EC2 instance to the ELB?

A.
The user must stop the ELB and add the sixth instance.

B.
The user can add the sixth instance on the fly through API, CLI or the AWS Management Console.

C.
The user can add the instance and change the ELB config file.

D.
The ELB can only have a maximum of five instances.

Answer: B
Explanation:

Elastic Load Balancing automatically distributes incoming traffic across multiple EC2 instances.

You create a load balancer and register instances with the load balancer in one or more Availability Zones. The load balancer serves as a single point of contact for clients. This enables you to increase the availability of your application. You can add and remove EC2 instances from your load balancer as your needs change, without disrupting the overall flow of information.

Reference:

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

QUESTION NO: 387

Which of the following programming languages is not supported by Amazon's Elastic Beanstalk?

A.
Ruby

B.
Java

C.
Node.js

D.
Perl

Answer: D
Explanation:

AWS Elastic Beanstalk web server environment tiers support applications developed in Java,

PHP, .NET, Node.js, Python, and Ruby as well as different container types for each language.

Worker environments are supported for all platforms except .NET.

Reference: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.platforms.html

QUESTION NO: 388

Amazon CloudFront is a _____.

A.
persistent block level storage volume

B.
content delivery network service

C.
fully managed desktop computing service in the cloud

D.
task coordination and state management service for cloud applications

Answer: B
Explanation:

Amazon CloudFront is a content delivery network (CDN) service. It integrates with other Amazon Web Services to give developers and businesses an easy way to distribute content to end users with low latency, high data transfer speeds, and no minimum usage commitments.

Reference: http://aws.amazon.com/cloudfront/

QUESTION NO: 389

In EC2, what happens to the data in an instance store if an instance reboots (either intentionally or unintentionally)?

A.
Data is partially present in the instance store.

B.
Data persists in the instance store.

C.
Data is deleted from the instance store for security reasons.

D.
Data in the instance store will be lost.

Answer: B
Explanation:

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data on instance store volumes is lost under the following circumstances.

Failure of an underlying drive

The instance is stopped

Terminating an instance

Reference:

http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/InstanceStorage.html

QUESTION NO: 390

What does Amazon EC2 provide?

A.
A platform to run code (Java, PHP, Python), paying on an hourly basis

B.
A physical computing environment

C.
Virtual Server Hosting

D.
Domain Name System (DNS)

Answer: C
Explanation:

Amazon EC2 provides Virtual Server Hosting.

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

QUESTION NO: 391

What does RRS stand, in the context of S3 services?

A.
Regional Rights Storage

B.
Relational Rights Storage

C.
Regional Rights Standard

D.
Reduced Redundancy Storage

Answer: D
Explanation:

In Amazon S3, RRS stands for Reduced Redundancy Storage. Reduced redundancy storage stores objects on multiple devices across multiple facilities, providing 400 times the durability of a typical disk drive, but it does not replicate objects as many times as Amazon S3 standard storage. In addition, reduced redundancy storage is designed to sustain the loss of data in a single facility.

Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingRRS.html

QUESTION NO: 392

Which choice is a storage option supported by Amazon EC2?

A.
Amazon SNS store

B.
Amazon Instance Store

C.
Amazon AppStream store

D.
None of these

Answer: B
Explanation:

Amazon EC2 supports the following storage options:

Amazon Elastic Block Store (Amazon EBS)

Amazon EC2 Instance Store

Amazon Simple Storage Service (Amazon S3)

Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION NO: 393

Amazon EC2 provides virtual computing environments known as _____.

A.
instances

B.
volumes

C.
microsystems

D.
servers

Answer: A

Explanation:

Amazon EC2 provides virtual computing environments known as instances. When you launch an

instance, the instance type that you specify determines the hardware of the host computer used for your instance. Each instance type offers different compute, memory, and storage capabilities and are grouped in instance families based on these capabilities. Select an instance type based on the requirements of the application or software that you plan to run on your instance.

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

QUESTION NO: 394

Which of the following services is offered by CloudWatch?

A.
Fixing broken links on the client's instances

B.
Creating IAM users for all services in AWS

C.
Monitoring estimated AWS charges

D.
Balancing the request load between various instances

Answer: C

Explanation:

AWS CloudWatch supports monitoring of the AWS estimated usage charges. You create an Amazon CloudWatch alarm that will monitor your estimated Amazon Web Services (AWS) charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/monitor_estimated_charges_with_cloudwatch.html

QUESTION NO: 395

The fastest way to load 300 TB of data to AWS is _____.

A.
to directly upload all data to S3 over a dedicated 100 Mbps connection

B.
to use AWS Import/Export Snowball

C.
to use VM Import/Export

D.
to zip all the data and then upload to S3

Answer: B

Explanation:

Even with high-speed Internet connections, it can take months to transfer large amounts of data.

For example, 100 terabytes of data will take more than 100 days to transfer over a dedicated 100 Mbps connection. That same transfer can be accomplished in less than one day, plus shipping time, using two Snowball appliances.

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

QUESTION NO: 396

AMIs can be _____.

A.
only private unless created by Amazon

B.
created only by Amazon

C.
created only for Linux instances

D.
public or private

Answer: D

Explanation:

After you create an AMI, you can keep it private so that only you can use it, or you can share it with a specified list of AWS accounts. You can also make your custom AMI public so that the community can use it. Building a safe, secure, usable AMI for public consumption is a fairly straightforward process, if you follow a few simple guidelines.

Reference:

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

QUESTION NO: 397

Can you configure multiple Load Balancers with a single Auto Scaling group?

A.
Yes, you can provide the ELB is configured with Amazon AppStream.

B.
No

C.
Yes

D.
Yes, you can but only if it is configured with Amazon Redshift.

Answer: C

Explanation:

Yes, you can configure more than one load balancer with an autoscaling group. Auto Scaling integrates with Elastic Load Balancing to enable you to attach one or more load balancers to an existing Auto Scaling group. After you attach the load balancer, it automatically registers the instances in the group and distributes incoming traffic across the instances.

Reference:

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

QUESTION NO: 398

A user is sending custom data metrics to CloudWatch. What is the allowed time stamp granularity for each data point published for the custom metric?

A.
1 nanosecond

B.
1 millisecond

C.
1 minute

D.
1 second

Answer: B

Explanation:

The user is allowed to send data up to one-thousandth of a second. CloudWatch aggregates the data by each minute and generates a metric for that.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION NO: 399

When rebalancing, Auto Scaling launches new instances before terminating the old ones, so that rebalancing does not compromise the performance or availability of your application. Because Auto Scaling attempts to launch new instances before terminating the old ones, being at or near the specified maximum capacity could impede or completely halt rebalancing activities. What does Auto Scaling do in order to avoid this problem?

A.
It can temporarily exceed the specified maximum capacity of a group by a 20 percent margin (or by a 2-instance margin, whichever is greater) during a rebalancing activity.

B.
It can add new reserved instances you have defined.

C.
It can temporarily exceed the specified maximum capacity of a group by a 10 percent margin (or by a 1-instance margin, whichever is greater) during a rebalancing activity.

D.
It can temporarily exceed the specified maximum capacity of a group by a 5 percent margin (or by a 1-instance margin, whichever is greater) during a rebalancing activity.

Answer: C
Explanation:

When rebalancing, Auto Scaling launches new instances before terminating the old ones, so that rebalancing does not compromise the performance or availability of your application. Because Auto Scaling attempts to launch new instances before terminating the old ones, being at or near the specified maximum capacity could impede or completely halt rebalancing activities. To avoid this problem, the system can temporarily exceed the specified maximum capacity of a group by a 10 percent margin (or by a 1-instance margin, whichever is greater) during a rebalancing activity.

Reference:

http://docs.aws.amazon.com/autoscaling/latest/userguide/auto-scaling-benefits.html

QUESTION NO: 400

What does the AWS Storage Gateway provide?

A.
It provides data security features by enabling an encrypted data storage on Amazon S3.

B.

It provides an encrypted SSL endpoint for backups in the cloud.

C.
It provides seamless integration with data security features between your on-premises IT environment and the Amazon Web Services (AWS) storage infrastructure.

D.
It provides a backup solution to on-premises Cloud storage.

Answer: C
Explanation:

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the Amazon Web Services (AWS) storage infrastructure.

Reference:

http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

QUESTION NO: 401

By default, how many Elastic IP addresses can you have per region for your EC2 instances?

A.
10

B.
2

C.
20

D.
5

Answer: D
Explanation:

The number of Elastic IP addresses you can have in EC2 per region is 5.

Reference: http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

QUESTION NO: 402

Elasticity is one of the benefits of using Elastic Beanstalk. Which of the following best describes the concept of elasticity?

A.
It is the ability for counting the number of architectural design considerations that are required to develop a console.

B.
It is the streamlining of resource acquisition and release, so that your infrastructure can rapidly scale in and scale out as demand fluctuates.

C.
It is the process of examining the amount of security credentials required to access a data volume.

D.
It is the procedure of estimating the resource cost, so that you can run a specific project on AWS.

Answer: B
Explanation:

Because applications deployed using Elastic Beanstalk run on Amazon cloud resources, you should keep several things in mind when designing your application: scalability, security, persistent storage, fault tolerance, content delivery, software updates and patching, and connectivity. Elasticity is the streamlining of resource acquisition and release, so that your infrastructure can rapidly scale in and scale out as demand fluctuates.

Reference:

http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.concepts.design.html

QUESTION NO: 403

What is an Auto Scaling group?

A.
It is a group of ELBs that are used to add instances from various regions.

B.

It is a logical grouping of EC2 instances that share similar characteristics for scaling and management.

C.
It is a collection of EC2 instance launch parameters with different characteristics for scaling and management.

D.
It is a group of launch configurations for Elastic load balancers in the same region.

Answer: B
Explanation:

An Auto Scaling group contains a collection of EC2 instances that share similar characteristics and are treated as a logical grouping for the purposes of instance scaling and management.

Reference:

http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html

QUESTION NO: 404

Which service is offered by Auto Scaling?

A.
Automatic scaling storage

B.
Automatic scale EC2 capacity

C.
Automatic scale ECS capacity

D.
Automatic scale elastic IP

Answer: B
Explanation:

Auto Scaling is a service that allows users to scale the EC2 resources up or down automatically according to the conditions or by manual intervention. It is a seamless process to scale the EC2

compute units up and down.

Reference: http://aws.amazon.com/autoscaling/

QUESTION NO: 405

Which of the scaling options given below is not supported by Auto Scaling?

A.
All these options are supported by Auto Scaling

B.
Manual scaling

C.
Scaling based on CPU utilization

D.
Scaling based on time

Answer: A
Explanation:

Auto Scaling supports three types of scaling:

Manual scaling

Scaling based on condition (e.g. CPU utilization is up or down, etc.) Scaling based on time (e.g. First day of the quarter, 6 am every day, etc.).

Reference:

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

QUESTION NO: 406

Security groups in Amazon VPC _____.

A.
control incoming traffic only

B.

control both inbound and outbound traffic

C.
control neither incoming nor outgoing traffic

D.
control outgoing traffic only

Answer: B
Explanation:

Security Groups in VPC allow you to specify rules for both outgoing and incoming traffic.

Reference:

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

QUESTION NO: 407

_____ in VPC are stateful where return traffic is automatically allowed, regardless of any rules.

A.
Security groups

B.
Availability Zones

C.
Network ACLs

D.
Geo Redundant Servers

Answer: A
Explanation:

Security groups in VPC are stateful where return traffic is automatically allowed without having to go through the whole evaluation process again. Network ACLs are stateless, meaning return traffic must be explicitly allowed by rules.

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

QUESTION NO: 408

What happens if the instance launched by Auto Scaling becomes unhealthy?

A.
Auto Scaling will terminate the instance and launch a new healthy instance.

B.
Auto Scaling will terminate the instance but not launch a new instance.

C.
The instance cannot become unhealthy.

D.
Auto Scaling will notify the user and the user can update the instance.

Answer: A

Explanation:

Auto Scaling keeps checking the health of the EC2 instances launched by it at regular intervals. If an instance is observed as unhealthy, Auto Scaling will automatically terminate the instance and launch a new healthy instance. Thus, it maintains the number of instances as per the Auto Scaling group configuration.

Reference:

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

QUESTION NO: 409

A user has set the Alarm for the CPU utilization > 50%. Due to an internal process, the current CPU utilization will be 80% for 6 hours. How can the user ensure that the CloudWatch alarm does not perform any action?

A.
The user can disable the alarm using the DisableAlarmActions API.

B.
The user can set CloudWatch in a sleep state using the CLI mon-sleep-alarm-action.

C.
The user can pause the alarm from the console.

D.
The user cannot stop the alarm from performing an action unless the alarm is deleted.

Answer: A
Explanation:

The user can disable or enable the CloudWatch alarm using the DisableAlarmActions and EnableAlarmActions APIs or the mon-disable-alarm-actions and mon-enable-alarm-actions commands.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html

QUESTION NO: 410

A user is sending a custom metric to CloudWatch. If the call to the CloudWatch APIs has different dimensions, but the same metric name, how will CloudWatch treat all the requests?

A.
It will treat each unique combination of dimensions as a separate metric.

B.
It will group all the calls into a single call.

C.
It will overwrite the previous dimension data with the new dimension data.

D.
It will reject the request as there cannot be a separate dimension for a single metric.

Answer: A
Explanation:

A dimension is a key-value pair used to uniquely identify a metric. CloudWatch treats each unique combination of dimensions as a separate metric. Thus, if the user is making 4 calls with the same metric name but a separate dimension, it will create 4 separate metrics.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION NO: 411

A user has enabled the CloudWatch alarm to estimate the usage charges. If the user disables monitoring of the estimated charges but does not delete the billing alert from the AWS account, what will happen?

A.
The user cannot edit the existing billing alarm.

B.
The data collection on estimated charges is stopped.

C.
It is not possible to disable monitoring of the estimated charges.

D.
AWS will stop sending the billing alerts to the user.

Answer: C
Explanation:

To create an alarm on the estimated AWS usage charges, a user must enable monitoring of estimated AWS charges. This enables creating the metric data, which will be used to create a billing alarm. Once the estimated charges monitoring is enabled, the user cannot disable it. The user has to delete the alarms to stop receiving any notifications on billing.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/gs_monitor_estimated_charges_with_cloudwatch.html

QUESTION NO: 412

What does enabling a sticky session with ELB do?

A.
Routes all the requests to a single DNS

B.
Ensures that all requests from the user's session are sent to multiple instances

C.
Binds the user session with a specific instance

D.
Provides a single ELB DNS for each IP address

Answer: C
Explanation:

By default, a load balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance.

Reference:

http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-sticky-sessions.html

QUESTION NO: 413

Which of the following statements is true of an Auto Scaling group?

A.
An Auto Scaling group cannot span multiple regions.

B.
An Auto Scaling group delivers log files within 30 minutes of an API call.

C.
Auto Scaling publishes new log files about every 15 minutes.

D.
An Auto Scaling group cannot be configured to scale automatically.

Answer: A
Explanation:

An Auto Scaling group can contain EC2 instances that come from one or more Availability Zones within the same region. However, an Auto Scaling group cannot span multiple regions.

Reference:

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

QUESTION NO: 414

Which of the following activities is NOT performed by the Auto Scaling policy?

A.
Changing instance types

B.
Scaling up instance counts

C.
Maintaining current instance levels

D.
Scaling down instance counts

Answer: A
Explanation:

Auto Scaling policies can scale up or down based on the user-defined policies, health status checks or schedules. It also performs a health check on the instances, terminates unhealthy instances, and launches healthy instances to maintain the current instance level. Scaling provides you with options, outside of scaling policies, to override attributes from the instance and use the values that you need. For example, you can override the instance type using AWS CLI commands.

Reference:

http://docs.aws.amazon.com/autoscaling/latest/userguide/create-lc-with-instanceID.html

QUESTION NO: 415

Which of the following services is used to monitor the Amazon Web Services resources?

A.
AWS CloudWatch

B.
AWS Cloudfront

C.

AWS Monitor

D.
AWS EC2

Answer: A
Explanation:

AWS CloudWatch is a service used to monitor the AWS resources and the applications running on EC2. It collects and tracks the metrics of various services or applications.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html

QUESTION NO: 416

What is Amazon Import/Export?

A.
A properly configured service role and instance profile

B.
An international shipping division to help you enhance your sales reach

C.
A service that accelerates transferring large amounts of data into and out of AWS using physical storage appliances

D.
A software developed by Amazon to migrate the data from/to your datacenter to AWS

Answer: C
Explanation:

AWS Import/Export accelerates transferring large amounts of data between the AWS cloud and portable storage devices that you mail to us. AWS transfers data directly onto and off of your storage devices using Amazon high-speed internal network.

Reference: http://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisIE.html

QUESTION NO: 417

Which of the choices below best describes what Auto Scaling is well suited for?

A.
only for applications that experience hourly, daily, or weekly variability in usage.

B.
Both for applications that have stable demand patterns and that experience hourly, daily, or weekly variability in usage.

C.
Both for applications that use frameworks and SDKs to enhance its customer relationship.

D.
only for applications with a stable usage pattern but extremely high workload.

Answer: B

Explanation:

Auto Scaling is well suited to both applications that have stable demand patterns and that experience hourly, daily, or weekly variability in usage. Whether the demand is predictable or unpredictable auto scaling can be a good choice. If the demand is predictable and long term you may choose reserved instances. If the demand is unpredictable you may choose on-demand or even spot instance (if you can afford to have an instance lost unexpectedly).

Reference: http://aws.amazon.com/autoscaling/

QUESTION NO: 418

True or False: Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services.

A.
False, you can only import an existing domain using Amazon Route 53.

B.
True, however, it only provides .com domains.

C.
FALSE

D.

TRUE

Answer: D

Explanation:

Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services.

Reference: http://aws.amazon.com/route53/faqs/

QUESTION NO: 419

Which of the following statements is true of Elastic Load Balancing?

A.
It distributes traffic only to instances across different Availability Zones.

B.
It distributes the outgoing traffic across multiple EC2 instances.

C.
It distributes incoming traffic across multiple EC2 instances.

D.
It distributes traffic only to instances across a single Availability Zone.

Answer: C

Explanation:

Elastic Load Balancing automatically distributes incoming traffic across multiple EC2 instances.

You create a load balancer and register instances with the load balancer in one or more Availability Zones. The load balancer serves as a single point of contact for clients.

Reference:

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

QUESTION NO: 420

You are setting up a VPC and you need to set up a public subnet within that VPC. Which following requirement must be met for this subnet to be considered a public subnet?

A.
Subnet's traffic is not routed to an internet gateway but has its traffic routed to a virtual private gateway.

B.
Subnet's traffic is routed to an internet gateway.

C.
Subnet's traffic is not routed to an internet gateway.

D.
None of these answers can be considered a public subnet.

Answer: B

Explanation:

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC: you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings. A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the Internet. If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. If a subnet doesn't have a route to the Internet gateway, the subnet is known as a private subnet. If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway, the subnet is known as a VPN-only subnet.

Reference:

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

QUESTION NO: 421

Which of the following services can receive an alert from CloudWatch?

A.
AWS Elastic Block Store

B.

AWS Relational Database Service

C.
AWS Auto Scaling

D.
AWS Elastic Load Balancing

Answer: C
Explanation:

AWS Auto Scaling and Simple Notification Service (SNS) work in conjunction with CloudWatch.

CloudWatch can send alerts to the AS policy or to the SNS end points.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/related_services.html

QUESTION NO: 422

A user creates an Auto Scaling group from the Amazon AWS Console and assigned a tag with a key of "environment" and a value of "Prod". Can the user assign tags to instances launched in the Auto Scaling group, to organize and manage them?

A.
Yes, this is possible only if the tags are configured at the launch configuration with a maximum length of 300 characters.

B.
Yes

C.
Yes, this is possible only if the tags are in the same AZ and the tag names are uppercase.

D.
No

Answer: B
Explanation:

You can organize and manage your Auto Scaling groups by assigning your own metadata to each group in the form of tags. You specify a key and a value for each tag. A key can be a general category, such as "project", "owner", or "environment", with specific associated values.

By default, the instance will have a tag with the key as "aws:autoscaling:groupName" and the value as the name of the group.

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

QUESTION NO: 423

How many metrics are supported by CloudWatch for Auto Scaling?

A.
8 metrics and 1 dimension

B.
7 metrics and 5 dimension

C.
5 metrics and 1 dimension

D.
1 metric and 5 dimensions

Answer: A
Explanation:

AWS Auto Scaling supports both detailed as well as basic monitoring of the CloudWatch metrics.

Basic monitoring happens every 5 minutes, while detailed monitoring happens every minute. It supports 8 metrics and 1 dimension.

The metrics are:

GroupMinSize

GroupMaxSize

GroupDesiredCapacity

GroupInServiceInstances

GroupPendingInstances

GroupStandbyInstances

GroupTerminatingInstances

GroupTotalInstances

The dimension is AutoScalingGroupName

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

QUESTION NO: 424

A user is aware that a huge download is occurring on his instance. He has already set the Auto Scaling policy to increase the instance count when the network I/O increases beyond a certain limit. How can the user ensure that this temporary event does not result in scaling?

A.
The policy cannot be set on the network I/O

B.
There is no way the user can stop scaling as it is already configured

C.
The network I/O are not affected during data download

D.
He can suspend scaling temporarily

Answer: D
Explanation:

The user may want to stop the automated scaling processes on the Auto Scaling groups either to

perform manual operations or during emergency situations. To perform this, the user can suspend one or more scaling processes at any time. Once it is completed, the user can resume all the suspended processes.

Reference:

http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html

QUESTION NO: 425

In the 'Detailed' monitoring data available for your Amazon EBS volumes, Provisioned IOPS

volumes automatically send _____ minute metrics to Amazon CloudWatch.

A.
4

B.
2

C.
1

D.
5

Answer: C
Explanation:

In the 'Detailed' monitoring data available for your Amazon EBS volumes, Provisioned IOPS volumes automatically send 1-minute metrics to Amazon CloudWatch.

Reference:

http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html

QUESTION NO: 426

Which of the following is true of Amazon CloudWatch?

A.
Amazon CloudWatch monitors Amazon Web Services (AWS) resources and the applications that run on AWS in real-time.

B.
Amazon CloudWatch is a web service that gives businesses an easy and cost effective way to distribute content with low latency and high data transfer speeds.

C.
Amazon CloudWatch runs code without provisioning or managing servers.

D.
None of these are true.

Answer: A

Explanation:

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time.

You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define. For example, you can monitor the CPU usage and disk reads and writes of your Amazon EC2 instances and then use this data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances to save money. In addition to monitoring the built-in metrics that come with AWS, you can monitor your own custom metrics.

With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html

QUESTION NO: 427

What is the minimum duration when setting an alarm on a detailed monitoring metric in CloudWatch?

A.
1 minute

B.
1 day

C.
5 minutes

D.
30 seconds

Answer: A

Explanation:

Statistics represents data aggregation of the metric data values over a specific period of time. The user can specify the start and end times that CloudWatch will use for the data aggregation of the statistics. The starting and ending points can be as close together as 60 seconds or as far apart as two weeks.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html#Metric

QUESTION NO: 428

In the AWS Storage Gateway, using the _____, you can cost-effectively and durably archive backup data in Amazon Glacier.

A.
Gateway-virtual tape library (Gateway-VTL)

B.
Gateway-stored volume

C.
Gateway-cached volume

D.
Volume gateway

Answer: A
Explanation:

In AWS Storage Gateway, using Gateway virtual tape library (VTL), you can cost-effectively and durably store archive and long-term backup data in Amazon Glacier. Gateway-VTL provides virtual tape infrastructure that scales seamlessly with your business needs and eliminates the operational burden of provisioning, scaling and maintaining a physical tape infrastructure.

Reference:

http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

QUESTION NO: 429

What are the benefits of CloudTrail integration with CloudWatch Logs?

A.

It delivers API activity captured by CloudTrail to an S3 bucket.

B.
It doesn't exist

C.
It delivers SDK activity captured by CloudTrail to a CloudWatch Logs log stream.

D.
It delivers API activity captured by CloudTrail to a CloudWatch Logs log stream.

Answer: D
Explanation:

CloudTrail integration with CloudWatch Logs delivers API activity captured by CloudTrail to a CloudWatch Logs log stream in the CloudWatch Logs log group you specify.

Reference: http://aws.amazon.com/cloudtrail/faqs/

QUESTION NO: 430

Security groups in VPC operate at the _____.

A.
data transport layer level

B.
subnet level

C.
instance level

D.
gateway level

Answer: C
Explanation:

You can secure your VPC instances using only security groups. When you launch an instance in

a VPC, you can associate one or more security groups that you've created. The security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

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

QUESTION NO: 431

Network ACLs are _____.

A.
stateful

B.
stateless

C.
asynchronous

D.
synchronous

Answer: B
Explanation:

Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

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

QUESTION NO: 432

Is it possible to publish your own metrics to CloudWatch?

A.
Yes, but only if the data is aggregated.

B.
No, it is not possible.

C.
No, metrics are in-built and cannot be defined explicitly.

D.
Yes, it can be done by using the put-metric-data command.

Answer: D

Explanation:

You can publish your own metrics to CloudWatch using the AWS CLI or an API. You can view statistical graphs of your published metrics with the AWS Management Console. CloudWatch stores data about a metric as a series of data points. Each data point has an associated time stamp. You can even publish an aggregated set of data points called a statistic set.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION NO: 433

Can you use CloudWatch to monitor memory and disk utilization usage for your Amazon EC2 Linux instances?

A.
CloudWatch can only measure memory usage.

B.
CloudWatch can only collect memory and disk usage metrics when an instance is running.

C.
It is possible only on Linux EC2 instances using the CloudWatch Monitoring scripts for Linux.

D.
CloudWatch can only measure disk usage.

Answer: C

Explanation:

Using the Cloudwatch Monitoring scripts for Linux, you can measure memory and disk usage of your Linux EC2 instances.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/mon-scripts.html

QUESTION NO: 434

An Auto Scaling group is running at the desired capacity of 5 instances and receives a trigger from the Cloudwatch Alarm to increase the capacity by 1. The cool down period is 5 minutes.

Cloudwatch sends another trigger after 2 minutes to decrease the desired capacity by 1. What will be the count of instances at the end of 4 minutes?

A.
7

B.
6

C.
4

D.
5

Answer: B
Explanation:

The cool down period is the time difference between the end of one scaling activity (can be start or terminate) and the start of another one (can be start or terminate). During the cool down period, Auto Scaling does not allow the desired capacity of the Auto Scaling group to be changed by any other CloudWatch alarm. Thus, in this case the trigger from the second alarm will have no effect.

Reference:

http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html#healthcheck

QUESTION NO: 435

An instance has enabled basic monitoring only for CloudWatch. What is the minimum time period available for basic monitoring?

A.
60 seconds

B.

360 seconds

C.
300 seconds

D.
240 seconds

Answer: C
Explanation:

When a user is setting up an alarm on the EC2 instance metric, the time period should be equal to or more than the metric frequency. For basic monitoring, the metric is monitored at every 5 minutes (300 seconds).

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API_MetricDatum.html

QUESTION NO: 436

Which of the following statements describes launch configuration in Auto Scaling?

A.
A launch configuration is a template that an Auto Scaling group uses to launch EC2 instances.

B.
A launch configuration is a template that an Auto Scaling group uses to define the max/minimum of instances.

C.
A launch configuration is a template that an Auto Scaling group uses to schedule the scaling activity.

D.
A launch configuration is a template that an Auto Scaling group uses to define the instance count.

Answer: A
Explanation:

A launch configuration represents a template that the Auto Scaling group uses to launch the Amazon EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping.

Reference:

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

QUESTION NO: 437

A user is collecting 1000 records per second. The user wants to send the data to CloudWatch

using a custom namespace. Which of the below mentioned options is recommended for this activity?

A.
Create one csv file of all the data and send a single file to CloudWatch

B.
Aggregate the data with statistics, such as Min, max, Average, Sum and Sample data and send the data to CloudWatch

C.
It is not possible to send all the data in one call. Thus, it should be sent one by one. CloudWatch will aggregate the data automatically

D.
Send all the data values to CloudWatch in a single command by separating them with a comma.

CloudWatch will parse automatically

Answer: B

Explanation:

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

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION NO: 438

Amazon RDS provides Amazon CloudWatch metrics for your DB Instance deployments at no additional charge. You can use the AWS Management Console to view key operational metrics for your DB Instance deployments, including ____.

A.
I/O activity, DB Instance connections, and number of users

B.
DB Engine Version Management

C.
username, I/O activity, and DB Instance connections

D.
compute/memory/storage capacity utilization, I/O activity, and DB Instance connections

Answer: D
Explanation:

Amazon RDS provides Amazon CloudWatch metrics for you DB Instance deployments at no additional charge. You can use the AWS Management Console to view key operational metrics for your DB Instance deployments, including compute/memory/storage capacity utilization, I/O activity, and DB Instance connections.

Reference: https://aws.amazon.com/rds/postgresql/

QUESTION NO: 439

A custom network ACL that you create ____ until you add rules, and is not associated with a subnet until you explicitly associate it with one.

A.
blocks only inbound traffic by default

B.
allows outbound traffic by default

C.
allows all inbound and outbound traffic by default

D.

blocks all inbound and outbound traffic by default

Answer: D

Explanation:

You can create a custom network ACL for your VPC. By default, a network ACL that you create blocks all inbound and outbound traffic until you add rules, and is not associated with a subnet until you explicitly associate it with one.

The default NACL that is created with your VPC allows all inbound and outbound traffic by default.

Reference:

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

QUESTION NO: 440

What does Amazon ELB stand for?

A.
Elastic Load Balancing

B.
Elastic Linux Box

C.
Encrypted Load Balancing

D.
Encrypted Linux Box

Answer: A

Explanation:

Amazon ELB stands for Elastic Load Balancing. Elastic Load Balancing distributes incoming application traffic across multiple EC2 instances, in multiple Availability Zones. This increases the fault tolerance of your applications.

Reference:

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

QUESTION NO: 441

In AWS Storage Gateway, Gateway-cached volumes allow you to retain _____.

A.
a durable and inexpensive offsite backup that you can recover locally

B.
your primary data locally, and asynchronously back up point-in-time snapshots of this data to Amazon S3

C.
your backup application with online access to virtual tapes

D.
low-latency access to your frequently accessed data

Answer: D
Explanation:

You store your data in Amazon S3 and retain a copy of frequently accessed data subsets locally.

Gateway-cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data.

Reference:

http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

QUESTION NO: 442

Which of the following states is not possible for the CloudWatch alarm?

A.
ALERT

B.
ALARM

C.
OK

D.

INSUFFICIENT_DATA

Answer: A

Explanation:

An alarm has three possible states:

OK--The metric is within the defined threshold

ALARM--The metric is outside of the defined threshold

INSUFFICIENT_DATA--The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html

QUESTION NO: 443

What is the default maximum number of VPCs allowed per region?

A.
5

B.
15

C.
100

D.
10

Answer: A

Explanation:

The maximum number of VPCs allowed per region is 5. The limit for Internet gateways per region is directly correlated to this one. Increasing this limit will increase the limit on Internet gateways per region by the same amount.

Reference:

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

QUESTION NO: 444

How often is metric data is sent to CloudWatch when detailed monitoring is enabled on an Amazon EC2 instance?

A.
Every 30 seconds

B.
Every 5 minutes

C.
Every 15 minutes

D.
Every minute

Answer: D
Explanation:

By default, Amazon EC2 metric data is automatically sent to CloudWatch in 5-minute periods.

However, you can, enable detailed monitoring on an Amazon EC2 instance, which sends data to CloudWatch in 1-minute periods

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.html

QUESTION NO: 445

A route table in VPC can be associated with multiple subnets. However, a subnet can be associated with only _____ route table(s) at a time.

A.
four

B.
two

C.
three

D.
one

Answer: D
Explanation:

Every subnet in your VPC must be associated with exactly one route table at a time. However, the same route table can be associated with multiple subnets.

Reference:

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

QUESTION NO: 446

Which of the following statements is NOT true of CloudWatch?

A.
CloudWatch can be accessed using the AWS SDKS.

B.
CloudWatch can be accessed using the AWS console.

C.
CloudWatch can be accessed using CloudWatch API.

D.
CloudWatch can be accessed using the CloudWatch CLI for iOS.

Answer: D
Explanation:

AWS Cloudwatch can be accessed from the Amazon CloudWatch Console, CloudWatch API, AWS CLI and AWS SDKs.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/accessing_cloudwatch.html

QUESTION NO: 447

Which of the following is an incorrect statement about Amazon CloudWatch?

A.
You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications.

B.
You can set CloudWatch alarms to send notifications or automatically make changes to the resources you are monitoring, based on rules that you define.

C.
You can control and monitor all Security Groups and their related rules.

D.
You gain system-wide visibility into resource utilization, application performance, and operational health.

Answer: C
Explanation:

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time.

You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define. For example, you can monitor the CPU usage and disk reads and writes of your Amazon Elastic Compute Cloud (Amazon EC2) instances and then use this data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances to save money. In addition to monitoring the built-in metrics that come with AWS, you can monitor your own custom metrics. With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html

QUESTION NO: 448

Which of the following terms is NOT a key CloudWatch concept?

A.
Namespaces

B.
Units

C.
Time Stamps

D.
Indexes

Answer: D

Explanation:

The terminology and concepts that are central to one's understanding and use of Amazon CloudWatch are as follows: metrics, namespaces, dimensions, timestamps, units, statistics, periods, aggregation, alarms, and regions.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION NO: 449

Network ACLs in a VPC operate at the _____.

A.
TCP level

B.
instance level

C.
subnet level

D.
gateway level

Answer: C

Explanation:

Security Groups in VPC operate at the instance level, providing a way to control the incoming and outgoing instance traffic. In contrast, network ACLs operate at the subnet level, providing a way to control the traffic that flows through the subnets of your VPC.

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

QUESTION NO: 450

Your VPC automatically comes with a modifiable default network ACL, which by default _____.

A.
blocks outbound traffic

B.
allows only inbound traffic

C.
allows all inbound and outbound traffic

D.
blocks all inbound and outbound traffic

Answer: C
Explanation:

Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound traffic.

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

QUESTION NO: 451

What is a placement group in Amazon EC2?

A.
It is a logical grouping of EC2 instances within a single Availability Zone.

B.
It the edge location of your web content.

C.
It is a group used to span multiple Availability Zones.

D.
It is the AWS region where you run the EC2 instance of your web content.

Answer: A
Explanation:

A placement group is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION NO: 452

In which screen does a user select the Availability Zones while configuring Auto Scaling?

A.
Auto Scaling Group Creation

B.
Auto Scaling Instance Creation

C.
Auto Scaling Launch config Creation

D.
Auto Scaling Policy Creation

Answer: A
Explanation:

You can take advantage of the safety and reliability of geographic redundancy by spanning your Auto Scaling group across multiple Availability Zones within a region and then attaching a load balancer to distribute incoming traffic across those Availability Zones. Incoming traffic is distributed equally across all Availability Zones enabled for your load balancer.

Reference:

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

QUESTION NO: 453

Which of the CloudWatch services mentioned below is NOT a part of the AWS free tier?

A.
10 alarms/month

B.
1 million API request/month

C.
10 metrics/month

D.
15 detailed monitoring metrics

Answer: D
Explanation:

CloudWatch provides the basic monitoring metrics (at five-minute frequency), 10 metrics (applicable to detailed monitoring for the Amazon EC2 instances or custom metrics), 10 alarms, and 1 million API requests each month at no additional charge.

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

QUESTION NO: 454

In the context of sending metrics to CloudWatch using Amazon Kinesis, which of the following statements best describes the metric "PutRecord.Latency"?

