Answer Sheet

Q1) 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

---

Q2) 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

Q3) 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

Q4) 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

---

Q5) 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.

Q6) Which of the following would you use to manage your encryption keys in the AWS Cloud? (Choose two)

- AWS CodeDeploy
- AWS Certificate Manager
- AWS CodeCommit
- ✅ AWS KMS

Explanation:-AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses FIPS 140-2 validated hardware security modules to protect the security of your keys. AWS Key Management Service is integrated with most other AWS services to help you protect the data you store with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
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. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries.

- ✅ CloudHSM

Explanation:-AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses FIPS 140-2 validated hardware security modules to protect the security of your keys. AWS Key Management Service is integrated with most other AWS services to help you protect the data you store with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
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. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries.

Q7) Which of the following services gives you access to all AWS auditor-issued reports and certifications?

- ✅ 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. Reports available in AWS Artifact include AWS Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).
a comperhenAccess all of AWS' auditor issued reports, certifications, accreditations and other third-party attestations.

- Amazon CloudWatch
- AWS CloudTrail
- AWS Config

Q8) A company has infrastructure hosted in an on-premises data center. They currently have an operations team that takes care of ID management. If they decide to migrate to the AWS cloud, which of the following services would help them perform the same role in AWS?

- Amazon Redshift
- ✅ AWS IAM

Explanation:-AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

- AWS Federation
- AWS X-Ray

Q9) What can you use to assign permissions to an IAM user?

- IAM Group
- ✅ IAM Policy

Explanation:-The policy is a JSON document that consists of:
1- Actions: what actions you will allow. Each AWS service has its own set of actions.
2- Resources: which resources you allow the action on.
3- Effect: what will be the effect when the user requests access—either allow or deny.
4- Conditions – which conditions must be present for the policy to take effect. For example, you might allow access only to the specific S3 buckets if the user is connecting from a specific IP range or has used multi-factor authentication at login.

- IAM Role
- IAM Identity

Q10) What best describes penetration testing?

- Testing your instances to check for the unhealthy ones
- Testing your software for bugs and errors
- ✅ Testing your network to find security vulnerabilities that an attacker could exploit

Explanation:-Penetration testing is the practice of testing a network or web application to find security vulnerabilities that an attacker could exploit.

- Testing your application's response time from different locations

---

Q11) Which of the following strategies helps protect your AWS root account?

- Apply MFA for the root account and use it for all of your work
- Only share your AWS account password or access keys with trusted persons
- ✅ Don't create an access key unless you need to

Explanation:-Anyone who has root user access keys for your AWS account has unrestricted access to all the resources in your account, including billing information. If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. If you do have an access key for your AWS account root user, delete it. If you must keep it, rotate (change) the access key regularly.

- Access the root account only from your personal Mobile Phone

---

Q12) Which of the following services provide real-time auditing for compliance and vulnerabilities? (Choose two)

- Amazon Redshift
- Amazon MQ
- ✅ AWS Trusted Advisor

Explanation:-Services like AWS Config, Amazon Inspector, and AWS Trusted Advisor continually monitor for compliance or vulnerabilities giving you a clear overview of which IT resources are in compliance, and which are not. With AWS Config rules you will also know if some component was out of compliance even for a brief period of time, making both point-in-time and period-in-time audits very effective.

- ✅ AWS Config

Explanation:-Services like AWS Config, Amazon Inspector, and AWS Trusted Advisor continually monitor for compliance or vulnerabilities giving you a clear overview of which IT resources are in compliance, and which are not. With AWS Config rules you will also know if some component was out of compliance even for a brief period of time, making both point-in-time and period-in-time audits very effective.

- Amazon Cognito

Q13) What are some key advantages of AWS security? (Choose two)

- All data is encrypted automatically on the server side
- Performed automatically
- Completely free
- ✅ Helps organizations to meet their compliance requirements

Explanation:-The Benefits of AWS Security include :
1- Keep Your Data Safe: The AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure AWS data centers.
2- Meet Compliance Requirements: AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
3- Save Money: Cut costs by using AWS data centers. Maintain the highest standard of security without having to manage your own facility.
4- Scale Quickly: Security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.

