AWS Solutions Architect important Questions Set-2

Question 1: Skipped

You want to use AWS Import/Export to send data from your S3 bucket to several of your branch offices. What should you do if you want to send 10 storage units to AWS?

- Make sure your disks are encrypted prior to shipping
- Make sure you format your disks prior to shipping.
- Make sure your disks are 1TB or more.
- Make sure you submit a separate job request for each device (Correct)

Explanation

When using Amazon Import/Export, a separate job request needs to be submitted for each physical device even if they belong to the same import or export job.

Question 2: Skipped

You need to measure the performance of your EBS volumes as they seem to be under performing. You have come up with a measurement of 1,024 KB I/O but your colleague tells you that EBS volume performance is measured in IOPS. How many IOPS is equal to 1,024 KB I/O?

- 16
- 256
- 8
- 4 (Correct)

Explanation

Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration. IOPS are input/output operations per second. Amazon EBS measures each I/O operation per second (that is 256 KB or smaller) as one IOPS. I/O operations that are larger than 256 KB are counted in 256 KB capacity units. For example, a 1,024 KB I/O operation would count as 4 IOPS. When you provision a 4,000 IOPS volume and attach it to an EBS-optimized instance that can provide the necessary bandwidth, you can transfer up to 4,000 chunks of data per second (provided that the I/O does not exceed the 128 MB/s per volume throughput limit of General Purpose (SSD) and Provisioned IOPS (SSD) volumes).

Question 3: Skipped

Having set up a website to automatically be redirected to a backup website if it fails, you realize that there are different types of failovers that are possible. You need all your resources to be available the majority of the time. Using Amazon Route 53 which configuration would best suit this requirement?

- Active-active failover. (Correct)
- Non
- Route 53 can't failover.
- Active-passive failover
- Active-active-passive and other mixed configuration

Explanation

You can set up a variety of failover configurations using Amazon Route 53 alias: weighted, latency, geolocation routing, and failover resource record sets. Active-active failover: Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Amazon Route 53 can detect that it's unhealthy and stop including it when responding to queries. Active-passive failover: Use this failover configuration when you want a primary group of resources to be available the majority of the time and you want a secondary group of resources to be on standby in case all of the primary resources become unavailable. When responding to queries, Amazon Route 53 includes only the healthy primary resources. If all of the primary resources are unhealthy, Amazon Route 53 begins to include only the healthy secondary resources in response to DNS queries. Active-active-passive and other mixed configurations: You can combine alias and non-alias resource record sets to produce a variety of Amazon Route 53 behaviors.

Question 4: Skipped

You decide that you need to create a number of Auto Scaling groups to try and save some money as you have noticed that at certain times most of your EC2 instances are not being used. By default, what is the maximum number of Auto Scaling groups that AWS will allow you to create?

- 12
- Unlimited
- 20 (Correct)
- 2

Explanation

: Auto Scaling is an AWS service that allows you to increase or decrease the number of EC2 instances within your application's architecture. With Auto Scaling, you create collections of EC2 instances, called Auto Scaling groups. You can create these groups from scratch, or from existing EC2 instances that are already in production.

Question 5: Skipped

A user needs to run a batch process which runs for 10 minutes. This will only be run once, or at maximum twice, in the next month, so the processes will be temporary only. The process needs 15 X-Large instances. The process downloads the code from S3 on each instance when it is launched, and then generates a temporary log file. Once the instance is terminated, all the data will be lost. Which of the below mentioned pricing models should the user choose in this case?

- Spot instance. (Correct)
- Reserved instance
- On-demand instance.
- EBS optimized instance

Explanation

: In Amazon Web Services, the spot instance is useful when the user wants to run a process temporarily. The spot instance can terminate the instance if the other user outbids the existing bid. In this case all storage is temporary and the data is not required to be persistent. Thus, the spot instance is a good option to save money.

Question 6: Skipped

Which of the following is NOT a characteristic of Amazon Elastic Compute Cloud (Amazon EC2)?