A.
It is the time taken per PutRecord operation, measured over the specified time period.

B.
It is the number of successful records in a PutRecords operation per Amazon Kinesis stream, measured over the specified time period.

C.
It is the time taken per PutRecords operation to calculate the statistics of the PutRecords operations.

D.
It is the number of successful PutRecord operations per Amazon Kinesis stream, measured over the specified time period.

Answer: A
Explanation:

The metric PutRecord.Latency measures the time taken per PutRecord operation, measured over the specified time period.

Dimensions: StreamName

Statistics: Minimum, Maximum, Average

Units: Milliseconds

Reference:

http://docs.aws.amazon.com/kinesis/latest/dev/monitoring_with_cloudwatch.html

QUESTION NO: 455

Can a user depict CloudWatch metrics such as CPU utilization in % and Network I/O in bytes on a single graph?

A.
No, a user cannot graph two separate metrics on the same graph.

B.
Yes, a user can graph several metrics over time on a single graph.

C.
No, a user cannot plot several metrics on a single graph since the units are different.

D.
Yes, a user can graph multiple metrics on the same graph provided they are of the same instance in the same AZ.

Answer: B

Explanation:

You can graph several metrics over time on the same graph. The user can select metrics across resources and graph them on a single graph. It is not required that they should be of the same instance. They can be of different instances with the same AMI or based on some other dimension. You can filter records and plot them all on the same graph.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/graph_a_metric_all_resources.html

QUESTION NO: 456

Which of the following comes before Auto Scaling group creation?

A.
Creating the Auto Scaling launch config

B.
Creating the Auto Scaling policy

C.
Creating the Auto Scaling tags

D.
Creating the Auto Scaling instance

Answer: A

Explanation:

The Auto Scaling launch config is the first step that should be run before a user can create an Auto Scaling group. The launch config has all the information, such as the instance type, AMI ID, and other instance launch parameters. The Auto Scaling group uses this launch config to create a new group.

Reference:

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

QUESTION NO: 457

A placement group in Amazon EC2 can

A.
place high memory instances in one logical group.

B.
logically name and tag different tiers of the system (DB, application, business logic etc).

C.
isolate any instance-type physically so that groups access local resources.

D.
reduce network latency and increase network throughput

Answer: D

Explanation:

A placement group is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.

Reference: https://aws.amazon.com/ec2/faqs/

QUESTION NO: 458

Which of the following statements is true about Auto Scaling?

A.
You can only delete your Auto Scaling group but not your Auto Scaling setup.

B.
If the Auto Scaling infrastructure is being deleted, it is not mandatory to delete the launch configuration.

C.
You can only delete your Auto Scaling set up but not your Auto Scaling group.

D.
If the Auto Scaling infrastructure is being deleted, it is mandatory to delete the launch

configuration.

Answer: B

Explanation:

You can create an Auto Scaling group to maintain the healthy number of instances at all times, and optionally delete this basic Auto Scaling infrastructure. You can either delete your Auto Scaling set up or delete just your Auto Scaling group and keep your launch configuration to use at a later time.

Reference:

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

QUESTION NO: 459

If you specify only the general endpoint (autoscaling.amazonaws.com), Auto Scaling directs your request to the:

A.
us-west-2 endpoint.

B.
eu-central-1.

C.
eu-west-1 endpoint.

D.
us-east-1 endpoint.

Answer: D

Explanation:

If you just specify the general endpoint (autoscaling.amazonaws.com), Auto Scaling directs your request to the us-east-1 endpoint.

Reference: http://docs.aws.amazon.com/general/latest/gr/rande.html

QUESTION NO: 460

A user has configured ELB with Auto Scaling. The user temporarily suspended the Auto Scaling terminate process. What might the Availability Zone Rebalancing process (AZRebalance) consequently cause during this period?

A.
Auto Scaling will keep launching instances in all AZs until the maximum instance number is reached.

B.
AZ Rebalancing might now allow Auto Scaling to launch or terminate any instances.

C.
AZ Rebalancing might allow the number instances in an Availability Zone to remain higher than the maximum size

D.
It is not possible to suspend the terminate process while keeping the launch active.

Answer: C

Explanation:

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

Reference:

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

QUESTION NO: 461

What is Amazon CloudFront?

A.
A global Content Delivery Network

B.
An encrypted endpoint to upload files to the Cloud

C.
A web service to schedule regular data movement

D.
A development front-end to Amazon Web Services

Answer: A
Explanation:

Amazon CloudFront is a global content delivery network (CDN) service that accelerates delivery of your websites, APIs, video content or other web assets through CDN caching. It integrates with other Amazon Web Services products to give developers and businesses an easy way to accelerate content to end users with no minimum usage commitments.

Reference: https://aws.amazon.com/cloudfront/

QUESTION NO: 462

You can create a CloudWatch alarm that watches a single metric. The alarm performs one or more actions based on the value of the metric relative to a threshold over a number of time periods. Which of the following states is possible for the CloudWatch alarm?

A.
OK

B.
ALERT

C.
THRESHOLD

D.
ERROR

Answer: A
Explanation:

You can create a CloudWatch alarm that watches a single metric. The alarm performs one or more actions based on the value of the metric relative to a threshold over a number of time periods. The action can be an Amazon EC2 action, an Auto Scaling action, or a notification sent to an Amazon SNS topic.

An alarm has three possible states:

OK--The metric is within the defined threshold

ALARM--The metric is outside of the defined threshold

INSUFFICIENT_DATA--The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html

QUESTION NO: 463

A user has enabled instance protection for his Auto Scaling group that has spot instances. If Auto Scaling wants to terminate an instance in this Auto Scaling group due to a CloudWatch trigger unrelated to bid price, what will happen?

A.
Auto Scaling will notify the user for the next action

B.
Auto Scaling will remove the instance from the Auto Scaling Group

C.
Auto Scaling overwrites the instance termination attribute and terminates the instances

D.
The EC2 instance will not be terminated since instance protection from scale-in is enabled.

Answer: D

Explanation:

Auto Scaling protects instances from termination during scale-in events. This means that Auto Scaling instance protection will receive the CloudWatch trigger to delete instances, and delete instances in the Auto Scaling group that do not have instance protection enabled. However, instance protection won't protect Spot instance termination triggered due to market price exceeding bid price.

Reference:

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

QUESTION NO: 464

In a hardware security module (HSM), what is the function of a Transparent Data Encryption (TDE)?

A.
To reduce the risk of confidential data theft

B.
To decrease latency

C.
To store SSL certificates

D.
To provide backup

Answer: A
Explanation:

In a hardware security module (HSM), Transparent Data Encryption (TDE) reduces the risk of confidential data theft by encrypting sensitive data.

Reference:

http://docs.aws.amazon.com/cloudhsm/latest/userguide/cloud-hsm-third-party-apps.html

QUESTION NO: 465

In IAM, a policy has to include the information about who (user) is allowed to access the resource, known as the _____.

A.
permission

B.
role

C.
license

D.
principal

Answer: D

Explanation:

To specify resource-based permissions, you can attach a policy to the resource, such as an Amazon SNS topic, an Amazon S3 bucket, or an Amazon Glacier vault. In that case, the policy has to include information about who is allowed to access the resource, known as the principal. (For user-based policies, the principal is the IAM user that the policy is attached to, or the user who gets the policy from a group.)

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

QUESTION NO: 466

Amazon S3 provides a number of security features for protection of data at rest, which you can use or not, depending on your threat profile. What feature of S3 allows you to create and manage your own encryption keys for sending data?

A.
Client-side Encryption

B.
Network traffic protection

C.
Data integrity compromise

D.
Server-side Encryption

Answer: A

Explanation:

With client-side encryption you create and manage your own encryption keys. Keys you create are not exported to AWS in clear text. Your applications encrypt data before submitting it to Amazon S3, and decrypt data after receiving it from Amazon S3. Data is stored in an encrypted form, with keys and algorithms only known to you. While you can use any encryption algorithm, and either symmetric or asymmetric keys to encrypt the data, the AWS-provided Java SDK offers Amazon S3 client-side encryption features.

Reference: https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf

QUESTION NO: 467

In AWS KMS, which of the following is NOT a mode of server-side encryption that you can use to protect data at rest in Amazon S3?

A.
SSE-S3

B.
SSE-K

C.
SSE-C

D.
SSE-KMS

Answer: B
Explanation:

You can protect data at rest in Amazon S3 by using three different modes of server-side encryption: SSE-S3, SSE-C, or SSE-KMS.

Reference: http://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

QUESTION NO: 468

AWS Cloud Hardware Security Modules (HSMs) are designed to _____.

A.
store your AWS keys safely

B.
provide another level of login security specifically for LDAP

C.
allow AWS to audit your infrastructure

D.
securely store cryptographic key material and use the key material without exposing it outside the cryptographic boundary of the appliance

Answer: D

Explanation:

A Hardware Security Module (HSM) is a hardware appliance that provides secure key storage and cryptographic operations within a tamper-resistant hardware device. They are designed to securely store cryptographic key material and also to be able to use this key material without exposing it outside the cryptographic boundary of the appliance.

Reference: https://aws.amazon.com/cloudhsm/faqs/

QUESTION NO: 469

Which of the following statements is true of IAM?

A.
If you are configuring MFA for a user who will use a smartphone to generate an OTP, you must have the smartphone available in order to finish the wizard.

B.
If you are configuring MFA for a user who will use a smartphone to generate an OTP, the smartphone is not required in order to finish the wizard.

C.
If you are configuring MFA for a user who will use a smartphone to generate an OTP, you can finish the wizard on any device and later use the smartphone for authentication.

D.
None of these are correct.

Answer: A

Explanation:

MFA can be used either with a specific MFA-enabled device or by installing an application on a smartphone. If a user chooses to use her smartphone, physical access to the device is required in order to complete the configuration wizard.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/GenerateMFAConfig.html

QUESTION NO: 470

Could you use IAM to grant access to Amazon DynamoDB resources and API actions?

A.
In DynamoDB there is no need to grant access

B.
Depended to the type of access

C.
No

D.
Yes

Answer: D

Explanation:

Amazon DynamoDB integrates with AWS Identity and Access Management (IAM). You can use AWS IAM to grant access to Amazon DynamoDB resources and API actions. To do this, you first write an AWS IAM policy, which is a document that explicitly lists the permissions you want to grant. You then attach that policy to an AWS IAM user or role.

Reference:

http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/UsingIAMWithDDB.html

QUESTION NO: 471

A user is planning to schedule a backup for an existing EBS volume. The user wants the backup to be created through snapshot, and for it to be encrypted. How can the user achieve data encryption with a snapshot?

A.
Encrypt the existing EBS volumes so that the snapshot will be encrypted by AWS when it is created

B.
By default the snapshot is encrypted by AWS

C.
While creating a snapshot select the snapshot with encryption

D.
Enable server side encryption for the snapshot using S3

Answer: A

Explanation:

AWS EBS supports encryption of the volume. It also supports creating volumes from existing snapshots provided the snapshots are created from encrypted volumes. The data at rest, the I/O as well as all the snapshots of the encrypted EBS will also be encrypted. EBS encryption is based on the AES-256 cryptographic algorithm, which is the industry standard.

Reference:

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

QUESTION NO: 472

What does the Server-side encryption provide in Amazon S3?

A.
Server-side encryption doesn't exist for Amazon S3, but only for Amazon EC2.

B.
Server-side encryption protects data at rest using Amazon S3-managed encryption keys (SSE-S3).

C.
Server-side encryption provides an encrypted virtual disk in the cloud.

D.
Server-side encryption allows to upload files using an SSL endpoint for a secure transfer.

Answer: B

Explanation:

Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.

Reference:

http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html

QUESTION NO: 473

The Statement element, of an AWS IAM policy, contains an array of individual statements. Each individual statement is a(n) _____ block enclosed in braces { }.

A.
JSON

B.
AJAX

C.
JavaScript

D.
jQuery

Answer: A

Explanation:

The Statement element, of an IAM policy, contains an array of individual statements. Each individual statement is a JSON block enclosed in braces { }.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

QUESTION NO: 474

You need to set up security for your VPC and you know that Amazon VPC provides two features that you can use to increase security for your VPC: Security groups and network access control lists (ACLs). You start to look into security groups first. Which statement below is incorrect in relation to security groups?

A.
Are stateful: Return traffic is automatically allowed, regardless of any rules.

B.
Support addition of individual allow and deny rules in both inbound and outbound.

C.
Security Groups can be added or removed from EC2 instances in a VPC at any time.

D.
Evaluate all rules before deciding whether to allow traffic.

Answer: B
Explanation:

Amazon VPC provides two features that you can use to increase security for your VPC:

Security groups--Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level and supports allow rules only.

Network access control lists (ACLs)--Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level and supports allow rules and deny rules.

Reference:

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

QUESTION NO: 475

What does Amazon IAM stand for?

A.
Amazon Identity and Authentication Mechanism

B.
Amazon Integrated Access Management

C.
Amazon Identity and Access Management

D.
None of these

Answer: C
Explanation:

Amazon IAM stands for Amazon Identity and Access Management. The "identity" aspect of AWS IAM helps you with the question "Who is that user?", often referred to as authentication.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_identity-management.html#intro-identity-users

QUESTION NO: 476

Can you use the AWS Identity and Access Management (IAM) to assign permissions determining who can manage or modify RDS resources?

A.
No, AWS IAM is used only to assign IDs to AWS users.

B.
No, this permission cannot be assigned by AWS IAM.

C.
Yes, you can.

D.
No, AWS IAM is used only to assign activities.

Answer: C
Explanation:

Use AWS Identity and Access Management (IAM) policies to assign permissions that determine who is allowed to manage RDS resources. For example, you can use IAM to determine who is allowed to create, describe, modify, and delete DB instances, tag resources, or modify DB security groups.

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

QUESTION NO: 477

You have been asked to design a layered security solution for protecting your organization's network infrastructure. You research several options and decide to deploy a network-level security control appliance, inline, where traffic is intercepted and analyzed prior to being forwarded to its final destination, such as an application server. Which of the following is NOT considered an inline threat protection technology?

A.
Intrusion prevention systems

B.
Third-party firewall devices installed on Amazon EC2 instances

C.
Data loss management gateways

D.
Augmented security groups with Network ACLs

Answer: D
Explanation:

Many organizations consider layered security to be a best practice for protecting network infrastructure. In the cloud, you can use a combination of Amazon VPC, implicit firewall rules at the hypervisor-layer, alongside network access control lists, security groups, host-based firewalls, and IDS/IPS systems to create a layered solution for network security. While security groups, NACLs and host-based firewalls meet the needs of many customers, if you're looking for defense in-depth, you should deploy a network-level security control appliance, and you should do so inline, where traffic is intercepted and analyzed prior to being forwarded to its final destination, such as an application server.

Examples of inline threat protection technologies include the following:

Third-party firewall devices installed on Amazon EC2 instances (also known as soft blades)

Unified threat management (UTM) gateways

Intrusion prevention systems

Data loss management gateways

Anomaly detection gateways

Advanced persistent threat detection gateways

Reference: https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf

QUESTION NO: 478

Is it possible to protect the connections between your application servers and your MySQL instances using SSL encryption?

A.
Yes, it is possible but only in certain regions.

B.
Yes

C.
No

D.
Yes, it is possible but only in VPC.

Answer: B

Explanation:

To further enhance the security of your infrastructure, AWS allows you to SSL encrypt the communications between your EC2 instances and your MySQL instances. Amazon RDS generates an SSL certificate for each DB Instance. Once an encrypted connection is established, data transferred between the DB Instance and your application will be encrypted during transfer.

Reference: http://aws.amazon.com/rds/faqs/#53

QUESTION NO: 479

You need to determine what encryption operations were taken with which key in AWS KMS to either encrypt or decrypt data in the AWS CodeCommit repository. Which of the following actions will best help you accomplish this?

A.
Searching for the AWS CodeCommit repository ID in AWS CloudTrail logs

B.
Searching for the encryption key ID in AWS CloudTrail logs

C.
Searching for the AWS CodeCommit repository ID in AWS CloudWatch

D.
Searching for the encryption key ID in AWS CloudWatch

Answer: A

Explanation:

The encryption context is additional authenticated information AWS KMS uses to check for data integrity. When specified for the encryption operation, it must also be specified in the decryption operation or decryption will fail. AWS CodeCommit uses the AWS CodeCommit repository ID for the encryption context. You can find the repository ID by using the get-repository command or by viewing repository details in the AWS CodeCommit console. Search for the AWS CodeCommit repository ID in AWS CloudTrail logs to understand which encryption operations were taken on

which key in AWS KMS to encrypt or decrypt data in the AWS CodeCommit repository.

Reference: http://docs.aws.amazon.com/codecommit/latest/userguide/encryption.html

QUESTION NO: 480

The AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon EBS, Amazon S3, Amazon Redshift, Elastic Transcoder, Amazon WorkMail, and Amazon RDS to make it simple to encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide you with key usage logs to help meet your regulatory and compliance needs. Which of the following types of cryptography keys is supported by AWS KMS currently?

A.
Private ephemeral key agreement cryptography

B.
Symmetric and asymmetric random number generation key cryptography

C.
Asymmetric key cryptography and symmetric key cryptography

D.
Only symmetric key cryptography

Answer: D

Explanation:

The AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon EBS, Amazon S3, Amazon Redshift, Elastic Transcoder, Amazon WorkMail, and Amazon RDS to make it simple to encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide you with key usage logs to help meet your regulatory and compliance needs. AWS KMS currently supports only symmetric (private) key cryptography.

Reference: http://docs.aws.amazon.com/kms/latest/developerguide/crypto-intro.html

QUESTION NO: 481

Your customers are concerned about the security of their sensitive data and their inquiry asks about what happens to old storage devices on AWS. What would be the best answer to this question?

A.
AWS uses a 3rd party security organization to destroy data as part of the decommissioning process.

B.
AWS uses the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process.

C.
AWS reformats the disks and uses them again.

D.
AWS uses their own proprietary software to destroy data as part of the decommissioning process.

Answer: B

Explanation:

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.

AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process.

All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Reference: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

QUESTION NO: 482

In AWS Identity and Access Management (IAM), you can make use of the _____ APIs to grant users temporary access to your resources.

A.
AWS Security Transport Service (STS)

B.
AWS Security Tree Service (STS)

C.
AWS Security Task Service (STS)

D.
AWS Security Token Service (STS)

Answer: D
Explanation:

AWS Security Token Service enables the creation of temporary credentials that can be used along with IAM in order to grant access to trusted entities and users to your AWS resources for a predefined amount of time.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

QUESTION NO: 483

An IAM user has two conflicting policies as part of two separate groups. One policy allows him to access an S3 bucket, while another policy denies him the access. Can the user access that bucket?

A.
Yes, always

B.
No

C.
Yes, provided he accesses with the group which has S3 access

D.
Yes, but just read only access of the bucket

Answer: B
Explanation:

When a request is made, the AWS IAM policy decides whether a given request should be allowed or denied. The evaluation logic follows these rules:

By default, all requests are denied. (In general, requests made using the account credentials for resources in the account are always allowed.)

An explicit allow policy overrides this default.

An explicit deny policy overrides any allows.

In this case since there is an explicit deny policy, it will over ride everything and the request will be denied.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html

QUESTION NO: 484

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants a particular group of IAM users to access only the test instances and not the production ones. They want to deploy the instances in various locations based on the factors that will change from time to time, especially in the test group. They expect instances will often need to be churned, i.e. deleted and replaced, especially in the testing group. This means the five instances they have created now will soon be replaced by a different set of five instances. The members of each group, production and testing, will not change in the foreseeable future. Given the situation, what choice below is the most efficient and time-saving strategy to define the IAM policy?

A.
By creating an IAM policy with a condition that allows access to only small instances

B.
By defining the IAM policy that allows access based on the instance ID

C.
By launching the test and production instances in separate regions and allowing region wise access to the group

D.
By defining the tags on the test and production team members IAM user IDs, and adding a condition to the IAM policy that allows access to specific tags

Answer: D

Explanation:

AWS Identity and Access Management is a web service that allows organizations to manage users and user permissions for various AWS services. The user can add conditions as a part of the IAM policies. The condition can be set on AWS Tags, Time, and Client IP as well as on various parameters. If the organization wants the user to access only specific instances, he should define proper tags and add to the IAM policy condition. The sample policy is shown below.

```
"Statement": [
{
"Action": "ec2:*",
"Effect": "All
ow",
"Resource": "*",
"Condition": {
"StringEquals": {
"ec2:ResourceTag/InstanceType": "Production"
}
}
}
]
```

BrainDumps

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/ExampleIAMPolicies.html

QUESTION NO: 485

For IAM user, a virtual Multi-Factor Authentication (MFA) device uses an application that generates _____-digit authentication codes that are compatible with the time-based one-time password (TOTP) standard.

A.
three

B.
four

C.
six

D.
five

Answer: C
Explanation:

A virtual MFA device uses an application that generates six-digit authentication codes that are compatible with the time-based one-time password (TOTP) standard. Therefore, any application that you wish to use in order to make your smart phone your virtual MFA device needs to conform with the standard.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html

QUESTION NO: 486

The _____ IAM policy element describes the specific action or actions that will be allowed or denied.

A.
Principal

B.
Action

C.
Vendor

D.
Not Principal

Answer: B
Explanation:

The Action element describes the specific action or actions that will be allowed or denied.

Statements must include either an Action or NotAction element. Each AWS service has its own set of actions that describe tasks that you can perform with that service.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

QUESTION NO: 487

A company wants to review the security requirements of Glacier. Which of the below mentioned statements is true with respect to the AWS Glacier data security?

A.
The user can set the serverside encryption flag to encrypt the data stored on Glacier.

B.
All data stored on Glacier is protected with AES-256 server-side encryption.

C.
All data stored on Glacier is protected with AES-128 server-side encryption.

D.
The data stored on Glacier is not encrypted by default.

Answer: B

Explanation:

For Amazon Web Services, all the data stored on Amazon Glacier is protected using serverside encryption. AWS generates separate unique encryption keys for each Amazon Glacier archive, and encrypts it using AES-256. The encryption key then encrypts itself using AES-256 with a master key that is stored in a secure location.

Reference: https://aws.amazon.com/glacier/faqs/

QUESTION NO: 488

A user has configured two security groups which allow traffic as given below:

1: SecGrp1:

Inbound on port 80 for 0.0.0.0/0

Inbound on port 22 for 0.0.0.0/0

2: SecGrp2:

Inbound on port 22 for 10.10.10.1/32

If both the security groups are associated with the same instance, which of the below mentioned statements is true?

A.
It is not possible to have more than one security group assigned to a single instance

B.
It allows inbound traffic for everyone on both ports 22 and 80

C.
It is not possible to create the security group with conflicting rules. AWS will reject the request

D.
It allows inbound traffic on port 22 for IP 10.10.10.1 and for everyone else on port 80

Answer: B

Explanation:

A user can attach more than one security group to a single EC2 instance. In this case, the rules from each security group are effectively aggregated to create one set of rules. AWS uses this set of rules to determine whether to allow access or not. Thus, here the rule for port 22 with IP 10.10.10.1/32 will merge with IP 0.0.0.0/0 and open ports 22 and 80 for all.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION NO: 489

Is it possible to create an S3 bucket accessible only by a certain IAM user using policies in a CloudFormation template?

A.
Yes, all these resources can be created using a CloudFormation template

B.
S3 is not supported by CloudFormation.

C.
No, you can only create the S3 bucket but not the IAM user.

D.
No, in the same template you can only create the S3 bucket and the relative policy.

Answer: A

Explanation:

With AWS Identity and Access Management (IAM), you can create IAM users to control who has access to which resources in your AWS account. You can use IAM with AWS CloudFormation to control what AWS CloudFormation actions users can perform, such as view stack templates, create stacks, or delete stacks.

In addition to AWS CloudFormation actions, you can manage what AWS services and resources are available to each user.

Reference:

http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-template.html

QUESTION NO: 490

In Amazon CloudFront, if you have chosen On for Logging, the access logs are stored in _____.

A.
Amazon S3 bucket.

B.
Amazon EBS.

C.
Amazon Edge locations.

D.
Amazon EC2 instance.

Answer: A
Explanation:

In Amazon CloudFront, if you chose On for Logging, the logs store in the Amazon S3 bucket that you want CloudFront to store access logs in. For example:

myawslogbucket.s3.amazonaws.com

If you enable logging, CloudFront records information about each end-user request for an object and stores the files in the specified Amazon S3 bucket.

Reference:

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesLoggingOnOff

QUESTION NO: 491

Does Amazon RDS support SSL encryption for SQL Server DB Instances?

A.
Yes, for all supported SQL Server editions

B.
No

C.
Yes, but only when the instances are in a single region

D.
No, encryption using SSL is supported only in the GovCloud.

Answer: A
Explanation:

Amazon RDS supports SSL encryption for SQL Server DB Instances. Using SSL, you can encrypt connections between your applications and your SQL Server DB Instances. This is available for all the versions of Microsoft SQL Server.

Reference:

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.DBEngine.SQLServer.html

QUESTION NO: 492

Amazon Cognito supports web identity federation through _____.

A.
custom sign-in code or own user identities

B.
Facebook, Google, and Amazon

C.
a configuration check for rules that deny access to specific ports

D.
an AWS user group

Answer: B
Explanation:

Amazon Cognito supports developer authenticated identities, in addition to web identity federation through Facebook, Google, and Amazon.

Reference:

http://docs.aws.amazon.com/cognito/devguide/identity/developer-authenticated-identities/

QUESTION NO: 493

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

A.
The user should create an IAM user with permissions to access DynamoDB and use its credentials within the application for connecting to DynamoDB

B.
The user should create an IAM user with DynamoDB and EC2 permissions. Attach the user with the application so that it does not use the root account credentials

C.
The user should attach an IAM role to the EC2 instance with necessary permissions for making API calls to DynamoDB.

D.
The user should create an IAM role with EC2 permissions to deploy the 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. Instead, the user should use roles for EC2 and give that role access to DynamoDB /S3. When the roles are attached to EC2, it will give temporary security credentials to the application hosted on that EC2, to connect with DynamoDB / S3.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_WorkingWithGroupsAndUsers.html

QUESTION NO: 494

A user is trying to create a list of IAM users with the AWS console. When the IAM users are created which of the below mentioned credentials will be enabled by default for the user?

A.
IAM X.509 certificates

B.
Nothing. Everything is disabled by default

C.
IAM passwords

D.
IAM access key and secret access key

Answer: B

Explanation:

Newly created IAM users have no password and no access key (access key ID and secret access key). If the user needs to administer your AWS resources using the AWS Management Console, you can create a password for the user. If the user needs to interact with AWS programmatically (using the command line interface (CLI), the AWS SDK, or service-specific APIs), you can create an access key for that user. The credentials you create for users are what they use to uniquely identify themselves to AWS.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_WorkingWithGroupsAndUsers.html

QUESTION NO: 495

You are setting up security groups for both incoming traffic and outgoing traffic in your VPC network on the AWS CLI. Which of the following AWS CLI commands would you use for adding one or more incoming traffic rules to a security group?

A.
authorize-security-group-egress

B.
authorize-security-group-ingress

C.
Grant-EC2SecurityGroupOutgress

D.
Get-EC2SecurityGroup

Answer: B

Explanation:

When setting up security groups for incoming traffic in your VPC network, to add one or more ingress (incoming traffic) rules to a security group. authorize-security-group-ingress (AWS CLI). ec2-authorize (Amazon EC2 CLI). Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell) In computer networking, ingress filtering is a technique used to make sure that incoming packets are actually from the networks that they claim to be from. In computer networking, egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically, it is information from a private TCP/IP computer network to the Internet that is controlled.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION NO: 496

The IAM entity "AWS Account" is similar to:

A.
The Unix concept of root or superuser

B.
The Unix concept of a non privilege user

C.
The Unix concept of guest user

D.
The primary billing entity

Answer: A

Explanation:

In IAM the AWS Account is the role with most important permissions. It's equivalent to the root account in a UNIX environment.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html

QUESTION NO: 497

AWS KMS (Key Management Service) uses symmetric key cryptography to perform encryption and decryption. Symmetric key cryptography uses the same algorithm and key to both encrypt and decrypt digital data. The unencrypted data is typically called plaintext whether it is text or not, and the encrypted data is typically called _____.

A.
ciphertext

B.
symtext

C.
encryptext

D.
cryptext

Answer: A
Explanation:

Encryption and Decryption

AWS KMS uses symmetric key cryptography to perform encryption and decryption. Symmetric key cryptography uses the same algorithm and key to both encrypt and decrypt digital data. The Unencrypted data is typically called plaintext whether it is text or not. The encrypted data is typically called ciphertext.

Reference: http://docs.aws.amazon.com/kms/latest/developerguide/crypto_overview.html

QUESTION NO: 498

Bob is an IAM user who has access to the EC2 services. Admin is an IAM user who has access to all the AWS services including IAM. Can Bob change his own password?

A.

No, the IAM user can never change the password

B.
Yes, only from AWS CLI

C.
Yes, only from the AWS console

D.
Yes, provided Admin has given Bob access to change his own password

Answer: D
Explanation:

The IAM users by default cannot change their password. The root owner or IAM administrator needs to set the policy in the password policy page, which should allow the user to change their password. Once it is enabled, the IAM user can always change their own passwords from the AWS console or CLI.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_ManagingUserPwdSelf.html

QUESTION NO: 499

ABC has three AWS accounts. They have created separate IAM users within each account.

ABC wants a single IAM login URL such as https://abc.signin.aws.amazon.com/console/ for use by IAM users in all three accounts.

How can this be achieved?

A.
Merge all the accounts with consolidated billing

B.
Create the S3 bucket with an alias name and use the redirect rule to forward requests to various accounts

C.
Create the same account alias with each account ID

D.
It is not possible to have the same IAM account login URL for separate AWS accounts

Answer: D

Explanation:

Users can create an alias for they accounts, but the alias should be unique to the account. For example, the alias "abc" can be assigned to only one account. If a user wants the URL of the AWS IAM sign-in page to have a company name instead of the AWS account ID, he can create an alias for his AWS account ID.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/AccountAlias.html

QUESTION NO: 500

Which of the following Identity and Access Management (IAM) policy keys of AWS Direct Connect is used for date/time conditions?

A.
aws:CurrentTime

B.
aws:UserAgent

C.
aws:SourceIp

D.
aws:SecureTransport

Answer: A

Explanation:

AWS Direct Connect implements the following policy keys of Identity and Access Management:

aws:CurrentTime (for date/time conditions)

aws:EpochTime (the date in epoch or UNIX time, for use with date/time conditions)

aws:SecureTransport (Boolean representing whether the request was sent using SSL)

aws:SourceIp (the requester's IP address, for use with IP address conditions) aws:UserAgent (information about the requester's client application, for use with string conditions)

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html

QUESTION NO: 501

In the context of AWS Security Best Practices for RDS, if you require encryption or data integrity authentication of data at rest for compliance or other purposes, you can add protection at the _____ using SQL cryptographic functions.

A.
physical layer

B.
security layer

C.
application layer

D.
data-link layer

Answer: C
Explanation:

Amazon RDS leverages the same secure infrastructure as Amazon EC2. You can use the Amazon RDS service without additional protection, but if you require encryption or data integrity authentication of data at rest for compliance or other purposes, you can add protection at the application layer, or at the platform layer using SQL cryptographic functions.

Reference:

https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf

QUESTION NO: 502

A root AWS account owner has created three IAM users: Bob, John and Michael. Michael is the IAM administrator. Bob and John are not the super users, but users with some pre-defined policies. John does not have access to modify his password. Thus, he asks Bob to change his password. How can Bob change John's password?

A.
This statement is false. Only Michael can change the password for John

B.
This is possible if Michael can add Bob to a group which has permissions to modify the IAM passwords

C.
It is not possible for John to modify his password

D.
Provided Bob is the manager of John

Answer: B

Explanation:

Generally, with IAM users, the password can be modified in two ways. The first option is to define the IAM level policy which allows each user to modify their own passwords. The other option is to create a group and create a policy for the group which can change the passwords of various IAM users.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/HowToPwdIAMUser.html

QUESTION NO: 503

You know that AWS Billing and Cost Management integrates with the AWS Identity and Access Management (IAM) service so that you can control who in your organization has access to specific pages on the AWS Billing and Cost Management console. Which of the following items can you control access to in AWS Billing and Cost Management?

A.
You can control access to payment methods only.

B.
You can control access to invoices only.

C.
You can control access to invoices and detailed information about charges and account activity, budgets, payment methods, and credits.

D.
You can control access to detailed information about charges and account activity only.

Answer: C

Explanation:

In AWS Billing and Cost Management console, you can control access to the following:

- invoices

- detailed information about charges

- account activity

- budgets

- payment methods

- credits

Reference:

http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/control-access-billing.html

QUESTION NO: 504

What does Amazon IAM provide?

A.
A mechanism to authorize Internet Access Modularity (IAM)

B.
A mechanism to authenticate users when accessing Amazon Web Services

C.
A mechanism to integrate on-premises authentication protocols with the Cloud

D.
None of the above

Answer: B
Explanation:

Amazon IAM provides a mechanism to authenticate users when accessing Amazon Web Services.

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_WorkingWithGroupsAndUsers.html

QUESTION NO: 505

An IAM group is a:

A.
group of EC2 machines that gain the permissions specified in the group.

B.
collection of IAM users.

C.
guide for IAM users.

D.
collection of AWS accounts.

Answer: B
Explanation:

Within the IAM service, a group is regarded as a collection of users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_WorkingWithGroupsAndUsers.html

QUESTION NO: 506

A group in IAM can contain many users. Can a user belong to multiple groups?

A.
Yes, a user can be a member of up to 150 groups.

B.
Yes, a user can be a member of up to 50 groups.

C.
Yes, a user can be a member of up to 100 groups.

D.
Yes, a user can be a member of up to 10 groups.

Answer: D
Explanation:

In Amazon IAM, a user can belong to up to 10 different groups.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

QUESTION NO: 507

Fill in the blanks: One of the basic characteristics of security groups for your VPC is that you _____ .

A.
can specify allow rules as well as deny rules

B.
can neither specify allow rules nor deny rules

C.
can specify allow rules, but not deny rules

D.
can specify deny rules, but not allow rules

Answer: C
Explanation:

Security Groups in VPC allow you to specify rules with reference to the protocols and ports through which communications with your instances can be established. One such rule is that you can specify allow rules, but not deny rules.

Reference:

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

QUESTION NO: 508

You can configure Amazon CloudFront to deliver access logs per _____ to an Amazon S3 bucket of your choice.

A.
Edge location

B.
Distribution

C.
Geo restriction

D.
Request

Answer: B
Explanation:

If you use a custom origin, you will need to create an Amazon S3 bucket to store your log files in. You can enable CloudFront to deliver access logs per distribution to an Amazon S3 bucket of your choice.

Reference:

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

QUESTION NO: 509

ABC (with AWS account ID 111122223333) has created 50 IAM users for its organization's employees. What will be the AWS console URL for these associates?

A.
https://signin.aws.amazon.com/console/111122223333/

B.
https://111122223333.signin.aws.amazon.com/console/

C.
https://signin.aws.amazon.com/111122223333/console/

D.
https://signin.aws.amazon.com/console/

Answer: B

Explanation:

When an organization is using AWS IAM for creating various users and manage their access rights, the IAM user cannot use the login URL http://aws.amazon.com/console to access AWS management console. The console login URL for the IAM user will have AWS account ID of that organization to identify the IAM user belongs to particular account. The AWS console login URL for the IAM user will be https:// <AWS_Account_ID>.signin.aws.amazon.com/console/. In this case it will be https://111122223333.signin.aws.amazon.com/console/

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/AccountAlias.html

QUESTION NO: 510

AWS IAM permissions can be assigned in two ways:

A.
as role-based or as resource-based.

B.
as identity-based or as resource-based.

C.
as security group-based or as key-based.

D.
as user-based or as key-based.

Answer: B

Explanation:

Permissions can be assigned in two ways: as identity-based or as resource-based. Identity-based, or IAM permissions, are attached to an IAM user, group, or role and let you specify what that user, group, or role can do. For example, you can assign permissions to the IAM user named Bob, stating that he has permission to use the Amazon Elastic Compute Cloud (Amazon EC2) RunInstances action and that he has permission to get items from an Amazon DynamoDB table named MyCompany. The user Bob might also be granted access to manage his own IAM security credentials. Identity-based permissions can be managed or inline.

