

AWS Certified Solutions Architect - Associate

Number: Architect-Associate

Passing Score: 800

Time Limit: 120 min

File Version: 1

AWS Certified Solutions Architect - Associate

Exam A

QUESTION 1

A 3-tier e-commerce web application is currently 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 failover 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: 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. 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.

Benefits

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.

No Administrative Intervention

DB Instance failover is fully automatic and requires no administrative intervention. Amazon RDS monitors the health of your primary and standbys, and initiates a failover automatically in response to a variety of failure conditions.

Failover conditions

Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention. Amazon RDS automatically performs a failover in the event of any of the following:

- Loss of availability in primary Availability Zone
- Loss of network connectivity to primary
- Compute unit failure on primary
- Storage failure on primary

Note: When operations such as DB Instance scaling or system upgrades like OS patching are initiated for Multi-AZ deployments, for enhanced availability, they are applied first on the standby prior to an automatic failover.

As a result, your availability impact is limited only to the time required for automatic failover to complete. Note that Amazon RDS Multi-AZ deployments do not failover automatically in response to database operations such as long running queries, deadlocks or database corruption errors.

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:

Point-In-Time Recovery

In addition to the daily automated backup, Amazon RDS archives database change logs. This enables you to recover your database to any point in time during the backup retention period, up to the last five minutes of database usage.

Amazon RDS stores multiple copies of your data, but for Single-AZ DB instances these copies are stored in a single availability zone. If for any reason a Single-AZ DB instance becomes unusable, you can use point-in-time recovery to launch a new DB instance with the latest restorable data. For more information on working with point-in-time recovery, go to [Restoring a DB Instance to a Specified Time](#).

Note

Multi-AZ deployments store copies of your data in different Availability Zones for greater levels of data durability. For more information on Multi-AZ deployments, see [High Availability \(Multi-AZ\)](#).

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: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://aws.amazon.com/blogs/aws/category/amazon-elastic-map-reduce/>

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 DynamoDB 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:

Web Identity Federation

Imagine that you are creating a mobile app that accesses AWS resources, such as a game that runs on a mobile device and stores player and score information using Amazon S3 and DynamoDB.

When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using web identity federation. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app.

With web identity federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) —such as Login with Amazon, Facebook, Google, or any other [OpenID Connect \(OIDC\)](#)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account. Using an IdP helps you keep your AWS account secure, because you don't have to embed and distribute long-term security credentials with your application.

For most scenarios, we recommend that you use [Amazon Cognito](#) because it acts as an identity broker and does much of the federation work for you. For details, see the following section, [Using Amazon Cognito for Mobile Apps](#).

If you don't use Amazon Cognito, then you must write code that interacts with a web IdP (Login with Amazon, Facebook, Google, or any other OIDC-compatible IdP) and then calls the AssumeRoleWithWebIdentity API to trade the authentication token you get from those IdPs for AWS temporary security credentials. If you have already used this approach for existing apps, you can continue to use it.

Using Amazon Cognito for Mobile Apps

The preferred way to use web identity federation is to use [Amazon Cognito](#). For example, Adele the developer is building a game for a mobile device where user data such as scores and profiles is stored in Amazon S3 and Amazon DynamoDB. Adele could also store this data locally on the device and use Amazon Cognito to keep it synchronized across devices. She knows that for security and maintenance reasons, long-term AWS security credentials should not be distributed with the game. She also knows that the game might have a large number of users. For all of these reasons, she does not want to create new user identities in IAM for each player.

Instead, she builds the game so that users can sign in using an identity that they've already established with a

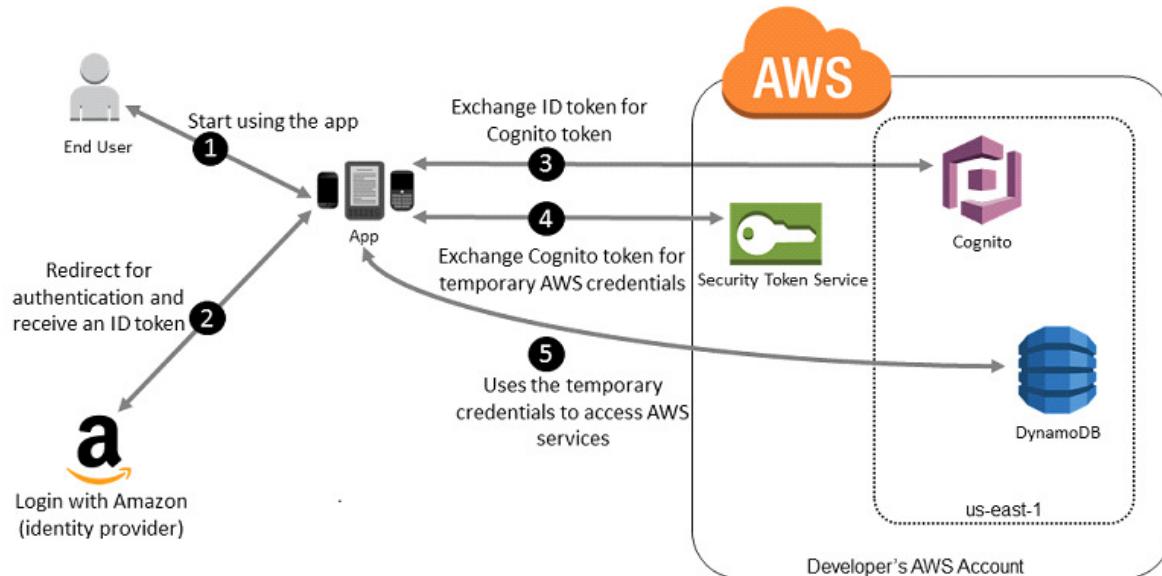
well-known identity provider, such as Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC)-compatible identity provider. Her game can take advantage of the authentication mechanism from one of these providers to validate the user's identity.

To enable the mobile app to access her AWS resources, Adele first registers for a developer ID with her chosen IdPs. She also configures the application with each of these providers. In her AWS account that contains the Amazon S3 bucket and DynamoDB table for the game, Adele uses Amazon Cognito to create IAM roles that precisely define permissions that the game needs. If she is using an OIDC IdP, she also creates an IAM OIDC identity provider entity to establish trust between her AWS account and the IdP.

In the app's code, Adele calls the sign-in interface for the IdP that she configured previously. The IdP handles all the details of letting the user sign in, and the app gets an OAuth access token or OIDC ID token from the provider. Adele's app can trade this authentication information for a set of temporary security credentials that consist of an AWS access key ID, a secret access key, and a session token. The app can then use these credentials to access web services offered by AWS. The app is limited to the permissions that are defined in the role that it assumes.

The following figure shows a simplified flow for how this might work, using Login with Amazon as the IdP. For Step 2, the app can also use Facebook, Google, or any OIDC-compatible identity provider, but that's not shown here.

Sample workflow using Amazon Cognito to federate users for a mobile application



A customer starts your app on a mobile device. The app asks the user to sign in.

The app uses Login with Amazon resources to accept the user's credentials.

The app uses Cognito APIs to exchange the Login with Amazon ID token for a Cognito token.

The app requests temporary security credentials from AWS STS, passing the Cognito token.

The temporary security credentials can be used by the app to access any AWS resources required by the app to operate. The role associated with the temporary security credentials and its assigned policies determines what can be accessed.

Use the following process to configure your app to use Amazon Cognito to authenticate users and give your app access to AWS resources. For specific steps to accomplish this scenario, consult the documentation for Amazon Cognito.

(Optional) Sign up as a developer with Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible identity provider and configure one or more apps with the provider. This step is optional because Amazon Cognito also supports unauthenticated (guest) access for your users.

Go to [Amazon Cognito in the AWS Management Console](#). Use the Amazon Cognito wizard to create an identity pool, which is a container that Amazon Cognito uses to keep end user identities organized for your apps. You can share identity pools between apps. When you set up an identity pool, Amazon Cognito creates one or two IAM roles (one for authenticated identities, and one for unauthenticated "guest" identities) that define permissions for Amazon Cognito users.

Download and integrate the [AWS SDK for iOS](#) or the [AWS SDK for Android](#) with your app, and import the files required to use Amazon Cognito.

Create an instance of the Amazon Cognito credentials provider, passing the identity pool ID, your AWS account number, and the Amazon Resource Name (ARN) of the roles that you associated with the identity pool. The

Amazon Cognito wizard in the AWS Management Console provides sample code to help you get started. When your app accesses an AWS resource, pass the credentials provider instance to the client object, which passes temporary security credentials to the client. The permissions for the credentials are based on the role or roles that you defined earlier.

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 (SQS) 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:

Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. By using Amazon SQS, developers can simply move data between distributed application components performing different tasks, without losing messages or requiring each component to be always available. Amazon SQS makes it easy to build a distributed, decoupled application, working in close conjunction with the Amazon Elastic Compute Cloud (Amazon EC2) and the other AWS infrastructure web services.

What can I do with Amazon SQS?

Amazon SQS is a web service that gives you access to a message queue that can be used to store messages while waiting for a computer to process them. This allows you to quickly build message queuing applications that can be run on any computer on the internet. Since Amazon SQS is highly scalable and you only pay for what you use, you can start small and grow your application as you wish, with no compromise on performance or reliability. This lets you focus on building sophisticated message-based applications, without worrying about how the messages are stored and managed. You can use Amazon SQS with software applications in various ways. For example, you can:

Integrate Amazon SQS with other AWS infrastructure web services to make applications more reliable and flexible.

Use Amazon SQS to create a queue of work where each message is a task that needs to be completed by a process. One or many computers can read tasks from the queue and perform them.

Build a microservices architecture, using queues to connect your microservices.

Keep notifications of significant events in a business process in an Amazon SQS queue. Each event can have a corresponding message in a queue, and applications that need to be aware of the event can read and process the messages.

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 0 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:

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 SQL 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 for each customer with a Bucket Policy that permits access only to that one customer.

Correct Answer: C

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.

QUESTION 12

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 c3.8xlarge instance in us-east-1. 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.
- B. 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.
- C. Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Provision 3x1TB 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.
- D. 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. E. Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Configure synchronous, block-level replication to an identically configured instance in us-east-1b.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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. IAM Roles

- C. Elastic IP Addresses (EIP)
- D. EC2 Key Pairs
- E. Launch configurations
- F. Security Groups

Correct Answer: AC

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 in each AZ inside an Auto Scaling Group behind an ELB 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.