- It can be used to launch as many or as few virtual servers as you need
- It increases the need to forecast traffic by providing dynamic IP addresses for static cloud computing. (Correct)
- It eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
- It offers scalable computing capacity in the Amazon Web Services (AWS) cloud

Explanation

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

Question 7: Skipped

You are setting up your first Amazon Virtual Private Cloud (Amazon VPC) so you decide to use the VPC wizard in the AWS console to help make it easier for you. Which of the following statements is correct regarding instances that you launch into a default subnet via the VPC wizard?

- Instances that you launch into a default subnet receive a public IP address and 10 private IP addresses.
- Instances that you launch into a default subnet receive both a public IP address and a private IP address (Correct)
- Instances that you launch into a default subnet don't receive any ip addresses and you need to define them manually.
- Instances that you launch into a default subnet receive a public IP address and 5 private IP addresse

Explanation

Instances that you launch into a default subnet receive both a public IP address and a private IP address. Instances in a default subnet also receive both public and private DNS hostnames. Instances that you launch into a nondefault subnet in a default VPC don't receive a public IP address or a DNS hostname. You can change your subnet's default public IP addressing behavior.

Question 8: Skipped

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

- The client can connect over IPV4 or IPV6 using Dualstack
- Communication between the load balancer and back-end instances is always through IPV4
- ELB DNS supports both IPV4 and IPV6
- The ELB supports either IPV4 or IPV6 but not both (Correct)

Explanation

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

Question 9: Skipped

Does AWS CloudFormation support Amazon EC2 tagging?

- Yes, AWS CloudFormation supports Amazon EC2 tagging (Correct)
- No, CloudFormation doesn't support any tagging
- No, it doesn't support Amazon EC2 tagging.
- It depends if the Amazon EC2 tagging has been defined in the template

Explanation

In AWS CloudFormation, Amazon EC2 resources that support the tagging feature can also be tagged in an AWS template. The tag values can refer to template parameters, other resource names, resource attribute values (e.g. addresses), or values computed by simple functions (e.g., a concatenated list of strings).

Question 10: Skipped

An existing client comes to you and says that he has heard that launching instances into a VPC (virtual private cloud) is a better strategy than launching instances into a EC2-classic which he knows is what you currently do. You suspect that he is correct and he has asked you to do some research about this and get back to him. Which of the following statements is true in regards to what ability launching your instances into a VPC instead of EC2-Classic gives you?

- All of the things listed here (Correct)
- Change security group membership for your instances while they're running
- Assign static private IP addresses to your instances that persist across starts and stops
- Define network interfaces, and attach one or more network interfaces to your instances

Explanation

By launching your instances into a VPC instead of EC2-Classic, you gain the ability to: Assign static private IP addresses to your instances that persist across starts and stops Assign multiple IP addresses to your instances Define network interfaces, and attach one or more network interfaces to your instances Change security group membership for your instances while they're running Control the outbound traffic from your instances (egress filtering) in addition to controlling the inbound traffic to them (ingress filtering) Add an additional layer of access control to your instances in the form of network access control lists (ACL) Run your instances on single-tenant hardware

Question 11: Skipped

A user is accessing an EC2 instance on the SSH port for IP 10.20.30.40. Which one is a secure way to configure that the instance can be accessed only from this IP?

- In the security group, open port 22 for IP 10.20.30.40
- In the security group, open port 22 for IP 10.20.30.40/32 (Correct)
- In the security group, open port 22 for IP 10.20.30.40/24
- In the security group, open port 22 for IP 10.20.30.40/0

Explanation

In AWS EC2, while configuring a security group, the user needs to specify the IP address in CIDR notation. The CIDR IP range 10.20.30.40/32 says it is for a single IP 10.20.30.40. If the user specifies the IP as 10.20.30.40 only, the security group will not accept and ask it in a CIRD format.

Question 12: Skipped

Which of the following statements is true of creating a launch configuration using an EC2 instance?

