Answer Sheet

Q1) Which of the following S3 storage classes is ideal for data with unpredictable access patterns?

● Amazon S3 Glacier
● Amazon S3 Standard
● Amazon S3 Standard-Infrequent Access
✓ Amazon S3 Intelligent-Tiering

Explanation:-The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, Amazon S3 monitors access patterns of the objects in S3 Intelligent-Tiering, and moves the ones that have not been accessed for 30 consecutive days to the infrequent access tier. If an object in the infrequent access tier is accessed, it is automatically moved back to the frequent access tier. There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers. It is the ideal storage class for long-lived data with access patterns that are unknown or unpredictable.

Q2) Which of the following is not a benefit of Amazon S3? (Choose TWO)

● Amazon S3 stores any number of objects, but with object size limits
● Amazon S3 provides 99.999999999% (11 9's) of data durability
● Amazon S3 provides unlimited storage for any type of data
✓ Amazon S3 can be scaled manually to store and retrieve any amount of data from anywhere

Explanation:-"Amazon S3 can be scaled manually to store and retrieve any amount of data from anywhere" is not a benefit of S3 and thus is a correct answer. Amazon S3 scales automatically to store and retrieve any amount of data from anywhere.

✓ Amazon S3 can run any type of application or backend system

Explanation:-"Amazon S3 can run any type of application or backend system" is not a benefit of S3 and thus is a correct answer. Amazon S3 is a storage service not a compute service.

Q3) Which service provides object-level storage in AWS?

● Amazon Instance Store
● Amazon EFS
✓ Amazon S3

Explanation:-Amazon S3 is an object level storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry.

● Amazon EBS

Q4)

The identification process of an online financial services company requires that new users must complete an online interview with their security team. After verifying users' identities, the recorded interviews are only required in the event of a legal issue or a regulatory compliance breach.

What is the most cost-effective service to store the recorded videos?

● AWS Marketplace
● S3 Intelligent-Tiering
✓ Amazon Glacier

Explanation:-Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for long-term data backup and archival. With Amazon Glacier, customers can reliably store their data for as little as $0.004 per gigabyte per month. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so that they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations.

● Amazon EBS

Q5) Which of the following procedures will help reduce your Amazon S3 costs?

● Pick the right Availability Zone for your S3 bucket
● Use the Import/Export feature to move old files automatically to Amazon Glacier
✓ Use the right combination of storage classes based on different use cases

Explanation:-Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation.

● Move all the data stored in S3 standard to EBS

Q6) What is the AWS service\feature that takes advantage of Amazon CloudFront's globally distributed edge locations to transfer files to S3 with higher upload speeds?

● AWS WAF
✓ S3 Transfer Acceleration

Explanation:-Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFrontâ€™s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

● AWS Snowmobile
● AWS Snowball

Q7) Where can you store files in AWS? (Choose two)

● Amazon EMR

✓ Amazon EBS

Explanation:-** Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It is easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily. Amazon EFS is built to elastically scale on demand without disrupting applications, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it. It is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS that scale as a file system grows, with consistent low latencies. As a regional service, Amazon EFS is designed for high availability and durability storing data redundantly across multiple Availability Zones.

** 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 EFS

Explanation:-** Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It is easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily. Amazon EFS is built to elastically scale on demand without disrupting applications, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it. It is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS that scale as a file system grows, with consistent low latencies. As a regional service, Amazon EFS is designed for high availability and durability storing data redundantly across multiple Availability Zones.

** 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 ECS

● Amazon SNS

Q8) What is the primary storage service used by Amazon RDS DB instances?

● Amazon S3

✓ Amazon EBS

Explanation:-DB instances for Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server use Amazon Elastic Block Store (Amazon EBS) volumes for database and log storage.

Additional information:

EBS volumes are performant for your most demanding workloads, including mission-critical applications such as SAP, Oracle, and Microsoft products. Amazon EBS scales with your performance needs, whether you are supporting millions of gaming customers or billions of e-commerce transactions. A broad range of workloads, such as relational databases (including Amazon RDS databases) and non-relational databases (including Cassandra and MongoDB), enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.

● Amazon Glacier

● Amazon EFS

Q9) Your company is designing a new application that will store and retrieve photos and videos. Which of the following services should you recommend to be used as the underlying storage mechanism?

✓ Amazon S3

Explanation:-Amazon S3 is object storage built to store and retrieve any amount of data from anywhere on the Internet. Itâ€™s a simple storage service that offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs. Amazon S3 can be used to

Common use cases of Amazon S3 include:

Media Hosting â€“ Build a redundant, scalable, and highly available infrastructure that hosts video, photo, or music uploads and downloads.

Backup and Storage â€“ Provide data backup and storage services for others.

Hosting static websites â€“ Host and manage static websites quickly and easily.

Deliver content globally - Use S3 in conjunction with CloudFront to distribute content globally with low latency.

Hybrid cloud storage - Create a seamless connection between on-premises applications and Amazon S3 with AWS Storage Gateway in order to reduce your data center footprint, and leverage the scale, reliability, and durability of AWS.

● Amazon Instance store

● Amazon EBS

● Amazon SQS

Q10) How much data can you store in S3?

✓ Storage capacity is virtually unlimited

Explanation:-The total volume of data and number of objects you can store are unlimited.