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 of 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 without having 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:

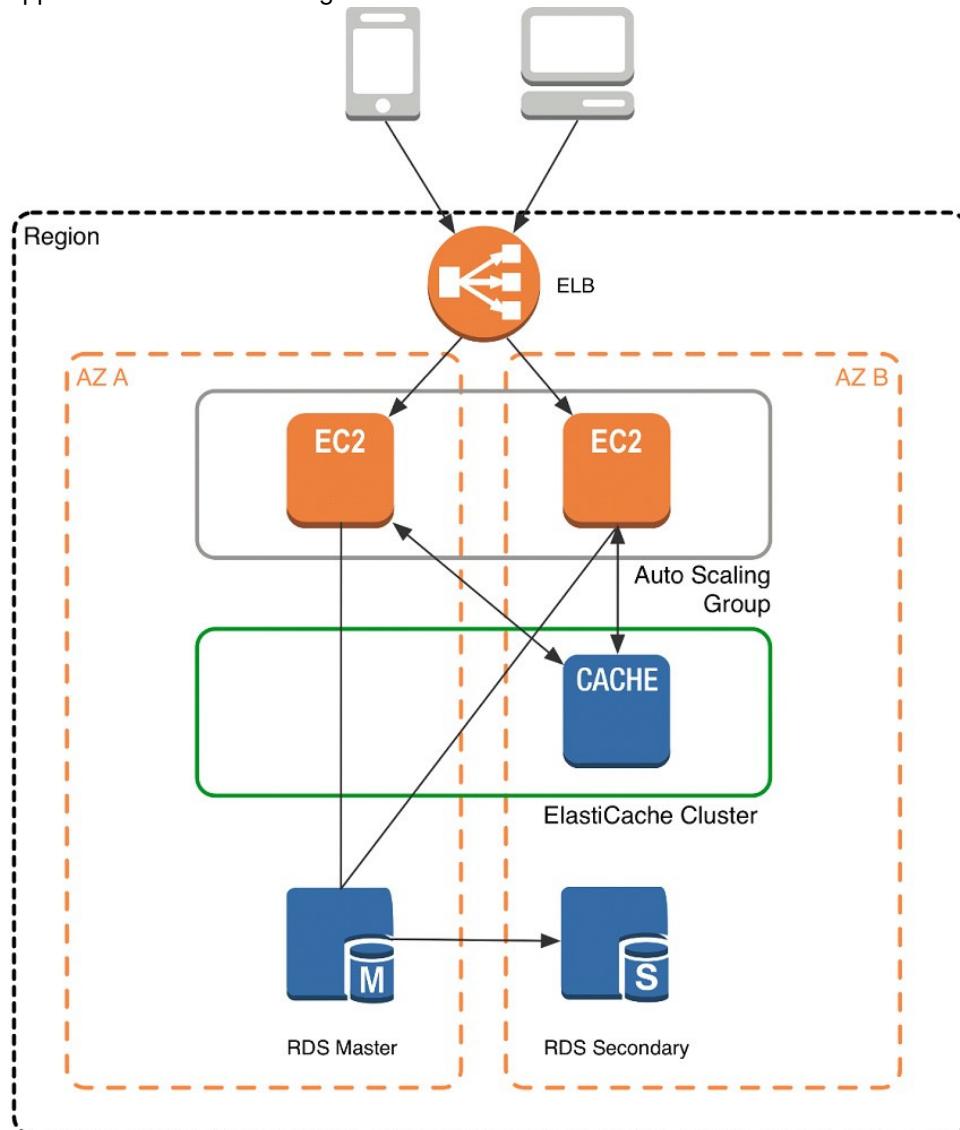
ElasticCache for Memcached

The primary goal of caching is typically to offload reads from your database or other primary data source. In most apps, you have hot spots of data that are regularly queried, but only updated periodically. Think of the front page of a blog or news site, or the top 100 leaderboard in an online game. In this type of case, your app can receive dozens, hundreds, or even thousands of requests for the same data before it's updated again. Having your caching layer handle these queries has several advantages. First, it's considerably cheaper to add an in-memory cache than to scale up to a larger database cluster. Second, an in-memory cache is also easier to scale out, because it's easier to distribute an in-memory cache horizontally than a relational database. Last, a caching layer provides a request buffer in the event of a sudden spike in usage. If your app or game ends up on the front page of Reddit or the App Store, it's not unheard of to see a spike that is 10 to 100 times your normal application load. Even if you autoscale your application instances, a 10x request spike will likely make your database very unhappy.

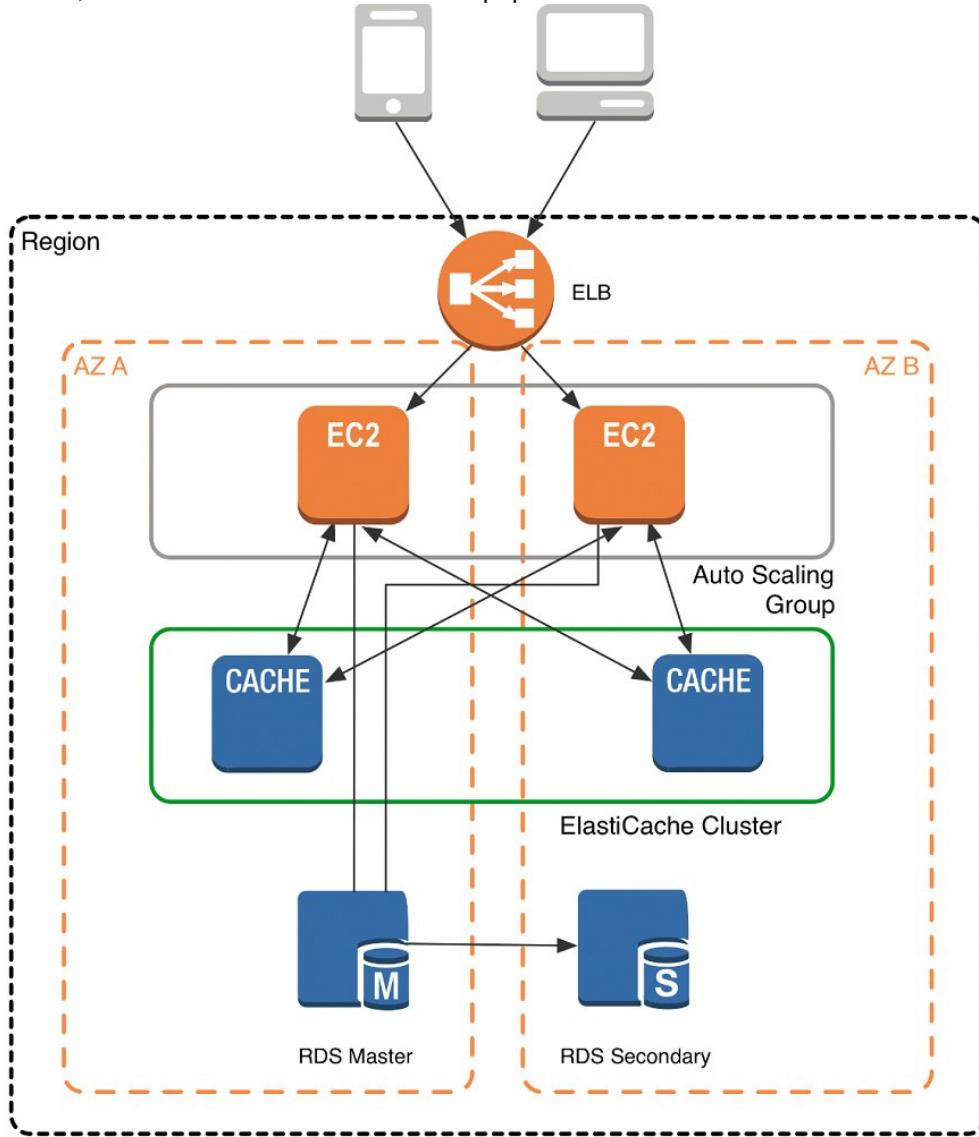
Let's focus on ElastiCache for Memcached first, because it is the best fit for a caching focused solution. We'll revisit Redis later in the paper, and weigh its advantages and disadvantages.

Architecture with ElastiCache for Memcached

When you deploy an ElastiCache Memcached cluster, it sits in your application as a separate tier alongside your database. As mentioned previously, Amazon ElastiCache does not directly communicate with your database tier, or indeed have any particular knowledge of your database. A simplified deployment for a web application looks something like this:

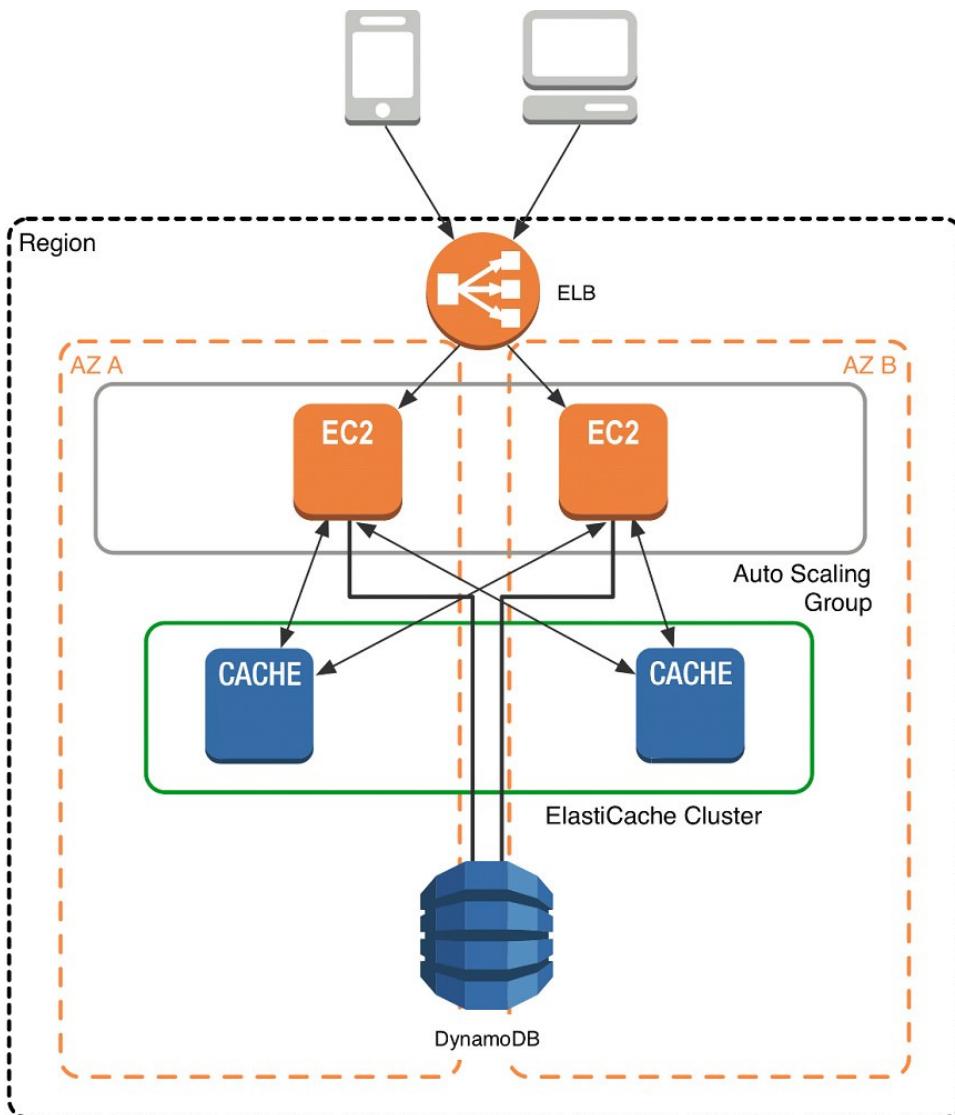


In this architecture diagram, the Amazon EC2 application instances are in an Auto Scaling group, located behind a load balancer using Elastic Load Balancing, which distributes requests among the instances. As requests come into a given EC2 instance, that EC2 instance is responsible for communicating with ElastiCache and the database tier. For development purposes, you can begin with a single ElastiCache node to test your application, and then scale to additional cluster nodes by modifying the ElastiCache cluster. As you add additional cache nodes, the EC2 application instances are able to distribute cache keys across multiple ElastiCache nodes. The most common practice is to use client-side sharding to distribute keys across cache nodes, which we will discuss later in this paper.



When you launch an ElastiCache cluster, you can choose the Availability Zone(s) that the cluster lives in. For best performance, you should configure your cluster to use the same Availability Zones as your application servers. To launch an ElastiCache cluster in a specific Availability Zone, make sure to specify the Preferred Zone(s) option during cache cluster creation. The Availability Zones that you specify will be where ElastiCache will launch your cache nodes. We recommend that you select Spread Nodes Across Zones, which tells ElastiCache to distribute cache nodes across these zones as evenly as possible. This distribution will mitigate the impact of an Availability Zone disruption on your ElastiCache nodes. The trade-off is that some of the requests from your application to ElastiCache will go to a node in a different Availability Zone, meaning latency will be slightly higher. For more details, refer to Creating a Cache Cluster in the Amazon ElastiCache User Guide.

As mentioned at the outset, ElastiCache can be coupled with a wide variety of databases. Here is an example architecture that uses Amazon DynamoDB instead of Amazon RDS and MySQL:



This combination of DynamoDB and ElastiCache is very popular with mobile and game companies, because DynamoDB allows for higher write throughput at lower cost than traditional relational databases. In addition, DynamoDB uses a key-value access pattern similar to ElastiCache, which also simplifies the programming model. Instead of using relational SQL for the primary database but then key-value patterns for the cache, both the primary database and cache can be programmed similarly. In this architecture pattern, DynamoDB remains the source of truth for data, but application reads are offloaded to ElastiCache for a speed boost.

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 the 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 the 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 each Ante into an SQS queue in the second region; use an auto-scaling group behind the SQS queue to replay the writes in the second region.

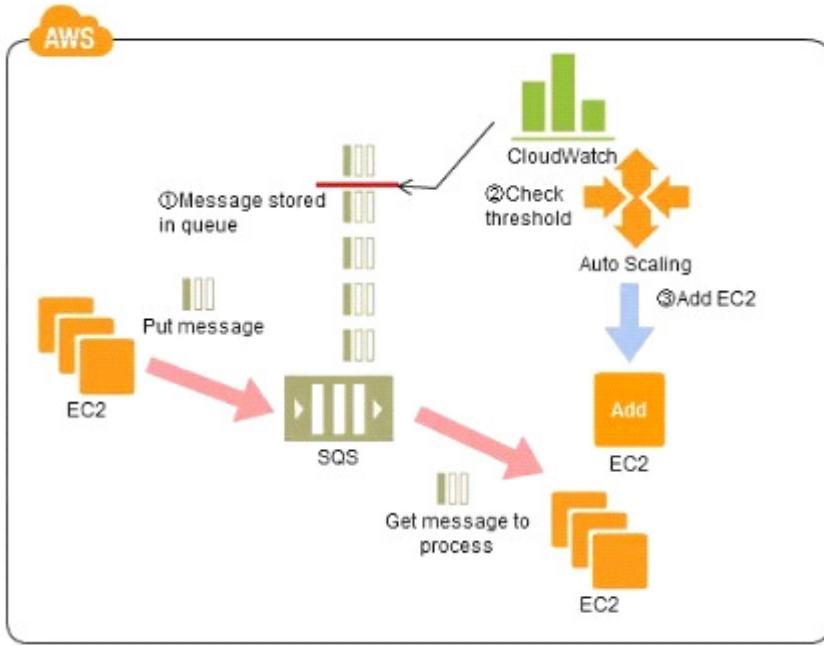
Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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 time 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.

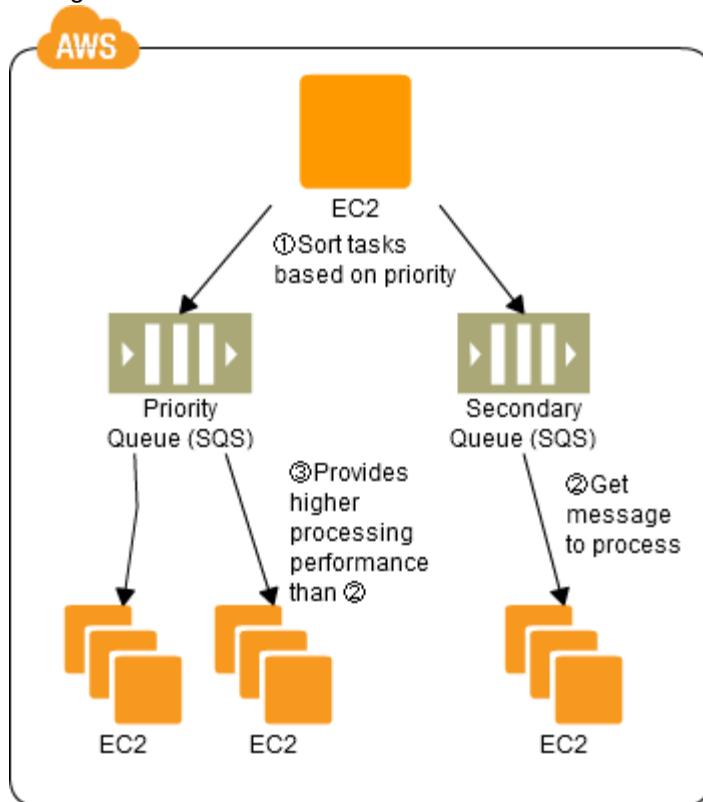
Use SQS to prepare multiple queues for the individual priority levels.

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 RDS 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 for 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

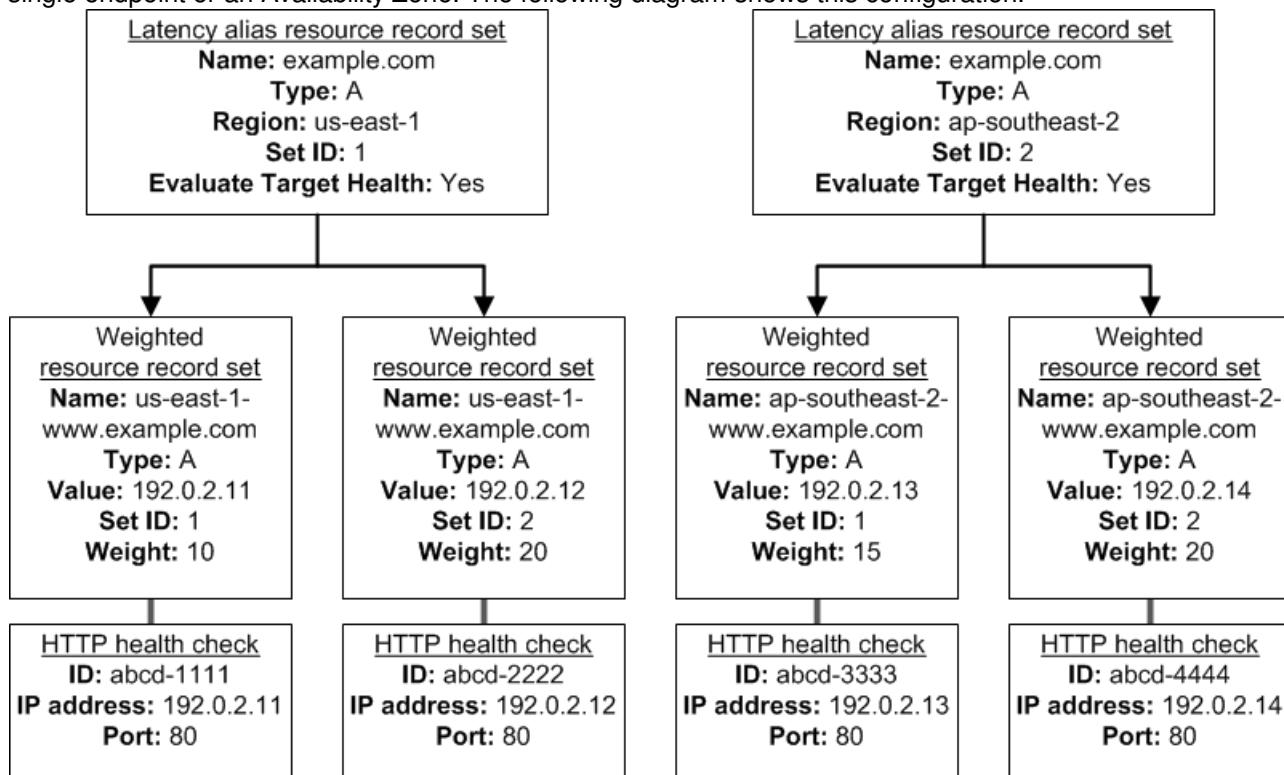
Explanation/Reference:

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.)

