Answer Sheet

Q1) Why are Serverless Architectures more economical than Server-based Architectures?

- When you reserve serverless capacity, you will get large discounts compared to server reservation
- Serverless Architectures use new powerful computing devices
- ✅ With the Server-based Architectures, servers continue to run all the time but with the serverless architectures the code runs only when needed

Explanation:-Serverless architectures can reduce costs because you don't have to manage or pay for underutilized servers, or provision redundant infrastructure to implement high availability. For example, you can upload your code to the AWS Lambda compute service, and the service can run the code on your behalf using AWS infrastructure. With AWS Lambda, you are charged for every 100ms your code executes and the number of times your code is triggered.

- With Serverless Architectures you have the ability to scale automatically up or down as demand changes

---

Q2) You have multiple standalone accounts and you want to decrease your AWS charges. What should you do ?

- Try to remove unnecessary accounts
- Track the AWS charges that are incurred by the member accounts
- ✅ Add the accounts to an organization and use Consolidated Billing

Explanation:-Consolidated billing has the following benefits:
1- One bill – You get one bill for multiple accounts.
2- Easy tracking – You can track each account's charges, and download the cost data in .csv format.
3- Combined usage – If you have multiple standalone accounts, your charges might decrease if you add the accounts to an organization. AWS combines usage from all accounts in the organization to qualify you for volume pricing discounts.
4- No extra fee – Consolidated billing is offered at no additional cost.

- Enable the AWS tiered-pricing before provisioning resources

---

Q3) How can you increase your application's fault-tolerance?

- By deploying the underlying resources across multiple subnets
- By hosting your application in one powerful instance instead of multiple instances
- ✅ By deploying your application across multiple Availability Zones

Explanation:-The fault tolerance of an application involves its ability to recover gracefully from failures. Deploying the application resources across multiple availability zones will guarantee that even if one availability zone goes down, there will still be other availability zones to run the application efficiently.

- By deploying your application across a large number of EC2 instances

---

Q4) Which of the following are part of the seven design principles for security in the cloud? (Choose two)

- Never store sensitive data in the cloud
- Use manual monitoring techniques to protect your AWS resources
- Scale horizontally to protect from failures
- ✅ Use IAM roles to grant temporary access instead of long-term credentials

Explanation:-There are seven design principles for security in the cloud:
1- Implement a strong identity foundation: Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize privilege management and reduce or even eliminate reliance on long-term credentials.
2- Enable traceability: Monitor, alert, and audit actions and changes to your environment in real time. Integrate logs and metrics with systems to automatically respond and take action.
3- Apply security at all layers: Rather than just focusing on protection of a single outer layer, apply a defense-in-depth approach with other security controls. Apply to all layers (e.g., edge network, VPC, subnet, load balancer, every instance, operating system, and application).
4- Automate security best practices: Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.
5- Protect data in transit and at rest: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.
6- Keep people away from data: Create mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of loss or modification and human error when handling sensitive data.
7- Prepare for security events: Prepare for an incident by having an incident management process that aligns to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

- ✅ Enable real-time traceability

Explanation:-There are seven design principles for security in the cloud:
1- Implement a strong identity foundation: Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize privilege management and reduce or even eliminate reliance on long-term credentials.
2- Enable traceability: Monitor, alert, and audit actions and changes to your environment in real time. Integrate logs and metrics with systems to automatically respond and take action.
3- Apply security at all layers: Rather than just focusing on protection of a single outer layer, apply a defense-in-depth approach with other security controls. Apply to all layers (e.g., edge network, VPC, subnet, load balancer, every instance, operating system, and application).
4- Automate security best practices: Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.
5- Protect data in transit and at rest: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.
6- Keep people away from data: Create mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of loss or modification and human error when handling sensitive data.
7- Prepare for security events: Prepare for an incident by having an incident management process that aligns to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Q5) Which of the following is a benefit of the "Loose Coupling" approach?

- Reduces Privileged Access to your resources
- Allows you to bid on spare Amazon EC2 computing capacity
- Enables users to quickly deploy only the approved IT services they need
- ✓ The development team can modify the underlying implementation without affecting other components of the application

Explanation:-As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies—a change or a failure in one component should not cascade to other components.

Q6)

The AWS Cloud elasticity enables you to save more costs compared to traditional hosting providers.

How can you apply this concept in your own work environment? (Choose two)

- ✓ Set up Amazon EC2 Auto Scaling

Explanation:-Another way you can save money with AWS is by taking advantage of the platform's elasticity. Elasticity means the ability to scale up or down when needed. This concept is most closely associated with the AWS auto scaling which monitors your applications and automatically adjusts capacity (up or down) to maintain steady, predictable performance at the lowest possible cost.
Serverless Computing provides the highest level of elasticity. Serverless enables you to build modern applications with increased agility and lower total cost of ownership. Serverless allows you to run applications and services without thinking about servers. It eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning. With serverless computing, everything required to run and scale your application with high availability is handled for you.

- Set up Elastic Load Balancing
- ✓ Use Serverless Computing whenever possible

Explanation:-Another way you can save money with AWS is by taking advantage of the platform's elasticity. Elasticity means the ability to scale up or down when needed. This concept is most closely associated with the AWS auto scaling which monitors your applications and automatically adjusts capacity (up or down) to maintain steady, predictable performance at the lowest possible cost.
Serverless Computing provides the highest level of elasticity. Serverless enables you to build modern applications with increased agility and lower total cost of ownership. Serverless allows you to run applications and services without thinking about servers. It eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning. With serverless computing, everything required to run and scale your application with high availability is handled for you.

- Deploy your resources in another region
- Deploy your resources across multiple Availability Zones

Q7) Which of the following makes it easier for you to manage and filter your resources?

