

### Question 1Skipped

Which pillar of the AWS Well-Architected Framework includes the design principle of defining workloads, applications, and infrastructure as code (IaC)?

**Correct answer**

**Operational excellence**

**Security**

**Reliability**

**Performance efficiency**

Overall explanation

There are five design principles for operational excellence in the cloud, the first one is:

**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. You can implement your operations procedures as code and automate their execution by triggering them in response to events. By performing operations as code, you limit human error and enable consistent responses to events.

**CORRECT:** "Operational excellence" is the correct answer (as explained above.)

**INCORRECT:** "Reliability" is incorrect, as using Infrastructure as Code doesn't inherently increase reliability.

**INCORRECT:** "Performance efficiency" is incorrect also as using Infrastructure as Code doesn't make your applications any more performant.

**INCORRECT:** "Security" is incorrect also as Security is not increased by using Infrastructure as Code.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/architecting-for-the-cloud/>

**Domain**

AWS Cloud Architecture & Design

### Question 2Skipped

A company currently uses a Security Assertion Markup Language (SAML) based application to log in to third-party business applications and would like to have this hosted in AWS using managed services.

Which AWS service will meet this requirement?

**AWS Single Sign-On.**

## **AWS CLI.**

## **AWS Identity and Access Management (IAM).**

### **Correct answer**

### **Amazon Cognito.**

#### Overall explanation

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.

**CORRECT:** "Amazon Cognito" is the correct answer (as explained above.)

**INCORRECT:** "AWS Identity and Access Management (IAM)" is incorrect. Although it is related to granting permissions, IAM is specifically used to grant access to users within an AWS account. Amazon Cognito is a managed identity providing services which gives third party access to your applications.

**INCORRECT:** "AWS Single Sign-On" is incorrect. AWS Single Sign-On (AWS SSO) is where you create, or connect, your workforce identities in AWS once and manage access centrally across your AWS organization and doesn't use SAML.

**INCORRECT:** "AWS CLI" is incorrect. The AWS Command Line Interface (AWS CLI) is a unified tool to manage your AWS services from the command line of your desktop. It has nothing to do with SAML or authentication.

#### **References:**

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

#### **Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

## **Domain**

AWS Security, Identity, & Compliance

### **Question 3Skipped**

Which Amazon EC2 pricing model is the most cost-effective for an always-up, right-sized database server running a project that will last 1 year?

### **Correct answer**

#### **Standard Reserved Instances**

#### **Spot Instances**

#### **On-Demand Instances**

#### **Convertible Reserved Instances**

#### Overall explanation

Reserved Instances (RIs) provide you with a significant discount (up to 72%) compared to On-Demand instance pricing. Standard reserved instances offer the most cost savings. RIs are based on a 1 or 3 year contract so they are suitable for workloads that will run for the duration of the contract period.

**CORRECT:** "Standard Reserved Instances" is the correct answer.

**INCORRECT:** "Convertible Reserved Instances" is incorrect. You have the flexibility to change families, OS types, and tenancies while benefitting from RI pricing when you use Convertible RIs. However, this is not required for a right-sized server.

**INCORRECT:** "On-Demand Instances" is incorrect. This pricing model offers not discounts.

**INCORRECT:** "Spot Instances" is incorrect. Though you can achieve greater cost savings with Spot instances, the instances can be terminated when AWS need the capacity back.

#### References:

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

#### Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-billing-and-pricing/>

#### Domain

AWS Cost Management

#### Question 4Skipped

A company has been using an AWS managed IAM policy for granting permissions to users but needs to add some permissions.

How can this be achieved?

**Edit the AWS managed policy.**

**Correct answer**

**Create a custom IAM policy.**

**Create a rule in AWS WAF.**

**Create a Service Control Policy.**

Overall explanation

AWS managed policies cannot be edited so if you need to add permissions to users that are not granted in the policy you must create your own custom IAM policy.

**CORRECT:** "Create a custom IAM policy" is the correct answer.

**INCORRECT:** "Edit the AWS managed policy" is incorrect. You cannot edit AWS managed policies.

**INCORRECT:** "Create a Service Control Policy" is incorrect. SCPs are used in AWS Organizations to restrict available permissions. They do not grant permissions.

**INCORRECT:** "Create a rule in AWS WAF" is incorrect. WAF is a web application firewall used for protecting resources from web-based attacks.

**References:**

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_create.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

**Domain**

AWS Security, Identity, & Compliance

**Question 5Skipped**

Which authentication method is used to authenticate programmatic calls to AWS services?

**Server certificate**

**Key pair**

**Console password**

**Correct answer**

**Access keys**

Overall explanation

Access keys are a combination of an access key ID and a secret access key. They are used to make programmatic calls to AWS using the API.

**CORRECT:** "Access keys" is the correct answer.

**INCORRECT:** "Console password" is incorrect. Console passwords are used for signing users into the AWS Management Console, not for making programmatic calls to AWS services.

**INCORRECT:** "Server certificate" is incorrect. Server certificates can be used to authenticate to some AWS services using HTTPS.

**INCORRECT:** "Key pair" is incorrect. Key pairs should not be confused with access keys. Key pairs are used for authenticating to Amazon EC2 instances.

**References:**

[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)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-identity-and-access-management/>

**Domain**

AWS Security, Identity, & Compliance

**Question 6Skipped**

A company requires a single service which can manage their backup and restore requirements, their data lakes, and archives all in one place.

Which AWS service is suitable for all these use cases?

**Amazon Elastic File System (Amazon EFS).**

**Amazon FSx for Lustre.**

**Correct answer**

**Amazon Simple Storage Service (Amazon S3).**

**Amazon Elastic Block Store (Amazon EBS).**

Overall explanation

Amazon S3 is the only service out of the answers which can be used for backup and restore, data lakes and archival solutions. Because S3 is an object storage service, there are lots of different use cases.

**CORRECT:** "Amazon Simple Storage Service (Amazon S3)" is the correct answer (as explained above.)

**INCORRECT:** "Amazon Elastic File System (Amazon EFS)" is incorrect because Amazon EFS is a fully managed service providing NFS shared file system storage for Linux workloads - and is not ideally suited for backup and restore, data lakes or archival storage.

**INCORRECT:** "Amazon FSx for Lustre" is incorrect. This is simply not a good use case for backup and restore, data lakes or for archival storage. EFS for Lustre was designed to support terabytes per second of throughput and millions of IOPS.

**INCORRECT:** "Amazon Elastic Block Store (Amazon EBS)" is incorrect as Amazon EBS is a block storage device which is massively scalable and resilient. It's typically used for persistent HDD / SSD storage for EC2 instances, not for data lakes, archives or for backup and restore.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-storage-services/>

**Domain**

AWS Storage

**Question 7Skipped**

A company has many different business units all using the same AWS services to manage their different applications.

Which AWS service or tool can the company use to receive volume discounts across multiple AWS accounts?

**AWS Cost and Usage Report**

## **AWS Budgets**

### **Correct answer**

## **AWS Organizations**

### **Cost Explorer**

#### **Overall explanation**

You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts. Every organization in AWS Organizations has a management account that pays the charges of all the member accounts. With consolidated billing you can take advantage of cost savings for services that have tiered licensing models.

**CORRECT:** "AWS Organizations" is the correct answer (as explained above.)

**INCORRECT:** "AWS Budgets" is incorrect as AWS Budgets is a cost controlling feature, which allows you to set custom budgets to alert at various spend levels. It does not apply discounts based on volume use.

**INCORRECT:** "Cost Explorer" is incorrect. AWS Cost Explorer lets you visualize, understand, and manage your AWS costs and usage over time, but does not have anything to do with discounting AWS Service spend.

**INCORRECT:** "AWS Cost and Usage Report" is incorrect also. The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available - but doesn't provide any discounts or consolidated billing.

#### **References:**

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

#### **Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-management-services/>

## **Domain**

AWS Management & Governance

### **Question 8Skipped**

Which AWS services facilitate building secure and scalable mobile and web applications, offering features such as real-time updates and offline functionalities? (Select TWO.)

## **AWS Lambda**

## **AWS CodeDeploy**

### **Correct selection**

## **AWS Amplify**

## **Amazon API Gateway**

### **Correct selection**

## AWS AppSync

Overall explanation

AWS AppSync and AWS Amplify are the correct answers as both services facilitate the building of secure and scalable mobile and web applications. AWS AppSync enables the creation of flexible APIs, including options for real-time updates and offline functionalities. AWS Amplify is a set of tools and services that can be used to build scalable full-stack apps powered by AWS, also supporting real-time functionalities and offline operations.

**CORRECT:** "AWS AppSync" is a correct answer (as explained above.)

**CORRECT:** "AWS Amplify" is also a correct answer (as explained above.)

**INCORRECT:** "AWS Lambda" is incorrect because, while it is a service that lets you run your code without provisioning or managing servers, it is more about executing backend functions rather than facilitating the development of secure and scalable applications with real-time and offline functionalities.

**INCORRECT:** "AWS CodeDeploy" is incorrect because it is a deployment service that automates application deployments to specified compute environments, including Amazon EC2 instances and AWS Lambda functions, but does not inherently facilitate the building of mobile and web applications with the described features.

**INCORRECT:** "Amazon API Gateway" is incorrect because, although it allows for the creation, publishing, maintenance, monitoring, and securing of REST, HTTP, and WebSocket APIs at any scale, it doesn't specifically facilitate building applications with real-time updates and offline functionalities as a standalone service.

### References:

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

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-analytics-services/>

## Domain

AWS Analytics

### Question 9Skipped

A user needs a quick way to determine if any Amazon EC2 instances have ports that allow unrestricted access.

Which AWS service will support this requirement?