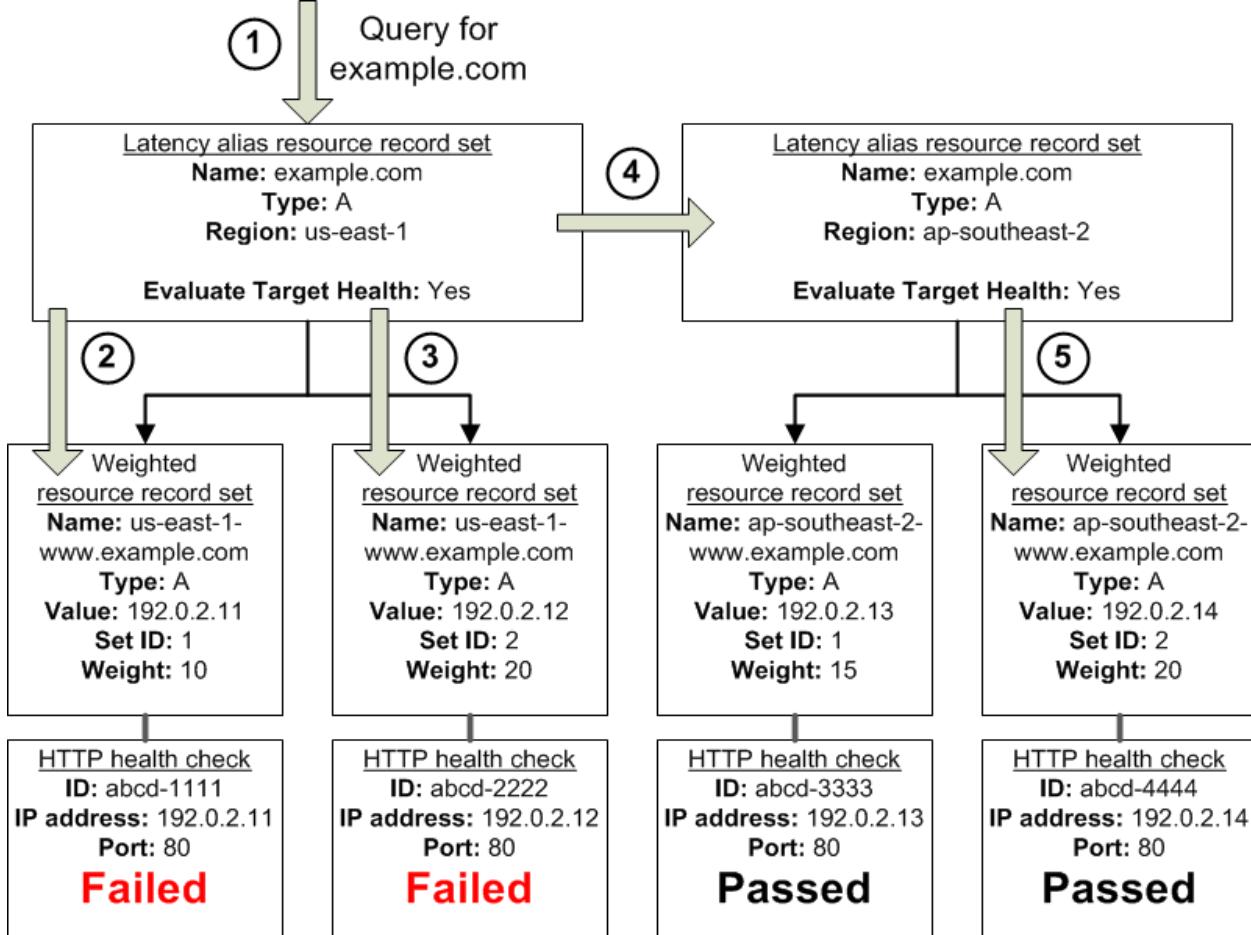
Within each region, you have two Amazon EC2 instances. You create a weighted resource record set for each instance. The name and the type are the same for both of the weighted resource record sets in each region. When you have multiple resources in a region, you can create weighted or failover resource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

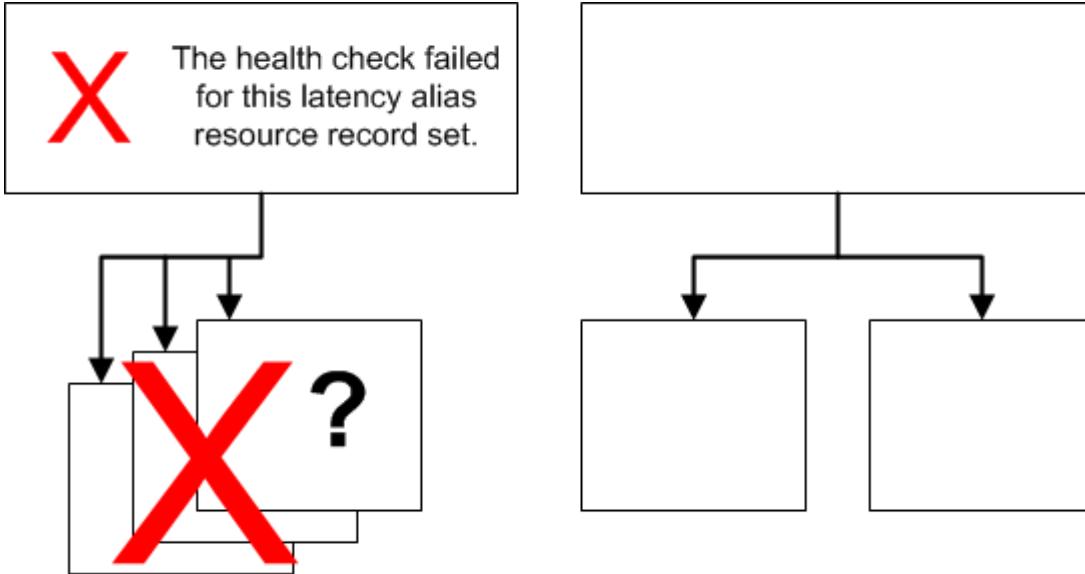
You assign a health check to a latency alias resource record set for which the alias target is a group of weighted resource record sets.

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.

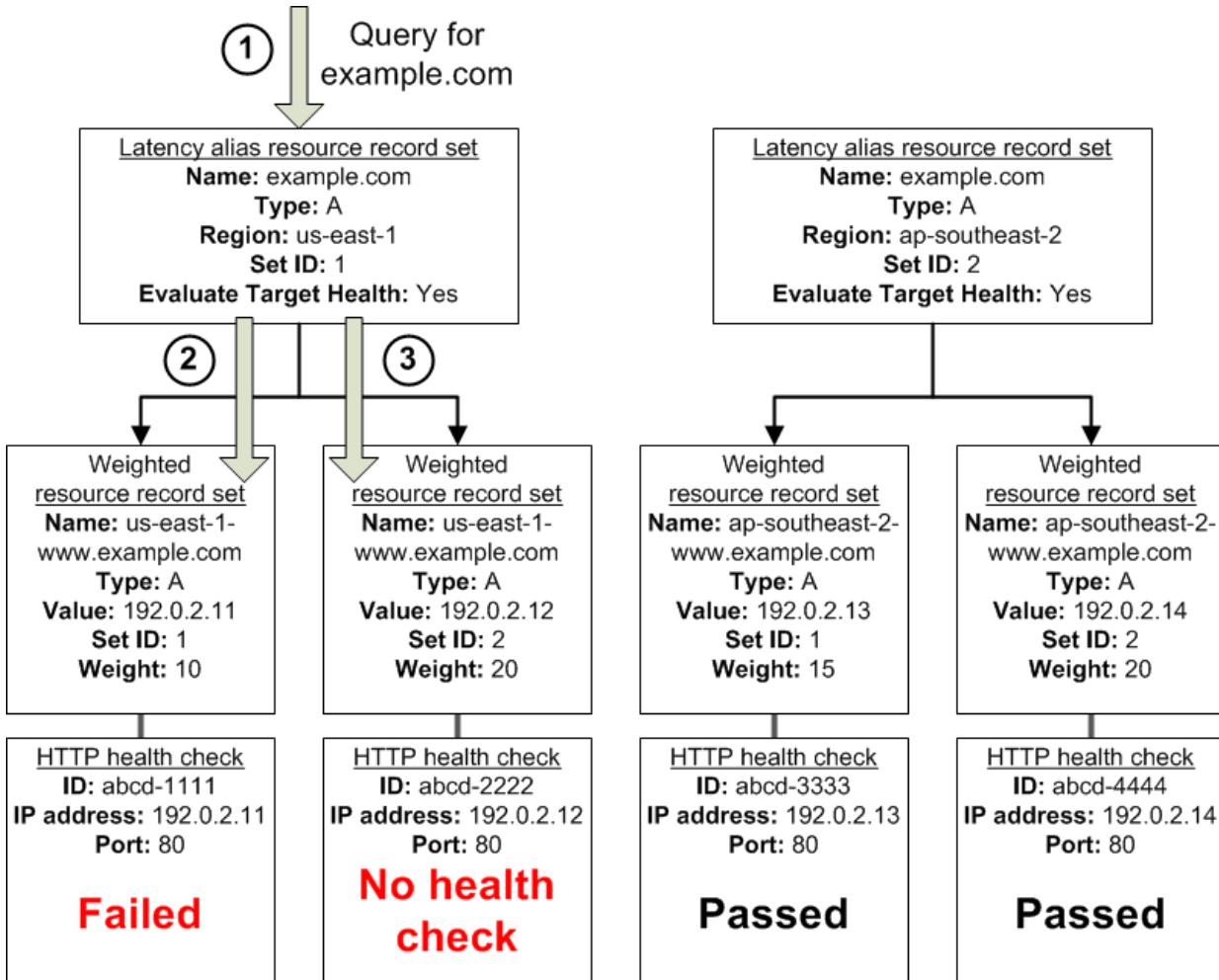
At least one weighted resource record set must be considered healthy, either because it's associated with a health check that passes or because it's not associated with a health check. In the latter case, Amazon Route 53 always considers the weighted resource record set healthy.