- AWS Service Catalog
- ✓ AWS Tagging

Explanation:-Amazon Web Services (AWS) allows customers to assign metadata to their AWS resources in the form of tags. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources. Although there are no inherent types of tags, they enable customers to categorize resources by purpose, owner, environment, or other criteria.

- Amazon CloudWatch
- AWS Directory Service

Q8) You have developed a web application targeting a global audience. Which of the following will help you achieve the highest redundancy and fault tolerance?

- Deploy the application in Multiple AZs in a Single AWS region
- Deploy the application in a Single Availability Zone (AZ)
- ✓ Deploy the application in Multiple AZs in many AWS regions

Explanation:-Since you are targeting a global audience then you should use many AWS regions around the world. The deployment option that gives you the highest redundancy is to deploy the application in multiple AZs within many AWS regions. This redundancy will also increase the fault tolerance of the application because if there is an outage in an AZ, the other AZs can handle requests.

- There's no need to architect for these capabilities in AWS

Q9) A company wants to reduce their overall AWS costs but they don't know where the high costs come from. What should they do? (Choose two)

- Use the AWS Simple Monthly Calculator to analyze the costs applied to their account
- Use Amazon Aurora to estimate and plan their AWS costs
- ✓ Use CloudWatch to create billing alerts that notify them when their usage of their services exceeds thresholds that they define

Explanation:-A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. A key can have more than one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.
Enabling billing alerts using CloudWatch will make it easier to track and manage your spending. The alarm triggers when your account billing exceeds the threshold you specify. Billing alerts can help prevent unexpected spend increases which may be due to unauthorized AWS account or Unknown EC2 instance usage, resources which have been provisioned in your account but are no longer in use or due to higher traffic load that can increase the utilization of all of your resources.

- Use the AWS Price List API
- ✓ Activate cost allocation tags to categorize and track their costs

Explanation:-A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. A key can have more than one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.
Enabling billing alerts using CloudWatch will make it easier to track and manage your spending. The alarm triggers when your account billing

exceeds the threshold you specify. Billing alerts can help prevent unexpected spend increases which may be due to unauthorized AWS account or Unknown EC2 instance usage, resources which have been provisioned in your account but are no longer in use or due to higher traffic load that can increase the utilization of all of your resources.

Q10)

For some services, AWS automatically replicates data across multiple AZs to provide fault tolerance in the event of a server failure or Availability Zone outage.

Select TWO services that automatically replicate data across AZs.

✅ S3

Explanation:-For S3 Standard, S3 Standard-IA, and S3 Glacier storage classes, your objects are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an AWS Region. This means your data is available when needed and protected against AZ failures, errors, and threats.
All of your data in DynamoDB is stored on solid state disks (SSDs) and is automatically replicated across multiple Availability Zones within an AWS region, providing built-in high availability and data durability.

✅ DynamoDB

Explanation:-For S3 Standard, S3 Standard-IA, and S3 Glacier storage classes, your objects are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an AWS Region. This means your data is available when needed and protected against AZ failures, errors, and threats.
All of your data in DynamoDB is stored on solid state disks (SSDs) and is automatically replicated across multiple Availability Zones within an AWS region, providing built-in high availability and data durability.

- Instance Store
- Amazon Route 53
- AWS VPN

Q11)

A hospital needs to store medical records for a minimum period of 10 years. The records being stored will only need to be recalled if there is a legal or audit need, which is expected to be extremely infrequent.

Which AWS Service offers the most cost-effective method for storing the records?

- Amazon S3 Standard
- Amazon Elastic Block Store
- ✅ Amazon S3 Glacier

Explanation:-Amazon S3 Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. With Amazon S3 Glacier, customers can reliably store their data for as little as $0.004 per gigabyte per month. Amazon S3 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 S3 Intelligent-Tiering

Q12) Which AWS Service helps enterprises extend their on-premises storage to AWS in a cost-effective manner?

- AWS Data Pipeline
- Amazon EFS
- ✅ AWS Storage Gateway

Explanation:-Enterprises can extend their on-premises storage to AWS Cloud for long-term backup retention and archiving, optimizing costs and increasing resilience and availability. AWS Storage Gateway is a hybrid storage service that enables on-premises applications to seamlessly use AWS cloud storage. Enterprises can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration. The storage gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, and AWS Backup, providing storage for files, volumes, snapshots, and virtual tapes in AWS.

- Amazon Aurora

Q13) Which AWS Service offers volume discounts based on usage?

- Amazon VPC
- ✅ Amazon S3

Explanation:-Some AWS services are priced in tiers, which specify unit costs for defined amounts of AWS usage. As your usage increases, your usage crosses thresholds into new pricing tiers that specify lower unit costs for additional usage in a month. For example, the more Amazon S3 capacity a customer uses, the lower the cost per unit volume.
The current S3 pricing for the us-east-1 region is:
1st tier: $0.023 per GB / month for the first 50 TB stored
2nd tier: $0.022 per GB / month for the next 450 TB stored
3rd tier: $0.021 per GB / month for all storage consumed above 500 TB.

- AWS Cost Explorer
- Amazon Lightsail

Q14) A company is building an online cloud storage platform. They need a storage service that can scale capacity automatically, while minimizing cost. Which AWS storage service should the company use to meet these requirements?

- AWS Storage Gateway
- Amazon Elastic Block Store
- ✅ Amazon Simple Storage Service

Explanation:-Amazon S3 is a storage service offered by AWS that offers highly redundant object storage to AWS customers. Amazon S3 allows customers to effectively store and retrieve any amount of data from anywhere. Amazon S3 offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs.

- Amazon Elastic Container Service

Q15) A customer is seeking to store objects in their AWS environment and to make those objects downloadable over the internet. Which AWS Service can be used to accomplish this?