Resource-based permissions are attached to a resource. You can specify resource-based permissions for Amazon S3 buckets, Amazon Glacier vaults, Amazon SNS topics, Amazon SQS queues, and AWS Key Management Service encryption keys. Resource-based permissions let you specify who has access to the resource and what actions they can perform on it. Resource-based policies are inline only, not managed.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/access_permissions.html

QUESTION NO: 511

Can you change the security groups associated with the primary network interface (eth0) of an EC2 instance running inside a VPC?

A.
Yes

B.
Only if the instance is stopped

C.
Only when the instance is launched

D.
No

Answer: A
Explanation:

After you launch an instance in a VPC, you can change its security groups. Security groups are associated with network interfaces. Changing an instance's security groups changes the security groups associated with the primary network interface (eth0)

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#vpc-security-groups

QUESTION NO: 512

Amazon Relational Database Service integrates with _____, a service that lets your organization

create users and groups under your organization's AWS account and assign unique security credentials to each user.

A.
Amazon RDS tags

B.
AWS IAM

C.
AWS Lambda

D.
Amazon EMR

Answer: B

Explanation:

Amazon Relational Database Service integrates with AWS IAM, a service that lets your organization create users and groups under your organization's AWS account and assign unique security credentials to each user.

Reference: http://awsdocs.s3.amazonaws.com/RDS/2011-04-01/rds-ug-2011-04-01.pdf

QUESTION NO: 513

The information within an IAM policy is described through a series of _____.

A.
elements

B.
macros

C.
classes

D.
namespaces

Answer: A

Explanation:

While creating an IAM policy, it includes many elements that you can use to define or create a policy. The elements that a policy can contain are as follows: Version, Id, Statement, Sid, Effect, Principal, NotPrincipal, Action, NonAction, Resource, NotResource, Condition, and Supported Data Types.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

QUESTION NO: 514

In Amazon VPC, the _____ encryption function is used to ensure privacy among both IKE and IPsec Security Associations.

A.
AES 192-bit

B.
AES 256-bit

C.
SHA 180-bit

D.
SHA 2-bit

Answer: B
Explanation:

When configuring your customer gateway to communicate with your VPC, the AES 128-bit or AES 256-bit encryption is used to ensure privacy among both IKE and IPSec Security Associations.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html

QUESTION NO: 515

In IAM, can you attach more than one inline policy to a particular entity such a user, role, or group?

A.
No

B.
Yes

C.
Yes, you can but only if you attach the policy within a VPC.

D.
Yes, you can but only if you attach the policy within the GovCloud.

Answer: B
Explanation:

In AWS IAM, you can add as many inline policies as you want to a user, role, or group, but the total aggregate policy size (the sum size of all inline policies) per entity cannot exceed the following limits: User policy size cannot exceed 2,048 characters.

Role policy size cannot exceed 10,240 characters. Group policy size cannot exceed 5,120 characters.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

QUESTION NO: 516

A customer enquires about whether all his data is secure on AWS, and is especially concerned about Elastic Map Reduce (EMR). You need to inform him of some of the security features in place for AWS. Which of the below statements is incorrect regarding EMR or S3?

A.
Every packet sent in the AWS network uses Internet Protocol Security (IPsec).

B.
Amazon S3 provides authentication mechanisms to ensure that stored data is secured against unauthorized access.

C.
Customers may encrypt the input data before they upload it to Amazon S3.

D.
Amazon EMR customers can choose to send data to Amazon S3 using the HTTPS protocol for secure transmission.

Answer: A

Explanation:

Amazon S3 provides authentication mechanisms to ensure that stored data is secured against unauthorized access. Unless the customer who is uploading the data specifies otherwise, only that customer can access the data. Amazon EMR customers can also choose to send data to Amazon S3 using the HTTPS protocol for secure transmission. In addition, Amazon EMR always uses HTTPS to send data between Amazon S3 and Amazon EC2. For added security, customers may encrypt the input data before they upload it to Amazon S3 (using any common data compression tool); they then need to add a decryption step to the beginning of their cluster when Amazon EMR fetches the data from Amazon S3. IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. Amazon supports Internet Protocol security (IPsec) VPN connections, but does not protect all data packets at this level.

Reference: https://aws.amazon.com/elasticmapreduce/faqs/

QUESTION NO: 517

If an IAM policy has multiple conditions, or if a condition has multiple keys, its boolean outcome will be calculated using a logical _____ operation.

A.
NAND

B.
OR

C.
AND

D.
None of these

Answer: C

Explanation:

If there are multiple condition operators, or if there are multiple keys attached to a single condition operator, the conditions are evaluated using a logical AND.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

QUESTION NO: 518

You have set up an IAM policy for your users to access Elastic Load Balancers and you know that an IAM policy is a JSON document that consists of one or more statements. Which of the following elements is not a part of the statement in an IAM policy document?

A.
Action

B.
Resource

C.
Effect

D.
Key

Answer: D
Explanation:

When you attach a policy to a user or group of users to control access to your load balancer, it allows or denies the users permission to perform the specified tasks on the specified resources.

An IAM policy is a JSON document that consists of one or more statements. Each statement is structured as follows:

Effect: The effect can be Allow or Deny. By default, IAM users don't have permission to use resources and API actions, so all requests are denied. An explicit allow overrides the default. An explicit deny overrides any allows.

Action: The action is the specific API action for which you are granting or denying permission.

Resource: The resource that's affected by the action. With many Elastic Load Balancing API actions, you can restrict the permissions granted or denied to a specific load balancer by specifying its Amazon Resource Name (ARN) in this statement. Otherwise, you can use the * wildcard to specify all of your load balancers.

Condition: You can optionally use conditions to control when your policies in effect.

Reference:

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

QUESTION NO: 519

In AWS Identity and Access Management, roles can be used by an external user authenticated by an external identity provider (IdP) service that is compatible with _____.

A.
BNML (Business Narrative Markup Language)

B.
CFML (ColdFusion Markup Language)

C.
SAML 2.0 (Security Assertion Markup Language 2.0)

D.
BPML (Business Process Modeling Language)

Answer: C
Explanation:

In AWS Identity and Access Management, roles can be used by an external user authenticated by an external identity provider (IdP) service that is compatible with SAML 2.0 (Security Assertion Markup Language 2.0).

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html

QUESTION NO: 520

Which of the below mentioned options is not a best practice to securely manage the AWS access credentials?

A.
Keep rotating your secure access credentials at regular intervals

B.
Create individual IAM users

C.
Create strong access key and secret access key and attach to the root account

D.

Enable MFA for privileged users

Answer: C

Explanation:

It is a recommended approach to avoid using the access and secret access keys of the root account. Thus, do not download or delete it. Instead make the IAM user as powerful as the root account and use its credentials. The user cannot generate their own access and secret access keys as they are always generated by AWS.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html

QUESTION NO: 521

The amount of data a company must back up has been increasing, and storage space is quickly running out. There is no budget to purchase new backup software that is capable of backing up data directly to the cloud.

What is the MOST cost-effective way to make storage available to the company's legacy backup system?

A.
Launch an Amazon EC2 instance, add large Amazon EBS volumes, and connect using VPN

B.
Ship backup tapes to AWS for storage in secure AWS Availability Zones

C.
Use AWS Snowball on a weekly basis to transfer data to Amazon Glacier

D.
Use AWS Storage Gateway to present a VTL using iSCSI to the legacy application

Answer: C

Explanation:

QUESTION NO: 522

The SysOps Administrator must integrate an existing on-premises asymmetrical key management

system into an AWS services platform.

How can the Administrator meet this requirement?

A.
Implement AWS KMS and integrate with the existing on-premises asymmetrical key management system

B.
Implement AWS CloudHSM and integrate it with the existing key management infrastructure

C.
Deploy an Amazon EC2 instance and choose an AMI from an AWS partner in the AWS Marketplace

D.
Create a master key in AWS KMS, and export that key to the existing on-premises asymmetrical key management system

Answer: C
Explanation:

QUESTION NO: 523

A Systems Administrator is planning to deploy multiple EC2 instances within two separate Availability Zones in the same AwS Region. The instances cannot be exposed to the Internet, but must be able to exchange traffic between one another. The data does not need to be encrypted.

What solution meets these requirements while maintaining the lowest cost?

A.
Create two private subnets within the same VPC. Communicate between instances using their private IP addresses

B.
Create 2 public subnets within the same VPC. Communicate between instances using their public IP addresses

C.
Create 2 separate VPCs, one for each Availability Zone. Create a private subnet within each VPC. Create a static route table pointing the destination CIDR to the other VPC

D.

Create 2 separate VPCs, one for each Availability Zone and create a public subnet in each. Deploy a VPN appliance within each VPC and establish a VPN tunnel between them. Communicate between instances by routing traffic through the VPN appliances

Answer: D

Explanation:

QUESTION NO: 524

A company website hosts patches for software that is sold globally. The website runs in AWS and performs well until a large software patch is released. The flood of downloads puts a strain on the web servers and leads to a poor customer experience.

What can the SysOps Administrator propose to enhance customer experience, create a more available web platform, and keep costs low?

A.
Use an Amazon CloudFront distribution to cache static content, including software patches

B.
Increase the size of the NAT instance to improve throughput

C.
Scale out of web servers in advance of patch releases to reduce Auto Scaling delays

D.
Move the content to IO1 and provision additional IOPS to the volume that contains the software patches

Answer: A

Explanation:

QUESTION NO: 525

An organization has developed a new memory-intensive application that is deployed to a large Amazon EC2 Linux fleet. There is concern about potential memory exhaustion, so the Development team wants to monitor memory usage by using Amazon CloudWatch.

What is the MOST efficient way to accomplish this goal?

A.
Deploy the solution to memory-optimized EC2 instances, and use the CloudWatch MemoryUtilization metric

B.
Enable the Memory Monitoring option by using AWS Config

C.
Install the AWS Systems Manager agent on the applicable EC2 instances to monitor memory

D.
Monitor memory by using a script within the instance, and send it to CloudWatch as a custom metric

Answer: B
Explanation:

QUESTION NO: 526

A SysOps Administrator is running Amazon EC2 instances in multiple AWS Regions. The Administrator wants to aggregate the CPU utilization for all instances onto an Amazon CloudWatch dashboard. Each region should be present on the dashboard and represented by a single graph that contains the CPU utilization for all instances in that region.

How can the Administrator meet these requirements?

A.
Create a cross-region dashboard using AWS Lambda and distribute it to all regions

B.
Create a custom CloudWatch dashboard and add a widget for each region in the AWS Management Console

C.
Enable cross-region dashboards under the CloudWatch section of the AWS Management Console

D.
Switch from basic monitoring to detailed monitoring on all instances

Answer: B
Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cross_region_dashboard.html

QUESTION NO: 527

A mobile application must allow users to securely access their own content stored in a shared Amazon S3 bucket.

Which AWS services should be used to enable this access? (Choose two.)

A.
AWS Directory Service

B.
AWS Shield

C.
IAM roles

D.
Amazon Cognito

E.
AWS Organizations

Answer: C,E
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

QUESTION NO: 528

A Development team has an application stack consisting of many OS dependencies and language runtime dependencies. When deploying the application to production, the most important factor is how quickly the instance is operational.

What deployment methodology should be used to update the running environments to meet the requirement?

A.

Use fully baked AMIs (“golden images”) created after each successful build, creating a new Auto Scaling group, and blue/green deployments with rollbacks.

B.
Use user-data scripts to configure the instance correctly on boot by installing all dependencies when needed.

C.
Use an AWS Lambda function to only update the application locally on each instance, then re-attach it to the load balancer when the process complete.

D.
Use AWS OpsWorks scripts to execute on reboot of each instance to install all known dependencies, then re-attach the instances to the load balancer.

Answer: A

Explanation:

QUESTION NO: 529

A web-based application is running in AWS. The application is using a MySQL Amazon RDS database instance for persistence. The application stores transactional data and is read-heavy. The RDS instance gets busy during the peak usage, which shows the overall application response times.

The SysOps Administrator is asked to improve the read queries performance using a scalable solution.

Which options will meet these requirements? (Choose two.)

A.
Scale up the RDS instance to a larger instance size

B.
Enable the RDS database Multi-AZ option

C.
Create a read replica of the RDS instance

D.
Use Amazon DynamoDB instead of RDS

E.
Use Amazon ElastiCache to cache read queries

Answer: C,E

Explanation:

QUESTION NO: 530

A Content Processing team has notified a SysOps Administrator that their content is sometimes taking a long time to process, whereas other times it processes quickly. The Content Processing submits messages to an Amazon Simple Queue Service (Amazon SQS) queue, which details the files that need to be processed. An Amazon EC2 instance polls the queue to determine which file to process next.

How could the Administrator maintain a fast but cost-effective processing time?

A.
Attach an Auto Scaling policy to the Amazon SQS queue to increase the number of EC2 instances based on the depth of the SQS queue

B.
Create an Auto Scaling policy to increase the number of EC2 instances polling the queue and a CloudWatch alarm to scale based on MaxVisibility Timeout

C.
Attach an Auto Scaling policy to the SQS queue to scale instances based on the depth of the dead-letter queue

D.
Create an Auto Scaling policy to increase the number of EC2 instances polling the queue and a CloudWatch alarm to scale based on ApproximateNumberOfMessagesVisible

Answer: C

Explanation:

QUESTION NO: 531

A SysOps Administrator receives reports of an Auto Scaling group failing to scale when the nodes running Amazon Linux in the cluster are constrained by high memory utilization.

What should the Administrator do to enable scaling to better adapt to the high memory utilization?

A.
Create a custom script that pipes memory utilization to Amazon S3, then, scale with an AWS Lambda-powered event

B.
Install the Amazon CloudWatch memory monitoring scripts, and create a custom metric based on the script's results

C.
Increase the minimum size of the cluster to meet memory and application load demands

D.
Deploy an Application Load Balancer to more evenly distribute traffic among nodes

Answer: D
Explanation:

QUESTION NO: 532

A SysOps Administrator has received a request from the Compliance Department to enforce encryption on all objects uploaded to the corp-compliance bucket.

How can the Administrator enforce encryption on all objects uploaded to the bucket?

A.
Enable Amazon S3 default encryption on the bucket

B.
Add the following policy statement to the bucket:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": [
                    "s3:PutObject"
               ],
               "Effect": "Deny",
               "Resource": "arn:aws:s3:::corp-compliance/",
               "Condition": {
                    "Bool": {
                         "aws:SecureTransport": "false"
                    }
               },
               "Principal": "*"
```

BrainDumps

C.

Add the following policy statement to the IAM user permissions policy:

```
{
     "Version": "2012-10-17",
     "Statement": [{
          "Effect": "Deny",
          "Action": "s3:PutObject",
          "Resource": "arn:aws:s3:::corp-compliance/",
          "Condition": {
               "Bool": {
                    "aws:SecureTransport": "false"
               }
          }
     }]
}
```

BrainDumps

D.
Generate a resigned URL for the Amazon S3 PUT operation with server-side encryption flag set, and send the URL to the user

Answer: B
Explanation:

QUESTION NO: 533

An errant process is known to use an entire processor and run at 100%. A SysOps Administrator wants to automate restarting the instance once the problem occurs for more than 2 minutes.

How can this be accomplished?

A.
Create an Amazon CloudWatch alarm for the 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 to restart the EC2 instance, triggered by EC2 health checks.

Answer: B

Explanation:

QUESTION NO: 534

A SysOps Administrator needs to report on Amazon EC2 instance cost by both project and environment (production, staging, development).

Which action would impact the operations team the LEAST?

A.
For each project and environment, create a new AWS account and link them to the master payer for unified management and billing

B.
Use AWS Organizations to create a new organization for each project, then for each environment use a separate linked AWS account

C.
Implement cost allocation tagging in the Billing and Cost Management console to implement tags to identify resources by project and environment

D.
Add the project and environment information to the instance metadata so that the values can be queried and rolled up into reports

Answer: C

Explanation:

QUESTION NO: 535

A web application’s performance has been degrading. Historically, the application has had highly-variable workloads, but lately, there has been a steady growth in traffic as the result of a new product launch. After reviewing several Amazon CloudWatch metrics, it is discovered that over the last two weeks the balance of CPU credits has dropped to zero several times.

Which solutions will improve performance? (Choose two.)

A.
Begin using the T2 instance type

B.
Purchase more CPU credits for the existing instance

C.
Increase the size of the current instance type

D.
Configure a CloudWatch alarm on the CPU credits metric

Answer: A,C
Explanation:

QUESTION NO: 536

An Amazon EC2 instance is in a private subnet. To SSH to the instance, it is required to use a bastion host that has an IP address of 10.0.0.5. SSH logs on the EC2 instance in the private subnet show that connections are being made over SSH from several other IP addresses. The EC2 instance currently has the following inbound security group rules applied:

Protocol: TCP

Port: 22

Source: 10.0.0.5/32

Protocol: TCP

Port: 22

Source: sg-xxxxxxxx

Protocol: TCP

Port: 389

Source: 0.0.0.0/0

What is the MOST likely reason that another IP addresses is able to SSH to the EC2 instance?

A.

The rule with 0.0.0.0/0 means SSH is open for any client to connect

B.
The rule with /32 is not limiting to a single IP address

C.
Any instance belonging to sg-xxxxxxxx is allowed to connect

D.
There is an outbound rule allowing SSH traffic

Answer: C
Explanation:

QUESTION NO: 537

An AWS CloudFormation template creates an Amazon RDS instance. This template is used to build up development environments as needed and then delete the stack when the environment is no longer required. The RDS-persisted data must be retained for further use, even after the CloudFormation stack is deleted.

How can this be achieved in a reliable and efficient way?

A.
Write a script to continue backing up the RDS instance every five minutes

B.
Create an AWS Lambda function to take a snapshot of the RDS instance, and manually execute the function before deleting the stack

C.
Use the Snapshot Deletion Policy in the CloudFormation template definition of the RDS instance

D.
Create a new CloudFormation template to perform backups of the RDS instance, and run this template before deleting the stack

Answer: D
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-rds-database-instance.html

QUESTION NO: 538

A company's IT Security team is performing an audit of the AWS environment to determine which servers need to be patched and where additional security controls need to be added.

The company is responsible for which of the following? (Choose two.)

A.
Patching the OS on Amazon RDS instances

B.
Patching the OS on Amazon EC2 instances

C.
Enabling server-side encryption with Amazon S3-Managed Keys (SSE-S3) on S3 objects

D.
Patching the database engine on RDS instances

E.
Patching PHP in an AWS Elastic Beanstalk managed EC2 application

Answer: B,C

Explanation:

QUESTION NO: 539

The InfoSec team has asked the SysOps Administrator to perform some hardening on the company Amazon RDS database instances.

Based on this requirement, what actions should be recommended for the start of the security review? (Choose two.)

A.
Use Amazon Inspector to present a detailed report of security vulnerabilities across the RDS database fleet

B.
Review the security group's inbound access rules for least privilege

C.
Export AWS CloudTrail entries detailing all SSH activity on the RDS instances

D.
Use the cat command to enumerate the allowed SSH keys in ~/.ssh on each RDS instance

E.
Report on the Parameter Group settings and ensure that encrypted connections are enforced

Answer: A,E
Explanation:

QUESTION NO: 540

A Big Data consulting company wants to separate its customers' workloads for billing and security reasons. The company would like to maintain billing and security controls on these workloads.

According to best practices, how can the workloads be separated if no shared resources are needed?

A.
Require each customer to create their own account. Contact AWS Support to receive a consolidated bill.

B.
Create customer accounts within AWS Organizations specifying consolidated billing features.

C.
Create a separate VPC for each customer. Use security groups to isolate traffic.

D.
Dedicate an AWS Region to each customer. Ensure that each entry in Amazon Route 53 is unique.

Answer: C
Explanation:

QUESTION NO: 541

An organization stores files on Amazon S3. Employees download the files, edit them with the same file name to the same folder on Amazon S3. Occasionally the files are unintentionally modified or deleted.

What is the MOST cost-effective way to ensure that these files can be recovered to their correct state?

A.
Enable cross-region replication on the Amazon S3 bucket

B.
Enable versioning on the Amazon S3 bucket

C.
Use Lifecycle Management to move the files to Amazon Glacier

D.
Copy the edited files to Amazon Elastic File System

Answer: B

Explanation:

QUESTION NO: 542

A company has a web application that runs both on-premises and on Amazon EC2 instances. Over time, both the on-premises servers and EC2 instances begin crashing. A SysOps Administrator suspects a memory leak in the application and wants a unified method to monitor memory utilization over time.

How can the Administrator track both the EC2 memory utilization and on-premises server memory utilization over time?

A.
Write a script or use a third-party application to report memory utilization for both EC2 instances and on-premises servers.

B.
Use Amazon CloudWatch agent for both Amazon EC2 instances and on-premises servers to report MemoryUtilization metrics to CloudWatch and set a CloudWatch alarm for notifications.

C.
Use CloudWatch agent for Amazon EC2 instances to report memory utilization to CloudWatch, and set CloudWatch alarms for notifications. Use a third-party application for the on-premises servers.

D.
Configure a load balancer to route traffic to both on-premises servers and EC2 instances, then use

CloudWatch as the unified view of the metrics for the load balancer.

Answer: B

Explanation:

QUESTION NO: 543

Website users report that an application's pages are loading slowly at the beginning of the workday. The application runs on Amazon EC2 instances, and data is stored in an Amazon RDS database. The SysOps Administrator suspects the issue is related to high CPU usage on a component of this application.

How can the Administrator find out which component is causing the performance bottleneck?

A.
Use AWS CloudTrail to review the resource usage history for each component.

B.
Use Amazon CloudWatch metrics to examine the resource usage of each component.

C.
Use Amazon Inspector to view the resource usage details for each component.

D.
Use Amazon CloudWatch Events to examine the high usage events for each component.

Answer: B

Explanation:

Enhanced Monitoring provides granular real-time metrics that you can review in addition to Amazon CloudWatch metrics, which provide statistics each minute.

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/rds-instance-high-cpu/

QUESTION NO: 544

A SysOps Administrator has an AWS Direct Connect connection in place in region us-east-1, between an AWS account and a data center. The Administrator is now required to connect the

data center to a VPC in another AWS Region, us-west-2, which must have consistent network performance and low-latency.

What is the MOST efficient and quickest way to establish this connectivity?

A.
Create an AWS VPN CloudHub architecture, and use software VPN to connect to the VPC in region us-west-2.

B.
Create a new Direct Connect connection between the data center and region us-west-2.

C.
Create a VPC peering connection between the VPC in region us-east-1 and us-west-2, and access the VPC in us-west-2 from the data center.

D.
Use Direct Connect gateway with the existing Direct Connect connection to connect to the Virtual Private Gateway of the VPC in region us-west-2.

Answer: D
Explanation:

QUESTION NO: 545

A new application is being tested for deployment on an Amazon EC2 instance that requires greater IOPS than currently provided by the single 4TB General Purpose SSD (gp2) volume.

Which actions should be taken to provide additional Amazon EBS IOPS for the application? (Choose two.)

A.
Increase the size of the General Purpose (gp2) volume

B.
Use RAID 0 to distribute I/O across multiple volumes

C.
Migrate to a Provisioned IOPS SSD (io1) volume

D.
Enable MAX I/O performance mode on the General Purpose (gp2) volume

E.
Use RAID 1 to distribute I/O across multiple volumes

Answer: A,D
Explanation:

QUESTION NO: 546

A web service runs on Amazon EC2 instances behind an Elastic Load Balancing (ELB) load balancer. External clients must whitelist specific public IP addresses in their firewalls to access the service.

What load balancer or ELB feature should be used for this application?

A.
Network Load Balancer

B.
Application Load Balancer

C.
Classic Load Balancer

D.
Load balancer target groups

Answer: B
Explanation:

QUESTION NO: 547

While creating the wait condition resource in AWS CloudFormation, a SysOps Administrator receives the error “received 0 signals out of the 1 expected from the EC2 instance”.

What steps should be taken to troubleshoot this issue? (Choose two.)

A.
Confirm from the cfn logs that the cfn-signal command was successfully run on the instance.

B.
Try to re-create the stack with a different IAM user.

C.
Check that the instance has a route to the Internet through a NAT device.

D.
Update the AWS CloudFormation stack service role to have iam:PassRole permission.

E.
Delete the existing stack and attempt to create a new once.

Answer: A,D
Explanation:

QUESTION NO: 548

An existing, deployed solution uses Amazon EC2 instances with Amazon EBS General Purpose SSD volumes, am Amazon RDS PostgreSQL database, an Amazon EFS file system, and static objects stored in an Amazon S3 bucket. The Security team now mandates that at-rest encryption be turned on immediately for all aspects of the application, without creating new resources and without any downtime.

To satisfy the requirements, which one of these services can the SysOps Administrator enable at-rest encryption on?

A.
EBS General Purpose SSD volumes

B.
RDS PostgreSQL database

C.
Amazon EFS file systems

D.
S3 objects within a bucket

Answer: A
Explanation:

QUESTION NO: 549

A SysOps Administrator noticed that a large number of Elastic IP addresses are being created on the company's AWS account., but they are not being associated with Amazon EC2 instances, and are incurring Elastic IP address charges in the monthly bill.

How can the Administrator identify who is creating the Elastic IP address?

A.
Attach a cost-allocation tag to each requested Elastic IP address with the IAM user name of the Developer who creates it.

B.
Query AWS CloudTrail logs by using Amazon Athena to search for Elastic IP address events.

C.
Create a CloudWatch alarm on the EIPCreated metric and send an Amazon SNS notification when the alarm triggers.

D.
Use Amazon Inspector to get a report of all Elastic IP addresses created in the last 30 days.

Answer: A
Explanation:

QUESTION NO: 550

An application is running on Amazon EC2 instances behind a Classic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. Occasionally multiple incoming requests will receive a 5xx HTTP response when making a request to the Classic Load Balancer. From the Amazon CloudWatch metrics, a SysOps Administrator observes the Elastic Load Balancing (ELB) SpillOverCount metric to be greater than zero during these occasions.

These errors can be avoided by triggering scaling actions on which ELB metric?

A.
HealthyHostCount

B.
BackendConnectionErrors

C.

SurgeQueueLength

D.
UnHealthyHostCount

Answer: C
Explanation:

QUESTION NO: 551

An application running by a SysOps Administrator is under repeated, large-scale distributed denial of service (DDoS) attacks. Each time an attack occurs, multiple customers reach out to the Support team to report outages. The Administrator wants to minimize potential downtime from the DDoS attacks. The company requires 24/7 support.

Which AWS service should be set up to protect the application?

A.
AWS Trusted Advisor

B.
AWS Shield Advanced

C.
Amazon Cognito

D.
Amazon Inspector

Answer: B
Explanation:

QUESTION NO: 552

Malicious traffic is reaching company web servers from a single IP address located in another country. The SysOps Administrator is tasked with blocking this IP address.

How should the Administrator implement the restriction?

A.
Edit the security group for the web servers and add a deny entry for the IP address

B.
Edit the network access control list for the web server subnet and add a deny entry for the IP address

C.
Edit the VPC route table to route the malicious IP address to a black hole

D.
Use Amazon CloudFront's geo restriction feature to block traffic from the IP address

Answer: D
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

QUESTION NO: 553

A SysOps Administrator needs Amazon EC2 instances in two different VPCs in private subnets to be able to communicate. A peering connection between the two VPCs has been created using the AWS Management Console and shows a status of Active. The instances are still unable to send traffic to each other.

Why are the EC2 instances unable to communicate?

A.
One or both of the VPCs do not have an Internet Gateway attached

B.
The route tables have not been updated

C.
The peering connection has not been properly tagged

D.
One or both of the instances do not have an Elastic IP address assigned

Answer: B
Explanation:

QUESTION NO: 554

A SysOps Administrator must ensure that AWS CloudFormation deployment changes are properly tracked for governance.

Which AWS service should be used to accomplish this?

A.
AWS Artifact

B.
AWS Config

C.
Amazon Inspector

D.
AWS Trusted Advisor

Answer: B
Reference: https://aws.amazon.com/blogs/mt/how-to-track-configuration-changes-to-cloudformation-stacks-using-aws-config/

QUESTION NO: 555

With the threat of ransomware viruses encrypting and holding company data hostage, which action should be taken to protect an Amazon S3 bucket?

A.
Deny Post, Put, and Delete on the bucket

B.
Enable server-side encryption on the bucket

C.
Enable Amazon S3 versioning on the bucket

D.
Enable snapshots on the bucket

Answer: B
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/

QUESTION NO: 556

A SysOps Administrator has implemented an Auto Scaling group with a step scaling policy. The

Administrator notices that the additional instances have not been included in the aggregated metrics.

Why are the additional instances missing from the aggregated metrics?

A.
The warm-up period has not expired

B.
The instances are still in the boot process

C.
The instances have not been attached to the Auto Scaling group

D.
The instances are included in a different set of metrics

Answer: C
Explanation:

QUESTION NO: 557

Recently several critical files were mistakenly deleted from a shared Amazon S3 bucket. A SysOps Administrator needs to prevent accidental deletions from occurring in the future by enabling MFA Delete.

Once enabled, which bucket activities will require MFA authentication? (Choose two.)

A.
Permanently removing an object version from the bucket

B.
Disabling default object encryption for the bucket

C.
Listing all versions of deleted objects in the bucket

D.
Suspending versioning on the bucket

E.
Enabling MFA Add on the bucket

Answer: C,E
Explanation:

QUESTION NO: 558

A SysOps Administrator has an AWS Lambda function that stops all Amazon EC2 instances in a test environment at night and on the weekend. Stopping instances causes some servers to become corrupt due to the nature of the applications running on them.

What can the SysOps Administrator use to identify these EC2 instances?

A.
AWS Config

B.
Amazon EC2 termination protection

C.
Resource tagging

D.
Amazon CloudWatch

Answer: D
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/

QUESTION NO: 559

A company has Amazon EC2 instances that serve web content behind an Elastic Load Balancing (ELB) load balancer. The ELB Amazon CloudWatch metrics from a few hours ago indicate a significant number of 4XX errors. The EC2 instances from the time of these errors have been deleted.

At the time of the 4XX errors, how can an Administrator obtain information about who originated these requests?

A.
If ELB access logs have been enabled, the information can be retrieved from the S3 bucket

B.
Contact AWS Support to obtain application logs from the deleted instances

C.
Amazon S3 always keeps a backup of application logs from EC2 instances. Retrieve these logs for analysis

D.
Use AWS Trusted Advisor to obtain ELB access logs

Answer: A
Explanation:

QUESTION NO: 560

A SysOps Administrator is managing an application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application stores data in an Amazon RDS MySQL DB instance. The Administrator must ensure that that application stays available if the database becomes unresponsive.

How can these requirements be met?

A.
Create read replicas for the RDS database and use them in case of a database failure

B.
Create a new RDS instance from the snapshot of the original RDS instance if a failure occurs

C.
Keep a separate RDS database running and switch the endpoint in the web application if a failure occurs

D.
Modify the RDS instance to be a Multi-AZ deployment

Answer: D

Explanation:

QUESTION NO: 561

A company has an asynchronous nightly process that feeds the results to a data warehouse system for weekly and monthly reporting. The process is running on a fleet of Amazon EC2 instances. A SysOps Administrator has been asked to identify ways to reduce the cost of running this process.

What is the MOST cost-effective solution?

A.
Use On-Demand EC2 instances in an Auto Scaling group

B.
Use Spot Instances to bid for the EC2 instances

C.
Use Reserved Instances to ensure the capacity

D.
Put the EC2 instances in a placement group

Answer: A
Explanation:

QUESTION NO: 562

A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.

What type of record should be set in Route 53 to point the website’s apex domain name (for example, “company.com”) to the Application Load Balancer?

A.
CNAME

B.
SOA

C.
TXT

D.
ALIAS

Answer: D
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

QUESTION NO: 563

An application running on Amazon EC2 allows users to launch batch jobs for data analysis. The jobs are run asynchronously, and the user is notified when they are complete. While multiple jobs can run concurrently, a user's request need not be fulfilled for up to 24 hours. To run a job, the application launches an additional EC2 instance that performs all the analytics calculations. A job takes between 75 and 110 minutes to complete and cannot be interrupted.

What is the MOST cost-effective way to run this workload?

A.
Run the application on On-Demand EC2 instances. Run the jobs on Spot Instances with a specified duration.

B.
Run the application on Reserved Instance EC2 instances. Run the jobs on AWS Lambda.

C.
Run the application on On-Demand EC2 instances. Run the jobs on On-Demand EC2 instances.

D.
Run the application on Reserved Instance EC2 instances. Run the jobs on Spot Instances with a specified duration.

Answer: D
Explanation:

QUESTION NO: 564

A developer deploys an application running on Amazon EC2 by using an AWS CloudFormation template. The developer launches the stack from the console logged in as an AWS Identity and Access Management (IAM) user. When a SysOps Administrator attempts to run the same AWS CloudFormation template in the same AWS account from the console, it fails and returns the error:

“The image id ‘[ami-2a69aa47]’ does not exist”

What is the MOST likely cause of the failure?

A.
The Administrator does not have the same IAM permissions as the developer.

B.
The Administrator used a different SSH key from that of the developer.

C.
The Administrator is running the template in a different region.

D.
The Administrator’s Amazon EC2 service limits have been exceeded

Answer: C
Explanation:

QUESTION NO: 565

A company has configured a library of IAM roles that grant access to various AWS resources. Each employee has an AWS IAM user, some of which have the permission to launch Amazon EC2 instances. The SysOps Administrator has attached the following policy to those users:

```
{
      "Version": "2012-10-17",
      "Statement": [{
        "Effect":"Allow",
        "Action":["ec2:*"],
        "Resource":"*"
      },
      {
        "Effect":"Allow",
        "Action":"iam:PassRole",
        "Resource":"arn:aws:iam::123456789012:role/InfraTeam*"
      }]
}
```

BrainDumps

What would be the result of this policy?

A.
Users are able to switch only to a role name that begins with “InfraTeam” followed by any other combination of characters.

B.
Users with the role of InfraTeamLinux are able to launch an EC2 instance and attach that role to it.

C.
“InfraTeam” role is being passed to a user who has full EC2 access.

D.
EC2 instances that are launched by these users have full AWS permissions.

Answer: A
Explanation:

QUESTION NO: 566

Application developers are reporting Access Denied errors when trying to list the contents of an Amazon S3 bucket by using the IAM user “arn:aws:iam::111111111111:user/application”. The following S3 bucket policy is in use:

