Free Questions for CLF-C02

Shared by Crosby on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which AWS Cloud Adoption Framework (AWS CAF) capability belongs to the people perspective?

Options:

A- Data architecture
B- Event management
C- Cloud fluency
D- Strategic partnership

Answer:

C

Explanation:

Cloud fluency is a capability that belongs to the people perspective of the AWS Cloud Adoption Framework (AWS CAF). Cloud fluency is the ability of the workforce to understand the benefits, challenges, and best practices of cloud computing, and to apply them to their roles and responsibilities. Cloud fluency helps the organization to adopt a cloud mindset, culture, and skills, and to leverage the full potential of the cloud. Cloud fluency can be achieved through various methods, such as training, certification, mentoring, coaching, and hands-on experience. Cloud fluency is one of the four capabilities of the people perspective, along with culture, organizational structure, and leadership. The other three capabilities belong to different perspectives of the AWS CAF. Data architecture is a capability of the platform perspective, which helps you design and implement data solutions that meet your business and technical requirements. Event management is a capability of the operations perspective, which helps you monitor and respond to events that affect the availability, performance, and security of your cloud resources. Strategic partnership is a capability of the business perspective, which helps you establish and maintain relationships with external stakeholders, such as customers, partners, suppliers, and regulators, to create value and achieve your business goals.References:AWS Cloud Adoption Framework: People Perspective,AWS CAF - Cloud Adoption Framework - W3Schools

Question 2

Question Type: MultipleChoice

Which AWS service supports a hybrid architecture that gives users the ability to extend AWS infrastructure, AWS services, APIs, and tools to data centers, co-location environments, or on-premises facilities?

Options:

A- AWS Snowmobile
B- AWS Local Zones
C- AWS Outposts
D- AWS Fargate

Answer:

C

Explanation:

AWS Outposts is a service that delivers AWS infrastructure and services to virtually any on-premises or edge location for a truly consistent hybrid experience. AWS Outposts allows you to extend and run native AWS services on premises, and is available in a variety of form factors, from 1U and 2U Outposts servers to 42U Outposts racks, and multiple rack deployments. With AWS Outposts, you can run some AWS services locally and connect to a broad range of services available in the local AWS Region.Run applications and workloads on premises using familiar AWS services, tools, and APIs2. AWS Outposts is the only AWS service that supports a hybrid architecture that gives users the ability to extend AWS infrastructure, AWS services, APIs, and tools to data centers, co-location environments, or on-premises facilities.References:On-Premises Infrastructure - AWS Outposts Family

Question 3

Question Type: MultipleChoice

A company wants to receive a notification when a specific AWS cost threshold is reached.

Which AWS services or tools can the company use to meet this requirement? (Select TWO.)

Options:

A- Amazon Simple Queue Service (Amazon SQS)

B- AWS Budgets
C- Cost Explorer
D- Amazon CloudWatch
E- AWS Cost and Usage Report

Answer:

B, D

Explanation:

AWS Budgets and Amazon CloudWatch are two AWS services or tools that the company can use to receive a notification when a specific AWS cost threshold is reached. AWS Budgets allows users to set custom budgets to track their costs and usage, and respond quickly to alerts received from email or Amazon Simple Notification Service (Amazon SNS) notifications if they exceed their threshold. Users can create cost budgets with fixed or variable target amounts, and configure their notifications for actual or forecasted spend. Users can also set up custom actions to run automatically or through an approval process when a budget target is exceeded. For example, users could automatically apply a custom IAM policy that denies them the ability to provision additional resources within an account. Amazon CloudWatch is a service that monitors applications, responds to performance changes, optimizes resource use, and provides insights into operational health. Users can use CloudWatch to collect and track metrics, which are variables they can measure for their resources and applications. Users can create alarms that watch metrics and send notifications or automatically make changes to the resources they are monitoring when a threshold is breached. Users can use CloudWatch to monitor their AWS costs and usage by creating billing alarms that send notifications when their estimated charges exceed a specified threshold amount. Users can also use CloudWatch to monitor their Reserved Instance (RI) or Savings Plans utilization and coverage, and receive notifications when they fall below a certain level.

