Answer Sheet

Q1) What are the AWS services\features that can help you maintain a highly available and fault-tolerant architecture in AWS? (Choose two)

● Network ACLs
● CloudFormation
✓ Elastic Load Balancer
Explanation:-Elastic Load Balancing provides an effective way to increase the availability and fault tolerance of a system. First ELB tries to discover the availability of your EC2 instances, it periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks. The load balancer routes user requests only to the healthy instances. When the load balancer determines that an instance is unhealthy, it stops routing requests to that instance. The load balancer resumes routing requests to the instance when it has been restored to a healthy state.
✓ Amazon EC2 Auto Scaling
Explanation:-Amazon EC2 Auto Scaling is a fully managed service designed to launch or terminate Amazon EC2 instances automatically to help ensure you have the correct number of Amazon EC2 instances available to handle the load for your application. Amazon EC2 Auto Scaling helps you maintain application availability and fault tolerance through fleet management for EC2 instances, which detects and replaces unhealthy instances, and by scaling your Amazon EC2 capacity automatically according to conditions you define. You can use Amazon EC2 Auto Scaling to automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
● AWS Direct Connect

Q2) Jessica is managing an e-commerce web application in AWS. The application is hosted on six EC2 instances. One day, three of the instances crashed; but none of her customers were affected. What has Jessica done correctly in this scenario?

● She has properly built an elastic system
● She has properly built a scalable system
● She has properly built an encrypted system
✓ She has properly built a fault tolerant system
Explanation:-Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some (one or more faults within) of its components. Visitors to a website expect the website to be available irrespective of when they visit. For example, when someone wants to visit Jessicaâ€™s website to purchase a product, whether it is at 9:00 AM on a Monday or 3:00 PM on holiday, he expects that the website will be available and ready to accept his purchase. Failing to meet these expectations can cause loss of business and contribute to the development of a negative reputation for the website owner, resulting in lost revenue.

Q3) Which of the below is a best-practice when building applications on AWS?

● Ensure that the application runs on hardware from trusted vendors
● Use IAM policies to maintain performance
✓ Decouple the components of the application so that they run independently
Explanation:-An application should be designed in a way that reduces interdependencies between its components. A change or a failure in one component should not cascade to other components. If the components of an application are tightly-coupled (interconnected) and one component fails, the entire application will also fail. Amazon SQS and Amazon SNS are powerful tools that help you build loosely-coupled applications. SQS and SNS can be integrated together to decouple application components so that they run independently, increasing the overall fault tolerance of the application.
Understanding how SQS and SNS services work is not required for the Cloud Practitioner level, but letâ€™s just take a simple example, let say you have two components in your application, Component A & Component B. Component A sends messages (jobs) to component B to process. Now, what happens if component A sends a large number of messages at the same time? Component B will fail, and the entire application will fail. SQS act as a middleman, receives and stores messages from component A, and component B pull and process messages at its own pace. This way, both components run independently from each other.
● Strengthen physical security by applying the principle of least privilege

---

Q4) Which of the following is a benefit of running an application in multiple Availability Zones?

● Reduces application response time between servers and global users
● Allows you to exceed AWS service limits
● Increases available compute capacity
✓ Increases the availability of your application
Explanation:-Placing instances that run your application in multiple Availability Zones improves the fault tolerance of your application. If one Availability Zone experiences an outage, traffic is routed to another Availability Zone, and this will increase the availability of your application.

Q5) Which design principles relate to performance efficiency in AWS? (Choose TWO)

● Enable audit logging
● Apply security at all layers
✓ Use serverless architectures
Explanation:-There are five design principles for performance efficiency in the cloud:
1- Democratize advanced technologies: Technologies that are difficult to implement can become easier to consume by pushing that knowledge and complexity into the cloud vendor's domain. Rather than having your IT team learns how to host and run a new technology, they can simply consume it as a service. For example, NoSQL databases, media transcoding, and machine learning are all technologies that require expertise that is not evenly dispersed across the technical community. In the cloud, these technologies become services that your team can consume while focusing on product development rather than resource provisioning and management.
2- Go global in minutes: Easily deploy your system in multiple Regions around the world with just a few clicks. This allows you to provide lower latency and a better experience for your customers at minimal cost.
3- Use serverless architectures: In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these

managed services operate at cloud scale.
4- Experiment more often: With virtual and automatable resources, you can quickly carry out comparative testing using different types of instances, storage, or configurations.
5- Mechanical sympathy: Use the technology approach that aligns best to what you are trying to achieve. For example, consider data access patterns when selecting database or storage approaches.