```
{
  "Id": "S3BucketPolicy",
  "Version": "2012-10-17",
  "Statement": [
     {
       "Sid": "List",
       "Action": [
          "s3:List*"
       ],
       "Effect": "Allow",
       "Resource": [
          "arn:aws:s3:::bucketname/*"
       ],
       "Principal": {
          "AWS": [
               "arn:aws:iam::111111111111:user/application"
       ]
     }
   }
  ]
}
```

BrainDumps

How should a SysOps Administrator modify the S3 bucket policy to fix the issue?

A.
Change the “Effect” from “Allow” to “Deny”

B.
Change the “Action” from “s3:List*” to “s3:ListBucket”

C.
Change the “Resource” from “arn:aws:s3:::bucketname/*” to “arn:aws:s3:::bucketname”

D.
Change the “Principal” from “arn:aws:iam::111111111111:user/application” to “arn:aws:iam::111111111111:role/application”

Answer: C
Explanation:

QUESTION NO: 567

An organization has hired an external firm to audit unauthorized changes on the company’s AWS environment, the external auditor needs appropriate access.

How can this be accomplished?

A.
Create an IAM user and assign them a new policy with GetResources access on AWS Artifact

B.
Create an IAM user and add them to the existing “Administrator” IAM group

C.
Create an IAM user and assign them a new IAM policy with read access to the AWS CloudTrail logs in Amazon S3

D.
Create an IAM user and assign them a new policy with ListFindings access on Amazon Inspector

Answer: C
Explanation:

QUESTION NO: 568

A SysOps Administrator wants to automate the process of configuration, deployment, and

management of Amazon EC2 instances using Chef or Puppet.

Which AWS service will satisfy the requirement?

A.
AWS Elastic Beanstalk

B.
AWS CloudFormation

C.
AWS OpsWorks

D.
AWS Config

Answer: C
Reference: https://aws.amazon.com/opsworks/

QUESTION NO: 569

A photo-sharing site delivers content worldwide from a library on Amazon S3 using Amazon CloudFront. Users are trying to access photos that either do not exist or they are not authorized to view.

What should be monitored to better understand the extent of this issue?

A.
GetRequests S3 metric on Amazon CloudWatch

B.
4XXErrorRate CloudFront metric on CloudWatch

C.
5XXErrorRate CloudFront metric on CloudWatch

D.
PostRequests S3 metric on CloudWatch

Answer: A
Explanation:

QUESTION NO: 570

A company must share monthly report files that are uploaded to Amazon S3 with a third party. The third-party user list is dynamic, is distributed, and changes frequently. The least amount of access must be granted to the third party. Administrative overhead must be low for the internal teams who manage the process.

How can this be accomplished while providing the LEAST amount of access to the third party?

A.
Allow only specified IP addresses to access the S3 buckets which will host files that need to be provided to the third party.

B.
Create an IAM role with the appropriate access to the S3 bucket, and grant login permissions to the console for the third party to access the S3 bucket.

C.
Create a pre-signed URL that can be distributed by email to the third party, allowing it to download specific S3 filed.

D.
Have the third party sign up for an AWS account, and grant it cross-account access to the appropriate S3 bucket in the source account.

Answer: A
Explanation:

QUESTION NO: 571

An administrator is responding to an alarm that reports increased application latency. Upon review, the Administrator notices that the Amazon RDS Aurora database frequently runs at 100% CPU utilization. The application is read heavy and does frequent lookups of a product table.

What should the Administrator do to reduce the application latency?

A.
Move the product table to Amazon Redshift and use an interleaved sort key

B.
Add Aurora Replicas and use a Reader Endpoint for product table lookups

C.
Move the product table to Amazon CloudFront and set the cache-control headers to public

D.
Use Auto Scaling to add extra Aurora nodes and set a trigger based on CPU utilization

Answer: B
Explanation:

QUESTION NO: 572

A company is running a new promotion that will result in a massive spike in traffic for a single application. The SysOps Administrator must prepare the application and ensure that the customers have a great experience. The application is heavy on memory and is running behind an AWS Application Load Balancer (ALB). The ALB has been pre-warmed, and the application is in an Auto Scaling group.

What built-in metric should be used to control the Auto Scaling group's scaling policy?

A.
RejectedConnection Count

B.
Request CountPerTarget

C.
CPUUtilization

D.
MemoryUtilization

Answer: C
Explanation:

QUESTION NO: 573

A SysOps Administrator is reviewing AWS Trusted Advisor warnings and encounters a warning for an S3 bucket policy that has open access permissions. While discussing the issue the bucket owner, the Administrator realizes the S3 bucket is an origin for an Amazon CloudFront web distribution.

Which action should the Administrator take to ensure that users access objects in Amazon S3 by using only CloudFront URLs?

A.
Encrypt the S3 bucket content with Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

B.
Create an origin access identity and grant it permissions to read objects in the S3 bucket

C.
Assign an IAM user to the CoudFront distribution and whitelist the IAM user in the S3 bucket policy

D.
Assign an IAM role to the CloudFront distribution and whitelist the IAM role in the S3 bucket policy

Answer: B
Reference: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

QUESTION NO: 574

An e-commerce company hosts its website on the AWS us-west-1 region. It plans to create a special site for a promotion that should be visible only to shoppers from Canada.

What change should the SysOps Administrator make to the company’s existing AWS setup to achieve this result?

A.
Update the Amazon Route 53 record set to use a latency routing policy for the new site

B.
Update the Application Load Balancer with a new host-based routing rule for the new site

C.
Update the Amazon Route 53 record set to use a geolocation routing policy for the new site

D.
Update the Application Load Balancer with a new path-based routing rule for the new site

Answer: C
Explanation:

QUESTION NO: 575

A company currently has a single AWS account used by all project teams. The company is migrating to a multi-account strategy, where each project team will have its own account. The AWS IAM configuration must have the same roles and policies for each of the accounts.

What is the MOST efficient way to implement and manage these new requirements?

A.
Create a portfolio in the AWS Service Catalog for the IAM roles and policies. Have a specific product in the portfolio for each environment, project, and team that can be launched independently by each user.

B.
Use AWS Organizations to create organizational units (OUs) for each group of projects and each team. Then leverage service control policies at the account level to restrict what services can used and what actions the users, groups, and roles can perform in those accounts.

C.
Create an AWS Lambda script that leverages cross-account access to each AWS account, and create all the roles and policies needed using the IAM API and JSON documents stored in Amazon S3.

D.
Create a single AWS CloudFormation template. Use CloudFormation StackSets to launch the CloudFormation template into each target account from the Administrator account.

Answer: B
Explanation:

Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization’s access control guidelines. SCPs are available only in an organization that has all features enabled. SCPs aren't available if your organization has enabled only the consolidated billing features.

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

QUESTION NO: 576

A SysOps Administrator is creating an Amazon EC2 instance and has received an InsufficientInstanceCapacity error.

What is the cause of the error and how can it be corrected?

A.
AWS does not currently have enough capacity to service the request for that instance type. A different Availability Zone or instance type must be used.

B.
The account has reached its concurrent running instance limit. An EC2 limit increase request must be filed with AWS Support.

C.
The APIs that service the EC2 requests have received too many requests and capacity has been reached. The request should be attempted again in a few minutes.

D.
The Administrator did not specify the correct size of the instance to support the capacity requirements of the workload. Select a bigger instance.

Answer: A
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-capacity

QUESTION NO: 577

A web application runs on Amazon EC2 instances with public IPs assigned behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application stores data in an Amazon RDS Multi-AZ DB instance. The Application Load Balancer, EC2 instances, and RDS DB instance all run in separate sets of subnets. The EC2 instances can communicate with the DB instance, but cannot connect with external services.

What is the MOST likely solution?

A.
Assign a public IP address to the database server and restart the database engine.

B.
Create and attach an Internet gateway to the VPC. Create a route table for the EC2 instance's subnets that sends Internet traffic to the gateway.

C.
Create and attach a virtual private gateway to the VPC. Create a route table for the EC2 instances' subnets that sends Internet traffic to the gateway.

D.
Create a VPC peering connection to a VPC that has an Internet gateway attached. Create a route table for the EC2 instances' subnets that sends Internet traffic to the peered VPC.

Answer: B
Explanation:

QUESTION NO: 578

A company has deployed a new application running on Amazon EC2 instances. The application team must verify for the Security team that all common vulnerabilities and exposures have been addressed, both now and regularly throughout the application's lifespan.

How can the Application team satisfy the Security team's requirement?

A.
Perform regular assessments with Amazon Inspector

B.
Perform regular assessments with AWS Trusted Advisor

C.
Integrate AWS Personal Health Dashboard with Amazon CloudWatch events to get security notifications

D.
Grant the Administrator and Security team access to AWS Artifact

Answer: A
Explanation:

QUESTION NO: 579

InfoSec is concerned that an employee may expose sensitive data in an Amazon S3 bucket.

How can this concern be addressed without putting undue restrictions on users?

A.
Apply an IAM policy on all users that denies the action s3:PutBucketPolicy

B.
Restrict S3 bucket access to specific IAM roles managed using federated access

C.
Activate an AWS Config rule to identify public buckets and alert InfoSec using Amazon SNS

D.
Email the findings of AWS Personal Health Dashboard to InfoSec daily

Answer: B
Explanation:

QUESTION NO: 580

A SysOps Administrator is using AWS CloudFormation to deploy resources but would like to manually address any issues that the template encounters.

What should the Administrator add to the template to support the requirement?

A.
Enable Termination Protection on the stack

B.
Set the OnFailure parameter to “DO_NOTHING”

C.
Restrict the IAM permissions for CloudFormation to delete resources

D.
Set the DeleteStack API action to “No”

Answer: A
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html

QUESTION NO: 581

A SysOps Administrator discovers the organization’s tape archival system is no longer functioning in its on-premises data center.

What AWS service can be used to create a virtual tape interface to replace the physical tape system?

A.
AWS Snowball

B.
AWS SMS

C.
Amazon Glacier

D.
AWS Storage Gateway

Answer: D
Explanation:

QUESTION NO: 582

A new application runs on Amazon EC2 instances and accesses data in an Amazon RDS database instance. When fully deployed in production, the application fails. The database can be queried from a console on a bastion host. When looking at the web server logs, the following error is repeated multiple times:

*** Error Establishing a Database Connection.

Which of the following may be causes of the connectivity problems? (Choose two.)

A.
The security group for the database does not have the appropriate egress rule from the database to the web server.

B.

The certificate used by the web server is not trusted by the RDS instance.

C.
The security group for the database does not have the appropriate ingress rule from the web server to the database.

D.
The database is still being created and is not available for connectivity.

Answer: A,C

Explanation:

QUESTION NO: 583

A recent audit found that most resources belonging to the Development team were in violation of patch compliance standards. The resources were properly tagged.

Which service should be used to quickly remediate the issue and bring the resources back into compliance?

A.
AWS Config

B.
Amazon Inspector

C.
AWS Trusted Advisor

D.
AWS Systems Manager

Answer: D
Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-compliance-fixing.html

QUESTION NO: 584

A SysOps Administrator has been able to consolidate multiple, secure websites onto a single

server, and each site is running on a different port. The Administrator now wants to start a duplicate server in a second Availability Zone and put both behind a load balancer for high availability.

What would be the command line necessary to deploy one of the sites' certificates to the load balancer?

A.

```
aws kms modify-listener --load-balancer-name my-load-
balancer - -certificates
CertificateArn=arn:aws:iam::123456789012:server-
certificate/my-new-server-cert
```

B.

```
aws elb set-load-balancer-listener-ssl-certificate - -load-
balancer-name my-load-balancer - -load-balancer-port 443 - -
ssl-certificate-id arn:aws:iam::123456789012:server-
certificate/new-server-cert
```

C.

```
aws ec2 put-ssl-certificate - -load-balancer-name my-load-
balancer - -load-balancer-port 443 - -ssl-certificate-id
arn:aws:iam::123456789012:server-certificate/new-server-
cert
```

D.