- ✅ Save money

Explanation:-The Benefits of AWS Security include :
1- Keep Your Data Safe: The AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure AWS data centers.
2- Meet Compliance Requirements: AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
3- Save Money: Cut costs by using AWS data centers. Maintain the highest standard of security without having to manage your own facility.
4- Scale Quickly: Security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.

Q14) Which statement is true in relation to security?

- ✅ AWS cannot access users' data

Explanation:-AWS has no idea about the user data and cannot read any data even if they wanted to. All data are protected by the customer access keys and secret access keys and the user's encryption methods.

- AWS manages everything related to the operating system
- AWS is responsible for the security of your application
- Server side encryption is the responsibility of AWS

Q15) What are the benefits of AWS Organizations? (Choose two)

- Help organizations achieve their desired business outcomes with AWS
- Help organizations design and travel an accelerated path to successful cloud adoption
- ✅ Control access to AWS services

Explanation:-AWS Organizations has five main benefits:
1) Centrally manage access polices across multiple AWS accounts.
2) Automate AWS account creation and management.
3) Control access to AWS services.
4) Consolidate billing across multiple AWS accounts.
5) Configure AWS services across multiple accounts.
** Control access to AWS services: AWS Organizations allows you to restrict what services and actions are allowed in your accounts. You can use Service Control Policies (SCPs) to apply permission guardrails on AWS Identity and Access Management (IAM) users and roles. For example, you can apply an SCP that restricts users in accounts in your organization from launching any resources in regions that you do not explicitly allow.
** Consolidate billing across multiple AWS accounts: You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon EC2 and Amazon S3.

- ✅ Consolidate billing across multiple AWS accounts

Explanation:-AWS Organizations has five main benefits:
1) Centrally manage access polices across multiple AWS accounts.

2) Automate AWS account creation and management.
3) Control access to AWS services.
4) Consolidate billing across multiple AWS accounts.
5) Configure AWS services across multiple accounts.
** Control access to AWS services: AWS Organizations allows you to restrict what services and actions are allowed in your accounts. You can use Service Control Policies (SCPs) to apply permission guardrails on AWS Identity and Access Management (IAM) users and roles. For example, you can apply an SCP that restricts users in accounts in your organization from launching any resources in regions that you do not explicitly allow.
** Consolidate billing across multiple AWS accounts: You can use AWS Organizations to set up a single payment method for all the AWS accounts in your organization through consolidated billing. With consolidated billing, you can see a combined view of charges incurred by all your accounts, as well as take advantage of pricing benefits from aggregated usage, such as volume discounts for Amazon EC2 and Amazon S3.
- Manage your organization's payment methods

Q16) Which feature enables users to sign in to their AWS accounts with their existing corporate credentials?

- Access keys
- Amazon Cognito
- ✅ Federation

Explanation:-With Federation, you can use single sign-on (SSO) to access your AWS accounts using credentials from your corporate directory. Federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML), to exchange identity and security information between an identity provider (IdP) and an application.
AWS offers multiple options for federating your identities in AWS:
1- AWS Identity and Access Management (IAM): You can use AWS Identity and Access Management (IAM) to enable users to sign in to their AWS accounts with their existing corporate credentials.
2- AWS Directory Service: AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft AD, uses secure Windows trusts to enable users to sign in to the AWS Management Console, AWS Command Line Interface (CLI), and Windows applications running on AWS using their existing corporate Microsoft Active Directory credentials.
- IAM Permissions

Q17) Which of the following can an AWS customer use to know more about prohibited uses of the web services offered by AWS?

- AWS CloudTrail
- AWS Artifact
- ✅ AWS Acceptable Use Policy

Explanation:-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. If you violate the Policy or authorize or help others to do so, AWS may suspend or terminate your use of the Services.
- AWS Budgets

Q18)

The AWS account administrator of your company has been fired. With the permissions granted to him as an administrator, he was able to create multiple IAM user accounts and access keys. Additionally, you are not sure whether he has access to the AWS root account or not.