● Implement strong Identity and Access controls
✓ Build multi-region architectures to better serve global customers

Explanation:-There are five design principles for performance efficiency in the cloud:
1- Democratize advanced technologies: Technologies that are difficult to implement can become easier to consume by pushing that knowledge and complexity into the cloud vendor's domain. Rather than having your IT team learns how to host and run a new technology, they can simply consume it as a service. For example, NoSQL databases, media transcoding, and machine learning are all technologies that require expertise that is not evenly dispersed across the technical community. In the cloud, these technologies become services that your team can consume while focusing on product development rather than resource provisioning and management.
2- Go global in minutes: Easily deploy your system in multiple Regions around the world with just a few clicks. This allows you to provide lower latency and a better experience for your customers at minimal cost.
3- Use serverless architectures: In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale.
4- Experiment more often: With virtual and automatable resources, you can quickly carry out comparative testing using different types of instances, storage, or configurations.
5- Mechanical sympathy: Use the technology approach that aligns best to what you are trying to achieve. For example, consider data access patterns when selecting database or storage approaches.

Q6) What are the benefits of using an AWS-managed service? (Choose two)

● Eliminates the need to encrypt data
● Allows developers to control all patching related activities
✓ Lowers operational complexity

Explanation:-AWS services that are managed lower operational complexity by automating time-consuming administration tasks such as hardware provisioning, software setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, security and compatibility they need. Because these services are instantly available to developers, they reduce dependency on in-house specialized skills and allow organizations to deliver new solutions faster.

✓ Allows customers to deliver new solutions faster

Explanation:-AWS services that are managed lower operational complexity by automating time-consuming administration tasks such as hardware provisioning, software setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, security and compatibility they need. Because these services are instantly available to developers, they reduce dependency on in-house specialized skills and allow organizations to deliver new solutions faster.

● Provides complete control over the virtual infrastructure

Q7) App development companies move their business to AWS to reduce time-to-market and improve customer satisfaction, what are the AWS automation tools that help them deploy their applications faster? (Choose two)

● AWS Migration Hub
✓ AWS Elastic Beanstalk

Explanation:-AWS Elastic Beanstalk makes it easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.
AWS CloudFormation automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. Creating and interconnecting all resources your application needs to run is now as simple as creating a single EC2 or RDS instance.

● AWS IAM
● Amazon Macie
✓ AWS CloudFormation

Explanation:-AWS Elastic Beanstalk makes it easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.
AWS CloudFormation automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. Creating and interconnecting all resources your application needs to run is now as simple as creating a single EC2 or RDS instance.

Q8) Which of the following AWS services scale automatically without your intervention? (Choose two)

● Amazon EMR
✓ AWS Lambda

Explanation:-Amazon S3 and Amazon EFS are storage services that scale automatically in storage capacity without any intervention to meet increased demand.
Also, AWS Lambda dynamically scales function execution in response to increased traffic.

● Amazon EC2
✓ Amazon S3

Explanation:-Amazon S3 and Amazon EFS are storage services that scale automatically in storage capacity without any intervention to meet increased demand.
Also, AWS Lambda dynamically scales function execution in response to increased traffic.

● Amazon EBS

Q9) Which of the following can be used to protect data at rest on Amazon S3? (Choose two)

● Decryption
✓ Versioning

Explanation:-Amazon S3 provides a number of security features for the protection of data at rest, which you can use or not depending on your

threat profile:
1- Permissions: Use bucket-level or object-level permissions alongside IAM policies to protect resources from unauthorized access and to prevent information disclosure, data integrity compromise or deletion.
2- Versioning: Amazon S3 supports object versions. Versioning is disabled by default. Enable versioning to store a new version for every modified or deleted object from which you can restore compromised objects if necessary.
3- Replication: Amazon S3 replicates each object across all Availability Zones within the respective region. Replication can provide data and service availability in the case of system failure, but provides no protection against accidental deletion or data integrity compromise – it replicates changes across all Availability Zones where it stores copies.
4- Backup: You can use application-level technologies to manually back up data stored in Amazon S3 to other AWS regions or to on-premises backup systems.
5- Encryption – server side: Amazon S3 supports server-side encryption of user data. Server-side encryption is transparent to the end user. AWS generates a unique encryption key for each object, and then encrypts the object using AES-256.
6- Encryption – client side: With client-side encryption you create and manage your own encryption keys. Keys you create are not exported to AWS in clear text. Your applications encrypt data before submitting it to Amazon S3, and decrypt data after receiving it from Amazon S3. Data is stored in an encrypted form, with keys and algorithms only known to you.
Additional information:
AWS also provides a fully managed security service called AWS Macie to help protect your sensitive data in AWS. 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.