- The launch configuration can be created only using the Query APIs.
- Auto Scaling automatically creates a launch configuration directly from an EC2 instance (Correct)
- A user should manually create a launch configuration before creating an Auto Scaling group.
- The launch configuration should be created manually from the AWS CL

Explanation

You can create an Auto Scaling group directly from an EC2 instance. When you use this feature, Auto Scaling automatically creates a launch configuration for you as well.

Question 13: Skipped

You need to set up a high level of security for an Amazon Relational Database Service (RDS) you have just built in order to protect the confidential information stored in it. What are all the possible security groups that RDS uses?

- DB security groups, VPC security groups, and EC2 security groups. (Correct)
- DB security groups only
- EC2 security groups only
- VPC security groups, and EC2 security group

Explanation

A security group controls the access to a DB instance. It does so by allowing access to IP address ranges or Amazon EC2 instances that you specify. Amazon RDS uses DB security groups, VPC security groups, and EC2 security groups. In simple terms, a DB security group controls access to a DB instance that is not in a VPC, a VPC security group controls access to a DB instance inside a VPC, and an Amazon EC2 security group controls access to an EC2 instance and can be used with a DB instance.

Question 14: Skipped

You have been using T2 instances as your CPU requirements have not been that intensive. However you now start to think about larger instance types and start looking at M and IV|3 instances. You are a little confused as to the differences between them as they both seem to have the same ratio of CPU and memory. Which statement below is incorrect as to why you would use one over the other?

- M3 instances are less expensive than M1 instances.
- IV|3 instances are configured with more swap memory than M instances. (Correct)
- IV|3 instances provide better, more consistent performance that M instances for most use-cases.
- M3 instances also offer SSD-based instance storage that delivers higher I/O performance

Explanation

Amazon EC2 allows you to set up and configure everything about your instances from your operating system up to your applications. An Amazon Nlachine Image (AMI) is simply a packaged-up environment that includes all the necessary bits to set up and boot your instance. M1 and M3 Standard instances have the same ratio of CPU and memory, some reasons below as to why you would use one over the other. IV|3 instances provide better, more consistent performance that M instances for most use-cases. M3 instances also offer SSD-based instance storage that delivers higher I/O performance. M3 instances are also less expensive than M1 instances. Due to these reasons, we recommend M3 for applications that require general purpose instances with a balance of compute, memory, and network resources. However, if you need more disk storage than what is provided in M3 instances, you may still find M1 instances useful for running your applications.

Question 15: Skipped

You have set up an Elastic Load Balancer (ELB) with the usual default settings, which route each request independently to the application instance with the smallest load. However, someone has asked you to bind a user's session to a specific application instance so as to ensure that all requests coming from the user during the session will be sent to the same application instance. AWS has a feature to do this. What is it called?

- Connection draining
- Proxy protocol
- Tagging
- Sticky session (Correct)

Explanation

An Elastic Load Balancer(ELB) by default, routes each request independently to the application instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific application instance. This ensures that all requests coming from the user during the session will be sent to the same application instance. The key to managing the sticky session is determining how long your load balancer should consistently route the user's request to the same application instance. If your application has its own session cookie, then you can set Elastic Load Balancing to create the session cookie to follow the duration specified by the application's session cookie. If your application does not have its own session cookie, then you can set Elastic Load Balancing to create a session cookie by specifying your own stickiness duration. You can associate stickiness duration for only HTTP/HTTPS load balancer listeners. An application instance must always receive and send two cookies: A cookie that defines the stickiness duration and a special Elastic Load Balancing cookie named AWSELB, that has the mapping to the application instance.

Question 16: Skipped

A user wants to achieve High Availability with PostgreSQL DB. Which of the below mentioned functionalities helps achieve HA?

- Multi AZ (Correct)
- Read Replica
- Multi region
- PostgreSQL does not support HA

Explanation

The Multi AZ feature allows the user to achieve High Availability. For Multi AZ, Amazon RDS automatically provisions and maintains a synchronous "standby" replica in a different Availability Zone.