```
aws acm put-ssl-certificate - -load-balancer-name my-load-
balancer- -load-balancer-port 443 - -ssl-certificate-id
arn:aws:iam::123456789012:server-certificate/new-server-
cert
```

Answer: B
Reference: https://docs.aws.amazon.com/ko_kr/cli/latest/reference/elb/set-load-balancer-listener-ssl-certificate.html

QUESTION NO: 585

An Amazon EBS volume attached to an EC2 instance was recently modified. Part of the modification included increasing the storage capacity. The SysOps Administrator notices that the increased storage capacity is not reflected in the file system.

Which step should the Administrator complete to use the increased storage capacity?

A.
Restart the EC2 instance.

B.
Extend the volume's file system.

C.
Detach the EBS volume, resize it, and attach it.

D.
Take an EBS snapshot and restore it to the bigger volume.

Answer: A
Reference: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/requesting-ebs-volume-modifications.html

QUESTION NO: 586

A SysOps Administrator is creating additional Amazon EC2 instances and receives an InstanceLimitExceeded error.

What is the cause of the issue and how can it be resolved?

A.
The Administrator has requested too many instances at once and must request fewer instances in batches.

B.
The concurrent running instance limit has been reached, and an EC2 limit increase request must be filed with AWS Support.

C.
AWS does not currently have enough available capacity and a different instance type must be used.

D.
The Administrator must specify the maximum number of instances to be created while provisioning EC2 instances.

Answer: B
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-limit

QUESTION NO: 587

A SysOps Administrator is troubleshooting Amazon EC2 connectivity issues to the internet. The EC2 instance is in a private subnet. Below is the route table that is applied to the subnet of the EC2 instance.

Destination – 10.2.0.0/16

Target – local

Status – Active

Propagated – No

Destination – 0.0.0.0/0

Target – nat-xxxxxxx

Status – Blackhole

Propagated – No

What has caused the connectivity issue?

A.
The NAT gateway no longer exists.

B.
There is no route to the internet gateway.

C.
The routes are no longer propagating.

D.
There is no route rule with a destination for the internet.

Answer: B
Explanation:

QUESTION NO: 588

Malicious traffic is reaching company web servers. A SysOps Administrator is tasked with blocking this traffic. The malicious traffic is distributed over many IP addresses and represents much higher traffic than is typically seen from legitimate users.

How should the Administrator protect the web servers?

A.
Create a security group for the web servers and add deny rules for malicious sources.

B.
Set the network access control list for the web servers' subnet and add deny entries.

C.
Place web servers behind AWS WAF and establish the rate limit to create a blacklist.

D.
Use Amazon CloudFront to cache all pages and remove the traffic from the web servers.

Answer: C
Reference: https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/

QUESTION NO: 589

A SysOps Administrator must evaluate storage solutions to replace a company's current user-shared drives infrastructure. Any solution must support security controls that enable Portable Operating System Interface (POSIX) permissions and Network File System protocols. Additionally, any solution must be accessible from multiple Amazon EC2 instances and on-premises servers connected to the Amazon VPC.

Which AWS service meets the user drive requirements?

A.
Amazon S3

B.
Amazon EFS

C.
Amazon EBS

D.
Amazon SQS

Answer: B
Reference: https://aws.amazon.com/efs/

QUESTION NO: 590

A Developer created an AWS Lambda function and has asked the SysOps Administrator to make this function run every 15 minutes.

What is the MOST efficient way to accomplish this request?

A.
Create an Amazon EC2 instance and schedule a cron to invoke the Lambda function.

B.
Create a Repeat Time variable inside the Lambda function to invoke the Lamdba function.

C.
Create a second Lambda function to monitor and invoke the first Lamdba function.

D.
Create an Amazon CloudWatch scheduled event to invoke the Lambda function.

Answer: D
Reference: https://docs.aws.amazon.com/lambda/latest/dg/with-scheduled-events.html

QUESTION NO: 591

A company's Auditor implemented a compliance requirement that all Amazon S3 buckets must have logging enabled.

How should the SysOps Administrator ensure this compliance requirement is met, while still permitting Developers to create and use new S3 buckets?

A.
Add AWS CloudTrail logging for the S3 buckets.

B.

Implement IAM policies to allow only the Storage team to create S3 buckets.

C.
Add the AWS Config managed rule S3_BUCKET_LOGGING_ENABLED.

D.
Create an AWS Lambda function to delete the S3 buckets if logging is not turned on.

Answer: C
Reference: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html

QUESTION NO: 592

An organization is concerned that its Amazon RDS databases are not protected. The solution to address this issue must be low cost, protect against table corruption that could be overlooked for several days, and must offer a 30-day window of protection.

How can these requirements be met?

A.
Enable Multi-AZ on the RDS instance to maintain the data in a second Availability Zone.

B.
Create a read replica of the RDS instance to maintain the data in a second region.

C.
Ensure that automated backups are enabled and set the appropriate retention period.

D.
Enable versioning in RDS to recover altered table data when needed.

Answer: C
Explanation:

QUESTION NO: 593

An organization is running multiple applications for their customers. Each application is deployed by running a base AWS CloudFormation template that configures a new VPC. All applications are run in the same AWS account and AWS Region. A SysOps Administrator has noticed that when

trying to deploy the same AWS CloudFormation stack, it fails to deploy.

What is likely to be the problem?

A.
The Amazon Machine image used is not available in that region.

B.
The AWS CloudFormation template needs to be updated to the latest version.

C.
The VPC configuration parameters have changed and must be updated in the template.

D.
The account has reached the default limit for VPCs allowed.

Answer: B
Explanation:

QUESTION NO: 594

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

A.
Performing underlying OS updates

B.
Provisioning of storage for database

C.
Scheduling maintenance, patches, and other updates

D.
Executing maintenance, patches, and other updates

Answer: D
Reference: https://www.skyhighnetworks.com/cloud-security-blog/aws-shared-responsibility-model-for-security-and-compliance/

QUESTION NO: 595

A web-commerce application stores its data in an Amazon Aurora DB cluster with an Aurora replica. The application displays shopping cart information by reading data from the reader endpoint. When monitoring the Aurora database, the SysOps Administrator sees that the AuroraReplicaLagMaximum metric for a single replica is high.

What behavior is the application MOST likely exhibiting to users?

A.
Users cannot add any items to the shopping cart.

B.
Users intermittently notice that the cart is not updated correctly.

C.
Users cannot remove any items from the shopping cart.

D.
Users cannot use the application because it is falling back to an error page.

Answer: B
Explanation:

QUESTION NO: 596

A company would like to review each change in the infrastructure before deploying updates in its AWS CloudFormation stacks.

Which action will allow an Administrator to understand the impact of these changes before implementation?

A.
Implement a blue/green strategy using AWS Elastic Beanstalk.

B.
Perform a canary deployment using Application Load Balancers and target groups.

C.
Create a change set for the running stack.

D.

Submit the update using the UpdateStack API call.

Answer: C
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html

QUESTION NO: 597

A Systems Administrator is responsible for maintaining custom, approved AMIs for a company. These AMIs must be shared with each of the company's AWS accounts.

How can the Administrator address this issue?

A.
Contact AWS Support for sharing AMIs with other AWS accounts.

B.
Modify the permissions on the AMIs so that they are publicly accessible.

C.
Modify the permissions on the IAM role that are associated with the AMI.

D.
Share the AMIs with each AWS account using the console or CLI.

Answer: D
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html

QUESTION NO: 598

A company's data retention policy dictates that backups be stored for exactly two years. After that time, the data must be deleted.

How can Amazon EBS snapshots be managed to conform to this data retention policy?

A.
Use an Amazon S3 lifecycle policy to delete snapshots older than two years.

B.
Configure Amazon Inspector to find and delete old EBS snapshots.

C.
Schedule an AWS Lambda function using Amazon CloudWatch Events to periodically run a script to delete old snapshots.

D.
Configure an Amazon CloudWatch alarm to trigger the launch of an AWS CloudFormation template that will clean the older snapshots.

Answer: A

Explanation:

QUESTION NO: 599

A SysOps Administrator must devise a strategy for enforcing tagging of all EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes.

What action can the Administrator take to implement this for real-time enforcement?

A.
Use the AWS Tag Editor to manually search for untagged resources and then tag them properly in the editor.

B.
Set up AWS Service Catalog with the TagOptions Library rule that enforces a tagging taxonomy proactively when instances and volumes are launched.

C.
In a PowerShell or shell script, check for untagged items by using the resource tagging GetResources API action, and then manually tag the reported items.

D.
Launch items by using the AWS API. Use the TagResources API action to apply the required tags when the instances and volumes are launched.

Answer: A

Explanation:

QUESTION NO: 600

During a security investigation, it is determined that there is a coordinated attack on the web applications deployed on Amazon EC2. The attack is performed through malformed HTTP headers.

What AWS service of feature would prevent this traffic from reaching the EC2 instances?

A.
Amazon Inspector

B.
Amazon Security Groups

C.
AWS WAF

D.
Application Load Balancer (ALB)

Answer: C
Reference: https://aws.amazon.com/waf/

QUESTION NO: 601

A company is deploying a legacy web application on Amazon EC2 instances behind an ELB Application Load Balancer. The application worked well in the test environment. However, in production, users report that they are prompted to log in to the system several times an hour.

Which troubleshooting step should be taken to help resolve the problem reported by users?

A.
Confirm that the Application Load Balancer is in a multi-AZ configuration.

B.
Enable health checks on the Application Load Balancer.

C.
Ensure that port 80 is configured on the security group.

D.
Enable sticky sessions on the Application Load Balancer.

Answer: D
Reference: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-alb.html

QUESTION NO: 602

A company has mandated the use of multi-factor authentication (MFA) for all IAM users, and requires users to make all API-calls using the CLI. However, users are not prompted to enter MFA tokens, and are able to run CLI commands without MFA. In an attempt to enforce MFA, the company attached an IAM policy to all users that denies API calls that have not been authenticated with MFA.

What additional step must be taken to ensure that API calls are authenticated using MFA?

A.
Enable MFA on IAM roles, and require IAM users to use role credentials to sign API calls.

B.
Ask the IAM users to log into the AWS Management Console with MFA before making API calls using the CLI.

C.
Restrict the IAM users to use of the console, as MFA is not supported for CLI use.

D.
Require users to use temporary credentials from the get-session token command to sign API calls.

Answer: D
Reference: https://aws.amazon.com/iam/faqs/ (Multi-factor authentication)

QUESTION NO: 603

An application is being developed that will be served across a fleet of Amazon EC2 instances, which require a consistent view of persistent data. Items stored vary in size from 1KB to 300MB; the items are read frequently, created occasionally, and often require partial changes without conflict. The data store is not expected to grow beyond 2TB, and items will be expired according to age and content type.

Which AWS service solution meets these requirements?

A.
Amazon S3 buckets with lifecycle policies to delete old objects.

B.
Amazon RDS PostgreSQL and a job that deletes rows based on age and file type columns.

C.
Amazon EFS and a scheduled process to delete files based on age and extension.

D.
An EC2 instance store synced on boot from a central Amazon EBS-backed instance.

Answer: D
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html

QUESTION NO: 604

A SysOps Administrator created an Amazon VPC with an IPv6 CIDR block, which requires access to the internet. However, access from the internet towards the VPC is prohibited. After adding and configuring the required components to the VPC, the Administrator is unable to connect to any of the domains that reside on the internet.

What additional route destination rule should the Administrator add to the route tables?

A.
Route ::/0 traffic to a NAT gateway

B.
Route ::/0 traffic to an internet gateway

C.
Route 0.0.0.0/0 traffic to an egress-only internet gateway

D.
Route ::/0 traffic to an egress-only internet gateway

Answer: A
Explanation:

QUESTION NO: 605

A recent organizational audit uncovered an existing Amazon RDS database that is not currently configured for high availability. Given the critical nature of this database, it must be configured for high availability as soon as possible.

How can this requirement be met?

A.
Switch to an active/passive database pair using the create-db-instance-read-replica with the - -availability-zone flag.

B.
Specify high availability when creating a new RDS instance, and live-migrate the data.

C.
Modify the RDS instance using the console to include the Multi-AZ option.

D.
Use the modify-db-instance command with the - -ha flag.

Answer: C
Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

QUESTION NO: 606

A company must ensure that any objects uploaded to an S3 bucket are encrypted.

Which of the following actions will meet this requirement? (Choose two.)

A.
Implement AWS Shield to protect against unencrypted objects stored in S3 buckets.

B.
Implement Object access control list (ACL) to deny unencrypted objects from being uploaded to the S3 bucket.

C.
Implement Amazon S3 default encryption to make sure that any object being uploaded is encrypted before it is stored.

D.
Implement Amazon Inspector to inspect objects uploaded to the S3 bucket to make sure that they are encrypted.

E.
Implement S3 bucket policies to deny unencrypted objects from being uploaded to the buckets.

Answer: C,E

Explanation:

Reference: https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html

https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/

QUESTION NO: 607

When the AWS Cloud infrastructure experiences an event that may impact an organization, which AWS service can be used to see which of the organization's resources are affected?

A.
AWS Service Health Dashboard

B.
AWS Trusted Advisor

C.
AWS Personal Health Dashboard

D.
AWS Systems Manager

Answer: C
Reference: https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/management-governance.html

QUESTION NO: 608

A company's static website hosted on Amazon S3 was launched recently, and is being used by tens of thousands of users. Subsequently, website users are experiencing 503 service unavailable errors.

Why are these errors occurring?

A.
The request rate to Amazon S3 is too high.

B.
There is an error with the Amazon RDS database.

C.
The requests to Amazon S3 do not have the proper permissions.

D.
The users are in a different geographical region and Amazon Route 53 is restricting access.

Answer: A
Reference: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/http-503-service-unavailable.html

QUESTION NO: 609

An organization has two AWS accounts: Development and Production. A SysOps Administrator manages access of IAM users to both accounts. Some IAM users in Development should have access to certain resources in Production.

How can this be accomplished?

A.
Create an IAM role in the Production account with the Development account as a trusted entity and then allow those users from the Development account to assume the Production account IAM role.

B.
Create a group of IAM users in the Development account, and add Production account service ARNs as resources in the IAM policy.

C.
Establish a federation between the two accounts using the on-premises Microsoft Active Directory, and allow the Development account to access the Production account through this federation.

D.
Establish an Amazon Cognito Federated Identity between the two accounts, and allow the Development account to access the Production account through this federation.

Answer: A

Explanation:

QUESTION NO: 610

A SysOps Administrator is responsible for managing a set of 12.micro Amazon EC2 instances. The Administrator wants to automatically reboot any instance that exceeds 80% CPU utilization.

Which of these solutions would meet the requirements?

A.
Create an Amazon CloudWatch alarm on the CPUCreditBalance metric and specify a terminate alarm action.

B.
Create an Amazon CloudWatch alarm on the CPUUtilization metric and specify a reboot alarm action.

C.
Create an Amazon CloudWatch alarm on the CPUCreditBalance metric and specify a reboot alarm action.

D.
Create an Amazon CloudWatch alarm on the CPUUtilization metric and specify a terminate alarm action.

Answer: B

Explanation:

QUESTION NO: 611

A company's customers are reporting increased latency while accessing static web content from Amazon S3. A SysOps Administrator observed a very high rate of read operations on a particular S3 bucket.

What will minimize latency by reducing load on the S3 bucket?

A.

Migrate the S3 bucket to a region that is closer to end users' geographic locations.

B.
Use cross-region replication to replicate all of the data to another region.

C.
Create an Amazon CloudFront distribution with the S3 bucket as the origin.

D.
Use Amazon ElastiCache to cache data being served from Amazon S3.

Answer: C
Explanation:

QUESTION NO: 612

A company requires that all access from on-premises applications to AWS services go over its AWS Direct Connect connection rather than the public internet.

How would a SysOps Administrator implement this requirement?

A.
Implement an IAM policy that uses the aws:sourceConnection condition to allow access from the AWS Direct Connect connection ID only

B.
Set up a public virtual interface on the AWS Direct Connect connection

C.
Configure AWS Shield to protect the AWS Management Console from being accessed by IP addresses other than those within the data center ranges

D.
Update all the VPC network ACLs to allow access from the data center IP ranges

Answer: D
Explanation:

QUESTION NO: 613

A SysOps Administrator must find a way to set up alerts when Amazon EC2 service limits are close to being reached.

How can the Administrator achieve this requirement?

A.
Use Amazon Inspector and Amazon CloudWatch Events.

B.
Use AWS Trusted Advisor and Amazon CloudWatch Events.

C.
Use the Personal Health Dashboard and CloudWatch Events.

D.
Use AWS CloudTrail and CloudWatch Events.

Answer: D
Explanation:

QUESTION NO: 614

A web application accepts orders from online users and places the orders into an Amazon SQS queue. Amazon EC2 instances in an EC2 Auto Scaling group read the messages from the queue, process the orders, and email order confirmations to the users. The Auto Scaling group scales up and down based on the queue depth. At the beginning of each business day, users report confirmation emails are delayed.

What action will address this issue?

A.
Create a scheduled scaling action to scale up in anticipation of the traffic.

B.
Change the Auto Scaling group to scale up and down based on CPU utilization.

C.
Change the launch configuration to launch larger EC2 instance types.

D.
Modify the scaling policy to deploy more EC2 instances when scaling up.

Answer: D
Reference: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html

QUESTION NO: 615

A company creates custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template. It installs and configures necessary software through AWS OpsWorks, and takes images of each EC2 instance. The process of installing and configuring software can take between 2 to 3 hours, but at times, the process stalls due to installation errors.

The SysOps Administrator must modify the CloudFormation template so if the process stalls, the entire stack will fail and roll back.

Based on these requirements, what should be added to the template?

A.
Conditions with a timeout set to 4 hours.

B.
CreationPolicy with a timeout set to 4 hours.

C.
DependsOn with a timeout set to 4 hours.

D.
Metadata with a timeout set to 4 hours.

Answer: A
Explanation:

QUESTION NO: 616

A SysOps Administrator must take a team’s single existing AWS CloudFormation template and split it into smaller, service-specific templates. All of the services 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: B
Explanation:

QUESTION NO: 617

After installing and configuring the Amazon CloudWatch agent on an EC2 instance, the anticipated system logs are not being received by CloudWatch Logs.

Which of the following are likely to be the cause of this problem? (Choose two.)

A.
A custom of third-party solution for logs is being used.

B.
The IAM role attached to the EC2 instance does not have the proper permissions.

C.
The CloudWatch agent does not support the operating system used.

D.
A billing constraint is limiting the number of CloudWatch Logs within this account.

E.
The EC2 instance is in a private subnet, and the VPC does not have a NAT gateway.

Answer: B,D
Explanation:

QUESTION NO: 618

A SysOps Administrator found that a newly-deployed Amazon EC2 application server is unable to connect to an existing Amazon RDS database. After enabling VPC Flow Logs and confirming that the flow log is active on the console, the log group cannot be located in Amazon CloudWatch.

What are the MOST likely reasons for this situation? (Choose two.)

A.
The Administrator must configure the VPC Flow Logs to have them sent to AWS CloudTrail.

B.
The Administrator has waited less than ten minutes for the log group to be created in CloudWatch.

C.
The account VPC Flow Logs have been disabled by using a service control policy.

D.
No relevant traffic has been sent since the VPC Flow Logs were created

E.
The account has Amazon GuardDuty enabled.

Answer: A,D
Explanation:

QUESTION NO: 619

An HTTP web application is launched on Amazon EC2 instances behind an ELB Application Load Balancer. The EC2 instances run across multiple Availability Zones. A network ACL and a security group for the load balancer and EC2 instances allow inbound traffic on port 80. After launch, the website cannot be reached over the internet.

What additional step should be taken?

A.
Add a rule to the security group allowing outbound traffic on port 80.

B.
Add a rule to the network ACL allowing outbound traffic on port 80.

C.

Add a rule to the security group allowing outbound traffic on ports 1024 through 65535.

D.
Add a rule to the network ACL allowing outbound traffic on ports 1024 through 65535.

Answer: B
Explanation:

QUESTION NO: 620

A company has an application that is running on an EC2 instance in one Availability Zone. A SysOps Administrator has been tasked with making the application highly available. The Administrator created a launch configuration from the running EC2 instance. The Administrator also properly configured a load balancer.

What step should the Administrator complete next to make the application highly available?

A.
Create an Auto Scaling group by using the launch configuration across at least 2 Availability Zones with a minimum size of 1, desired capacity of 1, and a maximum size of 1.

B.
Create an Auto Scaling group by using the launch configuration across at least 3 Availability Zones with a minimum size of 2, desired capacity of 2, and a maximum of 2.

C.
Create an Auto Scaling group by using the launch configuration across at least 2 regions with a minimum size of 1, desired capacity of 1, and a maximum size of 1.

D.
Create an Auto Scaling group by using the launch configuration across at least 3 regions with a minimum size of 2, desired capacity of 2, and a maximum size of 2.

Answer: A
Explanation:

QUESTION NO: 621

An Applications team has successfully deployed an AWS CloudFormation stack consisting of 30

t2-medium Amazon EC2 instances in the us-west-2 Region. When using the same template to launch a stack in us-east-2, the launch failed and rolled back after launching only 10 EC2 instances.

What is a possible cause of this failure?

A.
The IAM user did not have privileges to launch the CloudFormation template.

B.
The t2.medium EC2 instance service limit was reached.

C.
An AWS Budgets threshold was breached.

D.
The application's Amazon Machine Image (AMI) is not available in us-east-2.

Answer: D
Explanation:

QUESTION NO: 622

A SysOps Administrator stores crash dump files in Amazon S3. New security and privacy measures require that crash dumps older than 6 months be deleted.

Which approach meets this requirement?

A.
Use Amazon CloudWatch Events to delete objects older than 6 months.

B.
Implement lifecycle policies to delete objects older than 6 months.

C.
Use the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class to automatically delete objects older than 6 months.

D.
Create versioning rules to delete objects older than 6 months.

Answer: B

Explanation:

QUESTION NO: 623

The Accounting department would like to receive billing updates more than once a month. They would like the updates to be in a format that can easily be viewed with a spreadsheet application.

How can this request be fulfilled?

A.
Use Amazon CloudWatch Events to schedule a billing inquiry on a bi-weekly basis. Use AWS Glue to convert the output to CSV.

B.
Set AWS Cost and Usage Reports to publish bills daily to an Amazon S3 bucket in CSV format.

C.
Use the AWS CLI to output billing data as JSON. Use Amazon SES to email bills on a daily basis.

D.
Use AWS Lambda, triggered by CloudWatch, to query billing data and push to Amazon RDS.

Answer: B
Explanation:

QUESTION NO: 624

A SysOps Administrator is troubleshooting an AWS CloudFormation template whereby multiple Amazon EC2 instances are being created. The template is working in us-east-1, but it is failing in us-west-2 with the error code:

AMI [ami-12345678] does not exist

How should the Administrator ensure that the AWS CloudFormation template is working in every region?

A.
Copy the source region's Amazon Machine Image (AMI) to the destination region and assign it the

same ID.

B.
Edit the AWS CloudFormation template to specify the region code as part of the fully qualified AMI ID.

C.
Edit the AWS CloudFormation template to offer a drop-down list of all AMIs to the user by using the AWS::EC2::AMI::ImageID control.

D.
Modify the AWS CloudFormation template by including the AMI IDs in the “Mappings” section. Refer to the proper mapping within the template for the proper AMI ID.

Answer: D
Explanation:

QUESTION NO: 625

A SysOps Administrator needs to confirm that security best practices are being followed with the AWS account root user.

How should the Administrator ensure that this is done?

A.
Change the root user password by using the AWS CLI routinely.

B.
Periodically use the AWS CLI to rotate access keys and secret keys for the root user.

C.
Use AWS Trusted Advisor security checks to review the configuration of the root user.

D.
Periodically distribute the AWS compliance document from AWS Artifact that governs the root user configuration.

Answer: B
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

QUESTION NO: 626

The networking team has created a VPC in an AWS account. The application team has asked for access to resources in another VPC in the same AWS account. The SysOps Administrator has created the VPC peering connection between both the accounts, but the resources in one VPC cannot communicate with the resources in the other VPC.

What could be causing this issue?

A.
One of the VPCs is not sized correctly for peering.

B.
There is no public subnet in one of the VPCs.

C.
The route tables have not been updated.

D.
One VPC has disabled the peering flag.

Answer: A
Explanation:

QUESTION NO: 627

An organization has been running their website on several m2 Linux instances behind a Classic Load Balancer for more than two years. Traffic and utilization have been constant and predictable.

What should the organization do to reduce costs?

A.
Purchase Reserved Instances for the specific m2 instances.

B.
Change the m2 instances to equivalent m5 types, and purchase Reserved Instances for the specific m5 instances.

C.
Change the Classic Load Balancer to an Application Load Balancer, and purchase Reserved Instances for the specific m2 instances.

D.
Purchase Spot Instances for the specific m2 instances.

Answer: A
Explanation:

QUESTION NO: 628

A company is storing monthly reports on Amazon S3. The company's security requirement states that traffic from the client VPC to Amazon S3 cannot traverse the internet.

What should the SysOps Administrator do to meet this requirement?

A.
Use AWS Direct Connect and a public virtual interface to connect to Amazon S3.

B.
Use a managed NAT gateway to connect to Amazon S3.

C.
Deploy a VPC endpoint to connect to Amazon S3.

D.
Deploy an internet gateway to connect to Amazon S3.

Answer: C
Explanation:

QUESTION NO: 629

An application resides on multiple EC2 instances in public subnets in two Availability Zones. To improve security, the Information Security team has deployed an Application Load Balancer (ALB) in separate subnets and pointed the DNS at the ALB instead of the EC2 instances.

After the change, traffic is not reaching the instances, and an error is being returned from the ALB.

What steps must a SysOps Administrator take to resolve this issue and improve the security of the application? (Choose two.)

A.
Add the EC2 instances to the ALB target group, configure the health check, and ensure that the instances report healthy.

B.
Add the EC2 instances to an Auto Scaling group, configure the health check to ensure that the instances report healthy, and remove the public IPs from the instances.

C.
Create a new subnet in which EC2 instances and ALB will reside to ensure that they can communicate, and remove the public IPs from the instances.

D.
Change the security group for the EC2 instances to allow access from only the ALB security group, and remove the public IPs from the instances.

E.
Change the security group to allow access from 0.0.0.0/0, which permits access from the ALB.

Answer: B,D

Explanation:

QUESTION NO: 630

A SysOps Administrator is implementing SSL for a domain of an internet-facing application running behind an Application Load Balancer (ALB). The Administrator decides to use an SSL certificate from Amazon Certificate Manager (ACM) to secure it.

Upon creating a request for the ALB fully qualified domain name (FQDN), it fails, and the error message “Domain Not Allowed” is displayed.

How can the Administrator fix this issue?

A.
Contact the domain registrar and ask them to provide the verification required by AWS.

B.
Place a new request with the proper domain name instead of the ALB FQDN

C.
Select the certificate request in the ACM console and resend the validation email.

D.
Contact AWS Support and verify the request by answering security challenge questions.

Answer: C

Explanation:

QUESTION NO: 631

A SysOps Administrator runs a web application that is using a microservices approach whereby different responsibilities of the application have been divided in a separate microservice running on a different Amazon EC2 instance. The Administrator has been tasked with reconfiguring the infrastructure to support this approach.

How can the Administrator accomplish this with the LEAST administrative overhead?

A.
Use Amazon CloudFront to log the URL and forward the request.

B.
Use Amazon CloudFront to rewrite the header based on the microservice and forward the request.

C.
Use an Application Load Balancer (ALB) and do path-based routing.

D.
Use a Network Load Balancer (NLB) and do path-based routing.

Answer: C
Reference: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html

QUESTION NO: 632

A company is running a popular social media site on EC2 instances. The application stores data in an Amazon RDS for MySQL DB instance and has implemented read caching by using an ElastiCache for Redis (cluster mode enabled) cluster to improve read times. A social event is happening over the weekend, and the SysOps Administrator expects website traffic to triple.

What can a SysOps Administrator do to ensure improved read times for users during the social event?

A.
Use Amazon RDS Multi-AZ.

B.
Add shards to the existing Redis cluster.

C.
Offload static data to Amazon S3.

D.
Launch a second Multi-AZ Redis cluster.

Answer: B
Explanation:

QUESTION NO: 633

After a particularly high AWS 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 share it, and will also forecast expenses for the current billing period?

A.
AWS Trusted Advisor

B.
Amazon QuickSight

C.
AWS Cost and Usage Report

D.
AWS Cost Explorer

Answer: D
Reference: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-forecast.html

QUESTION NO: 634

A company has adopted a security policy that requires all customer data to be encrypted at rest. Currently, customer data is stored on a central Amazon EFS file system and accessed by a number of different applications from Amazon EC2 instances.

How can the SysOps Administrator ensure that all customer data stored on the EFS file system meets the new requirement?

A.
Update the EFS file system settings to enable server-side encryption using AES-256.

B.
Create a new encrypted EFS file system and copy the data from the unencrypted EFS file system to the new encrypted EFS file system.

C.
Use AWS CloudHSM to encrypt the files directly before storing them in the EFS file system.

D.
Modify the EFS file system mount options to enable Transport Layer Security (TLS) on each of the EC2 instances.

Answer: B

Explanation:

QUESTION NO: 635

The Database Administration team is interested in performing manual backups of an Amazon RDS Oracle DB instance.

What steps should be taken to perform the backups?

A.
Attach an Amazon EBS volume with Oracle RMAN installed to the RDS instance.

B.
Take a snapshot of the EBS volume that is attached to the DB instance.

C.
Install Oracle Secure Backup on the RDS instance and back up the Oracle database to Amazon S3.

D.
Take a snapshot of the DB instance.

Answer: D
Reference: https://aws.amazon.com/rds/faqs/

QUESTION NO: 636

An Auto Scaling group scales up and down based on Average CPU Utilization. The alarm is set to trigger a scaling event when the Average CPU Utilization exceeds 80% for 5 minutes. Currently, the Average CPU has been 95% for over two hours and new instances are not being added.

What could be the issue?

A.
A scheduled scaling action has not been defined.

B.
In the field Suspend Process, “ReplacesUnhealthy” has been selected.

C.
The maximum size of the Auto Scaling group is below or at the current group size.

D.
The Health Check Grace Period is set to less than 300 seconds.

Answer: C
Explanation:

QUESTION NO: 637

An application running on Amazon EC2 instances needs to write files to an Amazon S3 bucket.

What is the MOST secure way to grant the application access to the S3 bucket?

A.
Create an IAM user with the necessary privileges. Generate an access key and embed the key in the code running on the EC2 instances.

B.
Install secure FTP (SFTP) software on the EC2 instances. Use an AWS Lambda function to copy

the files from the EC2 instances to Amazon S3 using SFTP.

C.
Create an IAM role with the necessary privileges. Associate the role with the EC2 instances at launch.

D.
Use rsync and cron to set up the transfer of files from the EC2 instances to the S3 bucket. Enable AWS Shield to protect the data.

Answer: C
Explanation:

QUESTION NO: 638

In configuring an Amazon Route 53 health check, a SysOps Administrator selects ‘Yes’ to the String Matching option in the Advanced Configuration section. In the Search String box, the Administrator types the following text: /html.

This is to ensure that the entire page is loading during the health check. Within 5 minutes of enabling the health check, the Administrator receives an alert stating that the check failed. However, when the Administrator navigates to the page, it loads successfully.

What is the MOST likely cause of this false alarm?

A.
The search string is not HTML-encoded.

B.
The search string must be put in quotes.

C.
The search string must be escaped with a backslash (\) before the forward slash (/).

D.
The search string is not in the first 5120 bytes of the tested page.

Answer: A
Explanation:

QUESTION NO: 639

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 are 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: B
Reference: https://aws.amazon.com/blogs/security/how-to-create-a-limited-iam-administrator-by-using-managed-policies/

QUESTION NO: 640

Company A purchases Company B and inherits three new AWS accounts. Company A would like to centralize billing and Reserved Instance benefits but wants to keep all other resources separate.

How can this be accomplished?

A.
Implement AWS Organizations and create a service control policy that defines the billing relationship with the new master account.

B.
Configure AWS Organizations Consolidated Billing and provide the finance team with IAM access

to the billing console.

C.
Send Cost and Usage Reports files to a central Amazon S3 bucket, and load the data into Amazon Redshift. Use Amazon QuickSight to provide visualizations to the finance team.

D.
Link the Reserved Instances to the master payer account and use Amazon Redshift Spectrum to query Detailed Billing Report data across all accounts.

Answer: B
Explanation:

QUESTION NO: 641

A website uses Elastic Load Balancing (ELB) in front of several Amazon EC2 instances backed by an Amazon RDS database. The content is dynamically generated for visitors of a webpage based on their geographic location. and is updated daily. Some of the generated objects are large in size and are taking longer to download than they should, resulting in a poor user experience.

Which approach will improve the user experience?

A.
Implement Amazon ElastiCache to cache the content and reduce the load on the database.

B.
Enable an Amazon CloudFront distribution with Elastic Load Balancing as a custom origin.

C.
Use Amazon S3 to store and deliver the content.

D.
Enable Auto Scaling for the EC2 instances so that they can scale automatically.

Answer: A
Explanation:

QUESTION NO: 642

While setting up an AWS managed VPN connection, a SysOPs Administrator creates a customer gateway resource in AWS. The customer gateway device resides in a data center with a NAT gateway in front of it.

What address should be used to create the customer gateway resource?

A.
The private IP address of the customer gateway device

B.
The MAC address of the NAT device in front of the customer gateway device

C.
The public IP address of the customer gateway device

D.
The public IP address of the NAT device in front of the customer gateway device

Answer: D
Reference: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

QUESTION NO: 643

A SysOps Administrator attempting to delete an Amazon S3 bucket ran the following command:
aws s3 rb s3://my bucket

The command failed and bucket still exists. The administrator validated that no files existed in the bucket by running aws s3 1s s3://mybucket and getting an empty response.

Why is the Administrator unable to delete the bucket, and what must be done to accomplish this task?

A.
The bucket has MFA Delete enabled, and the Administrator must turn it off.

B.
The bucket has versioning enabled, and the Administrator must permanently delete the objects' delete markers.

C.
The bucket is storing files in Amazon Glacier, and the Administrator must wait 3-5 hours for the files to delete.

D.
The bucket has server-side encryption enabled, and the Administrator must run the aws s3 rb s3://my bucket -- sse command.

Answer: D
Explanation:

QUESTION NO: 644

A SysOps Administrator must provide data to show the overall usage of Amazon EC2 instances within each department, and must determine if the purchased Reserved Instances are being used effectively.

Which service should be used to provide the necessary information?

A.
AWS Personal Health Dashboard

B.
AWS Cost Explorer

C.
AWS Service Catalog

D.
AWS Application Discovery Service

Answer: B
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usage-reports.html

QUESTION NO: 645

A company has multiple web applications running on Amazon EC2 instances in private subnets. The EC2 instances require connectivity to the internet for patching purposes, but cannot be publicly accessible.

Which step will meet these requirements?

A.
Add an internet gateway and update the route tables.

B.
Add a NAT gateway to the VPC and update the route tables.

C.
Add an interface endpoint and update the route tables.

D.
Add a virtual gateway to the VPC and update the route tables.

Answer: B
Reference: http://jayendrapatil.com/aws-vpc-nat/

QUESTION NO: 646

A company has 50 AWS accounts and wants to create an identical Amazon VPC in each account. Any changes the company makes to the VPCs in the future must be implemented on every VPC.

What is the SIMPLEST method to deploy and update the VPCs in each account?

A.
Create an AWS CloudFormation template defines the VPC. Log in to the AWS Management Console under each account and create a stack from the template.

B.
Create a shell script that configures the VPC using the AWS CLI. Provide a list of accounts to the script from a text file, then create the VPC in every account in the list.

C.
Create an AWS Lambda function that configures the VPC. Store the account information in Amazon DynamoDB, grant Lambda access to the DynamoDB table, then create the VPC in every account in the list.

D.
Create an AWS CloudFormation template that defines the VPC. Create an AWS CloudFormation StackSet based on the template, then deploy the template to all accounts using the stack set.

Answer: D
Explanation:

QUESTION NO: 647

After a network change, application servers cannot connect to the corresponding Amazon RDS MySQL database.

What should the SysOps Administrator analyze?

A.
VPC Flow Logs

B.
Elastic Load Balancing logs

C.
Amazon CloudFront logs

D.
Amazon RDS MySQL error logs

Answer: D
Reference:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html

QUESTION NO: 648

A company wants to ensure that each department operates within their own isolated environment, and they are only able to use pre-approved services.

How can this requirement be met?

A.
Set up an AWS Organization to create accounts for each department, and apply service control policies to control access to AWS services.

B.
Create IAM roles for each department, and set policies that grant access to specific AWS services.

C.
Use the AWS Service Catalog to create catalogs of AWS services that are approved for use by

each department.

D.
Request that each department create and manage its own AWS account and the resources within it.

Answer: A
Explanation:

QUESTION NO: 649

A SysOps Administrator is receiving multiple reports from customers that they are unable to connect to the company's website. which is being served through Amazon CloudFront. Customers are receiving HTTP response codes for both 4XX and 5XX errors.

Which metric can the Administrator use to monitor the elevated error rates in CloudFront?

A.
TotalErrorRate

B.
RejectedConnectionCount

C.
NetworkTransmitThroughput

D.
HealthyHostCount

Answer: A
Reference: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/monitoring-using-cloudwatch.html

QUESTION NO: 650

A company is using AWS Organizations to manage all their accounts. The Chief Technology Officer wants to prevent certain services from being used within production accounts until the services have been internally certified. They are willing to allow developers to experiment with these uncertified services in development accounts but need a way to ensure that these services

are not used within production accounts.

Which option ensures that services are not allowed within the production accounts, yet are allowed in separate development accounts within the LEAST administrative overhead?

A.
Use AWS Config to shut down non-compliant services found within the production accounts on a periodic basis, while allowing these same services to run in the development accounts.

B.
Apply service control policies to the AWS Organizational Unit (OU) containing the production accounts to whitelist certified services. Apply a less restrictive policy to the OUs containing the development accounts.

C.
Use IAM policies applied to the combination of user and account to prevent developers from using these services within the production accounts. Allow the services to run in development accounts.

D.
Use Amazon CloudWatch to report on the use of non-certified services within any account, triggering an AWS Lambda function to terminate only those non-certified services when found in a production account.

Answer: B
Explanation:

QUESTION NO: 651

A SysOps Administrator has configured health checks on a load balancer. An Amazon EC2 instance attached to this load balancer fails the health check.

What will happen next? (Choose two.)

A.
The load balancer will continue to perform the health check on the EC2 instance.

B.
The EC2 instance will be terminated based on the health check failure.

C.
The EC2 instance will be rebooted.

D.

The load balancer will stop sending traffic to the EC2 instance.

E.
A new EC2 instance will be deployed to replace the unhealthy instance.

Answer: A,D
Explanation:

QUESTION NO: 652

An Application performs read-heavy operations on an Amazon Aurora DB instance. The SysOps Administrator monitors the CPUUtilization CloudWatch metric and has recently seen it increase to 90%. The Administrator would like to understand what is driving the CPU surge.

Which of the following should be Administrator additionally monitor to understand the CPU surge?

A.
FreeableMemory and DatabaseConnections to understand the amount of available RAM and number of connections to DB instance.

B.
FreeableMemory and EngineUptime to understand the amount of available RAM and the amount of time the instance has been up and running.

C.
DatabaseConnections and AuroraReplicaLag for the number of connections to the DB instance and the amount of lag when replicating updates from the primary instance.

D.
DatabaseConnections and InsertLatency for the number of connections to the DB instance and latency for insert queries.

Answer: D
Explanation:

QUESTION NO: 653

A SysOps Administrator must use a bastion host to administer a fleet of Amazon EC2 instances. All access to the bastion host is managed by the Security team.

What is the MOST secure way for the Security team to provide the SysOps Administrator access to the bastion host?

A.
Assign the same IAM role to the Administrator that is assigned to the bastion host.

B.
Provide the Administrator with the SSH key that was used for the bastion host when it was originally launched.

C.
Create a new IAM role with the same permissions as the Security team, and assign it to the Administrator.

D.
Create a new administrative account on the bastion host, and provide those credentials to the Administrator using AWS Secrets Manager.

Answer: B
Reference: https://cloud.ibm.com/docs/tutorials?topic=solution-tutorials-vpc-secure-management-bastion-server

QUESTION NO: 654

A database is running on an Amazon RDS Multi-AZ DB instance. A recent security audit found the database to be out of compliance because it was not encrypted.

Which approach will resolve the encryption requirement?

A.
Log in to the RDS console and select the encryption box to encrypt the database.

B.
Create a new encrypted Amazon EBS volume and attach it to the instance.

C.
Encrypt the standby replica in the secondary Availability Zone and promote it to the primary instance.

D.
Take a snapshot of the RDS instance, copy and encrypt the snapshot, and then restore to the new RDS instance.

Answer: A

Explanation:

QUESTION NO: 655

An Amazon EC2 instance is unable to connect an SMTP server in a different subnet. Other instances are successfully communicating with the SMTP server, however VPC 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

What can be done to correct this problem?

A.
Add the instance to the security group for the SMTP server and ensure that is permitted to communicate over TCP port 25.

B.
Disable the iptables service on the SMTP server so that the instance can properly communicate over the network.

C.
Install an email client on the instance to ensure that it communicates correctly on TCP port 25 to the SMTP server.

D.
Add a rule to the security group for the instance to explicitly permit TCP port 25 outbound to any address.

Answer: D

Explanation:

QUESTION NO: 656

A company's use of AWS Cloud services is quickly growing, so a SysOps Administrator has been asked to generate details of daily spending to share with management.

Which method should the Administrator choose to produce this data?

A.
Share the monthly AWS bill with management.

B.
Use AWS CloudTrail Logs to access daily costs in JSON format.

C.
Set up a daily Cost and Usage Report and download the output from Amazon S3.

D.
Monitor AWS costs with Amazon CloudWatch and create billing alerts and notifications.

Answer: C
Explanation:

QUESTION NO: 657

A company's Security team wants to track data encryption events across all company AWS accounts. The team wants to capture all AWS KMS events related to deleting or rotating customer master keys (CMKs) from all production AWS accounts. The KMS events will be sent to the Security team's AWS account for monitoring.

How can this be accomplished?

A.
Create an AWS Lambda function that will run every few minutes in each production account, parse the KMS log for KMS events, and sent the information to an Amazon SQS queue managed by the Security team.

B.
Create an event bus in the Security team's account, create a new Amazon CloudWatch Events rule that matches the KMS events in each production account, and then add the Security team's event bus as the target.

C.
Set up AWS CloudTrail for KMS events in every production account, and have the logs sent to an Amazon S3 bucket that is managed by the Security team.

D.
Create an AWS Config rule that checks for KMS keys that are in a pending deletion or rotated state in every production account, then send Amazon SNS notifications of any non-compliant KMS

resources to the Security team.

Answer: B

Explanation:

QUESTION NO: 658

A workload has been moved from a data center to AWS. Previously, vulnerability scans were performed nightly by an external testing company. There is a mandate to continue the vulnerability scans in the AWS environment with third-party testing occurring at least once each month.

What solution allows the vulnerability scans to continue without violating the AWS Acceptable Use Policy?

A.
The existing nightly scan can continue with a few changes. The external testing company must be notified of the new IP address of the workload and the security group of the workload must be modified to allow scans from the external company's IP range.

B.
If the external company is a vendor in the AWS Marketplace, notify them of the new IP address of the workload.

C.
Submit a penetration testing request every 90 days and have the external company test externally when the request is approved.

D.
AWS performs vulnerability testing behind the scenes daily and patches instances as needed. If a vulnerability cannot be automatically addressed, a notification email is distributed.

Answer: A

Explanation:

QUESTION NO: 659

A SysOps Administrator is writing a utility that publishes resources from an AWS Lambda function in AWS Account A to an Amazon S3 bucket in AWS Account B. The Lambda function is able to successfully write new objects to the S3 bucket, but IAM users in Account B are unable to delete

objects written to the bucket by Account A.

Which step will fix this issue?

A.
Add s3:DeleteObject permission to the IAM execution role of the AWS Lambda function in Account A.

B.
Change the bucket policy of the S3 bucket in Account B to allow s3:DeleteObject permission for Account A.

C.
Disable server-side encryption for objects written to the S3 bucket by the Lambda function.

D.
Call the S3:PutObjectAcl API operation from the Lambda function in Account A to specify bucket owner, full control.

Answer: D
Explanation:

QUESTION NO: 660

An organization would like to set up an option for its Developers to receive an email whenever production Amazon EC2 instances are running over 80% CPU utilization.

How can this be accomplished using an Amazon CloudWatch alarm?

A.
Configure the alarm to send emails to subscribers using Amazon SES.

B.
Configure the alarm to send emails to subscribers using Amazon SNS.

C.
Configure the alarm to send emails to subscribers using Amazon Inspector.

D.
Configure the alarm to send emails to subscribers using Amazon Cognito.

Answer: B

Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html

QUESTION NO: 661

Which of the following steps are required to configure SAML 2.0 for federated access to AWS? (Choose two.)

A.
Create IAM users for each identity provider (IdP) user to allow access to the AWS environment.

B.
Define assertions that map the company's identity provider (IdP) users to IAM roles.

C.
Create IAM roles with a trust policy that lists the SAML provider as the principal.

D.
Create IAM users, place them in a group named SAML, and grant them necessary IAM permissions.

E.
Grant identity provider (IdP) users the necessary IAM permissions to be able to log in to the AWS environment.

Answer: A,B

Explanation:

QUESTION NO: 662

A SysOps Administrator is attempting to download patches from the internet into an instance in a private subnet. An internet gateway exists for the VPC, and a NAT gateway has been deployed on the public subnet; however, the instance has no internet connectivity. The resources deployed into the private subnet must be inaccessible directly from the public internet.

Public Subnet (10.0.1.0/24) Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Private Subnet (10.0.2.0/24) Route Table

Destination	Target
10.0.0.0/16	local

BrainDumps

What should be added to the private subnet's route table in order to address this issue, given the information provided.

A.
0.0.0.0/0IGW

B.
0.0.0.0/0NAT

C.
10.0.1.0/24 IGW

D.
10.0.1.0/24NAT

Answer: B
Explanation:

QUESTION NO: 663

A SysOps Administrator is responsible for a large fleet of EC2 instances and must know whether any instances will be affected by upcoming hardware maintenance.

Which option would provide this information with the LEAST administrative overhead?

A.
Monitor AWS CloudTrail for StopInstances API calls related to upcoming maintenance.

B.
Review the Personal Health Dashboard for any scheduled maintenance.

C.
From the AWS Management Console, list any instances with failed system status checks.

D.
Deploy a third-party monitoring solution to provide real-time EC2 instance monitoring.

Answer: C
Explanation:

QUESTION NO: 664

An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba41fc, and it is actively used by 10 Amazon EC2 hosts. The organization has become concerned that the file system is not encrypted.

How can this be resolved?

A.
Enable encryption on each host's connection to the Amazon EFS volume. Each connection must be recreated for encryption to take effect.

B.
Enable encryption on the existing EFS volume by using the AWS Command Line Interface.

C.
Enable encryption on each host's local drive. Restart each host to encrypt the drive.

D.
Enable encryption on a newly created volume and copy all data from the original volume. Reconnect each host to the new volume.

Answer: D
Explanation:

QUESTION NO: 665

An organization finds that a high number of gp2 Amazon EBS volumes are running out of space.

Which solution will provide the LEAST disruption with MINIMAL effort?

A.
Create a snapshot and restore it to a larger gp2 volume.

B.
Create a RAID 0 with another new gp2 volume to increase capacity.

C.
Leverage the Elastic Volumes feature of EBS to increase gp2 volume size.

D.
Write a script to migrate data to a larger gp2 volume.

Answer: C
Reference: https://aws.amazon.com/ebs/features/

QUESTION NO: 666

An e-commerce company wants to lower costs on its nightly jobs that aggregate the current day's sales and store the results in Amazon S3. The jobs are currently run using multiple on-demand instances and the jobs take just under 2 hours to complete. If a job fails for any reason, it needs to be restarted from the beginning.

What method is the MOST cost effective based on these requirements?

A.
Use a mixture of On-Demand and Spot Instances for job execution.

B.
Submit a request for a Spot block to be used for job execution.

C.
Purchase Reserved Instances to be used for job execution.

D.
Submit a request for a one-time Spot Instance for job execution.

Answer: C
Explanation:

QUESTION NO: 667

An existing data management application is running on a single Amazon EC2 instance and needs to be moved to a new AWS Region in another AWS account.

How can a SysOps Administrator achieve this while maintaining the security of the application?

A.
Create an encrypted Amazon Machine Image (AMI) of the instance and make it public to allow the other account to search and launch an instance from it.

B.
Create an AMI of the instance, add permissions for the AMI to the other AWS account, and start a new instance in the new region by using that AMI.

C.
Create an AMI of the instance, copy the AMI to the new region, add permissions for the AMI to the other AWS account, and start new instance.

D.
Create an encrypted snapshot of the instance and make it public. Provide only permissions to decrypt to the other AWS account.

Answer: B

Explanation:

QUESTION NO: 668

A SysOps Administrator manages an application that stores object metadata in Amazon S3. There is a requirement to have S2 server-side encryption enabled on all new objects in the bucket.

How can the Administrator ensure that all new objects to the bucket satisfy this requirement?

A.
Create an S3 lifecycle rule to automatically encrypt all new objects.

B.
Enable default bucket encryption to ensure that all new objects are encrypted.

C.
Use put-object-acl to allow objects to be encrypted with S2 server-side encryption.

D.
Apply the authorization header to S3 requests for S3 server-side encryption.

Answer: B

Explanation:

QUESTION NO: 669

A company is using an AWS KMS customer master key (CMK) with imported key material. The company references the CMK by its alias in the Java application to encrypt data. The CMK must be rotated every 6 months.

What is the process to rotate the key?

A.
Enable automatic key rotation for the CMK, and specify a period of 6 months.

B.
Create a new CMK with new imported material, and update the key alias to point to the new CMK.

C.
Delete the current key material, and import new material into the existing CMK.

D.
Import a copy of the existing key material into a new CMK as a backup, and set the rotation schedule for 6 months.

Answer: A

Explanation:

Cryptographic best practices discourage extensive reuse of encryption keys. To create new cryptographic material for your AWS Key Management Service (AWS KMS) customer master keys (CMKs), you can create new CMKs, and then change your applications or aliases to use the new CMKs. Or, you can enable automatic key rotation for an existing CMK.

When you enable automatic key rotation for a customer managed CMK, AWS KMS generates new cryptographic material for the CMK every year. AWS KMS also saves the CMK's older cryptographic material in perpetuity so it can be used to decrypt data that it encrypted. AWS KMS does not delete any rotated key material until you delete the CMK.

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

QUESTION NO: 670

The Security team has decided that there will be no public internet access to HTTP (TCP port 80) because it is moving to HTTPS for all incoming web traffic. The team has asked a SysOps Administrator to provide a report on any security groups that are not compliant.

What should the SysOps Administrator do to provide near real-time compliance reporting?

A.
Enable AWS Trusted Advisor and show the Security team that the Security Groups unrestricted access check will alarm.

B.
Schedule an AWS Lambda function to run hourly to scan and evaluate all security groups, and send a report to the Security team.

C.
Use AWS Config to enable the restricted-common-ports rule, and add port 80 to the parameters.

D.
Use Amazon Inspector to evaluate the security groups during scans, and send the completed reports to the Security team.

Answer: D
Explanation:

QUESTION NO: 671

A SysOps Administrator has configured a CloudWatch agent to send custom metrics to Amazon CloudWatch and is now assembling a CloudWatch dashboard to display these metrics.

What steps should the Administrator take to complete this task?

A.
Select the AWS Namespace, filter by metric name, then add to the dashboard.

B.
Add a text widget, select the appropriate metric from the custom namespace, then add to the dashboard.

C.
Select the appropriate widget and metrics from the custom namespace, then add to the

dashboard.

D.
Open the CloudWatch console, from the CloudWatch Events, add all custom metrics.

Answer: D
Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create_dashboard.html

QUESTION NO: 672

An application is running on multiple EC2 instances. As part of an initiative to improve overall infrastructure security, the EC2 instances were moved to a private subnet. However, since moving, the EC2 instances have not been able to automatically update, and a SysOps Administrator has not been able to SSH into them remotely.

Which two actions could the Administrator take to securely resolve these issues? (Choose two.)

A.
Set up a bastion host in a public subnet, and configure security groups and route tables accordingly.

B.
Set up a bastion host in the private subnet, and configure security groups accordingly.

C.
Configure a load balancer in a public subnet, and configure the route tables accordingly.

D.
Set up a NAT gateway in a public subnet, and change the private subnet route tables accordingly.

E.
Set up a NAT gateway in a private subnet, and ensure that the route tables are configured accordingly.

Answer: A,D
Explanation:

QUESTION NO: 673

A SysOps Administrator has been tasked with deploying a company's infrastructure as code. The Administrator wants to write a single template that can be reused for multiple environments in a safe, repeatable manner.

What is the recommended way to use AWS CloudFormation to meet this requirement?

A.
Use parameters to provision the resources.

B.
Use nested stacks to provision the resources.

C.
Use Amazon EC2 user data to provision the resources.

D.
Use stack policies to provision the resources.

Answer: A
Explanation:

QUESTION NO: 674

An application accesses data through a file system interface. The application runs on Amazon EC2 instances in multiple Availability Zones, all of which must share the same data. While the amount of data is currently small, the company anticipates that it will grow to tens of terabytes over the lifetime of the application.

What is the MOST scalable storage solution to fulfill the requirement?

A.
Connect a large Amazon EBS volume to multiple instances and schedule snapshots.

B.
Deploy Amazon EFS is in the VPC and create mount targets in multiple subnets.

C.
Launch an EC2 instance and share data using SMB/CIFS or NFS.

D.
Deploy an AWS Storage Gateway cached volume on Amazon EC2.

Answer: D

Explanation:

QUESTION NO: 675

A company has Sales department and Marketing department. The company uses one AWS account. There is a need to determine what charges are incurred on the AWS platform by each department. There is also a need to receive notifications when a specified cost level is approached or exceeded.

Which two actions must a SysOps Administrator take to achieve both requirements with the LEAST amount of administrative overhead? (Choose two.)

A.
Use AWS Trusted Advisor to obtain a report containing the checked items in the Cost Optimization pillar.

B.
Download the detailed billing report, upload it to a database, and match the line items with a list of known resources by department.

C.
Create a script by using the AWS CLI to automatically apply tags to existing resources to each department. Schedule the script to run weekly.

D.
Use AWS Organizations to create a department Organizational Unit and allow only authorized personnel in each department to create resources.

E.
Create a Budget from the Billing and Cost Management console. Specify the budget type a Cost, assign tags for each department, define notifications, and specify any other options as required.

Answer: D,E

Explanation:

QUESTION NO: 676

A company has two AWS accounts: development and production. All applications send logs to a specific Amazon S3 bucket for each account, and the Developers are requesting access to the

production account S3 buckets to view the logs.

Which is the MOST efficient way to provide the Developers with access?

A.
Create an AWS Lambda function with an IAM role attached to it that has access to both accounts' S3 buckets. Pull the logs from the production S3 bucket to the development S3 bucket.

B.
Create IAM users for each Developer on the production account, and add the Developers to an IAM group that provides read-only access to the S3 log bucket.

C.
Create an Amazon EC2 bastion host with an IAM role attached to it that has access to the production S3 log bucket, and then provision access for the Developers on the host.

D.
Create a resource-based policy for the S3 bucket on the production account that grants access to the development account, and then delegate access in the development account.

Answer: B

Explanation:

QUESTION NO: 677

A company's application stores documents within an Amazon S3 bucket. The application is running on Amazon EC2 in a VPC. A recent change in security requirements states that traffic between the company's application and the S3 bucket must never leave the Amazon network.

What AWS feature can provide this functionality?

A.
Security groups

B.
NAT gateways

C.
Virtual private gateway

D.
Gateway VPC endpoints

Answer: D

Explanation:

Explanation

When using VPC with S3, use VPC S3 endpoints as

are horizontally scaled, redundant, and highly available VPC components

help establish a private connection between VPC and S3 and the traffic never leaves the Amazon network

QUESTION NO: 678

A SysOps Administrator is running an auto-scaled application behind a Classic Load Balancer. Scaling out is triggered when the CPUUtilization instance metric is more than 75% across the Auto Scaling group. The Administrator noticed aggressive scaling out and after discussing with developers, an application memory leak is suspected causing aggressive garbage collection cycle.

How can the Administrator troubleshoot the application without triggering the scaling process?

A.
Suspend the scaling process before troubleshooting.

B.
Delete the Auto Scaling group and recreate it when troubleshooting is complete.

C.
Remove impacted instances from the Classic Load Balancer.

D.
Create a scale down trigger when the CPUUtilization instance metric is at 70%.

Answer: A

Explanation:

QUESTION NO: 679

A company backs up data from its data center using a tape gateway on AWS Storage Gateway. The SysOps Administrator needs to reboot the virtual machine running Storage Gateway.

What process will protect data integrity?

A.
Stop Storage Gateway and reboot the virtual machine, then restart Storage Gateway.

B.
Reboot the virtual machine, then restart Storage Gateway.

C.
Reboot the virtual machine.

D.
Shut down the virtual machine and stop Storage Gateway, then turn on the virtual machine.

Answer: A
Explanation:

QUESTION NO: 680

An organization has decided to consolidate storage and move all of its backups and archives to Amazon S3. With all of the data gathered into a hierarchy under a single directory, the organization determines there is 70 TB of data that needs to be uploaded. The organization currently has a 150-Mbps connection with 10 people working at the location.

Which service would be the MOST efficient way to transfer this data to Amazon S3?

A.
AWS Snowball

B.
AWS Direct Connect

C.
AWS Storage Gateway

D.
Amazon S3 Transfer Acceleration

Answer: D
Explanation:

QUESTION NO: 681

A SysOps Administrator is deploying a legacy web application on AWS. The application has four Amazon EC2 instances behind a Classic Load Balancer and stores data in an Amazon RDS instance. The legacy application has known vulnerabilities to SQL injection attacks, but the application code is no longer available to update.

What cost-effective configuration change should the Administrator make to mitigate the risk of SQL injection attacks?

A.
Configure Amazon GuardDuty to monitor the application for SQL injection threats.

B.
Configure AWS WAF with a Classic Load Balancer for protection against SQL injection attacks.

C.
Replace the Classic Load Balancer with an Application Load Balancer and configure AWS WAF on the Application Load Balancer.

D.
Configure an Amazon CloudFront distribution with the Classic Load Balancer as the origin and subscribe to AWS Shield Standard.

Answer: B
Reference: http://jayendrapatil.com/page/15/?cat=-1

QUESTION NO: 682

A fleet of servers must send local logs to Amazon CloudWatch.

How should the servers be configured to meet this requirement?

A.
Configure AWS Config to forward events to CloudWatch.

B.
Configure a Simple Network Management Protocol (SNMP) agent to forward events to CloudWatch.

C.

Install and configure the unified CloudWatch agent.

D.
Install and configure the Amazon Inspector agent.

Answer: C
Explanation:

QUESTION NO: 683

According to the shared responsibility model, for which of the following Amazon EC2 activities is AWS responsible? (Choose two.)

A.
Patching the guest operating system

B.
Monitoring memory utilization

C.
Configuring network ACLs

D.
Patching the hypervisor

E.
Maintaining network infrastructure

Answer: D,E
Reference: https://aws.amazon.com/compliance/shared-responsibility-model/

QUESTION NO: 684

A company monitors its account activity using AWS CloudTrail, and is concerned that some log files are being tampered with after the logs have been delivered to the account's Amazon S3 bucket.

Moving forward, how can the SysOps Administrator confirm that the log files have not been modified after being delivered to the S3 bucket?

A.
Stream the CloudTrail logs to Amazon CloudWatch Logs to store logs at a secondary location.

B.
Enable log file integrity validation and use digest files to verify the hash value of the log file.

C.
Replicate the S3 log bucket across regions, and encrypt log files with S3 managed keys.

D.
Enable S3 server access logging to track requests made to the log bucket for security audits.

Answer: B
Explanation:

CloudTrail log file integrity validation can be used to check whether a log file was modified, deleted, or unchanged after CloudTrail delivered it

QUESTION NO: 685

After launching a new Amazon EC2 instance from a Microsoft Windows 2012 Amazon Machine Image (AMI), the SysOps Administrator is unable to connect to the instance using Remote Desktop Protocol (RDP). The instance is also unreachable. As part of troubleshooting, the Administrator deploys a second instance from a different AMI using the same configuration and is able to connect to the instance.

What should be the next logical step in troubleshooting the first instance?

A.
Use AWS Trusted Advisor to gather operating system log files for analysis.

B.
Use VPC Flow Logs to gather operating system log files for analysis.

C.
Use EC2Rescue to gather operating system log files for analysis.

D.
Use Amazon Inspector to gather operating system log files for analysis.

Answer: C
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/troubleshoot-remote-desktop-connection-ec2-windows/

QUESTION NO: 686

A custom application must be installed on all Amazon EC2 instances. The application is small, updated frequently and can be installed automatically.

How can the application be deployed on new EC2 instances?

A.
Launch a script that downloads and installs the application using the Amazon EC2 user data.

B.
Create a custom API using Amazon API Gateway to call an installation executable from an AWS CloudFormation Template.

C.
Use AWS Systems Manager to inject the application into an AMI.

D.
Configure AWS CodePipeline to deploy code changes and updates.

Answer: A
Explanation:

QUESTION NO: 687

A SysOps Administrator noticed that the cache hit ratio for an Amazon CloudFront distribution is less than 10%.

Which collection of configuration changes will increase the cache hit ratio for the distribution? (Choose two.)

A.
Ensure that only required cookies, query strings, and headers are forwarded in the Cache Behavior Settings

B.
Change the Viewer Protocol Policy to use HTTPS only

C.
Configure the distribution to use presigned cookies and URLs to restrict access to the distribution

D.
Enable automatic compression of objects in the Cache Behavior Settings

E.
Increase the CloudFront time to live (TTL) settings in the Cache Behavior Settings

Answer: A,E
Explanation:

QUESTION NO: 688

On a weekly basis, the Administrator for a photo sharing website receives an archive of all files users have uploaded the previous week. these file archives can be as large as 10TB in size. For legal reasons, these archives must be saved with no possibility of someone deleting or modifying these archives. Occasionally, there may be a need to view the contents, but it is expected that retrieving them can take three or more hours.

What should the Administrator do with the weekly archive?

A.
Upload the file to Amazon S3 through the AWS Management Console and apply a lifecycle policy to change the storage class to Amazon Glacier.

B.
Upload the archive to the Amazon Glacier with the AWS CLI and enable Vault Lock.

C.
Create a Linux EC2 instance with an encrypted Amazon EBS volume and copy each weekly archive file for this instance.

D.
Create a file gateway attached to a file share on an S3 bucket with the storage class S3 Infrequent Access. Upload the archives via the gateway.

Answer: A
Explanation:

QUESTION NO: 689

A SysOps Administrator is managing a Memcached cluster in Amazon ElastiCache. The cluster

has been heavily used recently, and the Administrator wants to use a larger instance type with more memory. What should the Administrator use to make this change?

A.
use the ModifyCacheCluster API and specify a new CacheNodeType

B.
use the CreateCacheCluster API and specify a new CacheNodeType

C.
use the ModifyCacheParameterGroup API and specify a new CacheNodeType

D.
use the RebootCacheCluster API and specify a new CacheNodeType

Answer: B

Explanation:

QUESTION NO: 690

A company with dozens of AWS accounts wants to ensure that governance rules are being applied across all accounts. The CIO has recommended that AWS Config rules be deployed using an AWS CloudFormation template. How should these requirements be met?

A.
Create a CloudFormation stack set, then select the CloudFormation template and use it to configure the AWS accounts

B.
Write a script that iterates over the company's AWS accounts and executes the CloudFormation template in each account

C.
Use AWS Organizations to execute the CloudFormation template in all accounts

D.
Create a CloudFormation stack in the master account of AWS Organizations and execute the CloudFormation template to create AWS Config rules in all accounts

Answer: A

Explanation:

QUESTION NO: 691

A company's Information Security team has requested information on AWS environment compliance for Payment Card Industry (PCI) workloads. They have requested assistance in understanding what specific areas of the PCI standards are the responsibility of the company.

Which AWS tool will provide the necessary information?

A.
AWS Macie

B.
AWS Artifact

C.
AWS OpsWorks

D.
AWS Organizations

Answer: B
Reference: https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

QUESTION NO: 692

A company has deployed a fleet of Amazon EC2 web servers for the upcoming release of a new product. The SysOps Administrator needs to test the Amazon CloudWatch notification settings for this deployment to ensure that a notification is sent using Amazon SNS if the CPU utilization of an EC2 instance exceeds 70%.

How should the Administrator accomplish this?

A.
Use the set-alarm-state command in AWS CloudTrail to invoke the Amazon SNS notification

B.
Use CloudWatch custom metrics to set the alarm state in AWS CloudTrail and enable Amazon SNS notifications

C.
Use EC2 instance metadata to manually set the CPU utilization to 75% and invoke the alarm state

D.
Use the set-alarm-state command in the AWS CLI for CloudWatch

Answer: D
Explanation:

QUESTION NO: 693

A SysOps Administrator has written an AWS Lambda function to launch new Amazon EC2 instances and deployed it in the us-east-1 region. The Administrator tested it by launching a new t2.nano instance in the us-east-1 region and it performed as expected. However, when the region name was updated in the Lambda function to launch an EC2 instance in the us-west-1 region, it failed.

What is causing this error?

A.
The AMI ID must be updated for the us-west-1 region in the Lambda function as well

B.
The Lambda function can only launch EC2 instances in the same region where it is deployed

C.
The Lambda function does not have the necessary IAM permission to launch more than one EC2 instance

D.
The instance type defined in the Lambda function is not available in the us-west-1 region

Answer: A
Explanation:

QUESTION NO: 694

A SysOps Administrator is required to monitor free space on Amazon EBS volumes attached to Microsoft Windows-based Amazon EC2 instances within a company's account. The Administrator must be alerted to potential issues.

What should the Administrator do to receive email alerts before low storage space affects EC2

instance performance?

A.
Use built-in Amazon CloudWatch metrics, and configure CloudWatch alarms and an Amazon SNS topic for email notifications

B.
Use AWS CloudTrail logs and configure the trail to send notifications to an Amazon SNS topic

C.
Use the Amazon CloudWatch agent to send disk space metrics, then set up CloudWatch alarms using an Amazon SNS topic

D.
Use AWS Trusted Advisor and enable email notification alerts for EC2 disk space

Answer: A
Explanation:

QUESTION NO: 695

A SysOps Administrator wants to prevent Developers from accidentally terminating Amazon EC2 instances.

How can this be accomplished?

A.
Use AWS Systems Manager to restrict EC2 termination

B.
Use AWS Config to restrict EC2 termination

C.
Apply Amazon CloudWatch Events to prevent EC2 termination

D.
Enable termination protection on EC2 instances

Answer: D
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/accidental-termination/

QUESTION NO: 696

A company has attached the following policy to an IAM user.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "rds:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "ec2:*",
                "s3:GetObject"
            ],
            "Resource": "*"
        }
    ]
}
```