References:Cloud Cost And Usage Budgets - AWS Budgets,What is Amazon CloudWatch?,Creating a billing alarm - Amazon CloudWatch

Question 4

Question Type: MultipleChoice

A network engineer needs to build a hybrid cloud architecture connecting on-premises networks to the AWS Cloud using AWS Direct Connect. The company has a few VPCs in a single AWS Region and expects to increase the number of VPCs to hundreds over time.

Which AWS service or feature should the engineer use to simplify and scale this connectivity as the VPCs increase in number?

Options:

A- VPC endpoints
B- AWS Transit Gateway
C- Amazon Route 53
D- AWS Secrets Manager

Answer:

B

Explanation:

AWS Transit Gateway is a network transit hub that you can use to interconnect your VPCs and on-premises networks through a central gateway. AWS Transit Gateway simplifies and scales the connectivity between your on-premises networks and AWS, as you only need to create and manage a single connection from the central gateway to each on-premises network, rather than individual connections to each VPC.You can also use AWS Transit Gateway to connect to other AWS services, such as Amazon S3, Amazon DynamoDB, and AWS PrivateLink12.AWS Transit Gateway supports thousands of VPCs per gateway, and enables you to peer Transit Gateways across AWS Regions3.

The other options are not AWS services or features that can simplify and scale the connectivity between on-premises networks and hundreds of VPCs using AWS Direct Connect.VPC endpoints enable private connectivity between your VPCs and supported AWS services, but do not support on-premises networks4.Amazon Route 53 is a DNS service that helps you route internet traffic to your resources, but does not provide network connectivity5.AWS Secrets Manager is a service that helps you securely store and manage secrets, such as database credentials and API keys, but does not relate to network connectivity

Question 5

Question Type: MultipleChoice

Which AWS Cloud benefit is shown by an architecture's ability to withstand failures with minimal downtime?

Options:

A- Agility
B- Elasticity
C- Scalability
D- High availability

Answer:

D

Explanation:

Understanding High Availability: High availability (HA) refers to systems that are durable and likely to operate continuously without failure for a long time. HA ensures that an architecture can withstand failures with minimal downtime.

Importance of High Availability:

Redundancy: Systems are designed with redundancy to prevent single points of failure.

Fault Tolerance: Ensures that failures do not result in significant downtime, maintaining service continuity.

Automated Recovery: Utilizes automated recovery mechanisms to quickly restore services in the event of a failure.

AWS Services for High Availability:

Multi-AZ Deployments: Services like RDS, DynamoDB, and others support Multi-AZ deployments for fault tolerance.

Elastic Load Balancing: Distributes traffic across multiple instances or availability zones to ensure no single point of failure.

Auto Scaling: Automatically adjusts the number of instances based on demand, ensuring availability even during traffic spikes.

References:

AWS Well-Architected Framework: Reliability

Question 6

Question Type: MultipleChoice

A company wants to monitor for misconfigured security groups that are allowing unrestricted

access to specific ports. Which AWS service will meet this requirement?

Options:

A- AWS Trusted Advisor
B- Amazon CloudWatch
C- Amazon GuardDuty
D- AWS Health Dashboard

Answer:

A

Explanation:

AWS Trusted Advisor is a service that provides real-time guidance to help optimize AWS resources, improve security, and maximize performance. It includes a Security category that can identify security group configurations that allow unrestricted access to specific ports.It offers recommendations and alerts to help remediate misconfigurations and ensure proper security practices1.References:

Amazon CLF-C02: Which AWS service monitor for misconfigured security groups allowing unrestricted access to specific ports - PUPUWEB

Question 7

Question Type: MultipleChoice

Which action is a security best practice for access to sensitive data that is stored in an Amazon S3 bucket?

Options:

A- Enable S3 Cross-Region Replication (CRR) on the S3 bucket.
B- Use IAM roles for applications that require access to the S3 bucket.
C- Configure AWS WAF to prevent unauthorized access to the S3 bucket.
D- Configure Amazon GuardDuty to prevent unauthorized access to the S3 bucket.

Answer:

B

Explanation:

Understanding IAM Roles: IAM (Identity and Access Management) roles in AWS are designed to delegate access permissions without sharing long-term security credentials. This means applications and services can use temporary security credentials, which enhances security.

Why IAM Roles are Best Practice:

Least Privilege Principle: By using IAM roles, you can ensure that applications only have the minimum permissions they need to function, reducing the risk of unauthorized access.

Temporary Credentials: Roles provide temporary security credentials, which reduce the risk if they are compromised compared to long-term access keys.

Automated Rotation: Temporary credentials automatically expire and are rotated, which means you don't have to manage the rotation manually.

How to Implement IAM Roles:

Create an IAM Role: In the AWS Management Console, navigate to IAM, and create a new role. Choose the type of trusted entity (e.g., EC2, Lambda).

Attach Policies: Attach the necessary policies to the role that define the permissions for accessing the S3 bucket.

Assign Role to Service: Attach the IAM role to your EC2 instances, Lambda functions, or other AWS services that need to access the S3 bucket.

Use AWS SDKs: When accessing S3 from your application, use the AWS SDKs to automatically assume the IAM role and obtain temporary credentials.

References:

AWS Identity and Access Management (IAM)

IAM Roles

Question 8

Question Type: MultipleChoice

A company wants to set up its workloads to perform their intended functions and recover quickly from failure. Which pillar of the AWS Well-Architected Framework aligns with these goals?

Options:

A- Performance efficiency
B- Sustainability
C- Reliability
D- Security

Answer:

C

Explanation:

Understanding the Reliability Pillar: The Reliability pillar of the AWS Well-Architected Framework focuses on 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.

Key Concepts of Reliability:

Foundations: Ensure a solid foundation on which to build, including AWS account management, limits, and networking.

Change Management: Manage changes in automation to ensure systems remain reliable during modifications.

Failure Management: Design systems to detect failures and automatically recover from them.

How to Align with Reliability Pillar:

Implement Multi-AZ Deployments: Deploy applications across multiple Availability Zones to ensure fault tolerance.

Use Auto Scaling: Automatically adjust resources to maintain system performance during demand fluctuations.

Monitor and Respond: Implement monitoring and alerting mechanisms using services like CloudWatch to detect and respond to issues proactively.

References:

AWS Well-Architected Framework: Reliability Pillar

Question 9

Question Type: MultipleChoice

According to security best practices, how should an Amazon EC2 instance be given access to an Amazon S3 bucket?

Options:

A- Hard code an IAM user's secret key and access key directly in the application, and upload the file.
B- Store the IAM user's secret key and access key in a text file on the EC2 instance, read the keys, then upload the file.
C- Have the EC2 instance assume a role to obtain the privileges to upload the file.
D- Modify the S3 bucket policy so that any service can upload to it at any time.

Answer:

C

Explanation:

According to security best practices, the best way to give an Amazon EC2 instance access to an Amazon S3 bucket is to have the EC2 instance assume a role to obtain the privileges to upload the file. A role is an AWS Identity and Access Management (IAM) entity that defines a set of permissions for making AWS service requests. You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you can create a role that allows EC2 instances to access S3 buckets, and then attach the role to the EC2 instance. This way, the EC2 instance can assume the role and obtain temporary security credentials to access the S3 bucket. This method is more secure and scalable than storing or hardcoding IAM user credentials on the EC2 instance, as it avoids the risk of exposing or compromising the credentials. It also allows you to manage the permissions centrally and dynamically, and to audit the access using AWS CloudTrail.For more information on how to create and use roles for EC2 instances, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances1

The other options are not recommended for security reasons. Hardcoding or storing IAM user credentials on the EC2 instance is a bad practice, as it exposes the credentials to potential attackers or unauthorized users who can access the instance or the application code. It also makes it difficult to rotate or revoke the credentials, and to track the usage of the credentials. Modifying the S3 bucket policy to allow any service to upload to it at any time is also a bad practice, as it opens the bucket to potential data breaches, data loss, or data corruption. It also violates the principle of least privilege, which states that you should grant only the minimum permissions necessary for a task.

References:Using an IAM role to grant permissions to applications running on Amazon EC2 instances