● Deduplication

✓ Permissions

Explanation:-Amazon S3 provides a number of security features for the protection of data at rest, which you can use or not depending on your threat profile:

1- Permissions: Use bucket-level or object-level permissions alongside IAM policies to protect resources from unauthorized access and to prevent information disclosure, data integrity compromise or deletion.
2- Versioning: Amazon S3 supports object versions. Versioning is disabled by default. Enable versioning to store a new version for every modified or deleted object from which you can restore compromised objects if necessary.
3- Replication: Amazon S3 replicates each object across all Availability Zones within the respective region. Replication can provide data and service availability in the case of system failure, but provides no protection against accidental deletion or data integrity compromise – it replicates changes across all Availability Zones where it stores copies.
4- Backup: You can use application-level technologies to manually back up data stored in Amazon S3 to other AWS regions or to on-premises backup systems.
5- Encryption – server side: Amazon S3 supports server-side encryption of user data. Server-side encryption is transparent to the end user. AWS generates a unique encryption key for each object, and then encrypts the object using AES-256.
6- Encryption – client side: With client-side encryption you create and manage your own encryption keys. Keys you create are not exported to AWS in clear text. Your applications encrypt data before submitting it to Amazon S3, and decrypt data after receiving it from Amazon S3. Data is stored in an encrypted form, with keys and algorithms only known to you.
Additional information:
AWS also provides a fully managed security service called AWS Macie to help protect your sensitive data in AWS. 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.

● Conversion

Q10) According to best practices, which of the below options is best suited for processing a large number of binary files?

● Running RDS instances in parallel

● Vertically scaling EC2 instances

✓ Running EC2 instances in parallel

Explanation:-One of the core principles of the AWS Well-Architected Framework is that of scaling horizontally. Horizontal scaling means adding several smaller instances when workloads increase, instead of adding additional CPU, memory, or disk capacity to a single instance. In the syntax of this question, running several EC2 instances in parallel achieves horizontal scalability and is the correct answer.
AWS recommends that customers should scale resources horizontally to increase aggregate system availability. Replacing a large resource with multiple small resources in parallel will reduce the impact of a single failure on the overall system. For example, if a customer wants to convert a large number of binary files to text files or transcode a large number of video files to another format, it is recommended that they use multiple EC2 instances in parallel instead of using one large instance.

● Vertically scaling RDS instances

Q11)

A key practice when designing solutions on AWS is to minimize dependencies between components so that the failure of a single component does not impact other components.

What is this practice called?

● Tightly coupling

● Elastic coupling

● Scalable coupling

✓ Loosely coupling

Explanation:-The concept of loosely coupling an application refers to breaking the application into components that perform aspects of a task independently of one another. Using this design concept minimizes the risk that a change or a failure in one component will impact other components.

Q12) Which of the below options is a best practice for making your application on AWS highly available?

● Deploy the application code on at least two servers in the same Availability Zone
● Use AWS Direct Connect to access the application
✓ Deploy the application to at least two Availability Zones
Explanation:-Each AWS Region contains multiple distinct locations, or Availability Zones. Each Availability Zone is engineered to be independent from failures in other Availability Zones. Deploying your application to multiple Availability Zones will increase the availability of your application. If one availability zone encounters an issue, the other availability zones can still serve your application.
● Rewrite the application code to handle all incoming requests

---

Q13) What are the advantages of using Auto Scaling Groups for EC2 instances?