### VPC Flow Logs

**Correct answer**

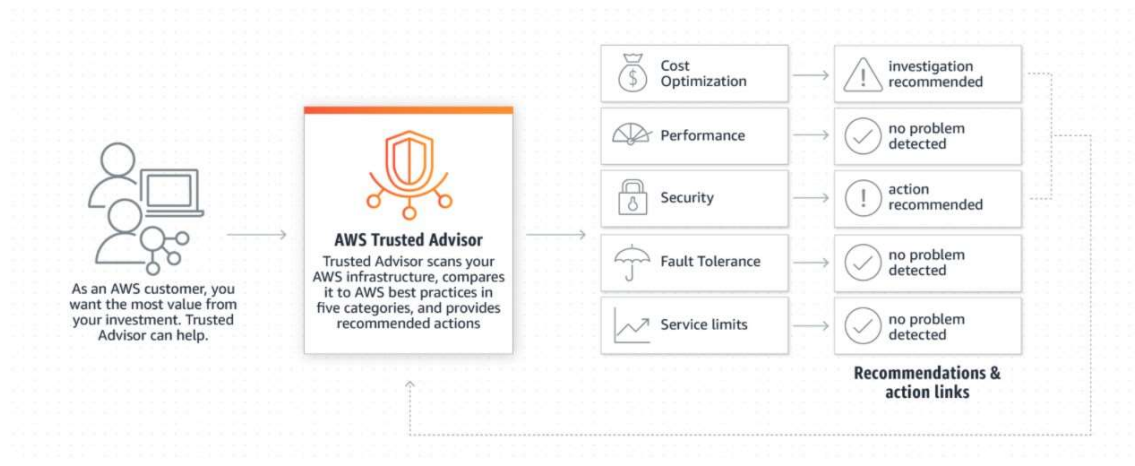
**AWS Trusted Advisor**

**AWS CloudWatch Logs**

## AWS Shield

### Overall explanation

Access to the ports on an Amazon EC2 instance is controlled through security groups. AWS Trusted Advisor scans the security groups in your account to see if any security groups allow unrestricted access to any ports. This information is then presented to you in the console and you can then act on this information to secure the ports through editing the rules in the security group.



**CORRECT:** "AWS Trusted Advisor" is the correct answer.

**INCORRECT:** "VPC Flow Logs" is incorrect. VPC Flow Logs capture information about the IP traffic going to and from network interfaces in your VPC.

**INCORRECT:** "AWS Shield" is incorrect. AWS Shield is a managed service for mitigating distributed denial of service (DDoS) attacks.

**INCORRECT:** "AWS CloudWatch Logs" is incorrect. CloudWatch Logs captures logging information from applications and AWS services.

### References:

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

### Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-security-services/>

## Domain

### AWS Management & Governance

#### Question 10Skipped

How does Amazon CloudFront deliver content to end users with low latency using the AWS global infrastructure?

## AWS Regions

## AWS Direct Connect connections



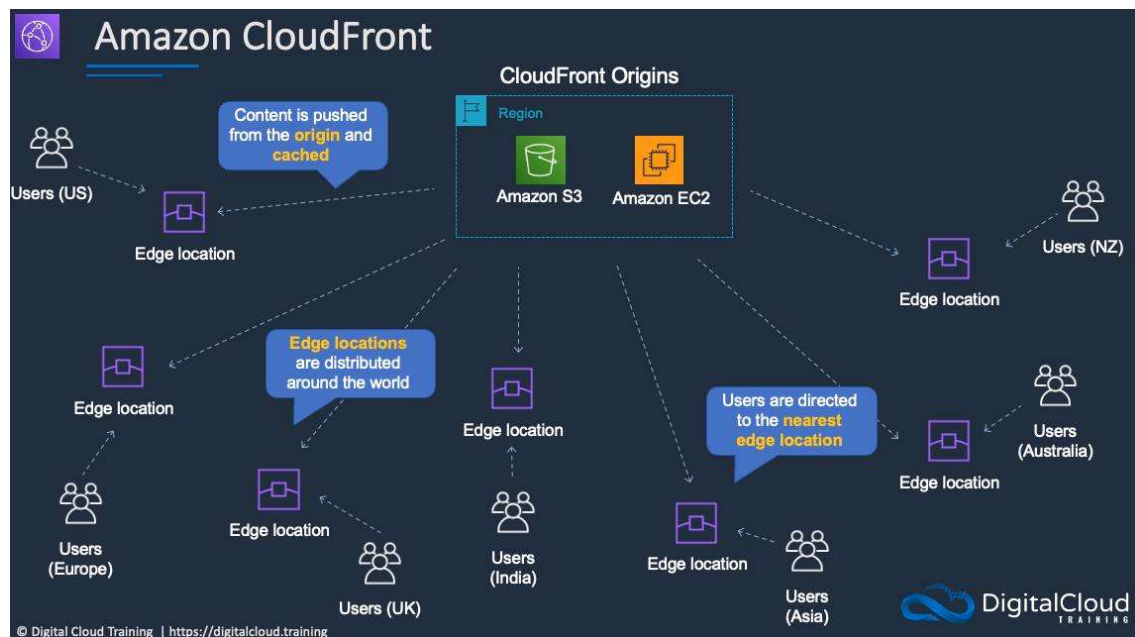
**Correct answer**

**Edge locations**

**Availability Zones**

Overall explanation

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.



**CORRECT:** "Edge locations" is the correct answer (as explained above.)

**INCORRECT:** "AWS Regions" is incorrect. AWS Regions are groups of Availability Zones, which do not serve CloudFront content - but are used instead to launch applications in of themselves.

**INCORRECT:** "Availability Zones" is incorrect as Availability Zones are groups of Data centers, and multiple Availability Zones combine to make AWS Regions.

**INCORRECT:** "AWS Direct Connect connections" is incorrect as Direct Connect is a way of connecting your on-premises environment into the AWS Cloud with a direct physical cable. This does not relate to Amazon CloudFront or Edge Locations.

**References:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-networking-services/>

**Domain**

**Question 11**Skipped

Are there any AWS services or features that will identify and search for externally shared AWS resources?

**Correct answer**

**AWS IAM Access Analyzer.**

**AWS Fargate.**

**Amazon OpenSearch Service (Amazon Elasticsearch Service).**

**AWS Control Tower.**

Overall explanation

Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, shared with an external entity. This lets you identify unintended access to your resources and data, which is a security risk.

**CORRECT:** "AWS IAM Access Analyzer" is the correct answer (as explained above.)

**INCORRECT:** "Amazon OpenSearch Service (Amazon Elasticsearch Service)" is incorrect. Amazon OpenSearch Service makes it easy for you to perform interactive log analytics, real-time application monitoring, website search, and more. OpenSearch is an open source, distributed search and analytics suite derived from Elasticsearch. It has nothing to do with identifying externally shared resources.

**INCORRECT:** "AWS Control Tower" is incorrect. AWS Control Tower provides the easiest way to set up and govern a secure, multi-account AWS environment, called a landing zone. This is a governance service and is not related to Identity and Access Management.

**INCORRECT:** "AWS Fargate" is incorrect. AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers. It does not reference Identity and Access management.

**References:**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

**Domain**

AWS Security, Identity, & Compliance

**Question 12**Skipped

Which AWS service helps you deploy application configuration changes with features like validation checks and timely deployment while avoiding the need to write additional code or restart application services?

**AWS CodeCommit**

## **AWS CloudFormation**

### **Correct answer**

## **AWS AppConfig**

## **AWS CodeStar**

### **Overall explanation**

AWS AppConfig is the correct answer because it allows users to deploy application configuration changes quickly and reliably without needing to write additional code or restart services. It supports validation checks to ensure configuration data is syntactically and semantically correct before deployment, avoiding potential outages.

**CORRECT:** "AWS AppConfig" is the correct answer (as explained above.)

**INCORRECT:** "AWS CodeStar" is incorrect because, while it provides a unified interface for managing software development activities in one place, it does not specifically deal with deploying application configuration changes with the features described in the question.

**INCORRECT:** "AWS CodeCommit" is incorrect because it is a source control service hosted by AWS for privately storing and managing assets in the cloud, not for deploying and managing application configurations specifically.

**INCORRECT:** "AWS CloudFormation" is incorrect because, even though it allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications, it doesn't specialize in deploying application configurations with validation checks as described in the scenario.

### **References:**

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

## **Domain**

AWS Cloud Architecture & Design

### **Question 13Skipped**

Which AWS services are associated with Edge Locations? (Select TWO.)

## **AWS Config**

## **Amazon EBS**

## **AWS Direct Connect**

### **Correct selection**

## **Amazon CloudFront**

### **Correct selection**

## **AWS Shield**

### **Overall explanation**

Edge Locations are parts of the Amazon CloudFront content delivery network (CDN) that are all around the world and are used to get content closer to end-users for better performance.

AWS Shield which protects against Distributed Denial of Service (DDoS) attacks is available globally on Amazon CloudFront Edge Locations.

**CORRECT:** "Amazon CloudFront" is a correct answer.

**CORRECT:** "AWS Shield" is also a correct answer.

**INCORRECT:** "AWS Direct Connect" is incorrect. AWS Direct Connect is a networking service used for creating a hybrid cloud between on-premises and AWS Cloud using a private network connection

**INCORRECT:** "Amazon EBS" is incorrect. Amazon EBS is a storage service.

**INCORRECT:** "AWS Config" is incorrect. AWS Config is used for evaluating the configuration state of AWS resources.

#### **References:**

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

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-content-delivery-and-dns-services/>

#### **Domain**

AWS Networking & Content Delivery

#### **Question 14Skipped**

An organization moves a workload to Amazon EC2 instances on AWS. Cost-effectiveness is the key to running the workload properly in the Cloud.

What can the company do to meet this requirement?

**Use AWS Key Management Service (AWS KMS).**

**Correct answer**

**Rightsize all the EC2 instances that are used in the deployment**

**Use multiple AWS accounts and consolidated billing.**

**Use AWS CloudFormation to deploy the infrastructure.**

Overall explanation

Rightsizing EC2 instances simply means making sure that the instances you are using are not too large or too small for the workloads they are running. The part of this which is related to cost optimization is ensuring that the EC2 instances provisioned are not too small for the workloads (i.e. you need a m5.2xlarge and you are using an m5.4xlarge instance type. As you simply get billed for the instance you are using and not how many VCPUs you are using, right sizing is a powerful way to optimize cost.

AWS Compute Optimizer is a useful tool that uses machine learning to report on overutilization and underutilization of resources. You can use Compute Optimizer to gather the information needed to rightsize your workloads.

**CORRECT:** "Rightsize all the EC2 instances that are used in the deployment" is the correct answer (as explained above.)

**INCORRECT:** "Use multiple AWS accounts and consolidated billing" is incorrect as whilst consolidated billing may give you only one bill for all the accounts under your Organization, this doesn't inherently provide any cost savings.

**INCORRECT:** "Use AWS CloudFormation to deploy the infrastructure" is incorrect. AWS CloudFormation is an infrastructure as code tool which provisions your infrastructure using either JSON or YAML. This may improve various aspects of your architecture but will not make it any cheaper.

**INCORRECT:** "Use AWS Key Management Service (AWS KMS)" is incorrect as AWS KMS is a managed encryption service which can be used to encrypt data across your infrastructure. This has nothing to do with cost optimization.