- Amazon Instance Store
- Amazon EBS
- ✅ Amazon S3

Explanation:-Amazon S3 provides a simple web service interface that you can use to store and retrieve any amount of data, any time, from anywhere on the internet. Amazon S3 assigns a URL for each object you upload. URLs are used to download the objects you want at any time. Amazon S3 is the only AWS service that provides object level storage.

- Amazon EFS

Q16) Which AWS Service offers a filesystem that can be mounted concurrently from multiple EC2 instances?

- Amazon Simple Storage Service
- AWS Storage Gateway
- ✅ Amazon Elastic File System

Explanation:-Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud. Amazon EFS is easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it. When mounted on Amazon EC2 instances, an Amazon EFS file system provides a standard file system interface and file system access semantics, allowing you to seamlessly integrate Amazon EFS with your existing applications and tools. Multiple EC2 instances can access an Amazon EFS file system at the same time, allowing Amazon EFS to provide a common data source for workloads and applications running on more than one EC2 instance.

- Amazon Elastic Block Store

Q17) How are S3 storage classes rated?

- ✅ Availability & Durability

Explanation:-Each S3 storage class is rated on its availability and durability.

- Scalability & Accessibility
- Availability & Scalability
- Durability & Accessibility

Q18) Which of the following are factors to consider for Amazon EBS pricing? (Choose two)

- The compute time you consume
- The compute capacity you consume
- The number of Snowball storage devices you request
- ✅ The amount of GB you provision per month

Explanation:-Amazon EBS pricing has three factors:
1- Volumes: Volume storage for all EBS volume types is charged by the amount of GB you provision per month, until you release the storage.
2- Snapshots: Snapshot storage is based on the amount of space your data consumes in Amazon S3. Because Amazon EBS does not save empty blocks, it is likely that the snapshot size will be considerably less than your volume size. Copying EBS snapshots is charged based on the volume of data transferred across regions. For the first snapshot of a volume, Amazon EBS saves a full copy of your data to Amazon S3. For each incremental snapshot, only the changed part of your Amazon EBS volume is saved. After the snapshot is copied, standard EBS snapshot charges apply for storage in the destination region.
3- Data transfer: Consider the amount of data transferred out of your application. Inbound data transfer is free, and outbound data transfer charges are tiered.

- ✅ The amount of data transferred out of your application

Explanation:-Amazon EBS pricing has three factors:
1- Volumes: Volume storage for all EBS volume types is charged by the amount of GB you provision per month, until you release the storage.
2- Snapshots: Snapshot storage is based on the amount of space your data consumes in Amazon S3. Because Amazon EBS does not save empty blocks, it is likely that the snapshot size will be considerably less than your volume size. Copying EBS snapshots is charged based on the volume of data transferred across regions. For the first snapshot of a volume, Amazon EBS saves a full copy of your data to Amazon S3. For each incremental snapshot, only the changed part of your Amazon EBS volume is saved. After the snapshot is copied, standard EBS snapshot charges apply for storage in the destination region.
3- Data transfer: Consider the amount of data transferred out of your application. Inbound data transfer is free, and outbound data transfer charges are tiered.

Q19) Which of the following will affect how much you are charged for storing objects in S3? (Choose two)

- The number of EBS volumes attached to your instances
- ✅ The total size in gigabytes of all objects stored

Explanation:-S3 pricing is based on four factors:
1- The storage class you have chosen.
2- The total amount of data (in GB) you've stored.
3- Data Transfer Out.
4- Number of Requests.

- Creating and deleting S3 buckets
- Using default encryption for any number of S3 buckets
- ✅ The storage class used for the objects stored

Explanation:-S3 pricing is based on four factors:
1- The storage class you have chosen.
2- The total amount of data (in GB) you've stored.
3- Data Transfer Out.

4- Number of Requests.

Q20) What is the maximum amount of data that can be stored in S3 in a single AWS account?

- 100 PetaBytes
- ✅ Virtually unlimited storage

Explanation:-The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes.

- 5 TeraBytes
- 10 Exabytes

Q21) In order to keep your data safe, you need to take a backup of your database regularly. What is the most cost-effective storage option that provides immediate retrieval of your backups?

- Amazon EBS
- ✅ Amazon S3

Explanation:-Database backup is an important operation to consider for any database system. Taking backups not only allows the possibility to restore upon database failure but also enables recovery from data corruption. Amazon S3 provides highly durable and reliable storage for database backups while reducing costs. Data stored in Amazon S3 can be retrieved immediately when needed.

- Amazon Glacier
- Instance Store

Q22) AWS provides the ability to create backups of any block-level Amazon EC2 volume. What is the name of this backup?

- Copy
- Image
- ✅ Snapshot

Explanation:-The question asks for creating backups for any block-level Amazon EC2 volume. Amazon EC2 block-level volumes are either EBS volumes or instance store volumes. You can backup EBS volumes by creating EBS snapshots. Data in instance store volumes are not persistent and cannot be used to backup data. In order to backup instance store volumes you should also use EBS.

- Version

Q23) What is the main benefit of the AWS Storage Gateway service?

- It provides physical devices to migrate data from on premises to AWS
- ✅ It allows one to integrate on premises IT environments with Cloud Storage

Explanation:-AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure.

- It provides automatic server-side encryption mechanism
- It provides hardware-based key storage for regulatory compliance

Q24) Which of the following storage classes is most appropriate to be used for a popular e-commerce website with stable access patterns?

- S3 Glacier Deep Archive
- ✅ S3 Standard

Explanation:-S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

- S3 Intelligent-Tiering
- S3 Standard-IA

Q25) What is the AWS S3 storage class that has the lowest availability rating?

- Standard
- ✅ S3 One Zone-IA

Explanation:-S3 One Zone-IA has the lowest availability rating: 99.5%.

