General Stuff

1. **Amazon Route 53:**
    - AWS's scalable Domain Name System (DNS) web service.
    - Provides various routing policies including failover routing.
    - Can perform health checks on your resources and **redirect traffic** based on the results.

Route 53 manages traffic at the DNS level, allowing for region-wide or global failover strategies.

You can launch a new RDS database cluster using the **AWS Management Console, AWS CLI, AWS SDK and AWS CloudFormation**.

Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. It utilizes a hosted Apache Hadoop framework running on the web-scale infrastructure of Amazon EC2 and Amazon S3. Amazon EMR lets you focus on crunching or analyzing your data without having to worry about time-consuming set-up, management, or tuning of Hadoop clusters or the compute capacity upon which they sit.

Amazon EMR (Elastic MapReduce)

- Key points: Managed big data platform for processing vast amounts of data
- Use cases: Log analysis, financial analysis, genomics
- Exam focus: Scalable solution for big data processing and analysis

Amazon MSK	Managed Kafka service	- Building data pipelines- Streaming analytics	- Fully compatible with Apache Kafka- Serverless option available

Amazon SQS	Message queuing	- Decoupling components- Handling high-volume messaging	- Asynchronous communication- Ensures reliable message delivery
AWS Step Functions	Workflow orchestration	- Coordinating multiple AWS services- Building complex processes	- Visual workflow creation- Manages state and error handling

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage when they need it.

Amazon WorkSpaces is a managed, secure Desktop-as-a-Service (DaaS) solution where you provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.

AWS Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to **automate operational tasks** across your AWS resources. You can perform actions such as automation, run specific commands to your EC2 instances, apply patch management, etc.

AWS Cloud9 is incorrect because this is simply a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. It includes a code editor, debugger, and terminal.

AWS Health provides ongoing visibility into your resource performance and the availability of your AWS services and accounts. You can use AWS Health ***events*** to learn how service and resource changes might affect your applications running on AWS. delivers **alerts** and notifications triggered by changes in the health of AWS resources so that you get near-instant event visibility and guidance to help accelerate troubleshooting.

There are actually only a handful of services that are considered **global** services**,** such as **IAM, STS, Route 53, CloudFront, and WAF.**

For Zonal services, the examples are **EC2 Instances and EBS Volumes which are tied to the Availability Zone**, where they were launched.

AWS Control Tower is for customers who want to create or manage their multi-account AWS environment with best practices. It offers prescriptive guidance to govern your AWS environment at scale. It gives you control over your environment without sacrificing the speed and agility AWS provides for builders.

Application Load Balancer - load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers.
Network Load Balancer - load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required.
Gateway Load Balancer - This provides both Layer 3 gateway and Layer 4 load balancing capabilities. It is a transparent bump-in-the-wire device that does not change any part of the packet.

There are two types of APN Partners:

1. **APN Consulting Partners**

2. **APN Technology Partners**

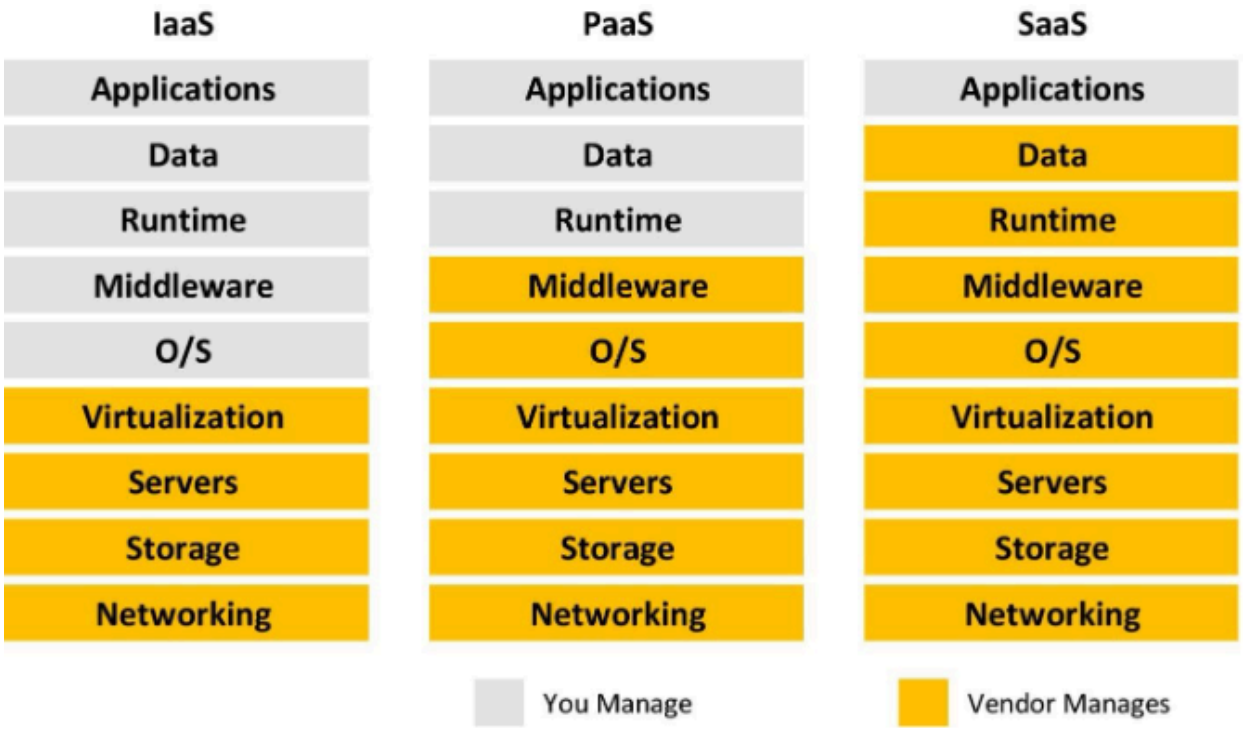
Key Distinction:

- Consulting: People-focused
- Technology: Product-focused

Roles:

- Consulting Partners: Offer expertise, guidance, and support services
- Technology Partners: Provide hardware, software, or other technology solutions

Exam Tip: If a question mentions "professional services" or "expert guidance," think Consulting Partner. If it talks about "software solutions" or "hardware integrations," think Technology Partner.



1. IaaS:
    - Definition: Provides virtualized computing resources over the internet.
    - AWS Examples:
        - Amazon EC2 (virtual servers)
        - Amazon VPC (networking)
        - Amazon EBS (block storage)

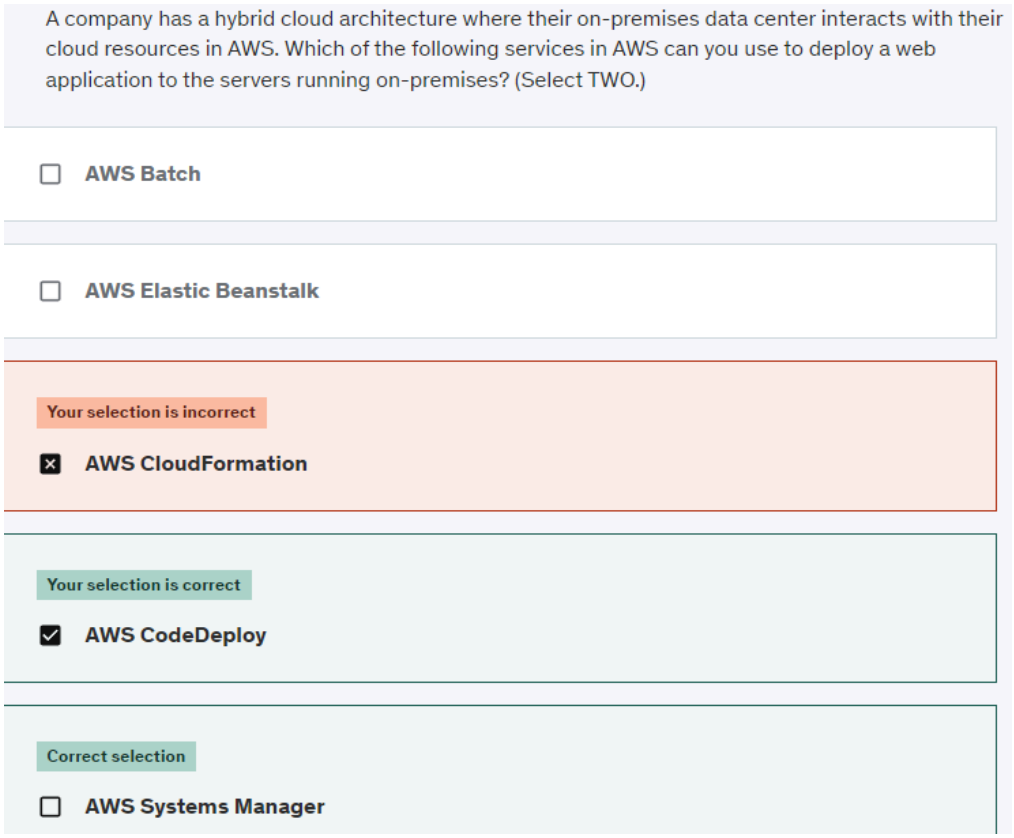
2. PaaS:
    - Definition: Provides a platform allowing customers to develop, run, and manage applications without the complexity of maintaining the infrastructure.
    - AWS Examples:
        - AWS Elastic Beanstalk (for web applications deployment)
        - AWS Lambda (serverless computing)
        - Amazon RDS (managed database service)

3. SaaS:
    - Definition: Delivers software applications over the internet, on a subscription basis.
    - AWS Examples:
        - Amazon Connect (contact center)
        - Amazon WorkSpaces (virtual desktops)
        - Amazon Chime (communication service)

End User Computing

Service	Primary Function	Use Case	Key Advantage
AppStream 2.0	Application streaming	Access specific applications	No application redesign needed
WorkSpaces	Full desktop experience	Remote work, consistent desktops	Managed VDI solution
WorkSpaces Web	Web-based workspace	Secure access to internal sites/SaaS	Lightweight, browser-based access

Code Deployment:



AWS Systems Manager – AWS Systems Manager allows you to manage servers running on AWS and in your on-premises data center through a single interface. It provides a centralized location for storing configuration variables, allowing configuration values to be updated in a single place and retrieved by all application instances. It also has the ability to run a particular command or script on multiple servers.