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:



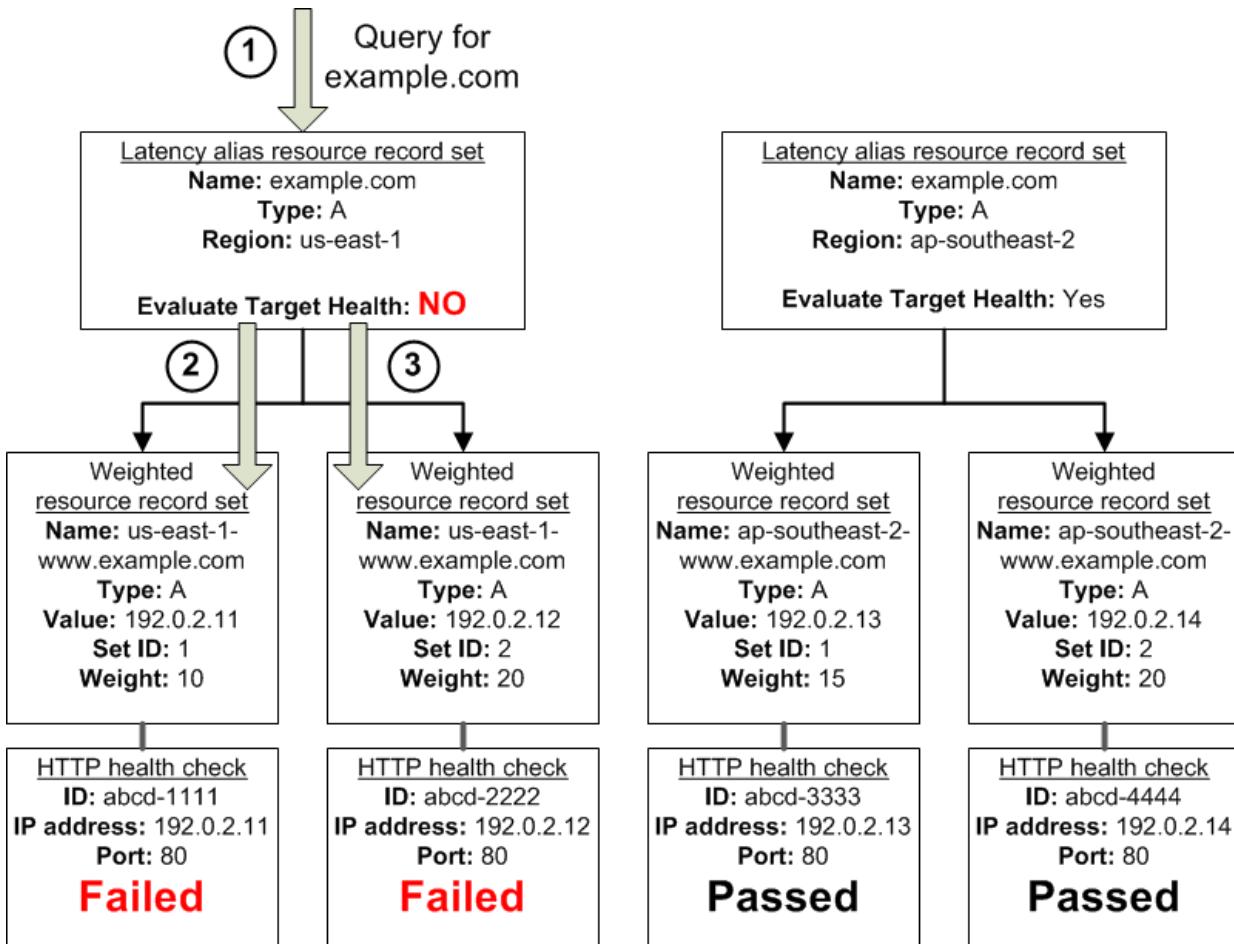
Here's what happens when you omit a health check on a non-alias resource record set in this configuration: Amazon Route 53 receives a query for example.com. Based on the latency for the user making the request, Amazon Route 53 selects the latency alias resource record set for the us-east-1 region.

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 for the application that leverages multiple regions for the most recently accessed content and latency sensitive portions of the web 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?

- 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 SQS workers for propagating updates to each table.
- 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.
- 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"
            ]
        }
    ]
}

```

```

        ]
    }
}

{
    "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 private 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: AC

Section: (none)

Explanation

Explanation/Reference:

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 will 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 verify network traffic is leveraging DirectConnect.
- B. Configure your DirectConnect router with a higher 8GP priority than 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 priority. And verify network traffic is leveraging the DirectConnect connection.

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 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 load balancer (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 NAT 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: D

Section: (none)

Explanation

Explanation/Reference:

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: A

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 CIDR block of 10.0.0.0/28. You initially deploy two web servers, two application servers, two database servers and one NAT instance for 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 traffic 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 be the root cause? (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:

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 ELB. 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

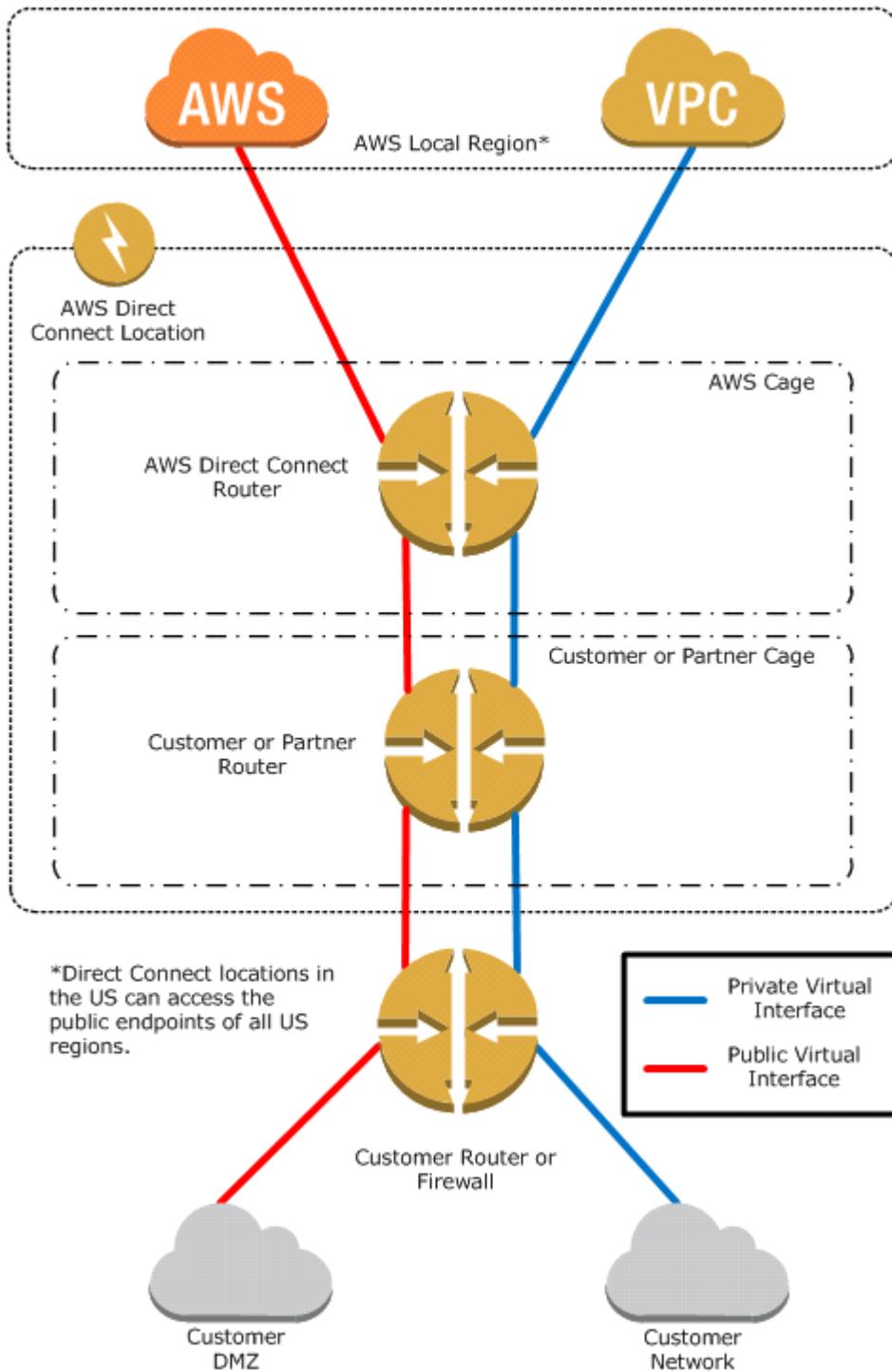
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth 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:

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 to 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 to store the search index and 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 Tomcat 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 its 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 underestimate 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 I can'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:

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 all 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:

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:

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: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

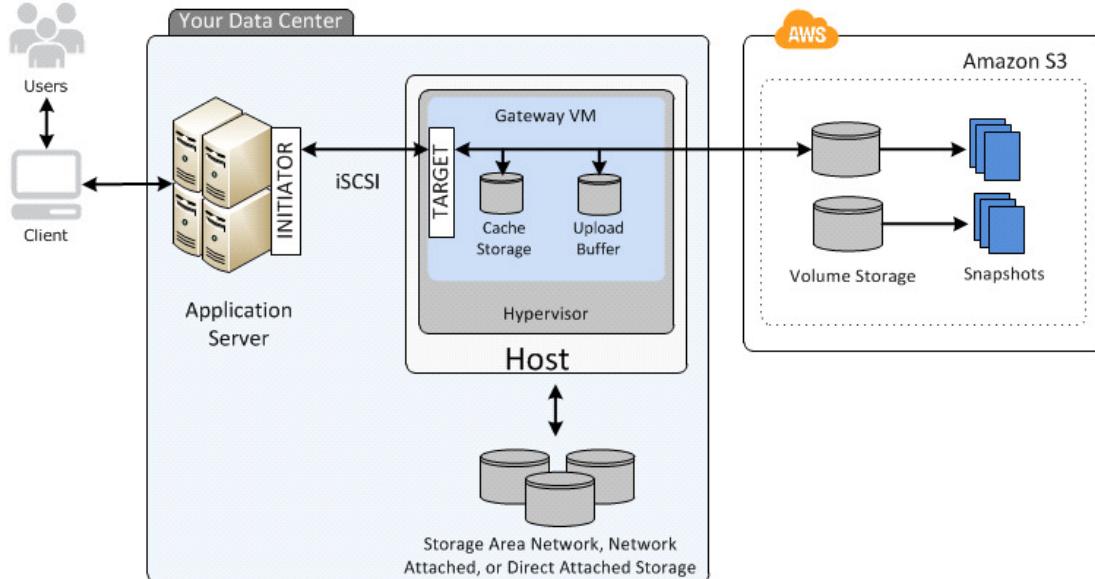
Gateway-Cached Volume Architecture

Gateway-cached volumes let you use Amazon Simple Storage Service (Amazon S3) as your primary data storage while retaining frequently accessed data locally in your storage gateway. Gateway-cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.

Gateway-cached volumes can range from 1 GiB to 32 TiB in size and must be rounded to the nearest GiB. Each gateway configured for gateway-cached volumes can support up to 32 volumes for a total maximum storage volume of 1,024 TiB (1 PiB).