What should you do immediately to protect your AWS infrastructure? (Choose two)

- Delete all IAM accounts and recreate others
- Download all the attached policies in a safe place
- ✅ Put IP restriction on all Users' accounts

Explanation:-To protect your AWS infrastructure in this situation you should lock down your root user and all accounts that the administrator had access to.
Here are some ways to do that:
1- Change the user name and the password of the root user account and all of the IAM accounts that the administrator has access to.
2- Rotate (change) all access keys for those accounts.
3- Enable MFA on those accounts.
4- Put IP restriction on all Users' accounts.
- ✅ Change the user name and the password and create MFA for the root account

Explanation:-To protect your AWS infrastructure in this situation you should lock down your root user and all accounts that the administrator had access to.
Here are some ways to do that:
1- Change the user name and the password of the root user account and all of the IAM accounts that the administrator has access to.
2- Rotate (change) all access keys for those accounts.
3- Enable MFA on those accounts.
4- Put IP restriction on all Users' accounts.
- Use the CloudWatch service to check all the API calls that have been made in your account since the administrator was fired

---

Q19) Which of the following requires an access key and a security access key to get programmatic access to AWS resources? (Choose two)

- IAM group
- IAM role
- ✅ AWS account root user

Explanation:-An AWS IAM user might need to make API calls or use the AWS CLI. In that case, you need to create an access key (access key ID and a secret access key) for that user. You can create IAM user access keys with the IAM console, AWS CLI,or AWS API.
To create access keys for your AWS account root user, you must use the AWS Management Console.
- ✅ IAM user

Explanation:-An AWS IAM user might need to make API calls or use the AWS CLI. In that case, you need to create an access key (access key ID and a secret access key) for that user. You can create IAM user access keys with the IAM console, AWS CLI,or AWS API.
To create access keys for your AWS account root user, you must use the AWS Management Console.

- TAM

Q20) How does AWS support customer compliance?

- It's not possible to meet regulatory compliance requirements in the Cloud
- ✅ AWS has achieved a number of common assurance certifications such as ISO 9001 and HIPAA

Explanation:-AWS environments are continuously audited, and its infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries, including PCI DSS, ISO 2700, ISO 9001, and HIPAA. You can use these certifications to validate the implementation and effectiveness of AWS security controls. For example, AWS companies that use AWS products and services to handle credit card information can rely on AWS technology infrastructure as they manage their PCI DSS compliance certification.

- AWS applies the most common Cloud security standards, and is responsible for complying with customers' applicable laws and regulations
- Many AWS services are assessed regularly to comply with local laws and regulations

---

Q21) Which of the following services enables you to easily generate and use your own encryption keys in the AWS Cloud?

- AWS Certificate Manager
- ✅ AWS CloudHSM

Explanation:-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 Shield
- AWS WAF

Q22) What are the services that AWS provide to protect against network and application layer DDoS attacks? (Choose two)

- AWS Systems Manager
- ✅ AWS Web Application Firewall

Explanation:-Amazon CloudFront, AWS Shield, AWS Web Application Firewall (WAF), and Amazon Route 53 work seamlessly together to create a flexible, layered security perimeter against multiple types of attacks including network and application layer DDoS attacks. All of these services are co-resident at the AWS edge location and provide a scalable, reliable, and high-performance security perimeter for your applications and content.
Additional information:
AWS Shield provides always-on DDoS detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications.

- Amazon EFS
- AWS Secrets Manager
- ✅ Amazon CloudFront

Explanation:-Amazon CloudFront, AWS Shield, AWS Web Application Firewall (WAF), and Amazon Route 53 work seamlessly together to create a flexible, layered security perimeter against multiple types of attacks including network and application layer DDoS attacks. All of these services are co-resident at the AWS edge location and provide a scalable, reliable, and high-performance security perimeter for your applications and content.
Additional information:
AWS Shield provides always-on DDoS detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications.

Q23) Which of the following services is used during the process of encrypting EBS volumes?

- Amazon ECR
- ✅ AWS KMS

Explanation:-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. You can use the AWS Key Management Service (AWS KMS) to create and control the encryption keys used to encrypt your data. AWS Key Management Service is also integrated with other AWS services including Amazon S3, and Amazon Redshift, to make it simple to encrypt your data with encryption keys that you manage.

- Amazon GuardDuty
- AWS WAF

Q24) What are the main differences between an IAM user and an IAM role? (Choose two)

- A role is uniquely associated with only one person, however an IAM user is intended to be assumable by anyone who needs it
- ✅ An IAM user has permanent credentials associated with it, however a role has temporary credentials associated with it

Explanation:-An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user.

- Using IAM users is more cost effective than IAM roles
- An IAM user has temporary credentials associated with it, however a role has permanent credentials associated with it
- ✅ An IAM user is uniquely associated with only one person, however a role is intended to be assumable by anyone who needs it

Explanation:-An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user.