Both **AWS CloudFormation and AWS Elastic Beanstalk** are incorrect because these services can only deploy applications to your AWS resources and not to the servers located in your on-premises data center.

- CodeDeploy can deploy to both EC2 and on-premises servers. Systems Manager can manage both AWS and on-premises resources.

AWS CloudFormation (Incorrect): enables users to automate the provisioning and management of AWS infrastructure through Infrastructure as Code (IaC). This allows developers to define and **manage their cloud resources** using templates written in JSON or YAML format.

AWS Elastic Beanstalk is a Platform as a Service (PaaS) offering that simplifies application deployment and management in the AWS cloud, but it doesn't support deploying to on-premises servers.

AWS Elastic Beanstalk:

- Platform as a Service (PaaS) offering
- Automatically handles deployment details like capacity provisioning, load balancing, auto-scaling, and application health monitoring
- Ideal for developers who want to deploy applications quickly without managing infrastructure

AWS CloudFormation:

- Infrastructure as Code (IaC) service
- Allows you to define and provision AWS infrastructure deployments predictably and repeatedly
- Requires more detailed knowledge of AWS resources and their configurations
- While powerful, it's not as quick or simple for application deployment as Elastic Beanstalk

AWS CodeDeploy:

- **Automates code deployments to any instance, including EC2 instances and on-premises servers**
- Helps minimize downtime during application updates

Amazon ECS (Elastic Container Service):

- Managed container orchestration service
- Used for deploying, managing, and scaling containerized applications

AWS Lambda:

- Serverless compute service
- Runs your code in response to events without provisioning or managing servers
- Ideal for event-driven, serverless application deployments

AWS AppRunner:

- Fully managed service for deploying containerized web applications and APIs
- Automatically builds and deploys the web application

AWS Amplify:

- Set of tools and services for building full-stack applications
- Simplifies the process of developing and deploying web and mobile applications

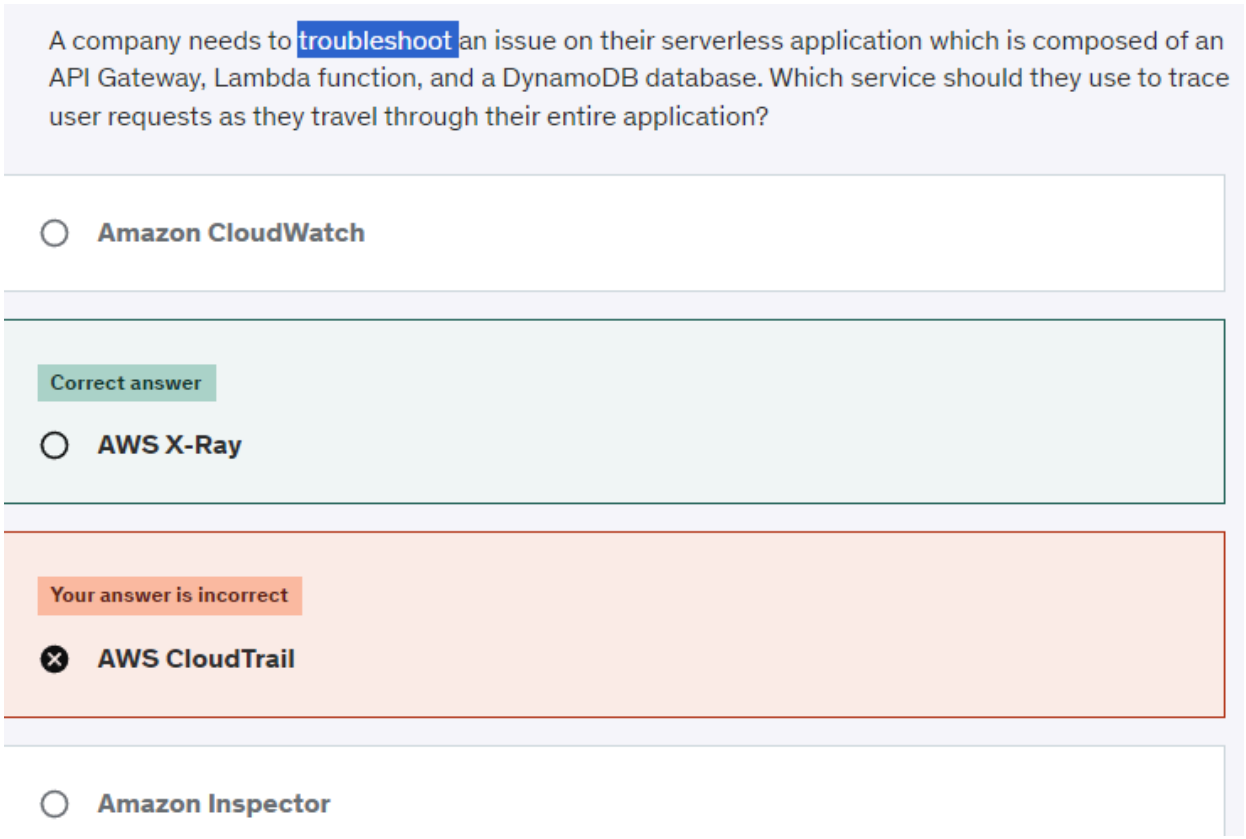
Know which service to choose based on the scenario:

- For simple, quick deployments: Elastic Beanstalk
- For infrastructure management: CloudFormation
- For containerized apps: ECS or AppRunner
- For serverless functions: Lambda
- For web and mobile apps: Amplify

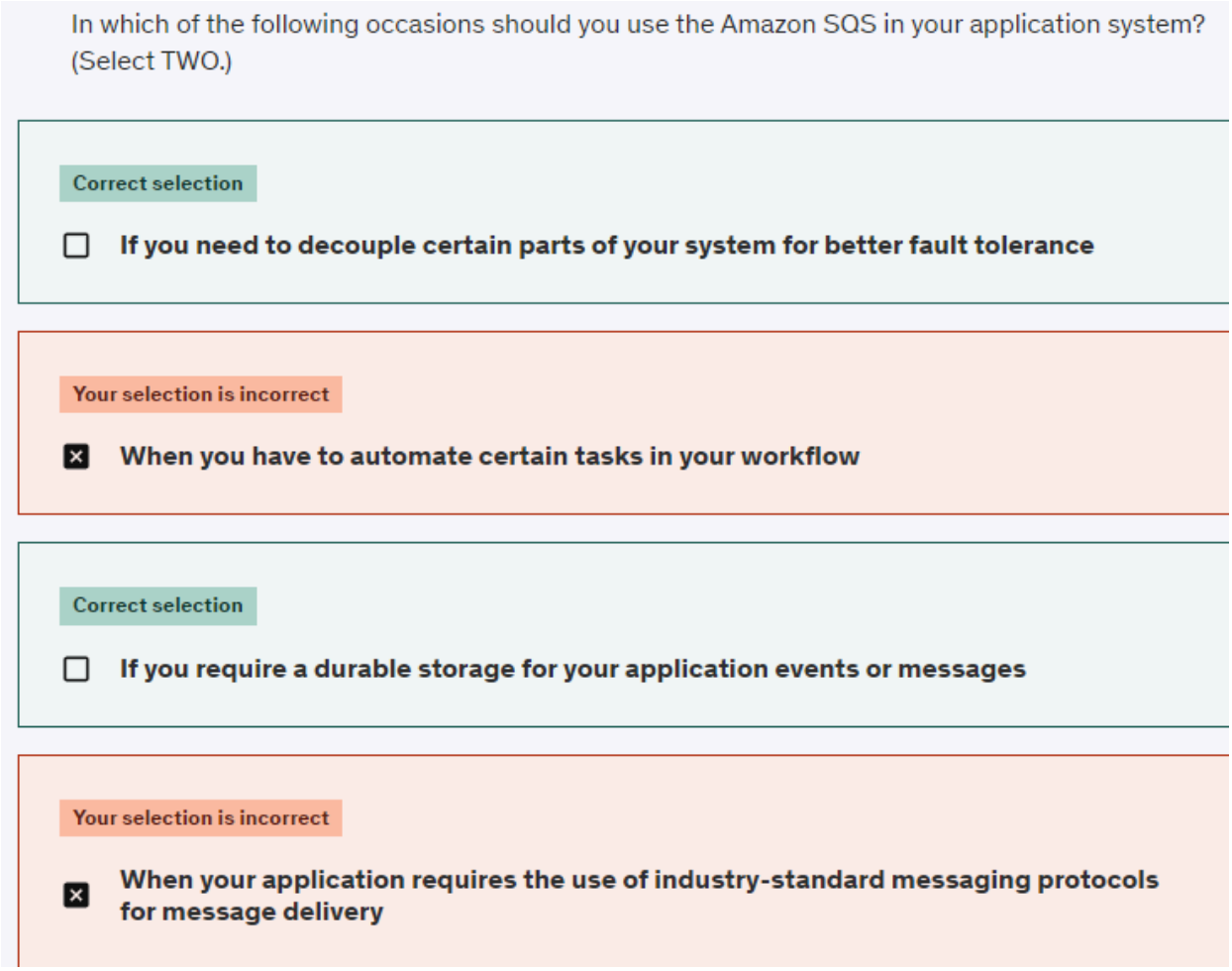
- CodeCommit (source control) → CodeBuild (build and test) → CodeDeploy (deployment) → CodePipeline (orchestrates/automate the entire process)
- CodeStar is an overarching service that sets up a complete development toolchain
- Cloud9 is IDE for writing code, while CloudShell is for running AWS CLI commands
- AppConfig is specifically for managing application configurations
- X-Ray is for application performance analysis and debugging

Serverless

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



AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.