#### References:

<https://aws.amazon.com/blogs/aws-cloud-financial-management/launch-resource-optimization-recommendations/>

#### Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-billing-and-pricing/>

#### Domain

AWS Compute

#### Question 15Skipped

Which AWS service or feature can be used to restrict the individual API actions that users and roles in each member account can access?

**AWS Shield**

**AWS IAM**

**Correct answer**

**AWS Organizations**

**Amazon Macie**

Overall explanation

AWS Organizations offers Service control policies (SCPs) which are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions (API actions) for all accounts in your organization. SCPs help you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled.

**CORRECT:** "AWS Organizations" is the correct answer.

**INCORRECT:** "Amazon Macie" is incorrect. Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS

**INCORRECT:** "AWS Shield" is incorrect. AWS Shield is a service that protects workloads against distributed denial of service (DDoS) attacks.

**INCORRECT:** "AWS IAM" is incorrect. AWS IAM is used for assigning permissions but SCPs in AWS Organizations are used to control which API actions are allowed in an account. You need to be granted permission in IAM and have the API allowed to be able to use the API successfully.

**References:**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-management-services/>

**Domain**

AWS Management & Governance

**Question 16**Skipped

An organization recently migrated to AWS and wants to enable intelligent threat protection and continuous monitoring across all its accounts.

Which AWS service should the company use to achieve this goal?

**AWS Shield**

**Amazon Detective**

**Correct answer**

**Amazon GuardDuty**

**Amazon Macie**

Overall explanation

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

**CORRECT:** "Amazon GuardDuty" is the correct answer (as explained above.)

**INCORRECT:** "Amazon Macie" is incorrect, as Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. It does not have anything to do with Amazon GuardDuty.

**INCORRECT:** "AWS Shield" is incorrect. AWS Shield is a managed DDoS prevention and mitigation service, and it doesn't provide intelligent threat detection on an account-by-account basis.

**INCORRECT:** "Amazon Detective" is incorrect. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations - but does not actively detect threats.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

**Domain**

AWS Security, Identity, & Compliance

**Question 17Skipped**

Which IAM entity can be used for assigning permissions to multiple users?

**Correct answer**

**IAM Group**

**IAM User**

**IAM Role**

**IAM password policy**

Overall explanation

Groups are collections of users and have policies attached to them. You can use groups to assign permissions to multiple users. To do this place the users in the group and then create an IAM policy with the correct permissions and attach it to the group.

You do not use an IAM User, Role, or password policy to assign permissions to multiple users.

**CORRECT:** "IAM Group" is the correct answer.

**INCORRECT:** "IAM User" is incorrect as explained above.

**INCORRECT:** "IAM Role" is incorrect as explained above.

**INCORRECT:** "IAM password policy" is incorrect as explained above.

**References:**

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_groups.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-identity-and-access-management/>

**Domain**

AWS Security, Identity, & Compliance

**Question 18Skipped**

How can a user block a suspicious IP address from connecting to an Amazon EC2 instance?

**Block the IP on the outbound rule of a security group.**

**Correct answer**

**Block the IP on the inbound rule of a network ACL.**

**Block the IP on the outbound rule of a security group and network ACL.**

**Block the IP on the inbound rule of a security group and network ACL.**

Overall explanation

With a Network ACL you can block a specific IP address that would be coming inbound into your subnet. This would prevent a specific IP from gaining access if you suspected them of being a bad actor.

The table below shows the key differences between Network ACLs and Security Groups:

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

**CORRECT:** "Block the IP on the inbound rule of a network ACL" is the correct answer (as explained above.)

**INCORRECT:** "Block the IP on the outbound rule of a security group" is incorrect as you cannot block individual IP addresses on Security Groups.

**INCORRECT:** "Block the IP on the inbound rule of a security group and network ACL" is incorrect as you cannot block individual IP addresses on Security Groups.

**INCORRECT:** "Block the IP on the outbound rule of a security group and network ACL" is incorrect as you cannot block individual IP addresses on Security Groups.

**References:**

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-block-or-allow-ips/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-networking-services/>

**Domain**



**Question 19Skipped**

A security operations engineer needs to implement threat detection and monitoring for malicious or unauthorized behavior. Which service should be used?

**AWS Shield**

**AWS CloudHSM**

**Correct answer**

**Amazon GuardDuty**

**AWS KMS**

Overall explanation

Amazon GuardDuty offers threat detection and continuous security monitoring for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

**CORRECT:** "AWS GuardDuty" is the correct answer.

**INCORRECT:** "AWS Shield" is incorrect. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service.

**INCORRECT:** "AWS KMS" is incorrect. AWS Key Management Service gives you centralized control over the encryption keys used to protect your data.

**INCORRECT:** "AWS CloudHSM" is incorrect. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

**Domain**

AWS Security, Identity, & Compliance

**Question 20Skipped**

What AWS service decouples application components so that they can run independently?

**Correct answer**

**Amazon Simple Queue Service (Amazon SQS)**

**Amazon Simple Workflow Service (Amazon SWF)**

**Amazon Simple Notification Service (Amazon SNS)**

**AWS Glue**

Overall explanation

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work.

**CORRECT:** "Amazon Simple Queue Service (SQS)" is the correct answer (as explained above.)

**INCORRECT:** "Amazon Simple Workflow Service (Amazon SWF)" is incorrect, as Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps, and is a fully managed state tracker and task coordinator in the Cloud.

**INCORRECT:** "Amazon Simple Notification Service (Amazon SNS)" is incorrect. Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication and does not directly decouple application components.

**INCORRECT:** "AWS Glue" is incorrect. AWS Glue is a serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development, and does not decouple your architecture.

**References:**

[www.aws.amazon.com/sqs](http://www.aws.amazon.com/sqs)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-application-integration/>

**Domain**

AWS Management & Governance

**Question 21**Skipped

Which service can be used to cost-effectively move exabytes of data into AWS?

**S3 Cross-Region Replication (CRR)**

**Correct answer**

**AWS Snowmobile**

**S3 Transfer Acceleration**

**AWS Snowball**

Overall explanation

With AWS Snowmobile you can move 100PB per snowmobile. AWS call this an "Exabyte-scale data transfer service".

**CORRECT:** "AWS Snowmobile" is the correct answer.

**INCORRECT:** "AWS Snowball" is incorrect. With AWS Snowball you can move up to 80TB per device. AWS call this a "petabyte-scale data transfer service".

**INCORRECT:** "S3 Transfer Acceleration" is incorrect. S3 Transfer Acceleration is meant speed up uploads to Amazon S3 but would not be used for exabytes of data.

**INCORRECT:** "S3 Cross-Region Replication (CRR)" is incorrect. S3 Cross-Region Replication is used for copying data between regions, not into AWS. It is also unsuitable for moving such as huge amount of data.

#### References:

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

Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-storage-services/>

#### Domain

AWS Migration & Transfer

#### Question 22Skipped

Which service allows an organization to view operational data from multiple AWS services through a unified user interface and automate operational tasks?

**Correct answer**

**AWS Systems Manager**

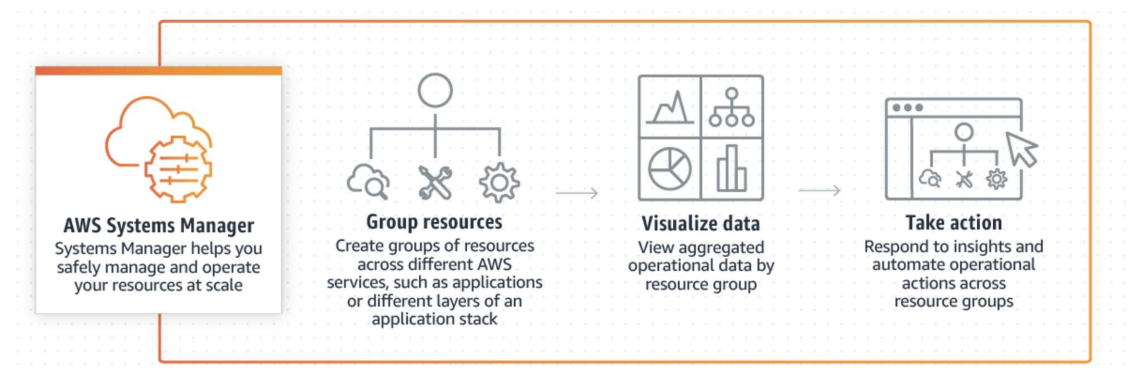
**AWS Config**

**AWS OpsWorks**

**Amazon CloudWatch**

Overall explanation

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.



**CORRECT:** "AWS Systems Manager" is the correct answer.

**INCORRECT:** "AWS Config" is incorrect. AWS Config is a fully-managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and regulatory compliance.

**INCORRECT:** "AWS OpsWorks" is incorrect. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.

**INCORRECT:** "Amazon CloudWatch" is incorrect. Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You use CloudWatch for performance monitoring, not automating operational tasks.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/additional-aws-services/>

**Domain**

AWS Management & Governance

**Question 23Skipped**

A company has a mission critical Linux-based application. The application must run every Monday from 6 AM until 10pm. As the application is critical, it cannot be interrupted.

Which Amazon EC2 instance purchasing option meets these requirements MOST cost-effectively?

**Correct answer**

**On-Demand Capacity Reservation with Savings Plan**

**Dedicated Hosts**

**Regional Reserved Instances**

**Spot Instances**

Overall explanation

On-Demand Capacity Reservation with Savings Plan is ideal in this scenario as the application will have predictable running times (every Monday from 6am till 10pm). It is also mission critical, so reserving the capacity within an Availability Zone using On-Demand Capacity Reservation with Savings Plan makes perfect sense. The savings plans will also make this application cost-effective whilst still maintaining the guaranteed availability that you cannot get with spot instances.

**CORRECT:** "On-Demand Capacity Reservation with Savings Plan" is the correct answer (as explained above.)

**INCORRECT:** "Spot Instances" is incorrect because although this will be the cheapest option, the application has been described as 'Mission Critical', and because spot terminations can happen at a two-minute notice, Spot would be unsuitable for this workload.

**INCORRECT:** "Regional Reserved Instances" is incorrect because it does not give you the guaranteed service availability that On Demand Capacity reservations have, therefore it is wrong.

**INCORRECT:** "Dedicated Hosts" is incorrect. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements, and as it is a single server, is not durable by default. Therefore it is not suitable; for this mission-critical use case. Also it is too expensive to be used for workloads you need to be cost-effective.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

**Domain**

AWS Cost Management

**Question 24**Skipped

Your CTO wants to move to cloud. What cost advantages are there to moving to cloud?