● You can store up to 1 PetaByte of data, then you are required to pay an additional fee

● You can store up to 1 PetaByte of data

● There is a soft limit of 100 TeraBytes for each AWS account

Q11) Amazon Glacier is an Amazon S3 storage class that is suitable for storing ____________ & _____________. (Choose two)

● Dynamic websitesâ€™ assets

● Cached data

✓ Active archives

Explanation:-Amazon S3 Glacier provides three retrieval options to fit your use case. Expedited retrievals typically return data in 1-5 minutes, and are best used for Active Archive use cases. Standard retrievals typically complete between 3-5 hours work, and work well for less time-sensitive needs like backup data, media editing, or long-term analytics. Bulk retrievals are the lowest-cost retrieval option, returning large amounts of data within 5-12 hours.

● Active databases

✓ Long-term analytic data

Explanation:-Amazon S3 Glacier provides three retrieval options to fit your use case. Expedited retrievals typically return data in 1-5 minutes, and are best used for Active Archive use cases. Standard retrievals typically complete between 3-5 hours work, and work well for less time-sensitive needs like backup data, media editing, or long-term analytics. Bulk retrievals are the lowest-cost retrieval option, returning large amounts of data within 5-12 hours.

Q12) A company is planning to migrate a database with high read/write activity to AWS. What is the best storage option to use?

● AWS Storage Gateway

✓ Amazon EBS

Explanation:-Databases require high read \ write performance and as such Amazon EBS is the correct answer. Amazon EBS volumes offer consistent and low-latency performance compared to other storage options. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application.

● Amazon S3

● Amazon Glacier

Q13) What are the benefits of having infrastructure hosted in AWS? (Choose two)

● There is no need to worry about security

✓ Increase speed and agility

Explanation:-All of the physical security are taken care of for you. Amazon data centers are surrounded by three physical layers of security. “Nothing can go in or out without setting off an alarm”. It’s important to keep bad guys out, but equally important to keep the data in which is why Amazon monitors incoming gear, tracking every disk that enters the facility. And “if it breaks we don’t return the disk for warranty. The only way a disk leaves our data center is when it’s confetti.”

Most (not all) data and network security are taken care of for you. When we talk about the data/network security, AWS has a “shared responsibility model” where AWS and the customer share the responsibility of securing them. For example the customer is responsible for creating rules to secure his network traffic using the security groups and is also responsible for protecting data with encryption.

"Increase speed and agility" is also a correct answer because in a cloud computing environment, new IT resources are only a click away, which means it requires less time to make those resources available to developers - from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

● Competitive upfront costs

✓ All of the physical security and most of the data/network security are taken care of for you

Explanation:-All of the physical security are taken care of for you. Amazon data centers are surrounded by three physical layers of security. “Nothing can go in or out without setting off an alarm”. It’s important to keep bad guys out, but equally important to keep the data in which is why Amazon monitors incoming gear, tracking every disk that enters the facility. And “if it breaks we don’t return the disk for warranty. The only way a disk leaves our data center is when it’s confetti.”

Most (not all) data and network security are taken care of for you. When we talk about the data/network security, AWS has a “shared responsibility model” where AWS and the customer share the responsibility of securing them. For example the customer is responsible for creating rules to secure his network traffic using the security groups and is also responsible for protecting data with encryption.

"Increase speed and agility" is also a correct answer because in a cloud computing environment, new IT resources are only a click away, which means it requires less time to make those resources available to developers - from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

● Gaining complete control over the physical infrastructure

Q14) Which of the below options are related to the reliability of AWS? (Choose two)

● Applying the principle of least privilege to all of its resources

● All AWS services are considered Global Services, and this design helps customers serve their international users

✓ Ability to recover quickly from failures

Explanation:-The reliability term encompasses the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. The automatic provisioning of resources and the ability to recover from failures meet these criteria.

● Providing compensation to customers if issues occur

✓ Automatically provisioning new resources to meet demand

Explanation:-The reliability term encompasses the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. The automatic provisioning of resources and the ability to recover from failures meet these criteria.

Q15)

Your application has recently experienced significant global growth, and international users are complaining of high latency.

What is the AWS characteristic that can help improve your international users experience?

● Elasticity

● Data durability

● High availability

✓ Global reach

Explanation:-With AWS, you can deploy your application in multiple regions around the world. The user will be redirected to the Region that provides the lowest possible latency and the highest performance. You can also use the CloudFront service that uses edge locations (which are located in most of the major cities across the world) to deliver content with low latency and high performance to your global users.

Q16) What are two advantages of using Cloud Computing over using traditional data centers? (Choose two)

● Reserved Compute capacity

● Virtualized compute resources

✓ Eliminating Single Points of Failure (SPOFs)

Explanation:-These are things that traditional web hosting cannot provide:
**High-availability (eliminating single points of failure): A system is highly available when it can withstand the failure of an individual component or multiple components, such as hard disks, servers, and network links. The best way to understand and avoid the single point of failure is to begin by making a list of all major points of your architecture. You need to break the points down and understand them further. Then, review each of these points and think what would happen if any of these failed. AWS gives you the opportunity to automate recovery and reduce disruption at every layer of your architecture.
**Distributed infrastructure: The AWS Cloud operates in over 60 Availability Zones within over 20 geographic Regions around the world, with announced plans for more Availability Zones and Regions, allowing you to reduce latency to users from all around the world.
**On-demand infrastructure for scaling applications or tasks: AWS allows you to provision the required resources for your application in minutes and also allows you to stop them when you donâ€™t need them.
**Cost savings: You don't have to run your own data center for internal or private servers, so your IT department doesn't have to make bulk purchases of servers which may never get used, or may be inadequate. The â€œpay as you goâ€ model from AWS allows you to pay only for what you use and the ability to scale down to avoid over-spending. With AWS you don't have to pay an entire IT department to maintain that hardware -- you don't even have to pay an accountant to figure out how much hardware you can afford or how much you need to purchase.