● Auto Scaling Groups scales EC2 instances across multiple regions to reduce latency for global users
● Auto Scaling Groups distributes application traffic across multiple Availability Zones to enhance performance
● Auto Scaling Groups caches the most recent responses at global edge locations to reduce latency and improve performance
✓ Auto Scaling Groups scales EC2 instances in multiple Availability Zones to increase application availability and fault tolerance
Explanation:-Amazon EC2 Auto Scaling offers the following benefits:
1- Better fault tolerance. Amazon EC2 Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. Also, Amazon EC2 Auto Scaling enables you to take advantage of the safety and reliability of geographic redundancy by spanning Auto Scaling groups across multiple Availability Zones within a Region. When one Availability Zone becomes unhealthy or unavailable, Auto Scaling launches new instances in an unaffected Availability Zone. When the unhealthy Availability Zone returns to a healthy state, Auto Scaling automatically redistributes the application instances evenly across all of the designated Availability Zones.
2- Better availability. Amazon EC2 Auto Scaling helps ensure that your application always has the right amount of capacity to handle the current traffic demand.
3- Better cost management. Amazon EC2 Auto Scaling can dynamically increase and decrease capacity as needed. Because you pay for the EC2 instances you use, you save money by launching instances when they are needed and terminating them when they aren't.

Q14)

A company is using EC2 Instances to run their e-commerce site on the AWS platform. If the site becomes unavailable, the company will lose a significant amount of money for each minute the site is unavailable.

Which design principle should the company use to minimize the risk of an outage?

● Pilot Light
✓ Fault Tolerance
Explanation:-A system that is designed to be fault tolerant can recover gracefully from EC2 instance failures. Amazon Web Services gives customers access to a vast amount of IT infrastructure–compute, storage, and communications–that they can allocate automatically (or nearly automatically) to account for almost any kind of failure.
● Least Privilege
● Multi-threading

Q15) Which of the following approaches will help you eliminate human error and automate the process of creating and updating your AWS environment?

● Migrate all of your applications to a dedicated host
● Use AWS CodeDeploy to build and automate your AWS environment
✓ Use code to provision and operate your AWS infrastructure
Explanation:-In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events. By performing operations as code, you limit human error and enable consistent responses to events.
You can define your infrastructure as code using approaches such as AWS CloudFormation templates. The use of templates allows you to build and rebuild your infrastructure, without having to perform manual actions or write custom scripts.
Codifying your infrastructure in a template allows you to treat your infrastructure as just code. You can author it with any code editor, check it into a version control system, and review the files with team members before deploying into production. This gives developers an easy way to build and update their entire AWS environment in a timely fashion.
● Use Software test automation tools

Q16) What are the key design principles of the AWS Cloud? (Choose two)

● Multi-AZ deployments instead of multi-region deployments
✓ Disposable resources instead of fixed servers
Explanation:-The AWS Cloud includes many design patterns and architectural options that you can apply to a wide variety of use cases. Some key design principles of the AWS Cloud include scalability, disposable resources, automation, loose coupling, managed services instead of servers, and flexible data storage options.
Disposable resources instead of fixed servers:
When designing for the cloud, you can think of servers and other components as temporary resources instead of fixed servers. This approach solves many problems that usually appear in traditional, on-premises environments. For example, changes and software patches applied through time to the same (fixed) server can result in untested and heterogeneous configurations across different environments. You can solve this problem in AWS with its immutable infrastructure pattern. With this approach, If a problem happens with a server (EC2 instance), rather than updating, it is replaced with a new server containing the latest patches and configuration. This enables resources to always be in a consistent (and tested) state and makes rollbacks easier to perform.
Loose coupling:
Loose coupling is an approach that involves interconnecting the components in a system or network so that those components depend on each other to the least extent practical. Engineers should architect their system or application such that failure in one component does not negatively affect other components. Loosely coupled components make the system resilient and allow it to recover gracefully from failure.
● Reserved capacity instead of on demand
● Servers instead of managed services

✓ Loose coupling

Explanation:-The AWS Cloud includes many design patterns and architectural options that you can apply to a wide variety of use cases. Some key design principles of the AWS Cloud include scalability, disposable resources, automation, loose coupling, managed services instead of servers, and flexible data storage options.

Disposable resources instead of fixed servers:

When designing for the cloud, you can think of servers and other components as temporary resources instead of fixed servers. This approach solves many problems that usually appear in traditional, on-premises environments. For example, changes and software patches applied through time to the same (fixed) server can result in untested and heterogeneous configurations across different environments. You can solve this problem in AWS with its immutable infrastructure pattern. With this approach, If a problem happens with a server (EC2 instance), rather than updating, it is replaced with a new server containing the latest patches and configuration. This enables resources to always be in a consistent (and tested) state and makes rollbacks easier to perform.