- S3 Standard-IA (Infrequent Access)
- Glacier

Q26) Which of the following actions may reduce Amazon EBS costs? (Choose two)

- Deleting unused buckets
- ✅ Changing the type of the volume

Explanation:-With Amazon EBS, it's important to keep in mind that you are paying for provisioned capacity and performance—even if the volume is unattached or has very low write activity. To optimize storage performance and costs for Amazon EBS, monitor volumes periodically to identify ones that are unattached or appear to be underutilized or overutilized, and adjust provisioning to match actual usage.

When you want to reduce the costs of Amazon EBS consider the following:

1- Delete Unattached Amazon EBS Volumes:

An easy way to reduce wasted spend is to find and delete unattached volumes. However, when EC2 instances are stopped or terminated, attached EBS volumes are not automatically deleted and will continue to accrue charges since they are still operating.

2- Resize or Change the EBS Volume Type:

Another way to optimize storage costs is to identify volumes that are underutilized and downsize them or change the volume type.

3- Delete Stale Amazon EBS Snapshots:

If you have a backup policy that takes EBS volume snapshots daily or weekly, you will quickly accumulate snapshots. Check for stale snapshots that are over 30 days old and delete them to reduce storage costs.

✅ Deleting unnecessary snapshots

Explanation:-With Amazon EBS, it's important to keep in mind that you are paying for provisioned capacity and performance—even if the volume is unattached or has very low write activity. To optimize storage performance and costs for Amazon EBS, monitor volumes periodically to identify ones that are unattached or appear to be underutilized or overutilized, and adjust provisioning to match actual usage.

When you want to reduce the costs of Amazon EBS consider the following:

1- Delete Unattached Amazon EBS Volumes:

An easy way to reduce wasted spend is to find and delete unattached volumes. However, when EC2 instances are stopped or terminated, attached EBS volumes are not automatically deleted and will continue to accrue charges since they are still operating.

2- Resize or Change the EBS Volume Type:

Another way to optimize storage costs is to identify volumes that are underutilized and downsize them or change the volume type.

3- Delete Stale Amazon EBS Snapshots:

If you have a backup policy that takes EBS volume snapshots daily or weekly, you will quickly accumulate snapshots. Check for stale snapshots that are over 30 days old and delete them to reduce storage costs.

⚪ Distributing requests to multiple volumes

⚪ Using reservations

Q27) How does AWS notify customers about the latest security and privacy events within AWS services?

✅ Using Security Bulletins

Explanation:-This option is correct. AWS publishes security bulletins about the latest security and privacy events with AWS services on the Security Bulletins page.

⚪ Using Compliance Resources

Explanation:-This option is not correct.

⚪ Using the AWS Management Console

Explanation:-This option is not correct. The AWS management Console is used to access AWS services, however security and privacy events are available - at the Security Bulletins page - without having to have an AWS account.

⚪ Using the AWS ACM service

Explanation:-This option is not correct. AWS Certificate Manager (ACM) is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

Q28)

You are developing a document generator application that helps users create and modify PDFs.

Which of the following allows you to publish your application?

⚪ AWS Marketplace

Explanation:-This option is not correct. The AWS Marketplace is not an application repository. It is an online store where customers can find, buy, and deploy third-party software and services that they need to build solutions and run their businesses on AWS. AWS Marketplace includes software listings from categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps.

⚪ Amazon AppStream

Explanation:-This option is not correct. You can use Amazon AppStream to deliver desktop applications to any user whatever the OS they are using (Chromebooks, Macs, or PCs).

⚪ Amazon Publisher

Explanation:-This option is inappropriate.

✅ AWS Serverless Application Repository

Explanation:-This option is correct. AWS Serverless Application Repository is used to share solutions with developers or to help your customers quickly understand the value of products and services you sell and support. Anyone with an AWS account can publish a serverless application or application component to the AWS Serverless Application Repository. You can share your published applications within your team, across your organization, or with the community at large.

Q29) Which of the following is the most cost-effective AWS service that can be used for long-term data backup and archiving?

⚪ AWS Data Pipeline

Explanation:-This option is not correct. AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources.

✅ AWS S3 Glacier

Explanation:-This option is correct. Amazon S3 Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as $0.004 per gigabyte per month, a significant savings compared to on-premises solutions. Refer: https://aws.amazon.com/glacier/faqs/#:~:text=Amazon%20S3%20Glacier%20is%20a,compared%20to%20on%2Dpremises%20solutions.

⚪ Amazon Aurora

Explanation:-This option is not correct. Amazon Aurora is a database service.

⚪ Amazon EFS

Explanation:-This option is not correct. Amazon EFS may be used to backup databases when you need temporary protection during updates or for development and test. It is not a cost effective solution for long term archival storage.

Q30) What considerations should be taken into account regarding storing data in Amazon Glacier?

⚪ Glacier can only be used to store frequently accessed data and data archives

⚪ Attach Glacier to an EC2 Instance to be able to store data

✅ Amazon Glacier doesn't provide immediate retrieval of data

Explanation:-Objects stored in Glacier take time to retrieve. You can pay for expedited retrieval, which will take several minutes or wait several hours for normal retrieval.

⚪ Amazon Glacier only accepts data in a compressed format

Q31) Amazon EBS volumes are automatically replicated within the same availability zone. What is the benefit of this?

- Accessibility
- Elasticity
- Traceability
- ✅ Durability

Explanation:-Durability refers to the ability of a system to assure data is stored and data remains consistent in the system as long as it is not changed by legitimate access. This means that data should not become corrupted or disappear due to a system malfunction.
Durability is used to measure the likelihood of data loss. For example, assume you have confidential data stored in your Laptop. If you make a copy of it and store it in a secure place, you have just improved the durability of that data. It is much less likely that all copies will be simultaneously destroyed.
Amazon EBS volume data is replicated across multiple servers in an Availability Zone to prevent the loss of data from the failure of any single component. The replication of data makes EBS volumes 20 times more durable than typical commodity disk drives, which fail with an AFR (annual failure rate) of around 4%. For example, if you have 1,000 EBS volumes running for 1 year, you should expect 1 to 2 will have a failure.
Additional information:
Amazon S3 is also considered a durable storage service. Amazon S3 is designed for 99.999999999% (11 9's) durability. This means that if you store 100 billion objects in S3, you will lose one object at most.