✓ Distributed infrastructure

Explanation:-These are things that traditional web hosting cannot provide:
**High-availability (eliminating single points of failure): A system is highly available when it can withstand the failure of an individual component or multiple components, such as hard disks, servers, and network links. The best way to understand and avoid the single point of failure is to begin by making a list of all major points of your architecture. You need to break the points down and understand them further. Then, review each of these points and think what would happen if any of these failed. AWS gives you the opportunity to automate recovery and reduce disruption at every layer of your architecture.
**Distributed infrastructure: The AWS Cloud operates in over 60 Availability Zones within over 20 geographic Regions around the world, with announced plans for more Availability Zones and Regions, allowing you to reduce latency to users from all around the world.
**On-demand infrastructure for scaling applications or tasks: AWS allows you to provision the required resources for your application in minutes and also allows you to stop them when you donâ€™t need them.
**Cost savings: You don't have to run your own data center for internal or private servers, so your IT department doesn't have to make bulk purchases of servers which may never get used, or may be inadequate. The â€œpay as you goâ€ model from AWS allows you to pay only for what you use and the ability to scale down to avoid over-spending. With AWS you don't have to pay an entire IT department to maintain that hardware -- you don't even have to pay an accountant to figure out how much hardware you can afford or how much you need to purchase.

● Dedicated hosting

Q17) Why would an organization decide to use AWS over an on-premises data center? (Choose two)

● Free commercial software licenses

● Free technical support

● On-site visits for auditing

✓ Elastic resources

Explanation:-AWS continues to lower the cost of cloud computing for its customers. AWS recently lowered prices again for compute, storage, caching, and database services for all customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO gap with traditional infrastructure.
Elasticity is a system’s ability to monitor user demand and automatically increase and decrease deployed resources accordingly. Elasticity is one of the most important advantages of AWS. The purpose of elasticity is to match the resources allocated with actual amount of resources needed at any given point in time. This ensures that you are only paying for the resources you actually need.

✓ Cost Savings

Explanation:-AWS continues to lower the cost of cloud computing for its customers. AWS recently lowered prices again for compute, storage, caching, and database services for all customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO gap with traditional infrastructure.
Elasticity is a system’s ability to monitor user demand and automatically increase and decrease deployed resources accordingly. Elasticity is one of the most important advantages of AWS. The purpose of elasticity is to match the resources allocated with actual amount of resources needed at any given point in time. This ensures that you are only paying for the resources you actually need.

Q18) Which statement best describes AWS?

✓ AWS is a cloud services provider

Explanation:-Amazon Web Services offers reliable, scalable, and inexpensive cloud computing services.

● AWS is a hosting services provider

● AWS is a networking services provider

● AWS is a security services provider

Q19) Which of the following statements describes the AWS Cloud’s agility?

● AWS allows you to pay upfront to reduce costs

● AWS allows you to host your applications in multiple regions around the world

✓ AWS allows you to provision resources in minutes

Explanation:-In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks (or months in some cases) to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.
In other words, instead of waiting weeks or months for hardware, you can instantly deploy new applications. Also, whether you need one virtual server or thousands, whether you need them for a few hours or 24/7, you still only pay for what you use.

● AWS provides customizable hardware at the lowest possible cost

Q20) The TCO gap between AWS infrastructure and traditional infrastructure has widened over the recent years. Which of the following could be the reason for that?

● AWS helps customers invest more in capital expenditures
● AWS secures AWS resources at no additional charge
✓ AWS continues to lower the cost of cloud computing for its customers
Explanation:-AWS continues to lower the cost of cloud computing for its customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO (Total Cost of Ownership) gap with traditional infrastructure. Since 2014, AWS has reduced the cost of compute by an average of 30%, storage by an average of 51% and relational databases by an average of 28%.
● AWS automates all infrastructure operations, so customers save more on human resources costs

---

Q21) Which of the following are advantages of using AWS as a cloud computing provider? (Choose two)

● Provides custom hardware to meet any specification
✓ Enables customers to trade their capital expenses for operational expenses
Explanation:-Advantages of Cloud Computing include: (IMPORTANT)
1- Trade capital for variable expense: Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can only pay when you consume computing resources, and only pay for how much you consume. By using AWS, infrastructure costs are converted to a pay-as-you-go model, where customers are charged for the resources that they consume, and those costs are incurred as operating costs instead of as capital expenditures.
2- Benefit from massive economies of scale: By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers are aggregated in the cloud, providers such as Amazon Web Services can achieve higher economies of scale which translates into lower pay as you go prices.
3- Stop guessing capacity: Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little as you need, and scale up and down as required with only a few minutes notice.
4- Increase speed and agility: In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.
5- Stop spending money on running and maintaining data centers: Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking and powering servers.
6- Go global in minutes: Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide a lower latency and better experience for your customers simply and at minimal cost.
✓ Eliminates the need to guess on infrastructure capacity needs
Explanation:-Advantages of Cloud Computing include: (IMPORTANT)
1- Trade capital for variable expense: Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can only pay when you consume computing resources, and only pay for how much you consume. By using AWS, infrastructure costs are converted to a pay-as-you-go model, where customers are charged for the resources that they consume, and those costs are incurred as operating costs instead of as capital expenditures.
2- Benefit from massive economies of scale: By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers are aggregated in the cloud, providers such as Amazon Web Services can achieve higher economies of scale which translates into lower pay as you go prices.
3- Stop guessing capacity: Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little as you need, and scale up and down as required with only a few minutes notice.
4- Increase speed and agility: In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.
5- Stop spending money on running and maintaining data centers: Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking and powering servers.
6- Go global in minutes: Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide a lower latency and better experience for your customers simply and at minimal cost.
● Eliminates the need to monitor servers and applications
● Manages all the compliance and auditing tasks