Use Amazon SQS to transmit any volume of data, at any level of throughput, without losing messages or requiring other services to be available. SQS lets you decouple application components so that they run and fail independently, increasing the overall fault tolerance of the system. Multiple copies of every message are stored redundantly across multiple availability zones so that they are available whenever needed.

Cost Management

AWS Cost Management Tools:

1. AWS Cost Explorer
    - Key function: **Visualize** and analyze AWS costs and usage over time
    - Unique feature: **Forecasts** future costs based on historical data - past & Future/Recommendation

    - cost analysis, visualization, past & Future/Recommendation cost prediction/compare
2. AWS Cost and Usage Report
    - Key function: Provides the most detailed AWS cost and usage data
    - Unique feature: Offers granular data at the resource level
    - comprehensive, detailed cost breakdowns, granular, raw data
3. AWS Budgets
    - Key function: Set custom cost and usage budgets with alerts
    - Unique feature: Proactive cost control with customizable thresholds
    - alerts or notifications about exceeding costs/ limits
4. AWS Trusted Advisor
    - Key function: Provides real-time guidance to help optimize AWS infrastructure
    - Unique feature: Offers recommendations across five categories, including cost optimization
    - Exam tip: Choose for questions about overall AWS best practices or multi-category optimization
5. AWS Pricing Calculator
    - Key function: Estimates costs for AWS services before deployment
    - Unique feature: Allows creation of estimates for complex, multi-service architectures
    - Exam tip: Select for questions about estimating costs for new or planned AWS deployments

Remember:

- Cost Explorer is for analysis and forecasting
- Cost and Usage Report is for detailed, historical data
- Budgets is for setting limits and getting alerts
- Trusted Advisor is for overall optimization recommendations
- Pricing Calculator is for estimating future deployments

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

With the **AWS Cost and Usage Report**, you can do the following:

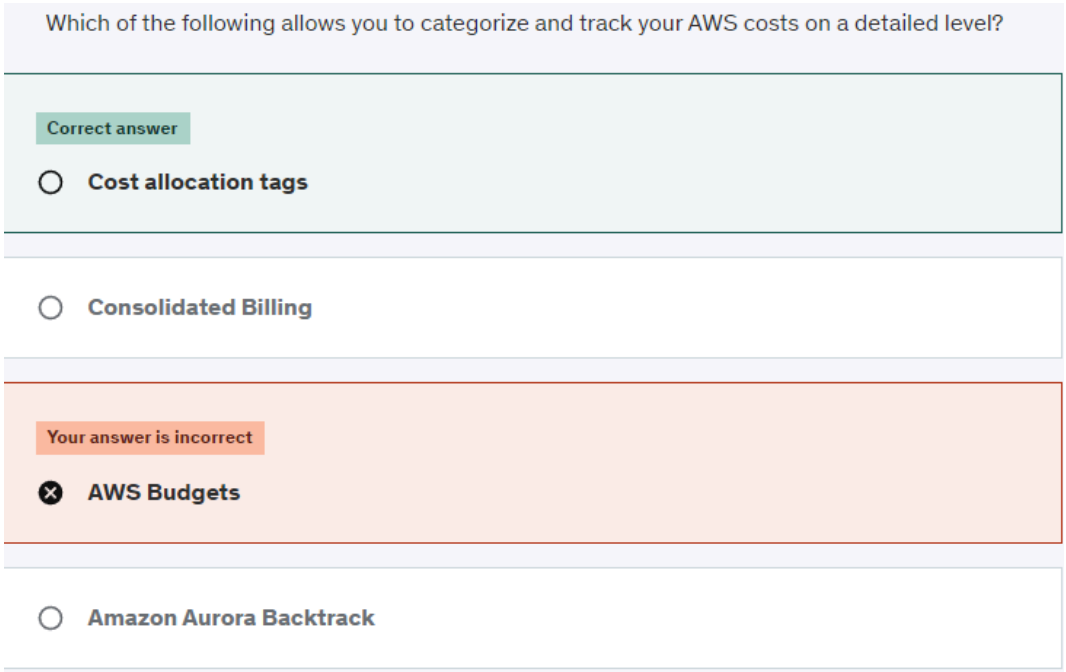
Access comprehensive AWS cost and usage information

Track your Amazon EC2 Reserved Instance (RI) usage

- Each line item of usage that receives an RI discount contains information about where the discount was allocated. This makes it easier to trace which instances are benefitting from specific reservations.

Leverage strategic data integrations

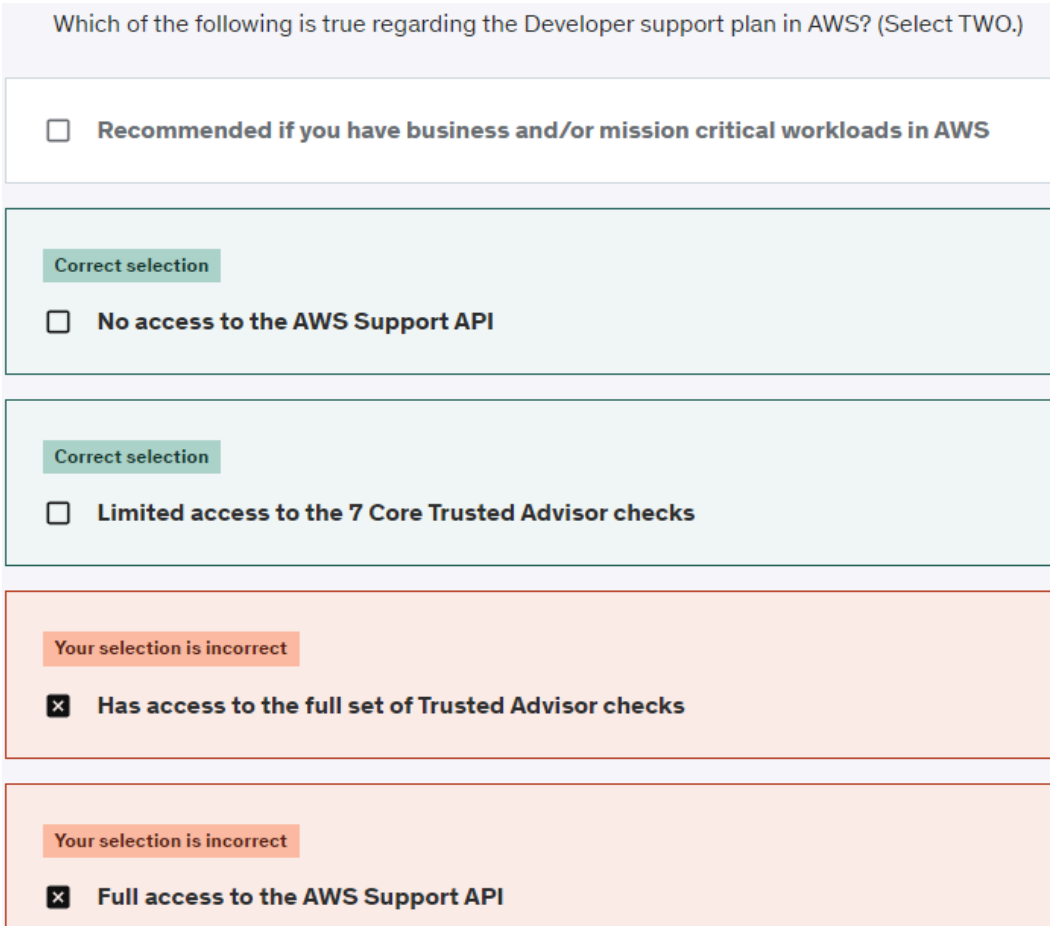
- Using the Amazon Athena **data integration feature**, you can quickly query your cost and usage information using standard SQL queries. You can also upload your data directly into Amazon Redshift or Amazon QuickSight.



