

Question 1:

**Skipped**

Which AWS team can assist you when your systems are impacted by AWS resources engaging in abusive activities such as phishing, malware, spam, and denial of service (DoS) or distributed denial of service (DDoS) incidents?


- **Architecture Support**
- **Concierge Support**
- **AWS Trust & Safety**

**(Correct)**


- **AWS Support API**

**Explanation**

**AWS Abuse** addresses many different types of potentially abusive activities such as phishing, malware, spam, and denial of service (DoS) or distributed denial of service (DDoS) incidents. When abuse is reported, AWS alerts customers so they can take the remediation action that is necessary.



English ▾

Console Log in 

### Details of reported abuse

If we are able to identify an EC2 customer responsible for the reported abuse, we will forward them the information that you provide below. We will not share the private information you provided in the previous section, but our customer can respond to you indirectly via email using our response web form.

Source IP address

The source IP address of the reported abuse

24.212.5.193

Destination IP addresses - *optional*

The destination IP address(es) of the reported abuse

Use commas to separate multiple IP addresses

Destination ports and protocols - *optional*

22/TCP


Destination URLs - *optional*

Use spaces to separate URLs

Time zone

(GMT +8:00) Beijing, Perth, Singapore, Hong Kong ▾

Abuse date

2021/09/15 

Abuse time

12:51

Enter the exact time that the abuse occurred in 24-hour format

☐ The host clock is synchronized by Network Time Protocol (NTP)

Your tracking reference - *optional*

Nominate an optional tracking identifier for your own reference

Type of abuse

Hosting a site advertised in spam ▾

The AWS Trust & Safety team can assist you when AWS resources are used to engage in the following types of abusive behavior:

**Spam:** You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are used to spam websites or forums.

**Port scanning:** Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server, and you believe this is an attempt to discover unsecured ports.

**Denial-of-service (DoS) attacks:** Your logs show that one or more AWS-owned IP addresses are used to flood ports on your resources with packets, and you believe that this is an attempt to overwhelm or crash your server or the software running on your server.

**Intrusion attempts:** Your logs show that one or more AWS-owned IP addresses are used to attempt to log in to your resources.

**Hosting objectionable or copyrighted content:** You have evidence that AWS resources are used to host or distribute illegal content or distribute copyrighted content without the consent of the copyright holder.

**Distributing malware:** You have evidence that AWS resources are used to distribute software that was knowingly created to compromise or cause harm to computers or machines on which it is installed.

Hence, the correct answer is **AWS AWS Trust & Safety**.

**Concierge Support** is incorrect because this is a team of experts that 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.

**AWS Support API** is incorrect because this is not a team in AWS, but a collection of APIs that provides programmatic access to AWS Support Center features. This is primarily used to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status.

**Architecture Support** is incorrect because this is a team that guides customers on how AWS services fit together to meet a specific architecture, use-case, workload, or application.

## References:

<https://aws.amazon.com/premiumsupport/knowledge-center/aws-abuse-report/>

<https://aws.amazon.com/blogs/mt/automating-processes-for-handling-and-remediating-aws-abuse-alerts/>

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

Question 2:

### Skipped

The Chief Technology Officer wants to control the use of services across multiple AWS accounts using AWS Organizations. Which of the following must be used to satisfy this requirement?

- **AWS Secrets Manager**
- **AWS Systems Manager**
- **Resource-based policy**
- **Service Control Policy**

(Correct)

### Explanation

**AWS Organizations** helps you centrally govern your environment as you grow and scale your workloads on AWS. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance.

[AWS Organizations](#) > Policies

## Policies

Policies in AWS Organizations enable you to manage different features of the AWS accounts in your organization. [Learn more](#)

### Supported policy types

Policy type	Status
<b>AI services opt-out policies</b> Artificial Intelligence (AI) services opt-out policies enable you to control whether AWS AI services can store and use your content. <a href="#">Learn more</a>	⊖ Disabled
<b>Backup policies</b> Backup policies enable you to deploy organization-wide backup plans to help ensure compliance across your organization's accounts. Using policies helps ensure consistency in how you implement your backup plans. <a href="#">Learn more</a>	⊖ Disabled
<b>Service control policies</b> Service control policies (SCPs) enable central administration over the permissions available within the accounts in your organization. This helps ensure that your accounts stay within your organization's access control guidelines. <a href="#">Learn more</a>	⊕ Enabled
<b>Tag policies</b> Tag policies help you standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values. <a href="#">Learn more</a>	⊖ Disabled

In SCPs, you can restrict which AWS services, resources, and individual API actions the users and roles in each member account can access. You can also define conditions for limiting access to AWS services, resources, and API actions.

Hence, the correct answer is: **Service Control Policy**.

**Resource-based policy** is incorrect. Although it can be used to control access, they are linked directly to a specific AWS resource and not managed through AWS Organizations.

**AWS Systems Manager** is incorrect because this just automates common maintenance and deployment tasks of EC2 instances and other AWS resources. It doesn't provide you control of services across multiple AWS accounts.

**AWS Secrets Manager** is incorrect because it only helps you protect secrets or credentials that are needed to access your applications, services, and IT resources. You can't restrict AWS services in your AWS Organizations using this service. The AWS Secrets Manager only enables you to easily rotate, manage, and retrieve credentials.

#### References:

<https://aws.amazon.com/organizations/>

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_example-scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html)

#### Check out this AWS Organizations Cheat Sheet:

<https://tutorialsdojo.com/aws-organizations/>

Question 3:

#### Skipped

In AWS, \_\_\_\_\_ is a managed service that enables you to easily create and control the encryption keys used for cryptographic operations without having to manage your own hardware module.

- **AWS Systems Manager**
- **AWS IAM**
- **AWS KMS**

**(Correct)**

- **AWS CloudHSM**

#### Explanation

**AWS KMS** is a managed service that easily enables you to create and control the keys used for cryptographic operations. The service provides a highly available key generation, storage, management, and auditing solution for you to encrypt or digitally sign data within your own applications or control the encryption of data across AWS services.

## Configure key

Key type [Help me choose](#)

☒ Symmetric  
A single encryption key that is used for both encrypt and decrypt operations

☐ Asymmetric  
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

### ▼ Advanced options

Key material origin  
[Help me choose](#)

- ☒ KMS  
☐ External  
☐ Custom key store (CloudHSM)

Regionality  
You cannot change this setting after the key is created. [Help me choose](#)

- ☒ Single-Region key  
Never allow this key to be replicated into other Regions  
☐ Multi-Region key  
Allow this key to be replicated into other Regions

Cancel

Next

KMS is a managed service that enables you to encrypt your data easily. It provides a highly available key storage, management, and auditing solution for you to encrypt data within your own applications and control the encryption of stored data across AWS services.

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

**AWS Systems Manager** is incorrect because this service simply gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. You cannot encrypt data in your AWS resources using AWS SSM.

**AWS IAM** is incorrect because this is just a service used to manage users, roles, and groups to AWS services and resources securely. This service does not provide a highly available HSM to encrypt data.

**AWS CloudHSM** is incorrect because this provides hardware security modules in the AWS Cloud that you can manage and control. Remember that in the scenario, the requirement is that you must be able to manage your encryption keys without having to manage your own hardware module. A hardware security module (HSM) is a

computing device that processes cryptographic operations and provides secure storage for cryptographic keys. If you want a managed service to create and control your encryption keys, but don't want to operate your own HSM, consider using AWS Key Management Service.

#### References:

<https://aws.amazon.com/kms/>

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

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

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

#### Check out this AWS KMS Cheat Sheet:

<https://tutorialsdojo.com/aws-key-management-service-aws-kms/>

Question 4:

#### Skipped

The security team needs to automate security vulnerability assessments throughout their development and production environments. Which service should they use to comply with this requirement?

- 

**Amazon Inspector**

**(Correct)**

- AWS Shield
- AWS WAF
- AWS Config

#### Explanation

**Amazon Inspector** allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations. Amazon Inspector is an API-driven service that uses an optional agent, making it easy to deploy, manage, and automate. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

<input type="checkbox"/>	Name	Duration	Target name	Last run	All runs
<input checked="" type="checkbox"/>	Assessment-Template-TutorialsDojo-Network	N/A	Assessment-Target-All-Instances-Network		

### Assessment Template - Assessment-Template-TutorialsDojo-Network

**Name** Assessment-Template-TutorialsDojo-Network

**ARN** arn:aws:inspector:us-east-1:189630120175:target/0-Q7QQZ3VQ/template/0-7PqaD4AY

**Target name** [Assessment-Target-All-Instances-Network](#) Preview Target

**Rules packages**

- Common Vulnerabilities and Exposures-1.1
- CIS Operating System Security Configuration Benchmarks-1.0
- Network Reachability-1.1
- Security Best Practices-1.0

**Security Assessments**

Preview Exclusions

**Duration** 1 Hour (Recommended)

**SNS topics** [+](#)

**Assessment Events** [+](#)

Rule Type	Rule Name
Scheduled Event	Amazon_Inspector_Assessment_0-5K35zzW0_Idgcjee

Click below to set up recurring assessment runs once every  days, with the first run **starting now**. [Learn more](#)

Add schedule

Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances.

Hence, the correct answer in this scenario is: **Amazon Inspector**.

**AWS Shield** is incorrect because this option is not a security assessment service. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. In addition, AWS Shield is mainly used to protect web applications, TCP-based applications, and UDP-based game servers against a DDoS attack.

**AWS WAF** is incorrect since this is a web application firewall that helps protect your web applications from common web exploits such as XSS and SQL injection, and not for automated security vulnerability assessments. You use AWS WAF to create custom rules that block common attack patterns and rules that are designed for your specific application.

**AWS Config** is incorrect because it is not intended specifically for automated security vulnerability assessments. Although AWS Config can keep track of changes to security groups, network ACLs, and other resources, it doesn't perform vulnerability scans that can identify security problems in applications, operating systems, or other components.



## References:

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

[https://docs.aws.amazon.com/inspector/latest/userguide/inspector\\_introduction.html](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html)

## Check out this Amazon Inspector Cheat Sheet:

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

Question 5:

### Skipped

A company has a suite of enterprise applications and wants to migrate its entire system to the AWS Cloud. The company needs to demonstrate incremental business value and gather crucial insights for future scaling and development.

Which phase of the cloud transformation journey includes these activities in AWS CAF?

- Scale
- Align
- Launch

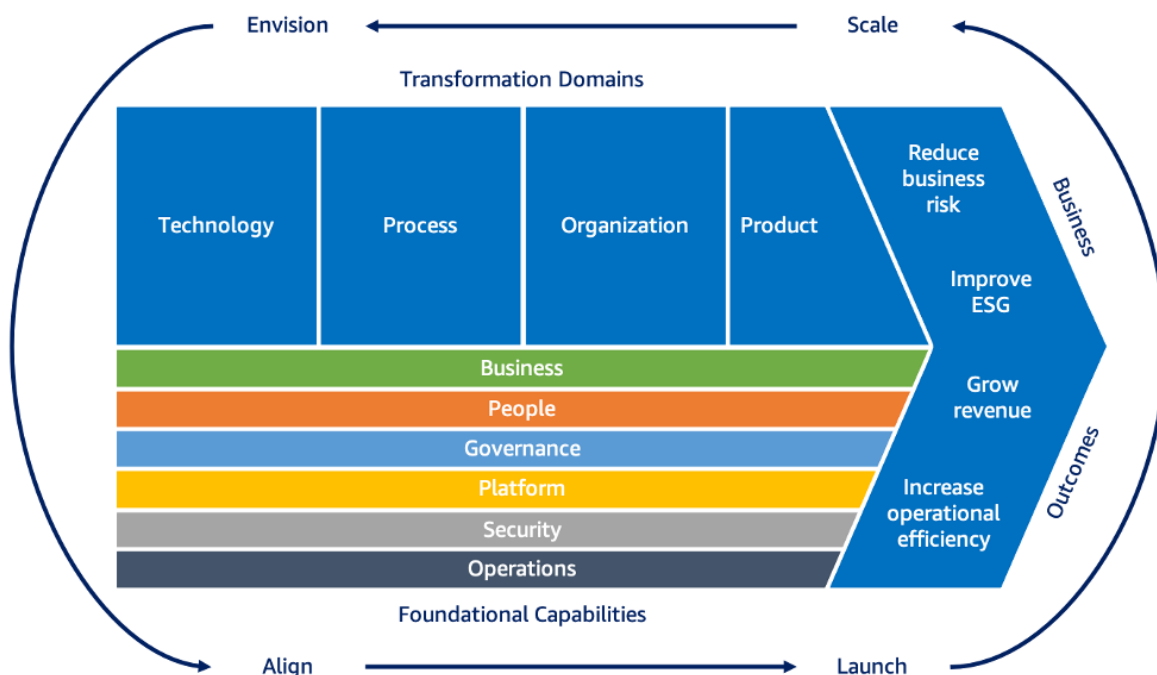
(Correct)

- Envision

### Explanation

The **AWS Cloud Adoption Framework (AWS CAF)** leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Adopting an iterative approach will help you maintain momentum and evolve your roadmap as you learn from experience. The AWS CAF recommends four iterative and incremental cloud transformation phases, shown below.



The **Launch phase** focuses on delivering pilot initiatives in production and on demonstrating incremental business value. Pilots should be highly impactful, and if/when successful, they will help influence future direction. Learning from pilots will help you adjust your approach before scaling to full production.

Hence, the correct answer is **Launch**.

**Envision** is incorrect because it primarily focuses on demonstrating how the cloud will help accelerate business outcomes rather than demonstrating incremental business value.

**Scale** is incorrect because it only expands pilots and business value to the desired scale. While it focuses on ensuring the realization and sustainability of cloud-related benefits, it does not involve the delivery of pilots in a production environment or gathering crucial insights for future scaling and development.

**Align** is incorrect because it just focuses on identifying capability gaps across the different AWS CAF perspectives. The Align phase prioritizes the process of identifying cross-organizational dependencies as well as surfacing stakeholder concerns and challenges.

## References:

<https://aws.amazon.com/cloud-adoption-framework/>

<https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/your-cloud-transformation-journey.html>

**Check out this AWS Cloud Adoption Framework:**

<https://tutorialsdojo.com/aws-cloud-adoption-framework-aws-caf/>

Question 6:

**Skipped**

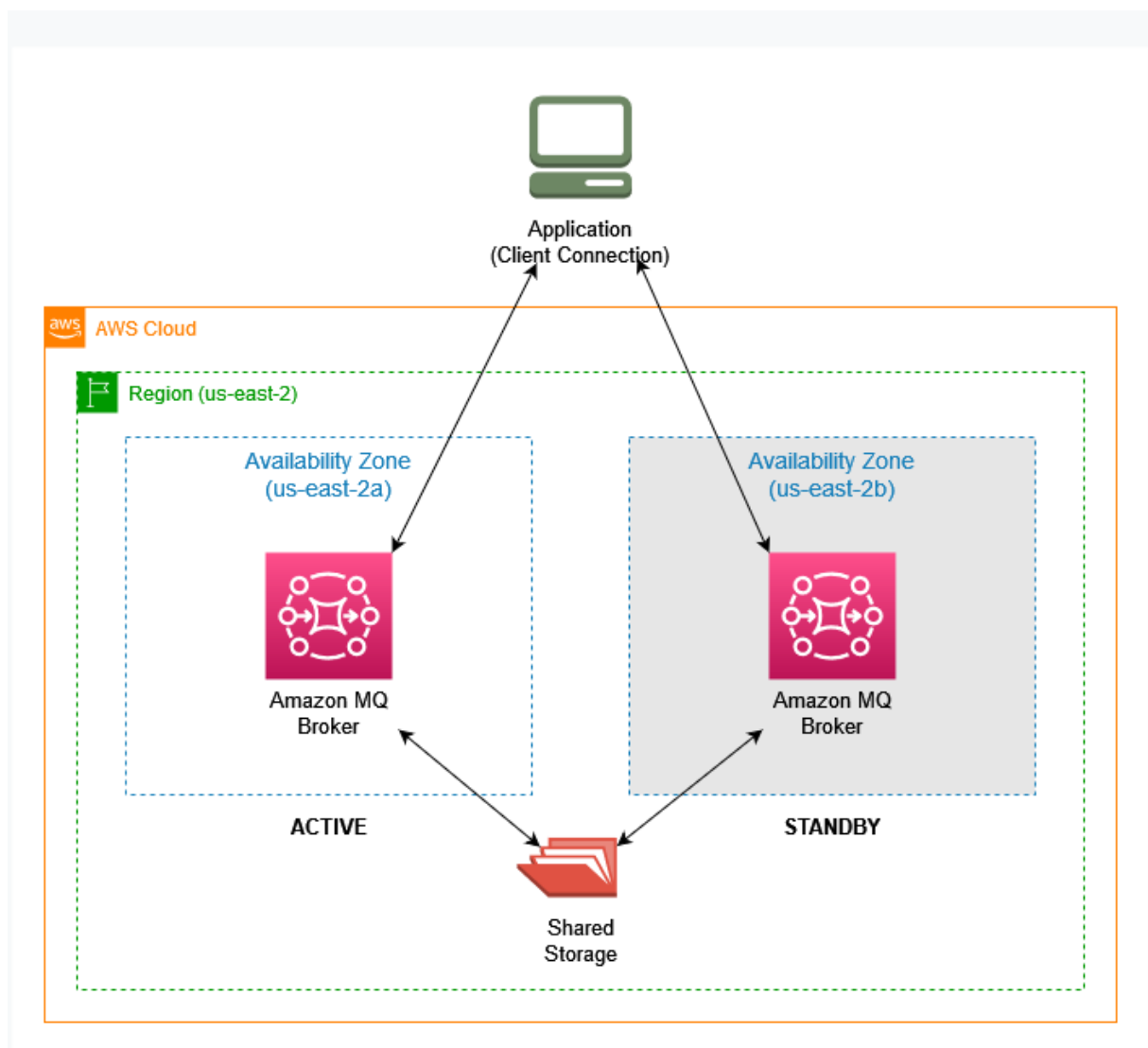
A developer needs to set up a message broker service for Apache ActiveMQ for its enterprise application running in AWS. Which service should be used in this scenario?

- Amazon Simple Email Service
- Amazon WorkMail
- Amazon Chime
- Amazon MQ

**(Correct)**

**Explanation**

**Amazon MQ** is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Amazon MQ manages the administration and maintenance of ActiveMQ, a popular open-source message broker. You can also get direct access to the ActiveMQ console and industry-standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket.



With Amazon MQ, you can easily move from any message broker that uses these standards to Amazon MQ because you don't have to rewrite any messaging code in your applications.

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

**Amazon Simple Email Service** is incorrect because this is only a cloud-based email sending service and not a message broker service for Apache ActiveMQ. Amazon SES is designed to help digital marketers and application developers send marketing, notification, and transactional emails.

**Amazon Chime** is incorrect because this is simply a communications service that lets you meet, chat, and place business calls inside and outside your organization, all using a single application. This service is not suitable for setting up a message broker service.

**Amazon WorkMail** is incorrect because this is just a service to manage your corporate email infrastructure and eliminates the need for up-front investments to license and provision on-premises email servers. This service does not provide direct

access to the ActiveMQ console and industry-standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket.

#### References:

<https://aws.amazon.com/amazon-mq/faqs/>

<https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/welcome.html>

#### Check out this Amazon MQ Cheat Sheet:

<https://tutorialsdojo.com/amazon-mq/>

Question 7:

#### Skipped

Which of the following benefits do AWS Organizations provide? (Select TWO.)

- **Allow Active Directory access controls**
- **Automate AWS account creation and management**

**(Correct)**

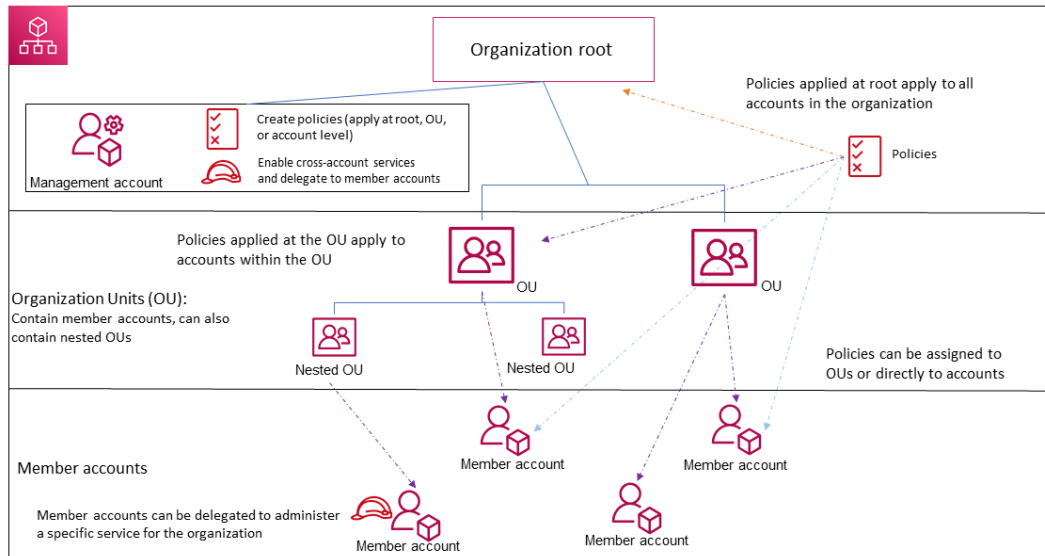
- **Ability to create IAM Roles**
- **Centrally manage policies across multiple AWS accounts**

**(Correct)**

- **Records AWS API calls**

#### Explanation

**AWS Organizations** helps you centrally govern your environment as you grow and scale your workloads on AWS. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance.



AWS Organizations benefits are:

- Centrally Manage Policies across Multiple AWS Accounts
- Automate AWS Account Creation and Management
- Consolidate Billing across Multiple AWS Accounts
- Govern Access to AWS Services, Resources, and Regions
- Configure AWS Services Across Multiple Accounts

Hence, the correct options that correctly describe AWS Organizations are:

- Automate AWS account creation and management
- Centrally manage policies across multiple AWS accounts

The option that says: **Ability to create IAM Roles** is incorrect because this is a feature of AWS IAM and not AWS Organizations. It uses roles to delegate access to users, applications, or services that don't normally access your AWS resources.

The option that says: **Allow Active Directory access controls** is incorrect because it is not a benefit of AWS Organizations. This option is related to AWS Managed Microsoft AD.

The option that says: **Records AWS API calls** is incorrect because this function is under AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in your AWS environment. AWS Organizations do not provide an event history of your AWS account.

## References:

<https://aws.amazon.com/organizations/>

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_introduction.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html)

## Check out this AWS Organizations Cheat Sheet:

<https://tutorialsdojo.com/aws-organizations/>

Question 8:

### Skipped

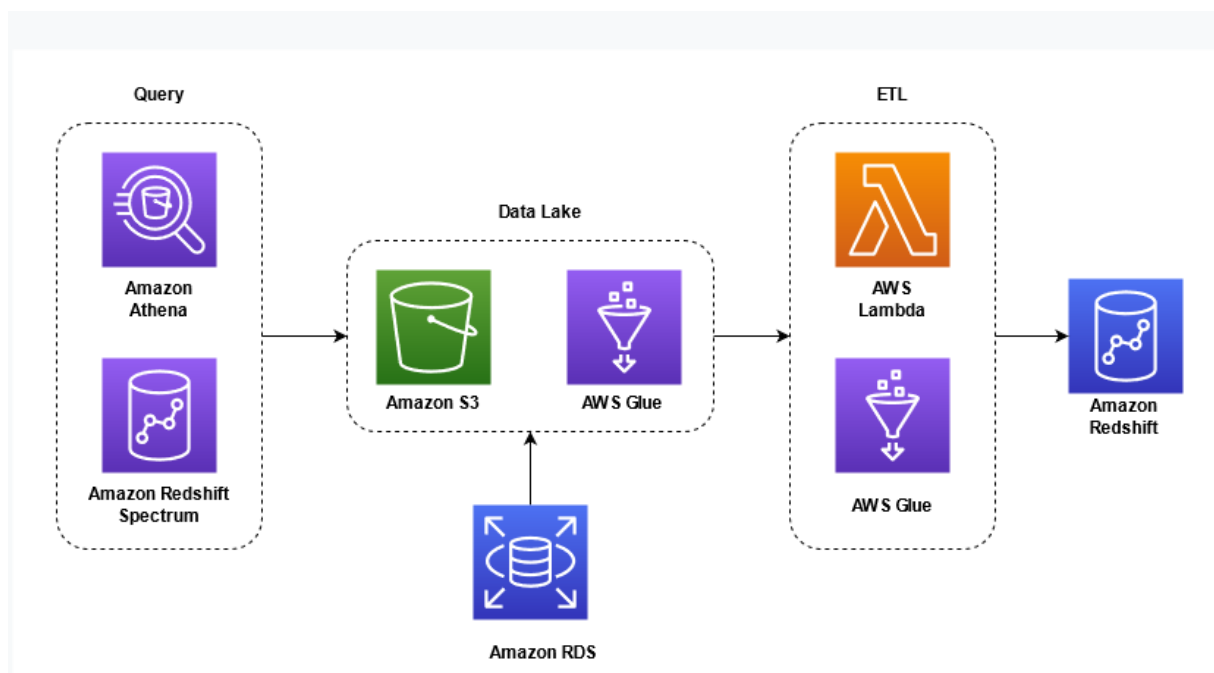
Which service should you use to run complex analytic queries against terabytes to petabytes of structured data?

- **Amazon S3**
- **Amazon DynamoDB**
- **Amazon Neptune**
- **Amazon Redshift**

**(Correct)**

### Explanation

**Amazon Redshift** is a fully-managed petabyte-scale cloud-based data warehouse product designed for large-scale data set storage and analysis. It allows you to run complex analytic queries against terabytes to petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.



Amazon Redshift has a feature of deepest integration with your data lake and AWS services. It lets you quickly and simply work with your data in open formats, including Avro, CSV, Grok, Amazon Ion, JSON, ORC, Parquet, RCFile, RegexSerDe, Sequence, Text, and TSV.

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

**Amazon DynamoDB** is incorrect because it is a NoSQL Database Service and not a cloud-based data warehouse for online analytic processing (OLAP) and business intelligence (BI) applications. DynamoDB is used for key-value and document database that delivers single-digit millisecond performance. It can also store the metadata of assets such as images, pages, and links, but this service does not natively support SQL.

**Amazon S3** is incorrect because this is an object storage service that offers industry-leading scalability, data availability, security, and performance. Amazon S3 is not a cloud-based data warehouse. It is primarily used for static website hosting, data storage, and archiving.

**Amazon Neptune** is incorrect because this is a Graph Database service that makes it easy for you to build and run applications that work with highly connected datasets. It is mainly used for recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security but not for running complex analytic queries.

## References:

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



<https://docs.aws.amazon.com/redshift/latest/gsg/getting-started.html>

**Amazon Redshift Overview:**

<https://youtu.be/jlLERNzhHOg>

**Check out this Amazon Redshift Cheat Sheet:**

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

Question 9:

**Skipped**

An e-commerce company is currently undergoing a technological transformation to modernize its infrastructure and transfer its operations to the cloud. The company's Chief Technology Officer (CTO) has decided to adopt Amazon Web Services (AWS) as its cloud service provider and intends to follow the AWS Cloud Adoption Framework (CAF) methodology to achieve this goal.

Which perspective of the AWS CAF would be most helpful in ensuring successful outcomes in this scenario?

- **People**
- **Business**
- **Governance**
- **Platform**

**(Correct)**

**Explanation**

The AWS CAF's Platform perspective focuses on the technical aspects of cloud adoption. This includes selecting the appropriate cloud services, designing the architecture, and managing the infrastructure.

# AWS CAF perspectives and foundational capabilities



## Business

Ensure that cloud investments accelerate your digital transformation ambitions and business outcomes.

- Strategy Management
- Innovation Management
- Strategic Partnership
- Business Insights
- Product Management
- Portfolio Management
- Data Science
- Data Monetization



## People

Evolve to a culture of continuous growth and learning, where change becomes business-as-usual.

- Culture Evolution
- Workforce Transformation
- Transformational Leadership
- Organizational Alignment
- Change Acceleration
- Organization Design
- Cloud Fluency



## Governance

Orchestrate cloud initiatives, maximize organizational benefits, and minimize transformation-related risks.

- Program and Project Management
- Cloud Financial Management
- Application Portfolio Management
- Risk Management
- Benefits Management
- Data Curation
- Data Governance



## Platform

Accelerate delivery of cloud workloads via an enterprise-grade, scalable, hybrid cloud environment.

- Platform Architecture
- Platform Engineering
- Provisioning and Orchestration
- Modern Application Development
- Data Engineering
- Data Architecture
- Continuous Integration and Delivery



## Security

Achieve confidentiality, integrity, and availability of data and cloud workloads.

- Infrastructure Protection
- Security Governance
- Vulnerability Management
- Incident Response
- Application Security
- Threat Detection
- Data Protection
- Security Assurance
- Identity and Access Management



## Operations

Ensure cloud service delivery at a level that satisfies your business stakeholders.

- Event Management (AIOps)
- Incident and Problem Management
- Configuration Management
- Application Management
- Performance and Capacity
- Patch Management
- Availability and Continuity Management
- Observability
- Change and Release Management

In the scenario, the Platform perspective can give guidance to the company in understanding the technical aspects of AWS services, architecture patterns, security, and operational considerations. This knowledge enables them to make informed decisions about selecting and configuring the appropriate AWS services to support their workloads, such as compute, storage, databases, and networking.

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

**Governance** is incorrect. The governance perspective focuses on implementing processes, policies, and controls to ensure compliance, manage risks, and optimize resource usage. However, it does not directly cover the operational readiness of the organization.

**Business** is incorrect because the question pertains to technological transformation and infrastructure modernization. From a business perspective, the focus is on aligning cloud adoption with the organization's goals and maximizing its overall value.

**People** is incorrect. This perspective emphasizes the skills and knowledge needed for successful cloud adoption through employee training and support. While it is important, the Platform perspective would be more relevant in the scenario since it deals with the actual technical considerations and cloud infrastructure design.

## References:

<https://aws.amazon.com/cloud-adoption-framework/>

<https://aws.amazon.com/what-is-cloud-computing/><https://docs.aws.amazon.com/whitepapers/latest/aws-caf-operations-perspective/aws-caf-operations-perspective.html>

Question 10:

### Skipped

Which of the following is an AWS service that provides secure key storage and cryptographic operations, such as encryption and decryption, hashing, and digital signing?

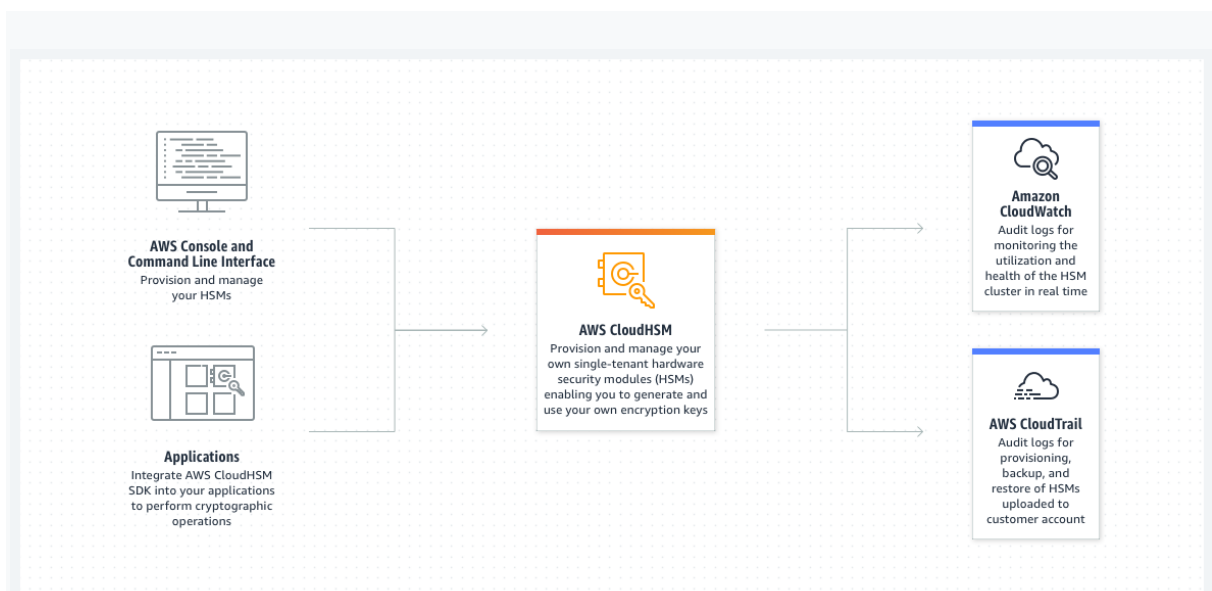
- AWS GuardDuty
- AWS Secrets Manager
- AWS CloudHSM

(Correct)

- AWS Inspector

### Explanation

**AWS CloudHSM** is an AWS service that enables the creation and maintenance of hardware security modules (HSMs) in your AWS environment for cryptographic purposes. These HSMs are devices that process cryptographic operations and securely store cryptographic keys. By using AWS CloudHSM, you can offload SSL/TLS processing for web servers, as well as provide protection for critical data such as financial records, personally identifiable information (PII), and intellectual property.



HSMs are arranged in clusters that are synchronized collections of HSMs in a specific Availability Zone (AZ). By increasing the number of HSMs in a cluster and distributing clusters across AZs, you can balance a load of cryptographic operations in your cloud environment and ensure high availability and redundancy in the event of an AZ outage. AWS CloudHSM also generates backups of your clusters at regular intervals and stores them securely, making it easy and secure to recover your data.

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

**AWS Secrets Manager** is incorrect because it only enables you to securely store and manage secrets, such as database credentials and API keys, but it does not provide key storage and cryptographic operations as AWS CloudHSM does.

**AWS GuardDuty** is incorrect because it is a threat detection service that continuously monitors and analyzes AWS account activity and helps to identify potential security threats and vulnerabilities. It is not a service that provides secure key storage or cryptographic operations such as encryption and decryption, hashing, and digital signing.

**AWS Inspector** is incorrect because it is a security assessment service that automatically assesses applications for vulnerabilities or deviations from best practices. It is not a service that provides secure key storage or cryptographic operations such as encryption and decryption, hashing, and digital signing.

## References:

<https://aws.amazon.com/cloudhsm/>

<https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-hsm.html>

Check out this AWS CloudHSM Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudhsm/>

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

<https://youtu.be/-1S-RdeAmMo>

Question 11:

**Skipped**

Which of the following cost management capabilities does AWS immediately provide you even before you create your AWS account?

- **Allows you to organize your resources according to your own cost allocation tagging strategy.**
- **Allows you to estimate your monthly spending in AWS.**

**(Correct)**

- **Allows you to request billing discounts in exchange for a committed level of instance usage.**
- **Allows you to create monthly reports on the cost behavior of your resources.**

**Explanation**

The **AWS Pricing Calculator** is an estimation tool that provides an approximate cost of using AWS services based on the usage parameters that you specify. AWS lets you estimate your possible monthly and yearly spending with no commitment through the AWS Pricing Calculator, and lets you explore AWS services and pricing for your architecture needs.

## EC2 instance specifications [Info](#)

### Operating system

Choose which operating system you'd like to run Amazon EC2 instances on.

Linux

### Instance type

#### t3.micro

On-Demand hourly cost

0.0104

vCPUs

2

GPUs

NA

1YR Std reserved hourly cost

0.0065

Memory (GiB)

1 GiB

Network performance

Up to 5 Gigabit

## Pricing strategy [Info](#)

### Pricing model

- ☐ EC2 Instance Savings Plans
- ☐ Compute Savings Plans
- ☐ Standard Reserved Instances
- ☐ Convertible Reserved Instances
- ☒ On-Demand Instances

### Reservation term

- ☐ 1 Year
- ☐ 3 Year

### Payment options

- ☐ No Upfront
- ☐ Partial Upfront
- ☐ All Upfront

### ▼ Show calculations

1 instances x 0.0104 USD x 730 hours in a month = 7.59 USD (monthly onDemand cost)

**Amazon EC2 On-Demand instances (monthly): 7.59 USD**

AWS Pricing Calculator is useful both for people who have never used AWS and for users who want to reorganize or expand their AWS usage. You can use this tool to model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. Pricing Calculator is free to use even if you have not created your own AWS account yet.

Hence, the correct answer is: **Allows you to estimate your monthly spending in AWS.**

The option that says: **Allows you to organize your resources according to your own cost allocation tagging strategy** is incorrect since you can only apply cost allocation tags to AWS resources that you have running, which means that you should have your own account by this time already.

The option that says: **Allows you to create monthly reports on the cost behavior of your resources** is incorrect since you can only create billing reports when you have historical spending data in AWS already.

The option that says: **Allows you to request billing discounts in exchange for a committed level of instance usage** is incorrect since you can only receive discounts for your instances by purchasing Reserved Instances or Savings Plans in an AWS account.

## References:

<https://docs.aws.amazon.com/pricing-calculator/latest/userguide/what-is-pricing-calculator.html>

<https://aws.amazon.com/aws-cost-management/>

## Check out this AWS Pricing Cheat Sheet:

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

Question 12:

### Skipped

What types of caching solutions are available in Amazon ElastiCache? (Select TWO.)

- **Amazon ElastiCache for Apache Kafka**
- **Amazon ElastiCache for Apache Ignite**
- **Amazon ElastiCache for Redis**

**(Correct)**

- **Amazon ElastiCache for Serverless**
- **Amazon ElastiCache for Memcached**

**(Correct)**

### Explanation

**Amazon ElastiCache** allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores.



## Create your Amazon ElastiCache cluster

Cluster engine ☒ **Redis**

In-memory data structure store used as database, cache and message broker. ElastiCache for Redis offers Multi-AZ with Auto-Failover and enhanced robustness.

☒ **Cluster Mode enabled**

☐ **Memcached**

High-performance, distributed memory object caching system, intended for use in speeding up dynamic web applications.

### Location

Choose a location

☒ **Amazon Cloud**

Use Amazon's cloud for your ElastiCache instances

☐ **On-Premises**

Create your ElastiCache instances on AWS Outposts. You need to create a subnet ID on an Outpost first.

The different types of ElastiCache services are:

**ElastiCache for Redis** - it is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications.

**ElastiCache for Memcached**- a Memcached-compatible in-memory key-value store service that can be used as a cache or a data store.

**ElastiCache for Redis Global Database** - you can write to your ElastiCache for Redis cluster in one region and have the data available to be read from two other cross-region replica clusters, thereby enabling low-latency reads and disaster recovery across regions.

Hence, the correct answers are:

- **ElastiCache for Redis**

- **ElastiCache for Memcached**

All the other options are incorrect since these are not a type of service in Amazon ElastiCache:

- **Amazon ElastiCache for Apache Spark**

- **Amazon ElastiCache for Apache Kafka**



## - Amazon ElastiCache for Apache Ignite

### References:

<https://aws.amazon.com/elasticache/>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/WhatIs.html>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/WhatIs.html>

### Check out this Amazon ElastiCache Cheat Sheet:

<https://tutorialsdojo.com/amazon-elasticache/>

Question 13:

#### Skipped

A startup company plans to create a user management and authentication service for its customers. The users need to sign in through an external identity provider to access their web and mobile applications. Which AWS service should they use to meet this requirement?

- **Amazon Macie**
- **AWS IAM**
- **Amazon Cognito**

**(Correct)**

- **AWS Artifact**

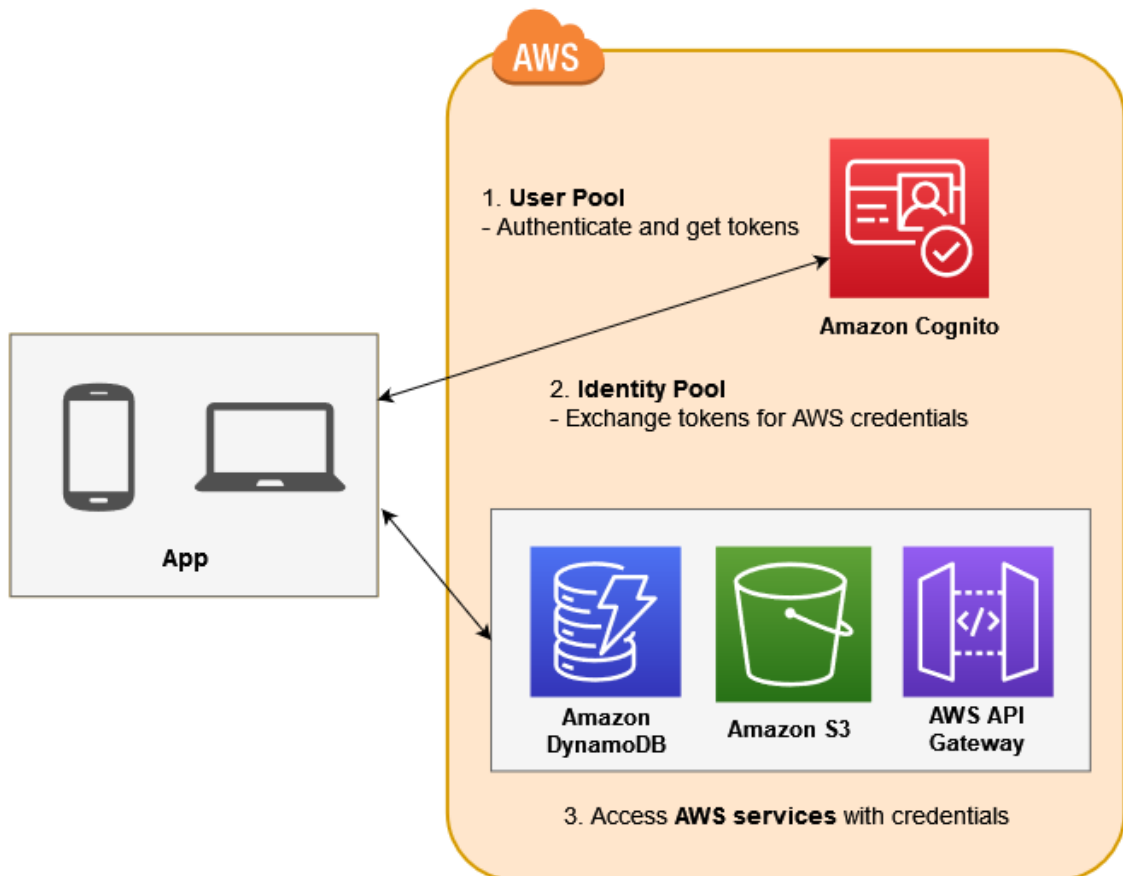
#### Explanation

**Amazon Cognito** lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. It provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, Google, or Apple.

The two main components of Amazon Cognito are user pools and identity pools.

**1. User pools** - are user directories that provide sign-up and sign-in options for your app users.

**2. Identity pools** - enable you to grant your users access to other AWS services. You can use identity pools and user pools separately or together.



Cognito is a user management and authentication service that can be integrated into your web or mobile applications. It also enables you to authenticate users through an external identity provider and provides temporary security credentials to access your app's backend resources in AWS or any service behind the Amazon API gateway.

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

**AWS IAM** is incorrect because this is just a service that enables you to manage users' access only in your AWS account. AWS IAM is not a suitable service to use for authenticating users through an external identity provider. It does not provide mobile authentication as well, unlike Amazon Cognito.

**Amazon Macie** and **AWS Artifact** are both incorrect because these services are not user management services.

#### References:

<https://aws.amazon.com/cognito/>

<https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html>

**Check out this Amazon Cognito Cheat Sheet:**

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

Question 14:

**Skipped**

An e-commerce company launches several EC2 instances to run their web application. Which of the following services can be used to help ensure security compliance? (Select TWO.)

- **AWS Systems Manager**
- **Amazon Inspector**

**(Correct)**

- **Amazon MQ**
- **AWS Trusted Advisor**

**(Correct)**

- **AWS CloudFormation**

**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.

<input type="checkbox"/>	Name	Duration	Target name	Last run	All runs
<input type="radio"/>	Assessment-Template-TutorialsDojo-Network	N/A	Assessment-Target-All-Instances-Network		

---

### Assessment Template - Assessment-Template-TutorialsDojo-Network

**Name** Assessment-Template-TutorialsDojo-Network

**ARN** arn:aws:inspector:us-east-1:189630120175:target/0-Q7QQZ3VQ/template/0-7PqD4AY

**Target name** [Assessment-Target-All-Instances-Network](#) Preview Target

**Rules packages**

- Common Vulnerabilities and Exposures-1.1
- CIS Operating System Security Configuration Benchmarks-1.0
- Network Reachability-1.1
- Security Best Practices-1.0

**Security Assessments**

Preview Exclusions

**Duration** 1 Hour (Recommended)

**SNS topics** [✎](#)

**Assessment Events** [✎](#)

Rule Type	Rule Name
Scheduled Event	Amazon_Inspector_Assessment_0-5K35zzW0_Idgcjee

Click below to set up recurring assessment runs once every  days, with the first run **starting now**. [Learn more](#)

Add schedule

**AWS Trusted Advisor** is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. AWS Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices.

Hence, the correct answers are:

- **Amazon Inspector**
- **AWS Trusted Advisor**

**Amazon MQ** is incorrect because this is a message broker service, not a security compliance service. It supports industry-standard APIs and protocols so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications.

**AWS Systems Manager** is incorrect because this is just a management solution for resources on AWS, other cloud services, or even hybrid environments. While it does provide some security and compliance features, it's primarily a management and operations tool, not a dedicated security service.

**AWS CloudFormation** is incorrect because it only helps you turn your infrastructure into code and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. CloudFormation automates and simplifies the task of repeatedly

and predictably creating groups of related resources that power your applications, and not for security compliance.

#### References:

[https://docs.aws.amazon.com/inspector/latest/userguide/inspector\\_introduction.html](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html)

<https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html>

#### Check out these Amazon Inspector and AWS Trusted Advisor Cheat Sheets:

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

<https://tutorialsdojo.com/aws-trusted-advisor/>

Question 15:

#### Skipped

Which of the following best describes Amazon Redshift?

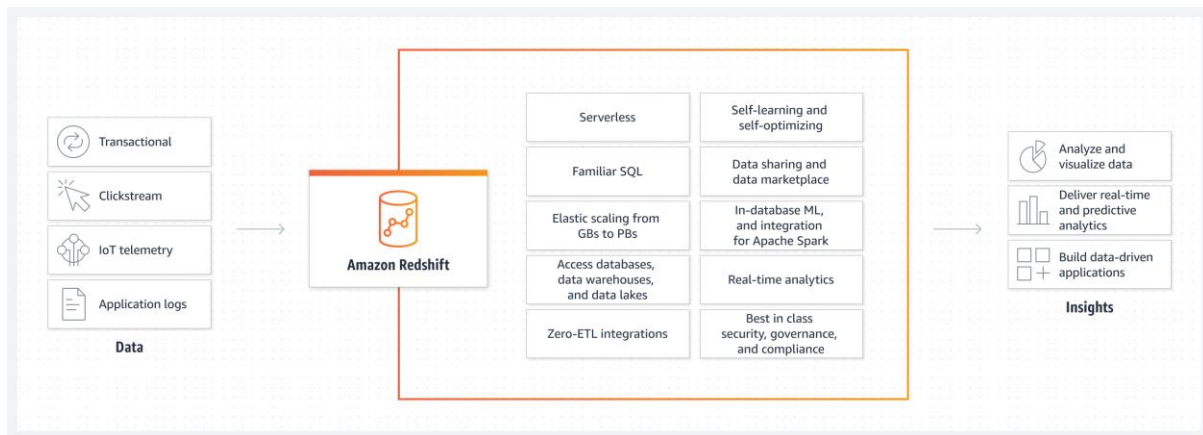
- A NoSQL database service.
- A managed data warehouse service.

(Correct)

- An Online Transaction Processing (OLTP) database.
- A messaging and queuing service.

#### Explanation

**AWS Redshift** is a managed service for data warehousing that is fast and cost-effective and allows for the analysis of data using SQL and Business Intelligence (BI) tools. This service enables users to execute complex queries against large datasets, which are stored in a secure and scalable data warehouse. Additionally, Redshift has the capability to scale compute and storage resources automatically to match user demands, facilitating the easy expansion of warehouse size when necessary.



Hence, the correct answer is: **A managed data warehouse service.**

The option that says: **A NoSQL database service** is incorrect because Amazon Redshift is actually a relational database service that uses SQL for data management and queries. It is designed for analytical workloads and allows running complex queries on structured and semi-structured data.

The option that says: **An Online Transaction Processing (OLTP) database** is incorrect because Amazon Redshift is not intended for OLTP workloads. OLTP databases are designed for handling high-volume transactional workloads that require fast response times and high throughput, whereas Amazon Redshift is categorized as an OLAP database, which means it is specifically designed to efficiently manage complex analytical queries and reporting tasks on large datasets.

The option that says: **A messaging and queuing service** is incorrect because its main purpose is to store and manage data for analysis purposes, and it is not designed to facilitate communication or exchange of messages between applications.

## References:

<https://aws.amazon.com/redshift/#>

<https://docs.aws.amazon.com/redshift/index.html>

Check out this **Amazon Redshift Cheat Sheet**:

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

**Amazon Redshift Overview:**

<https://youtu.be/jlLERNzhHOg>

Question 16:

### Skipped

A company needs to store frequently accessed data in Amazon S3. How will AWS bill you for storing objects in your S3 buckets?

- **By Instance Type**
- **Per Unique File Type**
- **Per Hour or Second**
- **Per GB**

(Correct)

### Explanation

**Amazon Simple Storage Service (S3)** is the object storage of AWS. It is used to store and retrieve any amount of data from anywhere on the Internet. It is also a service that offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at a very low cost.

Amazon S3 > tutorialsdojo

## tutorialsdojo

Objects Properties Permissions Metrics Management Access Points



### Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

 Find objects by prefix

< 1 > 

<input type="checkbox"/>	Name ▲	Type ▼	Last modified ▼	Size ▼	Storage class ▼
<input type="checkbox"/>	 <a href="#">Metro Manila.png</a>	png	March 13, 2021, 07:13:46 (UTC+08:00)	1.75 MB	Standard
<input type="checkbox"/>	 <a href="#">Noli Me Tangere.pdf</a>	pdf	March 13, 2021, 07:13:48 (UTC+08:00)	3.6 MB	Standard

**S3 Standard** is the general-purpose storage for any type of data, typically used for frequently accessed data. You only pay for storing objects in your S3 buckets. The rate you are charged depends on your objects' size, how long you stored the objects and the storage class.

Hence, the correct answer is: **Per GB**.

**Per Hour or Second** and **By Instance Type** are both incorrect because these are not valid S3 bucket pricing tiers. The usage of an EC2 instance is calculated by the hour or second based on the size of the instance, operating system, and the AWS Region where the instances are launched.

**Per Unique File Type** is incorrect because Amazon S3 does not have this sort of pricing scheme.

#### References:

<https://aws.amazon.com/s3/pricing/>

<https://aws.amazon.com/s3/faqs/>

#### Amazon S3 and S3 Glacier Overview:

<https://www.youtube.com/watch?v=1ymyeN2tki4>

#### Check out this Amazon S3 Cheat Sheet:

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

Question 17:

#### Skipped

A customer needs to store objects that are frequently accessed. To help the customer save costs, you must select a storage service free from retrieval charges. Which of the following S3 storage classes would meet this requirement? (Select TWO.)

- S3 Standard

(Correct)

- S3 Standard-IA
- S3 Intelligent Tiering

(Correct)

- S3 One Zone-IA
- S3 Glacier Deep Archive

#### Explanation

**S3 Standard** offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.



Storage Class	Designed for	Availability	Availability Zones	Min Storage Duration	Min Billable Object Size	Monitoring and Auto-Tiering Fees	Retrieval Fees
Standard	Frequently accessed data with milliseconds access	99.99%	≥ 3	-	-	-	-
Intelligent-Tiering	Data with changing or unknown access patterns	99.9%	≥ 3	-	-	Per-object fees apply for objects >= 128 KB	-
Standard-IA	Infrequently accessed data with milliseconds access	99.9%	≥ 3	30 days	128 KB	-	Per-GB fees apply
One Zone-IA	Infrequently accessed data stored in a single AZ with milliseconds access	99.5%	1	30 days	128 KB	-	Per-GB fees apply
Glacier Instant Retrieval	Long-lived archive data with instant retrieval in milliseconds	99.9%	≥ 3	90 days	128 KB	-	Per-GB fees apply
Glacier Flexible Retrieval	Long-lived archive data with retrieval of minutes to hours	99.99%	≥ 3	90 days	-	-	Per-GB fees apply
Glacier Deep Archive	Long-lived archive data with retrieval of hours	99.99%	≥ 3	180 days	-	-	Per-GB fees apply

The **S3 Intelligent-Tiering** storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier optimized for frequent access and another lower-cost tier optimized for infrequent access.

The S3 Standard-IA and S3 One Zone-IA storage classes are designed for long-lived and infrequently accessed data. (IA stands for infrequent access.) S3 Standard-IA and S3 One Zone-IA objects are available for millisecond access (same as the S3 Standard storage class). Amazon S3 charges a retrieval fee for these objects, so they are most suitable for infrequently accessed data.

Both the S3 Standard and S3 Intelligent-Tiering storage classes do not have retrieval fees.

Hence, the correct answers are:

- **S3 Standard**

- **S3 Intelligent-Tiering**

**S3 Glacier Deep Archive, S3 Standard-IA, and S3 One Zone-IA** are all incorrect since these storage tiers have object retrieval fees.

## References:

<https://aws.amazon.com/s3/pricing/>

<https://aws.amazon.com/s3/storage-classes/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html>

## Amazon S3 and S3 Glacier Overview:

<https://youtu.be/1ymyeN2tki4>

## Check out this Amazon S3 Cheat Sheet:

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

Question 18:

### Skipped

Which of the following is a benefit of using AWS Global Accelerator?

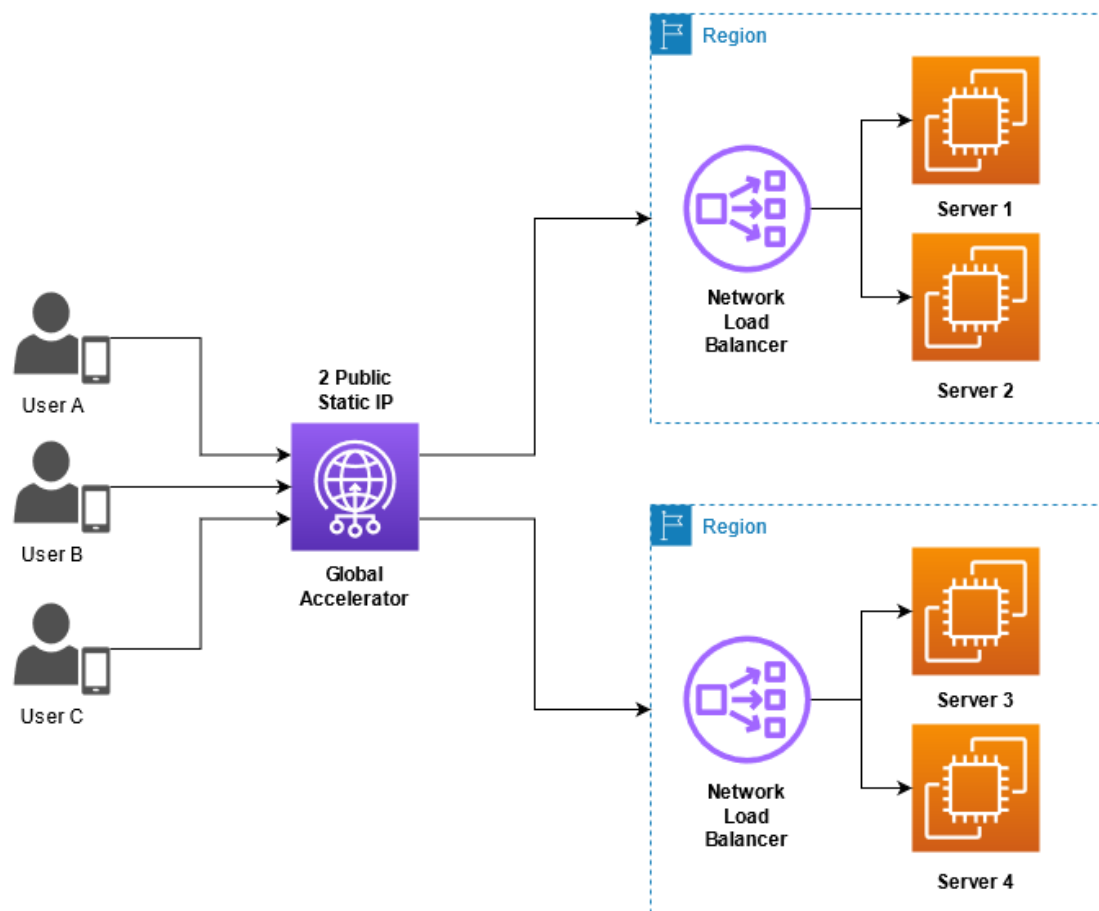
- **Reduced server costs in running AWS Services**
- **Decreased latency in accessing applications hosted in AWS**

**(Correct)**

- **Provides a highly durable data store in AWS**
- **Accelerates server performance of your Amazon EC2 instances globally**

### Explanation

**AWS Global Accelerator** is a service that improves the availability and performance of your applications with local or global users. It provides you with static IP addresses that serve as a fixed entry point to your applications hosted in one or more AWS Regions. These IP addresses are anycast from AWS edge locations, so they're announced from multiple AWS edge locations at the same time. This enables traffic to ingress onto the AWS global network as close to your users as possible.



Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your traffic by as much as 60%.

Hence, the correct answer is: **Decreased latency in accessing applications hosted in AWS.**

The following options are incorrect because these are not the benefits of using AWS Global Accelerator:

- Accelerates server performance of your Amazon EC2 instances globally
- Reduced server costs in running AWS Services
- Provides a highly durable data store in AWS

#### References:

<https://aws.amazon.com/global-accelerator/>

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

Check out this AWS Global Accelerator Cheat Sheet:

<https://tutorialsdojo.com/aws-global-accelerator/>

Question 19:

### Skipped

Which of the following provides the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud?

- **AWS Shared Responsibility Model**
- **AWS Reference Architecture Diagrams**
- **AWS Well-Architected Framework**

(Correct)

- **AWS Trusted Advisor**

### Explanation

**AWS Well-Architected Framework** has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications.

## AWS Well- Architected Framework: Six Pillars



This is based on six pillars namely:

1. **Operational Excellence** - The ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.
2. **Security** - The ability to protect the information, systems, and assets while delivering business value through risk assessments and mitigation strategies.
3. **Reliability** - The ability to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

4. **Performance Efficiency** - The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.

5. **Cost Optimization** - The ability to avoid or eliminate unneeded costs or suboptimal resources.

6. **Sustainability** - The ability to increase efficiency across all components of a workload by maximizing the benefits from the provisioned resources.

The AWS Well-Architected Framework describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. By answering a set of foundational questions, you learn how well your architecture aligns with cloud best practices and are provided guidance for making improvements. It provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

Hence, the correct answer is: **AWS Well-Architected Framework**.

**AWS Reference Architecture Diagrams** is incorrect because this is simply a collection of technical resources to help you build industry-tested architectures more effectively and efficiently in the AWS Cloud. It does not provide a set of foundational questions that you can use to evaluate if your architecture is aligned with AWS best practices.

**AWS Trusted Advisor** is incorrect. Although it's a helpful service that offers real-time guidance to optimize AWS resources and enhance security by following AWS best practices, it doesn't cover the fundamental concepts, architectural best practices, and design principles required to design and operate workloads in the cloud.

**AWS Shared Responsibility Model** is incorrect because this just describes the specific responsibilities of AWS and the customer in managing, maintaining, and securing AWS services, including its underlying resources.

## References:

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

<https://aws.amazon.com/blogs/apn/the-6-pillars-of-the-aws-well-architected-framework/>

**Check out these AWS Well-Architected Framework Cheat Sheets:**

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

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

Question 20:

### Skipped

Which feature will customers have access to by using the AWS Business Support plan?

- Access to online self-paced labs
- Technical Account Manager
- Architecture Support

(Correct)

- Concierge Support Team

### Explanation

**AWS Business Support Plan** is used if you have production workloads on AWS and want 24x7 access to technical support and architectural guidance in the context of your specific use cases.

	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, Business 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.

**Enhanced Technical Support** – 24x7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases. Response times are as follows:

General Guidance - < 24 hours

System Impaired - < 12 hours

Production System Impaired - < 4 hours

Production System Down - < 1 hour

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

**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.

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

**Access to Proactive Support Programs** – Ability to purchase Infrastructure Event Management for an additional fee. This provides Architecture and scaling guidance and real-time operational support during the preparation and execution of planned events, product launches, and migrations.

Hence, the correct answer is **Architecture Support**.

The other options are all incorrect because these are provided in the Enterprise Support Plan and are not available in the Business Support Plan.

- **Access to online self-paced labs**

- **Concierge Support Team**

- **Technical Account Manager**

#### References:

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

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

**Check out this AWS Support Plans Cheat Sheet:**

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

Question 21:

**Skipped**

A company plans to restrict access to content served from an Amazon S3 bucket using Amazon CloudFront. Which of the following features can you use to satisfy this requirement?

- **Origin Access Identity**

**(Correct)**

- **Server Name Indication**
- **Sticky Sessions**
- **Service Control Policies**

### 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.

## Create origin

### Settings

#### Origin domain

Choose an AWS origin, or enter your origin's domain name.

🔍 bucket-tutorialsdojo-demo.s3.ap-southeast-1.amazonaws.com ✕

#### Origin path - optional [Info](#)

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

#### Name

Enter a name for this origin.

s3-bucket-tutorialsdojo-demo

#### S3 bucket access [Info](#)

Use a CloudFront origin access identity (OAI) to access the S3 bucket.

- ☐ Don't use OAI (bucket must allow public access)
- ☒ Yes use OAI (bucket can restrict access to only CloudFront)

#### Origin access identity

Select an existing origin access identity (recommended) or create a new identity.

access-identity-bucket-tutorialsdojo-demo.s3.ap-southeast-1.amazonaws.com ▼

Create new OAI

#### Bucket policy

Update the S3 bucket policy to allow read access to the OAI.

- ☒ No, I will update the bucket policy
- ☐ Yes, update the bucket policy



An **Origin Access Identity** is used for sharing private content through CloudFront. The OAI is a virtual user identity that will be used to give your CloudFront distribution permission to fetch a private object from your origin server.

You can restrict access to content that you serve from Amazon S3 buckets by configuring this to your services:

Create a special CloudFront user called an origin access identity (OAI) and associate it with your distribution.

Configure your S3 bucket permissions so that CloudFront can use the OAI to access the files in your bucket and serve them to your users. Make sure that users can't use a direct URL to the S3 bucket to access a file there.

After the S3 and CloudFront configuration, your users can only access your files through CloudFront and not directly from the S3 bucket.

Hence, the correct answer is: **Origin Access Identity**.

**Service Control Policies** is incorrect because this is an AWS Organization policy and not an Amazon CloudFront feature. It is used to manage permissions in your organization and helps you ensure your accounts stay within your organization's access control guidelines.

**Server Name Indication** and **Sticky Sessions** are both incorrect because these are features of an Application Load Balancer. **Server Name Indication** is mainly used to host multiple secure applications, each with its own TLS certificate, on a single load balancer listener. While **sticky sessions** are a mechanism to route requests from the same client to the same target. If you need to restrict access directly in an Amazon S3 bucket, use Amazon CloudFront OAI instead.

## References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

<https://aws.amazon.com/cloudfront/faqs/>

Check out this **Amazon CloudFront Cheat Sheet**:

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

Question 22:

**Skipped**

Which AWS service allows you to easily manage access to multiple AWS accounts and provide users with single login access?

- **Amazon SES**
- **AWS IAM Identity Center**

**(Correct)**

- **Amazon SWF**
- **Amazon SQS**

### Explanation

**AWS IAM Identity Center (successor to AWS Single Sign-On)** enables you to securely establish or link your workforce identities and centrally administer their access to AWS accounts and applications. Regardless of the size or type of organization, the IAM Identity Center is the preferred solution for managing workforce authentication and authorization on AWS.



With the IAM Identity Center application configuration wizard, it is simpler to set up single sign-on access for applications that are compatible with SAML 2.0. Moreover, IAM Identity Center includes preconfigured settings for numerous cloud applications such as Salesforce, Box, and Microsoft 365.

Hence, the correct answer is: **AWS IAM Identity Center**.

**Amazon SES** is incorrect because this is just a cloud-based email service designed to help digital marketers and application developers send marketing, notification, and transactional emails. This option does not provide you a feature to log in to multiple AWS accounts.

**Amazon SWF** and **Amazon SQS** are both incorrect because these services just facilitate the integration of applications or microservices. These services are not suitable for managing or accessing multiple AWS accounts.

### References:

<https://aws.amazon.com/iam/identity-center/>

<https://docs.aws.amazon.com/controltower/latest/userguide/sso.html>

### **AWS Identity Services Overview:**

<https://youtu.be/AldUw0i8rr0>

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

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

Question 23:

#### **Skipped**

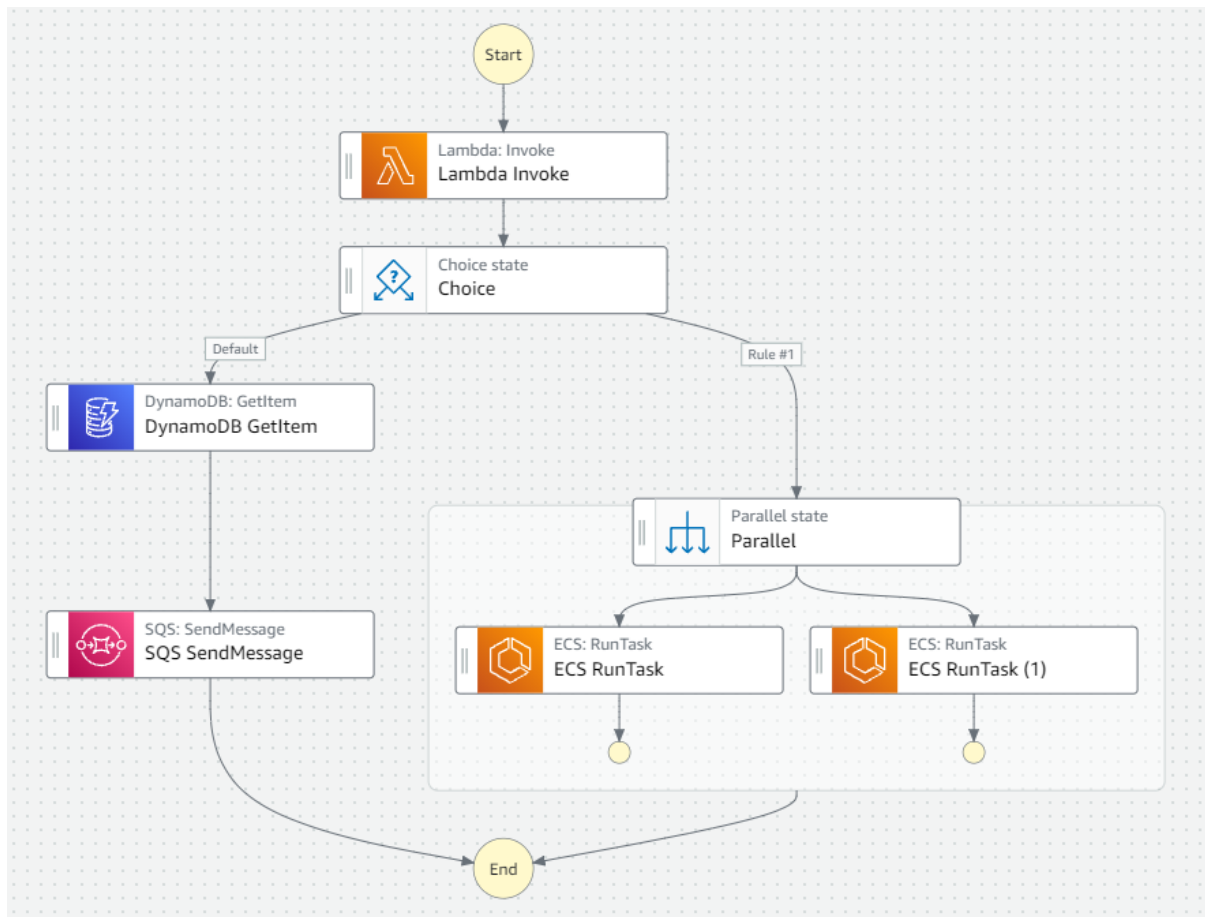
Which of the following AWS services helps you coordinate the components of distributed applications and microservices using visual workflows?

- **Amazon API Gateway**
- **Amazon Rekognition**
- **AWS Batch**
- **AWS Step Functions**

**(Correct)**

#### **Explanation**

**AWS Step Functions** is a web service that enables you to coordinate the components of distributed applications and microservices using visual workflows. You build applications from individual components that perform a discrete function, or task, allowing you to scale and change applications quickly. Step Functions provide auditable automation of routine deployments, upgrades, installations, and migrations.



Step Functions can easily automate recurring tasks such as patch management, infrastructure selection, and data synchronization, and Step Functions will automatically scale, respond to timeouts, and retry failed tasks.

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

**Amazon API Gateway** is incorrect because this is just a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. This service doesn't provide a way for you to easily coordinate workflows.

**AWS Batch** is incorrect because this service simply enables you to run batch computing workloads of any scale. AWS Batch automatically provisions compute resources and optimizes the workload distribution based on the quantity and scale of the workloads. This option is not related to event-driven workflows and orchestration.

**Amazon Rekognition** is incorrect because this is primarily used for image and video analysis. You can't use this service for patch management and infrastructure selection.

### References:

<https://aws.amazon.com/step-functions/>

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>

**Check out this AWS Step Functions Cheat Sheet:**

<https://tutorialsdodo.com/aws-step-functions/>

Question 24:

## Skipped

Which of the following services displays the general status of all available AWS Services and informs you if a service is experiencing availability issues?

- **AWS Trusted Advisor**
- **AWS Health Dashboard**

**(Correct)**

- AWS Config Dashboard
- Amazon CloudWatch

### Explanation

**AWS Health Dashboard** displays the general status of AWS services. It also provides the flexibility of displaying the history of a specific service within a geographical area. It is useful for determining whether a failure has had effects that you might have never encountered inside your own network. AWS keeps this history of service interruptions for a year.

## AWS Health Dashboard

Updated less than 1 minute ago

### Service health

View the current and historical status of all AWS services.

#### View your account health

Get a personalized view of events that affect your AWS account or organization.

[Open your account health](#)

---

Open and recent issues (0)
**Service history**

## No recent issues

Updated less than 1 minute ago

### Service history

The following table is a running log of AWS service status for the past 12 months. Choose a status icon to see status updates for that service. All dates and times are reported in Pacific Time (PST/PDT).

	North America	South America	Europe	Africa	Asia Pacific	Middle East
Service	RSS <<	Today	30 Jul	29 Jul	28 Jul	>>
Alexa for Business (N. Virginia)	🔊	✅	✅	✅	✅	✅
Amazon API Gateway (Montreal)	🔊	✅	✅	✅	✅	✅
Amazon API Gateway (N. California)	🔊	✅	✅	✅	✅	✅

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 Dashboard**.

**AWS Config Dashboard** is incorrect because it only gives you a compliance status of your resources. You have to use the AWS Health Dashboard to check the current status and status history of all AWS services in various regions.

**Amazon CloudWatch** is incorrect because this service is primarily used to monitor the performance and event history of your AWS services.

**AWS Trusted Advisor** is incorrect because this service suggests ways to optimize AWS resources and reduce expenses. It does not provide a comprehensive overview of the general status of all available AWS services.

#### References:

<https://status.aws.amazon.com/>

<https://docs.aws.amazon.com/health/latest/ug/what-is-aws-health.html>

#### Check out this AWS Health Cheat Sheet:

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

Question 25:

#### Skipped

Which of the following services can establish a connection from your on-premises environment and resources hosted on AWS? (Select TWO.)

- **AWS Direct Connect**

**(Correct)**

- **Amazon Connect**
- **AWS Snowcone**
- **AWS Site-to-Site VPN**

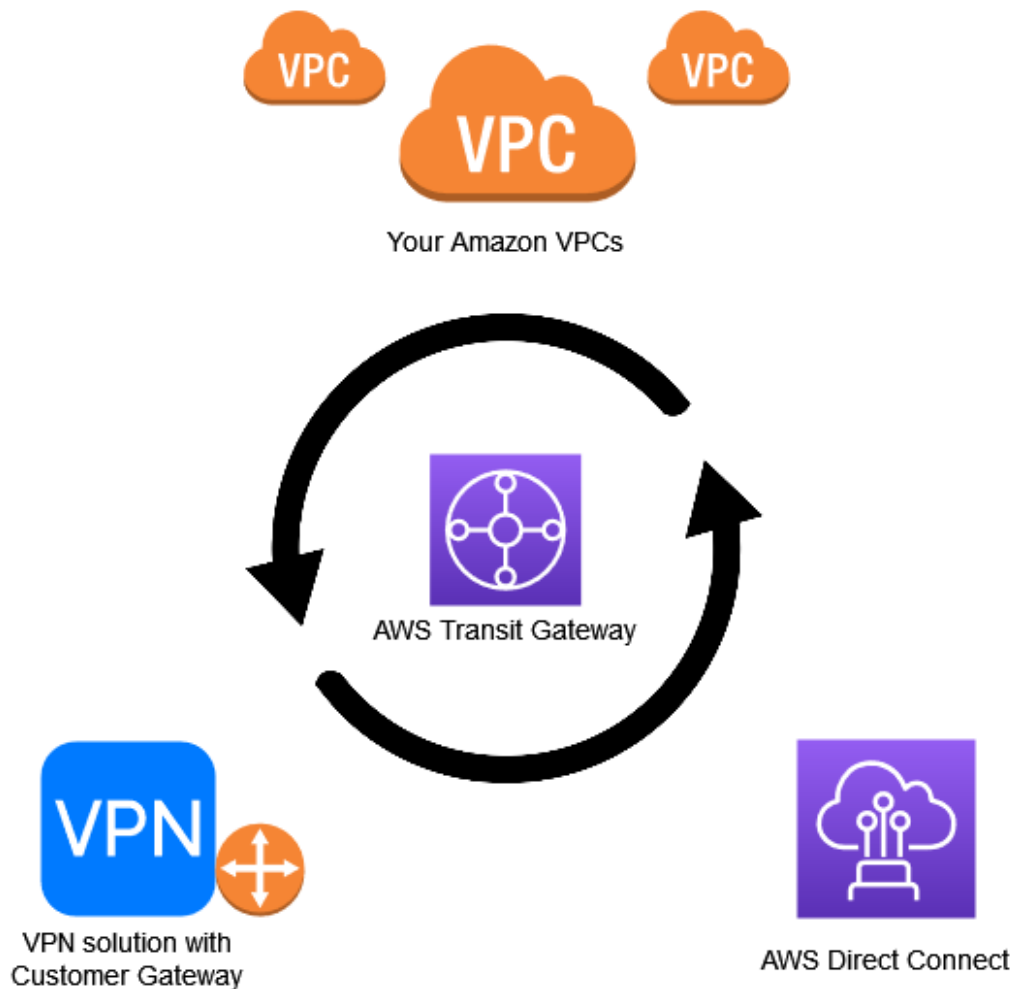
**(Correct)**

- **AWS Directory Service**

#### Explanation

**AWS Direct Connect** is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct

Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.



**AWS Site-to-Site VPN** creates a secure connection between your data center or branch office and your AWS cloud resources. For globally distributed applications, the Accelerated Site-to-Site VPN option provides even greater performance by working with AWS Global Accelerator.

Hence, the correct answers are:

- **AWS Direct Connect**

- **AWS Site-to-Site VPN**

**Amazon Connect** is incorrect because this is not a VPN connectivity option. It is a self-service, cloud-based contact center service in AWS that makes it easy for any business to deliver better customer service at a lower cost.

**AWS Directory Service** is incorrect because this is not a service for a dedicated network connection from your premises to AWS. Directory Service is a managed service offering directory that contains information about your organization, including users, groups, computers, and other resources.

**AWS Snowcone** is incorrect because this is just a portable data transfer device with secure edge computing capability. You can use this to transfer data from your on-premises data to AWS. However, it can't be used in establishing a dedicated networking connection between your on-premises data center and AWS.

#### References:

<https://docs.aws.amazon.com/directconnect/index.html>

<https://docs.aws.amazon.com/vpn/index.html>

#### Check out this AWS Direct Connect Cheat Sheet:

<https://tutorialsdojo.com/aws-direct-connect/>

Question 26:

#### Skipped

A Systems Administrator needs to create an account that will be used for long-term programmatic access to AWS. Which of the following IAM entities should be used to comply with this requirement?

- IAM Policy
- IAM User

(Correct)

- IAM Role
- 

IAM Group

#### Explanation

**AWS Identity and Access Management** enable you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.



## Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

Create access key

Access key ID	Created	Last used	Status	
AKCFWUKOEVNIAU87JDV3	2021-03-12 14:35 UTC+0800	N/A	Active	<a href="#">Make inactive</a> <span>✕</span>

IAM Users make use of access keys for long-term programmatic credentials. Access keys consist of two parts: an access key ID and a secret access key. You can use access keys to sign programmatic requests to the AWS CLI or AWS API.

Hence, the correct answer is: **IAM User**.

**IAM Role** is incorrect because it 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.

**IAM Group** is incorrect because this is basically used to group together multiple IAM users. IAM Groups let you specify permissions for multiple users, making it easier to manage the permissions for those users. An IAM Group doesn't provide a long-term programmatic credential, unlike an IAM User.

**IAM Policy** is incorrect because this is just used to define permissions to IAM Users and Roles. IAM Policy does not have long-term credentials.

## References:

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

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_access-keys.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html)

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

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

Question 27:

## Skipped

Which of the following services allows you to quickly query data in S3 using SQL without having to set up and manage any servers?

- **Amazon Athena**

**(Correct)**

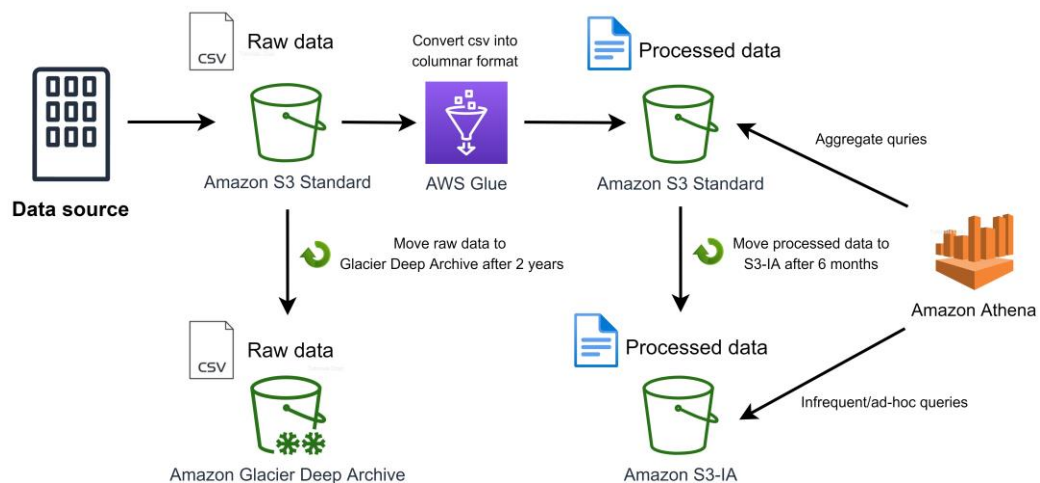
- 

## Amazon SQS

- AWS Lambda
- AWS Step Functions

### Explanation

**Amazon Athena** is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to set up or manage, and you can start analyzing data immediately. You don't even need to upload your data into Athena, as it works directly with data stored in S3.



Athena uses a managed Data Catalog to store information and schemas about the databases and tables that you create for your data stored in S3. You only pay for the queries that you run and you are charged based on the amount of data scanned by each query.

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

**Amazon SQS** is incorrect because this is a message queue service used by distributed applications to exchange messages through a polling model, and can be used to decouple sending and receiving components. You use Amazon SQS to decouple your applications, and not for querying data in S3.

**AWS Lambda** and **AWS Step Functions** are both incorrect. These serverless services don't have a built-in capability to analyze data in Amazon S3 using standard SQL.

### References:

<https://aws.amazon.com/athena/>

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

Check out this Amazon Athena Cheat Sheet:

<https://tutorialsdojo.com/amazon-athena/>

Question 28:

**Skipped**

Which is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy?

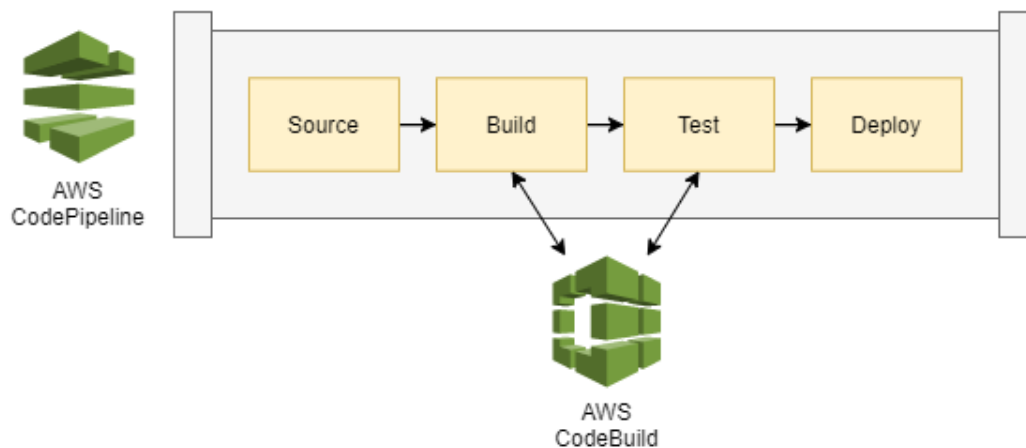
- **AWS CodeBuild**

**(Correct)**

- **AWS CodeDeploy**
- **AWS CodePipeline**
- **AWS CodeCommit**

**Explanation**

**AWS CodeBuild** is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue.



CodeBuild provides these benefits:

**Fully managed** – CodeBuild eliminates the need to set up, patch, update, and manage your own build servers.

**On-demand** – CodeBuild scales on-demand to meet your build needs. You pay only for the number of build minutes you consume.

**Out of the box** – CodeBuild provides preconfigured build environments for the most popular programming languages. All you need to do is point to your build script to start your first build.

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

**AWS CodeDeploy**, **AWS CodePipeline**, and **AWS CodeCommit** are all incorrect because these services are not suitable to build and test applications in AWS Cloud. **CodeDeploy** is primarily used to automate code deployments to any instance, including EC2 instances and instances running on-premises. **CodePipeline** is a continuous delivery service while **CodeCommit** is a fully-managed source control service.

#### References:

<https://aws.amazon.com/codebuild/>

<https://docs.aws.amazon.com/codebuild/latest/userguide/welcome.html>

Check out this **AWS CodeBuild Cheat Sheet**:

<https://tutorialsdojo.com/aws-codebuild/>

#### AWS CodeBuild Overview:

<https://youtu.be/1zA6mK9BdA4>

Question 29:

#### Skipped

Which AWS services should you use to upload SSL certificates? (Select TWO.)

- **AWS License Manager**
- **AWS Systems Manager**
- **AWS IAM**

**(Correct)**

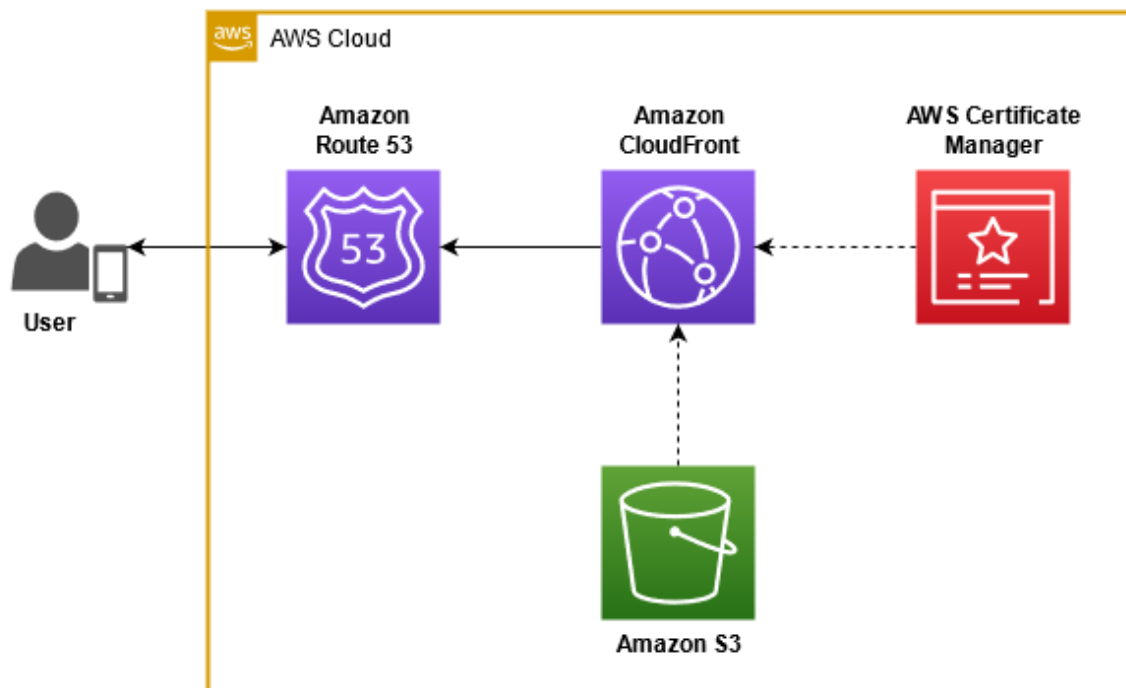
- **AWS Certificate Manager**

**(Correct)**

- **AWS KMS**

**Explanation**

**AWS Certificate Manager (ACM)** handles the complexity of creating, storing, and renewing public SSL/TLS X.509 certificates and keys that protect your AWS websites and applications. You can provide certificates for supported AWS services either by issuing them directly with ACM or by importing third-party certificates into the ACM management system. ACM certificates can secure multiple domain names and multiple names within a domain.



**ACM** is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

You can use **IAM** as a certificate manager only when you must support HTTPS connections in a region not supported by ACM. IAM securely encrypts your private keys and stores the encrypted version in IAM SSL certificate storage. IAM supports deploying server certificates in all Regions, but you must obtain your certificate from an external provider for use with AWS.

Hence, the correct answers are:

- **AWS Certificate Manager**
- **AWS Identity and Access Management**

All other options are incorrect because these services are not capable of storing SSL certificates.

**AWS Systems Manager** is incorrect because this service is a management solution for hybrid cloud environments. It allows you to perform routine operations, track development, test, and production environments, and proactively act on events or other operational incidents. If you need to store SSL certificates, use ACM or AWS IAM.

**AWS License Manager** is incorrect because this service is mainly used for managing software licenses from different vendors (Microsoft, Oracle, SAP, IBM) across AWS and on-premises environments. It is not capable of managing and storing SSL certificates.

**AWS Key Management Service** is incorrect because this is a managed service that allows you to create and control keys used for cryptographic operations. This means that this service is not capable of storing SSL certificates. Therefore, if you need full control over the management of your keys and also to share access to the keys across your resources, then use AWS KMS.

#### References:

<https://aws.amazon.com/certificate-manager/>

<https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

#### AWS Security Services Overview - Secrets Manager, ACM, Macie:

<https://youtu.be/ogVamzF2Dzk>

#### Check out this AWS Certificate Manager Cheat Sheet:

<https://tutorialsdojo.com/aws-certificate-manager/>

Question 30:

#### Skipped

Which service lets you create rules to filter web traffic based on conditions that include IP addresses, HTTP headers, or custom URIs?

- Network ACLs
- AWS WAF

(Correct)

- AWS Trusted Advisor
- Security Group

Explanation

**AWS Web Application Firewall** gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define.

Rule

Validate

Name

tutorialsdojo-rule

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and \_ (underscore).

Type

Rate-based rule

Select Rate-based rule

Request rate details

Rate limit

The rate limit is the maximum number of requests from a single IP address that are allowed in a five-minute period. This value is continually evaluated, and requests will be blocked once this limit is reached. The IP address is automatically unblocked after it falls below the limit.

100

Rate limit must be between 100 and 20,000,000.

IP address to use for rate limiting

When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

☒ Source IP address

☐ IP address in header

Criteria to count request towards rate limit

Choose whether to count all requests for each IP address or to only count requests that match the criteria of a rule statement.

☒ Consider all requests

☐ Only consider requests that match the criteria in a rule statement

AWS WAF conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection, and cross-site scripting. In addition, you can create rules that can block or rate-limit traffic from specific user-agents, from specific IP addresses, or that contain particular request headers.

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

**AWS Trusted Advisor** is incorrect because this is just an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. The AWS Trusted Advisor is not capable of filtering web traffic.

**Network Access Control List** and **Security Group** are both incorrect because these are just security layers inside your VPC. If you need to filter web traffic, AWS WAF is a suitable service to use.

## References:

<https://aws.amazon.com/waf/>

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html>

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

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

## Check out this AWS WAF Cheat Sheet:

<https://tutorialsdojo.com/aws-waf/>

Question 31:

### Skipped

Which of the following pricing options will automatically reduce your cost on any EC2 instance usage regardless of region, instance family, size, OS, or tenancy?

- **On-Demand Instances**
- **Dedicated Hosts**
- **Reserved Instances**
- **Savings Plans**

**(Correct)**

### Explanation

**AWS Savings Plan** is a flexible pricing model that saves up to 72 percent on Amazon EC2, AWS Fargate, and AWS Lambda usage. Savings Plans provides you lower prices for your Amazon EC2 usage, Fargate, and Lambda in exchange for a commitment to a consistent usage amount (measured in \$/hour) for a one or three-year term.



	Compute Savings Plans	EC2 Instance Savings Plans	Convertible RIs	Standard RIs
Savings over On-Demand	Up to 66 percent	Up to 72 percent	Up to 66 percent	Up to 72 percent
Automatically applies pricing to any instance family	✓	—	—	—
Automatically applies pricing to any instance size	✓	✓	Regional only	Regional only
Automatically applies pricing to any tenancy or OS	✓	✓	—	—
Automatically applies to Amazon ECS using Fargate and Lambda	✓	—	—	—
Automatically applies pricing across AWS Regions	✓	—	—	—
Term length options of 1 or 3 years	✓	✓	✓	✓

Savings Plans Types:

- **Compute Savings Plans** provide the most flexibility and prices of up to 66 percent off on-Demand rates. These plans automatically apply to your EC2 instance usage, regardless of instance family, instance sizes, region, operating system, or tenancy.
- **EC2 Instance Savings Plans** provide savings up to 72 percent off On-Demand, in exchange for a commitment to a specific instance family in a chosen AWS Region.

Hence, the correct answer is: **Savings Plans**.

**On-Demand Instances** is incorrect because this pricing model lets you pay for computing capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. Since you need to reduce your cost, on-demand is not the best option.

**Reserved Instances** is incorrect. Although it offers discounts on hourly costs, you still need to commit at least a whole year's worth of instance cost to fully maximize

the discounts. If you need to reduce your cost for AWS Fargate, this option is not suitable.

**Dedicated Hosts** is incorrect since 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 the most expensive pricing model. Therefore, it is incorrect.

### References:

<https://aws.amazon.com/savingsplans/>

<https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.html>

### Amazon EC2 Overview:

[https://www.youtube.com/watch?v=7VsGIHT\\_jQE](https://www.youtube.com/watch?v=7VsGIHT_jQE)

### Check out this AWS Savings Plan Cheat Sheet:

<https://tutorialsdojo.com/aws-savings-plan/>

Question 32:

#### Skipped

Which of the following AWS services allows you to query data directly in Amazon S3? (Select TWO.)

- Amazon Neptune
- Amazon Redshift Spectrum

(Correct)

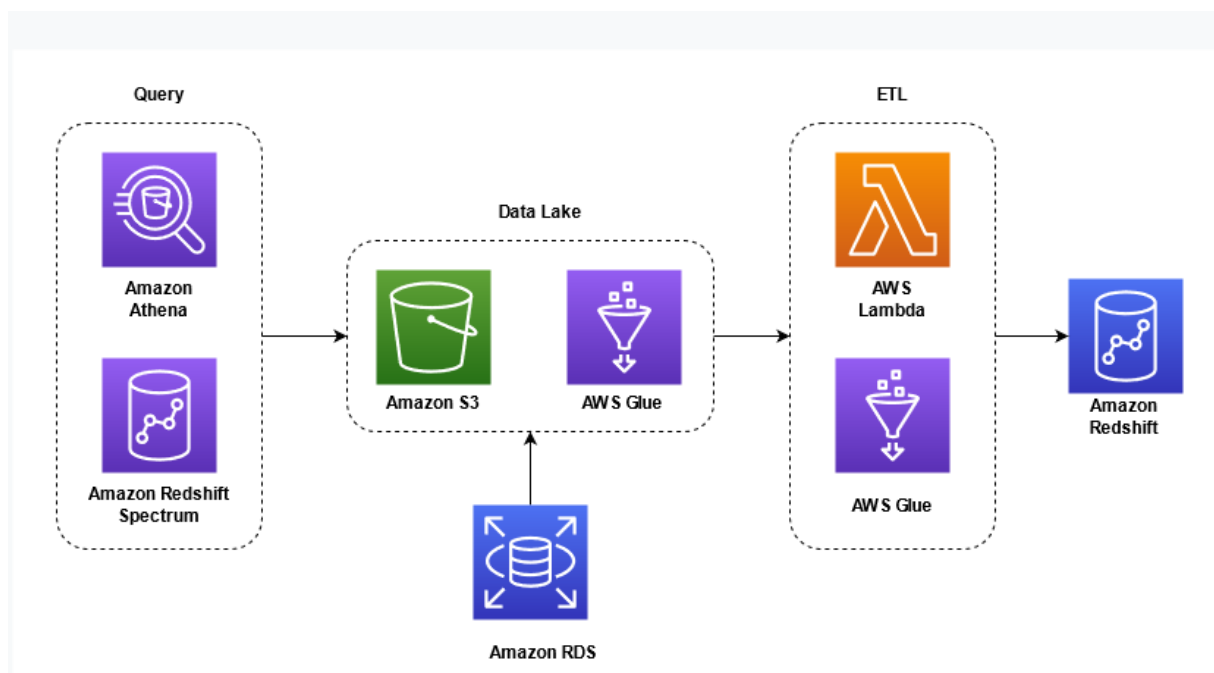
- Amazon Athena

(Correct)

- Amazon MQ
- Amazon ElastiCache

#### Explanation

**Amazon Athena** is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to set up or manage, and you can start analyzing data immediately. You don't even need to load your data into Athena, it works directly with data stored in S3.



**Amazon Redshift Spectrum** allows you to query and retrieve structured and semistructured data from files in Amazon S3 without having to load the data into Amazon Redshift tables. Much of the processing occurs in the Redshift Spectrum layer, and most of the data remain in Amazon S3. Multiple clusters can concurrently query the same dataset in Amazon S3 without the need to make copies of the data for each cluster.

Hence, the correct answers are:

- **Amazon Athena**
- **Amazon Redshift Spectrum**

**Amazon MQ** is incorrect because this is a message broker service for Apache ActiveMQ. This service is mainly used to migrate your existing RabbitMQ message brokers to AWS without having to rewrite code.

**Amazon Neptune** is incorrect because this is a fully managed graph database service. You cannot use this service to query the data stored in Amazon S3.

**Amazon ElastiCache** is incorrect because this is an in-memory data store and caching service. ElastiCache lets you create multiple replicas of a Redis primary. This allows you to scale database reads and to have highly available clusters.

## References:

<https://aws.amazon.com/athena/faqs/>

<https://docs.aws.amazon.com/redshift/latest/dg/c-getting-started-using-spectrum.html>

### Amazon Redshift Overview:

<https://youtu.be/jlLERNzhHOg>

### Check out these Amazon Athena and Amazon Redshift Cheat Sheets:

<https://tutorialsdojo.com/amazon-athena/>

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

Question 33:

#### Skipped

Which of the following AWS services does Amazon EBS use natively for encryption?

- AWS KMS

(Correct)

- AWS Shield
- Amazon S3 SSE
- AWS WAF

#### Explanation

**AWS KMS** is a managed service that enables you to create and control the keys used for cryptographic operations easily. The service provides a highly available key generation, storage, management, and auditing solution for you to encrypt or digitally sign data within your own applications or control the encryption of data across AWS services.

[Snapshots](#) > Create Volume

#### Create Volume

Snapshot ID snap-01032896d53a70cb2

Volume Type General Purpose SSD (gp2) ⓘ

Size (GiB) 100 (Min: 1 GiB, Max: 16384 GiB) ⓘ

IOPS 300 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS) ⓘ

Throughput (MB/s) Not applicable ⓘ

Availability Zone\* us-east-2a ⓘ

Fast Snapshot Restore Not enabled ⓘ

Encryption ☒ Encrypt this volume

Select a symmetric CMK

Master Key tutorialsdojo ⓘ

Amazon EBS encryption uses AWS Key Management Service (AWS KMS) customer master keys (CMK) when creating encrypted volumes and snapshots.

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

**AWS S3 SSE** is incorrect because this is a server encryption type used by Amazon S3, not EBS.

**AWS WAF** is incorrect because this is only a web application firewall that helps protect your web applications or APIs against common web exploits. WAF is mainly used to create a traffic filter, and not for EBS encryption.

**AWS Shield** is incorrect because this is not an encryption service. AWS Shield is a managed DDOS protection service that safeguards applications running on AWS.

#### References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

<https://aws.amazon.com/kms/faqs/>

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

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

#### Check out this AWS KMS Cheat Sheet:

<https://tutorialsdojo.com/aws-key-management-service-aws-kms/>

Question 34:

#### Skipped

What is the cloud computing model for services like Amazon RDS and Amazon ECS?

- IaaS
- SaaS
- PaaS

(Correct)

- FaaS

#### Explanation

There are three main models for cloud computing. Each model represents a different part of the cloud computing stack, they are:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

IaaS	PaaS	SaaS
Applications	Applications	Applications
Data	Data	Data
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Storage	Storage	Storage
Networking	Networking	Networking

You Manage
  Vendor Manages

**Platform as a Service**, sometimes abbreviated as PaaS, removes the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications.

Amazon RDS and ECS are considered PaaS because you don't need to worry about setting up servers, storage, and network. You only manage the application and the data.

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

**IAAS**, or infrastructure as a service, is incorrect. IAAS contains the basic building blocks for cloud IT and typically provides networking features, computers (virtual or on dedicated hardware), and data storage space. IAAS lets you manage your own infrastructure, but in RDS and ECS, you don't have total control over what could be done within the instances. Therefore, it's incorrect.

**SaaS**, or software as a service, is incorrect. Software as a Service provides you with a completed product that is run and managed by the service provider. With a SaaS offering, you only need to think about how you will use that particular piece of software. RDS and ECS are not a complete products since you are still managing the application and the data.

**FaaS**, or function as a service, is incorrect. Amazon RDS and ECS are not serverless computing services that execute modular pieces of code.

#### References:

<https://aws.amazon.com/types-of-cloud-computing/>

<https://aws.amazon.com/rds/>

<https://aws.amazon.com/ecs/>

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

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

Question 35:

#### Skipped

The root AWS account of your company was compromised and fortunately, there was no major data leak. What should you do to prevent this from happening again? (Select TWO.)

- **Grant full access for your IAM users**
- **Disable the rotation of credentials**
- **Configure a strong password policy for your users**

**(Correct)**

- **Enable MFA**

**(Correct)**

- **Share your root user access keys**

#### Explanation

**AWS Identity and Access Management (IAM)** enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

## Summary

[Delete user](#)**User ARN** arn:aws:iam::081918611225:user/tutorialsdojo-demo **Path** /**Creation time** 2021-01-05 15:04 UTC+0800[Permissions](#)[Groups \(1\)](#)[Tags](#)[Security credentials](#)[Access Advisor](#)

### Sign-in credentials

#### Summary

- Console sign-in link: <https://td-manila.signin.aws.amazon.com/console>
- MFA is required when signing in. [Learn more](#)

#### Console password

Enabled (last signed in 213 days) | [Manage](#)

#### Assigned MFA device

arn:aws:iam::081918611225:mfa/tutorialsdojo-demo (Virtual) | [Manage](#)

#### Signing certificates

None

The AWS IAM security best practices are:

**Enable MFA** - users have a device that generates a response to an authentication challenge.

**Configure a Strong Password Policy for your Users** -allow users to change their own passwords, require that they create strong passwords and that they rotate their passwords periodically.

**Lock Away Your AWS Account Root User Access Keys** - the access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information.

**Grant Least Privilege** - start with a minimum set of permissions and grant additional permissions as necessary.

**Rotate Credentials Regularly** - if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources.

Hence, the correct answers are:

- **Enable MFA**

- **Configure a strong password policy for your users**

The following options are not part of the best practices in securing your account using AWS IAM:

- **Disable the rotation of credentials**



- Grant full access for your IAM users
- Share your root user access keys

#### References:

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

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

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

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

Question 36:

#### Skipped

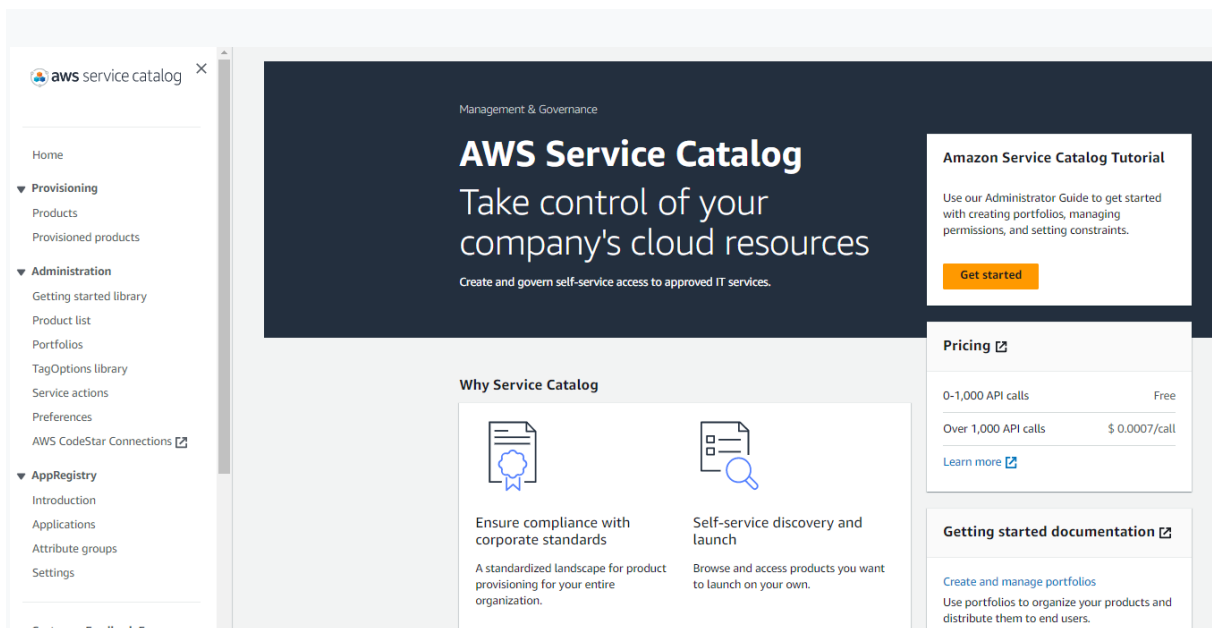
Which of the following services enables you to limit access to a portfolio of predefined AWS resources?

- AWS Config
- Amazon Grafana
- Amazon Pinpoint
- AWS Service Catalog

(Correct)

#### Explanation

**AWS Service Catalog** was developed for organizations, IT teams, and managed service providers (MSPs) that need to centralize policies. It allows IT administrators to vend and manage AWS resource and services. For large organizations, it provides a standard method of provisioning cloud resources for thousands of users. It is also suitable for small teams, where front-line development managers can provide and maintain a standard dev/test environment.



In AWS Service Catalog, a portfolio is a collection of IT services that have been pre-approved by an organization and made available to its users. A portfolio can contain one or more products, each of which is a set of AWS resources that have been preconfigured and tested to work together to provide a specific service or functionality.

You can create multiple portfolios with various products and access permissions tailored to different types of end users. A portfolio for a development team, for example, will most likely contain different products than a portfolio for a sales and marketing team. A single product can be published to multiple portfolios, each with its own set of access and provisioning policies.

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

The option that says: **AWS Config** is incorrect because this is primarily used to continuously monitors AWS resources, record changes, and provides configuration history, change notifications, and compliance reporting. You can't use AWS Config to create and manage catalogs of IT services that can be provisioned and deployed in a controlled and standardized way across your organization.

The option that says: **Amazon Pinpoint** is incorrect because this is a service for creating and sending messages, segmenting audiences, tracking user engagement, and analyzing campaign performance metrics to optimize messaging strategies. You can engage to users across multiple channels, such as email, SMS, push notifications, and voice messages.

The option that says: **Amazon Grafana** is incorrect because this is a service for creating and visualizing real-time operational dashboards. It does not have the capability to limit access to portfolios.

## References:

<https://aws.amazon.com/servicecatalog/faqs/>

<https://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html>

## Check out this AWS Service Catalog Cheat Sheet:

<https://tutorialsdojo.com/aws-service-catalog/>

Question 37:

### Skipped

Which service enables you to set up directories in the AWS cloud, or connect your AWS resources with an existing on-premises Microsoft Active Directory?

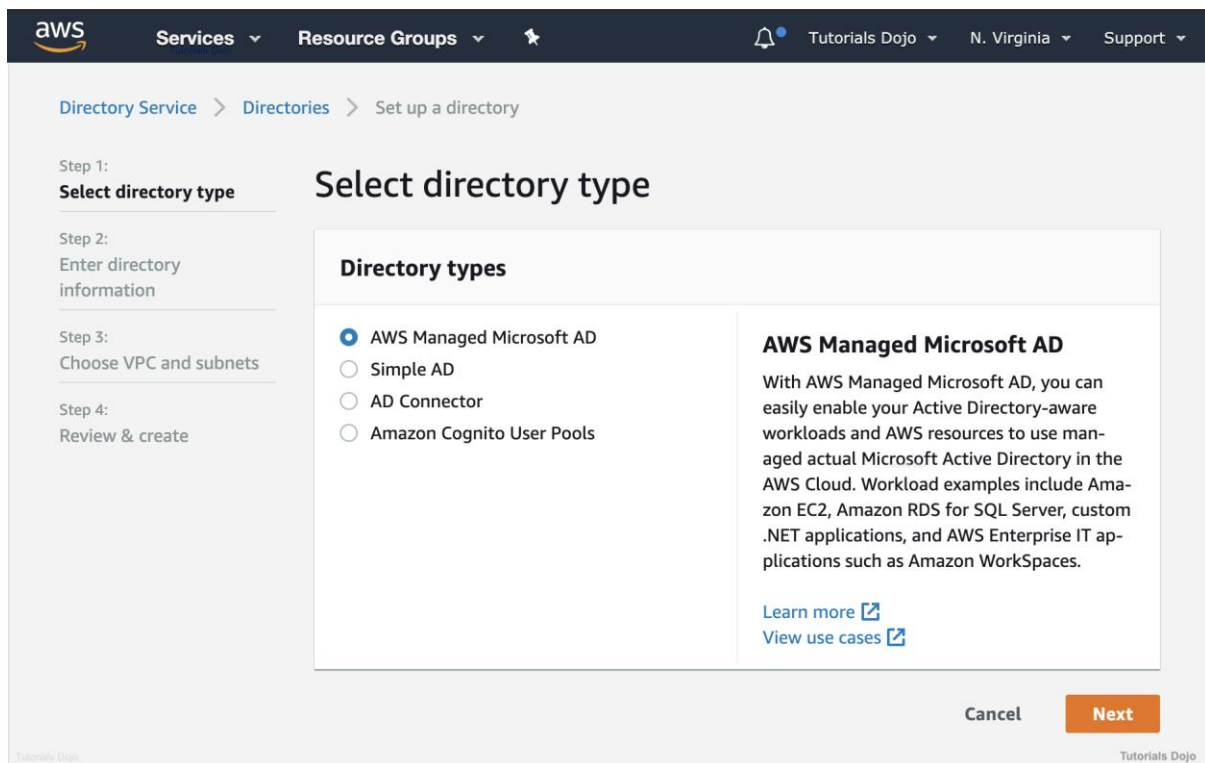
- **AWS Directory Service**

**(Correct)**

- **AWS Site-to-Site VPN**
- **Amazon Connect**
- **AWS Direct Connect**

### Explanation

**AWS Directory Service** for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Managed Microsoft AD is built on actual Microsoft Active Directory and does not require you to synchronize or replicate data from your existing Active Directory to the cloud.



Directory Service makes it easy to set up and run directories in the AWS Cloud or connect your AWS resources with an existing on-premises Microsoft Active Directory.

Once your directory is created, you can use it for a variety of tasks:

- Manage users and groups
- Provide single sign-on to applications and services
- Create and apply group policy
- Securely connect to Amazon EC2 Linux and Windows instances
- Simplify the deployment and management of cloud-based Linux and Microsoft Windows workloads
- You can use AWS Managed Microsoft AD to enable multi-factor authentication by integrating with your existing RADIUS-based MFA infrastructure to provide an additional layer of security when users access AWS applications.

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

**Amazon Connect** is incorrect because it is an omnichannel cloud contact center service that helps companies provide superior customer service across voice and chat at a lower cost than traditional contact center systems. This service can't be used to create directories.

**AWS Direct Connect** and **AWS Site-to-Site VPN** are both incorrect because these are primarily used to establish a connection between on-premises and AWS. These services are not capable of setting up directories in the AWS cloud.

#### References:

<https://aws.amazon.com/directoryservice/>

[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what\\_is.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html)

#### AWS Identity Services Overview:

<https://www.youtube.com/watch?v=AldUw0i8rr0>

#### Check out this AWS Directory Service Cheat Sheet:

<https://tutorialsdojo.com/aws-directory-service/>

Question 38:

#### Skipped

A company plans to work with a third-party provider to deploy a new application that will be accessed globally. You need to delegate permissions to access resources without using permanent credentials.

Which of the following should you use?

- **IAM Role**

**(Correct)**

- **IAM Group**
- **Service Control Policy**
- **IAM User**

#### Explanation

**AWS Identity and Access Management** enable you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Create role

1

2

3

4

Review

Provide the required information below and review this role before you create it.

Role name\*

TD-Serverless-Demo

Use alphanumeric and '+=, @-.' characters. Maximum 64 characters.

Role description


Allows Lambda functions to call AWS services on your behalf.


Maximum 1000 characters. Use alphanumeric and '+=, @-.' characters.


Trusted entities

AWS service: lambda.amazonaws.com

Policies

 AmazonS3FullAccess [↗](#)

 AmazonDynamoDBFullAccess [↗](#)

 AmazonSNSFullAccess [↗](#)

Permissions boundary

Permissions boundary is not set

\* Required

Cancel

Previous

Create role

IAM Roles are a secure way to grant permissions to entities you trust without creating dedicated user accounts. A role does not have any long-term credentials associated with it, such as a password or access keys. Instead, when you assume a role, you are given temporary security credentials for the duration of your role session.

Hence, the correct answer is: **IAM Role**.

**Service Control Policy** is incorrect because this is a feature of AWS Organizations. SCP is a policy that specifies the services and actions that users and roles can use in the accounts that the SCP affects. SCPs are similar to IAM permission policies except that they don't grant any permissions. Instead, SCPs are just filters that allow only the specified services and actions to be used in affected accounts.

**IAM User** is incorrect because this is only an IAM entity that you create in AWS to represent the person or application that uses it to interact with AWS. IAM users are for creating accounts with long-term credentials.

**IAM Group** is incorrect because this is simply 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. IAM Group does not provide temporary credentials to access your AWS resources.

**References:**

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

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_terms-and-concepts.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html)

<https://aws.amazon.com/blogs/security/now-create-and-manage-aws-iam-roles-more-easily-with-the-updated-iam-console/>

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

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

Question 39:

### **Skipped**

A company plans to deploy an enterprise web application that will be accessed globally. The architecture must provide the highest redundancy and fault tolerance to avoid user disruptions.

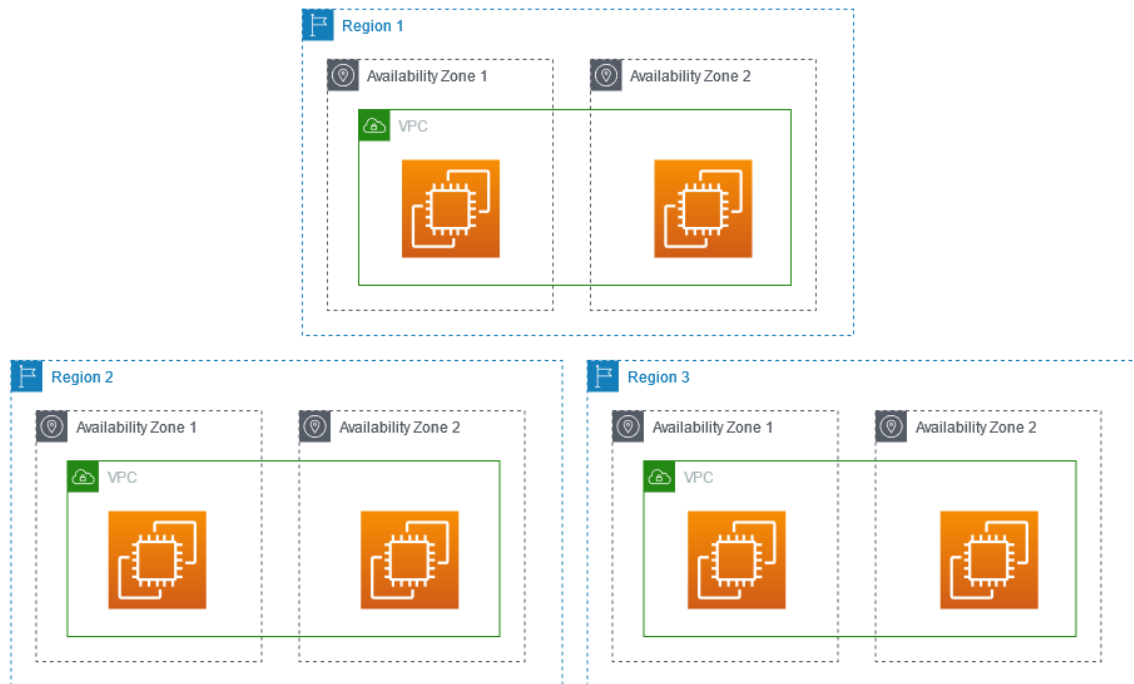
How should the Amazon EC2 instances be deployed to meet the above requirements?

- **Deploy in a single Availability Zone in a single AWS Region.**
- **Deploy to three AWS Regions with one Availability Zone for each region.**
- **Deploy to multiple Availability Zones in a single AWS Region.**
- **Deploy to multiple Availability Zones across three AWS Regions.**

**(Correct)**

### **Explanation**

When you launch an instance, you can select your preferred Availability Zone or let AWS choose one for you. If you distribute your instances across multiple Availability Zones and one instance fails, you can design your application so that an instance in another Availability Zone can handle requests. You can also deploy your applications to multiple AWS Regions to achieve high availability.



**High Availability (HA)** describes systems that are dependable enough to operate continuously without fail. They are well-tested and sometimes equipped with redundant components.

Hence, the correct answer is: **Deploy to multiple Availability Zones across three AWS Regions.**

The option that says: **Deploy in a single Availability Zone in a single AWS Region** is incorrect because if just a single Availability Zone goes down, the system will immediately experience an outage. Conversely, if the entire AWS Region experienced an outage, the application will not be available anymore since there is no secondary AWS Region used in this architecture.

The option that says: **Deploy to three AWS Regions with one Availability Zone for each region** is incorrect. Although it provides high availability, it is still better to deploy the application to multiple Availability Zones instead of just one.

The option that says: **Deploy to multiple Availability Zones in a single AWS Region** is incorrect because if there is an AWS Region outage, the enterprise application will not be able to recover or even failover to a secondary region.

## References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>



<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

**Check out these AWS Well-Architected Framework Cheat Sheets:**

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

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

Question 40:

**Skipped**

Which of the following provides a collection of technical resources to help you build more effectively and efficiently in the AWS Cloud?

- **AWS Config**
- **AWS Architecture Center**

**(Correct)**

- **AWS Trusted Advisor**
- **AWS Organizations**

**Explanation**

The **AWS Architecture Center** provides a collection of technical resources to help you build more effectively and efficiently in the AWS Cloud.

Technology domains:

**Analytics & Big Data** - build secure, reliable, cost-effective data-processing architectures.

**Compute & HPC** - develop, deploy, run, and scale your applications.

**Containers** - secure, reliable, and scalable way to run containers.

**Databases** - choose the right database for your use case and access patterns.

**Machine Learning** - build effective and efficient ML architectures.

**Migration** - move existing applications to the AWS Cloud.

**Security, Identity, & Compliance** - meet your security and compliance goals using AWS infrastructure and services.

**Storage** - design reliable, scalable, and secure data storage architectures.

Well-Architected Tool > Workloads > Define workload

Step 1  
Specify properties

Step 2  
Apply lenses

## Apply lenses

Lenses 1/4

Q Search by lens name < 1 >

**AWS Well-Architected Framework** ☒

Description  
The AWS Well-Architected Framework Lens provides a set of foundational questions for you to consider for all of your cloud architectures.

**FTR Lens** ☐

Description  
The AWS Foundational Technical Review (FTR) Lens provides a set of specific questions for ISVs to perform a workload self-assessment prior to requesting the Foundational Technical Review in the AWS Partner Network (APN).

**Serverless Lens** ☐

Description  
The AWS Serverless Application Lens provides a set of additional questions for you to consider for your serverless applications.

**SaaS Lens** ☐

Description  
The AWS SaaS Lens provides a set of additional questions for you to consider for your Software-as-a-Service (SaaS) applications.

Cancel Previous **Define workload**

You can use the AWS Well-Architected Tool, which 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 answer is: **AWS Architecture Center**.

**AWS Trusted Advisor** is incorrect because this is just an online tool that provides real-time guidance to help you provision your resources following AWS best practices. AWS Trusted Advisor provides recommendations for Cost Optimization, Performance, Security, Fault Tolerance, and Service Limits.

**AWS Organizations** is incorrect because this is only a service that centrally governs your environment as you grow and scale your workloads on AWS. This is mainly used in consolidated billing and management of multiple AWS accounts.

**AWS Config** is incorrect because this is simply a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config as your framework for creating and deploying governance and compliance rules across your AWS accounts and regions.

**References:**

<https://aws.amazon.com/architecture/>

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

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

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

Question 41:

**Skipped**

Which of the following AWS resources is a zonal service? (Select TWO.)

- Amazon S3
- Amazon Route 53
- Amazon EBS

(Correct)

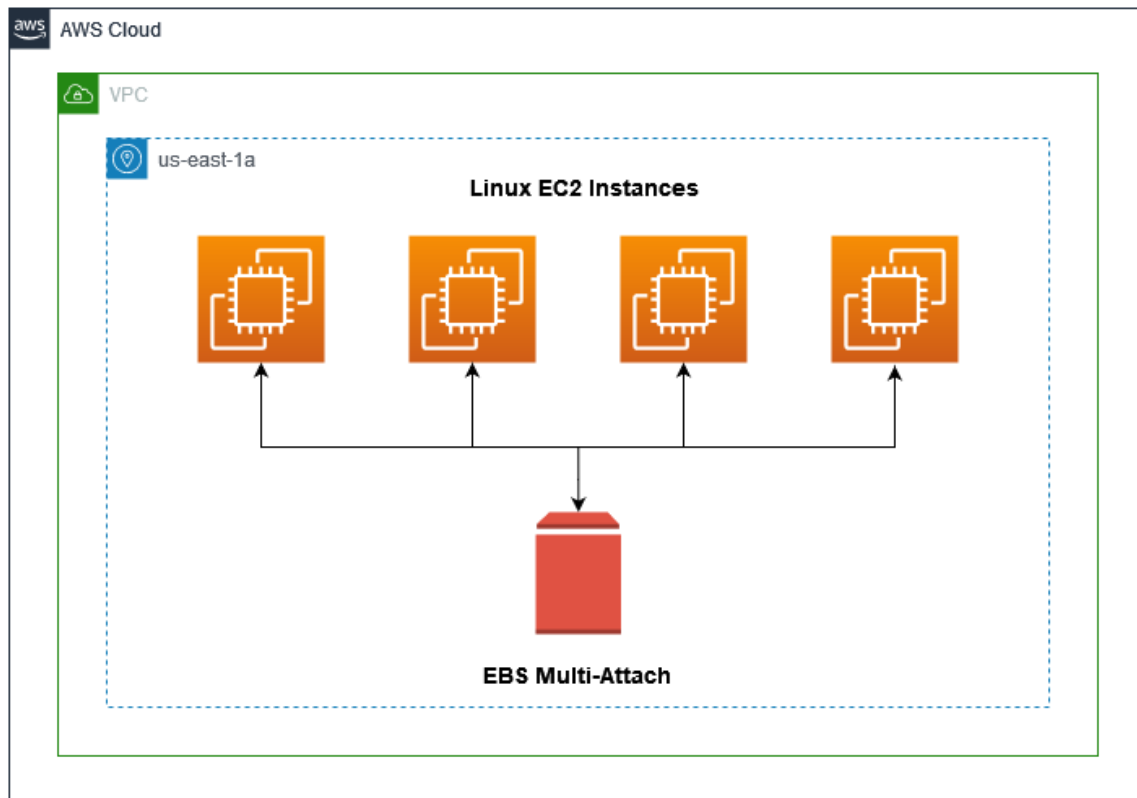
- Amazon EC2

(Correct)

- AWS IAM

**Explanation**

**Global Services** are not tied to a specific region and can be used in all regions. **Regional Services** are accessible by any resources within the same region. **Zonal Services** or **Availability Zone Services** are resources that are hosted in a zone and called per-zone resources. Zone-specific resources are unique to that zone and are only usable by other resources in the same zone.



**Amazon EC2** is a compute capacity in the cloud and **Amazon EBS** is a block storage service. Both are created in a specific Availability Zone, and EBS can be attached to any instances in that same Availability Zone.

Hence, the correct answers are:

- **Amazon EC2**
- **Amazon EBS**

**Amazon S3**, **Amazon Route 53**, and **AWS IAM** are all incorrect because these are global services offered by AWS. These services can be used across all AWS regions and are not Zone-specific.

### References:

<https://aws.amazon.com/about-aws/global-infrastructure/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

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

## AWS Global Infrastructure:

<https://www.youtube.com/watch?v=rno8iNfKChM>

## Check out this AWS Global Infrastructure Cheat Sheet:

<https://tutorialsdojo.com/aws-global-infrastructure/>

Question 42:

### Skipped

An organization is mandated to secure its Amazon S3 bucket and ensure that it cannot have any public objects to satisfy the compliance requirements.

What S3 feature should be used to easily accomplish this?

- **Security Groups**
- **Block Public Access**

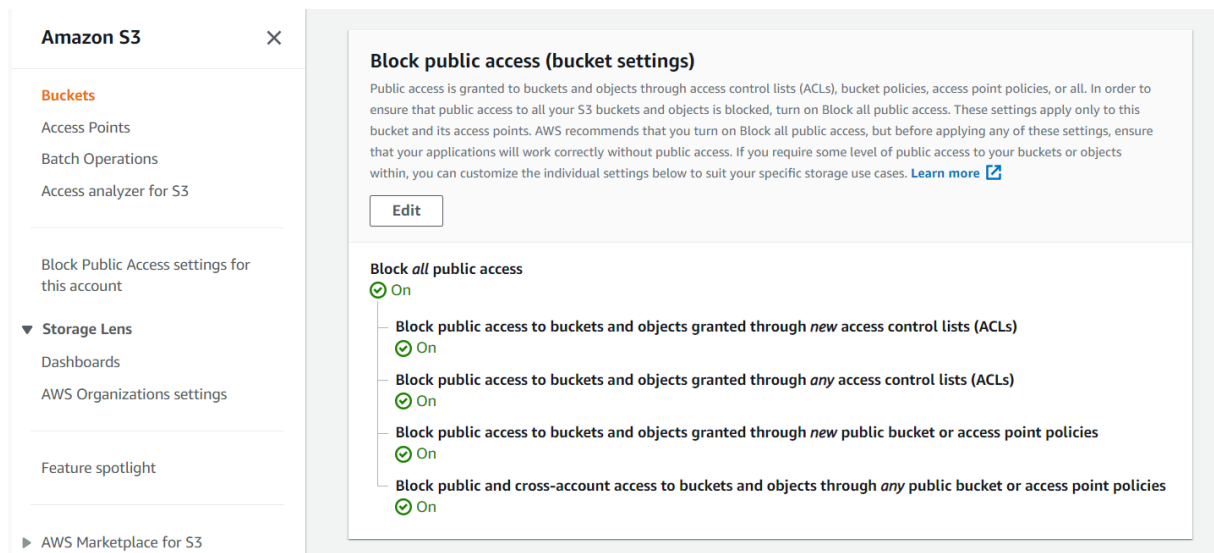
**(Correct)**

- **Network ACL**
- **VPC Endpoint**

### Explanation

**Amazon S3** provides Block Public Access settings for buckets and accounts to help you manage public access to Amazon S3 resources. By default, new buckets and objects don't allow public access, but users can modify bucket policies or object permissions to allow public access. Amazon S3 Block Public Access provides settings that override these policies and permissions so that you can limit public access to these resources.

With Amazon S3 Block Public Access, account administrators and bucket owners can easily set up centralized controls to limit public access to their Amazon S3 resources that are enforced regardless of how the resources are created.



When Amazon S3 receives a request to access a bucket or an object, it determines whether the bucket or the bucket owner's account has a Block Public Access setting. If there is an existing Block Public Access setting that prohibits the requested access, then Amazon S3 rejects the request. Amazon S3 Block Public Access provides four settings. These settings are independent and can be used in any combination, and each setting can be applied to a bucket or to an entire AWS account.

If a bucket has Block Public Access settings that are different from its owner's account, Amazon S3 applies the most restrictive combination of the bucket-level and account-level settings. Thus, when Amazon S3 evaluates whether an operation is prohibited by a Block Public Access setting, it rejects any request that would violate either a bucket-level or an account-level setting.

Hence, the correct answer is: **Block Public Access**.

**Network ACL** is incorrect because a Network ACL is primarily used for VPCs and not in S3 buckets. Amazon S3 has access control lists (ACLs) that enable you to manage access to buckets and objects. Remember that a Network ACL and S3 ACL are different from each other.

**Security Group** is incorrect because Amazon S3 doesn't have a security group.

**VPC Endpoint** is incorrect because this feature doesn't ensure that your objects are not accessible publicly. It just enables you to privately connect your VPC to Amazon S3 without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

**References:**

<https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

**Check out this Amazon S3 Cheat Sheet:**

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

**Amazon S3 and S3 Glacier Overview:**

<https://youtu.be/1ymyeN2tki4>

Question 43:

**Skipped**

A developer plans to build a serverless application with a key-value database. Which of the following AWS services can be used to fulfill this requirement? (Select TWO.)

- **Amazon SageMaker**
- **Amazon RDS**
- **Amazon ECR**
- **Amazon DynamoDB**

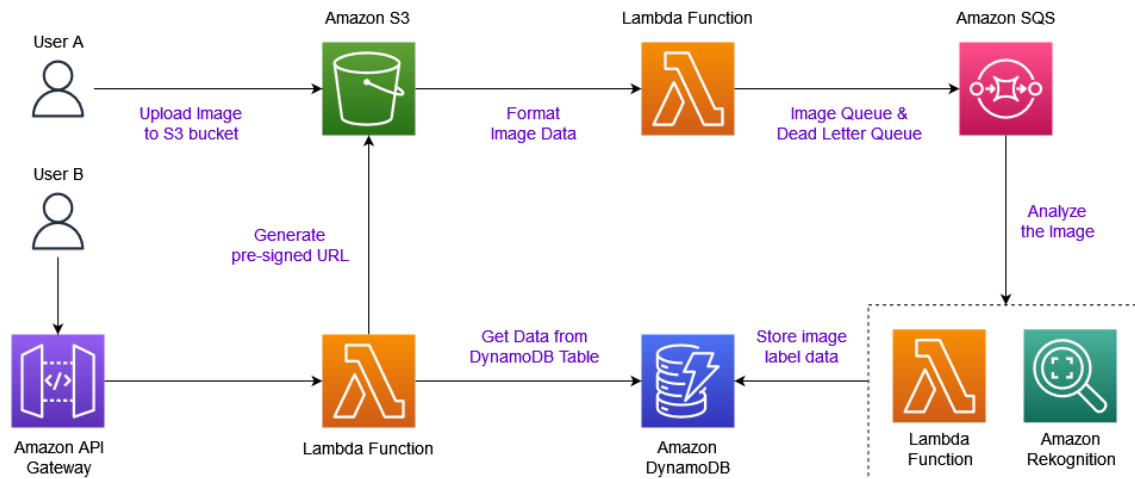
**(Correct)**

- **AWS Lambda**

**(Correct)**

**Explanation**

**AWS Lambda** is a serverless computing service. It lets you run your code without provisioning or managing servers. Serverless computing allows you to build and run applications and services without thinking about servers. With serverless computing, your application still runs on servers, but AWS does all the server management.



**Amazon DynamoDB** is aligned with the values of Serverless applications: automatic scaling according to your application load, pay-per-what-you-use pricing, easy to get started with, and no servers to manage. It makes DynamoDB a very popular choice for Serverless applications running in AWS.

Hence, the correct answers are:

- **AWS Lambda**

- **Amazon DynamoDB**

**Amazon RDS** is incorrect because it is not a key-value database. RDS is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. Also, RDS is not a suitable fit for key-value pairs.

**Amazon ECR** is incorrect because this is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images. ECR is not a serverless computing service. If you want to have a serverless container, you can use AWS Fargate.

**Amazon SageMaker** is incorrect because this is not a serverless service. SageMaker is primarily used to build, train, and deploy machine learning (ML) models quickly.

## References:

<https://docs.aws.amazon.com/lambda/latest/dg/getting-started.html>

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



## AWS Lambda Overview:

<https://www.youtube.com/watch?v=bPVX1zHwAnY>

## Check out these AWS Lambda and Amazon DynamoDB Cheat Sheets:

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

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

Question 44:

### Skipped

A company needs access to the full set of monitoring checks in AWS Trusted Advisor to ensure that its cloud environment is well-architected.

What is the MOST cost-effective support plan that the company should avail of?

- Basic
- Enterprise
- Developer
- Business

**(Correct)**

### Explanation

**AWS Support Plans** 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 offer 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.	24x7 phone, email, and chat access to Cloud Support Engineers	24x7 phone, email, and chat access to Cloud Support Engineers	24x7 phone, email, and chat access to Cloud Support Engineers
	Unlimited cases / 1 primary contact	Unlimited cases / unlimited contacts (IAM supported)	Unlimited cases / unlimited contacts (IAM supported)	Unlimited cases / unlimited contacts (IAM supported)
	Prioritized responses on AWS re:Post	Prioritized responses on AWS re:Post	Prioritized responses on AWS re:Post	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 Infrastructure Event Management for additional fee	Infrastructure Event Management (one-per-year)	Infrastructure Event Management
	Access to Support Automation Workflows with prefixes AWS::Support	Access to Support Automation Workflows with prefixes AWS::Support and AWS::PremiumSupport	Access to Support Automation Workflows with prefixes AWS::Support and AWS::PremiumSupport	Access to proactive reviews, workshops, and deep dives
				Access to Support Automation Workflows with prefixes AWS::Support and AWS::PremiumSupport

In addition to what is available with Basic Support, Business 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 Personal Health Dashboard** - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security.

**Enhanced Technical Support** - 24x7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases.

Hence, the correct answer is: **Business** support plan.

**Enterprise** is incorrect. Although it provides you with a full set of checks, this support plan is not cost-effective compared with the Business support plan.

**Basic** and **Developer** are both incorrect because these support plans only provide 7 Core Checks in AWS Trusted Advisor.

## References:

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

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

**Check out this AWS Support Plans Cheat Sheet:**

Question 45:

**Skipped**

A customer plans to use Amazon S3 to store their less frequently accessed data and reduce their costs. The data is re-creatable and will be used as a secondary backup. They also require S3's low latency and high throughput performance. Which of the following storage classes is the cheapest and most suitable option?

- **S3 Glacier Deep Archive**
- **S3 Standard**
- **S3 One Zone-IA**

**(Correct)**

- **S3 Glacier Flexible Retrieval**

**Explanation**

**S3 One Zone-IA** is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones, Amazon S3 stores the object data in only one Availability Zone, making it less expensive than S3 Standard-IA. However, the data is not resilient to the physical loss of the Availability Zone resulting from disasters, such as earthquakes and floods.

	S3 Standard	S3 Standard-Infrequent Access (IA)	S3 One Zone-Infrequent Access (IA)	S3 Intelligent Tiering
Features	General-purpose storage of frequently accessed data	For long-lived, rapid but less frequently accessed data; data is stored redundantly in multiple AZs	For long-lived, rapid but less frequently accessed data; data is stored redundantly in only one AZ of your choice	For long-lived data that have unpredictable access patterns
Durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Availability	99.99%	99.9%	99.5%	99.9%
Availability SLA	99.9%	99%	99%	99%
Number of Availability Zones	At least 3	At least 3	Only 1	At least 3
Minimum capacity charge per object	N/A	128KB	128KB	N/A
Minimum storage duration charge	N/A	30 days	30 days	30 days
Inserting data	Directly PUT into S3 Standard	Directly PUT into S3 Standard-IA or set Lifecycle policies to transition objects from the S3 Standard to the S3 Standard-IA storage class.	Directly PUT into S3 One Zone-IA or set Lifecycle policies to transition objects from the S3 Standard to the S3 One Zone-IA storage class.	Directly PUT into S3 Intelligent-Tiering or set Lifecycle policies to transition objects from the S3 Standard to the S3 Intelligent-Tiering storage class.
Retrieval fee	N/A	per GB retrieved	per GB retrieved	N/A
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds
Storage transition	S3 Standard to all other S3 storage types including Glacier	S3 Standard-IA to S3 One Zone-IA or S3 Glacier	S3 One Zone-IA to S3 Glacier	S3 Intelligent to S3 One Zone-IA or S3 Glacier
Use Cases	Cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.	Ideally suited for long-term file storage, older sync and share storage, and other aging data.	For infrequently-accessed storage, like backup copies, disaster recovery copies, or other easily recreatable data.	Data with unknown or changing access patterns, optimize storage costs automatically, and unpredictable workloads

S3 One Zone-IA is a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

Hence, the correct answer is: **S3 One Zone-IA**.

**S3 Standard** is incorrect because it is not the cheapest option available.

**S3 Glacier Flexible Retrieval** and **S3 Glacier Deep Archive** are both incorrect because they are designed for low-cost data archiving. These storage classes have retrieval options that take from a few minutes to hours.

#### References:

<https://aws.amazon.com/s3/storage-classes/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html>

#### Amazon S3 and S3 Glacier Overview:

<https://youtu.be/1ymyeN2tki4>

#### Check out this Amazon S3 Cheat Sheet:

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

#### S3 Standard vs S3 Standard-IA vs S3 One Zone-IA vs S3 Intelligent Tiering Comparison:

<https://tutorialsdojo.com/s3-standard-vs-s3-standard-ia-vs-s3-one-zone-ia/>

Question 46:

**Skipped**

Which of the following are the capabilities provided by Amazon Route 53? (Select TWO.)

- **Domain Registration**

**(Correct)**


- **Web traffic filtering**
- **DDoS Protection**
- **DNS Resolution**


**(Correct)**


- **Resource metrics collection**

**Explanation**

**Amazon Route 53** is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.tutorialsdojo.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

 Services ▾

 Search for services, features, marketplace products [Alt+S]

 Tutorials Dojo ▾

Global ▾

Support ▾

1: Domain Search

2: Contact Details

3: Verify & Purchase

## Choose a domain name

.com - \$12.00 Check

### Availability for 'manila-datacenter.com'

Domain Name	Status	Price /1 Year	Action
manila-datacenter.com	✓ Available	\$12.00	<button>Add to cart</button>

### Related domain suggestions

Domain Name	Status	Price /1 Year	Action
manila-datacenter.link	✓ Available	\$5.00	<button>Add to cart</button>
manila-datacenter.net	✓ Available	\$11.00	<button>Add to cart</button>
manila-datacenter.ninja	✓ Available	\$18.00	<button>Add to cart</button>
manila-datacenter.org	✓ Available	\$12.00	<button>Add to cart</button>
maniladatacenter.com	✓ Available	\$12.00	<button>Add to cart</button>
maniladatacenter.net	✓ Available	\$11.00	<button>Add to cart</button>
maniladatacenterfestival.com	✓ Available	\$12.00	<button>Add to cart</button>

Route 53 key features are:

- **Resolver** - get recursive DNS for your Amazon VPC and on-premises networks.
- **Traffic flow** - route end users to the best endpoint for your application based on geoproximity, latency, health, and other considerations.
- **Latency-based routing** - route end users to the AWS region that provides the lowest possible latency.
- **Geo DNS** - route end users to a particular endpoint that you specify based on the end user's geographic location.
- **Private DNS for Amazon VPC** - Manage custom domain names for your internal AWS resources without exposing DNS data to the public Internet.

- **DNS Failover** - automatically route your website visitors to an alternate location to avoid site outages.

- **Health Checks and Monitoring** - monitor your application's health and performance, as well as your web servers and other resources.

- **Domain Registration** - search for and register available domain names or transfer in existing domain names.

Hence, the correct answers are:

- **DNS Resolution**

- **Domain Registration**

**Web traffic filtering** is incorrect because it is simply a feature of AWS Web Application Firewall (WAF) that helps in creating rules for filtering web traffic based on the criteria you choose.

**Resource metrics collection** is incorrect because this is just a feature that gives data about the performance of your system using Amazon CloudWatch.

**DDoS Protection** is incorrect because this is an AWS Shield feature that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

#### References:

<https://aws.amazon.com/route53>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>

#### Amazon Route 53 Overview:

<https://www.youtube.com/watch?v=Su308t19ubY>

#### Check out this Amazon Route 53 Cheat Sheet:

<https://tutorialsdojo.com/amazon-route-53/>

Question 47:

**Skipped**

A team of developers needs to run hundreds of thousands of fully managed batch computing jobs on AWS. Which of the following service should they choose?

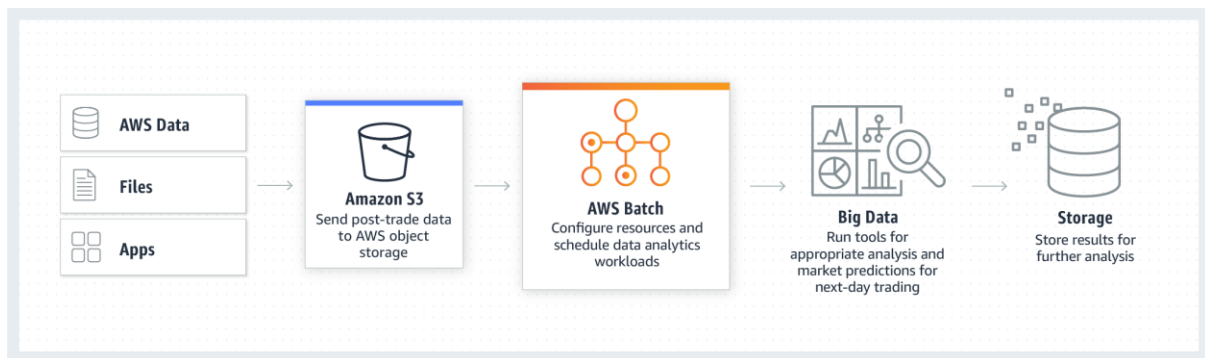
- **AWS Batch**

**(Correct)**

- **AWS Fargate**
- **AWS Lambda**
- **AWS Elastic Beanstalk**

#### Explanation

**AWS Batch** is a set of batch management capabilities that enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources based on the volume and specific resource requirements of the batch jobs submitted.



AWS Batch manages compute environments and job queues, allowing you to easily run thousands of jobs of any scale using EC2 and Spot Instances. It carefully monitors the progress of your jobs. When capacity is no longer needed, it will be removed.

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

**AWS Lambda** and **AWS Fargate** are both incorrect since these are just serverless computing services. Lambda lets you run code without provisioning or managing servers, while Fargate removes the need to provision and manage servers using a serverless compute engine built for containers on AWS. Therefore, these services are not suitable for the provision of thousands of computing jobs.

**AWS Elastic Beanstalk** is incorrect because this is simply a managed platform that supports running web applications developed for specific programming languages, frameworks, and web containers. Elastic Beanstalk is a Platform-as-a-Service cloud deployment model, and you don't manage the underlying infrastructure of this service. It is not suitable for running hundreds of thousands of batch computing jobs on AWS.

## References:

<https://aws.amazon.com/batch/>

<https://docs.aws.amazon.com/batch/latest/userguide/what-is-batch.html>

## Check out this AWS Batch Cheat Sheet:

<https://tutorialsdojo.com/aws-batch/>

Question 48:

### Skipped

A high-performance computing (HPC) application needs a storage service in AWS that can be used as a centralized Windows File Server for multiple EC2 instances.

Which of the following should they use?

- Amazon EBS
- Amazon S3
- Amazon FSx

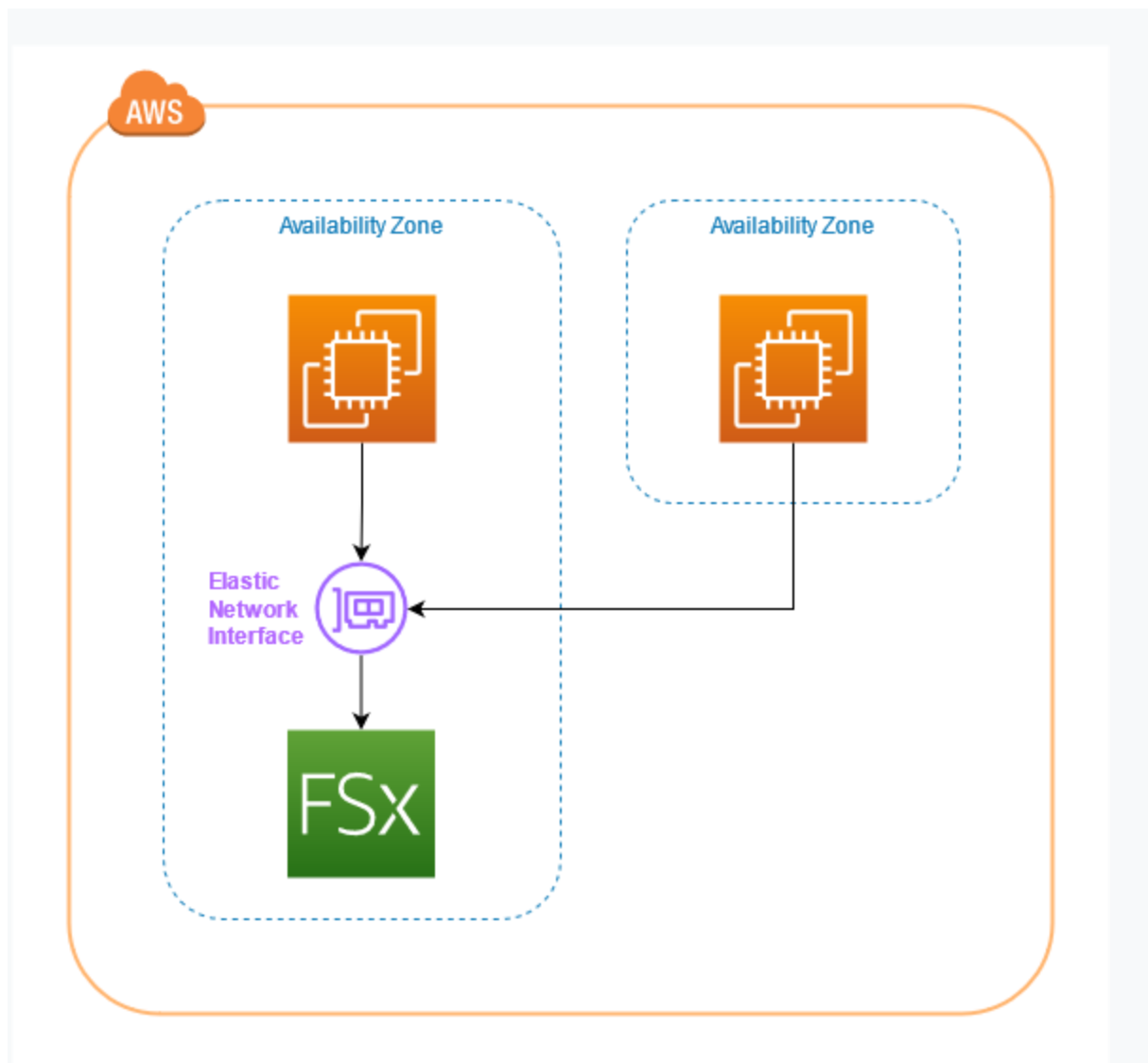
(Correct)

- Amazon EFS

### Explanation

**Amazon FSx** makes it easy and cost-effective to launch and run popular file systems. With Amazon FSx, you can leverage the rich feature sets and fast performance of widely-used open source and commercially licensed file systems, while avoiding time-consuming administrative tasks like hardware provisioning, software configuration, patching, and backups. It provides cost-efficient capacity and high levels of reliability, and it integrates with other AWS services so that you can manage and use the file systems in cloud-native ways.





Amazon FSx provides you with four file systems to choose from:

1. **Amazon FSx for Windows File Server** provides fully managed file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.
2. **Amazon FSx for Lustre** makes it easy and cost-effective to launch and run the world's most popular high-performance file system, Lustre.
3. **Amazon FSx for NetApp ONTAP** a cloud storage service for launching and managing ONTAP file systems.
4. **Amazon FSx for OpenZFS** a service for migrating data from on-premises ZFS or other Linux-based file servers to AWS.

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

**Amazon S3** is incorrect because this is just an object storage service. You can't use this as a centralized Windows File Server.

**Amazon EFS** is incorrect. Although it is a shared file system storage, EFS only supports Linux workloads.

**Amazon EBS** is incorrect. An EBS volume can only be accessed by multiple EC2 instances if it is a Provisioned IOPS EBS volume. A more suitable option here is to use Amazon FSx for Windows File Server.

#### References:

<https://aws.amazon.com/fsx/>

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html>

#### Check out this Amazon FSx Cheat Sheet:

<https://tutorialsdojo.com/amazon-fsx/>

Question 49:

#### Skipped

A company is planning to launch an Amazon EC2 instance with an attached EBS volume in a default configuration. You will be charged for your EBS storage only when your instance is in which instance state?

- **Terminated**
- **Pending**
- **Stopped**

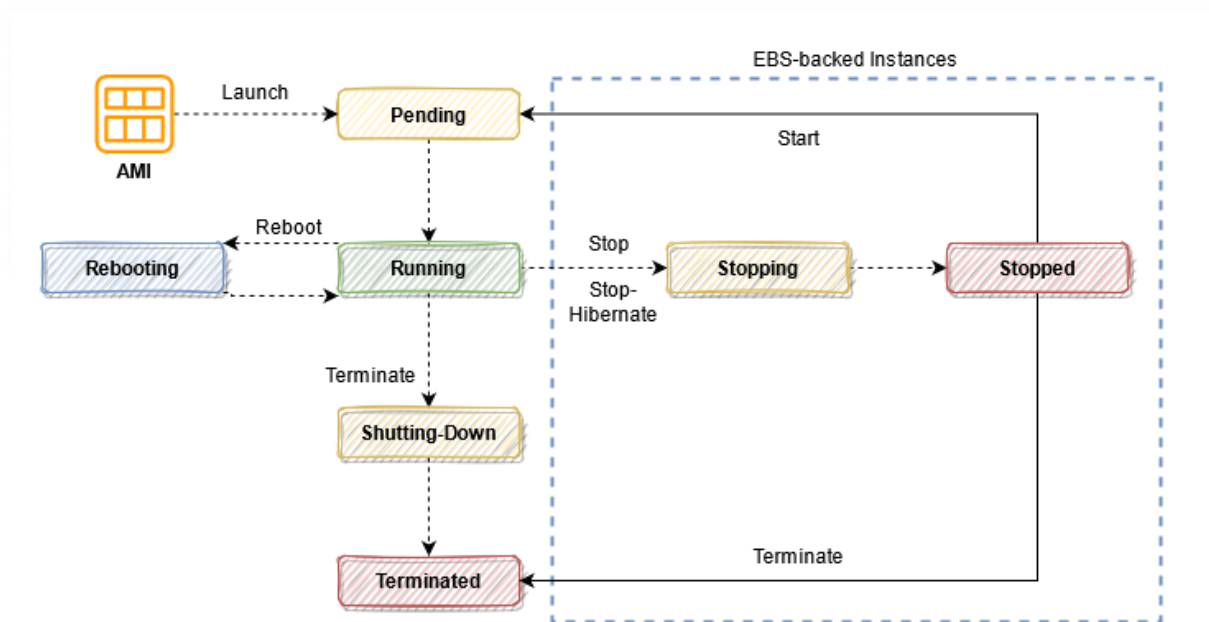
**(Correct)**

- **Running**

#### Explanation

When you launch an instance, it enters the PENDING state. The instance type that you specified at launch determines the hardware of the host computer for your instance. We use the Amazon Machine Image (AMI) you specified at launch to boot the instance. After the instance is ready for you, it enters the RUNNING state. You can connect to your running instance and use it the way that you'd use a computer sitting in front of you.

As soon as your instance transitions to the RUNNING state, you're billed for each second, with a one-minute minimum, that you keep the instance running, even if the instance remains idle and you don't connect to it.



When you **STOP** an instance, AWS shuts it down. AWS doesn't charge users for a stopped instance, or data transfer fees, but AWS does charge for the storage for any Amazon EBS volumes. Each time you start a stopped instance, AWS charges a minimum of one minute for usage. After one minute, AWS charges only for the seconds you use.

By default, Amazon EBS root device volumes are automatically deleted when the instance terminates. However, by default, any additional EBS volumes that you attach at launch, or any EBS volumes that you attach to an existing instance persist even after the instance terminates. This behavior is controlled by the volume's `DeleteOnTermination` attribute, which you can modify.

Hence, the correct answer in this scenario is: **Stopped**.

**Running** is incorrect because in this state, you are billed for the compute, memory, storage, and network of an EC2 instance. Take note that the scenario asks for the instance state where you'll only be charged for the EBS storage.

**Terminated** is incorrect because you won't be charged in this state and both the instance and EBS storage will be deleted by default. Remember that it was stated in the scenario that the Amazon EC2 instance with an attached EBS volume is using a default configuration.

**Pending** is incorrect because it is still preparing the instance to enter the running state. If the instance is not running, then you are not billed for the instance usage.

**References:**

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop\\_Start.html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html)

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

### Amazon EC2 Overview:

[https://youtu.be/7VsGIHT\\_jQE](https://youtu.be/7VsGIHT_jQE)

### Check out this Amazon EC2 Cheat Sheet:

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

Question 50:

#### Skipped

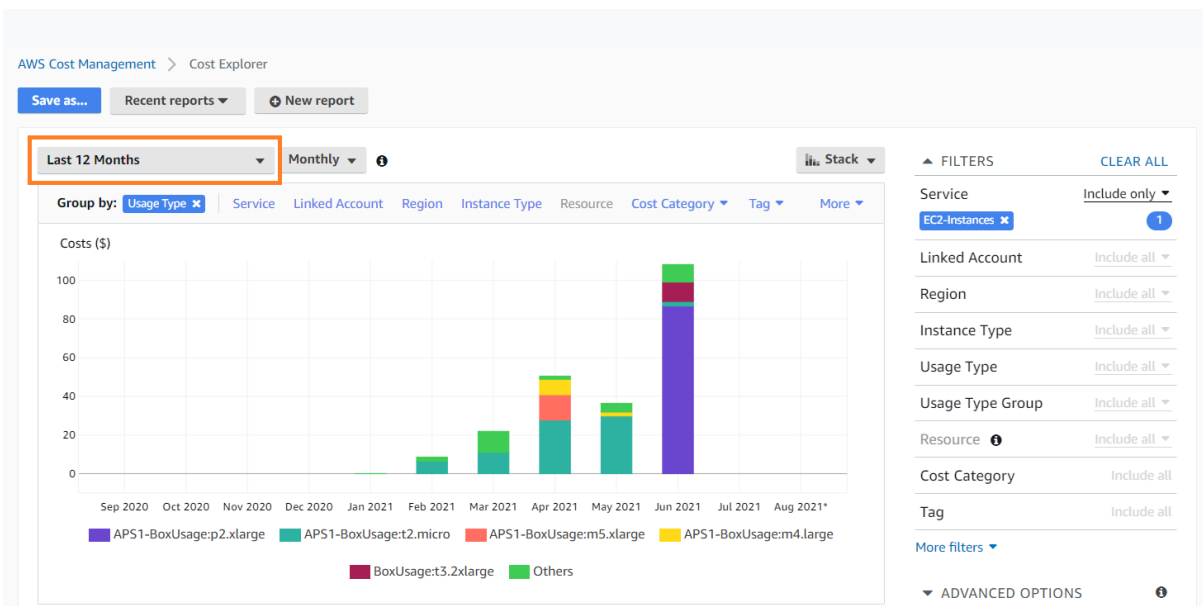
A company is using Cost Explorer to gain an understanding of its cost trends in AWS. How many months of historical data can Cost Explorer store and display?

- 3 Months
- 15 Months
- 6 Months
- 12 Months

(Correct)

#### Explanation

**AWS 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. It also identifies areas that need further inquiry and sees trends that you can use to understand your costs.



Cost Explorer can display up to 12 months of historical data, the current month, and the forecasted costs for the next three months.

Hence, the correct answer is: **12 Months**.

The option that says: **15 Months** is incorrect because this is beyond the capacity of Cost Explorer. This is only applicable in Amazon Cloudwatch which enables you to view both up-to-the-minute data, historical data, and kept for 15 months.

The option that says: **6 Months** and **3 Months** are both incorrect because you can view data for up to the last 12 months using AWS Cost Explorer.

## References:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-what-is.html>

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

**Check out this AWS Billing and Cost Management Cheat Sheet:**

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

Question 51:

## Skipped

Which of the following support plans provides access to the AWS Personal Health Dashboard?

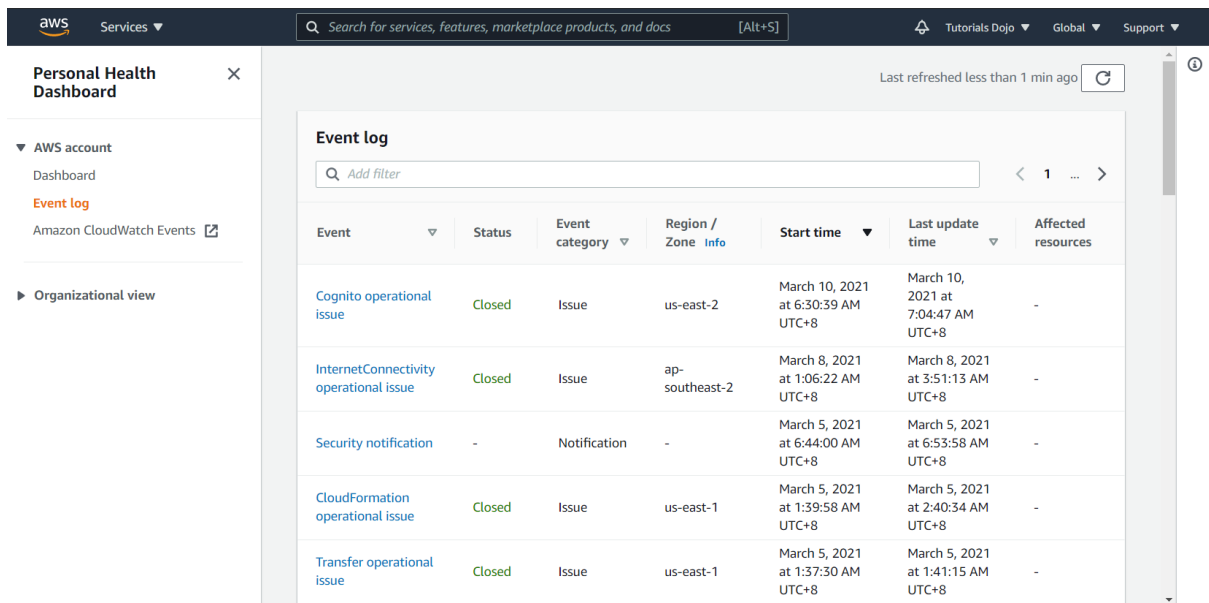
- Developer, Business, Enterprise
- Basic, Business, Enterprise
- Basic, Developer, Business

- **Basic, Developer, Business, Enterprise**

**(Correct)**

### Explanation

**AWS Support Plans** offers a range of plans that provide access to tools and expertise that support your AWS solutions' success and operational health. All support plans offer 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.



Basic Support is included for all AWS customers and includes:

**Customer Service & Communities** - 24x7 access to customer service, documentation, whitepapers, and support forums.

**AWS Trusted Advisor** - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security.

**AWS Personal Health Dashboard** - A personalized view of the health of AWS services, and alerts when your resources are impacted.

Hence, the correct answer is: **Basic, Developer, Business, and Enterprise** support plans.

All other choices are incorrect because all AWS Support Plans provide access to the AWS Personal Health Dashboard.

## References:

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

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

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

## Check out this AWS Support Plans Cheat Sheet:

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

Question 52:

### Skipped

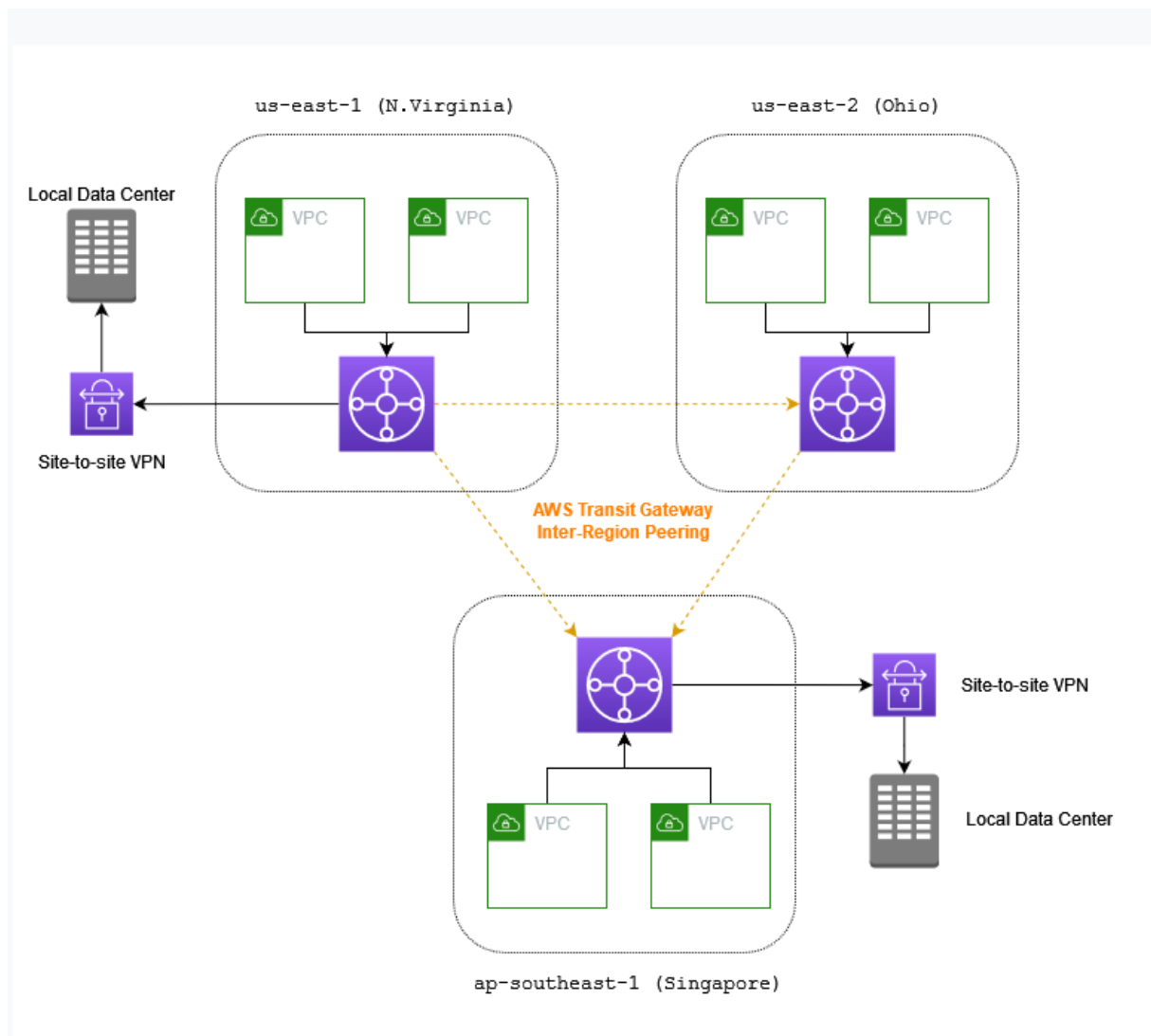
Which of the following services connects VPCs and on-premises networks through a central hub?

- **AWS Client VPN**
- **Amazon VPC Peering**
- **AWS Direct Connect**
- **AWS Transit Gateway**

**(Correct)**

### Explanation

**AWS Transit Gateway** connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once.



Without a central hub, the network complexity increases with scale. You must maintain routing tables within each VPC and connect to each onsite location using separate network gateways. But if you use a centralized hub, your network is more streamlined and scalable. AWS Transit Gateway routes all traffic to and from each VPC or VPN, and you have one place to manage and monitor it all.

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

**AWS Client VPN** is incorrect because this is just a VPN service used to securely access your AWS resources and resources in your on-premises network. You can't use AWS Client VPN to connect and manage multiple VPCs.

**VPC Peering** is incorrect. Although this service could connect two or more VPCs, it is not appropriate to use if you are managing multiple VPC peering connections and on-premises networks at scale.

**AWS Direct Connect** is incorrect because this is a dedicated network connection from your on-premises to AWS. Direct Connect doesn't support the peering between VPCs unless it is associated with Transit Gateway.



## References:

<https://aws.amazon.com/transit-gateway/>

<https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html>

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/transit-gateway-vs-vpc-peering.html>

## Check out this AWS Transit Gateway Cheat Sheet:

<https://tutorialsdojo.com/aws-transit-gateway/>

Question 53:

### Skipped

A customer plans to speed up the time it takes to download data between its clients and S3 bucket over long distances. Which service would meet this requirement?

- **Amazon Route 53**
- **AWS Elastic Load Balancing (ELB)**
- **Amazon Kinesis**
- **Amazon S3 Transfer Acceleration**


**(Correct)**

### Explanation

**Amazon S3 Transfer Acceleration** can speed up content transfers to and from Amazon S3 by as much as 50% - 500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet.

## Edit transfer acceleration

### Transfer acceleration


Use an accelerated endpoint for faster data transfers. [Learn more](#) 



Transfer acceleration

☐ Disable

☒ Enable

Accelerated endpoint

 tutorialsdojo-bucket.s3-accelerate.amazonaws.com

 Use the accelerated endpoint for faster data transfers, which will incur an additional fee. See [Amazon S3 pricing](#) 

Cancel

Save changes

S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrive at an edge location, they are routed to Amazon S3 over an optimized network path.

Hence, the correct answer is: **Amazon S3 Transfer Acceleration.**

**AWS Elastic Load Balancing (ELB)** is incorrect because it is a service that helps distribute incoming traffic across multiple targets (such as EC2 instances or containers) to improve the availability and scalability of applications. Although ELB can enhance application performance by distributing incoming traffic across multiple targets, it does not optimize data transfer speeds for S3 bucket downloads.

**Amazon Kinesis** is incorrect because it cannot accelerate the transfer of data over long distances from an S3 bucket. Kinesis is primarily used to collect, process, and analyze real-time streaming data to get timely insights and react quickly to new information.

**Amazon Route 53** is incorrect because this service just provides a highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services. You can use Route 53 to route end-users to Internet applications by translating names like tutorialsdojo.com into numeric IP addresses, and not for transferring files in an S3 bucket.

## References:

<https://aws.amazon.com/s3/transfer-acceleration/>

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

## Amazon S3 and S3 Glacier Overview:

<https://youtu.be/1ymyeN2tki4>

## S3 Transfer Acceleration vs Direct Connect vs VPN vs Snowball Edge vs Snowmobile Comparison:

<https://tutorialsdojo.com/s3-transfer-acceleration-vs-direct-connect-vs-vpn-vs-snowball-vs-snowmobile/>

Question 54:

### Skipped

A company wants to shift its operations to the AWS Cloud. The company is using the various AWS Cloud Adoption Framework (AWS CAF) perspectives to expand pilot initiatives and business value to the desired scale.

Which specific phase of the cloud transformation journey does this align with?

- **Scale**

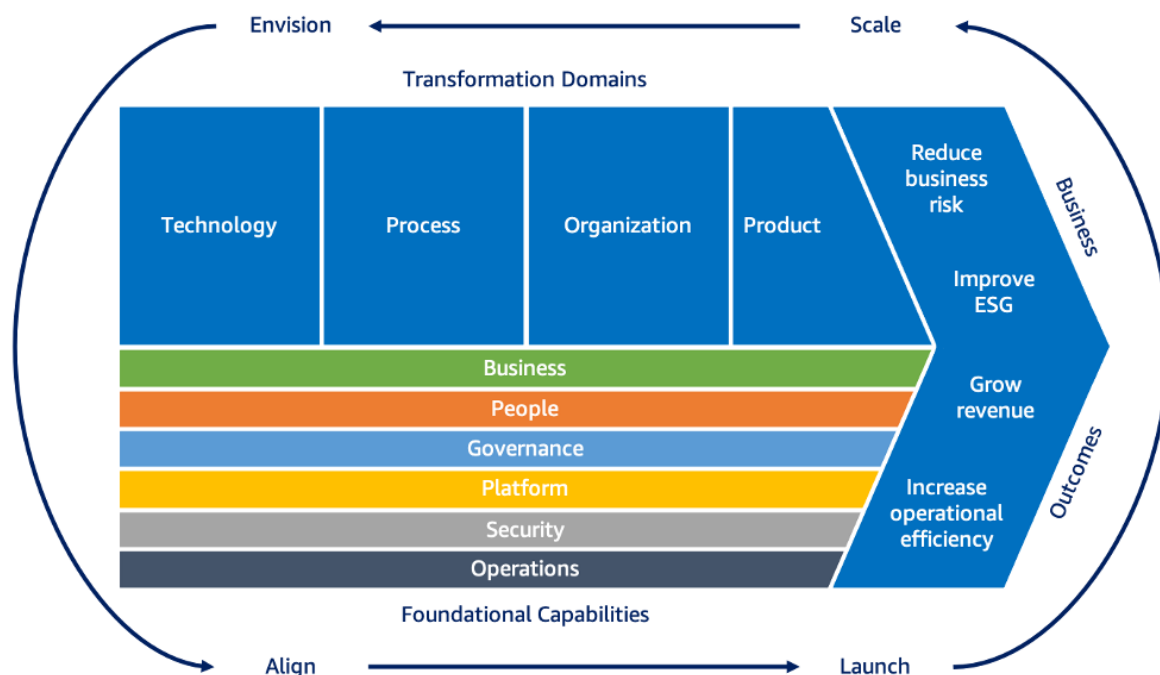
**(Correct)**

- **Launch**
- **Align**
- **Envision**

### Explanation

The **AWS Cloud Adoption Framework (AWS CAF)** leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Adopting an iterative approach will help you maintain momentum and evolve your roadmap as you learn from experience. The AWS CAF recommends four iterative and incremental cloud transformation phases, shown below.



The **Scale phase** focuses on expanding production pilots and business value to the desired scale and ensuring that the business benefits associated with your cloud investments are realized and sustained.

Hence, the correct answer is **Scale**.

**Envision** is incorrect because it primarily focuses on demonstrating how the cloud will help accelerate business outcomes rather than expanding pilots and business value to the desired scale.

**Align** is incorrect because it only focuses on identifying capability gaps across the different AWS CAF perspectives, identifying cross-organizational dependencies, and surfacing stakeholder concerns and challenges.

**Launch** is incorrect because it just focuses on delivering pilot initiatives in production and on demonstrating incremental business. It also ensures that the business benefits associated with your cloud investments are realized and sustained.

## References:

<https://aws.amazon.com/cloud-adoption-framework/>

<https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/your-cloud-transformation-journey.html>

Check out this AWS Cloud Adoption Framework:

<https://tutorialsdojo.com/aws-cloud-adoption-framework-aws-caf/>

Question 55:

**Skipped**

What is the main benefit of deploying instances to multiple availability zones?

- **Cost Optimization**
- **High Availability**

**(Correct)**

- **Security**
- **Agility**

#### Explanation

When you launch an instance, you can select your preferred Availability Zone or let AWS choose one for you. If you distribute your instances across multiple Availability Zones and one instance fails, you can design your application so that an instance in another Availability Zone can handle requests.



**High Availability (HA)** describes systems that are dependable enough to operate continuously without fail. They are well-tested and sometimes equipped with redundant components.

Hence, the correct answer is: **High Availability**.

**Agility** is incorrect because this is the ability to rapidly develop, test, and launch software applications that drive business growth. It is not the benefit of deploying instances to multiple availability zones.

**Cost Optimization** is incorrect because this is the ability to avoid or eliminate unneeded costs or suboptimal resources. This benefit is not related to the availability of your application.

**Security** is incorrect because this is the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

#### References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

#### Check out these AWS Well-Architected Framework Cheat Sheets:

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

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

Question 56:

#### Skipped

What is the MOST affordable AWS Support plan that provides users access to the AWS Support API?

- **Business**

**(Correct)**

- **Enterprise**
- **Developer**
- **Basic**

#### Explanation

**AWS Support Plans** 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 offer 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 AWS::Support	Access to Infrastructure Event Management for additional fee Access to Support Automation Workflows with prefixes AWS::Support and AWS::PremiumSupport	Infrastructure Event Management (one-per-year) Access to Support Automation Workflows with prefixes AWS::Support and AWS::PremiumSupport	Infrastructure Event Management Access to proactive reviews, workshops, and deep dives Access to Support Automation Workflows with prefixes AWS::Support and AWS::PremiumSupport

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

**AWS Support API** - Let you create support cases and add correspondence to them throughout investigations of your issues and interactions with the AWS Support staff.

**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 Personal Health Dashboard**- Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security.

**Enhanced Technical Support** - 24x7 access to Cloud Support Engineers via phone, chat, and email. You can have an unlimited number of contacts that can open an unlimited amount of cases.

Hence, the correct answer is: **Business** support plan.

**Enterprise** is incorrect. Although it will provide you AWS Support API access, this support plan is more expensive than the Business support plan.

**Basic** and **Developer** are both incorrect because these support plans don't offer access to AWS Support API for programmatic case management.

## References:

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

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

Check out this AWS Support Plans Cheat Sheet:

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

Question 57:

**Skipped**

Which AWS service provides tracing and monitoring capabilities for your Lambda function?

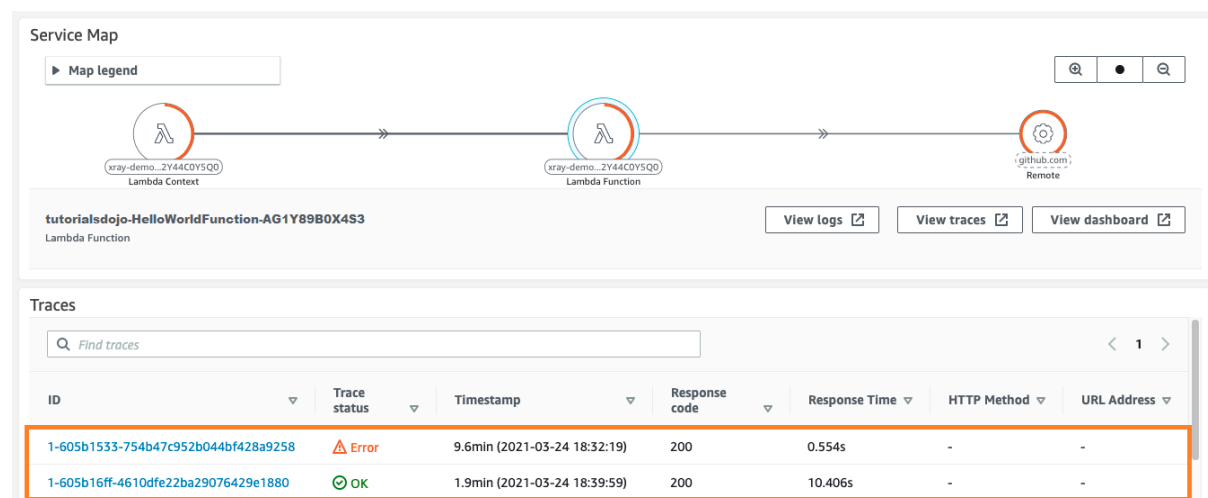
- Amazon Inspector
- AWS X-Ray

**(Correct)**

- AWS Shield
- Amazon Macie

**Explanation**

**AWS X-Ray** can trace requests made to your serverless applications built using AWS Lambda. It enables you to gain insights into the performance of serverless applications, allowing you to pinpoint the root cause of issues so that you can address them.



X-Ray makes it easy for you to:

**Create a service map** – By tracking requests made to your applications, X-Ray can create a map of services used by your application.

**Identify errors and bugs** – X-Ray can automatically highlight bugs or errors in your application code by analyzing the response code for each request made to your application.

**Build your own analysis and visualization apps** – X-Ray provides a set of query APIs that you can use to build your own analysis and visualization apps that use the data that X-Ray records.



Hence, the correct answer is: **AWS X-Ray**.

**Amazon Inspector** is incorrect because this is just a security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector cannot debug, trace, or monitor a Lambda function. It is primarily used to automatically assess applications for exposure, vulnerabilities, and deviations from AWS best practices.

**AWS Shield** is incorrect because this service cannot identify errors and bugs in your application or AWS Lambda function code. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

**Amazon Macie** is incorrect because this is simply a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. This option doesn't have tracing and monitoring capabilities.

#### References:

<https://aws.amazon.com/xray>

<https://docs.aws.amazon.com/lambda/latest/dg/services-xray.html>

#### Check out this AWS X-Ray Cheat Sheet:

<https://tutorialsdojo.com/aws-x-ray/>

Question 58:

#### Skipped

Which AWS service can automatically detect a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers?

- **Amazon Rekognition**
- **Amazon Macie**

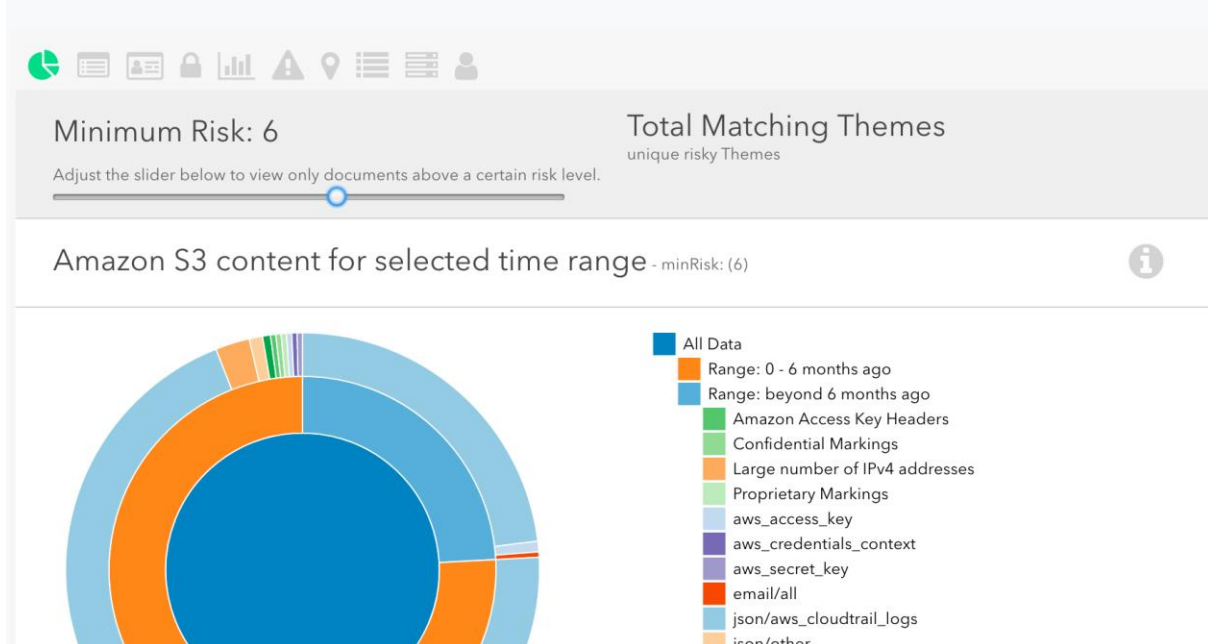
**(Correct)**

- **Amazon CloudWatch**
- **Amazon CloudSearch**

#### 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 these data are being accessed or moved.



You can use Amazon Macie to automatically detect a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers.

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

**Amazon Rekognition** is incorrect. Although it is a machine learning-based service like Amazon Macie, it is primarily used for image and video analysis but not for detecting personally identifiable information (PII). You can't use this to protect your sensitive data in AWS.

**Amazon CloudSearch** is incorrect because this service cannot protect sensitive data in AWS. CloudSearch is a service in the AWS Cloud that is used to set up, manage, and scale a search solution for your website or application in AWS.

**Amazon Cloudwatch** is incorrect because it is a monitoring service that provides operational insights into resources and applications running on AWS. Although it can help monitor logs, it does not have the specific capability to detect sensitive data types in logs.

## References:

<https://aws.amazon.com/macie/>

<https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html>

## AWS Security Services Overview - Secrets Manager, ACM, Macie:

<https://youtu.be/ogVamzF2Dzk>

Check out this Amazon Macie Cheat Sheet:

<https://tutorialsdojo.com/amazon-macie/>

Question 59:

### Skipped

A developer needs to install their application in Docker containers. Which of the following services eliminates the need to manage containers manually?

- Amazon FSx
- AWS Fargate

(Correct)

- Amazon ECS
- Amazon EC2

### Explanation

**AWS Fargate** is a serverless compute engine for containers. Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design.



```
"logConfiguration": {
  "logDriver": "awslogs",
  "options": {
    "awslogs-group": "awslogs-wordpress",
    "awslogs-region": "us-west-2",
    "awslogs-stream-prefix": "awslogs-example"
  }
}
```

Fargate lets you define your application content, networking, storage, and scaling requirements. There is no provisioning, patching, cluster capacity management, or any infrastructure management required.

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

**Amazon FSx** is incorrect because this is primarily used as a file system for Windows-based applications.

**Amazon ECS** is incorrect because by using this service, you still need to manage your own EC2 instances where your containers are hosted.

**Amazon EC2** is incorrect since you still need to provision and manage your Docker containers that are hosted in these EC2 instances.

#### References:

<https://aws.amazon.com/fargate/>

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html>

#### AWS Container Services Overview:

<https://www.youtube.com/watch?v=5QBgDX7O7pw>

#### Check out this AWS Fargate Cheat Sheet:

<https://tutorialsdojo.com/aws-fargate/>

Question 60:

#### Skipped

A company plans to encrypt and manage its own encryption keys using a single-tenant hardware security module. The company must also have exclusive control over how its keys are used via an authentication mechanism independent from AWS.

Which service would meet that requirement?

- **AWS CloudHSM**

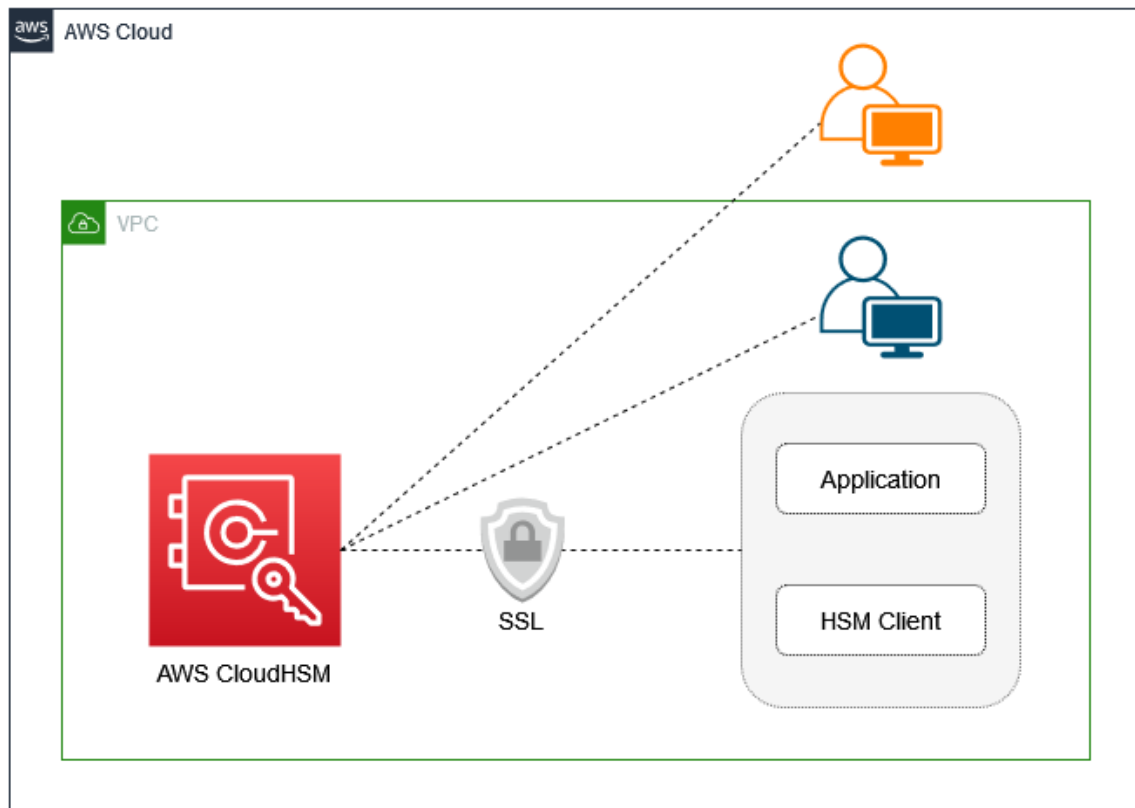
**(Correct)**

- Amazon S3
- AWS KMS
- Amazon GuardDuty

#### Explanation

**AWS CloudHSM** is standards-compliant and enables you to export all of your keys to most other commercially available HSMs, subject to your configurations. It is a fully

managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.



AWS CloudHSM provides you with a FIPS 140-2 Level 3 overall validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPC) to store and use your keys. You have exclusive control over how your keys are used via an authentication mechanism independent from AWS. You interact with keys in your AWS CloudHSM cluster similar to the way you interact with your applications running in Amazon EC2. You can use AWS CloudHSM to support a variety of use cases, such as Digital Rights Management (DRM), Public Key Infrastructure (PKI), document signing, and cryptographic functions using PKCS#11, Java JCE, or Microsoft CNG interfaces.

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

**Amazon GuardDuty** is incorrect because this is just a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. This service doesn't provide you a hardware security module.

**Amazon S3** is incorrect because this is simply a storage service and not an encryption service. You can use S3 to store and retrieve any amount of data, at any

time, from anywhere on the web. You can store as many objects as you want in one or more buckets, and each object can be up to 5 TB in size.

**AWS KMS** is incorrect because this service is primarily used to create and manage cryptographic keys, and control their use across a wide range of AWS services and in your applications. KMS CMKs are backed by multi-tenant, FIPS-validated hardware service modules (HSMs) that AWS manages. Take note that the requirement in the scenario is to have exclusive control over how its keys are used via an authentication mechanism independent from AWS. To manage your own HSMs, you have to use AWS CloudHSM.

#### References:

<https://aws.amazon.com/cloudhsm/>

<https://docs.aws.amazon.com/cloudhsm/latest/userguide/introduction.html>

<https://aws.amazon.com/kms/faqs/>

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

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

Question 61:

#### Skipped

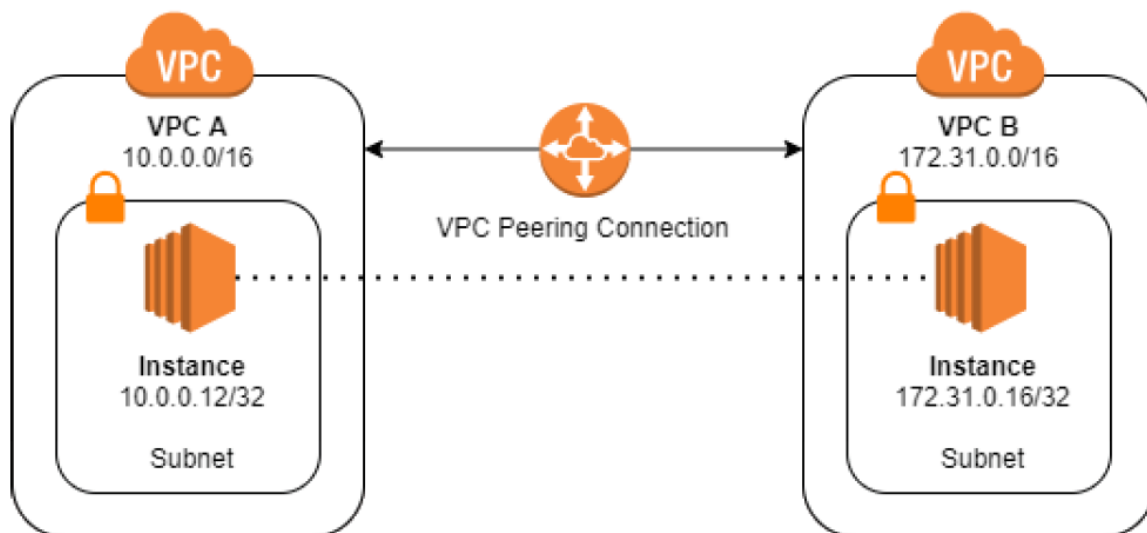
A customer needs to establish a private connection between two virtual private clouds (VPCs) without using additional software. Which of the following should they use?

- **AWS Site-to-Site VPN**
- **AWS Direct Connect**
- **Amazon Connect**
- **VPC Peering**

**(Correct)**

#### Explanation

A **VPC Peering** connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).



VPC Peering allows VPC resources, including EC2 instances, Amazon RDS databases, and Lambda functions that run in different AWS Regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections, or separate network appliances.

Hence, the correct answer is: **VPC Peering**.

**Amazon Connect** is incorrect because it is an omnichannel cloud contact center service that helps companies provide superior customer service across voice and chat at a lower cost than traditional contact center systems. This service doesn't provide a private connection between VPCs.

**Amazon Direct Connect** and **AWS Site-to-Site VPN** are both incorrect because these are just used to establish a connection between on-premises and AWS. The scenario doesn't need a hybrid architecture to establish a private connection between two VPCs. Therefore, these services are incorrect.

#### References:

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-peering.html>

Check out this **VPC Peering Cheat Sheet**:

<https://tutorialsdojo.com/vpc-peering/>

Question 62:

**Skipped**

A developer needs to collect and process large streams of data records in real-time. Which AWS service should be used for this task?

- **Amazon CloudWatch**
- **AWS Glue**
- **Amazon Kinesis Data Streams**

**(Correct)**

- **AWS CloudTrail**

#### Explanation

**Amazon Kinesis Data Streams (KDS)** is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources, such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. The data collected is available in milliseconds to enable real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing, and more.

Amazon Kinesis Consumer/Destinations	
Amazon Kinesis Data Stream Consumers	Amazon Kinesis Data Firehose Destinations
AWS Lambda	Amazon S3
Amazon Kinesis Data Analytics	Amazon Redshift
Amazon Elastic MapReduce (EMR)	Amazon ElasticSearch (ES)
Kinesis Data Firehose	Any HTTP endpoint owned by you or any of your third-party service providers, including Datadog, New Relic, and Splunk.
Applications hosted in Amazon EC2 that uses the Kinesis Client Library (KCL)	

Tutorials Dojo

Kinesis Data Streams helps you in collecting and processing large streams of data records in real-time. It can also create data-processing applications, known as Kinesis Data Streams applications. A typical Kinesis Data Streams application reads data from a data stream as data records.

Hence, the correct answer is: **Amazon Kinesis Data Streams.**



**AWS CloudTrail** is incorrect because this is a service that records important information about each action in your AWS environment, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. It is not a suitable service to capture large streams of data records in real-time.

**Amazon CloudWatch** is incorrect because this is a monitoring service for AWS cloud resources and the applications you run on AWS. It collects and tracks metrics, collects and monitors log files, and sets alarms. In the scenario, you need to process data in real-time, but CloudWatch cannot collect large streams of data records.

**AWS Glue** is incorrect because it is an ETL (Extract, Transform, and Load) service that enables you to prepare and load data for analytics. While it can handle large amounts of data, it is not designed specifically for real-time data processing.

#### References:

<https://aws.amazon.com/kinesis/data-streams/>

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

#### Check out this Amazon Kinesis Cheat Sheet:

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

Question 63:

#### Skipped

A company plans to use AWS to send email updates for their new products through SMTP. Which service should they use?

- Amazon SNS
- Amazon SWF
- Amazon SES

(Correct)

- Amazon SQS

#### Explanation

**Amazon Simple Email Service** is a highly scalable and cost-effective service for sending and receiving emails. Amazon SES eliminates the complexity and expense of building an in-house email solution or licensing, installing, and operating a third-party email solution. You can use the SMTP interface or one of the AWS SDKs to integrate Amazon SES directly into your existing applications. You can also embed the email sending capabilities of Amazon SES into the software you already use, such as ticketing systems and email clients.



SES is an excellent solution for anyone who needs a reliable, scalable, and inexpensive way to send and receive an email. AWS users include a diverse range of organizations, such as online retailers, application developers, and digital marketing organizations.

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

**Amazon SNS**, **Amazon SQS**, and **Amazon SWF** are all incorrect because the requirement is to send email updates through SMTP. Amazon SES is the appropriate service to use for this scenario.

#### References:

<https://aws.amazon.com/ses/>

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html>

Check out this **Amazon SES Cheat Sheet**:

<https://tutorialsdojo.com/amazon-ses/>

Question 64:

**Skipped**

What service will allow you to safely store and automatically rotate database secrets for services such as Amazon RDS and Amazon Redshift?

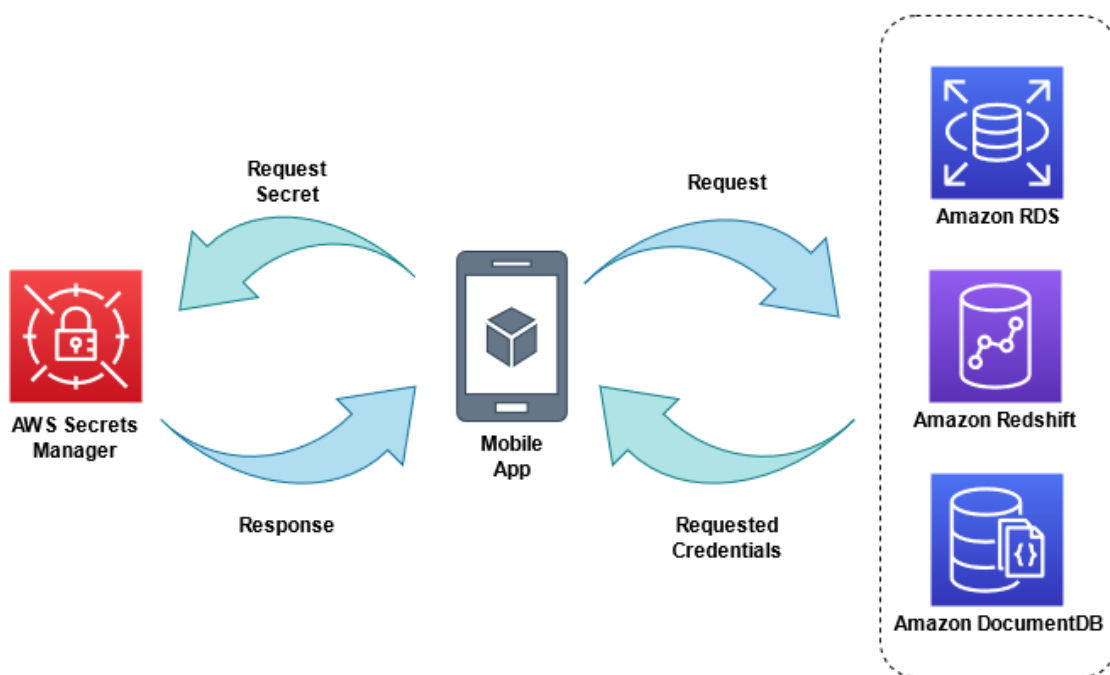
- **AWS Secrets Manager**

**(Correct)**

- AWS KMS
- AWS Systems Manager Parameter Store
- AWS Artifact

**Explanation**

**AWS Secrets Manager** helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.



Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. When you rotate a secret, you update the credentials in both the secret and the database. Applications that retrieve a secret from AWS Secrets Manager automatically get the new credentials after rotation.

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

**AWS Systems Manager Parameter Store** is incorrect. Although it can store database passwords and other credentials, it doesn't provide automatic rotation of secrets, unlike AWS Secrets Manager.

**AWS Artifact** is incorrect because the question isn't about a central repository for compliance-related information. AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. The compliance reports include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

**AWS KMS** is a key management service created for controlling access to encryption keys. It is not designed to store and manage credentials or provide automated secret rotation, but it does offer automatic key rotation. KMS is primarily used to encrypt data at rest and in transit.

#### References:

<https://aws.amazon.com/secrets-manager/>

<https://docs.aws.amazon.com/secretsmanager/>

#### AWS Security Services Overview - Secrets Manager, ACM, Macie:

<https://youtu.be/ogVamzF2Dzk>

#### Check out this AWS Secrets Manager Cheat Sheet:

<https://tutorialsdojo.com/aws-secrets-manager/>

Question 65:

#### Skipped

Which of the following Amazon RDS features should you use to achieve high availability with automatic failover?

- **Amazon RDS Multi-AZ Deployments**

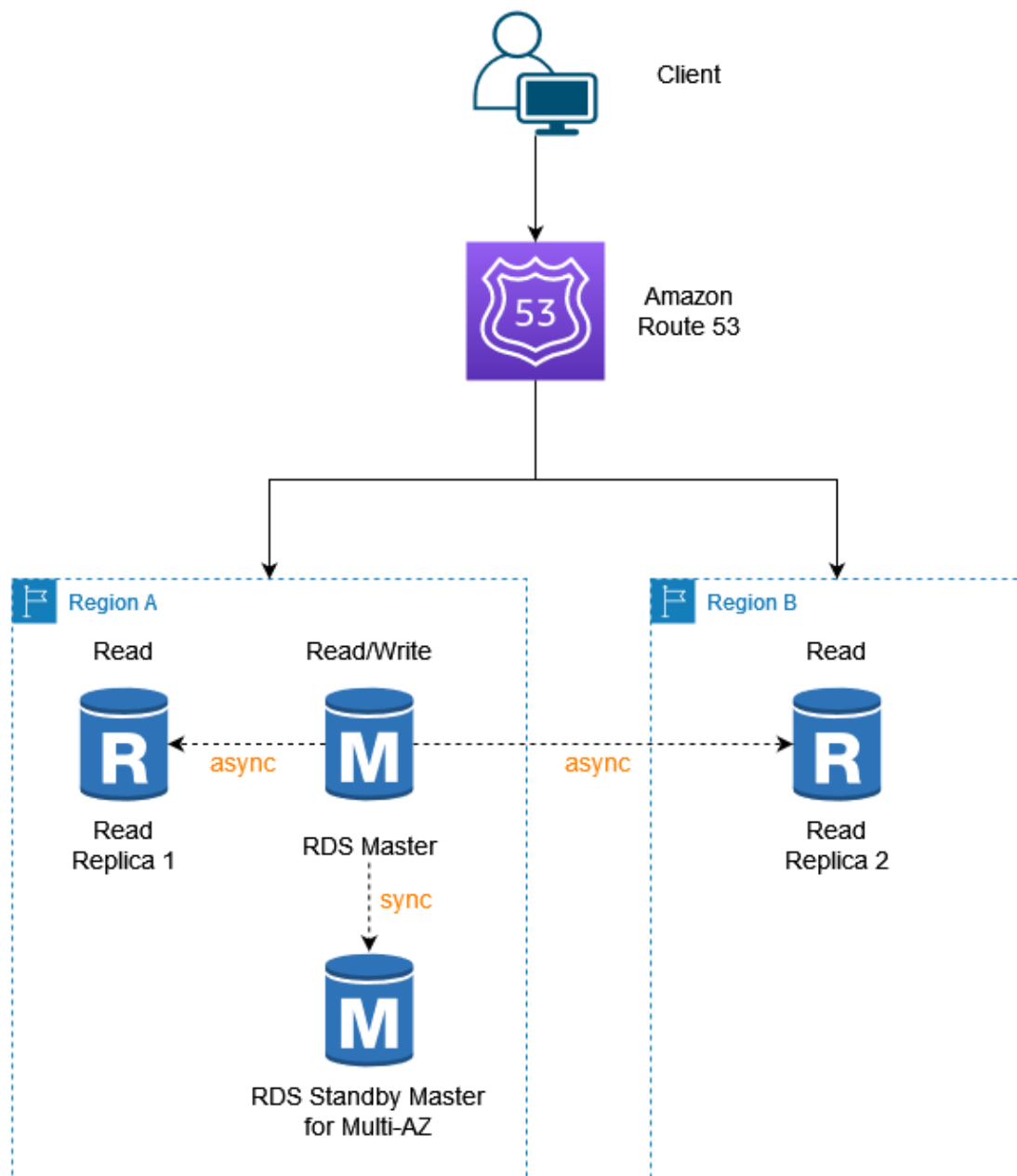
**(Correct)**

- **DB Snapshots**
- **Amazon RDS Read Replica**
- **Amazon RDS Performance Insights**

**Explanation**

**Amazon Relational Database Service** is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks, freeing you up to focus on your applications and business.

RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone.



**RDS Multi-AZ deployments** provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a

standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

Hence, the correct answer is: **Amazon RDS Multi-AZ Deployments**.

**Amazon RDS Read Replica** is incorrect because it just enables you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region. The updates made to the source database are then asynchronously copied to your Read Replicas. Moreover, it doesn't provide high availability and automatic failover.

**DB Snapshots** is incorrect because it only creates a snapshot of your DB instance. It helps store a backup of your data but you cannot achieve high availability with automatic failover.

**Amazon RDS Performance Insights** is incorrect because this feature does not provide enhanced availability for your database instances. RDS Performance Insights is simply a database performance tuning and monitoring feature that helps you quickly assess the load on your database, and determine when and where to take action.

## References:

<https://aws.amazon.com/rds/>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/>

## Amazon RDS Overview:

<https://youtu.be/aZmplI8K1UU?si=JBTDnzPsMARujkBS>

## Check out this Amazon RDS Cheat Sheet:

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