In the gateway-cached volume solution, AWS Storage Gateway stores all your on-premises application data in a storage volume in Amazon S3.

The following diagram provides an overview of the AWS Storage Gateway-cached volume deployment.



After you've installed the AWS Storage Gateway software appliance—the virtual machine (VM)—on a host in your data center and activated it, you can use the AWS Management Console to provision storage volumes backed by Amazon S3. You can also provision storage volumes programmatically using the AWS Storage Gateway API or the AWS SDK libraries. You then mount these storage volumes to your on-premises application servers as iSCSI devices.

You also allocate disks on-premises for the VM. These on-premises disks serve the following purposes:
Disks for use by the gateway as cache storage – As your applications write data to the storage volumes in AWS, the gateway initially stores the data on the on-premises disks referred to as cache storage before uploading the data to Amazon S3. The cache storage acts as the on-premises durable store for data that is waiting to upload to Amazon S3 from the upload buffer.

The cache storage also lets the gateway store your application's recently accessed data on-premises for low-latency access. If your application requests data, the gateway first checks the cache storage for the data before checking Amazon S3.

You can use the following guidelines to determine the amount of disk space to allocate for cache storage. Generally, you should allocate at least 20 percent of your existing file store size as cache storage. Cache storage should also be larger than the upload buffer. This latter guideline helps ensure cache storage is large enough to persistently hold all data in the upload buffer that has not yet been uploaded to Amazon S3.

Disks for use by the gateway as the upload buffer – To prepare for upload to Amazon S3, your gateway also stores incoming data in a staging area, referred to as an upload buffer. Your gateway uploads this buffer data over an encrypted Secure Sockets Layer (SSL) connection to AWS, where it is stored encrypted in Amazon S3.

You can take incremental backups, called snapshots, of your storage volumes in Amazon S3. These point-in-time snapshots are also stored in Amazon S3 as Amazon EBS snapshots. When you take a new snapshot, only the data that has changed since your last snapshot is stored. You can initiate snapshots on a scheduled or one-time basis. When you delete a snapshot, only the data not needed for any other snapshots is removed. You can restore an Amazon EBS snapshot to a gateway storage volume if you need to recover a backup of your data. Alternatively, for snapshots up to 16 TiB in size, you can use the snapshot as a starting point for a new Amazon EBS volume. You can then attach this new Amazon EBS volume to an Amazon EC2 instance. All gateway-cached volume data and snapshot data is stored in Amazon S3 encrypted at rest using server-side encryption (SSE). However, you cannot access this data with the Amazon S3 API or other tools such as the Amazon S3 console.

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 files 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:

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: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using Reduced Redundancy Storage

Amazon S3 stores objects according to their storage class. It assigns the storage class to an object when it is written to Amazon S3. You can assign objects a specific storage class (standard or reduced redundancy) only when you write the objects to an Amazon S3 bucket or when you copy objects that are already stored in Amazon S3. Standard is the default storage class. For information about storage classes, see [Object Key and Metadata](#).

In order to reduce storage costs, you can use reduced redundancy storage for noncritical, reproducible data at lower levels of redundancy than Amazon S3 provides with standard storage. The lower level of redundancy results in less durability and availability, but in many cases, the lower costs can make reduced redundancy storage an acceptable storage solution. For example, it can be a cost-effective solution for sharing media content that is durably stored elsewhere. It can also make sense if you are storing thumbnails and other resized images that can be easily reproduced from an original image.

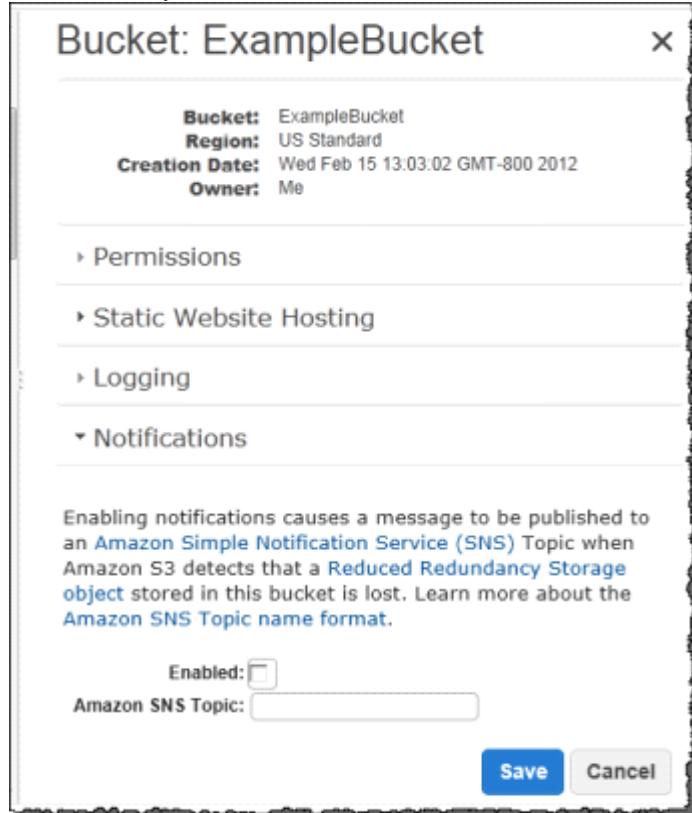
Reduced redundancy storage is designed to provide 99.99% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.01% of objects. For example, if you store 10,000 objects using the RRS option, you can, on average, expect to incur an annual loss of a single object per year (0.01% of 10,000 objects).

Note

This annual loss represents an expected average and does not guarantee the loss of less than 0.01% of objects in a given year.

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.

If an object in reduced redundancy storage has been lost, Amazon S3 will return a 405 error on requests made to that object. Amazon S3 also offers notifications for reduced redundancy storage object loss: you can configure your bucket so that when Amazon S3 detects the loss of an RRS object, a notification will be sent through Amazon Simple Notification Service (Amazon SNS). You can then replace the lost object. To enable notifications, you can use the Amazon S3 console to set the Notifications property of your bucket.



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 to 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: BD

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 DynamoDB 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 their PC. 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 AutoScaling 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 then 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 trail 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 that 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 for the SaaS application to work, provide the role ARN 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](#).

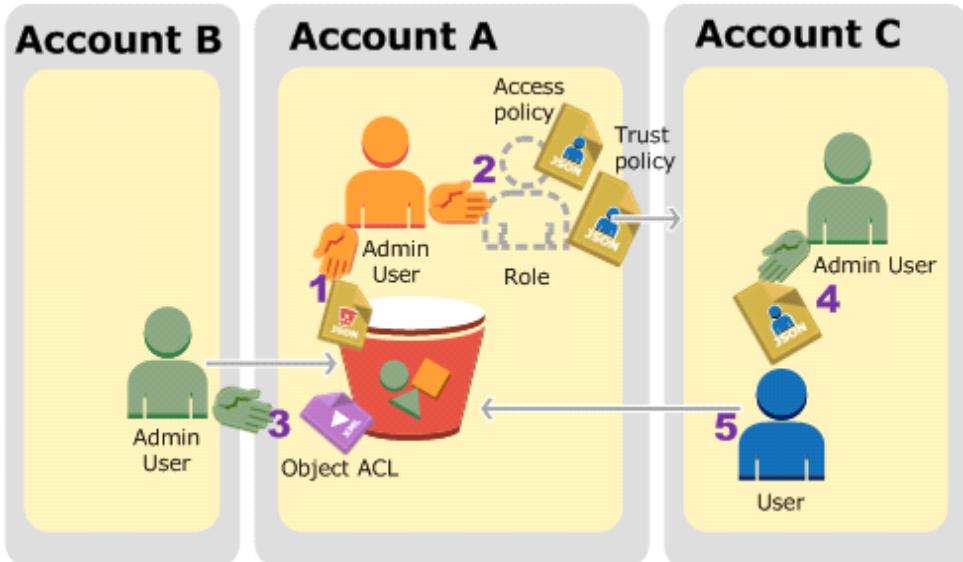
The AWS account identified in the trust policy then grants its user permission to assume the role. The user can then do the following to access objects:

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?

- Configure a web proxy server in your VPC and enforce URL-based rules for outbound access Remove default routes.
- Implement security groups and configure outbound rules to only permit traffic to software depots.
- 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.
- Implement network access control lists to all specific destinations, with an Implicit deny as a rule.

Correct Answer: A

Section: (none)**Explanation****Explanation/Reference:****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 have the user input Access and Secret Keys from an already created IAM user that has the 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 that 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 be 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 the 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 (that contains the specific instance-id).

Correct Answer: A**Section: (none)**

Explanation

Explanation/Reference:

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 SAML 2.0-compliant identity provider (IDP) to retrieve temporary security credentials to enable NOC members to sign in to the AWS Management Console.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

You are designing an SSL/TLS 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/443. 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:

QUESTION 53

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC Your server's on-premises will be communicating with your VPC instances You will be 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: BD

Section: (none)

Explanation

Explanation/Reference:

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: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

You have an application running on an EC2 Instance which will allow users to download files 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:

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: CEF

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 for 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 undertaken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware. The outcome was that all 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:

QUESTION 61

You have a periodic Image analysis application that gets some files In Input analyzes them and for 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 of 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 capturing 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 CloudFront 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: AC

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 Redshift 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: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTPS 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 all 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:

QUESTION 67

To serve Web traffic for a popular product your chief financial officer and IT director have purchased 10 m1 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 m1 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 Auto-scaling group and Launch Configuration with ELB to add up to 10 more on-demand m1 large instances when triggered by Cloudwatch shut off c3.2xlarge 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 Autoscailing group for up to two additional c3.2xlarge instances Shut on mi .large instances.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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 autoscaling 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:

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: ABD

Section: (none)

Explanation

Explanation/Reference:**QUESTION 70**

A large real-estate brokerage is exploring the option of 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 offers 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 offers. EC2 instances will communicate with mobile carriers/device providers to push alerts back to the 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 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 offers 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:****QUESTION 71**

A company is building a voting system for a popular TV show, viewers will 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 it 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 call the Login With Amazon service to authenticate the user then process the user's 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 user's 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 user's 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 will process the user's 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. 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's S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3 object directly utilizing STS, Web Identity Federation, and S3 ACLs to authenticate and authorize access.

Correct Answer: B**Section:** (none)**Explanation****Explanation/Reference:****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 app'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: A**Section:** (none)**Explanation****Explanation/Reference:**

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 account's bill to a Master AWS account using Consolidated Billing. To make sure you stay 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](#).