Loose coupling:

Loose coupling is an approach that involves interconnecting the components in a system or network so that those components depend on each other to the least extent practical. Engineers should architect their system or application such that failure in one component does not negatively affect other components. Loosely coupled components make the system resilient and allow it to recover gracefully from failure.

Q17) You have just set up your AWS environment and have created six IAM user accounts for the DevOps team. What is the AWS recommendation when granting permissions to those IAM accounts?

● Attach a separate IAM policy for each individual account

● Create six different IAM passwords

✓ Apply the principle of least privilege

Explanation:-The principle of least privilege (PoLP, also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose. For example, a user account for the sole purpose of creating backups does not need to install software: hence, it has rights only to run backup and backup-related applications. Any other privileges, such as installing new software, are blocked.

● For security purposes, you should not grant any permission to the DevOps team

---

Q18) You want to run a questionnaire application for only one day (without interruption), which AWS EC2 purchase option would you choose?

● Reserved instances

Explanation:-This option is not correct. Reserved instances are not appropriate in this case because you have to purchase capacity for at least one year.

● Spot instances

Explanation:-This option is not correct. Spot is not a good choice as the application must run without interruption.

● Dedicated instances

Explanation:-This option is not correct. Dedicated instances can be used if you require your instance be physically isolated at the host hardware level from instances that belong to other AWS accounts.

✓ On-demand instances

Explanation:-This option is correct. With On-Demand instances, you pay for compute capacity by the hour with no long-term commitments. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified hourly rate for the instances you use. The use of On-Demand instances frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs. On-Deman

---

Q19) 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

Q20) Which statement best describes the operational excellence pillar of the AWS Well-Architected Framework?

● The ability to provision resources on-demand

● The ability of a system to recover gracefully from failure

✓ The ability to monitor and improve system processes and procedures

Explanation:-The 5 Pillars of the AWS Well-Architected Framework:

1- Operational Excellence: The operational excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

2- Security: The security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

3- Reliability: The reliability pillar includes 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.

4- Performance Efficiency: The performance efficiency pillar includes the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.

5- Cost Optimization: The cost optimization pillar includes the ability to avoid or eliminate unneeded cost or sub-optimal resources.

Additional information:

Creating a software system is a lot like constructing a building. If the foundation is not solid, structural problems can undermine the integrity and function of the building. When architecting technology solutions on Amazon Web Services (AWS), if you neglect the five pillars of operational excellence, security, reliability, performance efficiency, and cost optimization, it can become challenging to build a system that delivers on your expectations and requirements. Incorporating these pillars into your architecture helps produce stable and efficient systems. This allows you to focus on the other aspects of design, such as functional requirements. The AWS Well-Architected Framework helps cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications.

● The ability to manage datacenter operations more efficiently

Q21) Which of the following activities may help reduce your AWS monthly costs?

✓ Enabling Amazon EC2 Auto Scaling for all of your workloads

Explanation:-Amazon EC2 Auto Scaling monitors your applications and automatically adjusts capacity (up or down) to maintain steady, predictable performance at the lowest possible cost.

● Deploying your AWS resources across multiple Availability Zones

● Using the AWS Network Load Balancer (NLB) to load balance the incoming HTTP requests

● Removing all of your Cost Allocation Tags

Q22) Which of the following is a cloud computing deployment model that connects infrastructure and applications between cloud-based resources and existing resources not located in the cloud ?

● Mixed

● Cloud

✓ Hybrid

Explanation:-A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud. The most common method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend, and grow, an organization's infrastructure into the cloud while connecting cloud resources to the internal system.

● On-premises

Q23) 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.

Q24)

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.

Q25) 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

Q26) 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

Q27) 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.

Q28)

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.

Q29) 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

Q30) What should you do if you see resources, which you don't remember creating, in the AWS Management Console? (Choose TWO)

● Stop all running services and open an investigation
✓ Open an investigation and delete any potentially compromised IAM users

Explanation:-If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:
1- Change your AWS root account password and the passwords of any IAM users.
2- Delete or rotate all root and AWS Identity and Access Management (IAM) access keys.
3- Delete any potentially compromised IAM users.
4- Delete any resources on your account you didn't create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users.
5- Respond to any notifications you received from AWS Support through the AWS Support Center.