BrainDumps

Which of the following actions are allowed for the IAM user?

A.

Amazon RDS DescribeDBInstances action in the us-east-1 Region

B.
Amazon S3 PutObject operation in a bucket named testbucket

C.
Amazon EC2 DescribeInstances action in the us-east-1 Region

D.
Amazon EC2 AttachNetworkInterface action in the eu-west-1 Region

Answer: A
Explanation:

QUESTION NO: 697

A SysOps Administrator launched an Amazon EC2 instance and received a message that the service limit was exceeded for that instance type. What action should the Administrator take to ensure that EC2 instances can be launched?

A.
Use Amazon Inspector to trigger an alert when the limits are exceeded

B.
Use the AWS CLI to bypass the limits placed on the account

C.
Sign in to the AWS Management Console and adjust the limit values to launch new resources

D.
Open a case with AWS Support requesting an increase of the EC2 instance limit

Answer: D
Explanation:

QUESTION NO: 698

A web application runs on Amazon EC2 instances behind an Elastic Load Balancing Application Load Balancer (ALB). The instances run in an Auto Scaling group across multiple Availability Zones. A SysOps Administrator has notice that some EC2 instances show up healthy in the Auto

Scaling console but show up as unhealthy in the ALB target console.

What could be the issue?

A.
The health check grace period for the Auto Scaling group is set too low; increase it

B.
The target group health check is incorrectly configured and needs to be adjusted

C.
The user data or AMI used for the Auto Scaling group launch configuration is incorrect

D.
The Auto Scaling group health check type is based on EC2 instance health instead of Elastic Load Balancing health checks

Answer: D
Explanation:

QUESTION NO: 699

A company is running critical applications on Amazon EC2 instances. The company needs to ensure its resources are automatically recovered if they become impaired due to an underlying hardware failure.

Which service can be used to monitor and recover the EC2 instances?

A.
Amazon EC2 Systems Manager

B.
Amazon Inspector

C.
AWS CloudFormation

D.
Amazon CloudWatch

Answer: D
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html

QUESTION NO: 700

A gaming application is deployed on four Amazon EC2 instances in a default VPC. The SysOps Administrator has noticed consistently high latency in responses as data is transferred among the four instances. There is no way for the Administrator to alter the application code.

The MOST effective way to reduce latency is to relaunch the EC2 instances in:

A.
a dedicated VPC.

B.
a single subnet inside the VPC.

C.
a placement group.

D.
a single Availability Zone.

Answer: C
Explanation:

QUESTION NO: 701

A company has created an online retail application that is hosted on a fleet of Amazon EC2 instances behind an ELB Application Load Balancer. User authentication is handled at the individual EC2 instance level. Once a user is authenticated; all requests from that user must go to the same EC2 instance.

What should the SysOps Administrator enable to meet these requirements?

A.
ELB TCP listeners

B.
ELB sticky sessions

C.
ELB connection draining

D.
ELB cross-zone load balancing

Answer: B

Explanation:

ELB can be configured to use sticky session feature (also called session affinity) which enables it to bind a user's session to an instance and ensures all requests are sent to the same instance.

Stickiness remains for a period of time which can be controlled by the application's session cookie, if one exists, or through cookie, named AWSELB, created through Elastic Load balancer.

Sticky sessions for ELB are disabled, by default.

QUESTION NO: 702

A SysOpsAdministrator is managing a large organization with multiple accounts on the Business Support plan all linked to a single payer account. The Administrator wants to be notified automatically of AWS Personal Health Dashboard events.

In the main payer account, the Administrator configures Amazon CloudWatch Events triggered by AWS Health events triggered by AWS Health triggered by AWS Health events to issue notifications using Amazon SNS, but alerts in the linked accounts failed to trigger.

Why did the alerts fail?

A.
Amazon SNS cannot be triggered from the AWS Personal Health Dashboard

B.
The AWS Personal Health Dashboard only reports events from one account, not linked accounts.

C.
The AWS Personal Health Dashboard must be configured from the payer account only; all events will then roll up into the payer account.

D.
AWS Organizations must be used to monitor linked accounts.

Answer: D
Reference: http://ask.whizlabs.com/t/personal-health-dashboard/3082

QUESTION NO: 703

A company is planning to expand into an additional AWS Region for disaster recovery purposes. The company uses AWS CloudFormation, and its infrastructure is well-defined as code. The company would like to reuse as much of its existing code as possible when deploying resources to additional Regions.

A SysOps Administrator is reviewing how Amazon Machine Images (AMIs) are selected in AWS CloudFormation, but is having trouble making the same stack work in the new Region.

Which action would make it easier to manage multiple Regions?

A.
Name each AMI in the new Region exactly the same as the equivalent AMI in the first Region.

B.
Duplicate the stack so unique AMI names can be coded into the appropriate stack.

C.
Create an alias for each AMI so that an AMI can be referenced by a common name across Regions.

D.
Create a Mappings section in the stack, and define the Region to AMI associations.

Answer: B
Explanation:

QUESTION NO: 704

An organization with a large IT department has decided to migrate to AWS. With different job functions in the IT department, it is not desirable to give all users access to all AWS resources. Currently the organization handles access via LDAP group membership.

What is the BEST method to allow access using current LDAP credentials?

A.
Create an AWS Directly Service Simple AD. Replicate the on-premises LDAP directory to Simple AD.

B.
Create a Lambda function to read LDAP groups and automate the creation of IAM users.

C.
Use AWS CloudFormation to create IAM roles. Deploy Direct Connect to allow access to the on-premises LDAP server.

D.
Federate the LDAP directory with IAM using SAML. Create different IAM roles to correspond to different LDAP groups to limit permissions.

Answer: D
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html

QUESTION NO: 705

An organization stores sensitive customer in S3 buckets protected by bucket policies. recently, there have been reports that unauthorized entities within the company have been trying to access the data on those S3 buckets. The Chief Information Security Officer (CISO) would like to know which buckets are being targeted and determine who is responsible for trying to access that information.

Which steps should a SysOps Administrator take to meet the CISO’s requirement? (Choose two.)

A.
Enable Amazon S3 Analytics on all affected S3 buckets to obtain a report of which buckets are being accessed without authorization.

B.
Enable Amazon S3 Server Access Logging on all affected S3 buckets and have the logs stored in a bucket dedicated for logs.

C.
Use Amazon Athena to query S3 Analytics report for HTTP 403 errors, and determine the IAM user or role making the requests.

D.
Use Amazon Athena to query the S3 Server Access Logs for HTTP 403 errors, and determine the IAM user or role making the requests.

E.
Use Amazon Athena to query the S3 Server Access Logs for HTTP 503 errors, and determine the

IAM user or role making the requests.

Answer: A,B
Explanation:

QUESTION NO: 706

A SysOps Administrator responsible for an e-commerce web application observes the application does not launch new Amazon EC2 instances at peak times, even though the maximum capacity of the Auto Scaling group has not been reached.

What should the Administrator do to identify the underlying problem? (Choose two.)

A.
Monitor service limits in AWS Trusted Advisor.

B.
Analyze VPC Flow Logs.

C.
Monitor limits in AWS Systems Manager.

D.
Use Amazon Inspector to gather performance information.

E.
Check the response for RunInstances requests in AWS CloudTrail logs.

Answer: C,D
Explanation:

QUESTION NO: 707

A SysOps Administrator must generate a report that provides a breakdown of all API activity by a specific user the course of a year.

Given that AWS Cloud Trail was enabled, how can this report be generated?

A.
Using the AWS management Console, search for the user name in the CloudTrail history. Then filter by API and download the report in CSV format.

B.
Use the CloudTrail digest files stored in the company's Amazon S3 bucket. then send the logs to Amazon QuickSight to create the report.

C.
Locate the monthly reports that CloudTrail sends that are emailed to the account's root user. Then forward the reports to the auditor using a secure channel.

D.
Access the CloudTrail logs stored in the Amazon S3 bucket tied to Cloud Trail. Use Amazon Athena to extract the information needed to generate the report.

Answer: D
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-for-activity/

QUESTION NO: 708

A company received its latest bill with a large increase in the number of requests against Amazon SQS as compared to the month prior. The company is not aware of any changes in its SQS usage. The company is concerned about the cost increase and who or what was making these calls.

What should the SysOps Administrator use to validate the calls made to SQS?

A.
AWS CloudTrail

B.
Amazon CloudWatch

C.
AWS Cost Explorer

D.
Amazon S3 server access logs

Answer: A

Explanation:

QUESTION NO: 709

An Amazon S3 bucket in a SysOps Administrator's account can be accesses by users in other SWS accounts.

How can the Administrator ensure that the bucket is only accessible to members of the Administrator's AWS account?

A.
Move the S3 bucket from a public subnet to a private subnet in the Amazon VPC.

B.
Change the bucket access control list (ACL) to restrict access to the bucket owner.

C.
Enable server-side encryption for all objects in the bucket.

D.
Use only Amazon S3 presigned URLs for accessing objects in the bucket.

Answer: B
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

QUESTION NO: 710

A company hosts its website on Amazon ECF2 instances behind an ELB Application Load Balancer. The company manages its DNS with Amazon Route 53, and wants to point its domain's zone apex to the website.

Which type of record should be used to meet these requirements?

A.
An AAA record for the domain's zone apex

B.
An A record for the domain's zone apex

C.
A CNAME record for the domain's zone apex

D.
An alias record for the domain's zone apex

Answer: B
Reference: https://aws.amazon.com/route53/faqs/

QUESTION NO: 711

A company has centralized all its logs into one Amazon CloudWatch Logs log group. The SysOps Administrator is to alert different teams of any issues relevant to them.

What is the MOST efficient approach to accomplish this?

A.
Write an AWS Lambda function that will query the logs every minute and contain the logic of which team to notify on which patterns and issues.

B.
Set up different metric filters for each team based on patterns and alerts. Each alarm will notify the appropriate notification list.

C.
Redesign the aggregation of logs so that each team's relevant parts are sent to a separate log group, then subscribe each team to its respective log group.

D.
Create an AWS Auto Scaling group of Amazon EC2 instances that will scale based on the amount of ingested log entries. This group will pull log streams, look for patterns, and send notifications to relevant teams.

Answer: C
Explanation:

QUESTION NO: 712

A company website hosts patches for software that is sold globally. The website runs in AWS and

performs well until a large software patch is released. The flood of downloads puts a strain on the web servers and leads to a poor customer experience.

What can the Sysops Administrator propose to enhance customer experience, create a more available web platform, and keep costs low?

A.
Use an Amazon CloudFront distribution to cache static content, including software patches.

B.
Increase the size of the NAT instance to improve throughput.

C.
Scale out the web servers in advance of patch releases to reduce Auto Scaling delays.

D.
Move the content to IO1 and provision additional IOPS to the volume that contains the software patches.

Answer: A
Explanation:

QUESTION NO: 713

A SysOps Administrator created an Application Load balancer (ALB) and placed two Amazon EC2 instances in the same subnet behind the ALB. During monitoring, the Administrator observes HealthyHostCount drop to 1 in Amazon CloudWatch.

What is MOST likely causing this issue?

A.
The EC2 instances are in the same Availability Zone, causing contention between the two.

B.
The route tables are not updated to allow traffic to flow between the ALB and the EC2 instances.

C.
The ALB health check has failed, and the ALB has taken EC2 instances out of service.

D.
The Amazon Route 53 health check has failed, and the ALB has taken EC2 instances out of service.

Answer: A

Explanation:

QUESTION NO: 714

A SysOps Administrator is managing an AWS account where Developers are authorized to launch Amazon EC2 instances to test new code. To limit costs, the Administrator must ensure that the EC2 instances in the account are terminated 24 hours after launch.

How should the Administrator meet these requirements?

A.
Create an Amazon CloudWatch alarm based on the CPUUtilization metric. When the metric is 0% for 24 hours, trigger an action to terminate the EC2 instance when the alarm is triggered.

B.
Create an AWS Lambda function to check all EC2 instances and terminate instances running more than 24 hours. Trigger the function with an Amazon CloudWatch Events event every 15 minutes.

C.
Add an action to AWS Trusted Advisor to turn off EC2 instances based on the Low Utilization Amazon EC2 Instances check, terminating instances identified by Trusted Advisor as running for more than 24 hours.

D.
Install the unified Amazon CloudWatch agent on every EC2 instance. Configure the agent to terminate instances after they have been running for 24 hours.

Answer: C

Explanation:

QUESTION NO: 715

An AWS CodePipeline in us-east-1 returns “InternalError” with the code “JobFailed” when launching a deployment using an artifact from an Amazon S3 bucket in us-west-1.

What is causing this error?

A.
S3 Transfer Acceleration is not enabled.

B.
The S3 bucket is not in the appropriate region.

C.
The S3 bucket is being throttled.

D.
There are insufficient permissions on the artifact in Amazon S3.

Answer: B
Reference:
https://docs.aws.amazon.com/codepipeline/latest/userguide/troubleshooting.html#troubleshooting-reg-1

QUESTION NO: 716

An application running on Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones was deployed using an AWS CloudFormation template. The SysOps team has patched the Amazon Machine Image (AMI) version and must update all the EC2 instances to use the new AMI.

How can the SysOps Administrator use CloudFormation to apply the new AMI while maintaining a minimum level of active instances to ensure service continuity?

A.
Run the aws cloudfomation update-stack command with the – rollback-configuration option

B.
Update the CloudFormation template with the new AMI ID, then reboot the EC2 instances

C.
Deploy a second CloudFormation stack and use Amazon Route 53 to redirect traffic to the new stack

D.
Set an AutoScalingUpdate policy in the CloudFormation template to update the stack.

Answer: D
Explanation:

QUESTION NO: 717

A SysOps Administrator is responsible for a legacy, CPU-heavy application. The application can only be scaled vertically. Currently, the application is deployed on a single t2.large Amazon EC2 instance. The system is showing 90% CPU usage and significant performance latency after a few minutes.

What change should be made to alleviate the performance problem?

A.
Change the Amazon EBS volume to Provisioned IOPs.

B.
Upgrade to a compute-optimized instance.

C.
Add additional t2.large instances to the application.

D.
Purchase Reserved Instances.

Answer: D
Explanation:

QUESTION NO: 718

A company recently implemented an Amazon S3 lifecycle rule that accidentally deleted objects from one of its S3 buckets. The bucket has S3 versioning enabled.

Which actions will restore the objects? (Choose two.)

A.
Use the AWS Management Console to delete the object delete markers.

B.
Create a new lifecycle rule to delete the object delete markers that were created.

C.
Use the AWS CLI to delete the object delete markers while specifying the version IDs of the delete markers.

D.
Modify the existing lifecycle rule to delete the object delete markers that were created.

E.
Use the AWS CLI to delete the object delete markers while specifying the name of the objects only.

Answer: A,D
Reference: https://docs.aws.amazon.com/AmazonS3/latest/user-guide/undelete-objects.html

QUESTION NO: 719

A company uses AWS CloudFormation to deploy its application infrastructure. Recently, a user accidentally changed a property of a database in a CloudFormation template and performed a stack update that caused an interruption to the application. A SysOps Administrator must determine how to modify the deployment process to allow the DevOps team to continue to deploy the infrastructure, but prevent against accidental modifications to specific resources.

Which solution will meet these requirements?

A.
Set up an AWS Config rule to alert based on changes to any CloudFormation stack. An AWS Lambda function can then describe the stack to determine if any protected resources were modified and cancel the operation.

B.
Set up an Amazon CloudWatch Events event with a rule to trigger based on any CloudFormation API call. An AWS Lambda function can then describe the stack to determine if any protected resources were modified and cancel the operation.

C.
Launch the CloudFormation templates using a stack policy with an explicit allow for all resources and an explicit deny of the protected resources with an action of Update:*.

D.
Attach an IAM policy to the DevOps team role that prevents a CloudFormation stack from updating, with a condition based on the specific Amazon Resource names (ARNs) of the protected resources.

Answer: C
Explanation:

QUESTION NO: 720

A SysOps Administrator is analyzing how Reserved Instance discounts are allocated to Amazon EC2 instances across accounts in the company's consolidated bill.

Which AWS tool will provide the details necessary to understand the billing charges?

A.
AWS Budgets

B.
AWS Cost and Usage report

C.
AWS Trusted Advisor

D.
AWS Organizations

Answer: D
Explanation:

Consolidated billing has the following benefits:

Reference: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html

QUESTION NO: 721

What should a SysOps Administrator do to ensure a company has visibility into maintenance events performed by AWS?

A.
Run a script that queries AWS Systems Manager for upcoming maintenance events, and then push these events to an Amazon SNS topic to which the Operations team is subscribed.

B.
Query the AWS Health API for upcoming maintenance events and integrate the results with the company’s existing operations dashboard.

C.

Integrate the AWS Service Health Dashboard's RSS feed into the company's existing operations dashboard.

D.
Use Amazon Inspector to send notifications of upcoming maintenance events to the Operations team distribution list.

Answer: C
Reference: https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/

QUESTION NO: 722

A SysOps Administrator manages a website running on Amazon EC2 instances behind an ELB Application Load Balancer. Users visiting the load balancer's DNS address in a browser are reporting errors. The administrator has confirmed:

The security groups and network ACLs are correctly configured.

The load balancer target group shows no healthy instances.

What should the Administrator do to resolve this issue?

A.
Review the application's logs for requests originating from the VPC DNS address.

B.
Review the load balancer access logs, looking for any issues or errors.

C.
Review the load balancer target group health check configuration.

D.
Review the load balancer listener configuration.

Answer: B
Explanation:

QUESTION NO: 723

A company is running multiple AWS Lambda functions in a non-VPC environment. Most of the functions are application-specific; an operational function is involved synchronously every hour.

Recently, the Applications team deployed new functions that are triggered based on an Amazon S3 event to process multiple files that are uploaded to an S3 bucket simultaneously. The SysOps Administrator notices that the operational function occasionally fails to execute due to throttling.

What step should the Administrator take to make sure that the operational function executes?

A.
Redeploy the operational function to a VPC.

B.
Increase the operational function timeout.

C.
Set the operational function concurrency to 1.

D.
Increase the operational function memory.

Answer: B
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/best-practices-custom-cf-lambda/

QUESTION NO: 724

A SysOps Administrator must ensure all Amazon EBS volumes currently in use, and those created in the future, are encrypted with a specific AWS KMS customer master key (CMK).

What is the MOST efficient way for the Administrator to meet this requirement?

A.
Create an AWS Lambda function to run on a daily schedule, and have the function run the aws ec2 describe-volumes --filters encrypted command.

B.
Within AWS Config, configure the encrypted-volumes managed rule and specify the key ID of the CMK.

C.
Log in to the AWS Management Console on a daily schedule, then filter the list of volumes by

encryption status, then export this list.

D.
Create an AWS Lambda function to run on a daily schedule, and have the function run the aws kms describe-key command.

Answer: D
Explanation:

QUESTION NO: 725

A company has an application running on a fleet of Microsoft Windows instances. Patches to the operating system need to be applied each month. AWS Systems Manager Patch Manager is used to apply the patches on a schedule.

When the fleet is being patched, customers complain about delayed service responses.

What can be done to ensure patches are deployed with MINIMAL customer impact?

A.
Change the number of instances patched at any one time to 100%.

B.
Create a snapshot of each server in the fleet using a Systems Manager Automation document before starting the patch process.

C.
Configure the maintenance window to patch 10% of the instances in the patch group at a time.

D.
Create a patched Amazon Machine Image (AMI). Configure the maintenance window option to deploy the patched AMI on only 10% of the fleet at a time.

Answer: C
Reference: https://aws.amazon.com/blogs/mt/patching-your-windows-ec2-instances-using-aws-systems-manager-patch-manager/

QUESTION NO: 726

A local agency plans to deploy 500 Raspberry Pi devices throughout a city. All the devices need to be managed centrally, and their configurations need to be consistent.

What is the BEST service for managing these devices?

A.
AWS Config

B.
AWS Systems Manager

C.
Amazon Inspector

D.
AWS Service Catalog

Answer: B
Reference: https://aws.amazon.com/blogs/mt/manage-raspberry-pi-devices-using-aws-systems-manager/

QUESTION NO: 727

A SysOps Administrator needs an Amazon EBS volume type for a big data application. The application data is accessed infrequently and stored sequentially.

What EBS volume type will be the MOST cost-effective solution?

A.
Provisioned IOPS SSD (io1)

B.
Cold HDD (sc1)

C.
Throughput Optimized HDD (st1)

D.
General Purpose SSD (gp2)

Answer: B

Explanation:

SC1 is backed by hard disk drives (HDDs) and provides the lowest cost per GB of all EBS volume types. It is ideal for less frequently accessed workloads with large, cold datasets. Similar to st1, sc1 provides a burst model: these volumes can burst up to 80 MB/s per TB, with a baseline throughput of 12 MB/s per TB and a maximum throughput of 250 MB/s per volume. For infrequently accessed data, sc1 provides extremely inexpensive storage. SC1 is designed to deliver the expected throughput performance 99% of the time and has enough I/O credits to support a full-volume scan at the burst rate.

Reference: https://aws.amazon.com/ebs/features/

QUESTION NO: 728

A SysOps Administrator created an AWS Service Catalog portfolio and shared the portfolio with a second AWS account in the company. The second account is controlled by a different Administrator.

Which action will the Administrator of the second account be able to perform?

A.
Add a product from the imported portfolio to a local portfolio.

B.
Add new products to the imported portfolio.

C.
Change the launch role for the products contained in the imported portfolio.

D.
Remove products from the imported portfolio.

Answer: A
Reference:
https://docs.aws.amazon.com/servicecatalog/latest/adminguide/catalogs_portfolios_sharing.html

QUESTION NO: 729

A SysOps Administrator must secure AWS CloudTrail logs. The Security team is concerned that an employee may modify or attempt to delete CloudTrail log files from its Amazon S3 bucket.

Which practices will ensure that the log files are available and unaltered? (Choose two.)

A.
Enable the CloudTrail log file integrity check in AWS Config Rules.

B.
Use CloudWatch Events to scan log files hourly.

C.
Enable CloudTrail log file integrity validation.

D.
Turn on Amazon S3 MFA Delete for the CloudTrail bucket.

E.
Implement a DENY ALL bucket policy on the CloudTrail bucket.

Answer: C,D

Explanation:

The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time. CloudTrail log file integrity validation uses industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally unfeasible to modify, delete or forge CloudTrail log files without detection. T

Configuring multi-factor authentication (MFA) ensures that any attempt to change the versioning state of your bucket or permanently delete an object version requires additional authentication. This helps prevent any operation that could compromise the integrity of your log files, even if a user acquires the password of an IAM user that has permissions to permanently delete Amazon S3 objects.

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html

QUESTION NO: 730

A company runs a web application that users access using the domain name www.example.com. The company manages the domain name using Amazon Route 53. The company created an Amazon CloudFront distribution in front of the application and would like www.example.com to

access the application through CloudFront.

What is the MOST cost-effective way to achieve this?

A.
Create a CNAME record in Amazon Route 53 that points to the CloudFront distribution URL.

B.
Create an ALIAS record in Amazon Route 53 that points to the CloudFront distribution URL.

C.
Create an A record in Amazon Route 53 that points to the public IP address of the web application.

D.
Create a PTR record in Amazon Route 53 that points to the public IP address of the web application.

Answer: B
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html

QUESTION NO: 731

A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted.

What is the SIMPLEST approach the SysOps Administrator can take to ensure S3 buckets in those accounts can never be deleted?

A.
Set up MFA Delete on all the S3 buckets to prevent the buckets from being deleted.

B.
Use service control policies to deny the s3:DeleteBucket action on all buckets in production accounts.

C.
Create an IAM group that has an IAM policy to deny the s3:DeleteBucket action on all buckets in production accounts.

D.

Use AWS Shield to deny the s3:DeleteBucket action on the AWS account instead of all S3 buckets.

Answer: B
Reference:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

QUESTION NO: 732

A company uses multiple accounts for its applications. Account A manages the company's Amazon Route 53 domains and hosted zones. Account B uses a load balancer fronting the company's web servers.

How can the company use Route 53 to point to the load balancer in the MOST cost-effective and efficient manner?

A.
Create an Amazon EC2 proxy in Account A that forwards requests to Account B.

B.
Create a load balancer in Account A that points to the load balancer in Account B.

C.
Create a CNAME record in Account A pointing to an alias record to the load balancer in Account B.

D.
Create an alias record in Account A pointing to the load balancer in Account B.

Answer: D
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

QUESTION NO: 733

A SysOps Administrator implemented the following bucket policy to allow only the corporate IP address range of 54.240.143.0/24 to access objects in an Amazon S3 bucket.

```
{
    "Version": "2012-10-17",
    "Id": "s3PolicyId1",
    "Statement": [
        {
            "Sid": "s3Allow",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource":[
                "arn:aws:s3:::examplebucket",
                "arn:aws:s3:::examplebucket/*"
            ]
        },
        {
            "Sid": "IPAllow",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::examplebucket",
                "arn:aws:s3:::examplebucket/*"
            ],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": "54.240.143.0/24"
                }
            }
        }
    ]
}
```

BrainDumps

Some employees are reporting that they are able to access the S3 bucket from IP addresses outside the corporate IP address range.

How can the Administrator address this issue?

A.
Modify the Condition operator to include both NotIpAddress and IpAddress to prevent unauthorized access to the S3 bucket.

B.
Modify the Condition element from the IAM policy to aws:StringEquals instead of aws:SourceIp.

C.
Modify the IAM policy instead of the bucket policy to restrict users from accessing the bucket based on their source IP addresses.

D.
Change Effect from Allow to Deny in the second statement of the policy to deny requests not from the source IP range.

Answer: D
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/block-s3-traffic-vpc-ip/

QUESTION NO: 734

A SysOps Administrator is notified that a security vulnerability affects a version of MySQL that is being used with Amazon RDS MySQL.

Who is responsible for ensuring that the patch is applied to the MySQL cluster?

A.
The database vendor

B.
The Security department of the SysOps Administrator's company

C.
AWS

D.
The SysOps Administrator

Answer: A
Explanation:

QUESTION NO: 735

A company's web application runs on Amazon EC2 instances behind an ELB Application Load Balancer. The EC2 instances run in an EC2 Auto Scaling group across multiple Availability Zones. Data is stored in an Amazon ElastiCache for Redis cluster and an Amazon RDS DB instance. Company policy requires all system patching to take place at midnight on Tuesday.

Which resources will need to have a maintenance window configured for midnight on Tuesday? (Choose two.)

A.
Elastic Load Balancer

B.
EC2 instances

C.
RDS instance

D.
ElastiCache cluster

E.
Auto Scaling group

Answer: C,D
Explanation:

QUESTION NO: 736

A SysOps Administrator is deploying a website with dynamic content. Company policy requires that users from certain countries or regions cannot access the web content and should receive an error page.

Which of the following can be used to implement this policy? (Choose two.)

A.
Amazon CloudFront geo-restriction

B.
Amazon GuardDuty geo-blocking

C.
Amazon Route 53 geolocation routing

D.
AWS Shield geo-restriction

E.
Network access control list (NACL) restriction

Answer: A,C
Reference: https://aws.amazon.com/cloudfront/faqs/

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

QUESTION NO: 737

A company stores thousands of non-critical log files in an Amazon S3 bucket. A set of reporting scripts retrieve these log files daily.

Which of the following storage options will be the MOST cost-efficient for the company's use case?

A.
Amazon Glacier

B.
Amazon S3 Standard IA (infrequent access) storage

C.
Amazon S3 Standard Storage

D.
AWS Snowball

Answer: C
Reference: https://aws.amazon.com/s3/faqs/

QUESTION NO: 738

A SysOps Administrator receives a connection timeout error when attempting to connect to an Amazon EC2 instance from a home network using SSH. The Administrator was able to connect to this EC2 instance using SSH from their office network in the past.

What caused the connection to time out?

A.
The IAM role associated with the EC2 instance does not allow SSH connections from the home network.

B.
The public key used by SSH located on the Administrator's server does not have the required permissions.

C.
The route table contains a route that sends 0.0.0.0/0 to the internet gateway for the VPC.

D.
The security group is not allowing inbound traffic from the home network on the SSH port.

Answer: D
Explanation:

QUESTION NO: 739

A company is deploying a web service to Amazon EC2 instances behind an Elastic Load Balancer. All resources will be defined and created in a single AWS CloudFormation stack using a template. The creation of each EC2 instance will not be considered complete until an initialization script has been run successfully on the EC2 instance. The Elastic Load Balancer cannot be created until all EC2 instances have been created.

