

# Exam Questions CLF-C02

AWS Certified Cloud Practitioner

<https://www.2passeasy.com/dumps/CLF-C02/>



### NEW QUESTION 1

- (Topic 3)

A company wants to monitor for misconfigured security groups that are allowing unrestricted access to specific ports. Which AWS service will meet this requirement?

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

**Answer:** A

#### Explanation:

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices, including security and performance. It can help you monitor for misconfigured security groups that are allowing unrestricted access to specific ports. Amazon CloudWatch is a service that monitors your AWS resources and the applications you run on AWS. Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior. AWS Health Dashboard provides relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities.

### NEW QUESTION 2

- (Topic 3)

A company wants durable storage for static content and infinitely scalable data storage infrastructure at the lowest cost. Which AWS service should the company choose?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon S3
- C. AWS Storage Gateway
- D. Amazon Elastic File System (Amazon EFS)

**Answer:** B

#### Explanation:

Amazon S3 is a service that provides durable storage for static content and infinitely scalable data storage infrastructure at the lowest cost. Amazon S3 is an object storage service that allows you to store and retrieve any amount of data from anywhere on the internet. Amazon S3 offers industry-leading scalability, availability, and performance, as well as 99.999999999% (11 9s) of durability and multi-AZ resilience. Amazon S3 also provides various storage classes that offer different levels of performance and cost optimization, such as S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access (S3 Standard-IA), S3 One Zone-Infrequent Access (S3 One Zone-IA), and S3 Glacier<sup>456</sup>. Amazon S3 is ideal for storing static content, such as images, videos, documents, and web pages, as well as building data lakes, backup and archive solutions, big data analytics, and machine learning applications<sup>456</sup>. References: 4: Cloud Storage on AWS, 5: Object Storage - Amazon Simple Storage Service (S3) - AWS, 6: Amazon S3 Documentation

### NEW QUESTION 3

- (Topic 3)

Which abilities are benefits of the AWS Cloud? (Select TWO.)

- A. Trade variable expenses for capital expenses.
- B. Deploy globally in minutes.
- C. Plan capacity in advance of deployments.
- D. Take advantage of economies of scale.
- E. Reduce dependencies on network connectivity.

**Answer:** AB

#### Explanation:

The AWS Cloud offers many benefits, such as:

? Trade variable expenses for capital expenses: You can pay only for the resources you use, instead of investing in fixed costs upfront. This reduces the risk and complexity of planning and managing your IT infrastructure<sup>4</sup>

? Deploy globally in minutes: You can leverage the global infrastructure of AWS to deploy your applications and data in multiple regions and availability zones. This enables you to reach your customers faster, improve performance, and increase reliability<sup>5</sup>

### NEW QUESTION 4

- (Topic 3)

A developer has been hired by a large company and needs AWS credentials. Which are security best practices that should be followed? (Select TWO.)

- A. Grant the developer access to only the AWS resources needed to perform the job.
- B. Share the AWS account root user credentials with the developer.
- C. Add the developer to the administrator's group in AWS IAM.
- D. Configure a password policy that ensures the developer's password cannot be changed.
- E. Ensure the account password policy requires a minimum length.

**Answer:** AE

#### Explanation:

The security best practices that should be followed are A and E.

\* A. Grant the developer access to only the AWS resources needed to perform the job. This is an example of the principle of least privilege, which means giving the minimum permissions necessary to achieve a task. This reduces the risk of unauthorized access, data leakage, or accidental damage to AWS resources. You can use AWS Identity and Access Management (IAM) to create users, groups, roles, and policies that grant fine-grained access to AWS resources<sup>12</sup>.

\* E. Ensure the account password policy requires a minimum length. This is a basic security measure that helps prevent brute-force attacks or guessing of passwords. A longer password is harder to crack than a shorter one. You can use IAM to configure a password policy that enforces a minimum password length,

as well as other requirements such as complexity, expiration, and history<sup>34</sup>.

\* B. Share the AWS account root user credentials with the developer. This is a bad practice that should be avoided. The root user has full access to all AWS resources and services, and can perform sensitive actions such as changing billing information, closing the account, or deleting all resources. Sharing the root user credentials exposes your account to potential compromise or misuse. You should never share your root user credentials with anyone, and use them only for account administration tasks<sup>5</sup>.

\* C. Add the developer to the administrator's group in IAM. This is also a bad practice that should be avoided. The administrator's group has full access to all AWS resources and services, which is more than what a developer needs to perform their job. Adding the developer to the administrator's group violates the principle of least privilege and increases the risk of unauthorized access, data leakage, or accidental damage to AWS resources. You should create a custom group for the developer that grants only the necessary permissions for their role<sup>12</sup>.

\* D. Configure a password policy that ensures the developer's password cannot be changed. This is another bad practice that should be avoided. Preventing the developer from changing their password reduces their ability to protect their credentials and comply with security policies. For example, if the developer's password is compromised, they cannot change it to prevent further unauthorized access. Or if the company requires periodic password rotation, they cannot update their password to meet this requirement. You should allow the developer to change their password as needed, and enforce a password policy that sets reasonable rules for password management<sup>34</sup>.

## NEW QUESTION 5

- (Topic 3)

A company wants to make an upfront commitment for continued use of its production Amazon EC2 instances in exchange for a reduced overall cost. Which pricing options meet these requirements with the LOWEST cost? (Select TWO.)

- A. Spot Instances
- B. On-Demand Instances
- C. Reserved Instances
- D. Savings Plans
- E. Dedicated Hosts

**Answer:** CD

### Explanation:

Reserved Instances (RIs) are a pricing model that allows you to reserve EC2 instances for a specified period of time (one or three years) and receive a significant discount compared to On-Demand pricing. RIs are suitable for workloads that have predictable usage patterns and require a long-term commitment. You can choose between three payment options: All Upfront, Partial Upfront, or No Upfront. The more you pay upfront, the greater the discount<sup>1</sup>.

Savings Plans are a flexible pricing model that can help you reduce your EC2 costs by up to 72% compared to On-Demand pricing, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a one or three year term. Savings Plans apply to usage across EC2, AWS Lambda, and AWS Fargate. You can choose between two types of Savings Plans: Compute Savings Plans and EC2 Instance Savings Plans. Compute Savings Plans offer the most flexibility and apply to any instance family, size, OS, tenancy, or region. EC2 Instance Savings Plans offer the highest discount and apply to a specific instance family within a region<sup>2</sup>.

Spot Instances are a pricing model that allows you to bid for unused EC2 capacity in the AWS cloud and are available at a discount of up to 90% compared to On-Demand pricing. Spot Instances are suitable for fault-tolerant or stateless workloads that can run on heterogeneous hardware and have flexible start and end times. However, Spot Instances are not guaranteed and can be interrupted by AWS at any time if the demand for capacity increases or your bid price is lower than the current Spot price<sup>3</sup>.

On-Demand Instances are a pricing model that allows you to pay for compute capacity by the hour or second with no long-term commitments. On-Demand Instances are suitable for short-term, spiky, or unpredictable workloads that cannot be interrupted, or for applications that are being developed or tested on EC2 for the first time. However, On-Demand Instances are the most expensive option among the four pricing models<sup>4</sup>.

Dedicated Hosts are physical EC2 servers fully dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, such as Windows Server, SQL Server, and SUSE Linux Enterprise Server. Dedicated Hosts can be purchased On-Demand or as part of Savings Plans. Dedicated Hosts are suitable for workloads that need to run on dedicated physical servers or have strict licensing requirements. However, Dedicated Hosts are not the lowest cost option among the four pricing models.

## NEW QUESTION 6

- (Topic 3)

Which AWS service is a cloud security posture management (CSPM) service that aggregates alerts from various AWS services and partner products in a standardized format?

- A. AWS Security Hub
- B. AWS Trusted Advisor
- C. Amazon EventBridge
- D. Amazon GuardDuty

**Answer:** A

### Explanation:

AWS Security Hub is a cloud security posture management (CSPM) service that performs security best practice checks, aggregates alerts, and enables automated remediation. Security Hub collects findings from the security services enabled across your AWS accounts, such as intrusion detection findings from Amazon GuardDuty, vulnerability scans from Amazon Inspector, and sensitive data identification findings from Amazon Macie. Security Hub also collects findings from partner security products using a standardized AWS Security Finding Format, eliminating the need for time-consuming data parsing and normalization efforts. Customers can designate an administrator account that can access all findings across their accounts. References: AWS Security Hub Overview, AWS Security Hub FAQs

## NEW QUESTION 7

- (Topic 3)

Which option is a customer responsibility under the AWS shared responsibility model?

- A. Maintenance of underlying hardware of Amazon EC2 instances
- B. Application data security
- C. Physical security of data centers
- D. Maintenance of VPC components

**Answer:** B

**Explanation:**

The option that is a customer responsibility under the AWS shared responsibility model is B. Application data security. According to the AWS shared responsibility model, AWS is responsible for the security of the cloud, while the customer is responsible for the security in the cloud. This means that AWS manages the security of the underlying infrastructure, such as the hardware, software, networking, and facilities that run the AWS services, while the customer manages the security of their applications, data, and resources that they use on top of AWS<sup>12</sup>. Application data security is one of the customer responsibilities under the AWS shared responsibility model. This means that the customer is responsible for protecting their application data from unauthorized access, modification, deletion, or leakage. The customer can use various AWS services and features to help with application data security, such as encryption, key management, access control, logging, and auditing<sup>12</sup>. Maintenance of underlying hardware of Amazon EC2 instances is not a customer responsibility under the AWS shared responsibility model. This is part of the AWS responsibility to secure the cloud. AWS manages the physical servers that host the Amazon EC2 instances and ensures that they are updated, patched, and replaced as needed<sup>13</sup>.

Physical security of data centers is not a customer responsibility under the AWS shared responsibility model. This is also part of the AWS responsibility to secure the cloud. AWS operates and controls the facilities where the AWS services are hosted and ensures that they are protected from unauthorized access, environmental hazards, fire, and theft<sup>14</sup>. Maintenance of VPC components is not a customer responsibility under the AWS shared responsibility model. This is a shared responsibility between AWS and the customer. AWS provides the VPC service and ensures that it is secure and reliable, while the customer configures and manages their own VPCs and related components, such as subnets, route tables, security groups, network ACLs, gateways, and endpoints<sup>15</sup>.

References:

1: Shared Responsibility Model - Amazon Web Services (AWS) 2: AWS Cloud Computing - W3Schools 3: [Amazon EC2 FAQs - Amazon Web Services] 4: [AWS Security - Amazon Web Services] 5: [Amazon Virtual Private Cloud (VPC) - Amazon Web Services]

**NEW QUESTION 8**

- (Topic 3)

A company wants high levels of detection and near-real-time (NRT) mitigation against large and sophisticated distributed denial of service (DDoS) attacks on applications running on AWS.

Which AWS service should the company use?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS Shield Advanced
- D. Amazon Macie

**Answer: C**

**Explanation:**

AWS Shield Advanced is a service that provides high levels of detection and near-real-time (NRT) mitigation against large and sophisticated distributed denial of service (DDoS) attacks on applications running on AWS. AWS Shield Advanced also provides you with 24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS attacks of any size or duration<sup>1</sup>. Amazon GuardDuty is a service that provides threat detection for your AWS accounts and workloads, but it does not offer DDoS protection<sup>3</sup>. Amazon Inspector is a service that helps you improve the security and compliance of your applications deployed on AWS by automatically assessing them for vulnerabilities and deviations from best practices. Amazon Macie is a service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

**NEW QUESTION 9**

- (Topic 3)

A company uses AWS Organizations. The company wants to apply security best practices from the AWS Well-Architected Framework to all of its AWS accounts. Which AWS service will meet these requirements?

- A. Amazon Macie
- B. Amazon Detective
- C. AWS Control Tower
- D. AWS Secrets Manager

**Answer: C**

**Explanation:**

AWS Control Tower is the easiest way to set up and govern a secure, multi-account AWS environment based on best practices established through AWS's experience working with thousands of enterprises as they move to the cloud. With AWS Control Tower, builders can provision new AWS accounts in a few clicks, while you have peace of mind knowing your accounts conform to your organization's policies. AWS Control Tower automates the setup of a baseline environment, or landing zone, that is a secure, well-architected multi-account AWS environment<sup>1</sup>. AWS Control Tower helps you apply security best practices from the AWS Well-Architected Framework to all of your AWS accounts<sup>2</sup>.

**NEW QUESTION 10**

- (Topic 3)

A company that has multiple business units wants to centrally manage and govern its AWS Cloud environments. The company wants to automate the creation of AWS accounts, apply service control policies (SCPs), and simplify billing processes.

Which AWS service or tool should the company use to meet these requirements?

- A. AWS Organizations
- B. Cost Explorer
- C. AWS Budgets
- D. AWS Trusted Advisor

**Answer: A**

**Explanation:**

AWS Organizations is an AWS service that enables you to centrally manage and govern your AWS Cloud environments across multiple business units. AWS Organizations allows you to create an organization that consists of AWS accounts that you create or invite to join. You can group your accounts into organizational units (OUs) and apply service control policies (SCPs) to them. SCPs are a type of policy that specify the maximum permissions for the accounts in your organization, and can help you enforce compliance and security requirements. AWS Organizations also simplifies billing processes by enabling you to consolidate and pay for all member accounts with a single payment method. You can also use AWS Organizations to automate the creation of AWS accounts by using APIs or AWS CloudFormation templates. References: What is AWS Organizations?, Policy-Based Management - AWS Organizations

### NEW QUESTION 10

- (Topic 3)

An ecommerce company has migrated its IT infrastructure from an on-premises data center to the AWS Cloud. Which cost is the company's direct responsibility?

- A. Cost of application software licenses
- B. Cost of the hardware infrastructure on AWS
- C. Cost of power for the AWS servers
- D. Cost of physical security for the AWS data center

**Answer:** A

#### Explanation:

The cost of application software licenses is the company's direct responsibility when it migrates its IT infrastructure from an on-premises data center to the AWS Cloud. Application software licenses are the agreements that grant users the right to use specific software products, such as operating systems, databases, or applications. Depending on the type and terms of the license, users may need to pay a fee to the software vendor or provider to use the software legally and access its features and updates. When users migrate their IT infrastructure to the AWS Cloud, they can choose to buy new licenses from AWS, bring their own licenses (BYOL), or use a combination of both. However, regardless of the option they choose, they are still responsible for complying with the license terms and paying the license fees to the software vendor or provider. AWS does not charge users for the application software licenses they bring or buy, but only for the AWS resources they use to run their applications. Therefore, the cost of application software licenses is the only cost among the options that is the company's direct responsibility. The other costs are either included in the AWS service fees or covered by AWS.

References: AWS License Manager Pricing, Software licensing: The blind spot in public cloud costs, Cost Optimization tips for SQL Server Licenses on AWS, Microsoft Licensing on AWS

### NEW QUESTION 14

- (Topic 3)

A company needs to engage third-party consultants to help maintain and support its AWS environment and the company's business needs. Which AWS service or resource will meet these requirements?

- A. AWS Support
- B. AWS Organizations
- C. AWS Service Catalog
- D. AWS Partner Network (APN)

**Answer:** D

#### Explanation:

The AWS service or resource that will meet these requirements is D. AWS Partner Network (APN).

AWS Partner Network (APN) is a global community of consulting and technology partners that offer a wide range of services and solutions for AWS customers. APN partners can help customers design, architect, build, migrate, and manage their workloads and applications on AWS. APN partners have access to various resources, training, tools, and support to enhance their AWS expertise and deliver value to customers<sup>12</sup>.

AWS Support is a service that provides technical assistance and guidance for AWS customers. AWS Support offers different plans with varying levels of response time, access channels, and features. AWS Support does not directly engage third-party consultants, but rather connects customers with AWS experts and resources<sup>3</sup>.

AWS Organizations is a service that allows customers to manage multiple AWS accounts within a single organization. AWS Organizations enables customers to create groups of accounts, apply policies, automate account creation, and consolidate billing. AWS Organizations does not directly engage third-party consultants, but rather helps customers simplify and optimize their AWS account management<sup>4</sup>.

AWS Service Catalog is a service that allows customers to create and manage catalogs of IT services that are approved for use on AWS. AWS Service Catalog enables customers to control the configuration, deployment, and governance of their IT services. AWS Service Catalog does not directly engage third-party consultants, but rather helps customers standardize and streamline their IT service delivery<sup>5</sup>.

References:

- 1: AWS Partner Network (APN) - Amazon Web Services (AWS)
- 2: Find an APN Partner - Amazon Web Services (AWS)
- 3: AWS Support – Amazon Web Services
- 4: AWS Organizations – Amazon Web Services
- 5: AWS Service Catalog – Amazon Web Services

### NEW QUESTION 19

- (Topic 3)

A company is planning to migrate to the AWS Cloud and wants to become more responsive to customer inquiries and feedback. The company wants to focus on organizational transformation.

A company wants to give its customers the ability to view specific data that is hosted in Amazon S3 buckets. The company wants to keep control over the full datasets that the company shares with the customers.

Which S3 feature will meet these requirements?

- A. S3 Storage Lens
- B. S3 Cross-Region Replication (CRR)
- C. S3 Versioning
- D. S3 Access Points

**Answer:** D

#### Explanation:

S3 Access Points are a feature of Amazon S3 that allows you to easily manage access to specific data that is hosted in S3 buckets. S3 Access Points are unique hostnames that customers can use to access data in S3 buckets. You can create multiple access points for a single bucket, each with its own name and permissions. You can use S3 Access Points to provide different levels of access to different groups of customers, such as read-only or write-only access. You can also use S3 Access Points to enforce encryption or logging requirements for specific data. S3 Access Points help you keep control over the full datasets that you share with your customers, while simplifying the access management and improving the performance and scalability of your applications.

### NEW QUESTION 24

- (Topic 3)

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.)

- A. Amazon Simple Queue Service (Amazon SQS)
- B. AWS Budgets
- C. Cost Explorer
- D. Amazon CloudWatch
- E. AWS Cost and Usage Report

**Answer:** BD

**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

**NEW QUESTION 28**

- (Topic 3)

A company wants to minimize network latency between its Amazon EC2 instances. The EC2 instances do not need to be highly available. Which solution meets these requirements?

- A. Use EC2 instances in a single Availability Zone.
- B. Use Amazon CloudFront as the database for the EC2 instances.
- C. Use EC2 instances in the same edge location and the same Availability Zone.
- D. Use EC2 instances in the same edge location and the same AWS Region.

**Answer:** A

**Explanation:**

Using EC2 instances in a single Availability Zone is a solution that meets the requirements of minimizing network latency between the EC2 instances and not needing high availability. An Availability Zone is a physically isolated location within an AWS Region that has its own power, cooling, and network connectivity. EC2 instances within the same Availability Zone can communicate with each other using low-latency private IP addresses. However, EC2 instances in a single Availability Zone are not highly available, because they are vulnerable to failures or disruptions that affect the Availability Zone

**NEW QUESTION 31**

- (Topic 3)

Which benefits can customers gain by using AWS Marketplace? (Select TWO.)

- A. Speed of business
- B. Fewer legal objections
- C. Ability to pay with credit cards
- D. No requirement for product licenses for any products
- E. Free use of all services for the first hour

**Answer:** AB

**Explanation:**

AWS Marketplace is a digital catalog that offers thousands of software products and solutions from independent software vendors (ISVs) and AWS partners. Customers can use AWS Marketplace to find, buy, and deploy software on AWS. Some of the benefits of using AWS Marketplace are:

? Speed of business: You can quickly and easily discover and deploy software that meets your business needs, without having to go through lengthy procurement processes. You can also use AWS Marketplace to test and compare different solutions before making a purchase decision.

? Fewer legal objections: You can benefit from standardized contract terms and conditions that are pre-negotiated between AWS and the ISVs. This reduces the time and effort required to review and approve legal agreements.

**NEW QUESTION 32**

- (Topic 3)

In the AWS shared responsibility model, which tasks are the responsibility of AWS? (Select TWO.)

- A. Patch an Amazon EC2 instance operating system.
- B. Configure a security group.
- C. Monitor the health of an Availability Zone.
- D. Protect the infrastructure that runs Amazon EC2 instances.
- E. Manage access to the data in an Amazon S3 bucket

**Answer:** CD

**Explanation:**

According to the AWS shared responsibility model, AWS is responsible for the security of the cloud, which includes the tasks of monitoring the health of an Availability Zone and protecting the infrastructure that runs Amazon EC2 instances. An Availability Zone is a physically isolated location within an AWS Region that has its own power, cooling, and network connectivity. AWS monitors the health and performance of each Availability Zone and notifies customers of any issues or disruptions. AWS also protects the infrastructure that runs AWS services, such as Amazon EC2, by implementing physical, environmental, and operational security measures. AWS is not responsible for patching an Amazon EC2 instance operating system, configuring a security group, or managing access to the data in an Amazon S3 bucket. These are the customer's responsibilities for security in the cloud. The customer must ensure that the operating system and applications on their EC2 instances are up to date and secure. The customer must also configure the security group rules that control the inbound and outbound traffic for their

EC2 instances. The customer must also manage the access permissions and encryption settings for their S3 buckets and objects2

#### NEW QUESTION 34

- (Topic 3)

A company is storing sensitive customer data in an Amazon S3 bucket. The company wants to protect the data from accidental deletion or overwriting. Which S3 feature should the company use to meet these requirements?

- A. S3 Lifecycle rules
- B. S3 Versioning
- C. S3 bucket policies
- D. S3 server-side encryption

**Answer: B**

#### Explanation:

S3 Versioning is a feature that allows you to keep multiple versions of an object in the same bucket. You can use S3 Versioning to protect your data from accidental deletion or overwriting by enabling it on a bucket or a specific object. S3 Versioning also allows you to restore previous versions of an object if needed. S3 Lifecycle rules are used to automate the transition of objects between storage classes or to expire objects after a certain period of time. S3 bucket policies are used to control access to the objects in a bucket. S3 server-side encryption is used to encrypt the data at rest in S3. References: S3 Versioning, S3 Lifecycle rules, S3 bucket policies, S3 server-side encryption

#### NEW QUESTION 35

- (Topic 3)

A company wants to integrate its online shopping website with social media login credentials. Which AWS service can the company use to make this integration?

- A. AWS Directory Service
- B. AWS Identity and Access Management (IAM)
- C. Amazon Cognito
- D. AWS IAM Identity Center (AWS Single Sign-On)

**Answer: C**

#### Explanation:

Amazon Cognito is a service that enables you to add user sign-up and sign-in features to your web and mobile applications. Amazon Cognito also supports social and enterprise identity federation, which means you can allow your users to sign in with their existing credentials from identity providers such as Google, Facebook, Apple, and Amazon. Amazon Cognito integrates with OpenID Connect (OIDC) and Security Assertion Markup Language (SAML) 2.0 protocols to facilitate the authentication and authorization process. Amazon Cognito also provides advanced security features, such as adaptive authentication, user verification, and multi-factor authentication (MFA). References: Amazon Cognito, What is Amazon Cognito?

#### NEW QUESTION 38

- (Topic 3)

According to the AWS shared responsibility model, which task is the customer's responsibility?

- A. Maintaining the infrastructure needed to run AWS Lambda
- B. Updating the operating system of Amazon DynamoDB instances
- C. Maintaining Amazon S3 infrastructure
- D. Updating the guest operating system on Amazon EC2 instances

**Answer: D**

#### Explanation:

The AWS shared responsibility model describes the division of responsibilities between AWS and the customer for security and compliance. AWS is responsible for the security of the cloud, which includes the hardware, software, networking, and facilities that run AWS services. The customer is responsible for security in the cloud, which includes the customer data, applications, operating systems, and network and firewall configurations. Therefore, updating the guest operating system on Amazon EC2 instances is the customer's responsibility2

#### NEW QUESTION 41

- (Topic 3)

Which AWS service can provide a dedicated network connection with consistent low latency from on premises to the AWS Cloud?

- A. Amazon VPC
- B. Amazon Kinesis Data Streams
- C. AWS Direct Connect
- D. Amazon OpenSearch Service

**Answer: C**

#### Explanation:

AWS Direct Connect is a service that provides a dedicated network connection from on premises to the AWS Cloud. It can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections. It can also provide low latency for applications that require real-time data transfer4. Amazon VPC is a service that provides a logically isolated section of the AWS Cloud where users can launch AWS resources in a virtual network that they define. Amazon Kinesis Data Streams is a service that provides a scalable and durable stream of data records for real-time data processing. Amazon OpenSearch Service is a service that provides a fully managed, scalable, and secure search and analytics solution that is compatible with Elasticsearch.

#### NEW QUESTION 42

- (Topic 3)

Which Amazon EC2 instance pricing model can provide discounts of up to 90%?

- A. Reserved Instances
- B. On-Demand
- C. Dedicated Hosts
- D. Spot Instances

**Answer:** D

**Explanation:**

Spot Instances are Amazon EC2 instances that are available at a discounted price compared to On-Demand pricing. Spot Instances use spare EC2 capacity that is not being used by other customers, and the price fluctuates based on supply and demand. Customers can request Spot Instances for their applications and specify the maximum price they are willing to pay per hour. If the Spot price is lower than the customer's bid, the Spot Instance is launched and the customer pays the current Spot price. However, if the Spot price rises above the customer's bid, the Spot Instance is terminated by AWS and the customer is charged for the partial hour of usage. Therefore, Spot Instances can provide discounts of up to 90% or more, but they are not suitable for applications that require continuous or predictable availability. Spot Instances are recommended for applications that are flexible, fault-tolerant, or have low priority, such as batch processing, data analysis, or testing and development.

**NEW QUESTION 43**

- (Topic 3)

A company needs a fully managed file server that natively supports Microsoft workloads and file systems. The file server must also support the SMB protocol. Which AWS service should the company use to meet these requirements?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon FSx for Windows File Server
- D. Amazon Elastic Block Store (Amazon EBS)

**Answer:** C

**Explanation:**

Amazon FSx for Windows File Server is a fully managed file server that supports Microsoft workloads and file systems, including the SMB protocol. It provides features such as user quotas, end-user file restore, and Microsoft Active Directory integration. Amazon EFS is a fully managed file system that supports the NFS protocol, not SMB. Amazon FSx for Lustre is a fully managed file system that supports high-performance computing workloads, not Microsoft workloads. Amazon EBS is a block storage service that does not provide a file system or SMB support. References: Amazon FSx for Windows File Server, Amazon FSx for Lustre, Amazon EFS, Amazon EBS

**NEW QUESTION 45**

- (Topic 3)

Which AWS service provides the ability to manage infrastructure as code?

- A. AWS CodePipeline
- B. AWS CodeDeploy
- C. AWS Direct Connect
- D. AWS CloudFormation

**Answer:** D

**Explanation:**

The AWS service that provides the ability to manage infrastructure as code is AWS CloudFormation. Infrastructure as code is a process of defining and provisioning AWS resources using code or templates, rather than manual actions or scripts. AWS CloudFormation allows you to create and update stacks of AWS resources based on predefined templates that describe the desired state and configuration of the resources. AWS CloudFormation automates and simplifies the deployment and management of AWS resources, and ensures consistency and repeatability across different environments and regions. AWS CloudFormation also supports rollback, change sets, drift detection, and nested stacks features that help you to monitor and control the changes to your infrastructure<sup>1</sup>.

**NEW QUESTION 49**

- (Topic 3)

A company wants to integrate natural language processing (NLP) into business intelligence (BI) dashboards. The company wants to ask questions and receive answers with relevant visualizations.

Which AWS service or tool will meet these requirements?

- A. Amazon Macie
- B. Amazon Rekognition
- C. Amazon QuickSight Q
- D. Amazon Lex

**Answer:** C

**Explanation:**

Amazon QuickSight Q is a natural language query feature that allows users to ask questions about their data and receive answers in the form of relevant visualizations<sup>1</sup>. Amazon Macie is a data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data in AWS<sup>2</sup>. Amazon Rekognition is a computer vision service that can analyze images and videos for faces, objects, scenes, text, and more<sup>3</sup>. Amazon Lex is a service for building conversational interfaces using voice and text<sup>4</sup>.

**NEW QUESTION 54**

- (Topic 3)

Which AWS service can identify when an Amazon EC2 instance was terminated?

- A. AWS Identity and Access Management (IAM)
- B. AWS CloudTrail
- C. AWS Compute Optimizer
- D. Amazon EventBridge

**Answer:** B

**Explanation:**

AWS CloudTrail is the AWS service that can identify when an Amazon EC2 instance was terminated. AWS CloudTrail is a service that records API calls and events for AWS accounts and resources. AWS CloudTrail can capture the `TerminateInstances` event, which is triggered when an EC2 instance is terminated by a user or an AWS service. The event contains information such as the instance ID, the user identity, the source IP address, the time, and the reason for the termination<sup>12</sup>. Customers can use the CloudTrail console, the AWS CLI, or the AWS SDKs to view and search for the `TerminateInstances` events in their event history or in their S3 buckets where they store their CloudTrail logs<sup>13</sup>.

**NEW QUESTION 59**

- (Topic 3)

A company is operating several factories where it builds products. The company needs the ability to process data, store data, and run applications with local system interdependencies that require low latency.

Which AWS service should the company use to meet these requirements?

- A. AWS IoT Greengrass
- B. AWS Lambda
- C. AWS Outposts
- D. AWS Snowball Edge

**Answer:** C

**Explanation:**

AWS Outposts is a service that provides fully managed AWS infrastructure and services on premises. It allows users to run applications that require low latency and local data processing, while seamlessly connecting to the AWS Cloud for a consistent hybrid experience. AWS IoT Greengrass is a service that provides local compute, messaging, data caching, sync, and ML inference capabilities for connected devices. AWS Lambda is a service that allows users to run code without provisioning or managing servers. AWS Snowball Edge is a device that provides a petabyte-scale data transport and edge computing solution.

**NEW QUESTION 61**

- (Topic 3)

A company is running its application in the AWS Cloud. The company wants to periodically review its AWS account for cost optimization opportunities.

Which AWS service or tool can the company use to meet these requirements?

- A. AWS Cost Explorer
- B. AWS Trusted Advisor
- C. AWS Pricing Calculator
- D. AWS Budgets

**Answer:** A

**Explanation:**

AWS Cost Explorer is an AWS service or tool that the company can use to periodically review its AWS account for cost optimization opportunities. AWS Cost Explorer is a tool that enables the company to visualize, understand, and manage their AWS costs and usage over time. The company can use AWS Cost Explorer to access interactive graphs and tables that show the breakdown of their costs and usage by service, region, account, tag, and more. The company can also use AWS Cost Explorer to forecast their future costs, identify trends and anomalies, and discover potential savings by using Reserved Instances or Savings Plans.

**NEW QUESTION 66**

- (Topic 3)

A company wants to migrate its high-performance computing (HPC) application to Amazon EC2 instances. The application has multiple components. The application must have fault tolerance and must have the ability to fail over automatically.

Which AWS infrastructure solution will meet these requirements with the LEAST latency between components?

- A. Multiple AWS Regions
- B. Multiple edge locations
- C. Multiple Availability Zones
- D. Regional edge caches

**Answer:** C

**Explanation:**

Using EC2 instances in multiple Availability Zones is an AWS infrastructure solution that meets the requirements of migrating a high performance computing (HPC) application to AWS with fault tolerance and failover capabilities, and with the least latency between components. An Availability Zone is a physically isolated location within an AWS Region that has its own power, cooling, and network connectivity. EC2 instances within the same Region can communicate with each other using low-latency private IP addresses. By using EC2 instances in multiple Availability Zones, the company can achieve fault tolerance and failover for their HPC application, because they can distribute the workload and data across different locations that are independent of each other. If one Availability Zone becomes unavailable or impaired, the company can redirect the traffic and data to another Availability Zone without affecting the performance and availability of the application<sup>5</sup>.

**NEW QUESTION 70**

- (Topic 3)

An IT engineer needs to access AWS services from an on-premises application. Which credentials or keys does the application need for authentication?

- A. AWS account user name and password

- B. IAM access key and secret
- C. Amazon EC2 key pairs
- D. AWS Key Management Service (AWS KMS) keys

**Answer:** B

**Explanation:**

IAM access keys are long-term credentials that consist of an access key ID and a secret access key. You use access keys to sign programmatic requests that you make to AWS. If you need to access AWS services from an on-premises application, you can use IAM access keys to authenticate your requests. AWS account user name and password are used to sign in to the AWS Management Console. Amazon EC2 key pairs are used to connect to your EC2 instances using SSH. AWS Key Management Service (AWS KMS) keys are used to encrypt and decrypt your data using the AWS Encryption SDK or the AWS CLI.

**NEW QUESTION 71**

- (Topic 3)

A company wants to launch multiple workloads on AWS. Each workload is related to a different business unit. The company wants to separate and track costs for each business unit.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Organizations and create one account for each business unit.
- B. Use a spreadsheet to control the owners and cost of each resource.
- C. Use an Amazon DynamoDB table to record costs for each business unit.
- D. Use the AWS Billing console to assign owners to resources and track costs.

**Answer:** A

**Explanation:**

AWS Organizations is a service that helps you centrally manage and govern your AWS environment. You can use AWS Organizations to create multiple accounts for different business units, and group them into organizational units (OUs) that reflect your organizational structure<sup>1</sup>. By doing so, you can separate and track costs for each business unit using the account ID as a cost allocation tag<sup>2</sup>. You can also use AWS Organizations to apply policies and controls to your accounts, such as service control policies (SCPs) and tag policies<sup>1</sup>.

The other options are not suitable for meeting the requirements with the least operational overhead. Using a spreadsheet or a DynamoDB table to control and record costs for each business unit would require manual data entry and maintenance, which is prone to errors and inconsistencies. Using the AWS Billing console to assign owners to resources and track costs would also require manual tagging of each resource, which is time-consuming and inefficient.

References:

? 1: What Is AWS Organizations? - AWS Organizations

? 2: Cost Tagging and Reporting with AWS Organizations | AWS Cloud Financial Management

**NEW QUESTION 74**

- (Topic 3)

A company's application has high customer usage during certain times of the day. The company wants to reduce the number of Amazon EC2 instances that run when application usage is low.

Which AWS service or instance purchasing option should the company use to meet this requirement?

- A. EC2 Instance Savings Plans
- B. Spot Instances
- C. Reserved Instances
- D. Amazon EC2 Auto Scaling

**Answer:** D

**Explanation:**

Amazon EC2 Auto Scaling is an AWS service that can help users reduce the number of Amazon EC2 instances that run when application usage is low. Amazon EC2 Auto Scaling allows users to create scaling policies that automatically adjust the number of EC2 instances based on the demand or a schedule. EC2 Instance Savings Plans, Spot Instances, and Reserved Instances are instance purchasing options that can help users save money on EC2 usage, but they do not automatically scale the number of instances according to the application usage .

**NEW QUESTION 79**

- (Topic 3)

A company has 5 TB of data stored in Amazon S3. The company plans to occasionally run queries on the data for analysis.

Which AWS service should the company use to run these queries in the MOST cost- effective manner?

- A. Amazon Redshift
- B. Amazon Athena
- C. Amazon Kinesis
- D. Amazon RDS

**Answer:** B

**Explanation:**

Amazon Athena is a serverless, interactive analytics service that allows users to run SQL queries on data stored in Amazon S3. It is ideal for occasional queries on large datasets, as it does not require any server provisioning, configuration, or management. Users only pay for the queries they run, based on the amount of data scanned. Amazon Athena supports various data formats, such as CSV, JSON, Parquet, ORC, and Avro, and integrates with AWS Glue Data Catalog to create and manage schemas. Amazon Athena also supports querying data from other sources, such as on- premises or other cloud systems, using data connectors<sup>1</sup>.

Amazon Redshift is a fully managed data warehouse service that allows users to run complex analytical queries on petabyte-scale data. However, it requires users to provision and maintain clusters of nodes, and pay for the storage and compute capacity they use. Amazon Redshift is more suitable for frequent and consistent queries on structured or semi-structured data<sup>2</sup>.

Amazon Kinesis is a platform for streaming data on AWS, enabling users to collect, process, and analyze real-time data. It is not designed for querying data stored in Amazon S3. Amazon Kinesis consists of four services: Kinesis Data Streams, Kinesis Data Firehose, Kinesis Data Analytics, and Kinesis Video Streams<sup>3</sup>.

Amazon RDS is a relational database service that provides six database engines: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL

Server. It simplifies database administration tasks such as backup, patching, scaling, and replication. However, it is not optimized for querying data stored in Amazon S3. Amazon RDS is more suitable for transactional workloads that require high performance and availability<sup>4</sup>.

References:

- ? Interactive SQL - Serverless Query Service - Amazon Athena - AWS
- ? [Amazon Redshift – Data Warehouse Solution - AWS]
- ? [Amazon Kinesis - Streaming Data Platform - AWS]
- ? [Amazon Relational Database Service (RDS) – AWS]

### NEW QUESTION 83

- (Topic 3)

A company needs to control inbound and outbound traffic for an Amazon EC2 instance.

Which AWS service or feature can the company associate with the EC2 instance to meet this requirement?

- A. Network ACL
- B. Security group
- C. AWS WAF
- D. VPC route tables

**Answer: B**

#### Explanation:

A security group is a virtual firewall that can be associated with an Amazon EC2 instance to control the inbound and outbound traffic for the instance. You can specify which protocols, ports, and source or destination IP ranges are allowed or denied by the security group. A network ACL is a stateless filter that can be associated with a subnet to control the traffic to and from the subnet, but it is not associated with an EC2 instance<sup>4</sup>. AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. VPC route tables are used to determine where network traffic is directed within a VPC or to an internet gateway, virtual private gateway, NAT device, VPC peering connection, or VPC endpoint.

### NEW QUESTION 87

- (Topic 3)

A company wants an AWS service to provide product recommendations based on its customer data.

Which AWS service will meet this requirement?

- A. Amazon Polly
- B. Amazon Personalize
- C. Amazon Comprehend
- D. Amazon Rekognition

**Answer: B**

#### Explanation:

Amazon Personalize is an AWS service that helps developers quickly build and deploy a custom recommendation engine with real-time personalization and user segmentation<sup>1</sup>. It uses machine learning (ML) to analyze customer data and provide relevant recommendations based on their preferences, behavior, and context. Amazon Personalize can be used for various use cases such as optimizing recommendations, targeting customers more accurately, maximizing the value of unstructured text, and promoting items using business rules<sup>1</sup>.

The other options are not suitable for providing product recommendations based on customer data. Amazon Polly is a service that converts text into lifelike speech. Amazon Comprehend is a service that uses natural language processing (NLP) to extract insights from text and documents. Amazon Rekognition is a service that uses computer vision (CV) to analyze images and videos for faces, objects, scenes, and activities.

References:

- ? 1: Cloud Products - Amazon Web Services (AWS)
- ? 2: Recommender System – Amazon Personalize – Amazon Web Services
- ? 3: Top 25 AWS Services List 2023 - GeeksforGeeks
- ? 4: AWS to Azure services comparison - Azure Architecture Center
- ? 5: The 25+ Best AWS Cost Optimization Tools (Updated 2023) - CloudZero
- ? 6: Amazon Polly – Text-to-Speech Service - AWS
- ? 7: Natural Language Processing - Amazon Comprehend - AWS
- ? 8: Image and Video Analysis - Amazon Rekognition - AWS

### NEW QUESTION 91

- (Topic 3)

What is the purpose of having an internet gateway within a VPC?

- A. To create a VPN connection to the VPC
- B. To allow communication between the VPC and the internet
- C. To impose bandwidth constraints on internet traffic
- D. To load balance traffic from the internet across Amazon EC2 instances

**Answer: B**

#### Explanation:

An internet gateway is a service that allows for internet traffic to enter into a VPC. Otherwise, a VPC is completely segmented off and then the only way to get to it is potentially through a VPN connection rather than through internet connection. An internet gateway is a logical connection between an AWS VPC and the internet. It supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic<sup>1</sup>. An internet gateway enables resources in your public subnets (such as EC2 instances) to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address<sup>2</sup>. An internet gateway also provides a target in your VPC route tables for internet-routable traffic. For communication using IPv4, the internet gateway also performs network address translation (NAT). For communication using IPv6, NAT is not needed because IPv6 addresses are public<sup>2</sup>. To enable access to or from the internet for instances in a subnet in a VPC using an internet gateway, you must create an internet gateway and attach it to your VPC, add a route to your subnet's route table that directs internet-bound traffic to the internet gateway, ensure that instances in your subnet have a public IPv4 address or an IPv6 address, and ensure that your network access control lists and security group rules allow the desired internet traffic to flow to and from your instance<sup>2</sup>. References: Connect to the internet using an internet gateway,

## AWS Internet Gateway and VPC Routing

### NEW QUESTION 93

- (Topic 3)

A company wants to run its workload on Amazon EC2 instances for more than 1 year. This workload will run continuously. Which option offers a discounted hourly rate compared to the hourly rate of On-Demand Instances?

- A. AWS Graviton processor
- B. Dedicated Hosts
- C. EC2 Instance Savings Plans
- D. Amazon EC2 Auto Scaling instances

**Answer:** C

#### Explanation:

EC2 Instance Savings Plans are a flexible pricing model that offer discounted hourly rates on Amazon EC2 instance usage for a 1 or 3 year term. EC2 Instance Savings Plans provide savings up to 72% off On-Demand rates, in exchange for a commitment to a specific instance family in a chosen AWS Region (for example, M5 in Virginia). These plans automatically apply to usage regardless of size (for example, m5.xlarge, m5.2xlarge, etc.), OS (for example, Windows, Linux, etc.), and tenancy (Host, Dedicated, Default) within the specified family in a Region. With an EC2 Instance Savings Plan, you can change your instance size within the instance family (for example, from c5.xlarge to c5.2xlarge) or the operating system (for example, from Windows to Linux), or move from Dedicated tenancy to Default and continue to receive the discounted rate provided by your EC2 Instance Savings Plan<sup>4567</sup>. References: 4: Compute Savings Plans – Amazon Web Services, 5: What are Savings Plans? - Savings Plans, 6: How To Cut Your AWS Bill With Savings Plans (and avoid some common ...), 7: AWS Savings Plans vs Reserved Instances  
- GorillaStack

### NEW QUESTION 94

- (Topic 3)

Which AWS service provides a single location to track the progress of application migrations?

- A. AWS Application Discovery Service
- B. AWS Application Migration Service
- C. AWS Service Catalog
- D. AWS Migration Hub

**Answer:** D

#### Explanation:

AWS Migration Hub is a service that provides a single location to track the progress of application migrations across multiple AWS and partner solutions. It allows you to choose the AWS and partner migration tools that best fit your needs, while providing visibility into the status of migrations across your portfolio of applications<sup>1</sup>. AWS Migration Hub supports migration status updates from the following tools: AWS Application Migration Service, AWS Database Migration Service, CloudEndure Migration, Server Migration Service, and Migrate for Compute Engine<sup>1</sup>.

The other options are not correct for the following reasons:

? AWS Application Discovery Service is a service that helps you plan your migration projects by automatically identifying servers, applications, and dependencies in your on-premises data centers<sup>2</sup>. It does not track the progress of application migrations, but rather provides information to help you plan and scope your migrations.

? AWS Application Migration Service is a service that helps you migrate and modernize applications from any source infrastructure to AWS with minimal downtime and disruption<sup>3</sup>. It is one of the migration tools that can send status updates to AWS Migration Hub, but it is not the service that provides a single location to track the progress of application migrations.

? AWS Service Catalog is a service that allows you to create and manage catalogs of IT services that are approved for use on AWS<sup>4</sup>. It does not track the progress of application migrations, but rather helps you manage the provisioning and governance of your IT services.

References:

? 1: What Is AWS Migration Hub? - AWS Migration Hub

? 2: What Is AWS Application Discovery Service? - AWS Application Discovery Service

? 3: App Migration Tool - AWS Application Migration Service - AWS

? 4: What Is AWS Service Catalog? - AWS Service Catalog

### NEW QUESTION 99

- (Topic 3)

A company wants to integrate natural language processing (NLP) into business intelligence (BI) dashboards. The company wants to ask questions and receive answers with relevant visualizations.

Which AWS service or tool will meet these requirements?

- A. Amazon Macie
- B. Amazon Rekognition
- C. Amazon QuickSight Q
- D. Amazon Lex

**Answer:** C

#### Explanation:

Amazon QuickSight Q is a natural language query feature that lets you ask questions about your data using everyday language and get answers in seconds. You can type questions such as “What are the total sales by region?” or “How did marketing campaign A perform?” and get answers in the form of relevant visualizations, such as charts or tables. You can also use Q to drill down into details, filter data, or perform calculations. Q uses machine learning to understand your data and your intent, and provides suggestions and feedback to help you refine your questions.

### NEW QUESTION 102

- (Topic 3)

Which AWS service uses AWS Compute Optimizer to provide sizing recommendations based on workload metrics?

- A. Amazon EC2
- B. Amazon RDS
- C. Amazon Lightsail
- D. AWS Step Functions

**Answer:** A

**Explanation:**

Amazon EC2 is a web service that provides secure, resizable compute capacity in the cloud. It allows you to launch virtual servers, called instances, with different configurations of CPU, memory, storage, and networking resources. AWS Compute Optimizer analyzes the specifications and utilization metrics of your Amazon EC2 instances and generates recommendations for optimal instance types that can reduce costs and improve performance. You can view the recommendations on the AWS Compute Optimizer console or the Amazon EC2 console<sup>12</sup>.

Amazon RDS, Amazon Lightsail, and AWS Step Functions are not supported by AWS Compute Optimizer. Amazon RDS is a managed relational database service that lets you set up, operate, and scale a relational database in the cloud. Amazon Lightsail is an easy- to-use cloud platform that offers everything you need to build an application or website, plus a cost-effective, monthly plan. AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly<sup>3</sup>.

**NEW QUESTION 104**

- (Topic 3)

A company has migrated its workloads to AWS. The company wants to adopt AWS at scale and operate more efficiently and securely. Which AWS service or framework should the company use for operational support?

- A. AWS Support
- B. AWS Cloud Adoption Framework (AWS CAF)
- C. AWS Managed Services (AMS)
- D. AWS Well-Architected Framework

**Answer:** D

**Explanation:**

The AWS Well-Architected Framework is a set of best practices and guidelines for designing and operating workloads on AWS. It helps customers achieve operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. The framework is based on six pillars, each with its own design principles, best practices, and questions. Customers can use the framework to assess their current state, identify gaps, and implement improvements<sup>12</sup>. AWS Support is a service that provides technical assistance, guidance, and resources for AWS customers. It offers different plans with varying levels of access to AWS experts, response times, and features<sup>3</sup>. AWS Support does not provide a comprehensive framework for operational support.

AWS Cloud Adoption Framework (AWS CAF) is a guidance tool that helps customers plan and execute their cloud migration journey. It provides a set of perspectives, capabilities, and best practices to align the business and technical aspects of cloud adoption<sup>4</sup>. AWS CAF does not focus on operational support for existing workloads on AWS.

AWS Managed Services (AMS) is a service that operates AWS infrastructure on behalf of customers. It provides a secure and compliant environment, automates common activities, and applies best practices for provisioning, patching, backup, recovery, and monitoring<sup>5</sup>. AMS does not provide a framework for customers to operate their own workloads on AWS.

**NEW QUESTION 109**

- (Topic 3)

A company wants a list of all users in its AWS account, the status of all of the users' access keys, and if multi-factor authentication (MFA) has been configured. Which AWS service or feature will meet these requirements?

- A. AWS Key Management Service (AWS KMS)
- B. IAM Access Analyzer
- C. IAM credential report
- D. Amazon CloudWatch

**Answer:** C

**Explanation:**

IAM credential report is a feature that allows you to generate and download a report that lists all IAM users in your AWS account and the status of their various credentials, including access keys and MFA devices. You can use this report to audit the security status of your IAM users and ensure that they follow the best practices for using AWS<sup>1</sup>.

AWS Key Management Service (AWS KMS) is a service that allows you to create and manage encryption keys to protect your data. It does not provide information about IAM users or their credentials<sup>2</sup>.

IAM Access Analyzer is a feature that helps you identify the resources in your AWS account, such as S3 buckets or IAM roles, that are shared with an external entity. It does not provide information about IAM users or their credentials<sup>3</sup>.

Amazon CloudWatch is a service that monitors and collects metrics, logs, and events from your AWS resources and applications. It does not provide information about IAM users or their credentials<sup>4</sup>.

References:

? Getting credential reports for your AWS account - AWS Identity and Access Management

? AWS Key Management Service - Amazon Web Services

? IAM Access Analyzer - AWS Identity and Access Management

? Amazon CloudWatch - Amazon Web Services

**NEW QUESTION 114**

- (Topic 3)

Which option is AWS responsible for under the AWS shared responsibility model?

- A. Network and firewall configuration
- B. Client-side data encryption
- C. Management of user permissions
- D. Hardware and infrastructure

**Answer:** D

**Explanation:**

Hardware and infrastructure is the option that AWS is responsible for under the AWS shared responsibility model. The AWS shared responsibility model describes how AWS and customers share responsibilities for security and compliance in the cloud. AWS is responsible for security of the cloud, which means protecting the infrastructure that runs all the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Customers are responsible for security in the cloud, which means taking care of the security of their own applications, data, and operating systems. This includes network and firewall configuration, client-side data encryption, management of user permissions, and more.

**NEW QUESTION 117**

- (Topic 3)

Which of the following is a benefit of using an AWS managed service?

- A. Reduced operational overhead for a company's IT staff
- B. Increased fixed costs that can be predicted by a finance team
- C. Removal of the need to have a backup strategy
- D. Removal of the need to follow compliance standards

**Answer:** A

**Explanation:**

This is a benefit of using an AWS managed service, such as Amazon S3, Amazon DynamoDB, or AWS Lambda. AWS managed services are fully managed by AWS, which means that AWS handles the provisioning, scaling, patching, backup, and recovery of the underlying infrastructure and software. This reduces the operational overhead for the company's IT staff, who can focus on their core business logic and innovation. You can learn more about the AWS managed services from this webpage or this digital course.

**NEW QUESTION 119**

- (Topic 3)

A company is considering migration to the AWS Cloud. The company wants a fully managed service or feature that can transfer streaming data from multiple sources to an Amazon S3 bucket.

Which AWS service or feature should the company use to meet these requirements?

- A. AWS DataSync
- B. Amazon Kinesis Data Firehose
- C. S3 Select
- D. AWS Transfer Family

**Answer:** B

**Explanation:**

Amazon Kinesis Data Firehose is a fully managed service that delivers real-time streaming data to destinations such as Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk. You can use Amazon Kinesis Data Firehose to capture, transform, and load streaming data from multiple sources, such as web applications, mobile devices, IoT sensors, and social media.

**NEW QUESTION 123**

- (Topic 3)

A company plans to migrate to the AWS Cloud. The company wants to use the AWS Cloud Adoption Framework (AWS CAF) to define and track business outcomes as part of its cloud transformation journey.

Which AWS CAF governance perspective capability will meet these requirements?

- A. Benefits management
- B. Risk management
- C. Application portfolio management
- D. Cloud financial management

**Answer:** A

**Explanation:**

The correct answer is A. Benefits management.

Benefits management is the AWS CAF governance perspective capability that helps you define and track business outcomes as part of your cloud transformation journey. Benefits management helps you align your cloud initiatives with your business objectives, measure the value and impact of your cloud investments, and communicate the benefits of cloud adoption to your stakeholders<sup>12</sup>.

Risk management is the AWS CAF governance perspective capability that helps you identify and mitigate the potential risks associated with cloud adoption, such as security, compliance, legal, and operational risks<sup>12</sup>.

Application portfolio management is the AWS CAF governance perspective capability that helps you assess and optimize your existing application portfolio for cloud migration or modernization. Application portfolio management helps you categorize your applications based on their business value and technical fit, prioritize them for cloud adoption, and select the best migration or modernization strategy for each application<sup>12</sup>.

Cloud financial management is the AWS CAF governance perspective capability that helps you manage and optimize the costs and value of your cloud resources. Cloud financial management helps you plan and budget for cloud adoption, track and allocate cloud costs, implement cost optimization strategies, and report on cloud financial performance<sup>12</sup>. References:

1: AWS Cloud Adoption Framework: Governance Perspective 2: All you need to know about AWS Cloud Adoption Framework — Governance Perspective

**NEW QUESTION 128**

- (Topic 3)

A company wants to use guidelines from the AWS Well-Architected Framework to limit human error and facilitate consistent responses to events.

Which of the following is a Well-Architected design principle that will meet these requirements?

- A. Use AWS CodeDeploy.
- B. Perform operations as code.
- C. Migrate workloads to a Dedicated Host.

D. Use AWS Compute Optimizer.

**Answer:** B

**Explanation:**

This is a design principle of the operational excellence pillar of the AWS Well-Architected Framework. Performing operations as code means using scripts, templates, or automation tools to perform routine tasks, such as provisioning, configuration, deployment, and monitoring. This reduces human error, increases consistency, and enables faster recovery from failures. You can learn more about the operational excellence pillar from this whitepaper or this digital course.

**NEW QUESTION 131**

- (Topic 3)

Which AWS service can a company use to visually design and build serverless applications?

- A. AWS Lambda
- B. AWS Batch
- C. AWS Application Composer
- D. AWS App Runner

**Answer:** C

**Explanation:**

AWS Application Composer is a service that allows users to visually design and build serverless applications. Users can drag and drop components, such as AWS Lambda functions, Amazon API Gateway endpoints, Amazon DynamoDB tables, and Amazon S3 buckets, to create a serverless application architecture. Users can also configure the properties, permissions, and dependencies of each component, and deploy the application to their AWS account with a few clicks. AWS Application Composer simplifies the design and configuration of serverless applications, and reduces the need to write code or use AWS CloudFormation templates. References: AWS Application Composer, AWS releases Application Composer to make serverless 'easier' but initial scope is limited

**NEW QUESTION 134**

- (Topic 3)

An ecommerce company wants to distribute traffic between the Amazon EC2 instances that host its website.

Which AWS service or resource will meet these requirements?

- A. Application Load Balancer
- B. AWS WAF
- C. AWS CloudHSM
- D. AWS Direct Connect

**Answer:** A

**Explanation:**

This is the AWS service or resource that will meet the requirements of distributing traffic between the Amazon EC2 instances that host the website. Application Load Balancer is a type of Elastic Load Balancing that distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. Application Load Balancer operates at the application layer (layer 7) of the OSI model and supports advanced features such as path-based routing, host-based routing, health checks, and SSL termination. You can learn more about Application Load Balancer from [this webpage] or [this digital course].

**NEW QUESTION 139**

- (Topic 3)

A company wants to use the AWS Cloud to deploy an application globally.

Which architecture deployment model should the company use to meet this requirement?

- A. Multi-Region
- B. Single-Region
- C. Multi-AZ
- D. Single-AZ

**Answer:** A

**Explanation:**

The architecture deployment model that the company should use to meet this requirement is A. Multi-Region.

A multi-region deployment model is a cloud computing architecture that distributes an application and its data across multiple geographic regions. A multi-region deployment model enables a company to achieve global reach, high availability, disaster recovery, and performance optimization. By deploying an application in multiple regions, a company can serve customers from the nearest region, reduce latency, increase redundancy, and comply with data sovereignty regulations<sup>12</sup>.

A single-region deployment model is a cloud computing architecture that runs an application and its data within a single geographic region. A single-region deployment model is simpler and cheaper than a multi-region deployment model, but it has limited scalability, availability, and performance. A single-region deployment model may not be suitable for a company that wants to deploy an application globally, as it may face challenges such as network latency, regional outages, or regulatory compliance<sup>12</sup>.

A multi-AZ (Availability Zone) deployment model is a cloud computing architecture that distributes an application and its data across multiple isolated locations within a single region. An Availability Zone is a physically separate location within an AWS Region that has independent power, cooling, and networking. A multi-AZ deployment model enhances the availability and durability of an application by providing redundancy and fault tolerance within a region<sup>34</sup>.

A single-AZ deployment model is a cloud computing architecture that runs an application and its data within a single Availability Zone. A single-AZ deployment model is the simplest and most cost-effective option, but it has no redundancy or fault tolerance. A single-AZ deployment model may not be suitable for a company that wants to deploy an application globally, as it may face challenges such as network latency, regional outages, or regulatory compliance<sup>34</sup>.

References:

1: AWS Cloud Computing - W3Schools 2: Understand the Different Cloud Computing Deployment Models Unit - Trailhead 3: Regions and Availability Zones - Amazon Elastic Compute Cloud 4: AWS Reference Architecture Diagrams

**NEW QUESTION 142**

- (Topic 3)

Which AWS service or feature identifies whether an Amazon S3 bucket or an IAM role has been shared with an external entity?

- A. AWS Service Catalog
- B. AWS Systems Manager
- C. AWS IAM Access Analyzer
- D. AWS Organizations

**Answer:** C

**Explanation:**

AWS IAM Access Analyzer is a service that helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. This lets you identify unintended access to your resources and data, which is a security risk. IAM Access Analyzer uses logic-based reasoning to analyze the resource-based policies in your AWS environment. For each instance of a resource shared outside of your account, IAM Access Analyzer generates a finding. Findings include information about the access and the external principal granted to it. References: 3: Using AWS Identity and Access Management Access Analyzer, 4: IAM Access Analyzer - Amazon Web Services (AWS), 5: Welcome - IAM Access Analyzer

**NEW QUESTION 145**

- (Topic 3)

A company's IT team is managing MySQL database server clusters. The IT team has to patch the database and take backup snapshots of the data in the clusters. The company wants to move this workload to AWS so that these tasks will be completed automatically. What should the company do to meet these requirements?

- A. Deploy MySQL database server clusters on Amazon EC2 instances.
- B. Use Amazon RDS with a MySQL database.
- C. Use an AWS CloudFormation template to deploy MySQL database servers on Amazon EC2 instances.
- D. Migrate all the MySQL database data to Amazon S3.

**Answer:** B

**Explanation:**

Amazon RDS is a service that makes it easy to set up, operate, and scale a relational database in the cloud. Amazon RDS supports MySQL as one of the database engines. By using Amazon RDS with a MySQL database, the company can offload the tasks of patching the database and taking backup snapshots to AWS. Amazon RDS automatically patches the database software and operating system of the database instances. Amazon RDS also automatically backs up the database and retains the backups for a user-defined retention period. The company can also restore the database to any point in time within the retention period. Deploying MySQL database server clusters on Amazon EC2 instances, using an AWS CloudFormation template to deploy MySQL database servers on Amazon EC2 instances, or migrating all the MySQL database data to Amazon S3 are not the best options to meet the requirements. These options would not automate the tasks of patching the database and taking backup snapshots, and would require more operational overhead from the company.

**NEW QUESTION 149**

- (Topic 3)

A company is looking for a managed machine learning (ML) service that can recommend products based on a customer's previous behaviors. Which AWS service meets this requirement?

- A. Amazon Personalize
- B. Amazon SageMaker
- C. Amazon Pinpoint
- D. Amazon Comprehend

**Answer:** A

**Explanation:**

The AWS service that meets the requirement of providing a managed machine learning (ML) service that can recommend products based on a customer's previous behaviors is Amazon Personalize. Amazon Personalize is a fully managed service that enables developers to create personalized recommendations for customers using their own data. Amazon Personalize can automatically process and examine the data, identify what is meaningful, select the right algorithms, and train and optimize a personalized recommendation model. Amazon SageMaker, Amazon Pinpoint, and Amazon Comprehend are other AWS services related to machine learning, but they do not provide the specific functionality of product recommendation.

**NEW QUESTION 150**

- (Topic 3)

Which AWS service is always provided at no charge?

- A. Amazon S3
- B. AWS Identity and Access Management (IAM)
- C. Elastic Load Balancers
- D. AWS WAF

**Answer:** B

**Explanation:**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You can use IAM to create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM is always provided at no charge. References: 1: AWS Identity and Access Management (IAM) - Amazon Web Services (AWS), 2: Which aws service is always provided at no charge? - Brainly.in

**NEW QUESTION 155**

- (Topic 3)

A company wants a time-series database service that makes it easier to store and analyze trillions of events each day. Which AWS service will meet this requirement?

- A. Amazon Neptune

- B. Amazon Timestream
- C. Amazon Forecast
- D. Amazon DocumentDB (with MongoDB compatibility)

**Answer:** B

**Explanation:**

Amazon Timestream is a fast, scalable, and serverless time-series database service for IoT and other operational applications that makes it easy to store and analyze trillions of events per day up to 1,000 times faster and at as little as 1/10th the cost of relational databases<sup>1</sup>. Amazon Timestream saves you time and cost in managing the lifecycle of time series data, and its purpose-built query engine lets you access and analyze recent and historical data together with a single query<sup>1</sup>. Amazon Timestream has built-in time series analytics functions, helping you identify trends and patterns in near real time<sup>1</sup>. The other options are not suitable for storing and analyzing trillions of events per day. Amazon Neptune is a graph database service that supports highly connected data sets. Amazon Forecast is a machine learning service that generates accurate forecasts based on historical data. Amazon DocumentDB (with MongoDB compatibility) is a document database service that supports MongoDB workloads.

References:

? 1: Time Series Database – Amazon Timestream – Amazon Web Services

**NEW QUESTION 160**

- (Topic 3)

An ecommerce company wants to use Amazon EC2 Auto Scaling to add and remove EC2 instances based on CPU utilization. Which AWS service or feature can initiate an Amazon EC2 Auto Scaling action to achieve this goal?

- A. Amazon Simple Queue Service (Amazon SQS)
- B. Amazon Simple Notification Service (Amazon SNS)
- C. AWS Systems Manager
- D. Amazon CloudWatch alarm

**Answer:** D

**Explanation:**

Amazon CloudWatch alarm is an AWS service or feature that can initiate an Amazon EC2 Auto Scaling action based on CPU utilization. Amazon CloudWatch is a monitoring and observability service that collects and tracks metrics, logs, events, and alarms for your AWS resources and applications. Amazon CloudWatch alarms are actions that you can configure to send notifications or automatically make changes to the resources you are monitoring based on rules that you define<sup>67</sup>.

Amazon EC2 Auto Scaling is a service that helps you maintain application availability and allows you to automatically add or remove EC2 instances according to definable conditions. You can create dynamic scaling policies that track a specific CloudWatch metric, such as CPU utilization, and define what action to take when the associated CloudWatch alarm is in ALARM. When the policy is in effect, Amazon EC2 Auto Scaling adjusts the group's desired capacity up or down when the threshold of an alarm is

breached<sup>89</sup>. References: 6: Cloud Monitoring - Amazon CloudWatch - AWS, 7: Amazon

CloudWatch Documentation, 8: Dynamic scaling for Amazon EC2 Auto Scaling, 9: Amazon EC2 Auto Scaling Documentation

**NEW QUESTION 165**

- (Topic 3)

A company is assessing its AWS Business Support plan to determine if the plan still meets the company's needs. The company is considering switching to AWS Enterprise Support.

Which additional benefit will the company receive with AWS Enterprise Support?

- A. A full set of AWS Trusted Advisor checks
- B. Phone, email, and chat access to cloud support engineers 24 hours a day, 7 days a week
- C. A designated technical account manager (TAM) to assist in monitoring and optimization
- D. A consultative review and architecture guidance for the company's applications

**Answer:** C

**Explanation:**

AWS Enterprise Support provides customers with a designated technical account manager (TAM) who is a single point of contact for all technical and operational issues. The TAM provides consultative architectural and operational guidance delivered in the context of the customer's applications and use-cases to help them achieve the greatest value from AWS. The TAM also helps customers with proactive services, such as strategic business reviews, security improvement programs, guided Well-Architected reviews, cost optimization workshops, and more<sup>1</sup>.

A full set of AWS Trusted Advisor checks is not an additional benefit of AWS Enterprise Support, as it is also included in the AWS Business Support plan<sup>2</sup>. AWS Trusted Advisor is a tool that provides best practice recommendations for cost optimization, performance, security, fault tolerance, and service limits.

Phone, email, and chat access to cloud support engineers 24 hours a day, 7 days a week is not an additional benefit of AWS Enterprise Support, as it is also included in the AWS Business Support plan<sup>2</sup>. Cloud support engineers can help customers with technical issues, such as troubleshooting, configuration, usage, and service features.

A consultative review and architecture guidance for the company's applications is not an additional benefit of AWS Enterprise Support, as it is also included in the AWS Business Support plan<sup>2</sup>. Customers can request a consultative review from a solutions architect who will provide best practices and recommendations based on the customer's use-cases and goals.

**NEW QUESTION 168**

- (Topic 3)

Which options are AWS Cloud Adoption Framework (AWS CAF) people perspective capabilities? (Select TWO.)

- A. Organizational alignment
- B. Portfolio management
- C. Organization design
- D. Risk management
- E. Modern application development

**Answer:** AC

**Explanation:**

The AWS Cloud Adoption Framework (AWS CAF) people perspective capabilities are the organizational skills and processes that enable effective cloud adoption. According to the AWS CAF people perspective whitepaper<sup>1</sup>, there are seven capabilities in this perspective, two of which are:

? Organizational alignment: This capability helps you align your organizational structure, roles, and responsibilities to support your cloud transformation goals and objectives. It involves assessing your current and desired state of alignment, identifying gaps and misalignments, and designing and implementing changes to optimize your cloud performance<sup>1</sup>.

? Organization design: This capability helps you design and evolve your organization to enable agility, innovation, and collaboration in the cloud. It involves defining your cloud operating model, identifying the skills and competencies needed for cloud roles, and creating career paths and development plans for your cloud workforce<sup>1</sup>.

The other options are not capabilities in the AWS CAF people perspective. Portfolio management, risk management, and modern application development are capabilities in the AWS CAF business perspective, governance perspective, and platform perspective respectively<sup>2</sup>.

References:

? 1: AWS Cloud Adoption Framework: People Perspective - AWS Cloud Adoption Framework: People Perspective

? 2: AWS Cloud Adoption Framework - AWS Cloud Adoption Framework

**NEW QUESTION 171**

- (Topic 3)

Which of the following is a software development framework that a company can use to define cloud resources as code and provision the resources through AWS CloudFormation?

- A. AWS CLI
- B. AWS Developer Center
- C. AWS Cloud Development Kit (AWS CDK)
- D. AWS CodeStar

**Answer: C**

**Explanation:**

AWS Cloud Development Kit (AWS CDK) is a software development framework that allows you to define cloud resources as code using familiar programming languages, such as TypeScript, Python, Java, .NET, and Go (in Developer Preview). You can use AWS CDK to model your application resources using high-level constructs that provide sensible defaults and best practices, or use low-level constructs that provide full access to the underlying AWS CloudFormation resources. AWS CDK synthesizes your code into AWS CloudFormation templates that you can deploy using the AWS CDK CLI or the AWS Management Console. AWS CDK also integrates with other AWS services, such as AWS CodeCommit, AWS CodeBuild, AWS CodePipeline, AWS Lambda, Amazon EC2, Amazon S3, and more, to help you automate your development and deployment processes. AWS CDK is an open-source framework that you can extend and contribute to. References:

Cloud Development Framework - AWS Cloud Development Kit -

AWS, AWS Cloud Development Kit Documentation, AWS Cloud Development Kit - Wikipedia, AWS CDK Intro Workshop | AWS CDK Workshop

**NEW QUESTION 172**

- (Topic 3)

A company is building an application on AWS. The application needs to comply with credit card regulatory requirements. The company needs proof that the AWS services and deployment are in compliance.

Which actions should the company take to meet these requirements? (Select TWO.)

- A. Use Amazon Inspector to submit the application for certification.
- B. Ensure that the application's underlying hardware components comply with requirements.
- C. Use AWS Artifact to access AWS documents about the compliance of the services.
- D. Get the compliance of the application certified by a company assessor.
- E. Use AWS Security Hub to certify the compliance of the application.

**Answer: CD**

**Explanation:**

Using AWS Artifact to access AWS documents about the compliance of the services, and getting the compliance of the application certified by a company assessor are actions that the company should take to meet the requirements of complying with credit card regulatory requirements. AWS Artifact is a service that provides on-demand access to AWS security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. AWS Artifact can help you demonstrate compliance with credit card regulatory requirements by providing you with proof that the AWS services and deployment are in compliance. Getting the compliance of the application certified by a company assessor is an action that the company should take to ensure that the application meets the specific requirements of the credit card industry. A company assessor is an independent third-party entity that is qualified to assess the compliance of the application with the relevant standards and regulations. Using Amazon Inspector to submit the application for certification is not an action that the company should take, because Amazon Inspector is a service that helps you improve the security and compliance of your applications deployed on AWS by automatically assessing them for vulnerabilities and deviations from best practices, but it does not provide certification for the applications. Ensuring that the application's underlying hardware components comply with requirements is not an action that the company should take, because the application is deployed on AWS, and AWS is responsible for the security and compliance of the underlying hardware components. This is part of the shared responsibility model, where AWS is responsible for security of the cloud, and customers are responsible for security in the cloud. Using AWS Security Hub to certify the compliance of the application is not an action that the company should take, because AWS Security Hub is a service that gives you a comprehensive view of your security posture across your AWS accounts and helps you check your environment against security industry standards and best practices, but it does not provide certification for the applications.

**NEW QUESTION 176**

- (Topic 3)

A company needs to search for text in documents that are stored in Amazon S3. Which AWS service will meet these requirements?

- A. Amazon Kendra
- B. Amazon Rekognition
- C. Amazon Polly
- D. Amazon Lex

**Answer: A**

**Explanation:**

Amazon Kendra is a highly accurate and easy to use intelligent search service powered by machine learning. It enables users to easily find the content they are looking for, even when it is scattered across multiple locations and content repositories within their organization. Amazon Kendra supports natural language queries, and can search for text in documents stored in Amazon S3, as well as other sources such as SharePoint, OneDrive, Salesforce, ServiceNow, and more. Amazon Rekognition is a computer vision service that makes it easy to add image and video analysis to applications. It can detect objects, faces, text, scenes, activities, and emotions in images and videos. However, it is not designed for searching for text in documents stored in Amazon S3.

Amazon Polly is a text-to-speech service that turns text into lifelike speech. It can create audio versions of books, articles, podcasts, and more. However, it is not designed for searching for text in documents stored in Amazon S3.

Amazon Lex is a service for building conversational interfaces using voice and text. It can create chatbots that can interact with users using natural language. However, it is not designed for searching for text in documents stored in Amazon S3.

**References:**

? Amazon Kendra – Intelligent Search Service Powered by Machine Learning

? Amazon Rekognition – Video and Image - AWS

? Amazon Polly – Text-to-Speech Service - AWS

? Amazon Lex – Build Conversation Bots - AWS

**NEW QUESTION 181**

- (Topic 3)

Which AWS service or feature will search for and identify AWS resources that are shared externally?

- A. Amazon OpenSearch Service
- B. AWS Control Tower
- C. AWS IAM Access Analyzer
- D. AWS Fargate

**Answer: C**

**Explanation:**

AWS IAM Access Analyzer is an AWS service that helps customers identify and review the resources in their AWS account that are shared with an external entity, such as another AWS account, a root user, an organization, or a public entity. AWS IAM Access Analyzer uses automated reasoning, a form of mathematical logic and inference, to analyze the resource-based policies in the account and generate comprehensive findings that show the access level, the source of the access, the affected resource, and the condition under which the access applies. Customers can use AWS IAM Access Analyzer to audit their shared resources, validate their access policies, and monitor any changes to the resource sharing status. References: AWS IAM Access Analyzer, Identify and review resources shared with external entities, How AWS IAM Access Analyzer works

**NEW QUESTION 184**

- (Topic 3)

A company wants to use the latest technologies and wants to minimize its capital investment. Instead of upgrading on-premises infrastructure, the company wants to move to the AWS Cloud.

Which AWS Cloud benefit does this scenario describe?

- A. Increased speed to market
- B. The trade of infrastructure expenses for operating expenses
- C. Massive economies of scale
- D. The ability to go global in minutes

**Answer: B**

**Explanation:**

The trade of infrastructure expenses for operating expenses is one of the benefits of the AWS Cloud. By moving to the AWS Cloud, the company can avoid the upfront costs of purchasing and maintaining on-premises infrastructure, such as servers, storage, network, and software. Instead, the company can pay only for the AWS resources and services that they use, as they use them. This reduces the risk and complexity of planning and managing IT infrastructure, and allows the company to focus on innovation and growth. Increased speed to market, massive economies of scale, and the ability to go global in minutes are also benefits of the AWS Cloud, but they are not the best ones to describe this scenario. Increased speed to market means that the company can launch new products and services faster by using AWS services and tools. Massive economies of scale means that the company can benefit from the lower costs and higher performance that AWS achieves by operating at a large scale. The ability to go global in minutes means that the company can deploy their applications and data in multiple regions and availability zones around the world to reach their customers faster and improve performance and reliability.

**NEW QUESTION 187**

- (Topic 3)

A company wants to migrate its server-based applications to the AWS Cloud. The company wants to determine the total cost of ownership for its compute resources that will be hosted on the AWS Cloud.

Which combination of AWS services or tools will meet these requirements?

- A. AWS Pricing Calculator
- B. Migration Evaluator
- C. AWS Support Center
- D. AWS Application Discovery Service
- E. AWS Database Migration Service (AWS DMS)

**Answer: AD**

**Explanation:**

AWS Pricing Calculator and AWS Application Discovery Service are the best combination of AWS services or tools to meet the requirements of determining the total cost of ownership for compute resources that will be hosted on the AWS Cloud. AWS Pricing Calculator is a tool that enables you to estimate the cost of using AWS services based on your usage scenarios and requirements. You can use AWS Pricing Calculator to compare the costs of running your applications on-premises or on AWS, and to optimize your AWS spending. AWS Application Discovery Service is a service that helps you plan your migration to the AWS Cloud by collecting and analyzing information about your on-premises servers, applications, and dependencies. You can use AWS Application Discovery Service to identify the inventory of your on-premises infrastructure, group servers by applications, and estimate the performance and resource utilization of your applications.

### NEW QUESTION 191

- (Topic 3)

Which capabilities are in the platform perspective of the AWS Cloud Adoption Framework (AWS CAF)? (Select TWO.)

- A. Performance and capacity management
- B. Data engineering
- C. Continuous integration and continuous delivery (CI/CD)
- D. Infrastructure protection
- E. Change and release management

**Answer:** BC

#### Explanation:

The platform perspective of the AWS Cloud Adoption Framework (AWS CAF) helps you build an enterprise-grade, scalable, hybrid cloud platform, modernize existing workloads, and implement new cloud-native solutions<sup>1</sup>. It comprises seven capabilities, two of which are data engineering and CI/CD<sup>1</sup>.

? Data engineering: This capability helps you design and evolve a fit-for-purpose data and analytics architecture that can reduce complexity, cost, and technical debt while enabling you to gain actionable insights from exponentially growing data volumes<sup>1</sup>. It involves selecting key technologies for each of your architectural layers, such as ingestion, storage, catalog, processing, and consumption. It also involves supporting real-time data processing and adopting a Lake House architecture to facilitate data movements between data lakes and purpose-built data stores<sup>1</sup>.

? CI/CD: This capability helps you automate the delivery of your cloud solutions using a set of practices and tools that enable faster and more reliable deployments<sup>1</sup>. It involves establishing a pipeline that can build, test, and deploy your code across multiple environments. It also involves adopting a DevOps culture that fosters collaboration, feedback, and continuous improvement among your development and operations teams<sup>1</sup>.

References:

? 1: Platform perspective: infrastructure and applications - An Overview of the AWS Cloud Adoption Framework

### NEW QUESTION 192

- (Topic 3)

Which AWS services make use of global edge locations'? (Select TWO.)

- A. AWS Fargate
- B. Amazon CloudFront
- C. AWS Global Accelerator
- D. AWS Wavelength
- E. Amazon VPC

**Answer:** BC

#### Explanation:

Amazon CloudFront and AWS Global Accelerator are two AWS services that make use of global edge locations. Edge locations are AWS sites that are deployed worldwide in major cities and places with a high population. Edge locations are used to cache data and reduce latency for end-user access<sup>1</sup>.

Amazon CloudFront is a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high

transfer speeds. Amazon CloudFront uses a global network of over 200 edge locations and 13 regional edge caches to cache your content closer to your viewers, improving performance and reducing costs<sup>23</sup>.

AWS Global Accelerator is a networking service that improves the availability and performance of your applications with local or global users. AWS Global Accelerator uses the AWS global network to route user traffic to the optimal endpoint based on health, performance, and policies. AWS Global Accelerator uses over 100 edge locations to bring your application endpoints closer to your users, reducing network hops and improving user experience<sup>45</sup>. References: 1: AWS for the Edge - Amazon Web Services

(AWS), 2: Content Delivery Network (CDN) - Amazon CloudFront - AWS, 3: Amazon CloudFront Documentation, 4: AWS Global Accelerator - Amazon Web Services, 5: AWS Global Accelerator Documentation

### NEW QUESTION 195

- (Topic 3)

How does the AWS Enterprise Support Concierge team help users?

- A. Supporting application development
- B. Providing architecture guidance
- C. Answering billing and account inquiries
- D. Answering questions regarding technical support cases

**Answer:** C

#### Explanation:

The AWS Enterprise Support Concierge team is a group of billing and account experts who specialize in working with enterprise customers. They can help customers with questions about billing, account management, cost optimization, and other non-technical issues. They can also assist customers with navigating and optimizing their AWS environment, such as setting up consolidated billing, applying for service limit increases, or requesting refunds. References:

? AWS Support Plan Comparison

? AWS Enterprise Support Plan

? Answer Explained: Which AWS Support plan provides access to AWS Concierge Support team for account assistance?

### NEW QUESTION 200

- (Topic 3)

A company wants to establish a private network connection between AWS and its corporate network.

Which AWS service or feature will meet this requirement?

- A. Amazon Connect
- B. Amazon Route 53
- C. AWS Direct Connect
- D. VPC peering

**Answer:** C

**Explanation:**

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections<sup>12</sup>. References: 1: Dedicated Network Connection - AWS Direct Connect - AWS, 2: What is AWS Direct Connect? - AWS Direct Connect

**NEW QUESTION 202**

- (Topic 3)

Which of the following are pillars of the AWS Well-Architected Framework? (Select TWO)

- A. High availability
- B. Performance efficiency
- C. Cost optimization
- D. Going global in minutes
- E. Continuous development

**Answer:** BC

**Explanation:**

The AWS Well-Architected Framework is a set of six pillars and lenses that help cloud architects design and run workloads in the cloud. The six pillars are: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. Each pillar has a set of design principles and best practices that guide the architectural decisions. High availability is not a separate pillar, but a quality that can be achieved by applying the principles of the reliability pillar. Going global in minutes and continuous development are not pillars of the framework, but possible benefits of using AWS services and following the framework's recommendations. References: AWS Well-Architected - Build secure, efficient cloud applications, AWS Well-Architected Framework, The 6 Pillars of the AWS Well-Architected Framework

**NEW QUESTION 204**

- (Topic 3)

Which AWS service is a continuous delivery and deployment solution?

- A. AWSAppSync
- B. AWS CodePipeline
- C. AWS Cloud9
- D. AWS CodeCommit

**Answer:** B

**Explanation:**

AWS CodePipeline is a continuous delivery and deployment service that automates the release process of software applications across different stages, such as source code, build, test, and deploy<sup>2</sup>. AWSAppSync, AWS Cloud9, and AWS CodeCommit are other AWS services related to application development, but they do not provide continuous delivery and deployment solutions<sup>34</sup>.

**NEW QUESTION 208**

- (Topic 3)

Which option is an AWS Cloud Adoption Framework (AWS CAF) foundational capability for the operations perspective?

- A. Performance and capacity management
- B. Application portfolio management
- C. Identity and access management
- D. Product management

**Answer:** C

**Explanation:**

Identity and access management is one of the foundational capabilities for the operations perspective of the AWS Cloud Adoption Framework (AWS CAF). It involves managing the identities, roles, permissions, and credentials of users and systems that interact with AWS resources. Performance and capacity management is a capability for the platform perspective. Application portfolio management is a capability for the business perspective. Product management is a capability for the governance perspective.

**NEW QUESTION 213**

- (Topic 3)

Which of the following is a fully managed graph database service on AWS?

- A. Amazon Aurora
- B. Amazon FSx
- C. Amazon DynamoDB
- D. Amazon Neptune

**Answer:** D

**Explanation:**

Amazon Neptune is a fully managed graph database service on AWS. A graph database is a type of database that stores and queries data as a network of nodes and edges, representing entities and relationships. Graph databases are useful for applications that deal with highly connected data, such as social networks, recommendation engines, fraud detection, and knowledge graphs<sup>45</sup>. Amazon Neptune is a fast, reliable, and scalable graph database service that supports two popular graph models: property graphs and RDF. Amazon Neptune also supports two open standards for querying graphs: Apache TinkerPop Gremlin and SPARQL. Amazon Neptune handles the heavy lifting of managing the database, such as provisioning, patching, backup, recovery, encryption, and replication<sup>456</sup>.

References: 4: Managed Graph Database - Amazon Neptune - AWS, 5: Amazon Neptune – A Fully Managed Graph Database Service, 6: Working with AWS Neptune. Neptune is a fully-managed graph ... - Medium

#### NEW QUESTION 215

- (Topic 3)

A company must archive Amazon S3 data that the company's business units no longer need to access. Which S3 storage class will meet this requirement MOST cost-effectively?

- A. S3 Glacier Instant Retrieval
- B. S3 Glacier Flexible Retrieval
- C. S3 Glacier Deep Archive
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

**Answer: C**

#### Explanation:

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. Customers can store large amounts of data at a very low cost, and reliably access it with a wait time of 12 hours.

#### NEW QUESTION 216

- (Topic 3)

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

- 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 instances](#)

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](#)

#### NEW QUESTION 221

- (Topic 3)

Which maintenance task is the customer's responsibility, according to the AWS shared responsibility model?

- A. Physical connectivity among Availability Zones
- B. Network switch maintenance
- C. Hardware updates and firmware patches
- D. Amazon EC2 updates and security patches

**Answer: D**

#### Explanation:

According to the AWS shared responsibility model, customers are responsible for managing their data, applications, operating systems, security groups, and other aspects of their AWS environment. This includes installing updates and security patches of the guest operating system and any application software or utilities installed by the customer on the instances. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud, such as data centers, hardware, software, networking, and facilities. This includes the physical connectivity among Availability Zones, the network switch maintenance, and the hardware updates and firmware patches. Therefore, option D is the correct answer, and options A, B, and C are AWS responsibilities, not customer responsibilities. References: [AWS Well-Architected Framework - Elasticity](#); [Reactive Systems on AWS - Elastic](#)

#### NEW QUESTION 224

- (Topic 3)

Which Amazon S3 storage class is the MOST cost-effective for long-term storage?

- A. S3 Glacier Deep Archive
- B. S3 Standard
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

**Answer: A**

#### Explanation:

Amazon S3 Glacier Deep Archive is the lowest-cost storage class in the cloud. It is designed for long-term data archiving that is rarely accessed. It offers a retrieval time of 12 hours and a durability of 99.999999999% (11 9's). It is ideal for data that must be retained for 7 years or longer to meet regulatory compliance requirements.

#### NEW QUESTION 227

- (Topic 3)

A company wants a key-value NoSQL database that is fully managed and serverless. Which AWS service will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS
- C. Amazon Aurora
- D. Amazon Memory DB for Redis

**Answer:** A

#### Explanation:

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It is a fully managed, serverless database that does not require provisioning, patching, or backup. It offers built-in security, backup and restore, and in-memory caching<sup>3</sup>. Amazon RDS is a relational database service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. However, it is not a key-value NoSQL database, and it is not serverless, as it requires you to choose an instance type and size<sup>4</sup>. Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. However, it is also not a key-value NoSQL database, and it is not serverless, as it requires you to choose an instance type and size. Amazon MemoryDB for Redis is a Redis-compatible, durable, in-memory database service that delivers ultra-fast performance and multi-AZ reliability for the most demanding applications. However, it is also not a key-value NoSQL database, and it is not serverless, as it requires you to choose a node type and size.

#### NEW QUESTION 232

- (Topic 3)

A developer who has no AWS Cloud experience wants to use AWS technology to build a web application. Which AWS service should the developer use to start building the application?

- A. Amazon SageMaker
- B. AWS Lambda
- C. Amazon Lightsail
- D. Amazon Elastic Container Service (Amazon ECS)

**Answer:** C

#### Explanation:

Amazon Lightsail is an easy-to-use cloud platform that offers everything you need to build an application or website, plus a cost-effective, monthly plan<sup>1</sup>. It is designed for developers who have little or no prior cloud experience and want to launch and manage applications on AWS with minimal complexity<sup>2</sup>. Amazon SageMaker is a service for building, training, and deploying machine learning models<sup>3</sup>. AWS Lambda is a service that lets you run code without provisioning or managing servers<sup>4</sup>. Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service.

#### NEW QUESTION 234

- (Topic 3)

A company wants to automatically add and remove Amazon EC2 instances. The company wants the EC2 instances to adjust to varying workloads dynamically. Which service or feature will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon EC2 Spot Instances
- C. AWS Snow Family
- D. Amazon EC2 Auto Scaling

**Answer:** D

#### Explanation:

Amazon EC2 Auto Scaling is a service that helps you maintain application availability and allows you to automatically add or remove EC2 instances according to definable conditions. You can create collections of EC2 instances, called Auto Scaling groups, and specify the minimum and maximum number of instances in each group. You can also define scaling policies that adjust the number of instances based on the demand on your application. Amazon EC2 Auto Scaling helps you improve the performance, reliability, and cost-efficiency of your EC2 workloads<sup>123</sup>. References: 1: VDI Desktops - Amazon WorkSpaces Family - AWS, 2: What is Amazon EC2 Auto Scaling? - Amazon EC2 Auto Scaling, 3: Discover Amazon EC2 Auto Scaling Unit | Salesforce Trailhead

#### NEW QUESTION 237

- (Topic 3)

Which AWS Support plan is the minimum recommended tier for users who have production workloads on AWS?

- A. AWS Developer Support
- B. AWS Enterprise Support
- C. AWS Business Support
- D. AWS Enterprise On-Ramp Support

**Answer:** C

#### Explanation:

AWS Business Support is the minimum recommended tier for users who have production workloads on AWS. AWS Business Support provides 24x7 access to cloud support engineers via phone, chat, or email, as well as a guaranteed response time of less than one hour for urgent issues. AWS Business Support also includes access to AWS Trusted Advisor, a tool that provides real-time guidance to help you provision your resources following AWS best practices<sup>4</sup>.

#### NEW QUESTION 241

- (Topic 3)

Which AWS services or features can a company use to connect the network of its on-premises data center to AWS? (Select TWO.)

- A. AWS VPN
- B. AWS Directory Service
- C. AWS Data Pipeline
- D. AWS Direct Connect
- E. AWS CloudHSM

**Answer:** AD

#### Explanation:

AWS VPN and AWS Direct Connect are two services that enable customers to connect their on-premises data center network to the AWS Cloud. AWS VPN establishes a secure and encrypted connection over the public internet, while AWS Direct Connect establishes a dedicated and private connection through a partner network. You can learn more about AWS VPN from [this webpage] or [this digital course]. You can learn more about AWS Direct Connect from [this webpage] or [this digital course].

#### NEW QUESTION 242

- (Topic 3)

Which AWS service provides protection against DDoS attacks for applications that run in the AWS Cloud?

- A. Amazon VPC
- B. AWS Shield
- C. AWS Audit Manager
- D. AWS Config

**Answer:** B

#### Explanation:

AWS Shield is an AWS service that provides protection against distributed denial of service (DDoS) attacks for applications that run in the AWS Cloud. DDoS attacks are attempts to make an online service unavailable by overwhelming it with traffic from multiple sources. AWS Shield provides two tiers of protection: AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is automatically enabled for all AWS customers at no additional charge. It provides protection against common and frequently occurring network and transport layer DDoS attacks. AWS Shield Advanced is an optional paid service that provides additional protection against larger and more sophisticated DDoS attacks. AWS Shield Advanced also provides access to 24/7 DDoS response team, cost protection, and enhanced detection and mitigation capabilities

#### NEW QUESTION 243

- (Topic 3)

Which task can only an AWS account root user perform?

- A. Changing the AWS Support plan
- B. Deleting AWS resources
- C. Creating an Amazon EC2 instance key pair
- D. Configuring AWS WAF

**Answer:** A

#### Explanation:

The AWS account root user is the email address that you use to sign up for AWS. The root user has complete access to all AWS services and resources in the account. The root user can perform tasks that only the root user can do, such as changing the AWS Support plan, closing the account, and restoring IAM user permissions<sup>34</sup>

#### NEW QUESTION 247

- (Topic 3)

A company wants to build a new web application by using AWS services. The application must meet the on-demand load for periods of heavy activity. Which AWS services or resources provide the necessary workload adjustments to meet these requirements? (Select TWO.)

- A. Amazon Machine Image (AMI)
- B. Amazon EC2 Auto Scaling
- C. Amazon EC2 instance
- D. AWS Lambda
- E. EC2 Image Builder

**Answer:** BD

#### Explanation:

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size<sup>4</sup>. AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

#### NEW QUESTION 248

- (Topic 3)

A company needs a graph database service that is scalable and highly available.

Which AWS service meets these requirements?

- A. Amazon Aurora
- B. Amazon Redshift
- C. Amazon DynamoDB
- D. Amazon Neptune

**Answer:** D

**Explanation:**

The AWS service that meets the requirements of providing a graph database service that is scalable and highly available is Amazon Neptune. Amazon Neptune is a fast, reliable, and fully managed graph database service that supports property graph and RDF graph models. Amazon Neptune is designed to store billions of relationships and query the graph with milliseconds latency. Amazon Neptune also offers high availability and durability by replicating six copies of the data across three Availability Zones and continuously backing up the data to Amazon S3. Amazon Aurora, Amazon Redshift, and Amazon DynamoDB are other AWS services that provide relational or non-relational database solutions, but they do not support graph database models.

**NEW QUESTION 249**

- (Topic 3)

A company wants to grant users in one AWS account access to resources in another AWS account. The users do not currently have permission to access the resources.

Which AWS service will meet this requirement?

- A. IAM group
- B. IAM role
- C. IAM tag
- D. IAM Access Analyzer

**Answer:** B

**Explanation:**

IAM roles are a way to delegate access to resources in different AWS accounts. IAM roles allow users to assume a set of permissions for a limited time without having to create or share long-term credentials. IAM roles can be used to grant cross-account access by creating a trust relationship between the accounts and specifying the permissions that the role can perform. Users can then switch to the role and access the resources in the other account using temporary security credentials provided by the role. References: Cross account resource access in IAM, IAM tutorial: Delegate access across AWS accounts using IAM roles, How to Enable Cross-Account Access to the AWS Management Console

**NEW QUESTION 250**

- (Topic 3)

A company needs to securely store important credentials that an application uses to connect users to a database.

Which AWS service can meet this requirement with the MINIMAL amount of operational overhead?

- A. AWS Key Management Service (AWS KMS)
- B. AWS Config
- C. AWS Secrets Manager
- D. Amazon GuardDuty

**Answer:** C

**Explanation:**

AWS Secrets Manager is a service that helps you protect secrets needed to access your applications, services, and IT resources. You can use AWS Secrets Manager to store, rotate, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. AWS Secrets Manager eliminates the need to hardcode sensitive information in plain text, and reduces the risk of unauthorized access or leakage. AWS Secrets Manager also integrates with other AWS services, such as AWS Lambda, Amazon RDS, and AWS CloudFormation, to simplify the management of secrets across your environment.

**NEW QUESTION 253**

- (Topic 3)

Which VPC component provides a layer of security at the subnet level?

- A. Security groups
- B. Network ACLs
- C. NAT gateways
- D. Route tables

**Answer:** B

**Explanation:**

Network ACLs are a feature that provide a layer of security at the subnet level by acting as a firewall to control traffic in and out of one or more subnets. Network ACLs can be configured with rules that allow or deny traffic based on the source and destination IP addresses, ports, and protocols. Security groups are a feature that provide a layer of security at the instance level by acting as a firewall to control traffic to and from one or more instances. Security groups can be configured with rules that allow or deny traffic based on the source and destination IP addresses, ports, protocols, and security groups. NAT gateways are a feature that enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. Route tables are a feature that determine where network traffic from a subnet or gateway is directed.

**NEW QUESTION 256**

- (Topic 3)

Which AWS service or feature gives users the ability to capture information about network traffic in a VPC?

- A. VPC Flow Logs

- B. Amazon Inspector
- C. VPC route tables
- D. AWS CloudTrail

**Answer:** A

**Explanation:**

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. You can use VPC Flow Logs to diagnose network issues, monitor traffic patterns, detect security anomalies, and comply with auditing requirements<sup>34</sup>. References: Logging IP traffic using VPC Flow Logs - Amazon Virtual Private Cloud, New – VPC Traffic Mirroring – Capture & Inspect Network Traffic | AWS News Blog

**NEW QUESTION 257**

- (Topic 3)

A company wants to migrate its workloads to AWS, but it lacks expertise in AWS Cloud computing. Which AWS service or feature will help the company with its migration?

- A. AWS Trusted Advisor
- B. AWS Consulting Partners
- C. AWS Artifacts
- D. AWS Managed Services

**Answer:** D

**Explanation:**

AWS Managed Services is a service that provides operational management for AWS infrastructure and applications. It helps users migrate their workloads to AWS and provides ongoing support, security, compliance, and automation. AWS Trusted Advisor is a service that provides best practices and recommendations for cost optimization, performance, security, and fault tolerance. AWS Consulting Partners are professional services firms that help customers design, architect, build, migrate, and manage their workloads and applications on AWS. AWS Artifacts is a service that provides on-demand access to AWS compliance reports and select online agreements.

**NEW QUESTION 259**

- (Topic 3)

Which of the following is an AWS Well-Architected Framework design principle for operational excellence in the AWS Cloud?

- A. Go global in minutes
- B. Make frequent, small, reversible changes
- C. Implement a strong foundation of identity and access management
- D. Stop spending money on hardware infrastructure for data center operations

**Answer:** B

**Explanation:**

Making frequent, small, reversible changes is one of the design principles for operational excellence in the AWS Cloud, as defined by the AWS Well-Architected Framework. This principle means that you should design your workloads to allow for rapid and safe changes, such as deploying updates, rolling back failures, and experimenting with new features. By making small and reversible changes, you can reduce the risk of errors, minimize the impact of failures, and increase the speed of recovery<sup>2</sup>. References: 2: AWS Documentation - AWS Well-Architected Framework - Operational Excellence Pillar

**NEW QUESTION 264**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CLF-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CLF-C02 Product From:

<https://www.2passeasy.com/dumps/CLF-C02/>

### Money Back Guarantee

#### **CLF-C02 Practice Exam Features:**

- \* CLF-C02 Questions and Answers Updated Frequently
- \* CLF-C02 Practice Questions Verified by Expert Senior Certified Staff
- \* CLF-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CLF-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year