Q22)

Amazon EC2 instances are conceptually very similar to traditional servers. However, using Amazon EC2 server instances in the same manner as traditional hardware server instances is only a starting point.

What are the main benefits of using the AWS EC2 instances instead of traditional servers? (Choose two)

● Provides automatic data backups
● Provides your business with a seamless remote accessibility
● Prevents unauthorized users from getting into your network
✓ Improves Fault-Tolerance
Explanation:-"Improves Fault-Tolerance" is a correct answer. AWS has unique set of services that you can use to build fault-tolerant applications in the cloud. For example you can get improved fault tolerance by placing your compute instances behind an Elastic Load Balancer, as it can automatically balance traffic across multiple instances and multiple Availability Zones and ensure that only healthy Amazon EC2 instances receive traffic.
ou can setup an Elastic Load Balancer to balance incoming application traffic across Amazon EC2 instances in a single Availability Zone or multiple Availability Zones. Elastic Load Balancing can detect the health of Amazon EC2 instances. When it detects unhealthy Amazon EC2 instances, it no longer routes traffic to those unhealthy instances. Instead, it spreads the load across the remaining healthy instances. If all of your Amazon EC2 instances in a particular Availability Zone are unhealthy, but you have set up instances in multiple Availability Zones, Elastic Load Balancing will route traffic to your healthy Amazon EC2 instances in those other zones. It will resume load balancing to the original Amazon EC2 instances when they have been restored to a healthy state.
Also, using Auto Scaling enables you to greatly reduce the amount of time and resources you need to monitor your servers –if a failure occurs, a replacement will be automatically launched for you. Diagnosing an unhealthy server can be as simple as terminating it and letting Auto Scaling launch a new one for you.
✓ Can be scaled manually in a shorter period of time
Explanation:-"Improves Fault-Tolerance" is a correct answer. AWS has unique set of services that you can use to build fault-tolerant applications in the cloud. For example you can get improved fault tolerance by placing your compute instances behind an Elastic Load Balancer, as it can

automatically balance traffic across multiple instances and multiple Availability Zones and ensure that only healthy Amazon EC2 instances receive traffic.
ou can setup an Elastic Load Balancer to balance incoming application traffic across Amazon EC2 instances in a single Availability Zone or multiple Availability Zones. Elastic Load Balancing can detect the health of Amazon EC2 instances. When it detects unhealthy Amazon EC2 instances, it no longer routes traffic to those unhealthy instances. Instead, it spreads the load across the remaining healthy instances. If all of your Amazon EC2 instances in a particular Availability Zone are unhealthy, but you have set up instances in multiple Availability Zones, Elastic Load Balancing will route traffic to your healthy Amazon EC2 instances in those other zones. It will resume load balancing to the original Amazon EC2 instances when they have been restored to a healthy state.
Also, using Auto Scaling enables you to greatly reduce the amount of time and resources you need to monitor your servers –if a failure occurs, a replacement will be automatically launched for you. Diagnosing an unhealthy server can be as simple as terminating it and letting Auto Scaling launch a new one for you.

Q23) A company has a large amount of data to be archived. What is the most cost-effective AWS storage service to use?

● Amazon S3 Standard
● Amazon EFS
✓ Amazon Glacier
Explanation:-Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provides comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.
● Amazon EBS

Q24)

A global company with a large number of AWS accounts is seeking a way in which they can centrally manage billing and security policies across all accounts.

Which AWS Service will assist them in meeting these goals?

● AWS Trusted Advisor
● IAM Groups
● AWS Config
✓ AWS Organizations
Explanation:-AWS Organizations helps customers centrally govern their environments as they grow and scale their workloads on AWS. Whether customers are a growing startup or a large enterprise, Organizations helps them to centrally manage billing; control access, compliance, and security; and share resources across their AWS accounts.
AWS Organizations has five main benefits:
1) Centrally manage access polices across multiple AWS accounts.
2) Automate AWS account creation and management.
3) Control access to AWS services.
4) Consolidate billing across multiple AWS accounts.
5) Configure AWS services across multiple accounts.

Q25) Which of the following is an example of horizontal scaling in the AWS Cloud?