Question 17: Skipped

A user has created an application which will be hosted on EC2. The application makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK to connect with from the EC2 instance. Which of the below mentioned statements is true with respect to the best practice for security in this scenario?

- The user should create an IAM user with DynamoDB access and use its credentials within the application to connect with DynamoDB
- The user should attach an IAM role with DynamoDB access to the EC2 instance (Correct)
- The user should create an IAM role, which has EC2 access so that it will allow deploying the application
- The user should create an IAM user with DynamoDB and EC2 acces
- Attach the user with the application so that it does not use the root account credentials

Explanation

With AWS IAM a user is creating an application which runs on an EC2 instance and makes requests to AWS, such as DynamoDB or S3 calls. Here it is recommended that the user should not create an IAM user and pass the user's credentials to the application or embed those credentials inside the application. Instead, the user should use roles for EC2 and give that role access to DynamoDB /S3. When the roles are attached to EC2, it will give temporary security credentials to the application hosted on that EC2, to connect with DynamoDB / S3.

Question 18: Skipped

After setting up several database instances in Amazon Relational Database Service (Amazon RDS) you decide that you need to track the performance and health of your databases. How can you do this?

- Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB snapshot, DB parameter group, or DB security group.
- Use the free Amazon CloudWatch service to monitor the performance and health of a DB instance.
- All of the items listed will track the performance and health of a database (Correct)
- View, download, or watch database log files using the Amazon RDS console or Amazon RDS API
- You can also query some database log files that are loaded into database tables.

Explanation

Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizeable capacity for an industry-standard relational database and manages common database administration tasks. There are several ways you can track the performance and health of a database or a DB instance. You can: Use the free Amazon CloudWatch service to monitor the performance and health of a DB instance. Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB snapshot, DB parameter group, or DB security group. View, download, or watch database log files using the Amazon RDS console or Amazon RDS APIs. You can also query some database log files that are loaded into database tables. Use the AWS CloudTrail service to record AWS calls made by your AWS account. The calls are recorded in log files and stored in an Amazon S3 bucket.

Question 19: Skipped

You are building a system to distribute confidential documents to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publically accessible from S3 directly?

- Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
- Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).
- Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI. (Correct)

Explanation

You restrict access to Amazon S3 content by creating an origin access identity, which is a special CloudFront user. You change Amazon S3 permissions to give the origin access identity permission to access your objects, and to remove permissions from everyone else. When your users access your Amazon S3 objects using CloudFront URLs, the CloudFront origin access identity gets the objects on your users' behalf. If your users try to access objects using Amazon S3 URLs, they're denied access. The origin access identity has permission to access objects in your Amazon S3 bucket, but users don't.

Question 20: Skipped

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

- The IP address may be attached to one of the instances
- The IP address belongs to a different zone than the subnet zone
- The user has not created an internet gateway
- The IP addresses belong to EC2 Classic; so they cannot be assigned to VPC (Correct)

Explanation

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

Question 21: Skipped

Select a true statement about Amazon EC2 Security Groups (EC2-Classic).

- After you launch an instance in EC2-Classic, you can't change its security groups. (Correct)
- After you launch an instance in EC2-Classic, you can change its security groups only once.
- After you launch an instance in EC2-Classic, you can only add rules to a security group.
- After you launch an instance in EC2-Classic, you cannot add or remove rules from a security group

Explanation

After you launch an instance in EC2-Classic, you can't change its security groups. However, you can add rules to or remove rules from a security group, and those changes are automatically applied to all instances that are associated with the security group.

Question 22: Skipped

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

- AWS Simple Notification Service
- AWS Simple Queue Service (Correct)
- AWS Elastic Transcoder
- AWS Glacier

Explanation

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

Question 23: Skipped

Which one of the following answers is not a possible state of Amazon CloudWatch Alarm?