**You can reduce your marketing costs**

**Correct answer**

**You provision only what you need and adjust to peak load**

**You don't need to pay for application licensing**

**You get free data transfer into and out of the cloud**

Overall explanation

One of the best benefits of cloud is that you can launch what you need to and automatically adjust your resources as demand changes. This means you only ever pay for what you're using.

**CORRECT:** "You provision only what you need and adjust to peak load" is the correct answer.

**INCORRECT:** "You can reduce your marketing costs" is incorrect. You don't reduce marketing costs when moving to the cloud, your organization still needs to do the same amount of marketing.

**INCORRECT:** "You don't need to pay for application licensing" is incorrect. It is not true that you don't need to pay for application licensing in the cloud. You still pay for your application licenses when running on Amazon EC2.

**INCORRECT:** "You get free data transfer into and out of the cloud" is incorrect. You do not get free bi-directional data transfer into and out of the cloud. AWS charge for outbound data transfer.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

## Domain

### AWS Cost Management

#### Question 25Skipped

How does the AWS global infrastructure offer high availability and fault tolerance to customers?

**The AWS infrastructure consists of subnets containing various Availability Zones with multiple data centers located in the same geographic location.**

**The AWS infrastructure is made up of multiple AWS Regions within various Availability Zones located in areas that have low flood risk and are interconnected with low-latency networks and redundant power supplies.**

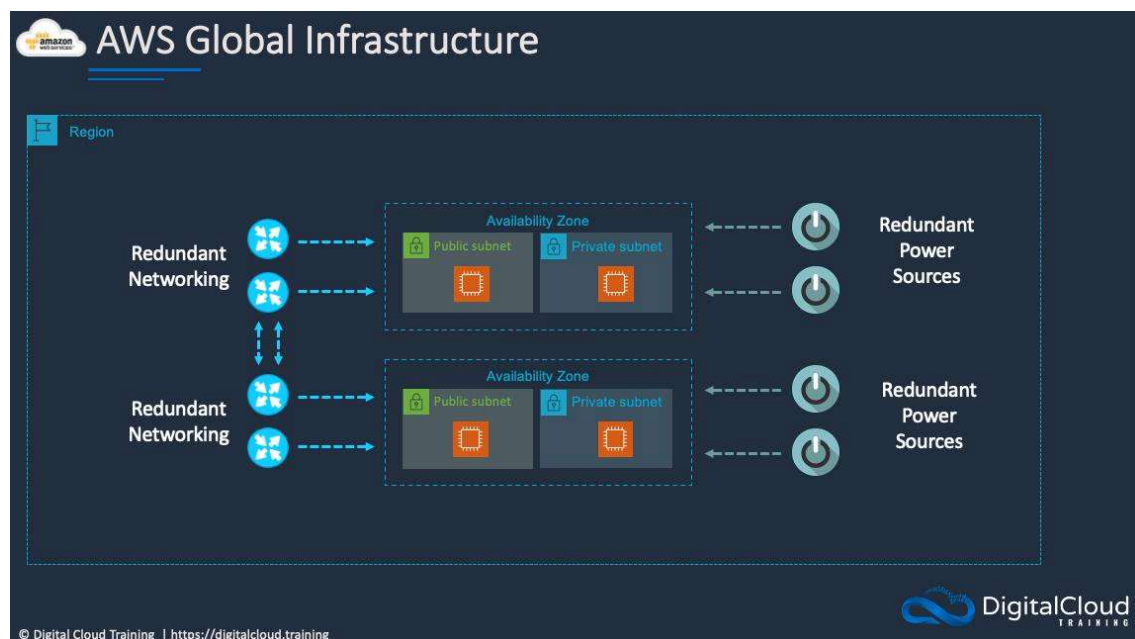
**AWS allows users to choose AWS Regions and data centers so that users can select the closest data centers in different Regions.**

#### Correct answer

**The AWS infrastructure consists of isolated AWS Regions with independent Availability Zones that are connected with low-latency networking and redundant power supplies.**

#### Overall explanation

AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. We call each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area. Each Region and each AZ is fully redundant from one another, meaning a failure in one AZ / Region will not impact another Region or AZ.



**CORRECT:** "The AWS infrastructure consists of isolated AWS Regions with independent Availability Zones that are connected with low-latency networking and redundant power supplies" is the correct answer (as explained above.)

**INCORRECT:** "The AWS infrastructure consists of subnets containing various Availability Zones with multiple data centers located in the same geographic location" is incorrect. Subnets are IP address ranges within a VPC in which you can host instances. They are not a physical component which is part of the AWS Global infrastructure.

**INCORRECT:** "AWS allows users to choose AWS Regions and data centers so that users can select the closest data centers in different Regions" is incorrect. Availability zones make up multiple Data Centers. We cannot choose at the level of any one data center where we can put our application, we can only choose to launch our services within an Availability Zone.

**INCORRECT:** "The AWS infrastructure is made up of multiple AWS Regions within various Availability Zones located in areas that have low flood risk and are interconnected with low-latency networks and redundant power supplies" is incorrect as AWS Regions are collections of Availability Zones, not the other way around.

**References:**

[https://aws.amazon.com/about-aws/global-infrastructure/regions\\_az/](https://aws.amazon.com/about-aws/global-infrastructure/regions_az/)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-computing-concepts/>

**Domain**

AWS Cloud Architecture & Design

**Question 26Skipped**

Which AWS tools can be used for automation? (Select TWO.)

**Correct selection**

**AWS Elastic Beanstalk**

**AWS Lambda**

**Elastic Load Balancing**

**Amazon Elastic File System (EFS)**

**Correct selection**

**AWS CloudFormation**

Overall explanation

AWS Elastic Beanstalk and AWS CloudFormation are both examples of automation. Beanstalk is a platform service that leverages the automation capabilities of CloudFormation to build out application architectures.

**CORRECT:** "AWS Elastic Beanstalk" is a correct answer.

**CORRECT:** "AWS CloudFormation" is also a correct answer.

**INCORRECT:** "Elastic Load Balancing" is incorrect. Elastic Load Balancing (ELB) is used for distributing incoming connections to Amazon EC2 instances. This is not an example of automation; it is load balancing.

**INCORRECT:** "Amazon Elastic File System (EFS)" is incorrect. Amazon EFS is a file system.

**INCORRECT:** "AWS Lambda" is incorrect. AWS Lambda is a compute service, not an automation service.

**References:**

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

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/additional-aws-services/>

**Domain**

AWS Management & Governance

**Question 27Skipped**

An architecture's ability to withstand failures with minimal downtime demonstrates which AWS Cloud benefit?

**Elasticity**

**Scalability**

**Correct answer**

**High availability**

**Agility**

Overall explanation

A high availability computing infrastructure continues to function even when some of its components fail. Mission-critical systems cannot tolerate interruptions in service, and any downtime can result in damage or financial losses.

**CORRECT:** "High Availability" is the correct answer (as explained above.)

**INCORRECT:** "Agility" is incorrect, as agility refers to the time to launch applications and services being massively reduced. This is not related to withstanding failure.

**INCORRECT:** "Scalability" is incorrect. Scalability is not related to downtime and reacting to interruptions of service directly. Scalability means how quickly our applications scales up and down under typical usage, not failure.

**INCORRECT:** "Elasticity" is incorrect. Elasticity is the ability to acquire resources as you need them and release resources when you no longer need them, and not related to interruption of service.

**References:**

<https://docs.aws.amazon.com/whitepapers/latest/real-time-communication-on-aws/high-availability-and-scalability-on-aws.html>



**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-computing-concepts/>

## **Domain**

AWS Cloud Benefits

### **Question 28Skipped**

Which of the following are advantages of the AWS Cloud? (Select TWO.)

#### **Correct selection**

**Users can stop spending money on the maintenance of data centers.**

**Expenses never change from month to month.**

#### **Correct selection**

**Users can stop guessing about resource capacity.**

**AWS manages all the security within the cloud.**

**Users do not need to deploy applications globally.**

Overall explanation

When you are using the Cloud and migrating your workloads out of your own data centers, you can stop spending money on the maintenance of data centers.

Also, the cloud allows you to stop guessing your resource capacity ahead of time as you do not need to provision capacity ahead of time.

**CORRECT:** "Users can stop spending money on the maintenance of data centers" is the correct answer (as explained above.)

**CORRECT:** "Users can stop guessing about resource capacity" is also a correct answer (as explained above.)

**INCORRECT:** "AWS manages all the security within the cloud" is incorrect as this is not true. AWS manages the security of the cloud, vs AWS customers looking after the data they store in the cloud. It is a shared responsibility.

**INCORRECT:** "Expenses never change from month to month" is incorrect as this is also untrue. Spend will be directly related to the number of resources provisioned which will scale up and down based on your application's need.

**INCORRECT:** "Users do not need to deploy applications globally" is incorrect as the ability to deploy application globally is an advantage the cloud provides over using your own data center.

#### **References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-computing-concepts/>

### Question 29Skipped

Which AWS service can be used to track the activity of users on AWS?

**Amazon CloudWatch**

**AWS Directory Service**

**Correct answer**

**AWS CloudTrail**

**Amazon Inspector**

Overall explanation

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

Think of CloudTrail is an auditing service (who did what and when), and CloudWatch as a performance monitoring service (how much resource was used).

**CORRECT:** "AWS CloudTrail" is the correct answer.

**INCORRECT:** "AWS Directory Service" is incorrect. This service provides several options for running directory services on AWS and connecting to directory services on-premises.

**INCORRECT:** "Amazon Inspector" is incorrect. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS

**INCORRECT:** "Amazon CloudWatch" is incorrect. CloudWatch is used for performance monitoring, not auditing.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-monitoring-and-logging-services/>

**Domain**

AWS Management & Governance

### Question 30Skipped

An Amazon EC2 instance running the Amazon Linux 2 AMI is billed in what increment?

**Per hour**

**Correct answer**

**Per second**

**Per GB**

## **Per CPU**

Overall explanation

Amazon EC2 instances running Linux are billed in one second increments, with a minimum of 60 seconds.

**CORRECT:** "Per second" is the correct answer.

**INCORRECT:** "Per hour" is incorrect. You do not pay per hour.

**INCORRECT:** "Per CPU" is incorrect. You do not pay per CPU.

**INCORRECT:** "Per GB" is incorrect. You pay for Amazon EBS on a per GB of provisioned storage basis.

## **References:**

<https://aws.amazon.com/about-aws/whats-new/2017/10/announcing-amazon-ec2-per-second-billing/>

[https://d1.awsstatic.com/whitepapers/aws\\_pricing\\_overview.pdf](https://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf)

## **Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

## **Domain**

AWS Compute

## **Question 31Skipped**

A company needs to invoke an AWS Step Functions workflow each time an Amazon EC2 instance state changes.