Support Plans

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

Severity Level	Developer	Business	Enterprise On-Ramp	Enterprise
General (G)	< 24h	< 24h	< 24h	< 24h
System Impaired (I)	< 12h	< 12h	< 12h	< 12h
Production System Down (P)	N/A	< 4h < 1h	< 4h < 1h	< 4h < 1h
Business-Critical (B)	N/A	N/A	< 30m	< 15m



Business or Enterprise support plan have access to these features:

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

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

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

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

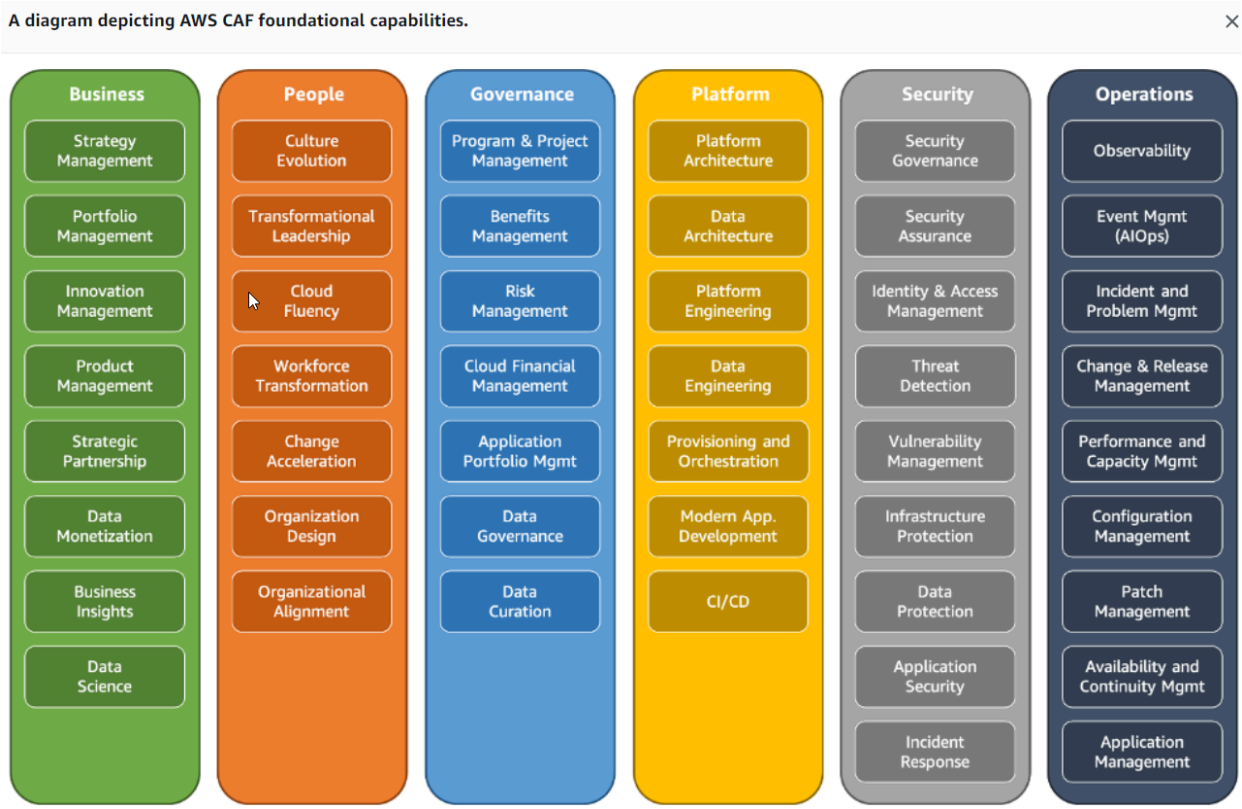
CAF

1. AWS CAF Perspectives:
    1. Business: investments in the cloud propel your digital transformation goals and business results.
    2. People: link between technology and business, speeding up the cloud journey to help organizations quickly evolve into a culture of continuous growth and learning, where change is the norm. It focuses on culture, organizational structure, leadership, and workforce.
    3. Governance: coordinate cloud initiatives while maximizing organizational benefits and minimizing risks associated with transformation.
    4. Platform: construct an enterprise-grade, scalable, hybrid cloud platform, modernize existing workloads, and implement new cloud-native solutions.
    5. Security: This perspective helps achieve the confidentiality, integrity, and availability of data and cloud workloads.
    6. Operations: This perspective helps ensure that cloud services are delivered at a level that meets the business needs.
2. Key Benefits of AWS CAF: a) Reduced Business Risk:
    1. Provides structured approach to cloud adoption, minimizing errors
    2. Ensures compliance and security measures are in place
    3. Exam tip: CAF helps identify and mitigate potential risks early in the cloud adoption process
3. b) Improved Environmental, Social, and Governance (ESG) Performance:
    1. Enables more efficient resource utilization, reducing environmental impact
    2. Promotes better governance practices
    3. Exam tip: CAF's governance perspective directly contributes to improved ESG performance

4. c) Increased Revenue:
    1. Accelerates time-to-market for new products and services
    2. Enables innovation through access to advanced cloud technologies
    3. Exam tip: CAF's business perspective focuses on aligning cloud initiatives with revenue growth
5. d) Increased Operational Efficiency:
    1. Streamlines processes and reduces manual tasks
    2. Improves resource allocation and utilization
    3. Exam tip: CAF's operations perspective directly addresses improving operational efficiency

1. **Envision**: - Focus: Define and prioritize transformation opportunities - Key activities: Identify business objectives, create a high-level vision

2. **Align**:
    - Focus: Identify gaps in current state vs. desired state
    - Key activities: Assess readiness, identify capability gaps, create roadmaps
    - This is where you use CAF perspectives to identify gaps and dependencies
3. Launch:
    - Focus: Implement and deliver pilot projects or initial workloads
    - Key activities: Design, implement, and validate initial cloud workloads
4. Scale:
    - Focus: Expand adoption across the organization
    - Key activities: Drive business value at scale, optimize and expand cloud adoption



Which of the following capabilities of the AWS Cloud Adoption Framework (AWS CAF) are under the Governance perspective? (Select TWO)

Your selection is correct

- [x] Data Governance

- [ ] Data Architecture

Correct selection

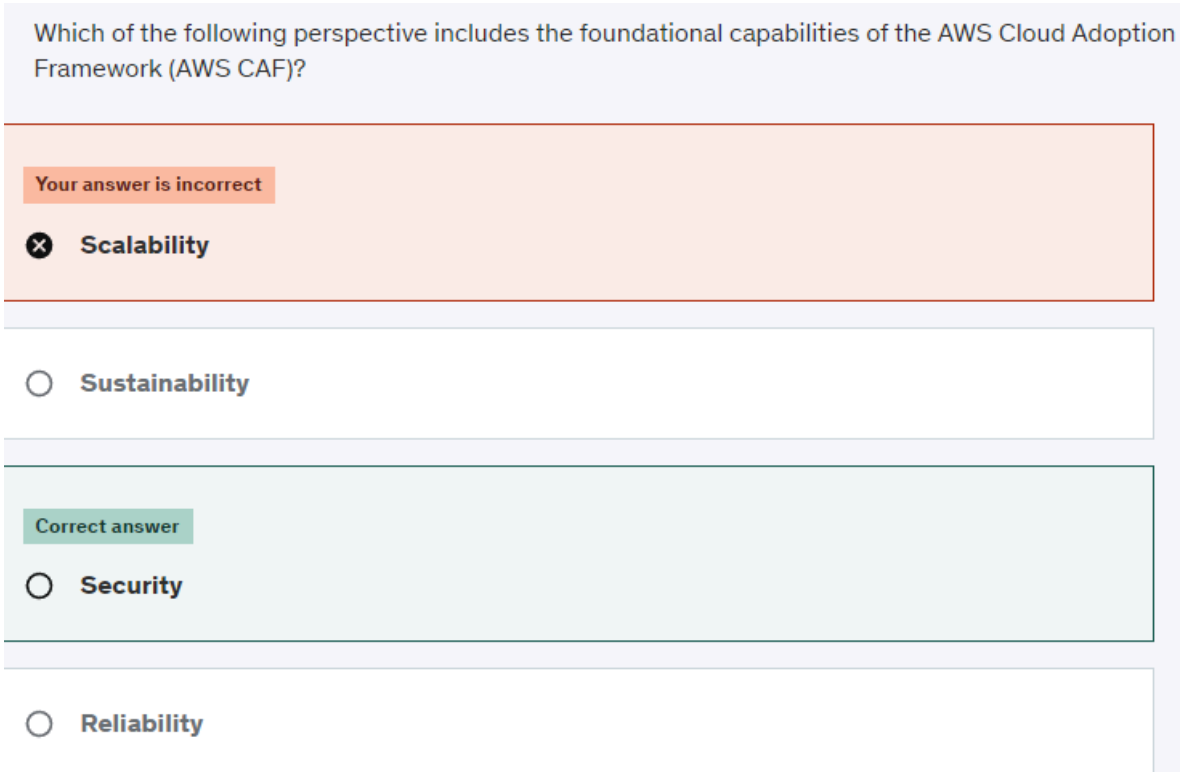
- [ ] Data Curation

Your selection is incorrect

- [x] Data Protection

benefits of using Cloud Computing:

1. **Agility**
2. **Deploy globally in minutes**
3. **Elasticity**
4. **Cost savings**



WAF

The AWS Well-Architected Framework upholds six (6) general **design principles**. The following are:

- Stop guessing your capacity needs.

- Test systems at production scale.

- Automate to make architectural experimentation easier.

- Allow for evolutionary architectures.

- Drive architectures using data.

- Improve through game days.

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

1. Design for failure

2. Decouple your components

3. Implement elasticity

4. Think parallel

AWS Well-Architected Framework

There are five design principles for **operational excellence** in the cloud:

- Perform operations as code: In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code.

- Make frequent, small, reversible changes: Design workloads to permit components to be updated regularly.

- Refine operations procedures frequently: As you use operations procedures, look for opportunities to improve them.

- Anticipate failure: Perform “pre-mortem” exercises to identify potential sources of loss so that they can be removed or mitigated.

- Learn from all operational failures: Drive improvement through lessons learned from all operational events and failures. Share what is learned across teams and through the entire organization.

Review

Pillar	Focus	Key Concepts	Remember As
Operational Excellence	Running and monitoring systems	- Automation- Continuous improvement- Observability	"Smooth Operations"
Security	Protecting data and systems	- Identity management- Encryption- Threat detection	"Protect Everything"
Reliability	System recovery and availability	- Fault tolerance- Disaster recovery- Scalability	"Always Works"
Performance Efficiency	Using resources efficiently	- **Right sizing**- Monitoring- Optimizing	"Fast and Lean"
Cost Optimization	Avoiding unnecessary costs	- **Resource allocation**- Matching supply and demand- Expenditure awareness	"Smart Spending"
Sustainability	Minimizing environmental impact	- Energy efficiency- Resource optimization- Sustainable practices	"Green Cloud"

Benefits of the AWS Cloud

6 advantages of cloud computing

1. Trade upfront expense for variable expense:

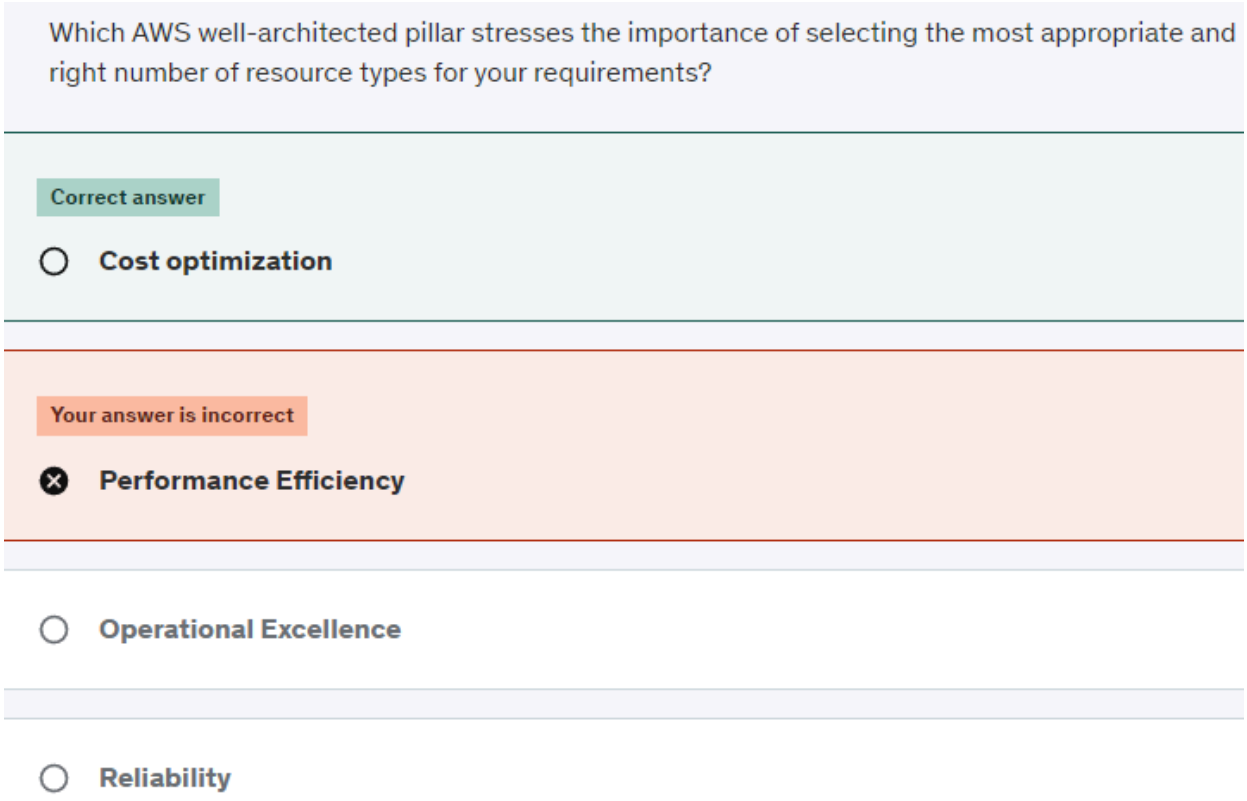
2. Benefit from massive economies of scale:
   Economies of scale translate into lower pay-as-you-go prices.

3. Stop guessing capacity

4. Increase speed and agility

5. Stop spending money running and maintaining data centers:

6. Go global in minutes: **with low latency.**

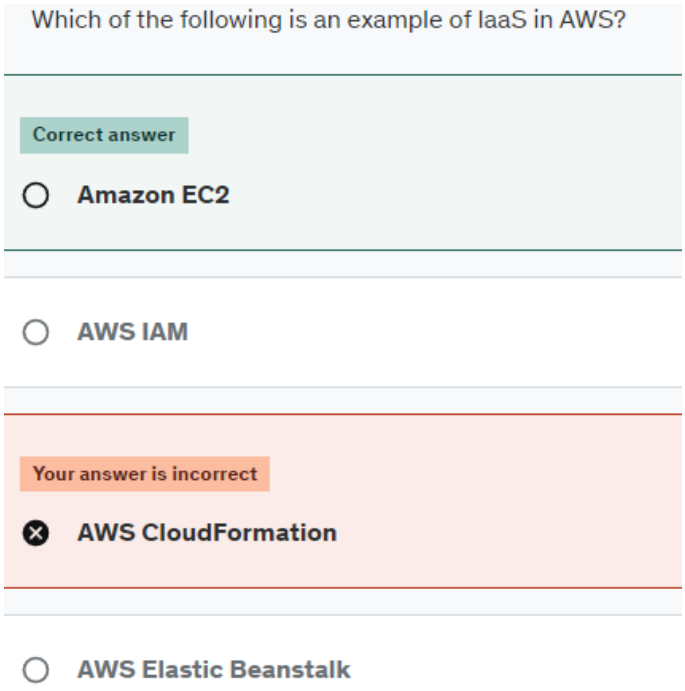


6 R's of Cloud Migration

1. Rehosting ("Lift and Shift"):
   - Moving applications without changes
   - Quick and simple, but may not fully leverage cloud capabilities
2. Replatforming ("Lift, Tinker, and Shift"):
   - Making a few cloud optimizations without changing the core architecture

    - Moderate effort, some cloud benefits
3. Repurchasing ("Drop and Shop"):
    - Moving from perpetual licenses to a software-as-a-service model
    - Example: Migrating from on-premises CRM to Salesforce.com
4. Refactoring / Re-architecting:
    - Reimagining how the application is architected using cloud-native features
    - Most effort, but maximum cloud benefits
5. Retire:
    - Identifying IT assets that are no longer useful and can be turned off
    - Results in savings
6. Retain:
    - Keeping certain applications on-premises
    - For applications that are not ready to migrate or require major refactoring

EC2



Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage.

Exam tip: When you see questions about long-term cost optimization across multiple compute services, Compute Savings Plans are often the best choice due to their flexibility and applicability to both EC2 and Lambda.

EC2 pricing options:

1. On-Demand Instances
    - Pay per second/hour with no commitment
    - Best for: Short-term, unpredictable workloads
    - Key point: Most flexible, no upfront cost
2. Reserved Instances (RI)
    - Up to 72% discount for 1 or 3-year commitment
    - Types: a) Standard RI: Deepest discount, limited flexibility b) Convertible RI: Some flexibility, lesser discount
    - Best for: Steady-state, predictable workloads
    - Key point: Significant savings for long-term use
3. Savings Plans
    - **Commitment** to spend a certain $ amount per hour
    - Similar discounts to RIs, more flexibility
    - Best for: Varied workloads across EC2, Fargate, Lambda
    - Key point: Flexible commitment to AWS compute usage
4. Spot Instances
    - Up to 90% discount, can be terminated by AWS
    - Best for: Fault-tolerant, flexible-time workloads
    - Key point: Cheapest option, but least reliable
5. Dedicated Hosts
    - Physical EC2 server dedicated for your use
    - Best for: Compliance requirements, existing server-bound licenses
    - Key point: Most expensive, used for specific regulatory needs

EC2 Instance Types:

1. General Purpose
    - Balanced compute, memory, and networking
    - Use case: Web servers, small databases
    - Key word: "Balance"
2. Compute Optimized
    - High-performance processors
    - Use cases: High-performance web servers, batch processing, gaming servers
    - Key words: "Compute-intensive", "High-performance"
3. Memory Optimized
    - Fast performance for large datasets in memory
    - Use cases: High-performance databases, real-time processing of unstructured data
    - Key words: "Large datasets", "In-memory processing"
4. Accelerated Computing
    - Hardware accelerators or co-processors
    - Use cases: Graphics applications, game streaming, data pattern matching
    - Key words: "GPU", "FPGA", "Graphics processing"
5. Storage Optimized
    - High, sequential read/write access to large datasets on local storage
    - Use cases: Distributed file systems, data warehousing, high-frequency OLTP
    - Key words: "High IOPS", "Sequential I/O", "Large datasets"

Exam Tips:

- Match instance type to workload characteristics
- Remember key use cases for each type
- "IOPS" is associated with Storage Optimized
- "In-memory" processing suggests Memory Optimized
- Batch processing often indicates Compute Optimized
- Graphics-intensive workloads point to Accelerated Computing

Instance Metadata:

- Definition: Data about your EC2 instance that you can use to configure or manage the running instance.
- Access: http://169.254.169.254/latest/meta-data/
- Contains: Instance ID, IP addresses, hostname, security groups, etc.
- Key Point: Accessible from within the EC2 instance itself.

Amazon Machine Image (AMI):

- Definition: A template for the root volume of an instance.
- Contains: OS, application server, applications.
- Key Point: Used to launch instances, but doesn't contain instance-specific data.

Resource Tags:

- Definition: Labels that you assign to AWS resources.
- Use: For categorization, billing, and management.
- Key Point: Not for storing instance-specific technical data.

Instance Profile:

- Definition: Container for an IAM role that you can use to pass role information to an EC2 instance.
- Use: To give EC2 instances permissions to access other AWS services.
- Key Point: Part of the instance metadata, but specifically for IAM roles.

Exam Tips:

1. If a question asks about retrieving instance-specific information from within the instance, think "Instance Metadata".
2. For launch-time configurations or scripts, remember "User Data".
3. AMIs are for launching instances, not for retrieving running instance information.
4. Tags are for organization and management, not for storing technical instance data.
5. Instance profiles are specifically for IAM roles and permissions, part of the instance metadata.

What feature will allow you to label and sort your EC2 instances according to their deployment stage (development, staging, production)? Instance Tags

comparison:

1. Instance Tags:
    - Key-value pairs attached to EC2 instances
    - Used for: Organizing, filtering, and managing resources
    - Example use: Tracking department ownership of instances

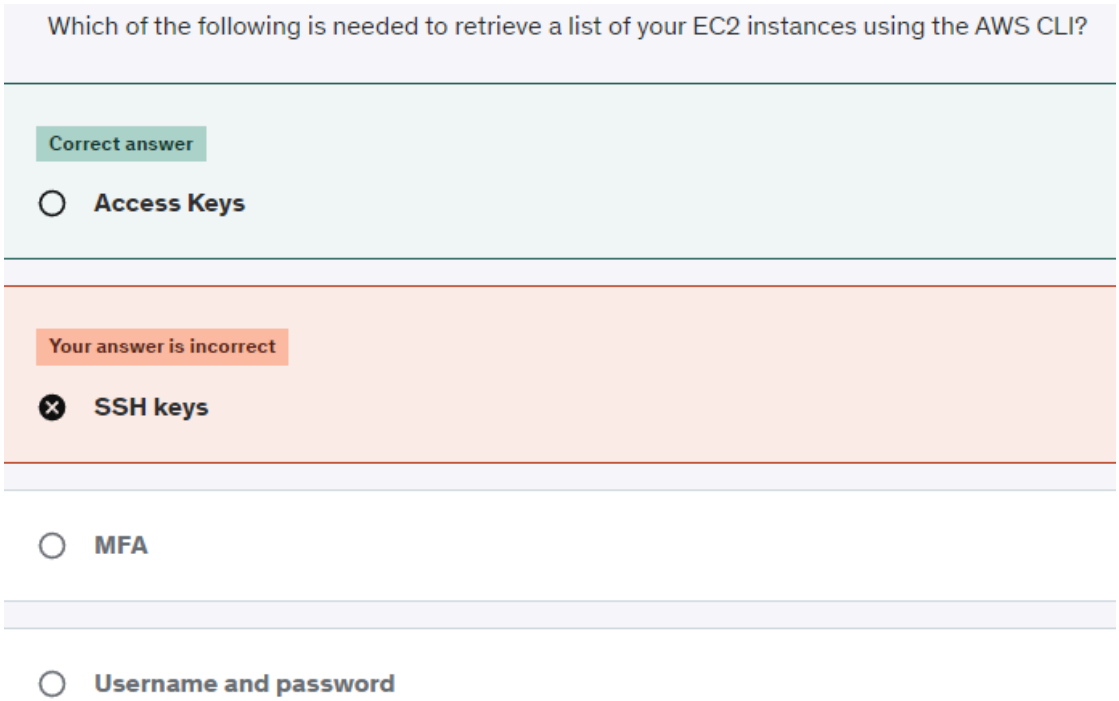
    - How to access: AWS Management Console, AWS CLI, or API calls
    - Key point: Can be modified after instance launch
2. Instance Metadata:
    - Data about the EC2 instance itself
    - Used for: Retrieving information about the instance
    - Examples: Instance ID, public IP, AMI ID
    - How to access: From within the instance via HTTP requests to a special IP (169.254.169.254)
    - Key point: Read-only and can't be modified
3. User Data:
    - Scripts or data provided at instance launch
    - Used for: Automating configuration tasks when an instance starts
    - Example use: Installing software or downloading files at launch
    - How to access: Can be viewed via instance metadata
    - Key point: Only runs at instance launch or restart
4. Instance Store (additional context):
    - Temporary block-level storage for EC2 instances
    - Used for: Temporary data that doesn't need to persist
    - Key point: Data is lost when the instance stops or terminates

Comparison:

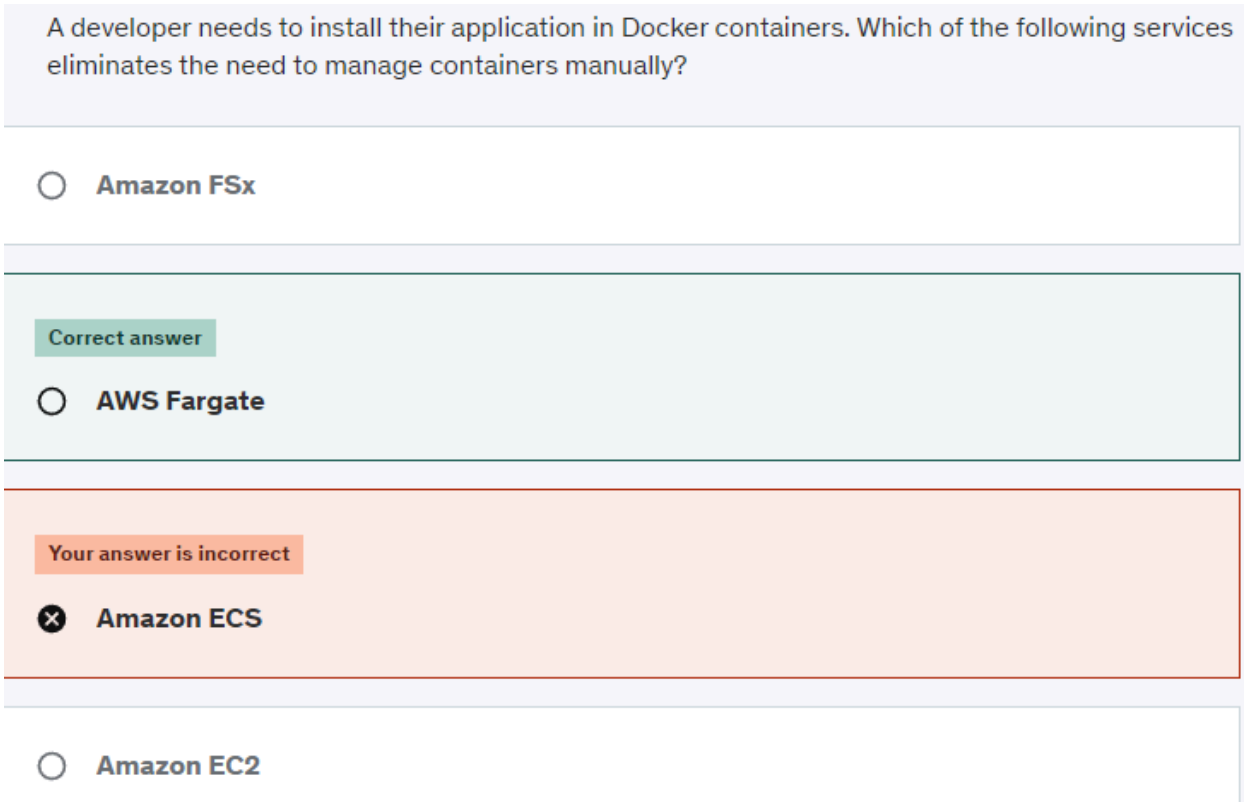
- Tags are for external management and organization
- Metadata is for retrieving instance information
- User Data is for instance configuration at launch
- Instance Store is for temporary storage

Exam tip: Be prepared to identify scenarios where each of these would be most appropriate. For example:

- If a question asks about labeling instances for cost allocation, think tags
- If it's about a script that needs to run when an instance starts, think user data
- If it's about an application needing to know its own instance ID, think metadata



Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). If you don't have access keys, you can create them from the AWS Management Console.
SSH keys is incorrect because this is primarily used to **authenticate your SSH connection** to an EC2 instance. For this question, these keys are not needed by the AWS CLI.



AWS Fargate is a serverless compute engine for containers.

Amazon ECS is incorrect because by using this service, you still need to manage your own EC2 instances where your containers are hosted.

Domain 2: Security and Compliance

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.
AWS CloudHSM provides hardware security modules in the AWS Cloud that you can manage and control.

Shared Responsibilities:

- Patch management

- Configuration management
- Awareness & Training

Capturing and Locating Security Logs:

a) AWS CloudTrail: Records API calls for your account and delivers log files to you.

- Location: Logs are stored in an S3 bucket you specify.

b) Amazon CloudWatch Logs: You can use it to monitor, store, and access log files from EC2 instances, CloudTrail, and other sources.

- Location: Logs are stored within CloudWatch Logs and can be exported to S3.

c) VPC Flow Logs: Captures information about IP traffic going to and from network interfaces in your VPC.

- Location: Can be published to CloudWatch Logs or S3.

d) AWS Config: Provides a detailed record of the configuration changes to your AWS resources.

- Location: Configuration history and snapshot files are stored in S3.

- CloudWatch can collect and monitor metrics from **on-premises** servers using the CloudWatch agent.
- Config can assess, audit, and evaluate configurations of on-premises servers.
- CloudTrail can be integrated with on-premises logging solutions.

AWS Artifact and Compliance Information:
AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements.

1. **Threat Detection and Monitoring:**

   • Amazon GuardDuty: Intelligent threat detection for AWS accounts and workloads

- Key point: Analyzes multiple data sources
- Trap: Don't confuse with Inspector (for vulnerability assessment)

• **Amazon Detective**: Analyze and **visualize** security data to investigate potential issues

- Key point: For **root cause analysis**
- Trap: Not a real-time threat detection service

• **Amazon Inspector**: **Automated** security assessment service

- Key point: For finding **vulnerabilities** and deviations from **best practices**
- Trap: Don't confuse with GuardDuty (for active threat detection)

• **Amazon Macie**: Discover and protect sensitive data

- Key point: Focuses on PII and sensitive data in S3
- Trap: Not a general-purpose security service

Permitted Services to conduct security assessments

- Amazon EC2 instances, WAF, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments
- Amazon Elastic Container Service
- AWS Fargate
- Amazon Elasticsearch

- S3 hosted applications (targeting S3 buckets is strictly prohibited)

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

- DNS zone walking via Amazon Route 53 Hosted Zones

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

- Port flooding

- Protocol flooding

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

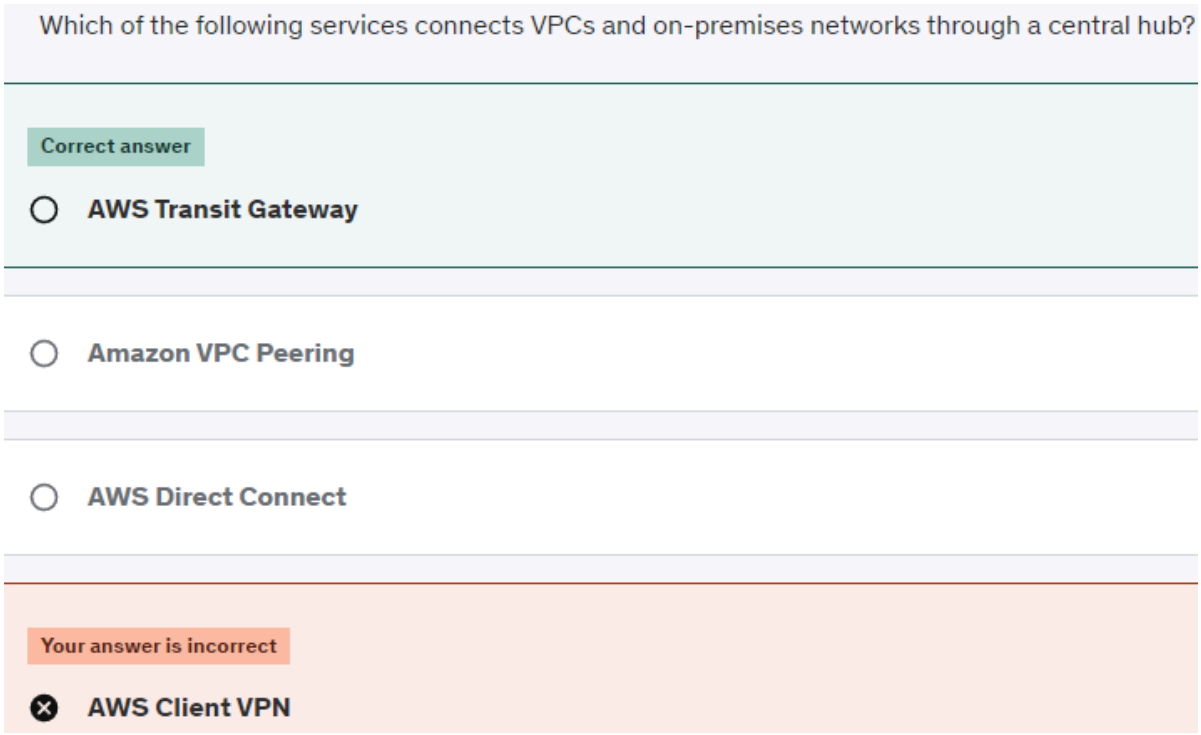
AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.
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 Inspector vs AWS Trusted Advisor:

1. Scope of analysis:
    - AWS Inspector is focused specifically on security vulnerabilities and compliance for EC2 instances and container images.
    - AWS Trusted Advisor has a much broader scope, covering best practices across your entire AWS environment.
2. Types of recommendations:
    - AWS Inspector provides detailed security findings related to vulnerabilities and compliance issues.
    - AWS Trusted Advisor offers recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, and Service Limits.

AWS and on-premises integration

- CodeDeploy can deploy to both EC2 and on-premises servers.
- Systems Manager can manage both AWS and on-premises resources.
- CloudWatch can collect and monitor metrics from on-premises servers using the CloudWatch agent.
- Config can assess, audit, and evaluate configurations of on-premises servers.
- CloudTrail can be integrated with on-premises logging solutions.
- Storage Gateway provides on-premises access to virtually unlimited cloud storage.
- **Outposts** brings AWS infrastructure on-premises for truly consistent hybrid operations.



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.

IAM

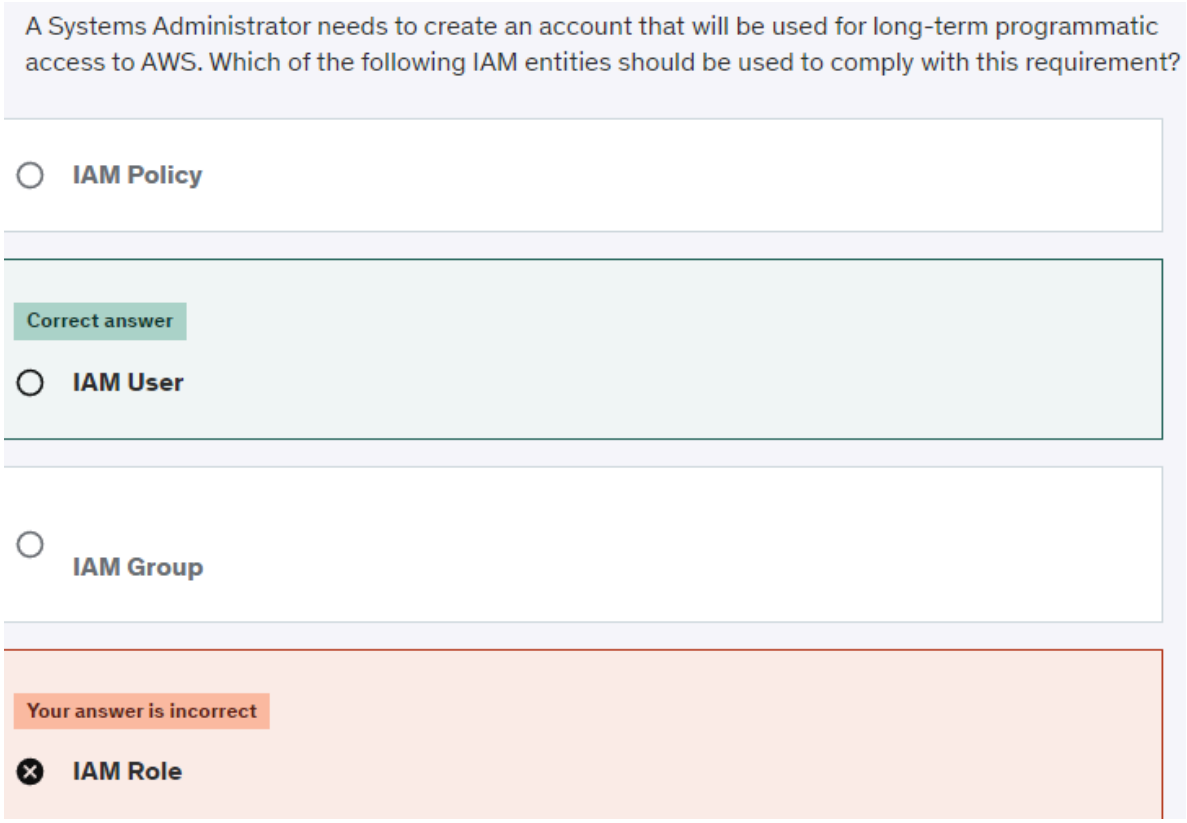
IAM is global, not region-specific.

Use IAM policies to grant specific permissions

Access Keys: Long-term credentials for programmatic access to AWS resources

IAM Groups, Users, and Policies

- Groups: Collection of IAM users
- Users: Individuals or services needing AWS access
- Managed Policies: Pre-defined, AWS-maintained policies
- Custom Policies: User-defined policies for specific permissions
- Exam tip: Using groups to assign permissions is a best practice



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.

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.

Which of the following IAM identities is associated with the access keys that are used in managing your cloud resources via the AWS Command Line Interface (AWS CLI)?

- IAM Policy

Correct answer

- IAM User

- IAM Group

Your answer is incorrect

- IAM Role

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Which among the services below can you use to test and troubleshoot IAM and resource-based policies?

Your answer is incorrect

- AWS Config

- Systems Manager

- Amazon Inspector

Correct answer

- IAM Policy Simulator

What is the most secure way to provide applications temporary access to your AWS resources?

Your answer is incorrect

✗ **Create an IAM group that has access to the resources, and add the application there**

Correct answer

○ **Create an IAM role and have the application assume the role**

○ **Create an IAM user with access keys and assign it to the application**

○ **Create an IAM policy that allows the application to access the resources, and attach the policy to the application**

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

○ **Amazon Cognito User Pool**

Correct answer

○ **Amazon Cognito Identity Pool**

Your answer is incorrect

✗ **AWS IAM Identity Center**

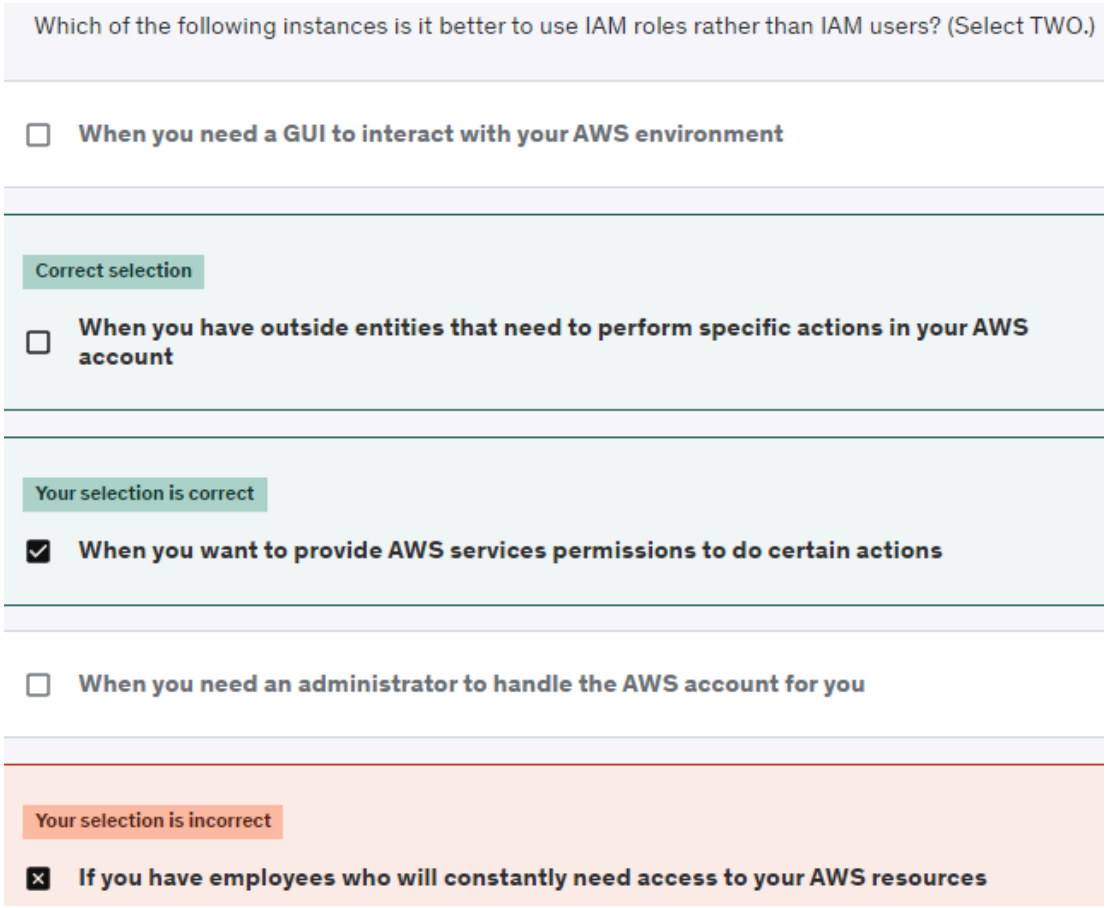
○ **AWS AppSync**

steps:

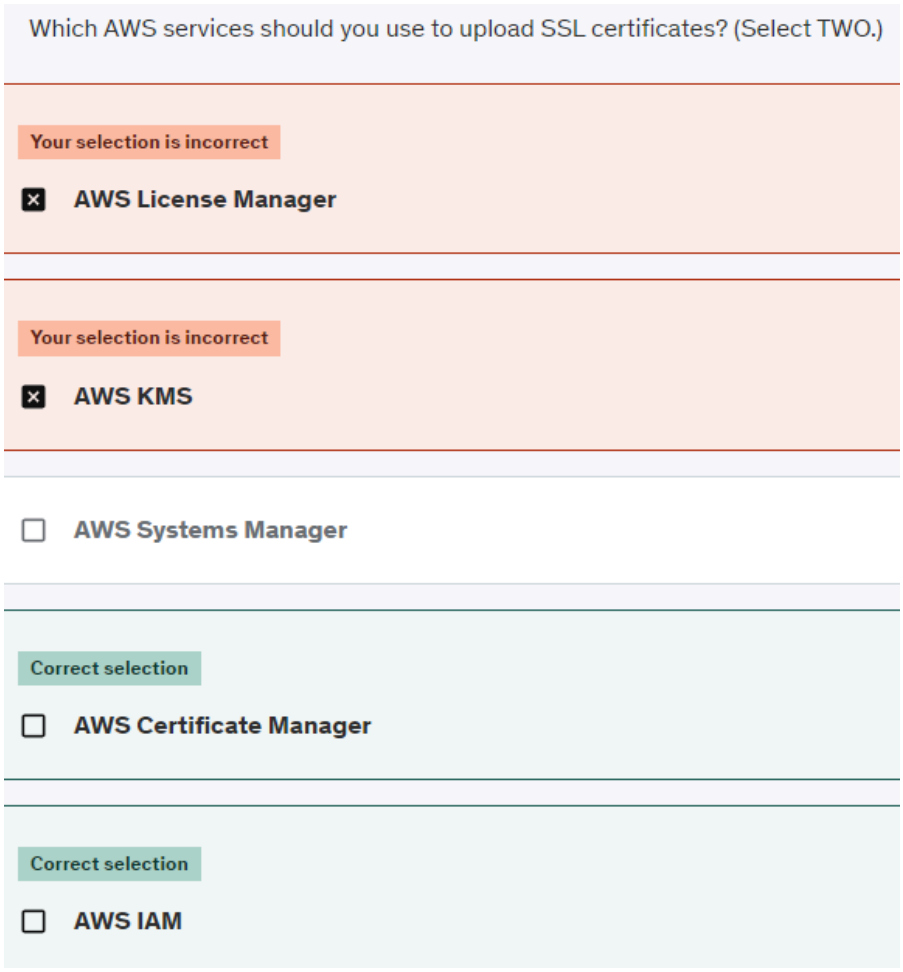
1. Understand IAM Roles vs. Other Options:
    - **IAM roles are designed for temporary access** and are the most secure option for **applications**.
    - They don't require long-term credentials stored in the application.
2. Key Concepts to Remember:

- Temporary Credentials: IAM roles provide temporary, automatically rotated credentials.
- Principle of Least Privilege: Roles can be scoped to exact permissions needed.
- Security Best Practice: **AWS recommends roles for EC2 instances and applications.**
- permanent credentials: IAM users, access keys

3. Exam Strategy:
    - When you see "temporary access" and "applications" together, lean towards IAM roles.



You can use IAM roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory.



S3 Policies & Access

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

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

Amazon S3 access control list is incorrect because this only grants permission to objects stored in S3 buckets to specific AWS accounts or IAM users.

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?

- Sticky Sessions

Your answer is incorrect

- Service Control Policies

Correct answer

- Origin Access Control

- Server Name Indication

Amazon CloudFront provides a feature called Origin Access Control (OAC) that allows CloudFront to send authenticated requests to an Amazon S3 origin. This feature is used to secure and restrict access to the content in an Amazon S3 bucket.

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

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.

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?

Correct answer

- ○ **Service Control Policy**

Your answer is incorrect

- ⊗ **AWS Systems Manager**
- ○ **AWS Secrets Manager**
- ○ **Resource-based policy**

Which of the following is an example of having a highly available application in AWS?

- ○ Using Amazon SQS to decouple messages between a sender and a receiver

Correct answer

- ○ Running your RDS instance with multi-AZ enabled

Your answer is incorrect

- ⊗ Running CloudFront for the static website in your S3 bucket

- ○ Running spot instances for your EC2 workloads

Running CloudFront for the static website in your S3 bucket is incorrect because this just allows your content to become globally available while at the same time enhancing delivery speeds.