- INSUFFICIENT_DATA
- ALARM
- OK
- STATUS_CHECK_FAILED (Correct)

Explanation

Amazon CloudWatch Alarms have three possible states: OK: The metric is within the defined threshold ALARM: The metric is outside of the defined threshold INSUFFICIENT_DATA: The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state

Question 24: Skipped

An accountant asks you to design a small VPC network for him and, due to the nature of his business, just needs something where the workload on the network will be low, and dynamic data will be accessed infrequently. Being an accountant, low cost is also a major factor. Which EBS volume type would best suit his requirements?

- Magnetic (Correct)
- Any, as they all perform the same and cost the same.
- General Purpose (SSD)
- Magnetic or Provisioned IOPS (SSD)

Explanation

You can choose between three EBS volume types to best meet the needs of their workloads: General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic. General Purpose (SSD) is the new, SSD-backed, general purpose EBS volume type that we recommend as the default choice for customers. General Purpose (SSD) volumes are suitable for a broad range of workloads, including small to medium sized databases, development and test environments, and boot volumes. Provisioned IOPS (SSD) volumes offer storage with consistent and low-latency performance, and are designed for I/O intensive applications such as large relational or NoSQL databases. Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types. Magnetic volumes are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.

Question 25: Skipped

Which of the following strategies can be used to control access to your Amazon EC2 instances?

- DB security groups
- IAM policies
- None of these
- EC2 security groups (Correct)

Explanation

IAM policies allow you to specify what actions your IAM users are allowed to perform against your EC2 Instances. However, when it comes to access control, security groups are what you need in order to define and control the way you want your instances to be accessed, and whether or not certain kind of communications are allowed or not.

Question 26: Skipped

A user has launched one EC2 instance in the US East region and one in the US West region. The user has launched an RDS instance in the US East region. How can the user configure access from both the EC2 instances to RDS?

- It is not possible to access RDS of the US East region from the US West region
- Configure the US West region's security group to allow a request from the US East region's instance and configure the RDS security group's ingress rule for the US East EC2 group
- Configure the security group of the US East region to allow traffic from the US West region's instance and configure the RDS security group's ingress rule for the US East EC2 group (Correct)
- Configure the security group of both instances in the ingress rule of the RDS security group

Explanation

The user cannot authorize an Amazon EC2 security group if it is in a different AWS Region than the RDS DB instance. The user can authorize an IP range or specify an Amazon EC2 security group in the same region that refers to an IP address in another region. In this case allow IP of US West inside US East's security group and open the RDS security group for US East region.

Question 27: Skipped

Do you need to shutdown your EC2 instance when you create a snapshot of EBS volumes that serve as root devices?

- Yes,
- No, you only need to shutdown an instance before deleting it (Correct)
- No
- Maybe

Explanation

Yes, to create a snapshot for Amazon EBS volumes that serve as root devices, you should stop the instance before taking the snapshot.

Question 28: Skipped

An organization has a statutory requirement to protect the data at rest for data stored in EBS volumes. Which of the below mentioned options can the organization use to achieve data protection?

- Data replication.
- Data encryption.
- Data snapshot.
- All the options listed her (Correct)

Explanation

For protecting the Amazon EBS data at REST, the user can use options, such as Data Encryption (Windows / Linux / third party based), Data Replication (AWS internally replicates data for redundancy), and Data Snapshot (for point in time backup).

Question 29: Skipped

A client of yours has a huge amount of data stored on Amazon S3, but is concerned about someone stealing it while it is in transit. You know that all data is encrypted in transit on AWS, but which of the following is wrong when describing server-side encryption on AWS?

- Amazon S3 server-side encryption employs strong multi-factor encryption.
- Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data
- In server-side encryption, you manage encryption/decryption of your data, the encryption keys, and related tools. (Correct)
- Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data as it writes it to disks.

Explanation

Amazon S3 encrypts your object before saving it on disks in its data centers and decrypts it when you download the objects. You have two options depending on how you choose to manage the encryption keys: Server-side encryption and client-side encryption. Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. Amazon S3 manages encryption and decryption for you. For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects. In client-side encryption, you manage encryption/decryption of your data, the encryption keys, and related tools. Server-side encryption is an alternative to clientside encryption in which Amazon S3 manages the encryption of your data, freeing you from the tasks of managing encryption and encryption keys. Amazon S3 server-side encryption employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Question 30: Skipped

A user is running a batch process which runs for 1 hour every day. Which of the below mentioned options is the right instance type and costing model in this case if the user performs the same task for the whole year?