Q25) Which of the following security resources are available for free? (Choose two)

- AWS Classroom Training
- ✅ AWS Security Blog

Explanation:-The AWS free security resources include AWS Security Blog, Whitepapers, Developer Documents, Articles and Tutorials, Training, Security Bulletins, Compliance Resources and Testimonials.

- ✅ AWS Bulletins

Explanation:-The AWS free security resources include AWS Security Blog, Whitepapers, Developer Documents, Articles and Tutorials, Training, Security Bulletins, Compliance Resources and Testimonials.

- AWS re:Invent
- AWS TAM

Q26) Which of the following are important design principles you should adopt when designing systems on AWS? (Choose two)

- Always use Global Services in your architecture rather than Regional Services
- Always choose to pay as you go
- Treat servers as fixed resources
- ✅ Automate wherever possible

Explanation:-A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. You can remove single points of failure by assuming everything will fail and designing your architecture to automatically detect react to failures. For example, configuring and deploying an auto-scaling group of EC2 instances will ensure that if one or more of the instances crashes, Auto-scaling will automatically replace them with new instances. You should also introduce redundancy to remove single points of failure, by deploying your application across multiple Availability Zones. If one Availability Zone goes down for any reason, the other Availability Zones can serve requests.
AWS helps you use automation so you can build faster and more efficiently. Using AWS services, you can automate manual tasks or processes such as deployments, development & test workflows, container management, and configuration management.

- ✅ Remove single points of failure

Explanation:-A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. You can remove single points of failure by assuming everything will fail and designing your architecture to automatically detect react to failures. For example, configuring and deploying an auto-scaling group of EC2 instances will ensure that if one or more of the instances crashes, Auto-scaling will automatically replace them with new instances. You should also introduce redundancy to remove single points of failure, by deploying your application across multiple Availability Zones. If one Availability Zone goes down for any reason, the other Availability Zones can serve requests.
AWS helps you use automation so you can build faster and more efficiently. Using AWS services, you can automate manual tasks or processes such as deployments, development & test workflows, container management, and configuration management.

Q27) Which of the following AWS services is designed with native Multi-AZ fault tolerance in mind? (Choose two)

- Amazon Redshift
- ✅ Amazon DynamoDB

Explanation:-The Multi-AZ principle involves deploying an AWS resource in multiple Availability Zones to achieve high availability for that resource. DynamoDB automatically spreads the data and traffic for your tables over a sufficient number of servers to handle your throughput and storage requirements, while maintaining consistent and fast performance. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in fault tolerance in the event of a server failure or Availability Zone outage.
Amazon S3 provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects. Data in all Amazon S3 storage classes is redundantly stored across multiple Availability Zones (except S3 One Zone-IA).

- ✅ Amazon Simple Storage Service

Explanation:-The Multi-AZ principle involves deploying an AWS resource in multiple Availability Zones to achieve high availability for that resource. DynamoDB automatically spreads the data and traffic for your tables over a sufficient number of servers to handle your throughput and storage requirements, while maintaining consistent and fast performance. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in fault tolerance in the event of a server failure or Availability Zone outage.
Amazon S3 provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects. Data in all Amazon S3 storage classes is redundantly stored across multiple Availability Zones (except S3 One Zone-IA).

- Amazon EBS
- AWS Snowball

Q28) A company is developing an application that will leverage facial recognition to automate photo tagging. Which AWS Service should the company use for facial recognition?

- Amazon Polly
- AWS IAM
- ✅ Amazon Rekognition

Explanation:-Amazon Rekognition is a service that makes it easy to add image analysis to your applications. With Rekognition, you can detect objects, scenes, and faces in images. You can also search and compare faces. The Amazon Rekognition API enables you to quickly add sophisticated deep-learning-based visual search and image classification to your applications.

- Amazon Kinesis

Q29) You are facing a lot of problems with your current contact center. Which service provides a cloud-based contact center that can deliver a better service for your customers?