● Adding more RAM capacity to an EC2 instance
● Replacing an existing EC2 instance with a larger, more powerful one
● Increasing the computing capacity of a single EC2 instance to address the growing demands of an application
✓ Adding more EC2 instances to handle an increase in traffic
Explanation:-Horizontal Scaling:
Scaling horizontally takes place through an increase in the number of resources (e.g., adding more hard drives to a storage array or adding more servers to support an application). This is a great way to build Internet-scale applications that leverage the elasticity of cloud computing.
Vertical Scaling:
Scaling vertically takes place through an increase in the specifications of an individual resource (e.g., upgrading a server with a larger hard drive, adding more memory, or provisioning a faster CPU). On Amazon EC2, this can easily be achieved by stopping an instance and resizing it to an instance type that has more RAM, CPU, I/O,or networking capabilities. This way of scaling can eventually hit a limit and it is not always a cost efficient or highly available approach. However, it is very easy to implement and can be sufficient for many use cases especially as a short term solution.
Additional information:
Vertical-scaling is often limited to the capacity constraints of a single machine, scaling beyond that capacity often involves downtime and comes with an upper limit. With horizontal-scaling it is often easier to scale dynamically by adding more machines in parallel. Hence, in most cases, horizontal-scaling is recommended over vertical-scaling.

Q26) What does the "Principle of Least Privilege" refer to?

● IAM users should not be granted any permissions; to keep your account safe
● All IAM users should have at least the necessary permissions to access the core AWS services
✓ You should grant your users only the permissions they need when they need them and nothing more
Explanation:-The principle of least privilege is one of the most important security practices and it means granting users the required permissions to perform the tasks entrusted to them and nothing more. The security administrator determines what tasks users need to perform and then attaches the policies that allow them to perform only those tasks. You should start with a minimum set of permissions and grant additional permissions when necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them down.
● All trusted IAM users should have access to any AWS service in the respective AWS account

---

Q27) Which of the following services can help protect your web applications from SQL injection and other vulnerabilities in your application code?

● AWS IAM

● Amazon Aurora

✓ AWS WAF

Explanation:-AWS WAF (Web Application Firewall) helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.

● Amazon Cognito

Q28) Which of the following can help protect your EC2 instances from DDoS attacks? (Choose two)

● AWS IAM

● AWS Batch

✓ Network Access Control Lists

Explanation:-A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. A Network Access Control List (NACL) acts as a firewall for controlling traffic in and out of one or more subnets. Therefore, if they are configured properly, they can protect your instances from DDoS attacks.

Additional information:

AWS does not configure security groups or NACLs to protect you from DDoS attacks. It is the responsibility of the customer to set the appropriate NACL and security group rules to protect from these attacks and secure their network.

In addition to Security Groups and NACLs, AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures that follow AWS Best Practices for DDoS Resiliency. These include services such as Amazon Route 53, Amazon CloudFront, Elastic Load Balancing, and AWS WAF to control and absorb traffic, and deflect unwanted requests. These services integrate with AWS Shield, a managed DDoS protection service that provides always-on detection and automatic inline mitigations to safeguard web applications running on AWS.

● AWS CloudHSM

✓ Security Groups

Explanation:-A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. A Network Access Control List (NACL) acts as a firewall for controlling traffic in and out of one or more subnets. Therefore, if they are configured properly, they can protect your instances from DDoS attacks.

Additional information:

AWS does not configure security groups or NACLs to protect you from DDoS attacks. It is the responsibility of the customer to set the appropriate NACL and security group rules to protect from these attacks and secure their network.

In addition to Security Groups and NACLs, AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures that follow AWS Best Practices for DDoS Resiliency. These include services such as Amazon Route 53, Amazon CloudFront, Elastic Load Balancing, and AWS WAF to control and absorb traffic, and deflect unwanted requests. These services integrate with AWS Shield, a managed DDoS protection service that provides always-on detection and automatic inline mitigations to safeguard web applications running on AWS.

Q29) Which IAM entity can best be used to grant temporary access to your AWS resources?

● Key Pair

● IAM Groups

✓ IAM Roles

Explanation:-An IAM role is an IAM entity that defines a set of permissions for making AWS service requests. IAM roles are not associated with a specific user or group. Instead, trusted entities assume roles, such as IAM users, applications, or AWS services such as EC2. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app. Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources. For these scenarios, you can delegate temporary access to AWS resources using an IAM role.

● IAM Users

Q30) Hundreds of thousands of DDoS attacks are recorded every month worldwide. What does AWS provide to protect from these attacks? (Choose two)

● AWS Config

✓ AWS WAF

Explanation:-AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures that follow AWS Best Practices for DDoS Resiliency. These include services such as Amazon Route 53, Amazon CloudFront, Elastic Load Balancing, and AWS WAF to control and absorb traffic, and deflect unwanted requests. These services integrate with AWS Shield, a managed DDoS protection service that provides always-on detection and automatic inline mitigations to safeguard web applications running on AWS.

✓ AWS Shield

Explanation:-AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures that follow AWS Best Practices for DDoS Resiliency. These include services such as Amazon Route 53, Amazon CloudFront, Elastic Load Balancing, and AWS WAF to control and absorb traffic, and deflect unwanted requests. These services integrate with AWS Shield, a managed DDoS protection service that provides always-on detection and automatic inline mitigations to safeguard web applications running on AWS.

● Amazon Cognito

● AWS KMS

Q31) What is the AWS feature that provides an additional level of security above the default authentication mechanism of usernames and passwords?

● AWS KMS

✓ AWS MFA

Explanation:-AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of using just your user name and password to authenticate.

● Email verification

● Encrypted keys

Q32)

An organization has a large number of technical employees who operate their AWS Cloud infrastructure.

What does AWS provide to help organize them in teams and then assign the appropriate permissions for each team?

● IAM users

✓ IAM Groups

Explanation:-An IAM group is a collection of IAM users that are managed as a unit. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a group called Admins and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old groups and add him or her to the appropriate new groups.