Which AWS service can the company use to meet this requirement?

## **Correct answer**

**Amazon EventBridge**

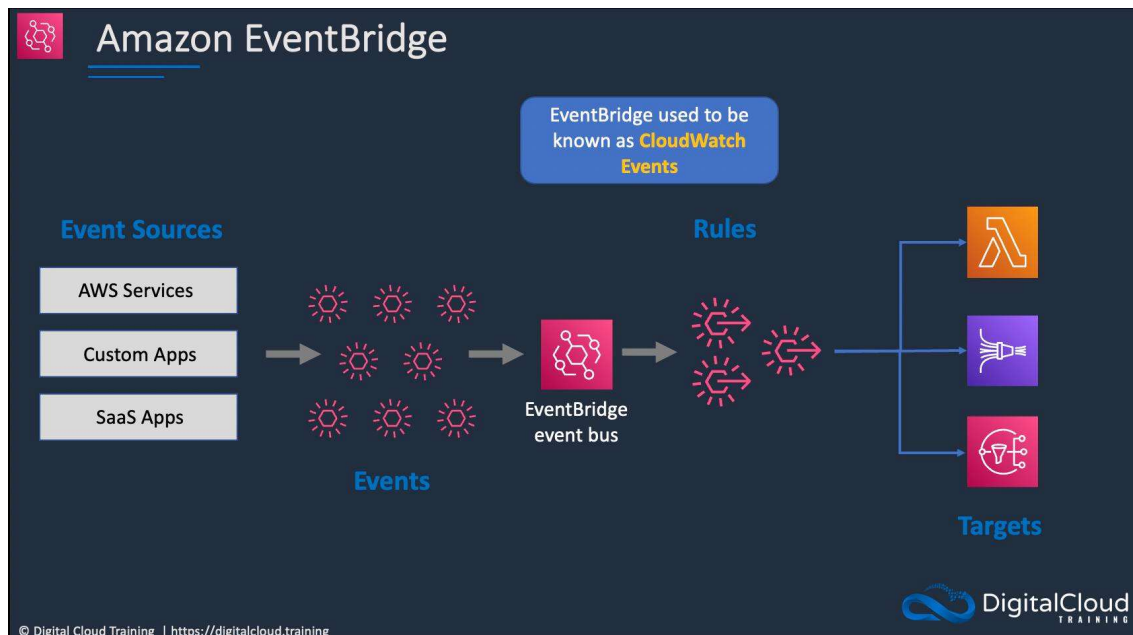
**AWS Fargate**

**Amazon SageMaker**

**Amazon Connect**

Overall explanation

Amazon EventBridge is a serverless event bus that makes it easier to build event-driven applications at scale using events generated from your applications. You can set rules for actions to take place when certain events happen, like instance state changes, items are uploaded to an S3 bucket etc.



**CORRECT:** "Amazon EventBridge" is the correct answer (as explained above.)

**INCORRECT:** "Amazon SageMaker" is incorrect. Amazon SageMaker is a Machine Learning service which allows you to build, train, and deploy machine learning models for any use case with fully managed infrastructure, tools, and workflows and has nothing to do with automation.

**INCORRECT:** "Amazon Connect" is incorrect as Connect is a cloud-based telecommunications service providing managed cloud-based customer contact centers, thus having nothing to do with workflow automation.

**INCORRECT:** "AWS Fargate" is incorrect also as Fargate is a serverless container service, which can be used within automation workflows, however, does not automate parts of your architecture in of itself.

#### References:

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

Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-cloud-management-services/>

#### Domain

AWS Management & Governance

#### Question 32Skipped

Which AWS service supports an in-memory data structure store, compatible with Redis, that delivers sub-millisecond latency for use cases such as caching, session stores, and real-time analytics?

**Correct answer**

**Amazon MemoryDB**

## Amazon RDS

## Amazon DynamoDB

## Amazon Redshift

Overall explanation

Amazon MemoryDB for Redis is the correct answer because it is a Redis-compatible, in-memory database service built on Redis architecture, which offers sub-millisecond latency, fulfilling the requirements mentioned in the question.

**CORRECT:** "Amazon MemoryDB " is the correct answer (as explained above.)

**INCORRECT:** "Amazon DynamoDB" is incorrect because, while it is a key-value and document database that delivers single-digit millisecond performance at any scale, it is not a Redis-compatible in-memory data structure store designed specifically to offer sub-millisecond latency for the use cases mentioned.

**INCORRECT:** "Amazon RDS" is incorrect because, although it is a relational database service that supports several database engines, it does not inherently support an in-memory data structure store that is compatible with Redis for sub-millisecond latency performance.

**INCORRECT:** "Amazon Redshift" is incorrect because it is a data warehousing solution optimized for analytic queries against large datasets and is not designed as a Redis-compatible in-memory data structure store offering sub-millisecond latency.

### References:

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

## Domain

AWS Database

### Question 33Skipped

A company has 50 different business units and requires that each business unit's billing information is viewed separately.

What should a cloud practitioner recommend?

### Correct answer

**Tag each business unit's resources, then filter by unit in Cost Explorer.**

**Use a different VPC for each business unit, then filter by unit using an AWS Cost and Usage Report.**

**Place each business unit in a different AWS Region, then filter by unit in Cost Explorer.**

**Use separate AWS accounts for each business unit, then filter by unit using the coverage report.**

Overall explanation

By using Tags, you can apply metadata to application components aligning each component to an application. You can then filter based on these tags within AWS Cost Explorer to see easily

how much each application costs. This is the easiest way to achieve the requirements out of the options.

**CORRECT:** "Tag each business unit's resources, then filter by unit in Cost Explorer" is the correct answer (as explained above.)

**INCORRECT:** "Use separate AWS accounts for each business unit, then filter by unit using the coverage report" is incorrect. The coverage report is a component of Savings Plans, which is a billing option for various services which applies discounts based on committed spend.

**INCORRECT:** "Place each business unit in a different AWS Region, then filter by unit in Cost Explorer" is incorrect. This would work but is unnecessary. Regions are not designed to isolate applications and are simply different geographic parts of the AWS Global infrastructure. You may also want your applications to be in the same region for other reasons such as latency, compliance etc.

**INCORRECT:** "Use a different VPC for each business unit, then filter by unit using an AWS Cost and Usage Report" is incorrect as this is also not necessary, and it is much easier to filter costs using tags.

#### References:

[https://docs.aws.amazon.com/general/latest/gr/aws\\_tagging.html](https://docs.aws.amazon.com/general/latest/gr/aws_tagging.html)

#### Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-billing-and-pricing/>

#### Domain

AWS Cost Management

#### Question 34Skipped

A company needs to optimize costs and resource usage through monitoring of operational health for all resources running on AWS.

Which AWS service will meet these requirements?

#### Correct answer

**Amazon CloudWatch**

**AWS CloudTrail**

**AWS Control Tower**

**AWS Config**

Overall explanation

Amazon CloudWatch is a performance monitoring tool that receives metrics from AWS services. This data can be used for monitoring the operational health of resources as well as being used to optimize costs through ensuring systems are right-sized and just enough capacity is provisioned.

**CORRECT:** "Amazon CloudWatch" is the correct answer.

**INCORRECT:** "AWS Control Tower" is incorrect. AWS Control Tower is a service that is intended for organizations with multiple accounts and teams who are looking for the easiest way to set up their new multi-account AWS environment and govern at scale

**INCORRECT:** "AWS CloudTrail" is incorrect. CloudTrail is used for auditing (who did what and when), it is not used for monitoring operational health.

**INCORRECT:** "AWS Config" is incorrect. Config is used for managing compliance for AWS services.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-monitoring-and-logging-services/>

**Domain**

AWS Management & Governance

**Question 35Skipped**

What are the benefits of using Amazon Rekognition with image files?

**Can be used to transcode audio**

**Correct answer**

**Can be used to identify objects in an image**

**Can help with image compression**

**Can be used to resize images**

Overall explanation

Rekognition Image is a deep learning powered image recognition service that detects objects, scenes, and faces; extracts text; recognizes celebrities; and identifies inappropriate content in images. It also allows you to search and compare faces.

**CORRECT:** "Can be used to identify objects in an image" is the correct answer.

**INCORRECT:** "Can be used to resize images" is incorrect. You cannot use Rekognition to resize images.

**INCORRECT:** "Can be used to transcode audio" is incorrect. You should use the Elastic Transcoder service to transcode audio.

**INCORRECT:** "Can help with image compression" is incorrect. You cannot use Rekognition to compress images.

**References:**

<https://aws.amazon.com/rekognition/image-features/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/additional-aws-services/>

## Domain

AWS Machine Learning

### Question 36Skipped

AWS Direct Connect is used by a company that wants to establish connectivity across multiple AWS Regions using VPCs.

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

### Correct answer

#### AWS Transit Gateway

#### Amazon Route 53

#### AWS PrivateLink

#### Amazon Connect

Overall explanation

AWS Transit Gateway connects your Amazon Virtual Private Clouds (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.

As you expand globally, inter-Region peering connects AWS Transit Gateways together using the AWS global network. Your data is automatically encrypted and never travels over the public internet.

**CORRECT:** "AWS Transit Gateway" is the correct answer (as explained above.)

**INCORRECT:** "AWS PrivateLink" is incorrect as although AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, it doesn't do this across multiple regions.

**INCORRECT:** "Amazon Connect" is incorrect as Connect is a cloud-based telecommunications service providing managed cloud-based customer contact centers - and has nothing to do connecting VPCs.

**INCORRECT:** "Amazon Route 53" is incorrect. Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service and can also be used to register domain names.

### References:

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-networking-services/>

## Domain

AWS Networking & Content Delivery



### Question 37Skipped

How does Amazon EC2 Auto Scaling help with resiliency?

**By changing instance types to increase capacity**

**Correct answer**

**By launching and terminating instances as needed**

**By automating the failover of applications**

**By distributing connections to EC2 instances**

Overall explanation

Amazon EC2 Auto Scaling launches and terminates instances as demand changes. This helps with resiliency and high availability as it can also be set to ensure a minimum number of instances are always available.

**CORRECT:** "By launching and terminating instances as needed" is the correct answer.

**INCORRECT:** "By distributing connections to EC2 instances" is incorrect. Auto Scaling is not responsible for distributing connections to EC2 instances, that is a job for an Elastic Load Balancer (ELB).

