Question 1:

Skipped

Which of the following should you use if you need to provide temporary AWS credentials for users who have been authenticated via their social media logins as well as for guest users who do not require any authentication?

- **AWS IAM Identity Center**
- **Amazon Cognito Identity Pool**

  (Correct)

- **AWS AppSync**
- **Amazon Cognito User Pool**

Explanation

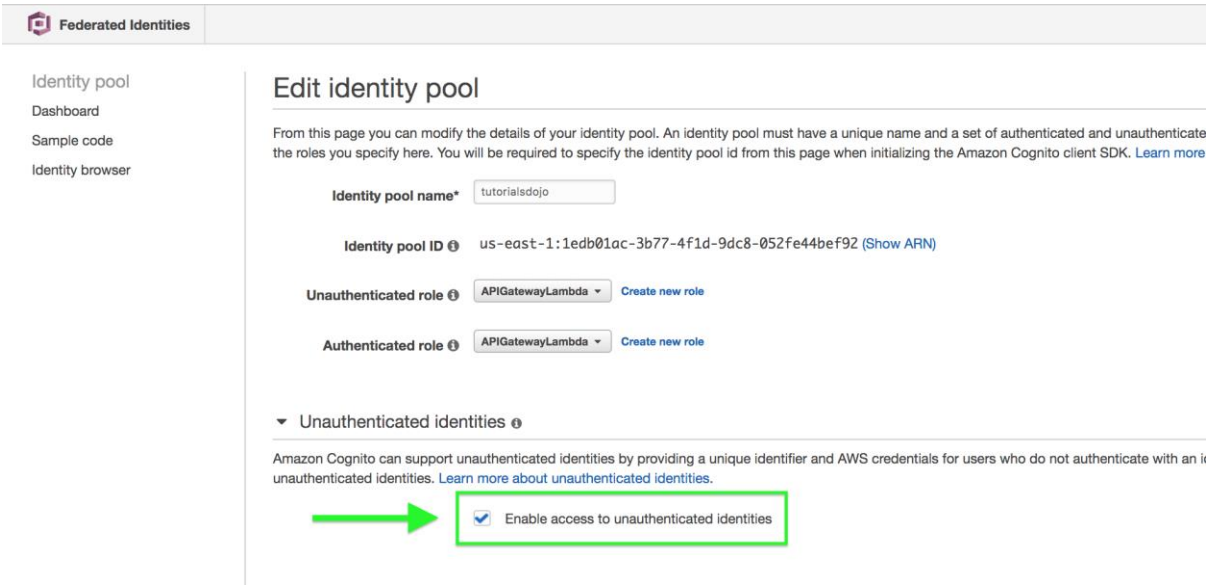
Amazon Cognito Identity Pool provides temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.

Amazon Cognito identity pools enable you to create unique identities and assign permissions for users. Your identity pool can include:

- Users in an Amazon Cognito user pool

- Users who authenticate with external identity providers such as Facebook, Google, or a SAML-based identity provider

- Users authenticated via your own existing authentication process



With an identity pool, you can obtain temporary AWS credentials with permissions you define to directly access other AWS services or to access resources through Amazon API Gateway.

Hence, the correct answer is: **Amazon Cognito Identity Pool.**

Amazon Cognito User Pool is incorrect because a user pool is a user directory in Amazon Cognito. In addition, it doesn't enable access to unauthenticated identities. You have to use an Identity Pool instead.

AWS AppSync is incorrect because this is a service that enables cross-device syncing of application-related user data. It's also a serverless GraphQL and Pub/Sub API service that makes it easier to build modern web and mobile apps.

AWS IAM Identity Center is incorrect because this service simply lets you centrally manage access to multiple AWS accounts using credentials from identity sources such as Microsoft Active Directory Domain Services, Okta. or Microsoft Azure AD. It also does not allow any "guest" or unauthenticated access, unlike Amazon Cognito.

References:

https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html

https://docs.aws.amazon.com/cognito/latest/developerguide/getting-started-with-identity-pools.html

Check out this Amazon Cognito Cheat Sheet:

https://tutorialsdojo.com/amazon-cognito/

AWS Identity Services Overview:

https://youtu.be/AIdUw0i8rr0?si=f8htGp8kjBwy1Qab

Question 2:

Skipped

When a company uses AWS and decouple from their on-premises data center, they will be able to have which of the following benefits? (Select TWO.)

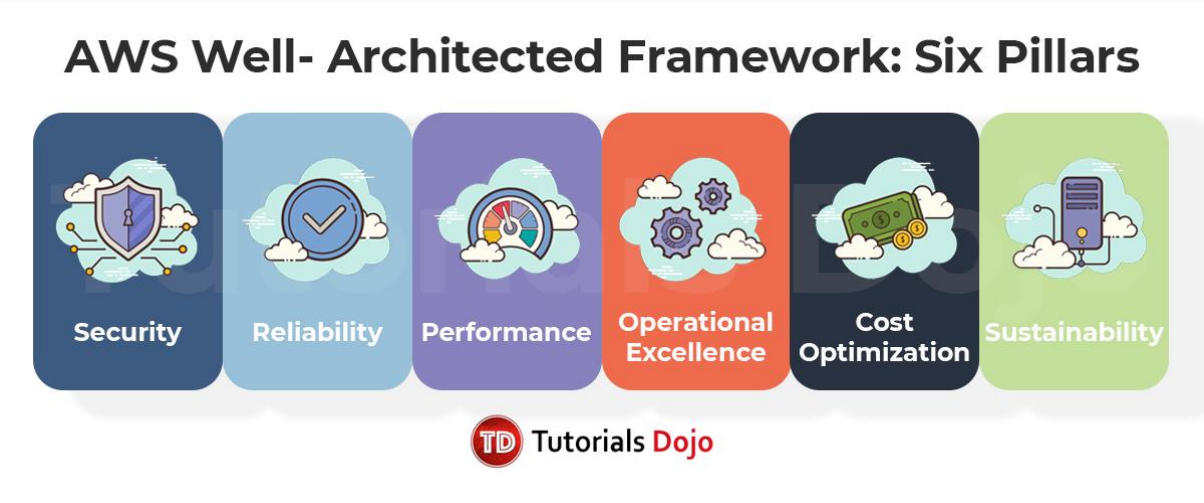
- **Massive discounts for bare metal servers from Amazon.com.**
- **Replace low variable costs with upfront capital expenses (CAPEX).**
- **Deferred payments to their operational expenditures.**
- **Reduce time to market.**

(Correct)

- **Decrease your TCO.**

(Correct)

Explanation
As the technology has matured over the last decade, companies are moving to the cloud to lower costs, reduce complexity, and increase flexibility. The cloud provides scalable and powerful compute solutions, low-cost, reliable storage, and database technologies that meet the most demanding workload requirements. In addition, cloud technologies can be used to deploy solutions quickly and cost-effectively around the world and on any device.



When you decouple from the data center, you'll be able to:

- **Decrease your TCO**: Eliminate many of the costs related to building and maintaining a data center or colocation deployment. Pay for only the resources you consume.

- **Reduce complexity**: Reduce the need to manage infrastructure, investigate licensing issues, or divert resources.

- **Adjust capacity on the fly**: Add or reduce resources, depending on seasonal business needs, using infrastructure that is secure, reliable, and broadly accessible.

- **Reduce time to market**: Design and develop new IT projects faster.

- **Deploy quickly, even worldwide**: Deploy applications across multiple geographic areas.

- **Increase efficiencies**: Use automation to reduce or eliminate IT management activities that waste time and resources.

- **Innovate more:** Spin up a new server and try out an idea. Each project moves through the funnel more quickly because the cloud makes it faster (and cheaper) to deploy, test, and launch new products and services.

- **Spend your resources strategically:** Switch to a DevOps model to free your IT staff from operations and maintenance that can be handled by the cloud services provider.

- **Enhance security:** Spend less time conducting security reviews on infrastructure. Mature cloud providers have teams of people who focus on security, offering best practices to ensure you're compliant, no matter what your industry.

Hence, the correct answers are:

- Decrease your TCO

- Reduce time to market

The option that says: **Deferred payments to their operational expenditures** is incorrect because this type of payment is not supported when you move to AWS.

The option that says: **Replace low variable costs with upfront capital expenses (CAPEX)** is incorrect because it is actually the other way around: Using AWS, companies will have the opportunity to replace upfront capital expenses (CAPEX) with low variable costs.

The option that says: **Massive discounts for bare metal servers from Amazon.com** is incorrect because this is not an advantage of using AWS. By moving from a traditional data center to the AWS cloud, you can reduce or eliminate the overhead related to managing, operating, and maintaining your data center. Hence, the reduction of your TCO is not from the massive discounts on the Amazon e-commerce website.

References:

https://d1.awsstatic.com/whitepapers/introduction-to-aws-cloud-economics-final.pdf

https://aws.amazon.com/economics/

Tutorials Dojo's AWS Certified Cloud Practitioner Exam Study Guide:

https://tutorialsdojo.com/aws-certified-cloud-practitioner/

Question 3:

Skipped

A customer currently has a Basic support plan and they are planning to use the Infrastructure Event Management, Well-Architected Reviews and Operations

Reviews features in AWS. What should they do in order to access these features in the most cost-effective manner?

- **None since these features are already included in their Basic support plan.**
- **Upgrade to Developer support plan.**
- **Upgrade to Enterprise support plan.**

  (Correct)

- **Upgrade to Business support plan.**

Explanation

AWS Enterprise Support provides you with a concierge-like service where the main focus is helping you achieve your outcomes and find success in the cloud.

With Enterprise Support, you get 24x7 technical support from high-quality engineers, tools, and technology to automatically manage the health of your environment, consultative architectural guidance delivered in the context of your applications and use-cases, and a designated Technical Account Manager (TAM) to coordinate access to proactive/preventative programs and AWS subject matter experts.

	DEVELOPER	BUSINESS	ENTERPRISE ON-RAMP	ENTERPRISE
Use Case	Recommended if you are experimenting or testing in AWS.	Recommended if you have production workloads in AWS.	Recommended if you have business and/or mission critical workloads in AWS.	Recommended if you have business and/or mission critical workloads in AWS.
AWS Trusted Advisor Best Practice Checks	Service Quota and basic Security checks	Full set of checks	Full set of checks	Full set of checks
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications	Consultative review and guidance based on your applications
Technical Account Management	✗	✗	A pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts	Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization and coordinate access to programs and
Training	✗	✗	✗	Access to online self-paced labs
Account Assistance	✗	✗	Concierge Support Team	Concierge Support Team
Enhanced Technical Support	Business hours** email access to Cloud Support Associates. Unlimited cases / 1 primary contact Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post
Programmatic Case Management	✗	AWS Support API	AWS Support API	AWS Support API
Third-Party Software Support	✗	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting
Proactive Programs	Access to Support Automation Workflows with prefixes AWSSupport	Access to Infrastructure Event Management for additional fee Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management (one-per-year) Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management Access to proactive reviews, workshops, and deep dives Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport

In addition to what is available with Basic Support, Enterprise Support provides:

AWS Trusted Advisor - Access to the full set of Trusted Advisor checks and guidance to provision your resources following best practices to help reduce costs, increase performance and fault tolerance, and improve security.

AWS Health - View the health of AWS services and sends you alerts when your resources are impacted. Also includes the Health API for integration with your existing management systems.

AWS Support API - Programmatic access to AWS Support Center features to create, manage, and close your support cases and operationally manage your Trusted Advisor check requests and status.

Proactive Technical Account Management - A Technical Account Manager (TAM) is your designated technical point of contact who provides advocacy and guidance to help plan and build solutions using best practices, coordinate access to subject matter experts and product teams, and proactively keep your AWS environment operationally healthy.

Architecture Support – Contextual guidance on how services fit together to meet your specific use case, workload, or application.

Third-Party Software Support - Guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

Proactive Support Programs – Included access to Well-Architected Reviews, Operations Reviews, and Infrastructure Event Management.

Support Concierge - the Concierge Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries and work with you to implement billing and account best practices so that you can focus on what matters: running your business.

For companies with a Business support plan, you can have access to Infrastructure Event Management for an additional fee. However, all other proactive support programs, such as Well-Architected Reviews and Operations Reviews, are exclusively available for companies who opted for Enterprise support.

Hence, the correct answer is: **Upgrade to Enterprise support plan.**

The option that says: **None since these features are already included in their Basic support plan** is incorrect because the Basic plan does not have any Proactive Support Programs such as Well-Architected Reviews, Operations Reviews, and Infrastructure Event Management.

The option that says: **Upgrade to Developer support plan** is incorrect because just like the Basic plan, this one does not have access to any of the Proactive Support Programs.

The option that says: **Upgrade to Business support plan** is incorrect. Although this has access to the Infrastructure Event Management feature for an additional fee, it doesn't have access to the Well-Architected Reviews or Operations Reviews. In this scenario, you must upgrade to the Enterprise support plan.

References:

https://aws.amazon.com/premiumsupport/plans/

https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html

https://aws.amazon.com/premiumsupport/plans/enterprise/

Check out this AWS Support Plans Cheat Sheet:

https://tutorialsdojo.com/aws-support-plans/

Question 4:

Skipped

In the AWS Shared Responsibility Model, whose responsibility is it to patch the host operating system of an Amazon EC2 instance?

- **Customer**
- **Both AWS and the customer**
- **AWS**

(Correct)

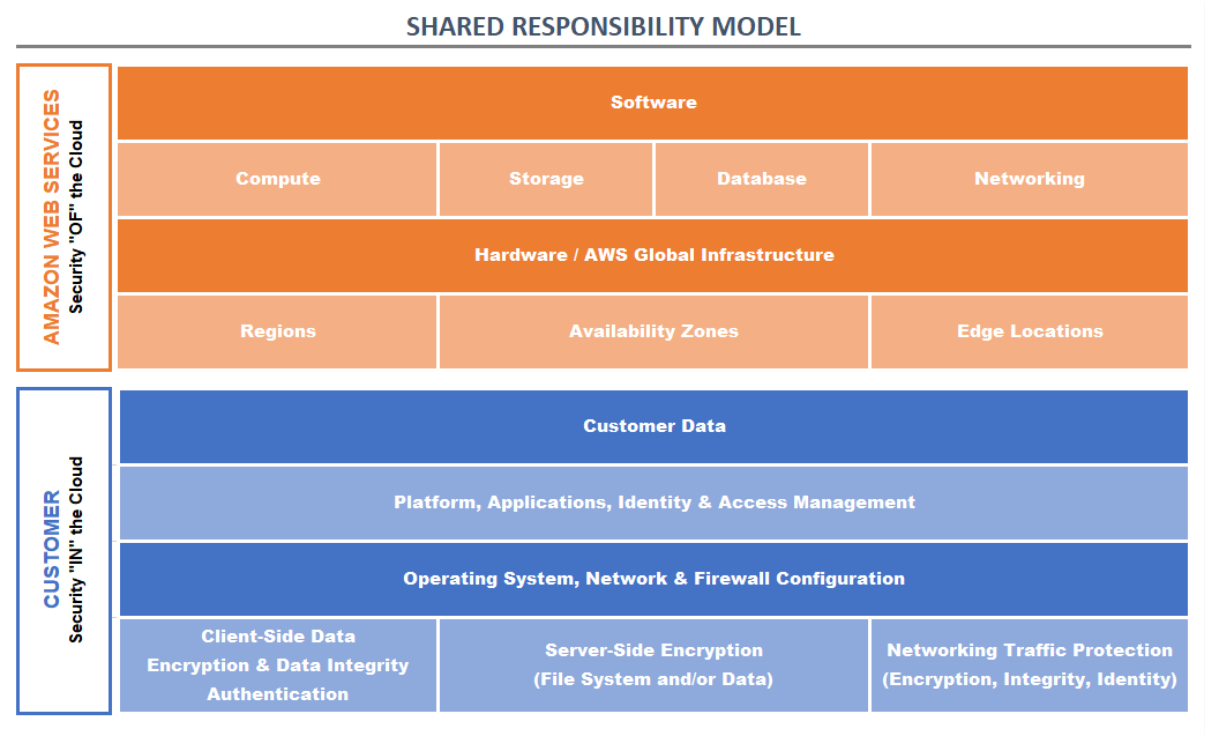
- **Neither AWS nor the customer**

Explanation

Security and Compliance are a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security **OF** the Cloud versus Security **IN** the Cloud.



This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation, and verification of IT controls shared. AWS can help relieve the customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment.

Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required. Below are examples of controls that are managed by AWS, AWS Customers, and/or both.

Inherited Controls: Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

Shared Controls: Controls that apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services.

Examples include:

- Patch Management: AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

- Configuration Management: AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

- Awareness & Training: AWS trains AWS employees, but a customer must train their own employees.

Customer Specific: Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services.

Examples include:

- Service and Communications Protection or Zone Security may require a customer to route or zone data within specific security environments.

The host operating system, which is managed by AWS, is the hypervisor that creates several guest operating systems that can be managed by different customers. Amazon EC2 uses a technology commonly known as virtualization to run multiple operating systems on a single physical machine. Virtualization ensures that each guest operating system receives its fair share of CPU time, memory, and I/O bandwidth to the local disk and to the network using a host operating system, sometimes known as a hypervisor. The hypervisor also isolates the guest operating systems from each other so that one guest cannot modify or otherwise interfere with another one on the same machine.

Hence, the correct answer is: **AWS**.

Customer is incorrect because their responsibility is to patch the guest operating system of their EC2 instance and not the host operating system.

Both AWS and the customer is incorrect because patching the host operating system of the Amazon EC2 instance is the responsibility of AWS. Take note that if you are using a fully-managed service like Amazon DynamoDB or Redshift, AWS will also be responsible for the underlying guest operating system.

Neither AWS nor the customer is incorrect as this task falls under the responsibilities of AWS.

References:

https://aws.amazon.com/compliance/shared-responsibility-model/

https://d1.awsstatic.com/Marketplace/scenarios/security/SEC_02_TSB_Final.pdf

https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

Tutorials Dojo's AWS Certified Cloud Practitioner Exam Study Guide:

https://tutorialsdojo.com/aws-certified-cloud-practitioner/

Question 5:

Skipped

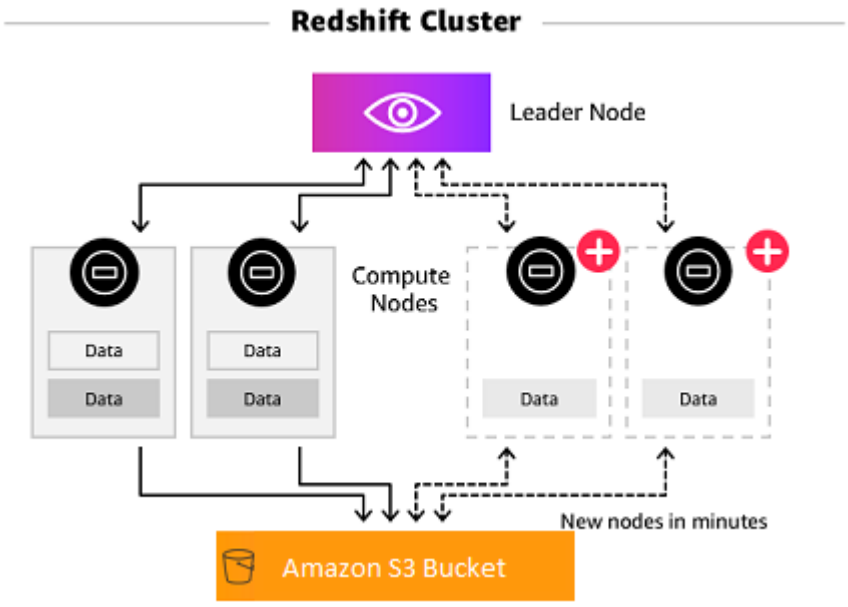
Which of the following will allow you to create a data warehouse in AWS for your business intelligence needs?

- **Amazon RDS**
- **Amazon S3**
- **Amazon DynamoDB**
- **Amazon Redshift**

(Correct)

Explanation

Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It allows you to run complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution. Most results come back in seconds. With Redshift, you can start small for just $0.25 per hour with no commitments and scale out to petabytes of data for $1,000 per terabyte per year, less than a tenth the cost of traditional solutions.



Amazon Redshift also includes Amazon Redshift Spectrum, allowing you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required, and you can use open data formats, including Avro, CSV, Grok, Ion, JSON, ORC, Parquet, RCFile, RegexSerDe, SequenceFile, TextFile, and TSV. Redshift Spectrum automatically scales query compute capacity based on the data being retrieved, so queries against Amazon S3 run fast, regardless of data set size.

Traditional data warehouses require significant time and resource to administer, especially for large datasets. In addition, the financial cost associated with building, maintaining, and growing self-managed, on-premise data warehouses is very high. As your data grows, you have to constantly trade-off what data to load into your data warehouse and what data to archive in storage so you can manage costs, keep ETL complexity low, and deliver good performance. Amazon Redshift not only significantly lowers the cost and operational overhead of a data warehouse, but with Redshift Spectrum, also makes it easy to analyze large amounts of data in its native format without requiring you to load the data.

Hence, the correct answer is **Amazon Redshift**.

Amazon Relational Database Service (Amazon RDS) is incorrect since this is a relational (SQL) database in the cloud, not a data warehouse.

Amazon DynamoDB is incorrect since this service is a non-relational (noSQL) database in the cloud, not a data warehouse.

Amazon S3 is incorrect since this service is a durable cloud storage for objects and files, and not a data warehouse.

References:

https://aws.amazon.com/redshift/

https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html

Amazon Redshift Overview:

https://youtu.be/jlLERNzhHOg

Check out this Amazon Redshift Cheat Sheet:

https://tutorialsdojo.com/amazon-redshift/

Question 6:

Skipped

A space agency is using Amazon S3 to store their high-resolution satellite images and videos everyday. Which of the following should they do to minimize the upload time?

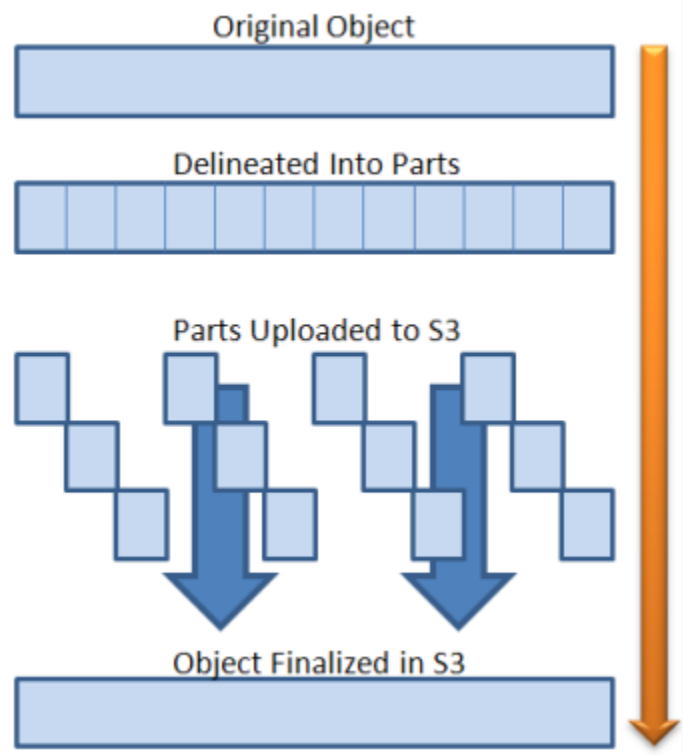
- **Upload the images and videos using the BatchWriteItem API**
- **Enable Cross-Origin Resource Sharing (CORS)**
- **Use the Multipart upload API**

  (Correct)

- **Shift to S3 Intelligent-Tiering storage class**

Explanation

Multipart upload allows you to upload a single object as a set of parts. Each part is a contiguous portion of the object's data. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.



Using multipart upload provides the following advantages:

- **Improved throughput** - You can upload parts in parallel to improve throughput.

- **Quick recovery from any network issues** - Smaller part size minimizes the impact of restarting a failed upload due to a network error.

- **Pause and resume object uploads** - You can upload object parts over time. Once you initiate a multipart upload there is no expiry; you must explicitly complete or abort the multipart upload.

- **Begin an upload before you know the final object size** - You can upload an object as you are creating it.

Hence, the correct answer in this scenario is: **Use the Multipart Upload API.**

The option that says: **Use the BatchWriteItem API** is incorrect because this is a DynamoDB API action and not S3.

The option that says: **Shift to S3 Intelligent-Tiering storage class** is incorrect because this is primarily used to optimize your storage costs automatically based on your data access patterns without performance impact or operational overhead.

The option that says: **Enable Cross-Origin Resource Sharing (CORS)** is incorrect because this is only applicable for client web applications that are loaded in one domain to interact with resources in a different domain.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

Check out this Amazon S3 Cheat Sheet:

https://tutorialsdojo.com/amazon-s3/

Question 7:

Skipped

Which of the following cloud design principles supports growth in users, traffic, or data size with no drop-in performance?

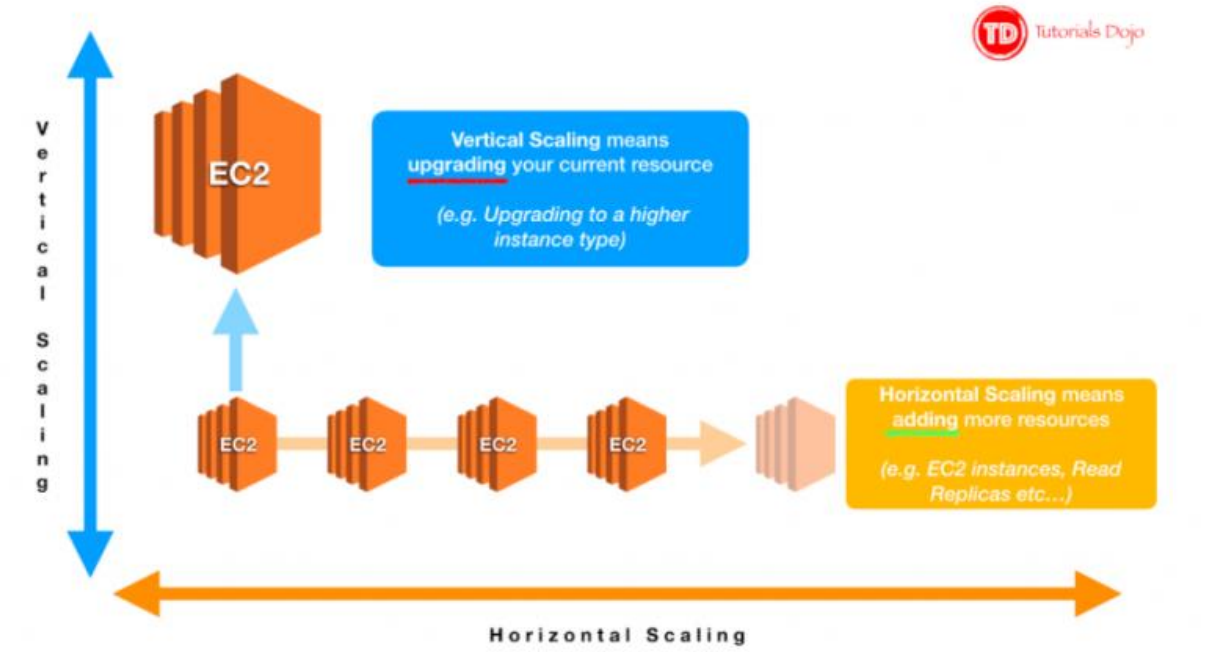
- **Design for failure**
- **Scalability**

  (Correct)

- **Decouple your components**
- **Go Serverless to reduce compute footprint**

Explanation

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



Systems that are expected to grow over time need to be built on top of a scalable architecture. Such an architecture can support growth in users, traffic, or data size with no drop-in performance. It should provide that scale in a linear manner where adding extra resources results in at least a proportional increase inability to serve additional load.

Growth should introduce economies of scale, and cost should follow the same dimension that generates business value out of that system. While cloud computing provides virtually unlimited on-demand capacity, your design needs to be able to take advantage of those resources seamlessly.

Hence, the correct answer is: **Scalability**.

The option that says: **Think parallel** is incorrect because this just internalizes the concept of parallelization when designing architectures in the cloud. It advocates not only implement parallelization wherever possible but also automate it because the cloud allows you to create a repeatable process very easily.

The option that says: **Design for failure** is incorrect because it only encourages you to be a pessimist when designing architectures in the cloud; assume things will fail. In other words, you should always design, implement and deploy for automated recovery from failure.

The option that says: **Go Serverless to reduce compute footprint** is incorrect because this is not considered as one of the key design principles of the AWS Cloud. Although it is true using a Serverless architecture can reduce your compute footprint, this is not applicable in every case. AWS Lambda is an example of a serverless service.

References:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

https://www.slideshare.net/AmazonWebServices/best-practices-for-architecting-in-the-cloud-jeff-barr

Check out this AWS Well-Architected Framework – Design Principles:

https://tutorialsdojo.com/aws-well-architected-framework-design-principles/

Question 8:

Skipped

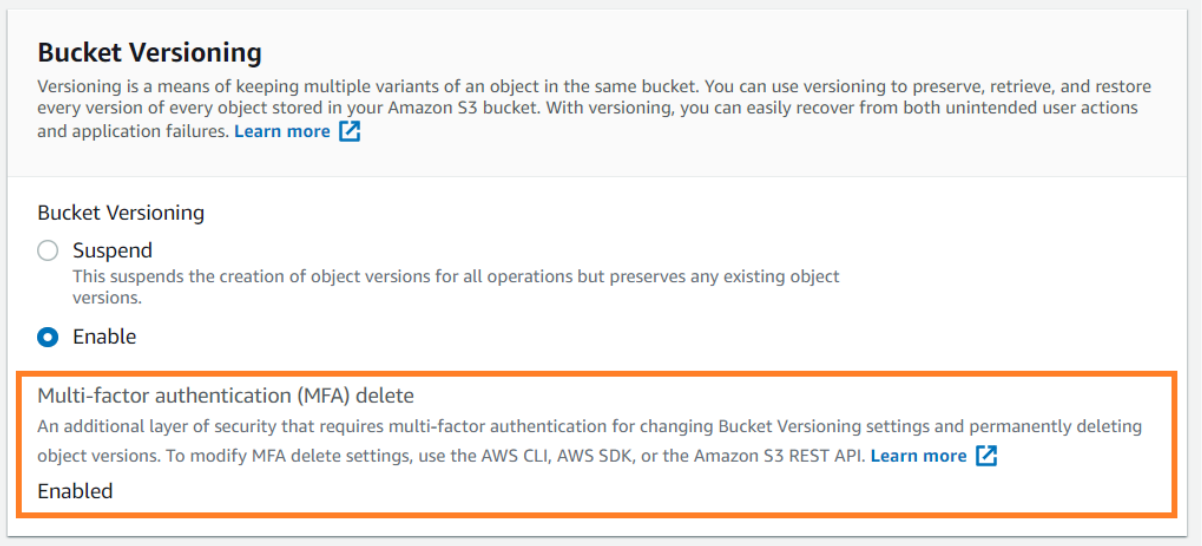
There is an incident with your team where an S3 object was deleted using an account without the owner's knowledge. What can be done to prevent unauthorized deletion of your S3 objects?

- **Set your S3 buckets to private so that objects are not publicly readable/writable**
- **Create access control policies so that only you can perform S3-related actions**
- **Set up stricter IAM policies that will prevent users from deleting S3 objects**
- **Configure MFA delete on the S3 bucket.**

(Correct)

Explanation

By setting up MFA, you add an extra layer of protection for your AWS accounts. This is very useful for preventing unwanted access to your AWS resources. In S3, once versioning is enabled for your objects, you can also set up MFA delete so that deleting objects require an additional MFA authentication.



MFA delete can help prevent accidental bucket deletions by requiring the user who initiates the delete action to prove physical possession of an MFA device with an MFA code and adding an extra layer of friction and security to the delete action. Remember that only the bucket owner (root account) can enable MFA delete.

Hence, the correct answer is: **Configure MFA delete on the S3 bucket.**

The option that says: **Set up stricter IAM policies that will prevent users from deleting S3 objects** is incorrect because you can prevent unwanted deletion by removing the permission from IAM Users. However, in this case, the issue is caused by unauthorized access to the account which had the capability of deleting objects. This will totally restrict the authorized users from deleting necessary objects.

The option that says: **Create access control policies so that only you can perform S3-related actions** is incorrect because this will not prevent unauthorized access to AWS accounts.

The option that says: **Set your S3 buckets to private so that objects are not publicly readable/writable** is incorrect because this is unrelated to the issue in this case.

References:

https://aws.amazon.com/iam/details/mfa/

https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html

Check out this AWS IAM Cheat Sheet:

https://tutorialsdojo.com/aws-identity-and-access-management-iam/

Question 9:

Skipped

A customer needs to retrieve the instance ID, instance profile permissions, and kernel information of their EC2 instance for an app that is running within the same instance. Where can the customer find this information?

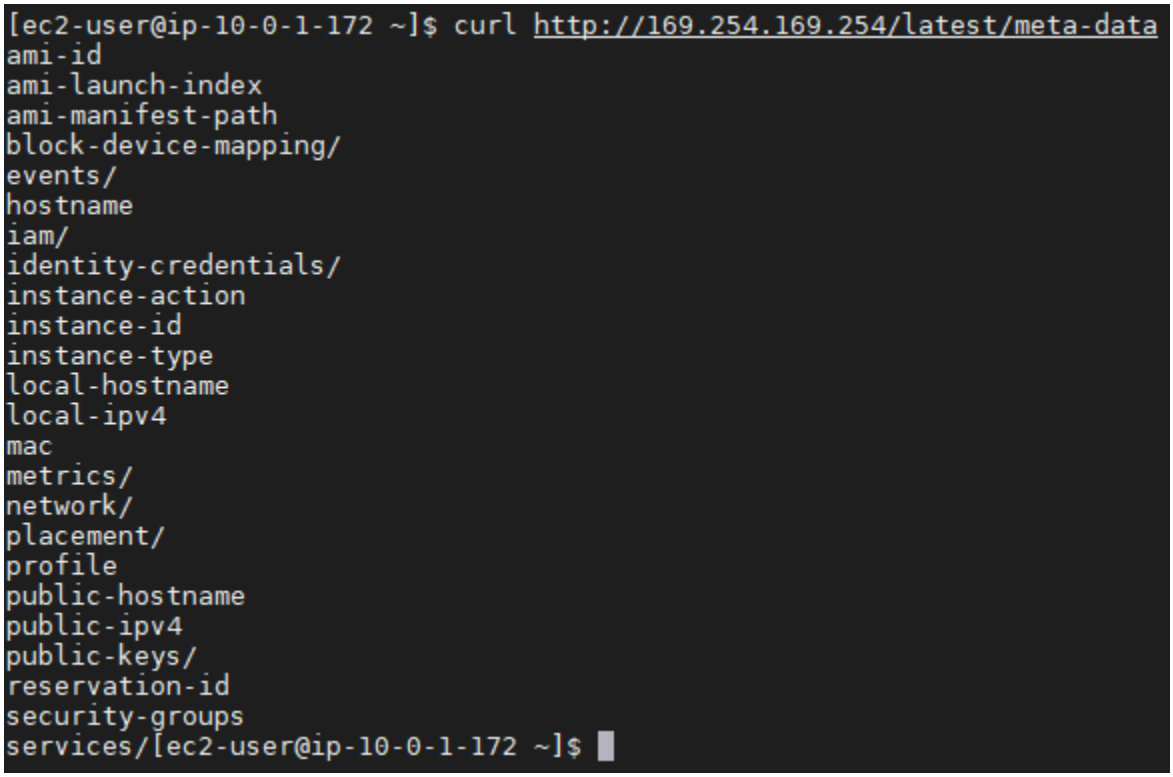
- **Amazon Machine Image**
- **Instance metadata**

  (Correct)

- **Resource tag**
- **Instance user data**

Explanation

When you run the AWS CLI from within an Amazon Elastic Compute Cloud (Amazon EC2) instance, you can simplify providing credentials to your commands. Each Amazon EC2 instance contains metadata that the AWS CLI can directly query for temporary credentials. When an IAM role is attached to the instance, the AWS CLI automatically and securely retrieves the credentials from the instance metadata.



Instance metadata is the data about your instance that you can use to configure or manage the running instance. You can get the instance ID, public keys, public IP address, and other information from the instance metadata by entering the following URL in your instance:

http://169.254.169.254/latest/meta-data/

To check the kernel version of an EC2 instance, you can type `uname -r` in the CLI.

Hence, the correct answer is: **Instance metadata.**

Instance user data is incorrect because this is primarily used to perform common automated configuration tasks and run custom scripts after the instance starts. It doesn't contain any information about the instance ID, public keys, or the public IP address of your EC2 instance.

Resource tag is incorrect because this is just a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define.

Amazon Machine Image is incorrect because this mainly provides the information required to launch an instance, which is a virtual server in the cloud.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instances-and-amis.html

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Amazon EC2 Overview:

https://youtu.be/7VsGIHT_jQE

Question 10:

Skipped

A company plans to migrate their on-premises MySQL database to Amazon RDS. Which AWS service should they use for this task?

- **AWS Application Migration Service**
- **AWS Schema Conversion Tool (AWS SCT)**
- **AWS Database Migration Service (AWS DMS)**

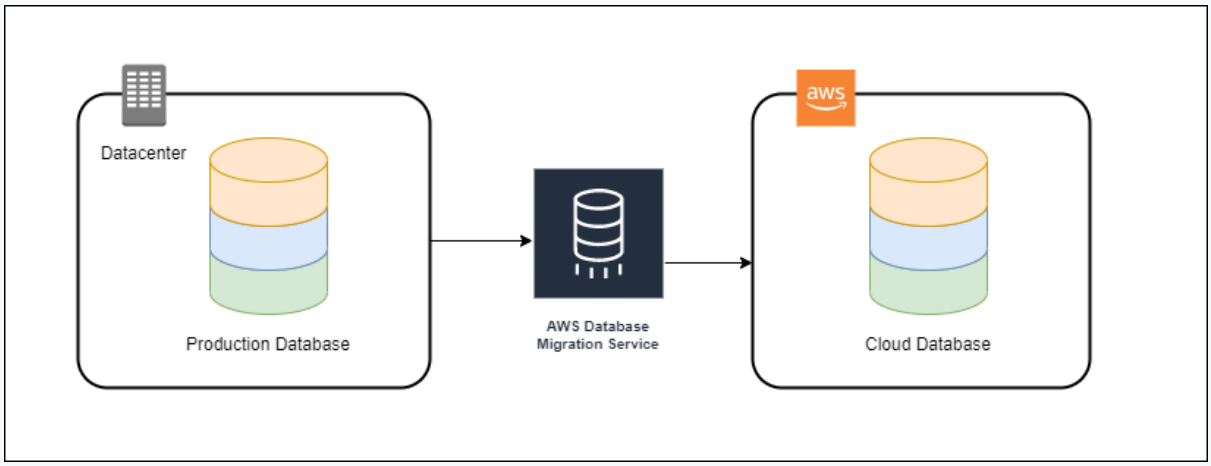
(Correct)

- **AWS Glue**

Explanation

AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from the most widely used commercial and open-source databases.

AWS Database Migration Service supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle or Microsoft SQL Server to Amazon Aurora. With AWS Database Migration Service, you can continuously replicate your data with high availability and consolidate databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift and Amazon S3.



The AWS Schema Conversion Tool makes heterogeneous database migrations predictable by automatically converting the source database schema and a majority of the database code objects, including views, stored procedures, and functions, to a format compatible with the target database. Any objects that cannot be automatically converted are clearly marked so that they can be manually converted to complete the migration. SCT can also scan your application source code for embedded SQL statements and convert them as part of a database schema conversion project.

During this process, SCT performs cloud-native code optimization by converting legacy Oracle and SQL Server functions to their equivalent AWS service thus helping you modernize the applications at the same time of database migration. Once schema conversion is complete, SCT can help migrate data from a range of data warehouses to Amazon Redshift using built-in data migration agents. For example, it can convert PostgreSQL to MySQL or an Oracle Data Warehouse to Amazon Redshift

Hence, the correct answer is **AWS Database Migration Service (AWS DMS).**

AWS Schema Conversion Tool (AWS SCT) is incorrect because this is primarily used to convert your existing database schema from one database engine to another. The

scenario didn't mention anything about migrating the MySQL database to another database type. Since the task is to just migrate their on-premises MySQL database to Amazon RDS, you simply need to use the AWS Database Migration Service (AWS DMS).

AWS Application Migration Service is incorrect. This service is primarily designed for migrating entire applications, including their operating systems and system state, from on-premises data centers or other cloud providers to AWS. It focuses on ensuring minimal downtime and is more about moving workloads rather than just database-specific migrations. This is not the appropriate service for migrating on-premises database.

AWS Glue is incorrect because this is just a service for preparing, moving, and integrating data from multiple sources for analytics, machine learning, and application development.

References:

https://aws.amazon.com/dms/

https://docs.aws.amazon.com/dms/latest/userguide/Welcome.html

Check out this AWS Database Migration Service Cheat Sheet:

https://tutorialsdojo.com/aws-database-migration-service/

AWS Migration Services Overview:

https://youtu.be/yqNBkFMnsL8?si=MXFp1QNPlf-SY_qo

Question 11:

Skipped

Which of the following is a fully managed database in AWS that can be used to store JSON documents?

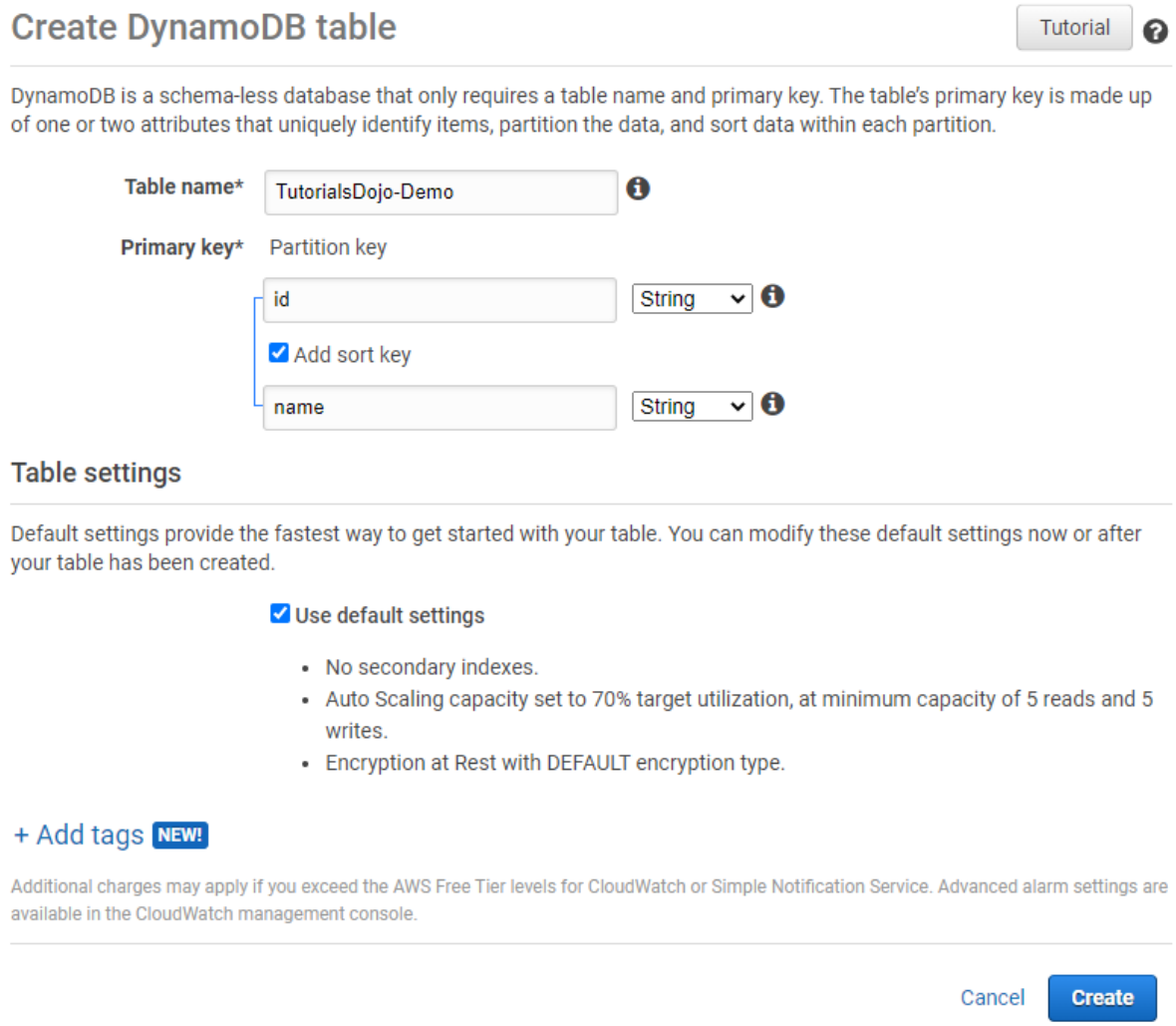
- **Amazon ElastiCache**
- **Amazon DynamoDB**

  (Correct)

- **Amazon Aurora**
- **Amazon Redshift**

Explanation

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. This is the perfect database to use for JSON-type documents.



DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale. You can build applications with virtually unlimited throughput and storage. DynamoDB global tables replicate your data across multiple AWS Regions to give you fast, local access to data for your globally distributed applications. For use cases that require even faster access with microsecond latency, DynamoDB Accelerator (DAX) provides a fully managed in-memory cache.

Hence, the correct answer is: **Amazon DynamoDB**.

Amazon Aurora is incorrect because this is a MySQL and PostgreSQL-compatible relational database. It will not be able to store JSON-type documents.

Amazon ElastiCache is incorrect because this is a service that offers a fully managed Redis and Memcached. Elasticache is a caching service and is not suited for persistent NoSQL database entries.

Amazon Redshift is incorrect because this is a data warehousing service that uses columnar storage. This is not the best option compared to using Amazon DynamoDB.

References:

https://aws.amazon.com/dynamodb/

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

Amazon DynamoDB Overview:

https://www.youtube.com/watch?v=3ZOyUNIeorU

Check out this Amazon DynamoDB Cheat Sheet:

https://tutorialsdojo.com/amazon-dynamodb/

Question 12:

Skipped

A company wants to launch a Microsoft SQL Server database in AWS. The database instance should only be managed by the company's DBA and must be accessible via RDP. A standard license for SQL Server is required but the company is not yet sure how much CPU and memory to allocate to the database.

Which option gives the most convenience and flexibility to determine the best database size while still being cost-effective?

- **Launch an RDS instance that runs MS SQL Server Standard. Purchase a Standard MSSQL license and store it in the AWS Managed Services (AMS).**
- **Use a Windows Server with SQL Server Standard bundled AMI so you won't need to buy and manage your own license.**

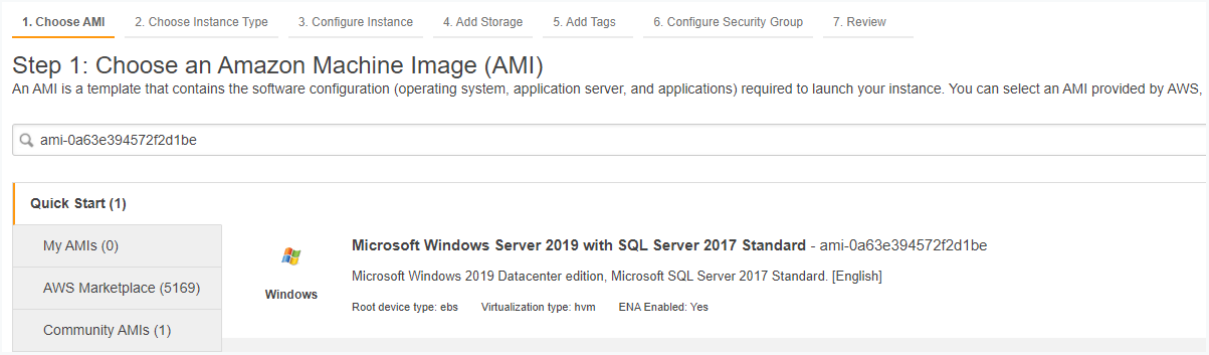
(Correct)

- **Launch an Amazon Aurora database that runs MS SQL Server. Buy a Standard MSSQL license from the AWS License Manager service.**

- **Launch an EC2 instance and install MS SQL Server. Purchase a Standard MSSQL license from Microsoft and apply it to the database you installed.**

Explanation

AWS offers multiple AMI configurations for Amazon EC2 - from community AMIs to AMIs sold by customers in the AWS Marketplace. If you launch an EC2 instance using a Windows AMI with a bundled MS SQL Server Standard, you won't need to purchase your own licenses from Microsoft. And since this is an EC2 instance, you can freely resize it to a different instance type or class of your choosing.



Amazon EC2 follows a pay-as-you-go model, so there are no long-term commitments when launching an EC2 instance, even if there is an MS SQL Server installed.

Hence, the correct answer is: **Use a Windows Server with SQL Server Standard bundled AMI so you won't need to buy and manage your own license.**

The option that says: **Launch an EC2 instance and install MS SQL Server. Purchase a Standard MSSQL license from Microsoft and apply it to the database you installed** is incorrect since this is not the most convenient method of launching an MS SQL Server in AWS. You typically use this solution if you already have a SQL Server license and you prefer to BYOL (bring your own license).

The option that says: **Launch an RDS instance that runs MS SQL Server Standard. Purchase a Standard MSSQL license and store it in the AWS Managed Services (AMS)** is incorrect. It is explicitly stated in the scenario that the database instance should only be managed by the company's DBA and must be accessible via RDP. You cannot directly establish an RDS connection to an Amazon RDS database. In addition, Amazon RDS costs more than Amazon EC2 because the infrastructure is managed by AWS.

The option that says: **Launch an Amazon Aurora database that runs MS SQL Server. Buy a Standard MSSQL license from the AWS License Manager service** is incorrect since Amazon Aurora does not support MS SQL Server. Moreover, you cannot directly buy software licenses from the AWS License Manager service. This is just used to easily manage your software licenses from various vendors such as Microsoft, SAP, Oracle, and IBM across AWS and on-premises environments.

References:

https://aws.amazon.com/sql/

https://aws.amazon.com/windows/resources/licensing/

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Question 13:

Skipped

Which of the following are defined as global services in AWS? (Select TWO.)

- **Amazon RDS**
- **AWS Batch**
- **Amazon DynamoDB**
- **AWS Identity and Access Management**

  (Correct)

- **Amazon CloudFront**

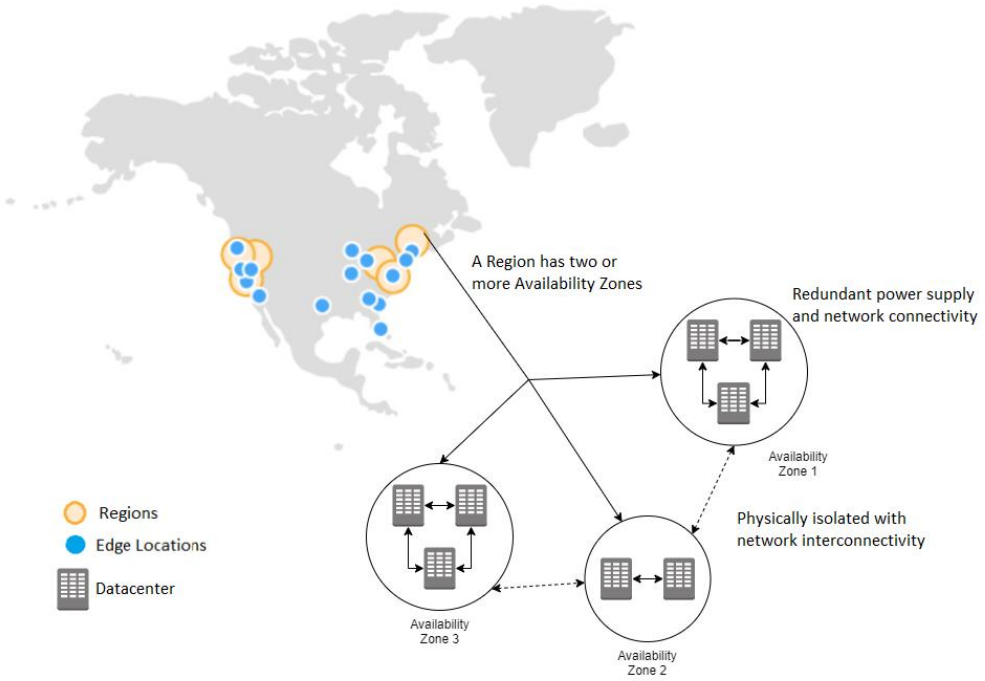
  (Correct)

Explanation

Amazon CloudFront is a global service that delivers your content through a worldwide network of data centers called edge locations or points of presence (POPs). If your content is not already cached in an edge location, CloudFront retrieves it from an origin that you've identified as the source for the definitive version of the content.

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

An AWS resource can be a Global, Regional, or Zonal service. A Global service means that it covers all of the AWS Regions across the globe, while a regional service means that a resource is only applicable to one specific region at a time. A regional service may or may not have the ability to replicate the same resource in another region. Lastly, a Zonal service can only exist in one Availability Zone.



You don't need to memorize the scope of all of the AWS services as long as you know the pattern. There are actually only a handful of services that are considered global services such as IAM, STS, Route 53, CloudFront, and WAF. For Zonal services, the examples are EC2 Instances and EBS Volumes which are tied to the Availability Zone where they were launched. Take note that although EBS Volumes are considered a zonal service, the EBS snapshots are considered regional since it is not tied to a specific Availability Zone. Most of the services are regional in scope.

Hence, the correct answers are:

- AWS Identity and Access Management

- Amazon CloudFront

AWS Batch, Amazon RDS, and Amazon DynamoDB are incorrect because these are considered regional services and not global.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

https://d1.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events

Check out these AWS IAM and Amazon CloudFront Cheat Sheets:

https://tutorialsdojo.com/aws-identity-and-access-management-iam/

https://tutorialsdojo.com/amazon-cloudfront/

Question 14:

Skipped

A manufacturing company has multiple AWS accounts for various departments. As the company grows, they are experiencing an increase in its AWS costs and want to optimize its expenses by taking advantage of any available discounts.

Which of the following actions below will allow you to take advantage of volume discounts in AWS?

- **Upgrade to an AWS Enterprise support plan.**
- **Opt for an All upfront Convertible Reserved Instance pricing for a 3-year term.**
- **Use AWS Organizations and enable the consolidated billing feature.**

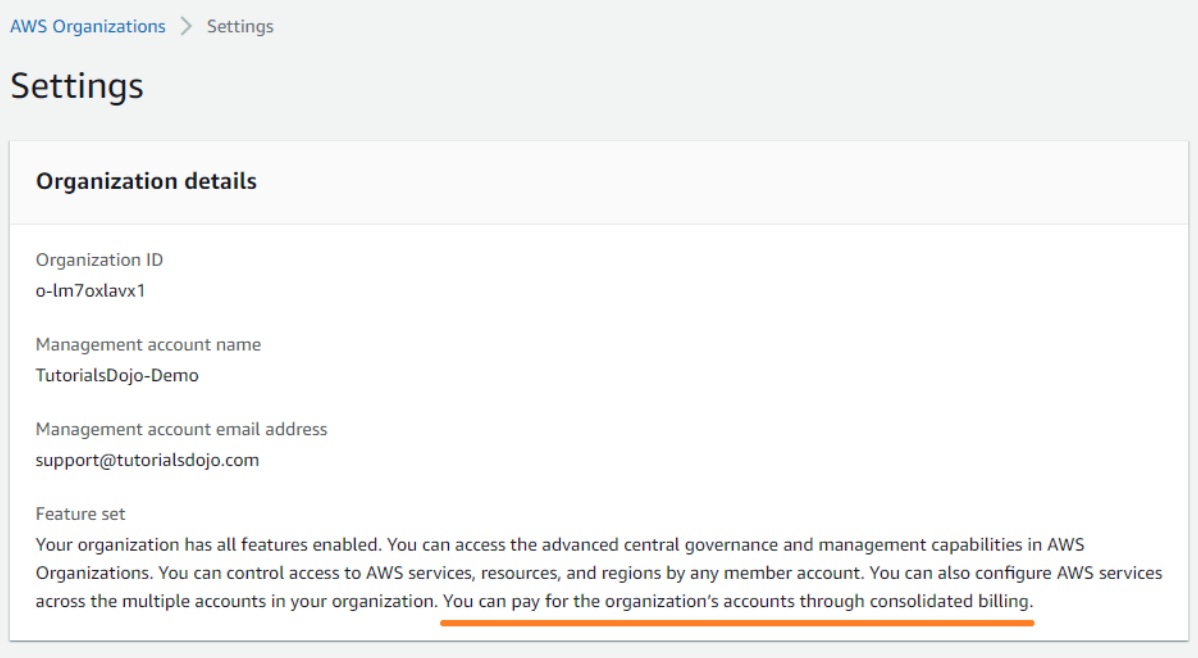
(Correct)

- **Move all of your AWS resources from multiple accounts to a single global account.**

Explanation

For billing purposes, AWS treats all the accounts in the organization as if they were one account. Some services, such as Amazon EC2 and Amazon S3, have **volume pricing** tiers across certain usage dimensions that give you lower prices the more you use the service.

With consolidated billing, AWS combines the usage from all accounts to determine which volume pricing tiers to apply, giving you a lower overall price whenever possible. AWS then allocates each linked account a portion of the overall volume discount based on the account's usage.



The Bills page for each linked account displays an average tiered rate that is calculated across all the accounts on the consolidated bill for the organization. For example, let's say that Bob's consolidated bill includes both Bob's own account and Susan's account. Bob's account is the payer account, so he pays the charges for both himself and Susan.

Hence, the correct answer is: **Use AWS Organizations and enable the consolidated billing feature.**

The option that says: **Move all of your AWS resources from multiple accounts to a single global account** is incorrect because you don't need to do this since you can simply use AWS Organizations to consolidate your resources.

The option that says: **Opt for an All upfront Convertible Reserved Instance pricing for a 3-year term** is incorrect because this type of discount is only applicable for Reserved Instances and is not related to Volume Pricing.

The option that says: **Upgrade to an AWS Enterprise support plan** is incorrect because doing this will only give you more access to various AWS support services like a Technical Account Manager, access to Concierge Support, and many others. In order to avail of volume pricing, you have to use AWS Organizations and enable Consolidated Billing.

References:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/useconsolidatedbilling-discounts.html

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html

Check out this AWS Billing and Cost Management Cheat Sheet:

https://tutorialsdojo.com/aws-billing-and-cost-management/

Question 15:

Skipped

An insurance company plans to use AWS to visually create, run, and monitor ETL workflows. Which of the following services would you recommend?

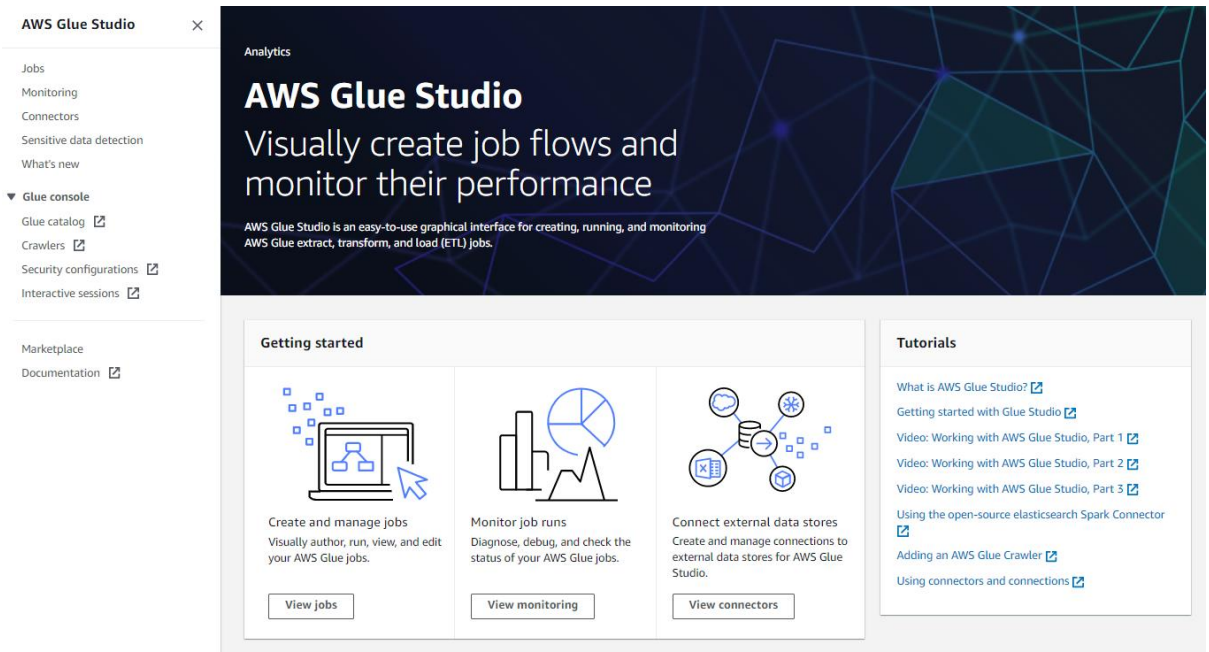
- **AWS Glue Studio**

  (Correct)

- **AWS Storage Gateway**
- **Amazon Athena**
- **Amazon QuickSight Q**

Explanation

AWS Glue is a serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development. AWS Glue provides all the capabilities needed for data integration, so you can start analyzing your data and putting it to use in minutes instead of months. AWS Glue provides both visual and code-based interfaces to make data integration easier.



In AWS Glue, you can visually create, run, and monitor ETL workflows using the feature AWS Glue Studio. You can create data transformation workflows visually and

run them on AWS Glue's Apache Spark-based serverless ETL engine. In addition, you can also inspect the schema and data results at each stage of the job.

You can use AWS Glue Studio to do the following:

- Retrieve data from sources such as Amazon S3, Amazon Kinesis, or JDBC.

- Set up a transformation that merges, samples, or changes the data.

- Designate a destination for the transformed data.

- Examine the schema or preview the dataset during the job process.

- Execute, oversee, and control jobs created in AWS Glue Studio.

Hence, the correct answer is: **AWS Glue Studio.**

Amazon QuickSight Q is incorrect because this is a natural language query feature of QuickSight that allows business users to ask simple questions about their data. It doesn't have the capability to extract, transform, and load (ETL) data.

Amazon Athena is incorrect because this service only analyzes petabytes of data using SQL and saves query results to a file on Amazon S3. Instead of Amazon Athena, use AWS Glue for ETL workflows.

AWS Storage Gateway is incorrect because this is just a hybrid cloud storage solution that allows on-premises applications to access virtually unlimited cloud storage.

References:

https://aws.amazon.com/glue/faqs/

https://docs.aws.amazon.com/glue/latest/ug/what-is-glue-studio.html

Check out this AWS Glue Cheat Sheet:

https://tutorialsdojo.com/aws-glue/

Question 16:

Skipped

Which of the following is the most cost-effective payment option when you purchase either a Standard or Convertible Reserved Instance for a 1-year term?

- **Partial Upfront**
- **All Upfront**

(Correct)

- **No Upfront**
- **Deferred**

Explanation

Reserved Instances provide you with a significant discount compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

Standard Reserved Instances provide you with a significant discount compared to On-Demand instance pricing and can be purchased for a 1-year or 3-year term. The average discount off On-Demand instances varies based on your term and chosen payment options. Customers have the flexibility to change the Availability Zone, the instance size, and networking type of their Standard Reserved Instances.

Convertible Reserved Instances provide you with a significant discount compared to On-Demand Instances and can be purchased for a 1-year or 3-year term. Purchase *Convertible Reserved Instances* if you need additional flexibility, such as the ability to use different instance families, operating systems, or tenancies over the Reserved Instance term.

Characteristic	Standard	Convertible
Terms (avg. discount off On-Demand)	1yr (40%), 3yr (60%)	1yr (31%), 3yr (54%)
Change Availability Zone, instance size (for Linux OS), networking type	Yes (Using ModifyReservedInstances API and console)	Yes (Using ExchangeReservedInstances API and console)
Change instance families, operating system, tenancy, and payment option		Yes
Benefit from Price Reductions		Yes
Sellable on the Reserved Instance Marketplace	Yes (After linking account with a US bank account)	Coming soon

You can choose between three payment options when you purchase a Standard or Convertible Reserved Instance:

All Upfront option: You pay for the entire Reserved Instance term with one upfront payment. This option provides you with the largest discount compared to On-Demand instance pricing.

Partial Upfront option: You make a low upfront payment and are then charged a discounted hourly rate for the instance for the duration of the Reserved Instance term.

No Upfront option: Does not require any upfront payment and provides a discounted hourly rate for the duration of the term.

As a general rule, Standard RI provides more savings than Convertible RI, which means that the former is the cost-effective option. The All Upfront option provides you with the largest discount compared with the other types. Opting for a longer compute reservation, such as the 3-year term, gives us greater discount as opposed to a shorter 1-year renewable term.

Hence, the correct answer is: **All Upfront.**

Partial Upfront is incorrect. Although it is more cost-effective than the No Upfront option, its cost is higher compared with the All Upfront option.

No Upfront is incorrect. Although it does not require any upfront payment and provides a discounted hourly rate for the duration of the term, it still costs higher than both the All Upfront and Partial Upfront options.

Deferred is incorrect because this is not an available option for Reserved Instance pricing.

References:

https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html

Amazon EC2 Overview:

https://youtu.be/7VsGIHT_jQE

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Question 17:

Skipped

Which of the following AWS Cost Management tools enable you to forecast future costs and usage of your AWS resources based on your past consumption?

- **AWS Cost and Usage report**
- **Amazon Forecast**
- **Cost Explorer**

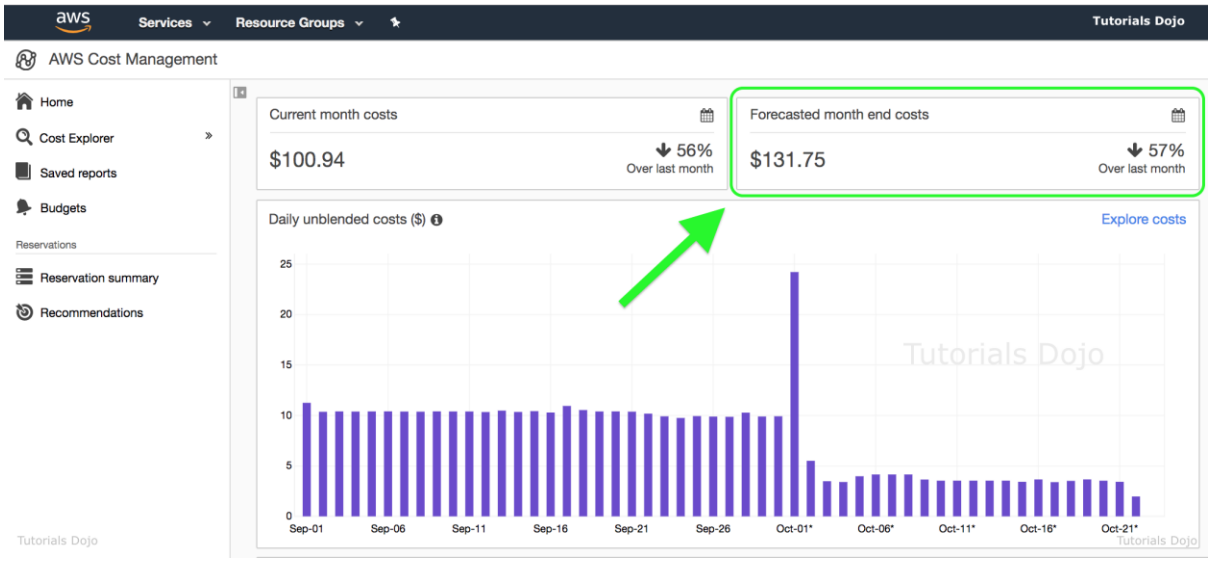
  (Correct)

- **AWS Pricing Calculator**

Explanation

Cost Explorer is a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. You can view data for up to the last 13 months, forecast how much you're likely to spend for the next three months if you set the detail level to at least daily and next twelve months if you set the detail level to at least monthly, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.

A forecast is a prediction of how much you will use AWS services over the forecast time period that you selected, based on your past usage. Forecasting provides an estimate of what your AWS bill will be and enables you to use alarms and budgets for amounts that you're predicted to use. Because forecasts are predictions, the forecasted billing amounts are estimated and might differ from your actual charges for each statement period.



When you first sign up for Cost Explorer, AWS prepares the data about your costs for the current month and the last three months and then calculates the forecast for the next three months or twelve months depending on the level of detail on the forecast (hourly, daily or monthly). The current month's data is available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer updates your cost data at least once every 24 hours. After you sign up, Cost Explorer can display up to 12 months of historical data (if you have that much), the current month, and the forecasted costs for the next three months or twelve months depending on the level of detail on the forecast (hourly, daily or monthly). The first time that you use

Cost Explorer, it walks you through the main parts of the console with an explanation for each section. You can trigger this walkthrough at a later time as well.

Hence, the correct answer is **AWS Cost Explorer**.

AWS Pricing Calculator is incorrect because this tool is used to estimate your AWS bill by manually entering your planned resources by service. It does not forecast future costs and usage of your AWS resources based on your past consumption, unlike the AWS Cost Explorer.

AWS Cost and Usage report is incorrect because this tool doesn't forecast your future costs. It just lists your AWS usage for each service category used by an account and its IAM users in hourly or daily line items, as well as any tags that you have activated for cost allocation purposes.

Amazon Forecast is incorrect because this is actually not considered as one of the AWS Cost Management tools. Amazon Forecast is a fully managed service that uses machine learning to deliver highly accurate forecasts of any time-series data, such as retail demand, manufacturing demand, travel demand, revenue, IT capacity, logistics, and web traffic.

References:

https://aws.amazon.com/aws-cost-management/aws-cost-explorer/

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-forecast.html

Check out this AWS Billing and Cost Management Cheat Sheet:

https://tutorialsdojo.com/aws-billing-and-cost-management/

Question 18:

Skipped

What services will help you create a highly available and scalable web app in the cloud? (Select TWO.)

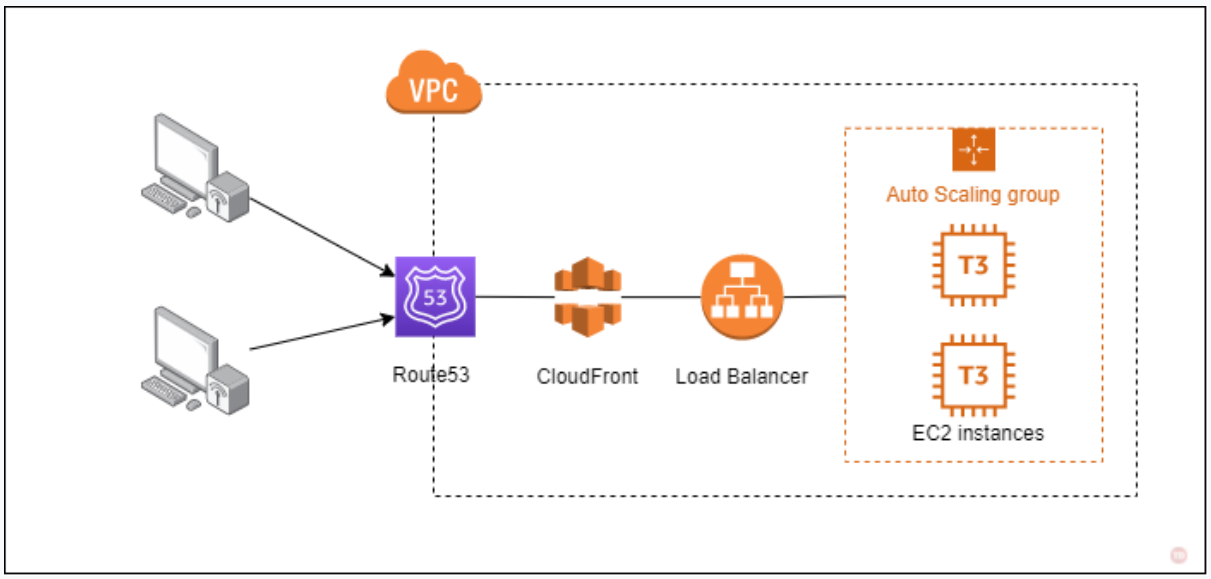
- **Amazon CloudFront**
- **Amazon CloudWatch**
- **AWS ELB**

(Correct)

- **Amazon AppStream 2.0**
- **Amazon EC2 Auto Scaling**

(Correct)

Explanation
The purpose of automatic scaling is to automatically increase the size of your Auto Scaling group when demand goes up and decrease it when demand goes down. As capacity is increased or decreased, the Amazon EC2 instances being added or removed must be registered or deregistered with a load balancer. This enables your application to automatically distribute incoming web traffic across such a dynamically changing number of instances.



Your load balancer acts as a single point of contact for all incoming web traffic to your Auto Scaling group. When an instance is added to your Auto Scaling group, it needs to register with the load balancer, or no traffic is routed to it. When an instance is removed from your Auto Scaling group, it must deregister from the load balancer or traffic continues to be routed to it.

Hence, the correct answers are:

- AWS ELB

- Amazon EC2 Auto Scaling

Amazon CloudWatch and **Amazon CloudFront** are both incorrect because these are not the primary services to be used to achieve a highly available and scalable application in the Cloud.

Amazon AppStream 2.0 is incorrect because this is just a fully managed application streaming service that you can use to centrally manage your desktop applications.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

https://aws.amazon.com/autoscaling/

https://aws.amazon.com/elasticloadbalancing/

Check out these Tutorials Dojo Cheat Sheets:

https://tutorialsdojo.com/aws-elastic-load-balancing-elb/

https://tutorialsdojo.com/aws-auto-scaling/

Question 19:

Skipped

A leading company wants to ensure that its cloud services are consistently delivered at the agreed-upon level of its business stakeholders. The company is considering using the AWS Cloud Adoption Framework (AWS CAF) to guide its cloud operations.

Which capabilities within the AWS CAF's Operations perspective would be most helpful for the company?

- **Performance and Capacity Management**

  (Correct)

- **Modern Application Development**
- **Program and Project Management**
- **Identity and Access Management**

Explanation

AWS Cloud Adoption Framework (CAF) is a comprehensive guide designed to help organizations effectively plan and implement their cloud adoption strategies. The framework addresses the various aspects of cloud adoption from different perspectives, including the business, people, governance, platform, operations, and security.

The **Operations Perspective** within the AWS CAF focuses on managing and maintaining cloud resources and services. It addresses the operational aspects of cloud adoption to ensure that organizations can effectively run their workloads in the cloud while optimizing for performance, cost, security, and reliability.

Performance and capacity management is one of the capabilities of the Operations Perspective. It focuses on optimizing the performance and capacity of cloud resources and services. By implementing performance and capacity management practices, organizations can monitor, analyze, and optimize the performance of their

cloud-based applications and infrastructure. This capability helps ensure that the cloud services meet the agreed-upon service level agreements (SLAs) and performance expectations of the business stakeholders. The following are the other capabilities of the AWS CAF - Operations Perspective:

- Observability

- Event management (AIOps)

- Incident and problem management

- Change and release management

- Performance and capacity management

- Configuration management

- Patch management

- Availability and continuity management

- Application management

Hence the correct answer is: **Performance and Capacity Management.**

Identity and Access Management is incorrect because it only focuses on managing user identities, authentication, and authorization, ensuring that the right individuals access the cloud resources appropriately. Moreover, Identity and access management fall under the security perspective of the AWS CAF.

Modern Application Development is incorrect because it only focuses on cloud applications' development, deployment, and management. Additionally, modern application development is not a foundational capability under the operations perspective of the AWS CAF.

Program and Project Management is incorrect because it just includes the management of the organizational and business aspects of cloud adoption, such as defining goals, aligning stakeholders, and managing budgets and resources. Moreover, the Program and project management fall under the AWS CAF Business perspective.

References:

https://docs.aws.amazon.com/whitepapers/latest/aws-caf-operations-perspective/aws-caf-operations-perspective.html

https://docs.aws.amazon.com/pdfs/whitepapers/latest/overview-aws-cloud-adoption-framework/overview-aws-cloud-adoption-framework.pdf

Question 20:

Skipped

Which AWS service is commonly used for streaming data in real-time?

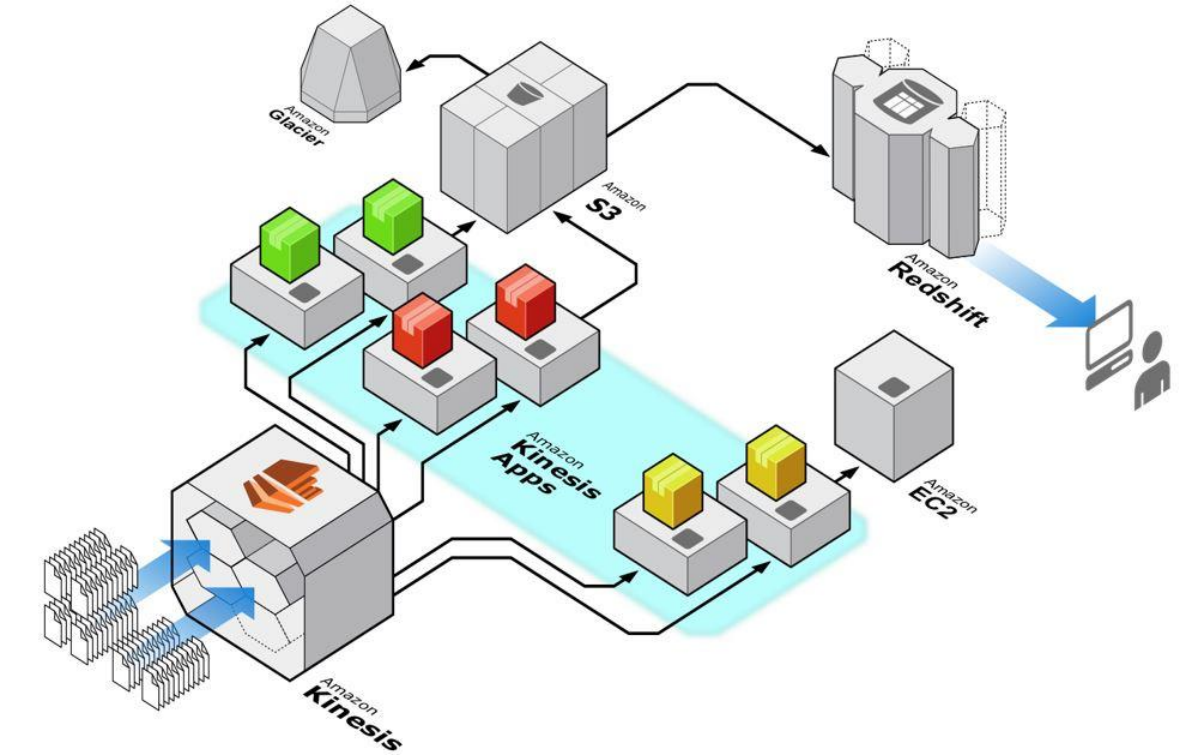
- **Amazon Kinesis**

  (Correct)

- **Amazon OpenSearch Service**
- **Amazon Data Pipeline**
- **Amazon EMR**

Explanation

Amazon Kinesis is the service used to ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and responds instantly instead of having to wait until all your data is collected before the processing can begin.



Kinesis can also handle any amount of streaming data and process data from hundreds of thousands of sources with very low latencies. Lastly, it enables you to ingest, buffer, and process streaming data in real-time, so you can derive insights in seconds or minutes instead of hours or days.

Hence, the correct answer is **Amazon Kinesis.**

Amazon OpenSearch Service is incorrect because this service is mainly used for deploying, operating, and scaling OpenSearch clusters in the AWS cloud.

Amazon EMR is incorrect since this is just a big data service that gives analytical teams the engines and elasticity to run Petabyte-scale analysis for a fraction of the cost of traditional on-premise clusters, using open source Apache tools.

Amazon Data Pipeline is incorrect because this is simply a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals.

References:

https://aws.amazon.com/kinesis/

https://docs.aws.amazon.com/streams/latest/dev/introduction.html

Check out this Amazon Kinesis Cheat Sheet:

https://tutorialsdojo.com/amazon-kinesis/

Question 21:

Skipped

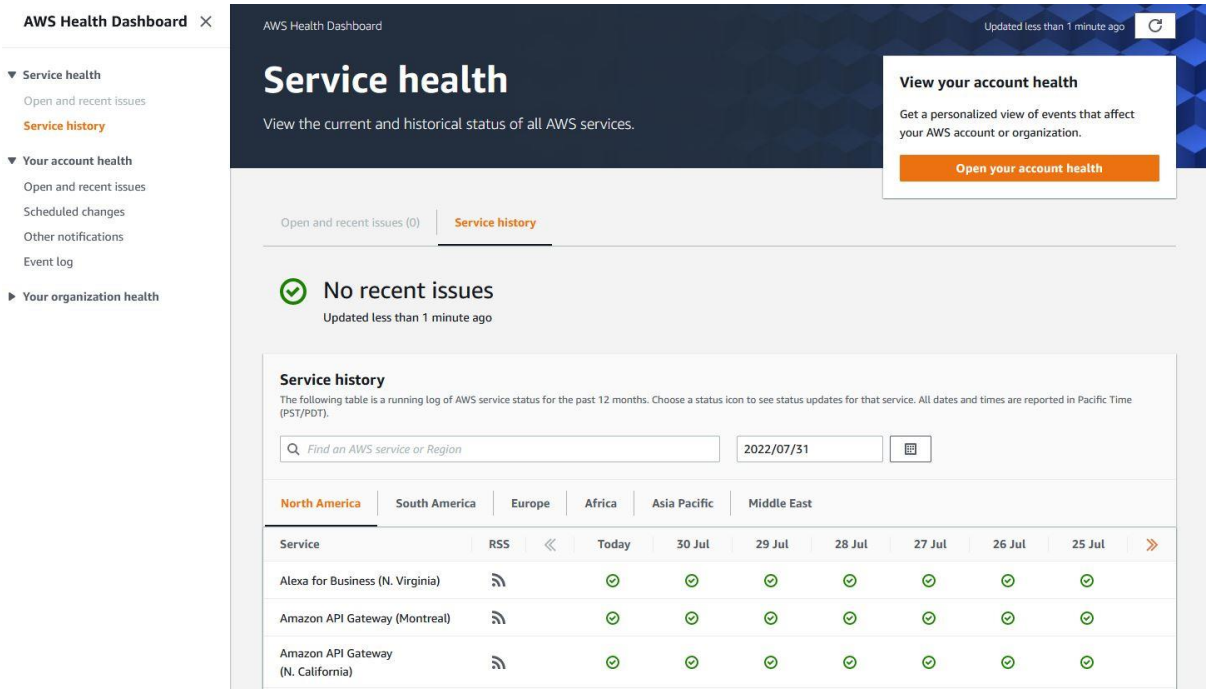
Which service does AWS use to notify you when AWS is experiencing events that may impact you?

- **Amazon CloudWatch**
- **Amazon SNS**
- **AWS Support Center**
- **AWS Health**

(Correct)

Explanation

AWS Health provides ongoing visibility into your resource performance and the availability of your AWS services and accounts. You can use AWS Health *events* to learn how service and resource changes might affect your applications running on AWS. AWS Health provides relevant and timely information to help you manage events in progress. AWS Health also helps you be aware of and to prepare for planned activities. The service delivers alerts and notifications triggered by changes in the health of AWS resources so that you get near-instant event visibility and guidance to help accelerate troubleshooting.



AWS Health Dashboard provides a complete health check of all services in all regions. Health events can help you learn how changes to services and resources may affect your AWS-hosted applications.

Hence, the correct answer is **AWS Health**.

AWS Support Center is incorrect because this is where you can check the support package you are subscribed to, and where you can file cases if you need assistance from the AWS support team. This option is incorrect since it does not provide the information stated in the scenario.

Amazon CloudWatch is incorrect because this collects data across all your AWS resources, applications, and services. Also, AWS does not use this dashboard to notify you of any upcoming changes or system-impactful issues.

Amazon SNS is incorrect because this is simply a messaging service used to deliver push notifications to recipients. This option is incorrect since it is the service used by AWS to notify you of any system-impactful issues.

References:

https://aws.amazon.com/premiumsupport/technology/personal-health-dashboard/

https://docs.aws.amazon.com/health/latest/ug/getting-started-phd.html

Check out this AWS Health Cheat Sheet:

https://tutorialsdojo.com/aws-health/

Question 22:

Skipped

Which of the following is best suited for load balancing Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Transport Layer Security (TLS) traffic and has the capability of handling millions of requests per second while maintaining ultra-low latencies?

- **None of the above**
- **Gateway Load Balancer**
- **Network Load Balancer**

  (Correct)

- **Application Load Balancer**

Explanation

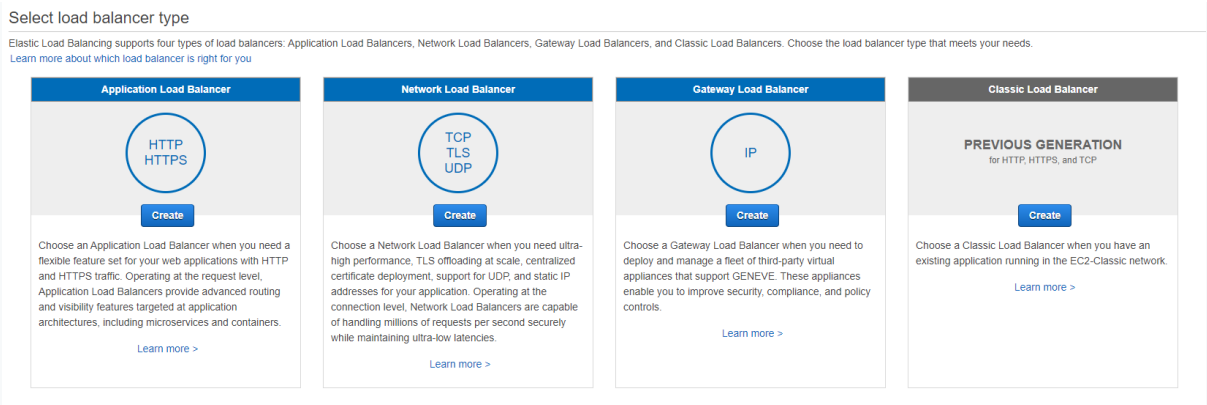
Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones.

Elastic Load Balancing offers four types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault-tolerant. They are:

Application Load Balancer - This is best suited for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers. Operating at the individual request level (Layer 7), Application Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) based on the content of the request.

Network Load Balancer - This is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. Operating at the connection level (Layer 4), Network Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) and is capable of handling millions of requests per second while maintaining ultra-low latencies. Network Load Balancer is also optimized to handle sudden and volatile traffic patterns.

Gateway Load Balancer - This provides both Layer 3 gateway and Layer 4 load balancing capabilities. It is a transparent bump-in-the-wire device that does not change any part of the packet. It is architected to handle millions of requests/second, volatile traffic patterns, and introduces extremely low latency.



The Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. Operating at the connection level (Layer 4), Network Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) and is capable of handling millions of requests per second while maintaining ultra-low latencies. Network Load Balancer is also optimized to handle sudden and volatile traffic patterns.

Hence, the correct type of elastic load balancer to use is the **Network Load Balancer**.

Application Load Balancer is incorrect because it is not suitable for handling TCP, UDP, and TLS traffic.

Gateway Load Balancer is incorrect because this type of load balancer passes all Layer 3 traffic through third-party virtual appliances to its intended targets. It is not designed for what a Network Load Balancer does.

The option that says: **None of the above** is incorrect because this requirement can be fulfilled by using a Network Load Balancer.

References:

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html

https://aws.amazon.com/elasticloadbalancing/features/?nc=sn&loc=2#Product_comparisons

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

https://tutorialsdojo.com/aws-cheat-sheet-aws-elastic-load-balancing-elb/

Application Load Balancer vs Network Load Balancer vs Classic Load Balancer vs Gateway Load Balancer:

https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/

Question 23:

Skipped

In compliance with the Sarbanes-Oxley Act (SOX) federal law, a US-based company is required to provide SOC 1 and SOC 2 reports of their cloud resources. Where are these AWS compliance documents located?

- **AWS Organizations**
- **AWS GovCloud**
- **AWS Artifact**

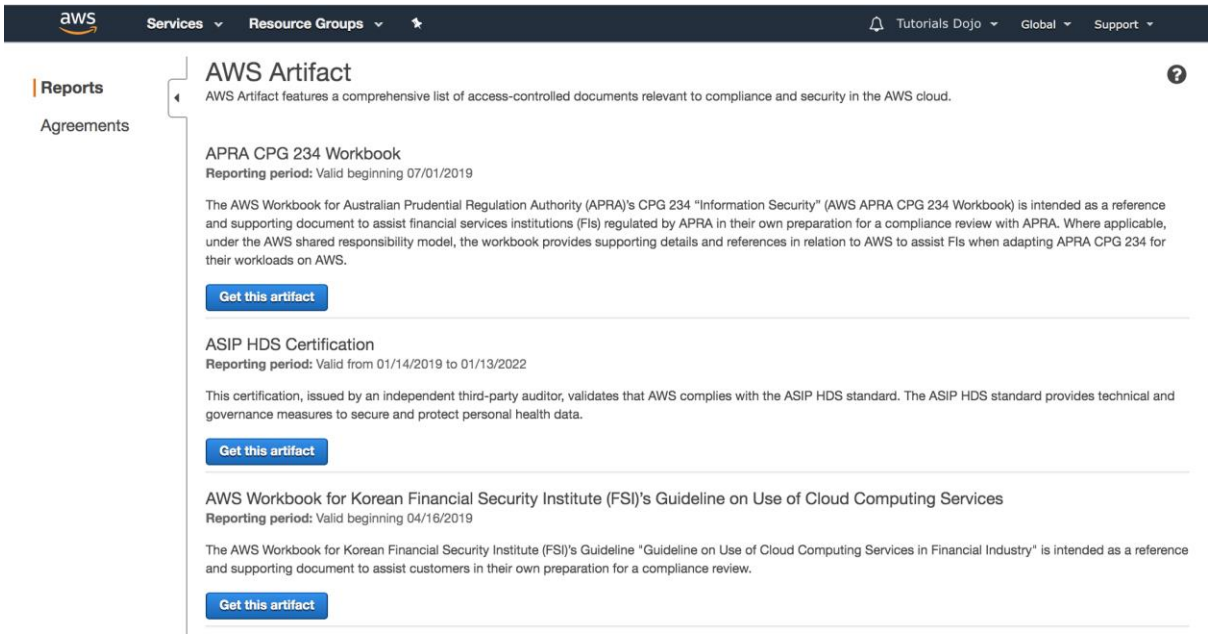
  (Correct)

- **AWS Certificate Manager**

Explanation

The Service Organization Controls (SOC) Reports are used to evaluate the effectiveness of AWS controls that might affect your internal controls over financial reporting (ICOFR). The audit is performed according to the SSAE 18 and ISAE 3402 standards. Many AWS customers use this report as an integral part of their Sarbanes-Oxley (SOX) efforts.

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include 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. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).



All AWS Accounts have access to AWS Artifact. Root users and IAM users with admin permissions can download all audit artifacts available to their account by agreeing to the associated terms and conditions. You will need to grant IAM users with non-admin permissions access to AWS Artifact using IAM permissions. This allows you to grant a user access to AWS Artifact, while restricting access to other services and resources within your AWS Account.

Hence, the correct answer in this scenario is **AWS Artifact**.

AWS GovCloud is incorrect as this is an isolated AWS Region and not a compliance document repository like AWS Artifact, which is designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements.

AWS Organizations is incorrect because this service helps you centrally govern your environment as you grow and scale your workloads in AWS.

AWS Certificate Manager is incorrect because this is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. This service does not store certifications or compliance-related documents.

References:

https://aws.amazon.com/artifact/getting-started/

https://docs.aws.amazon.com/artifact/latest/ug/what-is-aws-artifact.html

AWS Audit and Compliance Services Overview

https://www.youtube.com/watch?v=8wfBDOvrRnY

Check out this AWS Artifact Cheat Sheet:

https://tutorialsdojo.com/aws-artifact/

Question 24:

Skipped

Which of the following should you use to automatically transfer your infrequently accessed data in your S3 bucket to a more cost-effective storage class?

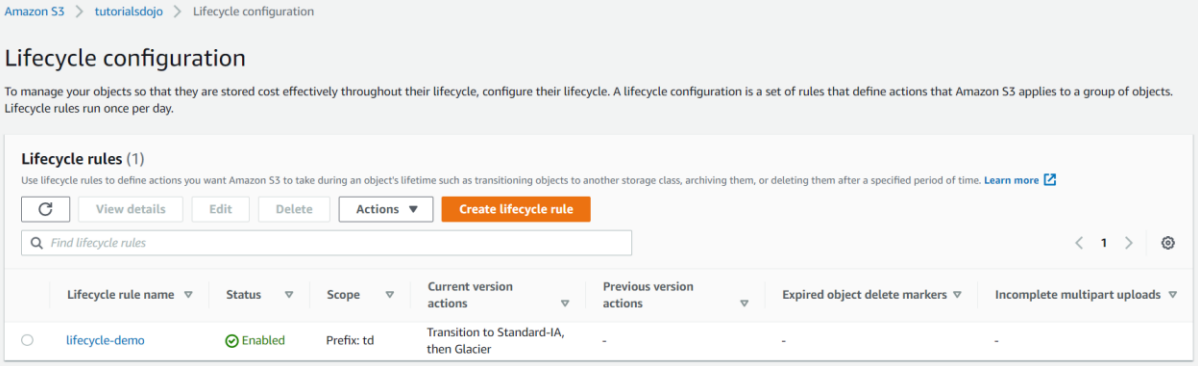
- **Amazon S3 access control list**
- **Amazon S3 Lifecycle Policy**

(Correct)

- **AWS Storage Gateway**
- **AWS Transfer Family**

Explanation

You can use lifecycle policies in S3 to automatically move your infrequently accessed data to a more cost-effective storage class such as S3-IA or Glacier.



Lifecycle configuration in Amazon S3 enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

Transition actions – In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation or archive objects to the GLACIER storage class one year after creation.

Expiration actions – In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Hence, the correct answer is: **Amazon S3 Lifecycle Policy**.

AWS Transfer Family is incorrect because this fully managed service enables you to transfer files over the internet using the FTP, FTPS, SFTP, and HTTP(S) protocols. It does not provide any features for managing S3 storage classes or automatically transitioning objects to different storage classes based on their age or usage patterns.

AWS Storage Gateway is incorrect because this hybrid cloud storage service enables you to integrate your on-premises applications with AWS storage services.

Amazon S3 access control list is incorrect because this only grants permission to objects stored in S3 buckets to specific AWS accounts or IAM users. It does not provide an automated transfer of infrequently accessed data to a more cost-effective storage class.

References:

http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

https://aws.amazon.com/blogs/aws/archive-s3-to-glacier/

Check out this Amazon S3 Cheat Sheet:

https://tutorialsdojo.com/amazon-s3/

Question 25:

Skipped

In AWS, which of the following is a design principle that you should implement when designing your cloud architecture?

- **Utilize free or open-source software**
- **Tightly couple your components**
- **Always use large servers to anticipate increase usage**
- **Use multiple Availability Zones**

(Correct)

Explanation

There are various best practices that you can follow which can help you build an application in the cloud. The notable ones are:

1. Design for failure

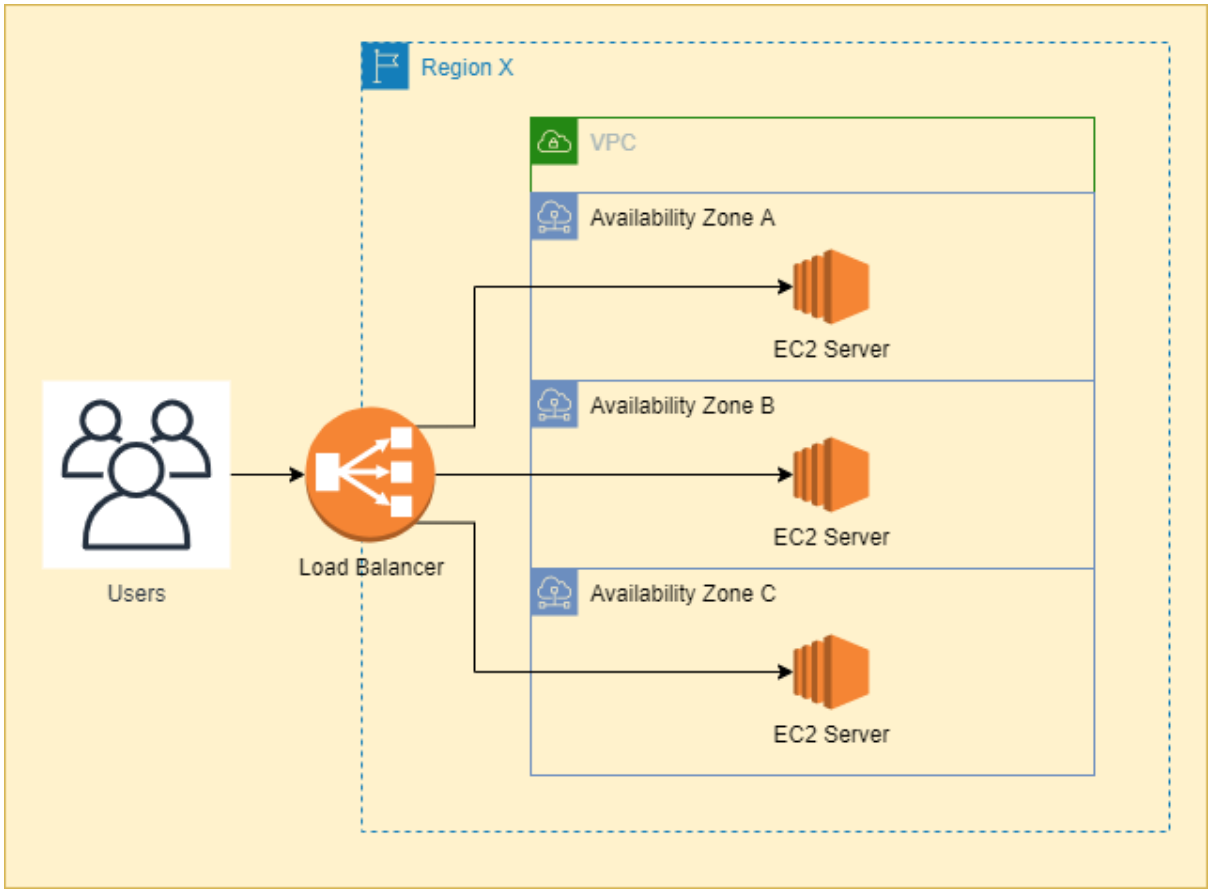
2. Decouple your components

3. Implement elasticity

4. Think parallel

In ***Design for failure***, it encourages you to be a pessimist when designing architectures in the cloud; assume things will fail. In other words, always design, implement, and deploy for automated recovery from failure.

In particular, assume that your hardware will fail. Assume that outages will occur. Assume that some disaster will strike your application. Assume that you will be slammed with more than the expected number of requests per second someday. Assume that with time your application software will fail too. By being a pessimist, you end up thinking about recovery strategies during design time, which helps in designing an overall system better.



Designing with an assumption that underlying hardware will fail, will prepare you for the future when it actually fails. This design principle will help you design operations-friendly applications. If you can extend this principle to pro-actively measure and balance load dynamically, you might be able to deal with variance in network and disk performance that exists due to the multi-tenant nature of the cloud.

AWS specific tactics for implementing this best practice are as follows:

1. Failover gracefully using Elastic IPs: Elastic IP is a static IP that is dynamically re-mappable. You can quickly remap and fail over to another set of servers so that your traffic is routed to the new servers. It works great when you want to upgrade from old to new versions or in case of hardware failures

2. Utilize multiple Availability Zones: Availability Zones are conceptually like logical datacenters. By deploying your architecture to multiple availability zones, you can ensure high availability. Utilize Amazon RDS Multi-AZ deployment functionality to automatically replicate database updates across multiple Availability Zones.

3. Maintain an Amazon Machine Image so that you can restore and clone environments very easily in a different Availability Zone; Maintain multiple Database slaves across Availability Zones and set up hot replication.

4. Utilize Amazon CloudWatch (or various real-time open source monitoring tools) to get more visibility and take appropriate actions in case of hardware failure or performance degradation. Setup an Auto Scaling group to maintain a fixed fleet size so that it replaces unhealthy Amazon EC2 instances with new ones.

5. Utilize Amazon EBS and set up cron jobs so that incremental snapshots are automatically uploaded to Amazon S3 and data is persisted independent of your instances.

6. Utilize Amazon RDS and set the retention period for backups, so that it can perform automated backups.

By focusing on concepts and best practices - like designing for failure, decoupling the application components, understanding and implementing elasticity, combining it with parallelization, and integrating security in every aspect of the application architecture - cloud architects can understand the design considerations necessary for building highly scalable cloud applications.

Hence, the correct answer is: **Use multiple Availability Zones**.

The option that says: **Tightly couple your components** is incorrect because this is exactly the opposite of the "Decouple your components" cloud design principle.

The option that says: **Always use large servers to anticipate increase usage** is incorrect because this action doesn't follow the concept of implementing elasticity to your cloud architecture. In this case, it is better to use Auto Scaling to automatically increase or decrease the number of your servers based on the application demand.

The option that says: **Utilize free or open-source software** is incorrect because this is not considered as one of the cloud design principles nor a best practice.

References:

https://www.slideshare.net/AmazonWebServices/best-practices-for-architecting-in-the-cloud-jeff-barr/9-1_Design_for_Failure_and

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

Check out this AWS Well-Architected Framework – Design Principles Cheat Sheet:

https://tutorialsdojo.com/aws-well-architected-framework-design-principles/

Question 26:

Skipped

Which of the following AWS service enables customers to analyze, investigate, and identify the root cause of potential security issues or suspicious activities in their AWS environment?

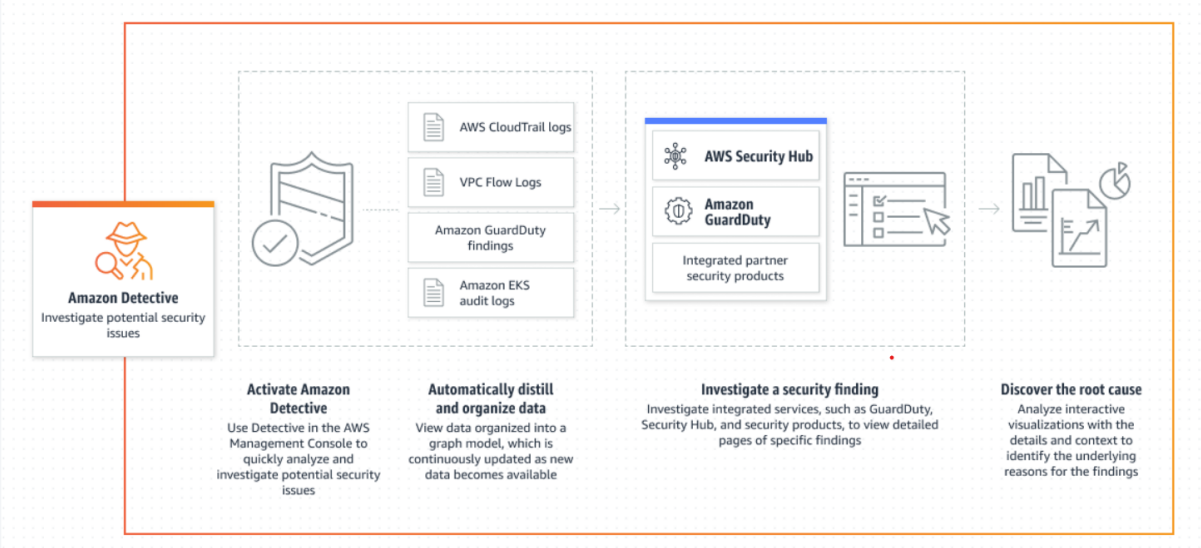
- **AWS Security Hub**
- **Amazon Detective**

(Correct)

- **Amazon GuardDuty**
- **Amazon Inspector**

Explanation

Amazon Detective is an AWS security service that allows you to assess, investigate, and pinpoint the source of suspected security vulnerabilities or suspicious activity in your AWS environment. It builds interactive visualizations and models of the AWS environment using machine learning, statistical analysis, and graph theory, allowing you to quickly and easily identify and investigate security problems. By collecting and analyzing log data from various AWS services, such as VPC Flow Logs, AWS CloudTrail, and Amazon GuardDuty, Amazon Detective allows you to have a comprehensive and centralized view of your AWS environment's security posture.



Amazon Detective automates many of the laborious processes associated with incident investigation and provides you with an easy and interactive interface for exploring and visualizing your data. It allows you to concentrate on the most severe security occurrences while immediately identifying and remediating security flaws. With Amazon Detective, you can improve your overall security posture and maintain compliance with security and privacy regulations by quickly identifying and addressing potential security issues.

Hence the correct answer is: **Amazon Detective.**

Amazon Inspector is incorrect because this service helps you assess and improve the security and compliance of your AWS applications by automatically analyzing application security vulnerabilities and deviations from best practices. Thus, Amazon Inspector is a security service that focuses on application-level security and not on investigating and identifying the root cause of potential security issues or suspicious activities in the AWS environment.

Amazon GuardDuty is incorrect because this threat detection service continuously monitors your AWS accounts and workloads for potential security threats and suspicious activities. It uses machine learning and anomaly detection to identify and alert customers to security issues, such as compromised EC2 instances, unauthorized API calls, and network attacks.

AWS Security Hub is incorrect because this service provides you with a comprehensive view of their security and compliance status across multiple AWS accounts and services. It aggregates and prioritizes security alerts and findings from various AWS services, including Amazon GuardDuty, Amazon Inspector, and AWS Config, and provides centralized visibility into security and compliance issues.

References:

https://docs.aws.amazon.com/detective/latest/userguide/detective-investigation-about.html

https://aws.amazon.com/detective/

Check out this Amazon Detective Cheat Sheet:

https://tutorialsdojo.com/amazon-detective/

Amazon Detective - AWS Cloud Practitioner Exam Topics:

https://youtu.be/2Un8x82sE8U

Question 27:

Skipped

Which of the following are the characteristics of Amazon EC2 Convertible Reserved Instances? (Select TWO.)

- **Has the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value**

  (Correct)

- **Allows the change of instance family, operating system, tenancy, and payment option**

  (Correct)

- **Provides the most significant discount of the RI types and are best suited for steady-state usage**
- **Allows you to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or lesser value**
- **Allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day, a week, or a month**

Explanation

Reserved Instances provide you with a significant discount compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

Convertible Reserved Instances is a type of RI that provides you with a significant discount compared to On-Demand Instances and can be purchased for a 1-year or 3-year term. Purchase *Convertible Reserved Instances* if you need additional flexibility,

such as the ability to use different instance families, operating systems, or tenancies over the Reserved Instance term.

Characteristic	Standard	Convertible
Terms (avg. discount off On-Demand)	1yr (40%), 3yr (60%)	1yr (31%), 3yr (54%)
Change Availability Zone, instance size (for Linux OS), networking type	Yes (Using ModifyReservedInstances API and console)	Yes (Using ExchangeReservedInstances API and console)
Change instance families, operating system, tenancy, and payment option		Yes
Benefit from Price Reductions		Yes
Sellable on the Reserved Instance Marketplace	Yes (After linking account with a US bank account)	Coming soon

With Reserved Instances (RIs), you can choose the type that best fits the needs of your application:

- Standard RIs: Are best suited for steady-state usage.

- Convertible RIs: These provide the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value. Like Standard RIs, Convertible RIs are best suited for steady-state usage.

Hence, the correct answers are:

- Allows the change of instance family, operating system, tenancy, and payment option.

- Has the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value.

The option that says: **Allows you to match your capacity reservation to a predictable recurring schedule that only requires a fraction of a day, a week, or a month** is incorrect because this is a description for Scheduled RIs and not for Convertible RIs.

The option that says: **Allows you to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or lesser value** is incorrect because it should be "equal or greater value" and not "equal or lesser value".

The option that says: **Provides the most significant discount of the RI types and are best suited for steady-state usage** is incorrect because this describes Standard RIs and not Convertible RIs.

References:

https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Amazon EC2 Overview:

https://youtu.be/7VsGIHT_jQE

Question 28:

Skipped

Which of the following is not required when launching an EBS-backed EC2 instance?

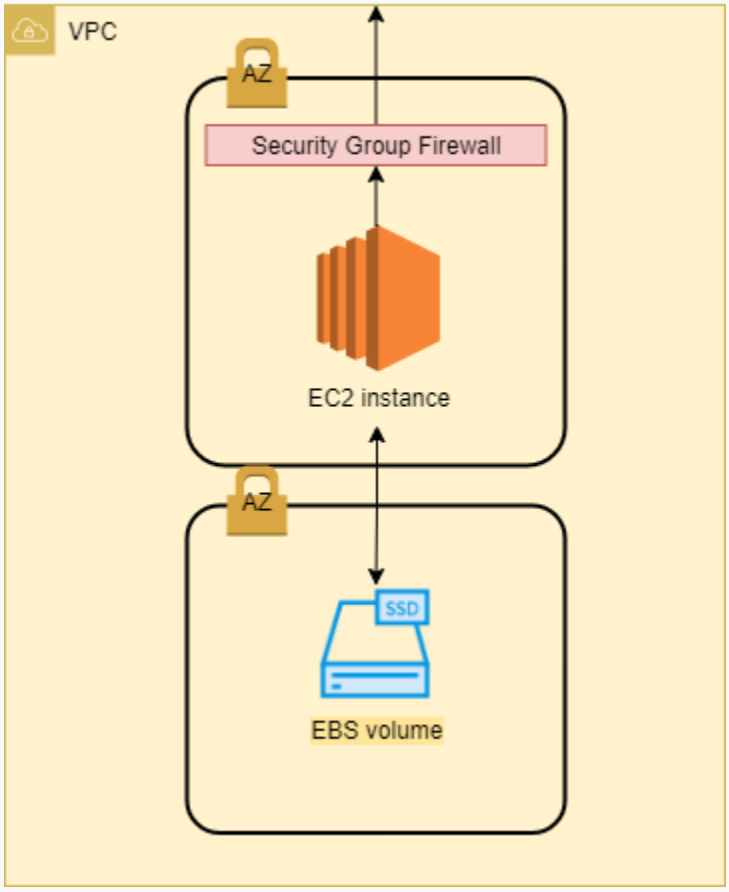
- **EBS Root volume**
- **Security group**
- **VPC and subnet specification**
- **Elastic IP address**

(Correct)

Explanation

Instances that use Amazon EBS for the root device automatically have an Amazon EBS volume attached. When you launch an Amazon EBS-backed instance, we create an Amazon EBS volume for each Amazon EBS snapshot referenced by the AMI you use. You can optionally use other Amazon EBS volumes or instance store volumes, depending on the instance type.

An Amazon EBS-backed instance can be stopped and later restarted without affecting data stored in the attached volumes. There are various instance/volume-related tasks you can do when an Amazon EBS-backed instance is in a stopped state. For example, you can modify the properties of the instance, change its size, or update the kernel it is using, or you can attach your root volume to a different running instance for debugging or any other purpose.



When launching an EC2 instance, you are not required to provide an Elastic IP address. If the instance is a public web server, then you can optionally choose to have an AWS-provided public IP address assigned to it. This IP address will depend on the setting of the subnet where you launched the instance.

Hence, the correct answer is: **Elastic IP address.**

Security group, EBS Root volume, and **VPC and subnet specification** are all required when launching an EC2 instance.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Amazon EC2 Overview:

https://youtu.be/7VsGIHT_jQE

Question 29:

Skipped

You are permitted to conduct security assessments and penetration testing without prior approval against which AWS resources? (Select TWO.)

- **Amazon S3**
- **Amazon Aurora**

  (Correct)

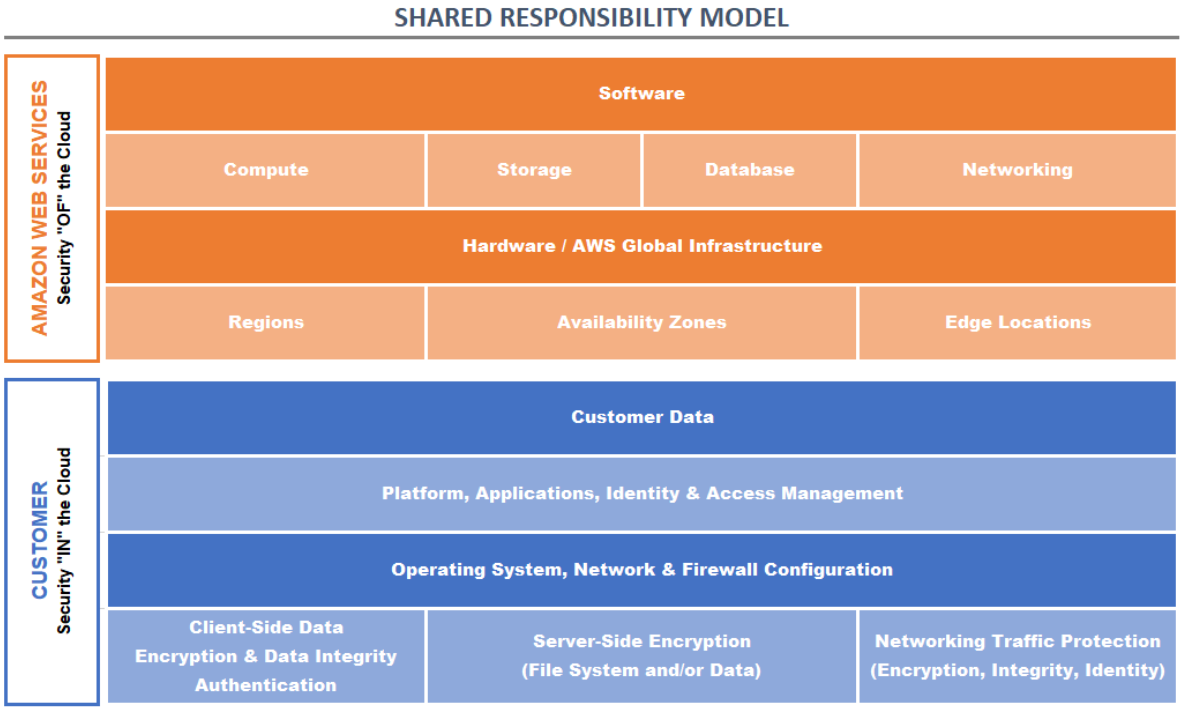
- **Amazon RDS**

  (Correct)

- **AWS Security Token Service (STS)**
- **AWS Identity and Access Management (IAM)**

Explanation

Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. An advantage of the AWS cloud is that it allows customers to scale and innovate while maintaining a secure environment. Customers pay only for the services they use, meaning that you can have the security you need, but without the upfront expenses, and at a lower cost than in an on-premises environment.



AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval to a few services only.

Permitted Services – You're welcome to conduct security assessments against AWS resources that you own if they make use of the services listed below. Take note that AWS is constantly updating this list:

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers

- Amazon RDS

- Amazon CloudFront

- Amazon Aurora

- Amazon API Gateways

- AWS Lambda and Lambda Edge functions

- Amazon Lightsail resources

- Amazon Elastic Beanstalk environments

Prohibited Activities – The following activities are prohibited at this time:

- DNS zone walking via Amazon Route 53 Hosted Zones

- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS

- Port flooding

- Protocol flooding

- Request flooding (login request flooding, API request flooding)

Hence, the correct answers are:

- Amazon RDS

- Amazon Aurora

All other options are incorrect since they are not included in the list shown above.

- Amazon S3

- AWS Identity and Access Management (IAM)

- AWS Security Token Service (STS)

References:

https://aws.amazon.com/security/

https://aws.amazon.com/security/penetration-testing/

https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/

Amazon Aurora Overview:

https://youtu.be/iwS1h7rLNBQ

Check out these Amazon RDS and Aurora Cheat Sheets:

https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/

https://tutorialsdojo.com/amazon-aurora/

Question 30:

Skipped

Which of the following policies grant the necessary permissions required to access your Amazon S3 resources? (Select TWO.)

- **Object policies**
- **Routing policies**

- **Network access control policies**
- **User policies**

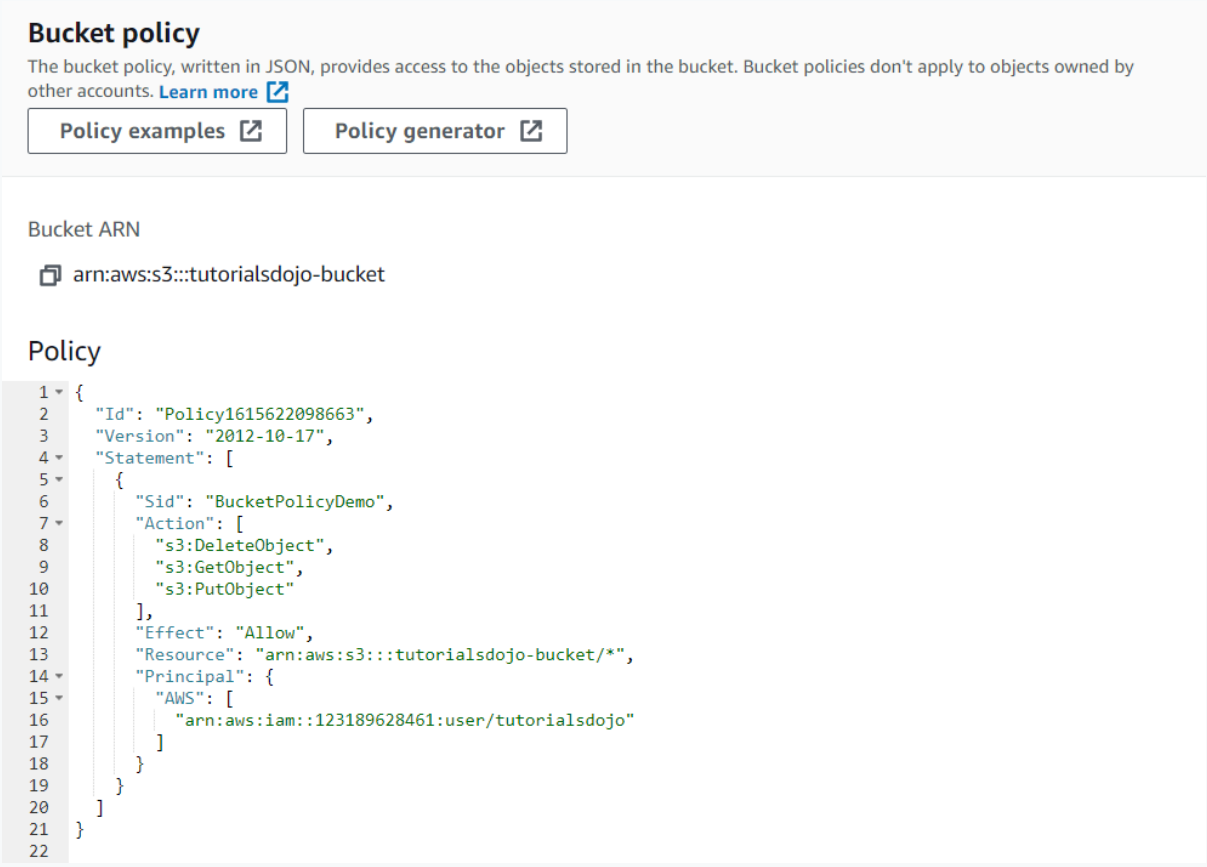
(Correct)

- **Bucket policies**

(Correct)

Explanation

When granting permissions, you decide who is getting them, which Amazon S3 resources they are getting permissions for, and specific actions you want to allow on those resources. Buckets and objects are Amazon S3 resources. By default, only the resource owner can access these resources. The resource owner refers to the AWS account that creates the resource.



Bucket policy and **user policy** are two of the access policy options available for you to grant permission to your Amazon S3 resources. Both use JSON-based access policy language. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. User policies are policies that allow an IAM user access to one of your buckets.

Hence, the correct answers are:

- Bucket policies

- User policies

All the other options are incorrect as these are not the correct features that will grant permissions to your Amazon S3 bucket.

- **Routing policies**

- Network access control policies

- Object policies

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html

https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/

Check out this Amazon S3 Cheat Sheet:

https://tutorialsdojo.com/amazon-s3/

Question 31:

Skipped

Which of the following is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using appliances with on-board storage and compute capabilities?

- **AWS Snowball Edge**

  (Correct)

- **Lambda@Edge**
- **AWS Snowcone**
- **AWS Snowmobile**

Explanation

AWS Snowball Edge is a data migration and edge computing device that comes in two options. Snowball Edge Storage Optimized provides both block storage and Amazon S3-compatible object storage and 24 vCPUs. It is well suited for local storage and large-scale data transfer. Snowball Edge Compute Optimized provides 52 vCPUs, block and object storage, and an optional GPU for use cases such as advanced machine learning and full-motion video analysis in disconnected environments. Customers can use these two options for data collection, machine learning and processing, and storage in environments with intermittent connectivity (such as manufacturing, industrial, and transportation) or in extremely remote locations (such as military or maritime operations) before shipping it back to AWS.

These devices may also be rack mounted and clustered together to build larger, temporary installations.

Snowball Edge supports specific Amazon EC2 instance types as well as AWS Lambda functions, so customers may develop and test in AWS and then deploy applications on devices in remote locations to collect, pre-process, and return the data. Common use cases include data migration, data transport, image collation, IoT sensor stream capture, and machine learning.

Hence, the correct answer is **AWS Snowball Edge.**

AWS Snowmobile is incorrect because this is primarily used to migrate tens of petabytes to exabytes of data in batches to the cloud.

AWS Snowcone is incorrect. Although it is a data transport solution like Snowball Edge, it is not suitable for moving terabytes to petabytes of data. Take note that the usable storage for Snowcone is only 8 TB.

Lambda@Edge is incorrect because this is just a feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency.

References:

https://aws.amazon.com/snowball-edge

https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html

https://docs.aws.amazon.com/snowball/latest/developer-guide/device-differences.html

Check out this AWS Snowball Edge Cheat Sheet:

https://tutorialsdojo.com/aws-snowball-edge/

AWS Snow Family Overview:

https://youtu.be/9Ar-51Ip53Q

Question 32:

Skipped

Which of the following is one of the benefits of migrating your systems from an on-premises data center to AWS Cloud?

- **Completely eliminates the administrative overhead of patching the guest operating system of their EC2 instances**
- **Eliminates the need for the customer to implement client-side or service-side encryption for their data**
- **Enables the customer to focus on business activities rather than on the heavy lifting of racking, stacking, and powering servers**

(Correct)

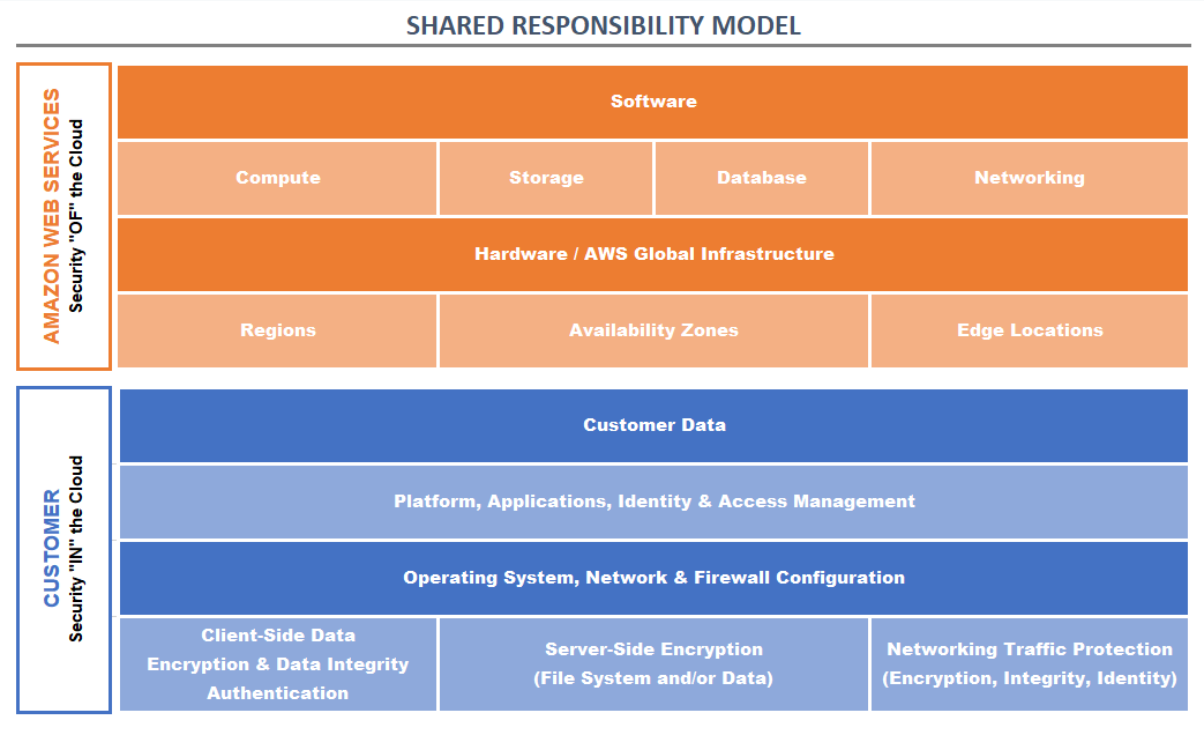
- **Enables the customer to eliminate high IT infrastructure costs since cloud computing is absolutely free**

Explanation

Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources via the internet with pay-as-you-go pricing.

Whether you are using it to run applications that share photos to millions of mobile users or to support business-critical operations, a cloud services platform provides rapid access to flexible and low-cost IT resources. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right

type and size of computing resources you need to power your newest idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use.



There are six advantages of using Cloud Computing:

1. Trade capital expense for variable expense

– Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can pay only when you consume computing resources, and pay only for how much you consume.

2. Benefit from massive economies of scale

– By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay-as-you-go prices.

3. Stop guessing capacity

– Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little capacity as you need, and scale up and down as required with only a few minutes' notice.

4. Increase speed and agility

– In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization since the cost and time it takes to experiment and develop is significantly lower.

5. Stop spending money running and maintaining data centers

– Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers.

6. Go global in minutes

– Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at a minimal cost.

Hence, the correct answer is: **Enables the customer to focus on business activities rather than on the heavy lifting of racking, stacking, and powering servers.**

The option that says: **Enables the customer to eliminate high IT infrastructure costs since cloud computing is absolutely free** is incorrect. Although it is true that cloud computing can lessen or eliminate exorbitant IT infrastructure costs, the customers will still be charged based on their usage in AWS. You can opt to use the AWS Free Tier (which has limited capabilities) for testing but this is not considered a benefit of using AWS over your traditional data center.

The option that says: **Completely eliminate the administrative overhead of patching the guest operating system of their EC2 instances** is incorrect because based on the Shared Responsibility Model, the customer is the one responsible for patching the guest OS while AWS is responsible for the underlying host OS of the EC2 instance.

The option that says: **Eliminates the need for the customer to implement client-side or service-side encryption for their data** is incorrect because based on the Shared Responsibility Model, the customer is responsible for applying the encryption of their data.

References:

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

https://d1.awsstatic.com/whitepapers/aws-overview.pdf

Tutorials Dojo's AWS Certified Cloud Practitioner Exam Study Guide:

https://tutorialsdojo.com/aws-certified-cloud-practitioner/

Question 33:

Skipped

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

- **Performance Efficiency**

  (Correct)

- **High Availability**
- **Agility**
- **Sustainability**

  (Correct)

- **Scalability**

Explanation

The Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. This is based on six pillars namely:

1. Operational Excellence

2. Security

3. Reliability

4. Performance Efficiency

5. Cost Optimization

6. Sustainability

This framework provides a consistent approach for customers and partners to evaluate architectures and implement designs that will scale over time.

The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using this Framework, you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement. The process for reviewing an architecture is a constructive conversation about architectural decisions and is not an audit mechanism. Having well-architected systems greatly increases the likelihood of business success.

AWS Solutions Architects have years of experience architecting solutions across a wide variety of business verticals and use cases. AWS has helped design and review thousands of customers' architectures on AWS. From this experience, AWS has identified best practices and core strategies for architecting systems in the cloud that you can also implement.

You can also use the AWS Well-Architected Tool; it helps you review the state of your workloads and compares them to the latest AWS architectural best practices. The tool is based on the AWS Well-Architected Framework, developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructure.

Hence, the correct answers are:

- Sustainability

- **Performance Efficiency**

High Availability, **Scalability**, and **Agility** are all incorrect because these are not part of the 6 AWS Well-Architected Framework pillars.

References:

https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html

https://aws.amazon.com/architecture/well-architected/

AWS Well-Architected Framework - Six Pillars Cheat Sheet:

https://tutorialsdojo.com/aws-well-architected-framework-five-pillars

Question 34:

Skipped

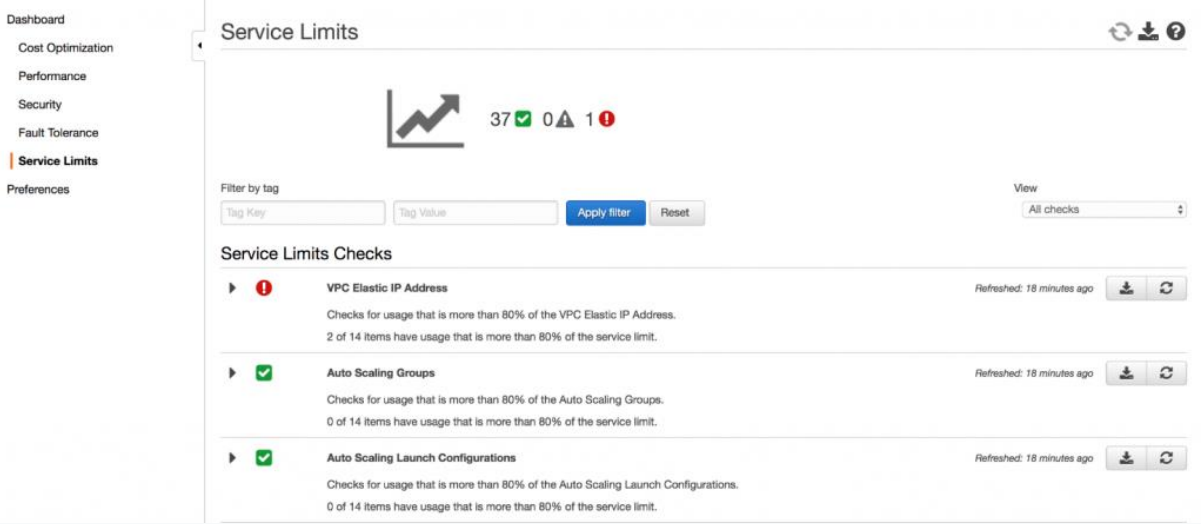
A new AWS customer needs to deploy up to 100 t3a.large EC2 instances on their recently launched VPC, which is way beyond the default service limit. What should they do so they can launch their additional instances?

- **Use AWS Trusted Advisor to increase the default service limits for EC2 instances.**
- **Enable Enhanced Networking.**
- **Do nothing. You can directly launch 100 t3a.large EC2 instances at the same time since AWS will automatically increase your service limit for you.**
- **Create a case in the AWS Support Center page and request a service limit increase.**

(Correct)

Explanation

AWS maintains service limits for each account to help guarantee the availability of AWS resources, as well as to minimize billing risks for new customers. Some service limits are raised automatically over time as you use AWS, though most AWS services require that you request limit increases manually.



By default, there is an imposed limit in launching EC2 instances in your VPC. These increases are not granted immediately, so it may take a couple of days for your increase to become effective. On-Demand Instance limits are managed in terms of the *number of virtual central processing units (vCPUs)* that your running On-Demand Instances are using, regardless of the instance type. Then for each Region, you can purchase 20 regional Reserved Instances per month plus an additional 20 zonal Reserved Instances per month for each Availability Zone.

To request a limit increase:

1. Open the AWS Support Center page, sign in if necessary, and choose: Create case.

2. For the "Regarding" field, choose: *Service Limit Increase*.

3. Complete the form. If this request is urgent, choose *Phone* as the method of contact instead of *Web*.

4. Choose Submit.

Hence, the correct answer is: **Create a case in the AWS Support Center page and request a service limit increase**.

The option that says: **Enable Enhanced Networking** is incorrect because this has nothing to do with service limits.

The option that says: **Use AWS Trusted Advisor to increase the default service limits for EC2 instances** is incorrect because you can't use AWS Trusted Advisor to increase your service limit. You have to raise a request to the AWS Support Center instead.

The option that says: **Do nothing. You can directly launch 100 t3a.large EC2 instances at the same time since AWS will automatically increase your service limit for you** is incorrect because AWS doesn't do this for you. It is your responsibility to raise a request to increase your service limit as this is not automatically done by AWS.

References:

https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html

https://aws.amazon.com/premiumsupport/knowledge-center/manage-service-limits/

https://aws.amazon.com/ec2/faqs/#how-many-instances-ec2

Tutorials Dojo's AWS Certified Cloud Practitioner Exam Study Guide:

https://tutorialsdojo.com/aws-certified-cloud-practitioner/

Question 35:

Skipped

Which of the following tasks fall under the sole responsibility of AWS based on the shared responsibility model?

- **Patch Management**
- **Implementing IAM policies**
- **Applying Amazon S3 bucket policies**
- **Physical and environmental controls**

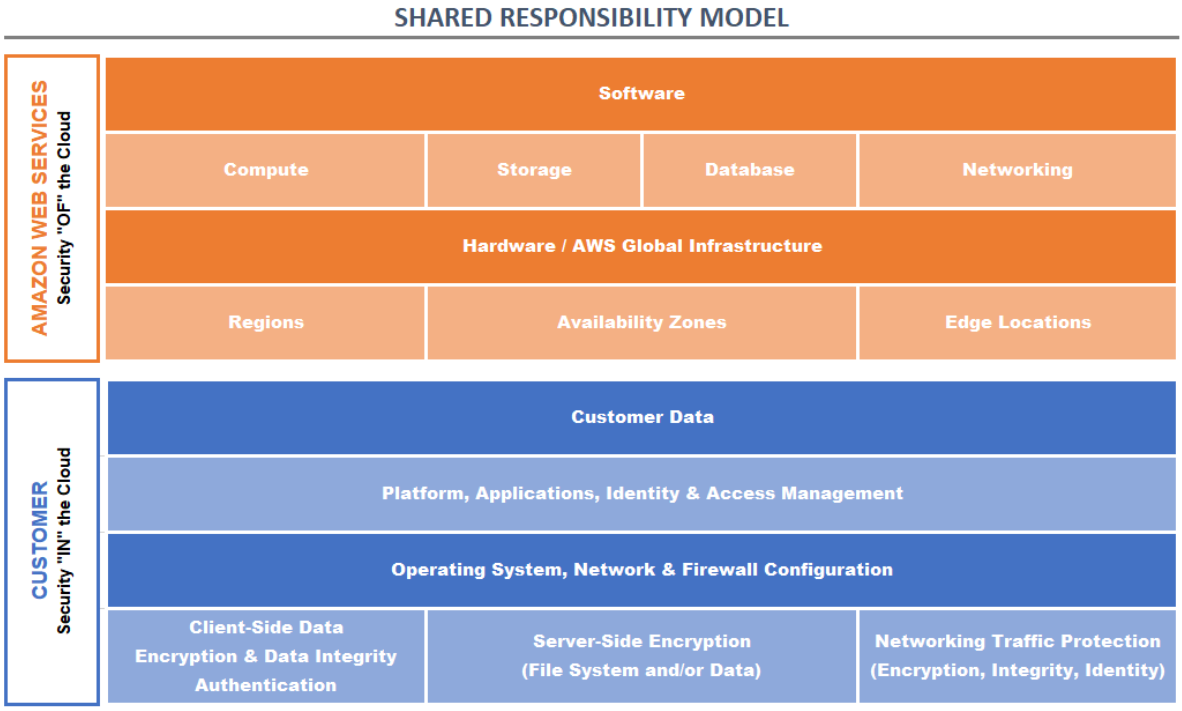
(Correct)

Explanation

Security and Compliance are a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security **OF** the Cloud versus Security **IN** the Cloud.



This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation, and verification of IT controls shared. AWS can help relieve the customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment.

Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required. Below are examples of controls that are managed by AWS, AWS Customers, and/or both.

Inherited Controls: Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

Shared Controls: Controls that apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services.

Examples include:

- Patch Management: AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

- Configuration Management: AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

- Awareness & Training: AWS trains AWS employees, but a customer must train their own employees.

Customer Specific: Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services.

Examples include:

- Service and Communications Protection or Zone Security may require a customer to route or zone data within specific security environments.

Hence, the correct answer is: **Physical and environmental controls**.

Implementing IAM policies and **Applying Amazon S3 bucket policies** are both incorrect because these are the responsibilities of the customer and not AWS.

Patch Management is incorrect because this is actually a shared control between AWS and the customer.

References:

https://aws.amazon.com/compliance/shared-responsibility-model/

https://d1.awsstatic.com/Marketplace/scenarios/security/SEC_02_TSB_Final.pdf

https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

Tutorials Dojo's AWS Certified Cloud Practitioner Exam Study Guide:

https://tutorialsdojo.com/aws-certified-cloud-practitioner/

Question 36:

Skipped

Which of the following is typically used to secure your VPC subnets?

- **AWS Config**
- **AWS IAM**

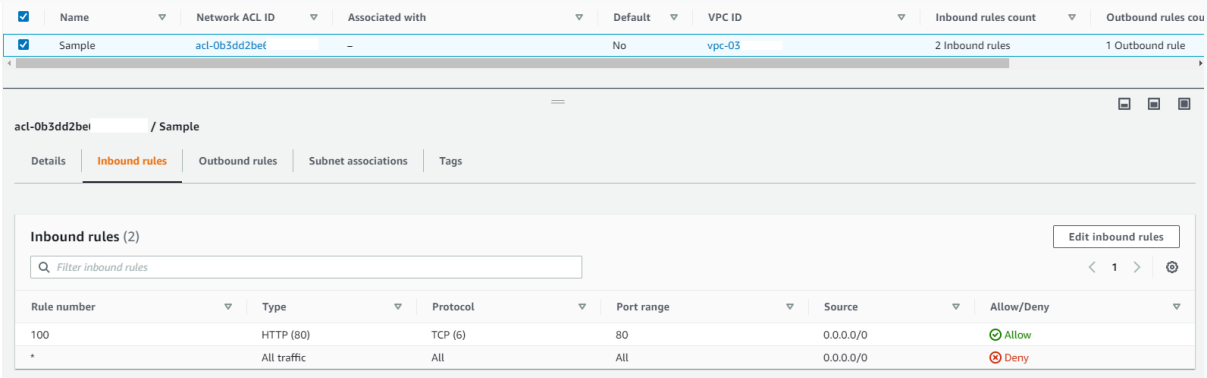
- **Network ACL**

(Correct)

- **Security Group**

Explanation

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



A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Hence, the correct answer is: **Network ACL.**

Security group is incorrect because this is used to secure your resource-level network such as EC2 instances and RDS databases, in a similar way with how network ACLs work. However, security groups do not operate on the subnet level.

AWS IAM is incorrect because it is a service used for account, user, and access management.

AWS Config is incorrect because it is a tool that checks for resource compliance in your account.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

https://aws.amazon.com/vpc/faqs/

Check out this Amazon VPC Cheat Sheet:

https://tutorialsdojo.com/amazon-vpc/

Question 37:

Skipped

In Amazon EC2, which pricing construct adjusts its price based on supply and demand of EC2 instances?

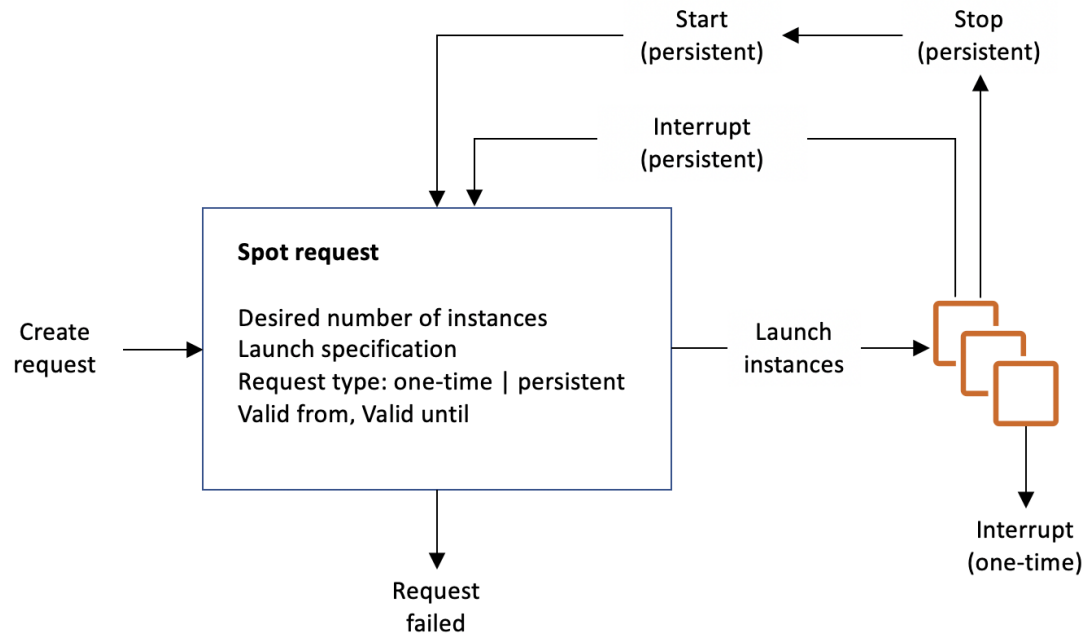
- **On-Demand Instance**
- **Standard Reserved Instance**
- **Convertible Reserved Instance**
- **Spot Instance**

(Correct)

Explanation

Amazon simplified the Amazon EC2 Spot instance pricing by moving to a model that delivers low, predictable prices that adjust gradually based on long-term trends in supply and demand. You will continue to save up to 90% off the On-Demand instance price, and you will continue to pay the Spot price that's in effect at the beginning of each instance hour for your running instance.

Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices. It can be interrupted by AWS EC2 with two minutes of notification when the service takes the capacity back.



To use Spot Instances, you create a Spot Instance request that includes the number of instances, the instance type, the Availability Zone, and the maximum price that you are willing to pay per instance hour. If your maximum price exceeds the current Spot price, Amazon EC2 fulfills your request immediately if capacity is available. Otherwise, Amazon EC2 waits until your request can be fulfilled or until you cancel the request.

Hence, the correct answer is: **Spot Instance.**

Standard Reserved Instance and Convertible Reserved Instance are both incorrect because these are types of Reserved Instance purchase options. This provides a capacity reservation that gives you additional confidence in your ability to launch instances when you need them.

On-Demand Instance is incorrect as this is the type where you pay for compute capacity by the hour or the second, depending on which instances you run.

References:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html

https://aws.amazon.com/ec2/pricing/

https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-ec2-spot-introduces-new-pricing-model-and-the-ability-to-launch-new-spot-instances-via-runinstances-api/

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Amazon EC2 Overview:

https://youtu.be/7VsGIHT_jQE

Question 38:

Skipped

Which of the following actions will AWS charge you for?

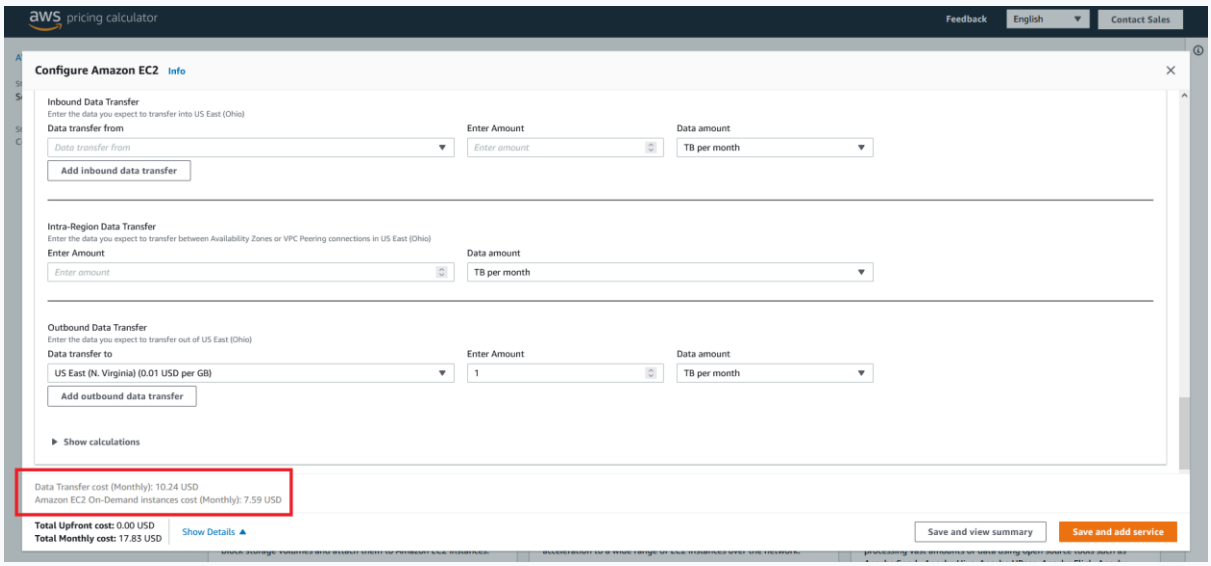
- **Provisioning elastic IPs and attaching them to running EC2 instances**
- **Transfer of EC2 files between two AWS Regions**

(Correct)

- **Network charges for the transfer of data from your data center to S3 through a VPN**
- **Setting up additional VPCs in your account**

Explanation

AWS Pricing Calculator is a web-based planning tool that you can use to create estimates for your AWS use cases. You can use it to model your solutions before building them, explore the AWS service price points, and review the calculations behind your estimates. You can use it to help you plan your spending, find cost-saving opportunities, and make informed decisions using Amazon Web Services.



AWS charges you for data transferred between two different Regions. This is similar to the costs incurred from the data transfer between the AWS network and the public internet.

Hence, the correct answer is: **Transfer of EC2 files between two AWS Regions.**

The option that says: **Network charges for the transfer of data from your data center to S3 through a VPN** is incorrect because the data coming in from your data center to AWS does not incur you charges.

The option that says: **Provisioning Elastic IPs and attaching them to running EC2 instances** is incorrect because Elastic IPs are only charged if they are not attached to running instances.

The option that says: **Setting up additional VPCs in your account** is incorrect because VPCs are free to use in AWS.

Reference:

https://calculator.aws/#/

https://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf

Check out this AWS Pricing Cheat Sheet:

https://tutorialsdojo.com/aws-pricing/

Question 39:

Skipped

Which of the following is used to enable instances in the public subnet to connect to the public Internet?

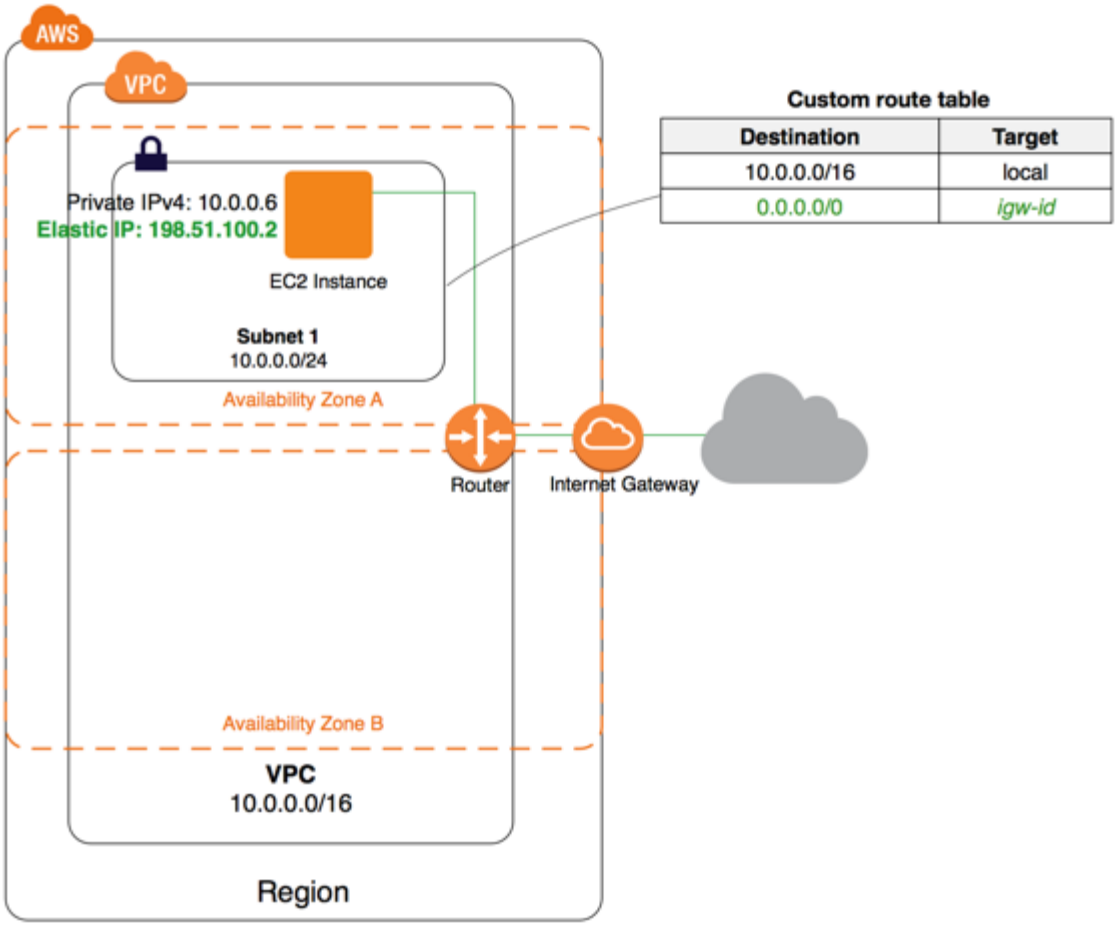
- **API Gateway**
- **NAT instance**
- **Internet Gateway**

  (Correct)

- **NAT Gateway**

Explanation

An **Internet gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.



To enable communication over the internet for IPv4, your instance must have a public IPv4 address or an Elastic IP address that's associated with a private IPv4 address on your instance. Your instance is only aware of the private (internal) IP address space defined within the VPC and subnet.

The Internet gateway logically provides the one-to-one NAT on behalf of your instance, so that when traffic leaves your VPC subnet and goes to the Internet, the reply address field is set to the public IPv4 address or Elastic IP address of your instance, and not its private IP address. Conversely, traffic that's destined for the public IPv4 address or Elastic IP address of your instance has its destination address translated into the instance's private IPv4 address before the traffic is delivered to the VPC.

Hence, the correct answer is: **Internet Gateway**.

Both **NAT Gateways** and **NAT Instances** are incorrect because these are simply used to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating connections with the instances.

API Gateway is incorrect since this is a service meant for creating, publishing, maintaining, monitoring, and securing APIs.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html

Check out this Amazon VPC Cheat Sheet:

https://tutorialsdojo.com/amazon-vpc/

Amazon VPC Overview:

https://www.youtube.com/watch?v=oIDHKeNxvQQ

Question 40:

Skipped

A customer in North Virginia, USA is doing some drone work and collecting environmental data. Which of the following services allows him to easily obtain terabytes of data storage for use in a space-constrained environment and allows him to transfer these data to AWS?

- **AWS Data Pipeline**
- **AWS Transit Gateway**
- **AWS Snowmobile**
- **AWS Snowcone**

(Correct)

Explanation

AWS Snowcone is the smallest member of the AWS Snow Family of edge computing, edge storage, and data transfer devices, weighing in at 4.5 pounds (2.1 kg) with 8 terabytes of usable storage. Snowcone is ruggedized, secure, and purpose-built for use outside of a traditional data center. Its small form factor makes it a perfect fit for tight spaces or where portability is a necessity and network connectivity is unreliable.

You can use Snowcone in backpacks on first responders, or for IoT, vehicular, and drone use cases. You can execute compute applications at the edge, and you can ship the device with data to AWS for offline data transfer, or you can transfer data online with AWS DataSync from edge locations. Snowcone is designed for data migration needs up to 8 terabytes per device and from space-constrained environments where AWS Snowball devices will not fit.

Hence, the correct answer is **AWS Snowcone.**

Amazon Data Pipeline is incorrect since this service does not offer an easy solution for providing data storage in outdoor locations and transporting terabyte-scale data to AWS.

AWS Snowmobile is incorrect. Although this service can transfer up to 100PB, you cannot use this service in a space-constrained environment. The AWS Snowcone is a better alternative in this circumstance because it is an ultra-portable data transfer and edge computing device that you can bring anywhere.

AWS Transit Gateway is incorrect since this is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway.

References:

https://aws.amazon.com/snowcone/

https://docs.aws.amazon.com/snowball/latest/snowcone-guide/snowcone-what-is-snowcone.html

AWS Snow Family Video Tutorial:

https://youtu.be/9Ar-51Ip53Q

Question 41:

Skipped

Which is a fully-managed source control service that allows you to host Git-based repositories and enable code collaboration for your team via pull requests, branching, and merging?

- **AWS CodeStar**
- **AWS CodeCommit**

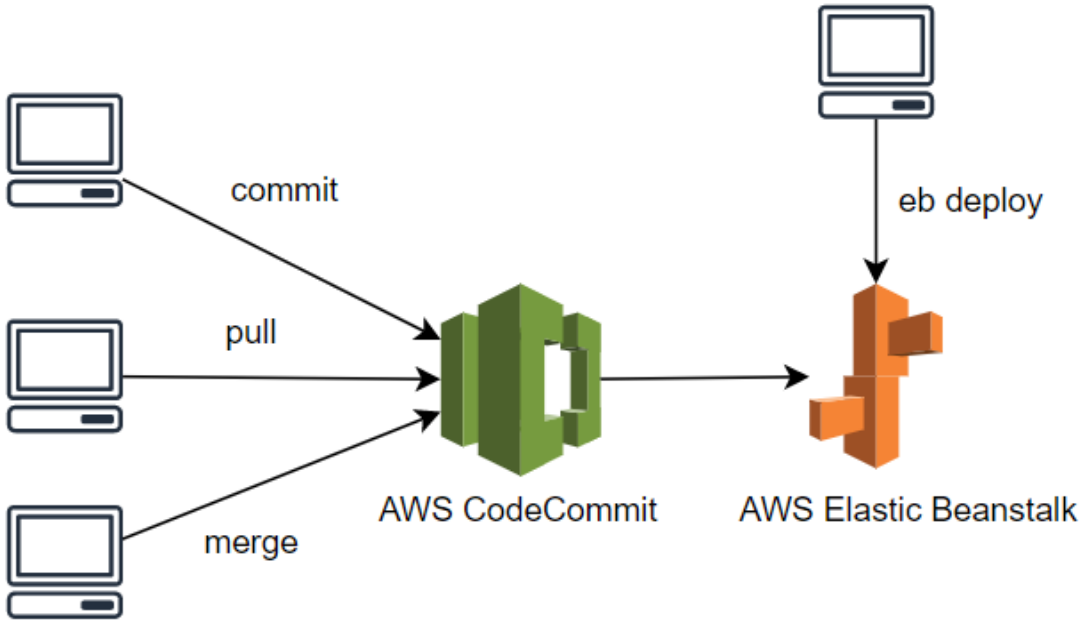
  (Correct)

- **AWS CodeBuild**
- **AWS CodeDeploy**

Explanation

AWS CodeCommit is a fully managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories. AWS CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use AWS CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

AWS CodeCommit helps you collaborate on code with teammates via pull requests, branching and merging. You can implement workflows that include code reviews and feedback by default and control who can make changes to specific branches.



AWS CodeCommit keeps your repositories close to your build, staging, and production environments in the AWS cloud. You can transfer incremental changes instead of the entire application. This allows you to increase the speed and frequency of your development lifecycle.

Hence, the correct answer is **AWS CodeCommit.**

AWS CodeStar is incorrect because this simply enables you to quickly develop, build, and deploy applications on AWS.

AWS CodeBuild is incorrect because this is just a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy.

AWS CodeDeploy is incorrect because this is primarily used to automate code deployments to any instance, including EC2 instances and instances running on-premises.

References:

https://aws.amazon.com/codecommit/

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/developer-tools.html

Check out this AWS CodeCommit Cheat Sheet:

https://tutorialsdojo.com/aws-codecommit/

Question 42:

Skipped

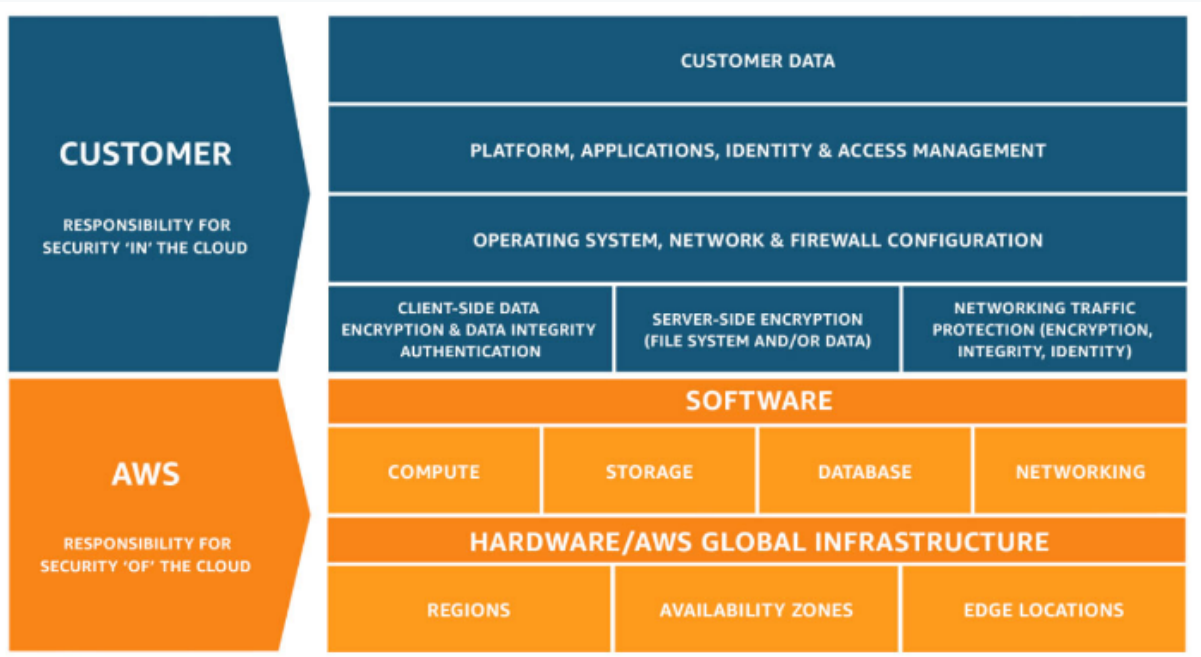
Which of the following statements accurately describes the AWS Shared Responsibility model?

- **Both AWS and customers are equally responsible for securing the physical infrastructure of the cloud, applications, and data in the cloud.**
- **AWS is responsible for securing the physical infrastructure of the cloud, applications, and data in the cloud, while customers are only responsible for managing the access and identity of their users.**
- **Customers are responsible for securing the physical infrastructure of the cloud, while AWS is responsible for securing their applications and data in the cloud.**
- **AWS is responsible for securing the physical infrastructure of the cloud, while customers are responsible for securing their applications and data in the cloud.**

(Correct)

Explanation

The **AWS Shared Responsibility Model** defines security responsibilities between AWS and its customers. AWS is responsible for protecting the underlying cloud infrastructure, such as servers, storage, and networks, and customers are responsible for protecting their applications, data, and systems running on AWS. On the other hand, customers are responsible for configuring their applications and infrastructure to meet security and compliance requirements, manage access controls, monitor their environments, and implement best practices. AWS also provides customers with various security controls, such as identity and access management, network security, and encryption, that customers can use to secure their applications and data in the cloud.



By understanding the shared responsibility model, AWS customers can better understand their security responsibilities when using AWS services. Customers can protect their applications and data with security controls and AWS best practices, such as implementing multi-factor authentication, monitoring their environments for suspicious activity, and encrypting data at storage and in transit. Customers must also understand their compliance requirements and ensure that their applications and data comply with them when running on AWS.

Hence the correct answer is: **AWS is responsible for securing the physical infrastructure of the cloud, while customers are responsible for securing their applications and data in the cloud.**

The option that says: **Customers are responsible for securing the physical infrastructure of the cloud, while AWS is responsible for securing their applications and data in the cloud** is incorrect because it implies that customers are in charge of protecting the cloud's physical infrastructure, which is not the case. In accordance with the AWS shared responsibility model, AWS is in charge of protecting the cloud's server, storage, and networking infrastructure. While the customers are in charge of protecting the systems, data, and applications they run on Amazon.

The option that says: **Both AWS and customers are equally responsible for securing the physical infrastructure of the cloud, applications, and data in the cloud** is incorrect because both AWS and customers don't have equal responsibilities in the AWS shared responsibility model. AWS is responsible for securing the underlying infrastructure of the cloud, while customers are responsible for securing their applications, data, and systems running on AWS.

The option that says: **AWS is responsible for securing the physical infrastructure of the cloud, applications, and data in the cloud, while customers are only responsible for managing the access and identity of their users** is incorrect because AWS is responsible for securing the infrastructure of the cloud while customers are

responsible for ensuring their applications, data, and systems running on AWS, including managing access and identity.

References:

https://aws.amazon.com/compliance/shared-responsibility-model/

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/security.html

Check out this AWS Shared Responsibility Model Cheat Sheet:

https://tutorialsdojo.com/aws-shared-responsibility-model/

Question 43:

Skipped

Which of the following services are part of the AWS serverless platform that does not require provisioning, maintaining, and administering servers for backend components? (Select TWO.)

- **Amazon OpenSearch**
- **Amazon API Gateway**

  (Correct)

- **Lambda@Edge**

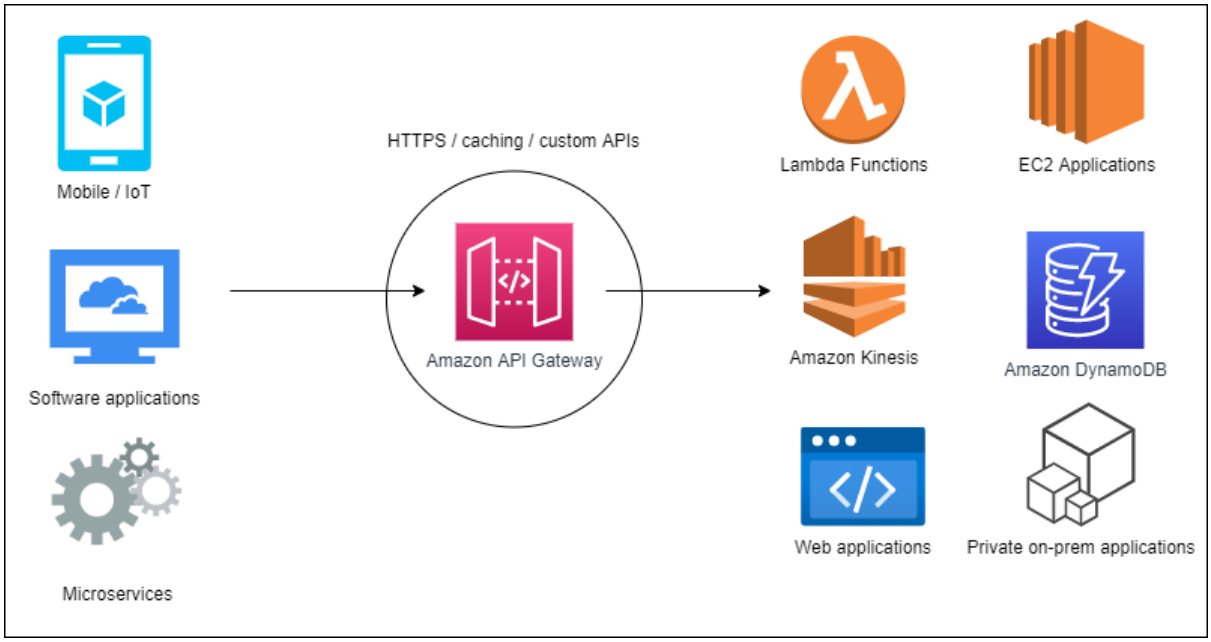
  (Correct)

- **Amazon EMR**
- **Amazon ElastiCache**

Explanation

Serverless is the native architecture of the cloud that enables you to shift more of your operational responsibilities to AWS, increasing your agility and innovation. Serverless allows you to build and run applications and services without thinking about servers. It eliminates infrastructure management tasks such as a server or cluster provisioning, patching, operating system maintenance, and capacity provisioning. You can build them for nearly any type of application or backend service, and everything required to run and scale your application with high availability is handled for you.

Serverless enables you to build modern applications with increased agility and a lower total cost of ownership. Building serverless applications means that your developers can focus on their core product instead of worrying about managing and operating servers or runtimes, either in the cloud or on-premises. This reduced overhead lets developers reclaim time and energy that can be spent on developing great products that scale and are reliable.



AWS provides a set of fully managed services that you can use to build and run serverless applications. Serverless applications don't require provisioning, maintaining, and administering servers for backend components such as computing, databases, storage, stream processing, message queueing, and more. You also no longer need to worry about ensuring application fault tolerance and availability. Instead, AWS handles all of these capabilities for you. This allows you to focus on product innovation while enjoying faster time-to-market.

AWS Lambda, Lambda@Edge, and AWS Fargate are the services that you can use for serverless computing. For your API Proxy, you can leverage the power of the Amazon API Gateway service.

Hence, the correct answers are:

- Amazon API Gateway.

- Lambda@Edge.

Amazon OpenSearch is incorrect because this managed search and analytics service makes searching, analyzing, and visualizing data easy. Thus, this service provides a fully managed solution that relieves you of managing and operating the underlying infrastructure.

Amazon ElastiCache is incorrect because this is a fully managed in-memory data store and cache service that can be used to improve the performance of web applications.

Amazon EMR is incorrect because this service is a managed cluster platform that simplifies the processing and analyzing large data frameworks such as Apache Hadoop and Apache Spark on AWS.

References:

https://aws.amazon.com/serverless/

https://aws.amazon.com/lambda/edge/

https://aws.amazon.com/api-gateway/

Check out these Amazon API Gateway and AWS Lambda Cheat Sheets:

https://tutorialsdojo.com/aws-lambda/

https://tutorialsdojo.com/amazon-api-gateway/

AWS Lambda Overview - Serverless Computing in AWS:

https://youtu.be/bPVX1zHwAnY

Question 44:

Skipped

_____ lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

- **Amazon VPC**

  (Correct)

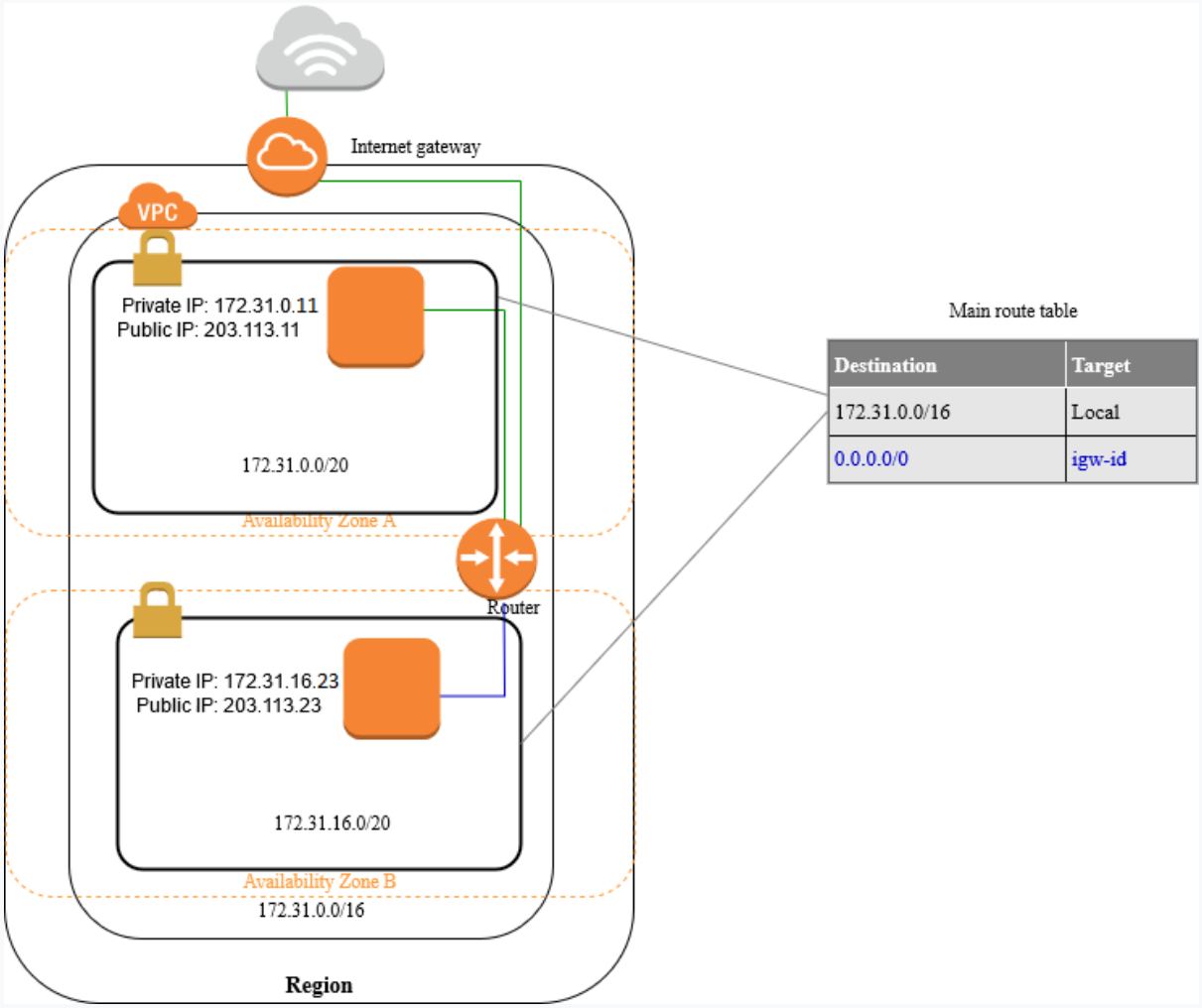
- **Virtual Private Gateway**
- **Amazon WorkSpaces**
- **Amazon Lightsail**

Explanation

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple

layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.



Hence, the correct answer is **Amazon VPC**.

Amazon LightSail is incorrect because this service is just a virtual private server (VPS) solution which provides developers with compute, storage, and networking capacity and capabilities to deploy and manage websites and web applications in the cloud.

Virtual Private Gateway is incorrect because this is primarily used for connecting your on-premises network to your VPC.

Amazon WorkSpaces is incorrect because this is just a Desktop-as-a-Service (DaaS) solution in AWS which allows you to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.

References:

https://aws.amazon.com/vpc/

https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

Check out this Amazon VPC Cheat Sheet:

https://tutorialsdojo.com/amazon-vpc/

Amazon VPC Overview Video Tutorial:

https://www.youtube.com/watch?v=oIDHKeNxvQQ

Question 45:

Skipped

Which of the following is true regarding the Business support plan in AWS?

- **Provides a 15-minute response time support if your business-critical system goes down**
- **Provides a 1-hour response time support if your production system got impaired**
- **Provides a 1-hour response time support if your production system goes down**

  (Correct)

- **Provides a 15-minute response time support if your production system goes down**

Explanation

AWS Support offers a range of plans that provide access to tools and expertise that support the success and operational health of your AWS solutions. All support plans provide 24x7 access to customer service, AWS documentation, whitepapers, and support forums. For technical support and more resources to plan, deploy, and improve your AWS environment, you can select a support plan that best aligns with your AWS use case.

	DEVELOPER	BUSINESS	ENTERPRISE ON-RAMP	ENTERPRISE
Use Case	Recommended if you are experimenting or testing in AWS.	Recommended if you have production workloads in AWS.	Recommended if you have business and/or mission critical workloads in AWS.	Recommended if you have business and/or mission critical workloads in AWS.
AWS Trusted Advisor Best Practice Checks	Service Quota and basic Security checks	Full set of checks	Full set of checks	Full set of checks
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications	Consultative review and guidance based on your applications
Technical Account Management	✕	✕	A pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts	Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization and coordinate access to programs and
Training	✕	✕	✕	Access to online self-paced labs
Account Assistance	✕	✕	Concierge Support Team	Concierge Support Team
Enhanced Technical Support	Business hours** email access to Cloud Support Associates. Unlimited cases / 1 primary contact Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post	24x7 phone, email, and chat access to Cloud Support Engineers Unlimited cases / unlimited contacts (IAM supported) Prioritized responses on AWS re:Post
Programmatic Case Management	✕	AWS Support API	AWS Support API	AWS Support API
Third-Party Software Support	✕	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting	Interoperability and configuration guidance and troubleshooting
Proactive Programs	Access to Support Automation Workflows with prefixes AWSSupport	Access to Infrastructure Event Management for additional fee Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management (one-per-year) Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport	Infrastructure Event Management Access to proactive reviews, workshops, and deep dives Access to Support Automation Workflows with prefixes AWSSupport and AWSPremiumSupport

AWS Support offers five support plans: Basic, Developer, Business, Enterprise On-Ramp, and Enterprise. The Basic plan is free of charge and offers support for account and billing questions and service limit increases. The other plans offer an unlimited number of technical support cases with pay-by-the-month pricing and no long-term contracts, providing the level of support that meets your needs.

In addition to the basic offerings, customers with a Business or Enterprise support plan have access to these features:

- Use-case guidance: what AWS products, features, and services to use to best support your specific needs.

- AWS Trusted Advisor, which inspects customer environments. Then, Trusted Advisor identifies opportunities to save money, close security gaps, and improve system reliability and performance.

- An API for interacting with Support Center and Trusted Advisor. This API allows for automated support case management and Trusted Advisor operations.

- Third-party software support: help with Amazon Elastic Compute Cloud (EC2) instance operating systems and configuration. Also, help with the performance of the most popular third-party software components on AWS.

The AWS Support API provides access to some of the features of the AWS Support Center. This API allows programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status. AWS provides this access for AWS Support customers who have a Business or Enterprise support plan.

	DEVELOPER	BUSINESS	ENTERPRISE ON-RAMP	ENTERPRISE
Case Severity / Response Times*	General guidance: < 24 hours**	General guidance: < 24 hours	General guidance: < 24 hours	General guidance: < 24 hours
	System impaired: < 12 hours**	System impaired: < 12 hours	System impaired: < 12 hours	System impaired: < 12 hours
		Production system impaired: < 4 hours	Production system impaired: < 4 hours	Production system impaired: < 4 hours
		Production system down: < 1 hour	Production system down: < 1 hour	Production system down: < 1 hour
			Business-critical system down: < 30 minutes	Business/Mission-critical system down: < 15 minutes

Hence, the correct answer is: **Provides a 1-hour response time support if your production system goes down.**

The option that says: **Provides a 15-minute response time support if your production system goes down** is incorrect because the Business support plan only provides a 1-hour response time and not 15 minutes.

The option that says: **Provides a 15-minute response time support if your business-critical system goes down** is incorrect because this high level of support is only available for Enterprise support plan.

The option that says: **Provides a 1-hour response time support if your production system got impaired** is incorrect because the Business support plan only gives you a 4-hour response time and not an hour in the event that your production system got impaired.

References:

https://aws.amazon.com/premiumsupport/plans/

https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html

https://aws.amazon.com/premiumsupport/plans/enterprise/

Check out this AWS Support Plans Cheat Sheet:

https://tutorialsdojo.com/aws-support-plans/

Question 46:

Skipped

Which of the following is the most cost-effective instance purchasing option for hosting an application which will run non-interruptible workloads for a period of three years?

- **Amazon EC2 On-Demand Instances**
- **Amazon EC2 Standard Reserved Instances**

(Correct)

- **Amazon EC2 Spot Instances**
- **Amazon EC2 Convertible Reserved Instances**

Explanation

Reserved Instances provide you with a significant discount compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

Standard Reserved Instances provide you with a significant discount compared to On-Demand instance pricing and can be purchased for a 1-year or 3-year term. The average discount off On-Demand instances varies based on your term and chosen payment options (up to 40% for 1-year and 60% for a 3-year term). Customers have the flexibility to change the Availability Zone, the instance size, and networking type of their Standard Reserved Instances.

Convertible Reserved Instances provide you with a significant discount compared to On-Demand Instances and can be purchased for a 1-year or 3-year term. Purchase *Convertible Reserved Instances* if you need additional flexibility, such as the ability to use different instance families, operating systems, or tenancies over the Reserved Instance term.

Characteristic	Standard	Convertible
Terms (avg. discount off On-Demand)	1yr (40%), 3yr (60%)	1yr (31%), 3yr (54%)
Change Availability Zone, instance size (for Linux OS), networking type	Yes (Using ModifyReservedInstances API and console)	Yes (Using ExchangeReservedInstances API and console)
Change instance families, operating system, tenancy, and payment option		Yes
Benefit from Price Reductions		Yes
Sellable on the Reserved Instance Marketplace	Yes (After linking account with a US bank account)	Coming soon

Hence, the correct answer is: **Amazon EC2 Standard Reserved Instances.**

The **Amazon EC2 Spot Instances** option is incorrect. Although this is the most cost-effective type, this instance can be interrupted by Amazon EC2 for capacity requirements making it not suitable for non-interruptible workloads.

The **Amazon EC2 Convertible Reserved Instances** option is incorrect because this type of reserved instances on average offers less pricing discount than Standard Reserved Instances.

The **Amazon EC2 On-Demand Instances**option is incorrect. Although it is suitable to run non-interruptible workloads for a period of three years, it entails a higher running cost compared to Reserved or Spot instances. In fact, this is actually the most expensive type of EC2 instance and not the cheapest one.

References:

https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html

Amazon EC2 Overview:

https://www.youtube.com/watch?v=7VsGIHT_jQE

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Question 47:

Skipped

Which service allows you to add powerful visual analysis feature to your applications that enables you to search, verify, and organize millions of images?

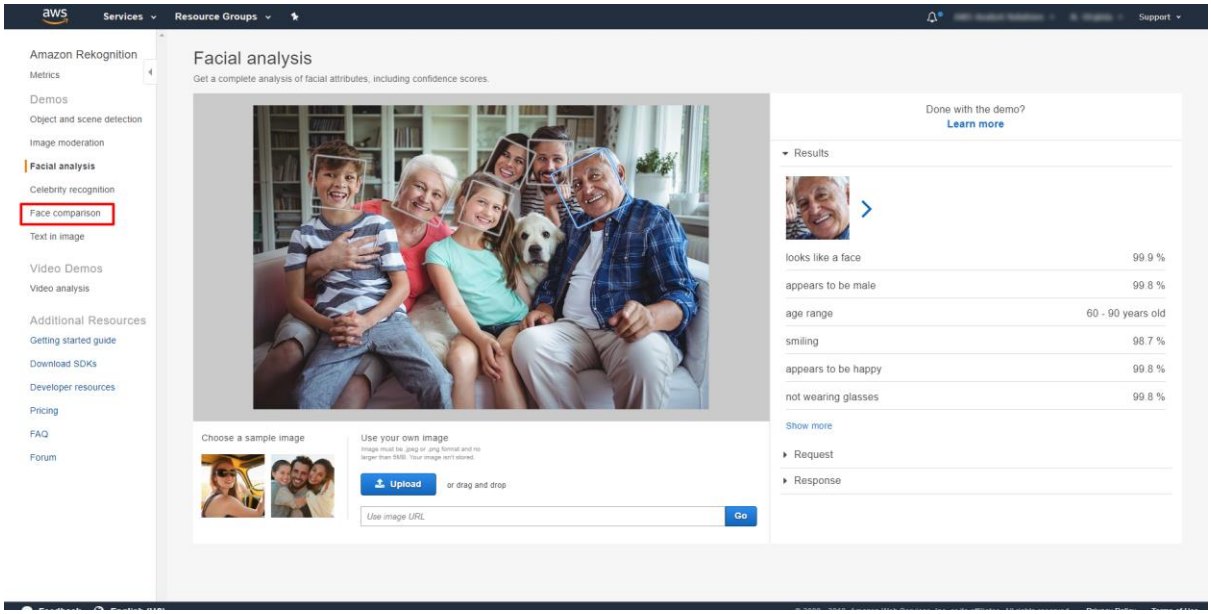
- **Amazon Rekognition**

  (Correct)

- **Amazon CloudSearch**
- **Amazon Macie**
- **Amazon SageMaker**

Explanation

Amazon Rekognition makes it easy to add image and video analysis to your applications. You just provide an image or video to the Rekognition API, and the service can identify the objects, people, text, scenes, and activities, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial recognition on images and video that you provide. You can detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.



Amazon Rekognition is based on the same proven, highly scalable, deep learning technology developed by Amazon's computer vision scientists to analyze billions of images and videos daily, and requires no machine learning expertise to use. Amazon Rekognition is a simple and easy to use API that can quickly analyze any image or video file stored in Amazon S3. Amazon Rekognition is always learning from new data, and we are continually adding new labels and facial recognition features to the service.

Hence, the correct answer is **Amazon Rekognition**.

Amazon Macie is incorrect because it is a security service and not suitable for visual analysis. It uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Amazon SageMaker is incorrect because this is a service that provides every developer and data scientist with the ability to build, train, and deploy machine learning models quickly in AWS.

Amazon CloudSearch is incorrect because this service is used to set up, manage, and scale a search solution for your website or application in AWS.

References:

https://aws.amazon.com/rekognition

https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html

Check out this Amazon Rekognition Cheat Sheet:

https://tutorialsdojo.com/amazon-rekognition/

Question 48:

Skipped

Which of the following is the benefit of using Amazon Relational Database Service (Amazon RDS) over traditional database management?

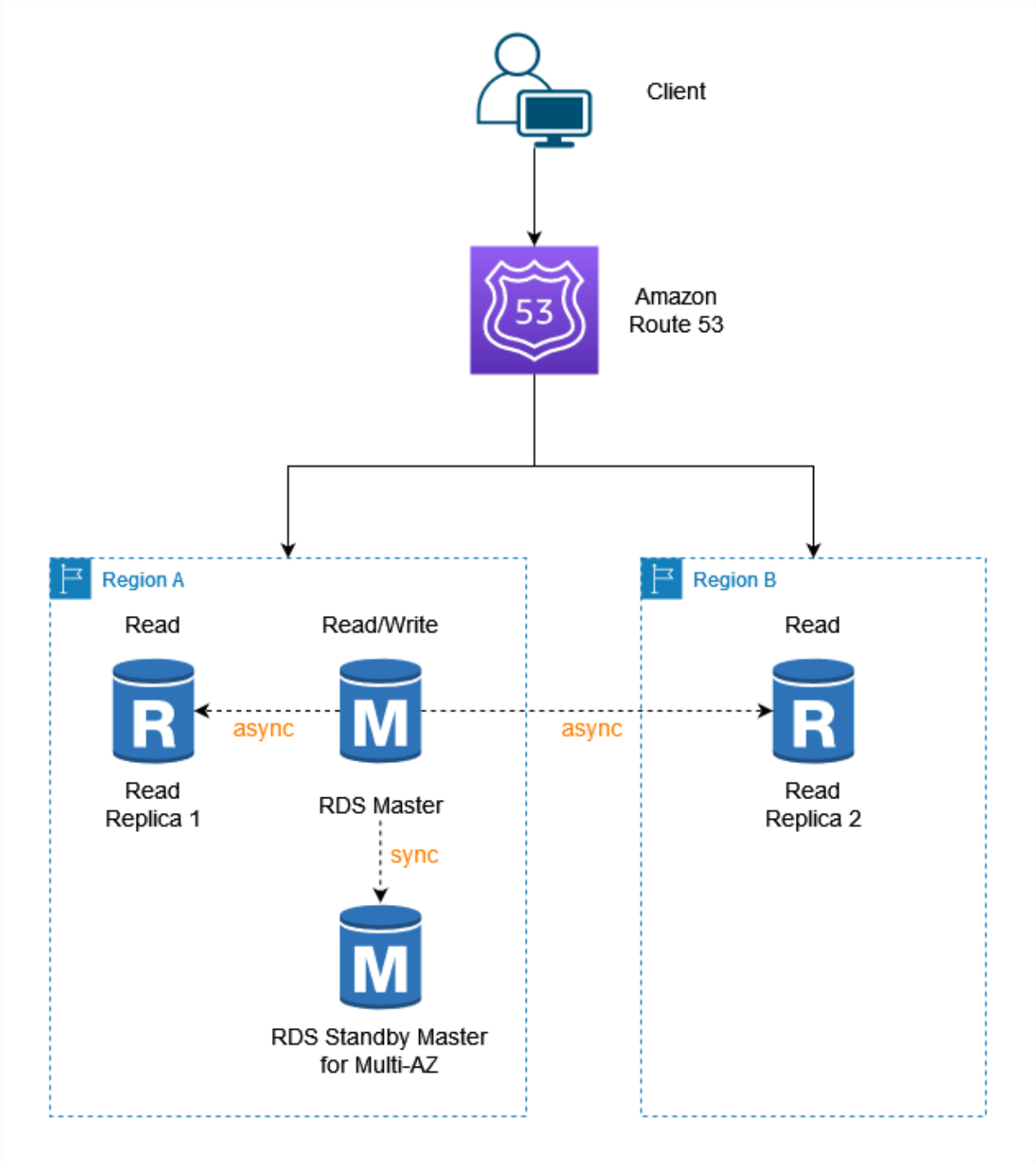
- **It is five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases**
- **Lower administrative burden through automatic software patching and maintenance of the underlying operating system**

(Correct)

- **Automatically scales up the instance type of your RDS cluster based on demand**
- **Automatically apply both client-side and server-side encryption to your data by default**

Explanation

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security, and compatibility they need.



Amazon RDS is available on several database instance types - optimized for memory, performance, or I/O - and provides you with several database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. You can use the AWS Database Migration Service to easily migrate or replicate your existing databases to Amazon RDS

Amazon RDS will make sure that the relational database software powering your deployment stays up-to-date with the latest patches. You can exert optional control over when and if your database instance is patched.

Hence, the correct answer is: **Lower the administrative burden through automatic software patching and maintenance of the underlying operating system**.

The option that says: **Automatically apply both client-side and server-side encryption to your data by default** is incorrect because this is not done by RDS at all. In RDS, you can manually configure your database cluster in order to secure your data at rest or in transit, but this is not done automatically by default.

The option that says: **Automatically scales up the instance type of your RDS cluster based on demand** is incorrect because with RDS, you still have to manually upgrade the underlying instance type of your database cluster in order to scale it up.

The option that says: **It is five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases** is incorrect because this is not a feature of Amazon RDS but of Amazon Aurora.

References:

https://aws.amazon.com/rds/features

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

Amazon RDS Overview:

https://youtu.be/aZmpLl8K1UU

Check out this Amazon RDS Cheat Sheet:

https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/

Amazon RDS vs DynamoDB:

https://tutorialsdojo.com/amazon-rds-vs-dynamodb/

Question 49:

Skipped

Which of the following cloud best practices reinforces the use of the Service-Oriented Architecture (SOA) design principle?

- **Decouple your components.**

  (Correct)

- **Implement elasticity.**
- **Design for failure.**
- **Think parallel.**

Explanation
There are various best practices that you can follow which can help you build an application in the AWS cloud. The notable ones are:

1. Design for failure

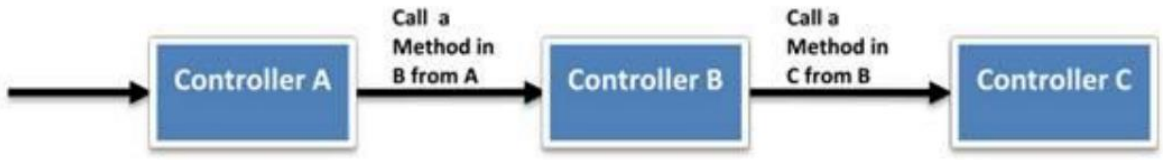
2. Decouple your components

3. Implement elasticity

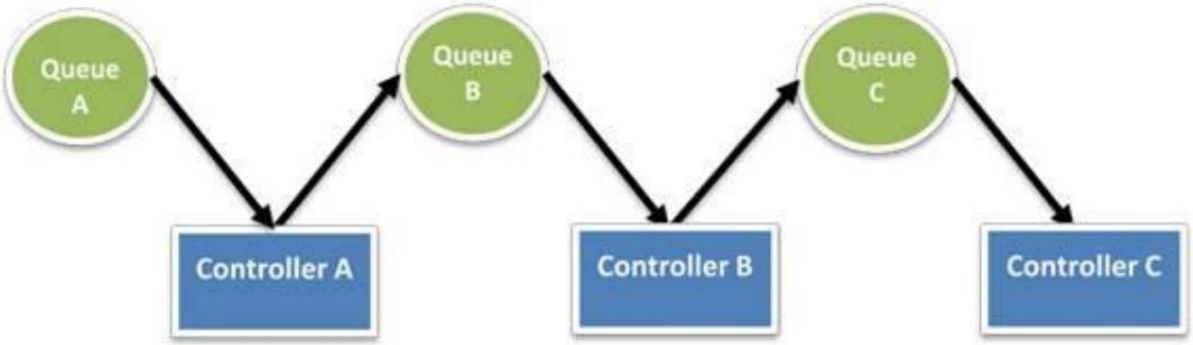
4. Think parallel

Decouple your components tells us that we should build components that do not have tight dependencies on each other, so that if one component were to die (fail), sleep (not respond) or remain busy (slow to respond) for some reason, the other components in the system are built so as to continue to work as if no failure is happening. The cloud reinforces the Service-Oriented Architecture (SOA) design principle that the more loosely coupled the components of the system, the bigger and better it scales.

You can build a loosely coupled system using messaging queues such as SQS. If a queue/buffer is used to connect any two components together, it can support concurrency, high availability, and load spikes. As a result, the overall system continues to perform even if parts of the components are momentarily unavailable. If one component dies or becomes temporarily unavailable, the system will buffer the messages and get them processed when the component comes back up.



Tight coupling (procedural programming)



Loose coupling (independent phases using queues)

In essence, loose coupling isolates the various layers and components of your application so that each component interacts asynchronously with the others and treats them as a “black box”. For example, in the case of web application architecture, you can isolate the app server from the web server and from the database. The app server does not know about your web server and vice versa, this gives decoupling between these layers and there are no dependencies code-wise or functional perspectives. In the case of batch-processing architecture, you can create asynchronous components that are independent of each other.

The AWS specific tactics for implementing this best practice are:

1. Use Amazon SQS to isolate components.

2. Use Amazon SQS as buffers between components.

3. Design every component such that it exposes a service interface and is responsible for its own scalability in all appropriate dimensions and interacts with other components asynchronously.

4. Bundle the logical construct of a component into an Amazon Machine Image so that it can be deployed more often.

5. Make your applications as stateless as possible. Store session state outside of component (in Amazon DynamoDB, if appropriate).

Hence, the correct answer is: **Decouple your components.**

Think parallel is incorrect because this just internalizes the concept of parallelization when designing architectures in the cloud. It advocates to not only implement parallelization wherever possible but also automate it because the cloud allows you to create a repeatable process very easily.

Implement elasticity is incorrect because this principle is primarily implemented by automating your deployment process and streamlining the configuration and build process of your architecture. This ensures that the system can scale without any human intervention.

Design for failure is incorrect because it only encourages you to be a pessimist when designing architectures in the cloud; assume things will fail. In other words, you should always design, implement and deploy for automated recovery from failure.

References:

https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html

https://www.slideshare.net/AmazonWebServices/best-practices-for-architecting-in-the-cloud-jeff-barr

Check out this AWS Well-Architected Framework Cheat Sheet:

https://tutorialsdojo.com/aws-well-architected-framework-design-principles/

Question 50:

Skipped

A customer is building a cloud architecture in AWS which should scale horizontally or vertically in order to automatically adjust capacity and maintain steady, predictable performance at the lowest possible cost. Which of the following statements are true regarding horizontal and vertical scaling? (Select TWO.)

- **Upgrading to a higher EC2 instance type is an example of Vertical Scaling**

  (Correct)

- **Upgrading to a higher EC2 instance type and adding more EC2 instances to your resource pool are both examples of Horizontal Scaling**
- **Adding more EC2 instances to your resource pool is an example of Horizontal Scaling**

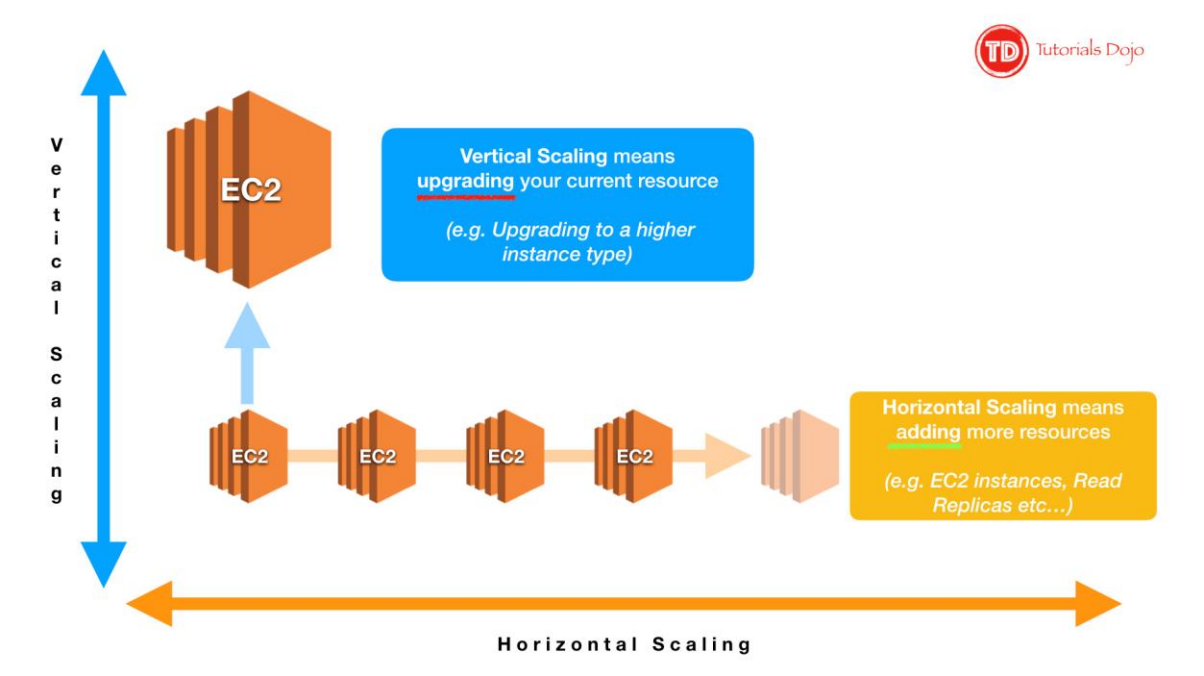
  (Correct)

- **Upgrading to a higher EC2 instance type is an example of Horizontal Scaling**
- **Adding more EC2 instances to your resource pool is an example of Vertical Scaling**

Explanation

Systems that are expected to grow over time need to be built on top of a scalable architecture. Such an architecture can support growth in users, traffic, or data size with no drop-in performance. It should provide that scale in a linear manner where adding extra resources results in at least a proportional increase in ability to serve additional load. Growth should introduce economies of scale, and cost should follow the same dimension that generates business value out of that system. While cloud computing provides virtually unlimited on-demand capacity, your design needs to be able to take advantage of those resources seamlessly.

There are generally two ways to scale an IT architecture: vertically and horizontally.



Vertical Scaling

- Scaling vertically takes place through an increase in the specifications of an individual resource, such as upgrading a server with a larger hard drive or a faster CPU. With Amazon EC2, you can stop an instance and resize it to an instance type that has more RAM, CPU, I/O, or networking capabilities. This way of scaling can eventually reach a limit, and it is not always a cost-efficient or highly available approach. However, it is very easy to implement and can be sufficient for many use cases especially in the short term.

Horizontal Scaling

- Scaling horizontally takes place through an increase in the number of resources, such as adding more hard drives to a storage array or adding more servers to support an application. This is a great way to build internet-scale applications that leverage the elasticity of cloud computing. Take note that not all architectures are designed to distribute their workload to multiple resources.

Hence, the correct answers are:

- Upgrading to a higher EC2 instance type is an example of Vertical Scaling

- **Adding more EC2 instances to your resource pool is an example of Horizontal Scaling**.

The option that says: **Upgrading to a higher EC2 instance type is an example of Horizontal Scaling** is incorrect because this is actually an example of Vertical Scaling.

The option that says: **Adding more EC2 instances to your resource pool is an example of Vertical Scaling** is incorrect because this is actually an example of Horizontal Scaling.

The option that says: **Upgrading to a higher EC2 instance type and adding more EC2 instances to your resource pool are both examples of Horizontal Scaling** is incorrect. Only the act of adding more EC2 instances to your resource pool is an example of Horizontal Scaling.

References:

https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/

Check out this AWS Well-Architected Framework – Design Principles Cheat Sheet:

https://tutorialsdojo.com/aws-well-architected-framework-design-principles/

Question 51:

Skipped

The IT Security team of your company needs to conduct a vulnerability analysis on your application servers to ensure that the EC2 instances comply with the annual security IT audit. You need to set up an automated security assessment service to improve the security and compliance of your applications. The solution should automatically assess applications for exposure, vulnerabilities, and deviations from the AWS best practices.

Which of the following options would you implement to satisfy this requirement?

- **AWS WAF**
- **AWS Inspector**

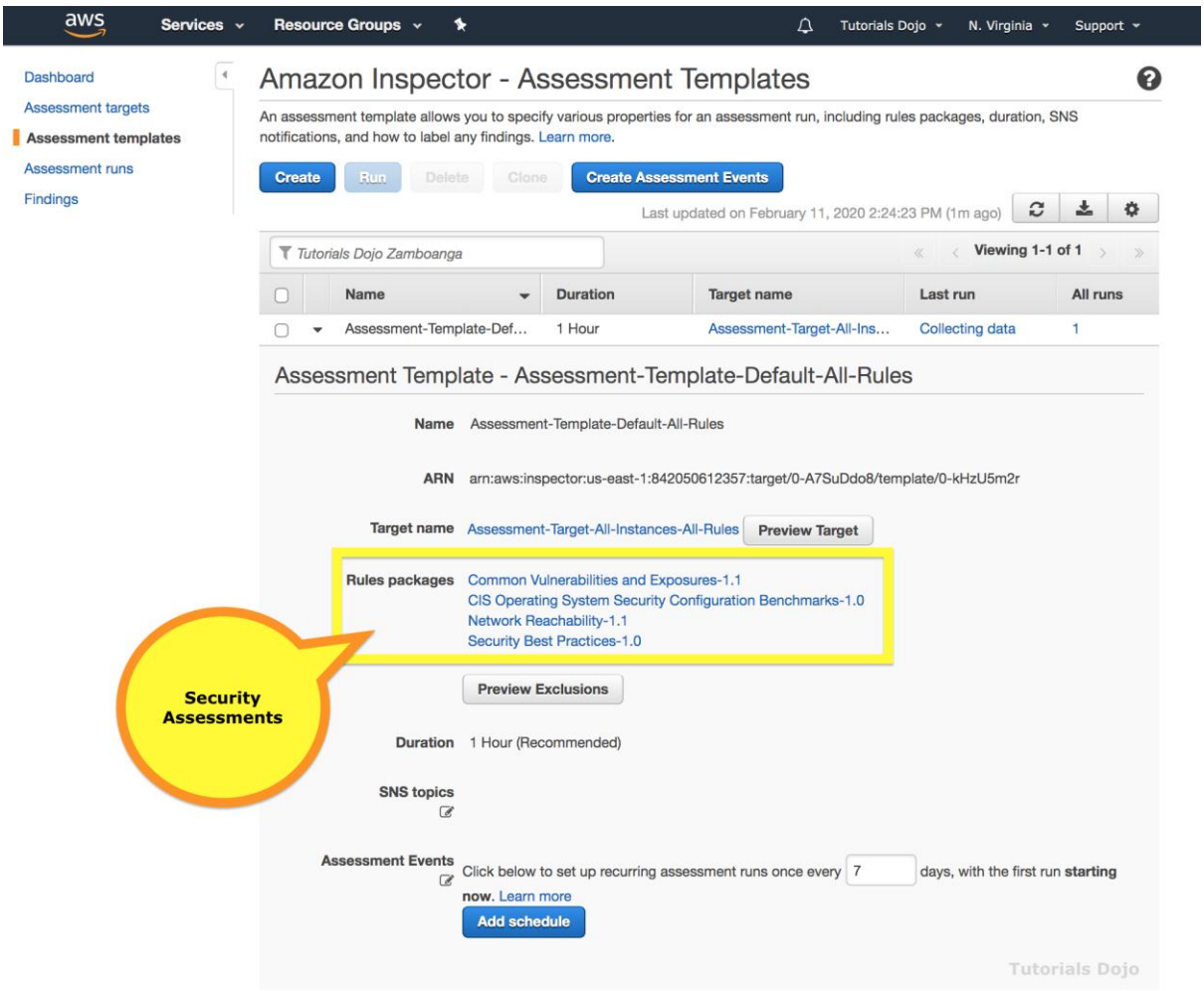
  (Correct)

- **Amazon CloudFront**
- **AWS Snowball**

Explanation

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be

reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.



Amazon Inspector security assessments help you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking for access to your EC2 instances from the internet, remote root login being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers.

Hence, the correct answer is: **Amazon Inspector.**

AWS WAF is incorrect because this is a firewall service to safeguard your VPC against DDoS, SQL Injection, and many other threats.

AWS Snowball Edge is incorrect because Snowball Edge is an appliance used to transfer terabytes to petabytes of data to AWS.

Amazon CloudFront is incorrect because CloudFront is a content distribution service (CDN).

References:

https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html

https://aws.amazon.com/inspector/

Check out this Amazon Inspector Cheat Sheet:

https://tutorialsdojo.com/amazon-inspector/

Question 52:

Skipped

A website is experiencing varying levels of traffic throughout the day and is not fully consuming server capacity all the time. Which advantage does AWS Cloud provide over traditional data centers when it comes to handling traffic load?

- **Quick capacity provisioning**
- **Elasticity**

  (Correct)

- **High Availability**
- **Durability**

Explanation

Elasticity is 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 automatically.

Most people associate cloud computing with the ease with which they can obtain resources when needed. This is only one aspect of elasticity. Another consideration is to contract when resources are no longer needed.

Hence, is the correct answer is: **Elasticity**.

Durability is incorrect since this characteristic concerns data durability than handling server load.

High availability is incorrect since, based on the scenario, the website is not experiencing downtime issues.

Quick capacity provisioning is incorrect since, as per the scenario requirement, you should be more concerned with handling traffic load than the agility in provisioning resources.

References:

https://aws.amazon.com/architecture/well-architected/

https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html

Check out this AWS Well-Architected Design Principles Cheat Sheet:

https://tutorialsdojo.com/aws-well-architected-framework-design-principles/

Question 53:

Skipped

What is the best type of instance purchasing option to choose if you will run an EC2 instance for 3 months to perform a job that is uninterruptible?

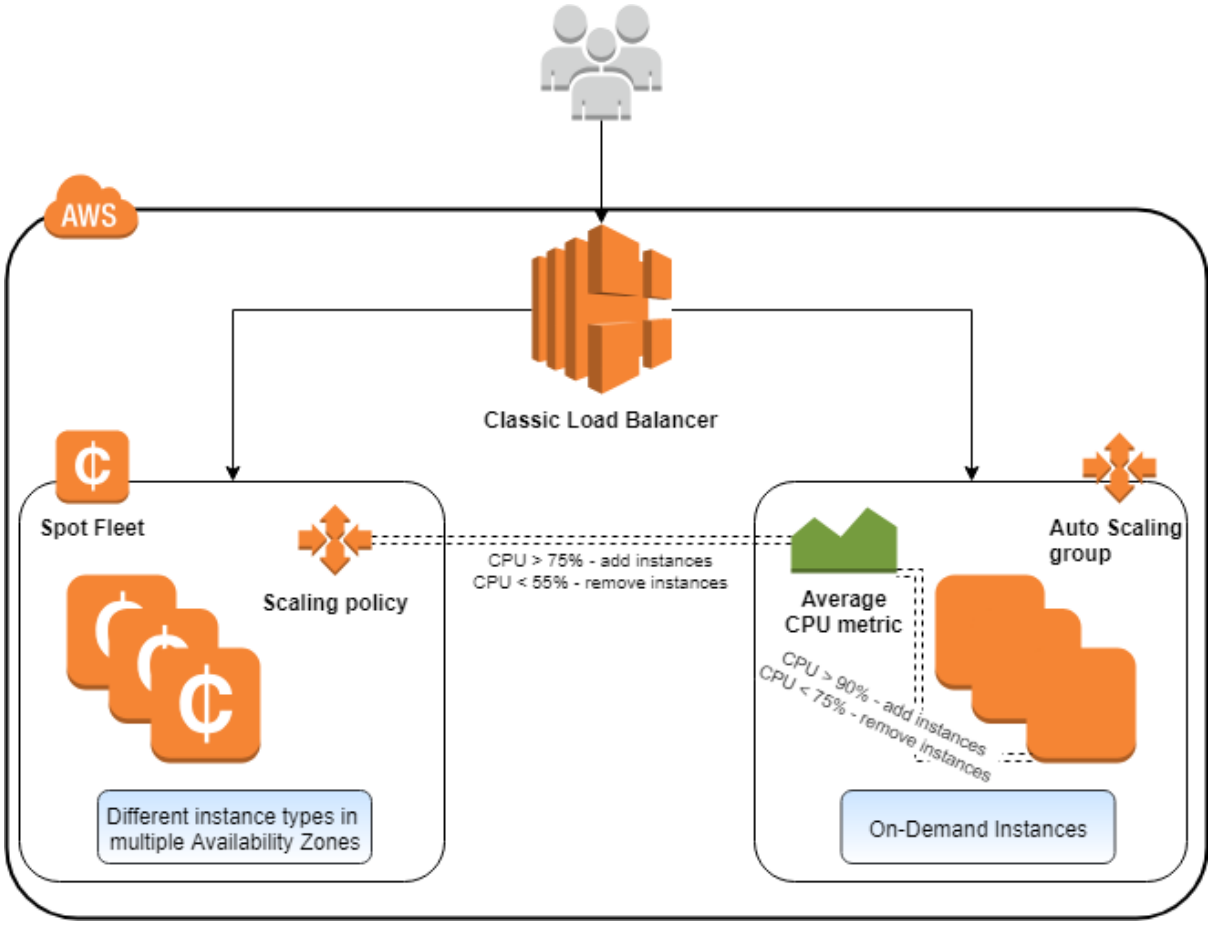
- **On-Demand**

  (Correct)

- **Dedicated**
- **Reserved**
- **Spot**

Explanation

With On-Demand instances, you only pay for the EC2 instances you use. The use of On-Demand instances frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.



This type of instance lets 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 costs.

On-Demand is the best instance type to use when you need instances for short periods of time and for uninterruptible workloads since they are the cheapest option for its span of time.

Hence, the correct answer is: **On-Demand Instance.**

Reserved instance is incorrect. Although it does offer discounts on hourly costs, you still need to commit at least a whole year's worth of instance cost to fully maximize the discounts. Since your workload will run for only 3 months, this option is not the most suitable.

Spot instance is incorrect because this can be terminated by Amazon EC2 based on the long-term supply of and demand for Spot Instances. Hence, this is not recommended for uninterruptible workloads.

Dedicated Instance is incorrect because this is just a type of Amazon EC2 instance that runs in a VPC on hardware that's dedicated to a single customer. This option is not relevant to the question, so this is incorrect.

References:

https://aws.amazon.com/ec2/pricing/on-demand/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Amazon EC2 Overview:

https://youtu.be/7VsGIHT_jQE

Question 54:

Skipped

Which of the folllowing is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads?

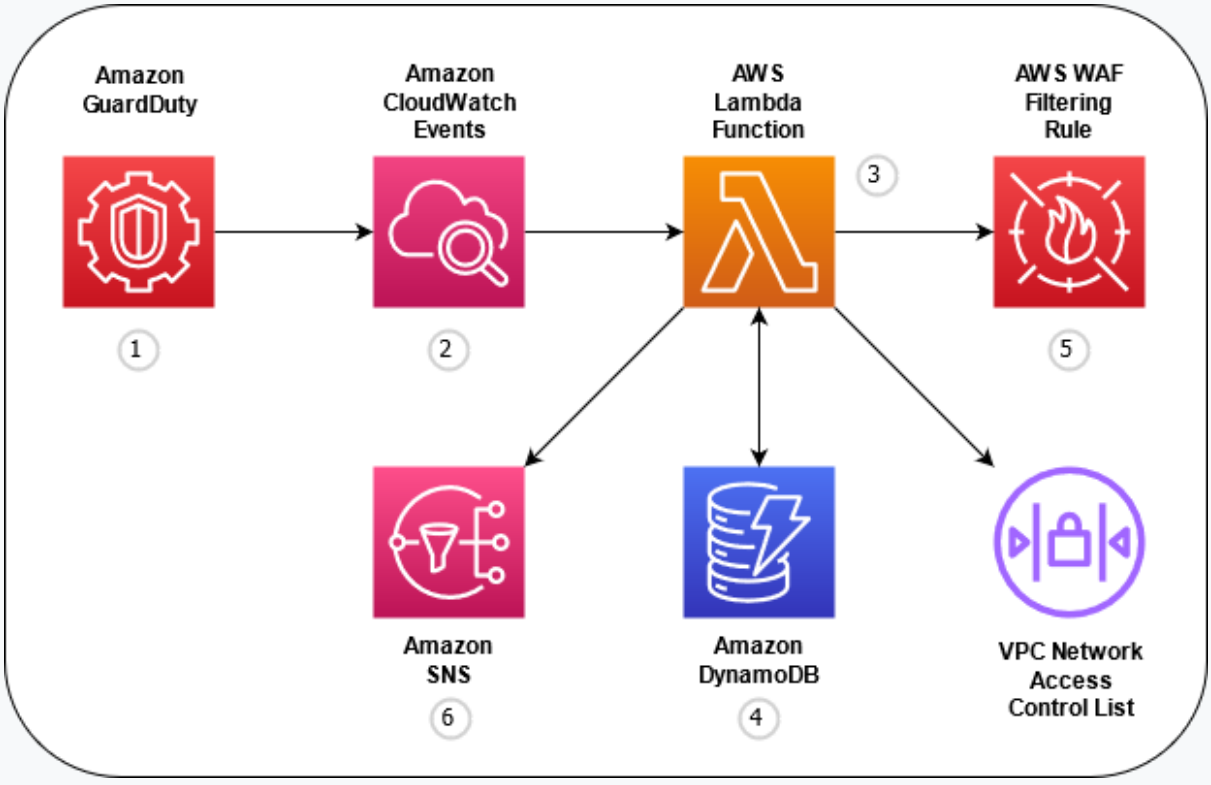
- **AWS WAF**
- **Amazon GuardDuty**

(Correct)

- **Amazon Macie**
- **AWS Shield**

Explanation

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. With the cloud, the collection and aggregation of account and network activities are simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in the AWS Cloud.



This service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon EventBridge (Amazon CloudWatch Events), GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

Hence, the correct answer is: **Amazon GuardDuty.**

Amazon Macie is incorrect because this is just a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

AWS Shield is incorrect because this is simply a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

AWS WAF is incorrect because this is basically a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

References:

https://aws.amazon.com/guardduty/

https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

Check out this Amazon GuardDuty Cheat Sheet:

https://tutorialsdojo.com/amazon-guardduty/

AWS Security Services Overview - WAF, Shield, CloudHSM, KMS:

https://youtu.be/-1S-RdeAmMo?si=JO1SylKbxOnS-8H9

Question 55:

Skipped

Which of the following are the best practices that can help secure your AWS resources using the AWS Identity and Access Management (IAM) service? (Select TWO.)

- **Use Bastion Hosts.**
- **Grant most privilege.**
- **Use Inline Policies instead of Customer Managed Policies.**
- **Grant least privilege.**

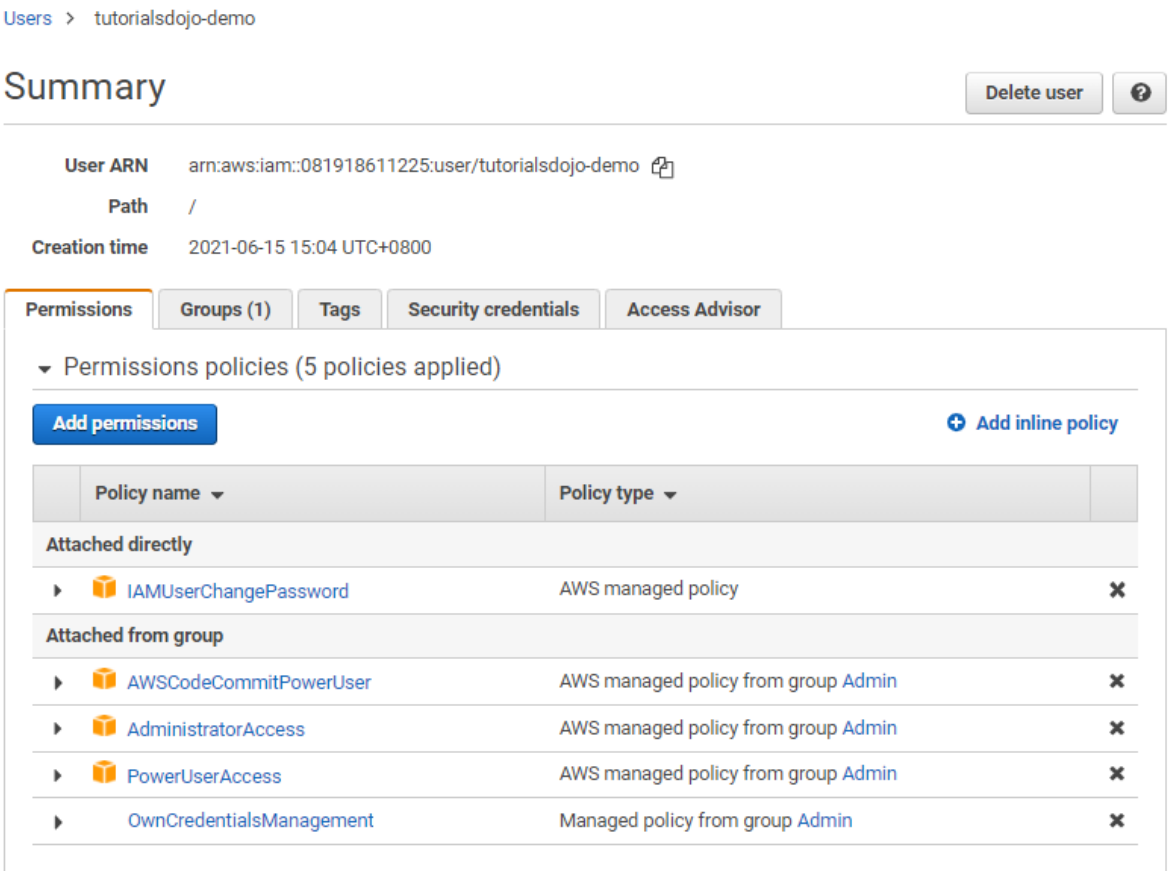
  (Correct)

- **Lock away your AWS account root user access keys.**

  (Correct)

Explanation

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



To help secure your AWS resources, follow the best practices in using your AWS Identity and Access Management (IAM) service:

```
- Lock Away Your AWS Account Root User Access Keys
- Create Individual IAM Users
- Use Groups to Assign Permissions to IAM Users
- Grant Least Privilege
- Get Started Using Permissions with AWS Managed Policies
- Use Customer Managed Policies Instead of Inline Policies
- Use Access Levels to Review IAM Permissions
- Configure a Strong Password Policy for Your Users
- Enable MFA
- Use Roles for Applications That Run on Amazon EC2 Instances
- Use Roles to Delegate Permissions
- Do Not Share Access Keys
- Rotate Credentials Regularly
- Remove Unnecessary Credentials
- Use Policy Conditions for Extra Security
- Monitor Activity in Your AWS Account
```

Hence, the correct answers are:

- Grant Least Privilege

- Lock away your AWS account root user access keys

The option that says: **Grant Most Privilege** is incorrect because it should be Grant Least Privilege.

The option that says: **Use Inline Policies instead of Customer Managed Policies** is incorrect because it should be the other way around. It is recommended to use Customer Managed Policies instead of Inline Policies.

The option that says: **Use Bastion Hosts** is incorrect because this relates more to your VPC Security than IAM. A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet.

References:

https://aws.amazon.com/iam/

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Check out this AWS Identity & Access Management (IAM) Cheat Sheet:

https://tutorialsdojo.com/aws-identity-and-access-management-iam/

Question 56:

Skipped

Which service would you use to speed up content delivery to your customers?

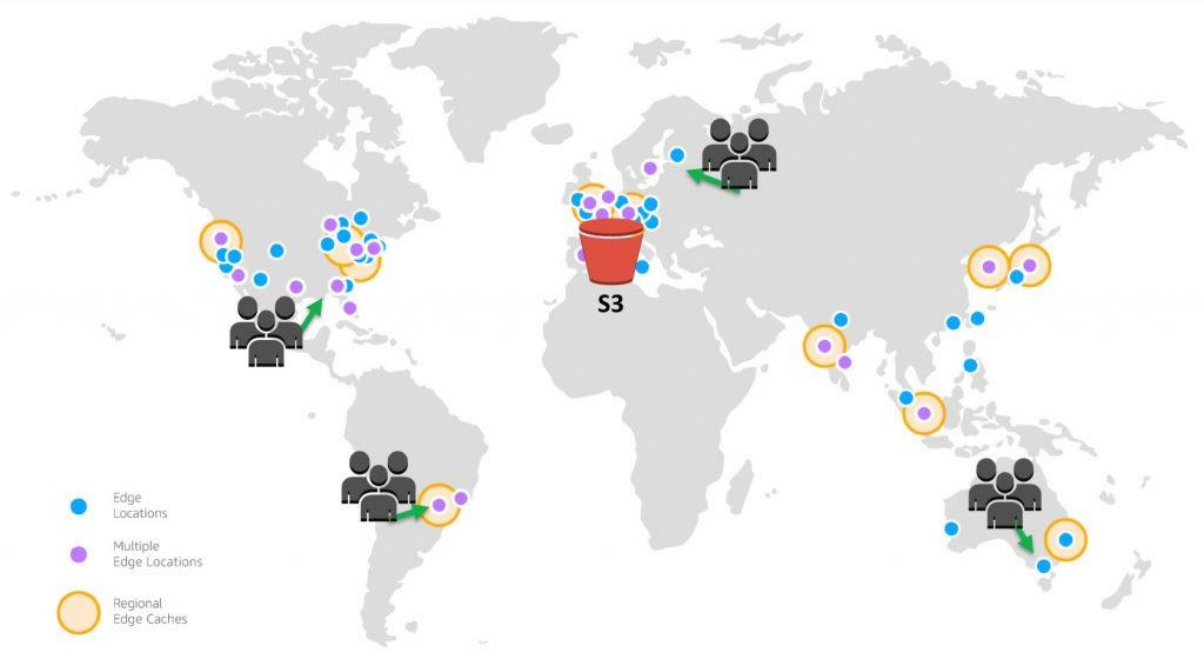
- **Amazon S3 Transfer Acceleration**
- **Amazon CloudWatch**
- **AWS CloudTrail**
- **Amazon CloudFront**

(Correct)

Explanation

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services. CloudFront works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code closer to customers' users and to customize the user experience. Lastly, if you use AWS origins such as Amazon S3, Amazon EC2 or

Elastic Load Balancing, you don't pay for any data transferred between these services and CloudFront.



You can get started with the Content Delivery Network in minutes, using the same AWS tools that you're already familiar with: APIs, AWS Management Console, AWS CloudFormation, CLIs, and SDKs. Amazon's CDN offers a simple, pay-as-you-go pricing model with no upfront fees or required long-term contracts, and support for the CDN is included in your existing AWS Support subscription.

Hence, the correct answer is: **Amazon CloudFront**.

Amazon S3 Transfer Acceleration only applies to S3 objects. It does not guarantee faster speeds as well. This service does not integrate with Amazon EC2 and the like.

Amazon CloudWatch is incorrect because it's a monitoring tool used to gather metrics on your AWS resources.

AWS CloudTrail is incorrect because it is another monitoring tool that captures API events in your account and lists them down in a history trail.

Reference:

https://aws.amazon.com/cloudfront/

Check out this Amazon CloudFront Cheat Sheet:

https://tutorialsdojo.com/amazon-cloudfront/

Question 57:

Skipped

A customer needs to establish a dedicated connection between their on-premises network and their AWS VPC that provides a more consistent network experience than Internet-based connections. Which of the following network services should they use?

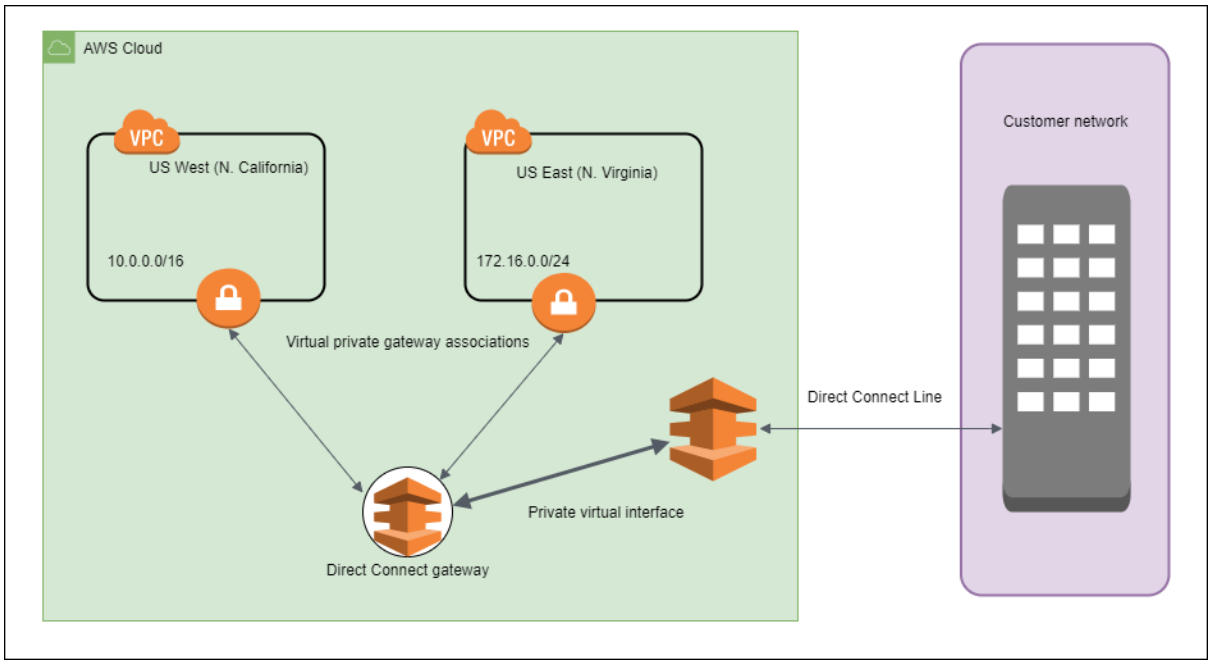
- **AWS Direct Connect**

  (Correct)

- **VPN Connection**
- **AWS VPN CloudHub**
- **VPC Peering**

Explanation

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. With the help of Direct Connect Partners, you can extend your preexisting data center or office network to a Direct Connect location. All AWS services, including Amazon Elastic Compute Cloud (EC2), Amazon Virtual Private Cloud (VPC), Amazon Simple Storage Service (S3), and Amazon DynamoDB can be used with Direct Connect.



Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Hence, the correct answer is: **AWS Direct Connect**.

VPN Connection and **AWS VPN CloudHub** are both incorrect because a VPN is an Internet-based connection, unlike Direct Connect which provides a dedicated connection. An Internet-based connection means that the traffic from the VPC and to the on-premises network traverses the public Internet, which is why it is slow. You should use Direct Connect instead.

VPC Peering is incorrect because this is mainly used to connect two or more VPCs and not your on-premises data center.

References:

https://aws.amazon.com/directconnect/

https://aws.amazon.com/products/networking/

Check out this AWS Direct Connect Cheat Sheet:

https://tutorialsdojo.com/aws-direct-connect/

Question 58:

Skipped

Which of the following is a valid characteristic of an IAM Group?

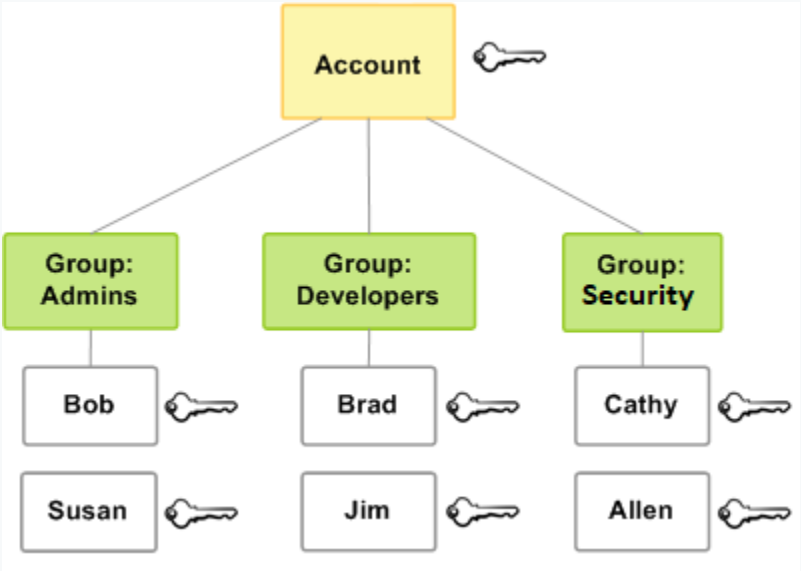
- **There is a default group that automatically includes all users in the AWS account.**
- **Groups can be nested.**
- **A group can contain many users, and a user can belong to multiple groups.**

  (Correct)

- **There's no limit to the number of groups you can have.**

Explanation

An **IAM group** is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a group called *Admins* and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group.



If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old groups and add him or her to the appropriate new groups.

Note that a group is not truly an "identity" in IAM because it cannot be identified as a `Principal` in a permission policy. It is simply a way to attach policies to multiple users at one time.

Following are some important characteristics of groups:

- A group can contain many users, and a user can belong to multiple groups.

- Groups can't be nested; they can contain only users, not other groups.

- There's no default group that automatically includes all users in the AWS account. If you want to have a group like that, you need to create it and assign each new user to it.

- There's a limit to the number of groups you can have, and a limit to how many groups a user can be in.

Hence, the correct answer is: **A group can contain many users, and a user can belong to multiple groups.**

The option that says: **Groups can be nested** is incorrect since this is not allowed in IAM Groups.

The option that says: **There's no limit to the number of groups you can have** is incorrect because there is actually a certain limit to the number of groups you can have as well as a limit to how many groups a user can be in.

The option that says: **There is a default group that automatically includes all users in the AWS account** is incorrect because there is no such thing as this in IAM Group.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_create.html

Check out this AWS Identity & Access Management (IAM) Cheat Sheet:

https://tutorialsdojo.com/aws-identity-and-access-management-iam/

Question 59:

Skipped

Which is a machine learning-powered security service that discovers, classifies, and protects sensitive data such as personally identifiable information (PII) or intellectual property?

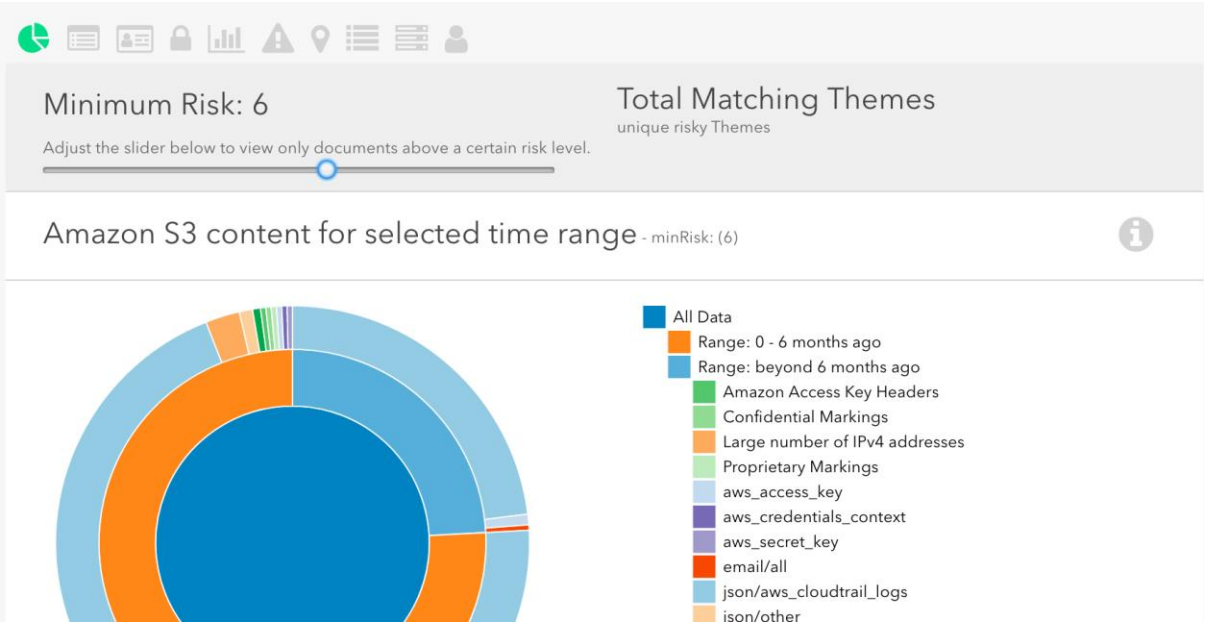
- **Amazon Rekognition**
- **Amazon Macie**

  (Correct)

- **Amazon Cognito**
- **Amazon GuardDuty**

Explanation

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks.



You can use Amazon Macie to protect against security threats by continuously monitoring your data and account credentials. Amazon Macie gives you an automated and low-touch way to discover and classify your business data and detect sensitive information such as personally identifiable information (PII) and credential data. When alerts are generated, you can use Amazon Macie for incident response, using Amazon EventBridge (Amazon CloudWatch Events) to swiftly take action to protect your data.

Hence, the correct answer is **Amazon Macie.**

Amazon Rekognition is incorrect. Although it is also a machine learning-based service like Amazon Macie, it is primarily used for image and video analysis. You can't use this to protect your sensitive data in AWS.

Amazon GuardDuty is incorrect because this is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

Amazon Cognito is incorrect because this is primarily used if you want to add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

References:

https://aws.amazon.com/macie/

https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html

Check out this Amazon Macie Cheat Sheet:

https://tutorialsdojo.com/amazon-macie/

AWS Security Services Overview - Secrets Manager, ACM, Macie:

https://youtu.be/ogVamzF2Dzk?si=clNxBHmzY9PHmwnm

Question 60:

Skipped

Which among the services below can you use to test and troubleshoot IAM and resource-based policies?

- **IAM Policy Simulator**

  (Correct)

- **Systems Manager**
- **Amazon Inspector**
- **AWS Config**

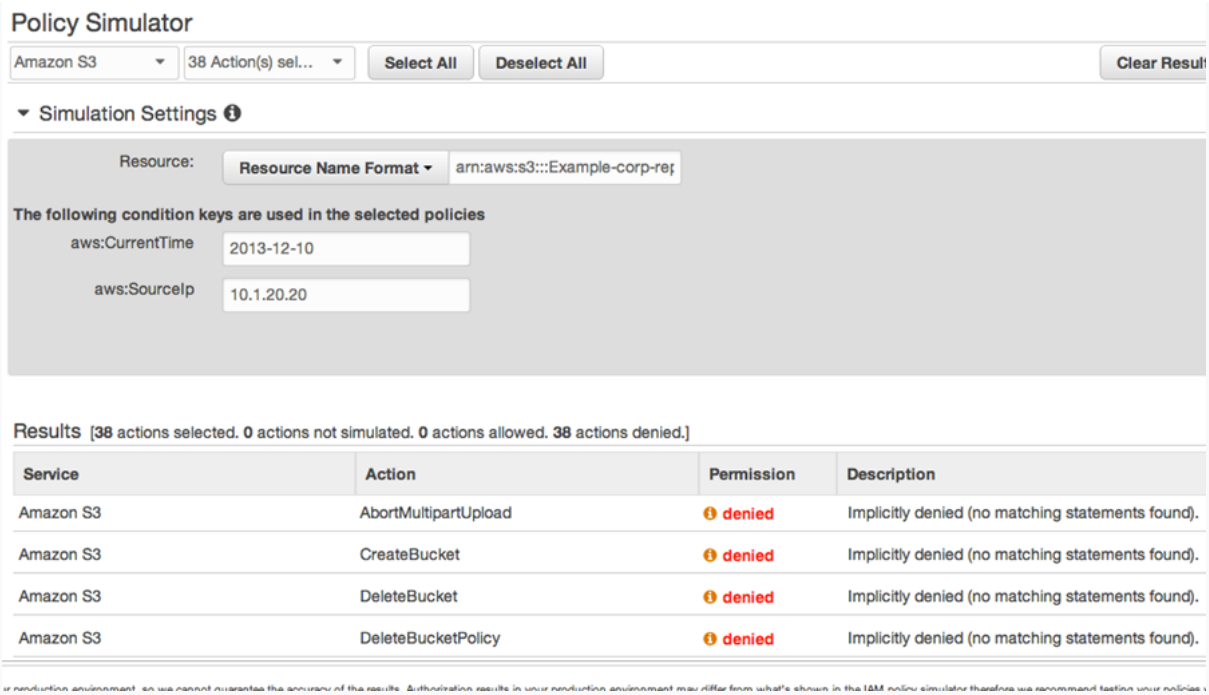
Explanation

The **IAM policy simulator** evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify. The simulator uses the same policy evaluation engine that is used during real requests to AWS services. But the simulator differs from the live AWS environment in the following ways:

- The simulator does not make an actual AWS service request, so you can safely test requests that might make unwanted changes to your live AWS environment.

- Because the simulator does not simulate running the selected actions, it cannot report any response to the simulated request. The only result returned is whether the requested action would be allowed or denied.

- If you edit a policy inside the simulator, these changes affect only the simulator. The corresponding policy in your AWS account remains unchanged.



With the IAM policy simulator, you can test and troubleshoot IAM and resource-based policies in the following ways:

- Test policies that are attached to IAM users, groups, or roles in your AWS account. If more than one policy is attached to the user, group, or role, you can test all the policies or select individual policies to test. You can test which actions are allowed or denied by the selected policies for specific resources.

- Test policies that are attached to AWS resources, such as Amazon S3 buckets, Amazon SQS queues, Amazon SNS topics, or Amazon S3 Glacier vaults.

- If your AWS account is a member of an organization in AWS Organizations, then you can test the impact of service control policies (SCPs) on your IAM policies and resource policies.

Hence, the correct answer is: **IAM Policy Simulator.**

AWS Config is incorrect because this is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

AWS Systems Manager is incorrect because this service 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. Unlike IAM Policy Simulator, it can't be used to simulate your policies.

Amazon Inspector is incorrect because it is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_testing-policies.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_iam_policy-sim-path-console.html

Check out this AWS Identity and Access Management (IAM) Cheat Sheet:

https://tutorialsdojo.com/aws-identity-and-access-management-iam/

Question 61:

Skipped

What is the most secure way to provide applications temporary access to your AWS resources?

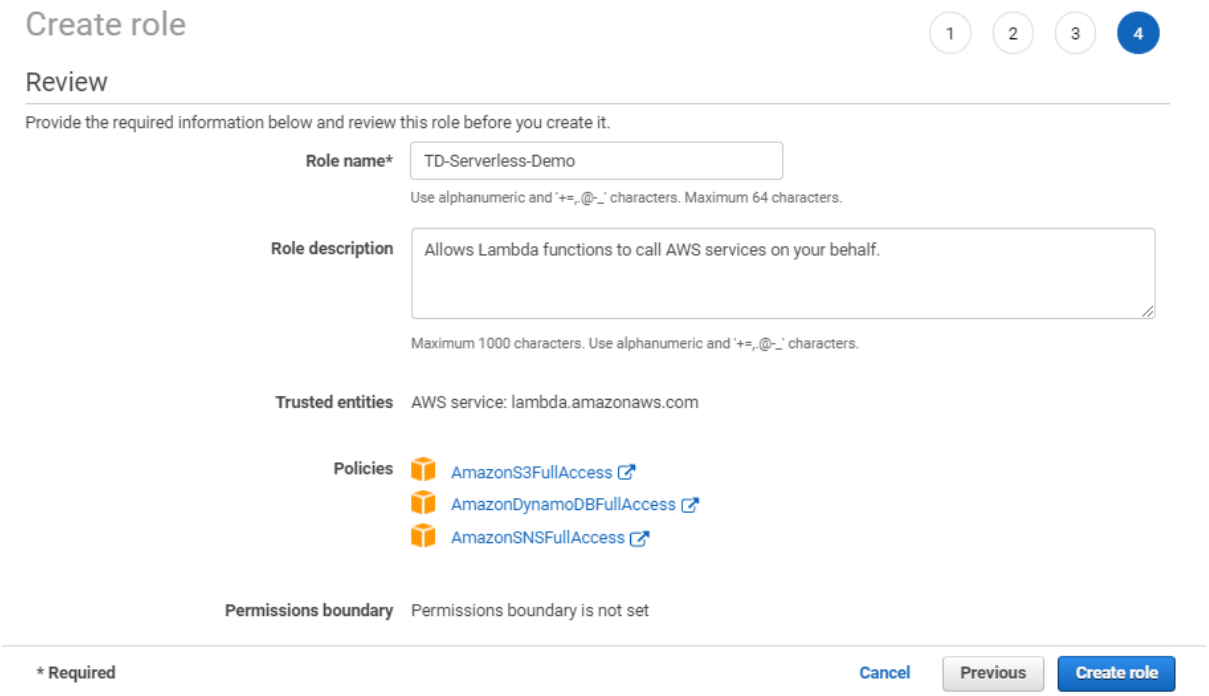
- **Create an IAM group that has access to the resources, and add the application there**
- **Create an IAM role and have the application assume the role**

  (Correct)

- **Create an IAM policy that allows the application to access the resources, and attach the policy to the application**
- **Create an IAM user with access keys and assign it to the application**

Explanation

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



An **IAM role** is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.

Hence, the correct answer is: **Create an IAM role and have the application assume the role**.

The option that says: **Create an IAM user with access keys and assign it to the application** is incorrect because an IAM User is primarily used for long-term credentials, not for temporary access.

The option that says: **Create an IAM group that has access to the resources, and add the application there** is incorrect because an IAM Group does not provide temporary access credentials.

The option that says: **Create an IAM policy that allows the application to access the resources, and attach the policy to the application** is incorrect because IAM policies are not entities that have credentials in AWS.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html

Check out this AWS Identity and Access Management (IAM) Cheat Sheet:

https://tutorialsdojo.com/aws-identity-and-access-management-iam/

Question 62:

Skipped

A customer has a number of on-demand instances running simultaneously to serve customer transactions. Occasionally, most of these instances do not perform any tasks when demand is low. What is a good cost optimization strategy to implement for this case?

- **Implement an auto scaling group to control the number of running instances at a time**

  (Correct)

- **Scale up the instances to a higher instance type to reduce the number of running instances at a time**
- **Create a script that would automatically shut down an instance when utilization is low**
- **Use spot instances instead of on-demand instances**

Explanation

Amazon EC2 Auto Scaling helps you maintain application availability and allows you to automatically add or remove EC2 instances according to conditions you define. You can use the fleet management features of EC2 Auto Scaling to maintain the health and availability of your fleet. You can also use the dynamic and predictive scaling features of EC2 Auto Scaling to add or remove EC2 instances. Dynamic scaling responds to changing demand and predictive scaling automatically schedules the right number of EC2 instances based on predicted demand. Dynamic scaling and predictive scaling can be used together to scale faster.

When your instances are experiencing varying levels of traffic, it is best to use an auto-scaling group to scale your instances based on the workload. So that when demand is low, the auto-scaling group can adjust the number of running instances to a bare minimum.

Hence, the correct answer is: **Implement an auto scaling group to control the number of running instances at a time**.

The option that says: **Scaling up your instances to a higher instance type** is incorrect since this will increase your AWS costs.

The option that says: **Using spot instances** is incorrect since this might affect your application. Spot instances can be terminated anytime the bid price changes. Although this might be cost-effective for you, it also affects your operations which should not happen.

The option that says: **Creating a script to shut down an instance** is incorrect because this is unnecessary. You would have to know when to start it up again, and it would be too much work than just using an auto-scaling group.

References:

https://aws.amazon.com/ec2/autoscaling/

https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

Check out this Amazon EC2 Cheat Sheet:

https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/

Question 63:

Skipped

Which of the following provides software solutions that are either hosted on or integrated with the AWS platform which may include Independent Software Vendors (ISVs), SaaS, PaaS, developer tools, management, and security vendors?

- **Concierge Support**
- **AWS Partner Network Consulting Partners**
- **Technical Account Management**
- **AWS Partner Network Technology Partners**

(Correct)

Explanation

The AWS Partner Network (APN) is focused on helping partners build successful AWS-based businesses to drive superb customer experiences. This is accomplished by developing a global ecosystem of *Partners* with specialties unique to each customer's needs.

There are two types of APN Partners:

1. **APN Consulting Partners**

2. **APN Technology Partners**

APN Consulting Partners are professional services firms that help customers of all sizes design, architect, migrate, or build new applications on AWS. Consulting Partners include System Integrators (SIs), Strategic Consultancies, Resellers, Digital Agencies, Managed Service Providers (MSPs), and Value-Added Resellers (VARs).

APN Technology Partners provide software solutions that are either hosted on or integrated with the AWS platform. Technology Partners include Independent Software Vendors (ISVs), SaaS, PaaS, developer tools, management, and security vendors.

Hence, the correct answer is: **APN Technology Partners.**

APN Consulting Partners is incorrect because this program helps customers to design, architect, migrate, or build new applications on AWS. You have to use APN Technology Partners instead.

Concierge Support is incorrect because this is a team composed of AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries and work with you to implement billing and account best practices so that you can focus on running your business.

Technical Account Management is incorrect because this is a part of AWS Enterprise Support which provides advocacy and guidance to help plan and build solutions using best practices, coordinate access to subject matter experts and product teams, and proactively keep your AWS environment operationally healthy.

References:

https://aws.amazon.com/partners/

https://aws.amazon.com/partners/consulting/journey/

https://aws.amazon.com/partners/technology/journey/

Question 64:

Skipped

A startup wants to move its on-premises infrastructure to AWS. The IT Security team wants to protect all of the applications against unintended and unauthorized access as well as potential vulnerabilities.

Which of the following capability of AWS CAF's Security perspective would be most relevant to address this concern?

- **Data Protection**
- **Infrastructure Protection**

(Correct)

- **Threat Detection**
- **Identity and Access Management**

Explanation

The **AWS Cloud Adoption Framework** is a comprehensive framework that intends to assist companies in planning, designing, and implementing their AWS cloud adoption journey. It provides a structured approach to cloud adoption based on best practices and lessons learned from AWS and its customers. AWS CAF is composed of six perspectives: Business, People, Governance, Platform, Security, and Operations. Each perspective comprises different capabilities that are functionally related to managing the cloud transformation journey.

The security perspective of the AWS Cloud Adoption Framework offers a range of capabilities to assist companies in securing their cloud infrastructure and applications on AWS. This viewpoint addresses companies' most prevalent security concerns by adopting data protection, identity and access management, network security, infrastructure protection, etc. However, Infrastructure Protection addresses every Chief Information Security Officer's concern about protecting their infrastructure from external threats. This capability includes a range of features that help to secure the underlying cloud infrastructure from unauthorized access and attacks. Thus, leveraging AWS CAF's Security perspective helps to simplify the process of securing the cloud infrastructure and reduce the risk of security breaches caused by human error or misconfiguration.

Hence the correct answer is: **Infrastructure Protection.**

Identity and Access Management is incorrect since this simply enables the CISCO to manage access to its cloud infrastructure by creating and managing AWS users, groups, and permissions. While IAM is essential to cloud security, this may not be the most relevant capability to address the CISCO's specific concern about external threats to the startup's infrastructure.

Data Protection is incorrect because this only focuses on securing data both at rest and in transit. Thus, it does not address the CISO's concerns about securing the underlying cloud infrastructure.

Threat Detection is incorrect because this only focuses on identifying security threats and vulnerabilities in the AWS environment. Therefore, it does not directly address CISCO's concern about protecting the infrastructure from external threats during the migration process.

References:

https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/foundational-capabilities.html

https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/security-perspective.html

Question 65:

Skipped

A company needs to troubleshoot an issue on their serverless application which is composed of an API Gateway, Lambda function, and a DynamoDB database. Which service should they use to trace user requests as they travel through their entire application?

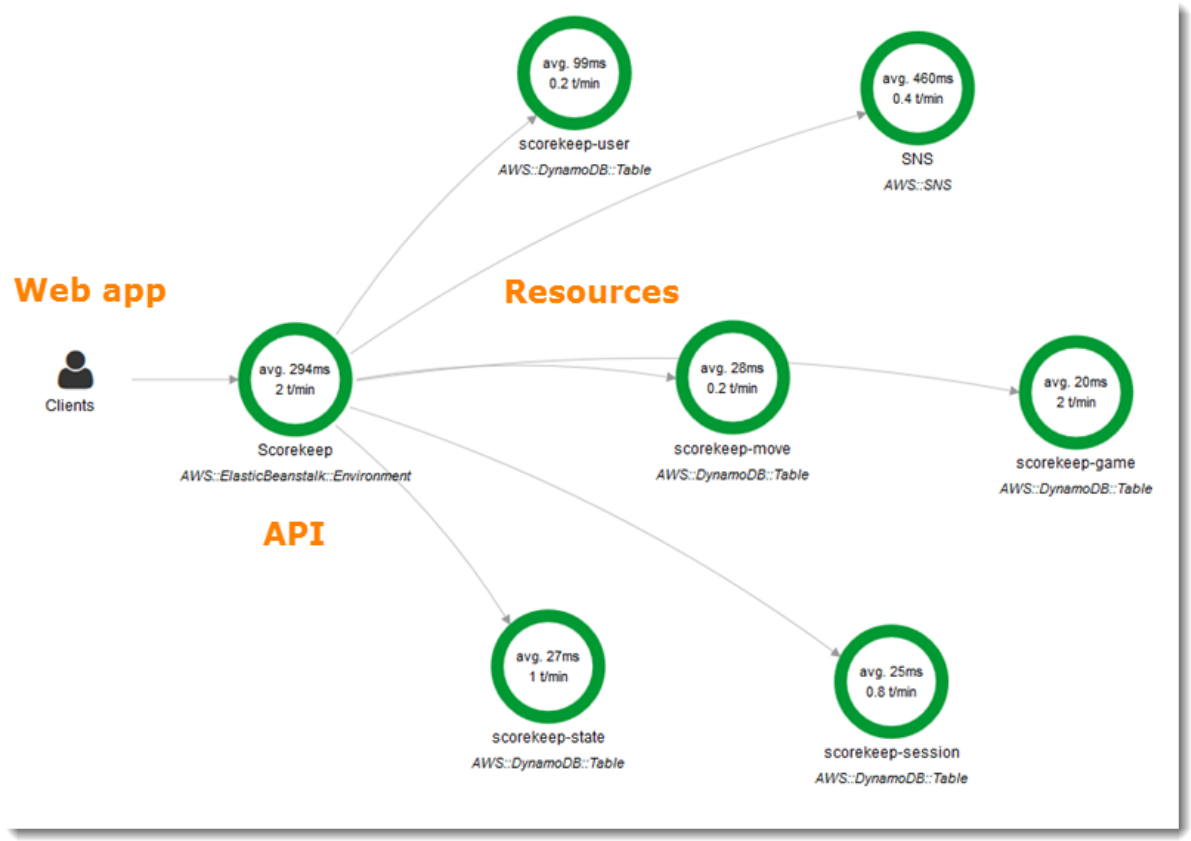
- **AWS X-Ray**

  (Correct)

- **AWS CloudTrail**
- **Amazon CloudWatch**
- **Amazon Inspector**

Explanation

AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components.



You can use X-Ray to analyze both applications in development and in production, from simple three-tier applications to complex microservices applications consisting of thousands of services.

AWS X-Ray works with Amazon EC2, Amazon EC2 Container Service (Amazon ECS), AWS Lambda, and AWS Elastic Beanstalk. You can use X-Ray with applications written in Java, Node.js, C# .NET, Python and Go that are deployed on these services.

Hence, the correct answer is **AWS X-Ray.**

Amazon CloudWatch is incorrect. Although you can troubleshoot the issue by checking the logs, it is still better to use AWS X-Ray as it enables you to analyze and debug your serverless application more effectively.

Amazon Inspector is incorrect because this is primarily used for EC2 and not for Lambda.

AWS CloudTrail is incorrect because this will only enable you to track all API calls to your Lambda, DynamoDB, and SNS. It is still better to use AWS X-Ray to debug your application.

References:

https://aws.amazon.com/xray/

https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html

Check out this AWS X-Ray Cheat Sheet:

https://tutorialsdojo.com/aws-x-ray/