● AWS Organizations

● IAM roles

Q33) Which of the following services allows customers to manage their agreements with AWS?

● AWS Organizations

✓ AWS Artifact

Explanation:-AWS Artifact is a self-service audit artifact retrieval portal that provides customers with on-demand access to AWS' compliance documentation and AWS agreements. You can use AWS Artifact Agreements to review, accept, and track the status of AWS agreements such as the Business Associate Addendum (BAA).

Additional information:

You can also use AWS Artifact Reports to download AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC) reports.

● AWS Certificate Manager

● AWS Systems Manager

Q34) A company has moved to AWS recently. Which of the following would help them ensure that the right security settings are put in place? (Choose two)

● Concierge Support Team

● Amazon SNS

● Amazon CloudWatch

✓ AWS Trusted Advisor

Explanation:-AWS Trusted Advisor offers a rich set of best practice checks and recommendations across five categories: cost optimization; security; fault tolerance; performance; and service limits. Like your customized cloud security expert, AWS Trusted Advisor analyzes your AWS environment and provides security recommendations to protect your AWS environment. The service improves the security of your applications by closing gaps, examining permissions, and enabling various AWS security features.

✓ Amazon Inspector

Explanation:-Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of a detailed assessment report which is available via the Amazon Inspector console or API. To help get started quickly, Amazon Inspector includes a knowledge base of hundreds of rules mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking for remote root login being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers.

Q35) Which of the following must an IAM user provide to interact with AWS services using the AWS Command Line Interface (AWS CLI)?

● User ID

✓ Access keys

Explanation:-Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests to AWS using the CLI or the SDK.

● User name and password

● Secret token

Q36) What are the default security credentials that are required to access the AWS management console for an IAM user account?

● MFA

● Security tokens

✓ A user name and password

Explanation:-The AWS Management Console allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface. You can only access the AWS management console if you have a valid user name and password.

● Access keys

Q37) What is the AWS service that enables you to manage all of your AWS accounts from a single master account?

● Amazon Config

✓ AWS Organizations

Explanation:-AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

AWS Organizations enables the following capabilities:

1- Automate AWS account creation and management

2- Consolidate billing across multiple AWS accounts

3- Govern access to AWS services, resources, and regions

4- Centrally manage access policies across multiple AWS accounts

5- Configure AWS services across multiple accounts

● AWS Trusted Advisor

● AWS WAF

Q38) An organization runs many systems and uses many AWS products. Which of the following services enables them to control how each developer interacts with these products?

● Network Access Control Lists

● Amazon RDS

✓ AWS Identity and Access Management

Explanation:-AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

● Amazon EMR

Q39) Which of the following is one of the benefits of AWS security?

● Starts automatically once you upload your data

● Increases Capital expenditure (CapEx)

● Free for AWS premium members

✓ Scales quickly with your AWS usage

Explanation:-Security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.

Q40) According to the AWS Shared responsibility model, which of the following are the responsibility of the customer? (Choose two)

● Controlling physical access to AWS Regions

✓ Patching applications installed on Amazon EC2

Explanation:-Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in AWS data centers). The AWS customer is responsible for protecting their data either at rest or in transit for all services (including S3).

Patch management is a shared control between AWS and the customer. AWS is responsible for patching the underlying hosts, updating the firmware, and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications.

● Ensuring that the underlying EC2 host is configured properly

● Managing environmental events of AWS data centers

✓ Protecting the confidentiality of data in transit in Amazon S3

Explanation:-Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in AWS data centers). The AWS customer is responsible for protecting their data either at rest or in transit for all services (including S3).

Patch management is a shared control between AWS and the customer. AWS is responsible for patching the underlying hosts, updating the firmware, and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications.

Q41) What is the AWS service that performs automated network assessments of Amazon EC2 instances to check for vulnerabilities?

● AWS Network Access Control Lists

✓ Amazon Inspector

Explanation:-Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to create assessment templates to automate security vulnerability assessments throughout your development and deployment pipelines or for static production systems.

● Amazon Kinesis

● Security groups

Q42) Which of the following is equivalent to a user name and password and is used to authenticate your programmatic access to AWS services and APIs?

● MFA

✓ Access Keys

Explanation:-Access keys consist of two parts: an access key ID and a secret access key. You use access keys to sign programmatic requests that you make to AWS if you use AWS CLI commands (using the SDKs) or using AWS API operations. Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests.

● Instance Password

● Key pairs

Q43) Which of the following AWS services can help you perform security analysis and regulatory compliance auditing? (Choose two)

● AWS Batch

✓ Amazon Inspector

Explanation:-With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. This allows you to make security testing a more regular occurrence as part of development and IT operations.

Additional information:

One of the most important services that performs security analysis and compliance auditing is AWS CloudTrail. AWS CloudTrail simplifies your compliance audits by automatically recording and storing event logs for actions made within your AWS account. With AWS CloudTrail, you can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time.

✓ AWS Config

Explanation:-With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. This allows you to make security testing a more regular occurrence as part of development and IT operations.

Additional information:

One of the most important services that performs security analysis and compliance auditing is AWS CloudTrail. AWS CloudTrail simplifies your compliance audits by automatically recording and storing event logs for actions made within your AWS account. With AWS CloudTrail, you can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time.

● Amazon ECS

● AWS Virtual Private Gateway

Q44) Which AWS Service is used to manage user permissions?

● Security Groups

● AWS Support

✓ AWS IAM

Explanation:-AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow or deny their access to AWS resources.