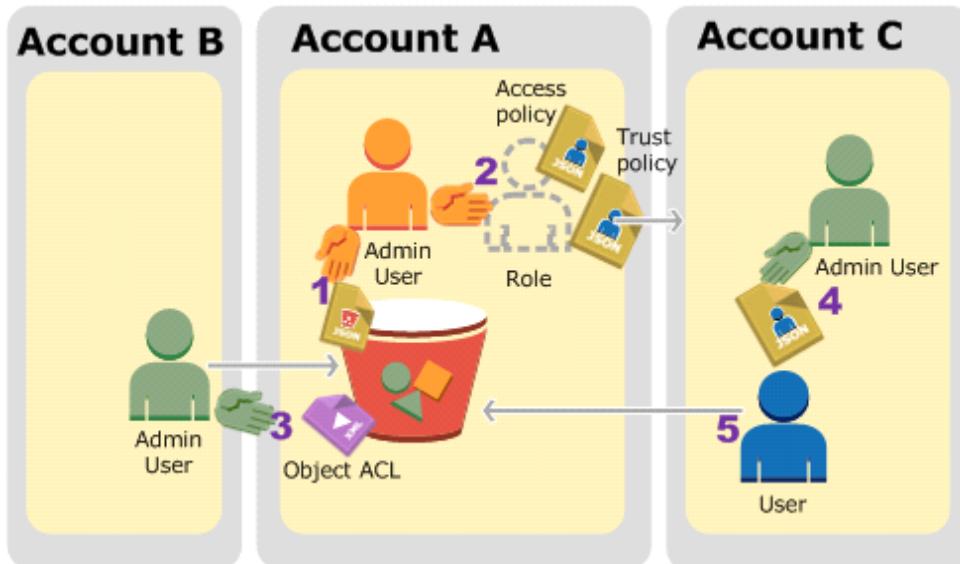
The AWS account identified in the trust policy then grants its user permission to assume the role. The user can then do the following to access objects:

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:

The throughput of an Amazon Kinesis stream is designed to scale without limits via increasing the number of shards within a stream. However, there are certain limits you should keep in mind while using Amazon Kinesis Streams:

By default, Records of a stream are accessible for up to 24 hours from the time they are added to the stream. You can raise this limit to up to 7 days by enabling extended data retention.

The maximum size of a data blob (the data payload before Base64-encoding) within one record is 1 megabyte (MB).

Each shard can support up to 1000 PUT records per second.

For more information about other API level limits, see [Amazon Kinesis Streams Limits](#).

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: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

You are running a successful multtier 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 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 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: C

Section: (none)

Explanation

Explanation/Reference:

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 and is therefore only done once per week.

Recently, a new chat feature has been implemented in nodejs and wants 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: C

Section: (none)

Explanation

Explanation/Reference:

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 often 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 SQS. 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: D

Section: (none)

Explanation

Explanation/Reference:

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:

QUESTION 82

You must assign each server to at least _____ security group

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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:

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:

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:

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:

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:

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:

Q: Will my standby be in the same Region as my primary?

Yes. Your standby is automatically provisioned in a [different Availability Zone of the same Region](#) as your DB instance primary.

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:

Troubleshooting Applications on Amazon RDS

Topics

- [Retrieving Errors](#)
- [Troubleshooting Tips](#)

Amazon Relational Database Service; provides specific and descriptive errors to help you troubleshoot problems while interacting with the Amazon RDS API.

Retrieving Errors

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 [Error](#) node in the response from the Amazon RDS API.

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

QUESTION 113

What are the two permission types used by AWS?

- Resource-based and Product-based
- Product-based and Service-based
- Service-based
- User-based and Resource-based

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 114

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

- FreeStorage
- FreeStorageSpace
- FreeStorageVolume
- FreeDBStorageSpace

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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:

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:

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:

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:

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:

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:

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:

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. If you create a second-tier Read Replica, you may be able to move some of the replication load from the master database instance to the second-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](#) to 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:

QUESTION 139

What is the durability of S3 RRS?

- A. 99.99%
- B. 99.95%
- C. 99.995%
- D. 99.99999999%

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

RRS = Reduced Redundancy Storage

	Standard	Standard - Infrequent Access	Reduced
Durability	99.999999999%	99.999999999%	

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:

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:

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:

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:

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:

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:

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:

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 ($\$0.10 \text{ per provisioned IOPS-month} * 1000 \text{ IOPS provisioned} * 15 \text{ days/30}$). 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

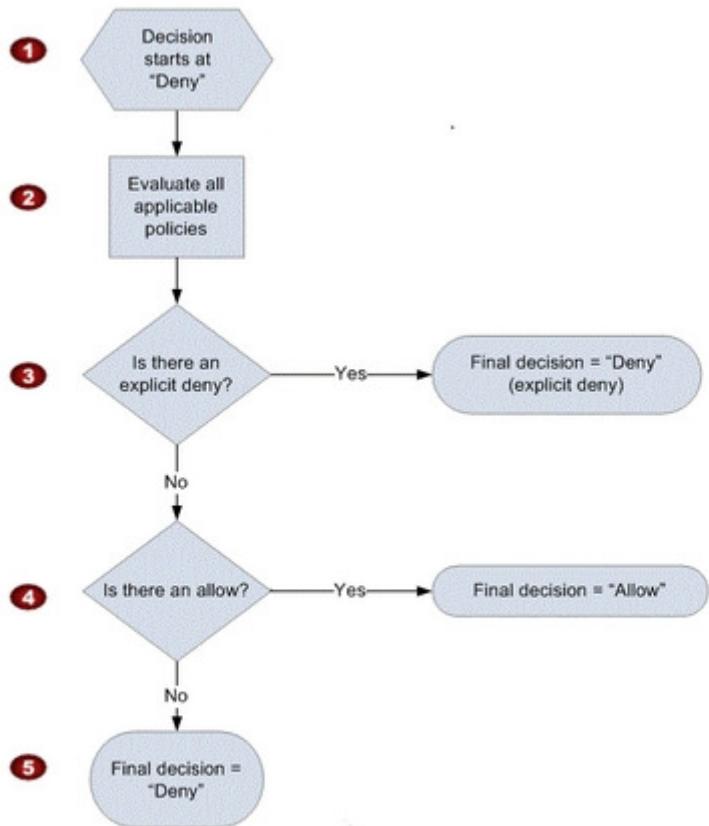
IAM's Policy Evaluation Logic always starts with a default _____ for every request, except for those that use the AWS account's root security credentials b

- 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. 1TB
- 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>

- JDeveloper
- NetBeans
- Application Testing Suite
- SQL Developer
- SQL Developer Data Modeler
- Application Development Framework
- Application Express
- Oracle REST Data Services
- Developer Tools for Visual Studio
- Discoverer
- Enterprise Pack for Eclipse
- JHeadstart
- Warehouse Builder
- XML Developer's Kit
- Zend Server
- Forms
- Oracle Help Technologies
- Oracle Mobile Application Framework
- WebRTC
- Oracle JET



What is SQL Developer?

Date: May 2014

Oracle SQL Developer is the Oracle Database IDE. A free graphical user interface, Oracle SQL Developer allows developers and administrators to do their database tasks in fewer clicks and keystrokes. A productivity tool designed to help the end user save time and maximize the return on investment in the Oracle Database.

SQL Developer supports Oracle Database 10g, 11g, and 12c and will run on any operating system.

For the Developer

SQL Developer provides powerful editors for working with SQL, PL/SQL, Stored Java Procedures, and more. It also includes features for generating execution plans, export data to the desired format (XML, Excel, HTML, PDF, etc.), execute, debug, and analyze programs, and much more with SQL Developer.

For the DBA

SQL Developer isn't just for developers! Since version 3.0, the DBA Panel (available under the Tools menu) provides a set of interfaces for their most critical tasks. SQL Developer will continue to support and enhance these features.

- Data Pump
- Recovery Manager (RMAN)
- Oracle Auditing
- User and Role management
- Storage management, including the ability to add space to your tablespaces
- Resource Manager

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:

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: A

Section: (none)

Explanation

Explanation/Reference:

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:

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: B

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: D

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:

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: A

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. DescribeFailure
- 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.

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: 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/>

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/>

Important Notes about Purchases

- If your needs change, you can modify or exchange reserved instances, or list eligible Standard Reserved Instances in the Reserved Instance Marketplace.
- You can purchase up to 20 Reserved Instances per Availability Zone each month. If you need additional Reserved Instances, contact AWS Support.
the form found [here](#).
- Purchases of Reserved Instances are **non-refundable**.
- If you purchase a Reserved Instance from a third-party seller, we will share your city, state, and zip code with the seller for marketing purposes. If you don't wish to purchase from a 3rd party seller, please make sure to select a Reserved Instance with the seller in the console purchasing screen.

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/>

Push-Button Scaling

- **DB Instance Class** – Using the Amazon RDS APIs or a few clicks of the AWS Management Console, you can scale memory resources powering your deployment up or down. Scaling operations typically complete within a handful of minutes.
- **Storage and IOPS** – As your storage requirements grow you can provision additional storage on-the-fly with zero downtime. Using RDS Provisioned IOPS, you can also scale the throughput of your DB instance by specifying the IOPS rate from **10,000 IOPS** in 1,000 IOPS increments and storage from 100GB to 6TB.

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:

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:

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: A

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 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:

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: B

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: A**Section: (none)****Explanation****Explanation/Reference:****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**

What does Amazon Elastic Beanstalk provide?

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

Correct Answer: C**Section: (none)****Explanation**

Explanation/Reference:**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:****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: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using Private Hosted Zones

If you want to access the resources in your VPC using custom DNS domain names, such as example.com, instead of using private IP addresses or AWS-provided private DNS hostnames, you can create a private hosted zone in Amazon Route 53. A private hosted zone is a container that holds information about how you want to route traffic for a domain and its subdomains within one or more VPCs without exposing your resources to the Internet. You can then create Amazon Route 53 resource record sets, which determine how Amazon Route 53 responds to queries for your domain and subdomains. For example, if you want browser requests for example.com to be routed to a web server in your VPC, you'll create an A record in your private hosted zone and specify the IP address of that web server. For more information about creating a private hosted zone, see Working with Private Hosted Zones in the Amazon Route 53 Developer Guide.

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 backups or imports, 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.Procedure.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:

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:

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:

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/>

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 us

Similarly, you can atomically add or remove to sets, lists, or maps. [View our documentation for more information on a](#)

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 of the Amazon Web Services cloud. It's designed to help you quickly and easily send and receive email without having to build and maintain your own email infrastructure. With Amazon SES, you can send and receive email with no required minimum commitment or setup fees. 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

Note

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.

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:

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 Availability 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.