- AWS Direct Connect
- ✅ Amazon Connect

Explanation:-Amazon Connect is a cloud-based contact center solution. Amazon Connect makes it easy to set up and manage a customer contact center and provide reliable customer engagement at any scale. You can set up a contact center in just a few steps, add agents from anywhere, and start to engage with your customers right away. Amazon Connect provides rich metrics and real-time reporting that allow you to optimize contact routing. You can also resolve customer issues more efficiently by putting customers in touch with the right agents. Amazon Connect integrates with your existing systems and business applications to provide visibility and insight into all of your customer interactions.

- AWS Elastic Beanstalk
- Amazon Lightsail

Q30)

You are working as a web app developer. You are currently facing issues in media playback for mobile devices. The problem is that the current format of your media does not support playback on mobile devices.

Which of the following AWS services can help you in this regard?

- Amazon Rekognition
- Amazon Pinpoint
- ✅ Amazon Elastic Transcoder

Explanation:-Amazon Elastic Transcoder is media transcoding in the cloud. It is designed to be a highly scalable, easy-to-use, and cost-effective way for developers and businesses to convert (or transcode) media files from their source format into versions that will play back on devices like smartphones, tablets, and PCs.

- Amazon S3

Q31) An organization has a legacy application designed using monolithic-based architecture. Which AWS Service can be used to decouple the components of the application?

- Amazon CloudFront
- AWS Artifact
- ✅ Amazon SQS

Explanation:-A monolithic application is designed to be self-contained; components of the application are interconnected and interdependent rather than loosely coupled as is the case with Microservices applications.
With monolithic architectures, all processes are tightly-coupled and run as a single service. This means that if one process of the application experiences a spike in demand, the entire architecture must be scaled. Adding or improving a monolithic application's features becomes more complex as the code base grows. This complexity limits experimentation and makes it difficult to implement new ideas. Monolithic architectures add risk for application availability because many dependent and tightly coupled processes increase the impact of a single process failure.
With a microservices architecture, an application is built as loosely-coupled components that run each application process as a service. These services communicate via a well-defined interface using lightweight APIs. Services are built for business capabilities and each service performs a single function. Because they are independently run, each service can be updated, deployed, and scaled to meet demand for specific functions of an application. Microservices architectures make applications easier to scale and faster to develop, enabling innovation and accelerating time-to-market for new features.
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS offers a reliable, highly-scalable hosted queue for storing messages as they travel between applications or microservices. It moves data between distributed application components and helps you decouple these components.

- Virtual Private Gateway

Q32) You need to migrate a large number of on-premises workloads to AWS. Which of the following is the fastest way to achieve your goal?

- Use the AWS Database Migration Service
- Use the AWS File Transfer Acceleration feature
- ✅ Use the AWS Server Migration Service

Explanation:-AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. AWS SMS allows you to automate, schedule, and track incremental replications of live server volumes, making it easier for you to coordinate large-scale server migrations.

- Use the AWS Application Discovery Service

Q33) 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

Q34) A company has deployed a new web application on multiple Amazon EC2 instances. Which of the following should they use to ensure that the incoming HTTP traffic is distributed evenly across the instances?

- AWS Auto Scaling
- ✅ AWS Application Load Balancer

Explanation:-Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. Elastic Load Balancing offers three types of load balancers: 1- Application Load Balancer. 2- Network Load Balancer. 3- Classic Load Balancer. Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic. In our case, the application receives HTTP traffic. Hence, the Application Load Balancer is the correct answer here.

- AWS Network Load Balancer
- AWS EC2 Auto Recovery

Q35) Which AWS Service can be used to register a new domain name?

- AWS KMS
- Amazon ECR
- ✅ Amazon Route 53

Explanation:-Route53 allows for registration of new domain names in AWS. Amazon Route 53 is a global service that provides a highly available and scalable Domain Name System (DNS) in the Cloud. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.
Route 53 also simplifies the hybrid cloud by providing recursive DNS for your Amazon VPC and on-premises networks over AWS Direct Connect or AWS VPN.

- AWS Config

Q36) Which AWS Service creates a virtual network in AWS?

- Amazon VPS
- ✅ Amazon VPC

Explanation:-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 Direct Connect
- AWS VPN

Q37) Which of the following is used to control network traffic in AWS? (Choose two)

- IAM Policies
- ✅ Network Access Control Lists (NACLs)

Explanation:-You can control network traffic in AWS by configuring security groups, network access control lists, and route tables.
1- Security groups: Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.
2- Network access control lists (ACLs): Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
3- Route Tables: A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.