● Amazon ECS

Q45) What does AWS offer to secure your network?

● Optimized instance types

● Instance reservations

● AWS-controlled network access control lists

✓ Customer-controlled encryption in transit

Explanation:-Data in transit (sometimes called data in motion) is a term used to describe data that is in transit through networks. Encrypting data in transit will add more security to your network by ensuring that data is unreadable as it travels from a service to another or from a network to another. The AWS Customer is responsible for encrypting their data either in transit or at rest.

Q46)

A developer needs to set up an SSL security certificate for a client's eCommerce website in order to use the HTTPS protocol.

Which of the following AWS services can be used to deploy the required SSL server certificates? (Choose TWO)

● AWS Directory Service

● AWS Data Pipeline

● Amazon Route 53

✓ AWS Identity & Access Management

Explanation:-To enable HTTPS connections to your website or application in AWS, you need an SSL/TLS server certificate. You can use a server certificate provided by AWS Certificate Manager (ACM) or one that you obtained from an external provider. You can use ACM or IAM to store and deploy server certificates. Use IAM as a certificate manager only when you must support HTTPS connections in a region that is not supported by ACM. IAM supports deploying server certificates in all regions, but you must obtain your certificate from an external provider for use with AWS.

Amazon Route 53 is used to register domain names or use your own domain name to route your end users to Internet applications. Route 53 is not responsible for creating SSL certifications.

✓ AWS ACM

Explanation:-To enable HTTPS connections to your website or application in AWS, you need an SSL/TLS server certificate. You can use a server certificate provided by AWS Certificate Manager (ACM) or one that you obtained from an external provider. You can use ACM or IAM to store and deploy server certificates. Use IAM as a certificate manager only when you must support HTTPS connections in a region that is not supported by ACM. IAM supports deploying server certificates in all regions, but you must obtain your certificate from an external provider for use with AWS.

Amazon Route 53 is used to register domain names or use your own domain name to route your end users to Internet applications. Route 53 is not responsible for creating SSL certifications.

Q47) Data security is one of the top priorities of AWS. How does AWS deal with old storage devices that have reached the end of their useful life?

● AWS sends the old devices for remanufacturing

● AWS stores the old devices in a secure place

✓ AWS destroys the old devices in accordance with industry-standard practices

Explanation:-When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses specific techniques to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

● AWS sells the old devices to other hosting providers

Q48) What is the AWS IAM feature that provides an additional layer of security on top of user-name and password authentication?

● Access Keys
✓ MFA
Explanation:-AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.
● SDK
● Key Pair

Q49) What is the AWS' recommendation regarding access keys?

● Only share them with trusted people
● Save them within your application code
● Delete all access keys and use passwords instead
✓ Rotate them regularly
Explanation:-AWS recommends that you change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources.

Q50) Which of the following services can be used to monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront?

● AWS CloudTrail
● AWS Cloud9
✓ AWS WAF
Explanation:-AWS WAF is a web application firewall that lets customers monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer. AWS WAF also lets customers control access to their content by defining customizable web security rules.
● Amazon CloudWatch

Q51) How does AWS notify customers about security and privacy events pertaining to AWS services?

● Using the AWS ACM service
● Using Compliance Resources
● Using the AWS Management Console
✓ Using Security Bulletins
Explanation:-AWS publishes security bulletins about the latest security and privacy events with AWS services on the Security Bulletins page.

Q52)

There is a requirement to grant a DevOps team full administrative access to all resources in an AWS account.

Who can grant them these permissions?

● AWS cloud support engineers
● AWS security team
● AWS technical account manager
✓ AWS account owner
Explanation:-The account owner is the entity that has complete control over all resources in his AWS account.

Q53) Which methods can be used by customers to interact with AWS Identity and Access Management (IAM)? (Choose TWO)

● AWS CodeCommit
● AWS Network Access Control Lists
✓ AWS CLI
Explanation:-Customers can work with AWS Identity and Access Management in any of the following ways:
1- AWS Management Console: The console is a browser-based interface that can be used to manage IAM and AWS resources.
2- AWS Command Line Tools: Customers can use the AWS command line tools to issue commands at your system's command line to perform IAM and AWS tasks. Using the command line can be faster and more convenient than the console. The command line tools are also useful if you want to build scripts that perform AWS tasks. AWS provides two sets of command line tools: the AWS Command Line Interface (AWS CLI) and the AWS Tools for Windows PowerShell.
3- AWS SDKs: AWS provides SDKs (software development kits) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to IAM and AWS. For example, the SDKs take care of tasks such as cryptographically signing requests, managing errors, and retrying requests automatically.
✓ AWS SDKs
Explanation:-Customers can work with AWS Identity and Access Management in any of the following ways:
1- AWS Management Console: The console is a browser-based interface that can be used to manage IAM and AWS resources.
2- AWS Command Line Tools: Customers can use the AWS command line tools to issue commands at your system's command line to perform IAM and AWS tasks. Using the command line can be faster and more convenient than the console. The command line tools are also useful if you want to

build scripts that perform AWS tasks. AWS provides two sets of command line tools: the AWS Command Line Interface (AWS CLI) and the AWS Tools for Windows PowerShell.
3- AWS SDKs: AWS provides SDKs (software development kits) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to IAM and AWS. For example, the SDKs take care of tasks such as cryptographically signing requests, managing errors, and retrying requests automatically.