**INCORRECT:** "By changing instance types to increase capacity" is incorrect. Auto Scaling does not change the instance type. You have to create a new launch configuration if you need to increase your instance size, this is not automatic.

**INCORRECT:** "By automating the failover of applications" is incorrect. Auto Scaling does not do application failover.

**References:**

<https://aws.amazon.com/ec2/autoscaling/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/auto-scaling-and-elastic-load-balancing/>

**Domain**

AWS Compute

### Question 38Skipped

Which of the following are advantages of the AWS Cloud? (Select TWO.)

**Correct selection**

**Launch globally in minutes.**

**Trade variable expenses for capital expenses.**

**Focus on managing hardware infrastructure.**

**Correct selection**

**High economies of scale.**

**Overprovision to ensure capacity.**

Overall explanation

Economies of scales refers to the fact that because AWS has a global customer base, they can afford to sell much cheaper to any one customer. This is a benefit of being on the cloud and the customer number keeps increasing, and the price keeps going down as a result.

Also as AWS have Regions placed all over the globe, there is a large degree of choice you have in where your applications are launched. In a traditional IT environment this would have been a big problem, and it would have been a logistical nightmare launching an application across multiple Regions.

**CORRECT:** "High economies of scale" is the correct answer (as explained above.)

**CORRECT:** "Launch globally in minutes" is also a correct answer (as explained above.)

**INCORRECT:** "Trade variable expenses for capital expenses" is incorrect as this is the opposite of what you gain from the cloud. You trade capital expenses for variable expenses.

**INCORRECT:** "Focus on managing hardware infrastructure" is incorrect. You do not have to manage hardware when you are using the cloud.

**INCORRECT:** "Overprovision to ensure capacity" is incorrect. Overprovisioning is not a good thing, and the advantage of the cloud is that you do not have to worry about physical hardware.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-computing-concepts/>

**Domain**

AWS Cloud Benefits

**Question 39**Skipped

Which AWS service provides on-demand downloads of AWS security and compliance reports?

**Amazon Inspector**

**AWS Directory Service**

**Correct answer**

**AWS Artifact**

**AWS Trusted Advisor**

Overall explanation

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

Reports available in AWS Artifact include 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.

**CORRECT:** "AWS Artifact" is the correct answer.

**INCORRECT:** "AWS Directory Service" is incorrect. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, is an AWS-managed directory service built on actual Microsoft Active Directory and powered by Windows Server 2012 R2.

**INCORRECT:** "AWS Trusted Advisor" is incorrect. AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices.

**INCORRECT:** "Amazon Inspector" is incorrect. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

**Domain**

AWS Security, Identity, & Compliance

**Question 40**Skipped

Which AWS service provides a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser, without needing to install any software or configure servers?

**Correct answer**

**AWS Cloud9**

**AWS CodeStar**

**AWS CodeBuild**

**Amazon WorkSpaces**

Overall explanation

AWS Cloud9 is the correct choice because it is a cloud-based integrated development environment (IDE) that allows developers to write, run, and debug their code using only a web browser. It eliminates the need to install software and configure servers, offering a seamless and convenient solution for developers.

**CORRECT:** "AWS Cloud" is the correct answer (as explained above.)

**INCORRECT:** "AWS CodeStar" is incorrect because, while it enables you to quickly develop, build, and deploy applications on AWS, it is not a service that provides a cloud-based IDE where you can write, run, and debug code directly from a web browser.

**INCORRECT:** "AWS CodeBuild" is incorrect because it is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. It does not offer a cloud-based IDE for writing, running, and debugging code.

**INCORRECT:** "Amazon WorkSpaces" is incorrect because, although it is a managed, secure Desktop-as-a-Service (DaaS) solution, it does not inherently provide a cloud-based IDE focused on coding, running, and debugging development projects directly in a browser.

**References:**

<https://aws.amazon.com/cloud9/>

**Domain**

AWS Cloud Architecture & Design

**Question 41Skipped**

You have been running an on-demand Amazon EC2 instance running Linux for 4hrs, 5 minutes and 6 seconds. How much time will you be billed for?

**4hrs**

**Correct answer**

**4hrs, 5mins, and 6 seconds**

**5hrs**

**4hrs, 6mins**

Overall explanation

On-demand, Reserved and Spot Amazon EC2 Linux instances are charged per second with a minimum charge of 1 minute. Therefore, as the minimum has been exceeded, exactly 4hrs, 5mins and 6 seconds will be charged.

**CORRECT:** "4hrs, 5mins, and 6 seconds" is the correct answer.

**INCORRECT:** "5hrs" is incorrect as explained above.

**INCORRECT:** "4hrs, 6mins" is incorrect as explained above.

**INCORRECT:** "4hrs" is incorrect as explained above.

**References:**

<https://aws.amazon.com/blogs/aws/new-per-second-billing-for-ec2-instances-and-ebs-volumes/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

## Domain

AWS Cost Management

### Question 42Skipped

A manager is planning to migrate applications to the AWS Cloud and needs to obtain AWS compliance reports.

How can these reports be generated?

**Download the reports from AWS Secrets Manager.**

**Correct answer**

**Download the reports from AWS Artifact.**

**Contact the AWS Compliance team.**

**Create a support ticket with AWS Support.**

Overall explanation

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

Reports available in AWS Artifact include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

**CORRECT:** "Download the reports from AWS Artifact" is the correct answer.

**INCORRECT:** "Contact the AWS Compliance team" is incorrect. You do not need to contact anyone at AWS, you can simply download this information.

**INCORRECT:** "Download the reports from AWS Secrets Manager" is incorrect. AWS Secrets Manager is used for storing secrets such as database authentication credentials or license codes. It is not used for storing compliance reports.

**INCORRECT:** "Create a support ticket with AWS Support" is incorrect. You do not need to contact anyone at AWS, you can simply download this information.

### References:

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

## Domain

AWS Security, Identity, & Compliance

**Question 43Skipped**

What is a specific benefit of an Enterprise Support plan?

**Included Technical Support Manager**

**Correct answer**

**Included Technical Account Manager**

**Included AWS Solutions Architect**

**Included Cloud Support Associate**

Overall explanation

Only the Enterprise Support plan gets a Technical Account Manager (TAM).

You do not get an AWS Solutions Architect with any plan.

Cloud Support Associates are provided in the Developer plan.

There's no such thing as a Technical Support Manager in the AWS support plans.

**CORRECT:** "Included Technical Account Manager" is the correct answer.

**INCORRECT:** "Included Technical Support Manager" is incorrect as explained above.

**INCORRECT:** "Included AWS Solutions Architect" is incorrect as explained above.

**INCORRECT:** "Included Cloud Support Associate" is incorrect as explained above.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

**Domain**

AWS Support

**Question 44Skipped**

Which of the below is an example of an architectural benefit of moving to the cloud?

**Proprietary hardware**

**Monolithic services**

**Correct answer**

**Elasticity**

**Vertical scalability**

Overall explanation

A key architectural benefit of moving to the cloud is that you get elasticity. This means your applications can scale as demand increases and scale back as demand decreases. This reduces cost as you only pay for what you use, when you need it.

**CORRECT:** "Elasticity" is the correct answer.

**INCORRECT:** "Monolithic services" is incorrect. Monolithic services are not a design pattern of the public cloud. Developers and architects prefer service oriented or micro-service architectures instead.

**INCORRECT:** "Proprietary hardware" is incorrect. You do not get to choose your hardware in AWS as the infrastructure on which your services run is managed and operated by AWS. So you cannot use proprietary hardware.

**INCORRECT:** "Vertical scalability" is incorrect. Vertical scalability is not unique to the cloud, nor is it something we aspire to as architects. Most of the time horizontal scalability is preferred and is something that the AWS cloud provides for many services.

#### References:

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

#### Save time with our AWS cheat sheets:

<https://digitalcloud.training/architecting-for-the-cloud/>

#### Domain

AWS Cloud Architecture & Design

#### Question 45Skipped

Which IAM entity is associated with an access key ID and secret access key?

**IAM Policy**

**IAM Role**

**IAM Group**

**Correct answer**

**IAM User**

Overall explanation

An access key ID and secret access key are used to sign programmatic requests to AWS. They are associated with an IAM user.

You cannot associate an access key ID and secret access key with an IAM Group, Role or Policy.

**CORRECT:** "IAM User" is the correct answer.

**INCORRECT:** "IAM Group" is incorrect as explained above.

**INCORRECT:** "IAM Role" is incorrect as explained above.

**INCORRECT:** "IAM Policy" is incorrect as explained above.

## References:

<https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys>

## Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-identity-and-access-management/>

## Domain

AWS Security, Identity, & Compliance

## Question 46Skipped

After an organization has migrated several servers into AWS, they are unsure as to what they must directly manage themselves.

Which cost is the company's direct responsibility?

**Cost of power for the AWS servers.**

**Correct answer**

**Cost of application software licenses.**

**Cost of the hardware infrastructure on AWS.**

**Cost of physical security for the AWS data center.**

Overall explanation

Licensing costs for applications still is part of the customer responsibility, as AWS only looks after the infrastructure which the applications are running on. The application layer itself is managed entirely by the customer - not AWS.

**CORRECT:** "Cost of application software licenses" is the correct answer (as explained above.)

**INCORRECT:** "Cost of the hardware infrastructure on AWS" is incorrect as this sits firmly on the AWS side of the shared responsibility model.

**INCORRECT:** "Cost of power for the AWS servers" is incorrect. AWS looks after the physical infrastructure, and customers have no input into how this is managed.

**INCORRECT:** "Cost of physical security for the AWS data center" is incorrect. Security *of* the cloud is an AWS responsibility and security *in* the cloud is a customer's responsibility.

## References:

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

## Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-shared-responsibility-model/>

## Domain

AWS Shared Responsibility Model

## Question 47Skipped



AWS Global Infrastructure consists of which of the following components?

**Correct answer**

**AWS Regions**

**AWS Organizations**

**Amazon LightSail**

**Amazon Alexa**

Overall explanation

AWS has the concept of a Region, which is a physical location around the world where we cluster Availability Zones. Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area. This is a key part of the AWS Global Infrastructure.

**CORRECT:** "AWS Regions" is the correct answer (as explained above.)

**INCORRECT:** "Amazon Alexa" is incorrect, is a virtual assistant technology, and is not part of the AWS Global infrastructure.