● Check the AWS CloudTrail logs and delete all IAM users that have access to your resources
✓ Change your AWS root account password and the passwords of any IAM users

Explanation:-If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:
1- Change your AWS root account password and the passwords of any IAM users.
2- Delete or rotate all root and AWS Identity and Access Management (IAM) access keys.
3- Delete any potentially compromised IAM users.
4- Delete any resources on your account you didn't create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users.
5- Respond to any notifications you received from AWS Support through the AWS Support Center.

● Give your root account password to AWS Support so that they can assist in troubleshooting and securing the account

---

Q31) Which of the following can help secure your sensitive data in Amazon S3? (Choose two)

● Delete all IAM users that have access to S3
● With AWS you do not need to worry about encryption
✓ 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.
2- Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

● Delete the encryption keys once your data is encrypted

✓ 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.
2- Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Q32) 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

Q33) 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.

Q34) A company is seeking to better secure its AWS account from unauthorized access. Which of the below options can the customer use to achieve this goal?

● Set up two login passwords
✅ Require Multi-Factor Authentication (MFA) for all IAM User access
Explanation:-For increased security, AWS recommends that you configure multi-factor authentication (MFA) to help protect your AWS resources. MFA adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services. You can also enforce MFA authentication for AWS service APIs via AWS Identity and Access Management (IAM) policies. This provides an extra layer of security over powerful API operations that you designate, such as terminating Amazon EC2 instances or reading sensitive data stored in Amazon S3.
● Restrict any API call made through SDKs or CLI
● Create one IAM account for each department in the company (Development, QA, Production), and share it across all staff in that department

---

Q35) Which AWS service enables you to quickly purchase and deploy SSL/TLS certificates?

● AWS WAF
✅ AWS ACM
Explanation:-AWS Certificate Manager (AWS 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. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.
AWS Certificate Manager removes many of the time-consuming and error-prone steps to acquire an SSL/TLS certificate for your website or application. With a few clicks in the AWS Management Console, you can request a trusted SSL/TLS certificate from AWS. Once the certificate is created, AWS Certificate Manager takes care of deploying certificates to help you enable SSL/TLS for your website or application.
● Amazon GuardDuty
● AWS Budgets

Q36) Which of the following can be used to enable the Virtual Multi-Factor Authentication? (Choose TWO)

✅ AWS Identity and Access Management (IAM)
Explanation:-You can use either the AWS IAM console or the AWS CLI to enable a virtual MFA device for an IAM user in your account.
● Amazon SNS
✅ AWS CLI
Explanation:-You can use either the AWS IAM console or the AWS CLI to enable a virtual MFA device for an IAM user in your account.
● Amazon Virtual Private Cloud
● Amazon Connect

Q37) 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

Q38) 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.

Q39)

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.

Q40) 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

Q41) 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

Q42) 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

Q43) 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.

Q44) 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

Q45) 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

Q46) 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

Q47) 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

Q48) 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.

Q49) 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.

Q50) 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

Q51) 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

Q52) 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

Q53) 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

Q54) Which of the following is NOT a factor when estimating the cost of Amazon CloudFront?

● Data Transfer Out
● The number and type of requests (HTTP or HTTPS) made
✓ Inbound traffic

Explanation:-Amazon CloudFront charges are based on the data transfer out of AWS and requests used to deliver content to your customers. There are no upfront payments or fixed platform fees, no long-term commitments, no premiums for dynamic content, and no requirements for professional services to get started. There is no charge for data transferred from AWS services such as Amazon S3 or Elastic Load Balancing.
When you begin to estimate the cost of Amazon CloudFront, consider the following:
- Traffic distribution: Data transfer and request pricing varies across geographic regions, and pricing is based on the edge location through which your content is served.
- Requests: The number and type of requests (HTTP or HTTPS) made and the geographic region in which the requests are made.
- Data transfer out: The amount of data transferred out of your Amazon CloudFront edge locations.

● The edge location through which your content is served

Q55) What is the main purpose of attaching security groups to an Amazon RDS instance?

● Manages user access and encryption keys
● Deploys SSL/TLS certificates for use with your database instance
✓ Controls what IP addresses or EC2 instances can connect to your database instance

Explanation:-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.