- EBS backed instance with on-demand instance pricing (Correct)
- EBS backed instance with heavy utilized reserved instance pricing.
- EBS backed instance with low utilized reserved instance pricing.
- Instance store backed instance with spot instance pricing

Explanation

For Amazon Web Services, the reserved instance helps the user save money if the user is going to run the same instance for a longer period. Generally if the user uses the instances around 30-40% annually it is recommended to use RI. Here as the instance runs only for 1 hour daily it is not recommended to have RI as it will be costlier. The user should use on-demand with EBS in this case.

Question 31: Skipped

You have just set up a large site for a client which involved a huge database which you set up with Amazon RDS to run as a Mu|ti-AZ deployment. You now start to worry about what will happen if the database instance fails. Which statement best describes how this database will function if there is a database failure?

- Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure. (Correct)
- Your database will not resume operation without manual administrative intervention
- Updates to your DB Instance are asynchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure
- Updates to your DB Instance are synchronously replicated across S3 to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure.

Explanation

Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity, while managing time-consuming database administration tasks, freeing you up to focus on your applications and business. When you create or modify your DB Instance to run as a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous "standby" replica in a different Availability Zone. Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB Instance failure. During certain types of planned maintenance, or in the unlikely event of DB Instance failure or Availability Zone failure, Amazon RDS will automatically failover to the standby so that you can resume database writes and reads as soon as the standby is promoted. Since the name record for your DB Instance remains the same, you application can resume database operation without the need for manual administrative intervention. With Mu|ti-AZ deployments, replication is transparent: you do not interact directly with the standby, and it cannot be used to serve read traffic. If you are using Amazon RDS for MySQL and are looking to scale read traffic beyond the capacity constraints of a single DB Instance, you can deploy one or more Read Replicas.

Question 32: Skipped

You are signed in as root user on your account but there is an Amazon S3 bucket under your account that you cannot access. What is a possible reason for this?

- An IAM user assigned a bucket policy to an Amazon S3 bucket and didn't specify the root user as a principal (Correct)
- The S3 bucket is full
- The S3 bucket has reached the maximum number of objects allowed.
- You are in the wrong availability zone

Explanation

With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access. In some cases, you might have an IAM user with full access to IAM and Amazon S3. If the IAM user assigns a bucket policy to an Amazon S3 bucket and doesn't specify the root user as a principal, the root user is denied access to that bucket. However, as the root user, you can still access the bucket by modifying the bucket policy to allow root user access.

Question 33: Skipped

A user is observing the EC2 CPU utilization metric on CloudWatch. The user has observed some interesting patterns while filtering over the 1 week period for a particular hour. The user wants to zoom that data point to a more granular period. How can the user do that easily with CloudWatch?

- The user can zoom a particular period by selecting that period with the mouse and then releasing the mouse (Correct)
- The user can zoom a particular period by specifying the aggregation data for that period
- The user can zoom a particular period by double clicking on that period with the mouse
- The user can zoom a particular period by specifying the period in the Time Range

Explanation

Amazon CloudWatch provides the functionality to graph the metric data generated either by the AWS services or the custom metric to make it easier for the user to analyse. The AWS CloudWatch console provides the option to change the granularity of a graph and zoom in to see data over a shorter time period. To zoom, the user has to click in the graph details pane, drag on the graph area for selection, and then release the mouse button.

Question 34: Skipped

A scope has been handed to you to set up a super fast gaming server and you decide that you will use Amazon DynamoDB as your database. For efficient access to data in a table, Amazon DynamoDB creates and maintains indexes for the primary key attributes. A secondary index is a data structure that contains a subset of attributes from a table, along with an alternate key to support Query operations. How many types of secondary indexes does DynamoDB support?

