2passeasy

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 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 resources12.
* 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 history34.
* 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 tasks5 .
* 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 role12.
* 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 management34.

NEW QUESTION 3
- (Topic 3)
A company is migrating to the AWS Cloud to meet storage needs. The company wants to optimize costs based on the amount of storage that the company uses.
Which AWS offering or benefit will meet these requirements MOST cost-effectively?

A. Pay-as-you-go pricing
B. Savings Plans
C. AWS Free Tier
D. Volume-based discounts

Answer: D

Explanation:
Volume-based discounts are an AWS offering or benefit that can help the company optimize costs based on the amount of storage that the company uses. Volume- based discounts are discounts that AWS provides for some storage services, such as Amazon S3 and Amazon EBS, when the company stores a large amount of data. The more data the company stores, the lower the price per GB. For example, Amazon S3 offers six storage classes, each with a different price per GB. The price per GB decreases as the amount of data stored in each storage class increases

NEW QUESTION 4
- (Topic 3)
A company is migrating its applications from on-premises to the AWS Cloud. The company wants to ensure that the applications are assigned only the minimum permissions that are needed to perform all operations.
Which AWS service will meet these requirements'?

A. AWS Identity and Access Management (IAM)

B. Amazon CloudWatch
C. Amazon Macie
D. Amazon GuardDuty

Answer: A

Explanation:
 AWS Identity and Access Management (IAM) is a service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization). IAM also enables you to follow the principle of least privilege, which means granting only the permissions that are necessary to perform a task1. References: AWS Identity and Access Management (IAM) - AWS Documentation

NEW QUESTION 5
- (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 duration1. Amazon GuardDuty is a service that provides threat detection for your AWS accounts and workloads, but it does not offer DDoS protection3. 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 6
- (Topic 3)
A company wants to migrate its on_premises workloads to the AWS Cloud. The company wants to separate workloads for chargeback to different departments.
Which AWS services or features will meet these requirements? (Select TWO.)

A. Placement groups
B. Consolidated billing
C. Edge locations
D. AWS Config
E. Multiple AWS accounts

Answer: BE

Explanation:
 Consolidated billing is a feature of AWS Organizations that enables customers to consolidate billing and payment for multiple AWS accounts. With consolidated billing, customers can group multiple AWS accounts under one payer account, making it easier to manage billing and track costs across multiple accounts. Consolidated billing also offers benefits such as volume discounts, Reserved Instance discounts, and Savings Plans discounts. Consolidated billing is offered at no additional cost.
Multiple AWS accounts is a feature of AWS Organizations that enables customers to create and manage multiple AWS accounts from a central location. With multiple AWS accounts, customers can isolate workloads for different departments, projects, or environments, and apply granular access controls and policies to each account. Multiple AWS accounts also helps customers improve security, compliance, and governance of their AWS resources56. References: 5: Consolidated billing for AWS Organizations - AWS
Billing, 6: Understanding Consolidated Bills - AWS Billing, 7: AWS Consolidated Billing: Tutorial & Best Practices, 8: Simplifying Your Bills With Consolidated Billing on AWS - Aimably, 9: AWS Consolidated Billing - W3Schools

NEW QUESTION 7
- (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 environment1. AWS Control Tower helps you apply security best practices from the AWS Well-Architected Framework to all of your AWS accounts2.

NEW QUESTION 8
- (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 9
- (Topic 3)
A company wants to ensure that all of its Amazon EC2 instances have compliant operating system patches.
Which AWS service will meet these requirements?

A. AWS Compute Optimizer
B. AWS Elastic Beanstalk
C. AWS AppSync
D. AWS Systems Manager

Answer: D

Explanation:

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. You can use Systems Manager to apply OS patches, create system images, configure Windows and Linux operating systems, and execute PowerShell commands5. Systems Manager can help you ensure that all of your Amazon EC2 instances have compliant operating system patches by using the Patch Manager feature.

NEW QUESTION 10
- (Topic 3)
What is a benefit of using AWS serverless computing?

A. Application deployment and management are not required
B. Application security will be fully managed by AWS
C. Monitoring and logging are not needed
D. Management of infrastructure is offloaded to AWS

Answer: D

Explanation:

AWS serverless computing is a way of building and running applications without thinking about servers. AWS manages the infrastructure for you, so you don't have to provision, scale, patch, or monitor servers. You only pay for the compute time you consume, and you can focus on your application logic instead of managing servers12. References: Serverless Computing – Amazon Web Services, AWS Serverless Computing, Benefits, Architecture and Use-cases - XenonStack

NEW QUESTION 10
- (Topic 3)
A company is running its application in the AWS Cloud and wants to protect against a DDoS attack. The company's security team wants near real-time visibility into DDoS attacks.
Which AWS service or traffic filter will meet these requirements with the MOST features for DDoS protection?

A. AWS Shield Advanced
B. AWS Shield
C. Amazon GuardDuty
D. Network ACLs

Answer: A

Explanation:

AWS Shield Advanced is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield Advanced
provides you with 24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS attacks of any size or duration. AWS Shield Advanced also provides near real-time visibility into attacks, advanced attack mitigation capabilities, and integration with AWS WAF and AWS Firewall Manager1. AWS Shield is a standard service that provides always-on detection and automatic inline mitigations to minimize application downtime and latency, but it does not offer the same level of features and support as AWS Shield Advanced2. Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior, but it does not provide DDoS protection3. Network ACLs are stateless filters that can be associated with a subnet to control the traffic to and from the subnet, but they are not designed to protect against DDoS attacks

NEW QUESTION 14
- (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 19
- (Topic 3)
A cloud practitioner needs to obtain AWS compliance reports before migrating an environment to the AWS Cloud How can these reports be generated?

A. Contact the AWS Compliance team
B. Download the reports from AWS Artifact
C. Open a case with AWS Support
D. Generate the reports with Amazon Made

Answer: B

Explanation:
 AWS Artifact is a service that provides on-demand access to security and compliance reports from AWS and Independent Software Vendors (ISVs) who sell their products on AWS Marketplace. You can use AWS Artifact to download auditor-issued reports, certifications, accreditations, and other third-party attestations of AWS compliance with various standards and regulations, such as PCI-DSS, HIPAA, FedRAMP, GDPR, and more1234. You can also use AWS Artifact to review, accept, and manage your agreements with AWS and apply them to current and future accounts within your organization2. References: 1: Cloud Compliance - Amazon Web Services
(AWS), 2: Security Compliance Management - AWS Artifact - AWS, 3: AWS Compliance Contact Us - Amazon Web Services, 4: AWS SECURITY AND COMPLIANCE QUICK REFERENCE GUIDE

NEW QUESTION 22
- (Topic 3)
Which AWS service or storage class provides low-cost, long-term data storage?

A. Amazon S3 Glacier Deep Archive
B. AWS Snowball
C. Amazon MQ
D. AWS Storage Gateway

Answer: A

Explanation:
 Amazon S3 Glacier Deep Archive is a storage class within Amazon S3 that provides the lowest-cost, long-term data storage for data that is rarely accessed. AWS Snowball is a service that provides a physical device for transferring large amounts of data into and out of AWS. Amazon MQ is a service that provides managed message broker service for Apache ActiveMQ. AWS Storage Gateway is a service that provides hybrid cloud storage for on-premises applications.

NEW QUESTION 26
- (Topic 3)
A company processes personally identifiable information (PII) and must keep data in the country where it was generated. The company wants to use Amazon EC2 instances for these workloads.
Which AWS service will meet these requirements?

A. AWS Outposts
B. AWS Storage Gateway
C. AWS DataSync
D. AWS OpsWorks

Answer: A

Explanation:
 AWS Outposts is an AWS service that extends AWS infrastructure, services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility. AWS Outposts enables you to run Amazon EC2 instances and other AWS services locally, while maintaining a consistent and seamless connection to the AWS Cloud. AWS Outposts is ideal for workloads that require low latency, local data processing, or data residency. By using AWS Outposts, the company can process personally identifiable information (PII) and keep data in the country where it was generated, while leveraging the benefits of AWS

NEW QUESTION 28
- (Topic 3)
A company wants its AWS usage to be more sustainable. The company wants to track, measure, review, and forecast polluting emissions that result from its AWS applications.

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

A. AWS Health Dashboard
B. AWS customer carbon footprint tool
C. AWS Support Center
D. Amazon QuickSight

Answer: B

Explanation:
 AWS customer carbon footprint tool is a tool that helps customers measure and manage their carbon emissions from their AWS usage. It provides data on the carbon intensity, energy consumption, and estimated emissions of AWS services across regions and time periods. It also enables customers to review and forecast their emissions, and compare them with industry benchmarks. AWS Health Dashboard is a service that provides personalized information about the health and performance of AWS services and resources. AWS Support Center is a service that provides access to AWS support resources, such as cases, forums, and documentation. Amazon QuickSight is a service that provides business intelligence and analytics for AWS data sources.

NEW QUESTION 30
- (Topic 3)
A company needs to run a workload for several batch image rendering applications. It is acceptable for the workload to experience downtime.
Which Amazon EC2 pricing model would be MOST cost-effective in this situation?

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

Answer: D

Explanation:
 Amazon EC2 Spot Instances are instances that use spare EC2 capacity that is available at up to a 90% discount compared to On-Demand prices. You can use Spot Instances for various stateless, fault-tolerant, or flexible applications such as big data, containerized workloads, high-performance computing (HPC), and test & development workloads. Spot Instances are ideal for workloads that can be interrupted, such as batch image rendering applications1. On-Demand Instances are instances that let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs2. Reserved Instances are instances that provide you with a significant discount (up to 75%) compared to On-Demand Instance pricing. In exchange, you select a term and make an upfront payment to reserve a certain amount of compute capacity for that term3. Dedicated Instances are instances that run in a VPC on hardware that's dedicated to a single customer. Your Dedicated Instances are physically isolated at the host hardware level from instances that belong to other AWS accounts4.

NEW QUESTION 33
- (Topic 3)
A company needs to deploy applications in the AWS Cloud as quickly as possible. The company also needs to minimize the complexity that is related to the management of AWS resources.
Which AWS service should the company use to meet these requirements?

A. AWS config
B. AWS Elastic Beanstalk
C. Amazon EC2
D. Amazon Personalize

Answer: B

Explanation:
 AWS Elastic Beanstalk is the AWS service that allows customers to deploy applications in the AWS Cloud as quickly as possible. AWS Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and auto-scaling to application health monitoring. Customers can upload their code and Elastic Beanstalk will take care of the rest1. AWS Elastic Beanstalk also minimizes the complexity that is related to the management of AWS resources. Customers can retain full control of the underlying AWS resources powering their applications and adjust the settings to suit their needs1. Customers can also use the AWS Management Console, the AWS Command Line Interface (AWS CLI), or APIs to manage their applications1.
AWS Config is the AWS service that enables customers to assess, audit, and evaluate the configurations of their AWS resources. AWS Config continuously monitors and records the configuration changes of the resources and evaluates them against desired configurations or best practices2. AWS Config does not help customers deploy applications in the AWS Cloud as quickly as possible or minimize the complexity that is related to the management of AWS resources.
Amazon EC2 is the AWS service that provides secure, resizable compute capacity in the cloud. Customers can launch virtual servers called instances and choose from various configurations of CPU, memory, storage, and networking resources3. Amazon EC2 does not automatically handle the deployment or management of AWS resources for customers. Customers have to manually provision, configure, monitor, and scale their instances and other related resources.
Amazon Personalize is the AWS service that enables customers to create personalized recommendations for their users based on their behavior and preferences. Amazon Personalize uses machine learning to analyze data and deliver real-time recommendations4. Amazon Personalize does not help customers deploy applications in the AWS Cloud as quickly as possible or minimize the complexity that is related to the management of AWS resources.

NEW QUESTION 38
- (Topic 3)
Which cloud computing advantage is a company applying when it uses AWS Regions to increase application availability to users in different countries?

A. Pay-as-you-go pricing
B. Capacity forecasting
C. Economies of scale
D. Global reach

Answer: D

Explanation:
 Global reach is a cloud computing advantage that a company can apply when it uses AWS Regions to increase application availability to users in different

countries. Global reach refers to the ability to deploy applications and services in multiple geographic locations around the world, and to serve customers with low latency and high performance. AWS has the largest and most reliable global infrastructure of any cloud provider, with 25 Regions and 81 Availability Zones across the Americas, Europe, Asia Pacific, Africa, and the Middle East123. By using AWS Regions, a company can choose the best location for its application based on customer proximity, compliance requirements, and disaster recovery strategies23. References: 1: AWS Global Infrastructure - Amazon Web Services (AWS), 2: Regions and Availability Zones - Amazon Elastic Compute Cloud, 3: AWS Infrastructure: Regions and Availability Zones Explained

NEW QUESTION 39
- (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 40
- (Topic 3)
A company needs to store infrequently used data for data archives and long-term backups.
A company needs a history report about how its Amazon EC2 instances were modified last month.
Which AWS service can be used to meet this requirement?

A. AWS Service Catalog
B. AWS Config
C. Amazon CloudWatch
D. AWS Artifact

Answer: B

Explanation:
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records
your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. AWS Config can also track changes to your EC2 instances over time and provide a history report of the modifications. AWS Service Catalog, Amazon CloudWatch, and AWS Artifact are not the best services to meet this requirement. AWS Service Catalog is a service that allows you to create and manage catalogs of IT services that are approved for use on AWS. Amazon CloudWatch is a service that monitors your AWS resources and applications and provides metrics, alarms, dashboards, and logs. AWS Artifact is a service that provides on-demand access to AWS security and compliance reports and online agreements

NEW QUESTION 44
- (Topic 3)
Which AWS service gives users the ability to discover and protect sensitive data that is stored in Amazon S3 buckets?

A. Amazon Macie
B. Amazon Detective
C. Amazon GuardDuty
D. AWS I AM Access Analyzer

Answer: A

Explanation:
Amazon Macie is a data security and privacy service offered by AWS that uses machine learning and pattern matching to discover the sensitive data stored within Amazon S3. You can define your own custom type of sensitive data category that might be unique to your business or use case. Macie also provides you with dashboards and alerts that give you visibility into how your data is being accessed or moved. Macie helps you protect your data by enabling you to apply data protection techniques such as encryption, deletion, access control, and auditing. References: Strengthen the security of sensitive data stored in Amazon S3 by using additional AWS services, Security best practices for
Amazon S3, Sensitive Data Protection on AWS, Sensitive Data Protection on Amazon Web Services

NEW QUESTION 46
- (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 48
- (Topic 3)
A company wants to set AWS spending targets and track costs against those targets. Which AWS tool or feature should the company use to meet these requirements?

A. AWS Cost Explorer
B. AWS Budgets
C. AWS Cost and Usage Report
D. Savings Plans

Answer: B

Explanation:
 AWS Budgets is a tool that allows users to set AWS spending targets and track costs against those targets. Users can create budgets for various dimensions, such as service, linked account, tag, and more. Users can also receive alerts when the actual or forecasted costs exceed or are projected to exceed the budgeted amount. AWS Cost Explorer, AWS Cost and Usage Report, and Savings Plans are other AWS tools or features that can help users manage and optimize their AWS costs, but they do not enable users to set and track spending targets .

NEW QUESTION 53
- (Topic 3)
A team of researchers is going to collect data at remote locations around the world Many locations do not have internet connectivity. The team needs to capture the data in the field, and transfer it to the AWS Cloud later
Which AWS service will support these requirements?

A. AWS Outposts
B. AWS Transfer Family
C. AWS Snow Family
D. AWS Migration Hub

Answer: C

Explanation:
 AWS Snow Family is a group of devices that transport data in and out of AWS. AWS Snow Family devices are physical devices that can transfer up to exabytes of data. One exabyte is 1 000 000 000 000 megabytes. AWS Snow Family devices are designed for use in remote locations where internet connectivity is limited or unavailable. You can use these devices to collect and process data at the edge, and then ship them back to AWS for data upload. AWS Snow Family consists of three types of devices: AWS Snowcone, AWS Snowball, and AWS Snowmobile1234. References: 1: Edge Computing Devices, Secure Data Transfer - AWS Snow Family - AWS, 2: AWS Snow Family Documentation, 3: AWS Snow Family - W3Schools, 4: AWS Snow Family: Data Storage, Migration, and Computation

NEW QUESTION 55
- (Topic 3)
A company wants to launch its web application in a second AWS Region. The company needs to determine which services must be regionally configured for this launch.
Which AWS services can be configured at the Region level? (Select TWO.)

A. Amazon EC2
B. Amazon Route 53
C. Amazon CloudFront
D. AWS WAF
E. Amazon DynamoDB

Answer: BD

Explanation:
 Amazon Route 53 and AWS WAF are AWS services that can be configured at the Region level. Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service that lets you register domain names, route traffic to resources, and check the health of your resources. 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. Amazon EC2, Amazon CloudFront, and Amazon DynamoDB are AWS services that can be configured at the global level or the Availability Zone level .

NEW QUESTION 60
- (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 infrastructure1.

NEW QUESTION 65
- (Topic 3)
Which AWS services can be used to store files? (Select TWO.)

A. Amazon S3
B. AWS Lambda
C. Amazon Elastic Block Store (Amazon EBS)
D. Amazon SageMaker
E. AWS Storage Gateway

Answer: AC

Explanation:
Amazon S3 and Amazon EBS are two AWS services that can be used to store files . Amazon S3 is an object storage service that offers high scalability, durability, availability, and performance. Amazon EBS is a block storage service that provides persistent and low-latency storage volumes for Amazon EC2 instances. AWS Lambda, Amazon SageMaker, and AWS Storage Gateway are other AWS services that have different purposes, such as serverless computing, machine learning, and hybrid cloud storage .

NEW QUESTION 66
- (Topic 3)
Which AWS service provides storage that can be mounted across multiple Amazon EC2 instances?

A. Amazon Workspaces
B. Amazon Elastic File System (Amazon EFS)
C. AWS Database Migration Service (AWS DMS)
D. AWS Snowball Edge

Answer: B

Explanation:
Amazon EFS is a fully managed service that provides scalable and elastic file storage for multiple Amazon EC2 instances. Amazon EFS supports the Network File System (NFS) protocol, which allows multiple EC2 instances to access the same file system concurrently. You can learn more about Amazon EFS from this webpage or this digital course.

NEW QUESTION 71
- (Topic 3)
A company has created an AWS Cost and Usage Report and wants to visualize the report. Which AWS service should the company use to ingest and display this information?

A. Amazon QuickSight
B. Amazon Pinpoint
C. Amazon Neptune
D. Amazon Kinesis

Answer: A

Explanation:
Amazon QuickSight is an AWS service that provides business intelligence and data visualization capabilities. Amazon QuickSight enables you to ingest, analyze, and display data from various sources, such as AWS Cost and Usage Reports, Amazon S3, Amazon Athena, Amazon Redshift, and Amazon RDS. You can use Amazon QuickSight to create interactive dashboards and charts that show insights and trends from your data. You can also share your dashboards and charts with other users or embed them into your applications.

NEW QUESTION 74
- (Topic 3)
A company has a large number of Linux Amazon EC2 instances across several Availability Zones in an AWS Region. Applications that run on the EC2 instances need access to a common set of files.
Which AWS service or device should the company use to meet this requirement?

A. AWS Backup
B. Amazon Elastic File System (Amazon EFS)
C. Amazon Elastic Block Store (Amazon EBS)
D. AWS Snowball Edge Storage Optimized

Answer: B

Explanation:
Amazon Elastic File System (Amazon EFS) is a service that provides a scalable and elastic file system for Linux-based workloads. It can be mounted on multiple Amazon EC2 instances across different Availability Zones within a region, allowing applications to access a common set of files1. AWS Backup is a service that provides a centralized and automated way to back up data across AWS services. Amazon Elastic Block Store (Amazon EBS) is a service that provides persistent block storage volumes for Amazon EC2 instances. AWS Snowball Edge Storage Optimized is a device that provides a petabyte-scale data transport and edge computing solution.

NEW QUESTION 75

- (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 76
- (Topic 3)
Which AWS services or features give users the ability to create a network connection between two VPCs? (Select TWO.)

A. VPC endpoints
B. Amazon Route 53
C. VPC peering
D. AWS Direct Connect
E. AWS Transit Gateway

Answer: CE

Explanation:
 VPC peering and AWS Transit Gateway are two AWS services or features that give users the ability to create a network connection between two VPCs. VPC peering is a networking connection between two VPCs that enables you to route traffic between them privately. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region. Traffic between peered VPCs never traverses the public internet. VPC peering does not support transitive peering relationships, which means that if VPC A is peered with VPC B, and VPC B is peered with VPC C, then VPC A and VPC C are not automatically peered789. AWS Transit Gateway is a networking service that acts as a regional router for your VPCs and on- premises networks. You can attach up to 5,000 VPCs and VPN connections to a single transit gateway and route traffic between them. AWS Transit Gateway simplifies the management and scalability of your network architecture, as you only need to create and manage a single connection from the central transit gateway to each connected network. AWS Transit Gateway supports transitive routing, which means that any network that is attached to the transit gateway can communicate with any other network that is attached to the same transit gateway . References: 7: VPC peering - Amazon Virtual Private Cloud, 8: Connect VPCs using VPC peering - Amazon Virtual Private Cloud, 9: Amazon VPC-to-Amazon VPC connectivity options - Amazon Virtual Private Cloud, : [AWS Transit Gateway - Amazon Web Services], : [Connect VPCs using AWS Transit Gateway - Amazon Virtual Private Cloud], : [AWS Transit Gateway: Simplify Your Network Architecture]

NEW QUESTION 80
- (Topic 3)
Elasticity in the AWS Cloud refers to which of the following? (Select TWO.)

A. How quickly an Amazon EC2 instance can be restarted
B. The ability to rightsized resources as demand shifts
C. The maximum amount of RAM an Amazon EC2 instance can use
D. The pay-as-you-go billing model
E. How easily resources can be procured when they are needed

Answer: BE

Explanation:
Elasticity in the AWS Cloud refers to the ability to acquire resources as you need them and release resources when you no longer need them. In the cloud, you want to do this automatically1. This means that you can rightsized resources as demand shifts, and you can easily procure resources when they are needed. Elasticity is not related to how quickly an Amazon EC2 instance can be restarted, the maximum amount of RAM an Amazon EC2 instance can use, or the pay-as-you-go billing model. These are aspects of scalability, performance, and cost, respectively2.
For more information on elasticity, you can refer to the following sources:
? Elasticity - AWS Well-Architected Framework
? Elastic - Reactive Systems on AWS
? What is the difference between scalability and elasticity?

NEW QUESTION 81
- (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 84
- (Topic 3)
A company is running a monolithic on-premises application that does not scale and is difficult to maintain. The company has a plan to migrate the application to AWS and divide the application into microservices.
Which best practice of the AWS Well-Architected Framework is the company following with this plan?

A. Integrate functional testing as part of AWS deployment.
B. Use automation to deploy changes.
C. Deploy the application to multiple locations.
D. Implement loosely coupled dependencies.

Answer: D

Explanation:
 The company is following the best practice of implementing loosely coupled dependencies by migrating the application to AWS and dividing the application into microservices. Loosely coupled dependencies are a design principle of the AWS Well- Architected Framework that helps to reduce the interdependencies between components and improve the scalability, reliability, and performance of the system. By breaking down the monolithic application into smaller, independent, and modular services, the company can reduce the complexity and maintenance costs, increase the agility and flexibility, and enable faster and more frequent deployments. AWS CloudFormation is an AWS service that provides the ability to manage infrastructure as code. 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 users 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 users to monitor and control the changes to their infrastructure.
References: Implementing Loosely Coupled Dependencies, What is AWS CloudFormation?

NEW QUESTION 86
- (Topic 3)
A company wants to migrate its database to a managed AWS service that is compatible with PostgreSQL.
Which AWS services will meet these requirements? (Select TWO)

A. Amazon Athena
B. Amazon RDS
C. Amazon EC2
D. Amazon DynamoDB
E. Amazon Aurora

Answer: BE

Explanation:
 Amazon RDS and Amazon Aurora are both managed AWS services that support the PostgreSQL database engine. Amazon RDS makes it easier to set up, operate, and scale PostgreSQL deployments on the cloud, while Amazon Aurora is a cloud-native database engine that is compatible with PostgreSQL and offers higher performance and availability. Amazon Athena is a serverless query service that does not support PostgreSQL, but can analyze data in Amazon S3 using standard SQL. Amazon EC2 is a compute service that allows users to launch virtual machines, but does not provide any database management features. Amazon DynamoDB is a NoSQL database service that is not compatible with PostgreSQL, but offers fast and consistent performance at any scale. References: Hosted PostgreSQL - Amazon RDS for PostgreSQL - AWS, Amazon RDS for PostgreSQL - Amazon Relational Database Service, AWS PostgreSQL: Managed or Self-Managed? - NetApp, AWS Announces Amazon Aurora Supports PostgreSQL 12 - InfoQ, Amazon Aurora vs PostgreSQL | What are the differences? - StackShare

NEW QUESTION 91
- (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 connectors1.
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 data2.
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 Streams3.
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 availability4.
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 95
- (Topic 3)
Which AWS services can a company use to achieve a loosely coupled architecture? (Select TWO.)

A. Amazon Workspaces
B. Amazon Simple Queue Service (Amazon SQS)
C. Amazon Connect
D. AWS Trusted Advisor
E. AWS Step Functions

Answer: BE

Explanation:
 Amazon Simple Queue Service (Amazon SQS) and AWS Step Functions are AWS services that can be used to achieve a loosely coupled architecture. Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Using Step Functions, you can design and run workflows that stitch together services such as AWS Lambda and Amazon SNS into feature-rich applications. References: Amazon SQS, AWS Step Functions

NEW QUESTION 96
- (Topic 3)
A development team wants to deploy multiple test environments for an application in a fast repeatable manner.
Which AWS service should the team use?

A. Amazon EC2
B. AWS CloudFormation
C. Amazon QuickSight
D. Amazon Elastic Container Service (Amazon ECS)

Answer: B

Explanation:
 AWS CloudFormation is a service that allows you to model and provision your AWS resources using templates. You can define your infrastructure as code and automate the creation and update of your resources. AWS CloudFormation also supports nested stacks, change sets, and rollback features to help you manage complex and dynamic environments34. References:
? AWS CloudFormation
? AWS Certified Cloud Practitioner Exam Guide

NEW QUESTION 99
- (Topic 3)
What is a customer responsibility when using AWS Lambda according to the AWS shared responsibility model?

A. Managing the code within the Lambda function
B. Confirming that the hardware is working in the data center
C. Patching the operating system
D. Shutting down Lambda functions when they are no longer in use

Answer: A

Explanation:
 According to the AWS shared responsibility model, AWS is responsible for
the security of the cloud, while customers are responsible for the security in the cloud. This means that AWS is responsible for the physical servers, networking, and operating system that run Lambda functions, while customers are responsible for the security of their code and AWS IAM to the Lambda service and within their function1. Customers need to manage the code within the Lambda function, such as writing, testing, debugging, deploying, and updating the code, as well as ensuring that the code does not contain any vulnerabilities or malicious code that could compromise the security or performance of the
function23. References: 2: AWS Lambda - Amazon Web Services (AWS), 3: AWS Lambda Documentation, 1: Amazon CLF-C02: What is customer responsibility under AWS … - PUPUWEB

NEW QUESTION 100
- (Topic 3)
A company wants to design a reliable web application that is hosted on Amazon EC2. Which approach will achieve this goal?

A. Launch large EC2 instances in the same Availability Zone.
B. Spread EC2 instances across more than one security group.
C. Spread EC2 instances across more than one Availability Zone.
D. Use an Amazon Machine Image (AMI) from AWS Marketplace.

Answer: C

Explanation:
 The approach that will achieve the goal of designing a reliable web application that is hosted on Amazon EC2 is to spread EC2 instances across more than one Availability Zone. An Availability Zone is a physically isolated location within an AWS Region that has its own power, cooling, and network connectivity. By spreading EC2 instances across multiple Availability Zones, users can increase the fault tolerance and availability of their web applications, as well as reduce latency for end users2. Launching large EC2 instances in the same Availability Zone, spreading EC2 instances across more than one security group, or using an Amazon Machine Image (AMI) from AWS Marketplace are not sufficient to ensure reliability, as they do not provide redundancy or resilience in case of an outage in one Availability Zone.

NEW QUESTION 103

- (Topic 3)
A company has teams that have different job roles and responsibilities. The company's employees often change teams. The company needs to manage permissions for the employees so that the permissions are appropriate for the job responsibilities.
Which IAM resource should the company use to meet this requirement with the LEAST operational overhead?

A. IAM user groups
B. IAM roles
C. IAM instance profiles
D. IAM policies for individual users

Answer: B

Explanation:
IAM roles are a way of granting temporary permissions to entities that need to access AWS resources, such as users, applications, or services. IAM roles allow customers to assign permissions to entities without having to create or manage IAM users or credentials for them. IAM roles can be assumed by different entities depending on the trust policy attached to the role. For example, IAM roles can be assumed by IAM users in the same or different AWS accounts, AWS services such as EC2 or Lambda, or external identities such as federated users or web identities. IAM roles can also be switched by IAM users to temporarily change their permissions. IAM roles are recommended for managing permissions for employees who often change teams, because they allow customers to define permissions based on job roles and responsibilities, and easily assign or revoke them as needed. IAM roles also reduce the operational overhead of creating, updating, or deleting IAM users or credentials for each employee or team change.

NEW QUESTION 106
- (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 segmentation1. 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 rules1.
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 109
- (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 Plan4567. 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 110
- (Topic 3)
A company needs an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities.
Which AWS service will meet these requirements?

A. Amazon GuardDuty

B. Amazon Inspector
C. AWS Security Hub
D. AWS Shield

Answer: B

Explanation:
The correct answer is B. Amazon Inspector.
Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. Amazon Inspector automatically discovers workloads, such as Amazon EC2 instances, containers, and Lambda functions, and scans them for software vulnerabilities and unintended network exposure12.
Amazon GuardDuty is a threat detection service that monitors your AWS accounts and workloads for malicious or unauthorized activity. Amazon GuardDuty does not scan for software vulnerabilities, but rather analyzes AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs to detect threats such as compromised credentials, backdoors, or crypto mining3.
AWS Security Hub is a security and compliance service that aggregates and prioritizes security findings from multiple AWS services and partner solutions. AWS Security Hub does not scan for software vulnerabilities, but rather provides a comprehensive view of your security posture across your AWS accounts4.
AWS Shield is a managed service that protects your web applications and network resources from distributed denial-of-service (DDoS) attacks. AWS Shield does not scan for software vulnerabilities, but rather provides detection and mitigation of DDoS attacks at the network and application layers5.
References:
1: Automated Software Vulnerability Management - Amazon Inspector - AWS 3: [Amazon GuardDuty – Intelligent Threat Detection Made Easy] 2: AWS Re-Launches Amazon Inspector with New Architecture and Features - InfoQ 4: [AWS Security Hub – Unified Security and Compliance Center] 5: [AWS Shield – Managed DDoS Protection]

NEW QUESTION 113
- (Topic 3)
A company needs to implement identity management for a fleet of mobile apps that are running in the AWS Cloud.
Which AWS service will meet this requirement?

A. Amazon Cognito
B. AWS Security Hub
C. AWS Shield
D. AWS WAF

Answer: A

Explanation:
Amazon Cognito is a service that provides identity management for mobile and web applications, allowing users to sign up, sign in, and access AWS resources with different identity providers. AWS Security Hub is a service that provides a comprehensive view of the security posture of AWS accounts and resources. AWS Shield is a service that provides protection against distributed denial of service (DDoS) attacks. AWS WAF is a web application firewall that helps protect web applications from common web exploits.

NEW QUESTION 117
- (Topic 3)
A company runs a MySQL database in its on-premises data center. The company wants to run a copy of this database in the AWS Cloud.
Which AWS service would support this workload?

A. Amazon RDS
B. Amazon Neptune
C. Amazon ElastiCache for Redis
D. Amazon Quantum Ledger Database (Amazon QLDB)

Answer: A

Explanation:
Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier 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. Amazon RDS supports six popular database engines: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. Amazon RDS can support running a copy of a MySQL database in the AWS Cloud, as it offers compatibility, scalability, and availability features.

NEW QUESTION 119
- (Topic 3)
A company wants to query its server logs to gain insights about its customers' experiences. Which AWS service will store this data MOST cost-effectively?

A. Amazon Aurora
B. Amazon Elastic File System (Amazon EFS)
C. Amazon Elastic Block Store (Amazon EBS)
D. Amazon S3

Answer: D

Explanation:
Amazon S3 is an AWS service that provides scalable, durable, and cost-effective object storage in the cloud. Amazon S3 can store any amount and type of data, such as server logs, and offers various storage classes with different performance and pricing characteristics. Amazon S3 is the most cost-effective option for storing server logs, as it offers low-cost storage classes, such as S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Intelligent-Tiering, that are suitable for infrequently accessed or changing access patterns data. Amazon S3 also integrates with other AWS services, such as Amazon Athena and Amazon OpenSearch Service, that can query the server logs directly from S3 without requiring any additional data loading or transformation. References: Amazon S3, Amazon S3 Storage Classes, Querying Data in Amazon S3

NEW QUESTION 124

- (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 129
- (Topic 3)
A company is moving to the AWS Cloud to reduce operational overhead for its application infrastructure.
Which IT operation will the company still be responsible for after the migration to AWS?

A. Security patching of AWS Elastic Beanstalk
B. Backups of data that is stored in Amazon Aurora
C. Termination of Amazon EC2 instances that are managed by AWS Auto Scaling
D. Configuration of IAM access controls

Answer: D

Explanation:
 AWS Elastic Beanstalk, Amazon Aurora, and AWS Auto Scaling are managed services that reduce the operational overhead for the customers. AWS is responsible for security patching, backups, and termination of these services. However, the customers are still responsible for configuring IAM access controls to manage the permissions and policies for their AWS resources. This is part of the AWS shared responsibility model, which defines the security and compliance responsibilities of AWS and the customers. You can learn more about the AWS shared responsibility model from this whitepaper or this digital course.

NEW QUESTION 134
- (Topic 3)
Which cloud concept is demonstrated by using AWS Compute Optimizer?

A. Security validation
B. Rightsizing
C. Elasticity
D. Global reach

Answer: B

Explanation:
 Rightsizing is the cloud concept that is demonstrated by using AWS Compute Optimizer. Rightsizing is the process of adjusting the type and size of your cloud resources to match the optimal performance and cost for your workloads. AWS Compute Optimizer is a service that analyzes the configuration and utilization metrics of your AWS resources, such as Amazon EC2 instances, Amazon EBS volumes, AWS Lambda functions, and Amazon ECS services on AWS Fargate. It reports whether your resources are optimal, and generates optimization recommendations to reduce the cost and improve the performance of your workloads. AWS Compute Optimizer uses machine learning to analyze your historical utilization data and compare it with the most cost-effective AWS alternatives. You can use the recommendations to evaluate the trade-offs between cost and performance, and decide when to move or resize your resources to achieve the best results. References: Workload Rightsizing - AWS Compute Optimizer - AWS, What is AWS Compute Optimizer? - AWS Compute Optimizer

NEW QUESTION 139
- (Topic 3)
A company hosts a large amount of data in AWS. The company wants to identify if any of the data should be considered sensitive.
Which AWS service will meet the requirement?

A. Amazon Inspector
B. Amazon Macie
C. AWS Identity and Access Management (IAM)
D. Amazon CloudWatch

Answer: B

Explanation:
 Amazon Macie is a fully managed service that uses machine learning and pattern matching to help you detect, classify, and better protect your sensitive data stored in the AWS Cloud1. Macie can automatically discover and scan your Amazon S3 buckets for sensitive data such as personally identifiable information (PII), financial information, healthcare information, intellectual property, and credentials1. Macie also provides you with a dashboard that shows the type, location, and volume of sensitive data in your AWS environment, as well as alerts and findings on potential security issues1.
The other options are not suitable for identifying sensitive data in AWS. Amazon Inspector is a service that helps you find security vulnerabilities and deviations from best practices in your Amazon EC2 instances2. AWS Identity and Access Management (IAM) is a service that helps you manage access to your AWS resources by creating users, groups, roles, and policies3. Amazon CloudWatch is a service that helps you monitor and troubleshoot your AWS resources and applications by collecting metrics, logs, events, and alarms4. References:
? 1: What Is Amazon Macie? - Amazon Macie
? 2: What Is Amazon Inspector? - Amazon Inspector
? 3: What Is IAM? - AWS Identity and Access Management

? 4: What Is Amazon CloudWatch? - Amazon CloudWatch

NEW QUESTION 140
- (Topic 3)
Which task must a user perform by using the AWS account root user credentials?

A. Make changes to AWS production resources.
B. Change AWS Support plans.
C. Access AWS Cost and Usage Reports.
D. Grant auditors' access to an AWS account for a compliance audit.

Answer: B

Explanation:
Changing AWS Support plans is a task that must be performed by using the AWS account root user credentials. The root user is the email address that you used to sign up for AWS. It has complete access to all AWS services and resources in the account. You should use the root user only to perform a few account and service management tasks, such as changing AWS Support plans, closing the account, or changing the account name or email address. Making changes to AWS production resources, accessing AWS Cost and Usage Reports, and granting auditors access to an AWS account for a compliance audit are tasks that can be performed by using IAM users or roles, which are entities that you create in AWS to delegate permissions to access AWS services and resources.

NEW QUESTION 145
- (Topic 3)
A company wants to verify if multi-factor authentication (MFA) is enabled for all users within its AWS accounts.
Which AWS service or resource will meet this requirement?

A. AWS Cost and Usage Report
B. IAM credential reports
C. AWS Artifact
D. Amazon CloudFront reports

Answer: B

Explanation:
The AWS service or resource that will meet the requirement of verifying if multi-factor authentication (MFA) is enabled for all users within its AWS accounts is IAM credential reports. IAM credential reports are downloadable reports that list all the users in an AWS account and the status of their various credentials, including passwords, access keys, and MFA devices. Users can use IAM credential reports to audit the security status of their AWS accounts and identify any issues or risks4. AWS Cost and Usage Report, AWS Artifact, and Amazon CloudFront reports are other AWS services or resources that provide different types of information, such as billing, compliance, and content delivery, but they do not show the MFA status of the users.

NEW QUESTION 146
- (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 improvements12.
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 features3. 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 adoption4. 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 monitoring5. AMS does not provide a framework for customers to operate their own workloads on AWS.

NEW QUESTION 147
- (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 AWS1.
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 credentials2.
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 credentials3.
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 credentials4.
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 152
- (Topic 3)
Which AWS Cloud Adoption Framework (AWS CAF) capability belongs to the people perspective?

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

Answer: C

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

NEW QUESTION 155
- (Topic 3)
A company must be able to develop, test, and launch an application in the AWS Cloud quickly.
Which advantage of cloud computing will meet these requirements?

A. Stop guessing capacity
B. Trade fixed expense for variable expense
C. Achieve economies of scale
D. Increase speed and agility

Answer: D

Explanation:
One of the benefits of cloud computing is that it enables customers to increase speed and agility in developing, testing, and launching applications. Cloud computing provides on-demand access to a variety of IT resources, such as compute, storage, networking, databases, and analytics, without requiring upfront investments or long-term commitments. Customers can provision and release resources in minutes, scale up and down as needed, and experiment with new technologies and features. This allows customers to accelerate their innovation cycles, deliver faster time-to-market, and respond to changing customer needs and demands

NEW QUESTION 157
- (Topic 3)
A company is running an Amazon EC2 instance in a VPC.
An ecommerce company is using Amazon EC2 Auto Scaling groups to manage a fleet of web servers running on Amazon EC2.
This architecture follows which AWS Well-Architected Framework best practice?

A. Secure the workload
B. Decouple infrastructure components
C. Design for failure
D. Think parallel

Answer: C

Explanation:
Design for failure is one of the best practices of the AWS Well-Architected Framework. It means that the architecture should be resilient and fault-tolerant, and able to handle failures without impacting the availability and performance of the applications. By using Amazon EC2 Auto Scaling groups, the ecommerce company can design for failure by automatically scaling the number of EC2 instances up or down based on demand or health status. Amazon EC2 Auto Scaling groups can also distribute the EC2 instances across multiple Availability Zones, which are isolated locations within an AWS Region that have independent power, cooling, and network connectivity. This way, the company can ensure that their web servers can handle traffic spikes, recover from failures, and provide a consistent user experience

NEW QUESTION 159
- (Topic 3)

Which of the following are general AWS Cloud design principles described in the AWS Well-Architected Framework?

A. Consolidate key components into monolithic architectures.
B. Test systems at production scale.
C. Provision more capacity than a workload is expected to need.
D. Drive architecture design based on data collected about the workload behavior and requirements.
E. Make AWS Cloud architectural decisions static, one-time events.

Answer: BD

Explanation:
These are two of the general AWS Cloud design principles described in the AWS Well-Architected Framework. Testing systems at production scale means using tools such as AWS CloudFormation, AWS CodeDeploy, and AWS X-Ray to simulate real-world scenarios and measure the performance, scalability, and availability of the system. Driving architecture design based on data means using tools such as Amazon CloudWatch, AWS CloudTrail, and AWS Config to collect and analyze metrics, logs, and events about the system and use the insights to optimize the system's design and operation. You can learn more about the AWS Well-Architected Framework from this whitepaper or [this digital course].

NEW QUESTION 164
- (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 169
- (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 stakeholders12.
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 risks12.
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 application12.
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 performance12. References:
1: AWS Cloud Adoption Framework: Governance Perspective 2: All you need to know about AWS Cloud Adoption Framework — Governance Perspective

NEW QUESTION 174
- (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 it345. 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 176
- (Topic 3)
A company wants to migrate to AWS and use the same security software it uses on premises. The security software vendor offers its security software as a service on AWS.
Where can the company purchase the security solution?

A. AWS Partner Solutions Finder
B. AWS Support Center
C. AWS Management Console
D. AWS Marketplace

Answer: D

Explanation:
AWS Marketplace is an online store that helps customers find, buy, and immediately start using the software and services that run on AWS. Customers can choose from a wide range of software products in popular categories such as security, networking, storage, machine learning, business intelligence, database, and DevOps. Customers can also use AWS Marketplace to purchase software as a service (SaaS) solutions that are integrated with AWS. Customers can benefit from simplified procurement, billing, and deployment processes, as well as flexible pricing options and free trials. Customers can also leverage AWS Marketplace to discover and subscribe to solutions offered by AWS Partners, such as the security software vendor mentioned in the question. References: AWS Marketplace, [AWS Marketplace: Software as a Service (SaaS)], [AWS Cloud Practitioner Essentials: Module 6 - AWS Pricing, Billing, and Support]

NEW QUESTION 181
- (Topic 3)
At what support level do users receive access to a support concierge?

A. Basic Support
B. Developer Support
C. Business Support
D. Enterprise Support

Answer: D

Explanation:
Users receive access to a support concierge at the Enterprise Support level. A support concierge is a team of AWS billing and account experts that specialize in working with enterprise accounts. They can help users with billing and account inquiries, cost optimization, FinOps support, cost analysis, and prioritized answers to billing questions. The support concierge is included as part of the Enterprise Support plan, which also provides access to a Technical Account Manager (TAM), Infrastructure Event Management, AWS Trusted Advisor, and 24/7 technical support. References: AWS Support Plan Comparison, AWS Enterprise Support Plan, AWS Support Concierge

NEW QUESTION 185
- (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 company3

NEW QUESTION 190
- (Topic 3)
A company is launching a mobile app. The company wants customers to be able to use the app without upgrading their mobile devices.
Which pillar of the AWS Well-Architected Framework does this goal represent?

A. Security
B. Reliability
C. Cost optimization
D. Sustainability

Answer: C

Explanation:
Cost optimization is one of the five pillars of the AWS Well-Architected Framework. It focuses on avoiding unnecessary costs, understanding and controlling where money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.

NEW QUESTION 195
- (Topic 3)
A user needs a relational database but does not have the resources to manage the hardware, resiliency, and replication.
Which AWS service option meets the user's requirements'?

A. Run MySQL on Amazon Elastic Container Service (Amazon ECS)
B. Run MySQL on Amazon EC2
C. Choose Amazon RDS for MySQL
D. Choose Amazon ElastiCache for Redis

Answer: C

Explanation:
Amazon RDS for MySQL is a fully managed, open-source cloud database service that allows you to easily operate and scale your relational database of choice, including MySQL. With Amazon RDS for MySQL, you don't have to worry about the hardware, resiliency, and replication of your database, as Amazon RDS handles these tasks for you. Amazon RDS for MySQL also provides features such as automated backups, multi-AZ deployments, read replicas, encryption, monitoring, and more. Amazon RDS for MySQL is compatible with the MySQL Community Edition versions 5.7 and 8.0, which means that you can use the same code, applications, and tools that you already use with MySQL4567. References: 4: Hosted MySQL - Amazon RDS for MySQL - AWS, 5: Amazon RDS for MySQL - Amazon Relational Database Service, 6: Amazon RDS for MySQL —, 7: Managed SQL Database - Amazon Relational Database Service (RDS) - AWS

NEW QUESTION 199
- (Topic 3)
Which of the following actions are controlled with AWS Identity and Access Management (IAM)? (Select TWO.)

A. Control access to AWS service APIs and to other specific resources.
B. Provide intelligent threat detection and continuous monitoring.
C. Protect the AWS environment using multi-factor authentication (MFA).
D. Grant users access to AWS data centers.
E. Provide firewall protection for applications from common web attacks.

Answer: AC

Explanation:
AWS Identity and Access Management (IAM) is a service that enables you to manage access to AWS services and resources securely. You can use IAM to perform the following actions:
? Control access to AWS service APIs and to other specific resources: You can create users, groups, roles, and policies that define who can access which AWS resources and how. You can also use IAM to grant temporary access to users or applications that need to perform certain tasks on your behalf3
? Protect the AWS environment using multi-factor authentication (MFA): You can enable MFA for your IAM users and root user to add an extra layer of security to your AWS account. MFA requires users to provide a unique authentication code from an approved device or SMS text message, in addition to their user name and password, when they sign in to AWS4

NEW QUESTION 200
- (Topic 3)
A company wants to migrate its on-premises relational databases to the AWS Cloud. The company wants to use infrastructure as close to its current geographical location as possible.
Which AWS service or resource should the company use to select its Amazon RDS deployment area?

A. Amazon Connect
B. AWS Wavelength
C. AWS Regions
D. AWS Direct Connect

Answer: C

Explanation:
AWS Regions are the AWS service or resource that the company should use to select its Amazon RDS deployment area. AWS Regions are separate geographic areas where AWS clusters its data centers. Each AWS Region consists of multiple, isolated, and physically separate Availability Zones within a geographic area. Each AWS Region is designed to be isolated from the other AWS Regions to achieve the highest possible fault tolerance and stability. AWS provides a more extensive global footprint than any other cloud provider, and to support its global footprint and ensure customers are served across the world, AWS opens new Regions rapidly. AWS maintains multiple geographic Regions, including Regions in North America, South America, Europe, China, Asia Pacific, South Africa, and the Middle East. Amazon RDS is available in several AWS Regions worldwide. To create or work with an Amazon RDS DB instance in a specific AWS Region, you must use the corresponding regional service endpoint. You can choose the AWS Region that meets your latency or legal requirements. You can also use multiple AWS Regions to design a disaster recovery solution or to distribute your read workload. References: Global Infrastructure Regions & AZs - aws.amazon.com, Regions, Availability Zones, and Local Zones - Amazon Relational Database Service

NEW QUESTION 201
- (Topic 3)
A company is using Amazon DynamoDB for its application database.
Which tasks are the responsibility of AWS, according to the AWS shared responsibility model? (Select TWO.)

A. Classify data.
B. Configure access permissions.
C. Manage encryption options.
D. Provide public endpoints to store and retrieve data.
E. Manage the infrastructure layer and the operating system.

Answer: DE

Explanation:
According to the AWS shared responsibility model, AWS is responsible for security of the cloud, while customers are responsible for security in the cloud. This

means that AWS is responsible for protecting the infrastructure that runs AWS services, such as hardware, software, networking, and facilities. Customers are responsible for managing their data, classifying their assets, and using IAM tools to apply the appropriate permissions. For abstracted services, such as Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and provides customers with public endpoints to store and retrieve data. Customers are responsible for classifying their data, managing their encryption options, and configuring their access permissions. References: Shared Responsibility Model, Security and compliance in Amazon DynamoDB, [AWS Cloud Practitioner Essentials: Module 2 - Security in the Cloud]

NEW QUESTION 206
- (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 209
- (Topic 3)
Which of the following is a pillar of the AWS Well-Architected Framework?

A. Redundancy
B. Operational excellence
C. Availability
D. Multi-Region

Answer: B

Explanation:
 The AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimization — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that can scale over time. Operational excellence is one of the pillars of the Framework, and it focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures.

NEW QUESTION 210
- (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 214
- (Topic 3)

Which AWS services are supported by Savings Plans? (Select TWO.)

A. Amazon EC2
B. Amazon RDS
C. Amazon SageMaker
D. Amazon Redshift
E. Amazon DynamoDB

Answer: AC

Explanation:
The AWS services that are supported by Savings Plans are:
? Amazon EC2: Amazon EC2 is a service that provides scalable computing capacity in the AWS cloud. You can use Amazon EC2 to launch virtual servers, configure security and networking, and manage storage. Amazon EC2 is eligible for both Compute Savings Plans and EC2 Instance Savings Plans12.
? Amazon SageMaker: Amazon SageMaker is a service that helps you build and deploy machine learning models. You can use Amazon SageMaker to access Jupyter notebooks, use common machine learning algorithms, train and tune models, and deploy them to a hosted environment. Amazon SageMaker is eligible for SageMaker Savings Plans13.
The other options are not supported by Savings Plans. Amazon RDS, Amazon Redshift, and Amazon DynamoDB are database services that are eligible for Reserved Instances, but not Savings Plans4.

NEW QUESTION 218
- (Topic 3)
Which AWS service or feature is an example of a relational database management system?

A. Amazon Athena
B. Amazon Redshift
C. Amazon S3 Select
D. Amazon Kinesis Data Streams

Answer: B

Explanation:
Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers. Amazon Redshift is a relational database management system (RDBMS), so it is compatible with other RDBMS applications. You can use standard SQL to query the data.

NEW QUESTION 221
- (Topic 3)
Which options are AWS Cloud Adoption Framework (AWS CAF) security perspective capabilities? (Select TWO.)

A. Observability
B. Incident and problem management
C. Incident response
D. Infrastructure protection
E. Availability and continuity

Answer: CD

Explanation:
The AWS Cloud Adoption Framework (AWS CAF) security perspective helps users achieve the confidentiality, integrity, and availability of their data and cloud workloads. It comprises nine capabilities that are grouped into three categories: preventive, detective, and responsive. Incident response and infrastructure protection are two of the capabilities in the responsive and preventive categories, respectively. Incident response helps users prepare for and respond to security incidents in a timely and effective manner, using tools and processes that leverage AWS features and services. Infrastructure protection helps users implement security controls and mechanisms to protect their cloud resources, such as network, compute, storage, and database, from unauthorized access or malicious attacks. References: Security perspective: compliance and assurance, AWS Cloud Adoption Framework

NEW QUESTION 223
- (Topic 3)
Which AWS service or feature offers security for a VPC by acting as a firewall to control traffic in and out of subnets?

A. AWS Security Hub
B. Security groups
C. Network ACL
D. AWSWAF

Answer: C

Explanation:
A network access control list (network ACL) is a feature that acts as a firewall for controlling traffic in and out of one or more subnets in a virtual private cloud (VPC). Network ACLs can be configured with rules that allow or deny traffic based on the source and destination IP addresses, ports, and protocols1. AWS Security Hub is a service that provides a comprehensive view of the security posture of AWS accounts and resources2. Security groups are features that act as firewalls for controlling traffic at the instance level3. AWS WAF is a web application firewall that helps protect web applications from common web exploits4.

NEW QUESTION 225
- (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 more1. 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 S32. 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 S33.
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 S34.
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 228
- (Topic 3)
A company is building an application in the AWS Cloud. The company wants to use temporary credentials for the application to access other AWS resources. Which AWS service will meet these requirements?

A. AWS Key Management Service (Aws KMS)
B. AWS CloudHSM
C. Amazon Cognito
D. AWS Security Token Service (Aws STS)

Answer: D

Explanation:
AWS Security Token Service (AWS STS) is a service that provides temporary security credentials to users or applications that need to access AWS resources. The temporary credentials have a limited lifetime and can be configured to last from a few minutes to several hours. The credentials are not stored with the user or application, but are generated dynamically and provided on request. The credentials work almost identically to long-term access key credentials, but have the advantage of not requiring distribution, rotation, or revocation1.
AWS Key Management Service (AWS KMS) is a service that provides encryption and decryption services for data and keys. It does not provide temporary security credentials2. AWS CloudHSM is a service that provides hardware security modules (HSMs) for cryptographic operations and key management. It does not provide temporary security credentials3.
Amazon Cognito is a service that provides user authentication and authorization for web and mobile applications. It can also provide temporary security credentials for authenticated users, but not for applications4.

NEW QUESTION 232
- (Topic 3)
According to the AWS shared responsibility model, who is responsible for the virtualization layer down to the physical security of the facilities in which AWS services operate?

A. It is the sole responsibility of the customer.
B. It is the sole responsibility of AWS.
C. It is a shared responsibility between AWS and the customer.
D. The customer's AWS Support plan tier determines who manages the configuration.

Answer: B

Explanation:
According to the AWS shared responsibility model, AWS is responsible for the security of the cloud, which includes the virtualization layer down to the physical security of the facilities in which AWS services operate1. The customer is responsible for the security in the cloud, which includes the configuration and management of the AWS resources and applications that they use1.

NEW QUESTION 236
- (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 241
- (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 reliability5

NEW QUESTION 243
- (Topic 3)
A company website is experiencing DDoS attacks.
Which AWS service can help protect the company website against these attacks?

A. AWS Resource Access Manager
B. AWS Amplify
C. AWS Shield
D. Amazon GuardDuty

Answer: C

Explanation:
AWS Shield is a managed DDoS protection service that safeguards applications running on AWS from distributed denial of service (DDoS) attacks. DDoS attacks are malicious attempts to disrupt the normal functioning of a website or application by overwhelming it with a large volume of traffic from multiple sources. AWS Shield provides two tiers of protection: Standard and Advanced. AWS Shield Standard is automatically enabled for all AWS customers at no additional cost. It protects your AWS resources, such as Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53, from the most common and frequently occurring network and transport layer DDoS attacks. AWS Shield Advanced is an optional paid service that provides additional protection for your AWS resources and applications, such as Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), and AWS Elastic Beanstalk. AWS Shield Advanced offers enhanced detection and mitigation capabilities, 24/7 access to the AWS DDoS Response Team (DRT), real-time visibility and reporting, and cost protection against DDoS-related spikes in your AWS bill12
References: AWS Shield, What is a DDOS Attack & How to Protect Your Site Against One

NEW QUESTION 244
- (Topic 3)
AWS has the ability to achieve lower pay-as-you-go pricing by aggregating usage across hundreds of thousands of users.
This describes which advantage of the AWS Cloud?

A. Launch globally in minutes
B. Increase speed and agility
C. High economies of scale
D. No guessing about compute capacity

Answer: C

Explanation:
 AWS has the ability to achieve lower pay-as-you-go pricing by aggregating usage across hundreds of thousands of users. This means that AWS can leverage its massive scale and purchasing power to reduce the costs of infrastructure, hardware, software, and operations. These savings are then passed on to the customers, who only pay for the resources they use. You can learn more about the AWS pricing model from [this webpage] or [this digital course].

NEW QUESTION 246
- (Topic 3)
Which AWS service could an administrator use to provide desktop environments for several employees?

A. AWS Organizations
B. AWS Fargate
C. AWS WAF
D. AWS Workspaces

Answer: D

Explanation:
 AWS Workspaces is a service that provides fully managed, secure, and reliable virtual desktops for your employees. You can access your personal Windows environment on various devices, such as Android, iOS, Fire, Mac, PC, Chromebook, and Linux. You can choose from different bundles of CPU, memory, storage, and software options to suit your needs. You can also integrate AWS Workspaces with your existing Active Directory, VPN, and security policies. AWS Workspaces helps you reduce the cost and complexity of managing your desktop infrastructure, while enhancing the productivity and security of your remote workers456. References: 4: Amazon WorkSpaces Client Download, 5: VDI Desktops - Amazon WorkSpaces Family - AWS, 6: Amazon WorkSpaces

NEW QUESTION 248
- (Topic 3)
A company wants to define a central data protection policy that works across AWS services for compute, storage, and database resources.
Which AWS service will meet this requirement?

A. AWS Batch
B. AWS Elastic Disaster Recovery
C. AWS Backup
D. Amazon FSx

Answer: C

Explanation:
 The AWS service that will meet this requirement is C. AWS Backup.
AWS Backup is a service that allows you to define a central data protection policy that works across AWS services for compute, storage, and database resources. You can use AWS Backup to create backup plans that specify the frequency, retention, and lifecycle of your backups, and apply them to your AWS resources using tags or resource IDs. AWS Backup supports various AWS services, such as Amazon EC2, Amazon EBS, Amazon RDS, Amazon DynamoDB, Amazon EFS, Amazon FSx, and AWS Storage Gateway12. AWS Batch is a service that allows you to run batch computing workloads on AWS. AWS Batch does not provide a central data protection policy, but rather enables you to optimize the allocation and utilization of your compute resources3.
AWS Elastic Disaster Recovery is a service that allows you to prepare for and recover from disasters using AWS. AWS Elastic Disaster Recovery does not provide a central data protection policy, but rather helps you minimize downtime and data loss by replicating your applications and data to AWS4.
Amazon FSx is a service that provides fully managed file storage for Windows and Linux applications. Amazon FSx does not provide a central data protection policy, but rather offers features such as encryption, snapshots, backups, and replication to protect your file systems5.
References:
1: AWS Backup – Centralized backup across AWS services 3: AWS Batch – Run Batch Computing Jobs on AWS 2: Data Protection Reference Architectures with AWS Backup 4: AWS Elastic Disaster Recovery – Prepare for and recover from disasters using AWS 5: Amazon FSx – Fully managed file storage for Windows and Linux applications

NEW QUESTION 250
- (Topic 3)
A company is planning to migrate to the AWS Cloud. The company is conducting organizational transformation and wants to become more responsive to customer inquiries and feedback.
Which tasks should the company perform to meet these requirements, according to the AWS Cloud Adoption Framework (AWS CAF)? (Select TWO.)

A. Realign teams to focus on products and value streams.
B. Create new value propositions with new products and services.
C. Use agile methods to rapidly iterate and evolve.
D. Use a new data and analytics platform to create actionable insights.
E. Migrate and modernize legacy infrastructure.

Answer: AC

Explanation:
 Realigning teams to focus on products and value streams, and using agile methods to rapidly iterate and evolve are tasks that the company should perform to meet the requirements of becoming more responsive to customer inquiries and feedback, according to the AWS Cloud Adoption Framework (AWS CAF). AWS CAF organizes guidance into six areas of focus, called perspectives: business, people, governance, platform, security, and operations. Each perspective is divided into capabilities, which describe the skills and processes to execute the transition effectively. The people perspective helps you prepare your organization for cloud adoption, and includes capabilities such as organizational change management, staff skills and readiness, and organizational alignment. The business perspective helps you align IT strategy with business strategy, and includes capabilities such as business case development, value proposition, and product ownership. Creating new value propositions with new products and services is a task that belongs to the business perspective, but it is not directly related to the requirement of becoming more responsive to customer inquiries and feedback. Using a new data and analytics platform to create actionable insights is a task that belongs to the platform perspective, which helps you design, implement, and optimize the architecture of the AWS environment. However, it is also not directly related to the requirement of becoming more responsive to customer inquiries and feedback. Migrating and modernizing legacy infrastructure is a task that belongs to the operations perspective, which helps you enable, run, use, operate, and recover IT workloads to the level agreed upon with your business stakeholders. However, it is also not directly related to the requirement of becoming more responsive to customer inquiries and feedback.

NEW QUESTION 251
- (Topic 3)
Which AWS service or feature can the company use to limit the access to AWS services for member accounts?

A. AWS Identity and Access Management (IAM)
B. Service control policies (SCPs)
C. Organizational units (OUs)
D. Access control lists (ACLs)

Answer: B

Explanation:
 Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines2. SCPs are available only in an organization that has all features enabled2.

NEW QUESTION 253
- (Topic 3)
Which service enables customers to audit API calls in their AWS accounts'?

A. AWS CloudTrail
B. AWS Trusted Advisor
C. Amazon Inspector

D. AWS X-Ray

Answer: A

Explanation:
 AWS CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service in your AWS account. CloudTrail captures all API calls for AWS services as events, including calls from the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services. You can use CloudTrail to monitor, audit, and troubleshoot your AWS account activity34. AWS Trusted Advisor is a service that provides best practices recommendations for cost optimization, performance, security, and fault tolerance in your AWS account5. 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 practices6. AWS X-Ray is a service that helps you analyze and debug your applications by collecting data about the requests that your application serves, and providing tools to view, filter, and gain insights into that data7. References: Logging AWS Audit Manager API calls with CloudTrail, Logging AWS Account Management API calls using AWS CloudTrail, Review API calls in your AWS account using CloudTrail, Monitor the usage of AWS API calls using Amazon CloudWatch, Which service enables customers to audit API calls in their AWS …

NEW QUESTION 257
- (Topic 3)
Which actions are best practices for an AWS account root user? (Select TWO.)

A. Share root user credentials with team members.
B. Create multiple root users for the account, separated by environment.
C. Enable multi-factor authentication (MFA) on the root user.
D. Create an IAM user with administrator privileges for daily administrative tasks, instead of using the root user.
E. Use programmatic access instead of the root user and password.

Answer: CD

Explanation:
 The AWS account root user is the identity that has complete access to all AWS services and resources in the account. It is accessed by signing in with the email address and password that were used to create the account1. The root user should be protected and used only for a few account and service management tasks that require it1. Therefore, the following actions are best practices for an AWS account root user:
? Enable multi-factor authentication (MFA) on the root user. MFA is a security feature that requires users to provide two or more pieces of information to authenticate themselves, such as a password and a code from a device. MFA adds an extra layer of protection for the root user credentials, which can access sensitive information and perform critical operations in the account2.
? Create an IAM user with administrator privileges for daily administrative tasks, instead of using the root user. IAM is a service that helps customers manage access to AWS resources for users and groups. Customers can create IAM users and assign them permissions to perform specific tasks on specific resources. Customers can also create IAM roles and policies to delegate access to other AWS services or external entities3. By creating an IAM user with administrator privileges, customers can avoid using the root user for everyday tasks and reduce the risk of accidental or malicious changes to the account1.

NEW QUESTION 262
- (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 access1.
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 costs23.
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 experience45. 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 267
- (Topic 3)
Which AWS service requires the customer to be fully responsible for applying operating system patches?

A. Amazon DynamoDB
B. AWS Lambda
C. AWS Fargate
D. Amazon EC2

Answer: D

Explanation:
Amazon EC2 is the AWS service that requires the customer to be fully responsible for applying operating system patches. Amazon EC2 is a service that provides secure, resizable compute capacity in the cloud. Customers can launch virtual servers called instances and choose from various configurations of CPU, memory, storage, and networking resources1. Customers have full control and access to their instances, which means they are also responsible for managing and

maintaining them, including applying
operating system patches2. Customers can use AWS Systems Manager Patch Manager, a feature of AWS Systems Manager, to automate the process of patching their EC2 instances with both security-related updates and other types of updates3.

NEW QUESTION 272
......

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