● Distributes incoming traffic across multiple targets

Q56) Which of the following affects Amazon CloudFront costs? (Choose two)

✓ Traffic Distribution

Explanation:-When you want to estimate the costs of Amazon CloudFront consider the following:
** Data Transfer Out.
** Traffic distribution.
** Number of requests.

● Storage Class

✓ Number of Requests

Explanation:-When you want to estimate the costs of Amazon CloudFront consider the following:
** Data Transfer Out.
** Traffic distribution.
** Number of requests.

● Instance type

● Number of Volumes

Q57)

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 Subnets

✓ Security Groups and NACLs

Explanation:-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.

● Security Groups and Internet Gateways

● NACLs and Traffic Manager

Q58) Which service can be used to route end users to the nearest datacenter to reduce latency?

● AWS Cloud9

✓ Amazon Route 53

Explanation:-When you use multiple AWS Regions, you can reduce latency for your users by serving their requests from the AWS Region for which network latency is lowest. Amazon Route 53 latency-based routing lets you use Domain Name System (DNS) to route user requests to the AWS Region that will give your users the fastest response.

● AWS Systems Manager

● Amazon Cognito

Q59) You are working as a site reliability engineer (SRE), which of the following services helps monitor your applications?

● Amazon CloudSearch

✓ Amazon CloudWatch

Explanation:-Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.

● Amazon CloudHSM

● Amazon Elastic MapReduce

Q60) Which of the below is a best-practice when designing solutions on AWS?

● Provision a large compute capacity to handle any spikes in load

✓ Automate wherever possible to make architectural experimentation easier

Explanation:-The Well-Architected Framework identifies a set of general design principles to facilitate good design in the cloud:
1- Stop guessing your capacity needs: Eliminate guessing about your infrastructure capacity needs. When you make a capacity decision before you deploy a system, you might end up sitting on expensive idle resources or dealing with the performance implications of limited capacity. With cloud computing, these problems can go away. You can use as much or as little capacity as you need, and scale up and down automatically.
2- Test systems at production scale: In the cloud, you can create a production-scale test environment on demand, complete your testing, and then decommission the resources. Because you only pay for the test environment when it's running, you can simulate your live environment for a fraction of the cost of testing on premises.
3- Automate to make architectural experimentation easier: Automation allows you to create and replicate your systems at low cost and avoid the expense of manual effort. You can track changes to your automation, audit the impact, and revert to previous parameters when necessary.
4- Allow for evolutionary architectures: Allow for evolutionary architectures. In a traditional environment, architectural decisions are often implemented as static, one-time events, with a few major versions of a system during its lifetime. As a business and its context continue to change, these initial decisions might hinder the system's ability to deliver changing business requirements. In the cloud, the capability to automate and test on demand lowers the risk of impact from design changes. This allows systems to evolve over time so that businesses can take advantage of innovations as a standard practice.
5- Drive architectures using data: In the cloud you can collect data on how your architectural choices affect the behavior of your workload. This lets you make fact-based decisions on how to improve your workload. Your cloud infrastructure is code, so you can use that data to inform your architecture choices and improvements over time.
6- Improve through game days: Test how your architecture and processes perform by regularly scheduling game days to simulate events in production. This will help you understand where improvements can be made and can help develop organizational experience in dealing with events.

● Invest heavily in architecting your environment, as it is not easy to change your design later

● Use AWS reservations to reduce costs when testing your production environment

---

Q61) One of the most important AWS best-practices to follow is the cloud architecture principle of elasticity. How does following this principle improve your architecture's design?

● By automatically scaling your on-premises resources based on changes in demand

✓ By automatically provisioning the required AWS resources based on changes in demand

Explanation:-Before cloud computing, you had to overprovision infrastructure to ensure you had enough capacity to handle your business operations at the peak level of activity. Now, you can provision the amount of resources that you actually need, knowing you can instantly scale up or down with the needs of your business. This reduces costs and improves your ability to meet your users' demands.

The concept of Elasticity involves the ability of a service to automatically scale its resources up or down based on changes in demand. For example, Amazon EC2 Autoscaling can help automate the process of adding or removing Amazon EC2 instances as demand increases or decreases.

● By reducing interdependencies between application components wherever possible

● By automatically scaling your AWS resources using the Elastic Load Balancer

---

Q62)

In order to implement best practices when dealing with a "Single Point of Failure," you should aim to build as much automation as possible in both detecting and reacting to failure.