Which CloudFormation resource will coordinate the Elastic Load Balancer creation in the CloudFormation stack template?

A.
CustomResource

B.
DependsOn

C.
Init

D.
WaitCondition

Answer: C
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html

QUESTION NO: 740

A company is concerned about a security vulnerability impacting its Linux operating system.

What should the SysOps Administrator do to alleviate this concern?

A.
Patch the vulnerability with Amazon Inspector.

B.
Provide an AWS Trusted Advisor report showing which Amazon EC2 instances have been patched.

C.
Redeploy the Amazon EC2 instances using AWS CloudFormation.

D.
Patch the Linux operating system using AWS Systems Manager.

Answer: D
Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html

QUESTION NO: 741

A SysOps Administrator is configuring AWS SSO for the first time. The Administrator has already created a directory in the master account using AWS Directory Service and enabled full access in AWS Organizations.

What should the Administrator do next to configure the service?

A.
Create IAM roles in each account to be used by AWS SSO, and associate users with these roles using AWS SSO.

B.
Create IAM users in the master account, and use AWS SSO to associate the users with the accounts they will access.

C.
Create permission sets in AWS SSO, and associate the permission sets with Directory Service users or groups.

D.
Create service control policies (SCPs) in Organizations, and associate the SCPs with Directory Service users or groups.

Answer: C
Reference: https://aws.amazon.com/blogs/security/how-to-create-and-manage-users-within-aws-sso/

QUESTION NO: 742

A web application runs on Amazon EC2 instances and accesses external services. The external services require authentication credentials. The application is deployed using AWS CloudFormation to three separate environments: development, test, and production. Each environment requires unique credentials for external services.

What option securely provides the application with the needed credentials while requiring MINIMAL administrative overhead?

A.
Pass the credentials for the target environment to the CloudFormation template as parameters. Use the user data script to insert the parameterized credentials into the EC2 instances.

B.
Store the credentials as secure strings in AWS Systems Manager Parameter Store. Pass an environment tag as a parameter to the CloudFormation template. Use the user data script to insert the environment tag in the EC2 instances. Access the credentials from the application.

C.
Create a separate CloudFormation template for each environment. In the Resources section, include a user data script for each EC2 instance. Use the user data script to insert the proper credentials for the environment into the EC2 instances.

D.
Create separate Amazon Machine Images (AMIs) with the required credentials for each environment. Pass the environment tag as a parameter to the CloudFormation template. In the Mappings section of the CloudFormation template, map the environment tag to the proper AMI, then use that AMI when launching the EC2 instances.

Answer: A
Explanation:

QUESTION NO: 743

A SysOps Administrator created an AWS CloudFormation template for the first time. The stack failed with a status of ROLLBACK_COMPLETE. The Administrator identified and resolved the template issue causing the failure.

How should the Administrator continue with the stack deployment?

A.
Delete the failed stack and create a new stack.

B.
Execute a change set on the failed stack.

C.
Perform an update-stack action on the failed stack.

D.
Run a validate-template command.

Answer: A
Explanation:

QUESTION NO: 744

A SysOps Administrator is building a process for sharing Amazon RDS database snapshots between different accounts associated with different business units within the same company. All data must be encrypted at rest.

How should the Administrator implement this process?

A.
Write a script to download the encrypted snapshot, decrypt it using the AWS KMS encryption key used to encrypt the snapshot, then create a new volume in each account.

B.
Update the key policy to grant permission to the AWS KMS encryption key used to encrypt the snapshot with all relevant accounts, then share the snapshot with those accounts.

C.
Create an Amazon EC2 instance based on the snapshot, then save the instance’s Amazon EBS volume as a snapshot and share it with the other accounts. Require each account owner to create a new volume from that snapshot and encrypt it.

D.

Create a new unencrypted RDS instance from the encrypted snapshot, connect to the instance using SSH/RDP, export the database contents into a file, then share this file with the other accounts.

Answer: B
Reference:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ShareSnapshot.html

QUESTION NO: 745

A SysOps Administrator has been notified that some Amazon EC2 instances in the company's environment might have a vulnerable software version installed.

What should be done to check all of the instances in the environment with the LEAST operational overhead?

A.
Create and run an Amazon Inspector assessment template.

B.
Manually SSH into each instance and check the software version.

C.
Use AWS CloudTrail to verify Amazon EC2 activity in the account.

D.
Write a custom script and use AWS CodeDeploy to deploy to Amazon EC2 instances.

Answer: A
Reference: https://aws.amazon.com/inspector/faqs/

QUESTION NO: 746

Development teams are maintaining several workloads on AWS. Company management is concerned about rising costs and wants the SysOps Administrator to configure alerts so teams are notified when spending approaches preset limits.

Which AWS service will satisfy these requirements?

A.
AWS Budgets

B.
AWS Cost Explorer

C.
AWS Trusted Advisor

D.
AWS Cost and Usage report

Answer: C
Reference: https://aws.amazon.com/solutions/limit-monitor/

QUESTION NO: 747

A SysOps Administrator is tasked with deploying and managing a single CloudFormation template across multiple AWS accounts.

What feature of AWS CloudFormation will accomplish this?

A.
Change sets

B.
Nested stacks

C.
Stack policies

D.
StackSets

Answer: D
Reference: https://aws.amazon.com/blogs/aws/use-cloudformation-stacksets-to-provision-resources-across-multiple-aws-accounts-and-regions/

QUESTION NO: 748

A company runs an application that uses Amazon RDS for MySQL. During load testing of equivalent production volumes, the Development team noticed a significant increase in query latency. A SysOps Administrator concludes from investigating Amazon CloudWatch Logs that the CPU utilization on the RDS MySQL instance was at 100%.

Which action will resolve this issue?

A.
Configure AWS Database Migration Service (AWS DMS) to allow Amazon RDS for MySQL to scale and accept more requests.

B.
Configure RDS for MySQL to scale horizontally by adding additional nodes to offload write requests.

C.
Enable the Multi-AZ feature for the RDS instance.

D.
Modify the RDS MySQL instance so it is a larger instance type.

Answer: D
Explanation:

QUESTION NO: 749

A SysOps Administrator is using AWS KMS with AWS-generated key material to encrypt an Amazon EBS volume in a company's AWS environment. The Administrator wants to rotate the KMS keys using automatic key rotation, and needs to ensure that the EBS volume encrypted with the current key remains readable.

What should be done to accomplish this?

A.
Back up the current KMS key and enable automatic key rotation.

B.
Create a new key in AWS KMS and assign the key to Amazon EBS.

C.

Enable automatic key rotation of the EBS volume key in AWS KMS.

D.
Upload new key material to the EBS volume key in AWS KMS to enable automatic key rotation for the volume.

Answer: C
Reference: https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

QUESTION NO: 750

A SysOps Administrator deployed an AWS Elastic Beanstalk worker node environment that reads messages from an auto-generated Amazon Simple Queue Service (Amazon SQS) queue and deletes them from the queue after processing. Amazon EC2 Auto Scaling scales in and scales out the number of worker nodes based on CPU utilization. After some time, the Administrator notices that the number of messages in the SQS queue are increasing significantly.

Which action will remediate this issue?

A.
Change the scaling policy to scale based upon the number of messages in the queue.

B.
Decouple the queue from the Elastic Beanstalk worker node and create it as a separate resource.

C.
Increase the number of messages in the queue.

D.
Increase the retention period of the queue.

Answer: D
Explanation:

Amazon SQS automatically deletes messages that have been in a queue for longer than the configured RetentionPeriod.n

Reference: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-tiers.html

QUESTION NO: 751

A Security team is concerned about the potential of intellectual property leaking to the internet. A SysOps Administrator is tasked with identifying controls to address the potential problem. The servers in question reside in a VPC and cannot be allowed to send traffic to the internet.

How can these requirements be met?

A.
Edit the route for the subnet with the following entry:

Destination 0.0.0.0/0

target: igw-xxxxxxxx

B.
Ensure that the servers do not have Elastic IP addresses.

C.
Enable Enhanced Networking on the instances to control traffic flows.

D.
Put the servers in a private subnet.

Answer: A
Explanation:

QUESTION NO: 752

A company is setting up a VPC peering connection between its VPC and a customer's VPC. The company VPC is an IPv4 CIDR block of 172.16.0.0/16, and the customer's is an IPv4 CIDR block of 10.0.0.0/16. The SysOps Administrator wants to be able to ping the customer's database private IP address from one of the company's Amazon EC2 instances.

What action should be taken to meet the requirements?

A.
Ensure that both accounts are linked and are part of consolidated billing to create a file sharing network, and then enable VPC peering.

B.
Ensure that both VPC owners manually add a route to the VPC route tables that points to the IP address range of the other VPC.

C.
Instruct the customer to set up a VPC with the same IPv4 CIDR block as that of the source VPC: 172.16.0.0/16.

D.
Instruct the customer to create a virtual private gateway to link the two VPCs.

Answer: C
Explanation:

QUESTION NO: 753

A company is concerned about its ability to recover from a disaster because all of its Amazon EC2 instances are located in a single Amazon VPC in us-east-1. A second Amazon VPC has been configured in eu-west-1 to act as a backup VPC in case of an outage. Data will be replicated from the primary region to the secondary region. The Information Security team's compliance requirements specify that all data must be encrypted and must not traverse the public internet.

How should the SysOps Administrator connect the two VPCs while meeting the compliance requirements?

A.
Configure EC2 instances to act as VPN appliances, then configure route tables.

B.
Configure inter-region VPC peering between the two VPCs, then configure route tables.

C.
Configure NAT gateways in both VPCs, then configure route tables.

D.
Configure an internet gateway in each VPC, and use these as the targets for the VPC route tables.

Answer: B
Reference: https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-full-access.html

QUESTION NO: 754

Two companies will be working on several development projects together. Each company has an AWS account with a single VPC in us-east-1. Two companies would like to access one another's development servers. The IPv4 CIDR blocks in the two VPCs does not overlap.

What can the SysOps Administrators for each company do to set up network routing?

A.
Each Administrator should create a custom routing table that points to the other company's internet gateway public IP address.

B.
Both Administrators should set up a NAT gateway in a public subnet in their respective VPCs. Then. using the public IP address from the NAT gateway, the Administrators should enable routing between the two VPCs.

C.
Both Administrators should install a 1 Gbps AWS Direct Connect circuit in their respective environments. Then, using the AWS Management Console, the Administrators should create an AWS Direct Connect routing requests to enable connectivity.

D.
One Administrator should create a VPC peering request and send it to the other Administrator's account. Once the other Administrator accepts the request, update the routing tables to enable traffic.

Answer: D
Explanation:

QUESTION NO: 755

A SysOps Administrator is responsible for maintaining an Amazon EC2 instance that acts as a bastion host. The Administrator can successfully connect to the instance using SSH, but attempts to ping the instance result in a timeout.

What is one reason for the issue?

A.
The instance does not have an Elastic IP address

B.

The instance has a security group that does not allow Internet Control Message Protocol (ICMP) traffic

C.
The instance is not set up in a VPC using AWS Direct Connect

D.
The instance is running in a peered VPC

Answer: D
Explanation:

QUESTION NO: 756

An enterprise company has discovered that a number of Amazon EC2 instances in a VPC are marked as high risk according to a Common Vulnerabilities and Exposures (CVE) report. The Security team requests that all these instances be upgraded.

Who is responsible for upgrading the EC2 instances?

A.
The AWS Security team

B.
The Amazon EC2 team

C.
The AWS Premium Support team

D.
The company's Systems Administrator

Answer: D
Explanation:

QUESTION NO: 757

A SysOps Administrator is maintaining a web application using an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and Amazon EC2 in a VPC. All

services have logging enabled. The Administrator needs to investigate HTTP Layer 7 status codes from the web application.

Which log sources contain the status codes? (Choose two.)

A.
VPC Flow Logs

B.
AWS CloudTrail logs

C.
ALB access logs

D.
CloudFront access logs

E.
RDS logs

Answer: B,D
Reference:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

QUESTION NO: 758

A company needs to ensure that all IAM users rotate their passwords on a regular basis.

Which action should be taken take to implement this?

A.
Configure multi-factor authentication for all IAM users

B.
Deactivate existing users and re-create new users every time a credential rotation is required

C.
Re-create identity federation with new identity providers every time a credential rotation is required

D.
Set up a password policy to enable password expiration for IAM users

Answer: D
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

QUESTION NO: 759

An application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group that terminates unhealthy instances. The Auto Scaling group is configured to determine the health status of EC2 instances using both EC2 status checks and ALB health checks. The Development team wants to analyze the unhealthy instances before termination.

What should the SysOps Administrator do to accomplish this?

A.
Configure the ALB health check to restart instances instead of terminating them.

B.
Configure an AWS Lambda function to take a snapshot of all instances before they are terminated.

C.
Implement Amazon CloudWatch Events to capture lifecycle events and trigger an AWS Lambda function for remediation.

D.
Use an Amazon EC2 Auto Scaling lifecycle hook to pause instance termination after the instance has been removed from service.

Answer: D
Reference: https://docs.aws.amazon.com/autoscaling/ec2/userguide/healthcheck.html

QUESTION NO: 760

An application running on Amazon EC2 needs login credentials to access a database. The login credentials are stored in AWS Systems Manager Parameter Store as secure string parameters.

What is the MOST secure way to grant the application access to the credentials?

A.
Create an IAM EC2 role for the EC2 instances and grant the role permission to read the Systems Manager parameters

B.
Create an IAM group for the application and grant the group permissions to read the Systems Manager parameters

C.
Create an IAM policy for the application and grant the policy permission to read the Systems Manager parameters

D.
Create an IAM user for the application and grant the user permission to read the Systems Manager parameters

Answer: C
Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/security_iam_service-with-iam.html

QUESTION NO: 761

A SysOps Administrator is receiving alerts related to high CPU utilization of a Memcached-based Amazon ElastiCache cluster.

Which remediation steps should be taken to resolve this issue? (Choose two.)

A.
Add a larger Amazon EBS volume to the ElastiCache cluster nodes

B.
Add a load balancer to route traffic to the ElastiCache cluster

C.
Add additional worker nodes to the ElastiCache cluster

D.
Create an Auto Scaling group for the ElastiCache cluster

E.
Vertically scale the ElastiCache cluster by changing the node type

Answer: A,C

Reference: https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/CacheMetrics.WhichShouldIMonitor.html

QUESTION NO: 762

A SysOps Administrator manages an Amazon RDS MySQL DB instance in production. The database is accessed by several applications. The Administrator needs to ensure minimal downtime of the applications in the event the database suffers a failure. This change must not impact customer use during regular business hours.

Which action will make the database MORE highly available?

A.
Contact AWS Support to pre-warm the database to ensure that it can handle any unexpected spikes in traffic

B.
Create a new Multi-AZ RDS DB instance. Migrate the data to the new DB instance and delete the old one

C.
Create a read replica from the existing database outside of business hours

D.
Modify the DB instance to outside of business hours be a Multi-AZ deployment

Answer: B
Explanation:

QUESTION NO: 763

An enterprise is using federated Security Assertion Markup Language (SAML) to access the AWS Management Console.

How should the SAML assertion mapping be configured?

A.
Map the group attribute to an AWS group. The AWS group is assigned IAM policies that govern access to AWS resources.

B.
Map the policy attribute to IAM policies the federated user is assigned to. These policies govern access to AWS resources.

C.
Map the role attribute to an AWS role. The AWS role is assigned IAM policies that govern access to AWS resources.

D.
Map the user attribute to an AWS user. The AWS user is assigned specific IAM policies that govern access to AWS resources.

Answer: C
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_saml_assertions.html

QUESTION NO: 764

A SysOps Administrator is managing a web application that runs on Amazon EC2 instances behind an ELB Application Load Balancer (ALB). The instances run in an EC2 Auto Scaling group. The administrator wants to set an alarm for when all target instances associated with the ALB are unhealthy.

Which condition should be used with the alarm?

A.
AWS/ApplicationELB HealthyHostCount <= 0

B.
AWS/ApplicationELB UnhealthyHostCount >= 1

C.
AWS/EC2 StatusCheckFailed <= 0

D.
AWS/EC2 StatusCheckFailed >= 1

Answer: B
Reference: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-cloudwatch-metrics.html

QUESTION NO: 765

A company has deployed a NAT instance to allow web servers to obtain software updates from the internet. There is high latency on the NAT instance as the network grows. A SysOps Administrator needs to reduce latency on the instance in a manner that is efficient, cost-effective, and allows for scaling with future demand.

Which action should be taken to accomplish this?

A.
Add a second NAT instance and place both instances behind a load balancer

B.
Convert the NAT instance to a larger instance size

C.
Replace the NAT instance with a NAT gateway

D.
Replace the NAT instance with a virtual private gateway

Answer: A
Explanation:

QUESTION NO: 766

A security researcher has published a new Common Vulnerabilities and Exposures (CVE) report that impacts a popular operating system. A SysOps Administrator is concerned with the new CVE report and wants to patch the company's systems immediately. The administrator contacts AWS Support and requests the patch be applied to all Amazon EC2 instances.

How will AWS respond to this request?

A.
AWS will apply the patch during the next maintenance window, and will provide the Administrator with a report of all patched EC2 instances.

B.
AWS will relaunch the EC2 instances with the latest version of the Amazon Machine Image (AMI),

and will provide the Administrator with a report of all patched EC2 instances.

C.
AWS will research the vulnerability to see if the Administrator's operating system is impacted, and will patch the EC2 instances that are affected.

D.
AWS will review the shared responsibility model with the Administrator and advise them regarding how to patch the EC2 instances.

Answer: A
Explanation:

QUESTION NO: 767

A Development team recently deployed a new version of a web application to production. After the release, penetration testing revealed a cross-site scripting vulnerability that could expose user data.

Which AWS service will mitigate this issue?

A.
AWS Shield Standard

B.
AWS WAF

C.
Elastic Load Balancing

D.
Amazon Cognito

Answer: B
Reference: https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-xss-match.html

QUESTION NO: 768

A Development team is designing an application that processes sensitive information within a hybrid deployment. The team needs to ensure the application data is protected both in transit and at rest.

Which combination of actions should be taken to accomplish this? (Choose two.)

A.
Use a VPN to set up a tunnel between the on-premises data center and the AWS resources

B.
Use AWS Certificate Manager to create TLS/SSL certificates

C.
Use AWS CloudHSM to encrypt the data

D.
Use AWS KMS to create TLS/SSL certificates

E.
Use AWS KMS to manage the encryption keys used for data encryption

Answer: B,E
Reference:

https://wa.aws.amazon.com/wat.question.SEC_10.en.html

https://aws.amazon.com/blogs/database/best-practices-for-securing-sensitive-data-in-aws-data-stores/

QUESTION NO: 769

A company is using AWS Storage Gateway to create block storage volumes and mount them as Internet Small Computer Systems Interface (iSCSI) devices from on-premises servers. As the Storage Gateway has taken on several new projects, some of the Development teams report that the performance of the iSCSI drives has degraded. When checking the Amazon CloudWatch metrics, a SysOps Administrator notices that the CacheHitPercent metric is below 60% and the CachePercentUsed metric is above 90%.

What steps should the Administrator take to increase Storage Gateway performance?

A.
Change the default block size for the Storage Gateway from 64 KB to 128 KB, 256 KB, or 512 KB to improve I/O performance.

B.
Create a larger disk for the cached volume. In the AWS Management Console, edit the local disks, then select the new disk as the cached volume.

C.
Ensure that the physical disks for the Storage Gateway are in a RAID 1 configuration to allow higher throughput.

D.
Take point-in-time snapshots of all the volumes in Storage Gateway, flush the cache completely, then restore the volumes from the clean snapshots.

Answer: B

Explanation:

QUESTION NO: 770

A SysOps Administrator observes a large number of rogue HTTP requests on an Application Load Balancer (ALB). The requests originate from various IP addresses.

Which action should be taken to block this traffic?

A.
Use Amazon CloudFront to cache the traffic and block access to the web servers

B.
Use Amazon GuardDuty to protect the web servers from bots and scrapers

C.
Use AWS Lambda to analyze the web server logs, detect bot traffic, and block the IP address in the security groups

D.
Use AWS WAF rate-based blacklisting to block this traffic when it exceeds a defined threshold

Answer: D

Explanation:

AWS WAF has rules that can protect web applications from HTTP flood attacks.

QUESTION NO: 771

A company issued SSL certificates to its users, and needs to ensure the private keys that are used to sign the certificates are encrypted. The company needs to be able to store the private keys and perform cryptographic signing operations in a secure environment.

Which service should be used to meet these requirements?

A.
AWS CloudHSM

B.
AWS KMS

C.
AWS Certificate Manager

D.
Amazon Connect

Answer: C
Reference: https://docs.aws.amazon.com/acm/latest/userguide/kms.html

QUESTION NO: 772

A SysOps Administrator is trying to set up an Amazon Route 53 domain name to route traffic to a website hosted on Amazon S3. The domain name of the website is www.anycompany.com and the S3 bucket name is anycompany-static. After the record set is set up in Route 53, the domain name www.anycompany.com does not seem to work, and the static website is not displayed in the browser.

Which of the following is a cause of this?

A.
The S3 bucket must be configured with Amazon CloudFront first

B.
The Route 53 record set must have an IAM role that allows access to the S3 bucket

C.
The Route 53 record set must be in the same region as the S3 bucket

D.
The S3 bucket name must match the record set name in Route 53

Answer: C
Explanation:

QUESTION NO: 773

A SysOps Administrator at an ecommerce company discovers that several 404 errors are being sent to one IP address every minute. The Administrator suspects a bot is collecting information about products listed on the company's website.

Which service should be used to block this suspected malicious activity?

A.
AWS CloudTrail

B.
Amazon Inspector

C.
AWS Shield Standard

D.
AWS WAF

Answer: D
Reference: https://docs.aws.amazon.com/waf/latest/developerguide/classic-tutorials-ddos-cross-service-WAF.html

QUESTION NO: 774

A company wants to reduce costs across the entire company after discovering that several AWS accounts were using unauthorized services and incurring extremely high costs.

Which AWS service enables the company to reduce costs by controlling access to AWS services for all AWS accounts?

A.
AWS Cost Explorer

B.
AWS Config

C.
AWS Organizations

D.
AWS Budgets

Answer: D
Reference: https://aws.amazon.com/aws-cost-management/

QUESTION NO: 775

A company has an application database on Amazon RDS that runs a resource-intensive reporting job. This is causing other applications using the database to run slowly.

What should the SysOps Administrator do to resolve this issue?

A.
Create Amazon RDS backups

B.
Create Amazon RDS read replicas to run the report

C.
Enable Multi-AZ mode on Amazon RDS

D.
Use Amazon RDS automatic host replacement

Answer: B
Explanation:

QUESTION NO: 776

A company wants to increase the availability and durability of a critical business application. The

application currently uses a MySQL database running on an Amazon EC2 instance. The company wants to minimize application changes.

How should the company meet these requirements?

A.
Shut down the EC2 instance. Enable multi-AZ replication within the EC2 instance, then restart the instance.

B.
Launch a secondary EC2 instance running MySQL. Configure a cron job that backs up the database on the primary EC2 instance and copies it to the secondary instance every 30 minutes.

C.
Migrate the database to an Amazon RDS Aurora DB instance and create a Read Replica in another Availability Zone.

D.
Create an Amazon RDS Microsoft SQL DB instance and enable multi-AZ replication. Back up the existing data and import it into the new database.

Answer: D
Reference:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_SQLServerMultiAZ.html

QUESTION NO: 777

A SysOps Administrator has an AWS CloudFormation template of the company's existing infrastructure in us-west-2. The Administrator attempts to use the template to launch a new stack in eu-west-1, but the stack only partially deploys, receives an error message, and then rolls back.

Why would this template fail to deploy? (Choose two.)

A.
The template referenced an IAM user that is not available in eu-west-1

B.
The template referenced an Amazon Machine Image (AMI) that is not available in eu-west-1

C.
The template did not have the proper level of permissions to deploy the resources

D.

The template requested services that do not exist in eu-west-1

E.
CloudFormation templates can be used only to update existing services

Answer: B,C
Explanation:

QUESTION NO: 778

A SysOps Administrator has been asked to configure user-defined cost allocation tags for a new AWS account. The company is using AWS Organizations for account management.

What should the Administrator do to enable user-defined cost allocation tags?

A.
Log in to the AWS Billing and Cost Management console of the new account, and use the Cost Allocation Tags manager to create the new user-defined cost allocation tags.

B.
Log in to the AWS Billing and Cost Management console of the payer account, and use Cost Allocation Tags manager to create the new user-defined cost allocation tags.

C.
Log in to the AWS Management Console of the new account, use the Tag Editor to create the new user-defined tags, then use the Cost Allocation Tags manager in the new account to mark the tags as cost allocation tags.

D.
Log in to the AWS Management Console of the new account, use the Tag Editor to create the new user-defined tags, then use the Cost Allocation Tags manager in the payer account to mark the tags as cost allocation tags.

Answer: B
Reference: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/activating-tags.html

QUESTION NO: 779

A company developed and now runs a memory-intensive application on multiple Amazon EC2

Linux instances. The memory utilization metrics of the EC2 Linux instances must be monitored every minute.

How should the SysOps Administrator publish the memory metrics? (Choose two.)

A.
Enable detailed monitoring on the instance within Amazon CloudWatch

B.
Publish the memory metrics to Amazon CloudWatch Events

C.
Publish the memory metrics using the Amazon CloudWatch agent

D.
Publish the memory metrics using Amazon CloudWatch Logs

E.
Set metrics_collection_interval to 60 seconds

Answer: A,B
Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/automating_with_cloudwatch_events.html

QUESTION NO: 780

A company is releasing a new static website hosted on Amazon S3. The static website hosting feature was enabled on the bucket and content was uploaded; however, upon navigating to the site, the following error message is received:

403 Forbidden – Access Denied

What change should be made to fix this error?

A.
Add a bucket policy that grants everyone read access to the bucket

B.
Add a bucket policy that grants everyone read access to the bucket objects

C.
Remove the default bucket policy that denies read access to the bucket

D.
Configure cross-origin resource sharing (CORS) on the bucket

Answer: B
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/s3-website-cloudfront-error-403/

QUESTION NO: 781

A company runs an Amazon RDS MySQL DB instance. Corporate policy requires that a daily backup of the database must be copied to a separate security account.

What is the MOST cost-effective way to meet this requirement?

A.
Copy an automated RDS snapshot to the security account using the copy-db-snapshot command with the AWS CLI.

B.
Create an RDS MySQL Read Replica for the critical database in the security account, then enable automatic backups for the Read Replica.

C.
Create an RDS snapshot with the AWS CLI create-db-snapshot command, share it with the security account, then create a copy of the shared snapshot in the security account.

D.
Use AWS DMS to replicate data from the critical database to another RDS MySQL instance in the security account, then use an automated backup for the RDS instance.

Answer: C
Explanation:

QUESTION NO: 782

A SysOps Administrator must set up notifications for whenever combined billing exceeds a certain threshold for all AWS accounts within a company. The Administrator has set up AWS Organizations and enabled Consolidated Billing.

Which additional steps must the Administrator perform to set up the billing alerts?

A.
In the payer account: Enable billing alerts in the Billing and Cost Management console; publish an Amazon SNS message when the billing alert triggers.

B.
In each account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.

C.
In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in the Billing and Cost Management console to publish an SNS message when the alarm triggers.

D.
In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.

Answer: D
Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

QUESTION NO: 783

A VPC is connected to a company data center by a VPN. An Amazon EC2 instance with the IP address 172.31.16.139 is within a private subnet of the VPC. A SysOps Administrator issued a ping command to the EC2 instance from an on-premises computer with the IP address 203.0.113.12 and did not receive an acknowledgment. VPC Flow Logs were enabled and showed the following:

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What action will resolve the issue?

A.
Modify the EC2 security group rules to allow inbound traffic from the on-premises computer

B.
Modify the EC2 security group rules to allow outbound traffic to the on-premises computer

C.
Modify the VPC network ACL rules to allow inbound traffic from the on-premises computer

D.
Modify the VPC network ACL rules to allow outbound traffic to the on-premises computer

Answer: B
Explanation:

QUESTION NO: 784

A web application runs on Amazon EC2 instances behind an ELB Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. Amazon Route 53 is used for DNS and points to the load balancer. A SysOps Administrator has launched a new Auto Scaling group with a new version of the application, and wants to gradually shift traffic to the new version.

How can this be accomplished?

A.
Create an Auto Scaling target tracking scaling policy to gradually move traffic from the old version to the new one

B.
Change the Application Load Balancer to a Network Load Balancer, then add both Auto Scaling groups as targets

C.
Use an Amazon Route 53 weighted routing policy to gradually move traffic from the old version to the new one

D.
Deploy Amazon Redshift to gradually move traffic from the old version to the new one using a set of predefined values

Answer: A
Reference: https://github.com/aws/containers-roadmap/issues/76

QUESTION NO: 785

A company uses federation to authenticate users and grant AWS permissions. The SysOps Administrator has been asked to determine who made a request to AWS Organizations for a new

AWS account.

What should the Administrator review to determine who made the request?

A.
AWS CloudTrail for the federated identity user name

B.
AWS IAM Access Advisor for the federated user name

C.
AWS Organizations access log for the federated identity user name

D.
Federated identity provider logs for the user name

Answer: D
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html

QUESTION NO: 786

A serverless application running on AWS Lambda is expected to receive a significant increase in traffic. A SysOps Administrator needs to ensure that the Lambda function is configured to scale so the application can process the increased traffic.

What should the Administrator do to accomplish this?

A.
Attach additional elastic network interfaces to the Lambda function

B.
Configure AWS Application Auto Scaling based on the Amazon CloudWatch Lambda metric for the number of invocations

C.
Ensure the concurrency limit for the Lambda function is higher than the expected simultaneous function executions

D.
Increase the memory available to the Lambda function

Answer: A

Explanation:

QUESTION NO: 787

A SysOps Administrator is notified that an Amazon EC2 instance has stopped responding. The AWS Management Console indicates that the system checks are failing.

What should the SysOps Administrator do first to resolve this issue?

A.
Reboot the EC2 instance so it can be launched on a new host.

B.
Stop and then start the EC2 instance so that it can be launched on a new host.

C.
Terminate the EC2 instance and relaunch it.

D.
View the AWS CloudTrail log to investigate what changed on the EC2 instance.

Answer: B
Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstances.html

QUESTION NO: 788

An ecommerce site is using Amazon ElastiCache with Memcached to store session state for a web application and to cache frequently used data. For the last month, users have been complaining about performance. The metric data for the Amazon EC2 instances and the Amazon RDS instance appear normal, but the eviction count metrics are high.

What should be done to address this issue and improve performance?

A.
Scale the cluster by adding additional nodes

B.

Scale the cluster by adding read replicas

C.
Scale the cluster by increasing CPU capacity

D.
Scale the web layer by adding additional EC2 instances

Answer: B
Explanation:

QUESTION NO: 789

A company needs to migrate an on-premises asymmetric key management system into AWS.

Which AWS service should be used to accomplish this?

A.
AWS Certificate Manager

B.
AWS CloudHSM

C.
AWS KMS

D.
AWS Secrets Manager

Answer: B
Reference: https://aws.amazon.com/blogs/security/how-to-byok-bring-your-own-key-to-aws-kms-for-less-than-15-00-a-year-using-aws-cloudhsm/

QUESTION NO: 790

A SysOps Administrator is deploying a test site running on Amazon EC2 instances. The application requires both incoming and outgoing connectivity to the Internet.

Which combination of steps are required to provide internet connectivity to the EC2 instances? (Choose two.)

A.
Add a NAT gateway to a public subnet

B.
Attach a private address to the elastic network interface on the EC2 instance

C.
Attach an Elastic IP address to the internet gateway

D.
Add an entry to the route table for the subnet that points to an internet gateway

E.
Create an internet gateway and attach it to a VPC

Answer: D,E
Explanation:

QUESTION NO: 791

A Security and Compliance team is reviewing Amazon EC2 workloads for unapproved AMI usage.

Which action should a SysOps Administrator recommend?

A.
Create a custom report using AWS Systems Manager Inventory to identify unapproved AMIs

B.
Run Amazon Inspector on all EC2 instances and flag instances using unapproved AMIs

C.
Use an AWS Config rule to identify unapproved AMIs

D.
Use AWS Trusted Advisor to identify EC2 workloads using unapproved AMIs

Answer: C
Reference: https://aws.amazon.com/blogs/devops/aws-config-checking-for-compliance-with-new-managed-rule-options/

QUESTION NO: 792

A company needs to have real-time access to image data while seamlessly maintaining a copy of the images in an offsite location.

Which AWS solution would allow access to the image data locally while also providing for disaster recovery?

A.
Create an AWS Storage Gateway volume gateway configured as a stored volume. Mount it from clients using Internet Small Computer System Interface (iSCSI).

B.
Mount an Amazon EFS volume on a local server. Share this volume with employees who need access to the images.

C.
Store the images in Amazon S3, and use AWS Data Pipeline to allow for caching of S3 data on local workstations.

D.
Use Amazon S3 for file storage, and enable S3 Transfer Acceleration to maintain a cache for frequently used files to increase local performance.

Answer: D
Explanation:

QUESTION NO: 793

A SysOps Administrator needs to create a replica of a company’s existing AWS infrastructure in a new AWS account. Currently, an AWS Service Catalog portfolio is used to create and manage resources.

What is the MOST efficient way to accomplish this?

A.
Create an AWS CloudFormation template to use the AWS Service Catalog portfolio in the new AWS account.

B.
Manually create an AWS Service Catalog portfolio in the new AWS account that duplicates the original portfolio.

C.
Run an AWS Lambda function to create a new AWS Service Catalog portfolio based on the output of the DescribePortfolio API operation.

D.
Share the AWS Service Catalog portfolio with the other AWS accounts and import the portfolio into the other AWS accounts.

Answer: A
Reference: https://aws.amazon.com/blogs/mt/automate-account-creation-and-resource-provisioning-using-aws-service-catalog-aws-organizations-and-aws-lambda/

QUESTION NO: 794

A company is operating a multi-account environment under a single organization using AWS Organizations. The Security team discovers that some employees are using AWS services in ways that violate company policies. A SysOps Administrator needs to prevent all users of an account, including the root user, from performing certain restricted actions.

What should be done to accomplish this?

A.
Apply service control policies (SCPs) to allow approved actions only

B.
Apply service control policies (SCPs) to prevent restricted actions

C.
Define permissions boundaries to allow approved actions only

D.
Define permissions boundaries to prevent restricted actions

Answer: B
Reference: https://aws.amazon.com/blogs/security/announcing-aws-organizations-centrally-manage-multiple-aws-accounts/

QUESTION NO: 795

An application is running on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are configured in an Amazon EC2 Auto Scaling group. A SysOps Administrator must configure the application to scale based on the number of incoming requests.

Which solution accomplishes this with the LEAST amount of effort?

A.
Use a simple scaling policy based on a custom metric that measures the average active requests of all EC2 instances

B.
Use a simple scaling policy based on the Auto Scaling group GroupDesiredCapacity metric

C.
Use a target tracking scaling policy based on the ALB's ActiveConnectionCount metric

D.
Use a target tracking scaling policy based on the ALB's RequestCountPerTarget metric

Answer: A
Explanation:

QUESTION NO: 796

A SysOps Administrator has created an Amazon EC2 instance using an AWS CloudFormation template in the us-east-1 Region. The Administrator finds that this template has failed to create an EC2 instance in the us-west-2 Region.

What is one cause for this failure?