- 2 (Correct)
- 16
- 4
- As many as you need

Explanation

DynamoDB supports two types of secondary indexes: Local secondary index — an index that has the same hash key as the table, but a different range key. A local secondary index is "local" in the sense that every partition of a local secondary index is scoped to a table partition that has the same hash key. Global secondary index — an index with a hash and range key that can be different from those on the table. A global secondary index is considered "global" because queries on the index can span all of the data in a table, across all partitions.

Question 35: Skipped

Select the correct statement: Within Amazon EC2, when using Linux instances, the device name /dev/sda1 is .

- reserved for EBS volumes
- recommended for EBS volumes
- recommended for instance store volumes
- reserved for the root device (Correct)

Explanation

Within Amazon EC2, when using a Linux instance, the device name /dev/sda1 is reserved for the root device.

Question 36: Skipped

The common use cases for DynamoDB Fine-Grained Access Control (FGAC) are cases in which the end user wants

- to change the hash keys of the table directly
- to check if an IAM policy requires the hash keys of the tables directly
- to read or modify any codecommit key of the table directly, without a middle-tier service
- to read or modify the table directly, without a middle-tier service (Correct)

Explanation

FGAC can benefit any application that tracks information in a DynamoDB table, where the end user (or application client acting on behalf of an end user) wants to read or modify the table directly, without a middle-tier service. For instance, a developer of a mobile app named Acme can use FGAC to track the top score of every Acme user in a DynamoDB table. FGAC allows the application client to modify only the top score for the user that is currently running the application.

Question 37: Skipped

A user has set up the CloudWatch alarm on the CPU utilization metric at 50%, with a time interval of 5 minutes and 10 periods to monitor. What will be the state of the alarm at the end of 90 minutes, if the CPU utilization is constant at 80%?

- ALERT
- ALARM (Correct)
- OK
- INSUFFICIENT_DATA

Explanation

In this case the alarm watches a metric every 5 minutes for 10 intervals. Thus, it needs at least 50 minutes to come to the "OK" state. Till then it will be in the |NSUFFUCIENT_DATA state. Since 90 minutes have passed and CPU utilization is at 80% constant, the state of alarm will be "ALARNI".

Question 38: Skipped

You need to set up security for your VPC and you know that Amazon VPC provides two features that you can use to increase security for your VPC: security groups and network access control lists (ACLs). You have already looked into security groups and you are now trying to understand ACLs. Which statement below is incorrect in relation to ACLs?

- Supports allow rules and deny rules.
- Is stateful: Return traffic is automatically allowed, regardless of any rules. (Correct)
- Processes rules in number order when deciding whether to allow traffic.
- Operates at the subnet level (second layer of defense).

Explanation

Amazon VPC provides two features that you can use to increase security for your VPC: Security groups—Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance levelNetwork access control lists (ACLs)—Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level Security groups are stateful: (Return traffic is automatically allowed, regardless of any rules) Network ACLs are stateless: (Return traffic must be explicitly allowed by rules)

Question 39: Skipped

You need to create an Amazon Machine Image (AM) for a customer for an application which does not appear to be part of the standard AWS AM template that you can see in the AWS console. What are the alternative possibilities for creating an AM on AWS?

- You can purchase an AMs from a third party but cannot create your own AM.
- You can purchase an AMIs from a third party or can create your own AMI. (Correct)
- Only AWS can create AMIs and you need to wait till it becomes available.
- Only AWS can create AMIs and you need to request them to create one for you

Explanation

You can purchase an AMIs from a third party, including AMIs that come with service contracts from organizations such as Red Hat. You can also create an AMI and sell it to other Amazon EC2 users. After you create an AMI, you can keep it private so that only you can use it, or you can share it with a specified list of AWS accounts. You can also make your custom AMI public so that the community can use it. Building a safe, secure, usable AMI for public consumption is a fairly straightforward process, if you follow a few simple guidelines.

Question 40: Skipped

Which one of the below is not an AWS Storage Service?