Amazon Elastic Block **Store** (Amazon EBS) provides persistent block 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: B

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.DBInstanceClasses.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

Is there a limit to the number of groups you can have?

- 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:

<http://aws.amazon.com/rds/faqs/#46>

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:

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>

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](#).

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 at <https://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: DE

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:

To ensure that a NAT instance works as it should, it is a rule by AWS that the Source/Destination Check attribute on the NAT instance should be disable.

Secondary private IPs	
VPC ID	vpc-6dcc550a
Subnet ID	subnet-e1665acb
Network interfaces	eth0
Source/dest. check	True
EBS-optimized	False
Root device type	ebs
Root device	/dev/xvda
Block devices	/dev/xvda

You can do this, by selecting the appropriate menu option as shown below in the EC2 dashboard.

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: ABE

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)

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: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html>

An "EBS-backed" instance is an EC2 instance which uses an EBS volume as its root device. An EBS volume behaves like a raw, unformatted, external block device that you can attach to a single instance and are not physically attached to the Instance host computer (more like a network attached storage). The volume persists independently from the running life of an instance. After an EBS volume is attached to an instance, you can use it like any other physical hard drive. You can also detach an EBS volume from one instance and attach it to another instance. EBS volumes can also be created as encrypted volumes using the Amazon EBS encryption feature.

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: AE

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.

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 AWS 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: AB

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 the 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 can't 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.

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.

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:

<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 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 its 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:

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:

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/AmazonCloudWatchLogs/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 properly 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: C

Section: (none)

Explanation

Explanation/Reference:

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

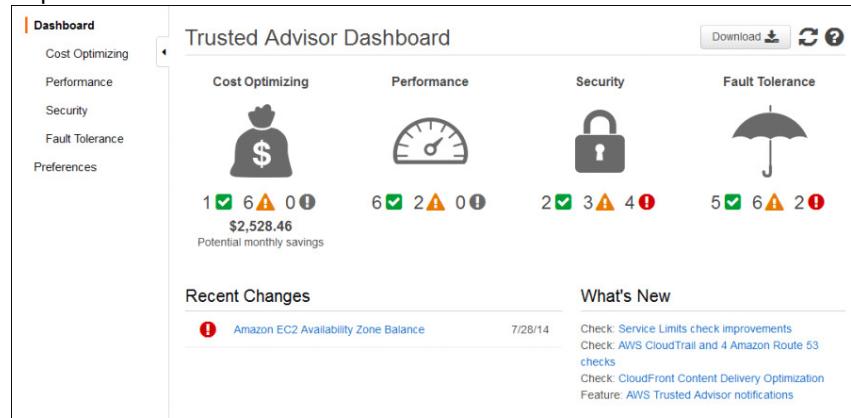
Correct Answer: C

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 (OIDC)-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 can have one Elastic IP (EIP) address associated with a running instance at no charge. If you associate additional EIPs with that instance, you will be charged for each additional EIP associated with that instance per hour on a pro rata basis.

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: C

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.amazonaws.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 that 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 properly 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:

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: BC

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 linguagem que trata configurações de servidor como código. O OpsWorks usa o Chef para automatizar a configuração, implantados e gerenciados em instâncias do Amazon Elastic Compute Cloud (EC2) e em máquinas 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 into 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 into 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 its 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.

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.

Comece a trabalhar com a AWS hoje

Experimente o Amazon S3 gratuitamente

O nível gratuito da AWS inclui 500 GB de armazenamento, 20.000 solicitações GET e 2.000 solicitações PUT com 100 MB.

[Consulte os detalhes do nível gratuito da AWS »](#)

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 reusable 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 are 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 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:

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:

Placement Groups

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. For more information, see [Enhanced Networking](#).

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:

Placement Groups

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. For more information, see [Enhanced Networking](#).

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 log all 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 determine 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 into 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	<ul style="list-style-type: none"> • Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ◦ MongoDB ◦ Cassandra ◦ Microsoft SQL Server ◦ MySQL ◦ PostgreSQL ◦ Oracle 	<ul style="list-style-type: none"> • Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume 	<ul style="list-style-type: none"> • 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.

Security Groups - Specific Ports Unrestricted, Service Limits, IAM Use, and MFA on Root Account.

Services ▾ Edit ▾

Dashboard

Cost Optimization

Performance

Security

Fault Tolerance

Preferences

Trusted Advisor Dashboard

Cost Optimization

Performance

Security

Fault Tolerance

Download

Recommended Actions

Security Groups - Specific Ports Unrestricted Updated: 7/30/14 3:47 PM

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.
1 of 1 security group rules allow unrestricted access to a specific port.

MFA on Root Account Updated: 7/30/14 3:47 PM

Checks the root account and warns if multi-factor authentication (MFA) is not enabled.
MFA is not enabled on the root account.

IAM Use Updated: 7/30/14 3:47 PM

Checks for your use of AWS Identity and Access Management (IAM).
At least one IAM user, group, or role has been created for this account.

Service Limits Updated: 7/30/14 3:47 PM

Checks for usage that is more than 80% of the service limit.
8 of 22 items have usage that is more than 80% of the service limit.

Upgrade your Support plan to unlock all Trusted Advisor recommendations!
You will have access to technical support from a cloud support engineer, with phone and chat support, support API, Identity and Access Management, Architecture support - use case guidance, and more.

Choose language English

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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:

Overview of AWS Import/Export

AWS Import/Export accelerates transferring data between the AWS cloud and portable storage devices that you mail to us. AWS Import/Export is a good choice if you have 16 terabytes (TB) or less of data to import into Amazon Simple Storage Service (Amazon S3), Amazon Glacier, or Amazon Elastic Block Store (Amazon EBS). You can also export data from Amazon S3 with AWS Import/Export.

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 POSTS 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-denialallow

- 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

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and manage 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 Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.

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 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 repetitive 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 orphanned 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.

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:

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:

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:

Explanation: EXEMPLO ONLINE

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:

Explanation: EXEMPLO ONLINE

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:

Explanation: EXEMPLO ONLINE

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: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: EXEMPLO ONLINE

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:

Explanation:SIMULADO PAGO

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:

Explanation:SIMULADO PAGO

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:

Explanation:SIMULADO PAGO

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:

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: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:SIMULADO PAGO

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:

Explanation:SIMULADO PAGO

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: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: SIMULADO PAGO

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:

Explanation:SIMULADO PAGO

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: D

Section: (none)

Explanation

Explanation/Reference:**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:**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:**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:

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.

A screenshot of the AWS IAM 'Create New Role' interface. On the left, a sidebar menu lists options: Dashboard, Groups, Users, Roles (which is selected and highlighted in orange), Policies, Identity providers, Account settings, and Credential report. The main panel title is 'Create New Role'. It features a 'Role Name' dropdown menu with 'Cloudwatchrole' selected. A 'Filter' input field is also present.

Once the role has been created, when creating the EC2 instance, in the Configure Instance Details screen, ensure to choose the IAM role.

A screenshot of the 'Configure Instance Details' step in the EC2 instance creation wizard. The top navigation bar shows steps 1 through 7. Step 3, 'Configure Instance Details', is active. The 'IAM role' dropdown is set to 'Cloudwatchrole'. Other configuration options shown include 'Number of Instances' (1), 'Purchasing option' (Request Spot instances), 'Network' (vpc-6dcc550a), 'Subnet' (No preference), 'Auto-assign Public IP' (Use subnet setting), and 'Launch into Auto Scaling Group'.

The correct answer is: Create a role which has the necessary privileges and can be assumed by the EC2 instance.

QUESTION 513

A customer has a requirement to extend their on-premises data center to AWS. The customer requires a 50-

Mbps dedicated and private connection to their VPC.
Which AWS product or feature satisfies this requirement?

- A. Amazon VPC
- 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 4GiB volume will not be accepted. An example is show below

Create Volume

Volume Type: Provisioned IOPS SSD (IO1)

Size (GiB): 4 (Min: 4 GiB, Max: 16384 GiB)

IOPS: 300 (Min: 100 IOPS, Max: 20000 IOPS)
⚠ Maximum ratio of 50:1 is permitted between IOPS and volume size

Throughput (MB/s): Not Applicable

Availability Zone: us-east-1a

Snapshot ID: Search (case-insensitive)

Encryption: Encrypt this volume

Create

The correct answer is: 200

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 specify 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

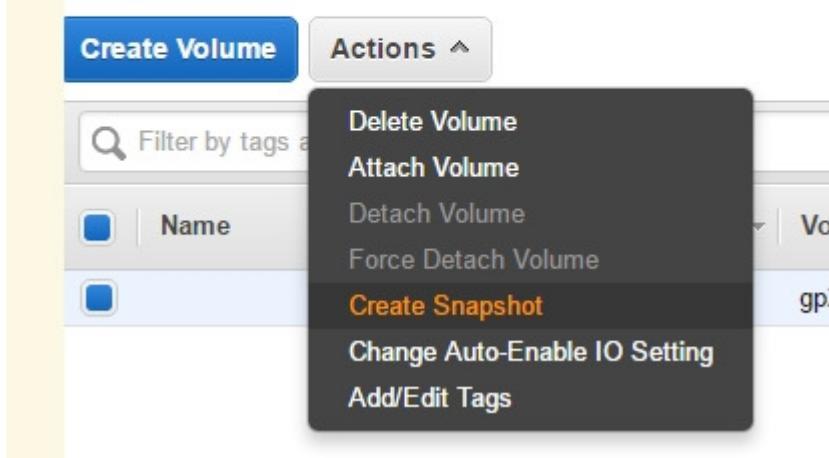
Explanation/Reference:

Explanation:

- Assume you have a volume as shown below in the Availability Zone – us-east-1a

Filter by tags and attributes or search by keyword						
Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
						Availability Zone
	vol-0492e9e...	100 GiB	gp2	300 / 3000		November 8, 2016 ... us-east-1a

- Click on the Actions->Create Snapshot option.



QUESTION 517

A company is hosting EC2 instances which focuses on work-loads which 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 this 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 you 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 Amazon RDS?

- A. MSSQL
- B. MySQL
- 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.

- Step 1: Select Engine
Step 2: Production?
Step 3: Specify DB Details
Step 4: Configure Advanced Settings

Configure Advanced Settings

Network & Security

VPC*	Default VPC (vpc-6dcc550a)
Subnet Group	default
Publicly Accessible	Yes
Availability Zone	No Preference
VPC Security Group(s)	<input type="button" value="Create new Security Group"/> AutoScaling-Security-Group-1 (VPC) default (VPC) launch-wizard-1 (VPC)

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 manage 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 your business. Amazon RDS provides you six familiar database engines to choose from, including Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.