Q32) A company needs to host a big data application on AWS. Which of the following AWS Storage services would they choose to automatically get high throughput to multiple compute nodes?

- S3
- AWS Storage Gateway
- Amazon Elastic Block Store
- ✅ Amazon Elastic File System

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.
Amazon EFS 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. With these capabilities, Amazon EFS is well suited to support a broad spectrum of use cases, including web serving and content management, enterprise applications, media and entertainment processing workflows, home directories, database backups, developer tools, container storage, and big data analytics workloads.

Q33) Which statement is true in relation to the security of Amazon EC2?

- You can track all API calls using Amazon Athena
- You should use instance store volumes to store login data
- You should deploy critical components of your application in the Availability Zone that you trust
- ✅ You should regularly patch the operating system and applications on your EC2 instances

Explanation:-Amazon EC2 is not a managed service, you should regularly patch, update, and secure the operating system and applications on your instance.

Q34) For Amazon RDS databases, What does AWS perform on your behalf? (Choose two)

- ✅ Database setup

Explanation:-In relation to Amazon RDS databases:
AWS is responsible for:
1- Managing the underlying infrastructure and foundation services.
2- Managing the operating system.
3- Database setup.
4- Patching and backups.
The customer is still responsible for:
1- Protecting the data stored in his databases (through encryption and IAM access control).
2- Managing the database settings that are specific to his application.
3- Building the relational schema.
4- Network traffic protection.

- Network traffic protection
- ✅ Managing the operating system

Explanation:-In relation to Amazon RDS databases:
AWS is responsible for:
1- Managing the underlying infrastructure and foundation services.
2- Managing the operating system.
3- Database setup.
4- Patching and backups.
The customer is still responsible for:
1- Protecting the data stored in his databases (through encryption and IAM access control).
2- Managing the database settings that are specific to his application.
3- Building the relational schema.
4- Network traffic protection.

- Managing firewall rules
- Access management

Q35) Which of the following is the responsibility of AWS according to the Shared Security Model?

- Performing auditing tasks
- Securing access to AWS resources
- Monitoring AWS resources usage

✅ Securing regions and edge locations

Explanation:-According to the Shared Security Model, AWS' responsibility is the Security of the Cloud. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Q36) Who is responsible for scaling the DynamoDB databases?

- The DevOps team
- The security team
- The development team
- ✅ AWS

Explanation:-DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS so that they don't have to worry about hardware provisioning, setup and configuration, throughput capacity planning, replication, software patching, or cluster scaling.

Q37) According to the AWS shared responsibility model, what are the controls that customers fully inherit from AWS? (Choose two)

- Resource Configuration Management
- ✅ Environmental controls

Explanation:-AWS is responsible for physical controls and environmental controls. Customers inherit these controls from AWS.
As mentioned in the AWS Shared Responsibility Model page, Inherited Controls are controls which a customer fully inherits from AWS such as physical controls and environmental controls.
As a customer deploying an application on AWS infrastructure, you inherit security controls pertaining to the AWS physical, environmental and media protection, and no longer need to provide a detailed description of how you comply with these control families.
For example: Let's say you have built an application in AWS for customers to securely store their data. But your customers are concerned about the security of the data and ensuring compliance requirements are met. To address this, you assure your customer that "our company does not host customer data in its corporate or remote offices, but rather in AWS data centers that have been certified to meet industry security standards." That includes physical and environmental controls to secure the data, which is the responsibility of Amazon. Companies do not have physical access to the AWS data centers, and as such, they fully inherit the physical and environmental security controls from AWS.

- Patch Management
- Communications controls
- ✅ Data center security controls

Explanation:-AWS is responsible for physical controls and environmental controls. Customers inherit these controls from AWS.
As mentioned in the AWS Shared Responsibility Model page, Inherited Controls are controls which a customer fully inherits from AWS such as physical controls and environmental controls.
As a customer deploying an application on AWS infrastructure, you inherit security controls pertaining to the AWS physical, environmental and media protection, and no longer need to provide a detailed description of how you comply with these control families.
For example: Let's say you have built an application in AWS for customers to securely store their data. But your customers are concerned about the security of the data and ensuring compliance requirements are met. To address this, you assure your customer that "our company does not host customer data in its corporate or remote offices, but rather in AWS data centers that have been certified to meet industry security standards." That includes physical and environmental controls to secure the data, which is the responsibility of Amazon. Companies do not have physical access to the AWS data centers, and as such, they fully inherit the physical and environmental security controls from AWS.

Q38)

On the monthly statement, there is a section where you can see the charges for outbound data transfer.

What is the name of that section?

- AWS Outbound

Explanation:-This option is incorrect.

- AWS Outbound Data Transfer

Explanation:-This option is incorrect.

- AWS Out Transfer

Explanation:-This option is incorrect.

- ✅ AWS Data Transfer Out

Explanation:-This option is correct. Outbound data transfer is aggregated across services and then charged at the outbound data transfer rate. This charge appears on the monthly statement as AWS Data Transfer Out.

Q39) Which of the following AWS services allows you to build a data warehouse in the cloud?

- AWS EMR

Explanation:-This option is not correct. EMR is used to process vast amounts of data easily and securely. Use cases include: big data, log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

- AWS Storage Gateway

Explanation:-This option is not correct. AWS Storage Gateway is a hybrid cloud storage service

- Amazon RDS

Explanation:-This option is not correct. Amazon Relational Database Service (Amazon RDS) is used to set up and operate a relational database in the cloud.