- Amazon S3
- Amazon Glacier
- Amazon CloudFront (Correct)
- Amazon EBS

Explanation

AWS Storage Services are: Amazon S3 Amazon Glacier Amazon EBS AWS Storage Gateway

Question 41: Skipped

You are very concerned about security on your network because you have multiple programmers testing APIs and SDKs and you have no idea what is happening. You think C|oudTrai| may help but are not sure what it does. Which of the following statements best describes the AWS service CloudTrail?

- With AWS CloudTrail you can get a history of AWS API calls and related events for your account. (Correct)
- With AWS CloudTrail you can get a history of IAM users for your account.
- With AWS CloudTrail you can get a history of S3 logfiles for your account.
- With AWS CloudTrail you can get a history of CloudFormation JSON scripts used for your account

Explanation

With AWS CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS IV|anagement Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can identify which users and accounts called AWS for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of your trails, and control how administrators turn CloudTrail logging on and off.

Question 42: Skipped

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

- AWS SES
- AWS SNS (Correct)
- None because the user infrastructure is in the private cloud.
- AWS SMS

Explanation

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

Question 43: Skipped

Regarding Amazon Route 53, if your application is running on Amazon EC2 instances in two or more Amazon EC2 regions and if you have more than one Amazon EC2 instance in one or more regions, you can use to route traffic to the correct region and then use to route traffic to instances within the region, based on probabilities that you specify.

- weighted-based routing; alias resource record sets
- latency-based routing; weighted resource record sets (Correct)
- weighted-based routing; weighted resource record sets
- latency-based routing; alias resource record sets

Explanation

Regarding Amazon Route 53, if your application is running on Amazon EC2 instances in two or more Amazon EC2 regions, and if you have more than one Amazon EC2 instance in one or more regions, you can use latency-based routing to route traffic to the correct region and then use weighted resource record sets to route traffic to instances within the region based on weights that you specify.

Question 44: Skipped

You have a lot of data stored in the AWS Storage Gateway and your manager has come to you asking about how the billing is calculated, specifically the Virtual Tape Shelf usage. What would be a correct response to this?

- You are billed for the virtual tape data you store in Amazon Glacier and are billed for the size of the virtual tape.
- You are billed for the virtual tape data you store in Amazon Glacier and billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape. (Correct)
- You are billed for the virtual tape data you store in Amazon S3 and billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape
- You are billed for the virtual tape data you store in Amazon S3 and are billed for the size of the virtual tape.

Explanation

The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. AWS Storage Gateway billing is as follows. Volume storage usage (per GB per month): You are billed for the Cached volume data you store in Amazon S3. You are only billed for volume capacity you use, not for the size of the volume you create. Snapshot Storage usage (per GB per month): You are billed for the snapshots your gateway stores in Amazon S3. These snapshots are stored and billed as Amazon EBS snapshots. Snapshots are incremental backups, reducing your storage charges. When taking a new snapshot, only the data that has changed since your last snapshot is stored. Virtual Tape Library usage (per GB per month): You are billed for the virtual tape data you store in Amazon S3. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape. Virtual Tape Shelf usage (per GB per month): You are billed for the virtual tape data you store in Amazon Glacier. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.

Question 45: Skipped

You are configuring a new VPC for one of your clients for a cloud migration project, and only a public VPN will be in place. After you created your VPC, you created a new subnet, a new internet gateway, and attached your internet gateway to your VPC. When you launched your first instance into your VPC, you realized that you aren't able to connect to the instance, even if it is configured with an elastic IP. What should be done to access the instance?

- A route should be created as 0.0.0.0/0 and your internet gateway as target. (Correct)
- Attach another ENI to the instance and connect via new ENI.
- A NAT instance should be created and all traffic should be forwarded to NAT instance.
- A NACL should be created that allows all outbound traffic

Explanation

All traffic should be routed via Internet Gateway. So, a route should be created with 0.0.0.0/0 as a source, and your Internet Gateway as your target.