● AWS Security Groups

Q54) Which of the following is a type of MFA device that customers can use to protect their AWS resources?

● AWS CloudHSM

✓ U2F Security Key

Explanation:-AWS multi-factor authentication (AWS MFA) provides an extra level of security that customers can apply to their AWS environment. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for the AWS account resources. AWS supports several MFA device options including Virtual MFA devices, Universal 2nd Factor (U2F) security key, and Hardware MFA devices.

● AWS Key Pair

● AWS Access Keys

Q55) Which AWS Service allows customers to download AWS SOC & PCI reports?

✓ AWS Artifact

Explanation:-AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as audit artifacts) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use these documents as guidelines to evaluate your own cloud architecture and assess the effectiveness of your company's internal controls.

● Amazon Chime

● AWS Well-Architected Tool

● AWS Glue

Q56)

You have just hired a skilled sys-admin to join your team. As usual, you have created a new IAM user for him to interact with AWS services. On his first day, you ask him to create snapshots of all existing Amazon EBS volumes and save them in a new Amazon S3 bucket.

However, the new member reports back that he is unable to create neither EBS snapshots nor S3 buckets.

What might prevent him from doing this simple task?

● The systems administrator must contact AWS Support first to activate his new IAM account

● EBS and S3 are accessible only to the root account owner

● There is not enough space in S3 to store the snapshots

✓ There is a non-explicit deny to all new users

Explanation:-When a new IAM user is created, that user has NO access to any AWS service. This is called a non-explicit deny. For that user, access must be explicitly allowed via IAM permissions.

Q57) Which AWS Service is used to manage the keys used to encrypt customer data?

● AWS Config

✓ AWS KMS

Explanation:-AWS Key Management Service (AWS KMS) is a managed service that enables customers to easily create and control the keys used for cryptographic operations. The service provides a highly available key generation, storage, management, and auditing solution for customers to encrypt or digitally sign data within their applications or to control the encryption of data across AWS services.

● Multi-Factor Authentication (MFA)

● Amazon Macie

Q58) Which of the following are types of AWS Identity and Access Management (IAM) identities? (Choose TWO)

● AWS Organizations

● IAM Policies

✓ IAM Roles

Explanation:-Identities on AWS include users (or groups) and roles. Customers create these identities on AWS to manage access to AWS resources and determine the actions that each identity can perform on those resources.
IAM Roles:
An IAM role is an IAM identity that you can create in your account that has specific permissions. IAM roles allow you to delegate access (for a limited time) to users, applications or services that normally don't have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources. Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources. For these scenarios, you can delegate access to AWS resources using an IAM role.
IAM Users:
An IAM user is an entity that you create in AWS to represent the person or service that uses it to directly interact with AWS. A primary use for IAM users is to grant individuals access to the AWS Management Console for interactive tasks and / or to make programmatic requests to AWS services using the API or CLI. A user in AWS consists of a name, a password to sign into the AWS Management Console, and up to two access keys that can be used with the API or CLI. When you create an IAM user, you grant it permissions by making it a member of a group that has appropriate permission policies attached (recommended), or by directly attaching policies to the user.

✓ IAM Users

Explanation:-Identities on AWS include users (or groups) and roles. Customers create these identities on AWS to manage access to AWS resources and determine the actions that each identity can perform on those resources.

IAM Roles:

An IAM role is an IAM identity that you can create in your account that has specific permissions. IAM roles allow you to delegate access (for a limited time) to users, applications or services that normally don't have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources. Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources. For these scenarios, you can delegate access to AWS resources using an IAM role.

IAM Users:

An IAM user is an entity that you create in AWS to represent the person or service that uses it to directly interact with AWS. A primary use for IAM users is to grant individuals access to the AWS Management Console for interactive tasks and / or to make programmatic requests to AWS services using the API or CLI. A user in AWS consists of a name, a password to sign into the AWS Management Console, and up to two access keys that can be used with the API or CLI. When you create an IAM user, you grant it permissions by making it a member of a group that has appropriate permission policies attached (recommended), or by directly attaching policies to the user.

● AWS Resource Groups

Q59) What does AWS offer to protect your data? (Choose TWO)

✓ Data encryption

Explanation:-AWS offers a lot of services and features that help you in protecting your data in the cloud. You can protect your data by encrypting it in transit and at rest. You can use Cloudtrail to log API and user activity, including who, what, and from where calls were made. You can also use the AWS Identity and Access Management (IAM) to control who can access or edit your data. You can also use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.

In brief, the customer is responsible for protecting their data in the following ways:

1- Data encryption (at rest and in transit)

2- Setting up access control

3- Monitoring user activity

4- Applying MFA

5- Using advanced managed security services such as Amazon Macie.

Additional information:

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks. Today, Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS data stores coming later this year.

● Unlimited storage

● Physical MFA devices

● Load balancing

✓ Access control

Explanation:-AWS offers a lot of services and features that help you in protecting your data in the cloud. You can protect your data by encrypting it in transit and at rest. You can use Cloudtrail to log API and user activity, including who, what, and from where calls were made. You can also use the AWS Identity and Access Management (IAM) to control who can access or edit your data. You can also use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.

In brief, the customer is responsible for protecting their data in the following ways:

1- Data encryption (at rest and in transit)

2- Setting up access control

3- Monitoring user activity

4- Applying MFA

5- Using advanced managed security services such as Amazon Macie.

Additional information:

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks. Today, Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS data stores coming later this year.