A.
Resources tags defined in the CloudFormation template are specific to the us-east-1 Region.

B.
The Amazon Machine Image (AMI) ID referenced in the CloudFormation template could not be found in the us-west-2 Region.

C.
The cfn-init script did not execute during resource provisioning in the us-west-2 Region.

D.
The IAM user was not created in the specified Region.

Answer: B
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html

QUESTION NO: 797

Users are struggling to connect to a single public-facing development web server using its public IP address on a unique port number of 8181. The security group is correctly configured to allow access on that port, and the network ACLs are using the default configuration.

Which log type will confirm whether users are trying to connect to the correct port?

A.
AWS CloudTrail logs

B.
Elastic Load Balancer access logs

C.
VPC Flow Logs

D.
Amazon S3 access logs

Answer: C
Explanation:

QUESTION NO: 798

The Security team at AnyCompany discovers that some employees have been using individual AWS accounts that are not under the control of AnyCompany. The team has requested that those individual accounts be linked to the central organization using AWS Organizations.

Which action should a SysOps Administrator take to accomplish this?

A.
Add each existing account to the central organization using AWS IAM.

B.
Create a new organization in each account and join them to the central organization.

C.
Log in to each existing account and add them to the central organization.

D.
Send each existing account an invitation from the central organization.

Answer: A
Explanation:

QUESTION NO: 799

A SysOps Administrator has received a request to enable access logging for a Network Load Balancer and is setting up an Amazon S3 bucket to store the logs.

What are the MINIMUM requirements for the S3 bucket? (Choose two.)

A.
The bucket must be in the same Region as the Network Load Balancer.

B.
The bucket must have a bucket policy that grants Elastic Load Balancing permissions to write the access logs to the bucket.

C.
The bucket must have encryption enabled.

D.
The bucket must have lifecycle policies set.

E.
The bucket must have public access disabled.

Answer: A,B
Reference: https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-access-logs.html (bucket requirements)

QUESTION NO: 800

An application is running on an Amazon EC2 instance. A SysOps Administrator is tasked with allowing the application access to an Amazon S3 bucket.

What should be done to ensure optimal security?

A.
Apply an S3 bucket policy to allow access from all EC2 instances.

B.
Create an IAM user and create a script to inject the credentials on boot.

C.
Create and assign an IAM role for Amazon S3 access to the EC2 instance.

D.
Embed an AWS credentials file for an IAM user inside the Amazon Machine Image (AMI).

Answer: C
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

QUESTION NO: 801

A company's Marketing department generates gigabytes of assets each day and stores them locally. They would like to protect the files by backing them up to AWS. All the assets should be stored on the cloud, but the most recent assets should be available locally for low latency access.

Which AWS service meets the requirements?

A.
Amazon EBS

B.
Amazon EFS

C.
Amazon S3

D.
AWS Storage Gateway

Answer: D
Reference: https://aws.amazon.com/storagegateway/faqs/

QUESTION NO: 802

A SysOps Administrator is attempting to use AWS Systems Manager Session Manager to initiate a SSH session with an Amazon EC2 instance running on a custom Linux Amazon Machine Image (AMI). The Administrator cannot find the target instance in the Session Manager console.

Which combination of actions will solve this issue? (Choose two.)

A.
Add Systems Manager permissions to the instance profile.

B.
Configure the bucket used by Session Manager logs to allow write access.

C.
Install Systems Manager Agent on the instance.

D.
Modify the instance security group to allow inbound traffic on SSH port 22.

E.
Reboot the instance with a new SSH key pair named ssm-user.

Answer: B,D
Explanation:

QUESTION NO: 803

A Storage team wants all data transfers to an Amazon S3 bucket to remain within the AWS network. The team makes all changes to the AWS network infrastructure manually. An S3 VPC endpoint is created, and an endpoint policy with the proper permissions is set up. However, the application running on Amazon EC2 instances in the VPC is still unable to access the S3 bucket endpoint.

What is one cause of this issue?

A.
Request metrics for the S3 bucket need to be enabled.

B.
S3 access logs need to be disabled for the VPC endpoints to function.

C.
The subnet does not have the VPC endpoint as a target in the route table.

D.
The EC2 instances need to have an Elastic Network Adapter enabled.

Answer: B
Explanation:

QUESTION NO: 804

As part of a federated identity configuration, an IAM policy is created and attached to an IAM role.

Who is responsible for creating the IAM policy and attaching it to the IAM role, according to the shared responsibility model?

A.
AWS is responsible for creating and attaching the IAM policy to the role.

B.
AWS is responsible for creating the role, and a SysOps Administrator is responsible for attaching the policy to the role.

C.
A SysOps Administrator is responsible for creating and attaching the IAM policy to the role.

D.
A SysOps Administrator is responsible for creating the role, and AWS is responsible for attaching the policy to the role.

Answer: C
Reference: https://aws.amazon.com/iam/faqs/

QUESTION NO: 805

An application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group across multiple Availability Zones. The Information Security team wants to track application requests by the originating IP and the EC2 instance that processes the request.

Which of the following tools or services provides this information?

A.
Amazon CloudWatch

B.
AWS CloudTrail

C.
Elastic Load Balancing access logs

D.
VPC Flow Logs

Answer: C
Reference: https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/elb.html

QUESTION NO: 806

An Amazon EC2 instance in a private subnet needs to copy data to an Amazon S3 bucket. For security reasons, the connection from the EC2 instance to Amazon S3 must not traverse across the Internet.

What action should the SysOps Administrator take to accomplish this?

A.
Create a NAT instance and route traffic destined to Amazon S3 through it.

B.
Create a VPN connection between the EC2 instance and Amazon S3.

C.

Create an S3 VPC endpoint in the VPC where the EC2 instance resides.

D.
Use AWS Direct Connect to maximize throughput and keep the traffic private.

Answer: D
Explanation:

QUESTION NO: 807

A SysOps Administrator is in the process of setting up a new AWS Storage Gateway. The Storage Gateway activation is failing when the Administrator attempts to activate the Storage Gateway from the Storage Gateway console.

What are the potential causes of this error? (Choose two.)

A.
The Storage Gateway does not have an upload buffer configured.

B.
The Storage Gateway does not have a backing Amazon S3 bucket configured.

C.
The Storage Gateway does not have a cache volume configured.

D.
The Storage Gateway does not have the correct time.

E.
The Storage Gateway is not accessible from the Administrator's client over port 80.

Answer: A,D
Reference:
https://docs.aws.amazon.com/storagegateway/latest/userguide/GatewayTroubleshooting.html

QUESTION NO: 808

A SysOps Administrator needs to monitor all the object upload and download activity of a single Amazon S3 bucket. Monitoring must include tracking the AWS account of the caller, the IAM user

role of the caller, the time of the API call, and the IP address of the API.

Where can the Administrator find this information?

A.
AWS CloudTrail data event logging

B.
AWS CloudTrail management event logging

C.
Amazon Inspector bucket event logging

D.
Amazon Inspector user event logging

Answer: A
Explanation:

QUESTION NO: 809

A company's website went down for several hours. The root cause was a full disk on one of the company's Amazon EC2 instances.

Which steps should the SysOps Administrator take to prevent this from happening in this future?

A.
Configure Amazon CloudWatch Events to filter and forward AWS Health events for disk space utilization to an Amazon SNS topic to notify the Administrator.

B.
Create an AWS Lambda function to describe the volume status for each EC2 instance. Post a notification to an Amazon SNS topic when a volume status is impaired.

C.
Enable detailed monitoring for the EC2 instances. Create an Amazon CloudWatch alarm to notify the Administrator when disk space is running low.

D.
Use the Amazon CloudWatch agent on the EC2 instances to collect disk metrics. Create a CloudWatch alarm to notify the Administrator when disk space is running low.

Answer: D

Explanation:

QUESTION NO: 810

A SysOps Administrator needs to retrieve a file from the GLACIER storage class of Amazon S3. The Administrator wants to receive an Amazon SNS notification when the file is available for access.

What action should be taken to accomplish this?

A.
Create an Amazon CloudWatch Events event for file restoration from Amazon S3 Glacier using the GlacierJobDescription API and send the event to an SNS topic the Administrator has subscribed to.

B.
Create an AWS Lambda function that performs a HEAD request on the object being restored and checks the storage class of the object. Then send a notification to an SNS topic the Administrator has subscribed to when the storage class changes to STANDARD.

C.
Enable an Amazon S3 event notification for the s3:ObjectCreated:Post event that sends a notification to an SNS topic the Administrator has subscribed to.

D.
Enable S3 event notification for the s3:ObjectCreated:Completed event that sends a notification to an SNS topic the Administrator has subscribed to.

Answer: C

Explanation:

QUESTION NO: 811

A company has received a notification in its AWS Personal Health Dashboard that one of its Amazon EBS-backed Amazon EC2 instances is on hardware that is scheduled for maintenance. The instance runs a critical production workload that must be available during normal business hours.

Which steps will ensure that the instance maintenance does not produce an outage?

A.
Configure an Amazon Lambda function to automatically start the instance if it is stopped.

B.
Create an Amazon Machine Image (AMI) of the instance and use the AMI to launch a new instance once the existing instance is retired.

C.
Enable termination protection on the EC2 instance.

D.
Stop and start the EC2 instance during a maintenance window outside of normal business hours.

Answer: A
Explanation:

QUESTION NO: 812

Security has identified an IP address that should be explicitly denied for both ingress and egress requests for all services in an Amazon VPC immediately.

Which feature can be used to meet this requirement?

A.
Host-based firewalls

B.
NAT Gateway

C.
Network access control lists

D.
Security Groups

Answer: A
Reference: https://aws.amazon.com/answers/networking/vpc-security-capabilities/

QUESTION NO: 813

An Application Load Balancer (ALB) is configured in front of Amazon EC2 instances. The current target group health check configuration is:

Interval: 30 seconds

Unhealthy threshold: 10

Healthy threshold: 5

Which steps should a SysOps Administrator take to reduce the amount of time needed to remove unhealthy instances? (Choose two.)

A.
Change the healthy threshold configuration to 1.

B.
Change the interval configuration to 15.

C.
Change the interval configuration to 60.

D.
Change the unhealthy threshold configuration to 15.

E.
Change the unhealthy threshold configuration to 5.

Answer: C,D
Explanation:

QUESTION NO: 814

A company has a web application that is used across all company divisions. Each application request contains a header that includes the name of the division making the request. The SysOps Administrator wants to identify and count the requests from each division.

Which condition should be added to the web ACL of the AWS WAF to accomplish this?

A.
Cross-site scripting

B.
Geo match

C.
IP match

D.
String match

Answer: C
Explanation:

QUESTION NO: 815

A SysOps Administrator is deploying an Amazon EC2 instance and is using third-party VPN software to route traffic to an on-premises data center.

Based on the shared responsibility model, AWS is responsible for managing which element of this deployment?

A.
Configuring Ipsec tunnels for the VPN.

B.
Ensuring high availability of the EC2 instance.

C.
Ensuring high availability of the VPN connection.

D.
Managing the health of the underlying EC2 host.

Answer: D
Explanation:

QUESTION NO: 816

A SysOps Administrator is notified that an automated failover of an Amazon RDS database has occurred.

What are possible causes for this? (Choose two.)

A.
A read contention on the database.

B.
A storage failure on the primary database.

C.
A write contention on the database.

D.
Database corruption errors.

E.
The database instance type was changed.

Answer: B,D
Reference: https://medium.com/@hk_it_er/summary-on-the-aws-rds-faq-90dd443f983

QUESTION NO: 817

A recent AWS CloudFormation stack update has failed and returned the error UPDATE_ROLLBACK_FAILED. A SysOps Administrator is tasked with returning the CloudFormation stack to its previous working state.

What must be done to accomplish this?

A.
Fix the error that caused the rollback to fail, then select the Continue Update Rollback action in the console.

B.
Select the Update Stack action with a working template in the console.

C.
Update the password of the IAM user, then select the Continue Update Rollback action in the console.

D.
Use the AWS CLI to manually change the stack status to UPDATE_COMPLETE, then continue updating the stack with a working template.

Answer: A
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-continueupdaterollback.html

QUESTION NO: 818

A company needs to run a distributed application that processes large amount of data across multiple Amazon EC2 instances. The application is designed to tolerate processing interruptions.

What is the MOST cost-effective Amazon EC2 pricing model for these requirements?

A.
Dedicated Hosts

B.
On-Demand Instances

C.
Reserved Instances

D.
Spot Instances

Answer: D
Reference: https://aws.amazon.com/blogs/big-data/best-practices-for-running-apache-spark-applications-using-amazon-ec2-spot-instances-with-amazon-emr/

QUESTION NO: 819

A SysOps Administrator working on an Amazon EC2 instance has misconfigured the clock by one hour. The EC2 instance is sending data to Amazon CloudWatch through the CloudWatch agent. The timestamps on the logs are 45 minutes in the future.

What will be the result of this configuration?

A.
Amazon CloudWatch will not capture the data because it is in the future.

B.
Amazon CloudWatch will accept the custom metric data and record it.

C.
The Amazon CloudWatch agent will check the Network Time Protocol (NTP) server before sending the data, and the agent will correct the time.

D.
The Amazon CloudWatch agent will check the Network Time Protocol (NTP) server, and the agent will not send the data because it is more than 30 minutes in the future.

Answer: B
Explanation:

QUESTION NO: 820

A company recently performed a security audit of all its internal applications developed in house. Certain business-critical applications that handle sensitive data were flagged because they use Amazon ES clusters that are open for read/write to a wider user group that intended.

Who is responsible for correcting the issue?

A.
AWS Premium Support

B.
the Amazon ES team

C.
the AWS IAM team

D.
a SysOps Administrator

Answer: A
Explanation:

QUESTION NO: 821

A SysOps Administrator has created a new Amazon S3 bucket named mybucket for the Operations team. Members of the team are part of an IAM group to which the following IAM policy has been assigned:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "s3:GetObject",
         "s3:GetObjectVersion",
         "s3:PutObject",
         "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::mybucket/*"
    }
  ]
}
```

BrainDumps

Which of the following actions will be allowed on the bucket? (Choose two.)

A.
Get the bucket's region.

B.
Delete an object.

C.
Delete the bucket.

D.
Download an object.

E.
List all the buckets in the account.

Answer: B,D

Explanation:

QUESTION NO: 822

A company needs to restrict access to an Amazon S3 bucket to Amazon EC2 instances in a VPC only. All traffic must be over the AWS private network.

What actions should the SysOps Administrator take to meet these requirements?

A.
Create a VPC endpoint for the S3 bucket, and create an IAM policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.

B.
Create a VPC endpoint for the S3 bucket, and create a S3 bucket policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.

C.
Create a service-linked role for Amazon EC2 that allows the EC2 instances to interact directly with Amazon S3, and attach an IAM policy to the role that allows the EC2 instances full access to the S3 bucket.

D.
Create a NAT gateway in the VPC, and modify the VPC route table to route all traffic destined for Amazon S3 through the NAT gateway.

Answer: B

Explanation:

QUESTION NO: 823

A Chief Financial Officer has asked for a breakdown of costs per project in a single AWS account using Cost Explorer.

Which combination of options should be set to accomplish this? (Choose two.)

A.
Activate AWS Budgets.

B.
Activate cost allocation tags.

C.
Create an organization using AWS Organizations.

D.
Create and apply resources tags.

E.
Enable AWS Trusted Advisor.

Answer: A,B
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/tags-billing-cost-center-project/

QUESTION NO: 824

A SysOps Administrator has implemented a VPC network design with the following requirements:

- Two Availability Zones (AZs)
- Two private subnets
- Two public subnets
- One internet gateway
- One NAT gateway

What would potentially cause applications in the VPC to fail during an AZ outage?

A.
A single virtual private gateway, because it can be associated with a single AZ only.

B.
A single internet gateway, because it is not redundant across both AZs.

C.
A single NAT gateway, because it is not redundant across both AZs.

D.
The default VPC route table, because it can be associated with a single AZ only.

Answer: D
Explanation:

QUESTION NO: 825

A SysOps Administration team is supporting an application that stores a configuration file in an Amazon S3 bucket. Previous revisions of the configuration file must be maintained for change control and rollback.

How should the S3 bucket be configured to meet these requirements?

A.
Enable a lifecycle policy on the S3 bucket.

B.
Enable cross-origin resource sharing on the S3 bucket.

C.
Enable object tagging on the S3 bucket.

D.
Enable versioning on the S3 bucket.

Answer: D
Reference: https://docs.aws.amazon.com/AmazonS3/latest/dev/RestoringPreviousVersions.html

QUESTION NO: 826

A company has an existing web application that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB) across two Availability Zones. The application uses an Amazon RDS Multi-AZ DB Instance. Amazon Route 53 record sets route requests for dynamic content to the load balancer and requests for static content to an Amazon S3 bucket. Site visitors are reporting extremely long loading times.

Which actions should be taken to improve the performance of the website? (Choose two.)

A.
Add Amazon CloudFront caching for static content.

B.
Change the load balancer listener from HTTPS to TCP.

C.
Enable Amazon Route 53 latency-based routing.

D.
Implement Amazon EC2 Auto Scaling for the web servers.

E.
Move the static content from Amazon S3 to the web servers.

Answer: C,D
Explanation:

QUESTION NO: 827

An application is being migrated to AWS with the requirement that archived data be retained for at least 7 years.

What Amazon Glacier configuration option should be used to meet this compliance requirement?

A.
A Glacier data retrieval policy

B.
A Glacier vault access policy

C.
A Glacier vault lock policy

D.
A Glacier vault notification

Answer: C
Reference: https://d0.awsstatic.com/whitepapers/Amazon-GlacierVaultLock_CohassetAssessmentReport.pdf

QUESTION NO: 828

A company has several AWS accounts and has set up consolidated billing through AWS Organizations. The total monthly bill has been increasing over several months, and a SysOps Administrator has been asked to determine what is causing this increase.

What is the MOST comprehensive tool that will accomplish this task?

A.
AWS Cost Explorer

B.
AWS Trusted Advisor

C.
Cost allocation tags

D.
Resource groups

Answer: C
Reference: https://aws.amazon.com/answers/account-management/aws-multi-account-billing-strategy/

QUESTION NO: 829

A company has deployed its infrastructure using AWS CloudFormation. Recently, the company made manual changes to the infrastructure. A SysOps Administrator is tasked with determining what was changed and updating the CloudFormation template.

Which solution will ensure all the changes are captured?

A.
Create a new CloudFormation stack based on the changes that were made. Delete the old stack and deploy the new stack.

B.
Update the CloudFormation stack using a change set. Review the changes and update the stack.

C.
Update the CloudFormation stack by modifying the selected parameters in the template to match what was changed.

D.
Use drift detection on the CloudFormation stack. Use the output to update the CloudFormation template and redeploy the stack.

Answer: B
Explanation:

QUESTION NO: 830

A user accidentally deleted a file from an Amazon EBS volume. The SysOps Administrator identified a recent snapshot for the volume.

What should the Administrator do to restore the user's file from the snapshot?

A.
Attach the snapshot to a new Amazon EC2 instance in the same Availability Zone, and copy the deleted file.

B.
Browse to the snapshot and copy the file to the EBS volume within an Amazon EC2 instance.

C.
Create a volume from the snapshot, attach the volume to an Amazon EC2 instance, and copy the deleted file.

D.
Restore the file from the snapshot onto an EC2 instance using the Amazon EC2 console.

Answer: C
Reference: https://aws.amazon.com/blogs/compute/recovering-files-from-an-amazon-ebs-volume-backup/

QUESTION NO: 831

Each SysOps Administrator at a company has a unique IAM user account. Each user is a member of the SysOps IAM group that has an IAM policy applied. A recent change to the IT security policy states that employees must now use their on-premises Active Directory user accounts to access the AWS Management Console.

Which solution should be used to satisfy these requirements?

A.
Configure the on-premises Active Directory to use AWS Direct Connect.

B.
Enable an Active Directory federation in an Amazon Route 53 private zone.

C.
Implement a VPN tunnel and configure an Active Directory connector.

D.
Implement multi-factor authentication for IAM and Active Directory.

Answer: A
Reference: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/usecase5.html

QUESTION NO: 832

A company needs to deploy a web application on two Amazon EC2 instances behind an Application Load Balancer (ALB). Two EC2 instances will also be deployed to host the database. The infrastructure needs to be designed across Availability Zones for high availability and must limit public access to the instances as much as possible.

How should this be achieved within a VPC?

A.
Create one public subnet for the Application Load Balancer, one public subnet for the web servers, and one private subnet for the database servers.

B.
Create one public subnet for the Application Load Balancer, two public subnets for the web servers, and two private subnets for the database servers.

C.
Create two public subnets for the Application Load Balancer, two private subnets for the web servers, and two private subnets for the database servers.

D.
Create two public subnets for the Application Load Balancer, two public subnets for the web servers, and two public subnets for the database servers.

Answer: B
Explanation:

QUESTION NO: 833

A SysOps Administrator receives an email from AWS about a production Amazon EC2 instance backed by Amazon EBS that is on a degraded host scheduled for retirement. The scheduled retirement occurs during business-critical hours.

What should be done to MINIMIZE disruption to the business?

A.
Reboot the instance as soon as possible to perform the system maintenance before the scheduled retirement.

B.
Reboot the instance outside business hours to perform the system maintenance before the scheduled retirement.

C.
Stop/start the instance outside business hours to move to a new host before the scheduled retirement.

D.
Write an AWS Lambda function to restore the system when the scheduled retirement occurs.

Answer: C
Explanation:

QUESTION NO: 834

A company has a business application hosted on Amazon EC2 instances behind an Application Load Balancer. Amazon CloudWatch metrics show that the CPU utilization on the EC2 instances is very high. There are also reports from users that receive HTTP 503 and 504 errors when they try to connect to the application.

Which action will resolve these issues?

A.
Place the EC2 instances into an AWS Auto Scaling group.

B.
Configure the ALB's Target Group to use more frequent health checks.

C.
Enable sticky sessions on the Application Load Balancer.

D.

Increase the idle timeout setting of the Application Load Balancer.

Answer: A
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/elb-capacity-troubleshooting/

QUESTION NO: 835

A SysOps Administrator is maintaining an application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). Users are reporting errors when attempting to launch the application. The Administrator notices an increase in the HTTPCode_ELB_5xx_Count Amazon CloudWatch metric for the load balancer.

What is a possible cause for this increase?

A.
The ALB is associated with private subnets within the VPC.

B.
The ALB received a request from a client, but the client closed the connection.

C.
The ALB security group is not configured to allow inbound traffic from the users.

D.
The ALB target group does not contain healthy EC2 instances.

Answer: D
Reference: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-cloudwatch-metrics.html

QUESTION NO: 836

An application is currently deployed on several Amazon EC2 instances that reside within a VPC. Due to compliance requirements, the EC2 instances cannot have access to the public internet. SysOps Administrators require SSH access to EC2 instances from their corporate office to perform maintenance and other administrative tasks.

Which combination of actions should be taken to permit SSH access to the EC2 instances while meeting the compliance requirements? (Choose two.)

A.
Attach a NAT gateway to the VPC and configure routing

B.
Attach a virtual private gateway to the VPC and configure routing

C.
Attach an internet gateway to the VPC and configure routing

D.
Configure a VPN connection back to the corporate office

E.
Configure an Application Load Balancer in front of the EC2 instances

Answer: A,D
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

QUESTION NO: 837

A developer is deploying a web application on Amazon EC2 instances behind an Application Load Balancer (ALB) and notices that the application is not receiving all the expected elements from HTTP requests. The developer suspects users are not sending the correct query string.

How should a sysops administrator verify this?

A.
Monitor the ALB default Amazon CloudWatch metrics. Verify that the requests contain the expected query string.

B.
onfigure the ALB to store access logs within Amazon S3. Verify that log entries contain the expected query string.

C.
Open the ALB logs in Amazon CloudWatch. Verify that requests contain the expected query string.

D.
Create a custom Amazon CloudWatch metric to store requests. Verify that the metric contains the expected query string.

Answer: A
Reference: https://aws.amazon.com/blogs/aws/new-advanced-request-routing-for-aws-application-load-balancers/

QUESTION NO: 838

A company's IT department noticed an increase in the spend of their Developer AWS account. There are over 50 Developers using the account, and the Finance team wants to determine the service costs incurred by each Developer.

What should a SysOps Administrator do to collect this information? (Choose two.)

A.
Activate the createdBy tag in the account

B.
Analyze the usage with Amazon CloudWatch dashboards

C.
Analyze the usage with Cost Explorer

D.
Configure AWS Trusted Advisor to track resource usage

E.
Create a billing alarm in AWS Budgets

Answer: D,E
Reference: https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

QUESTION NO: 839

An ecommerce company uses an Amazon ElastiCache for Memcached cluster for in-memory caching of popular product queries on the shopping site. When viewing recent Amazon CloudWatch metrics data for the ElastiCache cluster, the sysops administrator notices a large number of evictions.

Which of the following actions will reduce these evictions? (Choose two.)

A.
Add an additional node to the ElastiCache cluster

B.
Increase the ElastiCache time to live (TTL)

C.
Increase the individual node size inside the ElastiCache cluster

D.
Put an Elastic Load Balancer in front of the ElastiCache cluster

E.
Use Amazon Simple Queue Service (Amazon SQS) to decouple the ElastiCache cluster

Answer: A,C
Reference: https://shaikmdrafi.wordpress.com/2017/05/30/aws-certified-sysops-administrator-associate-level/

QUESTION NO: 840

A sysops administrator created an AWS Lambda function within a VPC with no access to the Internet. The Lambda function pulls messages from an Amazon SQS queue and stores them in an Amazon RDS instance in the same VPC. After executing the Lambda function, the data is not showing up on the RDS instance.

Which of the following are possible causes for this? (Choose two.)

A.
A VPC endpoint has not been created for Amazon RDS

B.
A VPC endpoint has not been created for Amazon SQS

C.
The RDS security group is not allowing connections from the Lambda function

D.
The subnet associated with the Lambda function does not have an internet gateway attached

E.
The subnet associated with the Lambda function has a NAT gateway

Answer: B,E

Explanation:

QUESTION NO: 841

A company designed a specialized Amazon EC2 instance configuration for its Data Scientists. The Data Scientists want to create and delete EC2 instances on their own, but are not comfortable with configuring all the settings for EC2 instances without assistance. The configuration runs proprietary software that must be kept private within the company's AWS accounts, and should be available to the Data Scientists, but no other users within the accounts.

Which solution should a SysOps Administrator use to allow the Data Scientists to deploy their workloads with MINIMAL effort?

A.
Create an Amazon Machine Image (AMI) of the EC2 instance. Share the AMI with authorized accounts owned by the company. Allow the Data Scientists to create EC2 instances with this AMI.

B.
Distribute an AWS CloudFormation template containing the EC2 instance configuration to the Data Scientists from an Amazon S3 bucket. Set the S3 template object to be readable from the AWS Organizations orgId.

C.
Publish the instance configuration to the Private Marketplace. Share the Private Marketplace with the company's AWS accounts. Allow the Data Scientists to subscribe and launch the product from the Private Marketplace.

D.
Upload an AWS CloudFormation template to AWS Service Catalog. Allow the Data Scientists to provision and deprovision products from the company's AWS Service Catalog portfolio.

Answer: B

Explanation:

QUESTION NO: 842

A company developed and now runs a memory-intensive application on multiple Amazon EC2 Linux instances. The memory utilization metrics of the EC2 Linux instances must be monitored.

Which combination of actions must be taken to accomplish this? (Choose two.)

A.
Enable detailed monitoring on the instance within Amazon CloudWatch.

B.
Implement an AWS Lambda function to track memory metrics.

C.
Install Amazon CloudWatch agent to track memory metrics.

D.
Publish the memory metrics to Amazon CloudWatch Events.

E.
Publish the memory metrics using Amazon CloudWatch Logs.

Answer: A,C
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html

QUESTION NO: 843

An Application team has asked a SysOps Administrator to provision an additional environment for an application in four additional regions. The application is running on more than 100 instances in us-east-1, using fully baked AMIs. An AWS CloudFormation template has been created to deploy resources in us-east-1.

What must the SysOps Administrator do to provision the application quickly?

A.
Copy the AMI to each region using aws ec2 copy-image. Update the CloudFormation mapping to include mappings for the copied AMIs.

B.
Create a snapshot of the running instance and copy the snapshot to the other regions. Create an AMI from the snapshots. Update the CloudFormation template for each region to use the new AMI.

C.
Run the existing CloudFormation template in each additional region based on the success of the template used currently in us-east-1.

D.
Update the CloudFormation template to include the additional regions in the Auto Scaling group.

Update the existing stack in us-east-1.

Answer: C
Explanation:

QUESTION NO: 844

A company wants to identify specific Amazon EC2 instances that are underutilized and the estimated cost savings for each instance.

How can this be done with MINIMAL effort?

A.
Use AWS Budgets to report on low utilization of EC2 instances.

B.
Run an AWS Systems Manager script to check for low memory utilization of EC2 instances.

C.
Run Cost Explorer to look for low utilization of EC2 instances.

D.
Use Amazon CloudWatch metrics to identify EC2 instances with low utilization.

Answer: D
Reference: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-rightsizing.html

QUESTION NO: 845

A SysOps Administrator needs to control access to groups of Amazon EC2 instances. Specific tags on the EC2 instances have already been added.

Which additional actions should the Administrator take to control access? (Choose two.)

A.
Attach an IAM policy to the users or groups that require access to the EC2 instances.

B.

Attach an IAM role to control access to the EC2 instances.

C.
Create a placement group for the EC2 instances and add a specific tag.

D.
Create a service account and attach it to the EC2 instances that need to be controlled.

E.
Create an IAM policy that grants access to any EC2 instances with a tag specified in the Condition element.

Answer: A,E
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/iam-ec2-resource-tags/

QUESTION NO: 846

A company is planning to deploy multiple ecommerce websites across the eu-west-1, ap-east-1, and us-west-1 Regions. The websites consist of Amazon S3 buckets, Amazon EC2 instances, Amazon RDS databases, and Elastic Load Balancers.

Which method will accomplish the deployment with the LEAST amount of effort?

A.
Configure deployment automation using AWS OpsWorks

B.
Configure S3 cross-Region replication

C.
Use AWS CloudFormation stack sets to deploy the application

D.
Use AWS Elastic Beanstalk to deploy the application

Answer: C
Explanation:

QUESTION NO: 847

A company manages multiple AWS accounts and wants to provide access to AWS from a single management account using an existing on-premises Microsoft Active Directory domain.

Which solution will meet these requirements with the LEAST amount of effort?

A.
Create an Active Directory connector using AWS Directory Service. Create IAM users in the target accounts with the appropriate trust policy.

B.
Create an Active Directory connector using AWS Directory Service. Associate the directory with AWS Single Sign-On (AWS SSO). Configure user access to target accounts through AWS SSO.

C.
Create an Amazon Cognito federated identity pool. Associate the pool identity with the on-premises directory. Configure the IAM roles with the appropriate trust policy.

D.
Create an identity provider in AWS IAM associated with the on-premises directory. Create IAM roles in the target accounts with the appropriate trust policy.

Answer: A
Reference: https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

QUESTION NO: 848

A company has an AWS account for each department and wants to consolidate billing and reduce overhead. The company wants to make sure that the finance team is denied from accessing services other than Amazon EC2, the security team is denied from accessing services other than AWS CloudTrail, and IT can access any resource.

Which solution meets these requirements with the LEAST amount of operational overhead?

A.
Create a role for each department within AWS IAM and assign each role the necessary permissions.

B.
Create a user for each department within AWS IAM and assign each user the necessary permissions.

C.
Implement service control policies within AWS Organizations to determine which resources each department can access.

D.
Place each department into an organizational unit (OU) within AWS Organizations and use IAM policies to determine which resources they can access.

Answer: C
Explanation:

QUESTION NO: 849

A company runs an image-processing application on a serverless infrastructure. Each processing job runs in a single AWS Lambda execution. A sysops administrator is tasked with ensuring there is enough capacity to run 500 simultaneous jobs even if other Lambda functions are being run for other applications. The administrator has already increased service limits within the Region.

Which action should be taken?

A.
Configure a dead-letter queue to retry any throttled executions

B.
Modify the memory settings on the Lambda function to allow for 500 parallel executions

C.
Move the image-processing logic to AWS Step Functions

D.
Set the reserved concurrency for the image-processing Lambda function to 500

Answer: D
Reference: https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html

QUESTION NO: 850

A sysops administrator has an AWS Lambda function that performs maintenance on various AWS resources. This function must be run nightly.

Which is the MOST cost-effective solution?

A.
Launch a single t2.nano Amazon EC2 instance and create a Linux cron job to invoke the Lambda function at the same time every night.

B.
Set up an Amazon CloudWatch metrics 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 AWS OpsWorks stack to invoke the Lambda function at the same time every night.

Answer: C
Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/RunLambdaSchedule.html

QUESTION NO: 851

A sysops administrator is managing an application on AWS that uses Amazon EC2 instances and Amazon Aurora MySQL. The EC2 instances and Aurora instances are in two different subnets. The application servers running in EC2 cannot connect to the Aurora database.

The EC2 subnet is 192.168.87.0/24 and has a security group named sg-123456 with the following configuration.

Inbound rules		
Protocol type	Port number	Source IP
TCP 22	(SSH)	192.168.87.0/24
ICMP	All	0.0.0.0/0
Outbound rules		
Protocol type	Port number	Destination IP
All	All	0.0.0.0/0

BrainDumps

The Aurora subnet is 192.168.88.0/24 and has a security group named sg-abcdef with the following configuration.

Inbound rules		
Protocol type	Port number	Source IP
MYSQL/Aurora	3306	192.168.88.0/24
Outbound rules		
Protocol type	Port number	Destination IP
All	All	0.0.0.0/0

BrainDumps

Which action should the sysops administrator take to allow the EC2 instances to connect to the Aurora database?

A.
In the inbound rules table of the Aurora security group, add an inbound TCP rule with the MySQL port and sg-123456 as the traffic source.

B.
In the inbound rules table of the EC2 security group, add an inbound TCP rule with the MySQL port and 192.168.88.0/24 as the traffic source.

C.
In the outbound rules table of the Aurora security group, add an outbound TCP rule with the

MySQL port and 192.168.87.0/24 as the destination.

D.
In the outbound rules table of the EC2 security group, add an outbound TCP rule with the MySQL port and sg-abcdef as the destination.

Answer: C
Explanation:

QUESTION NO: 852

A company has a multi-tier web application. In the web tier, all the servers are in private subnets inside a VPC. The development team wants to make changes to the application that requires access to Amazon S3.

What should be done to accomplish this?

A.
Create a customer gateway to connect to Amazon S3. Modify the route table of the private subnets to use the customer gateway.

B.
Create a gateway VPC endpoint for Amazon S3. Modify the route table of the private subnets to use the gateway VPC endpoint.

C.
Create a NAT gateway in the private subnets. Modify the route table of the subnets to use the NAT gateway.

D.
Create an S3 bucket policy to allow connections from the private subnets. Modify the route table.

Answer: C
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

QUESTION NO: 853

A sysops administrator is managing a VPC network consisting of public and private subnets. Instances in the private subnets access the Internet through a NAT gateway. A recent AWS bill

shows that the NAT gateway charges have doubled. The administrator wants to identify which instances are creating the most network traffic.

How should this be accomplished?

A.
Enable flow logs on the NAT gateway elastic network interface and use Amazon CloudWatch insights to filter data based on the source IP addresses.

B.
Run an AWS Cost and Usage report and group the findings by instance ID.

C.
Use the VPC traffic mirroring feature to send traffic to Amazon QuickSight.

D.
Use Amazon CloudWatch metrics generated by the NAT gateway for each individual instance.

Answer: A

Explanation: