AWS Certified Solutions Architect - Associate.examcollection.premium.exam.987q

Number: Architect-Associate
Passing Score: 800
Time Limit: 120 min
File Version: 4.0



AWS Certified Solutions Architect - Associate

Version 4.0

Exam A

QUESTION 1
A 3-tier e-commerce web application is current deployed on-premises and will be migrated to AWS for greater scalability and elasticity The web server currently shares read-only data using a network distributed file system The app server tier uses a clustering mechanism for discovery and shared session state that depends on IP multicast The database tier uses shared-storage clustering to provide database fall over capability, and uses several read slaves for scaling Data on all servers and the distributed file system directory is backed up weekly to off-site tapes
Which AWS storage and database architecture meets the requirements of the application?

A. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more read replicas. Backup: web servers, app servers, and database backed up weekly to Glacier using snapshots.
B. Web servers: store read-only data in an EC2 NFS server, mount to each web server at boot time. App servers: share state using a combination of DynamoDB and IP multicast. Database: use RDS with multi-AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
C. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
D. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://d0.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf
Amazon Glacier doesn't suit all storage situations. Listed following are a few storage needs for which you should consider other AWS storage options instead of Amazon Glacier.
Data that must be updated very frequently might be better served by a storage solution with lower read/write latencies, such as Amazon EBS, Amazon RDS, Amazon DynamoDB, or relational databases running on EC2.

QUESTION 2
Your customer wishes to deploy an enterprise application to AWS which will consist of several web servers, several application servers and a small (50GB) Oracle database information is stored, both in the database and the file systems of the various servers. The backup system must support database recovery whole server and whole disk restores, and individual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database.
Which backup architecture will meet these requirements?

A. Backup RDS using automated daily DB backups Backup the EC2 instances using AMIs and supplement with file-level backup to S3 using traditional enterprise backup software to provide file level restore
B. Backup RDS using a Multi-AZ Deployment Backup the EC2 instances using Amis, and supplement by copying file system data to S3 to provide file level restore.
C. Backup RDS using automated daily DB backups Backup the EC2 instances using EBS snapshots and supplement with file-level backups to Amazon Glacier using traditional enterprise backup software to provide file level restore
D. Backup RDS database to S3 using Oracle RMAN Backup the EC2 instances using Amis, and supplement with EBS snapshots for individual volume restore.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
You need to use enterprise backup software to provide file level restore. See https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf Page 18:
If your existing backup software does not natively support the AWS cloud, you can use AWS storage gateway products. AWS Storage Gateway is a virtual appliance that provides seamless and secure integration between your data center and the AWS storage infrastructure.

QUESTION 3
Your company has HQ in Tokyo and branch offices all over the world and is using a logistics software with a multi-regional deployment on AWS in Japan, Europe and USA, The logistic software has a 3-tier architecture and currently uses MySQL 5.6 for data persistence. Each region has deployed its own database.
In the HQ region you run an hourly batch process reading data from every region to compute cross-regional reports that are sent by email to all offices this batch process must be completed as fast as possible to quickly optimize logistics how do you build the database architecture in order to meet the requirements'?

A. For each regional deployment, use RDS MySQL with a master in the region and a read replica in the HQ region
B. For each regional deployment, use MySQL on EC2 with a master in the region and send hourly EBS snapshots to the HQ region
C. For each regional deployment, use RDS MySQL with a master in the region and send hourly RDS snapshots to the HQ region
D. For each regional deployment, use MySQL on EC2 with a master in the region and use S3 to copy data files hourly to the HQ region
E. Use Direct Connect to connect all regional MySQL deployments to the HQ region and reduce network latency for the batch process

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A customer has a 10 GB AWS Direct Connect connection to an AWS region where they have a web application hosted on Amazon Elastic Computer Cloud (EC2). The application has dependencies on an on-premises mainframe database that uses a BASE (Basic Available. Sort stale Eventual consistency) rather than an ACID (Atomicity. Consistency isolation. Durability) consistency model. The application is exhibiting undesirable behavior because the database is not able to handle the volume of writes. How can you reduce the load on your on-premises database resources in the most cost-effective way?

A. Use an Amazon Elastic Map Reduce (EMR) S3DistCp as a synchronization mechanism between the on-premises database and a Hadoop cluster on AWS.
B. Modify the application to write to an Amazon SQS queue and develop a worker process to flush the queue to the on-premises database.
C. Modify the application to use DynamoDB to feed an EMR cluster which uses a map function to write to the on-premises database.
D. Provision an RDS read-replica database on AWS to handle the writes and synchronize the two databases using Data Pipeline.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Reference:
https://aws.amazon.com/sqs/faqs/

QUESTION 5
Company B is launching a new game app for mobile devices. Users will log into the game using their existing social media account to streamline data capture. Company B would like to directly save player data and scoring information from the mobile app to a DynamoDS table named Score Data When a user saves their game the progress data will be stored to the Game state S3 bucket. What is the best approach for storing data to DynamoDB and S3?

A. Use an EC2 Instance that is launched with an EC2 role providing access to the Score Data DynamoDB table and the GameState S3 bucket that communicates with the mobile app via web services.
B. Use temporary security credentials that assume a role providing access to the Score Data DynamoDB table and the Game State S3 bucket using web identity federation.
C. Use Login with Amazon allowing users to sign in with an Amazon account providing the mobile app with access to the Score Data DynamoDB table and the Game State S3 bucket.
D. Use an IAM user with access credentials assigned a role providing access to the Score Data DynamoDB table and the Game State S3 bucket for distribution with the mobile app.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The requirements state “Users will log into the game using their existing social media account to streamline data capture.” This is what Cognito is used for, ie Web Identity Federation. Amazon also recommend to “build your app so that it requests temporary AWS security credentials dynamically when needed using web identity federation.”

QUESTION 6
Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes. To be certain that you do not drop any writes to a database hosted on AWS. Which service should you use?

A. Amazon RDS with provisioned IOPS up to the anticipated peak write throughput.
B. Amazon Simple Queue Service (SOS) for capturing the writes and draining the queue to write to the database.
C. Amazon ElastiCache to store the writes until the writes are committed to the database.
D. Amazon DynamoDB with provisioned write throughput up to the anticipated peak write throughput.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/sqs/faqs/
There is no limit on the number of messages that can be pushed onto SQS. The retention period
of the SQS is 4 days by default and it can be changed to 14 days. This will make sure that no writes are missed.

QUESTION 7
You have launched an EC2 instance with four (4) 500 GB EBS Provisioned IOPS volumes attached The EC2 Instance Is EBS-Optimized and supports 500 Mbps

throughput between EC2 and EBS The two EBS volumes are configured as a single RAID o device, and each Provisioned IOPS volume is provisioned with 4.000 IOPS (4 000 16KB reads or writes) for a total of 16.000 random IOPS on the instance The EC2 Instance initially delivers the expected 16 000 IOPS random read and write performance Sometime later in order to increase the total random I/O performance of the instance, you add an additional two 500 GB EBS Provisioned IOPS volumes to the RAID Each volume Is provisioned to 4.000 IOPs like the original four for a total of 24.000 IOPS on the EC2 instance Monitoring shows that the EC2 instance CPU utilization increased from 50% to 70%. but the total random IOPS measured at the instance level does not increase at all.
What is the problem and a valid solution?

A. Larger storage volumes support higher Provisioned IOPS rates: increase the provisioned volume storage of each of the 6 EBS volumes to 1TB
B. The EBS-Optimized throughput limits the total IOPS that can be utilized use an EBS-Optimized instance that provides larger throughput.
C. Small block sizes cause performance degradation, limiting the I'O throughput, configure the instance device driver and file system to use 64KB blocks to increase throughput.
D. RAID 0 only scales linearly to about 4 devices, use RAID 0 with 4 EBS Provisioned IOPS volumes but increase each Provisioned IOPS EBS volume to 6.000 IOPS.
E. The standard EBS instance root volume limits the total IOPS rate, change the instant root volume to also be a 500GB 4.000 Provisioned IOPS volume.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS.
During the pilot, you measured a peak or 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database.
The current deployment consists of a load-balanced auto scaled Ingestion layer using EC2 instances and a PostgreSQL RDS database with 500GB standard storage.
The pilot is considered a success and your CEO has managed to get the attention or some potential investors. The business plan requires a deployment of at least 100K sensors which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year Improvements.
To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling. Which setup win meet the requirements?

A. Add an SQS queue to the ingestion layer to buffer writes to the RDS instance
B. Ingest data into a DynamoDB table and move old data to a Redshift cluster
C. Replace the RDS instance with a 6 node Redshift cluster with 96TB of storage
D. Keep the current architecture but upgrade RDS storage to 3TB and 10K provisioned IOPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You cannot go with DynamoDB because the application is currently using a Postgre SQL which is an RDS. Replacing an RDS SQL with a noSQL DB, for the sake of scaling is not a sensible option.

QUESTION 9
Your company is in the process of developing a next generation pet collar that collects biometric information to assist families with promoting healthy lifestyles for their pets Each collar will push 30kb of biometric data In JSON format every 2 seconds to a collection platform that will process and analyze the data providing health trending

information back to the pet owners and veterinarians via a web portal Management has tasked you to architect the collection platform ensuring the following requirements are met.
Provide the ability for real-time analytics of the inbound biometric data
Ensure processing of the biometric data is highly durable. Elastic and parallel
The results of the analytic processing should be persisted for data mining
Which architecture outlined below win meet the initial requirements for the collection platform?

A. Utilize S3 to collect the inbound sensor data analyze the data from S3 with a daily scheduled Data Pipeline and save the results to a Redshift Cluster.
B. Utilize Amazon Kinesis to collect the inbound sensor data, analyze the data with Kinesis clients and save the results to a Redshift cluster using EMR.
C. Utilize SQS to collect the inbound sensor data analyze the data from SQS with Amazon Kinesis and save the results to a Microsoft SQL Server RDS instance.
D. Utilize EMR to collect the inbound sensor data, analyze the data from EUR with Amazon Kinesis and save me results to DynamoDB.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The POC solution is being scaled up by 1000, which means it will require 72TB of Storage to retain 24 months' worth of data. This rules out RDS as a possible DB solution which leaves you with RedShift. I believe DynamoDB is a more cost effective and scales better for ingest rather than using EC2 in an auto scaling group. Also, this example solution from AWS is somewhat similar for reference.
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_timeseriesprocessing_16.pdf

QUESTION 10
You need a persistent and durable storage to trace call activity of an IVR (Interactive Voice Response) system. Call duration is mostly in the 2-3 minutes timeframe. Each traced call can be either active or terminated. An external application needs to know each minute the list of currently active calls, which are usually a few calls/second. Put once per month there is a periodic peak up to 1000 calls/second for a few hours. The system is open 24/7 and any downtime should be avoided. Historical data is periodically archived to files. Cost saving is a priority for this project.
What database implementation would better fit this scenario, keeping costs as low as possible?

A. Use RDS Multi-AZ with two tables, one for -Active calls" and one for -Terminated calls". In this way the "Active calls_ table is always small and effective to access.
B. Use DynamoDB with a "Calls" table and a Global Secondary Index on a "IsActive"' attribute that is present for active calls only In this way the Global Secondary index is sparse and more effective.
C. Use DynamoDB with a 'Calls" table and a Global secondary index on a 'State" attribute that can equal to "active" or "terminated" in this way the Global Secondary index can be used for all Items in the table.
D. Use RDS Multi-AZ with a "CALLS" table and an Indexed "STATE* field that can be equal to 'ACTIVE" or -TERMINATED" In this way the SOL query Is optimized by the use of the Index.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q: Can a global secondary index key be defined on non-unique attributes?
Yes. Unlike the primary key on a table, a GSI index does not require the indexed attributes to be unique.

Q: Are GSI key attributes required in all items of a DynamoDB table?
No. GSIs are sparse indexes. Unlike the requirement of having a primary key, an item in a DynamoDB table does not have to contain any of the GSI keys. If a GSI key has both hash and range elements, and a table item omits either of them, then that item will not be indexed by the corresponding GSI. In such cases, a GSI can be very useful in efficiently locating items that have an uncommon attribute.
Reference: https://aws.amazon.com/dynamodb/faqs/

QUESTION 11
A web design company currently runs several FTP servers that their 250 customers use to upload and download large graphic files They wish to move this system to AWS to make it more scalable, but they wish to maintain customer privacy and Keep costs to a minimum.
What AWS architecture would you recommend?

A. ASK their customers to use an S3 client instead of an FTP client. Create a single S3 bucket Create an IAM user for each customer Put the IAM Users in a Group that has an IAM policy that permits access to sub-directories within the bucket via use of the 'username' Policy variable.
B. Create a single S3 bucket with Reduced Redundancy Storage turned on and ask their customers to use an S3 client instead of an FTP client Create a bucket for each customer with a Bucket Policy that permits access only to that one customer.
C. Create an auto-scaling group of FTP servers with a scaling policy to automatically scale-in when minimum network traffic on the auto-scaling group is below a given threshold. Load a central list of ftp users from S3 as part of the user Data startup script on each Instance.
D. Create a single S3 bucket with Requester Pays turned on and ask their customers to use an S3 client instead of an FTP client Create a bucket tor each customer with a Bucket Policy that permits access only to that one customer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In question we have keywords `scalable' and company wants to `move systems' to AWS, which is best suited for Auto-scaling group.

https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/

QUESTION 12
Amazon EC2 provides virtual computing environments known as _____.

A. instances
B. volumes
C. microsystems
D. servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 13
You would like to create a mirror image of your production environment in another region for disaster recovery purposes. Which of the following AWS resources do not need to be recreated in the second region? (Choose two.)

A. Route 53 Record Sets
B. IM1 Roles
C. Elastic IP Addresses (EIP)
D. EC2 Key Pairs
E. Launch configurations
F. Security Groups

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Route 53 and IAM are global.

As per the document defined, new IPs should be reserved not the same ones. Elastic IP Addresses are static IP addresses designed for dynamic cloud computing. Unlike traditional static IP addresses, however, Elastic IP addresses enable you to mask instance or Availability Zone failures by programmatically remapping your public IP addresses to instances in your account in a particular region. For DR, you can also pre-allocate some IP addresses for the most critical systems so that their IP addresses are already known before disaster strikes. This can simplify the execution of the DR plan.
Reference:
http://ltech.com/wp-content/themes/optimize/download/AWS_Disaster_Recovery.pdf (page 6)

QUESTION 14
Your company runs a customer facing event registration site This site is built with a 3-tier architecture with web and application tier servers and a MySQL database The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database. When deploying this application in a region with three availability zones (AZs) which architecture provides high availability?

A. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 2 AZs with 3 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB, and one RDS (Relational Database Service) instance deployed with read replicas in the other AZ.
B. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB and one RDS (Relational Database Service) Instance deployed with read replicas in the two other AZs.
C. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 2 AZs with 3 EC2 instances m each AZ inside an Auto Scaling Group behind an ELS and a Multi-AZ RDS (Relational Database Service) deployment.
D. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ Inside an Auto Scaling Group behind an ELB (elastic load balancer). And an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB. And a Multi-AZ RDS (Relational Database services) deployment.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS Multi-AZ Deployments
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. In case of an infrastructure failure (for example, instance hardware failure, storage failure, or network disruption), Amazon RDS performs an automatic failover to the standby, so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.
Enhanced Durability
Multi-AZ deployments for the MySQL, Oracle, and PostgreSQL engines utilize synchronous physical replication to keep data on the standby up-to-date with the primary. Multi-AZ deployments for the SQL Server engine use synchronous logical replication to achieve the same result, employing SQL Server-native Mirroring technology. Both approaches safeguard your data in the event of a DB Instance failure or loss of an Availability Zone.
If a storage volume on your primary fails in a Multi-AZ deployment, Amazon RDS automatically initiates a failover to the up-to-date standby. Compare this to a Single-AZ deployment: in case of a Single-AZ database failure, a user-initiated point-in-time-restore operation will be required. This operation can take several hours to complete, and any data updates that occurred after the latest restorable time (typically within the last five minutes) will not be available.
Amazon Aurora employs a highly durable, SSD-backed virtualized storage layer purpose-built for database workloads. Amazon Aurora automatically replicates your volume six ways, across three Availability Zones. Amazon Aurora storage is fault-tolerant, transparently handling the loss of up to two copies of data without affecting database write availability and up to three copies without affecting read availability. Amazon Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and replaced automatically.
Increased Availability
You also benefit from enhanced database availability when running Multi-AZ deployments. If an Availability Zone failure or DB Instance failure occurs, your availability impact is limited to the time automatic failover takes to complete: typically under one minute for Amazon Aurora and one to two minutes for other database engines (see the RDS FAQ for details).
The availability benefits of Multi-AZ deployments also extend to planned maintenance and backups. In the case of system upgrades like OS patching or DB Instance scaling, these operations are applied first on the standby, prior to the automatic failover. As a result, your availability impact is, again, only the time required for automatic failover to complete.
Unlike Single-AZ deployments, I/O activity is not suspended on your primary during backup for Multi-AZ deployments for the MySQL, Oracle, and PostgreSQL engines, because the backup is taken from the standby. However, note that you may still experience elevated latencies for a few minutes during backups for Multi-AZ deployments.
On instance failure in Amazon Aurora deployments, Amazon RDS uses RDS Multi-AZ technology to automate failover to one of up to 15 Amazon Aurora Replicas you have created in any of three Availability Zones. If no Amazon Aurora Replicas have been provisioned, in the case of a failure, Amazon RDS will attempt to create a new Amazon Aurora DB instance for you automatically.

https://www.airpair.com/aws/posts/building-a-scalable-web-app-on-amazon-web-services-p1

QUESTION 15
Your application is using an ELB in front of an Auto Scaling group of web/application servers deployed across two AZs and a Multi-AZ RDS Instance for data persistence. The database CPU is often above 80% usage and 90% of I/O operations on the database are reads. To improve performance you recently added a single-node Memcached ElastiCache Cluster to cache frequent DB query results. In the next weeks the overall workload is expected to grow by 30%.
Do you need to change anything in the architecture to maintain the high availability or the application with the anticipated additional load? Why?

A. Yes, you should deploy two Memcached ElastiCache Clusters in different AZs because the RDS instance will not be able to handle the load if the cache node fails.
B. No, if the cache node fails you can always get the same data from the DB withouthaving any availability impact.
C. No, if the cache node fails the automated ElastiCache node recovery feature will prevent any availability impact.
D. Yes, you should deploy the Memcached ElastiCache Cluster with two nodes in the same AZ as the RDS DB master instance to handle the load if one cache node fails.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A single-node Memcached ElastiCache cluster failure is nothing but a total failure. (Even though
AWS will automatically recover the failed node, there are no other nodes in the cluster)
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/BestPractices.html
Mitigating Node Failures
To mitigate the impact of a node failure, spread your cached data over more nodes. Because Memcached does not support replication, a node failure will always result in some data loss from
your cluster.
When you create your Memcached cluster you can create it with 1 to 20 nodes, or more by special request. Partitioning your data across a greater number of nodes means you'll lose less data if a node fails. For example, if you partition your data across 10 nodes, any single node stores approximately 10% of your cached data. In this case, a node failure loses approximately 10% of your cache which needs to be replaced when a replacement node is created and provisioned.
Mitigating Availability Zone Failures
To mitigate the impact of an availability zone failure, locate your nodes in as many availability zones as possible. In the unlikely event of an AZ failure, you will lose only the data cached in that AZ, not the data cached in the other AZs.

QUESTION 16
You are responsible for a legacy web application whose server environment is approaching end of life You would like to migrate this application to AWS as quickly as possible, since the application environment currently has the following limitations:
The VM's single 10GB VMDK is almost full
Me virtual network interface still uses the 10Mbps driver, which leaves your 100Mbps WAN connection completely underutilized
It is currently running on a highly customized. Windows VM within a VMware environment:
You do not have me installation media
This is a mission critical application with an RTO (Recovery Time Objective) of 8 hours. RPO (Recovery Point Objective) of 1 hour. How could you best migrate this application to AWS while meeting your business continuity requirements?

A. Use the EC2 VM Import Connector for vCenter to import the VM into EC2.
B. Use Import/Export to import the VM as an ESS snapshot and attach to EC2.
C. Use S3 to create a backup of the VM and restore the data into EC2.
D. Use me ec2-bundle-instance API to Import an Image of the VM into EC2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/developertools/2759763385083070

QUESTION 17
An International company has deployed a multi-tier web application that relies on DynamoDB in a single region. For regulatory reasons they need disaster recovery capability In a separate region with a Recovery Time Objective of 2 hours and a Recovery Point Objective of 24 hours They should synchronize their data on a regular basis and be able to provision me web application rapidly using CloudFormation.

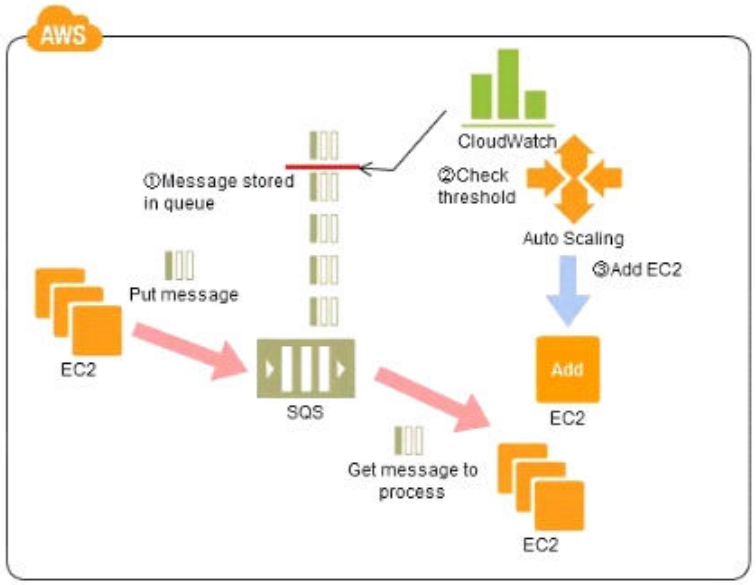
The objective is to minimize changes to the existing web application, control the throughput of DynamoDB used for the synchronization of data and synchronize only the modified elements.
Which design would you choose to meet these requirements?

A. Use AWS data Pipeline to schedule a DynamoDB cross region copy once a day. create a Lastupdated' attribute in your DynamoDB table that would represent the timestamp of the last update and use it as a filter.
B. Use EMR and write a custom script to retrieve data from DynamoDB in the current region using a SCAN operation and push it to DynamoDB in the second region.
C. Use AWS data Pipeline to schedule an export of the DynamoDB table to S3 in the current region once a day then schedule another task immediately after it that will import data from S3 to DynamoDB in the other region.
D. Send also each Ante into an SQS queue in me second region; use an auto-scaling group behind the SQS queue to replay the write in the second region.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/blogs/aws/copy-dynamodb-data-between-regions-using-the-aws-data-pipeline/

QUESTION 18



Refer to the architecture diagram above of a batch processing solution using Simple Queue Service (SQS) to set up a message queue between EC2 instances which are used as batch processors Cloud Watch monitors the number of Job requests (queued messages) and an Auto Scaling group adds or deletes batch servers automatically based on parameters set in Cloud Watch alarms. You can use this architecture to implement which of the following features in a cost effective and efficient manner?

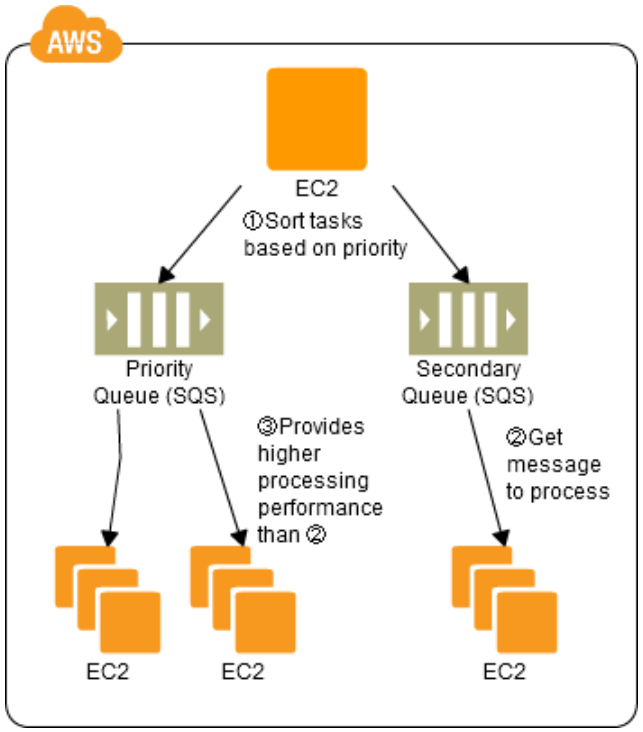
A. Reduce the overall lime for executing jobs through parallel processing by allowing a busy EC2 instance that receives a message to pass it to the next instance in a daisy-chain setup.

B. Implement fault tolerance against EC2 instance failure since messages would remain in SQS and worn can continue with recovery of EC2 instances implement fault tolerance against SQS failure by backing up messages to S3.
C. Implement message passing between EC2 instances within a batch by exchanging messages through SQS.
D. Coordinate number of EC2 instances with number of job requests automatically thus Improving cost effectiveness.
E. Handle high priority jobs before lower priority jobs by assigning a priority metadata field to SQS messages.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

There are cases where a large number of batch jobs may need processing, and where the the jobs may need to be re-prioritized.
For example, one such case is one where there are differences between different levels of services for unpaid users versus subscriber users (such as the time until publication) in services enabling, for example, presentation files to be uploaded for publication from a web browser. When the user uploads a presentation file, the conversion processes, for example, for publication are performed as batch processes on the system side, and the file is published after the conversion. Is it then necessary to be able to assign the level of priority to the batch processes for each type of subscriber.
Explanation of the Cloud Solution/Pattern
A queue is used in controlling batch jobs. The queue need only be provided with priority numbers. Job requests are controlled by the queue, and the job requests in the queue are processed by a batch server. In Cloud computing, a highly reliable queue is provided as a service, which you can use to structure a highly reliable batch system with ease. You may prepare multiple queues depending on priority levels, with job requests put into the queues depending on their priority levels, to apply prioritization to batch processes. The performance (number) of batch servers corresponding to a queue must be in accordance with the priority level thereof.
Implementation
In AWS, the queue service is the Simple Queue Service (SQS). Multiple SQS queues may be prepared to prepare queues for individual priority levels (with a priority queue and a secondary queue). Moreover, you may also use the message Delayed Send function to delay process execution.
Use SQS to prepare multiple queues for the individual priority levels.
Place those processes to be executed immediately (job requests) in the high priority queue.
Prepare numbers of batch servers, for processing the job requests of the queues, depending on the priority levels.
Queues have a message "Delayed Send" function. You can use this to delay the time for starting a process.
Configuration



Benefits

You can increase or decrease the number of servers for processing jobs to change automatically the processing speeds of the priority queues and secondary queues.
You can handle performance and service requirements through merely increasing or decreasing the number of EC2 instances used in job processing.
Even if an EC2 were to fail, the messages (jobs) would remain in the queue service, enabling processing to be continued immediately upon recovery of the EC2 instance, producing a system that is robust to failure.

Cautions

Depending on the balance between the number of EC2 instances for performing the processes and the number of messages that are queued, there may be cases where processing in the secondary queue may be completed first, so you need to monitor the processing speeds in the primary queue and the secondary queue.

QUESTION 19

Your company currently has a 2-tier web application running in an on-premises data center. You have experienced several infrastructure failures in the past two months resulting in significant financial losses. Your CIO is strongly agreeing to move the application to AWS. While working on achieving buy-in from the other company executives, he asks you to develop a disaster recovery plan to help improve Business continuity in the short term. He specifies a target Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour or less. He also asks you to implement the solution within 2 weeks. Your database is 200GB in size and you have a 20Mbps Internet connection. How would you do this while minimizing costs?

A. Create an EBS backed private AMI which includes a fresh install of your application. Develop a CloudFormation template which includes your AMI and the required EC2, AutoScaling, and ELB resources to support deploying the application across Multiple- Availability-Zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection.
B. Deploy your application on EC2 instances within an Auto Scaling group across multiple availability zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection.
C. Create an EBS backed private AMI which includes a fresh install of your application. Setup a script in your data center to backup the local database every 1 hour and

to encrypt and copy the resulting file to an S3 bucket using multi-part upload.

D. Install your application on a compute-optimized EC2 instance capable of supporting the application's average load. Synchronously replicate transactions from your on-premises database to a database instance in AWS across a secure Direct Connect connection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Overview of Creating Amazon EBS-Backed AMIs
First, launch an instance from an AMI that's similar to the AMI that you'd like to create. You can connect to your instance and customize it. When the instance is configured correctly, ensure data integrity by stopping the instance before you create an AMI, then create the image. When you create an Amazon EBS-backed AMI, we automatically register it for you.
Amazon EC2 powers down the instance before creating the AMI to ensure that everything on the instance is stopped and in a consistent state during the creation process. If you're confident that your instance is in a consistent state appropriate for AMI creation, you can tell Amazon EC2 not to power down and reboot the instance. Some file systems, such as XFS, can freeze and unfreeze activity, making it safe to create the image without rebooting the instance.
During the AMI-creation process, Amazon EC2 creates snapshots of your instance's root volume and any other EBS volumes attached to your instance. If any volumes attached to the instance are encrypted, the new AMI only launches successfully on instances that support Amazon EBS encryption. For more information, see Amazon EBS Encryption.
Depending on the size of the volumes, it can take several minutes for the AMI-creation process to complete (sometimes up to 24 hours). You may find it more efficient to create snapshots of your volumes prior to creating your AMI. This way, only small, incremental snapshots need to be created when the AMI is created, and the process completes more quickly (the total time for snapshot creation remains the same). For more information, see Creating an Amazon EBS Snapshot.
After the process completes, you have a new AMI and snapshot created from the root volume of the instance. When you launch an instance using the new AMI, we create a new EBS volume for its root volume using the snapshot. Both the AMI and the snapshot incur charges to your account until you delete them. For more information, see Deregistering Your AMI.
If you add instance-store volumes or EBS volumes to your instance in addition to the root device volume, the block device mapping for the new AMI contains information for these volumes, and the block device mappings for instances that you launch from the new AMI automatically contain information for these volumes. The instance-store volumes specified in the block device mapping for the new instance are new and don't contain any data from the instance store volumes of the instance you used to create the AMI. The data on EBS volumes persists. For more information, see Block Device Mapping.

QUESTION 20
An ERP application is deployed across multiple AZs in a single region. In the event of failure, the Recovery Time Objective (RTO) must be less than 3 hours, and the Recovery Point Objective (RPO) must be 15 minutes the customer realizes that data corruption occurred roughly 1.5 hours ago.
What DR strategy could be used to achieve this RTO and RPO in the event of this kind of failure?

A. Take hourly DB backups to S3, with transaction logs stored in S3 every 5 minutes.
B. Use synchronous database master-slave replication between two availability zones.
C. Take hourly DB backups to EC2 Instance store volumes with transaction logs stored In S3 every 5 minutes.
D. Take 15 minute DB backups stored In Glacier with transaction logs stored in S3 every 5 minutes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Your startup wants to implement an order fulfillment process for selling a personalized gadget that needs an average of 3-4 days to produce with some orders taking up to 6 months you expect 10 orders per day on your first day. 1000 orders per day after 6 months and 10,000 orders after 12 months.
Orders coming in are checked for consistency men dispatched to your manufacturing plant for production quality control packaging shipment and payment processing If the product does not meet the quality standards at any stage of the process employees may force the process to repeat a step Customers are notified via email about order status and any critical issues with their orders such as payment failure.
Your case architecture includes AWS Elastic Beanstalk for your website with an RDS MySQL instance for customer data and orders.
How can you implement the order fulfillment process while making sure that the emails are delivered reliably?

A. Add a business process management application to your Elastic Beanstalk app servers and re-use the ROS database for tracking order status use one of the Elastic Beanstalk instances to send emails to customers.
B. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1 Use the decider instance to send emails to customers.
C. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1 use SES to send emails to customers.
D. Use an SQS queue to manage all process tasks Use an Auto Scaling group of EC2 Instances that poll the tasks and execute them. Use SES to send emails to customers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ecommerce_checkout_13.pdf

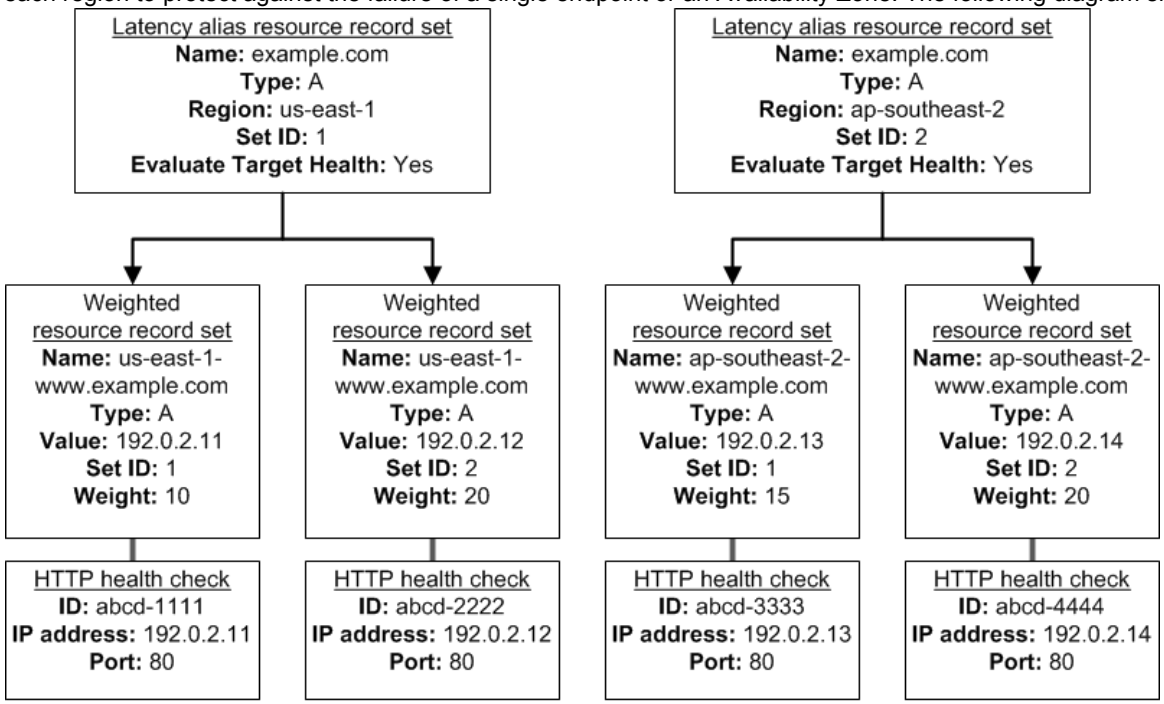
QUESTION 22
You have deployed a web application targeting a global audience across multiple AWS Regions under the domain name.example.com. You decide to use Route53 Latency-Based Routing to serve web requests to users from the region closest to the user. To provide business continuity in the event of server downtime you configure weighted record sets associated with two web servers in separate Availability Zones per region. Running a DR test you notice that when you disable all web servers in one of the regions Route53 does not automatically direct all users to the other region. What could be happening? (Choose two.)

A. Latency resource record sets cannot be used in combination with weighted resource record sets.
B. You did not setup an HTTP health check tor one or more of the weighted resource record sets associated with me disabled web servers.
C. The value of the weight associated with the latency alias resource record set in the region with the disabled servers is higher than the weight for the other region.
D. One of the two working web servers in the other region did not pass its HTTP health check.
E. You did not set "Evaluate Target Health" to "Yes" on the latency alias resource record set associated with example com in the region where you disabled the servers.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
How Health Checks Work in Complex Amazon Route 53 Configurations
Checking the health of resources in complex configurations works much the same way as in simple configurations. However, in complex configurations, you use a combination of alias resource record sets (including weighted alias, latency alias, and failover alias) and nonalias resource record sets to build a decision tree that gives you greater control over how Amazon Route 53 responds to requests. For more information, see How Health Checks Work in Simple Amazon Route 53 Configurations.

For example, you might use latency alias resource record sets to select a region close to a user and use weighted resource record sets for two or more resources within each region to protect against the failure of a single endpoint or an Availability Zone. The following diagram shows this configuration.



Here's how Amazon EC2 and Amazon Route 53 are configured:

You have Amazon EC2 instances in two regions, us-east-1 and ap-southeast-2. You want Amazon Route 53 to respond to queries by using the resource record sets in the region that provides the lowest latency for your customers, so you create a latency alias resource record set for each region. (You create the latency alias resource record sets after you create resource record sets for the individual Amazon EC2 instances.)

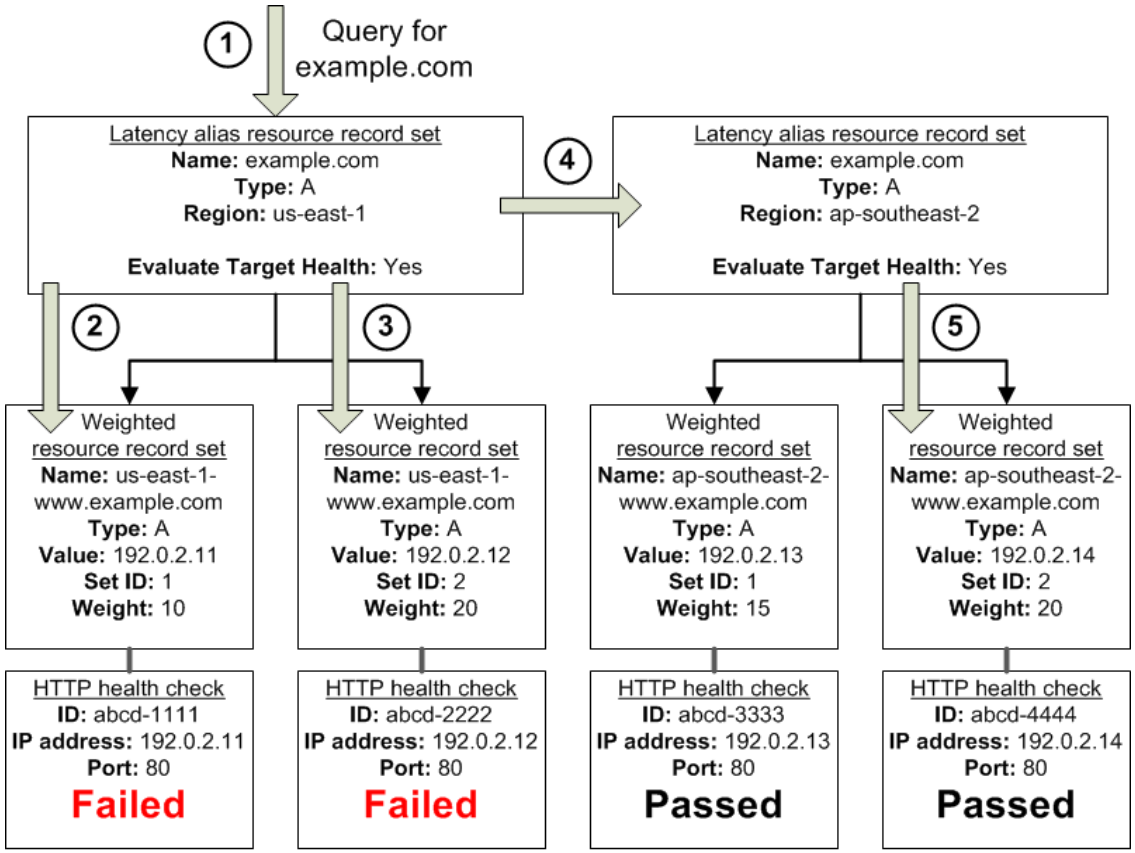
Within each region, you have two Amazon EC2 instances. You create a weighted resource record set for each instance. The name and the type are the same for both of the weighted resource record sets in each region.

When you have multiple resources in a region, you can create weighted or failover resource record sets for your resources. You can also create even more complex configurations by creating weighted alias or failover alias resource record sets that, in turn, refer to multiple resources.

Each weighted resource record set has an associated health check. The IP address for each health check matches the IP address for the corresponding resource record set. This isn't required, but it's the most common configuration.

For both latency alias resource record sets, you set the value of Evaluate Target Health to Yes.

You use the Evaluate Target Health setting for each latency alias resource record set to make Amazon Route 53 evaluate the health of the alias targets—the weighted resource record sets—and respond accordingly.



The preceding diagram illustrates the following sequence of events:

Amazon Route 53 receives a query for example.com. Based on the latency for the user making the request, Amazon Route 53 selects the latency alias resource record set for the us-east-1 region.

Amazon Route 53 selects a weighted resource record set based on weight. Evaluate Target Health is Yes for the latency alias resource record set, so Amazon Route 53 checks the health of the selected weighted resource record set.

The health check failed, so Amazon Route 53 chooses another weighted resource record set based on weight and checks its health. That resource record set also is unhealthy.

Amazon Route 53 backs out of that branch of the tree, looks for the latency alias resource record set with the next-best latency, and chooses the resource record set for ap-southeast-2.

Amazon Route 53 again selects a resource record set based on weight, and then checks the health of the selected resource record set. The health check passed, so Amazon Route 53 returns the applicable value in response to the query.

What Happens When You Associate a Health Check with an Alias Resource Record Set?

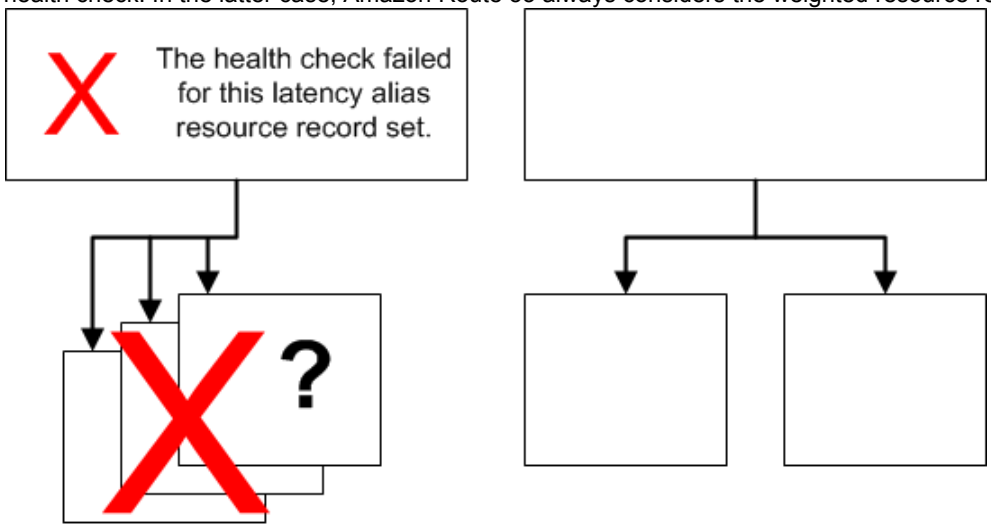
You can associate a health check with an alias resource record set instead of or in addition to setting the value of Evaluate Target Health to Yes. However, it's generally more useful if Amazon Route 53 responds to queries based on the health of the underlying resources—the HTTP servers, database servers, and other resources that your alias resource record sets refer to. For example, suppose the following configuration:

You assign a health check to a latency alias resource record set for which the alias target is a group of weighted resource record sets.

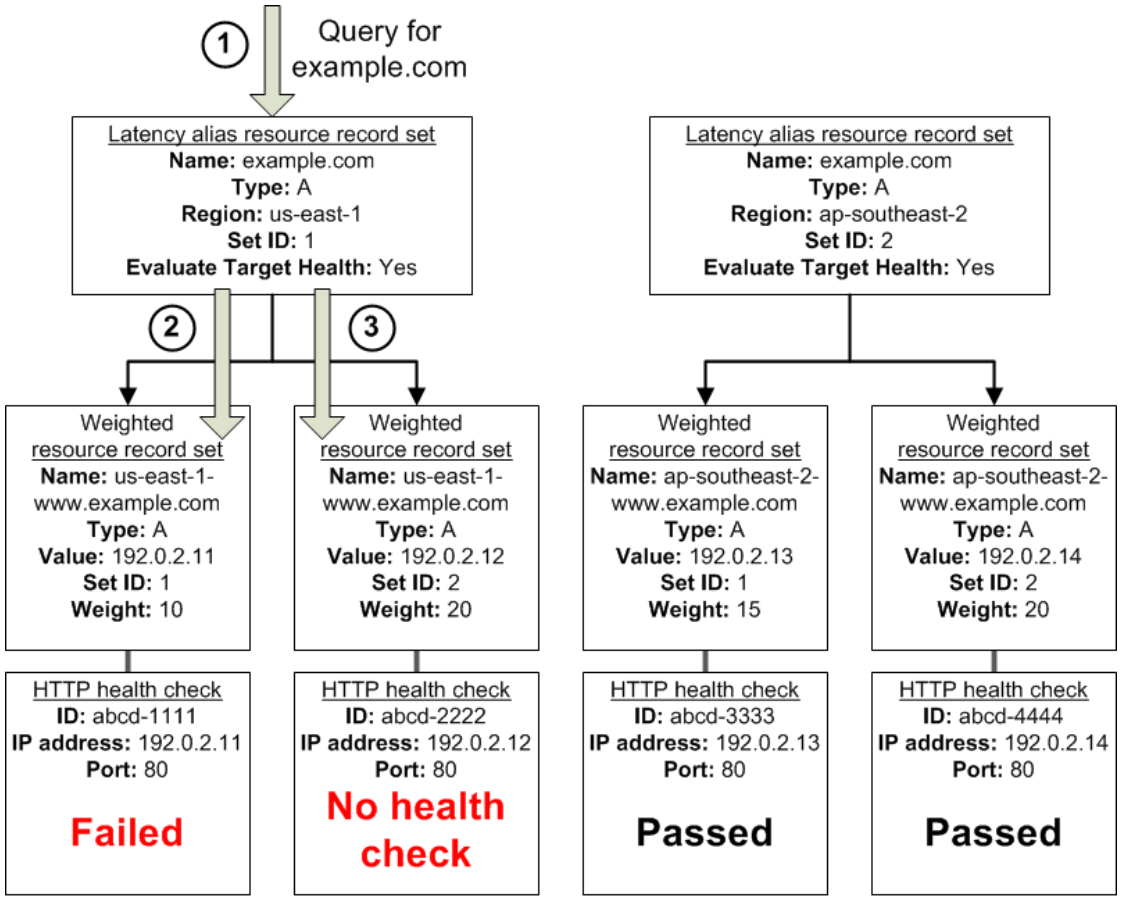
You set the value of Evaluate Target Health to Yes for the latency alias resource record set.

In this configuration, both of the following must be true before Amazon Route 53 will return the applicable value for a weighted resource record set:

The health check associated with the latency alias resource record set must pass.
At least one weighted resource record set must be considered healthy, either because it's associated with a health check that passes or because it's not associated with a health check. In the latter case, Amazon Route 53 always considers the weighted resource record set healthy.



If the health check for the latency alias resource record set fails, Amazon Route 53 stops responding to queries using any of the weighted resource record sets in the alias target, even if they're all healthy. Amazon Route 53 doesn't know the status of the weighted resource record sets because it never looks past the failed health check on the alias resource record set.
What Happens When You Omit Health Checks?
In a complex configuration, it's important to associate health checks with all of the non-alias resource record sets. Let's return to the preceding example, but assume that a health check is missing on one of the weighted resource record sets in the us-east-1 region:



Here's what happens when you omit a health check on a non-alias resource record set in this configuration:

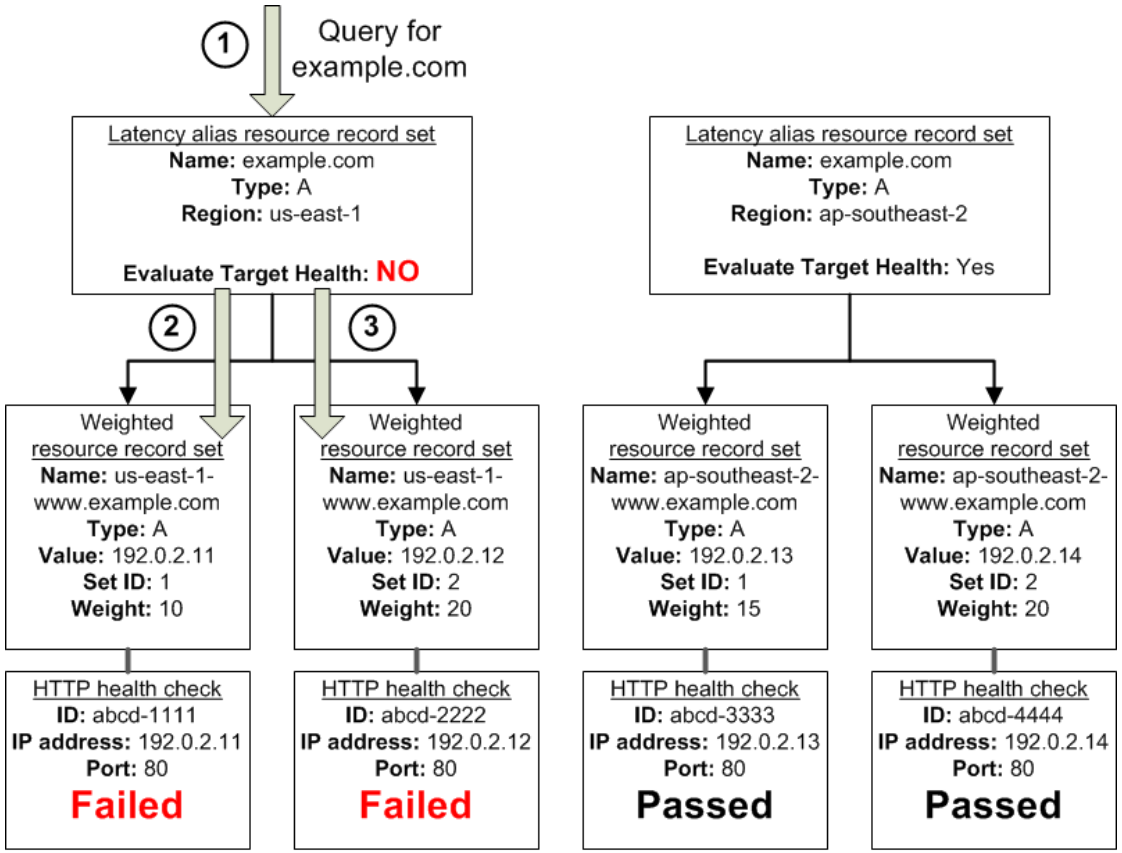
Amazon Route 53 receives a query for example.com. Based on the latency for the user making the request, Amazon Route 53 selects the latency alias resource record set for the us-east-1 region.

Amazon Route 53 looks up the alias target for the latency alias resource record set, and checks the status of the corresponding health checks. The health check for one weighted resource record set failed, so that resource record set is omitted from consideration.

The other weighted resource record set in the alias target for the us-east-1 region has no health check. The corresponding resource might or might not be healthy, but without a health check, Amazon Route 53 has no way to know. Amazon Route 53 assumes that the resource is healthy and returns the applicable value in response to the query.

What Happens When You Set Evaluate Target Health to No?

In general, you also want to set Evaluate Target Health to Yes for all of the alias resource record sets. In the following example, all of the weighted resource record sets have associated health checks, but Evaluate Target Health is set to No for the latency alias resource record set for the us-east-1 region:



Here's what happens when you set Evaluate Target Health to No for an alias resource record set in this configuration:
Amazon Route 53 receives a query for example.com. Based on the latency for the user making the request, Amazon Route 53 selects the latency alias resource record set for the us-east-1 region.
Amazon Route 53 determines what the alias target is for the latency alias resource record set, and checks the corresponding health checks. They're both failing.
Because the value of Evaluate Target Health is No for the latency alias resource record set for the us-east-1 region, Amazon Route 53 must choose one resource record set in this branch instead of backing out of the branch and looking for a healthy resource record set in the ap-southeast-2 region.

QUESTION 23
Your company hosts a social media site supporting users in multiple countries. You have been asked to provide a highly available design tor the application that leverages multiple regions tor the most recently accessed content and latency sensitive portions of the wet) site The most latency sensitive component of the application involves reading user preferences to support web site personalization and ad selection.
In addition to running your application in multiple regions, which option will support this application's requirements?

A. Serve user content from S3. CloudFront and use Route53 latency-based routing between ELBs in each region Retrieve user preferences from a local DynamoDB table in each region and leverage SQS to capture changes to user preferences with SOS workers for propagating updates to each table.
B. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3. CloudFront with dynamic content and an ELB in each region Retrieve user preferences from an ElasticCache cluster in each region and leverage SNS notifications to propagate user preference changes to a worker node

in each region.

C. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3 CloudFront and Route53 latency-based routing Between ELBs In each region Retrieve user preferences from a DynamoDB table and leverage SQS to capture changes to user preferences with SOS workers for propagating DynamoDB updates.

D. Serve user content from S3. CloudFront with dynamic content, and an ELB in each region Retrieve user preferences from an ElastiCache cluster in each region and leverage Simple Workflow (SWF) to manage the propagation of user preferences from a centralized OB to each ElastiCache cluster.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_mediasharing_09.pdf http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_adserving_06.pdf

QUESTION 24
Your system recently experienced down time during the troubleshooting process. You found that a new administrator mistakenly terminated several production EC2 instances.
Which of the following strategies will help prevent a similar situation in the future?
The administrator still must be able to:
- launch, start stop, and terminate development resources.
- launch and start production instances.

A. Create an IAM user, which is not allowed to terminate instances by leveraging production EC2 termination protection.

B. Leverage resource based tagging along with an IAM user, which can prevent specific users from terminating production EC2 resources.

C. Leverage EC2 termination protection and multi-factor authentication, which together require users to authenticate before terminating EC2 instances

D. Create an IAM user and apply an IAM role which prevents users from terminating production EC2 instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Working with volumes
When an API action requires a caller to specify multiple resources, you must create a policy statement that allows users to access all required resources. If you need to use a Condition element with one or more of these resources, you must create multiple statements as shown in this example.
The following policy allows users to attach volumes with the tag "volume_user=iam-user-name" to instances with the tag "department=dev", and to detach those volumes from those instances. If you attach this policy to an IAM group, the aws:username policy variable gives each IAM user in the group permission to attach or detach volumes from the instances with a tag named volume_user that has his or her IAM user name as a value.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/department": "dev"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/volume_user": "${aws:username}"
      }
    }
  }
 ]
}
```

Launching instances (RunInstances)

The RunInstances API action launches one or more instances. RunInstances requires an AMI and creates an instance; and users can specify a key pair and security group in the request. Launching into EC2-VPC requires a subnet, and creates a network interface. Launching from an Amazon EBS-backed AMI creates a volume. Therefore, the user must have permission to use these Amazon EC2 resources. The caller can also configure the instance using optional parameters to RunInstances, such as the instance type and a subnet. You can create a policy statement that requires users to specify an optional parameter, or restricts users to particular values for a parameter. The examples in this section demonstrate some of the many possible ways that you can control the configuration of an instance that a user can launch.

Note that by default, users don't have permission to describe, start, stop, or terminate the resulting instances. One way to grant the users permission to manage the resulting instances is to create a specific tag for each instance, and then create a statement that enables them to manage instances with that tag. For more information, see 2: Working with instances.

a. AMI

The following policy allows users to launch instances using only the AMIs that have the specified tag, "department=dev", associated with them. The users can't launch instances using other AMIs because the Condition element of the first statement requires that users specify an AMI that has this tag. The users also can't launch into a

subnet, as the policy does not grant permissions for the subnet and network interface resources. They can, however, launch into EC2-Classic. The second statement uses a wildcard to enable users to create instance resources, and requires users to specify the key pair project_keypair and the security group sg-1a2b3c4d. Users are still able to launch instances without a key pair.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/department": "dev"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/project_keypair",
      "arn:aws:ec2:region:account:security-group/sg-1a2b3c4d"
    ]
  }
 ]
}
```

Alternatively, the following policy allows users to launch instances using only the specified AMIs, ami-9e1670f7 and ami-45cf5c3c. The users can't launch an instance using other AMIs (unless another statement grants the users permission to do so), and the users can't launch an instance into a subnet.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-9e1670f7",
      "arn:aws:ec2:region::image/ami-45cf5c3c",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
    ]
   }
  ]
}
```

Alternatively, the following policy allows users to launch instances from all AMIs owned by Amazon. The Condition element of the first statement tests whether ec2:Owner is amazon. The users can't launch an instance using other AMIs (unless another statement grants the users permission to do so). The users are able to launch an instance into a subnet.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:Owner": "amazon"
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

b. Instance type

The following policy allows users to launch instances using only the t2.micro or t2.small instance type, which you might do to control costs. The users can't launch larger instances because the Condition element of the first statement tests whether ec2:InstanceType is either t2.micro or t2.small.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:InstanceType": ["t2.micro", "t2.small"]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

Alternatively, you can create a policy that denies users permission to launch any instances except t2.micro and t2.small instance types.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "ec2:InstanceType": ["t2.micro", "t2.small"]
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

c. Subnet

The following policy allows users to launch instances using only the specified subnet, subnet-12345678. The group can't launch instances into any another subnet (unless another statement grants the users permission to do so). Users are still able to launch instances into EC2-Classic.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:subnet/subnet-12345678",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
    ]
  }
  ]
}
```

Alternatively, you could create a policy that denies users permission to launch an instance into any other subnet. The statement does this by denying permission to create a network interface, except where subnet subnet-12345678 is specified. This denial overrides any other policies that are created to allow launching instances into other subnets. Users are still able to launch instances into EC2-Classic.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:network-interface/*"
    ],
    "Condition": {
      "ArnNotEquals": {
        "ec2:Subnet": "arn:aws:ec2:region:account:subnet/subnet-12345678
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

https://aws.amazon.com/blogs/security/resource-level-permissions-for-ec2-controlling-management-access-on-specific-instances/
August 2016 Update One way to work around this is to use a combination of an Amazon CloudWatch Events rule and AWS Lambda to **tag** newly created instances.

QUESTION 25
A customer has established an AWS Direct Connect connection to AWS. The link is up and routes are being advertised from the customer's end, however the customer is unable to connect from EC2 instances inside its VPC to servers residing in its datacenter.
Which of the following options provide a viable solution to remedy this situation? (Choose two.)

A. Add a route to the route table with an iPsec VPN connection as the target.
B. Enable route propagation to the virtual pinnate gateway (VGW).
C. Enable route propagation to the customer gateway (CGW).
D. Modify the route table of all Instances using the 'route' command.
E. Modify the Instances VPC subnet route table by adding a route back to the customer's on-premises environment.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://myawsscribble.wordpress.com/2015/09/25/setting-up-and-configuring-aws-directconnect/

QUESTION 26
Your company previously configured a heavily used, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and would like to start using the new connection. After configuring DirectConnect settings in the AWS Console, which of the following options win provide the most seamless transition for your users?

A. Delete your existing VPN connection to avoid routing loops configure your DirectConnect router with the appropriate settings and verity network traffic is leveraging DirectConnect.
B. Configure your DirectConnect router with a higher 8GP priority man your VPN router, verify network traffic is leveraging Directconnect and then delete your existing VPN connection.
C. Update your VPC route tables to point to the DirectConnect connection configure your DirectConnect router with the appropriate settings verify network traffic is leveraging DirectConnect and then delete the VPN connection.
D. Configure your DirectConnect router, update your VPC route tables to point to the DirectConnect connection, configure your VPN connection with a higher BGP pointy. And verify network traffic is leveraging the DirectConnect connection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Explanation:
Q. Can I use AWS Direct Connect and a VPN Connection to the same VPC simultaneously?
Yes. However, only in fail-over scenarios. The Direct Connect path will always be preferred, when established, regardless of AS path prepending.
https://aws.amazon.com/directconnect/faqs/

QUESTION 27
A web company is looking to implement an external payment service into their highly available application deployed in a VPC Their application EC2 instances are behind a public lacing ELB Auto scaling is used to add additional instances as traffic increases under normal load the application runs 2 instances in the Auto Scaling group but at peak it can scale 3x in size. The application instances need to communicate with the payment service over the Internet which requires whitelisting of all public IP addresses used to communicate with it. A maximum of 4 whitelisting IP addresses are allowed at a time and can be added through an API.
How should they architect their solution?

A. Route payment requests through two NAT instances setup for High Availability and whitelist the Elastic IP addresses attached to the MAT instances.
B. Whitelist the VPC Internet Gateway Public IP and route payment requests through the Internet Gateway.
C. Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB.
D. Automatically assign public IP addresses to the application instances in the Auto Scaling group and run a script on boot that adds each instances public IP address to the payment validation whitelist API.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B is incorrect as you do not have insight into the public ip associated with a VPC Internet Gateways.
C is incorrect as ELB receives a public DNS name.
D would exceed the maximum of 4 whitelisting IP addresses.

QUESTION 28
You are designing the network infrastructure for an application server in Amazon VPC Users will access all the application instances from the Internet as well as from an on-premises network The on-premises network is connected to your VPC over an AWS Direct Connect link.
How would you design routing to meet the above requirements?

A. Configure a single routing Table with a default route via the Internet gateway Propagate a default route via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets.
B. Configure a single routing table with a default route via the internet gateway Propagate specific routes for the on-premises networks via BGP on the AWS Direct Connect customer router Associate the routing table with all VPC subnets.
C. Configure a single routing table with two default routes: one to the internet via an Internet gateway the other to the on-premises network via the VPN gateway use this routing table across all subnets in your VPC,
D. Configure two routing tables one that has a default route via the Internet gateway and another that has a default route via the VPN gateway Associate both routing tables with each VPC subnet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
You are implementing AWS Direct Connect. You intend to use AWS public service end points such as Amazon S3, across the AWS Direct Connect link. You want other Internet traffic to use your existing link to an Internet Service Provider.
What is the correct way to configure AWS Direct connect for access to services such as Amazon S3?

A. Configure a public Interface on your AWS Direct Connect link Configure a static route via your AWS Direct Connect link that points to Amazon S3 Advertise a default route to AWS using BGP.
B. Create a private interface on your AWS Direct Connect link. Configure a static route via your AWS Direct connect link that points to Amazon S3 Configure specific routes to your network in your VPC,
C. Create a public interface on your AWS Direct Connect link Redistribute BGP routes into your existing routing infrastructure advertise specific routes for your network to AWS.
D. Create a private interface on your AWS Direct connect link. Redistribute BGP routes into your existing routing infrastructure and advertise a default route to AWS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/directconnect/faqs/

QUESTION 30
You have deployed a three-tier web application in a VPC with a CIOR block of 10 0 0 0/28 You initially deploy two web servers, two application servers, two database servers and one NAT instance tor a total of seven EC2 instances The web. Application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS Web (raffle gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load unfortunately some of these new instances fail to launch.
Which of the following could De the root caused? (Choose two.)

A. AWS reserves the first and the last private IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances
B. The Internet Gateway (IGW) of your VPC has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
C. The ELB has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
D. AWS reserves one IP address in each subnet's CIDR block for Route53 so you do not have enough addresses left to launch all of the new EC2 instances
E. AWS reserves the first four and the last IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances

Correct Answer: CE
Section: (none)
Explanation

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

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block `10.0.0.0/24`, the following five IP addresses are reserved:

- `10.0.0.0`: Network address.
- `10.0.0.1`: Reserved by AWS for the VPC router.
- `10.0.0.2`: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For more information, see Amazon DNS Server.
- `10.0.0.3`: Reserved by AWS for future use.
- `10.0.0.255`: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

QUESTION 31
You've been brought in as solutions architect to assist an enterprise customer with their migration of an e-commerce platform to Amazon Virtual Private Cloud (VPC) The

previous architect has already deployed a 3-tier VPC,
The configuration is as follows:

```
VPC: vpc-2f8bc447
IGW: igw-2d8bc445
NACL: ad-208bc448
Subnets and Route Tables:
Web servers: subnet-258bc44d
Application servers: subnet-248bc44c
Database servers: subnet-9189c6f9
Route Tables:
rrb-218bc449
rtb-238bc44b
Associations:
subnet-258bc44d : rtb-218bc449
subnet-248bc44c : rtb-238bc44b
subnet-9189c6f9 : rtb-238bc44b
```

You are now ready to begin deploying EC2 instances into the VPC. Web servers must have direct access to the internet. Application and database servers cannot have direct access to the internet.
Which configuration below will allow you the ability to remotely administer your application and database servers, as well as allow these servers to retrieve updates from the Internet?

A. Create a bastion and NAT instance in subnet-258bc44d, and add a route from rtb- 238bc44b to the NAT instance.
B. Add a route from rtb-238bc44b to igw-2d8bc445 and add a bastion and NAT instance within subnet-248bc44c.
C. Create a bastion and NAT instance in subnet-248bc44c, and add a route from rtb- 238bc44b to subnet-258bc44d.
D. Create a bastion and NAT instance in subnet-258bc44d, add a route from rtb-238bc44b to Igw-2d8bc445, and a new NACL that allows access between subnet-258bc44d and subnet-248bc44c.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Create NAT instance in public subnet which is web server subnet (suDnet-258Dc44d) and add route (rtD-238Dc44D) from private subnet (database subnet-9189c6f9) to the public NAT one to
retrieve the updates.

QUESTION 32
You are designing Internet connectivity for your VPC. The Web servers must be available on the Internet. The application must have a highly available architecture.
Which alternatives should you consider? (Choose two.)

A. Configure a NAT instance in your VPC. Create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address.
B. Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your

CloudFront distribution.

C. Place all your web servers behind EL8. Configure a Route53 CNMIE to point to the ELB DNS name.
D. Assign EIPs to all web servers. Configure a Route53 record set with all EIPs with health checks and DNS failover.
E. Configure ELB with an EIP. Place all your Web servers behind ELB. Configure a Route53 A record that points to the EIP.

Correct Answer: CD
Section: (none)
Explanation

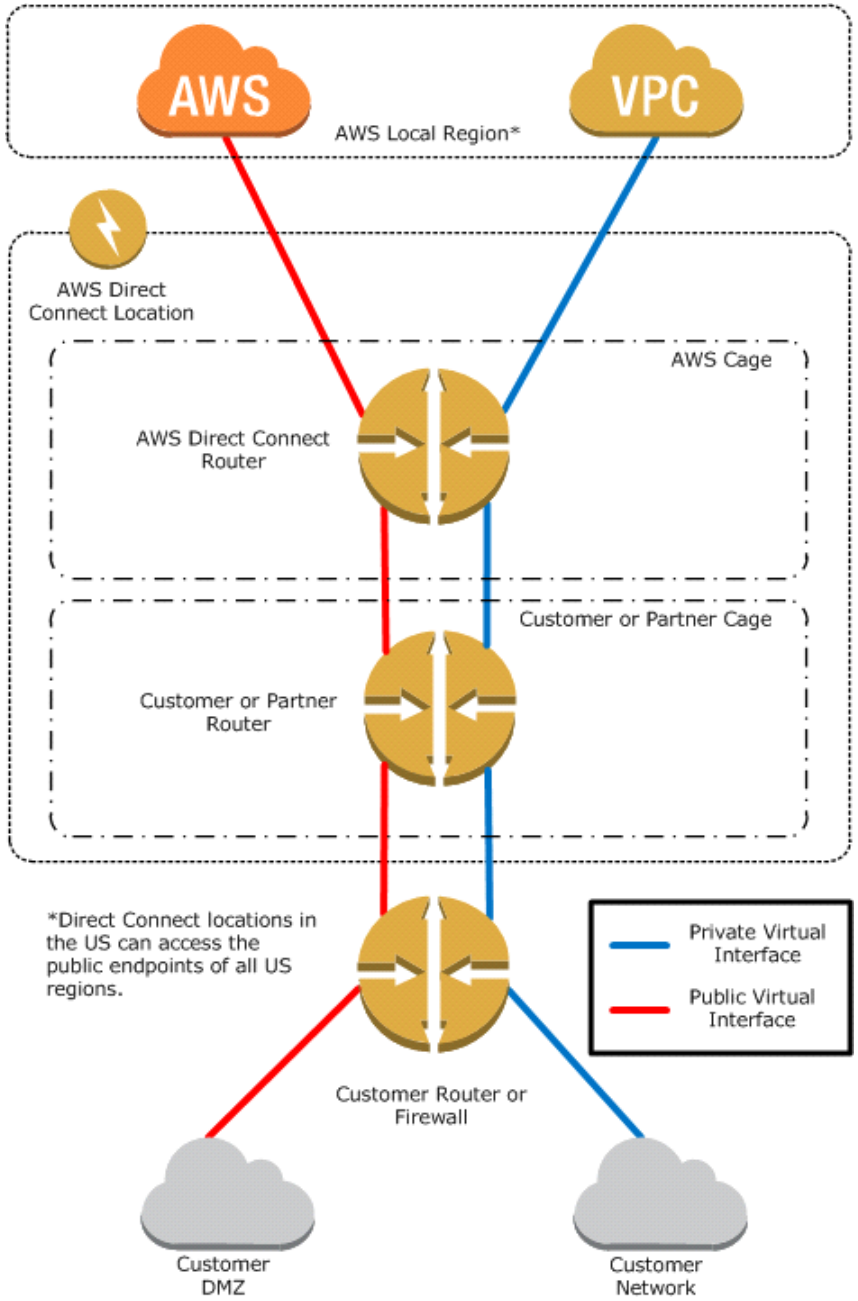
Explanation/Reference:

QUESTION 33
You are tasked with moving a legacy application from a virtual machine running Inside your datacenter to an Amazon VPC Unfortunately this app requires access to a number of on-premises services and no one who configured the app still works for your company. Even worse there's no documentation for it. What will allow the application running inside the VPC to reach back and access its internal dependencies without being reconfigured? (Choose three.)

A. An AWS Direct Connect link between the VPC and the network housing the internal services.
B. An Internet Gateway to allow a VPN connection.
C. An Elastic IP address on the VPC instance
D. An IP address space that does not conflict with the one on-premises
E. Entries in Amazon Route 53 that allow the Instance to resolve its dependencies' IP addresses
F. A VM Import of the current virtual machine

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space, while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.
What is AWS Direct Connect?
AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to the AWS cloud (for example, to Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3)) and to Amazon Virtual Private Cloud (Amazon VPC), bypassing Internet service providers in your network path. An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. For example, you can provision a single connection to any AWS Direct Connect location in the US and use it to access public AWS services in all US Regions and AWS GovCloud (US).
The following diagram shows how AWS Direct Connect interfaces with your network.



Requirements

To use AWS Direct Connect, your network must meet one of the following conditions:
Your network is colocated with an existing AWS Direct Connect location. For more information on available AWS Direct Connect locations, go to http://aws.amazon.com/directconnect/.
You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN). For a list of AWS Direct Connect partners who can help you connect, go to http://aws.amazon.com/directconnect.
You are working with an independent service provider to connect to AWS Direct Connect.
In addition, your network must meet the following conditions:
Connections to AWS Direct Connect require single mode fiber, 1000BASE-LX (1310nm) for 1 gigabit Ethernet, or 10GBASE-LR (1310nm) for 10 gigabit Ethernet. Auto Negotiation for the port must be disabled. You must support 802.1Q VLANs across these connections.
Your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication. Optionally, you may configure Bidirectional Forwarding Detection (BFD).
To connect to Amazon Virtual Private Cloud (Amazon VPC), you must first do the following:
Provide a private Autonomous System Number (ASN). Amazon allocates a private IP address in the 169.x.x.x range to you.
Create a virtual private gateway and attach it to your VPC. For more information about creating a virtual private gateway, see Adding a Hardware Virtual Private Gateway to Your VPC in the Amazon VPC User Guide.
To connect to public AWS products such as Amazon EC2 and Amazon S3, you need to provide the following:
A public ASN that you own (preferred) or a private ASN.
Public IP addresses (/31) (that is, one for each end of the BGP session) for each BGP session. If you do not have public IP addresses to assign to this connection, log on to AWS and then open a ticket with AWS Support.
The public routes that you will advertise over BGP.

QUESTION 34
You are migrating a legacy client-server application to AWS. The application responds to a specific DNS domain (e.g. www.example.com) and has a 2-tier architecture, with multiple application servers and a database server. Remote clients use TCP to connect to the application servers. The application servers need to know the IP address of the clients in order to function properly and are currently taking that information from the TCP socket. A Multi-AZ RDS MySQL instance will be used for the database.
During the migration you can change the application code, but you have to file a change request.
How would you implement the architecture on AWS in order to maximize scalability and high availability?

A. File a change request to implement Alias Resource support in the application. Use Route 53 Alias Resource Record to distribute load on two application servers in different AZs.
B. File a change request to implement Latency Based Routing support in the application. Use Route 53 with Latency Based Routing enabled to distribute load on two application servers in different AZs.
C. File a change request to implement Cross-Zone support in the application. Use an ELB with a TCP Listener and Cross-Zone Load Balancing enabled, two application servers in different AZs.
D. File a change request to implement Proxy Protocol support in the application. Use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://aws.amazon.com/blogs/aws/elastic-load-balancing-adds-support-for-proxy-protocol/

QUESTION 35
A newspaper organization has a on-premises application which allows the public to search its back catalogue and retrieve individual newspaper pages via a website written in Java They have scanned the old newspapers into JPEGs (approx 17TB) and used Optical Character Recognition (OCR) to populate a commercial search

product. The hosting platform and software are now end of life and the organization wants to migrate Its archive to AWS and produce a cost efficient architecture and still be designed for availability and durability. Which is the most appropriate?

A. Use S3 with reduced redundancy lo store and serve the scanned files, install the commercial search application on EC2 Instances and configure with auto-scaling and an Elastic Load Balancer.
B. Model the environment using CloudFormation use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the JPEGs and search index.
C. Use S3 with standard redundancy to store and serve the scanned files, use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.
D. Use a single-AZ RDS MySQL instance lo store the search index 33d the JPEG images use an EC2 instance to serve the website and translate user queries into SQL.
E. Use a CloudFront download distribution to serve the JPEGs to the end users and Install the current commercial search product, along with a Java Container Tor the website on EC2 instances and use Route53 with DNS round-robin.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There is no such thing as "Most appropriate" without knowing all your goals. I find your scenarios very fuzzy, since you can obviously mix-n-match between them. I think you should decide by layers instead:
Load Balancer Layer: ELB or just DNS, or roll-your-own. (Using DNS+EIPs is slightly cheaper, but less reliable than ELB.)
Storage Layer for 17TB of Images: This is the perfect use case for S3. Off-load all the web requests directly to the relevant JPEGs in S3. Your EC2 boxes just generate links to them.
If your app already serves it's own images (not links to images), you might start with EFS. But more than likely, you can just setup a web server to re-write or re-direct all JPEG links to S3 pretty easily.
If you use S3, don't serve directly from the bucket - Serve via a CNAME in domain you control. That way, you can switch in CloudFront easily.
EBS will be way more expensive, and you'll need 2x the drives if you need 2 boxes. Yuck.
Consider a smaller storage format. For example, JPEG200 or WebP or other tools might make for smaller images. There is also the DejaVu format from a while back.
Cache Layer: Adding CloudFront in front of S3 will help people on the other side of the world -- well, possibly. Typical archives follow a power law. The long tail of requests means that most JPEGs won't be requested enough to be in the cache. So you are only speeding up the most popular objects. You can always wait, and switch in CF later after you know your costs better. (In some cases, it can actually lower costs.)
You can also put CloudFront in front of your app, since your archive search results should be fairly static. This will also allow you to run with a smaller instance type, since CF will handle much of the load if you do it right.
Database Layer: A few options:
Use whatever your current server does for now, and replace with something else down the road. Don't under-estimate this approach, sometimes it's better to start now and optimize later.
Use RDS to run MySQL/Postgres
I'm not as familiar with ElasticSearch / Cloudsearch, but obviously Cloudsearch will be less maintenance+setup.
App Layer:
When creating the app layer from scratch, consider CloudFormation and/or OpsWorks. It's extra stuff to learn, but helps down the road.
Java+Tomcat is right up the alley of ElasticBeanstalk. (Basically EC2 + Autoscale + ELB).
Preventing Abuse: When you put something in a public S3 bucket, people will hot-link it from their web pages. If you want to prevent that, your app on the EC2 box can generate signed links to S3 that expire in a few hours. Now everyone will be forced to go thru the app, and the app can apply rate limiting, etc.
Saving money: If you don't mind having downtime:
run everything in one AZ (both DBs and EC2s). You can always add servers and AZs down the road, as long as it's architected to be stateless. In fact, you should use multiple regions if you want it to be really robust.
use Reduced Redundancy in S3 to save a few hundred bucks per month (Someone will have to "go fix it" every time it breaks, including having an off-line copy to repair

S3.)
Buy Reserved Instances on your EC2 boxes to make them cheaper. (Start with the RI market and buy a partially used one to get started.) It's just a coupon saying "if you run this type of box in this AZ, you will save on the per-hour costs." You can get 1/2 to 1/3 off easily.
Rewrite the application to use less memory and CPU - that way you can run on fewer/smaller boxes. (May or may not be worth the investment.)
If your app will be used very infrequently, you will save a lot of money by using Lambda. I'd be worried that it would be quite slow if you tried to run a Java application on it though.
We're missing some information like load, latency expectations from search, indexing speed, size of the search index, etc. But with what you've given us, I would go with S3 as the storage for the files (S3 rocks. It is really, really awesome). If you're stuck with the commercial search application, then on EC2 instances with autoscaling and an ELB. If you are allowed an alternative search engine, Elasticsearch is probably your best bet. I'd run it on EC2 instead of the AWS Elasticsearch service, as IMHO it's not ready yet. Don't autoscale Elasticsearch automatically though, it'll cause all sorts of issues. I have zero experience with CloudSearch so ic an't comment on that.
Regardless of which option, I'd use CloudFormation for all of it.

QUESTION 36
A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an iPsec VPN. The application must authenticate against the on-premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user.
Which two approaches can satisfy these objectives? (Choose two.)

A. Develop an identity broker that authenticates against IAM security Token service to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.
B. The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket.
C. Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.
D. The application authenticates against LDAP the application, then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials, the application can use the IAM temporary credentials to access the appropriate S3 bucket.
E. The application authenticates against IAM Security Token Service using the LDAP credentials, the application uses those temporary AWS security credentials to access the appropriate S3 bucket.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Imagine that in your organization, you want to provide a way for users to copy data from their computers to a backup folder. You build an application that users can run on their computers. On
the back end, the application reads and writes objects in an S3 bucket. Users don’t have direct access to AWS. Instead, the application communicates with an identity provider (IdP) to authenticate the user. The IdP gets the user information from your organization’s identity store (such as an LDAP directory) and then generates a SAML assertion that includes authentication and authorization information about that user. The application then uses that assertion to make a call to the AssumeRoleWithSAML API to get temporary security credentials. The app can then use those credentials to access a folder in the S3 bucket that’s specific to the user.
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

QUESTION 37
You are designing a multi-platform web application for AWS The application will run on EC2 instances and will be accessed from PCs. tablets and smart phones Supported accessing platforms are Windows. MACOS. IOS and Android Separate sticky session and SSL certificate setups are required for different platform types which of the following describes the most cost effective and performance efficient architecture setup?

A. Setup a hybrid architecture to handle session state and SSL certificates on-prem and separate EC2 Instance groups running web applications for different platform types running in a VPC
B. Set up one ELB for all platforms to distribute load among multiple instance under it Each EC2 instance implements ail functionality for a particular platform.
C. Set up two ELBs The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms for each ELB run separate EC2 instance groups to handle the web application for each platform.
D. Assign multiple ELBS to an EC2 instance or group of EC2 instances running the common components of the web application, one ELB for each platform type Session stickiness and SSL termination are done at the ELBs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
One ELB cannot handle different SSL certificates but since we are using sticky sessions it must be handled at the ELB level. SSL could be handled on the EC2 instances only with TCP configured ELB, ELB supports sticky sessions only in HTTP/HTTPS configurations.
The way the Elastic Load Balancer does session stickiness is on a HTTP/HTTPS listener is by utilizing an HTTP cookie. If SSL traffic is not terminated on the Elastic Load Balancer and is
terminated on the back-end instance, the Elastic Load Balancer has no visibility into the HTTP headers and therefore cannot set or read any of the HTTP headers being passed back and forth.
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-sticky-sessions.html

QUESTION 38
Your company has an on-premises multi-tier PHP web application, which recently experienced downtime due to a large burst In web traffic due to a company announcement Over the coming days, you are expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your infrastructures ability to handle unexpected increases in traffic.
The application currently consists of 2 tiers a web tier which consists of a load balancer and several Linux Apache web servers as well as a database tier which hosts a Linux server hosting a MySQL database.
Which scenario below will provide full site functionality, while helping to improve the ability of your application in the short timeframe required?

A. Failover environment: Create an S3 bucket and configure it for website hosting. Migrate your DNS to Route53 using zone file import, and leverage Route53 DNS failover to failover to the S3 hosted website.
B. Hybrid environment: Create an AMI, which can be used to launch web servers in EC2. Create an Auto Scaling group, which uses the AMI to scale the web tier based on incoming traffic. Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted In AWS.
C. Offload traffic from on-premises environment: Setup a CloudFront distribution, and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behavior, and select a TTL that objects should exist in cache.
D. Migrate to AWS: Use VM Import/Export to quickly convert an on-premises web server to an AMI. Create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffic. Create an RDS read replica and setup replication between the RDS instance and on-premises MySQL server to migrate the database.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can have CloudFront sit in front of your on-prem web environment, via a custom origin (the

origin doesn't have to be in AWS). This would protect against unexpected bursts in traffic by letting CloudFront handle the traffic that it can out of cache, thus hopefully removing some of the load from your on-prem web servers.

QUESTION 39
Your company produces customer commissioned one-of-a-kind skiing helmets combining nigh fashion with custom technical enhancements Customers can show off their Individuality on the ski slopes and have access to head-up-displays. GPS rear-view cams and any other technical innovation they wish to embed in the helmet.
The current manufacturing process is data rich and complex including assessments to ensure that the custom electronics and materials used to assemble the helmets are to the highest standards Assessments are a mixture of human and automated assessments you need to add a new set of assessment to model the failure modes of the custom electronics using GPUs with CUDA, across a cluster of servers with low latency networking.
What architecture would allow you to automate the existing process using a hybrid approach and ensure that the architecture can support the evolution of processes over time?

A. Use AWS Data Pipeline to manage movement of data & meta-data and assessments Use an auto-scaling group of G2 instances in a placement group.
B. Use Amazon Simple Workflow (SWF) to manages assessments, movement of data & meta-data Use an auto-scaling group of G2 instances in a placement group.
C. Use Amazon Simple Workflow (SWF) to manages assessments movement of data & meta-data Use an auto-scaling group of C3 instances with SR-IOV (Single Root I/O Virtualization).
D. Use AWS data Pipeline to manage movement of data & meta-data and assessments use auto-scaling group of C3 with SR-IOV (Single Root I/O virtualization).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
You're running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup. Your backup application is only able to write to POSIX-compatible block-based storage. You have 140TB of data and would like to mount it as a single folder on your file server Users must be able to access portions of this data while the backups are taking place. What backup solution would be most appropriate for this use case?

A. Use Storage Gateway and configure it to use Gateway Cached volumes.
B. Configure your backup software to use S3 as the target for your data backups.
C. Configure your backup software to use Glacier as the target for your data backups.
D. Use Storage Gateway and configure it to use Gateway Stored volumes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data is hosted on the On-premise server as well. The requirement for 140TB is for file server On-Premise more to confuse and not in AWS. Just need a backup solution hence stored instead of cached volumes.

QUESTION 41
You require the ability to analyze a large amount of data, which is stored on Amazon S3 using Amazon Elastic Map Reduce. You are using the cc2 8x large Instance type, whose CPUs are mostly idle during processing. Which of the below would be the most cost efficient way to reduce the runtime of the job?

A. Create more smaller flies on Amazon S3.
B. Add additional cc2 8x large instances by introducing a task group.
C. Use smaller instances that have higher aggregate I/O performance.
D. Create fewer, larger files on Amazon S3.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/elasticmapreduce/faqs/

QUESTION 42
Your department creates regular analytics reports from your company's log files All log data is collected in Amazon S3 and processed by daily Amazon Elastic MapReduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse.
Your CFO requests that you optimize the cost structure for this system.
Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data?

A. Use reduced redundancy storage (RRS) for all data In S3. Use a combination of Spot Instances and Reserved Instances for Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
B. Use reduced redundancy storage (RRS) for PDF and .csv data in S3. Add Spot Instances to EMR jobs. Use Spot Instances for Amazon Redshift.
C. Use reduced redundancy storage (RRS) for PDF and .csv data In Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
D. Use reduced redundancy storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reserved Instances (a.k.a. Reserved Nodes) are appropriate for steady-state production workloads, and offer significant discounts over On-Demand pricing.
https://aws.amazon.com/redshift
Q: What are some EMR best practices?
If you are running EMR in production you should specify an AMI version, Hive version, Pig version, etc. to make sure the version does not change unexpectedly (e.g. when EMR later adds support for a newer version). If your cluster is mission critical, only use Spot instances for task nodes because if the Spot price increases you may lose the instances. In development, use logging and enable debugging to spot and correct errors faster. If you are using GZIP, keep your file size to 1–2 GB because GZIP files cannot be split. Click here to download the white paper on Amazon EMR best practices.
https://aws.amazon.com/elasticmapreduce/faqs

QUESTION 43
You are the new IT architect in a company that operates a mobile sleep tracking application
When activated at night, the mobile app is sending collected data points of 1 kilobyte every 5 minutes to your backend
The backend takes care of authenticating the user and writing the data points into an Amazon DynamoDB table.
Every morning, you scan the table to extract and aggregate last night's data on a per user basis, and store the results in Amazon S3.
Users are notified via Amazon SMS mobile push notifications that new data is available, which is parsed and visualized by (The mobile app Currently you have around

100k users who are mostly based out of North America.
You have been tasked to optimize the architecture of the backend system to lower cost what would you recommend? (Choose two.)

A. Create a new Amazon DynamoDB (able each day and drop the one for the previous day after its data is on Amazon S3.
B. Have the mobile app access Amazon DynamoDB directly instead of JSON files stored on Amazon S3.
C. Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput.
D. Introduce Amazon Elasticache lo cache reads from the Amazon DynamoDB table and reduce provisioned read throughput.
E. Write data directly into an Amazon Redshift cluster replacing both Amazon DynamoDB and Amazon S3.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high resolution MP4 format. Your workforce is distributed globally often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video. Your company has no video transcoding expertise and it required you may need to pay for a consultant.
How do you implement the most cost-efficient architecture without compromising high availability and quality of video delivery'?

A. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days. CloudFront to serve HLS transcoded videos from EC2.
B. Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days. CloudFront to serve HLS transcoded videos from EC2.
C. Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. S3 to host videos with Lifecycle Management to archive original files to Glacier after a few days. CloudFront to serve HLS transcoded videos from S3.
D. A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue. S3 to host videos with Lifecycle Management to archive all files to Glacier after a few days. CloudFront to serve HLS transcoded videos from Glacier.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
You've been hired to enhance the overall security posture for a very large e-commerce site They have a well architected multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3 They are using a combination of RDS and DynamoOB for their dynamic data and then archiving nightly into S3 for further processing with EMR They are concerned because they found questionable log entries and suspect someone is attempting to gain unauthorized access.
Which approach provides a cost effective scalable mitigation to this kind of attack?

A. Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to theirvPC they would then establish Internet

connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF). And then pass the traffic through the DirectConnect connection into their application running in their VPC,

B. Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet.

C. Add a WAF tier by creating a new ELB and an AutoScalmg group of EC2 Instances running a host-based WAF They would redirect Route 53 to resolve to the new WAF tier ELB The WAF tier would thier pass the traffic to the current web tier The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group

D. Remove all but TLS 1 2 from the web tier ELB and enable Advanced Protocol Filtering This will enable the ELB itself to perform WAF functionality.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
You currently operate a web application In the AWS US-East region The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2.IAM And RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?

A. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.

B. Create a new CloudTrail with one new S3 bucket to store the logs Configure SNS to send log file delivery notifications to your management system Use IAM roles and S3 bucket policies on the S3 bucket mat stores your logs.

C. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.

D. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?

A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.

B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application create a new access and secret key for the user and provide these credentials to the SaaS provider.

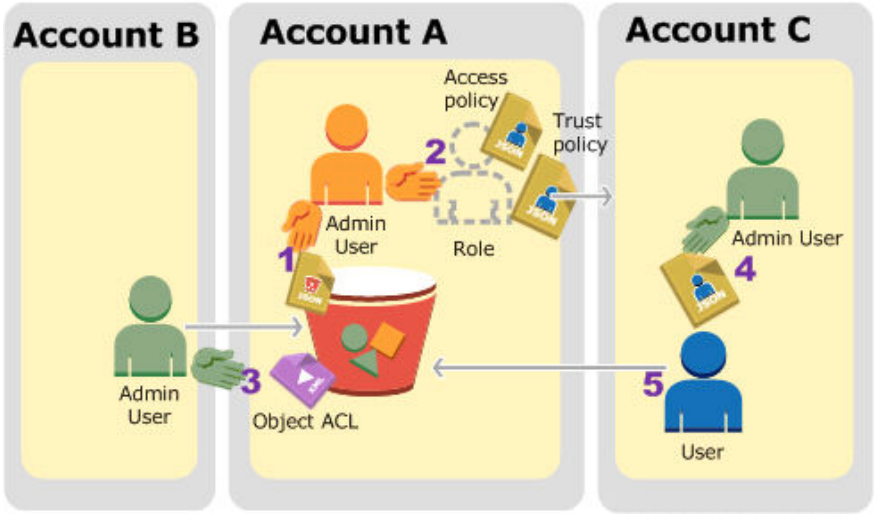
C. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the

SaaS application.

D. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARM to the SaaS provider to use when launching their application instances.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Granting Cross-account Permission to objects It Does Not Own
In this example scenario, you own a bucket and you have enabled other AWS accounts to upload objects. That is, your bucket can have objects that other AWS accounts own.
Now, suppose as a bucket owner, you need to grant cross-account permission on objects, regardless of who the owner is, to a user in another account. For example, that user could be a billing application that needs to access object metadata. There are two core issues:
The bucket owner has no permissions on those objects created by other AWS accounts. So for the bucket owner to grant permissions on objects it does not own, the object owner, the AWS account that created the objects, must first grant permission to the bucket owner. The bucket owner can then delegate those permissions.
Bucket owner account can delegate permissions to users in its own account but it cannot delegate permissions to other AWS accounts, because cross-account delegation is not supported.
In this scenario, the bucket owner can create an AWS Identity and Access Management (IAM) role with permission to access objects, and grant another AWS account permission to assume the role temporarily enabling it to access objects in the bucket.
Background: Cross-Account Permissions and Using IAM Roles
IAM roles enable several scenarios to delegate access to your resources, and cross-account access is one of the key scenarios. In this example, the bucket owner, Account A, uses an IAM role to temporarily delegate object access cross-account to users in another AWS account, Account C. Each IAM role you create has two policies attached to it:
A trust policy identifying another AWS account that can assume the role.
An access policy defining what permissions—for example, s3:GetObject—are allowed when someone assumes the role. For a list of permissions you can specify in a policy, see Specifying Permissions in a Policy.
The AWS account identified in the trust policy then grants its user permission to assume the role. The user can then do the following to access objects:
Assume the role and, in response, get temporary security credentials.
Using the temporary security credentials, access the objects in the bucket.
For more information about IAM roles, go to Roles (Delegation and Federation) in IAM User Guide.
The following is a summary of the walkthrough steps:



Account A administrator user attaches a bucket policy granting Account B conditional permission to upload objects.
Account A administrator creates an IAM role, establishing trust with Account C, so users in that account can access Account A. The access policy attached to the role limits what user in Account C can do when the user accesses Account A.
Account B administrator uploads an object to the bucket owned by Account A, granting full-control permission to the bucket owner.
Account C administrator creates a user and attaches a user policy that allows the user to assume the role.
User in Account C first assumes the role, which returns the user temporary security credentials. Using those temporary credentials, the user then accesses objects in the bucket.
For this example, you need three accounts. The following table shows how we refer to these accounts and the administrator users in these accounts. Per IAM guidelines (see About Using an Administrator User to Create Resources and Grant Permissions) we do not use the account root credentials in this walkthrough. Instead, you create an administrator user in each account and use those credentials in creating resources and granting them permissions

AWS Account ID	Account Referred To As	Administrator User in the Account
1111-1111-1111	Account A	AccountAadmin
2222-2222-2222	Account B	AccountBadmin
3333-3333-3333	Account C	AccountCadmin

QUESTION 48
You are designing a data leak prevention solution for your VPC environment. You want your VPC Instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via third party CONs by their URLs. You want to explicitly deny any other outbound connections from your VPC instances to hosts on the internet.
Which of the following options would you consider?

A. Configure a web proxy server in your VPC and enforce URL-based rules for outbound access Remove default routes.
B. Implement security groups and configure outbound rules to only permit traffic to software depots.
C. Move all your instances into private VPC subnets remove default routes from all routing tables and add specific routes to the software depots and distributions only.

D. Implement network access control lists to all specific destinations, with an Implicit deny as a rule.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Organizations usually implement proxy solutions to provide URL and web content filtering, IDS/IPS, data loss prevention, monitoring, and advanced threat protection.
https://d0.awsstatic.com/aws-answers/Controlling_VPC_Egress_Traffic.pdf

QUESTION 49
An administrator is using Amazon CloudFormation to deploy a three tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage when creating the CloudFormation template which of the following would allow the application instance access to the DynamoDB tables without exposing API credentials?

A. Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and associate the Role to the application instances by referencing an instance profile.
B. Use the Parameter section in the Cloud Formation template to nave the user input Access and Secret Keys from an already created IAM user that has me permissions required to read and write from the required DynamoDB table.
C. Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and reference the Role in the instance profile property of the application instance.
D. Create an identity and Access Management user in the CloudFormation template that has permissions to read and write from the required DynamoDB table, use the GetAtt function to retrieve the Access and secret keys and pass them to the application instance through user-data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
An AWS customer is deploying an application mat is composed of an AutoScaling group of EC2 Instances.
The customers security policy requires that every outbound connection from these instances to any other service within the customers
Virtual Private Cloud must be authenticated using a unique x 509 certificate that contains the specific instance-id.
In addition an x 509 certificates must Designed by the customer's Key management service in order to be trusted for authentication.
Which of the following configurations will support these requirements?

A. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure me Auto Scaling group to launch instances with this role Have the instances bootstrap get the certificate from Amazon S3 upon first boot.
B. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group Have the launched instances generate a certificate signature request with the instance's assigned instance-id to the Key management service for signature.
C. Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the Key management service generate a signed certificate and send it directly to the newly launched instance.
D. Configure the launched instances to generate a new certificate upon first boot Have the Key management service poll the AutoScaling group for associated instances and send new instances a certificate signature (hat contains the specific instance-id.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
http://jayendrapatil.com/tag/iam/

QUESTION 51
Your company has recently extended its datacenter into a VPC on AVVS to add burst computing capacity as needed Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary You don't want to create new IAM users for each NOC member and make those users sign in again to the AWS Management Console Which option below will meet the needs for your NOC members?

A. Use OAuth 2 0 to retrieve temporary AWS security credentials to enable your NOC members to sign in to the AVVS Management Console.
B. Use web Identity Federation to retrieve AWS temporary security credentials to enable your NOC members to sign in to the AWS Management Console.
C. Use your on-premises SAML 2.0-compliant identity provider (IDP) to grant the NOC members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.
D. Use your on-premises SAML2.0-compliam identity provider (IDP) to retrieve temporary security credentials to enable NOC members to sign in to the AWS Management Console.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

QUESTION 52
You are designing an SSUTLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient.
Which of the following options would you consider for configuring the web server infrastructure? (Choose two.)

A. Configure ELB with TCP listeners on TCP/4d3. And place the Web servers behind it.
B. Configure your Web servers with EIPS Place the Web servers in a Route53 Record Set and configure health checks against all Web servers.
C. Configure ELB with HTTPS listeners, and place the Web servers behind it.
D. Configure your web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This question is regarding “two-way” SSL authentication.

Currently, ELBs cannot support authentication for the client side SSL/TLS cert required for two-way SSL authentication to succeed. Therefore, you only have two options:

A. Configure the ELB with a TCP/443 listener. This is effectively TLS “pass through” mode, where the TLS connection does not terminate on the ELB, it is passed through and decrypted on the back-end servers. This will cause quite a bit of CPU overhead on the back-end instances, due to the lack of TLS offload that cannot happen on the ELB, so an auto-scaling group which monitors the web server CPU metrics would be essential here. (Not that you probably wouldn’t have it anyway, just saying!)

B. Don’t use an ELB. Just have the web servers act as the endpoint for the traffic, and let Route53 DNS serve in the place of the ELB by load balancing client DNS queries across the web servers.

C and D are not options here, since neither are supported by AWS.

QUESTION 53
You are designing a connectivity solution between on-premises infrastructure and Amazon VPC Your server’s on-premises will De communicating with your VPC instances You will De establishing IPSec tunnels over the internet You will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways.
Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? (Choose four.)

A. End-to-end protection of data in transit
B. End-to-end Identity authentication
C. Data encryption across the Internet
D. Protection of data in transit over the Internet
E. Peer identity authentication between VPN gateway and customer gateway
F. Data integrity protection across the Internet

Correct Answer: CDEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
You are designing an intrusion detection prevention (IDS/IPS) solution for a customer web application in a single VPC. You are considering the options for implementing IOS IPS protection for traffic coming from the Internet.
Which of the following options would you consider? (Choose two.)

A. Implement IDS/IPS agents on each Instance running In VPC
B. Configure an instance in each subnet to switch its network interface card to promiscuous mode and analyze network traffic.
C. Implement Elastic Load Balancing with SSL listeners In front of the web applications
D. Implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on each reverse proxy server.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

EC2 does not allow promiscuous mode, and you cannot put something in between the ELB and the web server (like a listener or IDP)

QUESTION 55
You are designing a photo sharing mobile app the application will store all pictures in a single Amazon S3 bucket.
Users will upload pictures from their mobile device directly to Amazon S3 and will be able to view and download their own pictures directly from Amazon S3.
You want to configure security to handle potentially millions of users in the most secure manner possible. What should your server-side application do when a new user registers on the photo-sharing mobile application?

A. Create a set of long-term credentials using AWS Security Token Service with appropriate permissions Store these credentials in the mobile app and use them to access Amazon S3.
B. Record the user's Information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app create temporary credentials using the AWS Security Token Service 'AssumeRole' function Store these credentials in the mobile app's memory and use them to access Amazon S3 Generate new credentials the next time the user runs the mobile app.
C. Record the user's Information In Amazon DynamoDB. When the user uses their mobile app create temporary credentials using AWS Security Token Service with appropriate permissions Store these credentials in the mobile app's memory and use them to access Amazon S3 Generate new credentials the next time the user runs the mobile app.
D. Create IAM user. Assign appropriate permissions to the IAM user Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
E. Create an IAM user. Update the bucket policy with appropriate permissions for the IAM user Generate an access Key and secret Key for the IAM user, store them In the mobile app and use these credentials to access Amazon S3.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html.

QUESTION 56
You have an application running on an EC2 Instance which will allow users to download flies from a private S3 bucket using a pre-assigned URL. Before generating the URL the application should verify the existence of the file in S3.
How should the application use AWS credentials to access the S3 bucket securely?

A. Use the AWS account access Keys the application retrieves the credentials from the source code of the application.
B. Create an IAM user for the application with permissions that allow list access to the S3 bucket launch the instance as the IAM user and retrieve the IAM user's credentials from the EC2 instance user data.
C. Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata
D. Create an IAM user for the application with permissions that allow list access to the S3 bucket. The application retrieves the IAM user credentials from a temporary directory with permissions that allow read access only to the application user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

QUESTION 57
You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks. Which of the below are viable mitigation techniques? (Choose three.)

A. Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
B. Use dedicated instances to ensure that each instance has the maximum performance possible.
C. Use an Amazon CloudFront distribution for both static and dynamic content.
D. Use an Elastic Load Balancer with auto scaling groups at the web. App and Amazon Relational Database Service (RDS) tiers
E. Add alert Amazon CloudWatch to look for high Network in and CPU utilization.
F. Create processes and capabilities to quickly add and remove rules to the instance OS firewall.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload tor the new fiscal year benefit enrollment period plus some extra overhead Enrollment proceeds nicely for two days and then the web tier becomes unresponsive, upon investigation using CloudWatch and other monitoring tools it is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers. The web tier instances are so overloaded that benefit enrollment administrators cannot even SSH into them. Which activity would be useful in defending against this attack?

A. Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (Internet Gateway)
B. Change the EIP (Elastic IP Address) of the NAT instance in the web tier subnet and update the Main Route Table with the new EIP
C. Create 15 Security Group rules to block the attacking IP addresses over port 80
D. Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Use AWS Identity and Access Management (IAM) to control who in your organization has permission to create and manage security groups and network ACLs (NACL). Isolate the responsibilities and roles for better defense. For example, you can give only your network administrators or security admin the permission to manage the security groups and restrict other roles.

QUESTION 59
Your fortune 500 company has under taken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware The outcome was that ail employees would be granted access to use Amazon S3 for storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? (Choose three.)

A. Setting up a federation proxy or identity provider
B. Using AWS Security Token Service to generate temporary tokens
C. Tagging each folder in the bucket
D. Configuring IAM role
E. Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Your company policies require encryption of sensitive data at rest. You are considering the possible options for protecting data while storing it at rest on an EBS data volume, attached to an EC2 instance. Which of these options would allow you to encrypt your data at rest? (Choose three.)

A. Implement third party volume encryption tools
B. Do nothing as EBS volumes are encrypted by default
C. Encrypt data inside your applications before storing it on EBS
D. Encrypt data using native data encryption drivers at the file system level
E. Implement SSL/TLS for all services running on the server

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Not E since SSL/TLS is encryption in transfer (https) and not encryption of sensitive data at rest.
And B is just not true. Although you nowadays can add encryption when creating a EBS volume
but it is NOT turned on by default.

QUESTION 61
You have a periodic Image analysis application that gets some files In Input analyzes them and tor each file writes some data in output to a ten file the number of files in input per day is high and concentrated in a few hours of the day.
Currently you have a server on EC2 with a large EBS volume that hosts the input data and the results it takes almost 20 hours per day to complete the process
What services could be used to reduce the elaboration time and improve the availability of the solution?

A. S3 to store I/O files. SQS to distribute elaboration commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the length of the SQS queue
B. EBS with Provisioned IOPS (PIOPS) to store I/O files. SNS to distribute elaboration commands to a group of hosts working in parallel Auto Scaling to dynamically size the group of hosts depending on the number of SNS notifications

C. S3 to store I/O files, SNS to distribute evaporation commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the number of SNS notifications

D. EBS with Provisioned IOPS (PIOPS) to store I/O files SOS to distribute elaboration commands to a group of hosts working in parallel Auto Scaling to dynamically size the group ot hosts depending on the length of the SQS queue.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances. Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use a block device. Amazon EBS volumes are placed in a specific Availability Zone, where they are automatically replicated to protect you from the failure of a single component.
Amazon EBS provides three volume types: General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic. The three volume types differ in performance characteristics and cost, so you can choose the right storage performance and price for the needs of your applications. All EBS volume types offer the same durable snapshot capabilities and are designed for 99.999% availability.

QUESTION 62
You require the ability to analyze a customer's clickstream data on a website so they can do behavioral analysis. Your customer needs to know what sequence of pages and ads their customer clicked on. This data will be used in real time to modify the page layouts as customers click through the site to increase stickiness and advertising click-through. Which option meets the requirements for captioning and analyzing this data?

A. Log clicks in weblogs by URL store to Amazon S3, and then analyze with Elastic MapReduce

B. Push web clicks by session to Amazon Kinesis and analyze behavior using Kinesis workers

C. Write click events directly to Amazon Redshift and then analyze with SQL

D. Publish web clicks by session to an Amazon SQS queue men periodically drain these events to Amazon RDS and analyze with sol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://www.slideshare.net/AmazonWebServices/aws-webcast-introduction-to-amazon-kinesis

QUESTION 63
An AWS customer runs a public blogging website. The site users upload two million blog entries a month The average blog entry size is 200 KB. The access rate to blog entries drops to negligible 6 months after publication and users rarely access a blog entry 1 year after publication. Additionally, blog entries have a high update rate during the first 3 months following publication, this drops to no updates after 6 months. The customer wants to use CloudFront to improve his user's load times. Which of the following recommendations would you make to the customer?

A. Duplicate entries into two different buckets and create two separate CloudFront distributions where S3 access is restricted only to Cloud Front identity

B. Create a CloudFront distribution with "US'Europe price class for US/Europe users and a different CloudFront distribution with All Edge Locations' for the remaining users.

C. Create a CloudFront distribution with S3 access restricted only to the CloudFront identity and partition the blog entry's location in S3 according to the month it was

uploaded to be used with CloudFront behaviors.

D. Create a CloudFronl distribution with Restrict Viewer Access Forward Query string set to true and minimum TTL of 0.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Your company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance. The site performs a high number of small reads and writes per second and relies on an eventual consistency model. After comprehensive tests you discover that there is read contention on RDS MySQL. Which are the best approaches to meet these requirements? (Choose two.)

A. Deploy ElasticCache in-memory cache running in each availability zone
B. Implement sharding to distribute load to multiple RDS MySQL instances
C. Increase the RDS MySQL Instance size and Implement provisioned IOPS
D. Add an RDS MySQL read replica in each availability zone

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A company is running a batch analysis every hour on their main transactional DB. running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift During the execution of the batch their transactional applications are very slow When the batch completes they need to update the top management dashboard with the new data The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required The on-premises system cannot be modified because is managed by another team.
How would you optimize this scenario to solve performance issues and automate the process as much as possible?

A. Replace RDS with Redshift for the batch analysis and SNS to notify the on-premises system to update the dashboard
B. Replace ROS with Redsnift for the oaten analysis and SQS to send a message to the on-premises system to update the dashboard
C. Create an RDS Read Replica for the batch analysis and SNS to notify me on-premises system to update the dashboard
D. Create an RDS Read Replica for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

If you want to prevent your reporting and analytic processing from interfering with the performance of your OLTP workload."
If I understand the above statement correctly, they are saying to separate reporting and analytic
processing from OLTP. In other word, use RedShift for reporting and analytic processing and use RDS for OLTP workload.

QUESTION 66
You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTP'S connections to specific domains from their EC2-hosted applications you deploy a single EC2 instance running proxy software and configure It to accept traffic from all subnets and EC2 instances in the VPC. You configure the proxy to only pass through traffic to domains that you define in its whitelist configuration You have a nightly maintenance window or 10 minutes where ail instances fetch new software updates. Each update Is about 200MB In size and there are 500 instances In the VPC that routinely fetch updates. After a few days you notice that some machines are failing to successfully download some, but not all of their updates within the maintenance window. The download URLs used for these updates are correctly listed in the proxy's whitelist configuration and you are able to access them manually using a web browser on the instances. What might be happening? (Choose two.)

A. You are running the proxy on an undersized EC2 instance type so network throughput is not sufficient for all instances to download their updates in time.
B. You are running the proxy on a sufficiently-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EC2 instance.
C. The route table for the subnets containing the affected EC2 instances is not configured to direct network traffic for the software update locations to the proxy.
D. You have not allocated enough storage to the EC2 instance running the proxy so the network buffer is filling up, causing some requests to fail.
E. You are running the proxy in a public subnet but have not allocated enough EIPs to support the needed network throughput through the Internet Gateway (IGW).

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-ec2-config.html

QUESTION 67
To serve Web traffic for a popular product your chief financial officer and IT director have purchased 10 ml large heavy utilization Reserved Instances (RIs) evenly spread across two availability zones: Route 53 is used to deliver the traffic to an Elastic Load Balancer (ELB). After several months, the product grows even more popular and you need additional capacity As a result, your company purchases two C3.2xlarge medium utilization Ris You register the two c3 2xlarge instances with your ELB and quickly find that the ml large instances are at 100% of capacity and the c3 2xlarge instances have significant capacity that's unused Which option is the most cost effective and uses EC2 capacity most effectively?

A. Use a separate ELB for each instance type and distribute load to ELBs with Route 53 weighted round robin
B. Configure Autoscaning group and Launch Configuration with ELB to add up to 10 more on-demand mi large instances when triggered by Cloudwatch shut off c3 2xiarge instances
C. Route traffic to EC2 ml large and c3 2xlarge instances directly using Route 53 latency based routing and health checks shut off ELB
D. Configure ELB with two c3 2xiarge Instances and use on-demand Autoscailng group for up to two additional c3.2xlarge instances Shut on mi .large instances.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Weighted Routing Policy
Use the weighted routing policy when you have multiple resources that perform the same function (for example, web servers that serve the same website) and you want

Amazon Route 53 to route traffic to those resources in proportions that you specify (for example, one quarter to one server and three quarters to the other). For more information about weighted resource record sets, see Weighted Routing.

QUESTION 68
A read only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically. What AWS services should be used meet these requirements?

A. Stateless instances for the web and application tier synchronized using Elasticache Memcached in an autoscaimg group monitored with CloudWatch. And RDSwith read replicas.
B. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and RDS with read replicas.
C. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch. And multi-AZ RDS.
D. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch and multi-AZ RDS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
“A readonly reporting site” - so stateless and read-replicas can be used to scale. Multi-AZ will not provide the scaling requirements.

QUESTION 69
You are running a news website in the eu-west-1 region that updates every 15 minutes. The website has a world-wide audience it uses an Auto Scaling group behind an Elastic Load Balancer and an Amazon RDS database Static content resides on Amazon S3, and is distributed through Amazon CloudFront. Your Auto Scaling group is set to trigger a scale up event at 60% CPU utilization, you use an Amazon RDS extra large DB instance with 10.000 Provisioned IOPS its CPU utilization is around 80%. While freeable memory is in the 2 GB range.
Web analytics reports show that the average load time of your web pages is around 1 5 to 2 seconds, but your SEO consultant wants to bring down the average load time to under 0.5 seconds.
How would you improve page load times for your users? (Choose three.)

A. Lower the scale up trigger of your Auto Scaling group to 30% so it scales more aggressively.
B. Add an Amazon ElastiCache caching layer to your application for storing sessions and frequent DB queries
C. Configure Amazon CloudFront dynamic content support to enable caching of re-usable content from your site
D. Switch Amazon RDS database to the high memory extra large Instance type
E. Set up a second installation in another region, and use the Amazon Route 53 latency-based routing feature to select the right region.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The freeable memory includes the amount of physical memory left unused by the system plus the total amount of buffer or page cache memory that are free and available.

So it’s freeable memory across the entire system. While MySQL is the main consumer of memory on the host we do have internal processes in addition to the OS that use up a small amount of additional memory.

If you see your freeable memory near 0 or also start seeing swap usage then you may need to scale up to a larger instance class or adjust MySQL memory settings. For example decreasing
the innodb_buffer_pool_size (by default set to 75% of physical memory) is one way example of adjusting MySQL memory settings

Takeaway: extra mem is not going to help page load times here, but a 2nd region might. Keep in mind they're going for a 66%-75% reduction in page load times – what if you added a region in Australia or HK, would that not help your worldwide users? rather than having traffic go to us-east.

QUESTION 70
A large real-estate brokerage is exploring the option o(adding a cost-effective location based alert to their existing mobile application The application backend infrastructure currently runs on AWS Users who opt in to this service will receive alerts on their mobile device regarding real-estate otters in proximity to their location. For the alerts to be relevant delivery time needs to be in the low minute count the existing mobile app has 5 million users across the us Which one of the following architectural suggestions would you make to the customer?

A. The mobile application will submit its location to a web service endpoint utilizing Elastic Load Balancing and EC2 instances: DynamoDB will be used to store and retrieve relevant otters EC2 instances will communicate with mobile earners/device providers to push alerts back to mobile application.
B. Use AWS DirectConnect or VPN to establish connectivity with mobile carriers EC2 instances will receive the mobile applications ' location through carrier connection: ROS will be used to store and relevant relevant offers EC2 instances will communicate with mobile carriers to push alerts back to the mobile application
C. The mobile application will send device location using SQS. EC2 instances will retrieve the relevant others from DynamoDB AWS Mobile Push will be used to send offers to the mobile application
D. The mobile application will send device location using AWS Mobile Push EC2 instances will retrieve the relevant offers from DynamoDB EC2 instances will communicate with mobile carriers/device providers to push alerts back to the mobile application.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS using SQS to store the message from mobile apps,and using AWS Mobile Push to send
offers to mobile apps.

QUESTION 71
A company is building a voting system for a popular TV show, viewers win watch the performances then visit the show's website to vote for their favorite performer. It is expected that in a short period of time after the show has finished the site will receive millions of visitors. The visitors will first login to the site using their Amazon.com credentials and then submit their vote. After the voting is completed the page will display the vote totals. The company needs to build the site such that can handle the rapid influx of traffic while maintaining good performance but also wants to keep costs to a minimum. Which of the design patterns below should they use?

A. Use CloudFront and an Elastic Load balancer in front of an auto-scaled set of web servers, the web servers will first can the Login With Amazon service to authenticate the user then process the users vote and store the result into a multi-AZ Relational Database Service instance.
B. Use CloudFront and the static website hosting feature of S3 with the Javascript SDK to call the Login With Amazon service to authenticate the user, use IAM Roles to gain permissions to a DynamoDB table to store the users vote.
C. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into a DynamoDB table using IAM Roles for EC2 instances to gain permissions to the DynamoDB table.
D. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first call the Login. With Amazon service to authenticate the user, the web servers win process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to

the SQS queue. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
You are developing a new mobile application and are considering storing user preferences in AWS.2w This would provide a more uniform cross-device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size Additionally 5 million customers are expected to use the application on a regular basis. The solution needs to be cost-effective, highly available, scalable and secure, how would you design a solution to meet the above requirements?

A. Setup an RDS MySQL instance in 2 availability zones to store the user preference data. Deploy a public facing application on a server in front of the database to manage security and access credentials
B. Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS. Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access.
C. Setup an RDS MySQL instance with multiple read replicas in 2 availability zones to store the user preference data .The mobile application will query the user preferences from the read replicas. Leverage the MySQL user management and access privilege system to manage security and access credentials.
D. Store the user preference data in S3 Setup a DynamoDB table with an item for each user and an item attribute pointing to the user' S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3 object directly utilize STS, Web identity Federation, and S3 ACLs to authenticate and authorize access.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/blogs/aws/fine-grained-access-control-for-amazon-dynamodb/
Here are some of the things that you can build using fine-grained access control:
A mobile app that displays information for nearby airports, based on the user's location. The app can access and display attributes such airline names, arrival times, and flight numbers. However,
it cannot access or display pilot names or passenger counts.
A mobile game which stores high scores for all users in a single table. Each user can update their own scores, but has no access to the other ones.

QUESTION 73
Your team has a tomcat-based Java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC .The optimal setup for persistence and security that meets the above requirements would be the following.

A. Create your RDS instance as part of your Elastic Beanstalk definition and alter its security group to allow access to it from hosts in your application subnets.
B. Create your RDS instance separately and add its IP address to your application's DB connection strings in your code Alter its security group to allow access to it from

hosts within your VPC's IP address block.

C. Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself.

D. Create your RDS instance separately and pass its DNS name to your's DB connection string as an environment variable Alter its security group to allow access to it from hosts in your application subnets.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Elastic Beanstalk provides support for running Amazon RDS instances in your Elastic Beanstalk environment. This works great for development and testing environments, but is not ideal for a production environment because it ties the lifecycle of the database instance to the lifecycle of your application's environment.
It can't be D because RDS is opened to all "hosts in your application subnets" where C only opens RDS to specific client machines in a specific security group.
http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.RDS.html

QUESTION 74
You are looking to migrate your Development (Dev) and Test environments to AWS. You have decided to use separate AWS accounts to host each environment. You plan to link each accounts bill to a Master AWS account using Consolidated Billing. To make sure you Keep within budget you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts. Identify which option will allow you to achieve this goal.

A. Create IAM users in the Master account with full Admin permissions. Create cross-account roles in the Dev and Test accounts that grant the Master account access to the resources in the account by inheriting permissions from the Master account.

B. Create IAM users and a cross-account role in the Master account that grants full Admin permissions to the Dev and Test accounts.

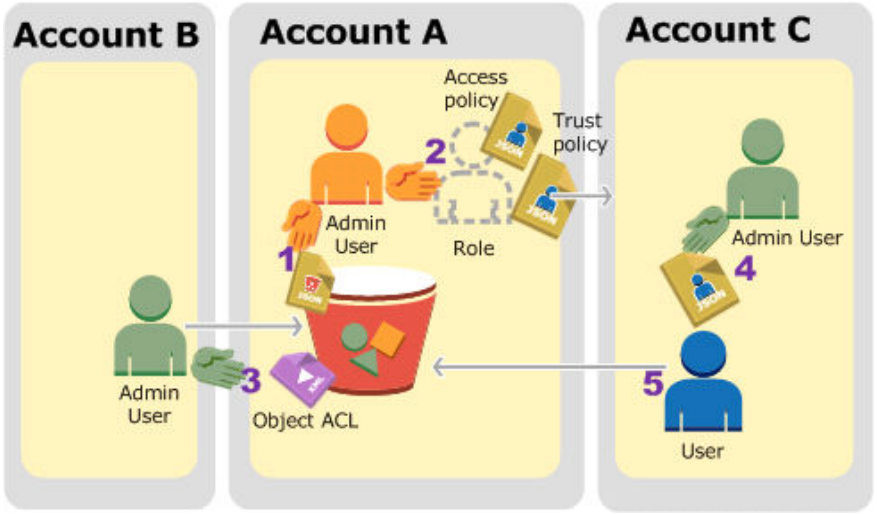
C. Create IAM users in the Master account Create cross-account roles in the Dev and Test accounts that have full Admin permissions and grant the Master account access.

D. Link the accounts using Consolidated Billing. This will give IAM users in the Master account access to resources in the Dev and Test accounts

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bucket Owner Granting Cross-account Permission to objects It Does Not Own
In this example scenario, you own a bucket and you have enabled other AWS accounts to upload objects. That is, your bucket can have objects that other AWS accounts own.
Now, suppose as a bucket owner, you need to grant cross-account permission on objects, regardless of who the owner is, to a user in another account. For example, that user could be a billing application that needs to access object metadata. There are two core issues:
The bucket owner has no permissions on those objects created by other AWS accounts. So for the bucket owner to grant permissions on objects it does not own, the object owner, the AWS account that created the objects, must first grant permission to the bucket owner. The bucket owner can then delegate those permissions.
Bucket owner account can delegate permissions to users in its own account but it cannot delegate permissions to other AWS accounts, because cross-account delegation is not supported.
In this scenario, the bucket owner can create an AWS Identity and Access Management (IAM) role with permission to access objects, and grant another AWS account

permission to assume the role temporarily enabling it to access objects in the bucket.
Background: Cross-Account Permissions and Using IAM Roles
IAM roles enable several scenarios to delegate access to your resources, and cross-account access is one of the key scenarios. In this example, the bucket owner, Account A, uses an IAM role to temporarily delegate object access cross-account to users in another AWS account, Account C. Each IAM role you create has two policies attached to it:
A trust policy identifying another AWS account that can assume the role.
An access policy defining what permissions—for example, s3:GetObject—are allowed when someone assumes the role. For a list of permissions you can specify in a policy, see Specifying Permissions in a Policy.
The AWS account identified in the trust policy then grants its user permission to assume the role. The user can then do the following to access objects:
Assume the role and, in response, get temporary security credentials.
Using the temporary security credentials, access the objects in the bucket.
For more information about IAM roles, go to Roles (Delegation and Federation) in IAM User Guide.
The following is a summary of the walkthrough steps:



Account A administrator user attaches a bucket policy granting Account B conditional permission to upload objects.
Account A administrator creates an IAM role, establishing trust with Account C, so users in that account can access Account A. The access policy attached to the role limits what user in Account C can do when the user accesses Account A.
Account B administrator uploads an object to the bucket owned by Account A, granting full-control permission to the bucket owner.
Account C administrator creates a user and attaches a user policy that allows the user to assume the role.
User in Account C first assumes the role, which returns the user temporary security credentials. Using those temporary credentials, the user then accesses objects in the bucket.
For this example, you need three accounts. The following table shows how we refer to these accounts and the administrator users in these accounts. Per IAM guidelines (see About Using an Administrator User to Create Resources and Grant Permissions) we do not use the account root credentials in this walkthrough. Instead, you create an administrator user in each account and use those credentials in creating resources and granting them permissions

AWS Account ID	Account Referred To As	Administrator User in the Account
1111-1111-1111	Account A	AccountAadmin
2222-2222-2222	Account B	AccountBadmin
3333-3333-3333	Account C	AccountCadmin

QUESTION 75
Your customer is willing to consolidate their log streams (access logs application logs security logs etc.) in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics. From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours?
What is the best approach to meet your customer's requirements?

A. Send all the log events to Amazon SQS. Setup an Auto Scaling group of EC2 servers to consume the logs and apply the heuristics.
B. Send all the log events to Amazon Kinesis develop a client process to apply heuristics on the logs
C. Configure Amazon Cloud Trail to receive custom logs, use EMR to apply heuristics the logs
D. Setup an Auto Scaling group of EC2 syslogd servers, store the logs on S3 use EMR to apply heuristics on the logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Kinesis Streams allows for real-time data processing. With Amazon Kinesis Streams, you can continuously collect data as it is generated and promptly react to critical information about your business and operations.
https://aws.amazon.com/kinesis/streams/

QUESTION 76
You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3. An Elastic Map Reduce job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO.
You recently improved overall performance of the website using Cloud Front for dynamic content delivery and your website as the origin.
After this architectural change, the usage dashboard shows that the traffic on your website dropped by an order of magnitude. How do you fix your usage dashboard'?

A. Enable Cloud Front to deliver access logs to S3 and use them as input of the Elastic Map Reduce job.
B. Turn on Cloud Trail and use trail log tiles on S3 as input of the Elastic Map Reduce job
C. Change your log collection process to use Cloud Watch ELB metrics as input of the Elastic Map Reduce job
D. Use Elastic Beanstalk "Rebuild Environment" option to update log delivery to the Elastic Map Reduce job.
E. Use Elastic Beanstalk 'Restart App server(s)" option to update log delivery to the Elastic Map Reduce job.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

QUESTION 77
You are running a successful multitier web application on AWS and your marketing department has asked you to add a reporting tier to the application. The reporting tier will aggregate and publish status reports every 30 minutes from user-generated information that is being stored in your web application s database. You are currently running a Multi-AZ RDS MySQL instance for the database tier. You also have implemented Elasticache as a database caching layer between the application tier and database tier. Please select the answer that will allow you to successfully implement the reporting tier with as little impact as possible to your database.

A. Continually send transaction logs from your master database to an S3 bucket and generate the reports off the S3 bucket using S3 byte range requests.
B. Generate the reports by querying the synchronously replicated standby RDS MySQL instance maintained through Multi-AZ.
C. Launch a RDS Read Replica connected to your Multi AZ master database and generate reports by querying the Read Replica.
D. Generate the reports by querying the ElastiCache database caching tier.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS allows you to use read replicas with Multi-AZ deployments. In Multi-AZ deployments for MySQL, Oracle, SQL Server, and PostgreSQL, the data in your primary DB Instance is synchronously replicated to to a standby instance in a different Availability Zone (AZ). Because of their synchronous replication, Multi-AZ deployments for these engines offer greater data durability benefits than do read replicas. (In all Amazon RDS for Aurora deployments, your data is automatically replicated across 3 Availability Zones.)
You can use Multi-AZ deployments and read replicas in conjunction to enjoy the complementary benefits of each. You can simply specify that a given Multi-AZ deployment is the source DB Instance for your Read replicas. That way you gain both the data durability and availability benefits of Multi-AZ deployments and the read scaling benefits of read replicas.
Note that for Multi-AZ deployments, you have the option to create your read replica in an AZ other than that of the primary and the standby for even more redundancy. You can identify the AZ corresponding to your standby by looking at the "Secondary Zone" field of your DB Instance in the AWS Management Console.

QUESTION 78
A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC,
How should they architect their solution to achieve these goals?

A. Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see an traffic across the VPC,
B. Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides.
C. Configure servers running in the VPC using the host-based 'route' commands to send all traffic through the platform to a scalable virtualized IDS/IPS.
D. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A. Not possible to set an instance's NIC into promiscuous mode.

B. Incorrect… VPC peering connections are not "transitive", i.e. you cannot pass traffic through a VPC peering connection into another VPC, and then have that other VPC send the traffic to some third VPC, or the Internet, or a VPN, or a direct connect circuit. (I would assume AWS does not allow redistribution of routes from one VPC's back-end VRF into another VPC's back-end VRF, unless it is that first VPC's CIDR block? Someone from AWS would have to chime in here, and they're probably not going to tell us.)

C. This one is incorrect because adding static routes on an instance won't affect the routing from any point after the packet leaves the instance's NIC. AWS will check the destination IP address in the packet header and forward according to the VPC routing table's routes. You'd need to make routing changes in the VPC route table for that instance's traffic to get sent through another device (e.g. NAT gateway, VPN instance, or security proxy in this case). (You could tunnel/proxy the traffic over through the IPS tier by changing the destination IP address in the IP header of the packet before it left the instance. But choice C did not state anything about doing anything like that. It just said add a static route on the instance, which does not change the destination IP address in the IP header of the packet.)

D. Correct, this is the standard approach, and is definitely scalable.

QUESTION 79
A web-startup runs its very successful social news application on Amazon EC2 with an Elastic Load Balancer, an Auto-Scaling group of Java/Tomcat application-servers, and DynamoDB as data store. The main web-application best runs on m2 x large instances since it is highly memory- bound Each new deployment requires semi-automated creation and testing of a new AMI for the application servers which takes quite a while ana is therefore only done once per week.
Recently, a new chat feature has been implemented in nodejs and wails to be integrated in the architecture. First tests show that the new component is CPU bound Because the company has some experience with using Chef, they decided to streamline the deployment process and use AWS Ops Works as an application life cycle tool to simplify management of the application and reduce the deployment cycles.
What configuration in AWS Ops Works is necessary to integrate the new chat module in the most cost-efficient and flexible way?

A. Create one AWS OpsWorks stack, create one AWS Ops Works layer, create one custom recipe
B. Create one AWS OpsWorks stack create two AWS Ops Works layers create one custom recipe
C. Create two AWS OpsWorks stacks create two AWS Ops Works layers create one custom recipe
D. Create two AWS OpsWorks stacks create two AWS Ops Works layers create two custom recipe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You only need one stack to contain two layers:
– one layer for the Java/Tomcat instances
– one layer for DynamoDB

You'd only need one custom recipe because the only OpsWorks Lifecycle Event that would be involved in rolling out the new chat feature would be "Deploy". (Or you could implement it in "Setup" if you choose to make including the chat app a new baseline standard for your instances in that layer. But even then, you'd only have one custom recipe because there would be no need to customize the "Deploy" event to install the chat app if you already installed out the chat app in "Setup".) So you'd need a custom recipe for that one lifecycle event. And it would only be used for the "Deploy" lifecycle event on the app layer, not on the DB layer

QUESTION 80
Your firm has uploaded a large amount of aerial image data to S3 In the past, in your on-premises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ - An open source messaging system to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost. Which is correct?

A. Use SQS for passing job messages use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
B. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SOS Once data is processed,
C. Change the storage class of the S3 objects to Reduced Redundancy Storage. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS Once data is processed, change the storage class of the S3 objects to Glacier.
D. Use SNS to pass job messages use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The question key part to focus on is “and leverage AWS archival storage and messaging services
to minimize cost.”
For that the storage that is the lowest cost in the answers is Glacier, in addition, the messaging cost is less for SQS then for SNS if they both exceed 1 million transactions which is free. The
only answer that satisfies the above two criteria is answer C. Also, there does not seem to be an
urgency in speed of messaging therefore SQS satisfies that need. SNS being more real time delivery mechanism.

QUESTION 81
What does Amazon S3 stand for?

A. Simple Storage Solution.
B. Storage Storage Storage (triple redundancy Storage).
C. Storage Server Solution.
D. Simple Storage Service.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonS3/latest/gsg/GetStartedWithS3.html

QUESTION 82
You must assign each server to at least _____ security group

A. 3
B. 2
C. 4

D. 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Your AWS account automatically has a default security group per region for EC2-Classic. When you create a VPC, we automatically create a default security group for the VPC. If you don't specify a different security group when you launch an instance, the instance is automatically associated with the appropriate default security group.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 83
Before I delete an EBS volume, what can I do if I want to recreate the volume later?

A. Create a copy of the EBS volume (not a snapshot)
B. Store a snapshot of the volume
C. Download the content to an EC2 instance
D. Back up the data in to a physical disk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
After you no longer need an Amazon EBS volume, you can delete it. After deletion, its data is gone and the volume can't be attached to any instance. However, before deletion, you can store a snapshot of the volume, which you can use to re-create the volume later.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-volume.html

QUESTION 84
Select the most correct answer: The device name /dev/sda1 (within Amazon EC2) is _____

A. Possible for EBS volumes
B. Reserved for the root device
C. Recommended for EBS volumes
D. Recommended for instance store volumes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html
The root device is typically /dev/sda1 (Linux) or xvda (Windows).

QUESTION 85
If I want an instance to have a public IP address, which IP address should I use?

A. Elastic IP Address
B. Class B IP Address
C. Class A IP Address
D. Dynamic IP Address

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
What does RRS stand for when talking about S3?

A. Redundancy Removal System
B. Relational Rights Storage
C. Regional Rights Standard
D. Reduced Redundancy Storage

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingRRS.html

QUESTION 87
All Amazon EC2 instances are assigned two IP addresses at launch, out of which one can only be reached from within the Amazon EC2 network?

A. Multiple IP address
B. Public IP address
C. Private IP address
D. Elastic IP Address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
What does Amazon SWF stand for?

A. Simple Web Flow
B. Simple Work Flow
C. Simple Wireless Forms
D. Simple Web Form

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
What is the Reduced Redundancy option in Amazon S3?

A. Less redundancy for a lower cost.
B. It doesn't exist in Amazon S3, but in Amazon EBS.
C. It allows you to destroy any copy of your files outside a specific jurisdiction.
D. It doesn't exist at all

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Fill in the blanks: Resources that are created in AWS are identified by a unique identifier called an _____

A. Amazon Resource Number
B. Amazon Resource Nametag
C. Amazon Resource Name
D. Amazon Resource Namespace

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
If I write the below command, what does it do?
ec2-run ami-e3a5408a -n 20 -g appserver

A. Start twenty instances as members of appserver group.
B. Creates 20 rules in the security group named appserver
C. Terminate twenty instances as members of appserver group.
D. Start 20 security groups

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
While creating an Amazon RDS DB, your first task is to set up a DB _____ that controls what IP addresses or EC2 instances have access to your DB Instance.

A. Security Pool
B. Secure Zone
C. Security Token Pool
D. Security Group

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
When you run a DB Instance as a Multi-AZ deployment, the "_____" serves database writes and reads

A. secondary
B. backup
C. stand by
D. primary

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 94
Every user you create in the IAM system starts with _____.

A. Partial permissions
B. Full permissions
C. No permissions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Can you create IAM security credentials for existing users?

A. Yes, existing users can have security credentials associated with their account.
B. No, IAM requires that all users who have credentials set up are not existing users
C. No, security credentials are created within GROUPS, and then users are associated to GROUPS at a later time.
D. Yes, but only IAM credentials, not ordinary security credentials.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
What does Amazon EC2 provide?

A. Virtual servers in the Cloud.
B. A platform to run code (Java, PHP, Python), paying on an hourly basis.
C. Computer Clusters in the Cloud.
D. Physical servers, remotely managed by the customer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Amazon SWF is designed to help users...

A. Design graphical user interface interactions
B. Manage user identification and authorization
C. Store Web content
D. Coordinate synchronous and asynchronous tasks which are distributed and fault tolerant.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Can I control if and when MySQL based RDS Instance is upgraded to new supported versions?

A. No
B. Only in VPC
C. Yes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
When you view the block device mapping for your instance, you can see only the EBS volumes, not the instance store volumes.

A. Depends on the instance type
B. FALSE
C. Depends on whether you use API call
D. TRUE

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When you view the block device mapping for your instance, you can see only the EBS volumes,
not the instance store volumes. You can use instance metadata to query the complete block device mapping. The base URI for all requests for instance metadata is http://169.254.169.254/latest/.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html#bdm-instance-metadata

QUESTION 100
By default, EBS volumes that are created and attached to an instance at launch are deleted when that instance is terminated. You can modify this behavior by changing the value of the flag_____ to false when you launch the instance

A. DeleteOnTermination
B. RemoveOnDeletion
C. RemoveOnTermination
D. TerminateOnDeletion

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By default, Amazon EBS root device volumes are automatically deleted when the instance terminates. However, by default, any additional EBS volumes that you attach at launch, or any EBS volumes that you attach to an existing instance persist even after the instance terminates.
This behavior is controlled by the volume's DeleteOnTermination attribute, which you can modify.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

QUESTION 101
What are the initial settings of an user created security group?

A. Allow all inbound traffic and Allow no outbound traffic
B. Allow no inbound traffic and Allow no outbound traffic
C. Allow no inbound traffic and Allow all outbound traffic
D. Allow all inbound traffic and Allow all outbound traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Will my standby RDS instance be in the same Region as my primary?

A. Only for Oracle RDS types
B. Yes
C. Only if configured at launch

D. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



QUESTION 103
What does Amazon Elastic Beanstalk provide?

A. A scalable storage appliance on top of Amazon Web Services.
B. An application container on top of Amazon Web Services.
C. A service by this name doesn't exist.
D. A scalable cluster of EC2 instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
True or False: When using IAM to control access to your RDS resources, the key names that can be used are case sensitive. For example, aws:CurrentTime is NOT equivalent to AWS:currenttime.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

AWS Direct Connect Keys

AWS Direct Connect implements the following policy keys:

- `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)

If you use `aws:SourceIp`, and the request comes from an Amazon EC2 instance, the instance's public IP address is used to determine if access is allowed.

> **Note**
>
> For services that use only SSL, such as Amazon Relational Database Service and Amazon Route 53, the `aws:SecureTransport` key has no meaning.

Key names are case-insensitive. For example, `aws:CurrentTime` is equivalent to `AWS:currenttime`.

http://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html

QUESTION 105
What will be the status of the snapshot until the snapshot is complete.

A. running
B. working
C. progressing
D. pending

Correct Answer: D
Section: (none)
Explanation

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

Creating an Amazon EBS Snapshot

After writing data to an EBS volume, you can periodically create a snapshot of the volume to use as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental so that only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the volume.

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is `pending` until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.

QUESTION 106
Can we attach an EBS volume to more than one EC2 instance at the same time?

A. No
B. Yes.
C. Only EC2-optimized EBS volumes.
D. Only in read mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
True or False: Automated backups are enabled by default for a new DB Instance.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
What does the AWS Storage Gateway provide?

A. It allows to integrate on-premises IT environments with Cloud Storage.

B. A direct encrypted connection to Amazon S3.
C. It's a backup solution that provides an on-premises Cloud storage.
D. It provides an encrypted SSL endpoint for backups in the Cloud.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Amazon RDS automated backups and DB Snapshots are currently supported for only the _____ storage engine

A. InnoDB
B. MyISAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Fill in the blanks: The base URI for all requests for instance metadata is _____

A. http://254.169.169.254/latest/
B. http://169.169.254.254/latest/
C. http://127.0.0.1/latest/
D. http://169.254.169.254/latest/

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://aws.amazon.com/search?searchQuery=metadata&searchPath=all&x=0&y=0

QUESTION 111
While creating the snapshots using the command line tools, which command should I be using?

A. ec2-deploy-snapshot
B. ec2-fresh-snapshot

C. ec2-create-snapshot
D. ec2-new-snapshot

Correct Answer: C
Section: (none)
Explanation

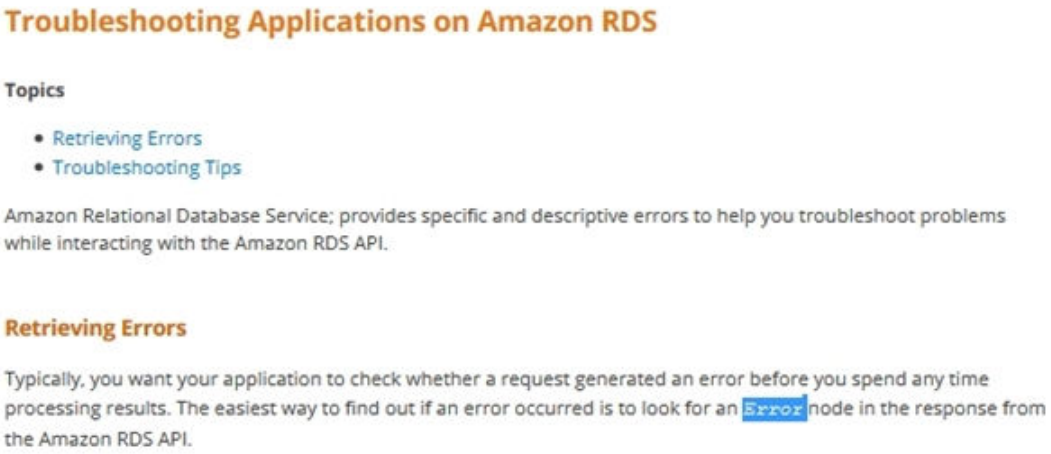
Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshot.html

QUESTION 112
Typically, you want your application to check whether a request generated an error before you spend any time processing results. The easiest way to find out if an error occurred is to look for an _____ node in the response from the Amazon RDS API.

A. Incorrect
B. Error
C. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/APITroubleshooting.html

QUESTION 113
What are the two permission types used by AWS?

A. Resource-based and Product-based
B. Product-based and Service-based
C. Service-based
D. User-based and Resource-based

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_controlling.html

QUESTION 114
In the Amazon cloudwatch, which metric should I be checking to ensure that your DB Instance has enough free storage space?

A. FreeStorage
B. FreeStorageSpace
C. FreeStorageVolume
D. FreeDBStorageSpace

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html

QUESTION 115
Amazon RDS DB snapshots and automated backups are stored in

A. Amazon S3
B. Amazon ECS Volume
C. Amazon RDS
D. Amazon EMR

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116

What is the maximum key length of a tag?

A. 512 Unicode characters
B. 64 Unicode characters
C. 256 Unicode characters
D. 128 Unicode characters

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 117
Groups can't _____.

A. be nested more than 3 levels
B. be nested at all
C. be nested more than 4 levels
D. be nested more than 2 levels

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Groups can’t be nested; they can contain only users, not other groups.
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

QUESTION 118
You must increase storage size in increments of at least _____ %

A. 40
B. 20
C. 50
D. 10

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference:
http://awsdocs.s3.amazonaws.com/RDS/2010-07-28/rds-ug-2010-07-28.pdf

QUESTION 119
Changes to the backup window take effect _____.

A. from the next billing cycle
B. after 30 minutes
C. immediately
D. after 24 hours

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Changes to the backup window take effect immediately, with the limitations that the specified backup window must be at least 10 minutes in the future, and the backup window cannot overlap with the weekly maintenance window for the instance.

QUESTION 120
Using Amazon CloudWatch's Free Tier, what is the frequency of metric updates which you receive?

A. 5 minutes
B. 500 milliseconds.
C. 30 seconds
D. 1 minute

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can get started with Amazon CloudWatch for free. Many applications should be able to operate within these free tier limits.
New and existing customers also receive 3 dashboards of up to 50 metrics each per month at no additional charge Basic Monitoring metrics (at five-minute frequency) for Amazon EC2 instances are free of charge, as are all metrics for Amazon EBS volumes, Elastic Load Balancers, and Amazon RDS DB instances.
https://aws.amazon.com/cloudwatch/pricing/

QUESTION 121
Which is the default region in AWS?

A. eu-west-1
B. us-east-1
C. us-east-2
D. ap-southeast-1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All the main AWS services (except Route 53 & CloudFront) allow you to select which region you would like to use. The US East (N. Virginia) is the default region. You can change the region by using the dropdown menu in the top right of the management console.

QUESTION 122
What are the Amazon EC2 API tools?

A. They don't exist. The Amazon EC2 AMI tools, instead, are used to manage permissions.
B. Command-line tools to the Amazon EC2 web service.
C. They are a set of graphical tools to manage EC2 instances.
D. They don't exist. The Amazon API tools are a client interface to Amazon Web Services.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://aws.amazon.com/developertools/351

QUESTION 123
What are the two types of licensing options available for using Amazon RDS for Oracle?

A. BYOL and Enterprise License
B. BYOL and License Included
C. Enterprise License and License Included
D. Role based License and License Included

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/rds/oracle/

You can run Amazon RDS for Oracle under two different licensing models – "License Included" and "Bring-Your-Own-License (BYOL)". In the "License Included" service model, you do not need separately purchased Oracle licenses; the Oracle Database software has been licensed by AWS. "License Included" pricing starts at $0.04 per hour, inclusive of software, underlying hardware resources, and Amazon RDS management capabilities. If you already own Oracle Database licenses, you can use the "BYOL" model to run Oracle databases on Amazon RDS, with rates starting at $0.025 per hour. The "BYOL" model is designed for customers who prefer to use existing Oracle database licenses or purchase new licenses directly from Oracle. For more information, see Licensing Amazon RDS for Oracle.

QUESTION 124
What does a "Domain" refer to in Amazon SWF?

A. A security group in which only tasks inside can communicate with each other
B. A special type of worker
C. A collection of related Workflows
D. The DNS record for the Amazon SWF service

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Domains provide a way of scoping Amazon SWF resources within your AWS account. All the components of a workflow, such as the workflow type and activity types, must be specified to be in a domain. It is possible to have more than one workflow in a domain; however, workflows in different domains cannot interact with each other. http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-dev-domain.html

QUESTION 125
EBS Snapshots occur _____

A. Asynchronously
B. Synchronously
C. Weekly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

QUESTION 126
Disabling automated backups _____ disable the point-in-time recovery.

A. if configured to can

B. will never
C. will

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Out of the stripping options available for the EBS volumes, which one has the following disadvantage : 'Doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you're mirroring all writes to a pair of volumes, limiting how much you can stripe.' ?

A. Raid 0
B. RAID 1+0 (RAID 10)
C. Raid 1
D. Raid

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/raid-config.html raid 0 and 1 are the common types. Raid 5 and 6 are not recommended because of the extended stripe. If you encounter this question on the exam I suspect the answer options will be different.
Raid 1 Disadvantage
Does not provide a write performance improvement; requires more Amazon EC2 to Amazon EBS bandwidth than non- RAID configurations because the data is written to multiple volumes simultaneously.
Raid 0 Disadvantage
Performance of the stripe is limited to the worst performing volume in the set. Loss of a single volume results in a complete data loss for the array.
Raid 5 and 6 notes
RAID 5 and RAID 6 are not recommended for Amazon EBS because the parity write operations of these RAID modes consume some of the IOPS available to your volumes. Depending on the configuration of your RAID array, these RAID modes provide 20-30% fewer usable IOPS than a RAID 0 configuration. Increased cost is a factor with these RAID modes as well; when using identical volume sizes and speeds, a 2-volume RAID 0 array can outperform a 4-volume RAID 6 array that costs twice as much.

QUESTION 128
Is creating a Read Replica of another Read Replica supported?

A. Only in certain regions
B. Only with MSSQL based RDS
C. Only for Oracle RDS types
D. No

Correct Answer: D
Section: (none)
Explanation

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

Q: Can I create a Read Replica of another Read Replica?

Amazon RDS for MySQL and MariaDB: You can create a second-tier Read Replica from an existing first-tier Read Replica. By creating a second-tier Read Replica, you may be able to move some of the replication load from the master database instance to a first-tier Read Replica. Please note that a second-tier Read Replica may lag further behind the master because of additional replication latency introduced as transactions are replicated from the master to the first tier replica and then to the second-tier replica.

Amazon RDS for PostgreSQL: Read Replicas of Read Replicas are not currently supported.

QUESTION 129
Can Amazon S3 uploads resume on failure or do they need to restart?

A. Restart from beginning
B. You can resume them, if you flag the "resume on failure" option before uploading.
C. Resume on failure
D. Depends on the file size

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which of the following cannot be used in Amazon EC2 to control who has access to specific Amazon EC2 instances?

A. Security Groups
B. IAM System
C. SSH keys
D. Windows passwords

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://blogs.aws.amazon.com/security/post/Tx29HCT3ABL7LP3/Resource-level-Permissions-for-EC2-Controlling- Management-Access-on-Specific-Ins

QUESTION 131
Fill in the blanks: _____ let you categorize your EC2 resources in different ways, for example, by purpose, owner, or environment.

A. wildcards
B. pointers
C. Tags
D. special filters

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
How can I change the security group membership for interfaces owned by other AWS, such as Elastic Load Balancing?

A. By using the service specific console or API\CLI commands
B. None of these
C. Using Amazon EC2 API/CLI
D. using all these methods

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-security-groups.html

Security Groups for Load Balancers in a VPC

When you use the AWS Management Console to create a load balancer in a VPC, you can choose an existing security group for the VPC or create a new security group for the VPC. If you choose an existing security group, it must allow traffic in both directions to the listener and health check ports for the load balancer. If you choose to create a security group, the console automatically adds rules to allow all traffic on these ports.

[Nondefault VPC] If you use the AWS CLI or API create a load balancer in a nondefault VPC, but you don't specify a security group, your load balancer is automatically associated with the default security group for the VPC.

[Default VPC] If you use the AWS CLI or API to create a load balancer in your default VPC, you can't choose an existing security group for your load balancer. Instead, Elastic Load Balancing provides a security group with rules to allow all traffic on the ports specified for the load balancer. Elastic Load Balancing creates only one such security group per AWS account, with a name of the form default_elb_*id* (for example, `default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE`). Subsequent load balancers that you create in the default VPC also use this security group. Be sure to review the security group rules to ensure that they allow traffic on the listener and health check ports for the new load balancer. When you delete your load balancer, this security group is not deleted automatically.

If you add a listener to an existing load balancer, you must review your security groups to ensure they allow traffic on the new listener port in both directions.

QUESTION 133
What is the maximum write throughput I can provision for a single Dynamic DB table?

A. 1,000 write capacity units
B. 100,000 write capacity units
C. Dynamic DB is designed to scale without limits, but if you go beyond 10,000 you have to contact AWS first.
D. 10,000 write capacity units

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/dynamodb/faqs/

Q: Is there a limit to how much throughput I can get out of a single table?

No, you can increase the throughput you have provisioned for your table using UpdateTable API or in the AWS Management Console. DynamoDB is able to operate at massive scale and there is no theoretical limit on the maximum throughput you can achieve. DynamoDB automatically divides your table across multiple partitions, where each partition is an independent parallel computation unit. DynamoDB can achieve increasingly high throughput rates by adding more partitions.

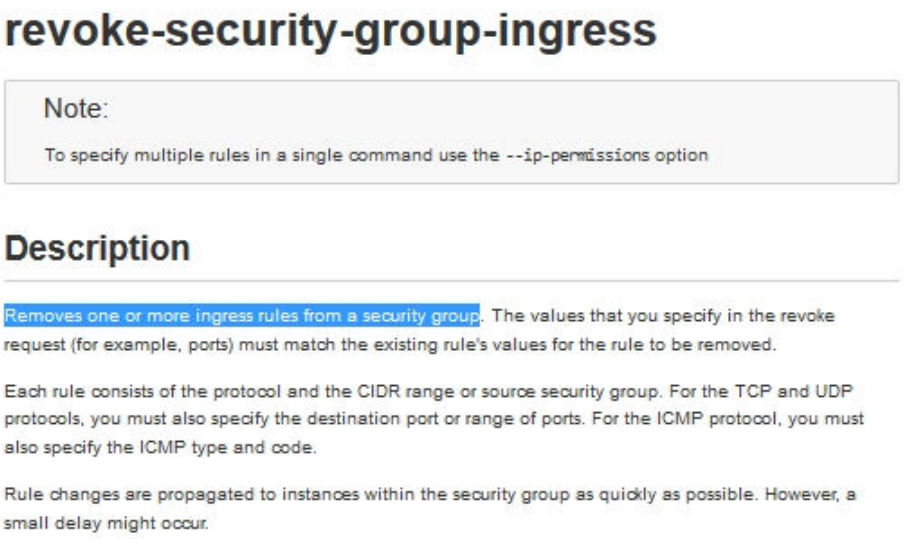
If you wish to exceed throughput rates of 10,000 writes/second or 10,000 reads/second, you must first contact Amazon through this online form.

QUESTION 134
What does the following command do with respect to the Amazon EC2 security groups?
ec2-revoke RevokeSecurityGroupIngress

A. Removes one or more security groups from a rule.
B. Removes one or more security groups from an Amazon EC2 instance.
C. Removes one or more rules from a security group.
D. Removes a security group from our account.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Removes one or more ingress rules from a security group. The values that you specify in the revoke request (for example, ports) must match the existing rule's values for the rule to be removed. http://docs.aws.amazon.com/cli/latest/reference/ec2/revoke-security-group-ingress.html



revoke-security-group-ingress

Note:

To specify multiple rules in a single command use the `--ip-permissions` option

Description

Removes one or more ingress rules from a security group. The values that you specify in the revoke request (for example, ports) must match the existing rule's values for the rule to be removed.

Each rule consists of the protocol and the CIDR range or source security group. For the TCP and UDP protocols, you must also specify the destination port or range of ports. For the ICMP protocol, you must also specify the ICMP type and code.

Rule changes are propagated to instances within the security group as quickly as possible. However, a small delay might occur.

QUESTION 135
Can a 'user' be associated with multiple AWS accounts?

A. No
B. Yes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
True or False: Manually created DB Snapshots are deleted after the DB Instance is deleted.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you choose not to create a final DB snapshot, you will not be able to later restore the DB instance to its final state. When you delete a DB instance, all automated backups are deleted and cannot be recovered. Manual DB snapshots of the instance are not deleted.

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_DeleteInstance.html

QUESTION 137
Can I move a Reserved Instance from one Region to another?

A. No
B. Only if they are moving into GovCloud
C. Yes
D. Only if they are moving to US East from another region

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
What is Amazon Glacier?

A. You mean Amazon "Iceberg": it's a low-cost storage service.
B. A security tool that allows to "freeze" an EBS volume and perform computer forensics on it.
C. A low-cost storage service that provides secure and durable storage for data archiving and backup.
D. It's a security tool that allows to "freeze" an EC2 instance and perform computer forensics on it.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Amazon Glacier is an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.

QUESTION 139
What is the durability of S3 RRS?

A. 99.99%
B. 99.95%
C. 99.995%
D. 99.999999999%

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RRS = **R**educed **R**edundancy **S**torage

	Standard	Standard - Infrequent Access	Reduced Redundancy Storage
Durability	99.999999999%	99.999999999%	99.99%

QUESTION 140
What does specifying the mapping /dev/sdc=none when launching an instance do?

A. Prevents /dev/sdc from creating the instance.
B. Prevents /dev/sdc from deleting the instance.
C. Set the value of /dev/sdc to 'zero'.
D. Prevents /dev/sdc from attaching to the instance.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
none - Suppresses an existing mapping of the device from the AMI used to launch the instance.
For example: “/dev/sdc=none”.
http://docs.aws.amazon.com/AWSEC2/latest/CommandLineReference/ApiReference-cmd-RegisterImage.html

QUESTION 141
Is Federated Storage Engine currently supported by Amazon RDS for MySQL?

A. Only for Oracle RDS instances
B. No
C. Yes
D. Only in VPC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Is there a limit to how many groups a user can be in?

A. Yes for all users
B. Yes for all users except root
C. No
D. Yes unless special permission granted

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Currently you can request to increase the limit on users per AWS account, groups per AWS account, roles per AWS account, instance profiles per AWS account, and server certificates per
AWS account.
This never states “groups a user can be in”

QUESTION 143
True or False: When you perform a restore operation to a point in time or from a DB Snapshot, a new DB Instance is created with a new endpoint.

A. FALSE
B. TRUE

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Restoring From a DB Snapshot
Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. You can create a DB instance by restoring from this
DB snapshot. When you restore the DB instance, you provide the name of the DB snapshot to restore from, and then provide a name for the new DB instance that is created from the restore.
You cannot restore from a DB snapshot to an existing DB instance; a new DB instance is created when you restore.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html

QUESTION 144
A/An _____ acts as a firewall that controls the traffic allowed to reach one or more instances.

A. security group
B. ACL
C. IAM
D. Private IP Addresses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A security group acts as a virtual firewall that controls the traffic for one or more instances.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 145
Will my standby RDS instance be in the same Availability Zone as my primary?

A. Only for Oracle RDS types
B. Yes
C. Only if configured at launch
D. No

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146

While launching an RDS DB instance, on which page I can select the Availability Zone?

A. REVIEW
B. DB INSTANCE DETAILS
C. MANAGEMENT OPTIONS
D. ADDITIONAL CONFIGURATION

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DB Instance detail -You just enable that your DB instance can be deploy in Multi-AZ. However,
you select the availability zone (Which AZ will be for primary and which one will be for secondary) in Additional configuration.

QUESTION 147
What does the following command do with respect to the Amazon EC2 security groups?
ec2-create-group CreateSecurityGroup

A. Groups the user created security groups in to a new group for easy access.
B. Creates a new security group for use with your account.
C. Creates a new group inside the security group.
D. Creates a new rule inside the security group.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/CommandLineReference/ApiReference-cmd-CreateSecurityGroup.html page 125

QUESTION 148
In the Launch Db Instance Wizard, where can I select the backup and maintenance options?

A. Under DB INSTANCE DETAILS
B. Under REVIEW
C. Under MANAGEMENT OPTIONS
D. Under ENGINE SELECTION

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://awsdocs.s3.amazonaws.com/RDS/latest/rds-gsg.pdf

QUESTION 149
What happens to the data on an instance if the instance reboots (intentionally or unintentionally)?

A. Data will be lost
B. Data persists
C. Data may persist however cannot be sure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instance Store Lifetime
You can specify instance store volumes for an instance only when you launch it. 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 in the instance store is lost under the following circumstances:
The underlying disk drive fails
The instance stops
The instance terminates
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

QUESTION 150
How many types of block devices does Amazon EC2 support?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html 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)
A block device mapping defines the block devices (instance store volumes and EBS volumes) to attach to an instance.

Block Device Mapping Concepts

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:

- Instance store volumes (virtual devices whose underlying hardware is physically attached to the host computer for the instance)
- EBS volumes (remote storage devices)

QUESTION 151
Provisioned IOPS Costs: you are charged for the IOPS and storage whether or not you use them in a given month.

A. FALSE
B. TRUE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Volume storage for EBS Provisioned IOPS SSD (io1) volumes is charged by the amount you provision in GB per month, until you release the storage. With Provisioned IOPS SSD (io1) volumes, you are also charged by the amount you provision in IOPS (input/output operations per second) multiplied by the percentage of days you provision for the month. For example, if you provision a volume with 1000 IOPS, and keep this volume for 15 days in a 30 day month, then in a Region that charges $0.10 per provisioned IOPS-month, you would be charged $50 for the IOPS that you provision ($0.10 per provisioned IOPS-month * 1000 IOPS provisioned * 15 days/30). You will be charged for the IOPS provisioned on a volume even when the volume is detached from an instance.

QUESTION 152
IAM provides several policy templates you can use to automatically assign permissions to the groups you create. The _____ policy template gives the Admins group permission to access all account resources, except your AWS account information

A. Read Only Access
B. Power User Access
C. AWS Cloud Formation Read Only Access
D. Administrator Access

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS managed policies are designed to provide permissions for many common use cases. For example, there are AWS managed policies that define typical permissions for administrators (all access), for power users (all access except IAM), and for other various levels of access to AWS services. AWS managed policies make it easier for

you to assign appropriate permissions to users, groups, and roles than if you had to write the policies yourself.

http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html

QUESTION 153
While performing the volume status checks, if the status is insufficient-data, what does it mean?

A. the checks may still be in progress on the volume
B. the check has passed
C. the check has failed

Correct Answer: A
Section: (none)
Explanation

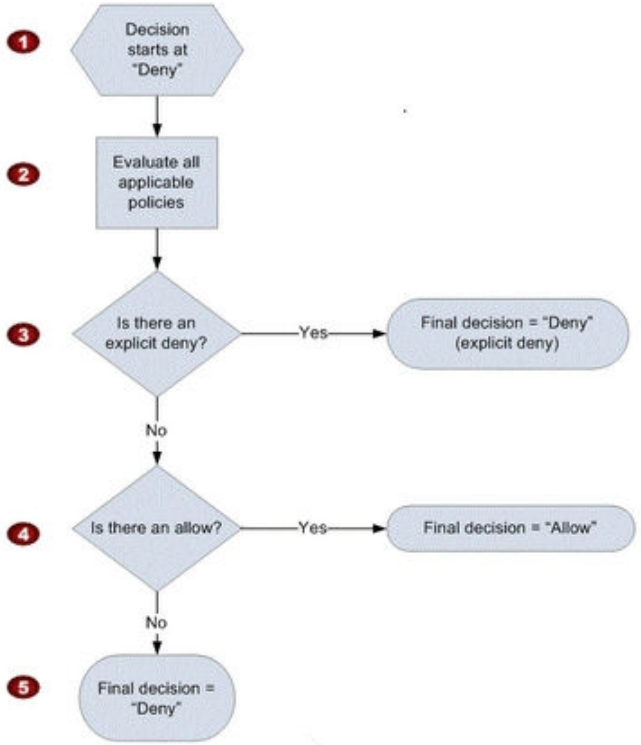
Explanation/Reference:
Explanation:
If the status is insufficient-data, the checks may still be in progress on the volume. You can view the results of volume status checks to identify any impaired volumes and take any necessary actions. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html#monitoring-volume-checks

QUESTION 154
IAM's Policy Evaluation Logic always starts with a default _____ for every request, except for those that use the AWS account's root security credentials b

A. Permit
B. Deny
C. Cancel

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html



1. The decision starts by assuming that the request will be denied.

QUESTION 155
By default, when an EBS volume is attached to a Windows instance, it may show up as any drive letter on the instance. You can change the settings of the _____ Service to set the drive letters of the EBS volumes per your specifications.

A. EBSConfig Service
B. AMIConfig Service
C. Ec2Config Service
D. Ec2-AMIConfig Service

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Ec2Config Service is like sysprep and used specifically for windows instances.. You can change parameters in OS before launching.

QUESTION 156
For each DB Instance class, what is the maximum size of associated storage capacity?

A. 5GB
B. 6TB
C. 2TB
D. 500GB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"You can now create MySQL, PostgreSQL, and Oracle RDS database instances with up to 6TB of storage and SQL Server RDS database instances with up to 4TB of storage when using the Provisioned IOPS and General Purpose (SSD) storage types. Existing MySQL, PostgreSQL, and Oracle RDS database instances can be scaled to these new database storage limits without any downtime."

QUESTION 157
SQL Server _____ store logins and passwords in the master database.

A. can be configured to but by default does not
B. doesn't
C. does

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are two authentications
Windows authentication
The credentials for which are not stored in SQL Server database and managed by windows/AD. There would be entry for windows authenticated logins in master database with respective SID but password would be with Active directory.
SQL Server authentication.
For 2nd we have password stored in hash format you can see it from sys.sql_logins. The information about SQL server logins are stored in master database and each login has SID receptive to it. Only SA login has same SID no matter what server it is. That is why when you move database by backup restore mechanism users are moved not logins and you finally have to create logins(if already not there) and map it to users. This is generally called as troubleshooting orphaned users

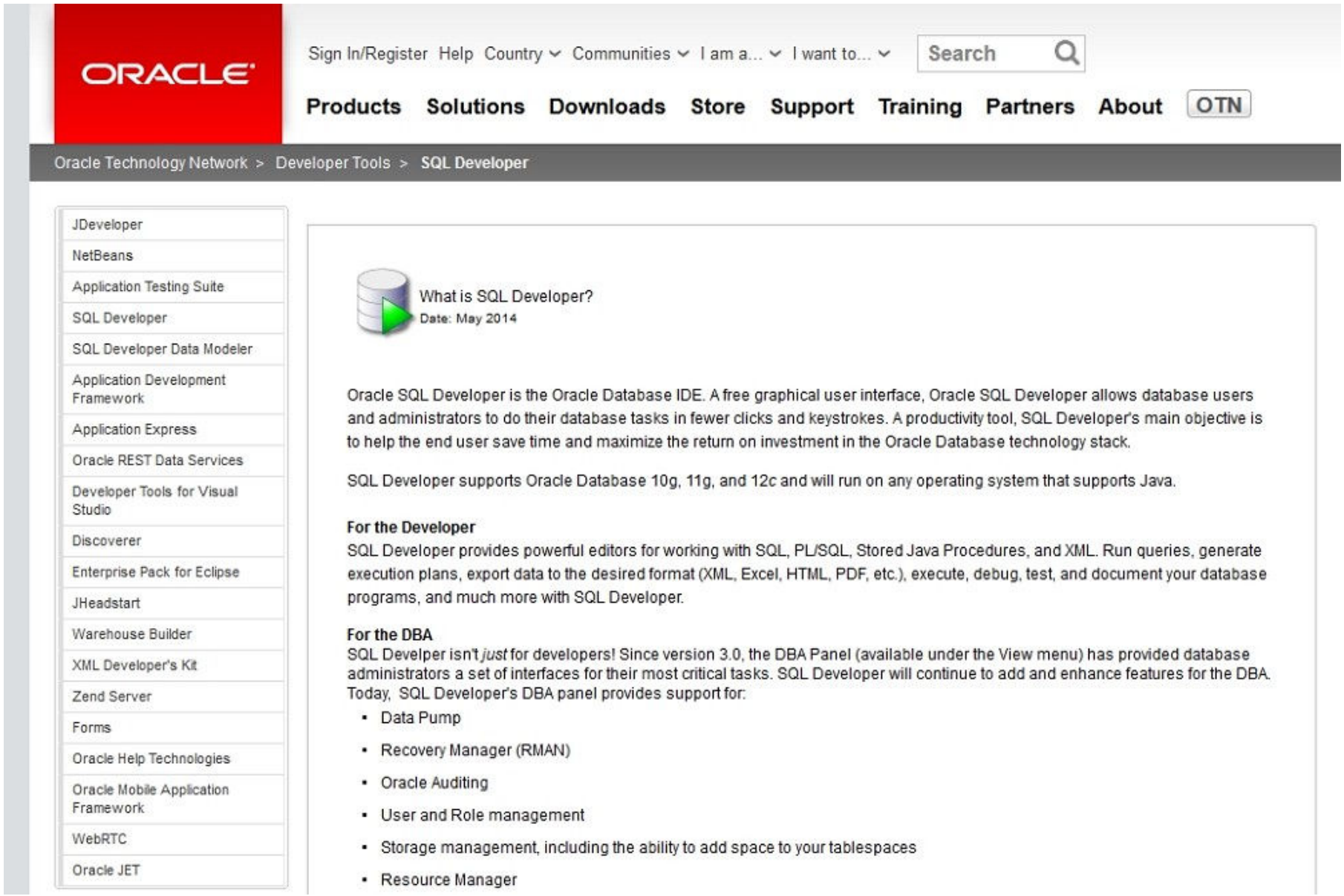
QUESTION 158
What is Oracle SQL Developer?

A. An AWS developer who is an expert in Amazon RDS using both the Oracle and SQL Server DB engines
B. A graphical Java tool distributed without cost by Oracle.

C. It is a variant of the SQL Server Management Studio designed by Microsoft to support Oracle DBMS functionalities
D. A different DBMS released by Microsoft free of cost

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://www.oracle.com/technetwork/developer-tools/sql-developer/what-is-sqldev-093866.html



QUESTION 159
Does Amazon RDS allow direct host access via Telnet, Secure Shell (SSH), or Windows Remote Desktop Connection?

A. Yes
B. No
C. Depends on if it is in VPC or not

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

In order to deliver a managed service experience, Amazon RDS does not provide shell access to DB instances, and it restricts access to certain system procedures and tables that require advanced privileges. Amazon RDS supports access to databases on a DB instance using any standard SQL client application such as Microsoft SQL Server Management Studio. Amazon RDS does not allow direct host access to a DB instance via Telnet, Secure Shell (SSH), or Windows Remote Desktop Connection. When you create a DB instance, you are assigned to the *db_owner* role for all databases on that instance, and you will have all database-level permissions except for those that are used for backups (Amazon RDS manages backups for you).

QUESTION 160
To view information about an Amazon EBS volume, open the Amazon EC2 console at https://console.aws.amazon.com/ec2/, click _____ in the Navigation pane.

A. EBS
B. Describe
C. Details
D. Volumes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-describing-volumes.html

Viewing Volume Information

You can view descriptive information for your Amazon EBS volumes in a selected region at a time in the AWS Management Console. You can also view detailed information about a single volume, including the size, volume type, whether or not the volume is encrypted, which master key was used to encrypt the volume, and the specific instance to which the volume is attached.

To view information about an EBS volume using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Volumes**.
3. To view more information about a volume, select it.

QUESTION 161
Using Amazon IAM, can I give permission based on organizational groups?

A. Yes but only in certain cases
B. No
C. Yes always

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.
http://docs.aws.amazon.com/IAM/latest/UserGuide/id.html

QUESTION 162
While creating the snapshots using the API, which Action should I be using?

A. MakeSnapShot
B. FreshSnapshot
C. DeploySnapshot
D. CreateSnapshot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 163
What is an isolated database environment running in the cloud (Amazon RDS) called?

A. DB Instance
B. DB Server
C. DB Unit
D. DB Volume

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
While signing in REST/ Query requests, for additional security, you should transmit your requests using Secure Sockets Layer (SSL) by using _____

A. HTTP
B. Internet Protocol Security(IPsec)
C. TLS (Transport Layer Security)
D. HTTPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
What happens to the I/O operations while you take a database snapshot?

A. I/O operations to the database are suspended for a few minutes while the backup is in progress.
B. I/O operations to the database are sent to a Replica (if available) for a few minutes while the backup is in progress.
C. I/O operations will be functioning normally
D. I/O operations to the database are suspended for an hour while the backup is in progress

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Creating this DB snapshot on a Single-AZ DB instance results in a brief I/O suspension that typically lasting no more than a few minutes. Multi-AZ DB instances are not affected by this I/O
suspension since the backup is taken on the standby.

QUESTION 166
Read Replicas require a transactional storage engine and are only supported for the _____ storage engine

A. OracleISAM
B. MSSQLDB
C. InnoDB
D. MyISAM

Correct Answer: C
Section: (none)
Explanation

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

- Using a non-transactional storage engine such as MyISAM. Read replicas require a transactional storage engine. Replication is only supported for the InnoDB storage engine on MySQL and the XtraDB storage engine on MariaDB.

QUESTION 167
When running my DB Instance as a Multi-AZ deployment, can I use the standby for read or write operations?

A. Yes
B. Only with MSSQL based RDS
C. Only for Oracle RDS instances
D. No

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Q: When running my DB instance as a Multi-AZ deployment, can I use the standby for read or write operations?

No, the standby replica cannot serve read requests. Multi-AZ deployments are designed to provide enhanced database availability and durability, rather than read scaling benefits. As such, the feature uses synchronous replication between primary and standby. Our implementation makes sure the primary and the standby are constantly in sync, but precludes using the standby for read or write operations. If you are interested in a read scaling solution, please see the FAQs on Read Replicas.

QUESTION 168
When should I choose Provisioned IOPS over Standard RDS storage?

A. If you have batch-oriented workloads
B. If you use production online transaction processing (OLTP) workloads.
C. If you have workloads that are not sensitive to consistent performance

Correct Answer: B
Section: (none)
Explanation

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

Amazon RDS provisions that IOPS rate and storage for the lifetime of the DB instance or until you change it. Provisioned IOPS storage is optimized for I/O intensive, online transaction processing (OLTP) workloads that have consistent performance requirements. Provisioned IOPS helps performance tuning.

QUESTION 169
In the 'Detailed' monitoring data available for your Amazon EBS volumes, Provisioned IOPS volumes automatically send _____ minute metrics to Amazon CloudWatch.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
What is the minimum charge for the data transferred between Amazon RDS and Amazon EC2 Instances in the same Availability Zone?

A. USD 0.10 per GB
B. No charge. It is free.
C. USD 0.02 per GB

D. USD 0.01 per GB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For data transferred between an Amazon EC2 instance and Amazon RDS DB Instance in different Availability Zones of the same Region, there is no Data Transfer charge for traffic in or out of the Amazon RDS DB Instance.
Reference: https://aws.amazon.com/rds/pricing/

QUESTION 171
Are Reserved Instances available for Multi-AZ Deployments?

A. Only for Cluster Compute instances
B. Yes for all instance types
C. Only for M3 instance types
D. No

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 172
Which service enables AWS customers to manage users and permissions in AWS?

A. AWS Access Control Service (ACS)
B. AWS Identity and Access Management (IAM)
C. AWS Identity Manager (AIM)
D. AWS Security Groups

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
Which Amazon Storage behaves like raw, unformatted, external block devices that you can attach to your instances?

A. None of these.
B. Amazon Instance Storage
C. Amazon EBS
D. All of these

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Which Amazon service can I use to define a virtual network that closely resembles a traditional data center?

A. Amazon VPC
B. Amazon ServiceBus
C. Amazon EMR
D. Amazon RDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
What is the command line instruction for running the remote desktop client in Windows?

A. desk.cpl
B. mstsc

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Amazon RDS automated backups and DB Snapshots are currently supported for only the _____ storage engine

A. MyISAM
B. InnoDB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_MySQL.html

QUESTION 177
MySQL installations default to port _____.

A. 3306
B. 443
C. 80
D. 1158

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 178
If you have chosen Multi-AZ deployment, in the event of a planned or unplanned outage of your primary DB Instance, Amazon RDS automatically switches to the standby replica. The automatic failover mechanism simply changes the _____ record of the main DB Instance to point to the standby DB Instance.

A. DNAME
B. CNAME
C. TXT
D. MX

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"When failing over, Amazon RDS simply flips the canonical name record (CNAME) for your DB Instance to point at the standby, which is in turn promoted to become the new primary"
https://aws.amazon.com/rds/faqs/

QUESTION 179
If I modify a DB Instance or the DB parameter group associated with the instance, should I reboot the instance for the changes to take effect?

A. No
B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
If I want to run a database in an Amazon instance, which is the most recommended Amazon storage option?

A. Amazon Instance Storage
B. Amazon EBS
C. You can't run a database inside an Amazon instance.
D. Amazon S3

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 181
In regards to IAM you can edit user properties later, but you cannot use the console to change the _____.

A. user name
B. password
C. default group

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Can I test my DB Instance against a new version before upgrading?

A. No
B. Yes

C. Only in VPC

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 183
True or False: If you add a tag that has the same key as an existing tag on a DB Instance, the new value overwrites the old value.

A. FALSE
B. TRUE

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 184
Can I use Provisioned IOPS with VPC?

A. Only Oracle based RDS
B. No
C. Only with MSSQL based RDS
D. Yes for all RDS instances

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Making your snapshot public shares all snapshot data with everyone. Can the snapshots with AWS Marketplace product codes be made public?

A. No
B. Yes

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
"Making your snapshot public shares all snapshot data with everyone; however, snapshots with AWS Marketplace product codes cannot be made public. Encrypted snapshots cannot be shared between accounts or made public." http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html
"This is not a valid option for encrypted snapshots or snapshots with AWS Marketplace product codes."

QUESTION 186
Fill in the blanks: "To ensure failover capabilities, consider using a _____ for incoming traffic on a network interface".

A. primary public IP
B. secondary private IP
C. secondary public IP
D. add on secondary IP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To ensure failover capabilities, consider using a secondary private IP for incoming traffic on an elastic network interface. In the event of an instance failure, you can move the interface and/or secondary private IP address to a standby instance

QUESTION 187
If I have multiple Read Replicas for my master DB Instance and I promote one of them, what happens to the rest of the Read Replicas?

A. The remaining Read Replicas will still replicate from the older master DB Instance
B. The remaining Read Replicas will be deleted
C. The remaining Read Replicas will be combined to one read replica

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If a source DB instance has several Read Replicas, promoting one of the Read Replicas to a DB instance has no effect on the other replicas.

QUESTION 188
What does Amazon CloudFormation provide?

A. The ability to setup Autoscaling for Amazon EC2 instances.
B. None of these.

C. A templated resource creation for Amazon Web Services.
D. A template to map network resources for Amazon Web Services.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.

QUESTION 189
Can I encrypt connections between my application and my DB Instance using SSL?

A. No
B. Yes
C. Only in VPC
D. Only in certain regions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
What are the four levels of AWS Premium Support?

A. Basic, Developer, Business, Enterprise
B. Basic, Startup, Business, Enterprise
C. Free, Bronze, Silver, Gold
D. All support is free

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q: How are the enhanced AWS Support tiers different from Basic Support? AWS Basic Support offers all AWS customers access to our Resource Center, Service Health Dashboard, Product FAQs, Discussion Forums, and Support for Health Checks at no additional charge. Customers who desire a deeper level of support can subscribe to AWS Support at the Developer, Business, or Enterprise level.

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

QUESTION 191
What can I access by visiting the URL: http://status.aws.amazon.com/?

A. Amazon Cloud Watch
B. Status of the Amazon RDS DB
C. AWS Service Health Dashboard
D. AWS Cloud Monitor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Please select the Amazon EC2 resource which cannot be tagged.

A. images (AMIs, kernels, RAM disks)
B. Amazon EBS volumes
C. Elastic IP addresses
D. VPCs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html#tag-restrictions

Resource	Tagging support	Tagging restrictions
AMI	Yes	None
Bundle task	No	
Customer gateway	Yes	None
Dedicated Host	No	
DHCP option	Yes	None
EBS volume	Yes	None
Instance store volume	No	
Elastic IP	No	
Egress-only Internet gateway	No	
Instance	Yes	None
Internet gateway	Yes	None
Key pair	No	
NAT gateway	No	
Network ACL	Yes	None
Network interface	Yes	None
Placement group	No	
Reserved Instance	Yes	None

QUESTION 193
Can the string value of 'Key' be prefixed with :aws:"?

A. Only in GovCloud
B. Only for S3 not EC2
C. Yes
D. No

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:
"The tag key is the required name of the tag. The string value can be from 1 to 128 Unicode characters in length and cannot be prefixed with "aws:" or "rds:"."
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Tagging.html
http://docs.aws.amazon.com/cli/latest/reference/rds/list-tags-for-resource.html

QUESTION 194
Because of the extensibility limitations of striped storage attached to Windows Server, Amazon RDS does not currently support increasing storage on a _____ DB Instance.

A. SQL Server
B. MySQL
C. Oracle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
Through which of the following interfaces is AWS Identity and Access Management available?

A) AWS Management Console
B) Command line interface (CLI)
C) IAM Query API
D) Existing libraries

A. Only through Command line interface (CLI)
B. A, B and C
C. A and C
D. All of the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Accessing IAM:
1 - AWS Management Console
2 - AWS Command Line Tools
3 - AWS SDKs (i.e. Existing libraries)
4 - IAM HTTPS API

http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html#intro-accessing

QUESTION 196
Select the incorrect statement

A. In Amazon EC2, the private IP addresses only returned to Amazon EC2 when the instance is stopped or terminated
B. In Amazon VPC, an instance retains its private IP addresses when the instance is stopped.
C. In Amazon VPC, an instance does NOT retain its private IP addresses when the instance is stopped.
D. In Amazon EC2, the private IP address is associated exclusively with the instance for its lifetime

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A private IP address remains associated with the network interface when the instance is stopped and restarted, and is released when the instance is terminated.

QUESTION 197
How are the EBS snapshots saved on Amazon S3?

A. Exponentially
B. Incrementally
C. EBS snapshots are not stored in the Amazon S3
D. Decrementally

Correct Answer: B
Section: (none)
Explanation

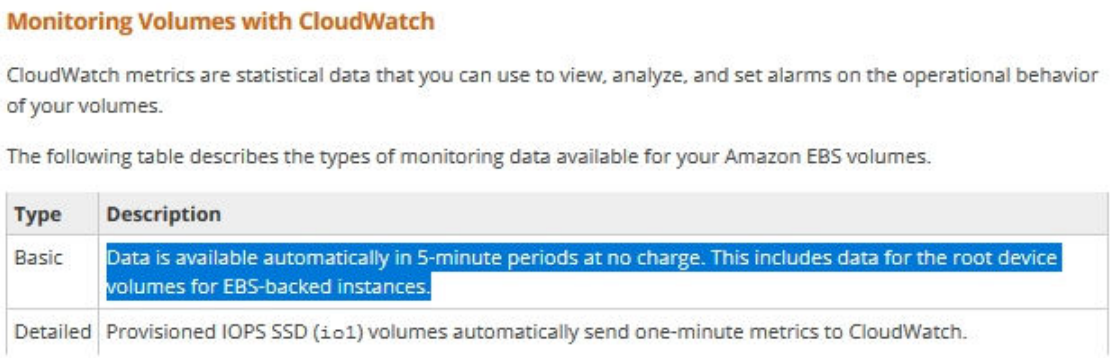
Explanation/Reference:

QUESTION 198
What is the type of monitoring data (for Amazon EBS volumes) which is available automatically in 5-minute periods at no charge called?

A. Basic
B. Primary
C. Detailed
D. Local

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Monitoring Volumes with CloudWatch
CloudWatch metrics are statistical data that you can use to view, analyze, and set alarms on the operational behavior of your volumes. The following table describes the types of monitoring data available for your Amazon EBS volumes:
Basic
Data is available automatically in 5-minute periods at no charge. This includes data for the root device volumes for EBS- backed instances.
Detailed
Provisioned IOPS SSD (io1) volumes automatically send one-minute metrics to CloudWatch. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html



Monitoring Volumes with CloudWatch

CloudWatch metrics are statistical data that you can use to view, analyze, and set alarms on the operational behavior of your volumes.

The following table describes the types of monitoring data available for your Amazon EBS volumes.

Type	Description
Basic	Data is available automatically in 5-minute periods at no charge. This includes data for the root device volumes for EBS-backed instances.
Detailed	Provisioned IOPS SSD (`io1`) volumes automatically send one-minute metrics to CloudWatch.

QUESTION 199
What happens when you create a topic on Amazon SNS?

A. The topic is created, and it has the name you specified for it.
B. An ARN (Amazon Resource Name) is created.
C. You can create a topic on Amazon SQS, not on Amazon SNS.
D. This question doesn't make sense.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
Can I delete a snapshot of the root device of an EBS volume used by a registered AMI?

A. Only via API
B. Only via Console
C. Yes

D. No

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Note that you can't delete a snapshot of the root device of an EBS volume used by a registered AMI. You must first deregister the AMI before you can delete the snapshot.
Source: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-snapshot.html

QUESTION 201
What is the maximum response time for a Business level Premium Support case?

A. 120 seconds
B. 1 hour
C. 10 minutes
D. 12 hours

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/premiumsupport/features/

QUESTION 202
The _____ service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console.

A. Amazon RDS
B. AWS Integrity Management
C. AWS Identity and Access Management
D. Amazon EMR

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/documentation/iam/?nc1=h_ls

QUESTION 203
True or False: Without IAM, you cannot control the tasks a particular user or system can do and what AWS resources they might use.

A. FALSE
B. TRUE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-setup.html

QUESTION 204
When you use the AWS Management Console to delete an IAM user, IAM also deletes any signing certificates and any access keys belonging to the user.

A. FALSE
B. This is configurable
C. TRUE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you use the AWS Management Console to delete an IAM user, IAM automatically deletes the following information for you:
The user
Any group memberships -- that is, the user is removed from any IAM groups that the user was a member of:
Any password associated with the user
Any access keys belonging to the user
All inline policies embedded in the user (policies that are applied to a user via group permissions are not affected) Note!
Any managed policies attached to the user are detached from the user when the user is deleted. Managed policies are not deleted when you delete a user.
Any associated MFA device
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_manage.html#id_users_deleting_console

QUESTION 205
When automatic failover occurs, Amazon RDS will emit a DB Instance event to inform you that automatic failover occurred. You can use the _____ to return information about events related to your DB Instance

A. FetchFailure
B. DescriveFailure
C. DescribeEvents
D. FetchEvents

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Q: Will I be alerted when automatic failover occurs?
Yes, Amazon RDS will emit a DB Instance event to inform you that automatic failover occurred. You can use the DescribeEvents to return information about events related to your DB Instance, or click the "DB Events" section of the AWS Management Console
https://aws.amazon.com/rds/faqs/

QUESTION 206
What is the default maximum number of MFA devices in use per AWS account (at the root account level)?

A. 1
B. 5
C. 15
D. 10

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html

QUESTION 207
Do the Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

A. Only if instructed to when created
B. Yes
C. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data persistence
An EBS volume is off-instance storage that can persist independently from the life of an instance. You continue to pay for the volume usage as long as the data persists.

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

QUESTION 208
Can we attach an EBS volume to more than one EC2 instance at the same time?

A. Yes.
B. No
C. Only EC2-optimized EBS volumes.
D. Only in read mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
EBS is network attached storage that can only be attached to one instance at a time https://aws.amazon.com/ebs/getting-started/

QUESTION 209
Select the correct set of options. These are the initial settings for the default security group:

A. Allow no inbound traffic, Allow all outbound traffic and Allow instances associated with this security group to talk to each other
B. Allow all inbound traffic, Allow no outbound traffic and Allow instances associated with this security group to talk to each other
C. Allow no inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other
D. Allow all inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#default-security-group A default security group is named default, and it has an ID assigned by AWS. The following are the initial settings for each default security group:
Allow inbound traffic only from other instances associated with the default security group Allow all outbound traffic from the instance
The default security group specifies itself as a source security group in its inbound rules. This is what allows instances associated with the default security group to communicate with other instances associated with the default security group.

Default Security Groups

Your AWS account automatically has a *default security group* per VPC and per region for EC2-Classic. If you don't specify a security group when you launch an instance, the instance is automatically associated with the default security group.

A default security group is named `default`, and it has an ID assigned by AWS. The following are the default rules for each default security group:

- Allows all inbound traffic from other instances associated with the default security group (the security group specifies itself as a source security group in its inbound rules)
- Allows all outbound traffic from the instance.

You can add or remove the inbound rules for any default security group. You can add or remove outbound rules for any VPC default security group.

You can't delete a default security group. If you try to delete the EC2-Classic default security group, you'll get the following error: `Client.InvalidGroup.Reserved: The security group 'default' is reserved.` If you try to delete a VPC default security group, you'll get the following error: `Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user.`

QUESTION 210
What does Amazon Route53 provide?

A. A global Content Delivery Network.
B. None of these.
C. A scalable Domain Name System.
D. An SSH endpoint for Amazon EC2.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/route53/

QUESTION 211
What does Amazon ElastiCache provide?

A. A service by this name doesn't exist. Perhaps you mean Amazon CloudCache.
B. A virtual server with a huge amount of memory.
C. A managed In-memory cache service.
D. An Amazon EC2 instance with the Memcached software already pre-installed.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
How many Elastic IP by default in Amazon Account?

A. 1 Elastic IP
B. 3 Elastic IP
C. 5 Elastic IP
D. 0 Elastic IP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"By default, all AWS accounts are limited to 5 Elastic IP addresses, because public (IPv4) Internet addresses are a scarce public resource."
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

QUESTION 213
What is a Security Group?

A. None of these.
B. A list of users that can access Amazon EC2 instances.
C. An Access Control List (ACL) for AWS resources.
D. A firewall for inbound traffic, built-in around every Amazon EC2 instance.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

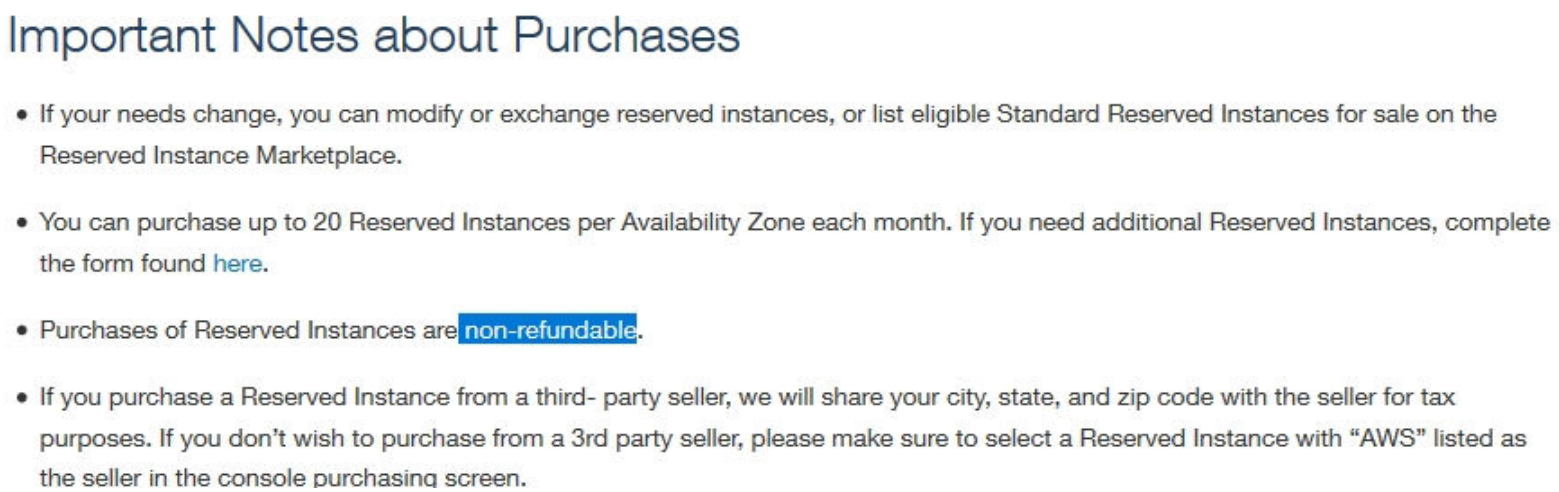
QUESTION 214
The one-time payment for Reserved Instances is _____ refundable if the reservation is cancelled.

A. always
B. in some circumstances

C. never

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
the one-time fee is non-refundable.
https://aws.amazon.com/ec2/purchasing-options/reserved-instances/buyer/



QUESTION 215
Please select the Amazon EC2 resource which can be tagged.

A. key pairs
B. Elastic IP addresses
C. placement groups
D. Amazon EBS snapshots

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Placement group and Elastic IP cannot be tagged.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html Snapshots can be tagged: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

Resource	Tagging support	Tagging restrictions
AMI	Yes	None
Bundle task	No	
Customer gateway	Yes	None
Dedicated Host	No	
DHCP option	Yes	None
EBS volume	Yes	None
Instance store volume	No	
Elastic IP	No	
Egress-only Internet gateway	No	
Instance	Yes	None
Internet gateway	Yes	None
Key pair	No	
NAT gateway	No	
Network ACL	Yes	None
Network interface	Yes	None
Placement group	No	
Reserved Instance	Yes	None
Reserved Instance listing	No	
Route table	Yes	None
Spot instance request	Yes	None
Security group - EC2-Classic	Yes	None
Security group - VPC	Yes	None
Snapshot	Yes	None

QUESTION 216
If an Amazon EBS volume is the root device of an instance, can I detach it without stopping the instance?

A. Yes but only if Windows instance
B. No
C. Yes
D. Yes but only if a Linux instance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"If an EBS volume is the root device of an instance, you must stop the instance before you can detach the volume." http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-detaching-volume.html

QUESTION 217
If you are using Amazon RDS Provisioned IOPS storage with MySQL and Oracle database engines, you can scale the throughput of your database Instance by specifying the IOPS rate from _____.

A. 1,000 to 100, 000
B. 100 to 1, 000
C. 10, 000 to 100, 000
D. 1, 000 to 10, 000

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you are using RDS Provisioned IOPS, you can also scale the throughput of your DB Instance by specifying the IOPS rate from 1,000 IOPS to 10,000 IOPS in 1,000 IOPS
https://aws.amazon.com/rds/mysql/



QUESTION 218
Every user you create in the IAM system starts with _____.

A. full permissions
B. no permissions
C. partial permissions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Permissions let you specify who has access to AWS resources, and what actions they can perform on those resources.
Every IAM user **starts with no permissions.**
http://docs.aws.amazon.com/IAM/latest/UserGuide/access_permissions.html#NoDefaultPermissions

QUESTION 219
Which of the following statements are true about Amazon Route 53 resource records? (Choose two.)

A. An Alias record can map one DNS name to another Amazon Route 53 DNS name.
B. A CNAME record can be created for your zone apex.
C. An Amazon Route 53 CNAME record can point to any DNS record hosted anywhere.
D. TTL can be set for an Alias record in Amazon Route 53.
E. An Amazon Route 53 Alias record can point to any DNS record hosted anywhere.

Correct Answer: AC
Section: (none)
Explanation

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

QUESTION 220
A_____ is an individual, system, or application that interacts with AWS programmatically.

A. user
B. AWS Account
C. Group
D. Role

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q: What is a user?
A user is a unique identity recognized by AWS services and applications. Similar to a login user in an operating system like Windows or UNIX, a user has a unique name and can identify itself

using familiar security credentials such as a password or access key. A user can be an individual,
system, or application requiring access to AWS services. IAM supports users (referred to as “IAM users”) managed in AWS’s identity management system, and it also enables you to grant access to AWS resources for users managed outside of AWS in your corporate directory (referred to as “federated users”).

QUESTION 221
Select the correct statement:

A. You don't need not specify the resource identifier while stopping a resource
B. You can terminate, stop, or delete a resource based solely on its tags
C. You can't terminate, stop, or delete a resource based solely on its tags
D. You don't need to specify the resource identifier while terminating a resource

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can’t terminate, stop, or delete a resource based solely on its tags; you must specify the resource identifier.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html#tag-restrictions

QUESTION 222
Amazon EC2 has no Amazon Resource Names (ARNs) because you can't specify a particular Amazon EC2 resource in an IAM policy.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://blogs.aws.amazon.com/security/post/Tx29HCT3ABL7LP3/Resource-level-Permissions-for-EC2-Controlling- Management-Access-on-Specific-Ins

QUESTION 223
Can I initiate a "forced failover" for my MySQL Multi-AZ DB Instance deployment?

A. Only in certain regions
B. Only in VPC
C. Yes
D. No

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If your DB instance is a Multi-AZ deployment, **you can force a failover from one availability zone to another when you select the Reboot option**. When you force a failover of your DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone and updates the DNS record for the DB instance to point to the standby DB instance. As a result, you will need to clean up and re-establish any existing connections to your DB instance. Reboot with failover is beneficial when you want to simulate a failure of a DB instance for testing, or restore operations to the original AZ after a failover occurs.
Source: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RebootInstance.html

QUESTION 224
A group can contain many users. Can a user belong to multiple groups?

A. Yes always
B. No
C. Yes but only if they are using two factor authentication
D. Yes but only in VPC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A group can contain many users, and a user can belong to multiple groups.
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

QUESTION 225
Is the encryption of connections between my application and my DB Instance using SSL for the MySQL server engines available?

A. Yes
B. Only in VPC
C. Only in certain regions
D. No

Correct Answer: A
Section: (none)
Explanation

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

Q: Can I encrypt connections between my application and my DB Instance using SSL?

Yes, this option is currently supported for the MySQL, MariaDB, SQL Server, PostgreSQL, and Oracle engines.

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.

QUESTION 226
Which AWS instance address has the following characteristics? :"If you stop an instance, its Elastic IP address is unmapped, and you must remap it when you restart the instance."

A. VPC Addresses
B. EC2 Addresses
C. Both A and B
D. None of the above

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

Stopping an instance

EC2-Classic
If you stop an instance, its Elastic IP address is disassociated, and you must reassociate the Elastic IP address when you restart the instance.

EC2-VPC
If you stop an instance, its Elastic IP address remains associated.

QUESTION 227
True or False: Common points of failures like generators and cooling equipment are shared across Availability Zones.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
Please select the most correct answer regarding the persistence of the Amazon Instance Store

A. The data on an instance store volume persists only during the life of the associated Amazon EC2 instance
B. The data on an instance store volume is lost when the security group rule of the associated instance is changed.
C. The data on an instance store volume persists even after associated Amazon EC2 instance is deleted

Correct Answer: A
Section: (none)
Explanation

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

Amazon EC2 Instance Store

Many instances can access storage from disks that are physically attached to the host computer. This disk storage is referred to as *instance store*. Instance store provides temporary block-level storage for instances. The data on an instance store volume persists only during the life of the associated instance; if you stop or terminate an instance, any data on instance store volumes is lost. For more information, see Amazon EC2 Instance Store.

QUESTION 229
Multi-AZ deployment _____ supported for Microsoft SQL Server DB Instances.

A. is not currently
B. is as of 2013
C. is planned to be in 2014
D. will never be

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://aws.amazon.com/about-aws/whats-new/2014/05/19/amazon-rds-for-sqlserver-introduces-multi-az-support/

QUESTION 230
Security groups act like a firewall at the instance level, whereas _____ are an additional layer of security that act at the subnet level.

A. DB Security Groups
B. VPC Security Groups
C. network ACLs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
While controlling access to Amazon EC2 resources, which of the following acts as a firewall that controls the traffic allowed to reach one or more instances?

A. A security group
B. An instance type
C. A storage cluster
D. An object

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A security group acts as a firewall that controls the traffic allowed to reach one or more instances. When you launch an instance, you assign it one or more security groups. http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM.html

QUESTION 232
Is the SQL Server Audit feature supported in the Amazon RDS SQL Server engine?

A. No
B. Yes

Correct Answer: A
Section: (none)
Explanation

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

The following server-level permissions are not available on SQL Server DB instances:

- ADMINISTER BULK OPERATIONS
- ALTER ANY CREDENTIAL
- ALTER ANY EVENT NOTIFICATION
- ALTER ANY EVENT SESSION
- ALTER ANY SERVER AUDIT
- ALTER RESOURCES
- ALTER SETTINGS (You can use the DB Parameter Group APIs to modify parameters. For more information, see Working with DB Parameter Groups.
- AUTHENTICATE SERVER
- CONTROL_SERVER
- CREATE DDL EVENT NOTIFICATION
- CREATE ENDPOINT
- CREATE TRACE EVENT NOTIFICATION
- EXTERNAL ACCESS ASSEMBLY
- SHUTDOWN (You can use the RDS reboot option instead)
- UNSAFE ASSEMBLY
- ALTER ANY AVAILABILITY GROUP (SQL Server 2012 only)
- CREATE ANY AVAILABILITY GROUP (SQL Server 2012 only)

QUESTION 233
Are you able to integrate a multi-factor token service with the AWS Platform?

A. Yes, using the AWS multi-factor token devices to authenticate users on the AWS platform.
B. No, you cannot integrate multi-factor token devices with the AWS platform.
C. Yes, you can integrate private multi-factor token devices to authenticate users to the AWS platform.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Private MFA does not apply here.
Q. What is AWS MFA?
AWS multi-factor authentication (AWS MFA) provides an extra level of security that you can apply to your AWS environment. You can enable AWS MFA for your AWS account and for individual AWS Identity and Access Management (IAM) users you create under your account.

QUESTION 234
My Read Replica appears "stuck" after a Multi-AZ failover and is unable to obtain or apply updates from the source DB Instance. What do I do?

A. You will need to delete the Read Replica and create a new one to replace it.
B. You will need to disassociate the DB Engine and re associate it.

C. The instance should be deployed to Single AZ and then moved to Multi- AZ once again
D. You will need to delete the DB Instance and create a new one to replace it.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q: My Amazon RDS for MySQL Read Replica appears "stuck" after a Multi-AZ failover and is unable to obtain or apply updates from the source DB Instance. What do I do? ... To resolve the current issue, you will need to delete the Read Replica and create a new one to replace it. "
https://aws.amazon.com/rds/faqs/

QUESTION 235
Which DNS name can only be resolved within Amazon EC2?

A. Internal DNS name
B. External DNS name
C. Global DNS name
D. Private DNS name

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To view DNS hostnames for an instance using the console
1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Instances.
3. Select your instance from the list.
4. In the details pane, the Public DNS (IPv4) and Private DNS fields display the DNS hostnames, if applicable.

QUESTION 236
If your DB instance runs out of storage space or file system resources, its status will change to_____ and your DB Instance will no longer be available.

A. storage-overflow
B. storage-full
C. storage-exceed
D. storage-overage

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
https://aws.amazon.com/ko/premiumsupport/knowledge-center/rds-out-of-storage/

Short Description

When an RDS DB instance reaches the STORAGE_FULL state, there is not enough space available for performing basic operations, eventually preventing you from restarting or making connections to the instance.

QUESTION 237
Is it possible to access your EBS snapshots?

A. Yes, through the Amazon S3 APIs.
B. Yes, through the Amazon EC2 APIs.
C. No, EBS snapshots cannot be accessed; they can only be used to create a new EBS volume.
D. EBS doesn't provide snapshots.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/ebs/faqs/?nc1=h_ls
Q: Will I be able to access my snapshots using the regular Amazon S3 API? No, snapshots are only available through the **Amazon EC2 API**.

QUESTION 238
Does Amazon RDS for SQL Server currently support importing data into the msdb database?

A. No
B. Yes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS for SQL Server does not currently support importing data into the msdb database, though we do support SQL Server Agent jobs. Some SQL Server features that use the msdb database, such as Database Mail and Replication, are not currently supported in Amazon RDS.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.Procedural.Importing.html#SQLServer.Proced ural.Importing.Procedure

QUESTION 239
Does Route 53 support MX Records?

A. Yes.

B. It supports CNAME records, but not MX records.
C. No
D. Only Primary MX records. Secondary MX records are not supported.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/ResourceRecordTypes.html#MXFormat

MX Format

Each value for an MX resource record set actually contains two values:

- An integer that represents the priority for an email server
- The domain name of the email server

If you specify only one server, the priority can be any integer between 0 and 65535. If you specify multiple servers, the value that you specify for the priority indicates which email server you want email to be routed to first, second, and so on. For example, if you have two email servers and you specify values of 10 and 20 for the priority, email always goes to the server with a priority of 10 unless it's unavailable. If you specify values of 10 and 10, email is routed to the two servers approximately equally.

Example for the Amazon Route 53 console

```
10 mail.example.com
```

Example for the Amazon Route 53 API

```
<Value>10 mail.example.com</Value>
```

QUESTION 240
Because of the extensibility limitations of striped storage attached to Windows Server, Amazon RDS does not currently support increasing storage on a _____ DB Instance.

A. SQL Server
B. MySQL
C. Oracle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
Which Amazon storage do you think is the best for my database-style applications that frequently encounter many random reads and writes across the dataset?

A. None of these.
B. Amazon Instance Storage
C. Any of these
D. Amazon EBS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"Amazon EBS is particularly helpful for database-style applications that frequently encounter many random reads and writes across the data set."
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

QUESTION 242
Select the correct set of steps for exposing the snapshot only to specific AWS accounts

A. Select public for all the accounts and check mark those accounts with whom you want to expose the snapshots and click save.
B. SelectPrivate, enter the IDs of those AWS accounts, and clickSave.
C. SelectPublic, enter the IDs of those AWS accounts, and clickSave.
D. SelectPublic, mark the IDs of those AWS accounts as private, and clickSave.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
“To expose the snapshot to only specific AWS accounts, choose Private, enter the ID of the AWS account (without hyphens) in the AWS Account Number field, and choose Add Permission. Repeat until you’ve added all the required AWS accounts”

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

QUESTION 243
Is decreasing the storage size of a DB Instance permitted?

A. Depends on the RDMS used
B. Yes
C. No

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"note that you cannot reduce storage size once it has been allocated" Source: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuideCHAP_Storage.html#CHAP_Storage.FactsAbout

QUESTION 244
In the context of MySQL, version numbers are organized as MySQL version = X.Y.Z. What does X denote here?

A. release level
B. minor version
C. version number
D. major version

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

MySQL on Amazon RDS Versions

For MySQL, version numbers are organized as version = X.Y.Z. In Amazon RDS terminology, X.Y denotes the major version, and Z is the minor version number. For Amazon RDS implementations, a version change is considered major if the major version number changes—for example, going from version 5.6 to 5.7. A version change is considered minor if only the minor version number changes—for example, going from version 5.6.22 to 5.6.23.

Amazon RDS currently supports MySQL major versions 5.5, 5.6, and 5.7. MySQL minor version support varies by AWS Region. Use the following table to see what MySQL minor versions are supported in each AWS Region.

QUESTION 245
In the 'Detailed' monitoring data available for your Amazon EBS volumes, Provisioned IOPS volumes automatically send _____ minute metrics to Amazon CloudWatch.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
It is advised that you watch the Amazon CloudWatch "_____" metric (available via the AWS Management Console or Amazon Cloud Watch APIs) carefully and recreate the Read Replica should it fall behind due to replication errors.

A. Write Lag
B. Read Replica
C. Replica Lag
D. Single Replica

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The amount of time a Read Replica DB instance lags behind the source DB instance. Applies to MySQL, MariaDB, and PostgreSQL Read Replicas.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/rds-metricscollected.html

ReplicaLag	The amount of time a Read Replica DB instance lags behind the source DB instance. Applies to MySQL, MariaDB, and PostgreSQL Read Replicas. Units: Seconds

QUESTION 247
Can the string value of 'Key' be prefixed with laws?

A. No
B. Only for EC2 not S3
C. Yes
D. Only for S3 not EC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/cli/latest/reference/rds/list-tags-for-resource.html

QUESTION 248
By default what are ENIs that are automatically created and attached to instances using the EC2 console set to do when the attached instance terminates?

A. Remain as is

B. Terminate
C. Hibernate
D. Pause

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By default, elastic network interfaces that are automatically created and attached to instances using the console are set to terminate when the instance terminates. However, network interfaces created using the command line interface aren't set to terminate when the instance terminates.
Source:http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#change_term_behavior

QUESTION 249
Are you able to integrate a multi-factor token service with the AWS Platform?

A. Yes, you can integrate private multi-factor token devices to authenticate users to the AWS platform.
B. No, you cannot integrate multi-factor token devices with the AWS platform.
C. Yes, using the AWS multi-factor token devices to authenticate users on the AWS platform.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Private MFA does not apply here.
Q. What is AWS MFA?
AWS multi-factor authentication (AWS MFA) provides an extra level of security that you can apply to your AWS environment. You can enable AWS MFA for your AWS account and for individual AWS Identity and Access Management (IAM) users you create under your account.

QUESTION 250
You can use _____ and _____ to help secure the instances in your VPC,

A. security groups and multi-factor authentication
B. security groups and 2-Factor authentication
C. security groups and biometric authentication
D. security groups and network ACLs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
Fill in the blanks: _____ is a durable, block-level storage volume that you can attach to a single, running Amazon EC2 instance.

A. Amazon S3
B. Amazon EBS
C. None of these
D. All of these

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
Do the Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

A. No
B. Only if instructed to when created
C. Yes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
If I want my instance to run on a single-tenant hardware, which value do I have to set the instance's tenancy attribute to?

A. dedicated
B. isolated
C. one
D. reserved

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://aws.amazon.com/ec2/dedicated-hosts/

Amazon EC2 Dedicated Hosts

An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts can help you address compliance requirements and reduce costs by allowing you to use your existing server-bound software licenses. Visit the EC2 Dedicated Host Pricing page for information on availability and pricing.

QUESTION 254
What does Amazon RDS stand for?

A. Regional Data Server.
B. Relational Database Service.
C. Nothing.
D. Regional Database Service.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
What is the maximum response time for a Business level Premium Support case?

A. 30 minutes
B. You always get instant responses (within a few seconds).
C. 10 minutes
D. 1 hour

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
What does Amazon ELB stand for?

A. Elastic Linux Box.
B. Encrypted Linux Box.
C. Encrypted Load Balancing.
D. Elastic Load Balancing.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
What is the minimum time Interval for the data that Amazon CloudWatch receives and aggregates?

A. One second
B. Five seconds
C. One minute
D. Three minutes
E. Five minutes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Many metrics are received and aggregated at 1-minute intervals. Some are at 3-minute or 5-minute intervals.

QUESTION 258
Is there a limit to the number of groups you can have?

A. Yes for all users except root
B. No
C. Yes unless special permission granted
D. Yes for all users

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Currently you can request to increase the limit on users per AWS account, groups per AWS account, roles per AWS account, instance profiles per AWS account, and server certificates per
AWS account.
http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html

QUESTION 259
Location of Instances are _____

A. Regional
B. based on Availability Zone
C. Global

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Regions and Availability Zones
Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones. Amazon EC2 provides you the ability to place resources, such as instances, and data in multiple locations. Resources aren't replicated across regions unless you do so specifically. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions- availability-zones

```
$ aws ec2 describe-availability-zones --region us-east-1
{
    "AvailabilityZones": [
        {
            "State": "available",
            "RegionName": "us-east-1",
            "Messages": [],
            "ZoneName": "us-east-1b"
        },
        {
            "State": "available",
            "RegionName": "us-east-1",
            "Messages": [],
            "ZoneName": "us-east-1c"
        },
        {
            "State": "available",
            "RegionName": "us-east-1",
            "Messages": [],
            "ZoneName": "us-east-1d"
        }
    ]
}
```

QUESTION 260

Is there any way to own a direct connection to Amazon Web Services?

A. You can create an encrypted tunnel to VPC, but you don't own the connection.
B. Yes, it's called Amazon Dedicated Connection.
C. No, AWS only allows access from the public Internet.
D. Yes, it's called Direct Connect.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
What is the maximum response time for a Business level Premium Support case?

A. 30 minutes
B. 1 hour
C. 12 hours
D. 10 minutes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
Does Dynamic DB support in-place atomic updates?

A. It is not defined
B. No
C. Yes
D. It does support in-place non-atomic updates

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q: Does DynamoDB support in-place atomic updates?
Amazon DynamoDB supports fast in-place updates. You can increment or decrement a numeric attribute in a row using a single API call. Similarly, you can atomically add

or remove to sets, lists, or maps.
https://aws.amazon.com/dynamodb/faqs/

QUESTION 263
Is there a method in the IAM system to allow or deny access to a specific instance?

A. Only for VPC based instances
B. Yes
C. No

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EC2 uses SSH keys, Windows passwords, and security groups to control who has access to the operating system of specific Amazon EC2 instances. There's no method in the IAM system to allow or deny access to the operating system of a specific instance.

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

QUESTION 264
What does Amazon SES stand for?

A. Simple Elastic Server
B. Simple Email Service
C. Software Email Solution
D. Software Enabled Server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://aws.amazon.com/ses/

Amazon Simple Email Service (Amazon SES) is a cost-effective email service built on the reliable and scalable infrastructure that Amazon.com developed to serve its own customer base. With Amazon SES, you can send and receive email with no required minimum commitments – you pay as you go, and you only pay for what you use.

QUESTION 265
Amazon S3 doesn't automatically give a user who creates _____ permission to perform other actions on that bucket or object.

A. a file

B. a bucket or object
C. a bucket or file
D. a object or file

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon S3 doesn't automatically give a user who creates a bucket or object permission to perform other actions on that bucket or object. Therefore, in your IAM policies, you must explicitly give users permission to use the Amazon S3 resources they create.
http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html

QUESTION 266
Can I attach more than one policy to a particular entity?

A. Yes always
B. Only if within GovCloud
C. No
D. Only if within VPC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267
Fill in the blanks: A_____ is a storage device that moves data in sequences of bytes or bits (blocks). Hint: These devices support random access and generally use buffered I/O.

A. block map
B. storage block
C. mapping device
D. block device

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268

Can I detach the primary (eth0) network interface when the instance is running or stopped?

A. Yes, You can.
B. No. You cannot
C. Depends on the state of the interface at the time

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each instance in a VPC has a default elastic network interface (the primary network interface, eth0) that is assigned a private IP address from the IP address range of your VPC. You cannot
detach a primary network interface from an instance.

QUESTION 269
What's an ECU?

A. Extended Cluster User.
B. None of these.
C. Elastic Computer Usage.
D. Elastic Compute Unit.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The EC2 Compute Unit (ECU) provides the relative measure of the integer processing power of an Amazon EC2 instance.
https://aws.amazon.com/ec2/faqs/

QUESTION 270
REST or Query requests are HTTP or HTTPS requests that use an HTTP verb (such as GET or POST) and a parameter named Action or Operation that specifies the API you are calling.

A. FALSE
B. TRUE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/APIReference/Query-Requests.html

Query Requests

Query requests are HTTP or HTTPS requests that use the HTTP verb GET or POST and a Query parameter named `Action`. For a list of Amazon EC2 API actions, see Actions.

Topics

- Structure of a GET Request
- Endpoints
- Query Parameters
- Query API Authentication
- Query Response Structures

QUESTION 271
Does AWS Direct Connect allow you access to all Availabilities Zones within a Region?

A. Depends on the type of connection
B. No
C. Yes
D. Only when there's just one availability zone in a region. If there are more than one, only one availability zone can be accessed directly.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each AWS Direct Connect location enables connectivity to all Availability Zones within the geographically nearest AWS region.
Reference: https://aws.amazon.com/directconnect/faqs/

QUESTION 272
What does the "Server Side Encryption" option on Amazon S3 provide?

A. It provides an encrypted virtual disk in the Cloud.
B. It doesn't exist for Amazon S3, but only for Amazon EC2.
C. It encrypts the files that you send to Amazon S3, on the server side.
D. It allows to upload files using an SSL endpoint, for a secure transfer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

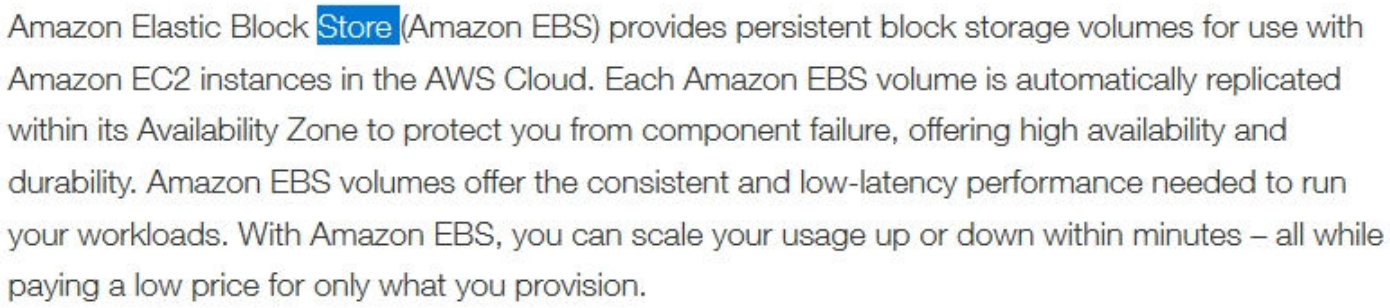
Explanation:
Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
Reference: https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html

QUESTION 273
What does Amazon EBS stand for?

A. Elastic Block Storage
B. Elastic Business Server
C. Elastic Blade Server
D. Elastic Block Store

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/ebs/
Amazon Elastic Block Store (EBS)
Amazon Elastic Block Store (Amazon EBS) provides persistent block level storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes offer the consistent and low- latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes all while paying a low price for only what you provision.



QUESTION 274
Within the IAM service a GROUP is regarded as a:

A. A collection of AWS accounts
B. It's the group of EC2 machines that gain the permissions specified in the GROUP.
C. There's no GROUP in IAM, but only USERS and RESOURCES.

D. A collection of users.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Use groups to assign permissions to IAM users
Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.), define the relevant permissions for each group, and then assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group. That way, you can make changes for everyone in a group in just one place. As people move around in your company, you can simply change what IAM group their IAM user belongs to.
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions

QUESTION 275
A _____ is the concept of allowing (or disallowing) an entity such as a user, group, or role some type of access to one or more resources.

A. user
B. AWS Account
C. resource
D. permission

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A permission is the concept of allowing (or disallowing) an entity such as a user, group, or role some type of access to one or more resources.

QUESTION 276
After an Amazon VPC instance is launched, can I change the VPC security groups it belongs to?

A. No. You cannot.
B. Yes. You can.
C. Only if you are the root user
D. Only if the tag "VPC_Change_Group" is true

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security groups are associated with network interfaces. After you launch an instance, you can change the security groups associated with the instance, which changes the

security groups associated with the primary network interface (eth0).

QUESTION 277
Do the system resources on the Micro instance meet the recommended configuration for Oracle?

A. Yes completely
B. Yes but only for certain situations
C. Not in any circumstance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
We recommend that you use db.t1.micro instances with Oracle to **test setup** and connectivity only; the system resources for a db.t1.micro instance do not meet the recommended configuration for Oracle. No Oracle options are supported on a db.t1.micro instance.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuideConcepts.DBInstanceClass.html#Concepts.DBInstanceCla ss.Previous

QUESTION 278
Will I be charged if the DB instance is idle?

A. No
B. Yes
C. Only is running in GovCloud
D. Only if running in VPC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
To help you manage your Amazon EC2 instances, images, and other Amazon EC2 resources, you can assign your own metadata to each resource in the form of_____

A. special filters
B. functions
C. tags
D. wildcards

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
Are you able to integrate a multi-factor token service with the AWS Platform?

A. No, you cannot integrate multi-factor token devices with the AWS platform.
B. Yes, you can integrate private multi-factor token devices to authenticate users to the AWS platform.
C. Yes, using the AWS multi-factor token devices to authenticate users on the AWS platform.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
True or False: When you add a rule to a DB security group, you do not need to specify port number or protocol.

A. Depends on the RDMS used
B. TRUE
C. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

DB Security Groups

Each DB security group rule enables a specific source to access a DB instance that is associated with that DB security group. The source can be a range of addresses (e.g., 203.0.113.0/24), or an EC2 security group. When you specify an EC2 security group as the source, you allow incoming traffic from all EC2 instances that use that EC2 security group. Note that DB security group rules apply to inbound traffic only; outbound traffic is not currently permitted for DB instances.

You do not need to specify a destination port number when you create DB security group rules; the port number defined for the DB instance is used as the destination port number for all rules defined for the DB security group. DB security groups can be created using the Amazon RDS APIs or the Amazon RDS page of the AWS Management Console.

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

QUESTION 282
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EC2 supports the following storage options:
Amazon Elastic Block Store (Amazon EBS)
Amazon EC2 Instance Store
Amazon Simple Storage Service (Amazon S3)
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 283
Can I initiate a "forced failover" for my Oracle Multi-AZ DB Instance deployment?

A. Yes

B. Only in certain regions
C. Only in VPC
D. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/public-data-sets/
If your DB instance is a Multi-AZ deployment, **you can force a failover from one availability zone to another when you select the Reboot option**. When you force a failover of your DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone and updates the DNS record for the DB instance to point to the standby DB instance. As a result, you will need to clean up and re-establish any existing connections to your DB instance. Reboot with failover is beneficial when you want to simulate a failure of a DB instance for testing, or restore operations to the original AZ after a failover occurs.
Source: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RebootInstance.html

QUESTION 284
Amazon EC2 provides a repository of public data sets that can be seamlessly integrated into AWS cloud-based applications.What is the monthly charge for using the public data sets?

A. A 1 time charge of 10$ for all the datasets.
B. 1$ per dataset per month
C. 10$ per month for all the datasets
D. There is no charge for using the public data sets

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
In the Amazon RDS Oracle DB engine, the Database Diagnostic Pack and the Database Tuning Pack are only available with _____

A. Oracle Standard Edition
B. Oracle Express Edition
C. Oracle Enterprise Edition
D. None of these

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
https://www.pythian.com/blog/a-most-simple-cloud-is-amazon-rds-for-oracle-right-for-you/

QUESTION 286
Without _____, you must either create multiple AWS accounts-each with its own billing and subscriptions to AWS products-or your employees must share the security credentials of a single AWS account.

A. Amazon RDS
B. Amazon Glacier
C. Amazon EMR
D. Amazon IAM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287
Amazon RDS supports SOAP only through _____.

A. HTTP or HTTPS
B. TCP/IP
C. HTTP
D. HTTPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS supports SOAP only through HTTPS
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/using-soap-api.html

WSDL and Schema Definitions

You can access the Amazon Relational Database Service using the SOAP web services messaging protocol. This interface is described by a Web Services Description Language (WSDL) document, which defines the operations and security model for the particular service. The WSDL references an XML Schema document, which strictly defines the data types that might appear in SOAP requests and responses. For more information on WSDL and SOAP, see Web Services References.

Note

Amazon RDS supports SOAP only through HTTPS.

QUESTION 288
The Amazon EC2 web service can be accessed using the _____ web services messaging protocol. This interface is described by a Web Services Description Language (WSDL) document.

A. SOAP
B. DCOM
C. CORBA
D. XML-RPC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSECommerceService/latest/DG/WSDLLocation.html

WSDL and Schema Definitions

You can access the Amazon Relational Database Service using the SOAP web services messaging protocol. This interface is described by a Web Services Description Language (WSDL) document, which defines the operations and security model for the particular service. The WSDL references an XML Schema document, which strictly defines the data types that might appear in SOAP requests and responses. For more information on WSDL and SOAP, see Web Services References.

Note

Amazon RDS supports SOAP only through HTTPS.

QUESTION 289
Is creating a Read Replica of another Read Replica supported?

A. Only in VPC
B. Yes
C. Only in certain regions
D. No

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
What is the charge for the data transfer incurred in replicating data between your primary and standby?

A. Same as the standard data transfer charge
B. Double the standard data transfer charge
C. No charge. It is free
D. Half of the standard data transfer charge

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q: How much do Read Replicas cost? When does billing begin and end?
A Read Replica is billed as a standard DB Instance and at the same rates. Click here for more information on DB Instance billing visit this FAQ. Just like a standard DB Instance, the rate per "DB Instance hour" for a Read Replica is determined by the DB Instance class of the Read Replica –please see Amazon RDS detail page for up-to-date pricing. You are not charged for the data transfer incurred in replicating data between your source DB Instance and Read Replica.
Billing for a Read Replica begins as soon as the Read Replica has been successfully created (i.e. when status is listed as "active"). The Read Replica will continue being billed at standard Amazon RDS DB Instance hour rates until you issue a command to delete it.

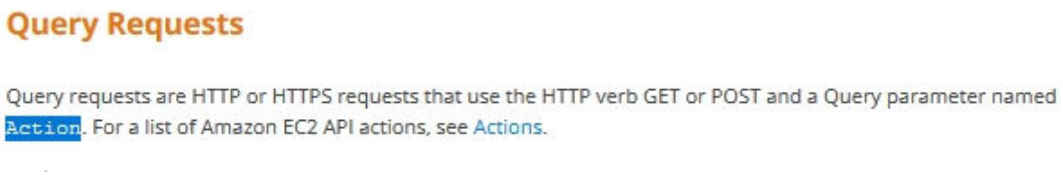
QUESTION 291
HTTP Query-based requests are HTTP requests that use the HTTP verb GET or POST and a Query parameter named_____.

A. Action
B. Value
C. Reset
D. Retrieve

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
http://docs.aws.amazon.com/AmazonS3/latest/dev/using-with-s3-actions.html



QUESTION 292
Amazon RDS creates an SSL certificate and installs the certificate on the DB Instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The _____ is stored athttps://rds.amazonaws.com/doc/rds-ssl-ca-cert.pem.

A. private key
B. foreign key
C. public key
D. protected key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks. The public key is stored at https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem.

QUESTION 293
_____ embodies the "share-nothing" architecture and essentially involves breaking a large database into several smaller databases. Common ways to split a database include 1) splitting tables that are not joined in the same query onto different hosts or 2) duplicating a table across multiple hosts and then using a hashing algorithm to determine which host receives a given update.

A. Sharding
B. Failure recovery
C. Federation
D. DDL operations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Amazon RDS for MySQL Now Supports Read Replica Promotion

Posted On: Oct 11, 2012

We are pleased to announce that Amazon RDS for MySQL now supports "Promote Read Replica" functionality. You can now convert a MySQL Read Replica into a "standalone" DB Instance using the "Promote Read Replica" option. This option stops replication and converts the Read Replica in its existing state into a "standalone" DB Instance.

You can use this option for a number of use cases including:

- **Perform DDL operations**: DDL operations such as creating/re-building indexes etc. could take a long time and impose significant performance penalty on your DB Instance. You can perform these operations on a Read Replica, and once the operations are complete and the updates are caught up with the Source DB Instance, you can promote the Read Replica, and point your applications to it.
- **Sharding** embodies the "share-nothing" architecture and essentially involves breaking a larger database up into smaller databases. Common ways to split a database are: Splitting tables that are not joined in the same query onto different hosts or duplicating a table across multiple hosts and then deciding on a hashing algorithm to figure out into which host a row goes. You can create Read Replicas corresponding to each of your "shards" and promote them when you decide to convert them into "standalone" shards. You can then delete the rows or tables that belong to the other shards.

More detailed information on the pros and cons of sharing can be found at the following sites:
http://technoroy.blogspot.com/2008/07/shard-database-design.html http://www.hibernate.org/subprojects/shards.html
How Amazon RDS Helps With Sharing Maintenance Overhead

QUESTION 294
What is the name of licensing model in which I can use your existing Oracle Database licenses to run Oracle deployments on Amazon RDS?

A. Bring Your Own License
B. Role Bases License
C. Enterprise License
D. License Included

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/oracle/

QUESTION 295
When you resize the Amazon RDS DB instance, Amazon RDS will perform the upgrade during the next maintenance window. If you want the upgrade to be performed now, rather than waiting for the maintenance window, specify the _____ option.

A. ApplyNow
B. ApplySoon
C. ApplyThis
D. ApplyImmediately

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.Modifying.html

QUESTION 296
Does Amazon Route 53 support NS Records?

A. Yes, it supports Name Service records.
B. No
C. It supports only MX records.
D. Yes, it supports Name Server records.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/route53/faqs/

QUESTION 297
The SQL Server _____ feature is an efficient means of copying data from a source database to your DB Instance. It writes the data that you specify to a data file, such as an ASCII file.

A. bulk copy
B. group copy
C. dual copy
D. mass copy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Bulk Copy

The SQL Server bulk copy feature is an efficient means of copying data from a source database to your DB instance. Bulk copy writes the data that you specify to a data file, such as an ASCII file. You can then run bulk copy again to write the contents of the file to the destination DB instance.

This section uses the **bcp** utility, which is included with all editions of SQL Server. For detailed information about bulk import and export operations, see the Microsoft SQL Server documentation.

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.Procedural.Importing.html

QUESTION 298
When using consolidated billing there are two account types. What are they?

A. Paying account and Linked account
B. Parent account and Child account
C. Main account and Sub account.
D. Main account and Secondary account.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You sign up for Consolidated Billing in the AWS Billing and Cost Management console, and designate your account as a payer account. Now your account can pay the charges of the other accounts, which are called linked accounts. The payer account and the accounts linked to it are called a Consolidated Billing account family. Source: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html

QUESTION 299
A _____ is a document that provides a formal statement of one or more permissions.

A. policy
B. permission
C. Role
D. resource

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 300
In the Amazon RDS which uses the SQL Server engine, what is the maximum size for a Microsoft SQL Server DB Instance with SQL Server Express edition?

A. 10 GB per DB
B. 100 GB per DB
C. 2 TB per DB
D. 1TB per DB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The maximum storage size for a Microsoft SQL Server DB Instance is 4 TB for all instances except the SQL Server Express edition, which limits storage to a total of 300 GB. The minimum storage size for a Microsoft SQL Server DB Instance is 20 GB for the Microsoft SQL Server Express and Web Editions and 200 GB for the Standard and Enterprise Editions.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html

QUESTION 301
Regarding the attaching of ENI to an instance, what does 'warm attach' refer to?

A. Attaching an ENI to an instance when it is stopped.
B. This question doesn't make sense.
C. Attaching an ENI to an instance when it is running
D. Attaching an ENI to an instance during the launch process

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Best Practices for Configuring Elastic Network Interfaces
You can attach an elastic network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#best-practices-for-configuring-network- interfaces

QUESTION 302
If I scale the storage capacity provisioned to my DB Instance by mid of a billing month, how will I be charged?

A. You will be charged for the highest storage capacity you have used
B. On a proration basis

C. You will be charged for the lowest storage capacity you have used

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/ebs/pricing/

QUESTION 303
You can modify the backup retention period; valid values are 0 (for no backup retention) to a maximum of _____ days.

A. 45
B. 35
C. 15
D. 5

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 304
A Provisioned IOPS volume must be at least _____ GB in size

A. 1
B. 50
C. 20
D. 10

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/ebs/details/

QUESTION 305
Will I be alerted when automatic failover occurs?

A. Only if SNS configured

B. No
C. Yes
D. Only if Cloudwatch configured

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
See http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.html
Amazon RDS uses the Amazon Simple Notification Service (Amazon SNS) to provide 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.
Amazon RDS groups these events into categories that you can subscribe to so that you can be notified when an event in that category occurs.
C is not correct because even though event is created by RDS you will not be alerted for it unless you configure your subscription in SNS.

QUESTION 306
If you're unable to connect via SSH to your EC2 instance, which of the following should you check and possibly correct to restore connectivity?

A. Adjust Security Group to permit egress traffic over TCP port 443 from your IP.
B. Configure the IAM role to permit changes to security group settings.
C. Modify the instance security group to allow ingress of ICMP packets from your IP.
D. Adjust the instance's Security Group to permit ingress traffic over port 22 from your IP.
E. Apply the most recently released Operating System security patches.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In a VPC everything is allowed out by default.

Reference:
http://docs.aws.amazon.com/cli/latest/reference/ec2/authorize-security-group-ingress.html

QUESTION 307
Which of the following features ensures even distribution of traffic to Amazon EC2 instances in multiple Availability Zones registered with a load balancer?

A. Elastic Load Balancing request routing
B. An Amazon Route 53 weighted routing policy
C. Elastic Load Balancing cross-zone load balancing
D. An Amazon Route 53 latency routing policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cross-zone load balancing is always enabled for an Application Load Balancer and is disabled by default for a Classic Load Balancer. If cross-zone load balancing is enabled, the load balancer distributes traffic evenly across all registered instances in all enabled Availability Zones. If cross-zone load balancing is disabled, the load balancer distributes traffic evenly across all enabled Availability Zones. For example, suppose that you have 10 instances in Availability Zone us-west-2a and 2 instances in us-west-2b. If cross-zone load balancing is disabled, the requests are distributed evenly between us-west-2a and us-west-2b. As a result, the 2 instances in us-west-2b serve the same amount of traffic as the 10 instances in us-west-2a. However, if cross-zone load balancing is enabled, the load balancer distributes incoming requests evenly across all 12 instances.

http://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html

QUESTION 308
You are using an m1.small EC2 Instance with one 300 GB EBS volume to host a relational database. You determined that write throughput to the database needs to be increased. Which of the following approaches can help achieve this? Choose 2 answers

A. Use an array of EBS volumes.
B. Enable Multi-AZ mode.
C. Place the instance in an Auto Scaling Groups
D. Add an EBS volume and place into RAID 5.
E. Increase the size of the EC2 Instance.
F. Put the database behind an Elastic Load Balancer.

Correct Answer: AE
Section: (none)
Explanation

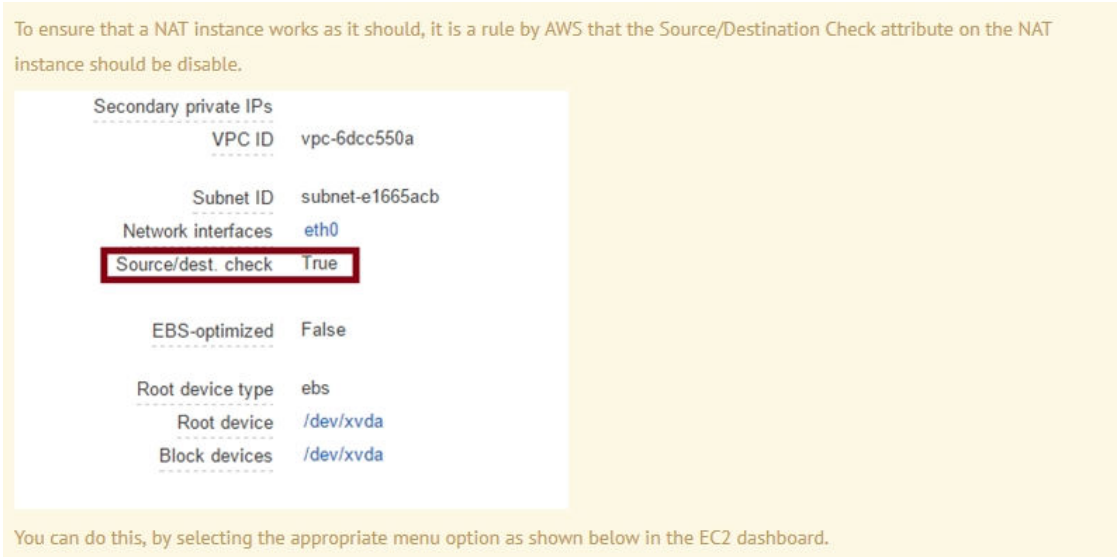
Explanation/Reference:

QUESTION 309
After launching an instance that you intend to serve as a NAT (Network Address Translation) device in a public subnet you modify your route tables to have the NAT device be the target of internet bound traffic of your private subnet. When you try and make an outbound connection to the internet from an instance in the private subnet, you are not successful. Which of the following steps could resolve the issue?

A. Disabling the Source/Destination Check attribute on the NAT instance
B. Attaching an Elastic IP address to the instance in the private subnet
C. Attaching a second Elastic Network Interface (ENI) to the NAT instance, and placing it in the private subnet
D. Attaching a second Elastic Network Interface (ENI) to the instance in the private subnet, and placing it in the public subnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:



Reference:
http://docs.aws.amazon.com/workspaces/latest/adminguide/gsg_create_vpc.html

QUESTION 310
You have multiple Amazon EC2 instances running in a cluster across multiple Availability Zones within the same region. What combination of the following should be used to ensure the highest network performance (packets per second), lowest latency, and lowest jitter? (Choose three.)

A. Amazon EC2 placement groups
B. Enhanced networking
C. Amazon PV AMI
D. Amazon HVM AMI
E. Amazon Linux
F. Amazon VPC

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Enhanced Networking enables you to get significantly higher packet per second (PPS) performance, lower network jitter and lower latencies. This feature uses a new network virtualization stack that provides higher I/O performance and lower CPU utilization compared to traditional implementations. In order to take advantage of Enhanced Networking, you should launch an HVM AMI in VPC, and install the appropriate driver. For instructions on how to enable Enhanced Networking on EC2 instances, see the Enhanced Networking on Linux and Enhanced Networking on Windows tutorials. For availability of this feature by instance, or to learn more, visit the Enhanced Networking FAQ section.

QUESTION 311
When using the following AWS services, which should be implemented in multiple Availability Zones for high availability solutions? Choose 2 answers

A. Amazon DynamoDB
B. Amazon Elastic Compute Cloud (EC2)
C. Amazon Elastic Load Balancing
D. Amazon Simple Notification Service (SNS)
E. Amazon Simple Storage Service (S3)

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 312
You have a video transcoding application running on Amazon EC2. Each instance polls a queue to find out which video should be transcoded, and then runs a transcoding process. If this process is interrupted, the video will be transcoded by another instance based on the queuing system. You have a large backlog of videos which need to be transcoded and would like to reduce this backlog by adding more instances. You will need these instances only until the backlog is reduced. Which type of Amazon EC2 instances should you use to reduce the backlog in the most cost efficient way?

A. Reserved instances
B. Spot instances
C. Dedicated instances
D. On-demand instances

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://aws.amazon.com/ec2/purchasing-options/spot-instances/

QUESTION 313
You have an EC2 Security Group with several running EC2 instances. You change the Security Group rules to allow inbound traffic on a new port and protocol, and launch several new instances in the same Security Group. The new rules apply:

A. Immediately to all instances in the security group.
B. Immediately to the new instances only.
C. Immediately to the new instances, but old instances must be stopped and restarted before the new rules apply.
D. To all instances, but it may take several minutes for old instances to see the changes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#vpc-security-groups

Visit PassLeader and Download Full Version AWS-Associate Exam Dumps

AWS-Associate Exam Dumps AWS-Associate Exam Questions AWS-Associate PDF Dumps AWS-Associate VCE Dumps http://www.passleader.com/aws-certified-solutions-architect-associate.html

QUESTION 314
Which services allow the customer to retain full administrative privileges of the underlying EC2 instances? (Choose two.)

A. Amazon Relational Database Service
B. Amazon Elastic Map Reduce
C. Amazon ElastiCache
D. Amazon DynamoDB
E. AWS Elastic Beanstalk

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 315
A company is building a two-tier web application to serve dynamic transaction-based content. The data tier is leveraging an Online Transactional Processing (OLTP) database. What services should you leverage to enable an elastic and scalable web tier?

A. Elastic Load Balancing, Amazon EC2, and Auto Scaling
B. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3
C. Amazon RDS with Multi-AZ and Auto Scaling
D. Amazon EC2, Amazon DynamoDB, and Amazon S3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fleet of spot EC2 instances. Files submitted by your premium customers must be transformed with the highest priority. How should you implement such a system?

A. Use a DynamoDB table with an attribute defining the priority level. Transformation instances will scan the table for tasks, sorting the results by priority level.
B. Use Route 53 latency based-routing to send high priority tasks to the closest transformation instances.
C. Use two SQS queues, one for high priority messages, the other for default priority. Transformation instances first poll the high priority queue; if there is no message, they poll the default priority queue.
D. Use a single SQS queue. Each message contains the priority level. Transformation instances poll high-priority messages first.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

A. Use an IAM policy that references the LDAP account identifiers and the AWS credentials.
B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
D. Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.
E. Use the LDAP credentials to restrict a group of users from launching specific EC2 instance types.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://d0.awsstatic.com/whitepapers/aws-whitepaper-single-sign-on-integrating-aws-open-ldap-and-shibboleth.pdf

QUESTION 318
Which of the following are characteristics of Amazon VPC subnets? (Choose two.)

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

Correct Answer: BD

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Even though we know the right Answers it is sometimes good to know why the other Answers are wrong.
A. Is wrong because a subnet maps to a single AZ.
C. Is wrong because /28 is the smallest subnet, amazon takes first four and last addresses per subnet.
E. Is wrong because a private subnet needs a NAT appliance.

QUESTION 319
A customer is leveraging Amazon Simple Storage Service in eu-west-1 to store static content for a web-based property. The customer is storing objects using the Standard Storage class. Where are the customers objects replicated?

A. A single facility in eu-west-1 and a single facility in eu-central-1
B. A single facility in eu-west-1 and a single facility in us-east-1
C. Multiple facilities in eu-west-1
D. A single facility in eu-west-1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Objects stored in a region never leave the region unless you explicitly transfer them to another region. For example, objects stored in the EU (Ireland) region never leave it.
http://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html#Regions

QUESTION 320
Your web application front end consists of multiple EC2 instances behind an Elastic Load Balancer. You configured ELB to perform health checks on these EC2 instances, if an instance fails to pass health checks, which statement will be true?

A. The instance gets terminated automatically by the ELB
B. The instance gets quarantined by the ELB for root cause analysis.
C. The instance is replaced automatically by the ELB
D. The ELB stops sending traffic to the instance that failed its health check.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 321
In AWS, which security aspects are the customer's responsibility? (Choose four.)

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

Correct Answer: ACDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 322
You have a web application running on six Amazon EC2 instances, consuming about 45% of resources on each instance. You are using auto-scaling to make sure that six instances are running at all times. The number of requests this application processes is consistent and does not experience spikes. The application is critical to your business and you want high availability at all times. You want the load to be distributed evenly between all instances. You also want to use the same Amazon Machine Image (AMI) for all instances. Which of the following architectural choices should you make?

A. Deploy 6 EC2 instances in one availability zone and use Amazon Elastic Load Balancer.
B. Deploy 3 EC2 instances in one region and 3 in another region and use Amazon Elastic Load Balancer.
C. Deploy 3 EC2 instances in one availability zone and 3 in another availability zone and use Amazon Elastic Load Balancer.
D. Deploy 2 EC2 instances in three regions and use Amazon Elastic Load Balancer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A load balancer accepts incoming traffic from clients and routes requests to its registered EC2 instances in one or more Availability Zones.
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/how-elb-works.html Updated Security Whitepaper link:
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Reference:
https://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf (page 8)
https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html

QUESTION 323
You have decided to change the instance type for instances running in your application tier that is using Auto Scaling. In which area below would you change the instance type definition?

A. Auto Scaling policy

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 324
When an EC2 EBS-backed (EBS root) instance is stopped, what happens to the data on any ephemeral store volumes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you stop a running instance, the following happens:

*The instance performs a normal shutdown and stops running; its status changes to stopping and then stopped.

*Any Amazon EBS volumes remain attached to the instance, and their data persists.

*Any data stored in the RAM of the host computer or the instance store volumes of the host computer is gone.

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

QUESTION 325
Which of the following items are required to allow an application deployed on an EC2 instance to write data to a DynamoDB table? Assume that no security keys are allowed to be stored on the EC2 instance. (Choose two.)

A. Create an IAM Role that allows write access to the DynamoDB table.
B. Add an IAM Role to a running EC2 instance.
C. Create an IAM User that allows write access to the DynamoDB table.
D. Add an IAM User to a running EC2 instance.
E. Launch an EC2 Instance with the IAM Role included in the launch configuration.

Correct Answer: AB

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TicTacToe.Phase3.html

QUESTION 326
When you put objects in Amazon S3, what is the indication that an object was successfully stored?

A. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
B. Amazon S3 is engineered for 99.999999999% durability. Therefore there is no need to confirm that data was inserted.
C. A success code is inserted into the S3 object metadata.
D. Each S3 account has a special bucket named _s3_logs. Success codes are written to this bucket with a timestamp and checksum.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To ensure that data is not corrupted traversing the network, use the Content-MD5 form field. When you use this form field, Amazon S3 checks the object against the provided MD5 value. If they do not match, Amazon S3 returns an error. The status code returned to the client upon successful upload if success_action_redirect is not specified. Accepts the values 200, 201, or 204 (default).
http://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html

QUESTION 327
What is one key difference between an Amazon EBS-backed and an instance-store backed instance?

A. Amazon EBS-backed instances can be stopped and restarted.
B. Instance-store backed instances can be stopped and restarted.
C. Auto scaling requires using Amazon EBS-backed instances.
D. Virtual Private Cloud requires EBS backed instances.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html#storage-for-the-root-device

QUESTION 328
A company wants to implement their website in a virtual private cloud (VPC). The web tier will use an Auto Scaling group across multiple Availability Zones (AZs). The database will use Multi-AZ RDS MySQL and should not be publicly accessible. What is the minimum number of subnets that need to be configured in the VPC?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since multi-AZ RDS needs 2 private subnets to provide high availability and 2 public subnets are needed for ELB(web-tier) application.

Would use VPC with private (DB) and public (WEB) subnets:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html
Multi AZ requirement forces me to multiply subnets by two.
Reasons:
For DB: Your VPC must have at least one subnet in at least two of the Availability Zones in the region where you want to deploy your DB instance. A subnet is a segment of a VPC's IP address
range that you can specify and that lets you group instances based on your security and operational needs
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html
For Web: After creating a VPC, you can add one or more subnets in each Availability Zone. Each subnet must reside entirely within one Availability Zone and cannot span zones
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 329
You have launched an Amazon Elastic Compute Cloud (EC2) instance into a public subnet with a primary private IP address assigned, an Internet gateway is attached to the VPC, and the public route table is configured to send all Internet-based traffic to the Internet gateway. The instance security group is set to allow all outbound traffic but cannot access the internet. Why is the Internet unreachable from this instance?

A. The instance does not have a public IP address.
B. The internet gateway security group must allow all outbound traffic.
C. The instance security group must allow all inbound traffic.
D. The instance "Source/Destination check" property must be enabled.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Ensure that instances in your subnet have public IP addresses or Elastic IP addresses. https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

QUESTION 330
You launch an Amazon EC2 instance without an assigned AVVS identity and Access Management (IAM) role. Later, you decide that the instance should be running with

an IAM role. Which action must you take in order to have a running Amazon EC2 instance with an IAM role assigned to it?

A. Create an image of the instance, and register the image with an IAM role assigned and an Amazon EBS volume mapping.
B. Create a new IAM role with the same permissions as an existing IAM role, and assign it to the running instance.
C. Create an image of the instance, add a new IAM role with the same permissions as the desired IAM role, and deregister the image with the new role assigned.
D. Create an image of the instance, and use this image to launch a new instance with the desired IAM role assigned.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/roles-usingrole-ec2instance.html

QUESTION 331
How can the domain's zone apex, for example, "myzoneapexdomain.com", be pointed towards an Elastic Load Balancer?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can create an alias resource record set at the zone apex. You cannot create a CNAME record at the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com.
http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

QUESTION 332
An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group is configured to allow SSH from any IP address and deny all outbound traffic. What changes need to be made to allow SSH access to the instance?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Need to open TCP Port 1024-65535 at Outbound Rules
"Allows outbound responses to the remote computer. Network ACLs are stateless, therefore this rule is required to allow response traffic for inbound requests."

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

QUESTION 333
For which of the following use cases are Simple Workflow Service (SWF) and Amazon EC2 an appropriate solution? (Choose two.)

A. Using as an endpoint to collect thousands of data points per hour from a distributed fleet of sensors
B. Managing a multi-step and multi-decision checkout process of an e-commerce website
C. Orchestrating the execution of distributed and auditable business processes
D. Using as an SNS (Simple Notification Service) endpoint to trigger execution of video transcoding jobs
E. Using as a distributed session store for your web application

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/swf/faqs/

QUESTION 334
A customer wants to leverage Amazon Simple Storage Service (S3) and Amazon Glacier as part of their backup and archive infrastructure. The customer plans to use third-party software to support this integration. Which approach will limit the access of the third party software to only the Amazon S3 bucket named "company-backup"?

A. A custom bucket policy limited to the Amazon S3 API in thee Amazon Glacier archive "company-backup"
B. A custom bucket policy limited to the Amazon S3 API in "company-backup"
C. A custom IAM user policy limited to the Amazon S3 API for the Amazon Glacier archive "company-backup".
D. A custom IAM user policy limited to the Amazon S3 API in "company-backup".

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AmazonS3/latest/dev/example-policies-s3.html

QUESTION 335
A client application requires operating system privileges on a relational database server. What is an appropriate configuration for a highly available database architecture?

A. A standalone Amazon EC2 instance

B. Amazon RDS in a Multi-AZ configuration
C. Amazon EC2 instances in a replication configuration utilizing a single Availability Zone
D. Amazon EC2 instances in a replication configuration utilizing two different Availability Zones

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"A client application requires operating system privileges". You cant have it using RDS.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

QUESTION 336
What is a placement group?

A. A collection of Auto Scaling groups in the same region
B. A feature that enables EC2 instances to interact with each other via high bandwidth, low latency connections
C. A collection of authorized CloudFront edge locations for a distribution
D. A collection of Elastic Load Balancers in the same Region or Availability Zone

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 337
A company has a workflow that sends video files from their on-premise system to AWS for transcoding. They use EC2 worker instances that pull transcoding jobs from SQS. Why is SQS an appropriate service for this scenario?

A. SQS guarantees the order of the messages.
B. SQS synchronously provides transcoding output.
C. SQS checks the health of the worker instances.
D. SQS helps to facilitate horizontal scaling of encoding tasks.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Imho the idea for SQS is to improve scalability.
Elastic Beanstalk is checking the health of EC2 instances, not sure if SQS does.

D. SQS helps to facilitate horizontal scaling of encoding tasks.

Yes, this is a great scenario for SQS. "Horizontal scaling" means you have multiple instances involved in the workload (encoding tasks in this case). You can drop messages indicating an encoding job needs to be performed into an SQS queue, immediately making the job notification message accessible to any number of encoding worker instances.

QUESTION 338
When creation of an EBS snapshot is initiated, but not completed, the EBS volume:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.

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

QUESTION 339
What are characteristics of Amazon S3? (Choose two.)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

QUESTION 340
Per the AWS Acceptable Use Policy, penetration testing of EC2 instances:

A. May be performed by AWS, and will be performed by AWS upon customer request.
B. May be performed by AWS, and is periodically performed by AWS.
C. Are expressly prohibited under all circumstances.
D. May be performed by the customer on their own instances with prior authorization from AWS.
E. May be performed by the customer on their own instances, only if performed from EC2 instances

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Our Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. However, because penetration testing and other simulated events are frequently indistinguishable from these activities, we have established a policy for customers to request permission to conduct penetration tests and vulnerability scans to or originating from the AWS environment.

http://aws.amazon.com/security/penetration-testing/

QUESTION 341
You are working with a customer who has 10 TB of archival data that they want to migrate to Amazon Glacier. The customer has a 1-Mbps connection to the Internet. Which service or feature provides the fastest method of getting the data into Amazon Glacier?

A. Amazon Glacier multipart upload
B. AWS Storage Gateway
C. VM Import/Export
D. AWS Import/Export

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can only perform an Amazon Glacier import from devices of 4 TB in size or smaller.
https://docs.aws.amazon.com/es_es/AWSImportExport/latest/DG/createGlacierimportjobs.html
http://docs.aws.amazon.com/amazonglacier/latest/dev/uploading-archive-mpu.html

QUESTION 342
How can you secure data at rest on an EBS volume?

A. Attach the volume to an instance using EC2's SSL interface.
B. Write the data randomly instead of sequentially.
C. Encrypt the volume using the S3 server-side encryption service.
D. Create an IAM policy that restricts read and write access to the volume.
E. Use an encrypted file system on top of the EBS volume.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://aws.amazon.com/blogs/aws/protect-your-data-with-new-ebs-encryption/

QUESTION 343
A customer needs to capture all client connection information from their load balancer every five minutes. The company wants to use this data for analyzing traffic patterns and troubleshooting their applications. Which of the following options meets the customer requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Wxplanation:
Elastic Load Balancing access logs
The access logs for Elastic Load Balancing capture detailed information for all requests made to your load balancer and stores them as log files in the Amazon S3 bucket that you specify. Each log contains details such as the time a request was received, the client's IP address, latencies, request path, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot your back-end applications. For more information, see Monitor Your Load Balancer Using Elastic Load Balancing Access Logs.

QUESTION 344
If you want to launch Amazon Elastic Compute Cloud (EC2) instances and assign each instance a predetermined private IP address you should:

A. Launch the instance from a private Amazon Machine Image (AMI).
B. Assign a group of sequential Elastic IP address to the instances.
C. Launch the instances in the Amazon Virtual Private Cloud (VPC).
D. Launch the instances in a Placement Group.
E. Use standard EC2 instances since each instance gets a private Domain Name Service (DNS) already.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each instance in a VPC has a default network interface (eth0) that is assigned the primary private IP address.

QUESTION 345
You need to configure an Amazon S3 bucket to serve static assets for your public-facing web application. Which methods ensure that all objects uploaded to the bucket are set to public read? (Choose two.)

A. Set permissions on the object to public read during upload.
B. Configure the bucket ACL to set all objects to public read.
C. Configure the bucket policy to set all objects to public read.
D. Use AWS Identity and Access Management roles to set the bucket to public read.
E. Amazon S3 objects default to public read, so no action is needed.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/articles/5050
You can use ACLs to grant permissions to individual AWS accounts; however, it is strongly recommended that you do not grant public access to your bucket using an ACL. So the recommended approach is create bucket policy, but not ACL. Following link give you an example about how to make the bucket content public.
http://docs.aws.amazon.com/AmazonS3/latest/dev/HostingWebsiteOnS3Setup.html#step2-add-bucket-policy-make- content-public

QUESTION 346
A company is storing data on Amazon Simple Storage Service (S3). The company's security policy mandates that data is encrypted at rest. Which of the following methods can achieve this? (Choose three.)

A. Use Amazon S3 server-side encryption with AWS Key Management Service managed keys.
B. Use Amazon S3 server-side encryption with customer-provided keys.
C. Use Amazon S3 server-side encryption with EC2 key pair.
D. Use Amazon S3 bucket policies to restrict access to the data at rest.
E. Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key.
F. Use SSL to encrypt the data while in transit to Amazon S3.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 347
Which procedure for backing up a relational database on EC2 that is using a set of RAIDed EBS volumes for storage minimizes the time during which the database cannot be written to and results in a consistent backup?

A. 1. Detach EBS volumes, 2. Start EBS snapshot of volumes, 3. Re-attach EBS volumes
B. 1. Stop the EC2 Instance. 2. Snapshot the EBS volumes
C. 1. Suspend disk I/O, 2. Create an image of the EC2 Instance, 3. Resume disk I/O
D. 1. Suspend disk I/O, 2. Start EBS snapshot of volumes, 3. Resume disk I/O
E. 1. Suspend disk I/O, 2. Start EBS snapshot of volumes, 3. Wait for snapshots to complete, 4. Resume disk I/O

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
https://aws.amazon.com/cn/premiumsupport/knowledge-center/snapshot-ebs-raid-array/ To create an "application-consistent" snapshot of your RAID array, stop applications from writing to the RAID array, and flush all caches to disk. Then ensure that the associated EC2 instance is no longer writing to the RAID array by taking steps such as freezing the file system, unmounting the RAID array, or *shutting down the associated EC2 instance*. After completing the steps to halt all I/O, take a snapshot of each EBS volume. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-detaching-volume.html You can detach an Amazon EBS volume from an instance explicitly or by terminating the instance. However, if the instance is running, you must first unmount the volume from the instance."

QUESTION 348
A company needs to deploy virtual desktops to its customers in a virtual private cloud, leveraging existing security controls. Which set of AWS services and features will meet the company's requirements?

A. Virtual Private Network connection. AWS Directory Services, and ClassicLink
B. Virtual Private Network connection. AWS Directory Services, and Amazon Workspaces
C. AWS Directory Service, Amazon Workspaces, and AWS Identity and Access Management
D. Amazon Elastic Compute Cloud, and AWS Identity and Access Management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To enable integration, you need to ensure that your domain is reachable via an Amazon Virtual Private Cloud VPC (this could mean that Active Directory domain controllers for your domain are running on Amazon EC2 instances, or that they are reachable via a VPN connection and are located in your on-premises network).

QUESTION 349
After creating a new IAM user which of the following must be done before they can successfully make API calls?

A. Add a password to the user.

B. Enable Multi-Factor Authentication for the user.
C. Assign a Password Policy to the user.
D. Create a set of Access Keys for the user.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_SettingUpUser.html

QUESTION 350
Which of the following are valid statements about Amazon S3? (Choose two.)

A. S3 provides read-after-write consistency for any type of PUT or DELETE
B. Consistency is not guaranteed for any type of PUT or DELETE
C. A successful response to a PUT request only occurs when a complete object is saved.
D. Partially saved objects are immediately readable with a GET after an overwrite PUT.
E. S3 provides eventual consistency for overwrite PUTS and DELETES.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Q: What data consistency model does Amazon S3 employ?

Amazon S3 buckets in all Regions provide read-after-write consistency for PUTS of new objects and eventual consistency for overwrite PUTS and DELETES.

PUT Object

Description

This implementation of the `PUT` operation adds an object to a bucket. You must have `WRITE` permissions on a bucket to add an object to it.

Amazon S3 never adds partial objects; if you receive a success response, Amazon S3 added the entire object to the bucket.

Reference:
http://api-portal.anypoint.mulesoft.com/amazon/api/amazon-s3-api/docs/concepts#DataConsistencyModel

QUESTION 351
You are configuring your company's application to use Auto Scaling and need to move user state information. Which of the following AWS services provides a shared data store with durability and low latency?

A. AWS ElastiCache Memcached
B. Amazon Simple Storage Service
C. Amazon EC2 instance storage
D. Amazon DynamoDB

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Explanation:
https://media.amazonwebservices.com/AWS_Storage_Options.pdf
To speed access to relevant data, many developers pair Amazon S3 with a database, such as Amazon DynamoDB or Amazon RDS. Amazon S3 stores the actual information, and the database serves as the repository for associated metadata (e.g., object name, size, keywords, and so on). Metadata in the database can easily be indexed and queried, making it very efficient to locate an object's reference via a database query. This result can then be used to pinpoint and then retrieve the object itself from Amazon S3.

QUESTION 352
Which features can be used to restrict access to data in S3? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon S3 is secure by default. Only the bucket and object owners originally have access to Amazon S3 resources they create. Amazon S3 supports user authentication to control access to data. You can use access control mechanisms such as bucket policies and Access Control Lists (ACLs) to selectively grant permissions to users and groups of users. You can securely upload/download your data to Amazon S3 via SSL endpoints using the HTTPS protocol. If you need extra security you can use the Server Side Encryption (SSE) option or the Server Side Encryption with Customer-Provide Keys (SSE-C) option to encrypt data stored-at-rest. Amazon S3 provides the encryption technology for both SSE and SSE-C. Alternatively you can use your own encryption libraries to encrypt data before storing it in Amazon S3.
https://aws.amazon.com/s3/faqs/

QUESTION 353
Which of the following are characteristics of a reserved instance? (Choose three.)

A. It can be migrated across Availability Zones
B. It is specific to an Amazon Machine Image (AMI)
C. It can be applied to instances launched by Auto Scaling
D. It is specific to an instance Type
E. It can be used to lower Total Cost of Ownership (TCO) of a system

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use Auto Scaling or other AWS services to launch the On-Demand instances that use your Reserved Instance benefits. For information about launching On-Demand instances, see Launch Your Instance. For information about launching instances using Auto Scaling, see the Auto Scaling User Guide. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts-on-demand-reserved-instances.html https://forums.aws.amazon.com/thread.jspa?threadID=56501

QUESTION 354
Which Amazon Elastic Compute Cloud feature can you query from within the instance to access instance properties?

A. Instance user data
B. Resource tags
C. Instance metadata
D. Amazon Machine Image

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Although you can only access instance metadata and user data from within the instance itself, the data is not protected by cryptographic methods.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html#instancedata-data-retrieval

QUESTION 355
Which of the following requires a custom CloudWatch metric to monitor?

A. Memory Utilization of an EC2 instance
B. CPU Utilization of an EC2 instance
C. Disk usage activity of an EC2 instance
D. Data transfer of an EC2 instance

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudWatch relies on the information provided by this hypervisor, which can only see the most hardware-sided part of the instance's status, including CPU usage (but not load), total memory size (but not memory usage), number of I/O operations on the hard disks (but not it's partition layout and space usage) and network traffic (but not the processes generating it).

QUESTION 356
You are tasked with setting up a Linux bastion host for access to Amazon EC2 instances running in your VPC. Only clients connecting from the corporate external public IP address 72.34.51.100 should have SSH access to the host. Which option will meet the customer requirement?

A. Security Group Inbound Rule: Protocol - TCP. Port Range - 22, Source 72.34.51.100/32
B. Security Group Inbound Rule: Protocol - UDP, Port Range - 22, Source 72.34.51.100/32
C. Network ACL Inbound Rule: Protocol - UDP, Port Range - 22, Source 72.34.51.100/32
D. Network ACL Inbound Rule: Protocol - TCP, Port Range-22, Source 72.34.51.100/0

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 357
A customer needs corporate IT governance and cost oversight of all AWS resources consumed by its divisions. The divisions want to maintain administrative control of the discrete AWS resources they consume and keep those resources separate from the resources of other divisions. Which of the following options, when used together will support the autonomy/control of divisions while enabling corporate IT to maintain governance and cost oversight? (Choose two.)

A. Use AWS Consolidated Billing and disable AWS root account access for the child accounts.
B. Enable IAM cross-account access for all corporate IT administrators in each child account.
C. Create separate VPCs for each division within the corporate IT AWS account.
D. Use AWS Consolidated Billing to link the divisions' accounts to a parent corporate account.
E. Write all child AWS CloudTrail and Amazon CloudWatch logs to each child account's Amazon S3 'Log' bucket.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B & D are correct when used in combination with each other.
C is theoretically correct by itself, but does not work well with the other choices since it involves only a single AWS account, and the other possibly correct choices (B & D) both involve separate AWS accounts. The question specifically states “Which of the following options, when used together”. So C is out.
A is incorrect because you don’t want to disable root access to the child accounts (well, except for their access keys for API calls, deleting those is OK).

E is incorrect because it's the exact opposite of a best practice to centralize logs/security audit info across multiple corporate AWS accounts.

http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html

QUESTION 358
You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to the photos on your site, causing loss to your business. What is an effective method to mitigate this?

A. Remove public read access and use signed URLs with expiry dates.
B. Use CloudFront distributions for static content.
C. Block the IPs of the offending websites in Security Groups.
D. Store photos on an EBS volume of the web server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A signed URL includes additional information, for example, an expiration date and time, that gives you more control over access to your content.

QUESTION 359
You are working with a customer who is using Chef configuration management in their data center. Which service is designed to let the customer leverage existing Chef recipes in AWS?

A. Amazon Simple Workflow Service
B. AWS Elastic Beanstalk
C. AWS CloudFormation
D. AWS OpsWorks

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 360
An Auto-Scaling group spans 3 AZs and currently has 4 running EC2 instances. When Auto Scaling needs to terminate an EC2 instance by default, AutoScaling will: (Choose two.)

A. Allow at least five minutes for Windows/Linux shutdown scripts to complete, before terminating the instance.
B. Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected.

C. Send an SNS notification, if configured to do so.
D. Terminate an instance in the AZ which currently has 2 running EC2 instances.
E. Randomly select one of the 3 AZs, and then terminate an instance in that AZ.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Auto Scaling determines whether there are instances in multiple Availability Zones. If so, it selects the Availability Zone with the most instances and at least one instance that is not protected from scale in. http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingBehavior.InstanceTermination.html

QUESTION 361
When an EC2 instance that is backed by an S3-based AMI is terminated, what happens to the data on the root volume?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Using the legacy S3 based AMIs, either of the above terminates the instance and you lose all local and ephemeral storage (boot disk and /mnt) forever. Hope you remembered to save the important stuff elsewhere.

QUESTION 362
In order to optimize performance for a compute cluster that requires low inter-node latency, which of the following feature should you use?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Reference:
http://aws.amazon.com/ec2/faqs/ (enhanced networking)

QUESTION 363
You have an environment that consists of a public subnet using Amazon VPC and 3 instances that are running in this subnet. These three instances can successfully communicate with other hosts on the Internet. You launch a fourth instance in the same subnet, using the same AMI and security group configuration you used for the others, but find that this instance cannot be accessed from the internet. What should you do to enable Internet access?

A. Deploy a NAT instance into the public subnet.
B. Assign an Elastic IP address to the fourth instance.
C. Configure a publically routable IP Address in the host OS of the fourth instance.
D. Modify the routing table for the public subnet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You launched your instance into a public subnet - a subnet that has a route to an Internet gateway. However, the instance in your subnet also needs a public IP address to be able to communicate with the Internet. By default, an instance in a nondefault VPC is not assigned a public IP address. In this step, you'll allocate an Elastic IP address to your account, and then associate it with your instance.

Visit PassLeader and Download Full Version AWS-Associate Exam Dumps

AWS-Associate Exam Dumps AWS-Associate Exam Questions AWS-Associate PDF Dumps AWS-Associate VCE Dumps http://www.passleader.com/aws-certified-solutions-architect-associate.html

QUESTION 364
You have a distributed application that periodically processes large volumes of data across multiple Amazon EC2 Instances. The application is designed to recover gracefully from Amazon EC2 instance failures. You are required to accomplish this task in the most cost-effective way.
Which of the following will meet your requirements?

A. Spot Instances
B. Reserved instances
C. Dedicated instances
D. On-Demand instances

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Using reserved instances is not the most cost-effective way.
https://aws.amazon.com/blogs/aws/new-scheduled-reserved-instances/ "Scheduled Reserved Instance model allows you to reserve instances for predefined blocks of

time on a recurring basis for a one-year term, with prices that are generally 5 to 10% lower than the equivalent On-Demand rates." You can get spot instances with much lower prices:
https://aws.amazon.com/ec2/spot/pricing/
"Spot instances are also available to run for a predefined duration in hourly increments up to six hours in length at a significant discount (30-45%) compared to On-Demand pricing plus an additional 5% during off-peak times for a total of up to 50% savings."

QUESTION 365
Which of the following are true regarding AWS CloudTrail? (Choose three.)

A. CloudTrail is enabled globally
B. CloudTrail is enabled by default
C. CloudTrail is enabled on a per-region basis
D. CloudTrail is enabled on a per-service basis.
E. Logs can be delivered to a single Amazon S3 bucket for aggregation.
F. CloudTrail is enabled for all available services within a region.
G. Logs can only be processed and delivered to the region in which they are generated.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
A: have a trail with the Apply trail to all regions option enabled.
C: have multiple single region trails.
E: Log files from all the regions can be delivered to a single S3 bucket. Global service events are always delivered to trails that have the Apply trail to all regions option enabled. Events are delivered from a single region to the bucket for the trail. This setting cannot be changed. If you have a single region trail, you should enable the Include global services option. If you have multiple single region trails, you should enable the Include global services option in only one of the trails.
D: Incorrect. Once enabled it is applicable for all the supported services, service can't be selected.

QUESTION 366
You have a content management system running on an Amazon EC2 instance that is approaching 100% CPU utilization. Which option will reduce load on the Amazon EC2 instance?

A. Create a load balancer, and register the Amazon EC2 instance with it
B. Create a CloudFront distribution, and configure the Amazon EC2 instance as the origin
C. Create an Auto Scaling group from the instance using the CreateAutoScalingGroup action
D. Create a launch configuration from the instance using the CreateLaunchConfiguration action

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
You can create an ASG from instance ID
http://docs.aws.amazon.com/AutoScaling/latest/APIReference/API_CreateAutoScalingGroup.html

QUESTION 367
You have a load balancer configured for VPC, and all back-end Amazon EC2 instances are in service. However, your web browser times out when connecting to the load balancer's DNS name. Which options are probable causes of this behavior? (Choose two.)

A. The load balancer was not configured to use a public subnet with an Internet gateway configured
B. The Amazon EC2 instances do not have a dynamically allocated private IP address
C. The security groups or network ACLs are not property configured for web traffic.
D. The load balancer is not configured in a private subnet with a NAT instance.
E. The VPC does not have a VGW configured.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There is no such thing as VGW. Hence E is not correct answer.

QUESTION 368
A company needs to deploy services to an AWS region which they have not previously used. The company currently has an AWS identity and Access Management (IAM) role for the Amazon EC2 instances, which permits the instance to have access to Amazon DynamoDB. The company wants their EC2 instances in the new region to have the same privileges. How should the company achieve this?

A. Create a new IAM role and associated policies within the new region
B. Assign the existing IAM role to the Amazon EC2 instances in the new region
C. Copy the IAM role and associated policies to the new region and attach it to the instances
D. Create an Amazon Machine Image (AMI) of the instance and copy it to the desired region using the AMI Copy feature

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
Which of the following notification endpoints or clients are supported by Amazon Simple Notification Service? (Choose two.)

A. Email
B. CloudFront distribution
C. File Transfer Protocol
D. Short Message Service
E. Simple Network Management Protocol

Correct Answer: AD

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://docs.aws.amazon.com/sns/latest/dg/welcome.html

QUESTION 370
Which set of Amazon S3 features helps to prevent and recover from accidental data loss?

A. Object lifecycle and service access logging
B. Object versioning and Multi-factor authentication
C. Access controls and server-side encryption
D. Website hosting and Amazon S3 policies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. In addition to that, they have made it a requirement that delete operations on versioned data can only be done using MFA (Multi factor authentication).

Reference:
http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 371
A company needs to monitor the read and write IOPs metrics for their AWS MySQL RDS instance and send real-time alerts to their operations team. Which AWS services can accomplish this? (Choose two.)

A. Amazon Simple Email Service
B. Amazon CloudWatch
C. Amazon Simple Queue Service
D. Amazon Route 53
E. Amazon Simple Notification Service

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B: Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console, or consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice.

E: Use Amazon RDS DB events to monitor failovers. For example, you can be notified by text message or email when a DB instance fails over. Amazon RDS uses the Amazon Simple Notification Service (Amazon SNS) to provide notification when an Amazon RDS event occurs.

QUESTION 372
A company is preparing to give AWS Management Console access to developers Company policy mandates identity federation and role-based access control. Roles are currently assigned using groups in the corporate Active Directory. What combination of the following will give developers access to the AWS console? (Select 2) Choose 2 answers

A. AWS Directory Service AD Connector
B. AWS Directory Service Simple AD
C. AWS Identity and Access Management groups
D. AWS identity and Access Management roles
E. AWS identity and Access Management users

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html

QUESTION 373
You are deploying an application to collect votes for a very popular television show. Millions of users will submit votes using mobile devices. The votes must be collected into a durable, scalable, and highly available data store for real-time public tabulation. Which service should you use?

A. Amazon DynamoDB
B. Amazon Redshift
C. Amazon Kinesis
D. Amazon Simple Queue Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This example looks at using AWS Lambda and Amazon API Gateway to build a dynamic voting
application, which receives votes via SMS, aggregates the totals into Amazon DynamoDB, and uses Amazon Simple Storage Service (Amazon S3) to display the results in real time.
http://www.allthingsdistributed.com/2016/06/aws-lambda-serverless-reference-architectures.html

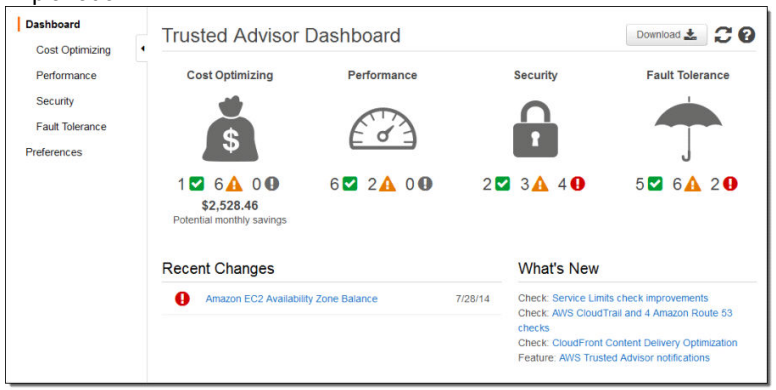
QUESTION 374
The Trusted Advisor service provides insight regarding which four categories of an AWS account?

A. Security, fault tolerance, high availability, and connectivity

B. Security, access control, high availability, and performance
C. Performance, cost optimization, security, and fault tolerance
D. Performance, cost optimization, access control, and connectivity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:



Explanation:
Reference:
https://aws.amazon.com/blogs/aws/category/aws-trusted-advisor/

QUESTION 375
You are deploying an application to track GPS coordinates of delivery trucks in the United States. Coordinates are transmitted from each delivery truck once every three seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple consumers. Which service should you use to implement data ingestion?

A. Amazon Kinesis
B. AWS Data Pipeline
C. Amazon AppStream
D. Amazon Simple Queue Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/streaming-data/

QUESTION 376

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Web identity federation - You can let users sign in using a well-known third party identity provider such as Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) 2.0 compatible provider. AWS STS web identity federation supports Login with Amazon, Facebook, Google, and any OpenID Connect (OICD)-compatible identity provider.

QUESTION 377
You have an application running on an Amazon Elastic Compute Cloud instance, that uploads 5 GB video objects to Amazon Simple Storage Service (S3). Video uploads are taking longer than expected, resulting in poor application performance. Which method will help improve performance of your application?

A. Enable enhanced networking
B. Use Amazon S3 multipart upload
C. Leveraging Amazon CloudFront, use the HTTP POST method to reduce latency.
D. Use Amazon Elastic Block Store Provisioned IOPs and use an Amazon EBS-optimized instance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Using multipart upload provides the following advantages:
- Improved throughput - You can upload parts in parallel to improve throughput.
- Quick recovery from any network issues - Smaller part size minimizes the impact of restarting a failed upload due to a network error.
- Pause and resume object uploads - You can upload object parts over time. Once you initiate a multipart upload there is no expiry; you must explicitly complete or abort the multipart upload.
- Begin an upload before you know the final object size.
- You can upload an object as you are creating it.
http://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html

QUESTION 378
A customer wants to track access to their Amazon Simple Storage Service (S3) buckets and also use this information for their internal security and access audits. Which of the following will meet the Customer requirement?

A. Enable AWS CloudTrail to audit all Amazon S3 bucket access.

B. Enable server access logging for all required Amazon S3 buckets.
C. Enable the Requester Pays option to track access via AWS Billing
D. Enable Amazon S3 event notifications for Put and Post.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References:
http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html
http://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html

QUESTION 379
A company is deploying a two-tier, highly available web application to AWS. Which service provides durable storage for static content while utilizing lower Overall CPU resources for the web tier?

A. Amazon EBS volume
B. Amazon S3
C. Amazon EC2 instance store
D. Amazon RDS instance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 380
You are designing a web application that stores static assets in an Amazon Simple Storage Service (S3) bucket. You expect this bucket to immediately receive over 150 PUT requests per second. What should you do to ensure optimal performance?

A. Use multi-part upload.
B. Add a random prefix to the key names.
C. Amazon S3 will automatically manage performance at this scale.
D. Use a predictable naming scheme, such as sequential numbers or date time sequences, in the key names

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you anticipate that your workload will consistently exceed 100 requests per second, you should avoid sequential key names. If you must use sequential numbers or date and time patterns in key names, add a random prefix to the key name. The randomness of the prefix more evenly distributes key names across multiple index partitions.

Examples of introducing randomness are provided later in this topic.

QUESTION 381
When will you incur costs with an Elastic IP address (EIP)?

A. When an EIP is allocated.
B. When it is allocated and associated with a running instance.
C. When it is allocated and associated with a stopped instance.
D. Costs are incurred regardless of whether the EIP is associated with a running instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You are allowed one EIP to be attached to a running instance at no charge. otherwise, it will incur a small fee. in this case, the instance is stopped, and thus, the EIP will be billed at the normal rate.
http://aws.amazon.com/ec2/pricing/

QUESTION 382
A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region. Test is peered to both Prod and Dev. All VPCs have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to Prod to speed up time to market. Which of the following options helps the company accomplish this?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 383
Which of the following instance types are available as Amazon EBS-backed only? (Choose two.)

A. General purpose T2
B. General purpose M3
C. Compute-optimized C4
D. Compute-optimized C3

E. Storage-optimized 12

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html

QUESTION 384
A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The customer also uses Amazon Route 53 to manage their public DNS. How should the customer configure the DNS zone apex record to point to the load balancer?

A. Create an A record pointing to the IP address of the load balancer
B. Create a CNAME record pointing to the load balancer DNS name.
C. Create a CNAME record aliased to the load balancer DNS name.
D. Create an A record aliased to the load balancer DNS name

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/using-domain-names-with-elb.html

QUESTION 385
You try to connect via SSH to a newly created Amazon EC2 instance and get one of the following error messages:
"Network error: Connection timed out" or "Error connecting to [instance], reason: -> Connection timed out: connect,"
You have confirmed that the network and security group rules are configured correctly and the instance is passing status checks. What steps should you take to identify the source of the behavior? Choose 2 answers

A. Verify that the private key file corresponds to the Amazon EC2 key pair assigned at launch.
B. Verify that your IAM user policy has permission to launch Amazon EC2 instances.
C. Verify that you are connecting with the appropriate user name for your AMI.
D. Verify that the Amazon EC2 Instance was launched with the proper IAM role.
E. Verify that your federation trust to AWS has been established.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

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

QUESTION 386
A customer is running a multi-tier web application farm in a virtual private cloud (VPC) that is not connected to their corporate network. They are connecting to the VPC over the Internet to manage all of their Amazon EC2 instances running in both the public and private subnets. They have only authorized the bastion-security-group with Microsoft Remote Desktop Protocol (RDP) access to the application instance security groups, but the company wants to further limit administrative access to all of the instances in the VPC. Which of the following Bastion deployment scenarios will meet this requirement?

A. Deploy a Windows Bastion host on the corporate network that has RDP access to all instances in the VPC,
B. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow SSH access to the bastion from anywhere.
C. Deploy a Windows Bastion host with an Elastic IP address in the private subnet, and restrict RDP access to the bastion from only the corporate public IP addresses.
D. Deploy a Windows Bastion host with an auto-assigned Public IP address in the public subnet, and allow RDP access to the bastion from only the corporate public IP addresses.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 387
A customer has a single 3-TB volume on-premises that is used to hold a large repository of images and print layout files. This repository is growing at 500 GB a year and must be presented as a single logical volume. The customer is becoming increasingly constrained with their local storage capacity and wants an off-site backup of this data, while maintaining low-latency access to their frequently accessed data. Which AWS Storage Gateway configuration meets the customer requirements?

A. Gateway-Cached volumes with snapshots scheduled to Amazon S3
B. Gateway-Stored volumes with snapshots scheduled to Amazon S3
C. Gateway-Virtual Tape Library with snapshots to Amazon S3
D. Gateway-Virtual Tape Library with snapshots to Amazon Glacier

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.aws.amazon.com/storagegateway/latest/userguide/storage-gateway-cached-concepts.html

QUESTION 388
You are building an automated transcription service in which Amazon EC2 worker instances process an uploaded audio file and generate a text file. You must store both of these files in the same durable storage until the text file is retrieved. You do not know what the storage capacity requirements are. Which storage option is both cost-efficient and scalable?

A. Multiple Amazon EBS volume with snapshots
B. A single Amazon Glacier vault
C. A single Amazon S3 bucket

D. Multiple instance stores

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 389
You need to pass a custom script to new Amazon Linux instances created in your Auto Scaling group. Which feature allows you to accomplish this?

A. User data
B. EC2Config service
C. IAM roles
D. AWS Config

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html#user-data-shell-scripts Not B, because EC2Config is used for Windows instances:
http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/UsingConfig_WinAMI.html

QUESTION 390
Which of the following services natively encrypts data at rest within an AWS region? (Choose two.)

A. AWS Storage Gateway
B. Amazon DynamoDB
C. Amazon CloudFront
D. Amazon Glacier
E. Amazon Simple Queue Service

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://media.amazonwebservices.com/AWS_Securing_Data_at_Rest_with_Encryption.pdf (page 12)

QUESTION 391
A company is building software on AWS that requires access to various AWS services. Which configuration should be used to ensure mat AWS credentials (i.e., Access

Key ID/Secret Access Key combination) are not compromised?

A. Enable Multi-Factor Authentication for your AWS root account.
B. Assign an IAM role to the Amazon EC2 instance.
C. Store the AWS Access Key ID/Secret Access Key combination in software comments.
D. Assign an IAM user to the Amazon EC2 Instance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Use roles for applications that run on Amazon EC2 instances.
Applications that run on an Amazon EC2 instance need credentials in order to access other AWS services. To provide credentials to the application in a secure way, use IAM roles. A role is an entity that has its own set of permissions, but that isn't a user or group. Roles also don't have their own permanent set of credentials the way IAM users do. In the case of Amazon EC2, IAM dynamically provides temporary credentials to the EC2 instance, and these credentials are automatically rotated for you.
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-roles-with-ec2

QUESTION 392
Which of the following are true regarding encrypted Amazon Elastic Block Store (EBS) volumes? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

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

QUESTION 393
A company is deploying a new two-tier web application in AWS. The company has limited staff and requires high availability, and the application requires complex queries and table joins. Which configuration provides the solution for the company's requirements?

A. MySQL Installed on two Amazon EC2 Instances in a single Availability Zone
B. Amazon RDS for MySQL with Multi-AZ
C. Amazon ElastiCache
D. Amazon DynamoDB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When is it appropriate to use DynamoDB instead of a relational database? From our own experience designing and operating a highly available, highly scalable ecommerce platform, we have come to realize that relational databases should only be used when an application really needs the complex query, table join and transaction capabilities of a full-blown relational database. In all other cases, when such relational features are not needed, a NoSQL database service like DynamoDB offers a simpler, more available, more scalable and ultimately a lower cost solution.

QUESTION 394
A t2.medium EC2 instance type must be launched with what type of Amazon Machine Image (AMI)?

A. An Instance store Hardware Virtual Machine AMI
B. An Instance store Paravirtual AMI
C. An Amazon EBS-backed Hardware Virtual Machine AMI
D. An Amazon EBS-backed Paravirtual AMI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You must launch a T2 instance using an HVM AMI. For more information, see Linux AMI Virtualization Types. You must launch your T2 instances using an EBS volume as the root device. For more information, see Amazon EC2 Root Device Volume.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html

QUESTION 395
You manually launch a NAT AMI in a public subnet. The network is properly configured. Security groups and network access control lists are property configured. Instances in a private subnet can access the NAT. The NAT can access the Internet. However, private instances cannot access the Internet. What additional step is required to allow access from the private instances?

A. Enable Source/Destination Check on the private Instances.
B. Enable Source/Destination Check on the NAT instance.
C. Disable Source/Destination Check on the private instances.
D. Disable Source/Destination Check on the NAT instance.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Disabling Source/Destination Checks.
Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. However, a NAT instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance. You can disable the SrcDestCheck attribute for a NAT instance that's either running or stopped using the console or the command line.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

QUESTION 396
Which of the following approaches provides the lowest cost for Amazon Elastic Block Store snapshots while giving you the ability to fully restore data?

A. Maintain two snapshots: the original snapshot and the latest incremental snapshot.
B. Maintain a volume snapshot; subsequent snapshots will overwrite one another
C. Maintain a single snapshot the latest snapshot is both Incremental and complete.
D. Maintain the most current snapshot, archive the original and incremental to Amazon Glacier.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-snapshot.html

QUESTION 397
An existing application stores sensitive information on a non-boot Amazon EBS data volume attached to an Amazon Elastic Compute Cloud instance. Which of the following approaches would protect the sensitive data on an Amazon EBS volume?

A. Upload your customer keys to AWS CloudHSM. Associate the Amazon EBS volume with AWS CloudHSM. Re-mount the Amazon EBS volume.
B. Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume. Delete the old Amazon EBS volume.
C. Unmount the EBS volume. Toggle the encryption attribute to True. Re-mount the Amazon EBS volume.
D. Snapshot the current Amazon EBS volume. Restore the snapshot to a new, encrypted Amazon EBS volume. Mount the Amazon EBS volume

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html To migrate data between encrypted and unencrypted volumes:
1. Create your destination volume (encrypted or unencrypted, depending on your need) by following the procedures in Creating an Amazon EBS Volume.
2. Attach the destination volume to the instance that hosts the data to migrate. For more information, see Attaching an Amazon EBS Volume to an Instance. procedures in Making an Amazon EBS Volume Available for Using. For Linux instances, you can create a mount point at /mnt/destination and mount the destination volume there.
4. Copy the data from your source directory to the destination volume. It may be most convenient to use a bulk-copy utility for this.

QUESTION 398
A US-based company is expanding their web presence into Europe. The company wants to extend their AWS infrastructure from Northern Virginia (us-east-1) into the Dublin (eu-west-1) region. Which of the following options would enable an equivalent experience for users on both continents?

A. Use a public-facing load balancer per region to load-balance web traffic, and enable HTTP health checks.
B. Use a public-facing load balancer per region to load-balance web traffic, and enable sticky sessions.
C. Use Amazon Route 53, and apply a geolocation routing policy to distribute traffic across both regions.
D. Use Amazon Route 53, and apply a weighted routing policy to distribute traffic across both regions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Explanation:
Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location from which DNS queries originate. For example, you might want all queries from Africa to be routed to a web server with an IP address of 192.0.2.111.
Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.
http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-weighted

QUESTION 399
Which of the following are use cases for Amazon DynamoDB? (Choose three)

A. Storing BLOB data.
B. Managing web sessions.
C. Storing JSON documents.
D. Storing metadata for Amazon S3 objects.
E. Running relational joins and complex updates.
F. Storing large amounts of infrequently accessed data.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Ideal Usage Patterns
•Amazon DynamoDB is ideal for existing or new applications that need a flexible NoSQL database with low read and write latencies, and the ability to scale storage and throughput up or down as needed without code changes or downtime.
•Use cases require a highly available and scalable database because downtime or performance degradation has an immediate negative impact on an organization's business. for e.g. mobile apps, gaming, digital ad serving, live voting and audience interaction for live events, sensor networks, log ingestion, access control for web-based content, metadata storage for Amazon S3 objects, e-commerce shopping carts, and web session management

QUESTION 400

A customer implemented AWS Storage Gateway with a gateway-cached volume at their main office. An event takes the link between the main and branch office offline. Which methods will enable the branch office to access their data? (Choose three.)

A. Use a HTTPS GET to the Amazon S3 bucket where the files are located.
B. Restore by implementing a lifecycle policy on the Amazon S3 bucket.
C. Make an Amazon Glacier Restore API call to load the files into another Amazon S3 bucket within four to six hours.
D. Launch a new AWS Storage Gateway instance AMI in Amazon EC2, and restore from a gateway snapshot.
E. Create an Amazon EBS volume from a gateway snapshot, and mount it to an Amazon EC2 instance.
F. Launch an AWS Storage Gateway virtual iSCSI device at the branch office, and restore from a gateway snapshot.

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A is certainly not right, because files persisted by Storage Gateway to S3 are not visible, let alone be accessible.
https://forums.aws.amazon.com/thread.jspa?threadID=109748
B is invalid option because you cannot apply Lifecycle Policies because AWS Storage Gateway
does not give you that option. Cached Volumes are never stored to Glacier and hence “C” is not valid.

QUESTION 401
A company has configured and peered two VPCs: VPC-1 and VPC-2. VPC-1 contains only private subnets, and VPC-2 contains only public subnets. The company uses a single AWS Direct Connect connection and private virtual interface to connect their on-premises network with VPC-1. Which two methods increases the fault tolerance of the connection to VPC-1? (Choose two.)

A. Establish a hardware VPN over the internet between VPC-2 and the on-premises network.
B. Establish a hardware VPN over the internet between VPC-1 and the on-premises network.
C. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
D. Establish a new AWS Direct Connect connection and private virtual interface in a different AWS region than VPC-1.
E. Establish a new AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 402
The new DB Instance that is created when you promote a Read Replica retains the backup window period.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"The new DB instance that is created when you promote a Read Replica retains the backup retention period, backup window period, and parameter group of the former Read Replica source." http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

QUESTION 403
With which AWS orchestration service can you implement Chef recipes?

A. CloudFormation
B. Elastic Beanstalk
C. Opsworks
D. Lambda

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

O AWS OpsWorks é um serviço de gerenciamento de configurações que usa o Chef, uma plataforma de automação que trata configurações de servidor como código. O OpsWorks usa o Chef para automatizar a forma como os servidores são configurados, implantados e gerenciados em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou em ambientes de computação locais. O OpsWorks oferece dois serviços, o AWS OpsWorks for Chef Automate e o AWS OpsWorks Stacks.

QUESTION 404
You work for a construction company that has their production environment in AWS. The production environment consists of 3 identical web servers that are launched from a standard Amazon linux AMI using Auto Scaling. The web servers are launched in to the same public subnet and belong to the same security group. They also sit behind the same ELB. You decide to do some test and dev and you launch a 4th EC2 instance in to the same subnet and same security group. Annoyingly your 4th instance does not appear to have internet connectivity. What could be the cause of this?

A. You need to update your routing table so as to provide a route out for this instance.
B. Assign an elastic IP address to the fourth instance.
C. You have not configured a NAT in the public subnet.
D. You have not configured a routable IP address in the host OS of the fourth instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 405
You need to add a route to your routing table in order to allow connections to the internet from your subnet. What route should you add?

A. Destination: 192.168.1.258/0 --> Target: your Internet gateway
B. Destination: 0.0.0.0/33 --> Target: your virtual private gateway
C. Destination: 0.0.0.0/0 --> Target: 0.0.0.0/24
D. Destination: 10.0.0.0/32 --> Target: your virtual private gateway
E. Destination: 0.0.0.0/0 --> Target: your Internet gateway

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 406
You have developed a new web application in us-west-2 that requires six Amazon Elastic Compute Cloud (EC2) instances running at all times. You have three availability zones available in that region (us-west-2a, us-west-2b, and us-west-2c). You need 100 percent fault tolerance if any single Availability Zone in us-west-2 becomes unavailable. How would you do this, each answer has 2 answers, select the answer with BOTH correct answers.

A. Answer 1 - Us-west-2a with two EC2 instances, us-west-2b with two EC2 instances, and us-west-2c with two EC2 instances. Answer 2 - Us-west-2a with six EC2 instances, us-west-2b with six EC2 instances, and us-west-2c with no EC2 instances
B. Answer 1 - Us-west-2a with six EC2 instances, us-west-2b with six EC2 instances, and us-west-2c with no EC2 instances. Answer 2 - Us-west-2a with three EC2 instances, us-west-2b with three EC2 instances, and us-west-2c with three EC2 instances.
C. Answer 1 - Us-west-2a with three EC2 instances, us-west-2b with three EC2 instances, and us-west-2c with no EC2 instances. Answer 2 - Us-west-2a with three EC2 instances, us-west-2b with three EC2 instances, and us-west-2c with three EC2 instances.
D. Answer 1 - Us-west-2a with three EC2 instances, us-west-2b with three EC2 instances, and us-west-2c with three EC2 instances. Answer 2 - Us-west-2a with four EC2 instances, us-west-2b with two EC2 instances, and us-west-2c with two EC2 instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 407

You work for a major news network in Europe. They have just released a new app which allows users to report on events as and when they happen using their mobile phone. Users are able to upload pictures from the app and then other users will be able to view these pics. Your organization expects this app to grow very quickly, essentially doubling it's user base every month. The app uses S3 to store the media and you are expecting sudden and large increases in traffic to S3 when a major news event takes place (as people will be uploading content in huge numbers). You need to keep your storage costs to a minimum however and it does not matter if some objects are lost. Which storage media should you use to keep costs as low as possible?

A. S3 - Infrequently Accessed Storage.
B. S3 - Reduced Redundancy Storage (RRS).
C. Glacier.
D. S3 - Provisioned IOPS.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



Amazon S3 Reduced Redundancy Storage

A Reduced Redundancy Storage (RRS) é uma opção de armazenamento do Amazon S3 que permite aos clientes reduzir custos armazenando dados reprodutíveis e não críticos com níveis de redundância mais baixos do que o armazenamento padrão do Amazon S3. Ele fornece uma solução altamente disponível e econômica para distribuir ou compartilhar conteúdo armazenado de forma durável em outro lugar ou para o armazenamento de miniaturas, mídia transcodificada ou outros dados processados que podem ser facilmente reproduzidos. A opção RRS armazena objetos em vários dispositivos em diversas instalações, oferecendo durabilidade 400 vezes maior que a de uma unidade de disco típica, mas não replica objetos tantas vezes quanto o armazenamento padrão do Amazon S3.

O Reduced Redundancy Storage é:

- Disponibilidade respaldada pelo Acordo de Nível de Serviço do Amazon S3.
- Projetado para fornecer 99,99% de durabilidade e 99,99% de disponibilidade de objetos em um determinado ano. Este nível de durabilidade corresponde a uma média de perda anual esperada de 0,01% de objetos.
- Projetado para sustentar a perda de dados em uma única instalação.

Comece a trabalhar com a AWS hoje

Experimente o Amazon S3 gratuitamente

O nível gratuito da AWS inclui 5 GB de armazenamento, 20.000 solicitações GET e 2.000 solicitações PUT com o Amazon S3.

Consulte os detalhes do nível gratuito da AWS »

QUESTION 408
You work for a famous bakery who are deploying a hybrid cloud approach. Their legacy IBM AS400 servers will remain on premise within their own datacenter however they will need to be able to communicate to the AWS environment over a site to site VPN connection. What do you need to do to establish the VPN connection?

A. Connect to the environment using AWS Direct Connect.
B. Assign a public IP address to your Amazon VPC Gateway.
C. Create a dedicated NAT and deploy this to the public subnet.
D. Update your route table to add a route for the NAT to 0.0.0.0/0.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 409
Your company has decided to set up a new AWS account for test and dev purposes. They already use AWS for production, but would like a new account dedicated for test and dev so as to not accidentally break the production environment. You launch an exact replica of your production environment using a CloudFormation template that your company uses in production. However CloudFormation fails. You use the exact same CloudFormation template in production, so the failure is something to do with your new AWS account. The CloudFormation template is trying to launch 60 new EC2 instances in a single AZ. After some research you discover that the problem is;

A. For all new AWS accounts there is a soft limit of 20 EC2 instances per region. You should submit the limit increase form and retry the template after your limit has been increased.
B. For all new AWS accounts there is a soft limit of 20 EC2 instances per availability zone. You should submit the limit increase form and retry the template after your limit has been increased.
C. You cannot launch more than 20 instances in your default VPC, instead reconfigure the CloudFormation template to provision the instances in a custom VPC.
D. Your CloudFormation template is configured to use the parent account and not the new account. Change the account number in the CloudFormation template and relaunch the template.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 410
You are a solutions architect who has been asked to do some consulting for a US company that produces re-useable rocket parts. They have a new web application that needs to be built and this application must be stateless. Which three services could you use to achieve this?

A. AWS Storage Gateway, Elasticache & ELB
B. ELB, Elasticache & RDS
C. Cloudwatch, RDS & DynamoDb
D. RDS, DynamoDB & Elasticache.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 411
You run an automobile reselling company that has a popular online store on AWS. The application sits behind an Auto Scaling group and requires new instances of the Auto Scaling group to identify their public and private IP addresses. How can you achieve this?

A. By using Ipconfig for windows or Ifconfig for Linux.
B. By using a cloud watch metric.
C. Using a Curl or Get Command to get the latest meta-data from http://169.254.169.254/latest/meta-data/
D. Using a Curl or Get Command to get the latest user-data from http://169.254.169.254/latest/user-data/

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 412
You are a solutions architect working for a biotech company who is pioneering research in immunotherapy. They have developed a new cancer treatment that may be able to cure up to 94% of cancers. They store their research data on S3, however recently an intern accidentally deleted some critical files. You've been asked to prevent this from happening in the future. What options below can prevent this?

A. Make sure the interns can only access data on S3 using signed URLs.
B. Enable S3 versioning on the bucket & enable Enable Multifactor Authentication (MFA) on the bucket.
C. Use S3 Infrequently Accessed storage to store the data on.
D. Create an IAM bucket policy that disables deletes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 413
You are a security architect working for a large antivirus company. The production environment has recently been moved to AWS and is in a public subnet. You are able to view the production environment over HTTP however when your customers try to update their virus definition files over a custom port, that port is blocked. You log in to the console and you allow traffic in over the custom port. How long will this take to take effect?

A. Straight away but to the new instances only.
B. Immediately.
C. After a few minutes this should take effect.
D. Straight away to the new instances, but old instances must be stopped and restarted before the new rules apply.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 414
You have been asked to identify a service on AWS that is a durable key value store. Which of the services below meets this definition?

A. Mobile Hub
B. Kinesis
C. Simple Storage Service (S3)
D. Elastic File Service (EFS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415
By definition a public subnet within a VPC is one that;

A. In it's routing table it has at least one route that uses an Internet Gateway (IGW).
B. Has at least one route in it's routing table that routes via a Network Address Translation (NAT) instance.
C. Where the the Network Access Control List (NACL) permitting outbound traffic to 0.0.0.0/0.
D. Has had the public subnet check box ticked when setting up this subnet in the VPC console.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 416
You work in the genomics industry and you process large amounts of genomic data using a nightly Elastic Map Reduce (EMR) job. This job processes a single 3 Tb file which is stored on S3. The EMR job runs on 3 on-demand core nodes and four on-demand task nodes. The EMR job is now taking longer than anticipated and you have

been asked to advise how to reduced the completion time?

A. Use four Spot Instances for the task nodes rather than four On-Demand instances.
B. You should reduce the input split size in the MapReduce job configuration and then adjust the number of simultaneous mapper tasks so that more tasks can be processed at once.
C. Store the file on Elastic File Service instead of S3 and then mount EFS as an independent volume for your core nodes.
D. Configure an independent VPC in which to run the EMR jobs and then mount EFS as an independent volume for your core nodes.
E. Enable termination protection for the job flow.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 417
You work for a toy company that has a busy online store. As you are approaching christmas you find that your store is getting more and more traffic. You ensure that the web tier of your store is behind an Auto Scaling group, however you notice that the web tier is frequently scaling, sometimes multiple times in an hour, only to scale back after peak usage. You need to prevent this so that Auto Scaling does not scale as rapidly, just to scale back again. What option would help you to achieve this?

A. Configure Auto Scaling to terminate your oldest instances first, then adjust your CloudWatch alarm.
B. Configure Auto Scaling to terminate your newest instances first, then adjust your CloudWatch alarm.
C. Change your Auto Scaling so that it only scales at scheduled times.
D. Modify the Auto Scaling group cool-down timers & modify the Amazon CloudWatch alarm period that triggers your Auto Scaling scale down policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Auto Scaling Cooldowns

The Auto Scaling cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that Auto Scaling doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple scaling policy, Auto Scaling waits for the cooldown period to complete before resuming scaling activities. When you manually scale your Auto Scaling group, the default is not to wait for the cooldown period, but you can override the default and honor the cooldown period. Note that if an instance becomes unhealthy, Auto Scaling does not wait for the cooldown period to complete before replacing the unhealthy instance.

QUESTION 418
You are a student currently learning about the different AWS services. Your employer asks you to tell him a bit about Amazon's glacier service. Which of the following best describes the use cases for Glacier?

A. Infrequently accessed data & data archives
B. Hosting active databases
C. Replicating Files across multiple availability zones and regions
D. Frequently Accessed Data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 419
You are a systems administrator and you need to monitor the health of your production environment. You decide to do this using Cloud Watch, however you notice that you cannot see the health of every important metric in the default dash board. Which of the following metrics do you need to design a custom cloud watch metric for, when monitoring the health of your EC2 instances?

A. CPU Usage
B. Memory usage
C. Disk read operations
D. Network in
E. Estimated charges

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 420
You working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security.

A. Save the API credentials to your php files.
B. Don't save your API credentials. Instead create a role in IAM and assign this role to an EC2 instance when you first create it.
C. Save your API credentials in a public Github repository.
D. Pass API credentials to the instance using instance userdata.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 421
You work for a cosmetic company which has their production website on AWS. The site itself is in a two-tier configuration with web servers in the front end and database servers at the back end. The site uses using Elastic Load Balancing and Auto Scaling. The databases maintain consistency by replicating changes to each other as and when they occur. This requires the databases to have extremely low latency. Your website needs to be highly redundant and must be designed so that if one availability zone goes offline and Auto Scaling cannot launch new instances in the remaining Availability Zones the site will not go offline. How can the current architecture be enhanced to ensure this?

A. Deploy your site in three different AZ's within the same region. Configure the Auto Scaling minimum to handle 50 percent of the peak load per zone.
B. Deploy your website in 2 different regions. Configure Route53 with a failover routing policy and set up health checks on the primary site.
C. Deploy your site in three different AZ's within the same region. Configure the Auto Scaling minimum to handle 33 percent of the peak load per zone.
D. Deploy your website in 2 different regions. Configure Route53 with Weighted Routing. Assign a weight of 25% to region 1 and a weight of 75% to region 2.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 422
You have been asked to create VPC for your company. The VPC must support both Internet-facing web applications (ie they need to be publicly accessible) and internal private applications (i.e. they are not publicly accessible and can be accessed only over VPN). The internal private applications must be inside a private subnet. Both the internet-facing and private applications must be able to leverage at least three Availability Zones for high availability. At a minimum, how many subnets must you create within your VPC to achieve this?

A. 5
B. 3
C. 4
D. 6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 423
You are hosting a MySQL database on the root volume of an EC2 instance. The database is using a large amount of IOPs and you need to increase the IOPs available to it. What should you do?

A. Migrate the database to an S3 bucket.
B. Migrate the database to Glacier.
C. Add 4 additional EBS SSD volumes and create a RAID 10 using these volumes.
D. Use Cloud Front to cache the database.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424
You have uploaded a file to S3. What HTTP code would indicate that the upload was successful?

A. HTTP 404
B. HTTP 501
C. HTTP 200
D. HTTP 307

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 425
You run a website which hosts videos and you have two types of members, premium fee paying members and free members. All videos uploaded by both your premium

members and free members are processed by a fleet of EC2 instances which will poll SQS as videos are uploaded. However you need to ensure that your premium fee paying members videos have a higher priority than your free members. How do you design SQS?

A. SQS allows you to set priorities on individual items within the queue, so simply set the fee paying members at a higher priority than your free members.
B. Create two SQS queues, one for premium members and one for free members. Program your EC2 fleet to poll the premium queue first and if empty, to then poll your free members SQS queue.
C. SQS would not be suitable for this scenario. It would be much better to use SNS to encode the videos.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 426
Amazon's Redshift uses which block size for its columnar storage?

A. 2KB
B. 8KB
C. 16KB
D. 32KB
E. 1024KB / 1MB

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 427
When creating an RDS instance you can select which availability zone in which to deploy your instance.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 428
You can select a specific Availability Zone in which to place your DynamoDB Table

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 429
In order to enable encryption at rest using EC2 and Elastic Block Store you need to

A. Configure encryption when creating the EBS volume
B. Configure encryption using the appropriate Operating Systems file system
C. Configure encryption using X.509 certificates
D. Mount the EBS volume in to S3 and then encrypt the bucket using a bucket policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 430
Amazon S3 provides;

A. Unlimited File Size for Objects
B. Unlimited Storage
C. A great place to run a No SQL database from
D. The ability to act as a web server for dynamic content (i.e. can query a database)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 431
Amazon S3 buckets in all other regions (other than US Standard) do not provide eventual consistency for overwrite PUTS and DELETES.

A. True

B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 432
Amazon S3 buckets in all other regions (other than US Standard) provide read-after-write consistency for PUTS of new objects.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 433
To retrieve instance metadata or userdata you will need to use the following IP Address;

A. http://127.0.0.1
B. http://192.168.0.254
C. http://10.0.0.1
D. http://169.254.169.254

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 434
You have an EC2 instance which needs to find out both its private IP address and its public IP address. To do this you need to;

A. Run IPCONFIG (Windows) or IFCONFIG (Linux)
B. Retrieve the instance Metadata from http://169.254.169.254/latest/meta-data/
C. Retrieve the instance Userdata from http://169.254.169.254/latest/meta-data/
D. Use the following command; AWS EC2 displayIP

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 435
It is possible to transfer a reserved instance from one Availability Zone to another.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 436
When you create new subnets within a custom VPC, by default they can communicate with each other, across availability zones.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

QUESTION 437
You can have 1 subnet stretched across multiple availability zones.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 438

Using SAML (Security Assertion Markup Language 2.0) you can give your federated users single sign-on (SSO) access to the AWS Management Console.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 439
Which of the services below do you get root access to?

A. Elasticache & Elastic MapReduce
B. RDS & DynamoDB
C. EC2 & Elastic MapReduce
D. Elasticache & DynamoDB

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 440
You are creating your own relational database on an EC2 instance and you need to maximize IOPS performance. What can you do to achieve this goal?

A. Add a single additional volume to the EC2 instance with provisioned IOPS.
B. Create the database on an S3 bucket.
C. Add multiple additional volumes with provisioned IOPS and then create a RAID 0 stripe across those volumes.
D. Attach the single volume to multiple EC2 instances so as to maximize performance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 441
You can add multiple volumes to an EC2 instance and then create your own RAID 5/RAID 10/RAID 0 configurations using those volumes.

A. True

B. False

Correct Answer: A
Section: (none)
Explanation

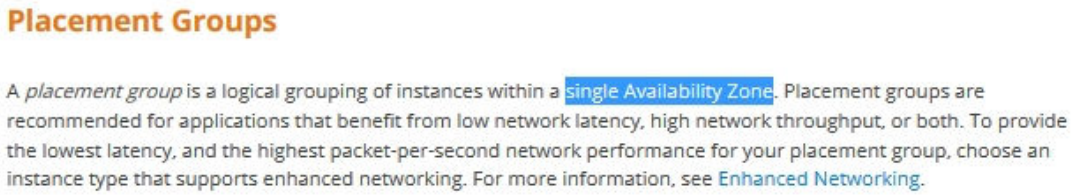
Explanation/Reference:

QUESTION 442
Placement Groups can be created across 2 or more Availability Zones.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:



Explanation:

QUESTION 443
Amazon S3 buckets in the US Standard region do not provide eventual consistency.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

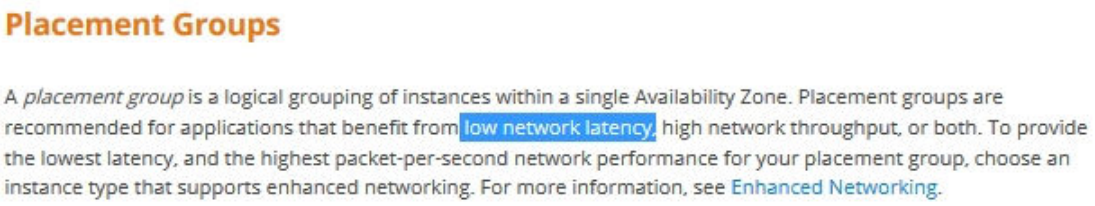
Explanation/Reference:

QUESTION 444
You have a high performance compute application and you need to minimize network latency between EC2 instances as much as possible. What can you do to achieve this?

A. Use Elastic Load Balancing to load balance traffic between availability zones
B. Create a CloudFront distribution and to cache objects from an S3 bucket at Edge Locations.
C. Create a placement group within an Availability Zone and place the EC2 instances within that placement group.
D. Deploy your EC2 instances within the same region, but in different subnets and different availability zones so as to maximize redundancy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:



QUESTION 445
You are appointed as your company's Chief Security Officer and you want to be able to track all changes made to your AWS environment, by all users and at all times, in all regions. What AWS service should you use to achieve this?

A. CloudAudit
B. CloudWatch
C. CloudTrail
D. CloudDetective

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

How do I know which user made a particular change to my AWS infrastructure?

Issue

I want to track which users are making changes to my AWS resources and infrastructure. How do I do this?

Resolution

Although AWS doesn't track this information by default, you can enable AWS CloudTrail for your resources, which will create logs of API calls made on your account and deliver them to an S3 bucket you specify. This will allow you to track changes to your resources, and see which user made the changes.

For more information about setting up CloudTrail, see Getting Started with CloudTrail.

Keywords

CloudTrail, API, log

QUESTION 446
Which of the following is NOT a valid SNS subscribers?

A. Lambda
B. SWF
C. SQS
D. Email
E. HTTPS
F. SMS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 447

You are hosting a website in Ireland called aloud.guru and you decide to have a static DR site available on S3 in the event that your primary site would go down. Your bucket name is also called "acloudguru". What would be the S3 URL of the static website?

A. https://acloudguru.s3-website-eu-west-1.amazonaws.com
B. https://s3-eu-east-1.amazonaws.com/acloudguru
C. https://acloudguru.s3-website-us-east-1.amazonaws.com
D. https://s3-eu-central-1.amazonaws.com/acloudguru

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 448
You are designing a site for a new start up which generates cartoon images for people automatically. Customers will log on to the site, upload an image which is stored in S3. The application then passes a job to AWS SQS and a fleet of EC2 instances poll the queue to receive new processing jobs. These EC2 instances will then turn the picture in to a cartoon and will then need to store the processed job somewhere. Users will typically download the image once (immediately), and then never download the image again. What is the most commercially feasible method to store the processed images?

A. Rather than use S3, store the images inside a BLOB on RDS with Multi-AZ configured for redundancy.
B. Store the images on S3 RRS, and create a lifecycle policy to delete the image after 24 hours.
C. Store the images on glacier instead of S3.
D. Use elastic block storage volumes to store the images.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 449
You have started a new role as a solutions architect for an architectural firm that designs large sky scrapers in the Middle East. Your company hosts large volumes of data and has about 250Tb of data on internal servers. They have decided to store this data on S3 due to the redundancy offered by it. The company currently has a telecoms line of 2Mbps connecting their head office to the internet. What method should they use to import this data on to S3 in the fastest manner possible.

A. Upload it directly to S3
B. Purchase and AWS Direct connect and transfer the data over that once it is installed.
C. AWS Data pipeline
D. AWS Import/Export

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 450
Which of the following is not a valid configuration type for AWS Storage gateway.

A. Gateway-accessed volumes
B. Gateway-cached volumes
C. Gateway-stored volumes
D. Gateway-Virtual Tape Library

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 451
What are the different types of virtualization available on EC2?

A. Pseudo-Virtual (PV) & Hardware Virtual Module (HSM)
B. Para-Virtual (PV) & Hardware Virtual Machine (HVM)
C. Pseudo-Virtual (PV) & Hardware Virtual Machine (HVM)
D. Para-Virtual (PV) & Hardware Virtual Module (HSM)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 452
You work for a market analysis firm who are designing a new environment. They will ingest large amounts of market data via Kinesis and then analyze this data using Elastic Map Reduce. The data is then imported in to a high performance NoSQL Cassandra database which will run on EC2 and then be accessed by traders from around the world. The database volume itself will sit on 2 EBS volumes that will be grouped into a RAID 0 volume. They are expecting very high demand during peak times, with an IOPS performance level of approximately 15,000. Which EBS volume should you recommend?

A. Magnetic
B. General Purpose SSD
C. Provisioned IOPS (PIOPS)
D. Turbo IOPS (TIOPS)

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of transactional workloads	Highest-performance SSD volume designed for mission-critical applications	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume • Large database workloads, such as: ○ MongoDB ○ Cassandra ○ Microsoft SQL Server ○ MySQL ○ PostgreSQL ○ Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS/Volume**	10,000	20,000	500	250

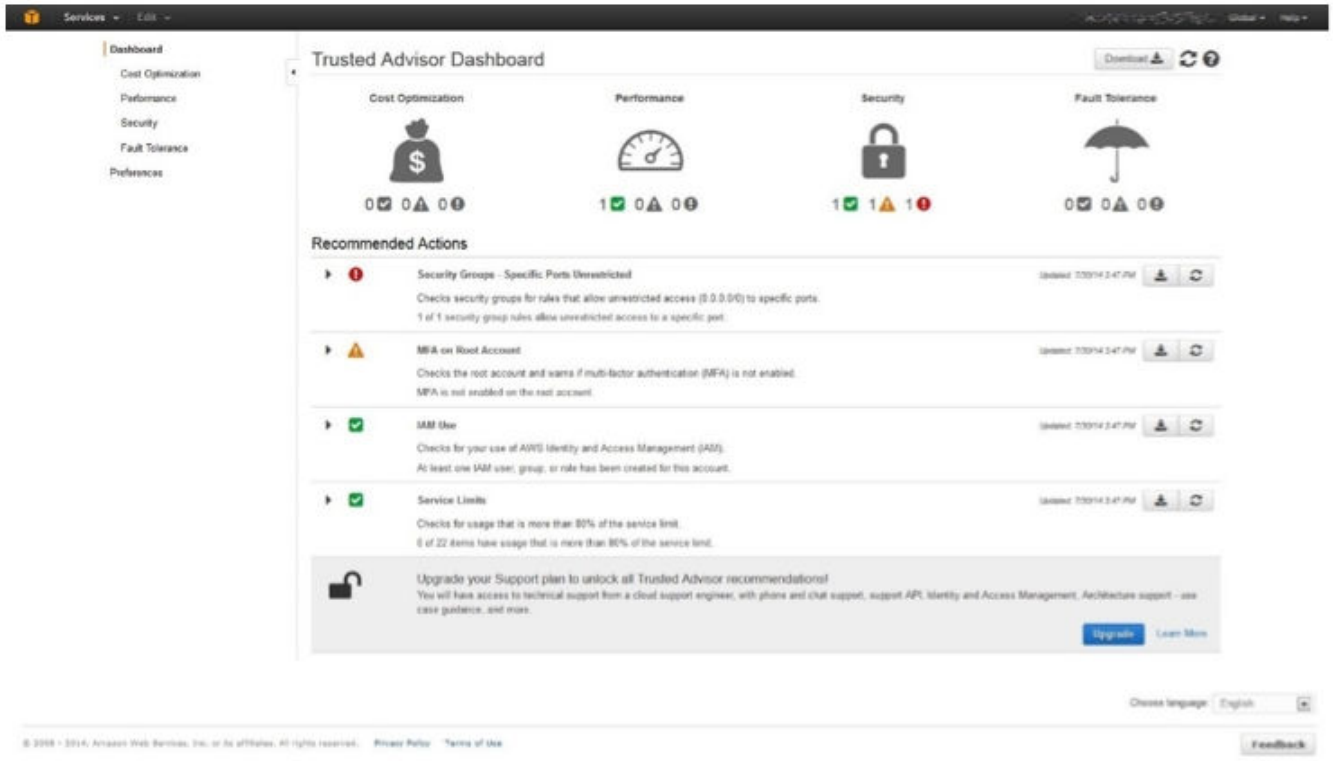
QUESTION 453
Which of the following is not a service of the security category of the AWS trusted advisor service?

A. Security Groups - Specific Ports Unrestricted
B. MFA on Root Account
C. IAM Use
D. Vulnerability scans on existing VPCs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The four free checks, available in the AWS Management Console, help you build a more secure and responsive cloud environment: **Security Groups - Specific Ports Unrestricted, Service Limits, IAM Use, and MFA on Root Account.**

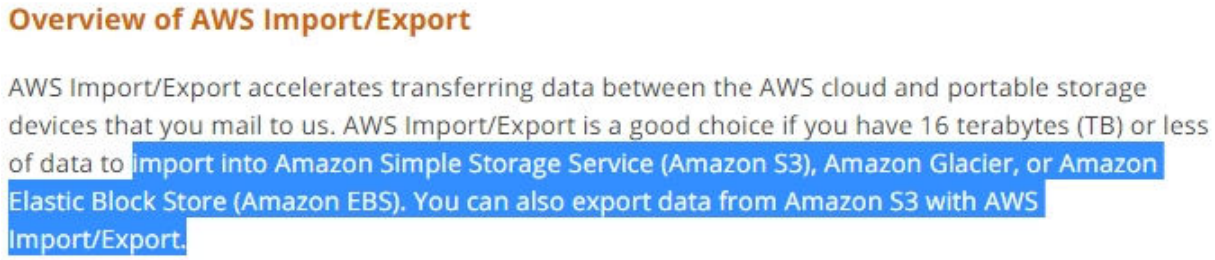


QUESTION 454
Which of the following is not supported by AWS Import/Export?

A. Import to Amazon S3
B. Export from Amazon S3
C. Import to Amazon EBS
D. Import to Amazon Glacier
E. Export to Amazon Glacier

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:



QUESTION 455
You are a solutions architect working for a large oil and gas company. Your company runs their production environment on AWS and has a custom VPC. The VPC contains 3 subnets, 1 of which is public and the other 2 are private. Inside the public subnet is a fleet of EC2 instances which are the result of an autoscaling group. All EC2 instances are in the same security group. Your company has created a new custom application which connects to mobile devices using a custom port. This application has been rolled out to production and you need to open this port globally to the internet. What steps should you take to do this, and how quickly will the change occur?

A. Open the port on the existing network Access Control List. Your EC2 instances will be able to communicate on this port after a reboot.
B. Open the port on the existing network Access Control List. Your EC2 instances will be able to communicate over this port immediately.
C. Open the port on the existing security group. Your EC2 instances will be able to communicate over this port immediately.
D. Open the port on the existing security group. Your EC2 instances will be able to communicate over this port as soon as the relevant Time To Live (TTL) expires.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 456
When trying to grant an amazon account access to S3 using access control lists what method of identification should you use to identify that account with?

A. The email address of the account or the canonical user ID
B. The AWS account number
C. The ARN
D. An email address with a 2FA token

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 457
Which of the following services allows you root access (i.e. you can login using SSH)?

A. Elastic Load Balancer
B. Elastic Map Reduce
C. Elasticache
D. RDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When you use SSH with AWS, you are connecting to an EC2 instance, which is a virtual server running in the cloud. When working with Amazon EMR, the most common use of SSH is to connect to the EC2 instance that is acting as the master node of the cluster.

QUESTION 458
What function of an AWS VPC is stateless?

A. Security Groups
B. Elastic Load Balancers
C. Network Access Control Lists
D. EC2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 459
Amazon S3 buckets in all Regions provide which of the following?

A. Read-after-write consistency for PUTS of new objects AND Strongly consistent for POST & DELETES
B. Read-after-write consistency for POST of new objects AND Eventually consistent for overwrite PUTS & DELETES
C. Read-after-write consistency for PUTS of new objects AND Eventually consistent for overwrite PUTS & DELETES
D. Read-after-write consistency for POST of new objects AND Strongly consistent for POST & DELETES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Q: What data consistency model does Amazon S3 employ?

Amazon S3 buckets in all Regions provide read-after-write consistency for PUTS of new objects and eventual consistency for overwrite PUTS and DELETES.

QUESTION 460
You are a solutions architect working for a large digital media company. Your company is migrating their production estate to AWS and you are in the process of setting up access to the AWS console using Identity Access Management (IAM). You have created 5 users for your system administrators. What further steps do you need to take to enable your system administrators to get access to the AWS console?

A. Generate an Access Key ID & Secret Access Key, and give these to your system administrators.
B. Enable multi-factor authentication on their accounts and define a password policy.
C. Generate a password for each user created and give these passwords to your system administrators.
D. Give the system administrators the secret access key and access key id, and tell them to use these credentials to log in to the AWS console.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 461
Amazon Web Services offer 3 different levels of support, which of the below are valid support levels.

A. Corporate, Business, Developer
B. Enterprise, Business, Developer
C. Enterprise, Business, Free Tier
D. Enterprise, Company, Free Tier

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 462
In Identity and Access Management, when you first create a new user, certain security credentials are automatically generated. Which of the below are valid security credentials?

A. Access Key ID, Authorized Key
B. Private Key, Secret Access Key
C. Private Key, Authorized Key
D. Access Key ID, Secret Access Key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 463
What are the valid methodologies for encrypting data on S3?

A. Server Side Encryption (SSE)-S3, SSE-C, SSE-KMS or a client library such as Amazon S3 Encryption Client.
B. Server Side Encryption (SSE)-S3, SSE-A, SSE-KMS or a client library such as Amazon S3 Encryption Client.
C. Server Side Encryption (SSE)-S3, SSE-C, SSE-SSL or a client library such as Amazon S3 Encryption Client.
D. Server Side Encryption (SSE)-S3, SSE-C, SSE-SSL or a server library such as Amazon S3 Encryption Client.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 464

You are a solutions architect working for a company that specializes in ingesting large data feeds (using Kinesis) and then analyzing these feeds using Elastic Map Reduce (EMR). The results are then stored on a custom MySQL database which is hosted on an EC2 instance which has 3 volumes, the root/boot volume, and then 2 additional volumes which are striped in to a RAID 1. Your company recently had an outage and lost some key data and have since decided that they will need to run nightly back ups. Your application is only used during office hours, so you can afford to have some down time in the middle of the night if required. You decide to take a snapshot of all three volumes every 24 hours. In what manner should you do this?

A. Take a snapshot of each volume independently, while the EC2 instance is running.
B. Stop the EC2 instance and take a snapshot of each EC2 instance independently. Once the snapshots are complete, start the EC2 instance and ensure that all relevant volumes are remounted.
C. Add two additional volumes to the existing RAID 0 volume and mirror these volumes creating a RAID 10. Take a snap of only the two new volumes.
D. Create a read replica of the existing EC2 instance and then take your snapshots from the read replica and not the live EC2 instance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 465
A Provisioned IOPS SSD volume must be at least _____ GB in size.

A. 1
B. 6
C. 20
D. 4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 466
In Amazon CloudWatch, which metric should I be checking to ensure that your DB Instance has enough free storage space?

A. FreeStorage
B. FreeStorageVolume
C. FreeStorageSpace
D. FreeStorageAllocation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 467
After an Amazon EC2-VPC instance is launched, can I change the VPC security groups it belongs to?

A. No
B. Yes
C. Only if you are the root user
D. Only if the tag "VPC_Change_Group" is true

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 468
Is there a method or command in the IAM system to allow or deny access to a specific instance?

A. Only for VPC based instances
B. Yes
C. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
E[planation:
http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow
- 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 overrides this default.
- An explicit deny overrides any allows.

QUESTION 469
What is the default VPC security group limit?

A. 500
B. 50
C. 5
D. There is no limit

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 470
What does ec2-create-group do with respect to the Amazon EC2 security groups?

A. Creates a new rule inside the security group.
B. Creates a new security group for use with your account.
C. Creates a new group inside the security group.
D. Groups the user created security groups in to a new group for easy access.

Correct Answer: B
Section: (none)
Explanation

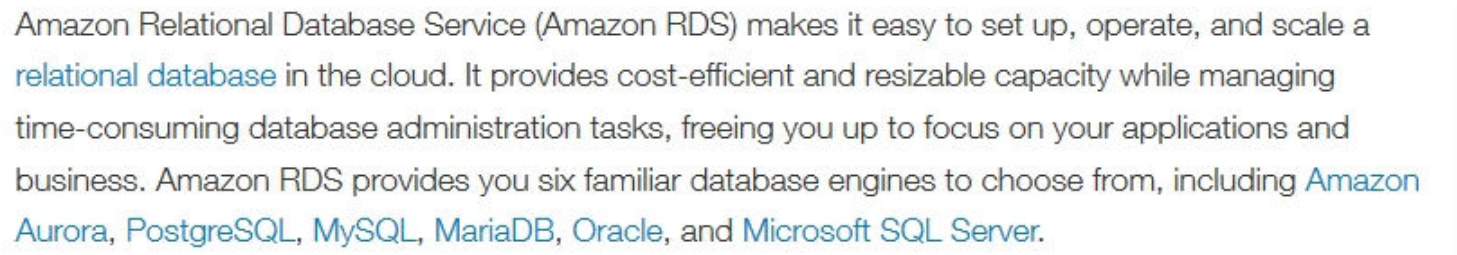
Explanation/Reference:

QUESTION 471
How many relational database engines does RDS currently support?

A. Three: MySQL, Oracle and Microsoft SQL Server.
B. Just two: MySQL and Oracle.
C. Six: Amazon Aurora, Oracle, Microsoft SQL Server, PostgreSQL, MySQL and MariaDB.
D. Just one: MySQL.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS provides you six familiar database engines to choose from, including Amazon Aurora, Oracle, Microsoft SQL Server, PostgreSQL, MySQL and MariaDB.
https://aws.amazon.com/rds/?nc1=h_ls



QUESTION 472
By default, what happens to ENIs that are automatically created and attached to EC2 instances when the attached instance terminates?

A. Remain as is
B. Terminate
C. Hibernate
D. Pause

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

By default, elastic network interfaces that are automatically created and attached to instances using the console are set to terminate when the instance terminates. However, network interfaces created using the command line interface aren't set to terminate when the instance terminates.
Source:http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#change_term_behavior

QUESTION 473
In a management network scenario, which interface on the instance handles public-facing traffic?

A. Primary network interface
B. Subnet interface
C. Secondary network interface

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 474
Does AWS allow for the use of Multi Factor Authentication tokens?

A. Yes, with both hardware or virtual MFA devices
B. Yes, but only virtual MFA devices.
C. Yes, but only physical (hardware) MFA devices.
D. No

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 475
Multi-AZ deployment is supported for Microsoft SQL Server DB Instances.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 476
What is a Security Group?

A. None of these.
B. A list of users that can access Amazon EC2 instances.
C. An Access Control List (ACL) for AWS resources.
D. It acts as a virtual firewall that controls the traffic for one or more instances.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 477
What is the default per account limit of Elastic IPs?

A. 1
B. 3
C. 5
D. 0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 478
New database versions will automatically be applied to AWS RDS instances as they become available.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 479
Reserved Instances are available for Multi-AZ Deployments.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 480
While creating an EC2 snapshot using the API, which Action should I be using?

A. MakeSnapShot
B. FreshSnapshot
C. DeploySnapshot
D. CreateSnapshot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 481
Using Amazon IAM, I can give permissions based on organizational groups?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 482
SQL Server stores logins and passwords in the master database.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

There are two authentications

Windows authetication
The credentials for which are not stored in SQl Server database and managed by windows/AD. There would be entry for windows autheticated logins in master database with respective SID but password would be with Active directory.

SQL Server authetication.
For 2nd we have password stored in hash format you can see it from sys.sql_logins. The information about SQl server logins are stored in master database and each login has SID repective to it. Only SA login has same SID no matter what server it is. That is why when you move database by backup restore mechanism users are moved not logins and you finally have to create logins(if already not there) and map it to users. This is generally called as troubleshooting orpahned users

QUESTION 483
While performing volume status checks using volume status checks, if the status is insufficient-data, what does it mean?

A. checks may still be in progress on the volume
B. check has passed
C. check has failed
D. there is no such status

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

> Volume status checks are automated tests that run every 5 minutes and return a pass or fail status. If all checks pass, the status of the volume is ok. If a check fails, the status of the volume is impaired. If the status is insufficient-data, the checks may still be in progress on the volume.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html

QUESTION 484
What is the maximum groups an IAM user be a member of?

A. 20
B. 5
C. 10
D. 15

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Resource Limit
Access keys assigned to an IAM user 2
Access keys assigned to the AWS account root user 2
Aliases for an AWS account 1
Groups an IAM user can be a member of 10
Identity providers (IdPs) associated with an IAM SAML provider object 10
Keys per SAML provider 10
Login profiles for an IAM user 1
Managed policies attached to an IAM group 10
Managed policies attached to an IAM role 10
Managed policies attached to an IAM user 10
MFA devices in use by an IAM user 1
MFA devices in use by the AWS account root user 1
Roles in an instance profile 1
SAML providers in an AWS account 100
Signing certificates assigned to an IAM user 2
SSH public keys assigned to an IAM user 5
Versions of a managed policy that can be stored 5

QUESTION 485
What is the maximum write throughput I can provision per table for a single DynamoDB table?

A. 5,000 us east, 1,000 all other regions
B. 100,000 us east, 10, 000 all other regions
C. Designed to scale without limits, but if you go beyond 40,000 us east/10,000 all other regions you have to contact AWS first.
D. There is no limit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 486
Out of the striping options available for the EBS volumes, which one has the following disadvantage : 'Doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you're mirroring all writes to a pair of volumes, limiting how much you can stripe.' ?

A. Raid 5
B. Raid 6
C. Raid 1
D. Raid 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 487
Disabling automated backups disables the point-in-time recovery feature.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 488
Can an EBS volume be attached to more than one EC2 instance at the same time?

A. No
B. Yes.
C. Only EC2-optimized EBS volumes.
D. Only in read mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
EBS is network attached storage that can only be attached to one instance at a time https://aws.amazon.com/ebs/getting-started/
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html

QUESTION 489
In the basic monitoring package for EC2, Amazon CloudWatch provides the following metrics:

A. web server visible metrics such as number failed transaction requests
B. operating system visible metrics such as memory utilization
C. database visible metrics such as number of connections
D. hypervisor visible metrics such as CPU utilization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: EXEMPLO ONLINE

QUESTION 490
Which of the following will occur when an EC2 instance in a VPC with an associated Elastic IP is stopped and started? (Choose 2 answers)

A. The Elastic IP will be dissociated from the instance
B. All data on instance-store devices will be lost
C. All data on EBS (Elastic Block Store) devices will be lost
D. The ENI (Elastic Network Interface) is detached
E. The underlying host for the instance is changed

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html

QUESTION 491
You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
B. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
C. Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
D. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

QUESTION 492
Amazon Glacier is designed for:
(Choose 2 answers)

A. active database storage.
B. infrequently accessed data.
C. data archives.
D. frequently accessed data.
E. cached session data

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 493
Which is an operational process performed by AWS for data security?

A. AES-256 encryption of data stored on any shared storage device
B. Decommissioning of storage devices using industry-standard practices
C. Background virus scans of EBS volumes and EBS snapshots
D. Replication of data across multiple AWS Regions
E. Secure wiping of EBS data when an EBS volume is unmounted

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.”

QUESTION 494
A customer's nightly EMR job processes a single 2-TB data file stored on Amazon Simple Storage Service (S3). The EMR job runs on two On-Demand core nodes and three On-Demand task nodes. Which of the following may help reduce the EMR job completion time?
Choose 2 answers

A. Use three Spot Instances rather than three On-Demand instances for the task nodes.
B. Change the input split size in the MapReduce job configuration.
C. Use a bootstrap action to present the S3 bucket as a local filesystem.
D. Launch the core nodes and task nodes within an Amazon Virtual Cloud.
E. Adjust the number of simultaneous mapper tasks.
F. Enable termination protection for the job flow.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:SIMULADO PAGO

QUESTION 495
Which route must be added to your routing table in order to allow connections to the Internet from your subnet?

A. Destination: 0.0.0.0/0 --> Target: your Internet gateway
B. Destination: 192.168.1.257/0 --> Target: your Internet gateway
C. Destination: 0.0.0.0/33 --> Target: your virtual private gateway
D. Destination: 0.0.0.0/0 --> Target: 0.0.0.0/24
E. Destination: 10.0.0.0/32 --> Target: your virtual private gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:SIMULADO PAGO

QUESTION 496
You are deploying an application on EC2 that must call AWS APIs. What method of securely passing credentials to the application should you use?

A. Use AWS Identity and Access Management roles for EC2 instances.
B. Pass API credentials to the instance using instance userdata.
C. Embed the API credentials into your JAR files.
D. Store API credentials as an object in Amazon Simple Storage Service.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: SIMULADO PAGO

QUESTION 497
You have a business-critical two-tier web app currently deployed in two AZs in a single region, using Elastic Load Balancing and Auto Scaling. The app depends on synchronous replication (very low latency connectivity) at the database layer. The application needs to remain fully available even if one application AZ goes off-line, and Auto Scaling cannot launch new instances in the remaining Availability Zones. How can the current architecture be enhanced to ensure this?

A. Deploy in two regions using Weighted Round Robin (WRR), with Auto Scaling minimums set for 50 percent peak load per Region.
B. Deploy in two regions using Weighted Round Robin (WRR), with Auto Scaling minimums set for 100 percent peak load per region.
C. Deploy in three Availability Zones, with Auto Scaling minimum set to handle 50 percent peak load per zone.
D. Deploy in three Availability Zones, with Auto Scaling minimum set to handle 33 percent peak load per zone.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 498
You are developing a highly available web application using stateless web servers. Which services are suitable for storing session state data?
Choose 3 answers

A. Amazon CloudWatch
B. Amazon Relational Database Service (RDS)
C. Elastic Load Balancing
D. Amazon ElastiCache
E. AWS Storage Gateway
F. Amazon DynamoDB

Correct Answer: BDF

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://aws.amazon.com/caching/session-management/

QUESTION 499
Which of the following requires a custom CloudWatch metric to monitor?

A. Memory use
B. CPU use
C. Disk read operations
D. Network in
E. Estimated charges

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 500
You receive a Spot Instance at a bid of $0.05/hr. After 30 minutes, the Spot Price increases to $0.06/hr and your Spot Instance is terminated by AWS. What was the total EC2 compute cost of running your Spot Instance?

A. $0.00
B. $0.02
C. $0.03
D. $0.05
E. $0.06

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://aws.amazon.com/ec2/faqs/#spot-instances

QUESTION 501
You have been tasked with creating a VPC network topology for your company. The VPC network must support both Internet-facing applications and internally-facing applications accessed only over VPN. Both Internet-facing and internally-facing applications must be able to leverage at least three AZs for high availability. At a minimum, how many subnets must you create within your VPC to accommodate these requirements?

A. 2
B. 3
C. 4
D. 6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-basics.html

QUESTION 502
What combination of the following options will protect S3 objects from both accidental deletion and accidental overwriting?
Choose 2 answers

A. Enable S3 versioning on the bucket.
B. Access S3 data using only signed URLs.
C. Disable S3 delete using an IAM bucket policy.
D. Enable S3 Reduced Redundancy Storage.
E. Enable multi-factor authentication (MFA) protected access.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 503
In reviewing the Auto Scaling events for your application you notice that your application is scaling up and down multiple times in the same hour. What design choice could you make to optimize for cost while preserving elasticity?
Choose 2 answers

A. Modify the Auto Scaling policy to use scheduled scaling actions
B. Modify the Auto Scaling group termination policy to terminate the oldest instance first.
C. Modify the Auto Scaling group cool-down timers.
D. Modify the Amazon CloudWatch alarm period that triggers your Auto Scaling scale down policy.
E. Modify the Auto Scaling group termination policy to terminate the newest instance first.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 504
A VPC public subnet is one that:

A. Has at least one route in its associated routing table that uses an Internet Gateway (IGW).
B. Includes a route in its associated routing table via a Network Address Translation (NAT) instance.
C. Has a Network Access Control List (NACL) permitting outbound traffic to 0.0.0.0/0.
D. Has the Public Subnet option selected in its configuration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html
If a subnet's traffic is routed to an Internet gateway, the subnet is known as a public subnet.

QUESTION 505
A startup company hired you to help them build a mobile application, that will ultimately store billions of images and videos in S3. The company is lean on funding, and wants to minimize operational costs, however, they have an aggressive marketing plan, and expect to double their current installation base every six months. Due to the nature of their business, they are expecting sudden and large increases in traffic to and from S3, and need to ensure that it can handle the performance needs of their application. What other information must you gather from this customer in order to determine whether S3 is the right option?

A. You must know how many customers the company has today, because this is critical in understanding what their customer base will be in two years.
B. You must find out the total number of requests per second at peak usage.
C. You must know the size of the individual objects being written to S3, in order to properly design the key namespace.
D. In order to build the key namespace correctly, you must understand the total amount of storage needs for each S3 bucket.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:SIMULADO PAGO

QUESTION 506
How can software determine the public and private IP addresses of the EC2 instance that it is running on?

A. Query the local instance metadata.
B. Query the local instance userdata.
C. Query the appropriate Amazon CloudWatch metric.
D. Use an ipconfig or ifconfig command.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

QUESTION 507
What action is required to establish a VPC VPN connection between an on-premises data center and an Amazon VPC virtual private gateway?

A. Modify the main route table to allow traffic to a network address translation instance.
B. Use a dedicated network address translation instance in the public subnet.
C. Assign a static Internet-routable IP address to an Amazon VPC customer gateway.
D. Establish a dedicated networking connection using AWS Direct Connect.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html

QUESTION 508
You have an application running in us-west-2 that requires six EC2 instances running at all times. With three AZs available in that region (us-west-2a, us-west-2b, and us-west-2c), which of the following deployments provides 100 percent fault tolerance if any single AZ in us-west-2 becomes unavailable?
Choose 2 answers

A. Us-west-2a with two EC2 instances, us-west-2b with two EC2 instances, and us-west-2c with two EC2 instances
B. Us-west-2a with three EC2 instances, us-west-2b with three EC2 instances, and us-west-2c with no EC2 instances
C. Us-west-2a with four EC2 instances, us-west-2b with two EC2 instances, and us-west-2c with two EC2 instances
D. Us-west-2a with six EC2 instances, us-west-2b with six EC2 instances, and us-west-2c with no EC2 instances
E. Us-west-2a with three EC2 instances, us-west-2b with three EC2 instances, and us-west-2c with three EC2 instances

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
option A : 2 2 2
option B : 3 3 –
option C : 4 2 2
option D : 6 6 –
option E : 3 3 3

so if one availability zone fails you need to have a backup of 6 instances running
only D & E has that chance

QUESTION 509
After creating a new AWS account, you use the API to request 40 on-demand EC2 instances in a single AZ. After 20 successful requests, subsequent requests failed. What could be a reason for this issue, and how would you resolve it?

A. You encountered a soft limit of 20 instances per region. Submit the limit increase form and retry the failed requests once approved.
B. AWS allows you to provision no more than 20 instances per Availability Zone. Select a different Availability Zone and retry the failed request.
C. You need to use Amazon Virtual Private Cloud (VPC) in order to provision more than 20 instances in a single Availability Zone. Simply terminate the resources already provisioned and re-launch them all in a VPC.
D. You encountered an API throttling situation and should try the failed requests using an exponential decay retry algorithm.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2

QUESTION 510
Which of the following is a durable key-value store?

A. Amazon Simple Storage Service
B. Amazon Simple Workflow Service
C. Amazon Simple Queue Service
D. Amazon Simple Notification Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
S3 is basically a key-value store. Another keyword is “durable”.
http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingObjects.html

QUESTION 511
Is an edge location in AWS the same as a region?

A. True
B. False

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

A region is a data center in a certain part of the globe which is used to host aws services. An AZ is a combination of one or more data centers in a given region.An edge location is where end users access services located at AWS. You can refer to the below link which has the up-to date details on the current AZ's , regions and edge locations provided by AWS.

https://aws.amazon.com/about-aws/global-infrastructure/

The correct answer is: **False**

QUESTION 512
When it comes to API credentials, what is the best practise recommended by AWS?

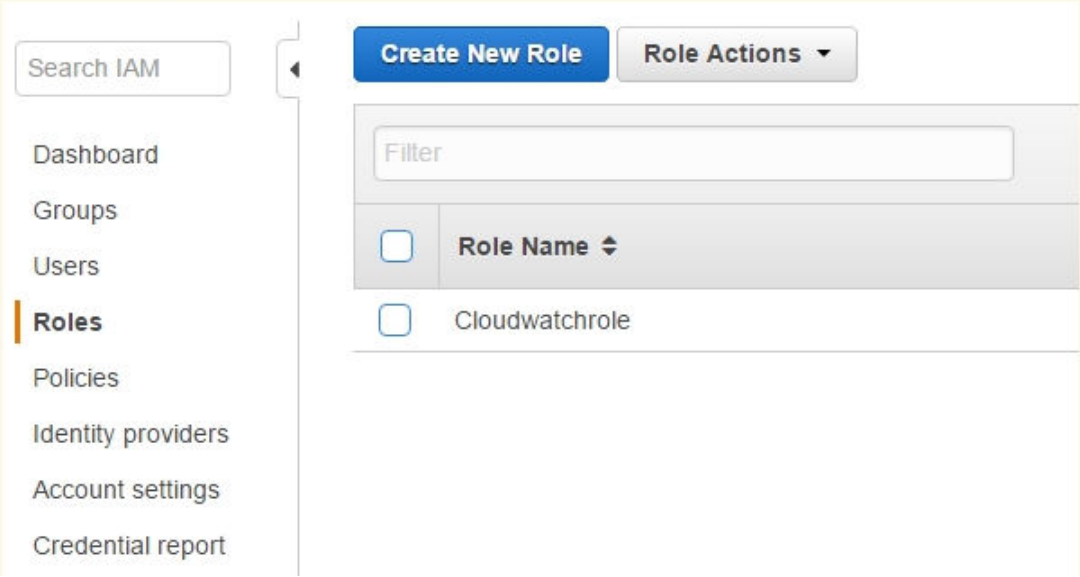
A. Create a role which has the necessary and can be assumed by the EC2 instance.
B. Use the API credentials from an EC2 instance.
C. Use the API credentials from a bastion host.
D. Use the API credentials from a NAT Instance.

Correct Answer: A
Section: (none)
Explanation

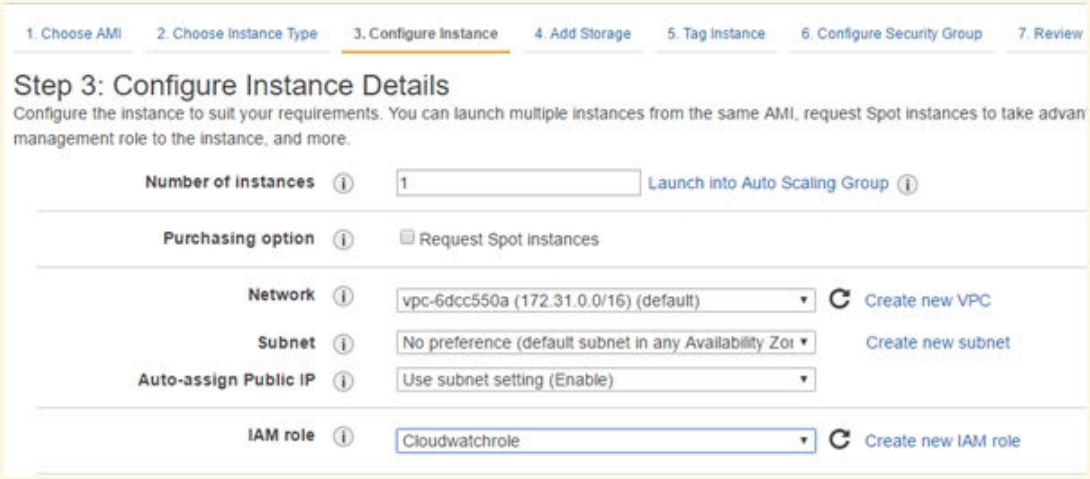
Explanation/Reference:
Explanation:

The best practise highlighted by AWS is always create a role which has select permissions and when creating an EC2 instance, ensure the role is attached to the EC2 instance.

So in the Security credentials in AWS, you first need to go to the Security Credentials section and create a role. The below example shows the creation of a Cloudwatch role which has the permissions to publish to cloudwatch.



Once the role has been created, when creating the EC2 instance, in the Configure Instance Details screen, ensure to choose the IAM role.



The correct answer is: **Create a role which has the necessary privileges and can be assumed by the EC2 instance.**

QUESTION 513
A custorner has a requirement to extend their on-premises data center to AWS. The custorner requires a 50-Mbps dedicated and private connection to their VPC. Which AWS product or feature satisfies this requirernent?

A. Amazon VPC Peering
B. Elastic IP Addresses
C. AWS Direct Connect
D. Amazon VPC virtual private gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

AWS Direct connect is the solution officially provided by AWS when the customer wants to have a dedicated and private connection to their AWS cloud.

The correct answer is: **AWS Direct Connect**

QUESTION 514
What is the minimum size of an EBS volume as per AWS?

A. 2TB
B. 1GiB
C. 1GB
D. 1Byte

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

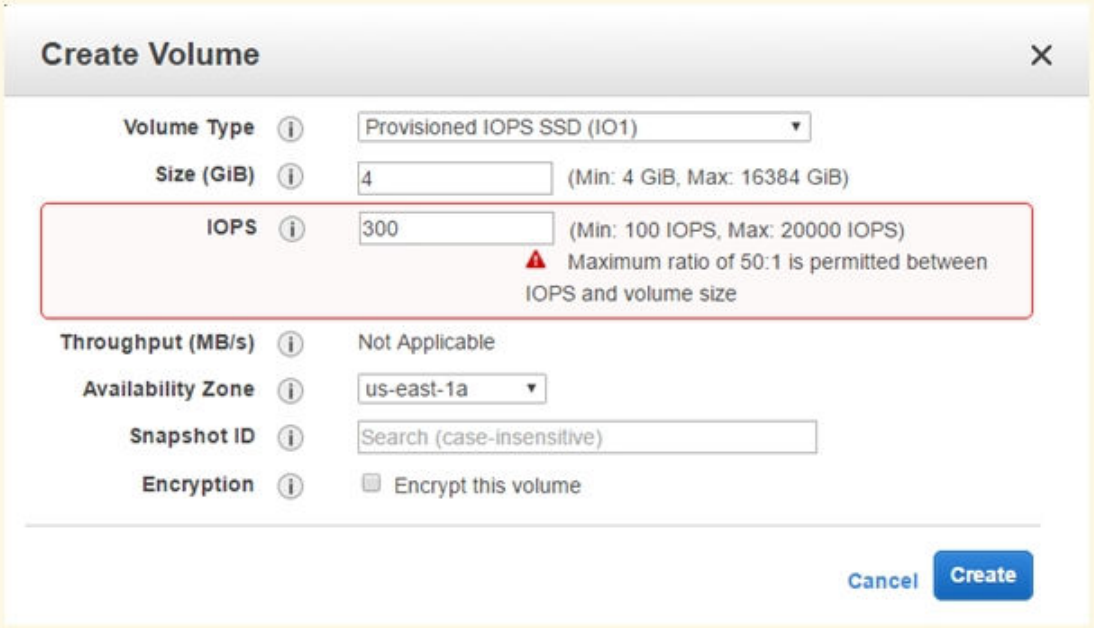
QUESTION 515
If a provisioned IOPS volume of 4iGB is created, what are the possible correct values for IOPS for the volume in order for it to be created?

A. 200
B. 300
C. 400
D. 500

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The maximum allowable ratio for Disk space to IOPS is 50:1 for provisioned IOPS. So any value greater than 200 for a 4iGB will not be accepted. An example is show below



The correct answer is: **200**

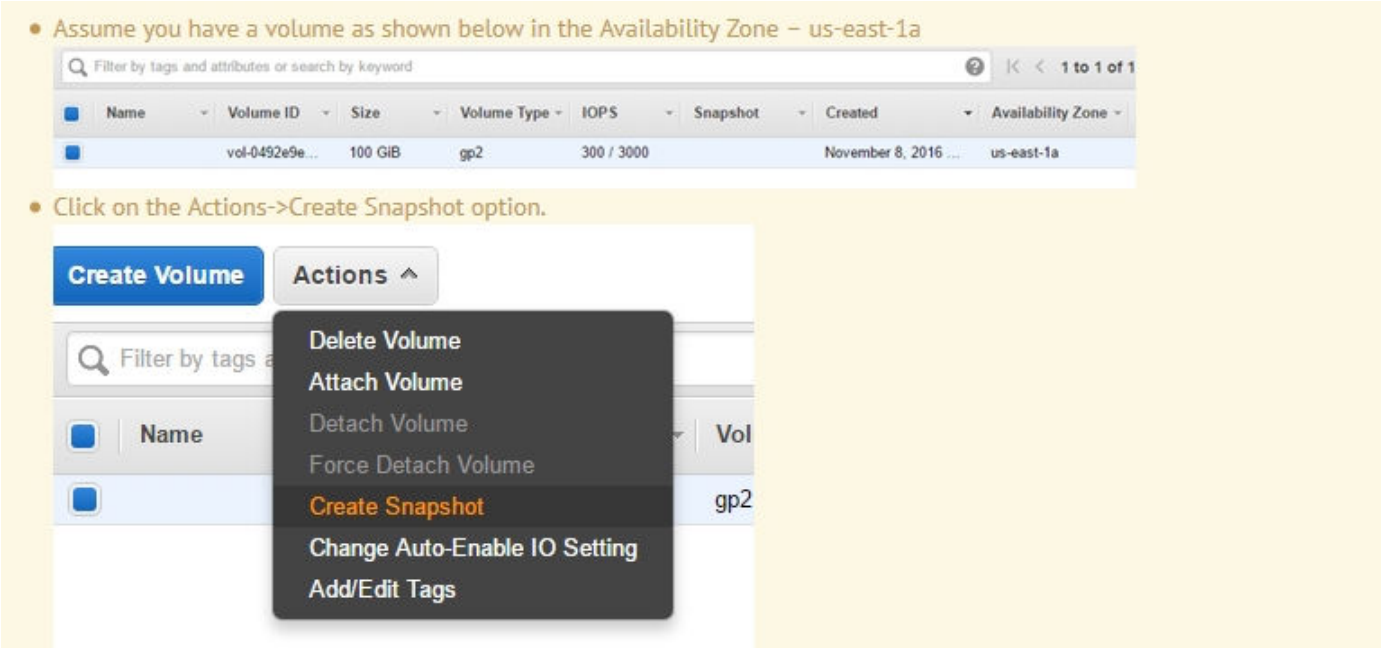
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

QUESTION 516
How can an EBS volume which is currently attached to an EC2 instance in one Availability Zone to another?

A. Detach the volume and attach to an EC2 instance in another AZ.
B. Create a new volume in the other AZ and speciW the current volume as the source.
C. Create a snapshot of the volume and then create a volume from the snapshot in the other AZ
D. Create a new volume in the AZ and do a disk copy of contents from one volume to another.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:



“Snapshots can be used to instantiate multiple new volumes, expand the size of a volume, or move volumes across Availability Zones. When a new volume is created, you may choose to create it based on an existing Amazon EBS snapshot. In that scenario, the new volume begins as an exact replica of the snapshot.”

https://aws.amazon.com/ebs/details/

QUESTION 517
A company is hosting EC2 instances which focuses on work-loads are on non-production and non-priority batch loads. Also these processes can be interrupted at any time.
What is the best pricing model which can be used for EC2 instances in ülis case?

A. Reserved Instances
B. On-Demand Instances
C. Spot Instances
D. Regular Instances

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Remember that whenever u see the keywords of non-production workloads which can be interrupted, immediately think of spot instances. These are the most cost efficient instances which can be used.

The correct answer is: **Spot Instances**

QUESTION 518
Which of the following databases is not supported on Arnazon RDS?

A. MSSOL
B. MySOL
C. Aurora
D. DB2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

DB2 is not yet supported on aws. To get the latest list of RDS's supported by AWS, please use the following link - https://aws.amazon.com/rds/

The correct answer is: **DB2**

QUESTION 519
Amazon rds provides a facility to modify the back-up retention policy for automated backups, with a value of 0 indicating for no backup retention. What is the maximum retention period allowed in days?

A. 45
B. 35
C. 15
D. 10

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When you configure the advanced settings when creating your rds , aws will provide the option to specify the retention period for automated backup's which is a value from 0 – 34 which equates to 35 days in maximum.



QUESTION 520
How many relational database engines does RDS currently support?

A. Three: MySQL, Oracle and Microsoft SQL Server.
B. Just two: MySQL and Oracle.
C. Six: Amazon Aurora, Oracle, Microsoft SQL Server, PostgreSQL, MySQL and MariaDB.
D. Just one: MySQL.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS provides you six familiar database engines to choose from, including Amazon Aurora, Oracle, Microsoft SQL Server, PostgreSQL, MySQL and MariaDB.
https://aws.amazon.com/rds/?nc1=h_ls

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in 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.

QUESTION 521
You have a web portal composed of two services. Each service must scale independently. Both services should be served under the same domain.
Which configuration allows this?

A. Use two AWS Application Load Balancers: one for each service. Assign the same CNAME to both.
B. Use one AWS Classic Load Balancer. Create a redirect in the web server based on user's source IPs.
C. Use two AWS Classic Load Balancers: one for each service. Assign the same CNAME to both.
D. Use one AWS Application Load Balancer. Specify listener rules to route requests to each service.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 522
You need a solution to distribute traffic evenly across all of the containers for a task running on Amazon ECS. Your task definitions define dynamic host port mapping for your containers.
What AWS feature provides this functionality?

A. Application Load Balancers support dynamic host port mapping.
B. CloudFront custom origins support dynamic host port mapping.
C. All Elastic Load Balancing instances support dynamic host port mapping.
D. Classic Load Balancers support dynamic host port mapping.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-load-balancing.html

QUESTION 523
You are migrating an existing enterprise application to AWS. It requires standard file system access from multiple instances. It also requires high storage throughput with consistently low latencies. You are looking for a storage solution that will grow and shrink capacity automatically.

How can you accomplish this in AWS?

A. Create an Amazon S3 bucket that the application can use for its storage requirements.
B. Create an Amazon EFS file system and mount it on all of the application instances.
C. Launch an EBS-backed EC2 instance. Create and share an NFS mount with the application.
D. Launch an Amazon Redshift cluster with dense storage nodes to use with the application.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html

QUESTION 524
Which Auto Scaling features allow you to scale ahead of expected increases in load? (Select TWO.)

A. Cooldown period
B. Lifecycle hooks
C. Desired capacity
D. Scheduled scaling
E. Health check grace period
F. Metric-based scaling

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 525
You have been asked to design a fault-tolerant and scalable web application across three Availability Zones. The presentation logic will reside on web servers behind an ELB Classic Load Balancer, and the application logic will reside on a set of app servers behind a second load balancer.
How should you use Auto Scaling groups?

A. Deploy one Auto Scaling group that includes all the web and app servers across all Availability Zones.
B. Deploy three Auto Scaling groups: one for each Availability Zone that includes both web and app servers.
C. Deploy two Auto Scaling groups: one for the web servers in all Availability Zones and one for the app servers in all Availability Zones.
D. Deploy six Auto Scaling groups: a web server group in each Availability Zone and an app server group in each Availability Zone.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 526
You are designing a scalable web application with stateless web servers.
Which service or feature is well suited to store user session information?

A. Amazon EBS
B. Amazon DynamoDB
C. Amazon EC2 instance store
D. Amazon SQS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/blogs/compute/an-ec2-spot-architecture-for-web-applications/

QUESTION 527
Your Amazon EC2 instances must access the AWS API, so you created a NAT gateway in an existing subnet. When you try to access the AWS API, you are unsuccessful.
What could be preventing access?

A. The NAT gateway subnet does not have a route to an Internet gateway.
B. The instances need an IAM granting access to the NAT gateway.
C. The NAT gateway does not have a route to the virtual private gateway.
D. The instances are not in the same subnet as the NAT gateway.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html

QUESTION 528
A company has a workflow that uploads video files from their data center to AWS for transcoding. They use Amazon EC2 worker instances that pull transcoding jobs from SQS.
Why is SQS an appropriate service for this scenario?

A. SQS can accommodate message payloads of any size.
B. SQS checks the health of the worker instances.
C. SQS synchronously provides transcoding output.
D. SQS decouples the transcoding task from the upload.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/sqs/faqs/

QUESTION 529
Your existing web application requires a persistent key-value store database that must service 50,000 reads/second. Your company is looking at 10% growth in traffic and data volume month over month for the next several years.
Which service meets these requirements?

A. Amazon Redshift
B. Amazon DynamoDB
C. Amazon SQS
D. Amazon RDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 530
You've been tasked with choosing a datastore to persist GPS coordinates for a new app. The service needs consistent, single-digit-millisecond latency at any scale.
Which AWS service meets your requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/dynamodb/

QUESTION 531
You originally built a VPC for a two-tier application. The subnets for the web and data tiers use all the IP address space in the VPC. Now you want to add subnets for an application tier.
How can you accommodate the new subnets in your VPC?

A. Reduce the CIDR block ranges of the existing subnets to make room for the new subnets.

B. Build a new VPC that can accommodate all the subnets, and migrate the application to the new VPC.
C. Change the CIDR block for the VPC to create enough free address space for the new subnets.
D. Create the new subnets in the VPC; the VPC will automatically scale to accommodate the new subnets.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 532
An application on an Amazon EC2 instance routinely stops responding to requests and requires a reboot to recover. The application logs are already exported into Amazon CloudWatch, and you notice that the problem consistently follows the appearance of a specific message in the log. The application team is working to address the bug, but has not provided a date for the fix.
What workaround can you implement to automate recovery of the instance until the fix is deployed?

A. Create an Amazon CloudWatch alarm on an Amazon CloudWatch Logs filter for that message; based on that alarm, trigger an Amazon CloudWatch action to reboot the instance.
B. Create an AWS CloudTrail alarm on low CPU; based on that alarm, trigger an Amazon SNS message to the Operations team.
C. Create an Amazon CloudWatch alarm on instance memory usage; based on that alarm, trigger an Amazon CloudWatch action to reboot the instance.
D. Create an AWS CloudTrail alarm to detect the deadlock; based on that alarm, trigger an Amazon SNS message to the Operations team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 533
You are architecting a web application that will be backed by a relational database. The application will be read-heavy, and database queries will be computationally intensive.
How can you improve overall application response for users?

A. Use ElastiCache to store critical pieces of data in memory for low-latency access.
B. use Amazon SQS to distribute messages among workers that are less busy.
C. Use an Auto Scaling group and ELB Classic Load Balancer for the application tier.
D. Use Data Pipeline to replicate your relational data across all of your web tier nodes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 534
Your Amazon VPC has a public subnet with a route that sends all Internet traffic to the Internet gateway. An Amazon EC2 instance in the public subnet has an assigned private IP address. The instance belongs to a security group set to allow all outbound traffic. The instance cannot access the Internet.
Why could the Internet be unreachable from this instance?

A. The instance does not have a public IP address.
B. The internet gateway security group must allow all outbound traffic.
C. The instance security group must allow all inbound traffic.
D. The instance "Source/Destination check" property must be enabled.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 535
You are launching an application in an Auto Scaling group. To store the user session state, you need a structured storage service with durability and low latency.
Which service meets your needs?

A. Amazon ElastiCache
B. Amazon S3
C. Amazon EC2 instance storage
D. Amazon DynamoDB

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/dynamodb/faqs/

QUESTION 536
You're building an API backend available at services.yourcompany.com. The API is implemented with API Gateway and Lambda. You successfully tested the API using curl. You implemented Javascript to call the API from a webpage on your corporate website, www.yourcompany.com. When you access that page in your browser, you get the following error:
"The same origin policy disallows reading the remote resource"
How can you allow your corporate webpages to invoice the API?

A. Disable CORS in the API Gateway.
B. Disable CORS in the Javascript frontend.
C. Enable CORS in the API Gateway.
D. Enable CORS in the Javascript frontend.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 537
Your company's IT policies mandate that all critical data must be duplicated in two physical locations at least 100 miles apart.
Which storage option meets this requirement?

A. Two Amazon S3 buckets in different regions
B. One Amazon S3 bucket
C. One Amazon Glacier archive
D. Two Amazon S3 buckets in the same region

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/blogs/aws/new-cross-region-replication-for-amazon-s3/

QUESTION 538
Which AWS services are valid origins for an Amazon CloudFront distribution? (Select TWO.)

A. Amazon RDS
B. ELB Classic Load Balancer
C. Amazon S3
D. Amazon DynamoDB
E. Amazon Galcier

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 539
Your company has separate AWS accounts for development and production. Each developer is assigned an IAM user in the development account. Developers occasionally need to access the production account to roll our changes to that environment. Your company does not allow the creation of IAM users in the production account.
What strategy will allow the development team to access the production account?

A. Create an IAM role in the development account. Allow IAM users in the development account to assume the role.

B. Create an IAM group in the production account. Grant IAM users in the development account membership in the group.
C. Create an IAM role in the production account. Aloow IAM users in the development account to assume the role.
D. Create an IAM group in the development account. Grant IAM users in the development account membership in the group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 540
A colleague asked for your advice about how to easily deploy, monitor, and scale a three-tier LAMP (Linux, Apache, MySQL, PHP) application on AWS. Your colleague has time and staffing constraints and wants to deploy and manage the application with minimal effort.
Which AWS service would you suggest?

A. Elastic Beanstalk
B. Data Pipeline
C. CloudFormation
D. CodeDeploy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/

QUESTION 541
Which services can invoke AWS Lambda functions? (Select TWO.)

A. Amazon SNS
B. Amazon Redshift
C. Amazon Route53
D. Amazon DynamoDB
E. Elastic Load Balancing

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/lambda/faqs/

QUESTION 542

Which aspects of Amazon EC2 security are the responsibility of AWS? (Select TWO.)

A. VPC and security group configuration
B. Physical security of hardware
C. Application authentication
D. Virtualization infrastructure
E. Guest operating systems

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloudacademy.com/blog/aws-shared-responsibility-model-security/

QUESTION 543
Your company has set up an application in eu-west-1 with a disaster recovery site in eu-central-1. You want to be notified of any AWS API activity in regions other than these two.
How can you monitor AWS API activity in other regions?

A. Create a CloudWatch alarm for CloudTrail events.
B. Create a CloudWatch alarm for Trusted Advisor.
C. Create a CloudWatch alarm for VPC flow logs.
D. Create a CloudWatch alarm for SSH key usage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://aws.amazon.com/about-aws/whats-new/2017/06/aws-cloudtrail-adds-amazon-cloudwatch-events-to-the-api-activity/

QUESTION 544
What services will help identify Amazon EC2 instances with underutilized CPU capacity? (Select TWO.)

A. Amazon CloudWatch
B. Cost Explorer
C. AWS Trusted Advisor
D. AWS CloudTrail
E. Amazon EC2 usage reports

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.stratoscale.com/blog/compute/7-ways-aws-users-can-optimize-their-cloud-compute-resource-consumption/

QUESTION 545
You have a Cassandra cluster running in private subnets in an Amazon VPC. A new application in a different Amazon VPC needs access to the database.
How can the new application access the database?

A. Set up a dual-homed instance with ENIs in both Amazon VPCs.
B. Set up a VPC peering connection between the two Amazon VPCs.
C. Set up a NAT Gateway in the database's Amazon VPC.
D. Set up a NAT Gateway in the application's Amazon VPC.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 546
Which security functions are based on AWS STS? (Select TWO.)

A. Using IAM roles with Amazon EC2 instances
B. Adding conditions to managed policies
C. Using access keys to authenticate IAM users
D. Using web federated identity to authenticate users
E. Assigning managed policies to IAM groups

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 547
You bid $0.22 for an Amazon EC2 Spot Instance when the market price was $0.20. For 90 minutes, the market price remained at $0.20. Then the market price changed to $0.25, and your instance was terminated by AWS.
What was your cost of running the instance for the entire duration?

A. $0.47
B. $0.20
C. $0.40
D. $0.22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 548
Your organization is looking for a solution that can help the business with streaming data. Several services will require access to read and process the same stream concurrently.
What AWS service meets the business requirements?

A. Amazon Kinesis Firehose
B. Amazon Kinesis Streams
C. Amazon CloudFront
D. Amazon SQS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/streams/latest/dev/introduction.html

QUESTION 549
A customer's security team requires the logging of all network access attempts to Amazon EC2 instances in their production VPC on AWS.
Which configuration will meet the security team's requirement?

A. Enable CloudTrail for the production VPC.
B. Enable VPC Flow Logs for the production VPC.
C. Enable both CloudTrail and VPC Flow Logs for the production VPC.
D. Enable both CloudTrail and VPC Flow Logs for the AWS account.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

QUESTION 550
Your company runs an application that generates several thousand 1-GB reports a month. Approximately 10% of these reports will be accessed once during the first 30 days and must be available on demand. After 30 days, reports are no longer accessed as a part of normal business processes but must be retained for compliance reasons.
Which architecture would meet these requirements with the lowest cost?

A. Upload the reports to Amazon S3 Standard storage class. Set a lifecycle configuration on the bucket to transition the reports to Amazon Glacier after 30 days.
B. Upload the reports to Amazon S3 Standard – Infrequent Access storage class. Set a lifecycle configuration on the bucket to transition the reports to Amazon Glacier after 30 days.
C. Upload the reports to Amazon Glacier. When reports are requested, copy them to Amazon S3 Standard storage class for access. Delete the copied reports after they have been viewed.
D. Upload the reports to Amazon S3 Standard – Infrequent Access storage class. When reports are requested, copy them to Amazon S3 Standard storage class for access. Delete the copied reports after they have been viewed.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-KSDNs4nfg5ikp6yBN9l/Exam%20Feedback

QUESTION 551
A stray Amazon EC2 r3.8xlarge instance is running in your AWS account. Before terminating it, you want to find the owner to confirm that it is not needed.
Where can you find the identity that launched this instance?

A. VPC flow logs
B. ELB access logs
C. CloudTrail logs
D. Operating system logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://stackoverflow.com/questions/23489381/which-user-launched-ec2-instance

QUESTION 552
You are running a web application with four Amazon EC2 instances across two Availability Zones. The instances are in an Auto Scaling group behind an ELB Classic Load Balancer. A scaling event adds one instance to the group. After the event, you notice that, although all instances are serving traffic, some instances are serving more traffic than others.
Which of the following could be the problem?

A. Cross-zone load balancing is not configured on the ELB Classic Load Balancer.
B. Access logs are not enabled on the ELB Classic Load Balancer.
C. A SSL/TLS certificate has not been deployed on the ELB Classic Load Balancer.
D. Sticky bits is not enabled on the ELB Classic Load Balancer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 553
You are running a mobile media application and are considering API Gateway for the client entry point.
What benefits would this provide? (Select TWO.)

A. Caching API responses
B. IP blacklisting
C. Intrusion prevention
D. Load balancing
E. Throttling traffic

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 554
Your application currently stores data on an unencrypted EBS volume. A new security policy mandates that all data must be encrypted at rest.
How can you encrypt the data?

A. Create a snapshot of the volume. Create a new, encrypted volume from the snapshot. Replace the volume.
B. Stop the instance. Detach the volume. Modify the EBS settings to encrypt the volume. Reattach the volume. Start the instance.
C. Create a snapshot of the volume. Make an encrypted copy of the snapshot. Create a new volume from the new snapshot. Replace the volume.
D. Modify the EBS settings to encrypt the volume. You do need to detach the volume or stop the instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 555
You have been asked to design the storage layer for an application.
The application requires disk performance of at least 100,000 IOPS in addition, the storage layer must be able to survive the loss of an individual disk. EC2 instance, or Availability Zone without any data loss.
The volume you provide must have a capacity of at least 3 TB.
Which of the following designs will meet these objectives?

A. Instantiate a 12 8xlarge instance in us-east-1a Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance Provision 3x1 TB EBS volumes attach them to the instance and configure them as a second RAID 0 volume Configure synchronous, block-level replication from the ephemeral-backed volume to the EBS-backed volume.

B. Instantiate a 12 8xlarge instance in us-east-1a create a raid 0 volume using the four 800GB SSD ephemeral disks provide with the Instance Configure synchronous block-level replication to an Identically configured Instance in us-east-1b.
C. Instantiate a c3 8xlarge Instance In us-east-1 Provision an AWS Storage Gateway and configure it for 3 TB of storage and 100 000 IOPS Attach the volume to the instance.
D. Instantiate a c3 8xlarge instance in us-east-i provision 4x1TB EBS volumes, attach them to the instance, and configure them as a single RAID 5 volume Ensure that EBS snapshots are performed every 15 minutes.
E. Instantiate a c3 8xlarge Instance in us-east-1 Provision 3x1TB EBS volumes attach them to the instance, and configure them as a single RAID 0 volume Ensure that EBS snapshots are performed every 15 minutes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It doesn't protect against a loss of two EC2 instances or two AZs, but the question asks about protection of ONE disk, EC2 instance or AZ loss.
https://acloud.guru/course/aws-certified-solutions-architect-associate/discuss/-KJdi4tFMp2x_O88J6U4/an-architecture-design-question

QUESTION 556
How can an EBS volume that is currently attached to an EC2 instance be migrated from one Availability Zone to another?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While EBS volumes are locked to the Availability Zone in which they reside, snapshots are available throughout their region of residence.

QUESTION 557
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://aws.amazon.com/cloudfront/

QUESTION 558
You are trying to launch an EC2 instance, however the instance seems to go into a terminated status immediately. What would probably not be a reason that this is happening?

A. The AMI is missing a required part.
B. The snapshot is corrupt.
C. You need to create storage in EBS first.
D. You've reached your volume limit.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EC2 provides a virtual computing environments, known as an instance. After you launch an instance, AWS recommends that you check its status to confirm that it goes from the pending status to the running status, the not terminated status. The following are a few reasons why an Amazon EBS-backed instance might immediately terminate:
You've reached your volume limit.
The AMI is missing a required part.
The snapshot is corrupt.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.html

QUESTION 559
You have set up an Auto Scaling group. The cool down period for the Auto Scaling group is 7 minutes. The first instance is launched after 3 minutes, while the second instance is launched after 4 minutes. How many minutes after the first instance is launched will Auto Scaling accept another scaling activity request?

A. 11 minutes
B. 7 minutes
C. 10 minutes
D. 14 minutes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If an Auto Scaling group is launching more than one instance, the cool down period for each instance starts after that instance is launched. The group remains locked until

the last instance that was launched has completed its cool down period. In this case the cool down period for the first instance starts after 3 minutes and finishes at the 10th minute (3+7 cool down), while for the second instance it starts at the 4th minute and finishes at the 11th minute (4+7 cool down). Thus, the Auto Scaling group will receive another request only after 11 minutes.
Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

QUESTION 560
In Amazon EC2 Container Service components, what is the name of a logical grouping of container instances on which you can place tasks?

A. A cluster
B. A container instance
C. A container
D. A task definition

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon ECS contains the following components:
A Cluster is a logical grouping of container instances that you can place tasks on. A Container instance is an Amazon EC2 instance that is running the Amazon ECS agent and has been registered into a cluster.
A Task definition is a description of an application that contains one or more container definitions. A Scheduler is the method used for placing tasks on container instances. A Service is an Amazon ECS service that allows you to run and maintain a specified number of instances of a task definition simultaneously.
A Task is an instantiation of a task definition that is running on a container instance. A Container is a Linux container that was created as part of a task.

Reference: http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html

QUESTION 561
In the context of AWS support, why must an EC2 instance be unreachable for 20 minutes rather than allowing customers to open tickets immediately?

A. Because most reachability issues are resolved by automated processes in less than 20 minutes
B. Because all EC2 instances are unreachable for 20 minutes every day when AWS does routine maintenance
C. Because all EC2 instances are unreachable for 20 minutes when first launched
D. Because of all the reasons listed here

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An EC2 instance must be unreachable for 20 minutes before opening a ticket, because most reachability issues are resolved by automated processes in less than 20 minutes and will not require any action on the part of the customer. If the instance is still unreachable after this time frame has passed, then you should open a case with support.
Reference: https://aws.amazon.com/premiumsupport/faqs/

QUESTION 562
Can a user get a notification of each instance start / terminate configured with Auto Scaling?

A. Yes, if configured with the Launch Config
B. Yes, always
C. Yes, if configured with the Auto Scaling group
D. No

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user can get notifications using SNS if he has configured the notifications while creating the Auto Scaling group.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html

QUESTION 563
Amazon EBS provides the ability to create backups of any Amazon EC2 volume into what is known as _____.

A. snapshots
B. images
C. instance backups
D. mirrors

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon allows you to make backups of the data stored in your EBS volumes through snapshots that can later be used to create a new EBS volume.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 564
To specify a resource in a policy statement, in Amazon EC2, can you use its Amazon Resource Name (ARN)?

A. Yes, you can.
B. No, you can't because EC2 is not related to ARN.
C. No, you can't because you can't specify a particular Amazon EC2 resource in an IAM policy.
D. Yes, you can but only for the resources that are not affected by the action.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Some Amazon EC2 API actions allow you to include specific resources in your policy that can be created or modified by the action. To specify a resource in the statement, you need to use its Amazon Resource Name (ARN).
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pd

QUESTION 565
After you recommend Amazon Redshift to a client as an alternative solution to paying data warehouses to analyze his data, your client asks you to explain why you are recommending Redshift. Which of the following would be a reasonable response to his request?

A. It has high performance at scale as data and query complexity grows.
B. It prevents reporting and analytic processing from interfering with the performance of OLTP workloads.
C. You don't have the administrative burden of running your own data warehouse and dealing with setup, durability, monitoring, scaling, and patching.
D. All answers listed are a reasonable response to his question

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Redshift delivers fast query performance by using columnar storage technology to improve I/O efficiency and parallelizing queries across multiple nodes. Redshift uses standard PostgreSQL JDBC and ODBC drivers, allowing you to use a wide range of familiar SQL clients.
Data load speed scales linearly with cluster size, with integrations to Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis or any SSH-enabled host.
AWS recommends Amazon Redshift for customers who have a combination of needs, such as:
High performance at scale as data and query complexity grows Desire to prevent reporting and analytic processing from interfering with the performance of OLTP workloads.
Large volumes of structured data to persist and query using standard SQL and existing BI tools Desire to the administrative burden of running one's own data warehouse and dealing with setup, durability, monitoring, scaling and patching
Reference: https://aws.amazon.com/running_databases/#redshift_anchor

QUESTION 566
One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway. However, you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?

A. Gateway-cached lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Gateway-stored enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.
B. Gateway-cached is free whilst gateway-stored is not.
C. Gateway-cached is up to 10 times faster than gateway-stored.
D. Gateway-stored lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Gateway-cached enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Volume gateways provide cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers. The gateway supports the following volume configurations:

Gateway-cached volumes. You store your data in Amazon Simple Storage Service (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.
Gateway-stored volumes. If you need low-latency access to your entire data set, you can configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive off-site backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.
Reference: http://docs.aws.amazon.com/storagegateway/latest/userguide/volume-gateway.html

QUESTION 567
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 AZ while launching an instance
B. Always select the US-East-1-a zone for HA
C. Do not select the AZ; instead let AWS select the AZ
D. The user can never select the availability zone while launching an instance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

QUESTION 568
A user is storing a large number of objects on AWS S3. The user wants to implement the search functionality among the objects. How can the user achieve this?

A. Use the indexing feature of S3.
B. Tag the objects with the metadata to search on that.
C. Use the query functionality of S3.
D. Make your own DB system which stores the S3 metadata for the search functionality.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Web Services, AWS S3 does not provide any query facility. To retrieve a specific object, the user needs to know the exact bucket / object key. In this case it is recommended to have an own DB system which manages the S3 metadata and key mapping.
Reference: http://media.amazonwebservices.com/AWS_Storage_Options.pdf

QUESTION 569
After setting up a Virtual Private Cloud (VPC) network, a more experienced cloud engineer suggests that to achieve low network latency and high network throughput you should look into setting up a placement group. You know nothing about this, but begin to do some research about it and are especially curious about its limitations. Which of the below statements is wrong in describing the limitations of a placement group?

A. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed.
B. A placement group can span multiple Availability Zones.
C. You can't move an existing instance into a placement group.
D. A placement group can span peered VPCs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 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.
Placement groups have the following limitations:
The name you specify for a placement group a name must be unique within your AWS account.
A placement group can't span multiple Availability Zones.
Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed. We recommend using the same instance type for all instances in a placement group.
You can't merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement group.
A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs. For more information about VPC peering connections, see VPC Peering in the Amazon VPC User Guide.
You can't move an existing instance into a placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 570
What is a placement group in Amazon EC2?

A. It is a group of EC2 instances within a single Availability Zone.
B. It the edge location of your web content.
C. It is the AWS region where you run the EC2 instance of your web content.

D. It is a group used to span multiple Availability Zones.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A placement group is a logical grouping of instances within a single Availability Zone.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

QUESTION 571
You are migrating an internal server on your DC to an EC2 instance with EBS volume. Your server disk usage is around 500GB so you just copied all your data to a 2TB disk to be used with AWS Import/Export. Where will the data be imported once it arrives at Amazon?

A. to a 2TB EBS volume
B. to an S3 bucket with 2 objects of 1TB
C. to an 500GB EBS volume
D. to an S3 bucket as a 2TB snapshot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An import to Amazon EBS will have different results depending on whether the capacity of your storage device is less than or equal to 1 TB or greater than 1 TB. The maximum size of an Amazon EBS snapshot is 1 TB, so if the device image is larger than 1 TB, the image is chunked and stored on Amazon S3. The target location is determined based on the total capacity of the device, not the amount of data on the device.
Reference: http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html

QUESTION 572
A client needs you to import some existing infrastructure from a dedicated hosting provider to AWS to try and save on the cost of running his current website. He also needs an automated process that manages backups, software patching, automatic failure detection, and recovery. You are aware that his existing set up currently uses an Oracle database. Which of the following AWS databases would be best for accomplishing this task?

A. Amazon RDS
B. Amazon Redshift
C. Amazon SimpleDB
D. Amazon ElastiCache

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Amazon RDS gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server, or PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user-defined retention period and enabling point-in-time recovery.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

QUESTION 573
True or false: A VPC contains multiple subnets, where each subnet can span multiple Availability Zones.

A. This is true only if requested during the set-up of VPC.
B. This is true.
C. This is false.
D. This is true only for US regions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A VPC can span several Availability Zones. In contrast, a subnet must reside within a single Availability Zone.
Reference: https://aws.amazon.com/vpc/faqs/

QUESTION 574
An edge location refers to which Amazon Web Service?

A. An edge location is referred to the network configured within a Zone or Region
B. An edge location is an AWS Region
C. An edge location is the location of the data center used for Amazon CloudFront.
D. An edge location is a Zone within an AWS Region

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudFront is a content distribution network. A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location. Amazon CloudFront can cache static content at each edge location. This means that your popular static content (e.g., your site's logo, navigational images, cascading style sheets, JavaScript code, etc.) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Amazon CloudFront also helps you offload requests for such files from your origin sever? CloudFront serves the cached copy when available and only makes a request to your origin server if the edge location receiving the browser's request does not have a copy of the file.
Reference: http://aws.amazon.com/cloudfront/

QUESTION 575
You are looking at ways to improve some existing infrastructure as it seems a lot of engineering resources are being taken up with basic management and monitoring

tasks and the costs seem to be excessive. You are thinking of deploying Amazon ElasticCache to help. Which of the following statements is true in regards to ElasticCache?

A. You can improve load and response times to user actions and queries however the cost associated with scaling web applications will be more.
B. You can't improve load and response times to user actions and queries but you can reduce the cost associated with scaling web applications.
C. You can improve load and response times to user actions and queries however the cost associated with scaling web applications will remain the same.
D. You can improve load and response times to user actions and queries and also reduce the cost associated with scaling web applications.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory caching system, instead of relying entirely on slower disk-based databases. The service simplifies and offloads the management, monitoring and operation of in-memory cache environments, enabling your engineering resources to focus on developing applications.
Using Amazon ElastiCache, you can not only improve load and response times to user actions and queries, but also reduce the cost associated with scaling web applications.
Reference: https://aws.amazon.com/elasticache/faqs/

QUESTION 576
Do Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

A. Yes, they do but only if they are detached from the instance.
B. No, you cannot attach EBS volumes to an instance.
C. No, they are dependent.
D. Yes, they do.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 EC2 instance.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 577
Your supervisor has asked you to build a simple file synchronization service for your department.
He doesn't want to spend too much money and he wants to be notified of any changes to files by email. What do you think would be the best Amazon service to use for the email solution?

A. Amazon SES

B. Amazon CloudSearch
C. Amazon SWF
D. Amazon AppStream

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
File change notifications can be sent via email to users following the resource with Amazon Simple Email Service (Amazon SES), an easy-to-use, cost-effective email solution.
Reference:
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_filesync_08.pdf

QUESTION 578
Your manager has just given you access to multiple VPN connections that someone else has recently set up between all your company's offices. She needs you to make sure that the communication between the VPNs is secure. Which of the following services would be best for providing a low-cost hub-and-spoke model for primary or backup connectivity between these remote offices?

A. Amazon CloudFront
B. AWS Direct Connect
C. AWS CloudHSM
D. AWS VPN CloudHub

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who would like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

QUESTION 579
Amazon EC2 provides a ____. It is an HTTP or HTTPS request that uses the HTTP verbs GET or POST.

A. web database
B. net framework
C. Query API
D. C library

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Amazon EC2 provides a Query API. These requests are HTTP or HTTPS requests that use the HTTP verbs GET or POST and a Query parameter named Action.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/APIReference/making-api-requests.html

QUESTION 580
In Amazon AWS, which of the following statements is true of key pairs?

A. Key pairs are used only for Amazon SDKs.
B. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
C. Key pairs are used only for Elastic Load Balancing and AWS IAM.
D. Key pairs are used for all Amazon services.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Key pairs consist of a public and private key, where you use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
Reference: http://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html

QUESTION 581
Does Amazon DynamoDB support both increment and decrement atomic operations?

A. Only increment, since decrement are inherently impossible with DynamoDB's data model.
B. No, neither increment nor decrement operations.
C. Yes, both increment and decrement operations.
D. Only decrement, since increment are inherently impossible with DynamoDB's data model.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon DynamoDB supports increment and decrement atomic operations.
Reference:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/APISummary.html

QUESTION 582
An organization has three separate AWS accounts, one each for development, testing, and production. The organization wants the testing team to have access to certain AWS resources in the production account. How can the organization achieve this?

A. It is not possible to access resources of one account with another account.
B. Create the IAM roles with cross account access.
C. Create the IAM user in a test account, and allow it access to the production environment with the IAM policy.
D. Create the IAM users with cross account access.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An organization has multiple AWS accounts to isolate a development environment from a testing or production environment. At times the users from one account need to access resources in the other account, such as promoting an update from the development environment to the production environment. In this case the IAM role with cross account access will provide a solution. Cross account access lets one account share access to their resources with users in the other AWS accounts.
Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 583
You need to import several hundred megabytes of data from a local Oracle database to an Amazon RDS DB instance. What does AWS recommend you use to accomplish this?

A. Oracle export/import utilities
B. Oracle SQL Developer
C. Oracle Data Pump
D. DBMS_FILE_TRANSFER

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
How you import data into an Amazon RDS DB instance depends on the amount of data you have and the number and variety of database objects in your database.
For example, you can use Oracle SQL Developer to import a simple, 20 MB database; you want to use Oracle Data Pump to import complex databases or databases that are several hundred megabytes or several terabytes in size.
Reference:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html

QUESTION 584
A user has created an EBS volume with 1000 IOPS. What is the average IOPS that the user will get for most of the year as per EC2 SLA if the instance is attached to the EBS optimized instance?

A. 950
B. 990
C. 1000
D. 900

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
As per AWS SLA if the instance is attached to an EBS-Optimized instance, then the Provisioned IOPS volumes are designed to deliver within 10% of the provisioned IOPS performance 99.9% of the time in a given year. Thus, if the user has created a volume of 1000 IOPS, the user will get a minimum 900 IOPS 99.9% time of the year.
Reference: http://aws.amazon.com/ec2/faqs/

QUESTION 585
You need to migrate a large amount of data into the cloud that you have stored on a hard disk and you decide that the best way to accomplish this is with AWS Import/Export and you mail the hard disk to AWS. Which of the following statements is incorrect in regards to AWS Import/Export?

A. It can export from Amazon S3
B. It can Import to Amazon Glacier
C. It can export from Amazon Glacier.
D. It can Import to Amazon EBS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Import/Export supports:
Import to Amazon S3
Export from Amazon S3
Import to Amazon EBS
Import to Amazon Glacier
AWS Import/Export does not currently support export from Amazon EBS or Amazon Glacier.
Reference: https://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisdisk.html

QUESTION 586
You are in the process of creating a Route 53 DNS failover to direct traffic to two EC2 zones. Obviously, if one fails, you would like to direct Route 53 traffic to the other region. Each region has an ELB with some instances being distributed. What is the best way for you to configure the Route 53 health check?

A. Route 53 doesn't support ELB with an internal health check. You need to create your own Route 53 health check of the ELB
B. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" off and "Associate with Health Check" on and R53 will use the ELB's internal health check.
C. Route 53 doesn't support ELB with an internal health check. You need to associate your resource record set for the ELB with your own health check
D. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" on and "Associate with Health Check" off and R53 will use the ELB's internal health check.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:
With DNS Failover, Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations where your application is operating properly. When you enable this feature, Route 53 uses health checks--regularly making Internet requests to your application's endpoints from multiple locations around the world--to determine whether each endpoint of your application is up or down. To enable DNS Failover for an ELB endpoint, create an Alias record pointing to the ELB and set the "Evaluate Target Health" parameter to true. Route 53 creates and manages the health checks for your ELB automatically. You do not need to create your own Route 53 health check of the ELB. You also do not need to associate your resource record set for the ELB with your own health check, because Route 53 automatically associates it with the health checks that Route 53 manages on your behalf. The ELB health check will also inherit the health of your backend instances behind that ELB.
Reference: http://aws.amazon.com/about-aws/whats-new/2013/05/30/amazon-route-53-adds-elb-integration-for-dns-failover/

QUESTION 587
A user wants to use an EBS-backed Amazon EC2 instance for a temporary job. Based on the input data, the job is most likely to finish within a week. Which of the following steps should be followed to terminate the instance automatically once the job is finished?

A. Configure the EC2 instance with a stop instance to terminate it.
B. Configure the EC2 instance with ELB to terminate the instance when it remains idle.
C. Configure the CloudWatch alarm on the instance that should perform the termination action once the instance is idle.
D. Configure the Auto Scaling schedule activity that terminates the instance after 7 days.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Auto Scaling can start and stop the instance at a pre-defined time. Here, the total running time is unknown. Thus, the user has to use the CloudWatch alarm, which monitors the CPU utilization.
The user can create an alarm that is triggered when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use. When the utilization is below the threshold limit, it will terminate the instance as a part of the instance action.
Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UingAlarmActions.htm

QUESTION 588
Which of the following is true of Amazon EC2 security group?

A. You can modify the outbound rules for EC2-Classic.
B. You can modify the rules for a security group only if the security group controls the traffic for just one instance.
C. You can modify the rules for a security group only when a new instance is created.
D. You can modify the rules for a security group at any time.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 589
An Elastic IP address (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Your EIP is associated with your AWS account, not a particular EC2 instance, and it remains associated with your account until you choose to explicitly release it. By default, how many EIPs is each AWS account limited to on a per region basis?

A. 1
B. 5
C. Unlimited
D. 10

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By default, all AWS accounts are limited to 5 Elastic IP addresses per region for each AWS account, because public (IPv4) Internet addresses are a scarce public resource. AWS strongly encourages you to use an EIP primarily for load balancing use cases, and use DNS hostnames for all other inter-node communication.
If you feel your architecture warrants additional EIPs, you would need to complete the Amazon EC2 Elastic IP Address Request Form and give reasons as to your need for additional addresses.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-ad dressing-limit

QUESTION 590
In Amazon EC2, partial instance-hours are billed _____.

A. per second used in the hour
B. per minute used
C. by combining partial segments into full hours
D. as full hours

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Partial instance-hours are billed to the next hour.
Reference: http://aws.amazon.com/ec2/faqs/

QUESTION 591

In EC2, what happens to the data in an instance store if an instance reboots (either intentionally or unintentionally)?

A. Data is deleted from the instance store for security reasons.
B. Data persists in the instance store.
C. Data is partially present in the instance store.
D. Data in the instance store will be lost.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 Stopping an Amazon EBS-backed instance Terminating an instance
Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/InstanceStorage.html

QUESTION 592
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 593
Can you specify the security group that you created for a VPC when you launch an instance in EC2-Classic?

A. No, you can specify the security group created for EC2-Classic when you launch a VPC instance.

B. No
C. Yes
D. No, you can specify the security group created for EC2-Classic to a non-VPC based instance only.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you're using EC2-Classic, you must use security groups created specifically for EC2-Classic.
When you launch an instance in EC2-Classic, you must specify a security group in the same region as the instance. You can't specify a security group that you created for a VPC when you launch an instance in EC2-Classic.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#ec2-classic-securit y-groups

QUESTION 594
While using the EC2 GET requests as URLs, the _____ is the URL that serves as the entry point for the web service.

A. token
B. endpoint
C. action
D. None of these

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The endpoint is the URL that serves as the entry point for the web service.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-query-api.html

QUESTION 595
You have been asked to build a database warehouse using Amazon Redshift. You know a little about it, including that it is a SQL data warehouse solution, and uses industry standard ODBC and JDBC connections and PostgreSQL drivers. However, you are not sure about what sort of storage it uses for database tables. What sort of storage does Amazon Redshift use for database tables?

A. InnoDB Tables
B. NDB data storage
C. Columnar data storage
D. NDB CLUSTER Storage

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Redshift achieves efficient storage and optimum query performance through a combination of massively parallel processing, columnar data storage, and very efficient, targeted data compression encoding schemes.
Columnar storage for database tables is an important factor in optimizing analytic query performance because it drastically reduces the overall disk I/O requirements and reduces the amount of data you need to load from disk.
Reference:
http://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html

QUESTION 596
You are checking the workload on some of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes and it seems that the I/O latency is higher than you require. You should probably check the _____ to make sure that your application is not trying to drive more IOPS than you have provisioned.

A. Amount of IOPS that are available
B. Acknowledgement from the storage subsystem
C. Average queue length
D. Time it takes for the I/O operation to complete

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In EBS workload demand plays an important role in getting the most out of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes. In order for your volumes to deliver the amount of IOPS that are available, they need to have enough I/O requests sent to them. There is a relationship between the demand on the volumes, the amount of IOPS that are available to them, and the latency of the request (the amount of time it takes for the I/O operation to complete). Latency is the true end-to-end client time of an I/O operation; in other words, when the client sends a IO, how long does it take to get an acknowledgement from the storage subsystem that the IO read or write is complete.
If your I/O latency is higher than you require, check your average queue length to make sure that your application is not trying to drive more IOPS than you have provisioned. You can maintain high IOPS while keeping latency down by maintaining a low average queue length (which is achieved by provisioning more IOPS for your volume).
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-workload-demand.htm

QUESTION 597
Which of the below mentioned options is not available when an instance is launched by Auto Scaling with EC2 Classic?

A. Public IP
B. Elastic IP
C. Private DNS
D. Private IP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Auto Scaling supports both EC2 classic and EC2-VPC. When an instance is launched as a part of EC2 classic, it will have the public IP and DNS as well as the private IP and DNS.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html

QUESTION 598
You have been given a scope to deploy some AWS infrastructure for a large organization. The requirements are that you will have a lot of EC2 instances but may need to add more when the average utilization of your Amazon EC2 fleet is high and conversely remove them when CPU utilization is low. Which AWS services would be best to use to accomplish this?

A. Auto Scaling, Amazon CloudWatch and AWS Elastic Beanstalk
B. Auto Scaling, Amazon CloudWatch and Elastic Load Balancing.
C. Amazon CloudFront, Amazon CloudWatch and Elastic Load Balancing.
D. AWS Elastic Beanstalk, Amazon CloudWatch and Elastic Load Balancing.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Auto Scaling enables you to follow the demand curve for your applications closely, reducing the need to manually provision Amazon EC2 capacity in advance. For example, you can set a condition to add new Amazon EC2 instances in increments to the Auto Scaling group when the average utilization of your Amazon EC2 fleet is high; and similarly, you can set a condition to remove instances in the same increments when CPU utilization is low. If you have predictable load changes, you can set a schedule through Auto Scaling to plan your scaling activities. You can use Amazon CloudWatch to send alarms to trigger scaling activities and Elastic Load Balancing to help distribute traffic to your instances within Auto Scaling groups. Auto Scaling enables you to run your Amazon EC2 fleet at optimal utilization.
Reference: http://aws.amazon.com/autoscaling/

QUESTION 599
You are building infrastructure for a data warehousing solution and an extra request has come through that there will be a lot of business reporting queries running all the time and you are not sure if your current DB instance will be able to handle it. What would be the best solution for this?

A. DB Parameter Groups
B. Read Replicas
C. Multi-AZ DB Instance deployment
D. Database Snapshots

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Read Replicas make it easy to take advantage of MySQL's built-in replication functionality to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. There are a variety of scenarios where deploying one or more Read Replicas for a given source DB Instance may make sense.

Common reasons for deploying a Read Replica include:
Scaling beyond the compute or I/O capacity of a single DB Instance for read-heavy database workloads. This excess read traffic can be directed to one or more Read Replicas. Serving read traffic while the source DB Instance is unavailable. If your source DB Instance cannot take I/O requests (e.g. due to I/O suspension for backups or scheduled maintenance), you can direct read traffic to your Read Replica(s). For this use case, keep in mind that the data on the Read Replica may be "stale" since the source DB Instance is unavailable.
Business reporting or data warehousing scenarios; you may want business reporting queries to run against a Read Replica, rather than your primary, production DB Instance.
Reference: https://aws.amazon.com/rds/faqs/

QUESTION 600
In DynamoDB, 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 601
Much of your company's data does not need to be accessed often, and can take several hours for retrieval time, so it's stored on Amazon Glacier. However, someone within your organization has expressed concerns that his data is more sensitive than the other data, and is wondering whether the high level of encryption that he knows is on S3 is also used on the much cheaper Glacier service. Which of the following statements would be most applicable in regards to this concern?

A. There is no encryption on Amazon Glacier, that's why it is cheaper.
B. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3 but you can change it to AES-256 if you are willing to pay more.
C. Amazon Glacier automatically encrypts the data using AES-256, the same as Amazon S3.
D. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Like Amazon S3, the Amazon Glacier service provides low-cost, secure, and durable storage. But where S3 is designed for rapid retrieval, Glacier is meant to be used as

an archival service for data that is not accessed often, and for which retrieval times of several hours are suitable.
Amazon Glacier automatically encrypts the data using AES-256 and stores it durably in an immutable form. Amazon Glacier is designed to provide average annual durability of 99.999999999% for an archive. It stores each archive in multiple facilities and multiple devices.
Unlike traditional systems which can require laborious data verification and manual repair, Glacier performs regular, systematic data integrity checks, and is built to be automatically self-healing.
Reference:
http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

QUESTION 602
Your EBS volumes do not seem to be performing as expected and your team leader has requested you look into improving their performance. Which of the following is not a true statement relating to the performance of your EBS volumes?

A. Frequent snapshots provide a higher level of data durability and they will not degrade the performance of your application while the snapshot is in progress.
B. General Purpose (SSD) and Provisioned IOPS (SSD) volumes have a throughput limit of 128 MB/s per volume.
C. There is a relationship between the maximum performance of your EBS volumes, the amount of I/O you are driving to them, and the amount of time it takes for each transaction to complete.
D. There is a 5 to 50 percent reduction in IOPS when you first access each block of data on a newly created or restored EBS volume

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration.
Frequent snapshots provide a higher level of data durability, but they may slightly degrade the performance of your application while the snapshot is in progress. This trade off becomes critical when you have data that changes rapidly. Whenever possible, plan for snapshots to occur during off-peak times in order to minimize workload impact.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html

QUESTION 603
You've created your first load balancer and have registered your EC2 instances with the load balancer. Elastic Load Balancing routinely performs health checks on all the registered EC2 instances and automatically distributes all incoming requests to the DNS name of your load balancer across your registered, healthy EC2 instances. By default, the load balancer uses the ___ protocol for checking the health of your instances.

A. HTTPS
B. HTTP
C. ICMP
D. IPv6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Elastic Load Balancing a health configuration uses information such as protocol, ping port, ping path (URL), response timeout period, and health check interval to

determine the health state of the instances registered with the load balancer.
Currently, HTTP on port 80 is the default health check.
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html

QUESTION 604
A major finance organization has engaged your company to set up a large data mining application. Using AWS you decide the best service for this is Amazon Elastic MapReduce(EMR) which you know uses Hadoop. Which of the following statements best describes Hadoop?

A. Hadoop is 3rd Party software which can be installed using AMI
B. Hadoop is an open source python web framework
C. Hadoop is an open source Java software framework
D. Hadoop is an open source JavaScript framework

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EMR uses Apache Hadoop as its distributed data processing engine. Hadoop is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware. Hadoop implements a programming model named "MapReduce," where the data is divided into many small fragments of work, each of which may be executed on any node in the cluster.
This framework has been widely used by developers, enterprises and startups and has proven to be a reliable software platform for processing up to petabytes of data on clusters of thousands of commodity machines.
Reference: http://aws.amazon.com/elasticmapreduce/faqs/

QUESTION 605
In Amazon EC2 Container Service, are other container types supported?

A. Yes, EC2 Container Service supports any container service you need.
B. Yes, EC2 Container Service also supports Microsoft container service.
C. No, Docker is the only container platform supported by EC2 Container Service presently.
D. Yes, EC2 Container Service supports Microsoft container service and Openstack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon EC2 Container Service, Docker is the only container platform supported by EC2 Container Service presently.
Reference: http://aws.amazon.com/ecs/faqs/

QUESTION 606
_____ is a fast, flexible, fully managed push messaging service.

A. Amazon SNS
B. Amazon SES
C. Amazon SQS
D. Amazon FPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 607
As AWS grows, most of your clients' main concerns seem to be about security, especially when all of their competitors also seem to be using AWS. One of your clients asks you whether having a competitor who hosts their EC2 instances on the same physical host would make it easier for the competitor to hack into the client's data. Which of the following statements would be the best choice to put your client's mind at rest?

A. Different instances running on the same physical machine are isolated from each other via a 256-bit Advanced Encryption Standard (AES-256).
B. Different instances running on the same physical machine are isolated from each other via the Xen hypervisor and via a 256-bit Advanced Encryption Standard (AES-256).
C. Different instances running on the same physical machine are isolated from each other via the Xen hypervisor.
D. Different instances running on the same physical machine are isolated from each other via IAM permissions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Elastic Compute Cloud (EC2) is a key component in Amazon's Infrastructure as a Service (IaaS), providing resizable computing capacity using server instances in AWS's data centers. Amazon EC2 is designed to make web-scale computing easier by enabling you to obtain and configure capacity with minimal friction.
You create and launch instances, which are collections of platform hardware and software.
Different instances running on the same physical machine are isolated from each other via the Xen hypervisor.
Amazon is active in the Xen community, which provides awareness of the latest developments. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.
Reference: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

QUESTION 608
In Amazon RDS, security groups are ideally used to:

A. Define maintenance period for database engines
B. Launch Amazon RDS instances in a subnet

C. Create, describe, modify, and delete DB instances
D. Control what IP addresses or EC2 instances can connect to your databases on a DB instance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon RDS, security groups are used to control what IP addresses or EC2 instances can connect to your databases on a DB instance.
When you first create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.html

QUESTION 609
You need to set up a complex network infrastructure for your organization that will be reasonably easy to deploy, replicate, control, and track changes on. Which AWS service would be best to use to help you accomplish this?

A. AWS Import/Export
B. AWS CloudFormation
C. Amazon Route 53
D. Amazon CloudWatch

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. You don't need to individually create and configure AWS resources and figure out what's dependent on what. AWS CloudFormation handles all of that.
Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

QUESTION 610
You have just been given a scope for a new client who has an enormous amount of data(petabytes) that he constantly needs to analyze. Currently he is paying a huge amount of money for a data warehousing company to do this for him and is wondering if AWS can provide a cheaper solution. Do you think AWS has a solution for this?

A. Yes. Amazon SimpleDB
B. No. Not presently
C. Yes. Amazon Redshift
D. Yes. Your choice of relational AMIs on Amazon EC2 and EBS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools. You can start small for just $0.25 per hour with no commitments or upfront costs and scale to a petabyte or more for $1,000 per terabyte per year, less than a tenth of most other data warehousing solutions. Amazon Redshift delivers fast query performance by using columnar storage technology to improve I/O efficiency and parallelizing queries across multiple nodes. Redshift uses standard PostgreSQL JDBC and ODBC drivers, allowing you to use a wide range of familiar SQL clients. Data load speed scales linearly with cluster size, with integrations to Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis or any SSH-enabled host.
Reference: https://aws.amazon.com/running_databases/#redshift_anchor

QUESTION 611
In an experiment, if the minimum size for an Auto Scaling group is 1 instance, which of the following statements holds true when you terminate the running instance?

A. Auto Scaling must launch a new instance to replace it.
B. Auto Scaling will raise an alarm and send a notification to the user for action.
C. Auto Scaling must configure the schedule activity that terminates the instance after 5 days.
D. Auto Scaling will terminate the experiment.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If the minimum size for an Auto Scaling group is 1 instance, when you terminate the running instance, Auto Scaling must launch a new instance to replace it.

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

QUESTION 612
In Amazon EC2, while sharing an Amazon EBS snapshot, can the snapshots with AWS Marketplace product codes be public?

A. Yes, but only for US-based providers.
B. Yes, they can be public.
C. No, they cannot be made public.
D. Yes, they are automatically made public by the system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Snapshots with AWS Marketplace product codes can't be made public.
Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html

QUESTION 613
An organization has created an application which is hosted on the AWS EC2 instance. The application stores images to S3 when the end user uploads to it. The organization does not want to store the AWS secure credentials required to access the S3 inside the instance. Which of the below mentioned options is a possible solution to avoid any security threat?

A. Use the IAM based single sign between the AWS resources and the organization application.
B. Use the IAM role and assign it to the instance.
C. Since the application is hosted on EC2, it does not need credentials to access S3.
D. Use the X.509 certificates instead of the access and the secret access keys.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The AWS IAM role uses temporary security credentials to access AWS services. Once the role is assigned to an instance, it will not need any security credentials to be stored on the instance.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

QUESTION 614
Can resource record sets in a hosted zone have a different domain suffix (for example, www.blog.acme.com and www.acme.ca)?

A. Yes, it can have for a maximum of three different TLDs.
B. Yes
C. Yes, it can have depending on the TLD.
D. No

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The resource record sets contained in a hosted zone must share the same suffix. For example, the example.com hosted zone can contain resource record sets for www.example.com and www.aws.example.com subdomains, but it cannot contain resource record sets for a www.example.ca subdomain.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHosedZones.html

QUESTION 615
You are running PostgreSQL on Amazon RDS and it seems to be all running smoothly deployed in one availability zone. A database administrator asks you if DB instances running PostgreSQL support Multi-AZ deployments. What would be a correct response to this question?

A. Yes.
B. Yes, but only for small db instances.

C. No.
D. Yes but you need to request the service from AWS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS supports DB instances running several versions of PostgreSQL. Currently we support PostgreSQL versions 9.3.1, 9.3.2, and 9.3.3. You can create DB instances and DB snapshots, point-in-time restores and backups.
DB instances running PostgreSQL support Multi-AZ deployments, Provisioned IOPS, and can be created inside a VPC. You can also use SSL to connect to a DB instance running PostgreSQL. You can use any standard SQL client application to run commands for the instance from your client computer. Such applications include pgAdmin, a popular Open Source administration and development tool for PostgreSQL, or psql, a command line utility that is part of a PostgreSQL installation. In order to deliver a managed service experience, Amazon RDS does not provide host access to DB instances, and it restricts access to certain system procedures and tables that require advanced privileges.
Amazon RDS supports access to databases on a DB instance using any standard SQL client application. Amazon RDS does not allow direct host access to a DB instance via Telnet or Secure Shell (SSH).
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_PostgreSQL.html

QUESTION 616
A user has launched 10 EC2 instances inside a placement group. Which of the below mentioned statements is true with respect to the placement group?

A. All instances must be in the same AZ
B. All instances can be across multiple regions
C. The placement group cannot have more than 5 instances
D. All instances must be in the same region

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A placement group is a logical grouping of EC2 instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gbps network.
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 617
Which of the following AWS CLI commands is syntactically incorrect?

1. $ aws ec2 describe-instances
2. $ aws ec2 start-instances --instance-ids i-1348636c
3. $ aws sns publish --topic-arn arn:aws:sns:us-east-1:546419318123:OperationsError -message "Script Failure"
4. $ aws sqs receive-message --queue-url https://queue.amazonaws.com/546419318123/Test

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following CLI command is missing a hyphen before "-message". aws sns publish --topic-arn arn:aws:sns:us-east-1:546419318123:OperationsError -message "Script Failure".
It has been added below in red aws sns publish --topic-arn arn:aws:sns:us-east-1:546419318123:OperationsError ---message
"Script Failure"
Reference: http://aws.amazon.com/cli/

QUESTION 618
An organization has developed a mobile application which allows end users to capture a photo on their mobile device, and store it inside an application. The application internally uploads the data to AWS S3. The organization wants each user to be able to directly upload data to S3 using their Google ID. How will the mobile app allow this?

A. Use the AWS Web identity federation for mobile applications, and use it to generate temporary security credentials for each user.
B. It is not possible to connect to AWS S3 with a Google ID.
C. Create an IAM user every time a user registers with their Google ID and use IAM to upload files to S3.
D. Create a bucket policy with a condition which allows everyone to upload if the login ID has a Google part to it.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For Amazon Web Services, the Web identity federation allows you to create cloud-backed mobile apps that use public identity providers, such as login with Facebook, Google, or Amazon. It will create temporary security credentials for each user, which will be authenticated by the AWS services, such as S3.
Reference: http://docs.aws.amazon.com/STS/latest/UsingSTS/CreatingWIF.htm

QUESTION 619
You are architecting an auto-scalable batch processing system using video processing pipelines and Amazon Simple Queue Service (Amazon SQS) for a customer. You are unsure of the limitations of SQS and need to find out. What do you think is a correct statement about the limitations of Amazon SQS?

A. It supports an unlimited number of queues but a limited number of messages per queue for each user but automatically deletes messages that have been in the queue for more than 4 weeks.
B. It supports an unlimited number of queues and unlimited number of messages per queue for each user but automatically deletes messages that have been in the queue for more than 4 days.
C. It supports an unlimited number of queues but a limited number of messages per queue for each user but automatically deletes messages that have been in the queue

for more than 4 days.

D. It supports an unlimited number of queues and unlimited number of messages per queue for each user but automatically deletes messages that have been in the queue for more than 4 weeks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Simple Queue Service (Amazon SQS) is a messaging queue service that handles message or workflows between other components in a system.
Amazon SQS supports an unlimited number of queues and unlimited number of messages perqueue for each user. Please be aware that Amazon SQS automatically deletes messages that have been in the queue for more than 4 days.
Reference: http://aws.amazon.com/documentation/sqs/

QUESTION 620
An online gaming site asked you if you can deploy a database that is a fast, highly scalable NoSQL database service in AWS for a new site that he wants to build. Which database should you recommend?

A. Amazon DynamoDB
B. Amazon RDS
C. Amazon Redshift
D. Amazon SimpleDB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon DynamoDB is ideal for database applications that require very low latency and predictable performance at any scale but don't need complex querying capabilities like joins or transactions. Amazon DynamoDB is a fully-managed NoSQL database service that offers high performance, predictable throughput and low cost. It is easy to set up, operate, and scale. With Amazon DynamoDB, you can start small, specify the throughput and storage you need, and easily scale your capacity requirements on the fly. Amazon DynamoDB automatically partitions data over a number of servers to meet your request capacity. In addition, DynamoDB automatically replicates your data synchronously across multiple Availability Zones within an AWS Region to ensure high-availability and data durability.
Reference: https://aws.amazon.com/running_databases/#dynamodb_anchor

QUESTION 621
You have been doing a lot of testing of your VPC Network by deliberately failing EC2 instances to test whether instances are failing over properly. Your customer who will be paying the AWS bill for all this asks you if he being charged for all these instances. You try to explain to him how the billing works on EC2 instances to the best of your knowledge. What would be an appropriate response to give to the customer in regards to this?

A. Billing commences when Amazon EC2 AMI instance is completely up and billing ends as soon as the instance starts to shutdown.
B. Billing only commences only after 1 hour of uptime and billing ends when the instance terminates.
C. Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance and billing ends when the instance shuts down.
D. Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance and billing ends as soon as the instance starts to shutdown.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance. Billing ends when the instance shuts down, which could occur through a web services command, by running "shutdown -h", or through instance failure.
Reference: http://aws.amazon.com/ec2/faqs/#Billing

QUESTION 622
You log in to IAM on your AWS console and notice the following message. "Delete your root access keys." Why do you think IAM is requesting this?

A. Because the root access keys will expire as soon as you log out.
B. Because the root access keys expire after 1 week.
C. Because the root access keys are the same for all users.
D. Because they provide unrestricted access to your AWS resources.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS an access key is required in order to sign requests that you make using the command-line interface (CLI), using the AWS SDKs, or using direct API calls. Anyone who has the access key for your root account has unrestricted access to all the resources in your account, including billing information. One of the best ways to protect your account is to not have an access key for your root account. We recommend that unless you must have a root access key (this is very rare), that you do not generate one. Instead, AWS best practice is to create one or more AWS Identity and Access Management (IAM) users, give them the necessary permissions, and use IAM users for everyday interaction with AWS.
Reference:
http://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html#root-Password

QUESTION 623
Once again your customers are concerned about the security of their sensitive data and with their latest enquiry ask about what happens to old storage devices on AWS. What would be the best answer to this question?

A. AWS reformats the disks and uses them again.
B. AWS uses the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process.
C. AWS uses their own proprietary software to destroy data as part of the decommissioning process.
D. AWS uses a 3rd party security organization to destroy data as part of the decommissioning process.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

QUESTION 624
Your company has been storing a lot of data in Amazon Glacier and has asked for an inventory of what is in there exactly. So you have decided that you need to download a vault inventory. Which of the following statements is incorrect in relation to Vault Operations in Amazon Glacier?

A. You can use Amazon Simple Notification Service (Amazon SNS) notifications to notify you when the job completes.
B. A vault inventory refers to the list of archives in a vault.
C. You can use Amazon Simple Queue Service (Amazon SQS) notifications to notify you when the job completes.
D. Downloading a vault inventory is an asynchronous operation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Glacier supports various vault operations.
A vault inventory refers to the list of archives in a vault. For each archive in the list, the inventory provides archive information such as archive ID, creation date, and size. Amazon Glacier updates the vault inventory approximately once a day, starting on the day the first archive is uploaded to the vault. A vault inventory must exist for you to be able to download it.
Downloading a vault inventory is an asynchronous operation. You must first initiate a job to download the inventory. After receiving the job request, Amazon Glacier prepares your inventory for download. After the job completes, you can download the inventory data.
Given the asynchronous nature of the job, you can use Amazon Simple Notification Service (Amazon SNS) notifications to notify you when the job completes. You can specify an Amazon SNS topic for each individual job request or configure your vault to send a notification when specific vault events occur. Amazon Glacier prepares an inventory for each vault periodically, every 24 hours. If there have been no archive additions or deletions to the vault since the last inventory, the inventory date is not updated. When you initiate a job for a vault inventory, Amazon Glacier returns the last inventory it generated, which is a point-in-time snapshot and not real-time data. You might not find it useful to retrieve vault inventory for each archive upload. However, suppose you maintain a database on the client-side associating metadata about the archives you upload to Amazon Glacier. Then, you might find the vault inventory useful to reconcile information in your database with the actual vault inventory.
Reference: http://docs.aws.amazon.com/amazonglacier/latest/dev/working-with-vaults.html

QUESTION 625
A customer enquires about whether all his data is secure on AWS and is especially concerned about Elastic Map Reduce (EMR) so you need to inform him of some of the security features in place for AWS. Which of the below statements would be an incorrect response to your customers enquiry?

A. Amazon EMR customers can choose to send data to Amazon S3 using the HTTPS protocol for secure transmission.
B. Amazon S3 provides authentication mechanisms to ensure that stored data is secured against unauthorized access.
C. Every packet sent in the AWS network uses Internet Protocol Security (IPsec).
D. Customers may encrypt the input data before they upload it to Amazon S3.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://aws.amazon.com/elasticmapreduce/faqs/

QUESTION 626
You are in the process of building an online gaming site for a client and one of the requirements is that it must be able to process vast amounts of data easily. Which AWS Service would be very helpful in processing all this data?

A. Amazon S3
B. AWS Data Pipeline
C. AWS Direct Connect
D. Amazon EMR

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Managing and analyzing high data volumes produced by online games platforms can be difficult.
The back-end infrastructures of online games can be challenging to maintain and operate. Peak usage periods, multiple players, and high volumes of write operations are some of the most common problems that operations teams face.Amazon Elastic MapReduce (Amazon EMR) is a service that processes vast amounts of data easily. Input data can be retrieved from web server logs stored on Amazon S3 or from player data stored in Amazon DynamoDB tables to run analytics on player behavior, usage patterns, etc.
Those results can be stored again on Amazon S3, or inserted in a relational database for further analysis with classic business intelligence tools.
Reference: http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_games_10.pdf

QUESTION 627
You need to change some settings on Amazon Relational Database Service but you do not want the database to reboot immediately which you know might happen depending on the setting that you change. Which of the following will cause an immediate DB instance reboot to occur?

A. You change storage type from standard to PIOPS, and Apply Immediately is set to true.
B. You change the DB instance class, and Apply Immediately is set to false.
C. You change a static parameter in a DB parameter group.
D. You change the backup retention period for a DB instance from 0 to a nonzero value or from a nonzero value to 0, and Apply Immediately is set to false.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A DB instance outage can occur when a DB instance is rebooted, when the DB instance is put into a state that prevents access to it, and when the database is restarted. A reboot can occur when you manually reboot your DB instance or when you change a DB instance setting that requires a reboot before it can take effect.
A DB instance reboot occurs immediately when one of the following occurs:
You change the backup retention period for a DB instance from 0 to a nonzero value or from a nonzero value to 0 and set Apply Immediately to true.
You change the DB instance class, and Apply Immediately is set to true. You change storage type from standard to PIOPS, and Apply Immediately is set to true. A DB instance reboot occurs during the maintenance window when one of the following occurs:
You change the backup retention period for a DB instance from 0 to a nonzero value or from a nonzero value to 0, and Apply Immediately is set to false.
You change the DB instance class, and Apply Immediately is set to false.
Reference:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html#CHAP_Troubleshooting.Security

QUESTION 628
What does the following policy for Amazon EC2 do?

```
{
"Statement":[{
"Effect":"Allow",
"Action":"ec2:Describe*",
"Resource":"*"
}]
}
```

A. Allow users to use actions that start with "Describe" over all the EC2 resources.
B. Share an AMI with a partner
C. Share an AMI within the account
D. Allow a group to only be able to describe, run, stop, start, and terminate instances

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use IAM policies to control the actions that your users can perform against your EC2 resources. For instance, a policy with the following statement will allow users to perform actions whose name start with "Describe" against all your EC2 resources.

```
{
"Statement":[{
"Effect":"Allow",
"Action":"ec2:Describe*",
"Resource":"*"
}]
}
```

Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM.html

QUESTION 629
You are setting up a very complex financial services grid and so far it has 5 Elastic IP (EIP) addresses. You go to assign another EIP address, but all accounts are limited to 5 Elastic IP addresses per region by default, so you aren't able to. What is the reason for this?

A. For security reasons.
B. Hardware restrictions.
C. Public (IPV4) internet addresses are a scarce resource.
D. There are only 5 network interfaces per instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Public (IPV4) internet addresses are a scarce resource. There is only a limited amount of public IP space available, and Amazon EC2 is committed to helping use that space efficiently. By default, all accounts are limited to 5 Elastic IP addresses per region. If you need more than 5 Elastic IP addresses, AWS asks that you apply for your limit to be raised. They will ask you to think through your use case and help them understand your need for additional addresses.
Reference:
http://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2

QUESTION 630
Amazon RDS provides high availability and failover support for DB instances using _____.

A. customized deployments
B. Appstream customizations
C. log events
D. Multi-AZ deployments

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Multi-AZ deployments for Oracle, PostgreSQL, MySQL, and

MariaDB DB instances use Amazon technology, while SQL Server DB instances use SQL Server Mirroring.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

QUESTION 631
A major customer has asked you to set up his AWS infrastructure so that it will be easy to recover in the case of a disaster of some sort. Which of the following is important when thinking about being able to quickly launch resources in AWS to ensure business continuity in case of a disaster?

A. Create and maintain AMIs of key servers where fast recovery is required.
B. Regularly run your servers, test them, and apply any software updates and configuration changes.
C. All items listed here are important when thinking about disaster recovery.
D. Ensure that you have all supporting custom software packages available in AWS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the event of a disaster to your AWS infrastructure you should be able to quickly launch resources in Amazon Web Services (AWS) to ensure business continuity.
The following are some key steps you should have in place for preparation:
1. Set up Amazon EC2 instances to replicate or mirror data.
2. Ensure that you have all supporting custom software packages available in AWS.
3. Create and maintain AMIs of key servers where fast recovery is required.
4. Regularly run these servers, test them, and apply any software updates and configuration changes.
5. Consider automating the provisioning of AWS resources.
Reference: http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf

QUESTION 632
What does Amazon DynamoDB provide?

A. A predictable and scalable MySQL database
B. A fast and reliable PL/SQL database cluster
C. A standalone Cassandra database, managed by Amazon Web Services
D. A fast, highly scalable managed NoSQL database service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon DynamoDB is a managed NoSQL database service offered by Amazon. It automatically manages tasks like scalability for you while it provides high availability and durability for your data, allowing you to concentrate in other aspects of your application.
Reference: https://aws.amazon.com/running_databases/

QUESTION 633
You want to use AWS Import/Export to send data from your S3 bucket to several of your branch offices. What should you do if you want to send 10 storage units to AWS?

A. Make sure your disks are encrypted prior to shipping.
B. Make sure you format your disks prior to shipping.
C. Make sure your disks are 1TB or more.
D. Make sure you submit a separate job request for each device.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When using Amazon Import/Export, a separate job request needs to be submitted for each physical device even if they belong to the same import or export job.
Reference:
http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html

QUESTION 634
What would be the best way to retrieve the public IP address of your EC2 instance using the CLI?

A. Using tags
B. Using traceroute
C. Using ipconfig
D. Using instance metadata

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To determine your instance's public IP address from within the instance, you can use instance metadata. Use the following command to access the public IP address: For Linux use, $ curl http://169.254.169.254/latest/meta-data/public-ipv4, and for Windows use, $ wget http://169.254.169.254/latest/meta-data/public-ipv4.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

QUESTION 635
You need to measure the performance of your EBS volumes as they seem to be under performing. You have come up with a measurement of 1,024 KB I/O but your colleague tells you that EBS volume performance is measured in IOPS. How many IOPS is equal to 1,024 KB I/O?

A. 16
B. 256
C. 8
D. 4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration. IOPS are input/output operations per second. Amazon EBS measures each I/O operation per second (that is 256 KB or smaller) as one IOPS. I/O operations that are larger than 256 KB are counted in 256 KB capacity units.
For example, a 1,024 KB I/O operation would count as 4 IOPS. When you provision a 4,000 IOPS volume and attach it to an EBS-optimized instance that can provide the necessary bandwidth, you can transfer up to 4,000 chunks of data per second (provided that the I/O does not exceed the 128 MB/s per volume throughput limit of General Purpose (SSD) and Provisioned IOPS (SSD) volumes).
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html

QUESTION 636
Having set up a website to automatically be redirected to a backup website if it fails, you realize that there are different types of failovers that are possible. You need all your resources to be available the majority of the time. Using Amazon Route 53 which configuration would best suit this requirement?

A. Active-active failover.
B. None. Route 53 can't failover.
C. Active-passive failover.
D. Active-active-passive and other mixed configurations.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can set up a variety of failover configurations using Amazon Route 53 alias: weighted, latency, geolocation routing, and failover resource record sets.
Active-active failover: Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Amazon Route 53 can detect that it's unhealthy and stop including it when responding to queries. Active-passive failover: Use this failover configuration when you want a primary group of resources to be available the majority of the time and you want a secondary group of resources to be on standby in case all of the primary resources become unavailable. When responding to queries, Amazon Route 53 includes only the healthy primary resources. If all of the primary resources are unhealthy, Amazon Route 53 begins to include only the healthy secondary resources in response to DNS queries. Active-active-passive and other mixed configurations: You can combine alias and non-alias resource record sets to produce a variety of Amazon Route 53 behaviors.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html

QUESTION 637
AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. What formatting is required for this template?

A. JSON-formatted document
B. CSS-formatted document
C. XML-formatted document
D. HTML-formatted document

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
You can write an AWS CloudFormation template (a JSON-formatted document) in a text editor or pick an existing template. The template describes the resources you want and their settings. For example, suppose you want to create an Amazon EC2. Your template can declare an instance Amazon EC2 and describe its properties, as shown in the following example:

```
{
"AWSTemplateFormatVersion" :
"2010
-
09
-
09",
"Des
cription" : "A simple Amazon EC2 instance",
"Resources" : {
"MyEC2Instance" : {
"Type" : "AWS::EC2::Instance",
Get
Latest & Actual
Amazon
Exam's Question and Answers
from Lead2pass.
http://www.
lead2pass
.com
172
"Properties" : {
"ImageId" : "ami
-
2f726546",
"InstanceType" : "t1.micro"
}
}
}
}
```

Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis-howdoesitwork.html

QUESTION 638

True or False: In Amazon Route 53, you can create a hosted zone for a top-level domain (TLD).

A. FALSE
B. False, Amazon Route 53 automatically creates it for you.
C. True, only if you send an XML document with a CreateHostedZoneRequest element for TLD.
D. TRUE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Route 53, you cannot create a hosted zone for a top-level domain (TLD).
Reference:
http://docs.aws.amazon.com/Route53/latest/APIReference/API_CreateHostedZone.html

QUESTION 639
You decide that you need to create a number of Auto Scaling groups to try and save some money as you have noticed that at certain times most of your EC2 instances are not being used. By default, what is the maximum number of Auto Scaling groups that AWS will allow you to create?

A. 12
B. Unlimited
C. 20
D. 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Auto Scaling is an AWS service that allows you to increase or decrease the number of EC2 instances within your application's architecture. With Auto Scaling, you create collections of EC2 instances, called Auto Scaling groups. You can create these groups from scratch, or from existing EC2 instances that are already in production.
Reference:
http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_autoscaling

QUESTION 640
A user needs to run a batch process which runs for 10 minutes. This will only be run once, or at maximum twice, in the next month, so the processes will be temporary only. The process needs 15 X-Large instances. The process downloads the code from S3 on each instance when it is launched, and then generates a temporary log file. Once the instance is terminated, all the data will be lost. Which of the below mentioned pricing models should the user choose in this case?

A. Spot instance.
B. Reserved instance.
C. On-demand instance.
D. EBS optimized instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Web Services, the spot instance is useful when the user wants to run a process temporarily. The spot instance can terminate the instance if the other user outbids the existing bid. In this case all storage is temporary and the data is not required to be persistent. Thus, the spot instance is a good option to save money.
Reference: http://aws.amazon.com/ec2/purchasing-options/spot-instances/

QUESTION 641
Which of the following is NOT a characteristic of Amazon Elastic Compute Cloud (Amazon EC2)?

A. It can be used to launch as many or as few virtual servers as you need.
B. It increases the need to forecast traffic by providing dynamic IP addresses for static cloud computing.
C. It eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
D. It offers scalable computing capacity in the Amazon Web Services (AWS) cloud.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

QUESTION 642
You have been storing massive amounts of data on Amazon Glacier for the past 2 years and now start to wonder if there are any limitations on this. What is the correct answer to your question?

A. The total volume of data is limited but the number of archives you can store are unlimited.
B. The total volume of data is unlimited but the number of archives you can store are limited.
C. The total volume of data and number of archives you can store are unlimited.
D. The total volume of data is limited and the number of archives you can store are limited.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An archive is a durably stored block of information. You store your data in Amazon Glacier as archives. You may upload a single file as an archive, but your costs will be

lower if you aggregate your data. TAR and ZIP are common formats that customers use to aggregate multiple files into a single file before uploading to Amazon Glacier.
The total volume of data and number of archives you can store are unlimited. Individual Amazon Glacier archives can range in size from 1 byte to 40 terabytes.
The largest archive that can be uploaded in a single upload request is 4 gigabytes. For items larger than 100 megabytes, customers should consider using the Multipart upload capability. Archives stored in Amazon Glacier are immutable, i.e. archives can be uploaded and deleted but cannot be edited or overwritten.
Reference: https://aws.amazon.com/glacier/faqs/

QUESTION 643
You are setting up your first Amazon Virtual Private Cloud (Amazon VPC) so you decide to use the VPC wizard in the AWS console to help make it easier for you. Which of the following statements is correct regarding instances that you launch into a default subnet via the VPC wizard?

A. Instances that you launch into a default subnet receive a public IP address and 10 private IP addresses.
B. Instances that you launch into a default subnet receive both a public IP address and a private IP address.
C. Instances that you launch into a default subnet don't receive any ip addresses and you need to define them manually.
D. Instances that you launch into a default subnet receive a public IP address and 5 private IP addresses.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instances that you launch into a default subnet receive both a public IP address and a private IP address. Instances in a default subnet also receive both public and private DNS hostnames. Instances that you launch into a nondefault subnet in a default VPC don't receive a public IP address or a DNS hostname. You can change your subnet's default public IP addressing behavior.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/default-vpc.html

QUESTION 644
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. Communication between the load balancer and back-end instances is always through IPV4
C. ELB DNS supports both IPV4 and IPV6
D. The ELB supports either IPV4 or IPV6 but not both

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/UserScenariosForEC2.html

QUESTION 645
Does AWS CloudFormation support Amazon EC2 tagging?

A. Yes, AWS CloudFormation supports Amazon EC2 tagging
B. No, CloudFormation doesn't support any tagging
C. No, it doesn't support Amazon EC2 tagging.
D. It depends if the Amazon EC2 tagging has been defined in the template.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudFormation, Amazon EC2 resources that support the tagging feature can also be tagged in an AWS template. The tag values can refer to template parameters, other resource names, resource attribute values (e.g. addresses), or values computed by simple functions (e.g., a concatenated list of strings).
Reference: http://aws.amazon.com/cloudformation/faqs/

QUESTION 646
An existing client comes to you and says that he has heard that launching instances into a VPC (virtual private cloud) is a better strategy than launching instances into a EC2-classic which he knows is what you currently do. You suspect that he is correct and he has asked you to do some research about this and get back to him. Which of the following statements is true in regards to what ability launching your instances into a VPC instead of EC2-Classic gives you?

A. All of the things listed here.
B. Change security group membership for your instances while they're running
C. Assign static private IP addresses to your instances that persist across starts and stops
D. Define network interfaces, and attach one or more network interfaces to your instances

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By launching your instances into a VPC instead of EC2-Classic, you gain the ability to:
Assign static private IP addresses to your instances that persist across starts andstops Assign multiple IP addresses to your instances.
Define network interfaces, and attach one or more network interfaces to your instances Change security group membership for your instances while they're running
Control the outbound traffic from your instances (egress filtering) in addition to controlling the inbound traffic to them (ingress filtering).
Add an additional layer of access control to your instances in the form of network access control lists (ACL).
Run your instances on single-tenant hardware
Reference: http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf

QUESTION 647
Amazon S3 allows you to set per-file permissions to grant read and/or write access. However, you have decided that you want an entire bucket with 100 files already in it to be accessible to the public. You don't want to go through 100 files individually and set permissions. What would be the best way to do this?

A. Move the bucket to a new region
B. Add a bucket policy to the bucket.
C. Move the files to a new bucket.
D. Use Amazon EBS instead of S3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon S3 supports several mechanisms that give you flexibility to control who can access your data as well as how, when, and where they can access it. Amazon S3 provides four different access control mechanisms: AWS Identity and Access Management (IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication. IAM enables organizations to create and manage multiple users under a single AWS account. With IAM policies, you can grant IAM users fine-grained control to your Amazon S3 bucket or objects. You can use ACLs to selectively add (grant) certain permissions on individual objects.
Amazon S3 bucket policies can be used to add or deny permissions across some or all of the objects within a single bucket.
With Query string authentication, you have the ability to share Amazon S3 objects through URLs that are valid for a specified period of time.
Reference: http://aws.amazon.com/s3/details/#security

QUESTION 648
A user is accessing an EC2 instance on the SSH port for IP 10.20.30.40. Which one is a secure way to configure that the instance can be accessed only from this IP?

A. In the security group, open port 22 for IP 10.20.30.40
B. In the security group, open port 22 for IP 10.20.30.40/32
C. In the security group, open port 22 for IP 10.20.30.40/24
D. In the security group, open port 22 for IP 10.20.30.40/0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS EC2, while configuring a security group, the user needs to specify the IP address in CIDR notation. The CIDR IP range 10.20.30.40/32 says it is for a single IP 10.20.30.40. If the user specifies the IP as 10.20.30.40 only, the security group will not accept and ask it in a CIDR format.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 649
Which of the following statements is true of creating a launch configuration using an EC2 instance?

A. The launch configuration can be created only using the Query APIs.
B. Auto Scaling automatically creates a launch configuration directly from an EC2 instance.
C. A user should manually create a launch configuration before creating an Auto Scaling group.
D. The launch configuration should be created manually from the AWS CLI.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can create an Auto Scaling group directly from an EC2 instance. When you use this feature, Auto Scaling automatically creates a launch configuration for you as well.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/create-lc-with-instanceID.html

QUESTION 650
You need to set up a high level of security for an Amazon Relational Database Service (RDS) you have just built in order to protect the confidential information stored in it. What are all the possible security groups that RDS uses?

A. DB security groups, VPC security groups, and EC2 security groups.
B. DB security groups only.
C. EC2 security groups only.
D. VPC security groups, and EC2 security groups.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A security group controls the access to a DB instance. It does so by allowing access to IP address ranges or Amazon EC2 instances that you specify.
Amazon RDS uses DB security groups, VPC security groups, and EC2 security groups. In simple terms, a DB security group controls access to a DB instance that is not in a VPC, a VPC security group controls access to a DB instance inside a VPC, and an Amazon EC2 security group controls access to an EC2 instance and can be used with a DB instance.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

QUESTION 651
You have been using T2 instances as your CPU requirements have not been that intensive. However, you now start to think about larger instance types and start looking at M1 and M3 instances. You are a little confused as to the differences between them as they both seem to have the same ratio of CPU and memory. Which statement below is incorrect as to why you would use one over the other?

A. M3 instances are less expensive than M1 instances.
B. M3 instances are configured with more swap memory than M1 instances.
C. M3 instances provide better, more consistent performance that M1 instances for most use-cases.
D. M3 instances also offer SSD-based instance storage that delivers higher I/O performance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EC2 allows you to set up and configure everything about your instances from your operating system up to your applications. An Amazon Machine Image (AMI) is

simply a packaged-up environment that includes all the necessary bits to set up and boot your instance.
M1 and M3 Standard instances have the same ratio of CPU and memory, some reasons below as to why you would use one over the other.
M3 instances provide better, more consistent performance that M1 instances for most use-cases.
M3 instances also offer SSD-based instance storage that delivers higher I/O performance. M3 instances are also less expensive than M1 instances. Due to these reasons, we recommend M3 for applications that require general purpose instances with a balance of compute, memory, and network resources.
However, if you need more disk storage than what is provided in M3 instances, you may still find M1 instances useful for running your applications.
Reference: https://aws.amazon.com/ec2/faqs/

QUESTION 652
You have set up an Elastic Load Balancer (ELB) with the usual default settings, which route each request independently to the application instance with the smallest load. However, someone has asked you to bind a user's session to a specific application instance so as to ensure that all requests coming from the user during the session will be sent to the same application instance.
AWS has a feature to do this. What is it called?

A. Connection draining
B. Proxy protocol
C. Tagging
D. Sticky session

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An Elastic Load Balancer(ELB) by default, routes each request independently to the application 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 application instance. This ensures that all requests coming from the user during the session will be sent to the same application instance. The key to managing the sticky session is determining how long your load balancer should consistently route the user's request to the same application instance. If your application has its own session cookie, then you can set Elastic Load Balancing to create the session cookie to follow the duration specified by the application's session cookie. If your application does not have its own session cookie, then you can set Elastic Load Balancing to create a session cookie by specifying your own stickiness duration. You can associate stickiness duration for only HTTP/HTTPS load balancer listeners. An application instance must always receive and send two cookies: A cookie that defines the stickiness duration and a special Elastic Load Balancing cookie named AWSELB, that has the mapping to the application instance.
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html#session-stickiness

QUESTION 653
A user wants to achieve High Availability with PostgreSQL DB.
Which of the below mentioned functionalities helps achieve HA?

A. Multi AZ
B. Read Replica
C. Multi region
D. PostgreSQL does not support HA

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
The Multi AZ feature allows the user to achieve High Availability. For Multi AZ, Amazon RDS automatically provisions and maintains a synchronous "standby" replica in a different Availability Zone.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

QUESTION 654
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 create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB
B. The user should attach an IAM role with DynamoDB access to the EC2 instance
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 655
After setting up several database instances in Amazon Relational Database Service (Amazon RDS) you decide that you need to track the performance and health of your databases. How can you do this?

A. Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB snapshot, DB parameter group, or DB security group.
B. Use the free Amazon CloudWatch service to monitor the performance and health of a DB instance.
C. All of the items listed will track the performance and health of a database.
D. View, download, or watch database log files using the Amazon RDS console or Amazon RDS APIs. You can also query some database log files that are loaded into database tables.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-

efficient, resizeable capacity for an industry-standard relational database and manages common database administration tasks. There are several ways you can track the performance and health of a database or a DB instance. You can:
Use the free Amazon CloudWatch service to monitor the performance and health of a DB instance. Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB snapshot, DB parameter group, or DB security group.View, download, or watch database log files using the Amazon RDS console or Amazon RDS APIs. You can also query some database log files that are loaded into database tables. Use the AWS CloudTrail service to record AWS calls made by your AWS account. The calls are recorded in log files and stored in an Amazon S3 bucket.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Monitoring.html

QUESTION 656
You are building a system to distribute confidential documents to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publically accessible from S3 directly?

A. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
B. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).
C. Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
D. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You restrict access to Amazon S3 content by creating an origin access identity, which is a special CloudFront user. You change Amazon S3 permissions to give the origin access identity permission to access your objects, and to remove permissions from everyone else. When your users access your Amazon S3 objects using CloudFront URLs, the CloudFront origin access identity gets the objects on your users' behalf. If your users try to access objects using Amazon S3 URLs, they're denied access. The origin access identity has permission to access objects in your Amazon S3 bucket, but users don't.
Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

QUESTION 657
A user has attached 1 EBS volume to a VPC instance. The user wants to achieve the best fault tolerance of data possible. Which of the below mentioned options can help achieve fault tolerance?

A. Attach one more volume with RAID 1 configuration.
B. Attach one more volume with RAID 0 configuration.
C. Connect multiple volumes and stripe them with RAID 6 configuration.
D. Use the EBS volume as a root device.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user can join multiple provisioned IOPS volumes together in a RAID 1 configuration to achieve better fault tolerance. RAID 1 does not provide a write performance improvement; it requires more bandwidth than non-RAID configurations since the data is written simultaneously to multiple volumes. Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

QUESTION 658
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/LaunchInstance.html

QUESTION 659
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 network I/O are not affected during data download
B. The policy cannot be set on the network I/O
C. There is no way the user can stop scaling as it is already configured
D. Suspend scaling

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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/DeveloperGuide/AS_Concepts.html

QUESTION 660
Select a true statement about Amazon EC2 Security Groups (EC2-Classic).

A. After you launch an instance in EC2-Classic, you can't change its security groups.

B. After you launch an instance in EC2-Classic, you can change its security groups only once.
C. After you launch an instance in EC2-Classic, you can only add rules to a security group.
D. After you launch an instance in EC2-Classic, you cannot add or remove rules from a security group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
After you launch an instance in EC2-Classic, you can't change its security groups. However, you can add rules to or remove rules from a security group, and those changes are automatically applied to all instances that are associated with the security group.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 661
A user has created 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 Simple Notification Service
B. AWS Simple Queue Service
C. AWS Elastic Transcoder
D. AWS Glacier

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 662
Which one of the following answers is not a possible state of Amazon CloudWatch Alarm?

A. INSUFFICIENT_DATA
B. ALARM
C. OK
D. STATUS_CHECK_FAILED

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch Alarms have 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/DeveoperGuide/AlarmThatSendsEmail.html

QUESTION 663
An accountant asks you to design a small VPC network for him and, due to the nature of his business, just needs something where the workload on the network will be low, and dynamic data will be accessed infrequently. Being an accountant, low cost is also a major factor. Which EBS volume type would best suit his requirements?

A. Magnetic
B. Any, as they all perform the same and cost the same.
C. General Purpose (SSD)
D. Magnetic or Provisioned IOPS (SSD)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can choose between three EBS volume types to best meet the needs of their workloads:
General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic. General Purpose (SSD) is the new, SSD-backed, general purpose EBS volume type that we recommend as the default choice for customers. General Purpose (SSD) volumes are suitable for a broad range of workloads, including small to medium sized databases, development and test environments, and boot volumes. Provisioned IOPS (SSD) volumes offer storage with consistent and low-latency performance, and are designed for I/O intensive applications such as large relational or NoSQL databases. Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types.
Magnetic volumes are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.
Reference: https://aws.amazon.com/ec2/faqs/

QUESTION 664
A user is planning to launch a scalable web application. Which of the below mentioned options will not affect the latency of the application?

A. Region.
B. Provisioned IOPS.
C. Availability Zone.
D. Instance size.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS, the instance size decides the I/O characteristics. The provisioned IOPS ensures higher throughput, and lower latency. The region does affect the latency; latency

will always be less when the instance is near to the end user. Within a region the user uses any AZ and this does not affect the latency.
The AZ is mainly for fault toleration or HA.
Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 665
Which of the following strategies can be used to control access to your Amazon EC2 instances?

A. DB security groups
B. IAM policies
C. None of these
D. EC2 security groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IAM policies allow you to specify what actions your IAM users are allowed to perform against your EC2 Instances. However, when it comes to access control, security groups are what you need in order to define and control the way you want your instances to be accessed, and whether or not certain kind of communications are allowed or not.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM.html

QUESTION 666
A user has launched one EC2 instance in the US East region and one in the US West region. The user has launched an RDS instance in the US East region. ow can the user configure access from both the EC2 instances to RDS?

A. It is not possible to access RDS of the US East region from the US West region
B. Configure the US West region's security group to allow a request from the US East region's instance and configure the RDS security group's ingress rule for the US East EC2 group
C. Configure the security group of the US East region to allow traffic from the US West region's instance and configure the RDS security group's ingress rule for the US East EC2 group
D. Configure the security group of both instances in the ingress rule of the RDS security group

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user cannot authorize an Amazon EC2 security group if it is in a different AWS Region than the RDS DB instance. The user can authorize an IP range or specify an Amazon EC2 security group in the same region that refers to an IP address in another region. In this case allow IP of US West inside US East's security group and open the RDS security group for US East region.
Reference:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithSecurtyGroups.

QUESTION 667

In Amazon EC2, if your EBS volume stays in the detaching state, you can force the detachment by clicking _____.

A. Force Detach
B. Detach Instance
C. AttachVolume
D. AttachInstance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If your volume stays in the detaching state, you can force the detachment by clicking Force Detach.
Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/ebs-detaching-volume.html

QUESTION 668
Do you need to shutdown your EC2 instance when you create a snapshot of EBS volumes that serve as root devices?

A. No, you only need to shutdown an instance before deleting it.
B. Yes
C. No, the snapshot would turn off your instance automatically.
D. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Yes, to create a snapshot for Amazon EBS volumes that serve as root devices, you should stop the instance before taking the snapshot.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

QUESTION 669
An organization has a statutory requirement to protect the data at rest for data stored in EBS volumes. Which of the below mentioned options can the organization use to achieve data protection?

A. Data replication.
B. Data encryption.
C. Data snapshot.
D. All the options listed here.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For protecting the Amazon EBS data at REST, the user can use options, such as Data Encryption (Windows / Linux / third party based), Data Replication (AWS internally replicates data for redundancy), and Data Snapshot (for point in time backup).
Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 670
A client of yours has a huge amount of data stored on Amazon S3, but is concerned about someone stealing it while it is in transit. You know that all data is encrypted in transit on AWS, but which of the following is wrong when describing server-side encryption on AWS?

A. Amazon S3 server-side encryption employs strong multi-factor encryption.
B. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
C. In server-side encryption, you manage encryption/decryption of your data, the encryption keys, and related tools.
D. Server-side encryption is about data encryption at rest--that is, Amazon S3 encrypts your data as it writes it to disks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon S3 encrypts your object before saving it on disks in its data centers and decrypts it when you download the objects. You have two options depending on how you choose to manage the encryption keys: Server-side encryption and client-side encryption. Server-side encryption is about data encryption at rest--that is, Amazon S3 encrypts your data as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. Amazon S3 manages encryption and decryption for you. For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects.
In client-side encryption, you manage encryption/decryption of your data, the encryption keys, and related tools. Server-side encryption is an alternative to client-side encryption in which Amazon S3 manages the encryption of your data, freeing you from the tasks of managing encryption and encryption keys. Amazon S3 server-side encryption 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. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html

QUESTION 671
A user is running a batch process which runs for 1 hour every day. Which of the below mentioned options is the right instance type and costing model in this case if the user performs the same task for the whole year?

A. EBS backed instance with on-demand instance pricing.
B. EBS backed instance with heavy utilized reserved instance pricing.
C. EBS backed instance with low utilized reserved instance pricing.
D. Instance store backed instance with spot instance pricing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For Amazon Web Services, the reserved instance helps the user save money if the user is going to run the same instance for a longer period. Generally, if the user uses the instances around 30-40% annually it is recommended to use RI. Here as the instance runs only for 1 hour daily it is not recommended to have RI as it will be costlier. The user should use on-demand with EBS in this case.
Reference: http://aws.amazon.com/ec2/purchasing-options/reserved-instances/

QUESTION 672
You have just set up a large site for a client which involved a huge database which you set up with Amazon RDS to run as a Multi-AZ deployment. You now start to worry about what will happen if the database instance fails. Which statement best describes how this database will function if there is a database failure?

A. Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure.
B. Your database will not resume operation without manual administrative intervention.
C. Updates to your DB Instance are asynchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure.
D. Updates to your DB Instance are synchronously replicated across S3 to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in 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.
When you create or modify your DB Instance to run as a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous "standby" replica in a different Availability Zone. Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure. During certain types of planned maintenance, or in the unlikely event of DB Instance failure or Availability Zone failure, Amazon RDS will automatically failover to the standby so that you can resume database writes and reads as soon as the standby is promoted. Since the name record for your DB Instance remains the same, your application can resume database operation without the need for manual administrative intervention. With Multi-AZ deployments, replication is transparent: you do not interact directly with the standby, and it cannot be used to serve read traffic. If you are using Amazon RDS for MySQL and are looking to scale read traffic beyond the capacity constraints of a single DB Instance, you can deploy one or more Read Replicas.
Reference: http://aws.amazon.com/rds/faqs/

QUESTION 673
Which IAM role do you use to grant AWS Lambda permission to access a DynamoDB Stream?

A. Dynamic role
B. Invocation role
C. Execution role
D. Event Source role

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You grant AWS Lambda permission to access a DynamoDB Stream using an IAM role known as the "execution role".
Reference: http://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html

QUESTION 674
Name the disk storage supported by Amazon Elastic Compute Cloud (EC2).

A. None of these
B. Amazon AppStream store
C. Amazon SNS store
D. Amazon Instance Store

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 675
You are signed in as root user on your account but there is an Amazon S3 bucket under your account that you cannot access. What is a possible reason for this?

A. An IAM user assigned a bucket policy to an Amazon S3 bucket and didn't specify the root user as a principal
B. The S3 bucket is full.
C. The S3 bucket has reached the maximum number of objects allowed.
D. You are in the wrong availability zone

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.
In some cases, you might have an IAM user with full access to IAM and Amazon S3. If the IAM user assigns a bucket policy to an Amazon S3 bucket and doesn't specify the root user as a principal, the root user is denied access to that bucket. However, as the root user, you can still access the bucket by modifying the bucket policy to allow root user access.
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/iam-troubleshooting.html#testing2

QUESTION 676

You have a number of image files to encode. In an Amazon SQS worker queue, you create an Amazon SQS message for each file specifying the command (jpeg-encode) and the location of the file in Amazon S3. Which of the following statements best describes the functionality of Amazon SQS?

A. Amazon SQS is a distributed queuing system that is optimized for horizontal scalability, not for single-threaded sending or receiving speeds.
B. Amazon SQS is for single-threaded sending or receiving speeds.
C. Amazon SQS is a non-distributed queuing system.
D. Amazon SQS is a distributed queuing system that is optimized for vertical scalability and for single-threaded sending or receiving speeds.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon SQS is a distributed queuing system that is optimized for horizontal scalability, not for single-threaded sending or receiving speeds. A single client can send or receive Amazon SQS messages at a rate of about 5 to 50 messages per second. Higher receive performance can be achieved by requesting multiple messages (up to 10) in a single call. It may take several seconds before a message that has been to a queue is available to be received.
Reference: http://media.amazonwebservices.com/AWS_Storage_Options.pdf

QUESTION 677
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 specifying the aggregation data for that period
C. The user can zoom a particular period by double clicking on that period with the mouse
D. The user can zoom a particular period by specifying the period in the Time Range

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch provides the functionality to graph the metric data generated either by the AWS services or the custom metric to make it easier for the user to analyse. The AWS CloudWatch console provides the option to change the granularity of a graph and zoom in to see data over a shorter time period. To zoom, the user has to click in the graph details pane, drag on the graph area for selection, and then release the mouse button.
Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveopeGuide/zoom_in_on_graph.html

QUESTION 678
A scope has been handed to you to set up a super-fast gaming server and you decide that you will use Amazon DynamoDB as your database. For efficient access to data in a table, Amazon DynamoDB creates and maintains indexes for the primary key attributes. A secondary index is a data structure that contains a subset of attributes from a table, along with an alternate key to support Query operations. How many types of secondary indexes does DynamoDB support?

A. 2

B. 16
C. 4
D. As many as you need.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DynamoDB supports two types of secondary indexes:
Local secondary index --an index that has the same hash key as the table, but a different range key. A local secondary index is "local" in the sense that every partition of a local secondary index is scoped to a table partition that has the same hash key.
Global secondary index --an index with a hash and range key that can be different from those on the table. A global secondary index is considered "global" because queries on the index can span all of the data in a table, across all partitions.
Reference:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SecondaryIndexes.html

QUESTION 679
Select the correct statement: Within Amazon EC2, when using Linux instances, the device name /dev/sda1 is _____.

A. reserved for EBS volumes
B. recommended for EBS volumes
C. recommended for instance store volumes
D. reserved for the root device

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Within Amazon EC2, when using a Linux instance, the device name /dev/sda1 is reserved for the root device.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/device_naming.html

QUESTION 680
The common use cases for DynamoDB Fine-Grained Access Control (FGAC) are cases in which the end user wants _____.

A. to change the hash keys of the table directly
B. to check if an IAM policy requires the hash keys of the tables directly
C. to read or modify any codecommit key of the table directly, without a middle-tier service
D. to read or modify the table directly, without a middle-tier service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FGAC can benefit any application that tracks information in a DynamoDB table, where the end user (or application client acting on behalf of an end user) wants to read or modify the table directly, without a middle-tier service. For instance, a developer of a mobile app named Acme can use FGAC to track the top score of every Acme user in a DynamoDB table. FGAC allows the application client to modify only the top score for the user that is currently running the application.
Reference: http://aws.amazon.com/dynamodb/faqs/#security_anchor

QUESTION 681
A user has set up the CloudWatch alarm on the CPU utilization metric at 50%, with a time interval of 5 minutes and 10 periods to monitor. What will be the state of the alarm at the end of 90 minutes, if the CPU utilization is constant at 80%?

A. ALERT
B. ALARM
C. OK
D. INSUFFICIENT_DATA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In this case the alarm watches a metric every 5 minutes for 10 intervals. Thus, it needs at least 50 minutes to come to the "OK" state.
Till then it will be in the INSUFFUCIENT_DATA state.
Since 90 minutes have passed and CPU utilization is at 80% constant, the state of alarm will be "ALARM".
Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html

QUESTION 682
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 have already looked into security groups and you are now trying to understand ACLs. Which statement below is incorrect in relation to ACLs?

A. Supports allow rules and deny rules.
B. Is stateful: Return traffic is automatically allowed, regardless of any rules.
C. Processes rules in number order when deciding whether to allow traffic.
D. Operates at the subnet level (second layer of defense).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Network access control lists (ACLs)--Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
Security groups are stateful: (Return traffic is automatically allowed, regardless of any rules)
Network ACLs are stateless: (Return traffic must be explicitly allowed by rules)
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html

QUESTION 683
A user comes to you and wants access to Amazon CloudWatch but only wants to monitor a specific LoadBalancer. Is it possible to give him access to a specific set of instances or a specific LoadBalancer?

A. No because you can't use IAM to control access to CloudWatch data for specific resources.
B. Yes. You can use IAM to control access to CloudWatch data for specific resources.
C. No because you need to be Sysadmin to access CloudWatch data.
D. Yes. Any user can see all CloudWatch data and needs no access rights.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch integrates with AWS Identity and Access Management (IAM) so that you can specify which CloudWatch actions a user in your AWS Account can perform. For example, you could create an IAM policy that gives only certain users in your organization permission to use GetMetricStatistics. They could then use the action to retrieve data about your cloud resources. You can't use IAM to control access to CloudWatch data for specific resources. For example, you can't give a user access to CloudWatch data for only a specific set of instances or a specific LoadBalancer. Permissions granted using IAM cover all the cloud resources you use with CloudWatch. In addition, you can't use IAM roles with the Amazon CloudWatch command line tools. Using Amazon CloudWatch with IAM doesn't change how you use CloudWatch. There are no changes to CloudWatch actions, and no new CloudWatch actions related to users and access control.
Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingIAM.html

QUESTION 684
A user is planning to make a mobile game which can be played online or offline and will be hosted on EC2. The user wants to ensure that if someone breaks the highest score or they achieve some milestone they can inform all their colleagues through email. Which of the below mentioned AWS services helps achieve this goal?

A. AWS Simple Workflow Service.
B. AWS Simple Email Service.
C. Amazon Cognito
D. AWS Simple Queue Service.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Simple Email Service (Amazon SES) is a highly scalable and cost-effective email-sending service for businesses and developers. It integrates with other AWS services, making it easy to send emails from applications that are hosted on AWS.
Reference: http://aws.amazon.com/ses/faqs/

QUESTION 685
You have multiple VPN connections and want to provide secure communication between sites using the AWS VPN CloudHub. Which statement is the most accurate in describing what you must do to set this up correctly?

A. Create a virtual private gateway with multiple customer gateways, each with unique Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs)
B. Create a virtual private gateway with multiple customer gateways, each with a unique set of keys
C. Create a virtual public gateway with multiple customer gateways, each with a unique Private subnet
D. Create a virtual private gateway with multiple customer gateways, each with unique subnet id

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices. To use the AWS VPN CloudHub, you must create a virtual private gateway with multiple customer gateways, each with unique Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs). Customer gateways advertise the appropriate routes (BGP prefixes) over their VPN connections. These routing advertisements are received and re-advertised to each BGP peer, enabling each site to send data to and receive data from the other sites. The routes for each spoke must have unique ASNs and the sites must not have overlapping IP ranges. Each site can also send and receive data from the VPC as if they were using a standard VPN connection.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

QUESTION 686
You need to create an Amazon Machine Image (AMI) for a customer for an application which does not appear to be part of the standard AWS AMI template that you can see in the AWS console. What are the alternative possibilities for creating an AMI on AWS?

A. You can purchase an AMIs from a third party but cannot create your own AMI.
B. You can purchase an AMIs from a third party or can create your own AMI.
C. Only AWS can create AMIs and you need to wait till it becomes available.
D. Only AWS can create AMIs and you need to request them to create one for you.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can purchase an AMIs from a third party, including AMIs that come with service contracts from organizations such as Red Hat. You can also create an AMI and sell it to other Amazon EC2 users. 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 687

Which one of the below is not an AWS Storage Service?

A. Amazon S3
B. Amazon Glacier
C. Amazon CloudFront
D. Amazon EBS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Storage Services are:
Amazon S3
Amazon Glacier
Amazon EBS
AWS Storage Gateway
Reference: https://console.aws.amazon.com/console

QUESTION 688
You are very concerned about security on your network because you have multiple programmers testing APIs and SDKs and you have no idea what is happening. You think CloudTrail may help but are not sure what it does. Which of the following statements best describes the AWS service CloudTrail?

A. With AWS CloudTrail you can get a history of AWS API calls and related events for your account.
B. With AWS CloudTrail you can get a history of IAM users for your account.
C. With AWS CloudTrail you can get a history of S3 logfiles for your account.
D. With AWS CloudTrail you can get a history of CloudFormation JSON scripts used for your account.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With AWS CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can identify which users and accounts called AWS for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of your trails, and control how administrators turn CloudTrail logging on and off.
Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/what_is_cloud_trail_top_level.html

QUESTION 689
A user has deployed an application on his private cloud. The user is using his own monitoring tool. He wants to configure it so that whenever there is an error, the monitoring tool will notify him via SMS. Which of the below mentioned AWS services will help in this scenario?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: http://aws.amazon.com/sns/

QUESTION 690
After setting up an EC2 security group with a cluster of 20 EC2 instances, you find an error in the security group settings. You quickly make changes to the security group settings. When will the changes to the settings be effective?

A. The settings will be effective immediately for all the instances in the security group.
B. The settings will be effective only when all the instances are restarted.
C. The settings will be effective for all the instances only after 30 minutes.
D. The settings will be effective only for the new instances added to the security group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Redshift applies changes to a cluster security group immediately. So if you have associated the cluster security group with a cluster, inbound cluster access rules in the updated cluster security group apply immediately.
Reference: http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-security-groups.html

QUESTION 691
Regarding Amazon Route 53, if your application is running on Amazon EC2 instances in two or more Amazon EC2 regions and if you have more than one Amazon EC2 instance in one or more regions, you can use _____ to route traffic to the correct region and then use _____to route traffic to instances within the region, based on probabilities that you specify.

A. weighted-based routing; alias resource record sets
B. latency-based routing; weighted resource record sets
C. weighted-based routing; weighted resource record sets
D. latency-based routing; alias resource record sets

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Regarding Amazon Route 53, if your application is running on Amazon EC2 instances in two or more Amazon EC2 regions, and if you have more than one Amazon EC2 instance in one or more regions, you can use latency-based routing to route traffic to the correct region and then use weighted resource record sets to route traffic to instances within the region based on weights that you specify.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Tutorials.html

QUESTION 692
You have a lot of data stored in the AWS Storage Gateway and your manager has come to you asking about how the billing is calculated, specifically the Virtual Tape Shelf usage. What would be a correct response to this?

A. You are billed for the virtual tape data you store in Amazon Glacier and are billed for the size of the virtual tape.
B. You are billed for the virtual tape data you store in Amazon Glacier and billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
C. You are billed for the virtual tape data you store in Amazon S3 and billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
D. You are billed for the virtual tape data you store in Amazon S3 and are billed for the size of the virtual tape.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure.
AWS Storage Gateway billing is as follows.
Volume storage usage (per GB per month):
You are billed for the Cached volume data you store in Amazon S3. You are only billed for volume capacity you use, not for the size of the volume you create. Snapshot Storage usage (per GB per month): You are billed for the snapshots your gateway stores in Amazon S3. These snapshots are stored and billed as Amazon EBS snapshots. Snapshots are incremental backups, reducing your storage charges. When taking a new snapshot, only the data that has changed since your last snapshot is stored.
Virtual Tape Library usage (per GB per month):
You are billed for the virtual tape data you store in Amazon S3. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
Virtual Tape Shelf usage (per GB per month):
You are billed for the virtual tape data you store in Amazon Glacier. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
Reference: https://aws.amazon.com/storagegateway/faqs/

QUESTION 693
You are configuring a new VPC for one of your clients for a cloud migration project, and only a public VPN will be in place. After you created your VPC, you created a new subnet, a new Internet gateway, and attached your internet gateway to your VPC. When you launched your first instance into your VPC, you realized that you aren't able to connect to the instance, even if it is configured with an elastic IP. What should be done to access the instance?

A. A route should be created as 0.0.0.0/0 and your internet gateway as target.
B. Attach another ENI to the instance and connect via new ENI.

C. A NAT instance should be created and all traffic should be forwarded to NAT instance.
D. A NACL should be created that allows all outbound traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All traffic should be routed via Internet Gateway. So, a route should be created with 0.0.0.0/0 as a source, and your Internet Gateway as your target.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

QUESTION 694
A user is currently building a website which will require a large number of instances in six months, when a demonstration of the new site will be given upon launch. Which of the below mentioned options allows the user to procure the resources beforehand so that they need not worry about infrastructure availability during the demonstration?

A. Procure all the instances as reserved instances beforehand.
B. Launch all the instances as part of the cluster group to ensure resource availability.
C. Pre-warm all the instances one month prior to ensure resource availability.
D. Ask AWS now to procure the dedicated instances in 6 months.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Web Services has massive hardware resources at its data centers, but they are finite. The best way for users to maximize their access to these resources is by reserving a portion of the computing capacity that they require. This can be done through reserved instances. With reserved instances, the user literally reserves the computing capacity in the Amazon Web Services cloud.
Reference:
http://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf

QUESTION 695
You receive a bill from AWS but are confused because you see you are incurring different costs for the exact same storage size in different regions on Amazon S3. You ask AWS why this is so.
What response would you expect to receive from AWS?

A. We charge less in different time zones.
B. We charge less where our costs are less.
C. This will balance out next bill.
D. It must be a mistake.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Amazon S3 is storage for the Internet. It's a simple storage service that offers software developers a highly-scalable, reliable, and low-latency data storage infrastructure at very low costs.
AWS charges less where their costs are less.
For example, their costs are lower in the US Standard Region than in the US West (Northern California) Region.
Reference: https://aws.amazon.com/s3/faqs/

QUESTION 696
You are setting up some EBS volumes for a customer who has requested a setup which includes a RAID (redundant array of inexpensive disks). AWS has some recommendations for RAID setups. Which RAID setup is not recommended for Amazon EBS?

A. RAID 5 only
B. RAID 5 and RAID 6
C. RAID 1 only
D. RAID 1 and RAID 6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With Amazon EBS, you can use any of the standard RAID configurations that you can use with a traditional bare metal server, as long as that particular RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level. For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together. RAID 5 and RAID 6 are not recommended for Amazon EBS because the parity write operations of these RAID modes consume some of the IOPS available to your volumes.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.htm

QUESTION 697
You receive the following request from a client to quickly deploy a static website for them, specifically, on AWS. The requirements are low-cost, reliable, online storage, and a reliable and cost-effective way to route customers to the website, as well as a way to deliver content with low latency and high data transfer speeds so that visitors to his website don't experience unnecessary delays. What do you think would be the minimum AWS services that could fulfill the client's request?

A. Amazon Route 53, Amazon CloudFront and Amazon VPC.
B. Amazon S3, Amazon Route 53 and Amazon RDS
C. Amazon S3, Amazon Route 53 and Amazon CloudFront
D. Amazon S3 and Amazon Route 53.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You can easily and inexpensively use AWS to host a website that uses client-side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET). This type of site is called a static website, and is used to display content that does not change frequently. Before you create and deploy a static website, you must plan your architecture to ensure that it meets your requirements. Amazon S3, Amazon Route 53, and Amazon CloudFront would be required in this instance.
Reference: http://docs.aws.amazon.com/gettingstarted/latest/swh/website-hosting-intro.html

QUESTION 698
What is the default maximum number of Access Keys per user?

A. 10
B. 15
C. 2
D. 20

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The default maximum number of Access Keys per user is 2.
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.htm

QUESTION 699
What is the network performance offered by the c4.8xlarge instance in Amazon EC2?

A. 20 Gigabit
B. 10 Gigabit
C. Very High but variable
D. 5 Gigabit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Networking performance offered by the c4.8xlarge instance is 10 Gigabit.
Reference: http://aws.amazon.com/ec2/instance-types/

QUESTION 700
Doug has created a VPC with CIDR 10.201.0.0/16 in his AWS account. In this VPC he has created a public subnet with CIDR block 10.201.31.0/24. While launching a new EC2 from the console, he is not able to assign the private IP address 10.201.31.6 to this instance. Which is the most likely reason for this issue?

A. Private IP address 10.201.31.6 is blocked via ACLs in Amazon infrastructure as a part of platform security.

B. Private address IP 10.201.31.6 is currently assigned to another interface.
C. Private IP address 10.201.31.6 is not part of the associated subnet's IP address range.
D. Private IP address 10.201.31.6 is reserved by Amazon for IP networking purposes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon VPC, you can assign any Private IP address to your instance as long as it is:
Part of the associated subnet's IP address range
Not reserved by Amazon for IP networking purposes
Not currently assigned to another interface
Reference: http://aws.amazon.com/vpc/faqs/

QUESTION 701
You need to create a JSON-formatted text file for AWS CloudFormation. This is your first template and the only thing you know is that the templates include several major sections but there is only one that is required for it to work. What is the only section required?

A. Mappings
B. Outputs
C. Resources
D. Conditions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.
A template is a JSON-formatted text file that describes your AWS infrastructure. Templates include several major sections.
The Resources section is the only section that is required. The first character in the template must be an open brace ({), and the last character must be a closed brace (}).
The following template fragment shows the template structure and sections.
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html

QUESTION 702
You are planning and configuring some EBS volumes for an application. In order to get the most performance out of your EBS volumes, you should attach them to an instance with enough _____ to support your volumes.

A. Redundancy
B. Storage

C. Bandwidth
D. Memory

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you plan and configure EBS volumes for your application, it is important to consider the configuration of the instances that you will attach the volumes to. In order to get the most performance out of your EBS volumes, you should attach them to an instance with enough bandwidth to support your volumes, such as an EBS-optimized instance or an instance with 10 Gigabit network connectivity. This is especially important when you use General Purpose (SSD) or Provisioned IOPS (SSD) volumes, or when you stripe multiple volumes together in a RAID configuration.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-ec2-config.html

QUESTION 703
Can a single EBS volume be attached to multiple EC2 instances at the same time?

A. Yes
B. No
C. Only for high-performance EBS volumes.
D. Only when the instances are located in the US regions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can't attach an EBS volume to multiple EC2 instances. This is because it is equivalent to using a single hard drive with many computers at the same time.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

QUESTION 704
How long does an AWS free usage tier EC2 last for?

A. Forever
B. 12 Months upon signup
C. 1 Month upon signup
D. 6 Months upon signup

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The AWS free usage tier will expire 12 months from the date you sign up. When your free usage expires or if your application use exceeds the free usage tiers, you simply pay the standard, pay-as-you-go service rates.
Reference: http://aws.amazon.com/free/faqs/

QUESTION 705
A user is hosting a website in the US West-1 region. The website has the highest client base from the Asia-Pacific (Singapore / Japan) region. The application is accessing data from S3 before serving it to client.
Which of the below mentioned regions gives a better performance for S3 objects?

A. Japan
B. Singapore
C. US East
D. US West-1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Access to Amazon S3 from within Amazon EC2 in the same region is fast. In this aspect, though the client base is Singapore, the application is being hosted in the US West-1 region. Thus, it is recommended that S3 objects be stored in the US-West-1 region.
Reference: http://media.amazonwebservices.com/AWS_Storage_Options.pdf

QUESTION 706
Which of the following statements is true of tagging an Amazon EC2 resource?

A. You don't need to specify the resource identifier while terminating a resource.
B. You can terminate, stop, or delete a resource based solely on its tags.
C. You can't terminate, stop, or delete a resource based solely on its tags.
D. You don't need to specify the resource identifier while stopping a resource.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Using_Tags.html

QUESTION 707
You have been setting up an Amazon Virtual Private Cloud (Amazon VPC) for your company, including setting up subnets. Security is a concern, and you are not sure which is the best security practice for securing subnets in your VPC. Which statement below is correct in describing the protection of AWS resources in each subnet?

A. You can use multiple layers of security, including security groups and network access control lists (ACL).

B. You can only use access control lists (ACL).
C. You don't need any security in subnets.
D. You can use multiple layers of security, including security groups, network access control lists (ACL) and CloudHSM.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.
To protect the AWS resources in each subnet, you can use multiple layers of security, including security groups and network access control lists (ACL).
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

QUESTION 708
You have been asked to tighten up the password policies in your organization after a serious security breach, so you need to consider every possible security measure. Which of the following is not an account password policy for IAM Users that can be set?

A. Force IAM users to contact an account administrator when the user has allowed his or her password to expire.
B. A minimum password length.
C. Force IAM users to contact an account administrator when the user has entered his password incorrectly.
D. Prevent IAM users from reusing previous passwords.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IAM users need passwords in order to access the AWS Management Console. (They do not need passwords if they will access AWS resources programmatically by using the CLI, AWS SDKs, or the APIs.)
You can use a password policy to do these things:
Set a minimum password length.
Require specific character types, including uppercase letters, lowercase letters, numbers, and non-alphanumeric characters. Be sure to remind your users that passwords are case sensitive.
Allow all IAM users to change their own passwords.
Require IAM users to change their password after a specified period of time (enable password expiration). Prevent IAM users from reusing previous passwords.
Force IAM users to contact an account administrator when the user has allowed his or her password to expire.
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_ManagingPasswordPolicies.html

QUESTION 709
Your organization is in the business of architecting complex transactional databases. For a variety of reasons, this has been done on EBS. What is AWS's recommendation for customers who have architected databases using EBS for backups?

A. Backups to Amazon S3 be performed through the database management system.

B. Backups to AWS Storage Gateway be performed through the database management system.
C. If you take regular snapshots no further backups are required.
D. Backups to Amazon Glacier be performed through the database management system.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.
For customers who have architected complex transactional databases using EBS, it is recommended that backups to Amazon S3 be performed through the database management system so that distributed transactions and logs can be checkpointed.
AWS does not perform backups of data that are maintained on virtual disks attached to running instances on Amazon EC2.
Reference:
http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

QUESTION 710
You have three Amazon EC2 instances with Elastic IP addresses in the US East (Virginia) region, and you want to distribute requests across all three IPs evenly for users for whom US East (Virginia) is the appropriate region.
How many EC2 instances would be sufficient to distribute requests in other regions?

A. 3
B. 9
C. 2
D. 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If your application is running on Amazon EC2 instances in two or more Amazon EC2 regions, and if you have more than one Amazon EC2 instance in one or more regions, you can use latency-based routing to route traffic to the correct region and then use weighted resource record sets to route traffic to instances within the region based on weights that you specify.
For example, suppose you have three Amazon EC2 instances with Elastic IP addresses in the US East (Virginia) region and you want to distribute requests across all three IPs evenly for users for whom US East (Virginia) is the appropriate region. Just one Amazon EC2 instance is sufficient in the other regions, although you can apply the same technique to many regions at once.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Tutorials.html

QUESTION 711
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. Rollback all the changes and terminate all the created services
B. It will wait for the user's input about the error and correct the mistake after the input
C. CloudFormation can never throw an error after launching a few services since it verifies all the steps before launching
D. It will warn the user about the error and ask the user to manually create RDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudFormation is an application management tool which provides application modeling, 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.
Reference: http://aws.amazon.com/cloudformation/faqs/

QUESTION 712
A major client who has been spending a lot of money on his internet service provider asks you to set up an AWS Direct Connection to try and save him some money. You know he needs high-speed connectivity. Which connection port speeds are available on AWS Direct Connect?

A. 500Mbps and 1Gbps
B. 1Gbps and 10Gbps
C. 100Mbps and 1Gbps
D. 1Gbps

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect is a network service that provides an alternative to using the internet to utilize AWS cloud services.
Using AWS Direct Connect, data that would have previously been transported over the Internet can now be delivered through a private network connection between AWS and your datacenter or corporate network.
1Gbps and 10Gbps ports are available. Speeds of 50Mbps, 100Mbps, 200Mbps, 300Mbps, 400Mbps, and 500Mbps can be ordered from any APN partners supporting AWS Direct Connect.
Reference: https://aws.amazon.com/directconnect/faqs/

QUESTION 713
In Amazon EC2, what is the limit of Reserved Instances per Availability Zone each month?

A. 5
B. 20
C. 50
D. 10

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are 20 Reserved Instances per Availability Zone in each month.
Reference: http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html

QUESTION 714
You have just finshed setting up an advertisement server in which one of the obvious choices for a service was Amazon Elastic Map Reduce (EMR) and are now troubleshooting some weird cluster states that you are seeing. Which of the below is not an Amazon EMR cluster state?

A. STARTING
B. STOPPED
C. RUNNING
D. WAITING

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Elastic Map Reduce (EMR) is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. Amazon EMR historically referred to an Amazon EMR cluster (and all processing steps assigned to it) as a "cluster". Every cluster has a unique identifier that starts with "j-". The different cluster states of an Amazon EMR cluster are listed below. STARTING? The cluster provisions, starts, and configures EC2 instances.
BOOTSTRAPPING - Bootstrap actions are being executed on the cluster.
RUNNING - A step for the cluster is currently being run.
WAITING - The cluster is currently active, but has no steps to run.
TERMINATING -The cluster is in the process of shutting down.
TERMINATED – The cluster was shut down without error.
TERMINATED_WITH_ERRORS - The cluster was shut down with errors.
Reference: https://aws.amazon.com/elasticmapreduce/faqs/

QUESTION 715
The AWS CloudHSM service defines a resource known as a high-availability (HA) _____, which is a virtual partition that represents a group of partitions, typically distributed between several physical HSMs for high-availability.

A. proxy group
B. partition group
C. functional group
D. relational group

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The AWS CloudHSM service defines a resource known as a high-availability (HA) partition group, which is a virtual partition that represents a group of partitions, typically distributed between several physical HSMs for high-availability.
Reference: http://docs.aws.amazon.com/cloudhsm/latest/userguide/configuring-ha.html

QUESTION 716
Is it possible to get a history of all EC2 API calls made on your account for security analysis and operational troubleshooting purposes?

A. Yes, by default, the history of your API calls is logged.
B. Yes, you should turn on the CloudTrail in the AWS console.
C. No, you can only get a history of VPC API calls.
D. No, you cannot store history of EC2 API calls on Amazon.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To get a history of all EC2 API calls (including VPC and EBS) made on your account, you simply turn on CloudTrail in the AWS Management Console.
Reference: https://aws.amazon.com/ec2/faqs/

QUESTION 717
You have just set up your first Elastic Load Balancer (ELB) but it does not seem to be configured properly. You discover that before you start using ELB, you have to configure the listeners for your load balancer. Which protocols does ELB use to support the load balancing of applications?

A. HTTP and HTTPS
B. HTTP, HTTPS, TCP, SSL and SSH
C. HTTP, HTTPS, TCP, and SSL
D. HTTP, HTTPS, TCP, SSL and SFTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Before you start using Elastic Load Balancing(ELB), you have to configure the listeners for your load balancer. A listener is a process that listens for connection requests. It is configured with a protocol and a port number for front-end (client to load balancer) and back-end (load balancer to back-end instance) connections.
Elastic Load Balancing supports the load balancing of applications using HTTP, HTTPS (secure HTTP), TCP, and SSL (secure TCP) protocols. The HTTPS uses the SSL protocol to establish secure connections over the HTTP layer. You can also use SSL protocol to establish secure connections over the TCP layer.
The acceptable ports for both HTTPS/SSL and HTTP/TCP connections are 25, 80, 443, 465, 587, and 1024-65535.
Reference: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-listener-config.html

QUESTION 718

After setting up some EC2 instances you now need to set up a monitoring solution to keep track of these instances and to send you an email when the CPU hits a certain threshold. Which statement below best describes what thresholds you can set to trigger a CloudWatch Alarm?

A. Set a target value and choose whether the alarm will trigger when the value is greater than (>), greater than or equal to (>=), less than (<), or less than or equal to (<=) that value.
B. Thresholds need to be set in IAM not CloudWatch
C. Only default thresholds can be set you can't choose your own thresholds.
D. Set a target value and choose whether the alarm will trigger when the value hits this threshold

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS.
You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms.
When you create an alarm, you first choose the Amazon CloudWatch metric you want it to monitor. Next, you choose the evaluation period (e.g., five minutes or one hour) and a statistical value to measure (e.g., Average or Maximum).
To set a threshold, set a target value and choose whether the alarm will trigger when the value is greater than (>), greater than or equal to (>=), less than (<), or less than or equal to (<=) that value.
Reference: http://aws.amazon.com/cloudwatch/faqs/

QUESTION 719
After moving an E-Commerce website for a client from a dedicated server to AWS you have also set up auto scaling to perform health checks on the instances in your group and replace instances that fail these checks. Your client has come to you with his own health check system that he wants you to use as it has proved to be very useful prior to his site running on AWS. What do you think would be an appropriate response to this given all that you know about auto scaling?

A. It is not possible to implement your own health check system. You need to use AWSs health check system.
B. It is not possible to implement your own health check system due to compatibility issues.
C. It is possible to implement your own health check system and then send the instance's health information directly from your system to Cloud Watch.
D. It is possible to implement your own health check system and then send the instance's health information directly from your system to Cloud Watch but only in the US East (N. Virginia) region.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Auto Scaling periodically performs health checks on the instances in your group and replaces instances that fail these checks. By default, these health checks use the results of EC2 instance status checks to determine the health of an instance. If you use a load balancer with your Auto Scaling group, you can optionally choose to include the results of Elastic Load Balancing health checks. Auto Scaling marks an instance unhealthy if the calls to the Amazon EC2 action DescribeInstanceStatus returns any other state other than running, the system status shows impaired, or the calls to Elastic Load Balancing action DescribeInstanceHealth returns OutOfService in the instance state field. After an instance is marked unhealthy because of an Amazon EC2 or Elastic Load Balancing health check, it is scheduled for replacement.
You can customize the health check conducted by your Auto Scaling group by specifying additional checks or by having your own health check system and then sending the instance's health information directly from your system to Auto Scaling.

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

QUESTION 720
When does the billing of an Amazon EC2 system begin?

A. It starts when the Status column for your distribution changes from Creating to Deployed.
B. It starts as soon as you click the create instance option on the main EC2 console.
C. It starts when your instance reaches 720 instance hours.
D. It starts when Amazon EC2 initiates the boot sequence of an AMI instance.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance. Billing ends when the instance terminates, which could occur through a web services command, by running "shutdown -h", or through instance failure. When you stop an instance, Amazon shuts it down but doesn't charge hourly usage for a stopped instance, or data transfer fees, but charges for the storage for any Amazon EBS volumes.
Reference: http://aws.amazon.com/ec2/faqs/

QUESTION 721
You have just discovered that you can upload your objects to Amazon S3 using Multipart Upload API. You start to test it out but are unsure of the benefits that it would provide. Which of the following is not a benefit of using multipart uploads?

A. You can begin an upload before you know the final object size.
B. Quick recovery from any network issues.
C. Pause and resume object uploads.
D. It's more secure than normal upload.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Multipart upload in Amazon S3 allows you to upload a single object as a set of parts. Each part is a contiguous portion of the object's data. You can upload these object parts independently and in any order. If transmission of any part fails, you can re-transmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.
Using multipart upload provides the following advantages:
Improved throughput--You can upload parts in parallel to improve throughput. Quick recovery from any network issues--Smaller part size minimizes the impact of restarting a failed upload due to a network error.
Pause and resume object uploads--You can upload object parts over time. Once you initiate a multipart upload there is no expiry; you must explicitly complete or abort the multipart upload. Begin an upload before you know the final object size--You can upload an object as you are creating it.
Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html

QUESTION 722
What is the data model of DynamoDB?

A. Since DynamoDB is schema-less, there is no data model.
B. "Items", with Keys and one or more Attribute; and "Attribute", with Name and Value.
C. "Table", a collection of Items; "Items", with Keys and one or more Attribute; and "Attribute", with Name and Value.
D. "Database", which is a set of "Tables", which is a set of "Items", which is a set of "Attributes".

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The data model of DynamoDB is:
"Table", a collection of Items;
"Items", with Keys and one or more Attribute;
"Attribute", with Name and Value.
Reference:
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DataModel.html

QUESTION 723
What happens to Amazon EBS root device volumes, by default, when an instance terminates?

A. Amazon EBS root device volumes are moved to IAM.
B. Amazon EBS root device volumes are copied into Amazon RDS.
C. Amazon EBS root device volumes are automatically deleted.
D. Amazon EBS root device volumes remain in the database until you delete them.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By default, Amazon EBS root device volumes are automatically deleted when the instance terminates.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

QUESTION 724
Which of the following would you use to list your AWS Import/Export jobs?

A. Amazon RDS
B. AWS Import/Export Web Service Tool
C. Amazon S3 REST API
D. AWS Elastic Beanstalk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can list AWS Import/Export jobs with the ListJobs command using the command line client or REST API.
Reference: http://docs.aws.amazon.com/AWSImportExport/latest/DG/ListingYourJobs.html

QUESTION 725
A gaming company comes to you and asks you to build them infrastructure for their site. They are not sure how big they will be as with all startups they have limited money and big ideas. What they do tell you is that if the game becomes successful, like one of their previous games, it may rapidly grow to millions of users and generate tens (or even hundreds) of thousands of writes and reads per second. After considering all of this, you decide that they need a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. Which of the following databases do you think would best fit their needs?

A. Amazon DynamoDB
B. Amazon Redshift
C. Any non-relational database.
D. Amazon SimpleDB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. Amazon DynamoDB enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS, so they don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling.
Today's web-based applications generate and consume massive amounts of data. For example, an online game might start out with only a few thousand users and a light database workload consisting of 10 writes per second and 50 reads per second. However, if the game becomes successful, it may rapidly grow to millions of users and generate tens (or even hundreds) of thousands of writes and reads per second. It may also create terabytes or more of data per day.
Developing your applications against Amazon DynamoDB enables you to start small and simply dial-up your request capacity for a table as your requirements scale, without incurring downtime.
You pay highly cost-efficient rates for the request capacity you provision, and let Amazon DynamoDB do the work over partitioning your data and traffic over sufficient server capacity to meet your needs. Amazon DynamoDB does the database management and administration, and you simply store and request your data. Automatic replication and failover provides built-in fault tolerance, high availability, and data durability. Amazon DynamoDB gives you the peace of mind that your database is fully managed and can grow with your application requirements.
Reference: http://aws.amazon.com/dynamodb/faqs

QUESTION 726
Mike is appointed as Cloud Consultant in ABC Inc. It has the following VPCs set-up in the US East Region:
A VPC with CIDR block 10.10.0.0/16, a subnet in that VPC with CIDR block 10.10.1.0/24 A VPC with CIDR block 10.40.0.0/16, a subnet in that VPC with CIDR block 10.40.1.0/24 N. ABC Inc is trying to establish network connection between two subnets, a subnet with CIDR block 10.10.1.0/24 and another subnet with CIDR block 10.40.1.0/24. Which one of the following solutions should Mike recommend to ABC Inc?

A. Create 2 Virtual Private Gateways and configure one with each VPC.
B. Create one EC2 instance in each subnet, assign Elastic IPs to both instances, and configure a set up Site-to-Site VPN connection between both EC2 instances.

C. Create a VPC Peering connection between both VPCs.
D. Create 2 Internet Gateways, and attach one to each VPC.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. EC2 instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

QUESTION 727
A favored client needs you to quickly deploy a database that is a relational database service with minimal administration as he wants to spend the least amount of time administering it. Which database would be the best option?

A. Amazon SimpleDB
B. Your choice of relational AMIs on Amazon EC2 and EBS.
C. Amazon RDS
D. Amazon Redshift

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Relational Database Service (Amazon RDS) is a web service that makes it easy to set up, operate, and scale a relational database in 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 gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server, or PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user-defined retention period and enabling point-in-time recovery.
Reference: https://aws.amazon.com/running_databases/#rds_anchor

QUESTION 728
You're trying to delete an SSL certificate from the IAM certificate store, and you're getting the message "Certificate: <certificate-id> is being used by CloudFront." Which of the following statements is probably the reason why you are getting this error?

A. Before you can delete an SSL certificate, you need to either rotate SSL certificates or revert from using a custom SSL certificate to using the default CloudFront certificate.
B. You can't delete SSL certificates. You need to request it from AWS.
C. Before you can delete an SSL certificate, you need to set up the appropriate access level in IAM
D. Before you can delete an SSL certificate you need to set up https on your server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudFront is a web service that speeds up distribution of your static and dynamic web content, for example, .html, .css, .php, and image files, to end users. Every CloudFront web distribution must be associated either with the default CloudFront certificate or with a custom SSL certificate.
Before you can delete an SSL certificate, you need to either rotate SSL certificates (replace the current custom SSL certificate with another custom SSL certificate) or revert from using a custom SSL certificate to using the default CloudFront certificate.
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Troubleshooting.html

QUESTION 729
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. Evaluate all rules before deciding whether to allow traffic.
C. Support allow rules and deny rules.
D. Operate at the instance level (first layer of defense).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 730
You are setting up some IAM user policies and have also become aware that some services support resource-based permissions, which let you attach policies to the service's resources instead of to IAM users or groups. Which of the below statements is true in regards to resource-level permissions?

A. All services support resource-level permissions for all actions.
B. Resource-level permissions are supported by Amazon CloudFront
C. All services support resource-level permissions only for some actions.
D. Some services support resource-level permissions only for some actions.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon RDS, and the AWS Management Console. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access. In addition to supporting IAM user policies, some services support resource-based permissions, which let you attach policies to the service's resources instead of to IAM users or groups. Resource-based permissions are supported by Amazon S3, Amazon SNS, and Amazon SQS. The resource-level permissions service supports IAM policies in which you can specify individual resources using Amazon Resource Names (ARNs) in the policy's Resource element. Some services support resource-level permissions only for some actions.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_SpecificProducts.html

QUESTION 731
A user wants to increase the durability and availability of the EBS volume. Which of the below mentioned actions should he perform?

A. Take regular snapshots.
B. Create an AMI.
C. Create EBS with higher capacity.
D. Access EBS regularly.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Web Services, Amazon EBS volumes that operate with 20 GB or less of modified data since their most recent snapshot can expect an annual failure rate (AFR) between 0.1% and 0.5%.
For this reason, to maximize both durability and availability of their Amazon EBS data, the user should frequently create snapshots of the Amazon EBS volumes.
Reference: http://media.amazonwebservices.com/AWS_Storage_Options.pdf

QUESTION 732
In relation to AWS CloudHSM, High-availability (HA) recovery is hands-off resumption by failed HA group members.
Prior to the introduction of this function, the HA feature provided redundancy and performance, but required that a failed/lost group member be _____reinstated.

A. automatically
B. periodically
C. manually
D. continuously

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In relation to AWS CloudHSM, High-availability (HA) recovery is hands-off resumption by failed HA group members.

Prior to the introduction of this function, the HA feature provided redundancy and performance, but required that a failed/lost group member be manually reinstated.
Reference: http://docs.aws.amazon.com/cloudhsm/latest/userguide/ha-best-practices.html

QUESTION 733
You have created a Route 53 latency record set from your domain to a machine in Northern Virginia and a similar record to a machine in Sydney.
When a user located in U S visits your domain he will be routed to:

A. Northern Virginia
B. Sydney
C. Both, Northern Virginia and Sydney
D. Depends on the Weighted Resource Record Sets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If your application is running on Amazon EC2 instances in two or more Amazon EC2 regions, and if you have more than one Amazon EC2 instance in one or more regions, you can use latency-based routing to route traffic to the correct region and then use weighted resource record sets to route traffic to instances within the region based on weights that you specify.
For example, suppose you have three Amazon EC2 instances with Elastic IP addresses in the US East (Virginia) region and you want to distribute requests across all three IPs evenly for users for whom US East (Virginia) is the appropriate region. Just one Amazon EC2 instance is sufficient in the other regions, although you can apply the same technique to many regions at once.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Tutorials.html

QUESTION 734
Any person or application that interacts with AWS requires security credentials. AWS uses these credentials to identify who is making the call and whether to allow the requested access. You have just set up a VPC network for a client and you are now thinking about the best way to secure this network. You set up a security group called vpcsecuritygroup. Which following statement is true in respect to the initial settings that will be applied to this security group if you choose to use the default settings for this group?

A. Allow all inbound traffic and allow no outbound traffic.
B. Allow no inbound traffic and allow all outbound traffic.
C. Allow inbound traffic on port 80 only and allow all outbound traffic.
D. Allow all inbound traffic and allow all outbound traffic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon VPC provides advanced security features such as security groups and network access control lists to enable inbound and outbound filtering at the instance level and subnet level. AWS assigns each security group a unique ID in the form sg-xxxxxxxx. The following are the initial settings for a security group that you create:
Allow no inbound traffic
Allow all outbound traffic

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 735
You are using Amazon SES as an email solution but are unsure of what its limitations are. Which statement below is correct in regards to that?

A. New Amazon SES users who have received production access can send up to 1,000 emails per 24-hour period, at a maximum rate of 10 emails per second
B. Every Amazon SES sender has the same set of sending limits
C. Sending limits are based on messages rather than on recipients
D. Every Amazon SES sender has a unique set of sending limits

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Simple Email Service (Amazon SES) is a highly scalable and cost-effective email-sending service for businesses and developers. Amazon SES eliminates the complexity and expense of building an in-house email solution or licensing, installing, and operating a third-party email service for this type of email communication.
Every Amazon SES sender has a unique set of sending limits, which are calculated by Amazon SES on an ongoing basis:
Sending quota --the maximum number of emails you can send in a 24-hour period.
Maximum send rate --the maximum number of emails you can send per second. New Amazon SES users who have received production access can send up to 10,000 emails per 24-hour period, at a maximum rate of 5 emails per second. Amazon SES automatically adjusts these limits upward, as long as you send high-quality email. If your existing quota is not adequate for your needs and the system has not automatically increased your quota, you can submit an SES Sending Quota Increase case at any time.
Sending limits are based on recipients rather than on messages. You can check your sending limits at any time by using the Amazon SES console.
Note that if your email is detected to be of poor or questionable quality (e.g., high complaint rates, high bounce rates, spam, or abusive content), Amazon SES might temporarily or permanently reduce your permitted send volume, or take other action as AWS deems appropriate.
Reference: https://aws.amazon.com/ses/faqs/

QUESTION 736
Having just set up your first Amazon Virtual Private Cloud (Amazon VPC) network, which defined a default network interface, you decide that you need to create and attach an additional network interface, known as an elastic network interface (ENI) to one of your instances. Which of the following statements is true regarding attaching network interfaces to your instances in your VPC?

A. You can attach 5 ENIs per instance type.
B. You can attach as many ENIs as you want.
C. The number of ENIs you can attach varies by instance type.
D. You can attach 100 ENIs total regardless of instance type.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each instance in your VPC has a default network interface that is assigned a private IP address from the IP address range of your VPC. You can create and attach an additional network interface, known as an elastic network interface (ENI), to any instance in your VPC. The number of ENIs you can attach varies by instance type.

QUESTION 737
A _____ for a VPC is a collection of subnets (typically private) that you may want to designate for your backend RDS DB Instances.

A. DB Subnet Set
B. RDS Subnet Group
C. DB Subnet Group
D. DB Subnet Collection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DB Subnet Groups are a set of subnets (one per Availability Zone of a particular region) designed for your DB instances that reside in a VPC. They make easy to manage Multi-AZ deployments as well as the conversion from a Single-AZ to a Mutli-AZ one.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSVPC.html

QUESTION 738
Amazon Elastic Load Balancing is used to manage traffic on a fleet of Amazon EC2 instances, distributing traffic to instances across all availability zones within a region. Elastic Load Balancing has all the advantages of an on-premises load balancer, plus several security benefits. Which of the following is not an advantage of ELB over an on-premise load balancer?

A. ELB uses a four-tier, key-based architecture for encryption.
B. ELB offers clients a single point of contact, and can also serve as the first line of defense against attacks on your network.
C. ELB takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer.
D. ELB supports end-to-end traffic encryption using TLS (previously SSL) on those networks that use secure HTTP (HTTPS) connections.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Elastic Load Balancing is used to manage traffic on a fleet of Amazon EC2 instances, distributing traffic to instances across all availability zones within a region. Elastic Load Balancing has all the advantages of an on-premises load balancer, plus several security benefits:
Takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer
Offers clients a single point of contact, and can also serve as the first line of defense against attacks on your network
When used in an Amazon VPC, supports creation and management of security groups associated with your Elastic Load Balancing to provide additional networking and security options
Supports end-to-end traffic encryption using TLS (previously SSL) on those networks that use secure HTTP (HTTPS) connections. When TLS is used, the TLS server certificate used to terminate client connections can be managed centrally on the load balancer, rather than on every individual instance.
Reference: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

QUESTION 739
You have set up an S3 bucket with a number of images in it and you have decided that you want anybody to be able to access these images, even anonymous users. To

accomplish this you create a bucket policy. You will need to use an Amazon S3 bucket policy that specifies a _____ in the principal element, which means anyone can access the bucket.

A. hash tag (#)
B. anonymous user
C. wildcard (*)
D. S3 user

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket.
You can then use the generated document to set your bucket policy by using the Amazon S3 console, by a number of third-party tools, or via your application.
You use an Amazon S3 bucket policy that specifies a wildcard (*) in the principal element, which means anyone can access the bucket. With anonymous access, anyone (including users without an AWS account) will be able to access the bucket.
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/iam-troubleshooting.html#d0e20565

QUESTION 740
You have been asked to build AWS infrastructure for disaster recovery for your local applications and within that you should use an AWS Storage Gateway as part of the solution. Which of the following best describes the function of an AWS Storage Gateway?

A. Accelerates transferring large amounts of data between the AWS cloud and portable storage devices
B. A web service that speeds up distribution of your static and dynamic web content.
C. Connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between your on-premises IT environment and AWS's storage infrastructure.
D. Is a storage service optimized for infrequently used data, or "cold data"

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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. You can use the service to store data in the AWS cloud for scalable and cost-effective storage that helps maintain data security. AWS Storage Gateway offers both volume-based and tape-based storage solutions:
Volume gateways
Gateway-cached volumes
Gateway-stored volumes
Gateway-virtual tape library (VTL)
Reference:
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_disasterrecovery_07.pdf

QUESTION 741
An organization has a statutory requirement to protect the data at rest for the S3 objects. Which of the below mentioned options need not be enabled by the organization to achieve data security?

A. MFA delete for S3 objects
B. Client side encryption
C. Bucket versioning
D. Data replication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS S3 provides multiple options to achieve the protection of data at REST. The options include Permission (Policy), Encryption (Client and Server Side), Bucket Versioning and MFA based delete. The user can enable any of these options to achieve data protection. Data replication is an internal facility by AWS where S3 replicates each object across all the Availability Zones and the organization need not enable it in this case.
Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 742
In Amazon CloudFront, if you use Amazon EC2 instances and other custom origins with CloudFront, it is recommended to_____.

A. not use Elastic Load Balancing
B. restrict Internet communication to private instances while allowing outgoing traffic
C. enable access key rotation for CloudWatch metrics
D. specify the URL of the load balancer for the domain name of your origin server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon CloudFront, you should use an Elastic Load Balancing load balancer to handle traffic across multiple Amazon EC2 instances and to isolate your application from changes to Amazon EC2 instances. When you create your CloudFront distribution, specify the URL of the load balancer for the domain name of your origin server.
Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/CustomOriginBestPractices.html

QUESTION 743
What is the time period with which metric data is sent to CloudWatch when detailed monitoring is enabled on an Amazon EC2 instance?

A. 15 minutes
B. 5 minutes
C. 1 minute
D. 45 seconds

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 744
A government client needs you to set up secure cryptographic key storage for some of their extremely confidential data. You decide that the AWS CloudHSM is the best service for this. However, there seem to be a few pre-requisites before this can happen, one of those being a security group that has certain ports open. Which of the following is correct in regards to those security groups?

A. A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network.
B. A security group that has no ports open to your network.
C. A security group that has only port 3389 (for RDP) open to your network.
D. A security group that has only port 22 (for SSH) open to your network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudHSM provides secure cryptographic key storage to customers by making hardware security modules (HSMs) available in the AWS cloud.
AWS CloudHSM requires the following environment before an HSM appliance can be provisioned. A virtual private cloud (VPC) in the region where you want the AWS CloudHSM service. One private subnet (a subnet with no Internet gateway) in the VPC. The HSM appliance is provisioned into this subnet.
One public subnet (a subnet with an Internet gateway attached). The control instances are attached to this subnet.
An AWS Identity and Access Management (IAM) role that delegates access to your AWS resources to AWS CloudHSM.
An EC2 instance, in the same VPC as the HSM appliance, that has the SafeNet client software installed. This instance is referred to as the control instance and is used to connect to and manage the HSM appliance.
A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network. This security group is attached to your control instances so you can access them remotely.

QUESTION 745
Which of the following features are provided by Amazon EC2?

A. Exadata Database Machine, Optimized Storage Management, Flashback Technology, and Data Warehousing
B. Instances, Amazon Machine Images (AMIs), Key Pairs, Amazon EBS Volumes, Firewall, Elastic IP address, Tags, and Virtual Private Clouds (VPCs)
C. Real Application Clusters (RAC), Elasticache Machine Images (EMIs), Data Warehousing, Flashback Technology, Dynamic IP address
D. Exadata Database Machine, Real Application Clusters (RAC), Data Guard, Table and Index Partitioning, and Data Pump Compression

Correct Answer: B
Section: (none)

Explanation

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

QUESTION 746
In Amazon Elastic Compute Cloud, which of the following is used for communication between instances in the same network (EC2-Classic or a VPC)?

A. Private IP addresses
B. Elastic IP addresses
C. Static IP addresses
D. Public IP addresses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A private IP address is an IP address that's not reachable over the Internet. You can use private IP addresses for communication between instances in the same network (EC2-Classic or a VPC).
Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

QUESTION 747
A friend tells you he is being charged $100 a month to host his WordPress website, and you tell him you can move it to AWS for him and he will only pay a fraction of that, which makes him very happy. He then tells you he is being charged $50 a month for the domain, which is registered with the same people that set it up, and he asks if it's possible to move that to AWS as well. You tell him you aren't sure, but will look into it. Which of the following statements is true in regards to transferring domain names to AWS?

A. You can't transfer existing domains to AWS.
B. You can transfer existing domains into Amazon Route 53's management.
C. You can transfer existing domains via AWS Direct Connect.
D. You can transfer existing domains via AWS Import/Export.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With Amazon Route 53, you can create and manage your public DNS records with the AWS Management Console or with an easy-to-use API. If you need a domain name, you can find an available name and register it using Amazon Route 53. You can also transfer existing domains into Amazon Route 53's management.
Reference: http://aws.amazon.com/route53/

QUESTION 748

Are penetration tests allowed as long as they are limited to the customer's instances?

A. Yes, they are allowed but only for selected regions.
B. No, they are never allowed.
C. Yes, they are allowed without any permission.
D. Yes, they are allowed but only with approval.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Penetration tests are allowed after obtaining permission from AWS to perform them.
Reference:
http://aws.amazon.com/security/penetration-testing/

QUESTION 749
A user has created an ELB with the availability zone US-East-1A. The user wants to add more zones to ELB to achieve High Availability. How can the user add more zones to the existing ELB?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user has created an Elastic Load Balancer with the availability zone and wants to add more zones to the existing ELB. The user can do so in two ways:
From the console or CLI, add new zones to ELB;
Launch instances in a separate AZ and add instances to the existing ELB.
Reference: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/enable-disable-az.html

QUESTION 750
What happens to data on an ephemeral volume of an EBS-backed EC2 instance if it is terminated or if it fails?

A. Data is automatically copied to another volume.
B. The volume snapshot is saved in S3.
C. Data persists.
D. Data is deleted.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Any data on the instance store volumes persists as long as the instance is running, but this data is deleted when the instance is terminated or if it fails (such as if an underlying drive has issues). After an instance store-backed instance fails or terminates, it cannot be restored.

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

QUESTION 751
A user is sending bulk emails using AWS SES. The emails are not reaching some of the targeted audience because they are not authorized by the ISPs. How can the user ensure that the emails are all delivered?

A. Send an email using DKIM with SES.
B. Send an email using SMTP with SES.
C. Open a ticket with AWS support to get it authorized with the ISP.
D. Authorize the ISP by sending emails from the development account.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Domain Keys Identified Mail (DKIM) is a standard that allows senders to sign their email messages and ISPs, and use those signatures to verify that those messages are legitimate and havenot been modified by a third party in transit.
Reference: http://docs.aws.amazon.com/ses/latest/DeveloperGuide/dkim.html

QUESTION 752
In AWS CloudHSM, in addition to the AWS recommendation that you use two or more HSM appliances in a high-availability configuration to prevent the loss of keys and data, you can also perform a remote backup/restore of a Luna SA partition if you have purchased a:

A. Luna Restore HSM.
B. Luna Backup HSM.
C. Luna HSM.
D. Luna SA HSM.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudHSM, you can perform a remote backup/restore of a Luna SA partition if you have purchased a Luna Backup HSM.
Reference:
http://docs.aws.amazon.com/cloudhsm/latest/userguide/cloud-hsm-backup-restore.html

QUESTION 753
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 instance from the US East region to the EU region
B. Use the "Launch more like this" option to copy the instance from one region to another
C. Copy the running instance using the "Instance Copy" command to the EU region
D. Create an AMI of the instance and copy the AMI to the EU region. Then launch the instance from the EU AMI

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 754
AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. In addition to supporting IAM user policies, some services support resource-based permissions. Which of the following services are supported by resource-based permissions?

A. Amazon SNS, and Amazon SQS and AWS Direct Connect.
B. Amazon S3 and Amazon SQS and Amazon ElastiCache.
C. Amazon S3, Amazon SNS, Amazon SQS, Amazon Glacier and Amazon EBS.
D. Amazon Glacier, Amazon SNS, and Amazon CloudWatch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In addition to supporting IAM user policies, some services support resource-based permissions, which let you attach policies to the service's resources instead of to IAM users or groups. Resource-based permissions are supported by Amazon S3, Amazon SNS, Amazon SQS, Amazon Glacier and Amazon EBS.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_SpecificProducts.html

QUESTION 755
Content and Media Server is the latest requirement that you need to meet for a client. The client has been very specific about his requirements such as low latency, high availability, durability, and access control. Potentially there will be millions of views on this server and because of "spiky" usage patterns, operations teams will need to provision static hardware, network, and management resources to support the maximum expected need. The Customer base will be initially low but is expected to grow and become more geographically distributed.
Which of the following would be a good solution for content distribution?

A. Amazon S3 as both the origin server and for caching
B. AWS Storage Gateway as the origin server and Amazon EC2 for caching
C. AWS CloudFront as both the origin server and for caching
D. Amazon S3 as the origin server and Amazon CloudFront for caching

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
As your customer base grows and becomes more geographically distributed, using a high-performance edge cache like Amazon CloudFront can provide substantial improvements in latency, fault tolerance, and cost.
By using Amazon S3 as the origin server for the Amazon CloudFront distribution, you gain the advantages of fast in-network data transfer rates, simple publishing/caching workflow, and a unified security framework.
Amazon S3 and Amazon CloudFront can be configured by a web service, the AWS Management Console, or a host of third-party management tools.
Reference: http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_media_02.pdf

QUESTION 756
You are setting up your first Amazon Virtual Private Cloud (Amazon VPC) network so you decide you should probably use the AWS Management Console and the VPC Wizard. Which of the following is not an option for network architectures after launching the "Start VPC Wizard" in Amazon VPC page on the AWS Management Console?

A. VPC with a Single Public Subnet Only
B. VPC with a Public Subnet Only and Hardware VPN Access
C. VPC with Public and Private Subnets and Hardware VPN Access
D. VPC with a Private Subnet Only and Hardware VPN Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon VPC enables you to build a virtual network in the AWS cloud -no VPNs, hardware, or physical datacenters required.
Your AWS resources are automatically provisioned in a ready-to-use default VPC. You can choose to create additional VPCs by going to Amazon VPC page on the AWS Management Console and click on the "Start VPC Wizard" button.
You'll be presented with four basic options for network architectures. After selecting an option, you can modify the size and IP address range of the VPC and its subnets. If you select an option with Hardware VPN Access, you will need to specify the IP address of the VPN hardware on your network. You can modify the VPC to add more subnets or add or remove gateways at any time after the VPC has been created.
The four options are:
VPC with a Single Public Subnet Only
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware
VPN Access VPC with a Private Subnet Only and Hardware VPN Access
Reference: https://aws.amazon.com/vpc/faqs/

QUESTION 757
An EC2 instance is connected to an ENI (Elastic Network Interface) in one subnet. What happens when you attach an ENI of a different subnet to this EC2 instance?

A. The EC2 instance follows the rules of the older subnet
B. The EC2 instance follows the rules of both the subnets
C. Not possible, cannot be connected to 2 ENIs
D. The EC2 instance follows the rules of the newer subnet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS allows you create an elastic network interface (ENI), attach an ENI to an EC2 instance, detach an ENI from an EC2 instance and attach this ENI to another EC2 instance. The attributes of a network traffic follow the ENI which is attached to an EC2 instance or detached from an EC2 instance. When you move an ENI from one EC2 instance to another, network traffic is redirected to the new EC2 instance. You can create and attach additional ENIs to an EC2 instance.
Attaching multiple network interfaces (ENIs) to an EC2 instance is useful to:
Create a management network.
Use network and security appliances in your VPC.
Create dual-homed instances with workloads/roles on distinct subnets
Create alow-budget, high-availability solution.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 758
Which one of the below doesn't affect Amazon CloudFront billing?

A. Distribution Type
B. Data Transfer Out
C. Dedicated IP SSL Certificates
D. Requests

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudFront is a web service for content delivery. CloudFront delivers your content using a global network of edge locations and works seamlessly with Amazon S3 which durably stores the original and definitive versions of your files.
Amazon CloudFront billing is mainly affected by:
Data Transfer Out
Edge Location Traffic Distribution
Requests
Dedicated IP SSL Certificates
Reference: http://calculator.s3.amazonaws.com/index.html

QUESTION 759
A user is trying to launch a similar EC2 instance from an existing instance with the option "Launch More like this". The AMI of the selected instance is deleted. What will happen in this case?

A. AWS does not need an AMI for the "Launch more like this" option
B. AWS will launch the instance but will not create a new AMI
C. AWS will create a new AMI and launch the instance
D. AWS will throw an error saying that the AMI is deregistered

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If the user has deregistered the AMI of an EC2 instance and is trying to launch a similar instance with the option "Launch more like this", AWS will throw an error saying that the AMI is deregistered or not available.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html

QUESTION 760
Your company has multiple IT departments, each with their own VPC. Some VPCs are located within the same AWS account, and others in a different AWS account. You want to peer together all VPCs to enable the IT departments to have full access to each other's' resources. There are certain limitations placed on VPC peering. Which of the following statements is incorrect in relation to VPC peering?

A. Private DNS values cannot be resolved between instances in peered VPCs.
B. You can have up to 3 VPC peering connections between the same two VPCs at the same time.
C. You cannot create a VPC peering connection between VPCs in different regions.
D. You have a limit on the number active and pending VPC peering connections that you can have per VPC.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To create a VPC peering connection with another VPC, you need to be aware of the following limitations and rules:
You cannot create a VPC peering connection between VPCs that have matching or overlapping CIDR blocks.
You cannot create a VPC peering connection between VPCs in different regions. You have a limit on the number active and pending VPC peering connections that you can have per VPC. VPC peering does not support transitive peering relationships; in a VPC peering connection, your VPC will not have access to any other VPCs that the peer VPC may be peered with. This includes VPC peering connections that are established entirely within your own AWS account. You cannot have more than one VPC peering connection between the same two VPCs at the same time. The Maximum Transmission Unit (MTU) across a VPC peering connection is 1500 bytes. A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs.
Unicast reverse path forwarding in VPC peering connections is not supported. You cannot reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group. Instead, reference CIDR blocks of the peer VPC as the source or destination of your security group's ingress or egress rules.
Private DNS values cannot be resolved between instances in peered VPCs.
Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpcpeering-overview.html#vpc-peering-limitations

QUESTION 761
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. All data stored on Glacier is protected with AES-256 serverside encryption.
B. All data stored on Glacier is protected with AES-128 serverside encryption.
C. The user can set the serverside encryption flag to encrypt the data stored on Glacier.
D. The data stored on Glacier is not encrypted by default.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 762
You are architecting a highly-scalable and reliable web application which will have a huge amount of content. You have decided to use Cloudfront as you know it will speed up distribution of your static and dynamic web content and know that Amazon CloudFront integrates with Amazon CloudWatch metrics so that you can monitor your web application. Because you live in Sydney you have chosen the the Asia Pacific (Sydney) region in the AWS console. However, you have set up this up but no CloudFront metrics seem to be appearing in the CloudWatch console. What is the most likely reason from the possible choices below for this?

A. Metrics for CloudWatch are available only when you choose the same region as the application you are monitoring.
B. You need to pay for CloudWatch for it to become active.
C. Metrics for CloudWatch are available only when you choose the US East (N. Virginia)
D. Metrics for CloudWatch are not available for the Asia Pacific region as yet.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudFront is a global service, and metrics are available only when you choose the US East (N. Virginia) region in the AWS console. If you choose another region, no CloudFront metrics will appear in the CloudWatch console.
Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/monitoring-using-cloudwatch.html

QUESTION 763
A friend wants you to set up a small BitTorrent storage area for him on Amazon S3. You tell him it is highly unlikely that AWS would allow such a thing in their infrastructure. However, you decide to investigate. Which of the following statements best describes using BitTorrent with Amazon S3?

A. Amazon S3 does not support the BitTorrent protocol because it is used for pirated software.

B. You can use the BitTorrent protocol but only for objects that are less than 100 GB in size.
C. You can use the BitTorrent protocol but you need to ask AWS for specific permissions first.
D. You can use the BitTorrent protocol but only for objects that are less than 5 GB in size.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
BitTorrent is an open, peer-to-peer protocol for distributing files. You can use the BitTorrent protocol to retrieve any publicly-accessible object in Amazon S3.
Amazon S3 supports the BitTorrent protocol so that developers can save costs when distributing content at high scale. Amazon S3 is useful for simple, reliable storage of any data. The default distribution mechanism for Amazon S3 data is via client/server download. In client/server distribution, the entire object is transferred point-to-point from Amazon S3 to every authorized user who requests that object. While client/server delivery is appropriate for a wide variety of use cases, it is not optimal for everybody. Specifically, the costs of client/server distribution increase linearly as the number of users downloading objects increases. This can make it expensive to distribute popular objects. BitTorrent addresses this problem by recruiting the very clients that are downloading the object as distributors themselves: Each client downloads some pieces of the object from Amazon S3 and some from other clients, while simultaneously uploading pieces of the same object to other interested "peers." The benefit for publishers is that for large, popular files the amount of data actually supplied by Amazon S3 can be substantially lower than what it would have been serving the same clients via client/server download. Less data transferred means lower costs for the publisher of the object.
Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/S3Torrent.html

QUESTION 764
After a major security breach your manager has requested a report of all users and their credentials in AWS. You discover that in IAM you can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, MFA devices, and signing certificates. Which following statement is incorrect in regards to the use of credential reports?

A. Credential reports are downloaded XML files.
B. You can get a credential report using the AWS Management Console, the AWS CLI, or the IAM API.
C. You can use the report to audit the effects of credential lifecycle requirements, such as password rotation.
D. You can generate a credential report as often as once every four hours.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To access your AWS account resources, users must have credentials.
You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, MFA devices, and signing certificates. You can get a credential report using the AWS Management Console, the AWS CLI, or the IAM API. You can use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password rotation. You can provide the report to an external auditor, or grant permissions to an auditor so that he or she can download the report directly.
You can generate a credential report as often as once every four hours. When you request a report, IAM first checks whether a report for the account has been generated within the past four hours. If so, the most recent report is downloaded. If the most recent report for the account is more than four hours old, or if there are no previous reports for the account, IAM generates and downloads a new report. Credential reports are downloaded as comma-separated values (CSV) files. You can open CSV files with common spreadsheet software to perform analysis, or you can build an application that consumes the CSV files programmatically and performs custom analysis.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/credential-reports.html

QUESTION 765
In the most recent company meeting, your CEO focused on the fact that everyone in the organization needs to make sure that all of the infrastructure that is built is truly scalable. Which of the following statements is incorrect in reference to scalable architecture?

A. A scalable service is capable of handling heterogeneity.
B. A scalable service is resilient.
C. A scalable architecture won't be cost effective as it grows.
D. Increasing resources results in a proportional increase in performance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS it is critical to build a scalable architecture in order to take advantage of a scalable infrastructure. The cloud is designed to provide conceptually infinite scalability. However, you cannot leverage all that scalability in infrastructure if your architecture is not scalable. Both have to work together. You will have to identify the monolithic components and bottlenecks in your architecture, identify the areas where you cannot leverage the on-demand provisioning capabilities in your architecture, and work to refactor your application, in order to leverage the scalable infrastructure and take advantage of the cloud.
Characteristics of a truly scalable application:
Increasing resources results in a proportional increase in performance
A scalable service is capable of handling heterogeneity
A scalable service is operationally efficient
A scalable service is resilient
A scalable service should become more cost effective when it grows (Cost per unit reduces as the number of units increases)
Reference: http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf

QUESTION 766
A user has defined an AutoScaling termination policy to first delete the instance with the nearest billing hour. AutoScaling has launched 3 instances in the US-East-1A region and 2 instances in the US-East-1B region. One of the instances in the US-East-1B region is running nearest to the billing hour.
Which instance will AutoScaling terminate first while executing the termination action?

A. Random Instance from US-East-1A
B. Instance with the nearest billing hour in US-East-1B
C. Instance with the nearest billing hour in US-East-1A
D. Random instance from US-East-1B

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Even though the user has configured the termination policy, before AutoScaling selects an instance to terminate, it first identifies the Availability Zone that has more instances than the other Availability Zones used by the group. Within the selected Availability Zone, it identifies the instance that matches the specified termination policy.

Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/us-termination-policy.html

QUESTION 767
A user has configured a website and launched it using the Apache web server on port 80. The user is using ELB with the EC2 instances for Load Balancing. What should the user do to ensure that the EC2 instances accept requests only from ELB?

A. Configure the security group of EC2, which allows access to the ELB source security group
B. Configure the EC2 instance so that it only listens on the ELB port
C. Open the port for an ELB static IP in the EC2 security group
D. Configure the security group of EC2, which allows access only to the ELB listener

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When a user is configuring ELB and registering the EC2 instances with it, ELB will create a source security group. If the user wants to allow traffic only from ELB, he should remove all the rules set for the other requests and open the port only for the ELB source security group.
Reference: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/using-elb-security-groups.html

QUESTION 768
A user is planning a highly available application deployment with EC2. Which of the below mentioned options will not help to achieve HA?

A. Elastic IP address
B. PIOPS
C. AMI
D. Availability Zones

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Web Service, the user can achieve HA by deploying instances in multiple zones. The elastic IP helps the user achieve HA when one of the instances is down but still keeps the same URL. The AMI helps launching the new instance. The PIOPS is for the performance of EBS and does not help for HA.
Reference: http://media.amazonwebservices.com/AWS_Web_Hosting_Best_Practices.pdf

QUESTION 769
You are playing around with setting up stacks using JSON templates in CloudFormation to try and understand them a little better. You have set up about 5 or 6 but now start to wonder if you are being charged for these stacks. What is AWS's billing policy regarding stack resources?

A. You are not charged for the stack resources if they are not taking any traffic.
B. You are charged for the stack resources for the time they were operating (even if you deleted the stack right away)
C. You are charged for the stack resources for the time they were operating (but not if you deleted the stack within 60 minutes)

D. You are charged for the stack resources for the time they were operating (but not if you deleted the stack within 30 minutes)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A stack is a collection of AWS resources that you can manage as a single unit. In other words, you can create, update, or delete a collection of resources by creating, updating, or deleting stacks. All the resources in a stack are defined by the stack's AWS CloudFormation template. A stack, for instance, can include all the resources required to run a web application, such as a web server, a database, and networking rules. If you no longer require that web application, you can simply delete the stack, and all of its related resources are deleted.
You are charged for the stack resources for the time they were operating (even if you deleted the stack right away).
Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacks.html

QUESTION 770
You have been given a scope to set up an AWS Media Sharing Framework for a new start up photo sharing company similar to flick. The first thing that comes to mind about this is that it will obviously need a huge amount of persistent data storage for this framework. Which of the following storage options would be appropriate for persistent storage?

A. Amazon Glacier or Amazon S3
B. Amazon Glacier or AWS Import/Export
C. AWS Import/Export or Amazon CloudFront
D. Amazon EBS volumes or Amazon S3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Persistent storage--If you need persistent virtual disk storage similar to a physical disk drive for files or other data that must persist longer than the lifetime of a single Amazon EC2 instance, Amazon EBS volumes or Amazon S3 are more appropriate.
Reference: http://media.amazonwebservices.com/AWS_Storage_Options.pdf

QUESTION 771
After deploying a new website for a client on AWS, he asks if you can set it up so that if it fails it can be automatically redirected to a backup website that he has stored on a dedicated server elsewhere. You are wondering whether Amazon Route 53 can do this.
Which statement below is correct in regards to Amazon Route 53?

A. Amazon Route 53 can't help detect an outage. You need to use another service.
B. Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations.
C. Amazon Route 53 can help detect an outage of your website but can't redirect your end users to alternate locations.
D. Amazon Route 53 can't help detect an outage of your website, but can redirect your end users to alternate locations.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:
With DNS Failover, Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations where your application is operating properly.
Reference:
http://aws.amazon.com/about-aws/whats-new/2013/02/11/announcing-dns-failover-for-route-53/

QUESTION 772
In Route 53, what does a Hosted Zone refer to?

A. A hosted zone is a collection of geographical load balancing rules for Route 53.
B. A hosted zone is a collection of resource record sets hosted by Route 53.
C. A hosted zone is a selection of specific resource record sets hosted by CloudFront for distribution to Route 53.
D. A hosted zone is the Edge Location that hosts the Route 53 records for a user.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Hosted Zone refers to a selection of resource record sets hosted by Route 53.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHostedZones.html

QUESTION 773
Which of the following statements is true of Amazon EC2 security groups?

A. You can change the outbound rules for EC2-Classic. Also, you can add and remove rules to a group at any time.
B. You can modify an existing rule in a group. However, you can't add and remove rules to a group.
C. None of the statements are correct.
D. You can't change the outbound rules for EC2-Classic. However, you can add and remove rules to a group at any time.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When dealing with security groups, bear in mind that you can freely add and remove rules from a group, but you can't change the outbound rules for EC2-Classic. If you're using the Amazon EC2 console, you can modify existing rules, and you can copy the rules from an existing security group to a new security group.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 774
While creating a network in the VPC, which of the following is true of a NAT device?

A. You have to administer the NAT Gateway Service provided by AWS.
B. You can choose to use any of the three kinds of NAT devices offered by AWS for special purposes.
C. You can use a NAT device to enable instances in a private subnet to connect to the Internet.
D. You are recommended to use AWS NAT instances over NAT gateways, as the instances provide better availability and bandwidth.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use a NAT device to enable instances in a private subnet to connect to the Internet (for example, for software updates) or other AWS services, but prevent the Internet from initiating connections with the instances. AWS offers two kinds of NAT devices? A NAT gateway or a NAT instance. We recommend NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI. You can choose to use a NAT instance for special purposes.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat.html

QUESTION 775
You need to create a management network using network interfaces for a virtual private cloud (VPC) network. Which of the following statements is incorrect pertaining to Best Practices for Configuring Network Interfaces.

A. You can detach secondary (ethN) network interfaces when the instance is running or stopped. However, you can't detach the primary (eth0) interface.
B. Launching an instance with multiple network interfaces automatically configures interfaces, private IP addresses, and route tables on the operating system of the instance.
C. You can attach a network interface in one subnet to an instance in another subnet in the same VPC, however, both the network interface and the instance must reside in the same Availability Zone.
D. Attaching another network interface to an instance is a valid method to increase or double the network bandwidth to or from the dual-homed instance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Best Practices for Configuring Network Interfaces
You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).
You can detach secondary (ethN) network interfaces when the instance is running or stopped. However, you can't detach the primary (eth0) interface.
You can attach a network interface in one subnet to an instance in another subnet in the same VPC, however, both the network interface and the instance must reside in the same Availability Zone. When launching an instance from the CLI or API, you can specify the network interfaces to attach to the instance for both the primary (eth0) and additional network interfaces. Launching an instance with multiple network interfaces automatically configures interfaces, private IP addresses, and route tables on the operating system of the instance. A warm or hot attach of an additional network interface may require you to manually bring up the second interface, configure the private IP address, and modify the route table accordingly. (Instances running Amazon Linux automatically recognize the warm or hot attach and configure themselves.)
Attaching another network interface to an instance is not a method to increase or double the network bandwidth to or from the dual-homed instance.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#use-network-and-security-appliances-in-your-vpc

QUESTION 776

All Amazon EC2 instances are assigned two IP addresses at launch. Which are those?

A. 2 Elastic IP addresses
B. A private IP address and an Elastic IP address
C. A public IP address and an Elastic IP address
D. A private IP address and a public IP address

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon EC2-Classic every instance is given two IP Addresses: a private IP address and a public IP address
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#differences

QUESTION 777
Your manager has asked you to set up a public subnet with instances that can send and receive Internet traffic, and a private subnet that can't receive traffic directly from the internet, but can initiate traffic to the Internet (and receive responses) through a NAT instance in the public subnet. Hence, the following 3 rules need to be allowed:
Inbound SSH traffic.
Web servers in the public subnet to read and write to MS SQL servers in the private subnet.
Inbound RDP traffic from the Microsoft Terminal Services gateway in the public private subnet.
What are the respective ports that need to be opened for this?

A. Ports 22,1433,3389
B. Ports 21,1433,3389
C. Ports 25,1433,3389
D. Ports 22,1343,3999

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A network access control list (ACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
The following ports are recommended by AWS for a single subnet with instances that can receive and send Internet traffic and a private subnet that can't receive traffic directly from the Internet.
However, it can initiate traffic to the Internet (and receive responses) through a NAT instance in the public subnet.
Inbound SSH traffic. Port 22Web servers in the public subnet to read and write to MS SQL servers in the private subnet. Port 1433 Inbound RDP traffic from the Microsoft Terminal Services gateway in the public private subnet. Port 3389.
Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_NACLs.html#VPC_Appendi x_NACLs_Scenario_2

QUESTION 778

You want to establish a dedicated network connection from your premises to AWS in order to save money by transferring data directly to AWS rather than through your internet service provider. You are sure there must be some other benefits beyond cost savings. Which of the following would not be considered a benefit if you were to establish such a connection?

A. Elasticity
B. Compatibility with all AWS services.
C. Private connectivity to your Amazon VPC.
D. Everything listed is a benefit.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS.
Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.
You could expect the following benefits if you use AWS Direct Connect:
Reduced bandwidth costs
Consistent network performance
Compatibility with all AWS services
Private connectivity to your Amazon VPC
Elasticity
Simplicity
Reference: http://aws.amazon.com/directconnect/

QUESTION 779
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 volume limit
B. The AMI is missing. It is the required part
C. The snapshot is corrupt
D. The user account has reached the maximum EC2 instance limit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 `Instance Limit Exceeded' 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.

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

QUESTION 780
Can I change the EC2 security groups after an instance is launched in EC2-Classic?

A. Yes, you can change security groups after you launch an instance in EC2-Classic.
B. No, you cannot change security groups after you launch an instance in EC2-Classic.
C. Yes, you can only when you remove rules from a security group.
D. Yes, you can only when you add rules to a security group.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
After you launch an instance in EC2-Classic, you can't change its security groups. However, you can add rules to or remove rules from a security group, and those changes are automatically applied to all instances that are associated with the security group.
Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/usingnetwork-security.html

QUESTION 781
You can seamlessly join an EC2 instance to your directory domain. What connectivity do you need to be able to connect remotely to this instance?

A. You must have IP connectivity to the instance from the network you are connecting from.
B. You must have the correct encryption keys to connect to the instance remotely.
C. You must have enough bandwidth to connect to the instance.
D. You must use MFA authentication to be able to connect to the instance remotely.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can seamlessly join an EC2 instance to your directory domain when the instance is launched using the Amazon EC2 Simple Systems Manager. If you need to manually join an EC2 instance to your domain, you must launch the instance in the proper region and security group or subnet, then join the instance to the domain. To be able to connect remotely to these instances, you must have IP connectivity to the instances from the network you are connecting from. In most cases, this requires that an Internet gateway be attached to your VPC and that the instance has a public IP address.
Reference:
http://docs.aws.amazon.com/directoryservice/latest/admin-guide/join_a_directory.html

QUESTION 782
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. All the instances of George and Ray can communicate over a private IP with a minimal cost

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

QUESTION 783
You are in the process of moving your friend's WordPress site onto AWS to try and save him some money, and you have told him that he should probably also move his domain name. He asks why he can't leave his domain name where it is and just have his infrastructure on AWS.
What would be an incorrect response to his question?

A. Route 53 offers low query latency for your end users.
B. Route 53 is designed to automatically answer queries from the optimal location depending on network conditions.
C. The globally distributed nature of AWS's DNS servers helps ensure a consistent ability to route your end users to your application.
D. Route 53 supports Domain Name System Security Extensions (DNSSEC).

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services.
Route 53 is built using AWS's highly available and reliable infrastructure. The globally distributed nature of our DNS servers helps ensure a consistent ability to route your end users to your application by circumventing any Internet or network related issues. Route 53 is designed to provide the level of dependability required by important applications. Using a global anycast network of DNS servers around the world, Route 53 is designed to automatically answer queries from the optimal location depending on network conditions. As a result, the service offers low query latency for your end users. Amazon Route 53 does not support Domain Name System Security Extensions (DNSSEC) at this time.
Reference: https://aws.amazon.com/route53/faqs/

QUESTION 784
Can you encrypt EBS volumes?

A. Yes, you can enable encryption when you create a new EBS volume using the AWS Management Console, API, or CLI.
B. No, you should use a third-party software to perform raw block-level encryption of an EBS volume.

C. Yes, but you must use a third-party API for encrypting data before it's loaded on EBS.
D. Yes, you can encrypt with the special "ebs_encrypt" command through Amazon APIs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With Amazon EBS encryption, you can now create an encrypted EBS volume and attach it to a supported instance type. Data on the volume, disk I/O, and snapshots created from the volume are then all encrypted. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. EBS encryption is based on the industry standard AES-256 cryptographic algorithm.
To get started, simply enable encryption when you create a new EBS volume using the AWS Management Console, API, or CLI. Amazon EBS encryption is available for all the latest EC2 instances in all commercially available AWS regions.
Reference: https://aws.amazon.com/about-aws/whats-new/2014/05/21/Amazon-EBS-encryption-now-available/

QUESTION 785
In Amazon EC2, you are billed instance-hours when _____.

A. your EC2 instance is in a running state
B. the instance exits from Amazon S3 console
C. your instance still exits the EC2 console
D. EC2 instances stop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You are billed instance-hours as long as your EC2 instance is in a running state.
Reference: http://aws.amazon.com/ec2/faqs/

QUESTION 786
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 auto registration Off
D. ELB connection draining

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 in-flight requests continue to be served.
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/config-conn-drain.html

QUESTION 787
A user is running a webserver on EC2. The user wants to receive the SMS when the EC2 instance utilization is above the threshold limit. Which AWS services should the user configure in this case?

A. AWS CloudWatch + AWS SQS.
B. AWS CloudWatch + AWS SNS.
C. AWS CloudWatch + AWS SES.
D. AWS EC2 + AWS Cloudwatch.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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. In this case, the user can configure that Cloudwatch sends an alarm on when the threshold is crossed to SNS which will trigger an SMS.
Reference: http://aws.amazon.com/sns/

QUESTION 788
Just when you thought you knew every possible storage option on AWS you hear someone mention Reduced Redundancy Storage (RRS) within Amazon S3. What is the ideal scenario to use Reduced Redundancy Storage (RRS)?

A. Huge volumes of data
B. Sensitve data
C. Non-critical or reproducible data
D. Critical data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reduced Redundancy Storage (RRS) is a new storage option within Amazon S3 that enables customers to reduce their costs by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. RRS provides a lower cost, less durable, highly available storage option that is designed to sustain the loss of data in a single facility.
RRS is ideal for non-critical or reproducible data.
For example, RRS is a cost-effective solution for sharing media content that is durably stored elsewhere. RRS also makes sense if you are storing thumbnails and other

resized images that can be easily reproduced from an original image.
Reference: https://aws.amazon.com/s3/faqs/

QUESTION 789
A user is making a scalable web application with compartmentalization. The user wants the log module to be able to be accessed by all the application functionalities in an asynchronous way.
Each module of the application sends data to the log module, and based on the resource availability it will process the logs.
Which AWS service helps this functionality?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Simple Queue Service (SQS) is a highly reliable distributed messaging system for storing messages as they travel between computers. By using Amazon SQS, developers can simply move data between distributed application components. It is used to achieve compartmentalization or loose coupling. In this case all the modules will send a message to the logger queue and the data will be processed by queue as per the resource availability.
Reference:
http://media.amazonwebservices.com/AWS_Building_Fault_Tolerant_Applications.pdf

QUESTION 790
You have some very sensitive data stored on AWS S3 and want to try every possible alternative to keeping it secure in regards to access control. What are the mechanisms available for access control on AWS S3?

A. (IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication.
B. (IAM) policies, Access Control Lists (ACLs) and bucket policies.
C. Access Control Lists (ACLs), bucket policies, and query string authentication
D. (IAM) policies, Access Control Lists (ACLs), bucket policies, query string authentication and encryption.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon S3 supports several mechanisms that give you flexibility to control who can access your data as well as how, when, and where they can access it.
Amazon S3 provides four different access control mechanisms:
AWS Identity and Access Management (IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication.
IAM enables organizations to create and manage multiple users under a single AWS account. With IAM policies, you can grant IAM users fine-grained control to your Amazon S3 bucket or objects. You can use ACLs to selectively add (grant) certain permissions on individual objects. Amazon S3 bucket policies can be used to add or deny permissions across some or all of the objects within a single bucket.

With Query string authentication, you have the ability to share Amazon S3 objects through URLs that are valid for a specified period of time.

QUESTION 791
Your manager has come to you saying that he is very confused about the bills he is receiving from AWS as he is getting different bills for every user and needs you to look into making it more understandable. Which of the following would be the best solution to meet his request?

A. AWS Billing Aggregation
B. Consolidated Billing
C. Deferred Billing
D. Aggregated Billing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Consolidated Billing enables you to consolidate payment for multiple AWS accounts within your company by designating a single paying account. Consolidated Billing enables you to see a combined view of AWS costs incurred by all accounts, as well as obtain a detailed cost report for each of the individual AWS accounts associated with your "Paying Account". Consolidated Billing is offered at no additional charge.
Reference: https://aws.amazon.com/billing/faqs/

QUESTION 792
A user is planning to host a mobile game on EC2 which sends notifications to active users on either high score or the addition of new features. The user should get this notification when he is online on his mobile device. Which of the below mentioned AWS services can help achieve this functionality?

A. AWS Simple Notification Service.
B. AWS Simple Email Service.
C. AWS Mobile Communication Service.
D. AWS Simple Queue Service.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, and 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

QUESTION 793
Which one of the following can't be used as an origin server with Amazon CloudFront?

A. A web server running in your infrastructure
B. Amazon S3

C. Amazon Glacier
D. A web server running on Amazon EC2 instances

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudFront is designed to work with Amazon S3 as your origin server, customers can also use Amazon CloudFront with origin servers running on Amazon EC2 instances or with any other custom origin.
Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web.html

QUESTION 794
You have written a CloudFormation template that creates 1 Elastic Load Balancer fronting 2 EC2 Instances. Which section of the template should you edit so that the DNS of the load balancer is returned upon creation of the stack?

A. Resources
B. Outputs
C. Parameters
D. Mappings

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use AWS CloudFormation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application.
Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/outputs-section-structure.html

QUESTION 795
You have been asked to set up a database in AWS that will require frequent and granular updates. You know that you will require a reasonable amount of storage space but are not sure of the best option. What is the recommended storage option when you run a database on an instance with the above criteria?

A. Amazon S3
B. Amazon EBS
C. AWS Storage Gateway
D. Amazon Glacier

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Amazon EBS provides durable, block-level storage volumes that you can attach to a running Amazon EC2 instance. You can use Amazon EBS as a primary storage device for data that requires frequent and granular updates. For example, Amazon EBS is the recommended storage option when you run a database on an instance.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 796
You have been asked to set up monitoring of your network and you have decided that Cloudwatch would be the best service to use. 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. Which of the following items listed can AWS Cloudwatch monitor?

A. Log files your applications generate.
B. All of the items listed on this page.
C. System-wide visibility into resource utilization, application performance, and operational health.
D. Custom metrics generated by your applications and services.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.
Reference: http://aws.amazon.com/cloudwatch/

QUESTION 797
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. 1 hour
B. 30 minutes
C. 5 minutes
D. 2 hours

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 in-flight requests continue to be served. The user can specify a maximum time of 3600 seconds (1 hour) 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.
Reference:

http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/config-conn-drain.html

QUESTION 798
How can you apply more than 100 rules to an Amazon EC2-Classic?

A. By adding more security groups
B. You need to create a default security group specifying your required rules if you need to use more than 100 rules per security group.
C. By default the Amazon EC2 security groups support 500 rules.
D. You can't add more than 100 rules to security groups for an Amazon EC2 instance.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 100 rules to a security group.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 799
You need to quickly set up an email-sending service because a client needs to start using it in the next hour. Amazon Simple Email Service (Amazon SES) seems to be the logical choice but there are several options available to set it up. Which of the following options to set up SES would best meet the needs of the client?

A. Amazon SES console
B. AWS CloudFormation
C. SMTP Interface
D. AWS Elastic Beanstalk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon SES is an outbound-only email-sending service that provides an easy, cost-effective way for you to send email.
There are several ways that you can send an email by using Amazon SES. You can use the Amazon SES console, the Simple Mail Transfer Protocol (SMTP) interface, or you can call the Amazon SES API. Amazon SES console--This method is the quickest way to set up your system
Reference: http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html

QUESTION 800
Identify a true statement about the On-Demand instances purchasing option provided by Amazon EC2.

A. Pay for the instances that you use by the hour, with no long-term commitments or up-front payments.
B. Make a low, one-time, up-front payment for an instance, reserve it for a one-or three-year term, and pay a significantly lower hourly rate for these instances.
C. Pay for the instances that you use by the hour, with long-term commitments or up-front payments.
D. Make a high, one-time, all-front payment for an instance, reserve it for a one-or three-year term, and pay a significantly higher hourly rate for these instances.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
On-Demand instances allow you to pay for the instances that you use by the hour, with no long-term commitments or up-front payments.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-offerings.html

QUESTION 801
Which of the following statements is NOT true about using Elastic IP Address (EIP) in EC2-Classic and EC2-VPC platforms?

A. In the EC2-VPC platform, the Elastic IP Address (EIP) does not remain associated with the instance when you stop it.
B. In the EC2-Classic platform, stopping the instance disassociates the Elastic IP Address (EIP) from it.
C. In the EC2-VPC platform, if you have attached a second network interface to an instance, when you disassociate the Elastic IP Address (EIP) from that instance, a new public IP address is not assigned to the instance automatically; you'll have to associate an EIP with it manually.
D. In the EC2-Classic platform, if you disassociate an Elastic IP Address (EIP) from the instance, the instance is automatically assigned a new public IP address within a few minutes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the EC2-Classic platform, when you associate an Elastic IP Address (EIP) with an instance, the instance's current public IP address is released to the EC2-Classic public IP address pool. If you disassociate an EIP from the instance, the instance is automatically assigned a new public IP address within a few minutes. In addition, stopping the instance also disassociates the EIP from it. But in the EC2-VPC platform, when you associate an EIP with an instance in a default Virtual Private Cloud (VPC), or an instance in which you assigned a public IP to the eth0 network interface during launch, its current public IP address is released to the EC2-VPC public IP address pool. If you disassociate an EIP from the instance, the instance is automatically assigned a new public IP address within a few minutes. However, if you have attached a second network interface to the instance, the instance is not automatically assigned a new public IP address; you'll have to associate an EIP with it manually. The EIP remains associated with the instance when you stop it.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

QUESTION 802
You have a Business support plan with AWS. One of your EC2 instances is running Microsoft Windows Server 2008 R2 and you are having problems with the software. Can you receive support from AWS for this software?

A. Yes
B. No, AWS does not support any third-party software.
C. No, Microsoft Windows Server 2008 R2 is not supported.
D. No, you need to be on the enterprise support plan.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Third-party software support is available only to AWS Support customers enrolled for Business or Enterprise Support. Third-party support applies only to software running on Amazon EC2 and does not extend to assisting with on-premises software. An exception to this is a VPN tunnel configuration running supported devices for Amazon VPC.
Reference:
https://aws.amazon.com/premiumsupport/features/

QUESTION 803
In Amazon EC2, how many Elastic IP addresses can you have by default?

A. 10
B. 2
C. 5
D. 20

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The number of Elastic IP addresses you can have in EC2 is 5.
Reference:
http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

QUESTION 804
After deciding that EMR will be useful in analyzing vast amounts of data for a gaming website that you are architecting you have just deployed an Amazon EMR Cluster and wish to monitor the cluster performance. Which of the following tools cannot be used to monitor the cluster performance?

A. Kinesis
B. Ganglia
C. CloudWatch Metrics
D. Hadoop Web Interfaces

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EMR provides several tools to monitor the performance of your cluster.
Hadoop Web Interfaces
Every cluster publishes a set of web interfaces on the master node that contain information about the cluster. You can access these web pages by using an SSH tunnel to connect them on the master node. For more information, see View Web Interfaces Hosted on Amazon EMR Clusters.

CloudWatch Metrics
Every cluster reports metrics to CloudWatch. CloudWatch is a web service that tracks metrics, and which you can use to set alarms on those metrics. For more information, see Monitor Metrics with CloudWatch.
Ganglia
Ganglia is a cluster monitoring tool. To have this available, you have to install Ganglia on the cluster when you launch it. After you've done so, you can monitor the cluster as it runs by using an SSH tunnel to connect to the Ganglia UI running on the master node. For more information, see Monitor Performance with Ganglia.
Reference: http://docs.aws.amazon.com/ElasticMapReduce/latest/DeveloperGuide/emr-troubleshoot-tools.html

QUESTION 805
A user has launched one EC2 instance in the US West region. The user wants to access the RDS instance launched in the US East region from that EC2 instance. How can the user configure the access for that EC2 instance?

A. Configure the IP range of the US West region instance as the ingress security rule of RDS
B. It is not possible to access RDS of the US East region from the US West region
C. Open the security group of the US West region in the RDS security group's ingress rule
D. Create an IAM role which has access to RDS and launch an instance in the US West region with it

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user cannot authorize an Amazon EC2 security group if it is in a different AWS Region than the RDS DB instance. The user can authorize an IP range or specify an Amazon EC2 security group in the same region that refers to an IP address in another region.
Reference:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithSecurityGroups.html

QUESTION 806
You need to create a load balancer in a VPC network that you are building. You can make your load balancer internal (private) or internet-facing (public). When you make your load balancer internal, a DNS name will be created, and it will contain the private IP address of the load balancer. An internal load balancer is not exposed to the internet. When you make your load balancer internet-facing, a DNS name will be created with the public IP address. If you want the Internet-facing load balancer to be connected to the Internet, where must this load balancer reside?

A. The load balancer must reside in a subnet that is connected to the internet using the Internet gateway.
B. The load balancer must reside in a subnet that is not connected to the Internet.
C. The load balancer must not reside in a subnet that is connected to the Internet.
D. The load balancer must be completely outside of your VPC.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you create an internal Elastic Load Balancer in a VPC, you need to select private subnets that are in the same Availability Zone as your instances. If the VPC Elastic Load Balancer is to be public facing, you need to create the Elastic Load Balancer in a public subnet. A subnet is a public subnet if it is attached to an Internet

Gateway (IGW) with a defined route to that gateway.
Selecting more than one public subnet increases the availability of your Elastic Load Balancer. NB-Elastic Load Balancers in EC2-Classic are always Internet-facing load balancers.
Reference: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-internet-facing-load-balancers.html

QUESTION 807
Can you move a Reserved Instance from one Availability Zone to another?

A. Yes, but each Reserved Instance is associated with a specific Region that cannot be changed.
B. Yes, only in US-West-2.
C. Yes, only in US-East-1.
D. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each Reserved Instance is associated with a specific Region, which is fixed for the lifetime of the reservation and cannot be changed. Each reservation can, however, be used in any of the available AZs within the associated Region.
Reference: https://aws.amazon.com/rds/faqs/

QUESTION 808
An application hosted at the EC2 instance receives an HTTP request from ELB. The same request has an X-Forwarded-For header, which has three IP addresses. Which system's IP will be a part of this header?

A. Previous Request IP address.
B. Client IP address.
C. All of the answers listed here.
D. Load Balancer IP address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When a user sends a request to ELB over HTTP/HTTPS, the request header log at the instance will only receive the IP of ELB. This is because ELB is the interceptor between the EC2 instance and the client request. To get the client IP, use the header X-Forwarded-For in header. The client IP address in the X-Forwarded-For request header is followed by the IP addresses of each successive proxy that passes along the request. The last IP address is the IP address thatconnects to the back-end application instance. e.g. if the HTTP request already has a header when it reaches the Load Balancer, the IP address from which the request came is appended at the end of the header followed by the IP address of the Load Balancer. In such cases, the X-Forwarded-For request header takes the following form:
X-Forwarded-For: clientIPAddress, previousRequestIPAddress, LoadBalancerIPAddress.
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/TerminologyandKeyConcepts.html

QUESTION 809
You need to develop and run some new applications on AWS and you know that Elastic Beanstalk and CloudFormation can both help as a deployment mechanism for a broad range of AWS resources. Which of the following statements best describes the differences between Elastic Beanstalk and CloudFormation?

A. Elastic Beanstalk uses Elastic load balancing and CloudFormation doesn't.
B. CloudFormation is faster in deploying applications than Elastic Beanstalk.
C. Elastic Beanstalk is faster in deploying applications than CloudFormation.
D. CloudFormation is much more powerful than Elastic Beanstalk, because you can actually design and script custom resources

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
These services are designed to complement each other. AWS Elastic Beanstalk provides an environment to easily develop and run applications in the cloud. It is integrated with developer tools and provides a one-stop experience for you to manage the lifecycle of your applications.
AWS CloudFormation is a convenient deployment mechanism for a broad range of AWS resources. It supports the infrastructure needs of many different types of applications such as existing enterprise applications, legacy applications, applications built using a variety of AWS resources and container-based solutions (including those built using AWS Elastic Beanstalk).
AWS CloudFormation introduces two new concepts: The template, a JSON-format, text-based file that describes all the AWS resources you need to deploy to run your application and the stack, the set of AWS resources that are created and managed as a single unit when AWS CloudFormation instantiates a template.
Reference: http://aws.amazon.com/cloudformation/faqs/

QUESTION 810
You need to set up a security certificate for a client's e-commerce website as it will use the HTTPS protocol. Which of the below AWS services do you need to access to manage your SSL server certificate?

A. AWS Directory Service
B. AWS Identity & Access Management
C. AWS CloudFormation
D. Amazon Route 53

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS.All your SSL server certificates are managed by AWS Identity and Access management (IAM).
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/ManagingServerCerts.html

QUESTION 811
When controlling access to Amazon EC2 resources, each Amazon EBS Snapshot has a _____ attribute that controls which AWS accounts can use the snapshot.

A. createVolumePermission
B. LaunchPermission
C. SharePermission
D. RequestPermission

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each Amazon EBS Snapshot has a createVolumePermission attribute that you can set to one or more AWS Account IDs to share the AMI with those AWS Accounts. To allow several AWS Accounts to use a particular EBS snapshot, you can use the snapshots's createVolumePermission attribute to include a list of the accounts that can use it.
Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM.html

QUESTION 812
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In a hardware security module (HSM), Transparent Data Encryption (TDE) reduces the risk of confidential data theft by encrypting sensitive data.
http://docs.aws.amazon.com/cloudhsm/latest/userguide/cloud-hsm-third-party-apps.html

QUESTION 813
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.)
http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

QUESTION 814
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf

QUESTION 815
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

QUESTION 816
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
https://aws.amazon.com/cloudhsm/faqs/

QUESTION 817
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/IAM/latest/UserGuide/GenerateMFAConfig.html

QUESTION 818
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

Correct Answer: A

Section: (none)
Explanation

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

QUESTION 819
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html

QUESTION 820
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Statement element, of an IAM policy, contains an array of individual statements. Each individual statement is a JSON block enclosed in braces { }.
http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

QUESTION 821
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_identity-management.html #intro-identity-users

QUESTION 822
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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 823
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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
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

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

QUESTION 824
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://aws.amazon.com/rds/faqs/#53

QUESTION 825
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/codecommit/latest/userguide/encryption.html

QUESTION 826
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/kms/latest/developerguide/crypto-intro.html

QUESTION 827
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)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

QUESTION 828
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html

QUESTION 829
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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": "Allow",
"Resource": "*",
"Condition": {
"StringEquals": {
"ec2:ResourceTag/InstanceType": "Production"
}
}
}
]
```

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

QUESTION 830
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html

QUESTION 831
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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 832
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 833
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.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-template.html

QUESTION 834
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesLoggingOnOff

QUESTION 835
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.DBEngine.SQLServer.html

QUESTION 836
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Cognito supports developer authenticated identities, in addition to web identity federation through Facebook, Google, and Amazon.
http://docs.aws.amazon.com/cognito/devguide/identity/developer-authenticated-identities/

QUESTION 837
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 838
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 839
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 840
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In IAM the AWS Account is the role with most important permissions. It's equivalent to the root account in a UNIX environment.
http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html

QUESTION 841
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/kms/latest/developerguide/crypto_overview.html

QUESTION 842
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 843
Company has three AWS accounts. They have created separate IAM users within each account.
Company wants a single IAM login URL such as https://company.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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Users can create an alias for they accounts, but the alias should be unique to the account. For example, the alias "company" 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.

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

QUESTION 844
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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)
http://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html

QUESTION 845
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf

QUESTION 846
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/IAM/latest/UserGuide/HowToPwdIAMUser.html

QUESTION 847
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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
http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/control-access-billing.html

QUESTION 848
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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).

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

QUESTION 849
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 850
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon IAM, a user can belong to up to 10 different groups.

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

QUESTION 851
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 852
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

QUESTION 853
Company (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/

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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/.

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

QUESTION 854
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 855
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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).

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#vpc-security-groups

QUESTION 856
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://awsdocs.s3.amazonaws.com/RDS/2011-04-01/rds-ug-2011-04-01.pdf

QUESTION 857
The information within an IAM policy is described through a series of _____.

A. elements
B. macros
C. classes
D. namespaces

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 858
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html

QUESTION 859
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 860
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 861
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 policy is in effect.

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

QUESTION 862
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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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).

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html

QUESTION 863
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 864
A user is creating multiple IAM users and want to place them in IAM groups. What advice should be given to him to enhance the security?

A. Only grant relevant privileges to the IAM groups and assign IAM users to those groups.
B. Grant all higher privileges to the IAM group
C. Grant less privileges for user, but higher privileges for the group
D. Grant more privileges to the user, but least privileges to the group

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.). Next, define the relevant permissions for each group. Finally, assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group. That way, you can make changes for everyone in a group in just one place. As people move around in your company, you can simply change what IAM group their IAM user belongs to.

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

QUESTION 865
Does Amazon CloudFront work well for delivery of static objects that are frequently accessed?

A. Yes, it does, and your objects can be served more quickly than if they were served from one of Amazon S3 central locations.
B. No, it does not as your static objects that aren't accessed frequently remain in Amazon CloudFront edge locations' caches.
C. No, delivery out of Amazon S3 (rather than from Amazon CloudFront) may be a better choice for more popular objects.
D. Yes, it does, but your objects will be served slower than if they were served from one of Amazon S3 central locations.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Amazon CloudFront works well for delivery of static objects that are frequently accessed? "popular" objects. With Amazon CloudFront, copies of your popular objects are cached in a network of edge locations around the world. Because these edge locations are close to your viewers, your objects can be served more quickly than if they were served from one of Amazon S3's central locations.

http://aws.amazon.com/cloudfront/details/

QUESTION 866
A user is planning a highly available application deployment with EC2. Which of the below mentioned options will not help to achieve HA?

A. Using an AMI
B. Deploying in multiple Availability Zones
C. Using an Elastic IP address
D. Using load balancing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Web Service, the user can achieve HA by deploying instances in multiple zones. The elastic IP helps the user achieve HA when one of the instances is down by still keeps the same URL. Load balancing helps with distribution of traffic across multiple availability zones. An AMI helps launch the instance, but aside from how the AMI is configured to best suite high availability, it does not affect the availability of the instance once it is launched.

https://d0.awsstatic.com/whitepapers/aws-web-hosting-best-practices.pdf

QUESTION 867
A user has configured a CloudWatch alarm to fire off when the CPU utilization metric goes over 50% with a time interval of 5 minutes for 10 consecutive periods. What will be the state of the alarm at the end of 30 minutes, if the CPU utilization is constant at 20%?

A. ALARM
B. OK
C. ALERT
D. INSUFFICIENT_DATA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 868

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 overwrites the instance termination attribute and terminates the instances
B. Auto Scaling will notify the user for the next action
C. The EC2 instance will not be terminated since instance protection from scale-in is enabled.
D. Auto Scaling will remove the instance from the Auto Scaling Group

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 869
A custom NAT instance that performs source/destination checks by default is launched in a VPC's public subnet. All security, NACL, and routing definitions are configured as expected. A custom NAT instance is launched.
Which of the following must be done for the custom NAT instance to work?

A. The NAT instance should be launched in a private subnet.
B. The source/destination checks should be disabled on the NAT instance.
C. The NAT instance should be configured with a public IP address.
D. The NAT instance should be configured with an elastic IP address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 870
The AWS Trusted Advisor provides best practices (or checks) in four categories for no cost.
Which of the following choices is not a category practiced by the AWS Trusted Advisor?

A. Security
B. Performance improvement
C. Cost optimization
D. Compliance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The AWS Trusted Advisor provides best practices (or checks) in four categories:
- cost optimization
- security
- fault tolerance
- performance improvement.

https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/

QUESTION 871
Which of the following statements is true of using a network in Amazon CloudFront?

A. CloudFront loads static content from all edge locations.
B. CloudFront provides a capacity reservation for EC2 instances in an Availability Zone.
C. CloudFront caches content at edge locations for a specified period of time.
D. CloudFront detects unhealthy instances and stops sending traffic to them.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudFront caches content at edge locations for a period of time that you specify. When a visitor requests content that has been cached for longer than the expiration date, CloudFront checks the origin server to see if a newer version of the content is available.

http://docs.aws.amazon.com/gettingstarted/latest/swh/getting-started-create-cfdist.html

QUESTION 872
A user has created a mobile application on an EC2 instance 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 security method below does AWS recommend in this scenario?

A. The user should create a separate IAM user for each mobile application and provide DynamoDB access with it
B. Create an IAM Role with DynamoDB access and attach it with the mobile application
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. 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 873

An organization hosts an app on EC2 instances which multiple developers need access to in order to perform updates.
The organization plans to implement some security best practices related to instance access.
Which one of the following recommendations will not help improve its security in this way?

A. Create a procedure to revoke the access rights of the individual user when they are not required to connect to EC2 instance anymore for the purpose of application configuration.
B. Create an IAM policy allowing only IAM users to connect to the EC2 instances with their own SSH key.
C. Apply the latest patch of OS and always keep it updated.
D. Disable the password based login for all the users. All the users should use their own keys to connect with the instance securely.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since AWS is a public cloud any application hosted on EC2 is prone to hacker attacks. It becomes extremely important for a user to setup a proper security mechanism on the EC2 instances. A few of the security measures are listed below:

- Always keep the OS updated with the latest patch
- Always create separate users with in OS if they need to connect with the EC2 instances, create their keys and disable their password
- Create a procedure using which the admin can revoke the access of the user when the business work on the EC2 instance is completed.

Lock down unnecessary ports.
Audit any proprietary applications that the user may be running on the EC2 instance. Provide temporary escalated privileges, such as sudo for users who need to perform occasional privileged tasks IAM is useful when users are required to work with AWS resources and actions, such as launching an instance. It is not useful in this case because it does not manage who can connect via RDP or SSH with an instance.

http://aws.amazon.com/articles/1233/

QUESTION 874
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. ERROR
B. THRESHOLD
C. ALERT
D. OK

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveoperGuide/AlarmThatSendsEmail.html

QUESTION 875
Identify the custom termination policy, supported by Auto Scaling, that selects the instance for termination with the least time to the next billing hour?

A. ClosestToNextInstanceHour
B. NewestInstance
C. Default
D. OldestLaunchConfiguration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the ClosestToNextInstanceHour custom termination policy, Auto Scaling terminates instances that are closest to the next billing hour.
This policy helps you maximize the use of your instances and manage costs.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingBehavior.InstanceTermination.html

QUESTION 876
An EC2 instance has one additional EBS volume attached to it. How can a user attach the same volume to another running instance in the same AZ?

A. Detach the volume first and attach to new instance
B. Attach the volume as read only to the second instance
C. Terminate the first instance and only then attach to the new instance
D. No need to detach. Just select the volume and attach it to the new instance, it will take care of mapping internally

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If an EBS volume is attached to a running EC2 instance, the user needs to detach the volume from the original instance and then attach it to a new running instance.
The user doesn't need to stop / terminate the original instance.

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

QUESTION 877
An instance running a webserver is launched in a VPC subnet. A security group and a custom NACL are configured to allow inbound port 80.
What else should be done to make the web server allow all inbound and outbound HTTP traffic?

A. Outbound Port 80 rule should be enabled on the custom NACL.

B. The new instance should be terminated and relaunched.
C. Inbound port 1433 rule should be enabled on security groups.
D. The NAT instance should be configured with a public IP address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa (security groups are therefore stateful). Access Control Lists, on the other hand, are stateless, and must have outbound rules configured explicitly. While NACLs automatically created with a new VPC allow all inbound and outbound traffic by default, custom NACLs denies all inbound and outbound traffic by default.

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

QUESTION 878
A user has configured the Dev/Test environment with AWS and created the IAM users with EC2, AS, ELB, and CloudWatch access. The CFO wants to save money on Dev/Test and terminate all the idle instances. Which of the following is the best possible solution for the user to terminate the idle instances?

A. Launch all the instances with the IAM Role and activate CloudWatch to automatically terminate the idle instances.
B. Use Cloud Watch Alarms actions to automatically terminate the idle instances.
C. Use AS to automatically call the CloudWatch alarm when idle instances are encountered.
D. Provide the user using the AWS account with EC2DescribeInstanceRecoveryAttribute access for idle instances to terminate automatically.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your Amazon Elastic Compute Cloud (Amazon EC2) instances.
You can use the stop or terminate actions to help you save money when you no longer need an instance to be running.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html

QUESTION 879
In Amazon CloudFront, after you've created your distribution, does CloudFront know the location of your Amazon S3 origin server?

A. No, you must configure your CloudFront to address your Amazon S3 origin server.
B. No, you should configure your Amazon S3 origin manually to be connected to your CloudFront.
C. Yes, only if you have mentioned it in the template JSON file.
D. Yes

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 880
Someone is setting up a website with AWS services. She is configuring various security measures to be performed on the Amazon EC2 instances. Which security mechanisms below will help her avoid future data leaks and identify security vulnerabilities?

A. Perform SQL injection for application testing.
B. Run penetration testing on AWS with prior approval from Amazon.
C. Perform a hardening test on the instance.
D. All of the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS security follows the shared security model where the user is as much responsible as Amazon. Since Amazon is a public cloud it is bound to be targeted by hackers. If an organization is planning to host their application on Amazon EC2, they should perform the below mentioned security checks as a measure to find any security weakness/data leaks:
Perform penetration testing as performed by attackers to find any vulnerability. The organization must take an approval from AWS before performing penetration testing Perform hardening testing to find if there are any unnecessary ports open Perform SQL injection to find any DB security issues The code memory checks are generally useful when the organization wants to improve the application performance.

http://aws.amazon.com/security/penetration-testing/

QUESTION 881
A user has created an Auto Scaling group with default configurations from CLI. The user wants to configure CloudWatch alarm on the EC2 instances, which are launched by the Auto Scaling group. The user has created an alarm to monitor the CPU utilization every minute. Which of the below mentioned statements is true?

A. The alarm creation will fail since the user has not enabled detailed monitoring on the EC2 instances
B. The user has to first enable detailed monitoring on the EC2 instances to support alarm monitoring at every minute
C. 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
D. It will fetch the data every minute from EC2 instances regardless if detailed monitoring is enabled or not.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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. Auto Scaling does not need Detailed Monitoring for alarm creation on 1 min period. The Detailed Monitoring flag in launch config is for making metrics available on individual instances for 1 min period.

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

QUESTION 882
In Amazon CloudFront, to create signed URLs, an AWS account must have at least _____.

A. one active CloudFront Trusted Signer
B. one active CloudFront key pair
C. one active CloudFront administrator user
D. two CloudFront secret keys

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon CloudFront, to create signed URLs, an AWS account must have at least one active CloudFront key pair.

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html

QUESTION 883
A user is planning to host a website as well as an application on a single EC2 instance which is a part of the public subnet of a VPC. How can the user configure two separate public IPs, and separate security groups for both the application as well as the website?

A. Launch the host EC2 instance within a VPC with ELB such that it redirects requests to separate VPC instances of the public subnet.
B. Launch the host EC2 instance within a VPC with two separate subnets and make the instance a part of both the subnets.
C. Launch the host EC2 instance within a VPC with two network interfaces. Assign a separate security group to each and AWS will assign a separate public IP to them.
D. Launch the host EC2 instance with two network interfaces within a VPC. Assign a separate Security Group and Elastic IP (EIP) to each of the network interfaces.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you need to host multiple websites (with different IPs) on a single EC2 instance, the following is the suggested method from AWS.
Launch an EC2 instance with two network interfaces within a VPC. Assign elastic IPs from VPC EIP pool to those interfaces (Because, when the user has attached more than one network interface with an instance, AWS cannot assign public IPs to them.) Assign separate Security Groups if separate Security Groups are needed This scenario also helps for operating network appliances, such as firewalls or load balancers that have multiple private IP addresses for each network interface.

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

QUESTION 884
Which of the following AWS services is a good choice for transferring very large amounts of data (up to 16TBs) to Amazon S3?

A. AWS Multi-part upload
B. AWS Direct Import
C. AWS Import/Export
D. Amazon Storage Gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 885
If you enable Amazon CloudFront access logging, can you identify the requests that CloudFront rejected with an HTTP status code of 403?

A. Yes, CloudFront access logging enables you to identify the requests that CloudFront rejected using the HTTP status code (403).
B. No, CloudFront access logging cannot distinguish requests with HTTP status code of 403.
C. Yes, if you change the default setting of CloudFront access logging, it helps to identify the requests that CloudFront rejected using the HTTP status code (403).
D. No, CloudFront cannot log any HTTP status.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you enable Amazon CloudFront access logging, you can identify the requests that CloudFront rejected with an HTTP status code of 403. However, using only the access logs, you can't distinguish a request that CloudFront rejected based on the location of the user from a request that CloudFront rejected because the user didn't have permission to access the object for another reason.

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

QUESTION 886
You shut down a running DB instance on which you have been getting a discounted rate as a result of a reserved DB instance purchase and the term of the reserved DB instance has not yet expired. You launch another DB instance with the same specifications during the term. Which of the following is true for this scenario?

A. You will be paying only for the newly launched instance.
B. You will not be charged.
C. You will continue to get the discounted rate.
D. You will be not given the discounted rate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you shut down a running DB instance on which you have been getting a discounted rate as a result of a reserved DB instance purchase, and the term of the reserved DB instance has not yet expired, you will continue to get the discounted rate if you launch another DB instance with the same specifications during the term.

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithReservedDBInstances.html

QUESTION 887
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 cannot stop the alarm from performing an action unless the alarm is deleted.
B. The user can pause the alarm from the console.
C. The user can disable the alarm using the DisableAlarmActions API.
D. The user can set CloudWatch in a sleep state using the CLI mon-sleep-alarm-action.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html

QUESTION 888
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/monitor_estimated_charges_with_cloudwatch.html

QUESTION 889
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/importexport/

QUESTION 890
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 891
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 892
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION 893
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/autoscaling/latest/userguide/auto-scaling-benefits.html

QUESTION 894
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

QUESTION 895
By default, how many Elastic IP addresses can you have per region for your EC2 instances?

A. 10
B. 2
C. 20
D. 5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The number of Elastic IP addresses you can have in EC2 per region is 5.

http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

QUESTION 896
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.concepts.design.html

QUESTION 897
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html

QUESTION 898
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/autoscaling/

QUESTION 899
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.)

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

QUESTION 900
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security Groups in VPC allow you to specify rules for both outgoing and incoming traffic.

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

QUESTION 901
_____ 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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 902
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 903
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION 904
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/gs_monitor_estimated_charges_with_cloudwatch.html

QUESTION 905
What does enabling sticky sessions 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-sticky-sessions.html

QUESTION 906
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 907
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/autoscaling/latest/userguide/create-lc-with-instanceID.html

QUESTION 908

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html

QUESTION 909
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisIE.html

QUESTION 910
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.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
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).
http://aws.amazon.com/autoscaling/

QUESTION 911
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services.
http://aws.amazon.com/route53/faqs/

QUESTION 912
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 913

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/related_services.html

QUESTION 914
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 915
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

QUESTION 916
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html

QUESTION 917
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html#Metric

QUESTION 918
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

QUESTION 919
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 920
Security groups in VPC operate at the _____.

A. data transport layer level
B. subnet level
C. instance level
D. gateway level

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 921
Network ACLs are _____.

A. stateful
B. stateless
C. asynchronous
D. synchronous

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

QUESTION 922
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION 923
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Using the Cloudwatch Monitoring scripts for Linux, you can measure memory and disk usage of your Linux EC2 instances.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/mon-scripts.html

QUESTION 924
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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html#healthcheck

QUESTION 925
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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).

http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API_MetricDatum.html

QUESTION 926
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.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 927

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION 928
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
https://aws.amazon.com/rds/postgresql/

QUESTION 929
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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 930
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

QUESTION 931
Which of the following states is not possible for the CloudWatch alarm?

A. ALERT
B. ALARM
C. OK
D. INSUFFICIENT_DATA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html

QUESTION 932
What is the default maximum number of VPCs allowed per region?

A. 5
B. 15
C. 100
D. 10

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 933
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.html

QUESTION 934
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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 935
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Cloudwatch can be accessed from the Amazon CloudWatch Console, CloudWatch API, AWS CLI and AWS SDKs.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/accessing_cloudwatch.html

QUESTION 936
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html

QUESTION 937
Which of the following terms is NOT a key CloudWatch concept?

A. Namespaces
B. Units
C. Time Stamps
D. Indexes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION 938
Network ACLs in a VPC operate at the _____.

A. TCP level
B. instance level
C. subnet level
D. gateway level

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 939
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound traffic.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

QUESTION 940
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 941
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 942
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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
http://docs.aws.amazon.com/kinesis/latest/dev/monitoring_with_cloudwatch.html

QUESTION 943
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/graph_a_metric_all_resources.html

QUESTION 944
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 945
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
https://aws.amazon.com/ec2/faqs/

QUESTION 946
Which of the following statements is true of 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 AutoScaling group.
D. If the Auto Scaling infrastructure is being deleted, it is mandatory to delete the launch configuration.

Correct Answer: B

Section: (none)
Explanation

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

QUESTION 947
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you just specify the general endpoint (autoscaling.amazonaws.com), Auto Scaling directs your request to the us-east-1 endpoint.
http://docs.aws.amazon.com/general/latest/gr/rande.html

QUESTION 948
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 949
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

https://aws.amazon.com/cloudfront/

QUESTION 950
Elastic Load Balancing automatically distributes incoming traffic across multiple _____ instances.

A. EC2
B. RDS
C. M3
D. DB

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 951
_____ is a task coordination and state management service for cloud applications.

A. Amazon SWF
B. Amazon FPS

C. Amazon SES
D. Amazon SNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/swf/

QUESTION 952
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html

QUESTION 953
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.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
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.
https://aws.amazon.com/articles/5050

QUESTION 954
_____ is a fast, reliable, scalable, fully managed message queuing service.

A. AWS Data Pipeline
B. Amazon SES
C. Amazon SQS
D. Amazon SNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/sqs/

QUESTION 955
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/vpc/faqs/#G1

QUESTION 956
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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 957
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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 958
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

QUESTION 959
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/rds/faqs/#1

QUESTION 960
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingRRS.html

QUESTION 961
_____ is a fast, flexible, fully managed pub/sub messaging service.

A. Amazon SQS
B. Amazon SES
C. Amazon FPS
D. Amazon SNS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/sns/?nc1=h_l2_as

QUESTION 962
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can access and manage Amazon Web Services through a simple and intuitive web-based user interface known as the AWS Management Console.
http://aws.amazon.com/console/

QUESTION 963

What is the maximum size of an object in Amazon S3?

A. 4 TB
B. Unlimited
C. 5 TB
D. 500 MB

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/s3/faqs/#How_much_data_can_I_store

QUESTION 964
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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 965
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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 966
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 967
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/rds/multi-az/

QUESTION 968
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html#amazon-linux

QUESTION 969
_____ 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/mobile/sdkforandroid/developerguide/kinesis.html

QUESTION 970
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 971
Where is an object stored in Amazon S3?

A. in a Bucket
B. in a Collector
C. in an Archive
D. in a Vault

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Every object in Amazon S3 is stored in a bucket. Before you can store data in Amazon S3, you must create a bucket.
http://docs.aws.amazon.com/AmazonS3/latest/gsg/CreatingABucket.html

QUESTION 972
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

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

QUESTION 973
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 974
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are four general categories of time-flexible and interruption-tolerant tasks that work well with Spot Instances: Delay able tasks, Optional tasks, Tasks that can be sped up by adding additional computing power and at the end, Tasks that require a large number of compute instances that you can't access any other way.

http://aws.amazon.com/ec2/spot-instances/

QUESTION 975
What does Amazon EMR stand for?

A. Elastic Magnetic Resonance

B. Encrypted Machine Reads
C. Elastic MapReduce
D. Encrypted Machine Rendering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/ElasticMapReduce/latest/DeveloperGuide/emr-what-is-emr.html

QUESTION 976
What is the main use of EMR?

A. Data-sensitive storage
B. Encryption
C. Data-intensive processing tasks
D. authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
https://aws.amazon.com/elasticmapreduce/faqs/

QUESTION 977
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html

QUESTION 978
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-instance_linux.html

QUESTION 979
In regard to AWS CloudFormation, to pass values to your template at runtime you should use _____.

A. parameters
B. conditions
C. resources
D. mapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/concept-template.html

QUESTION 980
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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).
https://aws.amazon.com/workspaces/

QUESTION 981
What does AMI stand for?

A. Amazon Machine Image
B. Advanced Machine Instance
C. Amazon Micro Instance
D. Advanced Machine Image

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 982
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Using_Tags.html

QUESTION 983
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 autoresponders, email unsubscribe systems, and applications that generate customer support tickets from incoming emails.

http://aws.amazon.com/ses/

QUESTION 984
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
https://aws.amazon.com/blogs/aws/new-per-second-billing-for-ec2-instances-an-ebs-volumes/

QUESTION 985
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
http://aws.amazon.com/glacier/faqs/#How_do_vaults_work

QUESTION 986
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

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

QUESTION 987
Which of the following programming languages is not supported by Amazon's Elastic Beanstalk?

A. Ruby
B. Java
C. Node.js
D. Perl

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.platforms.html