**INCORRECT:** "Amazon LightSail" is incorrect. Amazon LightSail is a virtual private server (VPS) provider and is the easiest way to get started with AWS for developers, small businesses, students, and other users who need a solution to build and host their applications on cloud. Amazon LightSail is not part of the AWS Global Infrastructure.

**INCORRECT:** "AWS Organizations" is incorrect. AWS Organizations is a way of managing multiple accounts under your root AWS account and is not a part of the AWS global infrastructure.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-global-infrastructure/>

**Domain**

AWS Cloud Architecture & Design

**Question 48Skipped**

A company plans to connect their on-premises data center to the AWS Cloud and requires consistent bandwidth and performance.

Which AWS service should the company choose?

**Amazon Connect**

**Amazon CloudFront**

**Correct answer**

## **AWS Direct Connect**

### **AWS VPN**

Overall 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.

**CORRECT:** "AWS Direct Connect" is the correct answer.

**INCORRECT:** "AWS VPN" is incorrect. A virtual private network (VPN) uses the internet and does not offer consistent network bandwidth or performance.

**INCORRECT:** "Amazon Connect" is incorrect. This is contact centre solution, not a networking technology.

**INCORRECT:** "Amazon CloudFront" is incorrect. CloudFront is a CDN used for caching content. It is not used for connecting from on-premises data centers to the AWS Cloud.

#### **References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-networking-services/>

### **Domain**

AWS Networking & Content Delivery

#### **Question 49Skipped**

Which service can be used to easily create multiple accounts?

**Correct answer**

**AWS Organizations**

**AWS IAM**

**Amazon Connect**

**AWS CloudFormation**

Overall explanation

AWS Organizations can be used for automating AWS account creation via the Organizations API.

**CORRECT:** "AWS Organizations" is the correct answer.

**INCORRECT:** "AWS IAM" is incorrect. You cannot use IAM for creating accounts.

**INCORRECT:** "AWS CloudFormation" is incorrect. You could theoretically use AWS CloudFormation to automate the account creation along with some scripting, but that is certainly not an easy way to reach this result.

**INCORRECT:** "Amazon Connect" is incorrect. Amazon Connect is a self-service, cloud-based contact center service that makes it easy for businesses to deliver better customer service at a lower cost.

**References:**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_create.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_create.html)

<https://aws.amazon.com/blogs/security/how-to-use-aws-organizations-to-automate-end-to-end-account-creation/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

**Domain**

AWS Security, Identity, & Compliance

**Question 50Skipped**

To gain greater discounts, which services can be reserved? (Select TWO.)

**Correct selection**

**Amazon RedShift**

**AWS Lambda**

**Amazon CloudWatch**

**Amazon S3**

**Correct selection**

**Amazon DynamoDB**

Overall explanation

Reservations provide you with greater discounts, up to 75%, by paying for capacity ahead of time. Some of the services you can reserve include: EC2, DynamoDB, ElastiCache, RDS, and RedShift.

**CORRECT:** "Amazon RedShift" is a correct answer.

**CORRECT:** "Amazon DynamoDB" is also a correct answer.

**INCORRECT:** "Amazon S3" is incorrect. You cannot reserve Amazon S3, you pay for what you use.

**INCORRECT:** "AWS Lambda" is incorrect. AWS Lambda is a service that provides functions and cannot be reserved.

**INCORRECT:** "Amazon CloudWatch" is incorrect. You cannot reserve Amazon CloudWatch which is a monitoring service.

**References:**

[https://d1.awsstatic.com/whitepapers/aws\\_pricing\\_overview.pdf](https://d1.awsstatic.com/whitepapers/aws_pricing_overview.pdf)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

**Domain**

AWS Cost Management

**Question 51Skipped**

How can an organization track resource inventory and configuration history for the purpose of security and regulatory compliance?

**Implement Amazon GuardDuty**

**Create an Amazon CloudTrail trail**

**Run a report with AWS Artifact**

**Correct answer**

**Configure AWS Config with the resource types**

Overall explanation

AWS Config is a fully-managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and regulatory compliance.

**CORRECT:** "Configure AWS Config with the resource types" is the correct answer.

**INCORRECT:** "Create an Amazon CloudTrail trail" is incorrect. CloudTrail tracks API activity. This means it is used to monitor who does what on Amazon. It does not provide a resource inventory or configuration history.

**INCORRECT:** "Implement Amazon GuardDuty" is incorrect. Amazon GuardDuty offers threat detection and continuous security monitoring for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

**INCORRECT:** "Run a report with AWS Artifact" is incorrect. AWS Artifact is used for obtaining on-demand security and compliance reports and select online agreements. This service provides access to AWS security and compliance reports such as SOC and PCI. You don't use Artifact to track your own resource inventory and configuration history.

**References:**

<https://docs.aws.amazon.com/config/latest/developerguide/gs-console.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-security-services/>

## Domain

AWS Security, Identity, & Compliance

### Question 52Skipped

What are the benefits of using reserved instances? (Select TWO.)

**High availability**

**Uses dedicated hardware**

**More flexibility**

**Correct selection**

**Reduced cost**

**Correct selection**

**Reserve capacity**

Overall explanation

With reserved instances you commit to a 1- or 3-year term and get a significant discount from the on-demand rate. You can also reserve capacity in an availability zone with reserved instances.

**CORRECT:** "Reduced cost" is a correct answer.

**CORRECT:** "Reserve capacity" is also a correct answer.

**INCORRECT:** "More flexibility" is incorrect. You don't get more flexibility with reserved instances. If you need flexibility on-demand is better but more costly.

**INCORRECT:** "Uses dedicated hardware" is incorrect. Reserved instances are different to dedicated instances. Dedicated instances and dedicated hosts use dedicated hardware but reserved instances do not.

**INCORRECT:** "High availability" is incorrect. You do not get high availability with reserved instances; this is a pricing model.

### References:

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-billing-and-pricing/>

## Domain

AWS Cost Management

### Question 53Skipped

Which AWS service or VPC component allows inbound traffic from the internet to access a VPC?

## **Virtual Private Gateway**

## **VPC Route Table**

## **NAT Gateway**

## **Correct answer**

## **Internet gateway**

### **Overall explanation**

An Internet gateway is attached to a VPC and allows inbound traffic from the internet to access the VPC. It is also used as a target in route tables for outbound internet traffic.

**CORRECT:** "Internet gateway" is the correct answer.

**INCORRECT:** "NAT Gateway" is incorrect. A NAT gateway is used for outbound internet access for instances running in a private subnet.

**INCORRECT:** "VPC Route Table" is incorrect. The route table is used within a VPC for directing traffic.

**INCORRECT:** "Virtual Private Gateway" is incorrect. A VGW is used for IPSec VPN connections to access a VPC.

## **References:**

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html)

## **Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-networking-services/>

## **Domain**

AWS Networking & Content Delivery

## **Question 54Skipped**

A company has a website that delivers static content from an Amazon S3 bucket to users from around the world. Which AWS service will deliver the content with low latency?

## **AWS Lambda**

## **Correct answer**

## **Amazon CloudFront**

## **AWS Elastic Beanstalk**

## **AWS Global Accelerator**

### **Overall explanation**

Amazon CloudFront is a content delivery network (CDN) and can use an Amazon S3 bucket configured as a static website as an origin for the content. CloudFront caches content globally. CloudFront reduces latency for global users by serving the requested content from a local cache.

**CORRECT:** "Amazon CloudFront" is the correct answer.

**INCORRECT:** "AWS Lambda" is incorrect. Lambda is a serverless compute service that runs code in response to triggers.

**INCORRECT:** "AWS Elastic Beanstalk" is incorrect. Elastic Beanstalk is a platform as a service offering that is used to run applications on a managed platform.

**INCORRECT:** "AWS Global Accelerator" is incorrect. Global Accelerator is used to direct traffic to application endpoints in different Regions using the AWS global network. It does not cache content and would not be used in front of an S3 bucket.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-content-delivery-and-dns-services/>

**Domain**

AWS Networking & Content Delivery

**Question 55Skipped**

Under the AWS shared responsibility model, which of the following is an example of customer responsibility in the AWS Cloud?

**Managing edge locations**

**Physical security**

**Correct answer**

**Firewall configuration**

**Global infrastructure**

Overall explanation

Firewall configuration is an example of “security in the cloud”. This is the customer’s responsibility, not an AWS responsibility.

**CORRECT:** "Firewall configuration" is the correct answer.

**INCORRECT:** "Managing edge locations" is incorrect. This is an example of “security of the cloud” and is an AWS responsibility.

**INCORRECT:** "Physical security" is incorrect. This is an example of “security of the cloud” and is an AWS responsibility.

**INCORRECT:** "Global infrastructure" is incorrect. This is an example of “security of the cloud” and is an AWS responsibility.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-shared-responsibility-model/>

## **Domain**

AWS Shared Responsibility Model

## **Question 56Skipped**

An ecommerce company is using Auto Scaling groups to manage a group of web servers running on Amazon EC2 and are additionally placed behind an Elastic Load balancer.

This architecture follows which AWS Well-Architected Framework best practice?

**Think parallel**

**Decouple infrastructure components**

**Correct answer**

**Design for failure**

**Secure the workload**

Overall explanation

Designing for failure is an important part of architecting for cloud workloads and the easiest way to do this when using Amazon EC2 instances is to put the within an Auto Scaling group and then place them behind an Elastic Load balancer.

An Auto Scaling group contains a collection of EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.

An Elastic load balancer distributes the load to each of these web servers in a distributed manner, allowing for scalable and flexible architecture.

The combination of both features of Amazon EC2 will enable high availability and is an example of designing for failure.

**CORRECT:** "Design for failure" is the correct answer (as explained above.)

**INCORRECT:** "Secure the workload" is incorrect as whilst there are some security benefits of using an Elastic Load Balancer, the main reason why we would use one is to attach it to an Auto Scaling group and to distribute traffic to the instances within it.

**INCORRECT:** "Decouple infrastructure components" is incorrect. Auto Scaling Groups and Elastic Load Balancers are typically not used to decouple architecture, and there are other services which are specifically designed to do this such as the Amazon Simple Queue Service (SQS) or AWS Lambda.

**INCORRECT:** "Think parallel" is incorrect. This is about experimenting with different architectures at the same time. There is no reference made in this question statement regarding



any other different architectures that are being compared to the setup of the Elastic Load Balancers and the Auto Scaling group.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/architecting-for-the-cloud/>

**Domain**

AWS Cloud Architecture & Design

**Question 57Skipped**

Which IAM entity can be used for assigning permissions to AWS services?