- ✅ AWS Redshift

Explanation:-This option is correct. Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers.

Q40) Under the shared responsibility model, Which of the following is the AWS' responsibility?

- Server-side encryption
- ✅ Configuring infrastructure devices

Explanation:-Under the shared responsibility model, AWS is responsible for the hardware and software that run AWS services. This includes patching the infrastructure software and configuring infrastructure devices. As a customer, you are responsible for implementing best practices for data encryption, patching guest operating system and applications, identity and access management, and network & firewall configurations.

- Filtering traffic with Security Groups
- Client-side encryption

Q41) What should you do in order to keep the data on EBS volumes safe? (Choose two)

- ✅ Ensure that EBS data is encrypted at rest

Explanation:-Creating snapshots of EBS Volumes can help ensure that you have a backup of your EBS volumes just in case any issues arise. Amazon EBS encryption offers a straight-forward encryption solution for your EBS resources that doesn't require you to build, maintain, and secure your own key management infrastructure. Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

- Regularly update firmware on EBS devices
- Store a backup daily in an external drive
- ✅ Create EBS snapshots

Explanation:-Creating snapshots of EBS Volumes can help ensure that you have a backup of your EBS volumes just in case any issues arise. Amazon EBS encryption offers a straight-forward encryption solution for your EBS resources that doesn't require you to build, maintain, and secure your own key management infrastructure. Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

- Prevent any unauthorized access to AWS data centers

Q42) Which statement is true regarding the AWS shared responsibility model?

- Security of the managed services is the responsibility of the customer
- ✅ Responsibilities vary depending on the services used

Explanation:-Customers should be aware that their responsibilities may vary depending on the AWS services chosen. For example, when using Amazon EC2, you are responsible for applying operating system and application security patches regularly. However, such patches are applied automatically when using Amazon RDS.

- Security of the IaaS services is the responsibility of AWS
- Patching the guest OS is the responsibility of AWS for all services

---

Q43) Under the Shared Responsibility Model, which of the following controls do customers fully inherit from AWS? (Choose two)

- Patch management controls
- Database controls
- ✅ Physical controls

Explanation:-AWS is responsible for physical controls and environmental controls. Customers inherit these controls from AWS.
As mentioned in the AWS Shared Responsibility Model page, Inherited Controls are controls which a customer fully inherits from AWS such as physical controls and environmental controls.
As a customer deploying an application on AWS infrastructure, you inherit security controls pertaining to the AWS physical, environmental and media protection, and no longer need to provide a detailed description of how you comply with these control families.
For example: Letâ€™s say you have built an application in AWS for customers to securely store their data. But your customers are concerned about the security of the data and ensuring compliance requirements are met. To address this, you assure your customer that â€œour company does not host customer data in its corporate or remote offices, but rather in AWS data centers that have been certified to meet industry security standards.â€ That includes physical and environmental controls to secure the data, which is the responsibility of Amazon. Companies do not have physical access to the AWS data centers, and as such, they fully inherit the physical and environmental security controls from AWS.

- Awareness & Training
- ✅ Environmental controls

Explanation:-AWS is responsible for physical controls and environmental controls. Customers inherit these controls from AWS.
As mentioned in the AWS Shared Responsibility Model page, Inherited Controls are controls which a customer fully inherits from AWS such as physical controls and environmental controls.
As a customer deploying an application on AWS infrastructure, you inherit security controls pertaining to the AWS physical, environmental and media protection, and no longer need to provide a detailed description of how you comply with these control families.
For example: Letâ€™s say you have built an application in AWS for customers to securely store their data. But your customers are concerned about the security of the data and ensuring compliance requirements are met. To address this, you assure your customer that â€œour company does not host customer data in its corporate or remote offices, but rather in AWS data centers that have been certified to meet industry security standards.â€ That includes physical and environmental controls to secure the data, which is the responsibility of Amazon. Companies do not have physical access to the AWS data centers, and as such, they fully inherit the physical and environmental security controls from AWS.

Q44) In Amazon RDS, security groups are ideally used to:

- Launch Amazon RDS instances in a subnet

Explanation:-This option is not correct.

- Create, describe, modify, and delete DB instances

Explanation:-This option is not correct.

- ✅ Control what IP addresses or EC2 instances can connect to your database instance.

Explanation:-This option is correct. In Amazon RDS, security groups are used to control which IP addresses or EC2 instances can connect to your databases on a DB instance. When you first create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.

- Define a maintenance period for database engines

Explanation:-This option is not correct.

Q45) Where to go to search for and buy third-party software solutions and services that run on AWS?

✅ AWS Marketplace

Explanation:-This option is correct. AWS Marketplace is a curated digital catalog that makes it easy for customers to find, buy, deploy, and manage third-party software and services that customers need to build solutions and run their businesses. AWS Marketplace includes thousands of software listings from popular categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps. AWS Marketplace also simplifies software licensing and procurement.

⚪ AWS DevPay

Explanation:-This option is not correct. Amazon DevPay is a cloud-based billing and account management service that enables developers to collect payment for their AWS applications.

⚪ Resource Groups

Explanation:-This option is not correct. Resource Groups helps you organize multiple AWS resources in groups. By default, the AWS Management Console is organized by AWS service. But with the Resource Groups tool, you can create a custom console that organizes and consolidates information based on your project and the resources that you use.

⚪ AWS Application Discovery service.

Explanation:-This option is not correct. AWS Application Discovery Service helps enterprise customers plan migration projects by gathering information about their on-premises data centers

---

Q46) Where to go to find more information about prohibited uses of the web services offered by AWS?

⚪ AWS CloudTrail

Explanation:-This option is not correct. AWS CloudTrail is used to track and log all user's interactions with AWS services.