- Key Pairs
- Access Keys
- ✅ Security Groups

Explanation:-You can control network traffic in AWS by configuring security groups, network access control lists, and route tables.
1- Security groups: Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.
2- Network access control lists (ACLs): Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
3- Route Tables: A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.

Q38) How do ELBs improve the reliability of your application?

- By replicating data to multiple availability zones
- By creating database Read Replicas
- ✅ By ensuring that only healthy targets receive traffic

Explanation:-The reliability term encompasses the ability of a system to recover from infrastructure or service disruptions, and dynamically acquire computing resources to meet demand. ELBs continuously perform health checks on the registered targets (such as Amazon EC2 instances) and only routes traffic to the healthy ones. This increases the fault tolerance of your application and makes it more reliable.

- By distributing traffic across multiple S3 buckets

Q39) Which AWS Service can perform health checks on Amazon EC2 instances?

- Amazon Chime
- AWS CloudFormation
- Amazon Aurora
- ✅ Amazon Route 53

Explanation:-Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet

applications by translating names like example.com into the numeric IP addresses, such as 192.0.2.1, that computers use to connect to each other. Route 53 also offers health checks to monitor the health and performance of your application as well as your web servers and other resources. Route 53 can be configured to route traffic only to the healthy endpoints to achieve greater levels of fault tolerance in your applications.

Q40) Which of the below options are use cases of the Amazon Route 53 service? (Choose TWO)

- Point-to-point connectivity between an on-premises data center and AWS
- ✅ DNS configuration and management

Explanation:-Amazon Route 53 is AWS's domain and DNS management service. You can use it to register new domain names, as well as manage your Domain Name System (DNS) in the Cloud.
Amazon Route 53 also simplifies the hybrid cloud by providing recursive DNS for your Amazon VPC and on-premises networks over AWS Direct Connect or AWS VPN.

- ✅ Domain Registration

Explanation:-Amazon Route 53 is AWS's domain and DNS management service. You can use it to register new domain names, as well as manage your Domain Name System (DNS) in the Cloud.
Amazon Route 53 also simplifies the hybrid cloud by providing recursive DNS for your Amazon VPC and on-premises networks over AWS Direct Connect or AWS VPN.

- Detects configuration changes in the AWS environment
- Provides infrastructure security optimization recommendations

---

Q41)

A company has a web application that is hosted on a single EC2 instance and is approaching 100 percent CPU Utilization during peak loads. Rather than scaling the server vertically, the company has decided to deploy three Amazon EC2 instances in parallel and to distribute traffic across the three servers.

What AWS Service should the company use to distribute the traffic evenly?

- AWS Global Accelerator
- Amazon CloudFront
- ✅ AWS Application Load Balancer (ALB)

Explanation:-AWS Application Load Balancer (ALB) is part of the AWS Elastic Load Balancing family that is specifically designed to handle HTTP and HTTPS traffic. An ALB automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. Once you register the Amazon EC2 instances with the ALB, it automatically distributes the incoming traffic across those instances. The Load Balancer also performs health checks on the instances and routes traffic only to the healthy ones.

- Transit VPC

Q42) Which of the below options is true of Amazon VPC?

- AWS is responsible for all the management and configuration details of Amazon VPC
- ✅ AWS Customers have complete control over their Amazon VPC virtual networking environment

Explanation:-Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

- Amazon VPC allows customers to control user interactions with all other AWS resources
- Amazon VPC helps customers to review their AWS architecture and adopt best practices

---

Q43) Which service can you use to route traffic to the endpoint that provides the best application performance for your users worldwide?

- AWS Transfer Acceleration
- AWS Data Pipeline
- ✅ AWS Global Accelerator

Explanation:-AWS Global Accelerator is a networking service that improves the availability and performance of the applications that you offer to your global users. Today, if you deliver applications to your global users over the public internet, your users might face inconsistent availability and performance as they traverse through multiple public networks to reach your application. These public networks can be congested and each hop can introduce availability and performance risk. AWS Global Accelerator uses the highly available and congestion-free AWS global network to direct internet traffic from your users to your applications on AWS, making your users' experience more consistent. To improve the availability of your application, you must monitor the health of your application endpoints and route traffic only to healthy endpoints. AWS Global Accelerator improves application availability by continuously monitoring the health of your application endpoints and routing traffic to the closest healthy endpoints.

- AWS DAX Accelerator