**IAM Policy**

**IAM Access Key ID and Secret Access Key**

**Correct answer**

**IAM Role**

**Security Token Service (STS)**

Overall explanation

With IAM Roles you can delegate permissions to resources for users and services without using permanent credentials (e.g. username and password). To do so you can create a role and assign an IAM policy to the role that has the permissions required.

**CORRECT:** "IAM Role" is the correct answer.

**INCORRECT:** "IAM Access Key ID and Secret Access Key" is incorrect. An access key ID and secret access key are assigned to IAM users and used for programmatic access using the API or CLI.

**INCORRECT:** "IAM Policy" is incorrect. An IAM policy is a policy document that is used to define permissions that can be applied to users, groups and roles. You don't apply the policy to the service, you apply it to the role. The role is then used to assign permissions to the AWS service.

**INCORRECT:** "Security Token Service (STS)" is incorrect. This service is used for gaining temporary security credentials.

**References:**

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_create\\_for-service.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-identity-and-access-management/>

**Domain**

AWS Security, Identity, & Compliance

### Question 58Skipped

Which AWS service or feature can be used to capture information about inbound and outbound IP traffic on network interfaces in a VPC?

**VPC Endpoint**

**AWS CloudTrail**

**Internet gateway**

**Correct answer**

**VPC Flow Logs**

Overall explanation

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Flow logs can help you with a number of tasks, such as:

- Diagnosing overly restrictive security group rules
- Monitoring the traffic that is reaching your instance
- Determining the direction of the traffic to and from the network interfaces

Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. You can create or delete flow logs without any risk of impact to network performance.

**CORRECT:** "VPC Flow Logs" is the correct answer.

**INCORRECT:** "Internet gateway" is incorrect. An internet gateway is attached to a VPC and used for sending and receiving data from the internet.

**INCORRECT:** "AWS CloudTrail" is incorrect. CloudTrail is used for auditing API activity.

**INCORRECT:** "VPC Endpoint" is incorrect. VPC endpoints are used for connecting to public AWS services using private IP addresses.

**References:**

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-networking-services/>

**Domain**

AWS Networking & Content Delivery

### Question 59Skipped

Which of the following is an advantage of AWS Cloud computing?

**Trade operational excellence for agility.**

**Trade security for elasticity.**

**Trade elasticity for performance.**

**Correct answer**

**Trade fixed expenses for variable expenses.**

Overall explanation

Trading capital expenditure for operational expenditure is an advantage of the cloud. When you are using the cloud, you do not have to worry about any upfront costs. The billing model is different in that you pay monthly instead of upfront.

**CORRECT:** "Trade fixed expenses for variable expenses" is the correct answer (as explained above.)

**INCORRECT:** "Trade security for elasticity" is incorrect. Security is job zero, and you should never choose elasticity over security.

**INCORRECT:** "Trade operational excellence for agility" is incorrect. You do not need to trade any of the advantages for any other advantages, operational excellence and elasticity are both advantages.

**INCORRECT:** "Trade elasticity for performance" is incorrect. You do not need to trade any of the advantages for any other advantages, elasticity and performance efficiency are both advantages.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-computing-concepts/>

**Domain**

AWS Cloud Benefits

**Question 60**Skipped

An IT company has deployed its infrastructure on the AWS cloud. There must be a database that supports reads with a latency of under a millisecond for critical applications.

Which AWS service will meet this requirement?

**Amazon RDS**

**AWS Glue**

**Correct answer**

**Amazon ElastiCache**

## Amazon EMR

Overall explanation

Amazon ElastiCache is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Built on open-source Redis or Memcached, ElastiCache works seamlessly with Redis or Memcached without any code changes.

**CORRECT:** "Amazon ElastiCache" is the correct answer (as explained above.)

**INCORRECT:** "Amazon EMR" is incorrect, as Amazon EMR is a cloud big data platform that can be queried using SQL. This is not a database solution designed to be used for single millisecond latency.

**INCORRECT:** "AWS Glue" is incorrect. AWS Glue is an event-driven, serverless computing platform. It is a computing service that runs code in response to events and automatically manages the computing resources required by that code. This does not store data natively and cannot handle rapid queries.

**INCORRECT:** "Amazon RDS" is incorrect. Whilst RDS is a database solution, it cannot handle single millisecond queries.

### References:

[www.aws.amazon.com/elasticache](http://www.aws.amazon.com/elasticache)

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-database-services/>

## Domain

AWS Database

### Question 61 Skipped

An organization is considering implementing a new workload in the AWS Cloud. However, the company first wants to forecast costs.

Which tool should the company use to estimate the cost of the workload?

**AWS Billing and Cost Management dashboard.**

**Cost Explorer.**

**Correct answer**

**AWS Pricing Calculator.**

**AWS Cost and Usage Report.**

Overall explanation

AWS Pricing Calculator is a web-based planning tool that you can use to create estimates for your AWS use cases. You can use it to model your solutions before building them, explore the AWS service price points, and review the calculations behind your estimates. You can use it to

help you plan how you spend, find cost saving opportunities, and make informed decisions when using Amazon Web Services.

**CORRECT:** "AWS Pricing Calculator" is the correct answer (as explained above.)

**INCORRECT:** "Cost Explorer" is incorrect. AWS Cost Explorer is a way to visualize your current spend across your accounts, and to forecast future spend. It does not help create estimates of how much money you would spend through building on the AWS platform.

**INCORRECT:** "AWS Billing and Cost Management dashboard" is incorrect, as you cannot calculate estimates for Cloud based workloads within the console.

**INCORRECT:** "AWS Cost and Usage Report" is incorrect. The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own and doesn't show costs for new workloads.

#### References:

<https://calculator.aws/#/>

#### Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-billing-and-pricing/>

#### Domain

AWS Cost Management

#### Question 62Skipped

A new web application is being developed by a company. Logging into the application through a social identity provider is a must have requirement for the company.

Which AWS service will meet these requirements?

**AWS Identity and Access Management (IAM).**

**AWS Single Sign-On.**

**AWS Directory Service.**

**Correct answer**

**Amazon Cognito.**

Overall explanation

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.

**CORRECT:** "Amazon Cognito" is the correct answer (as explained above.)

**INCORRECT:** "AWS Directory Service" is incorrect. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft Active Directory (AD), enables your directory-

aware workloads and AWS resources to use managed Active Directory (AD) in AWS. Although it is related to permissions and authorization, it does not

**INCORRECT:** "AWS Identity and Access Management (IAM)" is incorrect. IAM does not grant permissions to external third parties - only to internal AWS identity.

**INCORRECT:** "AWS Single Sign-On" is incorrect. AWS Single Sign-On (AWS SSO) is where you create, or connect, your workforce identities in AWS once and manage access centrally across your AWS organization. This does not allow users to login through a social identity provider.

#### References:

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

#### Save time with our AWS cheat sheets:

<https://digitalcloud.training/aws-security-services/>

#### Domain

AWS Security, Identity, & Compliance

#### Question 63Skipped

Under the AWS shared responsibility model, which actions are the responsibility of AWS?  
(Select TWO.)

#### Correct selection

**Scanning AWS service endpoints for vulnerabilities.**

**Configuring security group rules.**

**Enforcing application access restrictions.**

#### Correct selection

**Encrypting traffic on the AWS backbone between global and regional AWS facilities.**

**Enabling encryption on an Amazon S3 bucket.**

Overall explanation

Scanning endpoints owned by AWS sits firmly under AWS's responsibility, as you as an AWS user do not have access or insight into how AWS private endpoints work behind the scenes. This is abstracted away from the end user meaning it sits under the sole responsibility of AWS. As for encrypting traffic on the AWS backbone, as the lines and the network is solely owned and operated by AWS, it is AWS's responsibility to maintain the security of it. This sits under security *of* the cloud vs *in* the cloud.

**CORRECT:** "Scanning AWS service endpoints for vulnerabilities" is the correct answer (as explained above.)

**CORRECT:** "Encrypting traffic on the AWS backbone between global and regional AWS facilities" is also a correct answer (as explained above.)

**INCORRECT:** "Enabling encryption on an Amazon S3 bucket" is incorrect; this sits firmly under the customer responsibility under the AWS shared responsibility model.

**INCORRECT:** "Configuring security group rules" is incorrect as you as the AWS customer configure security group rules depending on how your application is going to function.

**INCORRECT:** "Enforcing application access restrictions" is incorrect as AWS has no insight into the application which you build upon AWS, only the infrastructure of which it is hosted upon.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-shared-responsibility-model/>

**Domain**

AWS Shared Responsibility Model

**Question 64Skipped**

What is a benefit of moving an on-premises database to Amazon Relational Database Service (RDS)?

**There is no database administration required**

**You can scale vertically without downtime**

**Correct answer**

**There is no need to manage operating systems**

**You can run any database engine**

Overall explanation

With Amazon RDS, which is a managed service, you do not need to manage operating systems. This reduces operational costs.

**CORRECT:** "There is no need to manage operating systems" is the correct answer.

**INCORRECT:** "You can scale vertically without downtime" is incorrect. You cannot scale vertically without downtime. When scaling with RDS you must change the instance type, and this requires a short period of downtime while the instances' operating system reboots.

**INCORRECT:** "There is no database administration required" is incorrect. There is still database administration required in the cloud. You don't manage the underlying operating system but still need to manage your own tables and data within the DB.

**INCORRECT:** "You can run any database engine" is incorrect. You cannot run any database engine with RDS. The options are MySQL, Microsoft SQL, MariaDB, Oracle, PostgreSQL and Aurora.

**References:**

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-database-services/>

## Domain

AWS Database

### Question 65Skipped

It is important for users to have access to as many resources as they need. Also, the user needs the ability to scale up and down quickly.

These capabilities are described by which AWS Cloud benefit?

### Correct answer

**Elasticity**

**Reliability**

**Economy of scale**

**Pay-as-you-go pricing**

Overall explanation

Elasticity is the ability to acquire resources as you need them and release resources when you no longer need them. This would allow users to scale up and down quickly.

**CORRECT:** "Elasticity" is the correct answer (as explained above.)

**INCORRECT:** "Reliability" is incorrect. Reliability is the ability of a workload to perform its intended function correctly and consistently when it's expected to.

**INCORRECT:** "Economy of scale" incorrect. This refers to the fact that because there is a large AWS customer base, every individual AWS user pays much less on aggregate.

**INCORRECT:** "Pay-as-you-go pricing" is incorrect as this refers to the CAPEX vs OPEX model and does not have anything to do with scalability.

### References:

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

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/aws-cloud-computing-concepts/>

## Domain

AWS Cloud Benefits