⚪ AWS Budgets

Explanation:-This option is not correct. AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

⚪ AWS Artifact

Explanation:-This option is not correct. AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports.

✅ AWS Acceptable Use Policy

Explanation:-This option is correct. The AWS Acceptable Use Policy describes prohibited uses of the web services offered by Amazon Web Services, Inc. and its affiliates (the "Services") and the website located at http://aws.amazon.com (the "AWS Site"). The examples described in this Policy are not exhaustive. AWS may modify this Policy at any time by posting a revised version on the AWS Site. By using the Services or accessing the AWS Site, you agree to the latest version of this Policy.

Q47)

You have been tasked with auditing the security of your VPC. As part of this process, you need to start by analyzing what traffic is allowed to and from various EC2 instances.

What two parts of the VPC do you need to check to accomplish this task?

⚪ NACLs and Traffic Manager

Explanation:-This option is incorrect.

⚪ NACLs and Subnets

Explanation:-This option is incorrect.

⚪ Security Groups and Internet Gateways

Explanation:-This option is incorrect.

✅ Security Groups and NACLs

Explanation:-This option is correct. Security Groups and NACLs are the two parts of the VPC Security Layer. Security Groups are a firewall at the instance layer, and NACLs are a firewall at the subnet layer.

Q48) Select the services that can be used to build hybrid cloud architectures. (Choose two)

⚪ AWS Artifact

Explanation:-AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements.

⚪ AWS CloudTrail

Explanation:-AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

✅ AWS Storage Gateway

Explanation:-AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving tape backups to the cloud, reducing on-premises storage with cloud-backed file shares, providing low latency access to data in AWS for on-premises applications, as well as various migration, archiving, processing, and disaster recovery use cases.

✅ AWS Direct Connect

Explanation:-AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment.

⚪ AWS Cloud9

Explanation:-
AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser.

Q49) If your organization is concerned about storing sensitive data in the AWS Cloud, you should _____. (Choose two)

⚪ Delete all IAM users that have access to S3.

Explanation:-This option is not correct. Instead of deleting your IAM users, you should restrict access to the S3 buckets using IAM policies.

With AWS you do not need to worry about encryption.

Explanation:-This option is not correct. AWS does not encrypt the customer data automatically. The customer is responsible for encrypting their data.

Encrypt the data prior to uploading it.

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 Amazon data centers). You can protect data in transit by using SSL or by using client-side encryption.
Also, You have the following options of protecting data at rest in Amazon S3.
1- Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Enable S3 Encryption.

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 Amazon data centers). You can protect data in transit by using SSL or by using client-side encryption.
Also, You have the following options of protecting data at rest in Amazon S3.
1- Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Delete the encryption keys once your data is encrypted.

Explanation:-This option is not correct. These keys are required to perform the decryption process.

Q50) Which of the following AWS support plans provides access to only the 7 core Trusted Advisor checks? (Choose two)

Business

Explanation:-There is no correct option.

Enterprise

Explanation:-There is no correct option.

Developer

Explanation:-Basic and Developer Support Plans provide access to only 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. Business and Enterprise level Support Plans provide access to a full set of Trusted Advisor checks.

Basic

Explanation:-Basic and Developer Support Plans provide access to only 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security. Business and Enterprise level Support Plans provide access to a full set of Trusted Advisor checks.

Q51) Under what circumstances would someone want to use ElastiCache? (Choose two)

They need to distribute requests to multiple instances.

Explanation:-This option is not correct. Elastic Load Balancing is the service that can be used to distribute requests to multiple instances.
Option E is not correct. ElastiCache is not “Chef-compatible”. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. The AWS service that uses Chef and Puppet is AWS OpsWorks.

They need a Chef-compatible cache to speed up their applications.

Explanation:-This option is not correct.

They need to improve the performance of their web application.

Explanation:-Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory system, instead of relying entirely on slower disk-based databases. Amazon ElastiCache works as an in-memory data store and cache to support the most demanding applications requiring sub-millisecond response times.

They need to reduce delivery costs using Edge Locations.

Explanation:-This option is not correct. Edge Locations are used for caching content with the CloudFront service.

They need an in-memory data store service.

Explanation:-Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory system, instead of relying entirely on slower disk-based databases. Amazon ElastiCache works as an in-memory data store and cache to support the most demanding applications requiring sub-millisecond response times.

Q52) Which of the following can be used to increase the fault tolerance of an application?

Deploying resources across multiple VPC’s

Explanation:-This option is incorrect.

Deploying resources across multiple AWS Accounts

Explanation:-This option is incorrect.

Deploying resources across multiple Availability Zones

Explanation:-This option is correct. The fault tolerance of an application involves its ability to recover gracefully from failures. Deploying the application resources across multiple availability zones will guarantee that even if one availability zone goes down, there will still be other availability zones to run the application efficiently.

Deploying resources across multiple edge locations

Explanation:-This option is incorrect.

Q53)

You need to permanently prevent anyone from terminating running instances in your production environment.

What steps should you do?

Create a role document that allows EC2 termination and attach it to all existing IAM identities.

Explanation:-This option is incorrect.

Create a policy document that denies EC2 termination and attach it to all existing IAM identities.

Explanation:-This option is correct. You create IAM identities to provide authentication for people and processes in your AWS account. If you want to prevent those identities from performing any action in your production environment simply create a policy document that denies this action and attach it to the identities you want.

Create a policy document that allows EC2 termination and attach it to all existing IAM identities.

Explanation:-This option is incorrect.

Create a role document that denies EC2 termination and attach it to all existing IAM identities.

Explanation:-This option is incorrect.

Q54) Which of the following services allows you to install and run your custom relational database software?

Amazon RDS

Explanation:-This option is not correct. Amazon RDS provides you with only six database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. These engines are already installed and ready to be used. You cannot install your custom database software on RDS.