Which of the following AWS services would help? (Choose two)

● Amazon Athena

● Amazon EC2

✓ Auto Scaling

Explanation:-You should aim to build as much automation as possible in both detecting and reacting to failure. You can use services like ELB and Amazon Route53 to configure health checks and mask failure by only routing traffic to healthy endpoints. In addition, Auto Scaling can be configured to automatically replace unhealthy nodes. You can also replace unhealthy nodes using the Amazon EC2 auto-recovery feature or services such as AWS OpsWorks and AWS Elastic Beanstalk. It won't be possible to predict every possible failure scenario on day one. Make sure you collect enough logs and metrics to understand normal system behavior. After you understand that, you will be able to set up alarms that trigger automated response or manual intervention.

● ECR

✓ ELB

Explanation:-You should aim to build as much automation as possible in both detecting and reacting to failure. You can use services like ELB and Amazon Route53 to configure health checks and mask failure by only routing traffic to healthy endpoints. In addition, Auto Scaling can be configured to automatically replace unhealthy nodes. You can also replace unhealthy nodes using the Amazon EC2 auto-recovery feature or services such as AWS OpsWorks and AWS Elastic Beanstalk. It won't be possible to predict every possible failure scenario on day one. Make sure you collect enough logs and metrics to understand normal system behavior. After you understand that, you will be able to set up alarms that trigger automated response or manual intervention.

Q63) A company has developed an eCommerce web application in AWS. What should they do to ensure that the application has the highest level of availability?

● Deploy the application across multiple VPC's and subnets

● Deploy the application across multiple Availability Zones and Edge locations

● Deploy the application across multiple Availability Zones and subnets

✓ Deploy the application across multiple Regions and Availability Zones

Explanation:-The AWS Global infrastructure is built around Regions and Availability Zones (AZs). Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones. Availability Zones in a region are connected with low latency, high throughput, and highly redundant networking. These Availability Zones offer AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures.

In addition to replicating applications and data across multiple data centers in the same Region using Availability Zones, you can also choose to increase redundancy and fault tolerance further by replicating data between geographic Regions (especially if you are serving customers from all over the world). You can do so using both private, high speed networking and public internet connections to provide an additional layer of business continuity, or to provide low latency access across the globe.

Q64) The principle "design for failure and nothing will fail" is very important when designing your AWS Cloud architecture. Which of the following would help adhere to this principle? (Choose two)

● AWS KMS

● Amazon Elastic File System

✓ AWS Elastic Load Balancer

Explanation:-Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones. When designing your AWS Cloud architecture, you should make sure that your system will continue to run even if failures happen. You can achieve this by deploying your AWS resources in multiple Availability zones. Availability zones are isolated from each other, therefore if one availability zone goes down, the other AZ's will still be up and running and hence your application will be more fault tolerant. In addition to availability zones you can build a disaster recovery solution by deploying your AWS resources in other regions. If an entire region goes down you will still have resources in another region able to continue to provide a solution. Finally, you can use the Elastic Load Balancer to regularly perform health checks and distribute traffic only to the healthy instances.

● Amazon Elastic MapReduce

✓ Availability Zones

Explanation:-Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones. When designing your AWS Cloud architecture, you should make sure that your system will continue to run even if failures happen. You can achieve this by deploying your AWS resources in multiple Availability zones. Availability zones are isolated from each other, therefore if one availability zone goes down, the other AZ's will still be up and running and hence your application will be more fault tolerant. In addition to availability zones you can build a disaster recovery solution by deploying your AWS resources in other regions. If an entire region goes down you will still have resources in another region able to continue to provide a solution. Finally, you can use the Elastic Load Balancer to regularly perform health checks and distribute traffic only to the healthy instances.

Q65) Adjusting compute capacity dynamically to reduce cost is an implementation of which AWS cloud best practice?

● Build security in every layer

● Parallelize tasks

✓ Implement elasticity

Explanation:-In the traditional data center-based model of IT, once infrastructure is deployed, it typically runs whether it is needed or not, and all the capacity is paid for, regardless of how much it gets used. In the cloud, resources are elastic, meaning they can instantly grow (to maintain performance) or shrink (to reduce costs).

● Adopt monolithic architecture