✅ Amazon EC2

Explanation:-This option is correct. If you need a full control over your database, AWS provides a wide range of Amazon EC2 instances—with different hardware characteristics—on which you can install and run your custom relational database software.
Please note that if you use EC2 instead of RDS to run your relational database, you will be responsible for managing everything related to this database.

Amazon Cognito

Explanation:-This option is not correct. Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

Amazon Inspector

Explanation:-This option is not correct. Amazon Inspector is an automated security assessment service to help improve the security and compliance of applications deployed on AWS.

Q55) Which of the following services enables you to easily generate and use your own encryption keys in the AWS Cloud?

✅ AWS CloudHSM

Explanation:-This option is correct. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

AWS WAF

Explanation:-This option is not correct. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

AWS Certificate Manager

Explanation:-This option is not correct. AWS Certificate Manager is a service that lets you provision, manage, and deploy (SSL/TLS) certificates for use with AWS services and your internal connected resources.

AWS Shield

Explanation:-This option is not correct. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service.

Q56)

A company wants to add an extra layer of protection to their current authentication mechanism of usernames and passwords.

Which of the following can be used to best achieve this goal?

✅ Use MFA

Explanation:-This option is correct. 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

Use Password Policies

Explanation:-This option is not correct. A password policy on your AWS account enables you to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. For example you can use a password policy to set a minimum password length, Require specific character types, including uppercase letters, lowercase letters, numbers, and so on.

Use a mix of user names

Explanation:-This option is not correct. Using a mix of user names may not add any security benefits.

Use AWS WAF

Explanation:-This option is not correct. AWS WAF is a AWS web application firewall that helps protect your web applications.

Q57) Which of the following is equivalent to virtual servers hosted in an on-premise location?

AWS IAM

Explanation:-This option is not correct. AWS IAM enables you to manage access to AWS services and resources securely.

AWS Managed Servers

Explanation:-This option is not correct. Amazon EC2 instances are not managed by AWS. It is the responsibility of the customer to manage everything related to their instances.

✅ AWS EC2 Instances

Explanation:-This option is correct. Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

AWS Regions

Explanation:-This option is not correct. An AWS Region is a geographic location where you choose to deploy your resources to based on its proximity to your end users, data sovereignty and costs.

Q58) Amazon SWF is designed to help users _____.

Manage user identification and authorization.
Explanation:-This option is incorrect.
Store Web content.
Explanation:-This option is incorrect.
Coordinate tasks across distributed application components.
Explanation:-This option is correct. Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. Amazon SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks.
Design graphical user interface interactions.
Explanation:-This option is incorrect.

Q59)

Your company wants to migrate their website to AWS.Security is a major concern to them, so they need to host their website on exclusive hardware

that is NOT shared with any other AWS customers.

Which of the following EC2 instance types is the most appropriate choice?

Independent instances
Explanation:-This options is not correct. Independent instances and Distinct instances are bogus options.
Distinct instances
Explanation:-This options is not correct. Independent instances and Distinct instances are bogus options.
Dedicated instances
Explanation:-This option is correct. Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at the hardware level. In addition, Dedicated Instances that belong to AWS accounts that are linked to a single payer account are also physically isolated at the hardware level.
Reserved instances
Explanation:-This option is not correct. Reserved instances share hardware with other customers.

Q60) Which of the following support plans include the AWS Support Concierge Service?

Business
Explanation:-This option is incorrect.
Developer
Explanation:-This option is incorrect.
Basic
Explanation:-This option is incorrect.
Enterprise
Explanation:-This option is correct. Only the Enterprise plan includes the AWS Support Concierge Service.

Q61) Which of the following AWS services can assist you with cost optimization?

AWS Shield
Explanation:-This option is not correct. AWS Shield is used to protect from DDoS attacks.
AWS Inspector
Explanation:-This option is not correct. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.
AWS WAF
Explanation:-This option is not correct. AWS WAF is a firewall.
AWS Trusted Advisor
Explanation:-This option is correct. AWS Trusted Advisor is an application that draws upon best practices learned from AWS' aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and makes recommendations for saving money, improving system performance, and closing security gaps.

Q62) Which statement best describes the concept of an AWS region?

It is the same as an Availability Zone
Explanation:-This option is incorrect.
It is a geographical area divided into Availability Zones
Explanation:-This option is correct. An AWS Region is a geographic location with a collection of availability zones mapped to physical data centers within that region. Every region is physically isolated from and independent of every other region in terms of location, power, water, supply, etc.
It is a collection of Edge locations
Explanation:-This option is incorrect.
It is a collection of Compute resources
Explanation:-This option is incorrect.

Q63) How does AWS Lambda work?

Configure an AutoScaling group and attach the Lambda instance to it, then upload and run your code.
Explanation:-This option is incorrect.
Setup the Storage, Compute Capacity, Security Groups, then upload and run your code.
Explanation:-This option is incorrect.
Just upload your code and watch it run.
Explanation:-This option is correct. AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high

availability. You can set up your code to automatically trigger from other AWS service.

Upload your code to an S3 bucket then link it to Lambda to run it.

Explanation:-This option is incorrect.

Q64) Which networking service enables one to create a virtual network within AWS?

Amazon Virtual Private Cloud (Amazon VPC)

Explanation:-This option is correct. Amazon Virtual Private Cloud (Amazon VPC) is the service that allows a customer to create a virtual network for their resources in an isolated section of the AWS cloud.

AWS Config

Explanation:-This option is not correct. AWS Config is used to record and evaluate configurations of your AWS resources.

AWS Direct Connect

Explanation:-This option is not correct. AWS Direct Connect allows you to establish a dedicated network connection from your premises to AWS.

Amazon Route 53

Explanation:-This option is not correct. Amazon Route 53 is a domain name system (DNS) in the AWS cloud.
